THIS FILE IS MADE AVAILABLE THROUGH THE DECLASSIFICATION EFFORTS AND RESEARCH OF:

THE BLACK VAULT

THE BLACK VAULT IS THE LARGEST ONLINE FREEDOM OF INFORMATION ACT / GOVERNMENT RECORD CLEARING HOUSE IN THE WORLD. THE RESEARCH EFFORTS HERE ARE RESPONSIBLE FOR THE DECLASSIFICATION OF THOUSANDS OF DOCUMENTS THROUGHOUT THE U.S. GOVERNMENT, AND ALL CAN BE DOWNLOADED BY VISITING:

HTTP://WWW.BLACKVAULT.COM

YOU ARE ENCOURAGED TO FORWARD THIS DOCUMENT TO YOUR FRIENDS, BUT PLEASE KEEP THIS IDENTIFYING IMAGE AT THE TOP OF THE .PDF SO OTHERS CAN DOWNLOAD MORE!

United States Department of State

Washington, D.C. 20520

Mr. John Greenewald, Jr.
[redacted]

RE: Freedom of Information Act Request No. 200905723

Dear Mr. Greenewald:

Reference is made to your July 10, 2009, Freedom of Information Act request to the Department of State concerning cyber attacks. The Bureau of Diplomatic Security has searched its system of records and has located 22 documents (001-022) relevant to your request.

Information has been withheld from these documents based on the provisions of 5 USC 552 (b)(7)(C) and (b)(7)(E). An explanation of exemptions is enclosed.

Under the Department's regulations, you may appeal any denial of information to the Department's Appeals Review Panel. Appeals should be sent to: Chairman, Appeals Review Panel, c/o Appeals Officer, A/GIS/IPS/PP/LC, SA-2, Department of State, Room 8100, Washington, DC 20522-8100. A copy of the Department's Appeals Procedures is enclosed.

If you have any questions regarding a particular aspect of this case, you should contact the Office of Information Programs and Services, (A/GIS/IPS), Department of State, SA-2, Washington, DC 20522-8100. In any communication, please refer to the case number.

Sincerely,

William R. Terrini
Deputy Executive Director
Bureau of Diplomatic Security

Enclosures:
Explanation of Exemptions
Appeals Procedures
Documents

63934 Federal Register/Vol. 69, No 212
Rules and Regulations

Subpart F – Appeal Procedures

§ 171.52 Appeal of denial of access to, declassification of, amendment of, accounting of disclosures of, or challenge to classification of records.

(a) *Right of administrative appeal.* Except for records that have been reviewed and withheld within the past two years or are the subject of litigation, any requester whose request for access to records, declassification of records, amendment of records, accounting of disclosures of records, or any authorized holder of classified information whose classification challenge has been denied, has a right to appeal the denial to the Department's Appeals Review Panel. This appeal right includes the right to appeal the determination by the Department that no records responsive to an access request exist in Department files. Privacy Act appeals may be made only by the individual to whom the records pertain.

(b) *Form of appeal.* There is no required form for an appeal. However, it is essential that the appeal contain a clear statement of the decision or determination by the Department being appealed. When possible, the appeal should include argumentation and documentation to support the appeal and to contest the bases for denial cited by the Department. The appeal should be sent to: Chairman, Appeals Review Panel, c/o Appeals Officer, A/RPS/IPS/PP/LC, U.S. Department of State, SA-2, Room 8100, Washington, DC 20522-8100.

(c) *Time limits.* The appeal should be received within 60 days of the date of receipt by the requester of the Department's denial. The time limit for response to an appeal begins to run on the day that the appeal is received. The time limit (excluding Saturdays, Sundays, and legal public holidays) for agency decision on an administrative appeal is 20 days under the FOIA (which may be extended for up to an additional 10 days in unusual circumstances) and 30 days under the Privacy Act (which the Panel may extend an additional 30 days for good cause shown). The Panel shall decide mandatory declassification review appeals as promptly as possible.

(d) *Notification to appellant.* The Chairman of the Appeals Review Panel shall notify the appellant in writing of the Panel's decision on the appeal. When the decision is to uphold the denial, the Chairman shall include in his notification the reasons therefore. The appellant shall be advised that the decision of the Panel represents the final decision of the Department and of the right to seek judicial review of the Panel's decision, when applicable. In mandatory declassification review appeals, the Panel shall advise the requester of the right to appeal the decision to the Interagency Security Classification Appeals Panel under § 3.5(d) of E.O. 12958.

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552 (FOIA):

(b) (1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;

(b)(2) related solely to the internal personnel rules and practices of an agency;

(b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information, (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of aright to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(b)(9) geological and geophysical information and data, including maps, concerning wells

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a (PA):

(b) No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains,

(d)(5) information compiled in reasonable anticipation of a civil action proceeding.

General Exemptions:

(j)(1) applies to CIA records and information provided by foreign governments;

(j)(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, except records of arrest.

Specific Exemptions:

(k)(1) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;

(k)(2) investigatory material compiled for law enforcement purposes, other than criminal which did not result in loss of a right, benefit or privilege under Federal law, or which would identify a source under an express promise of confidentiality, or, prior to the effective date of this section, under an implied promise of confidentiality;

(k)(3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of Title 18;

(k)(4) required by statute to be maintained and used solely as statistical records;

(k)(5) investigatory material compiled solely for the purpose of determining suit ability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, the disclosure of such material would reveal the identity of a source under an express promise of confidentiality, or, prior to the effective date of this section, under an implied promise of confidentiality;

(k)(6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the testing or examination process; or

(k)(7) evaluation material used to determine potential for promotion in the armed services, the disclosure of such material would reveal the identity of a source under an express promise of confidentiality, or, prior to the effective date of this section, under an implied promise of confidentiality.

b7E T b7E

b7C OOL b7C

DECLASSIFIED

- CIRT -

COMPUTER INCIDENT RESPONSE TEAM

MONTHLY REPORT

June 2009

BUREAU OF DIPLOMATIC SECURITY

Office of Computer Security
Monitoring and Incident Response Division – DS/CS/MIR
1801 North Lynn Street, 15th Floor
Arlington, VA 22209

Computer Incident Response Team (CIRT)

DECLASSIFIED

The Computer Incident Response Team (CIRT) is federally mandated and was established in 1999 as the central point for the reporting of computer security incidents that occur on the Department of State networks. To report a computer security event, contact your ISSO or the CIRT [redacted] CIRT may also be reached via email at CIRT@state.gov (unclassified) or [redacted](classified).

b7C

b7E

For more information on the following ~~events and/or CIRT~~ activity, please contact DS/CS/MIRD Chief Bobby Miller [redacted] Please visit our Web site at [redacted]

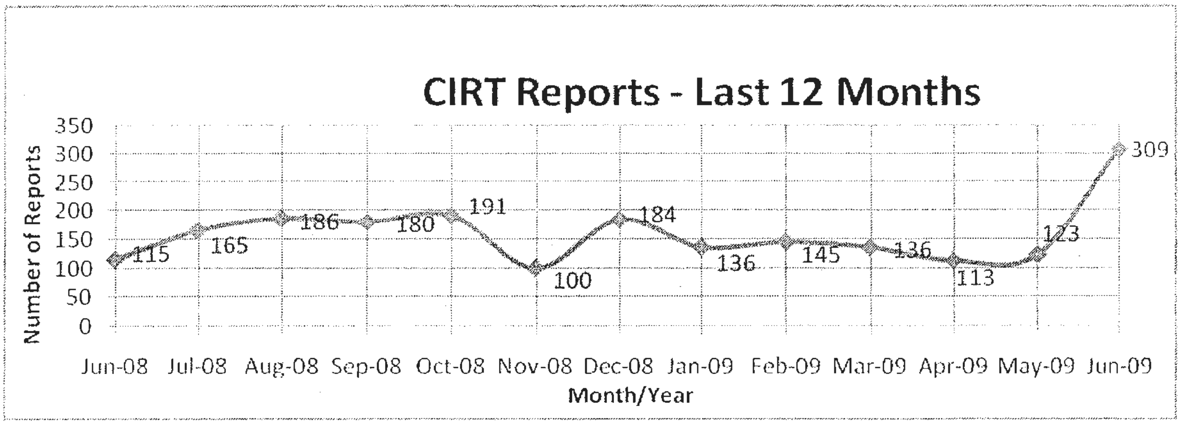
1.0 OVERVIEW OF MONTHLY ACTIVITY

RADAR Ticket Summary	Number of Tickets
1. Open Tickets from previous month(s)	35
2. New Tickets opened this month	285
3. Total of Open Tickets (1+2)	320
4. Total number of Closed Tickets	309
5. Open tickets carried over to next month (3-4)	11

Monthly Overview of CIRT Activity

US-CERT Events	Number of Events
1. Events Generated by US-CERT Reports	22
2. Events Reported to US-CERT	(12 PII, 10 Cyber)

2.0 HISTORICAL ONE YEAR OVERVIEW OF CIRT ACTIVITY



DECLASSIFIED

3.0 REPORTING GROUPS/SOURCES

The majority of computer security reports received by the CIRT come from the following sources:

1) Network Security Monitoring Operations
2) Information System Security Officers (ISSOs) and/or DoS users
3) US-CERT
4) Cyber Threat Analysis Division (CTAD)
5) Other Federal Agencies

4.0 CONFIRMED EVENT TYPES OF CLOSED TICKETS

The following table summarizes confirmed event types of the tickets escalated to the CIRT and closed during the reported period.

Count	Confirmed Event Type	Description
47	Non-event	**Non-event:** The ticket was not considered a computer security issue; no remediation was required.
120	Malicious Code directed toward internal machine	**Malicious Code directed toward internal machine:** Analysis of network traffic and/or evidence on the machine confirmed malicious code was directed at an internal machine.
27	Email - Phishing	**Email - Phishing:** The CIRT received a report of email received by Department user(s) that attempted to gain personal information.
8	Operational/Approved Activity	**Operational/Approved Activity:** The CIRT received confirmation that the activity was operational and/or approved.
25	Information Security Issue (violation or infraction)	**Information Security Issue (violation or infraction):** All information security issues (improper handling of classified data) are referred to DS/SI/APD.
2	Unauthorized Hardware connected to DOS network	**Unauthorized Hardware connected to DOS network:** Unauthorized hardware was confirmed to have been connected to the Department's network (laptops, USB drives, cameras, etc…).
28	Email - Malicious Payload (Code, Attachment, Link)	**Email - Malicious Payload (Code, Attachment, Link):** An email with a malicious payload was sent to a Department user.

DECLASSIFIED

Count	Confirmed Event Type	Description
2	Compromised System on DOS network	**Compromised System on DOS network:** Unauthorized computers have been detected connected to network.
3	Suspicious/Abnormal traffic	**Suspicious/Abnormal traffic:** Analysis indicated definite suspicious/abnormal traffic to or from an internal machine without a conclusive cause. Depending on the potential threat, the ISSO may be advised to re-image the hard drive.
2	Machine Patched or Not Vulnerable to Exploit	**Machine Patched or Not Vulnerable to Exploit:** CIRT detected a large number of e-mail messages with PDF attachments attempting to connect to an external IP address
4	Unauthorized Software Installed on DOS machine	**Unauthorized Software Installed on DOS machine:** Unauthorized software was confirmed to have been installed.
19	Virus/Worm on internal machine	**Virus/Worm on Internal Machine:** CIRT has received reports or detected through monitoring devices possible virus on DoS internal machines.
1	Undetermined/Unknown	**Undetermined/Unknown:** The definitive cause of the event/IDS alert could not be positively determined.
3	Violation of Computer Security Policy by DOS user (CSIP issue)	**Violation of Computer Security Policy:** Final analysis indicates that compliance with computer security policies was not met. These events are referred to the appropriate entities for follow up.
2	Scan Activity (internal source with no notification to CIRT)	**Scan Activity:** Authorized Scanning activity was conducted but CIRT was not notified of the activity in advance
19	Spyware/Trojan on internal machine	**Spyware/Trojan on internal machine:** Spyware or a Trojan was confirmed to have been on a machine. The anti-virus software may quarantine and delete the code or the ISSO will reformat and re-image the hard drive.
1	Configuration Issue (software or hardware on DOS network)	**Configuration Issue (software or hardware on DOS network.** [redacted]

b 7E

DECLASSIFIED

DECLASSIFIED

5.0 INCIDENTS AND EVENTS OF NOTE

Reported events are escalated to incidents due to their potential threat to the network and/or their significance to the Department. Additional details can be obtained by contacting the CIRT.

There were multiple events of note during the reporting period, which are summarized in the table below:

Number	Description
Multiple	CIRT continues to detect increasing numbers of spear phishing events targeting users within the Department of State and we are seeing more frequent instances of malicious code embedded in [redacted] attachments in e-mail messages. These attacks are becoming more targeted. *Analyst Note: Due to the pervasiveness of the [redacted] as a legitimate document format, IT Leadership should consider strategies to reduce the time required to deploy patches to correct [redacted] vulnerabilities throughout the enterprise. CIRT also advises additional consideration for deployment of [redacted] and workstation filtering. CIRT also advises to add to Top 5 Challenges.*

b7E

6.0 CIRT LISTSERV ANNOUNCEMENTS

CIRT posted **two (2) announcements** to the CIRT ListServ distribution list during the monthly reporting period. The list is used to rapidly disseminate information to anyone with an interest in computer security within the Department. For more information on the CIRT ListServ please visit http://lmlist.state.gov/archives/cirt.html. The subject lines of notifications CIRT posted are listed below:

- CIRT Monthly Report
- CIRT Advisory – Malicious E-mail Warning

7.0 CIRT DATA CALLS

CIRT received **no (0) requests** for information during the reporting period.

8.0 OTHER CIRT HIGHLIGHTS

- **Joint Agency Cybersecurity Knowledge Exchange (JACKE):** Representatives from CIRT attended the Joint Agency Cyber Knowledge Exchange (JACKE) at the Department of Commerce. JACKE meetings are sponsored by US-CERT and are

DECLASSIFIED

focused on coordinating, sharing information and responding to intrusion sets at the Secret level and occur on a weekly basis. Information obtained from the meeting has allowed CIRT to take protective actions for OpenNet based on the information provided.

- **Daily CIRT Briefings:** The CIRT conducts daily 9 A.M. meetings with appropriate stakeholders to discuss reported events and any other issues. These meetings are held in SA-20 in the 15th Floor Monitoring and Incident Response Conference Room.
- **Cyber Command Center**
  - CIRT Operations Manager coordinated a site visit on June 17 to the Army National Guard operations center to begin planning layout for the new Cyber Command Center.

DECLASSIFIED

002

H

Cyber Security Brief

United States Department of State
Bureau of Diplomatic Security
as of June 2, 2009-1400 EST

June 3, 2009

Current DoS Cyber Threat Condition

GUARDED

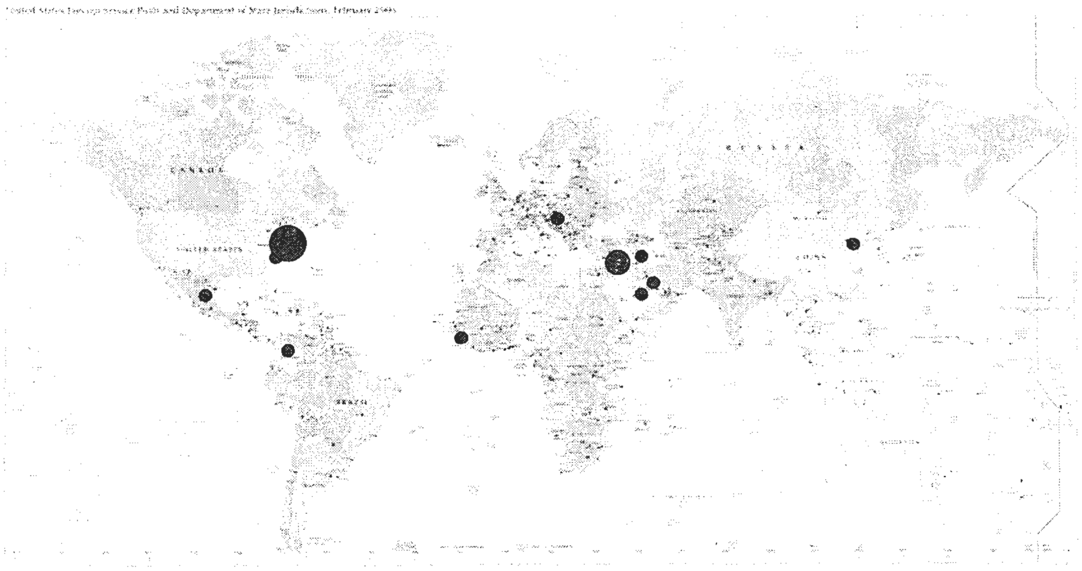
No change from last reported condition

Nuisance cyber attack activity is present

Executive Summary

1. CIRT
   - Nothing substantial to report
2. Cyber Threat Analysis Division
   - Daily Read File: (U) Hackers Develop New Method of Hiding from Researchers
3. Personally identifiable information (PII) loss reported
   - One passport application missing
4. Classified spillage incident
   - E-mail containing classified information sent to unclassified DoS system

Geographic Distribution of Computer Incident Response Team (CIRT) Events



Legend: • *1 event* ● *2 events* ⬤ *3+ events*

DECLASSIFIED

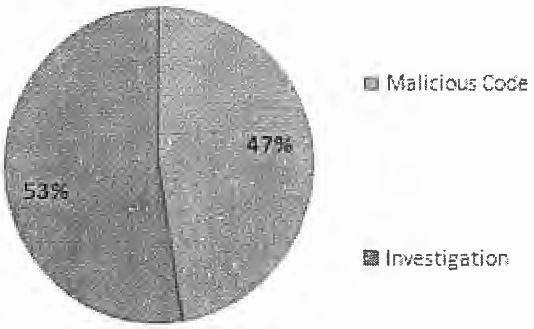
E

b7E

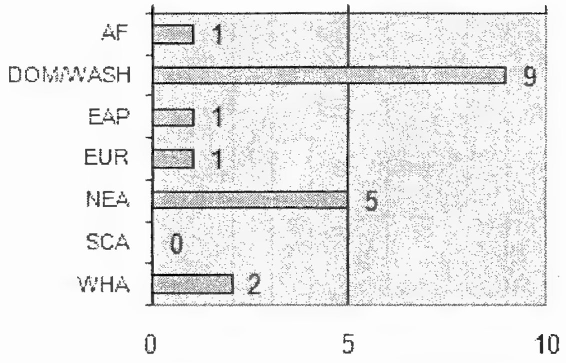
***Open CIRT Events*:** 15

***Closed CIRT Events*:** 4

CIRT Events by US-CERT Category



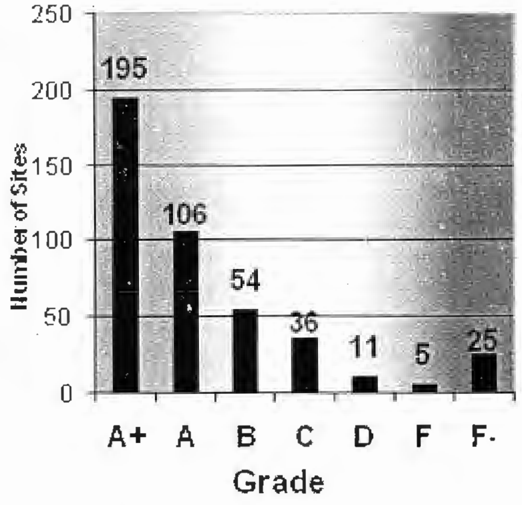
CIRT Events by Bureau



Firewall Block Request Summary

- Nothing substantial to report

Enterprise Risk Score Grade Distribution



Computer Incident Response Team (CIRT)

- Nothing substantial to report

Personally identifiable information (PII) loss reported

- One passport application electronically transmitted from the US Treasury Department [redacted] could not be physically located at the agency. This event has been referred to US-CERT and the Privacy Team.

b7E

b7E

Classified spillage incident(s) reported to CIRT and referred to DS/IS/APD

- An e-mail attachment containing unmarked classified material was sent to an unclassified DoS system. The e-mail was sent from a U.S. government entity outside the Department of State. DS/ADP and appropriate contacts have been notified of this incident.

US-CERT Coordination

- Nothing substantial to report

Compliance & Vulnerability Scanning

- *See Appendix B for statistics*

Cyber Threat Analysis Division (CTAD)

DAILY READ FILE: (U) Hackers Develop New Method of Hiding from Researchers

(U) Key Highlights:

- *Cybercrime forum registrants have developed a new technique to avoid being tracked*
-
-
- *Researchers can overcome this obstacle*

b6

(U) Source Paragraph: "In addition to online hacking, many hackers often

b7F

***Virus Incident Response Team (VIRT) Statistics** (as of midnight eastern time)*

Spam Blocked at Perimeter:	**Virus Blocked at Perimeter:**
Previous day: **1,194,544**	Previous day:**133**
Month to date - June: **1,194,544**	Month to date - June: **133**
Year to date for 2009: **250,985,641**	Year to date for 2009: **20,248**

Cyber Security News Headlines

10 Key Tasks of the Cybersecurity Czar *[Source: govinfosecurity.com]*

Obama: Battling Cyber-Turf Wars *[Source: newsfactor.com]*

DECLASSIFIED

b7E

DECLASSIFIED

Appendix A –CIRT Event Summaries

Legend:	*Open Events: 15*	*Closed Events: 4*

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Compromised System on a DoS network

Ticket Number: [redacted]	**Location** [redacted]
Date and Time Ticket Created: 05/29/2009 1258 GMT	**Affected Bureau:** EUR

b7E

Event Description
US-CERT notified CIRT about suspicious traffic.

Current Status
2 Jun: CIRT received a response from the ISSO that the incident is in the process of being researched.

Status History
29 May: CIRT provided the ISSO remediation instructions via Classified e-mail.
1 Jun: CIRT requested a status update from the ISSO via e-mail.

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: E-mail - Phishing

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 05/21/2009 1656 GMT	**Affected Bureau:** NEA

b7E

Event Description
An employee notified CIRT that he had received a suspicious e-mail message with a PDF attachment.

Current Status
2 Jun: CIRT sent another expedited request to the CISO and proper contacts. CIRT will telephone the ISSO during Post's operating hours to request an update.

DECLASSIFIED

b7E

Status History

22 May: CIRT requested that the ISSO determine if the message was opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
26 May: CIRT requested a status update from the ISSO via e-mail.
27 May: CIRT requested a status update from the ISSO via e-mail.
28 May: CIRT called the ISSO requesting a status update.
29 May: CIRT requested a status update from the ISO and IPO via e-mail.
1 Jun: CIRT expedited this ticket to the CISO for further assistance.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 05/21/2009 1657 GMT	**Affected Bureau:** EAP

b7E

Event Description

An employee notified CIRT that he had received a suspicious e-mail message with a PDF attachment.

Current Status

2 Jun: CIRT sent another expedited request to the CISO and proper contacts. . CIRT will telephone the ISSO during Post's operating hours to request an update.

Status History

22 May: CIRT requested that the ISSO determine if the message was opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
24 May: CIRT requested a status update from the ISSO via e-mail.
26 May: CIRT requested a status update from the ISSO via e-mail.
27 May: CIRT requested a status update from the ISSO via e-mail.
28 May: CIRT called the ISSO requesting a status update.
29 May: CIRT was informed that the Post was closed due to a local holiday.
1 Jun: CIRT expedited this ticket to the CISO for further assistance.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 05/27/2009 1615 GMT	**Affected Bureau:** DOM

b7E

Event Description

CIRT was notified by US-CERT of spear phishing e-mail attempts targeting DoS personnel.

Current Status

2 Jun: CIRT requested a status update from the IT Service Center via e-mail.

Status History

28 May: CIRT requested that the IT Service Center direct the ISSO to determine if the user had received the suspicious message and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
29 May: CIRT requested a status update from the IT Service Center via e-mail and phone.
1 Jun: CIRT received an update from the ISSO that this event is in the process of being researched and remediated.

E
b7E

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 05/27/2009 1742 GMT	**Affected Bureau:** DOM

b7E

Event Description
CIRT was notified by US-CERT of spear phishing e-mail attempts targeting DoS personnel.

Current Status
2 Jun: CIRT requested a status update from the IT Service Center via e-mail.

Status History
28 May: CIRT requested that the IT Service Center direct the ISSO to determine if the user had received the suspicious message and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
29 May: CIRT requested a status update from the IT Service Center via e-mail and phone.
1 Jun: CIRT requested a status update from the IT Service Center via e-mail.

b7E

Ticket Number: [redacted]	**Location** [redacted]
Date and Time Ticket Created: 05/28/2009 1524 GMT	**Affected Bureau:** DOM

Event Description
CIRT was notified by US-CERT of spear phishing e-mail attempts targeting DoS personnel.

Current Status
2 Jun: CIRT requested a status update from the IT Service Center via telephone. The ISSO is currently researching the incident and will contact CIRT with an update at his next opportunity.

Status History
28 May: CIRT requested that the IT Service Center direct the ISSO to determine if the user had received the suspicious message and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
29 May: CIRT requested a status update from the IT Service Center via e-mail and phone.
1 Jun: CIRT requested a status update from the IT Service Center via e-mail.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 05/27/2009 1853 GMT	**Affected Bureau:** DOM

Event Description
CIRT was notified by US-CERT of spear phishing e-mail attempts targeting DoS personnel.

Current Status
2 Jun: CIRT requested a status update from the IT Service Center via e-mail.

Status History
28 May: CIRT requested that the IT Service Center direct the ISSO to determine if the user

b7E

had received the suspicious message and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
29 May: CIRT requested a status update from the IT Service Center via e-mail and phone.
1 Jun: CIRT requested a status update from the IT Service Center via e-mail.

b-b7E

Ticket Number: [redacted]	**Location** [redacted]
Date and Time Ticket Created: 05/27/2009 1915 GMT	**Affected Bureau:** DOM

Event Description
CIRT was notified by US-CERT of spear phishing e-mail attempts targeting DoS personnel.

Current Status
2 Jun: CIRT sent a request to the IT Service Center that the remediation steps addressed in the initial request must be implemented.

Status History
28 May: CIRT requested that the IT Service Center direct the ISSO to determine if the user had received the suspicious message and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
29 May: CIRT requested a status update from the IT Service Center via e-mail and phone.
1 Jun: The IT Service Center informed CIRT that remedial actions have taken place. CIRT requested that the IT Service Center provide further details regarding the remedial actions.

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: E-mail - Phishing

b7E

Ticket Number: [redacted]	**Location** [redacted]
Date and Time Ticket Created: 05/21/2009 1332 GMT	**Affected Bureau:** NEA

Event Description
CIRT received information from US-CERT of possible malware being directed at a DoS workstation.

Current Status
2 Jun: CIRT received updated ISSO contact information and resent the initial notification to the correct contact.

Status History
21 May: CIRT requested that the ISSO search for specific files and reimage the operating system if the files are found.
22 May: CIRT sent a status request email to the ISSO found.
26 May: CIRT requested a status update from the ISSO via e-mail.
27 May: CIRT called and left a voicemail for the ISSO to provide a status update.
28 May: CIRT requested a status update from the ISSO via e-mail and phone.
29 May: CIRT requested a status update from the ISO and IPO via e-mail.

b7E

1 Jun: CIRT expedited this ticket to the CISO for further assistance.

DECLASSIFIED

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Malicious Code directed towards an internal machine

b7E

Ticket Number [redacted]	**Location** [redacted]
Date and Time Ticket Created: 05/21/2009 1845 GMT	**Affected Bureau:** NEA

Event Description
CIRT detected a malicious code exposure attempting [redacted]

b7E

Current Status
2 Jun: **CIRT received an update from the ISSO that remediation actions are being completed.**

Status History
21 May: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.
22 May: CIRT requested a status update from the ISSO via e-mail.
26 May: CIRT requested a status update from the ISSO via e-mail.
27 May: CIRT requested a status update from the ISSO via e-mail.
28 May: CIRT requested a status update from the ISSO via e-mail.
29 May: CIRT requested a status update from the ISO and IPO via e-mail.
1 Jun: CIRT requested a status update from the ISSO via telephone. The ISSO is in the process of remediating and will provide further details shortly.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/01/2009 1125 GMT	**Affected Bureau:** AF

Event Description
CIRT detected the download of an executable onto a DoS workstation.

Current Status
2 Jun: **CIRT requested a status update from the ISSO via e-mail.**

Status History
1 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

Ticket Number: [redacted]	**Location:** [redacted]

DECLASSIFIED

b7E

DECLASSIFIED

Date and Time Ticket Created: 06/01/2009 1156 GMT	**Affected Bureau:** WHA
Event Description CIRT detected the download of an executable onto a DoS workstation.	
Current Status **2 Jun: CIRT requested a status update from the ISSO via e-mail.**	
Status History **1 Jun:** CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.	

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/01/2009 1503 GMT	**Affected Bureau:** DOM
Event Description US-CERT notified CIRT concerning suspicious traffic.	
Current Status **2 Jun: CIRT requested that the ISSO determine if the suspicious message had been received and if it had been opened or deleted. If the message was opened, CIRT requested that the ISSO remove the workstation from the network and await further instructions.**	
Status History **N/A - New Event**	

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Suspicious/Abnormal traffic

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/01/2009 1325 GMT	**Affected Bureau:** DOM
Event Description US-CERT notified CIRT of suspicious [redacted] that may represent a security issue.	
Current Status **2 Jun: CIRT is awaiting the results of an antivirus scan.**	
Status History **1 Jun:** The ISSO informed CIRT that [redacted]	

b7E

b7E

DECLASSIFIED

b2

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Violation of Computer Security Policy by a DoS user (CSIP issue)

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 05/27/2009 0919 GMT	**Affected Bureau:** NEA

b2

Event Description

The ISSO informed CIRT of a potential violation of computer security. Additional details are available on CLAN.

Current Status

2 Jun: CIRT requested a status update from the ISSO via e-mail.

Status History

27 May: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.
28 May: CIRT requested a status update from the ISSO via e-mail.
29 May: CIRT requested a status update from the ISSO via e-mail.
31 May: CIRT requested a status update from the ISSO via e-mail.
1 Jun: CIRT received an update from the ISSO that this event is in the process of remediation.

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Malicious Code directed towards an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/01/2009 0743 GMT	**Affected Bureau:** WHA

b2

Event Description

CIRT detected a DoS workstation accessing a suspicious website known to host malicious [redacted] An executable was downloaded from the website.

7E

Final Action

2 Jun: The ISSO reported that the registry change was identified and the PC was removed from the network. The PC will be re-imaged prior to being replaced on the network.

Status History

1 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Information Security Issue (Violation or infraction)

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/01/2009 1512 GMT	**Affected Bureau:** DOM
Event Description Personally Identifiable Information (PII) may have been breached or disclosed to unauthorized third parties.	
Final Action **2 Jun: This event has been referred to US-CERT and the Privacy Team.**	
Status History **N/A - New Event**	

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Non-event

Ticket Number [redacted]	**Location** [redacted]
Date and Time Ticket Created: 06/01/2009 1825 GMT	**Affected Bureau:** DOM
Event Description CIRT was notified of a Classified Spillage.	
Final Action **2 Jun: DS/ADP and appropriate contacts have been notified of the possible classified spillage.**	
Status History **N/A - New Event**	

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Scan Activity (internal source with no notification to CIRT)

Ticket Number [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/02/2009 1152 GMT	**Affected Bureau:** NEA

Event Description

RCSO NEA requested assistance with suspicious activity concerning the servers in Riyadh.

UNCLASSIFIED

Final Action

2 Jun: CIRT received confirmation from the Scanning Team that they were performing routine scanning.

Status History

N/A - New Event

L75

DECLASSIFIED

Appendix B – Compliance & Vulnerability Scanning Statistics

Vulnerability Totals:

Total Critical Vulnerabilities: 9,347

Total High Vulnerabilities: 489,838

Top 10 Critical Vulnerabilities

7E

Vulnerability	CVSS Score	Count
[redacted]	10.00	1565
[redacted]	10.00	1163
[redacted]	10.00	1120
[redacted]	10.00	810
[redacted]	10.00	509
[redacted]	10.00	508
[redacted]	10.00	421
[redacted]	10.00	394
[redacted]	10.00	311
[redacted]	10.00	218

Top 10 High Vulnerabilities

7E

Vulnerability	CVSS Score	Count
[redacted]	9.30	22430
[redacted]	7.00	21831
[redacted]	9.30	20298
[redacted]	9.30	20259
[redacted]	9.30	20060
[redacted]	9.30	19499
[redacted]	9.30	11785
[redacted]	9.30	11328
[redacted]	9.30	11288

E

Cumulative Security Update [redacted]	9.30	10674

b7E

DECLASSIFIED

Top 10 Most Common Vulnerabilities

Vulnerability	CVSS Score	Count
[redacted]	5.10	24169
[redacted]	9.30	22430
[redacted]	7.00	21831
[redacted]	9.30	20298
[redacted]	9.30	20259
[redacted]	9.30	20060
[redacted]	9.30	19499
[redacted]	9.30	11785
[redacted]	9.30	11328
[redacted]	9.30	11288

b7E

Top 10 Compliance Failures

Configuration Setting	Count
[redacted]	63183
[redacted]	62974
[redacted]	62972
[redacted]	60925
[redacted]	60709
[redacted]	60708
[redacted]	53571
[redacted]	51949
[redacted]	43967
[redacted]	41510

b7E

DECLASSIFIED

DECLASSIFIED

Appendix C – DoS Cyber Condition (CyberCon) Levels

CyberCon Level	Tripwires	Actions
EMERGENCY **Significant cyber attacks are currently occurring**	• Degradation, denial, or destruction of systems • Highly sophisticated attacks • Major tensions within country / significant catastrophic events • ***DoS is unable to execute its diplomatic mission*** • ***Widespread or focused attacks targeting vulnerabilities within the enterprise require an immediate coordinated response.*** • ***Network infrastructure throughput is severed.*** • ***Common network services are disrupted.*** • ***Sensitive information in the enterprise is at high risk of compromise.***	• Disconnection of Internet connectivity • Task Force initialization • Documented Remediation Steps completed and verified prior to re-connection
HIGH **Significant cyber attacks are imminent or moderate attacks are occurring**	• Widespread malicious activity • Intelligence indicates targeted activity • Increase in sophisticated recon and probes • Heightened tensions within country or major event • ***DoS must resort to alternative communications means to execute its diplomatic mission*** • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at moderate risk of compromise.***	• Initiate Management Team briefings • Three-times-a-day notification to pre-determined recipient list • Additional sniffers deployed as needed • Authorize limited OT for analysts

DECLASSIFIED

DECLASSIFIED

ELEVATED **Moderate cyber attacks are imminent**	• Increased risk • Limited malicious activity • Intelligence indicates general threats • Specific incidents reported and under review • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at some risk of compromise.***	• Ensure protective measures implemented • Increase backups, audits, etc. • Verify response action plans & staff ready • Document changes in cyber security posture
GUARDED **Nuisance cyber attack activity is present**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Potential malicious activity within the enterprise may be handled thorough routine channels and procedures.*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.*** • ***Existing countermeasures are likely to be adequate to counter this threat***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures
LOW **Nuisance cyber attack activity is expected**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Automated response is sufficient to counter potential malicious activity within the enterprise*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures

DECLASSIFIED

Appendix D – Intranet Web Links of Interest

DECLASSIFIED

Within the Office of Computer Security

- **Awareness**
  Periodic Update: http://cs.ds.state.gov/ETPA/ETPA_03.cfm
- **Computer Incident Response Team (CIRT)**
  Periodic Update: http://cs.ds.state.gov/CIRT/CIRT_08.cfm
- **Cyber Threat Analysis Division (CTAD)**
  Daily Read File: http://source.ds.state.sgov.gov (ClassNet)
  Tactical Awareness: http://cs.ds.state.gov/CTAD/CTAD_07.cfm
- **The Office of Computer Security**
  Periodic Update: http://cs.ds.state.gov/index.cfm
- **Compliance and Vulnerability Scanning**
  Periodic Update: http://cs.ds.state.gov/index.cfm

Outside of the Office of Computer Security

- **Cyber Security Incident Program**
  Periodic Update: http://csip.ds.state.gov
- **Enterprise Network Management**
  Periodic Update: http://enm.irm.state.gov
- **The Office of Information Assurance**
  Periodic Update: http://ia.irm.state.gov/
- **Patch Management**
  Periodic Update: http://enm.irm.state.gov/nlm/patch/Default.htm
- **Virus Incident Response Team (VIRT)**
  Periodic Update: http://sysintegweb.irm.state.gov/si/AntiVirus.html

The CIRT welcomes all constructive feedback to the daily Cyber Security Brief. If you have feedback for the CSB, please send it to CIRT@state.gov

P
003 b7E
E

Cyber Security Brief

United States Department of State
Bureau of Diplomatic Security
as of June 4, 2009-1400 EST

[illegible]

June 5, 2009

Current DoS Cyber Threat Condition

ELEVATED

Increased from last reported condition of "Guarded"

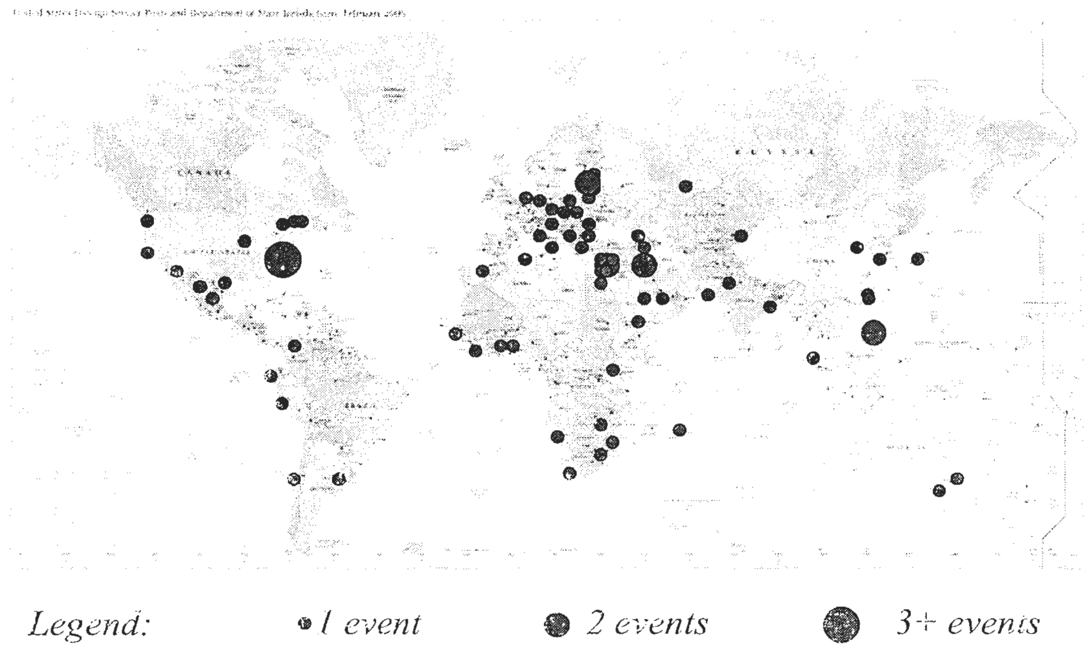
Moderate cyber attacks are imminent

Executive Summary

1. CIRT
   - CIRT continues to notify DoS ISSO's due to a large spear-phishing attack

2. CTAD Daily Read File
   - (Classified content)

Geographic Distribution of Computer Incident Response Team (CIRT) Events


United States Foreign Service Posts and Department of State Jurisdictions February 2005
CANADA
RUSSIA
Legend:
● 1 event
● 2 events
● 3+ events

DECLASSIFIED

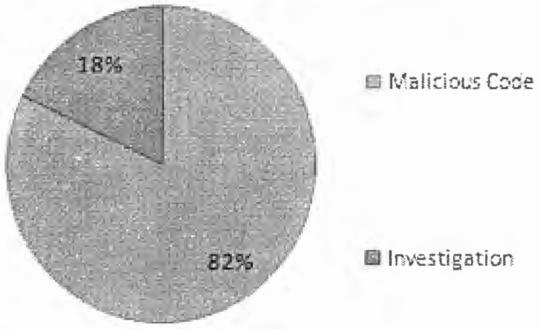
E

***Open CIRT Events*: 50**

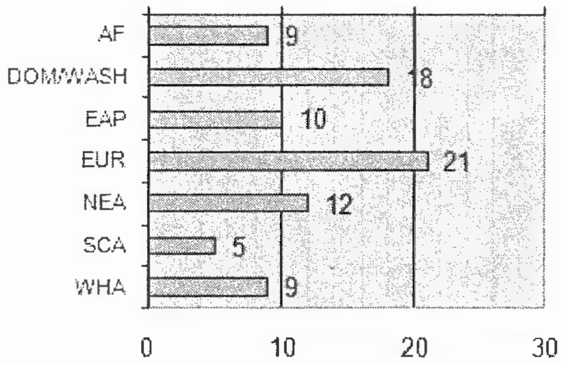
***Closed CIRT Events*: 34**

b7E

CIRT Events by US-CERT Category



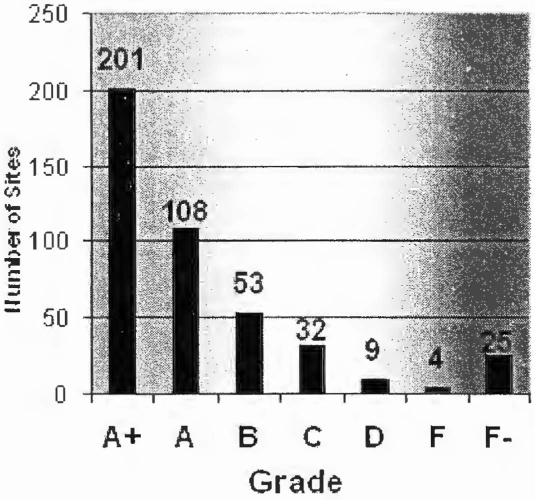
CIRT Events by Bureau



Firewall Block Request Summary

- Nothing substantial to report

Enterprise Risk Score Grade Distribution



Computer Incident Response Team (CIRT)

- CIRT continues to notify DoS ISSO's of an e-mail with a malicious pdf attachment. These e-mail messages contained PDF attachments [redacted] Due to the large number of tickets generated by this event, these tickets are presented in table format.

b7E

DECLASSIFIED

Personally identifiable information (PII) loss reported

- Nothing substantial to report

Classified spillage incident(s) reported to CIRT and referred to DS/IS/APD

- A classified document was sent via e-mail on OpenNet in Istanbul. This event has been referred to APD.

US-CERT Nothing substantial to report Coordination

- Nothing substantial to report

Compliance & Vulnerability Scanning

- *See Appendix B for statistics*

Cyber Threat Analysis Division (CTAD)

DAILY READ FILE: (Classified content – See CTAD Daily Read File on ClassNet for details)

***Virus Incident Response Team (VIRT) Statistics** (as of midnight eastern time)*

Spam Blocked at Perimeter:	Virus Blocked at Perimeter:
Previous day: 862,421	Previous day:142
Month to date - June: 2,994,328	Month to date - June:424
Year to date for 2009: 252,785,425	Year to date for 2009: 20,539

Cyber Security News Headlines

Is the Hacking Threat To National Security Overblown? *[Source: wired.com]*
U.S. Nuclear Information Leaked on GPO Web site *[Source: eweek.com]*

b7C

DECLASSIFIED

Appendix A –CIRT Event Summaries

Legend:	Open Events: 50	Closed Events: 34

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Malicious Code directed towards an internal machine

[redacted] CIRT detected a large number of e-mail messages [redacted]

b7E

b7E

Ticket Number	Location	Date Opened	Awaiting Post Response	Post is Remediating	Date Closed
[redacted]	[redacted]	June 02	X		
[redacted]	[redacted]	June 03			June 03
[redacted]	[redacted]	June 03			June 03
[redacted]	[redacted]	June 03			June 03
[redacted]	[redacted]	June 03			June 03
[redacted]	[redacted]	June 03		X	
[redacted]	[redacted]	June 03			June 04
[redacted]	[redacted]	June 03			June 04
[redacted]	[redacted]	June 03			June 04
[redacted]	[redacted]	June 03			June 04
[redacted]	[redacted]	June 03			June 04
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 03			June 03
[redacted]	[redacted]	June 03			June 04
[redacted]	[redacted]	June 03			June 04
[redacted]	[redacted]	June 03		X	
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 03			June 04
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 03			June 04
[redacted]	[redacted]	June 03		X	
[redacted]	[redacted]	June 03			June 04
[redacted]	[redacted]	June 03			June 04
[redacted]	[redacted]	June 03	X		

DECLASSIFIED

b7E

7E

Ticket Number	cation	Date Opened	Awaiting Post Response	Post is Remediating	Date Closed
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 03			June 04
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 03		X	
[redacted]	[redacted]	June 03		X	
[redacted]	[redacted]	June 03			June 04
[redacted]	[redacted]	June 03			June 04
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 03			June 04
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 03			June 04
[redacted]	[redacted]	June 03		X	
[redacted]	[redacted]	June 03		X	
[redacted]	[redacted]	June 03			June 04
[redacted]	[redacted]	June 03			June 04
[redacted]	[redacted]	June 03			June 04
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 03			June 04
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 03		X	
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 03			June 04
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 03			June 04
[redacted]	[redacted]	June 03			June 04
[redacted]	[redacted]	June 03			June 04
[redacted]	[redacted]	June 03			June 04
[redacted]	[redacted]	June 04			June 04
[redacted]	[redacted]	June 04	X		
[redacted]	[redacted]	June 04			June 04
[redacted]	[redacted]	June 04			June 04
[redacted]	[redacted]	June 04			June 04
[redacted]	[redacted]	June 04		X	
[redacted]	[redacted]	June 04			June 04
[redacted]	[redacted]	June 04	X		
[redacted]	[redacted]	June 04		X	
[redacted]	[redacted]	June 04	X		
[redacted]	[redacted]	June 04	X		
[redacted]	[redacted]	June 04	X		
[redacted]	[redacted]	June 04	X		
[redacted]	[redacted]	June 04	X		
[redacted]	[redacted]	June 04			June 04
[redacted]	[redacted]	June 04			June 04

DECLASSIFIED

5 AE

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Compromised System on a DoS network

Ticket Number:	**Location:**

DECLASSIFIED

b5

Date and Time Ticket Created: 05/29/2009 1258 GMT	**Affected Bureau:** EUR
Event Description US-CERT notified CIRT about suspicious traffic.	
Current Status 4 Jun: **CIRT is awaiting confirmation from the ISSO that the hard drive has been shipped.**	
Status History **29 May:** CIRT provided the ISSO remediation instructions via Classified e-mail. **1 Jun:** CIRT requested a status update from the ISSO via e-mail. **2 Jun:** CIRT received a response from the ISSO that the incident is in the process of being researched. **3 Jun:** CIRT received an update from the ISSO that the hard drive will be shipped out and a tracking number will be provided.	

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: E-mail - Phishing

Ticket Number [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 05/21/2009 1657 GMT	**Affected Bureau:** EAP
Event Description An employee notified CIRT that he had received a suspicious e-mail message with a PDF attachment.	
Current Status 4 Jun: **CIRT requested a status update from the ISSO via e-mail.**	
Status History **22 May:** CIRT requested that the ISSO determine if the message was opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system. **24 May:** CIRT requested a status update from the ISSO via e-mail. **26 May:** CIRT requested a status update from the ISSO via e-mail. **27 May:** CIRT requested a status update from the ISSO via e-mail. **28 May:** CIRT called the ISSO requesting a status update. **29 May:** CIRT was informed that the Post was closed due to a local holiday. **1 Jun:** CIRT expedited this ticket to the CISO for further assistance. **2 Jun:** CIRT sent another expedited request to the CISO and proper contacts. CIRT telephoned the ISSO during Post's operating hours to request an update. **3 Jun:** CIRT received an update from the ISSO stating that he is in the process of remediating the incident.	

Ticket Number: [redacted]	**Location** [redacted]

b7E

Date and Time Ticket Created: 05/27/2009 1615 GMT	**Affected Bureau:** DOM
Event Description CIRT was notified by US-CERT of spear phishing e-mail attempts, containing a PDF attachment, which target DoS personnel.	
Current Status **4 Jun: CIRT received an update from the IT Service Center that the ticket is still in the remediation process.**	
Status History **28 May:** CIRT requested that the IT Service Center direct the ISSO to determine if the user had received the suspicious message and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system. **29 May:** CIRT requested a status update from the IT Service Center via e-mail and phone. **1 Jun:** CIRT received an update from the ISSO that this event is in the process of being researched and remediated. **2 Jun:** CIRT requested a status update from the IT Service Center via e-mail. **3 Jun:** CIRT contacted the IT Service Center via phone and was informed that the ISSO is still examining this event.	

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 05/27/2009 1742 GMT	**Affected Bureau:** DOM
Event Description CIRT was notified by US-CERT of spear phishing e-mail attempts, containing a PDF attachment, which target DoS personnel.	
Current Status **4 Jun: The IT Service Center informed CIRT that they are currently awaiting feedback from SES Administrators.**	
Status History **28 May:** CIRT requested that the IT Service Center direct the ISSO to determine if the user had received the suspicious message and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system. **29 May:** CIRT requested a status update from the IT Service Center via e-mail and phone. **1 Jun:** CIRT requested a status update from the IT Service Center via e-mail. **2 Jun:** CIRT requested a status update from the IT Service Center via e-mail. **3 Jun:** CIRT received an update from IT Service Center that the ticket has been recreated in the proper ticketing system and resent to the proper ISSO.	

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 05/28/2009 1524 GMT	**Affected Bureau:** DOM
Event Description CIRT was notified by US-CERT of spear phishing e-mail attempts, containing a PDF	

b7E

DECLASSIFIED

attachment, which target DoS personnel.

Current Status

4 Jun: CIRT requested a status update from the ISSO via e-mail.

Status History

28 May: CIRT requested that the IT Service Center direct the ISSO to determine if the user had received the suspicious message and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
29 May: CIRT requested a status update from the IT Service Center via e-mail and phone.
1 Jun: CIRT requested a status update from the IT Service Center via e-mail.
2 Jun: CIRT called the ISSO for an update. The ISSO is currently researching the incident and will contact CIRT with an update at their next opportunity.
3 Jun: CIRT requested a status update from the ISSO via e-mail.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 05/27/2009 1853 GMT	**Affected Bureau:** DOM

Event Description

CIRT was notified by US-CERT of spear phishing e-mail attempts, containing a PDF attachment, which target DoS personnel.

Current Status

4 Jun: CIRT requested a status update from the ISSO via e-mail.

Status History

28 May: CIRT requested that the IT Service Center direct the ISSO to determine if the user had received the suspicious message and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
29 May: CIRT requested a status update from the IT Service Center via e-mail and phone.
1 Jun: CIRT requested a status update from the IT Service Center via e-mail.
2 Jun: CIRT requested a status update from the IT Service Center via e-mail.
3 Jun: CIRT requested a status update from the ISSO via e-mail.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 05/27/2009 1915 GMT	**Affected Bureau:** DOM

Event Description

CIRT was notified by US-CERT of spear phishing e-mail attempts, containing a PDF attachment, which target DoS personnel.

Current Status

4 Jun: The ISSO informed CIRT that he is in the process of contacting the user to remediate the incident. The ISSO will contact CIRT with any updates.

Status History

28 May: CIRT requested that the IT Service Center direct the ISSO to determine if the user

b7E

had received the suspicious message and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.

29 May: CIRT requested a status update from the IT Service Center via e-mail and phone.

1 Jun: CIRT received an update from IT Service Center that remediation actions have taken place. CIRT requested that the IT Service Center provide further details regarding the remediation actions taken.

2 Jun: CIRT sent a request to the IT Service Center that further remediation actions addressed in the initial request need to be taken for this incident.

3 Jun: CIRT called the ISSO to confirm that the incident is still in the process of being remediated.

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Malicious Code directed towards an internal machine

✓

Ticket Number:	**Location:**
Date and Time Ticket Created: 06/01/2009 1125 GMT	**Affected Bureau:** AF

Event Description

CIRT detected the download of an executable into a DoS workstation.

Current Status

4 Jun: CIRT requested a status update from the ISSO via e-mail.

Status History

1 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

2 Jun: CIRT requested a status update from the ISSO via e-mail.

3 Jun: CIRT requested a status update from the ISSO via e-mail.

✓

Ticket Number:	**Location**
Date and Time Ticket Created: 06/01/2009 1503 GMT	**Affected Bureau:** DOM

Event Description

US-CERT notified CIRT about suspicious traffic.

Current Status

4 Jun: CIRT requested a status update from the IT Service Center via e-mail.

Status History

2 Jun: CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO remove the workstation from the network and await further instructions.

3 Jun: CIRT received confirmation from IT Service Center that the event is in the process of

b7E

being examined.

UNCLASSIFIED

Ticket Number: [redacted]	**Location** [redacted]
Date and Time Ticket Created: 06/04/2009 1206 GMT	**Affected Bureau:** DOM

Event Description
CIRT detected a DoS workstation communicating with a malicious website and possibly downloading a malicious executable.

Current Status
4 Jun: CIRT requested that the ISSO search for specific files and reimage the workstation if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

Status History
N/A - New Event

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Unauthorized Hardware connected to DoS network

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/03/2009 2115 GMT	**Affected Bureau:** SCA

Event Description
CIRT detected the connection of an unauthorized [redacted] laptop to the DoS OpenNet network. This event involved an [redacted].

b7E

Current Status
4 Jun: CIRT requested that the ISSO search for the unauthorized hardware and remove it from the DoS network.

Status History
N/A - New Event

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Undetermined/Unknown

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/03/2009 2008 GMT	**Affected Bureau:** EUR

b2E

Event Description The ISSO in Baku reported the installation of [redacted]
Current Status **4 Jun: CIRT requested from the IT Service Center that the ISSO coordinate with the SMS team to determine the origin of the traffic.**
Status History **N/A - New Event**

DECLASSIFIED

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Violation of Computer Security Policy by a DoS user (CSIP issue)

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 05/27/2009 0919 GMT	**Affected Bureau:** NEA
Event Description The ISSO informed CIRT of a potential violation of computer security. Additional details are available on CLAN.	
Current Status **4 Jun: CIRT telephoned the ISSO and left a voicemail requesting an update.**	
Status History **27 May:** CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management. **28 May:** CIRT requested a status update from the ISSO via e-mail. **29 May:** CIRT requested a status update from the ISSO via e-mail. **31 May:** CIRT requested a status update from the ISSO via e-mail. **1 Jun:** CIRT received an update from the ISSO that this event is in the process of remediation. **2 Jun:** CIRT requested a status update from the ISSO via e-mail. **3 Jun:** CIRT recuested a status update from the ISSO via e-mail.	

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: E-mail - Phishing

Ticket Number: [redacted]	**Location:** [redacted]

Date and Time Ticket Created: 05/21/2009 1332 GMT	**Affected Bureau:** NEA

DECLASSIFIED

Event Description

CIRT received information from US-CERT of possible malware being directed at a DoS workstation.

Final Action

4 Jun: The ISSO informed CIRT that the e-mail in question was not found on the workstation. A full virus scan was performed and no threats were detected.

Status History

21 May: CIRT requested that the ISSO search for specific files and reimage the operating system if the files are found.
22 May: CIRT requested a status update from the ISSO via e-mail.
26 May: CIRT requested a status update from the ISSO via e-mail.
27 May: CIRT requested a status update from the ISSO via telephone.
28 May: CIRT requested a status update from the ISSO via e-mail and phone.
29 May: CIRT requested a status update from the ISO and IPO via e-mail.
1 Jun: CIRT expedited this ticket to the CISO for further assistance.
2 Jun: CIRT received updated ISSO contact information and resent the initial notification to the correct contact.
3 Jun: CIRT received an update from the ISSO that this event will be examined tomorrow.

Ticket Number:	**Location**
Date and Time Ticket Created: 06/04/2009 0252 GMT	**Affected Bureau:** EAP

Event Description

A suspicious e-mail with an attachment was directed towards a DoS user.

Final Action

4 Jun: CIRT received confirmation from the ISSO that the workstation is being reimaged.

Status History

N/A - New Event

US-CERT Category: CAT 3 (Malicicus Code)
Event Type Confirmed: Malicious Code directed towaros an internal machine

Ticket Number:	**Location:**
Date and Time Ticket Created: 05/21/2009 1845 GMT	**Affected Bureau:** NEA

Event Description

CIRT detected a malicious code exposure attempting [redacted]

DECLASSIFIED

b7E

Final Action

4 Jun: The ISSO reported that no unauthorized files were found and that a virus scan was performed with negative results. [redacted]

b7E

Status History

21 May: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.
22 May: CIRT requested a status update from the ISSO via e-mail
26 May: CIRT requested a status update from the ISSO via e-mail.
27 May: CIRT requested a status update from the ISSO via e-mail.
28 May: CIRT requested a status update from the ISSO via e-mail.
29 May: CIRT requested a status update from the ISO and IPO via e-mail.
1 Jun: CIRT called and spoke with the ISSO, requesting an update. The ISSO is in the process of remediating and will provide further details shortly.
2 Jun: CIRT received an update from the ISSO that remediation actions are being completed.
3 Jun: CIRT received confirmation from the ISSO that this workstation will be removed from the network and reimaged. CIRT requested confirmation once the workstation has been removed from the network.

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Information Security Issue (violation or infraction)

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/04/2009 0749 GMT	**Affected Bureau:** EUR

Event Description

CIRT has been notified of a Classified Spillage in Istanbul.

Final Action

4 Jun: This event has been forwarded to the APD group for remediation.

Status History

N/A - New Event

DECLASSIFIED

b2

DECLASSIFIED

Appendix B – Compliance & Vulnerability Scanning Statistics

VULNERABILITY TOTALS:

Total Critical Vulnerabilities: 9,030
Total High Vulnerabilities: 485,226

TOP 10 CRITICAL VULNERABILITIES

Vulnerability	CVSS Score	Count
[redacted]	10.00	1476
[redacted]	10.00	1168
[redacted]	10.00	1103
[redacted]	10.00	811
[redacted]	10.00	533
[redacted]	10.00	503
[redacted]	10.00	390
[redacted]	10.00	326
[redacted]	10.00	227
[redacted]	10.00	203

b7E

TOP 10 HIGH VULNERABILITIES

Vulnerability	CVSS Score	Count
[redacted]	9.30	22065
[redacted]	7.00	21421
[redacted]	9.30	19907
[redacted]	9.30	19852
[redacted]	9.30	19657
[redacted]	9.30	18941
[redacted]	9.30	11357
[redacted]	9.30	11318
[redacted]	9.30	11009

b7E

DECLASSIFIED

b7E

[redacted]	9.30	9961

DECLASSIFIED

Top 10 Most Common Vulnerabilities

Vulnerability	CVSS Score	Count
[redacted]	5.10	24162
[redacted]	9.30	22065
[redacted]	7.00	21421
[redacted]	9.30	19907
[redacted]	9.30	19852
[redacted]	9.30	19657
[redacted]	9.30	18941
[redacted]	9.30	11357
[redacted]	9.30	11318
[redacted]	9.30	11009

b7E

Top 10 Compliance Failures

Configuration Setting	Count
[redacted]	63292
[redacted]	63019
[redacted]	63017
[redacted]	61048
[redacted]	60826
[redacted]	60824
[redacted]	53718
[redacted]	51988
[redacted]	44007
[redacted]	35986

b7E

DECLASSIFIED

Appendix C – DoS Cyber Condition (CyberCon) Levels

CyberCon Level	Tripwires	Actions
EMERGENCY **Significant cyber attacks are currently occurring**	• Degradation, denial, or destruction of systems • Highly sophisticated attacks • Major tensions within country / significant catastrophic events • ***DoS is unable to execute its diplomatic mission*** • ***Widespread or focused attacks targeting vulnerabilities within the enterprise require an immediate coordinated response.*** • ***Network infrastructure throughput is severed.*** • ***Common network services are disrupted.*** • ***Sensitive information in the enterprise is at high risk of compromise.***	• Disconnection of Internet connectivity • Task Force initialization • Documented Remediation Steps completed and verified prior to re-connection
HIGH **Significant cyber attacks are imminent or moderate attacks are occurring**	• Widespread malicious activity • Intelligence indicates targeted activity • Increase in sophisticated recon and probes • Heightened tensions within country or major event • ***DoS must resort to alternative communications means to execute its diplomatic mission*** • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at moderate risk of compromise.***	• Initiate Management Team briefings • Three-times-a-day notification to pre-determined recipient list • Additional sniffers deployed as needed • Authorize limited OT for analysts

DECLASSIFIED

ELEVATED **Moderate cyber attacks are imminent**	• Increased risk • Limited malicious activity • Intelligence indicates general threats • Specific incidents reported and under review • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at some risk of compromise.***	• Ensure protective measures implemented • Increase backups, audits, etc. • Verify response action plans & staff ready • Document changes in cyber security posture
GUARDED **Nuisance cyber attack activity is present**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Potential malicious activity within the enterprise may be handled thorough routine channels and procedures.*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.*** • ***Existing countermeasures are likely to be adequate to counter this threat***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures
LOW **Nuisance cyber attack activity is expected**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Automated response is sufficient to counter potential malicious activity within the enterprise*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures

Appendix D – Intranet Web Links of Interest

DECLASSIFIED

Within the Office of Computer Security

- **Awareness**
  Periodic Update: http://cs.ds.state.gov/ETPA/ETPA_03.cfm
- **Computer Incident Response Team (CIRT)**
  Periodic Update: http://cs.ds.state.gov/CIRT/CIRT_08.cfm
- **Cyber Threat Analysis Division (CTAD)**
  Daily Read File: http://source.ds.state.sgov.gov (ClassNet)
  Tactical Awareness: http://cs.ds.state.gov/CTAD/CTAD_07.cfm
- **The Office of Computer Security**
  Periodic Update: http://cs.ds.state.gov/index.cfm
- **Compliance and Vulnerability Scanning**
  Periodic Update: http://cs.ds.state.gov/index.cfm

Outside of the Office of Computer Security

- **Cyber Security Incident Program**
  Periodic Update: http://csip.ds.state.gov
- **Enterprise Network Management**
  Periodic Update: http://enm.irm.state.gov
- **The Office of Information Assurance**
  Periodic Update: http://ia.irm.state.gov/
- **Patch Management**
  Periodic Update: http://enm.irm.state.gov/nlm/patch/Default.htm
- **Virus Incident Response Team (VIRT)**
  Periodic Update: http://sysintegweb.irm.state.gov/si/AntiVirus.html

The CIRT welcomes all constructive feedback to the daily Cyber Security Brief
If you have feedback for the CSB, please send it to CIRT@state.gov

P
004

Cyber Security Brief

United States Department of State
Bureau of Diplomatic Security
as of June 8, 2009-1400 EST

June 9, 2009

b7E

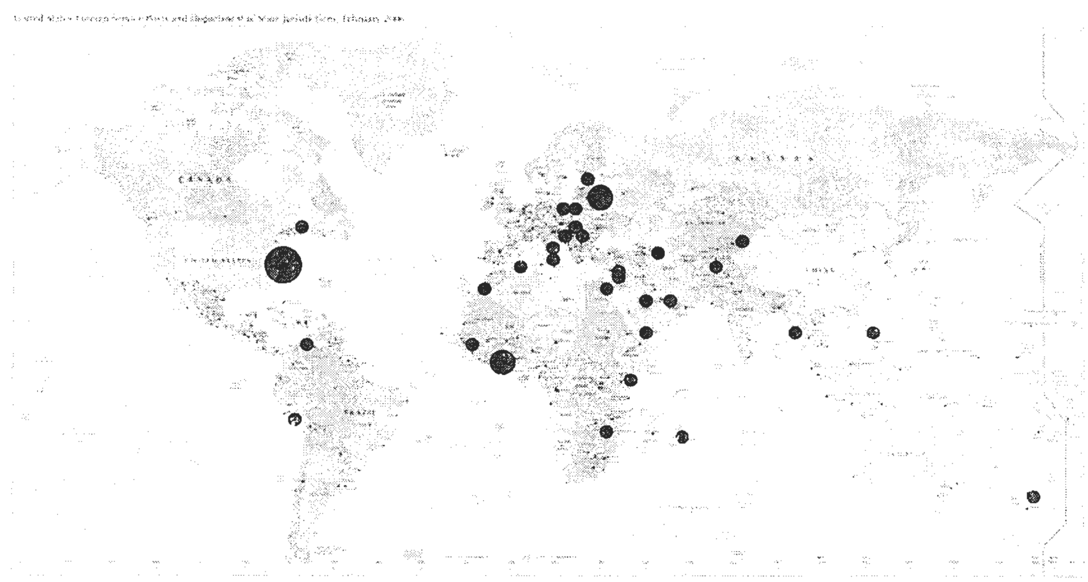
Current DoS Cyber Threat Condition GUARDED **No change from previous condition**

Nuisance cyber attack activity is present

Executive Summary

1. **CIRT**
   - CIRT continues to notify DoS ISSOs due to a large spear-phishing attack
2. **Cyber Threat Analysis Division**
   - Daily Read File: (U)
   - Weekly Telewall Report
3. **Classified spillage**
   - Classified files sent via OpenNet

Geographic Distribution of Computer Incident Response Team (CIRT) Events



Legend: ● *1 event* ● *2 events* ● *3+ events*

DECLASSIFIED

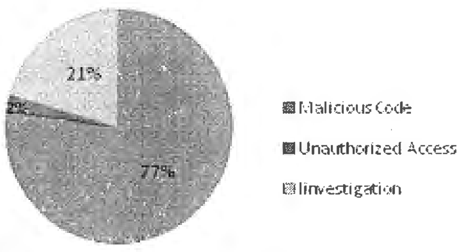
b7E

E

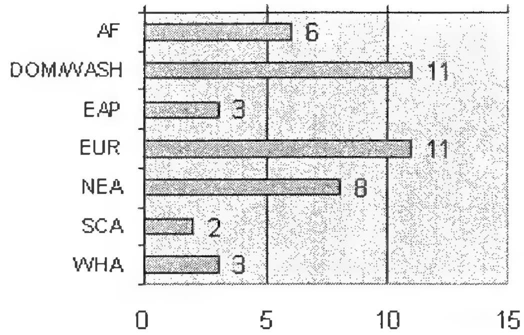
Open CIRT Events: 26

Closed CIRT Events: 18

CIRT Events by US-CERT Category



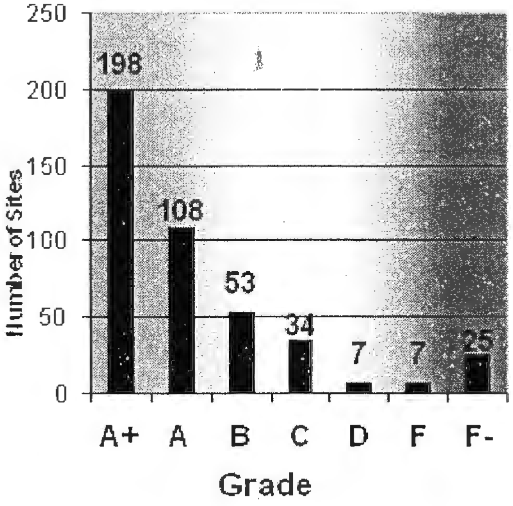
CIRT Events by Bureau



Firewall Block Request Summary

Enterprise Risk Score Grade Distribution

b7E



Computer Incident Response Team (CIRT)

- CIRT continues to notify DoS ISSOs of an e-mail with a malicious pdf attachment

b7E

b7E

Personally identifiable information (PII) loss reported

- Nothing substantial to report

Classified spillage incident(s) reported to CIRT and referred to DS/IS/APD

- A classified spillage occurred in Washington D.C. Classified documents were scanned and sent via OpenNet. This incident was reported to APD.

US-CERT Coordination

- Nothing substantial to report

Compliance & Vulnerability Scanning

- *See Appendix B for statistics*

Cyber Threat Analysis Division (CTAD)

b7E

DAILY READ FILE: (U

(SBU) Key Highlight

7E

(SBU) Source Paragr

b7E

Telewall Activity from 05/30/2009 to 06/06/2009

247,989	Calls Logged
0	Calls Blocked
8	911 Email Alerts
1	Reports Run for External Customers

Notable Events:

None

DECLASSIFIED

Virus Incident Response Team (VIRT) Statistics *(as of midnight eastern time)*

Spam Blocked at Perimeter:
Previous day: 929,266
Month to date - June: 6,804,329
Year to date for 2009: 256,595,426

Virus Blocked at Perimeter:
Previous day:17
Month to date - June:2,320
Year to date for 2009: 22,435

Cyber Security News Headlines

Obama Taps Well-Known Hacker as Security Adviser *[Source: foxnews.com]*
How Can Cyberspace Be Defended? *[Source: nationaljournal.com]*

b7E

Appendix A –CIRT Event Summaries

Legend:	Open Events: 26	Closed Events: 18

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Malicious Code directed towards an internal machine

[redacted] CIRT detected a large number of e-mail messages [redacted]

b7E

b7E

Ticket Number	Location	Date Opened	Awaiting Post Response	Post is Remediating	Date Closed
[redacted]	[redacted]	June 02	X		
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 03			June 08
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 03			June 08
[redacted]	[redacted]	June 03			June 08
[redacted]	[redacted]	June 03			June 08
[redacted]	[redacted]	June 03			June 08
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 03		X	
[redacted]	[redacted]	June 03			June 08
[redacted]	[redacted]	June 03			June 08
[redacted]	[redacted]	June 03		X	
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 03			June 08
[redacted]	[redacted]	June 03			June 08
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 03			June 08
[redacted]	[redacted]	June 04	X		
[redacted]	[redacted]	June 04			June 08
[redacted]	[redacted]	June 04	X		
[redacted]	[redacted]	June 04	X		
[redacted]	[redacted]	June 04			June 08
[redacted]	[redacted]	June 04			June 08
[redacted]	[redacted]	June 05			June 08

DECLASSIFIED

b7E

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Compromised System on a DoS network

Ticket Number:	**Location:**
Date and Time Ticket Created: 05/29/2009 1258 GMT	**Affected Bureau:** EUR

✓

Event Description
US-CERT notified CIRT about suspicious traffic.

Current Status
8 Jun: CIRT requested that the ISSO provide the tracking number for the shipped hard drive once it becomes available.

Status History
29 May: CIRT provided the ISSO remediation instructions via Classified e-mail.
1 Jun: CIRT requested a status update from the ISSO via e-mail.
2 Jun: CIRT received a response from the ISSO that the incident is in the process of being researched.
3 Jun: CIRT received an update from the ISSO that the hard drive will be shipped out and a tracking number will be provided.
4 Jun: CIRT is awaiting confirmation from the ISSO that the hard drive has been shipped.
5 Jun: Post is closed and a status request was sent via e-mail and phone

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Email - Malicious Payload (Code, Attachment, Link)

Ticket Number:	**Location:**
Date and Time Ticket Created: 06/05/2009 2316 GMT	**Affected Bureau:** EAP

✓

Event Description
CSIP referred a possible event to the CIRT involving an e-mail attachment received by a DoS employee

Current Status
8 Jun: CIRT requested that the ISSO perform a complete virus scan of the workstation

b7E

Status History
N/A - New Event

b7E

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: E-mail - Phishing

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 05/27/2009 1615 GMT	**Affected Bureau:** DOM

Event Description
CIRT was notified by US-CERT of spear phishing e-mail attempts, containing a PDF attachment, which target DoS personnel.

Current Status
8 Jun: CIRT requested a status update from the ISSO via e-mail.

Status History
28 May: CIRT requested that the IT Service Center direct the ISSO to determine if the user had received the suspicious message and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
29 May: CIRT requested a status update from the IT Service Center via e-mail and phone.
1 Jun: CIRT received an update from the ISSO that this event is in the process of being researched and remediated.
2 Jun: CIRT requested a status update from the IT Service Center via e-mail.
3 Jun: CIRT contacted IT Service Center via phone and was informed that the ISSO is still examining this event.
4 Jun: CIRT received an update from the IT Service Center that the ticket is still in the remediation process.
5 Jun: The IT Service Center informed CIRT that the ticket is currently being examined.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 05/27/2009 1742 GMT	**Affected Bureau:** DOM

Event Description
CIRT was notified by US-CERT of spear phishing e-mail attempts, containing a PDF attachment, which target DoS personnel.

Current Status
8 Jun: CIRT requested assistance from the CISO in obtaining a status update.

Status History
28 May: CIRT requested that the IT Service Center direct the ISSO to determine if the user had received the suspicious message and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
29 May: CIRT requested a status update from the IT Service Center via e-mail and phone.
1 Jun: CIRT requested a status update from the IT Service Center via e-mail.
2 Jun: CIRT requested a status update from the IT Service Center via e-mail.
3 Jun: CIRT received an update from IT Service Center that the ticket has been recreated in

b7E

the proper ticketing system and resent to the proper ISSO.
4 Jun: The IT Service Center informed CIRT that they are currently awaiting feedback from the SES Administrators.
5 Jun: CIRT telephoned the IT Service Center to request an update. The IT Service Center will provide CIRT with an update soon.

b2 ✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 05/27/2009 1853 GMT	**Affected Bureau:** DOM

Event Description
CIRT was notified by US-CERT of spear phishing e-mail attempts, containing a PDF attachment, which target DoS personnel.

Current Status
8 Jun: CIRT requested assistance from the CISO in obtaining a status update.

Status History
28 May: CIRT requested that the IT Service Center direct the ISSO to determine if the user had received the suspicious message and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
29 May: CIRT requested a status update from the IT Service Center via e-mail and phone.
1 Jun: CIRT requested a status update from the IT Service Center via e-mail.
2 Jun: CIRT requested a status update from the IT Service Center via e-mail.
3 Jun: CIRT requested a status update from the ISSO via e-mail.
4 Jun: CIRT requested a status update from the ISSO via e-mail.
5 Jun: This ticket has been expedited to the CISO.

b2 ✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 05/27/2009 1915 GMT	**Affected Bureau:** DOM

Event Description
CIRT was notified by US-CERT of spear phishing e-mail attempts, containing a PDF attachment, which target DoS personnel.

Current Status
8 Jun: CIRT requested assistance from the CISO in obtaining a status update.

Status History
28 May: CIRT requested that the IT Service Center direct the ISSO to determine if the user had received the suspicious message and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
29 May: CIRT requested a status update from the IT Service Center via e-mail and phone.
1 Jun: The IT Service Center informed CIRT that remediation actions have taken place. CIRT requested that the IT Service Center provide further details regarding the remediation actions taken.
2 Jun: CIRT sent a request to the IT Service Center that the remediation actions addressed in the initial request need to be taken for this incident.

b7E

3 Jun: CIRT contacted the ISSO via telephone and received confirmation that the incident is still in the process of being remediated.
4 Jun: The ISSO informed CIRT that he is in the process of contacting the user in order to remediate the incident. The ISSO will contact CIRT with any updates.
5 Jun: CIRT requested a status update from the IT Service Center

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Malicious Code directed towards an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/01/2009 1125 GMT	**Affected Bureau:** AF

Event Description
CIRT detected the download of an executable into a DoS workstation.

Current Status
8 Jun: The ISSO informed CIRT that the incident is in the process of being remediated.

Status History
1 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.
2 Jun: CIRT requested a status update from the ISSO via e-mail.
3 Jun: CIRT requested a status update from the ISSO via e-mail.
4 Jun: CIRT requested a status update from the ISSO via e-mail.
5 Jun: CIRT requested a status update from the ISSO via e-mail.

Ticket Number: [redacted]	**Location** [redacted]
Date and Time Ticket Created: 06/01/2009 1503 GMT	**Affected Bureau:** DOM

Event Description
US-CERT notified CIRT about suspicious traffic.

Current Status
8 Jun: CIRT requested assistance from the CISO in obtaining a status update.

Status History
2 Jun: CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO remove the workstation from the network and await further instructions.
3 Jun: CIRT received confirmation from the IT Service Center that the event is in the process of being examined.
4 Jun: CIRT requested a status update from the IT Service Center via e-mail.

b7E

5 Jun: CIRT requested a status update from the IT Service Center via e-mail.

DECLASSIFIED

Ticket Number:	**Location:**
Date and Time Ticket Created: 06/04/2009 1206 GMT	**Affected Bureau:** DOM
Event Description CIRT detected a DoS workstation communicating with a malicious website and possibly downloading a malicious executable.	
Current Status **8 Jun: CIRT requested assistance from the CISO in obtaining a status update.**	
Status History **4 Jun:** CIRT requested that the ISSO search for specific files and reimage the workstation if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management. **5 Jun:** The ticket was forwarded to the Mobile Computing Team. CIRT is waiting for a response.	

US-CERT Category: CAT 6 (Investigation) **Event Type Suspected:** Violation of Computer Security Policy by a DoS user (CSIP issue)

b7E

Ticket Number:	**Location:**
Date and Time Ticket Created: 05/27/2009 0919 GMT	**Affected Bureau:** NEA
Event Description The ISSO informed CIRT of a potential violation of computer security. Additional details are available on CLAN.	
Current Status **8 Jun: CIRT requested assistance from the CISO in obtaining a status update.**	
Status History **27 May:** CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT requested the ISSO perform an antivirus scan and verify the workstation is up to date with all of the latest patches from IRM Patch Management. **28 May:** CIRT requested a status update from the ISSO via e-mail. **29 May:** CIRT requested a status update from the ISSO via e-mail. **31 May:** CIRT requested a status update from the ISSO via e-mail. **1 Jun:** CIRT received an update from the ISSO that this event is in the process of remediation. **2 Jun:** CIRT requested a status update from the ISSO via e-mail.	

3 Jun: CIRT requested a status update from the ISSO via e-mail.
4 Jun: CIRT called and left a voicemail for the ISSO requesting an update.
5 Jun: CIRT expedited the ticket to the CISO.

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Virus/Worm on an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/05/2009 1213 GMT	**Affected Bureau:** NEA

Event Description

CIRT detected a DoS workstation communicating with a malicious website and possibly downloading a malicious executable.

Current Status

8 Jun: The ISSO informed CIRT that remediation actions have been completed, but he is still in the process of determining if the workstation contains all current patches. The ISSO will contact the CIRT with those details once they become available.

Status History

5 Jun: CIRT requested that the ISSO search the workstation for the executable and any possible malware. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation has all of the latest patches from IRM Patch Management.
6 Jun: CIRT received updated ISSO contact information and resent the initial notification to the correct contact.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/05/2009 1232 GMT	**Affected Bureau:** EAP

Event Description

CIRT detected a DoS workstation communicating with a suspicious website and possibly downloading a malicious .exe file.

Current Status

8 Jun: CIRT requested a status update from the ISSO via e-mail.

Status History

5 Jun: CIRT requested that the ISSO perform an antivirus scan and verify that the workstation has all of the latest patches from IRM Patch Management.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/05/2009 1241 GMT	**Affected Bureau:** AF

b7E

Event Description CIRT detected a DoS workstation communication with suspicious website and possibly downloading a malicious file.
Current Status **8 Jun: CIRT requested a status update from the ISSO via e-mail.**
Status History **5 Jun:** CIRT requested that the ISSO perform an antivirus scan and verify that the workstation has all of the latest patches from IRM Patch Management.

DECLASSIFIED

US-CERT Category: CAT 1 (Unauthorized Access)
Event Type Confirmed: Unauthorized Hardware connected to a DoS network

b7E

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/03/2009 2115 GMT	**Affected Bureau:** SCA
Event Description CIRT detected the connection of an unauthorized [redacted] ıptop to the DoS OpenNet network. This event involved [redacted]	
Final Action **8 Jun: CIRT received confirmation from the ISSO that the unauthorized laptop was located and removed from the network.**	
Status History **4 Jun:** CIRT requested that the ISSO search for the unauthorized hardware and remove it from the DoS network. **5 Jun:** [redacted]	

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Virus/Worm on internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 05/28/2009 1524 GMT	**Affected Bureau:** DOM
Event Description CIRT was notified by US-CERT of spear phishing e-mail attempts, containing a PDF attachment, which target DoS personnel.	

DECLASSIFIED

E
b7E

Final Action

8 Jun: CIRT received confirmation from the ISSO that the e-mails were not received, no malicious files were found on the workstations, and a virus scan of both workstations indicated no threats.

Status History

28 May: CIRT requested that the IT Service Center direct the ISSO to determine if the user had received the suspicious message and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
29 May: CIRT requested a status update from the IT Service Center via e-mail and phone.
1 Jun: CIRT requested a status update from the IT Service Center via e-mail.
2 Jun: CIRT called the ISSO for an update. The ISSO is currently researching the incident and will contact CIRT with an update at their next opportunity.
3 Jun: CIRT requested a status update from the ISSO via e-mail.
4 Jun: CIRT requested a status update from the ISSO via e-mail.
5 Jun: CIRT requested a status update from the ISSO via e-mail.

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Information Security Issue (violation or infraction)

Ticket Number:	**Location:**
Date and Time Ticket Created: 06/08/2009 1054 GMT	**Affected Bureau:** DOM

R ✓

Event Description

CIRT was notified of a Classified Spillage.

Final Action

8 Jun: This event has been referred to DS-ADP for remediation.

Status History

N/A - New Event

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Operational/Approved Activity

Ticket Number:	**Location:**
Date and Time Ticket Created: 06/03/2009 2008 GMT	**Affected Bureau:** EUR

R ✓

Event Description

The ISSO in Baku reported the installation of

b7E ✓

DECLASSIFIED

b7C

DECLASSIFIED

Final Action

8 Jun: CIRT received confirmation from the ISSO and the SMS Group that the

b7E

Status History

4 Jun: CIRT requested that the IT Service Center and the ISSO coordinate with the SMS team to determine the origin of the traffic.

5 Jun: POST is closed for the weekend. CIRT will request an update on Sunday.

DECLASSIFIED

b7E

DECLASSIFIED

Appendix B – Compliance & Vulnerability Scanning Statistics

VULNERABILITY TOTALS:

Total Critical Vulnerabilities:	8,564
Total High Vulnerabilities:	498,931

TOP 10 CRITICAL VULNERABILITIES

Vulnerability	CVSS Score	Count
[redacted]	10.00	1168
[redacted]	10.00	1123
[redacted]	10.00	1039
[redacted]	10.00	803
[redacted]	10.00	582
[redacted]	10.00	473
[redacted]	10.00	367
[redacted]	10.00	341
[redacted]	10.00	236
[redacted]	10.00	222

b7E

TOP 10 HIGH VULNERABILITIES

Vulnerability	CVSS Score	Count
[redacted]	9.30	24917
[redacted]	7.00	24086
[redacted]	9.30	22540
[redacted]	9.30	22465
[redacted]	9.30	22260
[redacted]	9.30	16896
[redacted]	9.30	12345
[redacted]	9.30	12274
[redacted]	9.30	7804
[redacted]	9.30	7747

b7E

E b7E

DECLASSIFIED

Top 10 Most Common Vulnerabilities

Vulnerability	CVSS Score	Count
[redacted]	9.30	24917
[redacted]	7.00	24086
[redacted]	5.10	23747
[redacted]	9.30	22540
[redacted]	9.30	22465
[redacted]	9.30	22260
[redacted]	9.30	16896
[redacted]	9.30	12345
[redacted]	9.30	12274
[redacted]	9.30	7804

b7E

Top 10 Compliance Failures

Configuration Setting	Count
[redacted]	63740
[redacted]	63538
[redacted]	63536
[redacted]	60915
[redacted]	60679
[redacted]	60676
[redacted]	54102
[redacted]	52423
[redacted]	44186
[redacted]	33475

b7E

Appendix C – DoS Cyber Condition (CyberCon) Levels

CyberCon Level	Tripwires	Actions
EMERGENCY **Significant cyber attacks are currently occurring**	• Degradation, denial, or destruction of systems • Highly sophisticated attacks • Major tensions within country / significant catastrophic events • ***DoS is unable to execute its diplomatic mission*** • ***Widespread or focused attacks targeting vulnerabilities within the enterprise require an immediate coordinated response.*** • ***Network infrastructure throughput is severed.*** • ***Common network services are disrupted.*** • ***Sensitive information in the enterprise is at high risk of compromise.***	• Disconnection of Internet connectivity • Task Force initialization • Documented Remediation Steps completed and verified prior to re-connection
HIGH **Significant cyber attacks are imminent or moderate attacks are occurring**	• Widespread malicious activity • Intelligence indicates targeted activity • Increase in sophisticated recon and probes • Heightened tensions within country or major event • ***DoS must resort to alternative communications means to execute its diplomatic mission*** • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at moderate risk of compromise.***	• Initiate Management Team briefings • Three-times-a-day notification to pre-determined recipient list • Additional sniffers deployed as needed • Authorize limited OT for analysts

UNCLASSIFIED

ELEVATED **Moderate cyber attacks are imminent**	• Increased risk • Limited malicious activity • Intelligence indicates general threats • Specific incidents reported and under review • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at some risk of compromise.***	• Ensure protective measures implemented • Increase backups, audits, etc. • Verify response action plans & staff ready • Document changes in cyber security posture
GUARDED **Nuisance cyber attack activity is present**	• No significant malicious activity • Network operating within “acceptable risk” range • Incident detection and response capability normal • ***Potential malicious activity within the enterprise may be handled thorough routine channels and procedures.*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.*** • ***Existing countermeasures are likely to be adequate to counter this threat***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures
LOW **Nuisance cyber attack activity is expected**	• No significant malicious activity • Network operating within “acceptable risk” range • Incident detection and response capability normal • ***Automated response is sufficient to counter potential malicious activity within the enterprise*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures

Appendix D – Intranet Web Links of Interest

DECLASSIFIED

Within the Office of Computer Security

- **Awareness**
  Periodic Update: http://cs.ds.statc.gov/ETPA/ETPA_03.cfm
- **Computer Incident Response Team (CIRT)**
  Periodic Update: http://cs.ds.state.gov/CIRT/CIRT_08.cfm
- **Cyber Threat Analysis Division (CTAD)**
  Daily Read File: http://source.ds.state.sgov.gov (ClassNet)
  Tactical Awareness: http://cs.ds.state.gov/CTAD/CTAD_07.cfm
- **The Office of Computer Security**
  Periodic Update: http://cs.ds.state.gov/index.cfm
- **Compliance and Vulnerability Scanning**
  Periodic Update: http://cs.ds.state.gov/index.cfm

Outside of the Office of Computer Security

- **Cyber Security Incident Program**
  Periodic Update: http://csip.ds.state.gov
- **Enterprise Network Management**
  Periodic Update: http://enm.irm.state.gov
- **The Office of Information Assurance**
  Periodic Update: http://ia.irm.state.gov/
- **Patch Management**
  Periodic Update: http://enm.irm.state.gov/nlm/patch/Default.htm
- **Virus Incident Response Team (VIRT)**
  Periodic Update: http://sysintegweb.irm.state.gov/si/AntiVirus.html

The CIRT welcomes all constructive feedback to the daily Cyber Security Brief. If you have feedback for the CSB, please send it to CIRT@state.gov

005

376

Cyber Security Brief

United States Department of State
Bureau of Diplomatic Security
as of June 9, 2009-1400 EST

June 10, 2009

Current DoS Cyber Threat Condition

GUARDED

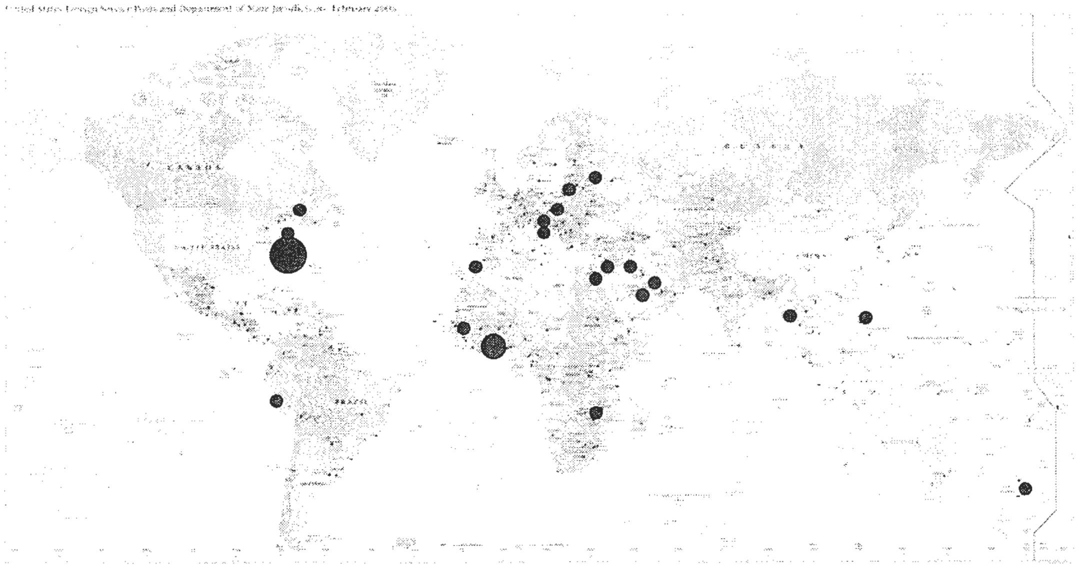
No change from last reported condition

Nuisance cyber attack activity is present

Executive Summary

1. <u>CIRT</u>
   - CIRT is awaiting the ISSOs' responses and remediation confirmations on the remaining spear-phishing attack notifications.
2. **CTAD Daily Read File:**
   - (U) British National Party Comes Under DDOS Attack
3. **Personally identifiable information (PII) Loss Reported**
   - Two passport applications missing

Geographic Distribution of Computer Incident Response Team (CIRT) Events


United States Foreign Service Posts and Department of State Jurisdictions - February 2009

Legend: ● *1 event* ● *2 events* ● *3+ events*

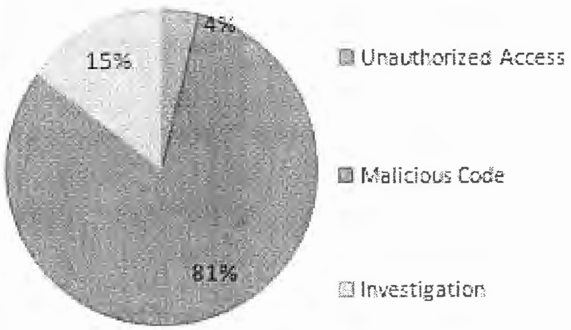
DECLASSIFIED

b7E

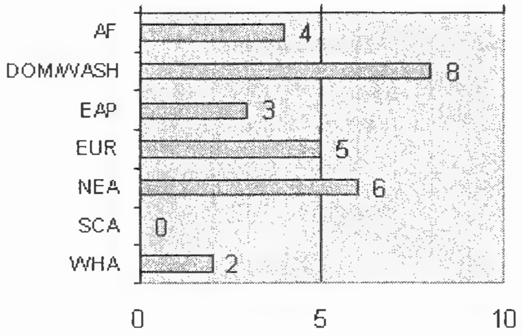
Open CIRT Events: 9

Closed CIRT Events: 19

CIRT Events by US-CERT Category



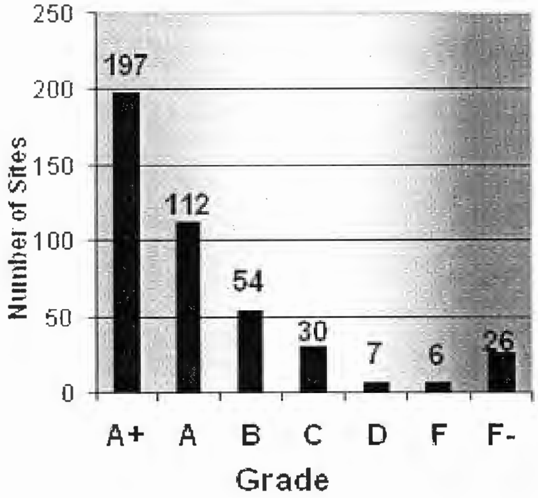
CIRT Events by Bureau



Firewall Block Request Summary

- Nothing substantial to report

Enterprise Risk Score Grade Distribution



Computer Incident Response Team (CIRT)

- CIRT is awaiting the ISSOs' responses and remediation confirmations on the remaining spear-phishing attack notifications of e-mails with a malicious pdf attachment. These e-mail messages contained PDF attachments which were made to appear as if sent by

b7E

b7E

Due to the large number of tickets generated by this event, these tickets are presented in table format.

Personally identifiable information (PII) loss reported

- Two passport applications mailed from a non-postal acceptance facility to the Lindbergh Postal Distribution Center (Philadelphia) cannot be located at this time.

Classified spillage incident(s) reported to CIRT and referred to DS/IS/APD

- Nothing substantial to report

US-CERT Coordination

- Nothing substantial to report

Compliance & Vulnerability Scanning

- *See Appendix B for statistics*

Cyber Threat Analysis Division (CTAD)

DAILY READ FILE: (U) British National Party Comes Under Distributed Denial of Service (DDOS) Attack

(SBU) Key Highlights:

- *The Web site of the British National Party (BNF) came under sporadic DDOS attack for two days in May*
- *The BNP blamed the attack on domestic rivals* [redacted]

b7E

(U) Source Paragraph: "In an e-mail to supporters, Griffin writes that the 'BNP website [was] taken offline [the] largest cyber attack in recorded history' and of a scale only once seen before in a 2001 attack against Microsoft."

Source: The Register (http://www.theregister.co.uk), "BNP pleads for cash after reported DDOS assault," 27 May 2009

DECLASSIFIED

***Virus Incident Response Team (VIRT) Statistics** (as of midnight eastern time)*

Spam Blocked at Perimeter:	**Virus Blocked at Perimeter:**
Previous day: 1,259,031	Previous day:103
Month to date - June: 8,063,360	Month to date - June:2,423
Year to date for 2009: 257,854,457	Year to date for 2009: 22,538

Cyber Security News Headlines

National Cyber Security: Cornell's Fred Schneider Will Tell Congress Ways to Shore up Vulnerability *[Source: scienceblog.com]*

DECLASSIFIED

b7E

DECLASSIFIED

Appendix A –CIRT Event Summaries

Legend:	*Open Events: 9*	*Closed Events: 19*

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Malicious Code directed toward internal machine

[redacted] CIRT detected a large number of e-mail messages [redacted]

b7E

Ticket Number	Location	Date Opened	Awaiting Post Response	Post is Remediating	Date Closed
[redacted]	[redacted]	June 02			X
[redacted]	[redacted]	June 03		X	
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 03			X
[redacted]	[redacted]	June 03			X
[redacted]	[redacted]	June 03			X
[redacted]	[redacted]	June 03		X	
[redacted]	[redacted]	June 03			X
[redacted]	[redacted]	June 03			X
[redacted]	[redacted]	June 03	X		
[redacted]	[redacted]	June 04		X	
[redacted]	[redacted]	June 04			X
[redacted]	[redacted]	June 04			X

b7E

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: E-mail - Malicious Payload (Code, Attachment, Link)

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/05/2009 2316 GMT	**Affected Bureau:** EAP

DECLASSIFIED

E

575

Event Description
CSIP referred a possible event to the CIRT involving an e-mail attachment received by a DoS employee.

Current Status
9 Jun: CIRT requested a status update from the ISSO via e-mail.

Status History
8 Jun: CIRT requested that the ISSO perform a complete virus scan of the workstation using the latest signatures and determine if any malware still resides in the system.

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Violation of Computer Security Policy by a DoS user (CSIP issue)

Ticket Number:	**Location**
Date and Time Ticket Created: 05/27/2009 0919 GMT	**Affected Bureau:** NEA

Event Description
The ISSO informed CIRT of a potential violation of computer security. Additional details are available on CLAN.

Current Status
9 Jun: CIRT requested further assistance from the CISO.

Status History

27 May: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT requested the ISSO perform an antivirus scan and verify the workstation is up to date with all of the latest patches from IRM Patch Management.
28 May: CIRT requested a status update from the ISSO via e-mail.
29 May: CIRT requested a status update from the ISSO via e-mail.
31 May: CIRT requested a status update from the ISSO via e-mail.
1 Jun: The ISSO informed CIRT that this event is in the process of remediation.
2 Jun: CIRT requested a status update from the ISSO via e-mail.
3 Jun: CIRT requested a status update from the ISSO via e-mail.
4 Jun: CIRT called and left a voicemail for the ISSO requesting an update.
5 Jun: CIRT requested a status update from the ISSO via e-mail.
8 Jun: CIRT requested the assistance of the CISO in obtaining a status update.

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Virus/Worm on an internal machine

Ticket Number:	**Location:**

b7E

Date and Time Ticket Created: 06/05/2009 1232 GMT	**Affected Bureau:** EAP

Event Description CIRT detected a DoS workstation communicating with a suspicious website and possibly downloading a malicious .exe file.
Current Status **9 Jun: CIRT requested a status update from the ISSO via e-mail.**
Status History **5 Jun:** CIRT requested that the ISSO perform an antivirus scan and verify that the workstation has all of the latest patches from IRM Patch Management. **8 Jun:** CIRT requested a status update from the ISSO via e-mail.

BM ✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/09/2009 0726 GMT	**Affected Bureau:** NEA

Event Description CIRT detected a DoS workstation in communication with a [redacted] possibly downloading an executable file.
Current Status **9 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.**
Status History **N/A - New Event**

b7E

US-CERT Category: CAT 1 (Unauthorized Access)
Event Type Confirmed: Information Security Issue (violation or infraction)

BM ✓

Ticket Number: [redacted]	**Location** [redacted]
Date and Time Ticket Created: 06/09/2009 1055 GMT	**Affected Bureau:** DOM

Event Description Personally Identifiable Information (PII) may have been breached or disclosed to unauthorized third parties.
Final Action **9 Jun: This event was reported to US-CERT and the Privacy Team.**

b7E

Status History
N/A - New Event

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Compromised System on a DoS network

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 05/29/2009 1258 GMT	**Affected Bureau:** EUR

Event Description
US-CERT notified CIRT about suspicious traffic.

Final Action
9 Jun: The system hard drive has been replaced and the compromised drive has been shipped to TASO. The tracking number is provided in the work log.

Status History
29 May: CIRT provided the ISSO remediation instructions via Classified e-mail.
1 Jun: CIRT requested a status update from the ISSO via e-mail.
2 Jun: CIRT received a response from the ISSO that the incident is in the process of being researched.
3 Jun: CIRT received an update from the ISSO that the hard drive will be shipped out and a tracking number will be provided.
4 Jun: CIRT is awaiting confirmation from the ISSO that the hard drive has been shipped.
5 Jun: Post is closed and a status request was sent via e-mail and phone
8 Jun: CIRT requested that the ISSO provide the tracking number for the shipped hard drive once it becomes available.

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: E-mail - Phishing

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 05/27/2009 1742 GMT	**Affected Bureau:** DOM

Event Description
CIRT was notified by US-CERT of spear phishing e-mail attempts, containing a PDF attachment, which target DoS personnel.

Final Action
9 Jun: The IT Service Center reported that the e-mail was permanently deleted from the user's inbox. No other threats were detected on the workstation.

b7C

Status History

- **28 May:** CIRT requested that the IT Service Center direct the ISSO to determine if the user had received the suspicious message and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
- **29 May:** CIRT requested a status update from the IT Service Center via e-mail and phone.
- **1 Jun:** CIRT requested a status update from the IT Service Center via e-mail.
- **2 Jun:** CIRT requested a status update from the IT Service Center via e-mail.
- **3 Jun:** CIRT received an update from IT Service Center that the ticket has been recreated in the proper ticketing system and resent to the proper ISSO.
- **4 Jun:** CIRT received a ticket status update from IT Service Center that they are currently awaiting feedback from SES Administrators.
- **5 Jun:** CIRT requested a status update from IT Service Center by phone. The IT Service Center will provide an update soon.
- **8 Jun:** CIRT requested the assistance of the CISO in obtaining a status update.

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Malicious Code directed towards an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 05/27/2009 1853 GMT	**Affected Bureau:** DOM

Event Description

CIRT was notified by US-CERT of spear phishing e-mail attempts, containing a PDF attachment, which target DoS personnel.

Final Action

9 Jun: The workstation has been re-imaged by the ISSO and placed back on the network.

Status History

- **28 May:** CIRT requested that the IT Service Center direct the ISSO to determine if the user had received the suspicious message and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
- **29 May:** CIRT requested a status update from the IT Service Center via e-mail and phone.
- **1 Jun:** CIRT requested a status update from the IT Service Center via e-mail.
- **2 Jun:** CIRT requested a status update from the IT Service Center via e-mail.
- **3 Jun:** CIRT requested a status update from the ISSO via e-mail.
- **4 Jun:** CIRT requested a status update from the ISSO via e-mail.
- **5 Jun:** This ticket has been expedited to the CISO.
- **8 Jun:** CIRT requested the assistance of the CISO in obtaining a status update.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/01/2009 1125 GMT	**Affected Bureau:** AF

Event Description

CIRT detected the download of an executable into a DoS workstation.

Final Action

9 Jun: The workstation has been re-imaged by the ISSO and placed back on the network.

Status History

1 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.
2 Jun: CIRT requested a status update from the ISSO via e-mail.
3 Jun: CIRT requested a status update from the ISSO via e-mail.
4 Jun: CIRT requested a status update from the ISSO via e-mail.
5 Jun: CIRT requested a status update from the ISSO via e-mail.
8 Jun: CIRT received an e-mail response that the incident is in the process of being remediated.

Ticket Number:	**Location:**
Date and Time Ticket Created: 06/01/2009 1503 GMT	**Affected Bureau:** DOM

Event Description

US-CERT notified CIRT about suspicious traffic.

Final Action

9 Jun: CIRT received confirmation from the ISSO that the e-mail was located and removed from the workstation. An antivirus scan did not detect any further threats.

Status History

2 Jun: CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO remove the workstation from the network and await further instructions.

3 Jun: CIRT received confirmation from IT Service Center that the event is in the process of being examined.

4 Jun: CIRT requested a status update from the IT Service Center via e-mail.

5 Jun: CIRT requested a status update from the IT Service Center via e-mail.

8 Jun: CIRT requested the assistance of the CISO in obtaining a status update.

Ticket Number:	**Location:**
Date and Time Ticket Created: 06/05/2009 1213 GMT	**Affected Bureau:** NEA

Event Description

CIRT detected a DoS workstation communicating with a malicious website and possibly downloading a malicious executable.

Final Action

9 Jun: CIRT received confirmation from the ISSO that no malicious files were found on

b7c

the workstation and that it is fully patched with all the latest patches.

DECLASSIFIED

Status History

5 Jun: CIRT sent an initial request to the ISSO, requesting that the workstation be searched for the executable and any possible malware. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation has all of the latest patches from IRM Patch Management.

6 Jun: CIRT received updated ISSO contact information and resent the initial notification to the correct contact.

8 Jun: CIRT received an update from the ISSO that remediation actions have been completed, but that he is still in the process of determining if the workstation contains all of the latest patches. The ISSO will follow up with those details once they become available.

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Virus/Worm on an internal machine

Ticket Number:	**Location:**
Date and Time Ticket Created: 05/27/2009 1615 GMT	**Affected Bureau:** DOM

Event Description

CIRT was notified by US-CERT of spear phishing e-mail attempts, containing a PDF attachment, which target DoS personnel.

Final Action

9 Jun: CIRT received confirmation from the ISSO that the e-mails in question were located and deleted. A search of the computer confirmed no malicious files were found and an antivirus scan detected no threats.

Status History

28 May: CIRT requested that the IT Service Center direct the ISSO to determine if the user had received the suspicious message and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.

29 May: CIRT requested a status update from the IT Service Center via e-mail and phone.

1 Jun: CIRT received an update from the ISSO that this event is in the process of being researched and remediated.

2 Jun: CIRT requested a status update from the IT Service Center via e-mail.

3 Jun: CIRT contacted the IT Service Center via phone and was informed that the ISSO is still examining this event.

4 Jun: CIRT received an update from the IT Service Center that the ticket is still in the remediation process.

5 Jun: The IT Service Center reported that the ticket is still being examined.

8 Jun: CIRT requested a status update from the ISSO via e-mail.

Ticket Number:	**Location**
Date and Time Ticket Created: 05/27/2009 1915 GMT	**Affected Bureau:** DOM

b7E

Event Description

CIRT was notified by US-CERT of spear phishing e-mail attempts containing a PDF attachment, which target DoS personnel.

Final Action

9 Jun: CIRT received confirmation from the ISSO that the suspicious PDF was not found on the user's workstation.

Status History

28 May: CIRT requested that the IT Service Center direct the ISSO to determine if the user had received the suspicious message and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
29 May: CIRT requested a status update from the IT Service Center via e-mail and phone.
1 Jun: CIRT received an update from IT Service Center that remediation actions have taken place. CIRT requested that the IT Service Center provide further details regarding the remediation actions taken.
2 Jun: CIRT sent a request to the IT Service Center that further remediation actions addressed in the initial request need to be taken for this incident.
3 Jun: CIRT called the ISSO to confirm that the incident is still in the process of being remediated.
4 Jun: The ISSO informed CIRT that he is in the process of contacting the user to remediate the incident. The ISSO will contact CIRT with any updates.
5 Jun: CIRT requested a status update from the IT Service Center
8 Jun: CIRT requested the assistance of the CISO in obtaining a status update.

Ticket Number:	**Location:**
Date and Time Ticket Created: 06/05/2009 1241 GMT	**Affected Bureau:** AF

Event Description

CIRT detected a DoS workstation communicating with a suspicious website and possibly downloading a malicious file.

Final Action

9 Jun: The file was not found on the workstation. The workstation has been removed from the network and an antivirus scan will be performed prior to reconnection.

b7E

Status History

5 Jun: CIRT requested that the ISSO perform an antivirus scan and verify that the workstation has all of the latest patches from IRM Patch Management.
8 Jun: CIRT requested a status update from the ISSO via e-mail.

Ticket Number:	**Location:**
Date and Time Ticket Created: 06/04/2009 1206 GMT	**Affected Bureau:** DOM

Event Description

CIRT detected a DoS workstation communicating with a malicious website and possibly downloading a malicious executable.

DECLASSIFIED

Final Action

9 Jun: CIRT received confirmation from the ISSO that no malicious files were detected on the workstation. An antivirus scan was performed and no threats were detected.

Status History

4 Jun: CIRT requested that the ISSO search for specific files and reimage the workstation if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

5 Jun: The ticket was forwarded to the Mobile Computing Team.

8 Jun: CIRT requested the assistance of the CISO in obtaining a status update.

DECLASSIFIED

Appendix B – Compliance & Vulnerability Scanning Statistics

b7E

DECLASSIFIED

Vulnerability Totals:

Total Critical Vulnerabilities:	8,513
Total High Vulnerabilities:	508,558

Top 10 Critical Vulnerabilities

Vulnerability	CVSS Score	Count
[redacted]	10.00	1185
[redacted]	10.00	1168
[redacted]	10.00	1027
[redacted]	10.00	803
[redacted]	10.00	528
[redacted]	10.00	470
[redacted]	10.00	364
[redacted]	10.00	334
[redacted]	10.00	238
[redacted]	10.00	217

b7E

Top 10 High Vulnerabilities

Vulnerability	CVSS Score	Count
[redacted]	9.30	25839
[redacted]	7.00	25129
[redacted]	9.30	23502
[redacted]	9.30	23437
[redacted]	9.30	23225
[redacted]	9.30	17466
[redacted]	9.30	12727
[redacted]	9.30	12656
[redacted]	9.30	8023
[redacted]	9.30	7966

b7E

DECLASSIFIED

b7E

DECLASSIFIED

Top 10 Most Common Vulnerabilities

Vulnerability	CVSS Score	Count
[redacted]	9.30	25839
[redacted]	7.00	25129
[redacted]	5.10	23700
[redacted]	9.30	23502
[redacted]	9.30	23437
[redacted]	9.30	23225
[redacted]	9.30	17466
[redacted]	9.30	12727
[redacted]	9.30	12656
[redacted]	9.30	8023

b7E

Top 10 Compliance Failures

Configuration Setting	Count
[redacted]	63824
[redacted]	62346
[redacted]	62344
[redacted]	61003
[redacted]	60767
[redacted]	60763
[redacted]	54174
[redacted]	52486
[redacted]	44253
[redacted]	32579

b7E

DECLASSIFIED

DECLASSIFIED

Appendix C – DoS Cyber Condition (CyberCon) Levels

CyberCon Level	Tripwires	Actions
EMERGENCY **Significant cyber attacks are currently occurring**	• Degradation, denial, or destruction of systems • Highly sophisticated attacks • Major tensions within country / significant catastrophic events • ***DoS is unable to execute its diplomatic mission*** • ***Widespread or focused attacks targeting vulnerabilities within the enterprise require an immediate coordinated response.*** • ***Network infrastructure throughput is severed.*** • ***Common network services are disrupted.*** • ***Sensitive information in the enterprise is at high risk of compromise.***	• Disconnection of Internet connectivity • Task Force initialization • Documented Remediation Steps completed and verified prior to re-connection
HIGH **Significant cyber attacks are imminent or moderate attacks are occurring**	• Widespread malicious activity • Intelligence indicates targeted activity • Increase in sophisticated recon and probes • Heightened tensions within country or major event • ***DoS must resort to alternative communications means to execute its diplomatic mission*** • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at moderate risk of compromise.***	• Initiate Management Team briefings • Three-times-a-day notification to pre-determined recipient list • Additional sniffers deployed as needed • Authorize limited OT for analysts

DECLASSIFIED

DECLASSIFIED

ELEVATED **Moderate cyber attacks are imminent**	• Increased risk • Limited malicious activity • Intelligence indicates general threats • Specific incidents reported and under review • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at some risk of compromise.***	• Ensure protective measures implemented • Increase backups, audits, etc. • Verify response action plans & staff ready • Document changes in cyber security posture
GUARDED **Nuisance cyber attack activity is present**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Potential malicious activity within the enterprise may be handled thorough routine channels and procedures.*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.*** • ***Existing countermeasures are likely to be adequate to counter this threat***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures
LOW **Nuisance cyber attack activity is expected**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Automated response is sufficient to counter potential malicious activity within the enterprise*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures

Appendix D – Intranet Web Links of Interest

DECLASSIFIED

Within the Office of Computer Security

- **Awareness**
  Periodic Update: http://cs.ds.state.gov/ETPA/ETPA_03.cfm
- **Computer Incident Response Team (CIRT)**
  Periodic Update: http://cs.ds.state.gov/CIRT/CIRT_08.cfm
- **Cyber Threat Analysis Division (CTAD)**
  Daily Read File: http://source.ds.state.sgov.gov (ClassNet)
  Tactical Awareness: http://cs.ds.state.gov/CTAD/CTAD_07.cfm
- **The Office of Computer Security**
  Periodic Update: http://cs.ds.state.gov/index.cfm
- **Compliance and Vulnerability Scanning**
  Periodic Update: http://cs.ds.state.gov/index.cfm

Outside of the Office of Computer Security

- **Cyber Security Incident Program**
  Periodic Update: http://csip.ds.state.gov
- **Enterprise Network Management**
  Periodic Update: http://enm.irm.state.gov
- **The Office of Information Assurance**
  Periodic Update: http://ia.irm.state.gov/
- **Patch Management**
  Periodic Update: http://enm.irm.state.gov/nlm/patch/Default.htm
- **Virus Incident Response Team (VIRT)**
  Periodic Update: http://sysintegweb.irm.state.gov/si/AntiVirus.html

The CIRT welcomes all constructive feedback to the daily Cyber Security Brief. If you have feedback for the CSB, please send it to CIRT@state.gov

p 006
b7E

006

Cyber Security Brief

United States Department of State
Bureau of Diplomatic Security
as of June 15, 2009-1400 EST

June 16, 2009

Current DoS Cyber Threat Condition

GUARDED

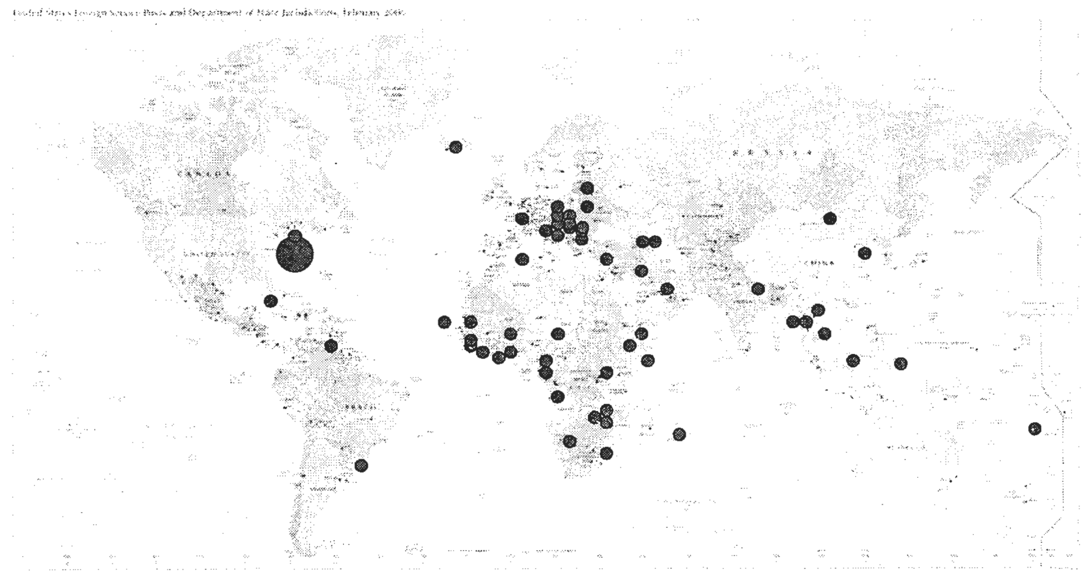
Decreased from last reported condition

Nuisance cyber attack activity is present

Executive Summary

1. <u>CIRT</u>
   - CIRT is awaiting the ISSOs' responses and remediation confirmations on the spear-phishing attack notifications.
2. <u>CTAD Daily Read File</u>
   - (SBU) Oman Attempts to Improve Cyber Awareness and CND Capabilities
3. <u>Classified spillage incident reported to CIRT</u>
   - SCI information sent via e-mail
4. <u>Personally identifiable information loss reported</u>
   - Three passport applications missing
   - One DoS laptop reported missing

Geographic Distribution of Computer Incident Response Team (CIRT) Events



United States Foreign Service Posts and Department of State Jurisdictions, February 2008

Legend: ● *1 event* ● *2 events* ● *3+ events*

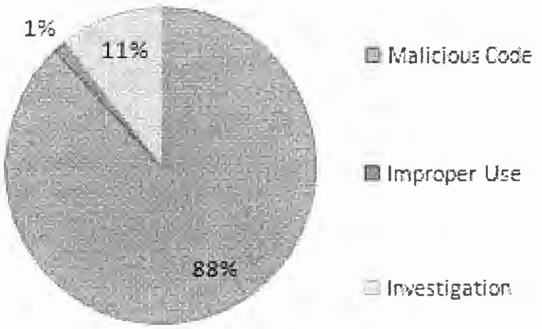
DECLASSIFIED

E
b7E

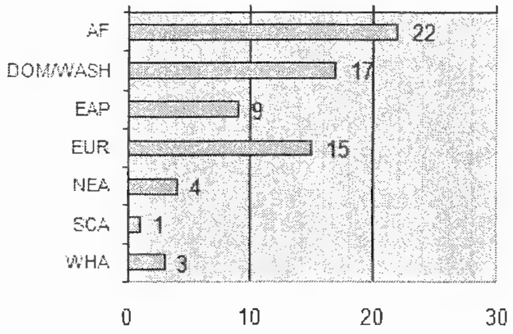
Open CIRT Events: 39

Closed CIRT Events: 32

CIRT Events by US-CERT Category



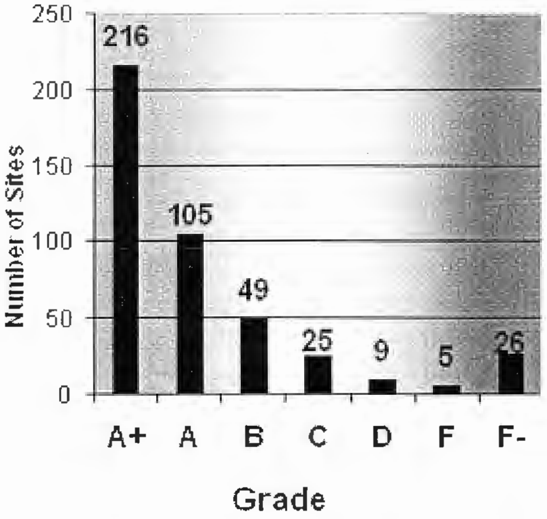
CIRT Events by Bureau



Firewall Block Request Summary

- Nothing substantial to report

Enterprise Risk Score Grade Distribution



Computer Incident Response Team (CIRT)

- CIRT detected a large scale spear phishing campaign targeting DoS employees, both stateside and abroad.

b7E

DECLASSIFIED

b7E

Personally identifiable information (PII) loss reported

- Three passport applications mailed from a postal acceptance facility in the Boston Passport Agency region to the Lindbergh Postal Distribution Center (Philadelphia, PA) cannot be located at this time. This event was referred to US-CERT and the Privacy Team.
- One DoS laptop is missing. [redacted] b7E

Classified spillage incident(s) reported to CIRT and referred to DS/IS/APD

- One report that a DoS user in Washington sent an e-mail containing SCI information. This event was referred to APD.

US-CERT Coordination

- Nothing substantial to report

Compliance & Vulnerability Scanning

- *See Appendix B for statistics*

Cyber Threat Analysis Division (CTAD)

DAILY READ FILE: (SBU) Oman Attempts to Improve Cyber Awareness and CND (Computer Network Defense) Capabilities

(SBU) Key Highlights:

- *eOman represents a sweeping effort to modernize the nation's IT knowledge and programs*
- *The ITA is being reorganized to support government and private sector networks*
- *Oman's National CERT is seeking to develop computer and network forensics capabilities*
- *Efforts include extensive computer training and cyber awareness campaigns for all citizens*

(SBU) Source Paragraph: "Oman's Information Technology Authority (ITA) was established under the Ministry of National Economy in 2006. On approximately 23 May 2009, ITA was restructured in accordance with Oman's new digital strategy, dubbed eOman."

Source: DIA Cable, IIR 6874 0152 09, "Oman Modernizes to Defend Against Cyber Crimes and Computer and Network Intrusions and Attack (U//FOUO)," 02 June 2009

DECLASSIFIED

0313122A 1030

Telewall Activity from 06/06/2009 to 06/13/2009

254,793	Calls Logged
0	Calls Blocked
14	911 Email Alerts
4	Reports Run for External Customers

Notable Events:

- None

Virus Incident Response Team (VIRT) Statistics *(as of midnight eastern time)*

Spam Blocked at Perimeter:
Previous day: 700,322
Month to date - June: 12,925,199
Year to date for 2009: 262,716,296

Virus Blocked at Perimeter:
Previous day:28
Month to date - June:3,044
Year to date for 2009: 23,159

Cyber Security News Headlines

Homeland Security Keeps Cybersecurity Role *[Source: fcw.com]*
Feds Push Cybersecurity *[Source: pcworld.com]*

DECLASSIFIED

E

Appendix A –CIRT Event Summaries

0317122AJ030

b7E

Legend:	Open Events: 39	Closed Events: 32

US-CIRT Category: CAT 3 (Malicious Code)
Event Type Suspected: Malicious Code directed towards an internal machine

[redacted] CIRT detected a large number of e-mail messages [redacted]

b7E

b7E

Ticket Nu	Location	Bureau	Date Opened	Awaiting Post Response	Post is Remediating	Date Closed
[redacted]	[redacted]	WHA/US	06-12-09			6-15
[redacted]	[redacted]	WHA/US	06-12-09	Yes		
[redacted]	[redacted]	WHA/US	06-12-09			6-15
[redacted]	[redacted]	WHA/US	06-12-09	Yes		
[redacted]	[redacted]	WHA/US	06-12-09			6-15
[redacted]	[redacted]	WHA/US	06-12-09	Yes		
[redacted]	[redacted]	WHA/US	06-12-09			6-15
[redacted]	[redacted]	WHA/US	06-12-09	Yes		
[redacted]	[redacted]	WHA/US	06-12-09	Yes		
[redacted]	[redacted]	WHA/US	06-12-09	Yes		
[redacted]	[redacted]	AF	06-12-09			6-15
[redacted]	[redacted]	EUR	06-12-09	Yes		
[redacted]	[redacted]	EAP	06-12-09	Yes		
[redacted]	[redacted]	EUR	06-12-09			6-15
[redacted]	[redacted]	EUR	06-12-09	Yes		
[redacted]	[redacted]	EAP	06-12-09	Yes		
[redacted]	[redacted]	EUR	06-12-09	Yes		
[redacted]	[redacted]	EUR	06-12-09	Yes		
[redacted]	[redacted]	EUR	06-12-09			6-15
[redacted]	[redacted]	EUR	06-12-09			6-15
[redacted]	[redacted]	EAP	06-12-09			6-15
[redacted]	[redacted]	EUR	06-12-09	Yes		
[redacted]	[redacted]	AF	06-12-09	Yes		

[illegible]

Ticket Numb	Location	Bureau	Date Opened	Awaiting Post Response	Post is Remediating	Date Closed
[redacted]	[redacted]	AF	06-12-09			6-15
[redacted]	[redacted]	EUR	06-12-09			6-15
[redacted]	[redacted]	EAP	06-12-09			6-15
[redacted]	[redacted]	EUR	06-12-09			6-15
[redacted]	[redacted]	AF	06-12-09	Yes		
[redacted]	[redacted]	AF	06-12-09	Yes		
[redacted]	[redacted]	SCA	06-12-09	Yes		
[redacted]	[redacted]	EUR	06-12-09	Yes		
[redacted]	[redacted]	AF	06-12-09	Yes		
[redacted]	[redacted]	EUR	06-12-09			6-15
[redacted]	[redacted]	AF	06-12-09			6-15
[redacted]	[redacted]	WHA	06-12-09	Yes		
[redacted]	[redacted]	AF	06-12-09	Yes		
[redacted]	[redacted]	NEA	06-12-09	Yes		
[redacted]	[redacted]	AF	06-12-09	Yes		
[redacted]	[redacted]	AF	06-12-09			6-15
[redacted]	[redacted]	AF	06-12-09	Yes		
[redacted]	[redacted]	AF	06-12-09			6-15
[redacted]	[redacted]	EUR	06-12-09			6-15
[redacted]	[redacted]	AF	06-12-09			6-15
[redacted]	[redacted]	AF	06-12-09	Yes		
[redacted]	[redacted]	EAP	06-12-09			6-15
[redacted]	[redacted]	AF	06-12-09	Yes		
[redacted]	[redacted]	AF	06-12-09			6-15
[redacted]	[redacted]	AF	06-12-09			6-15
[redacted]	[redacted]	AF	06-12-09	Yes		
[redacted]	[redacted]	AF	06-12-09	Yes		
[redacted]	[redacted]	AF	06-12-09	Yes		
[redacted]	[redacted]	EAP	06-12-09			6-15
[redacted]	[redacted]	EAP	06-12-09			6-15
[redacted]	[redacted]	EUR	06-12-09	Yes		
[redacted]	[redacted]	NEA	06-12-09	Yes		
[redacted]	[redacted]	NEA	06-12-09	Yes		
[redacted]	[redacted]	AF	06-12-09			6-15
[redacted]	[redacted]	AF	06-12-09			6-15
[redacted]	[redacted]	EUR	06-12-09			6-15

b7E

DECLASSIFIED

b7E

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Suspicious/Abnormal traffic

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/12/2009 0424 GMT	**Affected Bureau:** EAP

Event Description
CIRT detected an exposure to malicious code, [redacted]

b7E

Current Status
15 Jun: The ISSO reported that the user is traveling this week and therefore he is unable to check the user's mailbox.

Status History
12 Jun: CIRT requested that the ISSO search for malicious files and verify that the installed [redacted] ie.

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: E-mail - Malicious Payload (Code, Attachment, Link)

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/11/2009 1301 GMT	**Affected Bureau:** DOM

Event Description
CIRT was notified by CTAD regarding malicious e-mail attachments that have been sent to DoS users.

Current Status
15 Jun: The CIRT requested an update from the ISSO via e-mail.

Status History
11 Jun: CIRT requested that the ISSO determine if the suspicious e-mails had been delivered to the mailboxes of the recipients in question. If found, CIRT requested that the [redacted]

b7E

12 Jun: CIRT was notified by the IT Service Center that two of the four recipients are currently out of the office. One of the recipients reported that he did not receive the e-mail message.

DECLASSIFIED

b7C
E

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: E-mail - Phishing

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/13/2009 0759 GMT	**Affected Bureau:** DOM

Event Description
CIRT detected a malicious PDF [redacted] being directed at a DoS workstation.

b7C

Current Status
15 Jun: CIRT requested a status update from the ISSO via e-mail.

Status History
13 Jun: CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/13/2009 0950 GMT	**Affected Bureau:** DOM

Event Description
CIRT detected a malicious PDF [redacted] being directed at a DoS workstation.

b7E

Current Status
15 Jun: The ISSO is examining this event and will update CIRT once completed.

Status History
13 Jun: CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Malicious Code directed towards an internal machine

Ticket Number: [redacted]	**Location** [redacted]
Date and Time Ticket Created: 06/15/2009 1134 GMT	**Affected Bureau:** EUR

Event Description
CIRT detected a malicious executable file directed at a DoS workstation.

Current Status
15 Jun: CIRT requested that the ISSO search for specific files and remove the files if

b 7E

they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

Status History
N/A - New Event

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Non-event

Ticket Number:	**Location:**
Date and Time Ticket Created: 06/15/2009 1308 GMT	**Affected Bureau:** WHA

Event Description
One DoS laptop containing PII is missing.

Current Status
15 Jun: This PII event has been forwarded to US-CERT and the Privacy Team. CIRT is awaiting confirmation from both groups that the PII incident report has been received.

Status History
N/A - New Event

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Unauthorized Software Installed on a DoS machine

Ticket Number:	**Location:**
Date and Time Ticket Created: 06/12/2009 0948 GMT	**Affected Bureau:** EUR

Event Description
CIRT was notified of unauthorized software being installed onto DoS workstations.

Current Status
15 Jun: CIRT requested an update from the ISSO via e-mail.

Status History
12 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

DECLASSIFIED

b7E

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Email - Malicious Payload (Code, Attachment, Link)

[redacted] CIRT detected a large number of e-mail messages [redacted]

b7E

Ticket Number	Location	Date Opened	Awaiting Post Response	Post is Remediating	Date Closed
12864	SA-44	June 04			June 14

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Virus/Worm on internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/10/2009 1335 GMT	**Affected Bureau:** WHA

Event Description
CIRT detected a DoS workstation communicating with a suspicious website and possibly downloading a malicious .exe file.

Final Action
15 Jun: The ISSO confirmed that the workstation has been removed from the network and re-imaged.

Status History
10 Jun: The ISSO reported that he will examine the workstation and inform CIRT of the results.
11 Jun: CIRT requested a status update from the ISSO via e-mail.
12 Jun: CIRT requested that the ISSO disconnect the workstation from the network and reimage the operating system.
14 Jun: CIRT requested a status update from the ISSO via e-mail.

US-CERT Category: CAT 4 (Improper Usage)
Event Type Confirmed: Unauthorized Software Downloaded to a DoS machine

DECLASSIFIED

Ticket Number:	**Location**
Date and Time Ticket Created: 06/12/2009 0959 GMT	**Affected Bureau:** DOM
Event Description CIRT detected the download of a malicious executable to a DoS workstation.	
Final Action **15 Jun: The ISSO reported that none of the files described were found. A virus scan showed no trace of malicious activity. The patches are up-to-date.**	
Status History **12 Jun:** CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management. **14 Jun:** CIRT requested a status update from the ISSO via e-mail.	

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Information Security Issue (violation or infraction)

Ticket Number:	**Location:**
Date and Time Ticket Created: 06/15/2009 0712 GMT	**Affected Bureau:** DOM
Event Description A DoS Bureau reported a possible classified spillage.	
Final Action **15 Jun: This event was referred to APD.**	
Status History **N/A - New Event**	

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Non-event

Ticket Number:	**Location**
Date and Time Ticket Created: 06/15/2009 1225 GMT	**Affected Bureau:** DOM
Event Description Personally Identifiable Information (PII) may have been breached or disclosed to unauthorized third parties.	

Final Action

15 Jun: This event has been referred to US-CERT and the Privacy Team.

DECLASSIFIED

Status History

N/A - New Event

DECLASSIFIED

b7E

Appendix B – Compliance & Vulnerability Scanning Statistics

Vulnerability Totals:

Total Critical Vulnerabilities: 8,422
Total High Vulnerabilities: 498,550

Top 10 Critical Vulnerabilities

Vulnerability	CVSS Score	Count
	10.00	1182
	10.00	1163
	10.00	1005
	10.00	800
	10.00	543
	10.00	490
	10.00	371
	10.00	360
	10.00	243
	10.00	217

b7E

Top 10 High Vulnerabilities

	CVSS Score	Count
	9.30	26335
	7.00	25683
	9.30	24035
	9.30	23987
	9.30	23779
	9.30	16627
	9.30	12744
	9.30	12733
	9.30	7806

b7E

DECLASSIFIED

QuickTime < 7.2 Security Update (Windows)	9.30	7786

DECLASSIFIED

Top 10 Most Common Vulnerabilities

Vulnerability	CVSS Score	Count
	9.30	26335
	7.00	25683
	9.30	24035
	9.30	23987
	9.30	23779
	5.10	23611
	9.30	16627
	9.30	12744
	9.30	12733
	9.30	7806

b7E

Top 10 Compliance Failures

Configuration Setting	Count
	63848
	61204
	60870
	60869
	54313
	52366
	44313
	34906
	34904
	32491

b7E

DECLASSIFIED

DECLASSIFIED

Appendix C – DoS Cyber Condition (CyberCon) Levels

CyberCon Level	Tripwires	Actions
EMERGENCY **Significant cyber attacks are currently occurring**	• Degradation, denial, or destruction of systems • Highly sophisticated attacks • Major tensions within country / significant catastrophic events • ***DoS is unable to execute its diplomatic mission*** • ***Widespread or focused attacks targeting vulnerabilities within the enterprise require an immediate coordinated response.*** • ***Network infrastructure throughput is severed.*** • ***Common network services are disrupted.*** • ***Sensitive information in the enterprise is at high risk of compromise.***	• Disconnection of Internet connectivity • Task Force initialization • Documented Remediation Steps completed and verified prior to re-connection
HIGH **Significant cyber attacks are imminent or moderate attacks are occurring**	• Widespread malicious activity • Intelligence indicates targeted activity • Increase in sophisticated recon and probes • Heightened tensions within country or major event • ***DoS must resort to alternative communications means to execute its diplomatic mission*** • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at moderate risk of compromise.***	• Initiate Management Team briefings • Three-times-a-day notification to pre-determined recipient list • Additional sniffers deployed as needed • Authorize limited OT for analysts

DECLASSIFIED

DECLASSIFIED

ELEVATED **Moderate cyber attacks are imminent**	• Increased risk • Limited malicious activity • Intelligence indicates general threats • Specific incidents reported and under review • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at some risk of compromise.***	• Ensure protective measures implemented • Increase backups, audits, etc. • Verify response action plans & staff ready • Document changes in cyber security posture
GUARDED **Nuisance cyber attack activity is present**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Potential malicious activity within the enterprise may be handled thorough routine channels and procedures.*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.*** • ***Existing countermeasures are likely to be adequate to counter this threat***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures
LOW **Nuisance cyber attack activity is expected**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Automated response is sufficient to counter potential malicious activity within the enterprise*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures

Appendix D – Intranet Web Links of Interest

DECLASSIFIED

Within the Office of Computer Security

- **Awareness**
  Periodic Update: http://cs.ds.state.gov/ETPA/ETPA_03.cfm
- **Computer Incident Response Team (CIRT)**
  Periodic Update: http://cs.ds.state.gov/CIRT/CIRT_08.cfm
- **Cyber Threat Analysis Division (CTAD)**
  Daily Read File: http://source.ds.state.sgov.gov (ClassNet)
  Tactical Awareness: http://cs.ds.state.gov/CTAD/CTAD_07.cfm
- **The Office of Computer Security**
  Periodic Update: http://cs.ds.state.gov/index.cfm
- **Compliance and Vulnerability Scanning**
  Periodic Update: http://cs.ds.state.gov/index.cfm

Outside of the Office of Computer Security

- **Cyber Security Incident Program**
  Periodic Update: http://csip.ds.state.gov
- **Enterprise Network Management**
  Periodic Update: http://enm.irm.state.gov
- **The Office of Information Assurance**
  Periodic Update: http://ia.irm.state.gov/
- **Patch Management**
  Periodic Update: http://enm.irm.state.gov/nlm/patch/Default.htm
- **Virus Incident Response Team (VIRT)**
  Periodic Update: http://sysintegweb.irm.state.gov/si/AntiVirus.html

The CIRT welcomes all constructive feedback to the daily Cyber Security Brief. If you have feedback for the CSB, please send it to CIRT@state.gov

007

b7C

Cyber Security Brief

United States Department of State
Bureau of Diplomatic Security
as of June 16, 2009-1400 EST

June 17, 2009

Current DoS Cyber Threat Condition

GUARDED

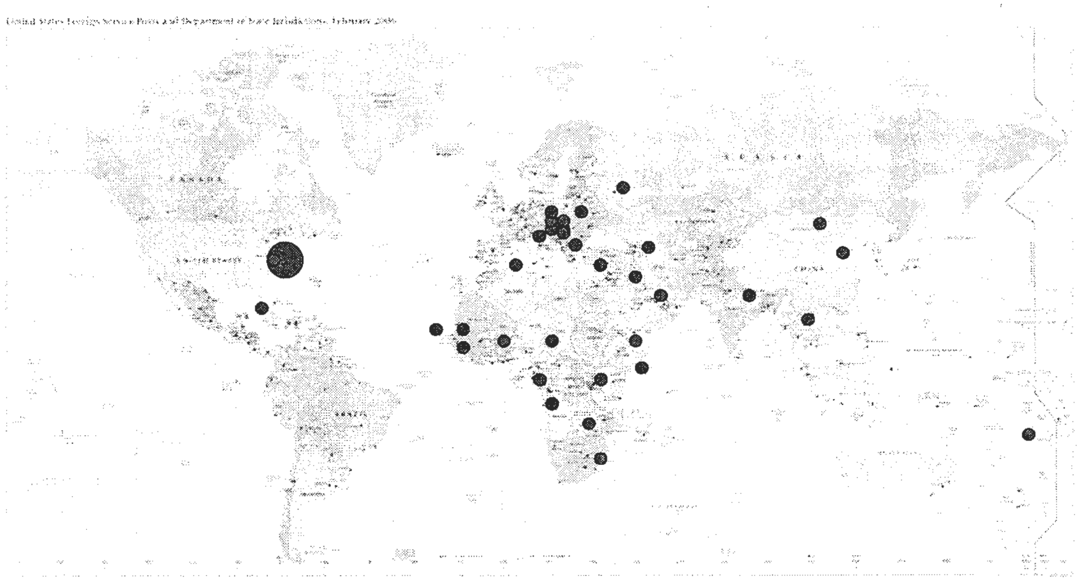
No change from last reported condition

Nuisance cyber attack activity is present

Executive Summary

1. CIRT
   - CIRT is awaiting the ISSOs' responses and remediation confirmations on the remaining spear-phishing attack notifications.
2. CTAD Daily Read File
   - (Classified content)
3. Personally identifiable information (PII) loss reported
   - One passport application missing

Geographic Distribution of Computer Incident Response Team (CIRT) Events

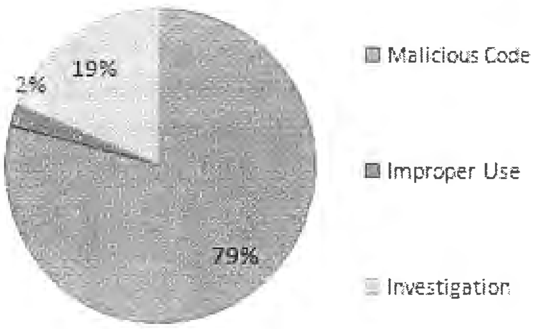

United States Foreign Service Posts and Department of State Jurisdictions, February 2006

Legend: ● *1 event* ● *2 events* ● *3+ events*

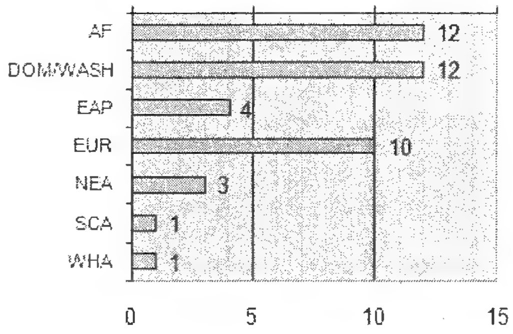
DECLASSIFIED

***Open CIRT Events:* 27** ***Closed CIRT Events:* 16**

CIRT Events by US-CERT Category



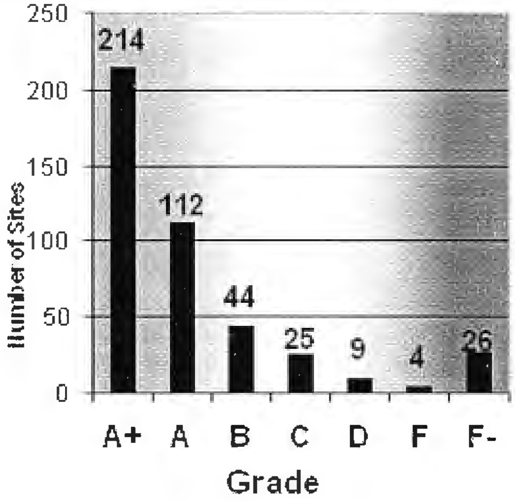
CIRT Events by Bureau



Firewall Block Request Summary

- Nothing substantial to report

Enterprise Risk Score Grade Distribution



Computer Incident Response Team (CIRT)

- CIRT is awaiting the ISSOs' responses and remediation confirmations on the remaining spear-phishing attack notifications of e-mails with a malicious PDF attachment. Due to the large number of tickets generated by this event, these tickets are presented in <u>table</u> format.

DECLASSIFIED

Personally identifiable information (PII) loss reported:

- One passport application mailed from a postal acceptance facility in the Philadelphia Passport Agency region cannot be located at this time. This event was referred to US-CERT and the Privacy Team.

Classified spillage incident(s) reported to CIRT and referred to DS/IS/APD

- Nothing substantial to report

US-CERT Coordination

- Nothing substantial to report

Compliance & Vulnerability Scanning

- *See Appendix B for statistics*

Cyber Threat Analysis Division (CTAD)

DAILY READ FILE: (Classified content – See CTAD Daily Read File on ClassNet for details)

Virus Incident Response Team (VIRT) Statistics *(as of midnight eastern time)*

Spam Blocked at Perimeter:	**Virus Blocked at Perimeter:**
Previous day: 1,002,128	Previous day:104
Month to date - June: 13,927,327	Month to date - June:3,148
Year to date for 2009: 263,718,424	Year to date for 2009: 23,263

Cyber Security News Headlines

IG: DHS Intel Folks Need Cyber Education *[Source: techinsider.nextgov.com]*

DECLASSIFIED

b7E

Appendix A –CIRT Event Summaries

Legend:	Open Events: 27	Closed Events: 16

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Malicious Code directed towards an internal machine

[redacted] CIRT detected a large number of e-mail messages [redacted]

b7E

Ticket Number	Location	Bureau	Date Opened	Post Response	Post is Remediating	Date Closed
		WHA/US	06-12-09	Yes		
		WHA/US	06-12-09	Yes		
		WHA/US	06-12-09	Yes		
		WHA/US	06-12-09	Yes		
		WHA/US	06-12-09			6-16
		WHA/US	06-12-09			6-16
		EAP	06-12-09	Yes		
		EAP	06-12-09	Yes		
		EUR	06-12-09			6-16
		EAP	06-12-09	Yes		
		EUR	06-12-09	Yes		
		EUR	06-12-09			6-16
		EUR	06-12-09			6-16
		AF	06-12-09	Yes		
		AF	06-12-09	Yes		
		AF	06-12-09			6-16
		SCA	06-12-09			6-16
		EUR	06-12-09	Yes		
		AF	06-12-09	Yes		
		WHA	06-12-09	Yes		
		AF	06-12-09	Yes		
		NEA	06-12-09	Yes		
		AF	06-12-09			6-16
		AF	06-12-09			6-16
		AF	06-12-09	Yes		
		AF	06-12-09	Yes		

b7E

DECLASSIFIED

E b7E

Ticket Number	Location	Bureau	Date Opened	Awaiting Post Response	Post is Remediating	Date Closed
[redacted]	[redacted]	AF	06-12-09	Yes		
[redacted]	[redacted]	AF	06-12-09			6-16
[redacted]	[redacted]	AF	06-12-09	Yes		
[redacted]	[redacted]	EUR	06-12-09	Yes		
[redacted]	[redacted]	NEA	06-12-09			6-16
[redacted]	[redacted]	NEA	06-12-09	Yes		

b7E

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Suspicious/Abnormal traffic

✓

Ticket Number: 1[redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/12/2009 0424 GMT	**Affected Bureau:** EAP

Event Description
CIRT detected an exposure to malicious code. This event consisted of malicious[redacted] contained within a PDF document. b7E

Current Status
16 Jun: The CIRT is awaiting a response from the ISSO.

Status History
12 Jun: CIRT requested that the ISSO search for malicious files and verify that the installed [redacted] b7E
15 Jun: The ISSO reported that the user is traveling this week and is unable to check his mailbox. CIRT will follow up next week when the user returns.

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: E-mail - Malicious Payload (Code, Attachment, Link)

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/11/2009 1301 GMT	**Affected Bureau:** DOM

Event Description
CIRT was notified by CTAD regarding malicious e-mail attachments that have been sent to DoS users.

Current Status
16 Jun: The ISSO informed CIRT that the e-mail has been deleted from the user's

workstation; however, he is still in the process of removing it from the user's blackberry. CIRT is awaiting confirmation from the ISSO that the e-mail has been fully removed from all devices.
Status History **11 Jun:** CIRT requested that the ISSO determine if the suspicious e-mails had been delivered to the mailboxes of the recipients in question. If found, CIRT requested that the e-mails be deleted [redacted] **12 Jun:** CIRT was notified by the IT Service Center that two of the four recipients are currently out of the office. One of the recipients reported that he did not receive the e-mail message. **15 Jun:** CIRT requested an update from the ISSO via e-mail.

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Malicious Code directed towards an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 0831 GMT	**Affected Bureau:** EUR
Event Description CIRT detected a malicious code being directed to a DoS workstation in an attempt to download an executable file.	
Current Status **16 Jun: CIRT requested that the ISSO search for specific files and reimage the operating system if the files are found.**	
Status History **N/A - New Event**	

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Unauthorized Software Installed on a DoS machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/12/2009 0948 GMT	**Affected Bureau:** EUR
Event Description CIRT was notified of unauthorized software being installed onto DoS workstations.	

UNCLASSIFIED

Current Status **16 Jun: CIRT requested a status update from the ISSO via e-mail.**
Status History **12 Jun:** CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management. **15 Jun:** CIRT requested a status update from the ISSO via e-mail.

US-CERT Category: CAT 6 (Investigation) **Event Type Suspected:** Virus/Worm on an internal machine

Ticket Number:	**Location:**
Date and Time Ticket Created: 06/16/2009 0951 GMT	**Affected Bureau:** DOM
Event Description CIRT detected a DoS workstation communicating with a suspicious website and possibly downloading a	
Current Status **16 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.**	
Status History **N/A - New Event**	

b7E

Ticket Number:	**Location:**
Date and Time Ticket Created: 06/16/2009 1345 GMT	**Affected Bureau:** EUR
Event Description CIRT detected a DoS workstation communicating with a suspicious website and downloading an executable file.	
Current Status **16 Jun: CIRT requested that the ISSO search for specific files and perform an antivirus scan.**	
Status History **N/A - New Event**	

b7E

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: E-mail - Malicious Payload (Code, Attachment, Link)

b7C

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/13/2009 0759 GMT	**Affected Bureau:** DOM

Event Description
CIRT detected a malicious PDF [redacted] being directed at a DoS workstation.

b7C

Final Action
16 Jun: The ISSO responded that the e-mail has been deleted and was not forwarded.

Status History
13 Jun: CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
15 Jun: CIRT requested a status update from the ISSO via e-mail.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/13/2009 0950 GMT	**Affected Bureau:** DOM

Event Description
CIRT detected a malicious [redacted] being directed at a DoS workstation.

b7E

Final Action
16 Jun: The ISSO responded that the e-mail has been deleted and was not forwarded.

Status History
13 Jun: CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
15 Jun: The ISSO is examining this issue and will update CIRT once completed.

US-CERT Category: CAT 4 (Improper Usage)
Event Type Confirmed: Unauthorized Software Downloaded to a DoS machine

Ticket Number: [redacted]	**Location:** F [redacted]
Date and Time Ticket Created: 06/15/2009 1134 GMT	**Affected Bureau:** EUR

Event Description
CIRT detected a malicious executable file directed at a DoS workstation.

DECLASSIFIED

b7E

Final Action
16 Jun: The ISSO reported that the user received an [redacted]

Status History
15 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Non-event

Ticket Number: [redacted]	**Location** [redacted]
Date and Time Ticket Created: 06/15/2009 2119 GMT	**Affected Bureau:** DOM

b7E

Event Description
A DoS employee contacted CIRT regarding the use of a [redacted] n her DoS workstation.

Final Action
16 Jun: No malicious activity was found.

Status History
N/A - New Event

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 1100 GMT	**Affected Bureau:** DOM

Event Description
Personally Identifiable Information (PII) may have been breached or disclosed to unauthorized third parties.

Final Action
16 Jun: This event has been referred to US-CERT and the Privacy Team.

Status History
N/A - New Event

DECLASSIFIED

b7E

DECLASSIFIED

Appendix B – Compliance & Vulnerability Scanning Statistics

VULNERABILITY TOTALS:

Total Critical Vulnerabilities: 8,314
Total High Vulnerabilities: 502,641

TOP 10 CRITICAL VULNERABILITIES

Vulnerability	CVSS Score	Count
[redacted]	10.00	1163
[redacted]	10.00	1113
[redacted]	10.00	965
[redacted]	10.00	800
[redacted]	10.00	551
[redacted]	10.00	491
[redacted]	10.00	373
[redacted]	10.00	361
[redacted]	10.00	243
[redacted]	10.00	216

b7E

TOP 10 HIGH VULNERABILITIES

[redacted]	CVSS Score	Count
[redacted]	9.30	26537
[redacted]	7.00	25867
[redacted]	9.30	24339
[redacted]	9.30	24291
[redacted]	9.30	24084
[redacted]	9.30	16625
[redacted]	9.30	12915
[redacted]	9.30	12905
[redacted]	9.30	7968

b7E

DECLASSIFIED

b6

	9.30	7948

DECLASSIFIED

Top 10 Most Common Vulnerabilities

b7E

CVSS Score	Count
9.30	26537
7.00	25867
9.30	24339
9.30	24291
9.30	24084
5.10	23487
9.30	16625
9.30	12915
9.30	12905
9.30	7968

I op 10 Compliance Failures

b7E

Configuration Setting	Count
	63851
	61207
	60873
	60872
	54316
	52369
	44318
	34909
	34907
	32490

DECLASSIFIED

Appendix C – DoS Cyber Condition (CyberCon) Levels

CyberCon Level	Tripwires	Actions
EMERGENCY **Significant cyber attacks are currently occurring**	• Degradation, denial, or destruction of systems • Highly sophisticated attacks • Major tensions within country / significant catastrophic events • ***DoS is unable to execute its diplomatic mission*** • ***Widespread or focused attacks targeting vulnerabilities within the enterprise require an immediate coordinated response.*** • ***Network infrastructure throughput is severed.*** • ***Common network services are disrupted.*** • ***Sensitive information in the enterprise is at high risk of compromise.***	• Disconnection of Internet connectivity • Task Force initialization • Documented Remediation Steps completed and verified prior to re-connection
HIGH **Significant cyber attacks are imminent or moderate attacks are occurring**	• Widespread malicious activity • Intelligence indicates targeted activity • Increase in sophisticated recon and probes • Heightened tensions within country or major event • ***DoS must resort to alternative communications means to execute its diplomatic mission*** • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at moderate risk of compromise.***	• Initiate Management Team briefings • Three-times-a-day notification to pre-determined recipient list • Additional sniffers deployed as needed • Authorize limited OT for analysts

DECLASSIFIED

DECLASSIFIED

ELEVATED **Moderate cyber attacks are imminent**	• Increased risk • Limited malicious activity • Intelligence indicates general threats • Specific incidents reported and under review • *Attacks targeting vulnerabilities within the enterprise may require a coordinated response.* • *Network infrastructure throughput is noticeably diminished.* • *Common network services are partially disrupted.* • *Sensitive information in the enterprise is at some risk of compromise.*	• Ensure protective measures implemented • Increase backups, audits, etc. • Verify response action plans & staff ready • Document changes in cyber security posture
GUARDED **Nuisance cyber attack activity is present**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • *Potential malicious activity within the enterprise may be handled thorough routine channels and procedures.* • *Network infrastructure throughput is normal.* • *Common network services are not impaired* • *Sensitive information in the enterprise is at slight risk of compromise.* • *Existing countermeasures are likely to be adequate to counter this threat*	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures
LOW **Nuisance cyber attack activity is expected**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • *Automated response is sufficient to counter potential malicious activity within the enterprise* • *Network infrastructure throughput is normal.* • *Common network services are not impaired* • *Sensitive information in the enterprise is at slight risk of compromise.*	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures

DECLASSIFIED

Appendix D – Intranet Web Links of Interest

DECLASSIFIED

Within the Office of Computer Security

- **Awareness**
  Periodic Update: http://cs.ds.state.gov/ETPA/ETPA_03.cfm
- **Computer Incident Response Team (CIRT)**
  Periodic Update: http://cs.ds.state.gov/CIRT/CIRT_08.cfm
- **Cyber Threat Analysis Division (CTAD)**
  Daily Read File: http://source.ds.state.sgov.gov (ClassNet)
  Tactical Awareness: http://cs.ds.state.gov/CTAD/CTAD_07.cfm
- **The Office of Computer Security**
  Periodic Update: http://cs.ds.state.gov/index.cfm
- **Compliance and Vulnerability Scanning**
  Periodic Update: http://cs.ds.state.gov/index.cfm

Outside of the Office of Computer Security

- **Cyber Security Incident Program**
  Periodic Update: http://csip.ds.state.gov
- **Enterprise Network Management**
  Periodic Update: http://enm.irm.state.gov
- **The Office of Information Assurance**
  Periodic Update: http://ia.irm.state.gov/
- **Patch Management**
  Periodic Update: http://enm.irm.state.gov/nlm/patch/Default.htm
- **Virus Incident Response Team (VIRT)**
  Periodic Update: http://sysintegweb.irm.state.gov/si/AntiVirus.html

The CIRT welcomes all constructive feedback to the daily Cyber Security Brief. If you have feedback for the CSB, please send it to CIRT@state.gov

008 b7E

Cyber Security Brief

United States Department of State
Bureau of Diplomatic Security
as of June 17, 2009-1400 EST

June 18, 2009

Current DoS Cyber Threat Condition

GUARDED

No change from last reported condition

Nuisance cyber attack activity is present

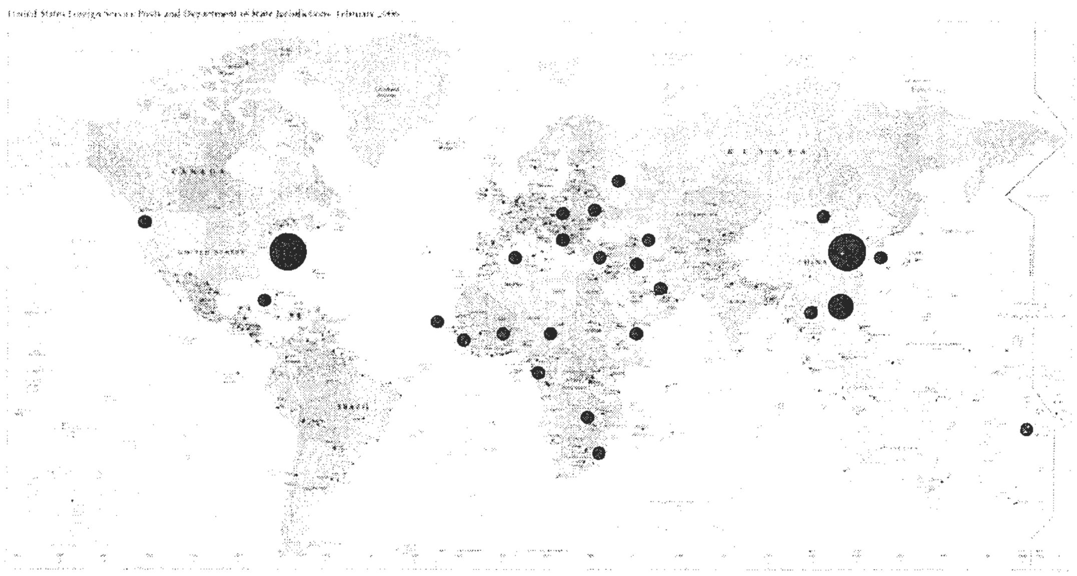
Executive Summary

1. <u>CIRT</u>
   - → b7E
   - CIRT is awaiting the ISSOs' responses and remediation confirmations on the remaining spear-phishing attack notifications.

2. <u>CTAD Daily Read File</u>
   - (U) The Internet, Information Operations, and Iranian Unrest

3. <u>Personally identifiable information (PII) loss reported</u>
   - Two passport applications missing

Geographic Distribution of Computer Incident Response Team (CIRT) Events



Legend: ● *1 event* ● *2 events* ● *3+ events*

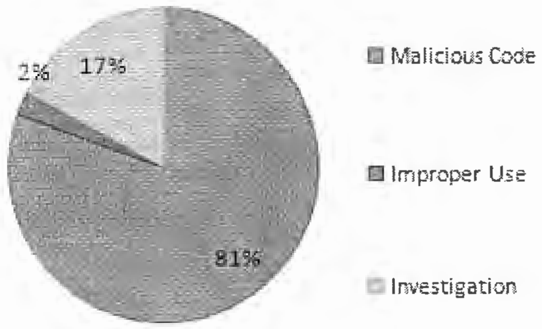
DECLASSIFIED

b7E

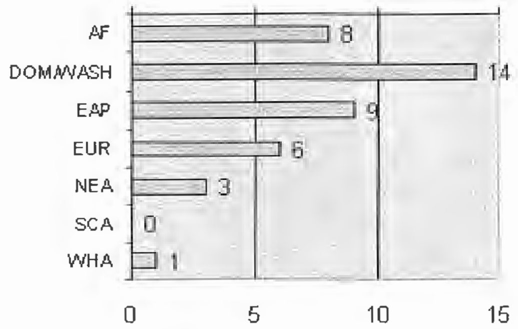
Open CIRT Events: 25

Closed CIRT Events: 16

CIRT Events by US-CERT Category



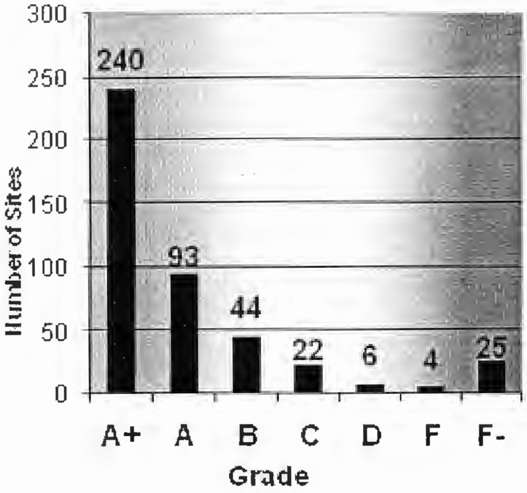
CIRT Events by Bureau



Firewall Block Request Summary

- Nothing substantial to report

Enterprise Risk Score Grade Distribution



Computer Incident Response Team (CIRT)

- An ISSO in Manila, Philippines reported [redacted] b7E
- ~~CIRT is awaiting the ISSOs'~~ responses and remediation confirmations on the remaining spear-phishing attack notifications of e-mails with a malicious PDF attachment. Due to the large number of tickets generated by this event, these tickets are presented in table format.

DECLASSIFIED

Personally identifiable information (PII) loss reported

- Two passport applications mailed from a non-postal acceptance facility in the Seattle Passport Agency region to the Los Angeles Post Office cannot be located at this time. This event has been referred to US-CERT and the Privacy Team.

Classified spillage incident(s) reported to CIRT and referred to DS/IS/APD

- Nothing substantial to report

US-CERT Coordination

- Nothing substantial to report

Compliance & Vulnerability Scanning

- *See Appendix B for statistics*

Cyber Threat Analysis Division (CTAD)

DAILY READ FILE: (U) The Internet, Information Operations, and Iranian Unrest

Key Highlights: (contains classified information)

(U) Source Paragraph: "Pro-democracy activists on the Web are asking supporters to use relatively simple hacking tools to flood the [Iranian] regime's propaganda sites with junk traffic . . . The impact of these distributed denial-of-service (DDOS) attacks isn't clear. But official online outlets like leader.ir, ahmadinejad.ir, and iribnews.ir are currently inaccessible."
Source: Wired (http://www.wired.com),"Activists Launch Hack Attacks on Tehran Regime," 15 June 2009

***Virus Incident Response Team (VIRT) Statistics** (as of midnight eastern time)*

Spam Blocked at Perimeter:	Virus Blocked at Perimeter:
Previous day: 1,002,128	Previous day:104
Month to date - June: 13,927,327	Month to date - June:3,148
Year to date for 2009: 263,718,424	Year to date for 2009: 23,263

Cyber Security News Headlines

New Security for America, via Europe *[Source: newsweek.washingtonpost.com]*
Potential Cyber Chief Hathaway Developing Cybersecurity Response Plan *[Source:gcn.com]*
Cyberdefense Center Will Lead in Education *[Source: infoworld.com]*

DECLASSIFIED

E

b7E

Appendix A –CIRT Event Summaries

DECLASSIFIED

Legend:	Open Events: 25	Closed Events: 16

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Malicious Code directed towards an internal machine

CIRT detected a large number of e-mail messages

b7E

Ticket Number	Location	Bureau	Date Opened	Post Response	Post is Remediating	Date Closed
		WHA/US	06-12-09	Yes		
		WHA/US	06-12-09		Yes	
		WHA/US	06-12-09	Yes		
		WHA/US	06-12-09		Yes	
		EAP	06-12-09	Yes		
		EAP	06-12-09		Yes	
		EAP	06-12-09		Yes	
		EUR	06-12-09	Yes		
		AF	06-12-09	Yes		
		AF	06-12-09	Yes		
		EUR	06-12-09			06-17
		AF	06-12-09			06-17
		WHA	06-12-09			06-17
		AF	06-12-09		Yes	
		NEA	06-12-09			06-17
		AF	06-12-09		Yes	
		AF	06-12-09	Yes		
		AF	06-12-09			06-17
		AF	06-12-09	Yes		
		EUR	06-12-09	Yes		
		NEA	06-12-09			06-17

b7E

DECLASSIFIED

b7E

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Defaced DOS Website (internally or externally hosted)

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 2124 GMT	**Affected Bureau:** DOM

Event Description
An ISSO reported to CIRT that a DoS website [redacted]

b7E

Current Status
17 Jun: CIRT requested a status update from the ISSO via e-mail.

Status History
16 Jun: CIRT requested that the ISSO disconnect the workstation from the network and reimage the operating system.

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: E-mail - Malicious Payload (Code, Attachment, Link)

Ticket Number: [redacted]	**Location** [redacted]
Date and Time Ticket Created: 06/16/2009 1613 GMT	**Affected Bureau:** EAP

Event Description
CIRT detected a large number of e-mail messages with PDF attachments from [redacted]

b7E

Current Status
17 Jun: The ISSO informed CIRT that the workstation has the current version of [redacted]

b7E

Status History
16 Jun: CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.

Ticket Number [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 2023 GMT	**Affected Bureau:** DOM

b7E

Event Description CIRT detected a large number of e-mail messages with PDF attachments from " [redacted]
Current Status **17 Jun: CIRT requested a status update from the ISSO via e-mail.**
Status History **16 Jun:** CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.

b7E

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 2052 GMT	**Affected Bureau:** DOM

Event Description CIRT detected a large number of e-mail messages with PDF attachments from " [redacted]
Current Status **17 Jun: The IT Service Center has provided a reference number for this event.**
Status History **16 Jun:** CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.

b7E

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Malicious Code directed toward internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 1540 GMT	**Affected Bureau:** EAP

Event Description CIRT detected a large number of e-mail messages with PDF attachments from [redacted]

b7E

DECLASSIFIED

b7E

Current Status
17 Jun: **The ISSO reported that he is attempting to contact the e-mail recipients.**

Status History
16 Jun: CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 1827 GMT	**Affected Bureau:** EAP

b7E

Event Description
CIRT detected a large number of e-mail messages with PDF attachments from " [redacted]

b7E

Current Status
17 Jun: CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.

Status History
N/A - New Event

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: E-mail - Malicious Payload (Code, Attachment, Link)

Ticket Number: [redacted]	**Location** [redacted]
Date and Time Ticket Created: 06/11/2009 1301 GMT	**Affected Bureau:** DOM

b7E

Event Description
CIRT was notified by CTAD regarding malicious e-mail attachments that have been sent to DoS users.

Current Status
17 Jun: CIRT requested that the ISSO reimage the workstation of a user who was forwarded the malicious e-mail.

Status History
11 Jun: CIRT requested that the ISSO determine if the suspicious e-mails had been delivered to the mailboxes of the recipients in question. If found, CIRT requested that the e-mails be deleted. [redacted]

b7E

the workstation be removed from the network and re-imaged.

12 Jun: CIRT was notified by the IT Service Center that two of the four recipients are currently out of the office. One of the recipients reported that he did not receive the e-mail message.

15 Jun: CIRT requested an update from the ISSO via e-mail.

16 Jun: The ISSO informed CIRT that the e-mail has been deleted from the user's workstation; however, he is still in the process of removing it from the user's blackberry. CIRT is awaiting confirmation from the ISSO that the e-mail has been fully removed from all devices.

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Malicious Code directed towards an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/17/2009 1006 GMT	**Affected Bureau:** EUR

Event Description

CIRT detected a DoS workstation communicating with a suspicious website and possibly downloading a malicious executable.

Current Status

17 Jun: CIRT requested that the ISSO search for specific files and reimage the operating system if the files are found.

Status History

N/A - New Event

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/17/2009 1408 GMT	**Affected Bureau:** DOM

Event Description

CIRT detected a malicious executable file directed at a DoS workstation

Current Status

17 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

Status History

N/A - New Event

b2

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Virus/Worm on an internal machine

b2

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/17/2009 0904 GMT	**Affected Bureau:** EAP

Event Description
CIRT detected a DoS workstation in communication with a malicious website containing [redacted]

b7E

Current Status
17 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

Status History
N/A - New Event

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Suspicious/Abnormal traffic

b2

Ticket Number: [redacted]	**Location** [redacted]
Date and Time Ticket Created: 06/12/2009 0424 GMT	**Affected Bureau:** EAP

Event Description
CIRT detected an exposure to malicious code. This event consisted of [redacted] contained within a PDF document.

b7E

Final Action
17 Jun: The ISSO informed CIRT that the PDF was not found in the user's e-mail inbox.

Status History
12 Jun: CIRT requested that the ISSO search for malicious files and [redacted]

b7E

15 Jun: The ISSO reported that the user is traveling this week and is unable to check the user's mailbox. CIRT will follow up next week when the user returns.
16 Jun: CIRT is awaiting an update from the ISSO.

b 7E

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: E-mail - Malicious Payload (Code, Attachment, Link)

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 1743 GMT	**Affected Bureau:** EAP

b6

Event Description
CIRT detected a large number of e-mail messages with PDF attachments from [redacted]

b7E

Final Action
17 Jun: The e-mail and attachment were not found on the user's computer. The user does not recall this particular e-mail and regularly deletes these types of e-mails without opening them. The user states that he did not forward this email to anyone.

Status History
16 Jun: CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 1746 GMT	**Affected Bureau:** DOM

b6

Event Description
CIRT detected a large number of e-mail messages with PDF attachments from [redacted]

b7E

Final Action
17 Jun: The IT Service Center/DSD reported that the user deleted the e-mail. The [redacted]

b7E

Status History
16 Jun: CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 2013 GMT	**Affected Bureau:** NEA

b6

b7E

Event Description CIRT detected a large number of e-mail messages with PDF attachments from " [redacted]
Final Action **17 Jun: The ISSO informed CIRT that the e-mail was not forwarded. It has been permanently deleted.**
Status History **16 Jun:** CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.

DECLASSIFIED

b7E

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 1950 GMT	**Affected Bureau:** DOM
Event Description CIRT detected a large number of e-mail messages with PDF attachments from " [redacted]	
Final Action **17 Jun: The ISSO reported that the inbox is not in use. The e-mail was never opened, read or forwarded. It has been permanently deleted.**	
Status History **16 Jun:** CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.	

b7E

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Machine Patched or Not Vulnerable to Exploit

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 0951 GMT	**Affected Bureau:** DOM
Event Description CIRT detected a DoS workstation communicating with a suspicious website and possibly downloading a [redacted]	

b7E

Final Action **17 Jun: The ISSO informed CIRT that the file was not found on the workstation. The results of a virus scan were negative, and patches are current.**	
Status History **16 Jun:** CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.	

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Malicious Code directed toward internal machine

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 1345 GMT	**Affected Bureau:** EUR
Event Description CIRT detected a DoS workstation communicating with a suspicious website and downloading an executable file.	
Final Action **17 Jun: The ISSO confirmed that no unauthorized files were located. A virus scan was performed with negative results.**	
Status History **16 Jun:** CIRT requested that the ISSO search for specific files and perform an antivirus scan.	

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 2040 GMT	**Affected Bureau:** DOM
Event Description CIRT detected a large number of e-mail messages with PDF attachments from " [redacted]	
Final Action **17 Jun: ISSO confirmed that the e-mail was not received by the user and that the** [redacted]	
Status History **16 Jun:** CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.	

b7E

b7E

b7E

US-CERT Category: CAT 4 (Improper Usage)
Event Type Confirmed: Unauthorized Software Installed on a DoS machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/12/2009 0948 GMT	**Affected Bureau:** EUR

Event Description

CIRT was notified of unauthorized software being installed onto DoS workstations.

Final Action

17 Jun: The ISSO informed CIRT that the unauthorized software was removed. A virus scan was performed with negative results.

Status History

12 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

16 Jun: CIRT requested a status update from the ISSO via e-mail.

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Non-event

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 1541 GMT	**Affected Bureau:** DOM

Event Description

Personally Identifiable Information (PII) may have been breached or disclosed to unauthorized third parties.

Final Action

17 Jun: This event has been referred to US-CERT and the Privacy Team.

Status History

N/A - New Event

E

b7E

Appendix B – Compliance & Vulnerability Scanning Statistics

VULNERABILITY TOTALS:

Total Critical Vulnerabilities: 8,419
Total High Vulnerabilities: 509,779

TOP 10 CRITICAL VULNERABILITIES

Vulnerability	CVSS Score	Count
[redacted]	10.00	1167
[redacted]	10.00	1156
[redacted]	10.00	964
[redacted]	10.00	801
[redacted]	10.00	555
[redacted]	10.00	489
[redacted]	10.00	378
[redacted]	10.00	368
[redacted]	10.00	245
[redacted]	10.00	215

b7E

TOP 10 HIGH VULNERABILITIES

[redacted]	CVSS Score	Count
[redacted]	9.30	27136
[redacted]	7.00	26477
[redacted]	9.30	25004
[redacted]	9.30	24958
[redacted]	9.30	24752
[redacted]	9.30	16885
[redacted]	9.30	13185
[redacted]	9.30	13177
[redacted]	9.30	8064

b7E

E

[redacted]	9.30	8044

b7E

DECLASSIFIED

Top 10 Most Common Vulnerabilities

	CVSS Score	Count
[redacted]	9.30	27136
[redacted]	7.00	26477
[redacted]	9.30	25004
[redacted]	9.30	24958
[redacted]	9.30	24752
[redacted]	5.10	23561
[redacted]	9.30	16885
[redacted]	9.30	13185
[redacted]	9.30	13177
[redacted]	9.30	8064

b7E

Top 10 Compliance Failures

Configuration Setting	Count
[redacted]	63993
[redacted]	61381
[redacted]	61042
[redacted]	61041
[redacted]	54477
[redacted]	52488
[redacted]	44402
[redacted]	32634
[redacted]	31801
[redacted]	31799

b7E

DECLASSIFIED

Appendix C – DoS Cyber Condition (CyberCon) Levels

CyberCon Level	Tripwires	Actions
EMERGENCY **Significant cyber attacks are currently occurring**	• Degradation, denial, or destruction of systems • Highly sophisticated attacks • Major tensions within country / significant catastrophic events • ***DoS is unable to execute its diplomatic mission*** • ***Widespread or focused attacks targeting vulnerabilities within the enterprise require an immediate coordinated response.*** • ***Network infrastructure throughput is severed.*** • ***Common network services are disrupted.*** • ***Sensitive information in the enterprise is at high risk of compromise.***	• Disconnection of Internet connectivity • Task Force initialization • Documented Remediation Steps completed and verified prior to re-connection
HIGH **Significant cyber attacks are imminent or moderate attacks are occurring**	• Widespread malicious activity • Intelligence indicates targeted activity • Increase in sophisticated recon and probes • Heightened tensions within country or major event • ***DoS must resort to alternative communications means to execute its diplomatic mission*** • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at moderate risk of compromise.***	• Initiate Management Team briefings • Three-times-a-day notification to pre-determined recipient list • Additional sniffers deployed as needed • Authorize limited OT for analysts

DECLASSIFIED

UNCLASSIFIED

ELEVATED **Moderate cyber attacks are imminent**	• Increased risk • Limited malicious activity • Intelligence indicates general threats • Specific incidents reported and under review • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at some risk of compromise.***	• Ensure protective measures implemented • Increase backups, audits, etc. • Verify response action plans & staff ready • Document changes in cyber security posture
GUARDED **Nuisance cyber attack activity is present**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Potential malicious activity within the enterprise may be handled thorough routine channels and procedures.*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.*** • ***Existing countermeasures are likely to be adequate to counter this threat***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures
LOW **Nuisance cyber attack activity is expected**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Automated response is sufficient to counter potential malicious activity within the enterprise*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures

Appendix D – Intranet Web Links of Interest

DECLASSIFIED

Within the Office of Computer Security

- **Awareness**
  Periodic Update: http://cs.ds.state.gov/ETPA/ETPA_03.cfm
- **Computer Incident Response Team (CIRT)**
  Periodic Update: http://cs.ds.state.gov/CIRT/CIRT_08.cfm
- **Cyber Threat Analysis Division (CTAD)**
  Daily Read File: http://source.ds.state.sgov.gov (ClassNet)
  Tactical Awareness: http://cs.ds.state.gov/CTAD/CTAD_07.cfm
- **The Office of Computer Security**
  Periodic Update: http://cs.ds.state.gov/index.cfm
- **Compliance and Vulnerability Scanning**
  Periodic Update: http://cs.ds.state.gov/index.cfm

Outside of the Office of Computer Security

- **Cyber Security Incident Program**
  Periodic Update: http://csip.ds.state.gov
- **Enterprise Network Management**
  Periodic Update: http://enm.irm.state.gov
- **The Office of Information Assurance**
  Periodic Update: http://ia.irm.state.gov/
- **Patch Management**
  Periodic Update: http://enm.irm.state.gov/nlm/patch/Default.htm
- **Virus Incident Response Team (VIRT)**
  Periodic Update: http://sysintegweb.irm.state.gov/si/AntiVirus.html

The CIRT welcomes all constructive feedback to the daily Cyber Security Brief. If you have feedback for the CSB, please send it to CIRT@state.gov

DECLASSIFIED

P 009

b7E

b7E

Cyber Security Brief

United States Department of State
Bureau of Diplomatic Security
as of June 18, 2009-1400 EST

June 19, 2009

Current DoS Cyber Threat Condition

GUARDED

No change from last reported condition

Nuisance cyber attack activity is present

Executive Summary

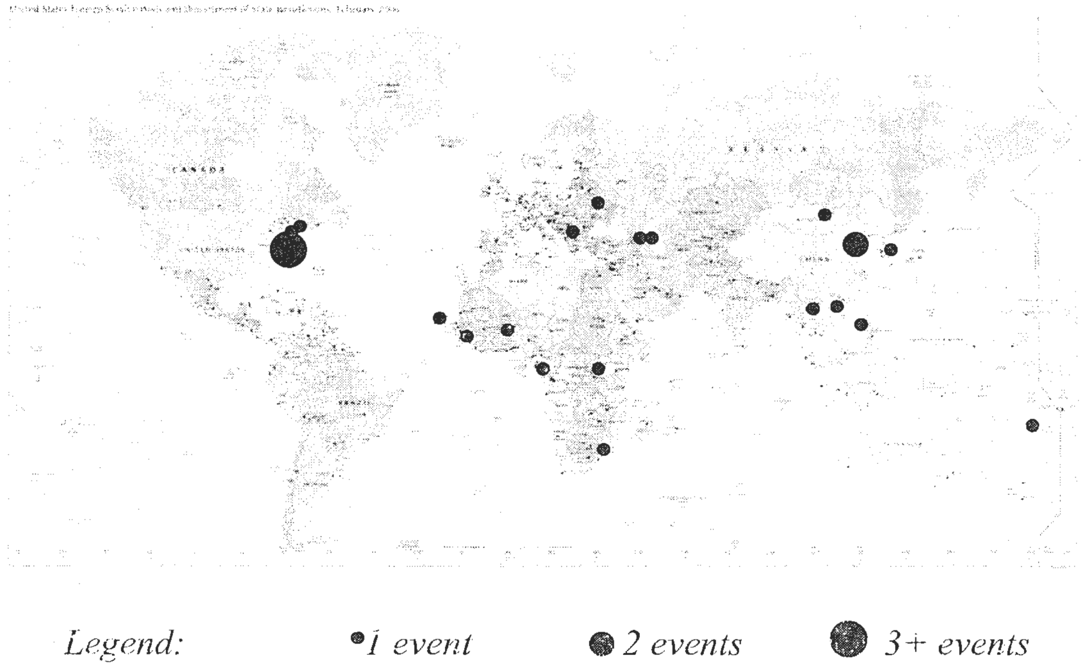
1. CIRT
   - CIRT is awaiting the ISSOs' responses and remediation confirmations on the remaining spear-phishing attack notifications.

2. CTAD Daily Read File
   -

b7E

3. Personally identifiable information (PII) loss reported
   - Twenty-three passport applications missing

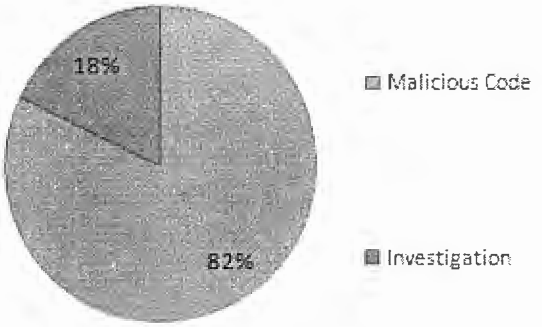
Geographic Distribution of Computer Incident Response Team (CIRT) Events



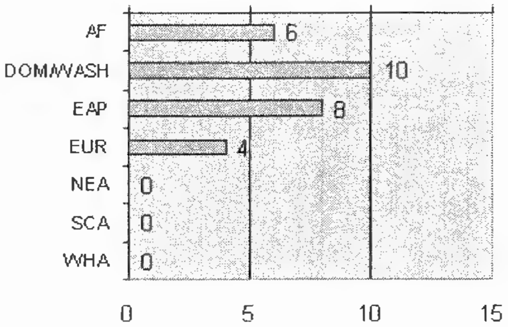
Open CIRT Events: 16

Closed CIRT Events: 12

CIRT Events by US-CERT Category



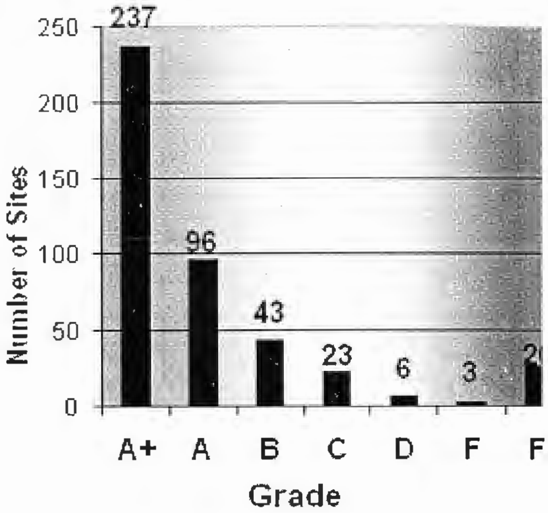
CIRT Events by Bureau



Firewall Block Request Summary

- Nothing substantial to report

Enterprise Risk Score Grade Distribution



Computer Incident Response Team (CIRT)

- CIRT is awaiting the ISSOs' responses and remediation confirmations on the remaining spear-phishing attack notifications of e-mails with a malicious PDF attachment. Due to the large number of tickets generated by this event, these tickets are presented in table format.

b7E

Personally identifiable information (PII) loss reported

- Three passport applications mailed from a postal acceptance facility in the Boston Passport Agency region to the Lindberg Postal Distribution Center cannot be located at this time. This event has been referred to US-CERT and the Privacy Team.
- Twenty passport applications mailed from a postal acceptance facility in the New York Passport Agency region to the Lindberg Postal Distribution Center cannot be located at this time. This event has been referred to US-CERT and the Privacy Team.

Classified spillage incident(s) reported to CIRT and referred to DS/IS/APD

- Nothing substantial to report

US-CERT Coordination

- Nothing substantial to report

Compliance & Vulnerability Scanning

- *See Appendix B for statistics*

Cyber Threat Analysis Division (CTAD)

DAILY READ FILE: (SBU) [[redacted]

Key Highlights: (classified content)

(U) Source Paragraph: "China and the U.S. failed to achieve a breakthrough at their latest round of climate talks on Wednesday, raising the stakes in the global effort to fight global climate change. The two countries responsible for almost half of the world's greenhouse gas [GHG] emissions ended three days of negotiations in Beijing."
Source: Financial Times (http://www.ft.com), "Biggest emitters fail to show the way forward," 10 June 2009.

***Virus Incident Response Team (VIRT) Statistics** (as of midnight eastern time)*

Spam Blocked at Perimeter:	Virus Blocked at Perimeter:
Previous day: 1,002,128	Previous day:104
Month to date - June: 13,927,327	Month to date - June:3,148
Year to date for 2009: 263,718,424	Year to date for 2009: 23,263

Cyber Security News Headlines

New Information Security Controls to Strengthen Federal Cybersecurity Standards *[Source: gcn.com]*
NIST Revises Guidance for Telework Security *[Source: gcn.com]*
Picking the Cybersecurity Czar *[Source: govinfosecurity.com]*

b7E

Appendix A –CIRT Event Summaries

Legend:	*Open Events: 16*	*Closed Events: 12*

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Malicious Code directed towards an internal machine

[redacted] CIRT detected a large number of e-mail messages [redacted]

b7E

Ticket Number	Location	Bureau	Date Opened	Awaiting Post Response	Post is Remediating	Date Closed
[redacted]	[redacted]	WHA/US	06-12-09	Yes		
[redacted]	[redacted]	WHA/US	06-12-09		Yes	
[redacted]	[redacted]	WHA/US	06-12-09	Yes		
[redacted]	[redacted]	WHA/US	06-12-09			06-18
[redacted]	[redacted]	EAP	06-12-09	Yes		
[redacted]	[redacted]	EAP	06-12-09		Yes	
[redacted]	[redacted]	EAP	06-12-09		Yes	
[redacted]	[redacted]	EUR	06-12-09			06-18
[redacted]	[redacted]	AF	06-12-09	Yes		
[redacted]	[redacted]	AF	06-12-09			06-18
[redacted]	[redacted]	AF	06-12-09			06-18
[redacted]	[redacted]	AF	06-12-09		Yes	
[redacted]	[redacted]	AF	06-12-09	Yes		
[redacted]	[redacted]	AF	06-12-09	Yes		
[redacted]	[redacted]	EUR	06-12-09			06-18

b7E

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Defaced DoS Website (internally or externally hosted)

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 2124 GMT	**Affected Bureau:** EAP
Event Description An ISSO reported to CIRT that a DoS website [redacted]	

b7E

[redacted]

b7E

Current Status
18 Jun: CIRT requested additional information from the ISSO.

Status History
16 Jun: CIRT requested that the ISSO disconnect the workstation from the network and reimage the operating system.
17 Jun: CIRT requested a status update from the ISSO via e-mail.

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: E-mail - Malicious Payload (Code, Attachment, Link)

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 2023 GMT	**Affected Bureau:** DOM

B ✓

Event Description
CIRT detected a large number of e-mail messages with PDF attachments from " [redacted]

b7E

Current Status
18 Jun: CIRT requested a status update from the ISSO via e-mail.

Status History
16 Jun: CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
17 Jun: CIRT requested a status update from the ISSO via e-mail.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 2052 GMT	**Affected Bureau:** DOM

Bm ✓

Event Description
CIRT detected a large number of e-mail messages with PDF attachments from " [redacted]

b7E

Current Status
18 Jun: CIRT requested a status update from the ISSO via e-mail.

Status History

16 Jun: CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
17 Jun: The IT Service Center has provided a reference number for this event.

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Malicious Code directed towards an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 1540 GMT	**Affected Bureau:** EAP

Event Description
CIRT detected a large number of e-mail messages with PDF attachments from [redacted]

b7E

Current Status
18 Jun: The ISSO informed CIRT that the user is at a remote office. The ISSO will contact the user for more information regarding this e-mail.

Status History
16 Jun: CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted.
17 Jun: The ISSO responded that he is attempting to contact the e-mail recipients.

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Malicious Code directed towards an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/17/2009 1408 GMT	**Affected Bureau:** DOM

Event Description
CIRT detected a malicious executable file directed at a DoS workstation

Current Status
18 Jun: CIRT requested a status update from the ISSO via e-mail.

Status History
17 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

DECLASSIFIED

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Virus/Worm on internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/17/2009 0904 GMT	**Affected Bureau:** EAP

Event Description
CIRT detected a DoS workstation in communication with a malicious website containing [redacted]s.

b7E

Current Status
18 Jun: CIRT requested a status update from the ISSO via e-mail.

Status History
17 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: E-mail - Malicious Payload (Code, Attachment, Link)

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/11/2009 1301 GMT	**Affected Bureau:** DOM

Event Description
CIRT was notified by CTAD regarding malicious e-mail attachments that have been sent to DoS users.

Final Action
18 Jun: The ISSO informed CIRT that the machine has been reimaged. The e-mail has been removed from all devices.

Status History
11 Jun: CIRT requested that the ISSO determine if the suspicious e-mails had been delivered to the mailboxes of the recipients in question. [redacted]

b7E

12 Jun: CIRT was notified by the IT Service Center that two of the four recipients are currently out of the office. One of the recipients reported that he did not receive the e-mail message.
16 Jun: The ISSO informed CIRT that the e-mail has been deleted from the user's workstation; however, he is still in the process of removing it from the user's blackberry. CIRT is awaiting confirmation from the ISSO that the e-mail has been fully removed from all devices.
17 Jun: CIRT requested that the ISSO reimage the workstation of a user who was forwarded

b7E

the malicious e-mail.

DECLASSIFIED

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 1613 GMT	**Affected Bureau:** EAP
Event Description CIRT detected a large number of e-mail messages with PDF attachments from " [redacted]	
Final Action **18 Jun: The ISSO confirmed that the e-mail was not received by the user and that the** [redacted]	
Status History **16 Jun:** CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system. **17 Jun:** The ISSO informed CIRT that [redacted] the user is on leave until June 18th. CIRT will await confirmation from the ISSO that the e-mail has been deleted once the user returns.	

b7E

b7E

b7E

US-CERT Category: CAT 3 (Malicious Code) **Event Type Confirmed:** Malicious Code directed towards an internal machine

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/17/2009 1558 GMT	**Affected Bureau:** EUR
Event Description CIRT detected a DoS workstation communicating with a suspicious website and possibly downloading a malicious .exe file with a PDF attachment.	
Final Action **18 Jun: CIRT requested that the ISSO search for a malicious file on the workstation. The ISSO informed CIRT that the file was not found. The results of a virus scan were negative.**	
Status History **N/A - New Event**	

✓

Ticket Number: [redacted]	**Location:** [redacted]

DECLASSIFIED

b7E

Date and Time Ticket Created: 06/17/2009 1006 GMT	**Affected Bureau:** EUR
Event Description CIRT detected a DoS workstation communicating with a suspicious website and possibly downloading a malicious executable.	
Final Action **18 Jun: The ISSO informed CIRT that no malicious or unauthorized files were found. Antivirus definitions are up-to-date, and a scan was successfully completed with negative results. The computer is current with all of the latest patches from IRM Patch Management.**	
Status History **17 Jun:** CIRT requested that the ISSO search for specific files and reimage the operating system if the files are found.	

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Non-event

EM ✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 1827 GMT	**Affected Bureau:** EAP
Event Description CIRT detected a large number of e-mail messages with PDF attachments from " [redacted]	
Final Action **18 Jun: The ISSO informed CIRT that the Exchange administrator was able to delete the e-mail from the Exchange server. The e-mail had not been opened.**	
Status History **17 Jun:** CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.	

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Information Security Issue (violation or infraction)

EM ✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/18/2009 1004 GMT	**Affected Bureau:** DOM
Event Description	

b7E

Personally Identifiable Information (PII) may have been breached or disclosed to unauthorized third parties.
Final Action **18 Jun: This event has been referred to US-CERT and the Privacy Team.**
Status History **N/A - New Event**

DECLASSIFIED

Ticket Number:	**Location:**
Date and Time Ticket Created: 06/18/2009 1015 GMT	**Affected Bureau:** DOM
Event Description Personally Identifiable Information (PII) may have been breached or disclosed to unauthorized third parties.	
Final Action **18 Jun: This event has been referred to US-CERT and the Privacy Team**	
Status History **N/A - New Event**	

DECLASSIFIED

b7E

DECLASSIFIED

Appendix B – Compliance & Vulnerability Scanning Statistics

Vulnerability Totals:

Total Critical Vulnerabilities: 8,526
Total High Vulnerabilities: 512,659

Top 10 Critical Vulnerabilities

Vulnerability	CVSS Score	Count
[redacted]	10.00	1190
[redacted]	10.00	1151
[redacted]	10.00	971
[redacted]	10.00	802
[redacted]	10.00	541
[redacted]	10.00	484
[redacted]	10.00	399
[redacted]	10.00	373
[redacted]	10.00	259
[redacted]	10.00	216

b7E

Top 10 High Vulnerabilities

[redacted]	CVSS Score	Count
[redacted]	9.30	27248
[redacted]	7.00	26476
[redacted]	9.30	25149
[redacted]	9.30	25100
[redacted]	9.30	24908
[redacted]	9.30	17002
[redacted]	9.30	13307
[redacted]	9.30	13296
[redacted]	9.30	8151
[redacted]	9.30	8124

b7E

DECLASSIFIED

b7E

DECLASSIFIED

Top 10 Most Common Vulnerabilities

Vulnerability	CVSS Score	Count
[redacted]	9.30	27248
[redacted]	7.00	26476
[redacted]	9.30	25149
[redacted]	9.30	25100
[redacted]	9.30	24908
[redacted]	5.10	23592
[redacted]	9.30	17002
[redacted]	9.30	13307
[redacted]	9.30	13296
[redacted]	9.30	8151

b7E

Top 10 Compliance Failures

Configuration Setting	Count
[redacted]	64757
[redacted]	62137
[redacted]	61793
[redacted]	61793
[redacted]	55122
[redacted]	53057
[redacted]	44903
[redacted]	33283
[redacted]	28872
[redacted]	28850

b7E

DECLASSIFIED

DECLASSIFIED

Appendix C – DoS Cyber Condition (CyberCon) Levels

CyberCon Level	Tripwires	Actions
EMERGENCY **Significant cyber attacks are currently occurring**	• Degradation, denial, or destruction of systems • Highly sophisticated attacks • Major tensions within country / significant catastrophic events • *DoS is unable to execute its diplomatic mission* • *Widespread or focused attacks targeting vulnerabilities within the enterprise require an immediate coordinated response.* • *Network infrastructure throughput is severed.* • *Common network services are disrupted.* • *Sensitive information in the enterprise is at high risk of compromise.*	• Disconnection of Internet connectivity • Task Force initialization • Documented Remediation Steps completed and verified prior to re-connection
HIGH **Significant cyber attacks are imminent or moderate attacks are occurring**	• Widespread malicious activity • Intelligence indicates targeted activity • Increase in sophisticated recon and probes • Heightened tensions within country or major event • *DoS must resort to alternative communications means to execute its diplomatic mission* • *Attacks targeting vulnerabilities within the enterprise may require a coordinated response.* • *Network infrastructure throughput is noticeably diminished.* • *Common network services are partially disrupted.* • *Sensitive information in the enterprise is at moderate risk of compromise.*	• Initiate Management Team briefings • Three-times-a-day notification to pre-determined recipient list • Additional sniffers deployed as needed • Authorize limited OT for analysts

DECLASSIFIED

UNCLASSIFIED

ELEVATED **Moderate cyber attacks are imminent**	• Increased risk • Limited malicious activity • Intelligence indicates general threats • Specific incidents reported and under review • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at some risk of compromise.***	• Ensure protective measures implemented • Increase backups, audits, etc. • Verify response action plans & staff ready • Document changes in cyber security posture
GUARDED **Nuisance cyber attack activity is present**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Potential malicious activity within the enterprise may be handled thorough routine channels and procedures.*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.*** • ***Existing countermeasures are likely to be adequate to counter this threat***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures
LOW **Nuisance cyber attack activity is expected**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Automated response is sufficient to counter potential malicious activity within the enterprise*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures

DECLASSIFIED

Appendix D – Intranet Web Links of Interest

UNCLASSIFIED

Within the Office of Computer Security

- **Awareness**
  Periodic Update: http://cs.ds.state.gov/ETPA/ETPA_03.cfm
- **Computer Incident Response Team (CIRT)**
  Periodic Update: http://cs.ds.state.gov/CIRT/CIRT_08.cfm
- **Cyber Threat Analysis Division (CTAD)**
  Daily Read File: http://source.ds.state.sgov.gov (ClassNet)
  Tactical Awareness: http://cs.ds.state.gov/CTAD/CTAD_07.cfm
- **The Office of Computer Security**
  Periodic Update: http://cs.ds.state.gov/index.cfm
- **Compliance and Vulnerability Scanning**
  Periodic Update: http://cs.ds.state.gov/index.cfm

Outside of the Office of Computer Security

- **Cyber Security Incident Program**
  Periodic Update: http://csip.ds.state.gov
- **Enterprise Network Management**
  Periodic Update: http://enm.irm.state.gov
- **The Office of Information Assurance**
  Periodic Update: http://ia.irm.state.gov/
- **Patch Management**
  Periodic Update: http://enm.irm.state.gov/nlm/patch/Default.htm
- **Virus Incident Response Team (VIRT)**
  Periodic Update: http://sysintegweb.irm.state.gov/si/AntiVirus.html

The CIRT welcomes all constructive feedback to the daily Cyber Security Brief. If you have feedback for the CSB, please send it to CIRT@state.gov

DECLASSIFIED

Ø1Ø

Pc
b7E

E

Cyber Security Brief

United States Department of State
Bureau of Diplomatic Security
as of June 22, 2009-1400 EST

June 23, 2009

Current DoS Cyber Threat Condition

GUARDED

No change from last reported condition

Nuisance cyber attack activity is present

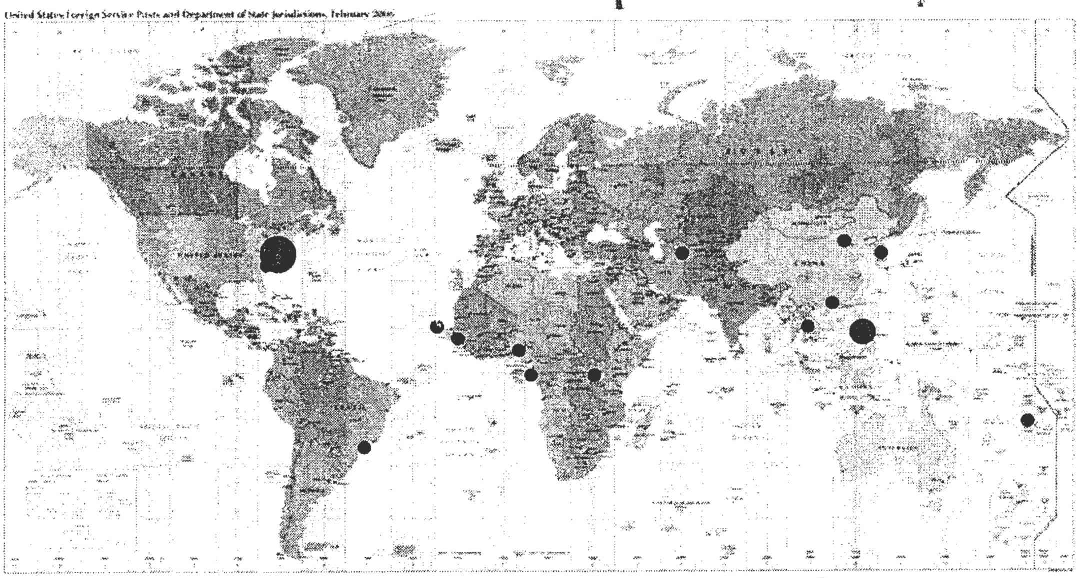
Executive Summary

1. **CIRT**
   - CIRT is awaiting the ISSOs' responses and remediation confirmations on the remaining spear-phishing attack notifications.

2. **CTAD Daily Read File**
   - (U) New Efforts to Bypass Government-Imposed Internet Restrictions in Iran

3. **Classified spillage incident**
   - One instance of classified spillage reported

Geographic Distribution of Computer Incident Response Team (CIRT) Events

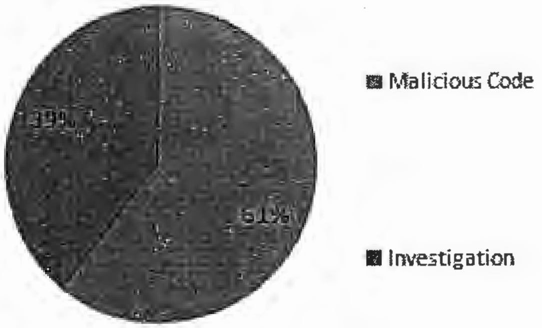

United States Foreign Service Posts and Department of State Jurisdictions, February 2006

Legend: ● *1 event* ● *2 events* ● *3+ events*

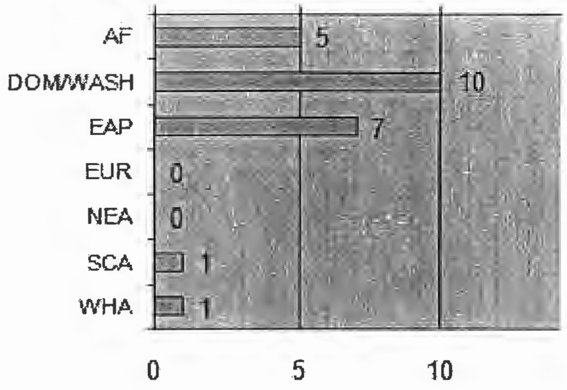
DECLASSIFIED

__Open CIRT Events:__ 17 __Closed CIRT Events:__ 7

__*CIRT Events by US-CERT Category*__



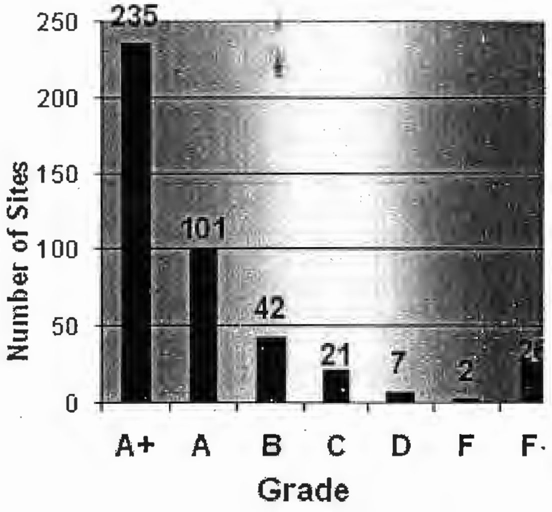
__*CIRT Events by Bureau*__



__*Firewall Block Request Summary*__

- Nothing substantial to report

__*Enterprise Risk Score Grade Distribution*__



__*Computer Incident Response Team (CIRT)*__

- CIRT is awaiting the ISSOs' responses and remediation confirmations on the remaining spear-phishing attack notifications of e-mails with a malicious PDF attachment. Due to the large number of tickets generated by this event, these tickets are presented in table format.

DECLASSIFIED

DECLASSIFIED

Personally identifiable information (PII) loss reported

- Nothing substantial to report

Classified spillage incident(s) reported to CIRT and referred to DS/IS/APD

- One instance of classified spillage in Washington, D.C. has been referred to APD.

US-CERT Coordination

- Nothing substantial to report

Compliance & Vulnerability Scanning

- *See Appendix B for statistics*

Cyber Threat Analysis Division (CTAD)

DAILY READ FILE: (U) New Efforts to Bypass Government-Imposed Internet Restrictions in Iran

(U) Key Highlights:

- *The turmoil in Iran continues following the country's highly contested elections*
- *The situation has called for new ways to help Iranians communicate with others*
- *Facebook, Google, and YouTube have joined efforts to facilitate information-sharing*
- *As citizens continue to bypass Internet restrictions, the government of Iran also strives to maintain control over the flow information*

(U) Source Paragraph: "Some of the Web's leading firms are rolling out new features, to accommodate worldwide interest in the protests in Iran—and to not-so-subtly help out the pro-democracy movement inside the country, Iran's activists have been relying on blogs [Web logs], Tweets, text messages, Facebook groups, and uploaded YouTube videos to share information with one another, and with t he outside world."

Source: Wired (http://www.wired.com), "Facebook, Google Go Persian, aiding Iran's Activists," 19 June 2009

***Virus Incident Response Team (VIRT) Statistics** (as of midnight eastern time)*

Spam Blocked at Perimeter:	**Virus Blocked at Perimeter:**
Previous day: 1,378,302	Previous day:38
Month to date - June: 20,925,340	Month to date - June:7,313
Year to date for 2009: 270,716,437	Year to date for 2009: 27,246

Cyber Security News Headlines

DECLASSIFIED

E

Group to Monitor Obama's Cybersecurity Promises *[Source: govinfosecurity.com]*
Twitter Message Could Be Cyber Criminal at Work *[Source: editon.cnn.com]*

b7E

DECLASSIFIED

Appendix A –CIRT Event Summaries

Legend:	*Open Events: 17*	*Closed Events: 7*

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Malicious Code directed towards an internal machine

[redacted] CIRT detected a large number of e-mail messages [redacted]

b7E

Ticket Number	Location	Bureau	Date Opened	Awaiting Post Response	Post is Remediating	Date Closed
[redacted]	[redacted]	WHA/US	06-12-09		Yes	
[redacted]	[redacted]	WHA/US	06-12-09		Yes	
[redacted]	[redacted]	WHA/US	06-12-09	Yes		
[redacted]	[redacted]	EAP	06-12-09	Yes		
[redacted]	[redacted]	EAP	06-12-09		Yes	
[redacted]	[redacted]	AF	06-12-09			06-22
[redacted]	[redacted]	AF	06-12-09	Yes		
[redacted]	[redacted]	AF	06-12-09		Yes	
[redacted]	[redacted]	AF	06-12-09		Yes	

b7E

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Email - Malicious Payload (Code, Attachment, Link)

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 2023 GMT	**Affected Bureau:** DOM

Event Description
CIRT detected a large number of e-mail messages with PDF attachments from " [redacted]

BM ✓

b7E

DECLASSIFIED

E

[redacted] b7E

DECLASSIFIED

Current Status

22 Jun: CIRT requested a status update from the IT Service Center via e-mail and phone.

Status History

16 Jun: CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
17 Jun: CIRT requested a status update from the ISSO via e-mail.
18 Jun: CIRT requested a status update from the ISSO via e-mail.
19 Jun: CIRT requested a status update from the ISSO via e-mail and phone.

Ticket Number: [redacted]	**Location** [redacted]
Date and Time Ticket Created: 06/16/2009 2052 GMT	**Affected Bureau:** DOM

BM ✓

Event Description

CIRT detected a large number of e-mail messages with PDF attachments from " [redacted] b7E

Current Status

22 Jun: CIRT requested a status update from the IT Service Center via e-mail and phone.

Status History

16 Jun: CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
17 Jun: The IT Service Center has provided a reference number for this event.
18 Jun: CIRT requested a status update from the ISSO via e-mail.
19 Jun: The IT Service Center informed CIRT that the ticket has been assigned to the appropriate point of contact, and that remediation is in progress.
20 Jun: ITSC sent the initial e-mail to the incorrect ISSO, and resent the e-mail to the ITSC.

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Malicious Code directed towards an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 1540 GMT	**Affected Bureau:** EAP

BM ✓

Event Description

E

CIRT detected a large number of e-mail messages with PDF attachments from [redacted]

UNCLASSIFIED

b7E

Current Status
22 Jun: **CIRT requested a status update from the ISSO, the IMO, and the IPO via e-mail.**

Status History
16 Jun: CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted.
17 Jun: The ISSO responded that he is attempting to contact the e-mail recipients.
18 Jun: The ISSO informed CIRT that the user is at a remote office and he will contact the user for more information regarding this e-mail.
18 Jun: The ISSO informed CIRT that seven of the e-mails were not opened and were deleted; five of the users are in pending status. The ISSO will provide CIRT with an update soon. [redacted]
19 Jun: CIRT requested a status update from the ISSO via e-mail.

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Malicious Code directed towards an internal machine

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/19/2009 1136 GMT	**Affected Bureau:** EAP

Event Description
CIRT detected communication between a DoS workstation and a malicious host domain

Current Status
22 Jun: CIRT requested a status update from the ISSO via e-mail.

Status History
19 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

✓

Ticket Number: [redacted]	**Location:** [redacted] D
Date and Time Ticket Created: 06/20/2009 0744 GMT	**Affected Bureau:** DOM

Event Description
CIRT detected the download of an executable from a suspected phishing site.

Current Status

UNCLASSIFIED

b7E

22 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

Status History
N/A - New Event

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/19/2009 1148 GMT	**Affected Bureau:** DOM

✓

Event Description
CIRT detected a DoS workstation communicating with a suspicious website and possibly downloading a [redacted]

b7E

Current Status
22 Jun: CIRT requested a status update from the ISSO via e-mail.

Status History
19 Jun: CIRT requested that the ISSO search for specific files and reimage the operating system if the files are found.
20 Jun: The ISSO informed CIRT that he is currently examining this event. A virus scan was performed with negative results. The workstation will be reimaged as a precaution. The ISSO will provide CIRT with an update upon completion.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/22/2009 1057 GMT	**Affected Bureau:** DOM

✓

Event Description
CIRT detected the download of an executable from a suspicious website

Current Status
22 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

Status History
N/A - New Event

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Unauthorized Software Downloaded to a DoS machine

E b7E

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/22/2009 1230 GMT	**Affected Bureau:** AF

Event Description
CIRT detected the download of a malicious executable to a DoS workstation.

Current Status
22 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

Status History
N/A - New Event

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Virus/Worm on internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/17/2009 0904 GMT	**Affected Bureau:** EAP

b7E

Event Description
CIRT detected a DoS workstation in communication with a malicious website containing [redacted]

Current Status
22 Jun: CIRT requested a status update from the ISSO and the RSO via e-mail.

Status History
17 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.
18 Jun: CIRT requested a status update from the ISSO via e-mail.
19 Jun: CIRT requested a status update from the ISSO via e-mail.

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: E-mail - Phishing

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/20/2009 0802 GMT	**Affected Bureau:** EAP

DECLASSIFIED

b7E
E

DECLASSIFIED

Event Description CIRT detected a DoS workstation downloading a malicious .PDF file from an external host.
Final Action **22 Jun: The ISSO informed CIRT that the workstation was successfully reimaged.**
Status History **N/A - New Event**

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Malicious Code directed towards an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 2124 GMT	**Affected Bureau:** EAP
Event Description An ISSO reported to CIRT that a DoS website [redacted]	
Final Action **20 Jun: The ISSO informed CIRT that the workstation was successfully reimaged.**	
Status History **16 Jun:** CIRT requested that the ISSO disconnect the workstation from the network and reimage the operating system. **17 Jun:** CIRT requested a status update from the ISSO via e-mail. **18 Jun:** CIRT requested additional information from the ISSO. **19 Jun:** CIRT requested a status update from the ISSO via e-mail.	

b7E

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Virus/Worm on an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/19/2009 0949 GMT	**Affected Bureau:** WHA
Event Description CIRT detected a DoS workstation communicating with a suspicious website and possibly downloading a malicious .exe file.	
Final Action **22 Jun: The ISSO informed CIRT that the workstation was successfully reimaged.**	

DECLASSIFIED

b7E

Status History

19 Jun: CIRT requested that the ISSO disconnect the workstation from the network and reimage the operating system.
21 Jun: CIRT requested a status update from the ISSO via e-mail.

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/17/2009 1408 GMT	**Affected Bureau:** DOM

Event Description

CIRT detected a malicious executable file directed at a DoS workstation

Final Action

22 Jun: The ISSO informed CIRT that the malicious files were found and removed. Antivirus definitions are up-to-date, and a scan was successfully completed with negative results. The computer is current with all of the latest patches from IRM Patch Management.

Status History

17 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.
18 Jun: CIRT requested a status update from the ITSC. The ITSC informed CIRT that this ticket is currently assigned to the administrator responsible for examining the incident.
19 Jun: CIRT requested a status update from the ITSC.

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Information Security Issue (violation or infraction)

✓

Ticket Number [redacted]	**Location** [redacted]
Date and Time Ticket Created: 06/19/2009 1718 GMT	**Affected Bureau:** DOM

Event Description

CIRT was notified of a Classified Spillage

Final Action

19 Jun: This event has been referred to the APD team.

Status History

N/A - New Event

DECLASSIFIED

E

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Non-event

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/22/2009 1209 GMT	**Affected Bureau:** SCA

Event Description

CIRT detected the download of a malicious executable to a DoS workstation.

Final Action

22 Jun: The ISSO informed CIRT that no malicious or unauthorized files were found. Antivirus definitions are up-to-date, and a scan was successfully completed with negative results. The computer is current with all of the latest patches from IRM Patch Management.

Status History

N/A - New Event

✓

E

b7E

DECLASSIFIED

Appendix B – Compliance & Vulnerability Scanning Statistics

VULNERABILITY TOTALS:

Total Critical Vulnerabilities: 8,741

Total High Vulnerabilities: 519,421

TOP 10 CRITICAL VULNERABILITIES

b7E

Vulnerability	CVSS Score	Count
[redacted]	10.00	1234
[redacted]	10.00	1153
[redacted]	10.00	971
[redacted]	10.00	803
[redacted]	10.00	580
[redacted]	10.00	485
[redacted]	10.00	450
[redacted]	10.00	376
[redacted]	10.00	269
[redacted]	10.00	220

TOP 10 HIGH VULNERABILITIES

b7E

Vulnerability	CVSS Score	Count
[redacted]	9.30	28246
[redacted]	7.00	27711
[redacted]	9.30	25671
[redacted]	9.30	25625
[redacted]	9.30	25432
[redacted]	9.30	17749
[redacted]	9.30	13385
[redacted]	9.30	13343
[redacted]	9.30	8338
[redacted]	9.30	8308

DECLASSIFIED

E

b7E

DECLASSIFIED

Top 10 Most Common Vulnerabilities

[redacted]	CVSS Score	Count
[redacted]	9.30	28246
[redacted]	7.00	27711
[redacted]	9.30	25671
[redacted]	9.30	25625
[redacted]	9.30	25432
[redacted]	5.10	23268
[redacted]	9.30	17749
[redacted]	9.30	13385
[redacted]	9.30	13343
[redacted]	9.30	8338

b7E

Top 10 Compliance Failures

Configuration Setting	Count
[redacted]	65806
[redacted]	62934
[redacted]	62595
[redacted]	62587
[redacted]	55858
[redacted]	53540
[redacted]	45291
[redacted]	33387
[redacted]	29338
[redacted]	29308

b7E

DECLASSIFIED

DECLASSIFIED

Appendix C – DoS Cyber Condition (CyberCon) Levels

CyberCon Level	Tripwires	Actions
Significant cyber attacks are currently occurring	• Degradation, denial, or destruction of systems • Highly sophisticated attacks • Major tensions within country / significant catastrophic events • ***DoS is unable to execute its diplomatic mission*** • ***Widespread or focused attacks targeting vulnerabilities within the enterprise require an immediate coordinated response.*** • ***Network infrastructure throughput is severed.*** • ***Common network services are disrupted.*** • ***Sensitive information in the enterprise is at high risk of compromise.***	• Disconnection of Internet connectivity • Task Force initialization • Documented Remediation Steps completed and verified prior to re-connection
HIGH **Significant cyber attacks are imminent or moderate attacks are occurring**	• Widespread malicious activity • Intelligence indicates targeted activity • Increase in sophisticated recon and probes • Heightened tensions within country or major event • ***DoS must resort to alternative communications means to execute its diplomatic mission*** • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at moderate risk of compromise.***	• Initiate Management Team briefings • Three-times-a-day notification to pre-determined recipient list • Additional sniffers deployed as needed • Authorize limited OT for analysts

UNCLASSIFIED

ELEVATED **Moderate cyber attacks are imminent**	• Increased risk • Limited malicious activity • Intelligence indicates general threats • Specific incidents reported and under review • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at some risk of compromise.***	• Ensure protective measures implemented • Increase backups, audits, etc. • Verify response action plans & staff ready • Document changes in cyber security posture
GUARDED **Nuisance cyber attack activity is present**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Potential malicious activity within the enterprise may be handled thorough routine channels and procedures.*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.*** • ***Existing countermeasures are likely to be adequate to counter this threat***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures
LOW **Nuisance cyber attack activity is expected**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Automated response is sufficient to counter potential malicious activity within the enterprise*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures

DECLASSIFIED

Appendix D – Intranet Web Links of Interest

DECLASSIFIED

Within the Office of Computer Security

- **Awareness**
  Periodic Update: http://cs.ds.state.gov/ETPA/ETPA_03.cfm
- **Computer Incident Response Team (CIRT)**
  Periodic Update: http://cs.ds.state.gov/CIRT/CIRT_08.cfm
- **Cyber Threat Analysis Division (CTAD)**
  Daily Read File: http://source.ds.state.sgov.gov (ClassNet)
  Tactical Awareness: http://cs.ds.state.gov/CTAD/CTAD_07.cfm
- **The Office of Computer Security**
  Periodic Update: http://cs.ds.state.gov/index.cfm
- **Compliance and Vulnerability Scanning**
  Periodic Update: http://cs.ds.state.gov/index.cfm

Outside of the Office of Computer Security

- **Cyber Security Incident Program**
  Periodic Update: http://csip.ds.state.gov
- **Enterprise Network Management**
  Periodic Update: http://enm.irm.state.gov
- **The Office of Information Assurance**
  Periodic Update: http://ia.irm.state.gov/
- **Patch Management**
  Periodic Update: http://enm.irm.state.gov/nlm/patch/Default.htm
- **Virus Incident Response Team (VIRT)**
  Periodic Update: http://sysintegweb.irm.state.gov/si/AntiVirus.html

The CIRT welcomes all constructive feedback to the daily Cyber Security Brief. If you have feedback for the CSB, please send it to CIRT@state.gov

DECLASSIFIED

Ø11 b7E

E

Cyber Security Brief

United States Department of State
Bureau of Diplomatic Security
as of June 23, 2009-1400 EST

June 24, 2009

Current DoS Cyber Threat Condition

GUARDED

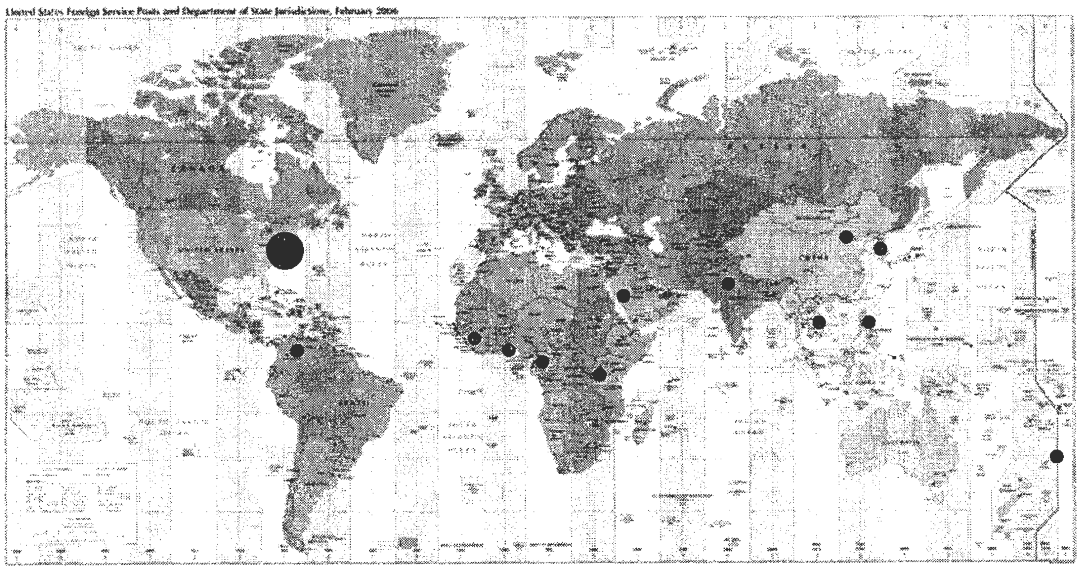
No change from last reported condition

Nuisance cyber attack activity is present

Executive Summary

1. CIRT
   - CIRT is awaiting the ISSOs' responses and remediation confirmations on the remaining spear-phishing attack notifications.
2. CTAD Daily Read File
   - (U) DDOS Attack on Belarus Site
3. Classified spillage incident
   - One instance of classified spillage has been referred to APD

Geographic Distribution of Computer Incident Response Team (CIRT) Events


United States Foreign Service Posts and Department of State Jurisdictions, February 2006

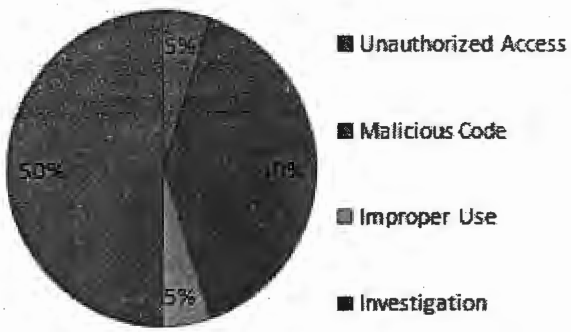
Legend: ● *1 event* ● *2 events* ● *3+ events*

Open CIRT Events: 8

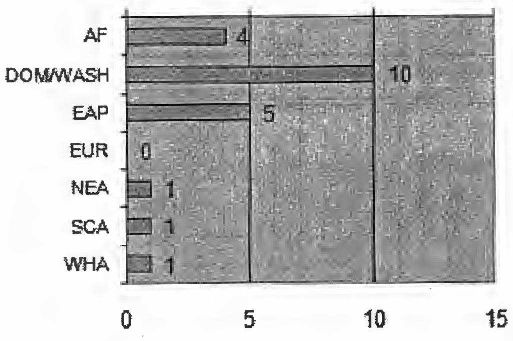
Closed CIRT Events: 14

DECLASSIFIED

CIRT Events by US-CERT Category



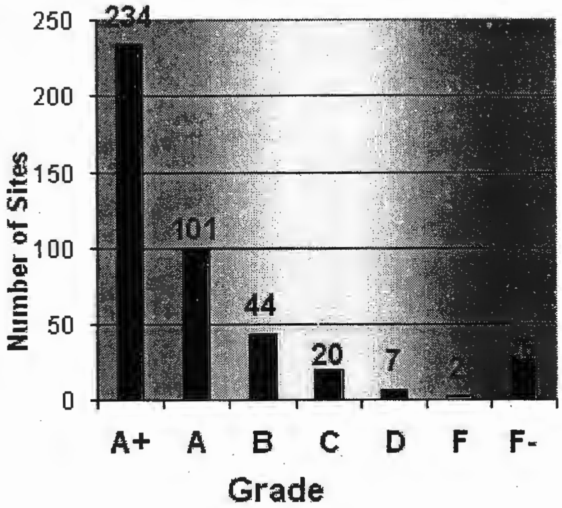
CIRT Events by Bureau



Firewall Block Request Summary

- Nothing substantial to report

Enterprise Risk Score Grade Distribution



Computer Incident Response Team (CIRT)

- CIRT is awaiting the ISSOs' responses and remediation confirmations on the remaining spear-phishing attack notifications of e-mails with a malicious PDF attachment. Due to the large number of tickets generated by this event, these tickets are presented in table format.

Personally identifiable information (PII) loss reported

- Nothing substantial to report

DECLASSIFIED

Classified spillage incident(s) reported to CIRT and referred to DS/IS/APD

- One instance of classified spillage in Washington, DC has been referred to DS/IS/APD. An e-mail with an attachment containing classified information was sent from Congressional Research Services (CRS) to multiple Federal agencies.

US-CERT Coordination

- Nothing substantial to report

Compliance & Vulnerability Scanning

- *See Appendix B for statistics*

Cyber Threat Analysis Division (CTAD)

DAILY READ FILE: (U) DDOS Attack on Belarus Site

(SBU) Key Highlights:

- *The Web site of Charter 97, a human rights organization and media outlet was attacked*
- *The Charter 97 site was previously attacked along with RFE/RL sites in 2008*
- *Current attacks coincide with diplomatic tensions between the GoB and the RF*
- *It is unlikely recent attacks were spurred by the relationship between the GoB and the RF*

(U)Source Paragraph: "The new wave of the distributed denial of service [DDOS] attack continues with renewed vigour and gains momentum. The web site will probably be unavailable again."

Source: Charter 97 (http://www.charter97.org), "Attack on charter97.org for second day," 09 June 2009

Virus Incident Response Team (VIRT) Statistics (as of midnight eastern time)

Spam Blocked at Perimeter:	Virus Blocked at Perimeter:
Previous day: 1,378,302	Previous day:38
Month to date - June: 20,925,340	Month to date - June:7,313
Year to date for 2009: 270,716,437	Year to date for 2009: 27,246

Cyber Security News Headlines

Cyber Security Czar Front-Runner No Friend of Privacy *[Source: wired.com]*
5 Fed Cybersecurity Priorities for the Summer *[Source: govinfosecurity.com]*
Information Security: the Good, the Bad and the Ugly *[Source: tmcnet.com]*

E

Appendix A –CIRT Event Summaries

DECLASSIFIED b7E

Legend: ▨ Open Events: 8 ▨ Closed Events: 14

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Malicious Code directed towards an internal machine

[redacted] CIRT detected a large number of e-mail messages [redacted]

b7E

Ticket Number	Location	Bureau	Date Opened	Awaiting Post Response	Post is Remediating	Date Closed
[redacted]	[redacted]	WHA/US	06-12-09		Yes	
[redacted]	[redacted]	WHA/US	06-12-09			06-23
[redacted]	[redacted]	WHA/US	06-12-09			06-23
[redacted]	[redacted]	EAP	06-12-09			06-23
[redacted]	[redacted]	EAP	06-12-09		Yes	
[redacted]	[redacted]	AF	06-12-09			06-23
[redacted]	[redacted]	AF	06-12-09			06-23
[redacted]	[redacted]	AF	06-12-09		Yes	

b7E

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Email - Malicious Payload (Code, Attachment, Link)

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 2052 GMT	**Affected Bureau:** DOM

—✓

Event Description

CIRT detected a large number of e-mail messages with PDF attachments from " [redacted]

b7E

Current Status

23 Jun: CIRT requested additional information regarding the physical location of the

b7E
E

DECLASSIFIED

user.
Status History **16 Jun:** CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system. **17 Jun:** The IT Service Center has provided a reference number for this event. **18 Jun:** CIRT requested a status update from the ISSO via e-mail. **19 Jun:** The IT Service Center informed CIRT that the ticket has been assigned to the appropriate point of contact, and remediation is in progress. **20 Jun:** The IT Service Center resent the initial e-mail to the correct ISSO. **22 Jun:** CIRT requested a status update from the IT Service Center via e-mail and phone.

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Malicious Code directed towards an internal machine

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/20/2009 0744 GMT	**Affected Bureau:** DOM
Event Description CIRT detected the download of an executable from a suspected phishing site.	
Current Status **23 Jun: CIRT requested a status update from the ISSO via e-mail.**	
Status History **22 Jun:** CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.	

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/19/2009 1148 GMT	**Affected Bureau:** DOM
Event Description CIRT detected a DoS workstation communicating with a suspicious website and possibly downloading a [redacted]	
Current Status **23 Jun: The ISSO informed CIRT that he is still examining this event.**	
Status History **19 Jun:** CIRT requested that the ISSO search for specific files and reimage the operating system if the files are found.	

b7E

DECLASSIFIED

E b7E

20 Jun: The ISSO informed CIRT that he is currently examining this event. A virus scan was performed with negative results. The workstation will be reimaged as a precaution. The ISSO will provide CIRT with an update on completion.
22 Jun: CIRT requested a status update from the ISSO via e-mail.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/22/2009 1419 GMT	**Affected Bureau:** WHA
Event Description CIRT detected a malicious executable file directed at a DoS workstation.	
Current Status **23 Jun: CIRT requested a status update from the ISSO via e-mail.**	
Status History **22 Jun:** CIRT requested that the ISSO disconnect the workstation from the network and reimage the operating system.	

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Unauthorized Software Downloaded to a DoS machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/22/2009 1230 GMT	**Affected Bureau:** AF
Event Description CIRT detected the download of a malicious executable to a DoS workstation.	
Current Status **23 Jun: The ISSO informed CIRT that he is currently examining this event.**	
Status History **22 Jun:** CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.	

US-CERT Category: CAT 1 (Unauthorized Access)
Event Type Confirmed: Non-event

Ticket Number: [redacted]	**Location:** [redacted]

b7E

Date and Time Ticket Created: 06/22/2009 2109 GMT	**Affected Bureau:** NEA
Event Description CIRT was notified of an ISSO-reported event on CLAN.	
Final Action **23 Jun: A review of the workstation indicated** [redacted]	
Status History **N/A - New Event**	

b7E

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: E-mail - Malicious Payload (Code, Attachment, Link)

✓

Ticket Number: 13012	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 2023 GMT	**Affected Bureau:** DOM
Event Description CIRT detected a large number of e-mail messages with PDF attachments from " [redacted]	
Final Action **23 Jun: The ISSO did not find the e-mail on the user's workstation.**	
Status History **N/A - New Event** **16 Jun:** CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system. **17 Jun:** CIRT requested a status update from the ISSO via e-mail. **18 Jun:** **19 Jun:** CIRT requested a status update from the ISSO via e-mail and phone. **22 Jun:** CIRT requested a status update from the IT Service Center by e-mail and phone.	

b7E

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: E-mail - Phishing

✓

Ticket Number: [redacted]	**Location** [redacted]
Date and Time Ticket Created: 06/23/2009 1218 GMT	**Affected Bureau:** DOM

E

Event Description

CIRT detected a malicious PDF [redacted] an internal DoS workstation.

UNCLASSIFIED

b7E

Final Action

23 Jun: The users were contacted and CTAD is analyzing the event.

Status History

N/A - New Event

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 1540 GMT	**Affected Bureau:** EAP

Event Description

CIRT detected a large number of e-mail messages with PDF attachments from [redacted]

b7E

Final Action

23 Jun: The ISSO informed CIRT that all the users had deleted the e-mail without opening it.

Status History

16 Jun: CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted.

17 Jun: The ISSO responded that he is attempting to contact the e-mail recipients.

18 Jun: The ISSO informed CIRT that the user is at a remote office and he will contact the user for more information regarding this e-mail.

19 Jun: The ISSO informed CIRT that seven of the e-mails were not opened and were deleted; five of the users are in pending status. The ISSO will provide CIRT with an update soon. [redacted]

b7E

22 Jun: CIRT requested a status update from the ISSO via e-mail.

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Malicious Code directed towards an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/22/2009 1057 GMT	**Affected Bureau:** DOM

Event Description

CIRT detected the download of an executable from a suspicious website

UNCLASSIFIED

b7E

Final Action

23 Jun: CIRT received confirmation from the ISSO that the workstation was searched for malicious files and nothing was found. All patches are current.

Status History

22 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

US-CERT Category: CAT 4 (Improper Usage)
Event Type Confirmed: Violation of Computer Security Policy by a DoS user (CSIP issue)

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/23/2009 0559 GMT	**Affected Bureau:** SCA

Event Description

An ISSO reported inappropriate use of the Department of State's assets by DoS employees.

Final Action

23 Jun: This event has been forwarded to DS/ICI/PR.

Status History

N/A - New Event

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Information Security Issue (violation or infraction)

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/23/2009 1123 GMT	**Affected Bureau:** DOM

Event Description

CIRT was notified of a Classified Spillage

Final Action

23 Jun: This instance of Classified Spillage has been referred to the APD team for remediation.

Status History

N/A - New Event

DECLASSIFIED

E b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Malicious Code directed towards an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/19/2009 1136 GMT	**Affected Bureau:** EAP

Event Description
CIRT detected communication between a DoS workstation and a malicious host domain

Final Action
23 Jun: The ISSO informed CIRT that no unauthorized software was found on the workstation. The results of a virus scan were negative and all patches are current.

Status History
19 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.
22 Jun: CIRT requested a status update from the ISSO via e-mail.

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Non-event

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/17/2009 0904 GMT	**Affected Bureau:** EAP

Event Description
CIRT detected a DoS workstation in communication with a malicious website containing [redacted]

b7E

Final Action
23 Jun: The ISSO informed CIRT that no malicious files were found on the workstation. The user does not remember downloading the executable from the website.

Status History
17 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.
18 Jun: CIRT requested a status update from the ISSO via e-mail.
19 Jun: CIRT requested a status update from the ISSO via e-mail.
22 Jun: CIRT requested a status update from the ISSO and the RSO via e-mail.

DECLASSIFIED

E

576

DECLASSIFIED

Appendix B – Compliance & Vulnerability Scanning Statistics

VULNERABILITY TOTALS:

Total Critical Vulnerabilities: 8,808
Total High Vulnerabilities: 511,197

TOP 10 CRITICAL VULNERABILITIES

b7E

Vulnerability	CVSS Score	Count
[redacted]	10.00	1245
[redacted]	10.00	1153
[redacted]	10.00	961
[redacted]	10.00	803
[redacted]	10.00	598
[redacted]	10.00	485
[redacted]	10.00	459
[redacted]	10.00	376
[redacted]	10.00	275
[redacted]	10.00	227

TOP 10 HIGH VULNERABILITIES

b7E

Vulnerability	CVSS Score	Count
[redacted]	9.30	27798
[redacted]	7.00	27243
[redacted]	9.30	25119
[redacted]	9.30	25074
[redacted]	9.30	24883
[redacted]	9.30	17373
[redacted]	9.30	13044
[redacted]	9.30	13001
[redacted]	9.30	8183
[redacted]	9.30	8151

E

DECLASSIFIED

b7E

Top 10 Most Common Vulnerabilities

Vulnerability	CVSS Score	Count
[redacted]	9.30	27798
[redacted]	7.00	27243
[redacted]	9.30	25119
[redacted]	9.30	25074
[redacted]	9.30	24883
[redacted]	5.10	23293
[redacted]	9.30	17373
[redacted]	9.30	13044
[redacted]	9.30	13001
[redacted]	9.30	8183

b7E

Top 10 Compliance Failures

Configuration Setting	Count
[redacted]	65795
[redacted]	62921
[redacted]	62584
[redacted]	62577
[redacted]	55862
[redacted]	53533
[redacted]	45275
[redacted]	33390
[redacted]	29329
[redacted]	29300

b7E

DECLASSIFIED

DECLASSIFIED

Appendix C – DoS Cyber Condition (CyberCon) Levels

CyberCon Level	Tripwires	Actions
[redacted] **Significant cyber attacks are currently occurring**	• Degradation, denial, or destruction of systems • Highly sophisticated attacks • Major tensions within country / significant catastrophic events • ***DoS is unable to execute its diplomatic mission*** • ***Widespread or focused attacks targeting vulnerabilities within the enterprise require an immediate coordinated response.*** • ***Network infrastructure throughput is severed.*** • ***Common network services are disrupted.*** • ***Sensitive information in the enterprise is at high risk of compromise.***	• Disconnection of Internet connectivity • Task Force initialization • Documented Remediation Steps completed and verified prior to re-connection
HIGH **Significant cyber attacks are imminent or moderate attacks are occurring**	• Widespread malicious activity • Intelligence indicates targeted activity • Increase in sophisticated recon and probes • Heightened tensions within country or major event • ***DoS must resort to alternative communications means to execute its diplomatic mission*** • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at moderate risk of compromise.***	• Initiate Management Team briefings • Three-times-a-day notification to pre-determined recipient list • Additional sniffers deployed as needed • Authorize limited OT for analysts

DECLASSIFIED

UNCLASSIFIED

ELEVATED **Moderate cyber attacks are imminent**	• Increased risk • Limited malicious activity • Intelligence indicates general threats • Specific incidents reported and under review • *Attacks targeting vulnerabilities within the enterprise may require a coordinated response.* • *Network infrastructure throughput is noticeably diminished.* • *Common network services are partially disrupted.* • *Sensitive information in the enterprise is at some risk of compromise.*	• Ensure protective measures implemented • Increase backups, audits, etc. • Verify response action plans & staff ready • Document changes in cyber security posture
GUARDED **Nuisance cyber attack activity is present**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • *Potential malicious activity within the enterprise may be handled thorough routine channels and procedures.* • *Network infrastructure throughput is normal.* • *Common network services are not impaired* • *Sensitive information in the enterprise is at slight risk of compromise.* • *Existing countermeasures are likely to be adequate to counter this threat*	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures
LOW **Nuisance cyber attack activity is expected**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • *Automated response is sufficient to counter potential malicious activity within the enterprise* • *Network infrastructure throughput is normal.* • *Common network services are not impaired* • *Sensitive information in the enterprise is at slight risk of compromise.*	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures

Appendix D – Intranet Web Links of Interest

DECLASSIFIED

Within the Office of Computer Security

- **Awareness**
  Periodic Update: http://cs.ds.state.gov/ETPA/ETPA_03.cfm
- **Computer Incident Response Team (CIRT)**
  Periodic Update: http://cs.ds.state.gov/CIRT/CIRT_08.cfm
- **Cyber Threat Analysis Division (CTAD)**
  Daily Read File: http://source.ds.state.sgov.gov (ClassNet)
  Tactical Awareness: http://cs.ds.state.gov/CTAD/CTAD_07.cfm
- **The Office of Computer Security**
  Periodic Update: http://cs.ds.state.gov/index.cfm
- **Compliance and Vulnerability Scanning**
  Periodic Update: http://cs.ds.state.gov/index.cfm

Outside of the Office of Computer Security

- **Cyber Security Incident Program**
  Periodic Update: http://csip.ds.state.gov
- **Enterprise Network Management**
  Periodic Update: http://enm.irm.state.gov
- **The Office of Information Assurance**
  Periodic Update: http://ia.irm.state.gov/
- **Patch Management**
  Periodic Update: http://enm.irm.state.gov/nlm/patch/Default.htm
- **Virus Incident Response Team (VIRT)**
  Periodic Update: http://sysintegweb.irm.state.gov/si/AntiVirus.html

The CIRT welcomes all constructive feedback to the daily Cyber Security Brief. If you have feedback for the CSB, please send it to CIRT@state.gov

E P 012
b7E

012

Cyber Security Brief

United States Department of State
Bureau of Diplomatic Security
as of June 29, 2009-1400 EST

June 30, 2009

Current DoS Cyber Threat Condition

GUARDED

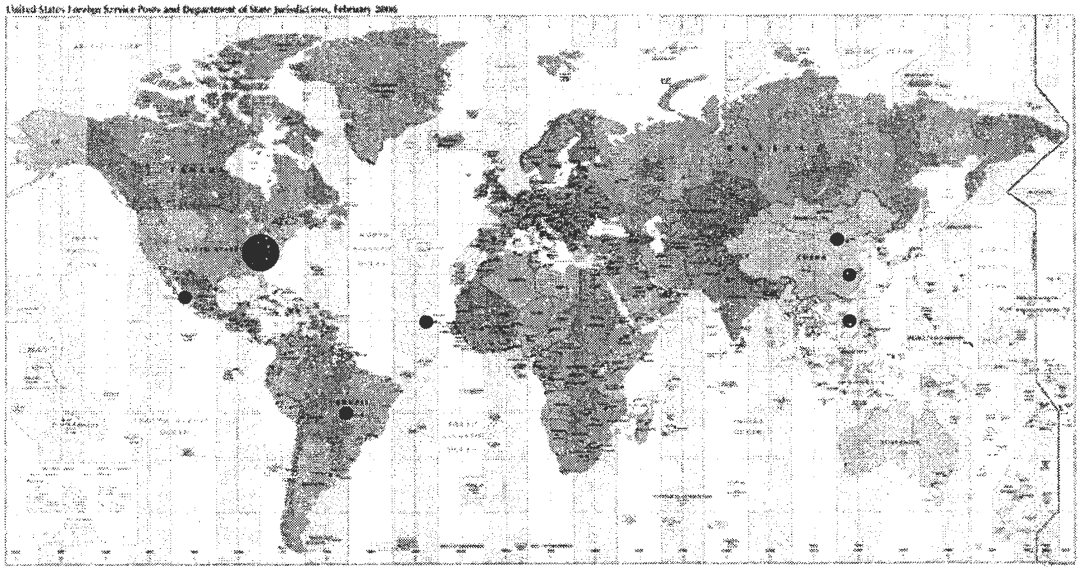
No change from last reported condition

Nuisance cyber attack activity is present

Executive Summary

1. <u>CIRT</u>
   - Nothing substantial to report
2. <u>CTAD Daily Read File</u>
   - (U) Phishers Baiting Tweets with Worms
3. <u>Personally identifiable information (PII) loss reported</u>
   - One passport application missing

<u>Geographic Distribution of Computer Incident Response Team (CIRT) Events</u>

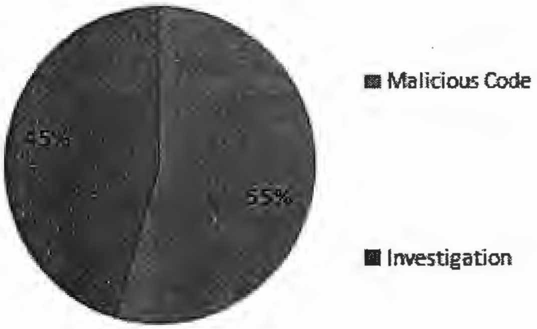

United States Foreign Service Posts and Department of State Jurisdictions, February 2006

Legend: ● *1 event* ● *2 events* ● *3+ events*

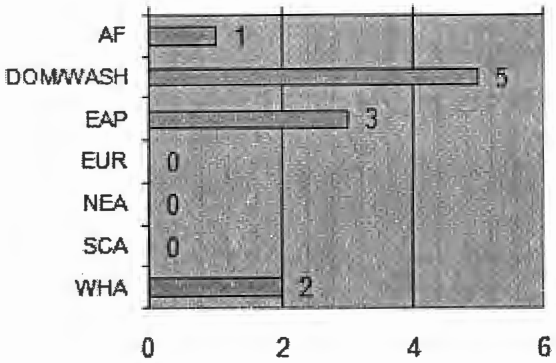
Open CIRT Events: 6

Closed CIRT Events: 5

CIRT Events by US-CERT Category



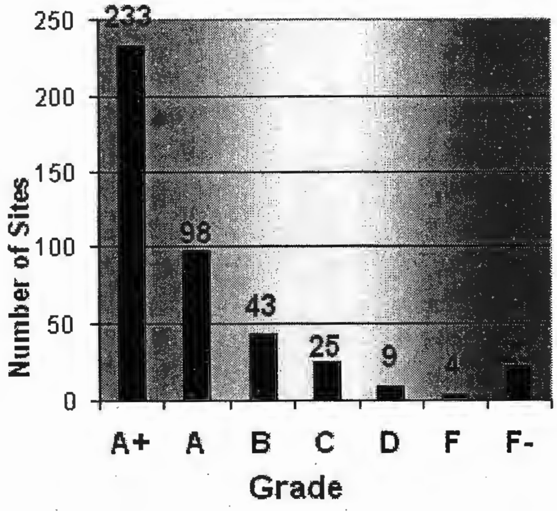
CIRT Events by Bureau



Firewall Block Request Summary

- Nothing substantial to report

Enterprise Risk Score Grade Distribution



Computer Incident Response Team (CIRT)

- Nothing substantial to report

Personally identifiable information (PII) loss reported

- One passport application mailed from a postal acceptance facility in the Philadelphia Passport Agency region to the Lindberg Postal Distribution Center cannot be located.

Classified spillage incident(s) reported to CIRT and referred to DS/IS/APD

- Nothing substantial to report

US-CERT Coordination

- Nothing substantial to report

Compliance & Vulnerability Scanning

- *See Appendix B for statistics*

Cyber Threat Analysis Division (CTAD)

DAILY READ FILE: (U) Phishers Baiting Tweets with Worms

(U) Key Highlights:

- *Symantec recently issued advisories about a new worm being employed against Twitter users*
- *Ackannta.B is a variant of malware observed in February 2009 which was used in e-mail spam*
- *Several other worms have also been identified in schemes specifically targeting Twitter users*
- *Users must remain aware of the emerging threats associated with using social networking sites*

(U) Source Paragraph: "Twitter spam bearing a worm virus is on the loose today trying to lure Twitter users into opening a malicious file attachment containing malware [malicious software] that could take over Windows-based machines, Symantec is warning."
Source: PC World (www.pcworld.com), "Twitter Spam Spreads Worm," 20 June 2009.

***Virus Incident Response Team (VIRT) Statistics** (as of midnight eastern time)*

Spam Blocked at Perimeter:
Previous day: 902,317
Month to date - June: 30,848,832
Year to date for 2009: 280,639,929

Virus Blocked at Perimeter:
Previous day:67
Month to date - June:7,800
Year to date for 2009: 27,915

Cyber Security News Headlines

CIOS, CISOS Await the Cybersecurity Czar *[Source: fiercegovernmentit.com]*
Obama and Cyber Defense *[Source: online.wsj.com]*
Feds Eye Economic Incentives for Secure Software *[Source: fiercegovernmentit.com]*

E

Appendix A –CIRT Event Summaries

b7E

Legend:	Open Events: 6	Closed Events: 5

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: E-mail - Malicious Payload (Code, Attachment, Link)

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 2052 GMT	**Affected Bureau:** DOM

Event Description

CIRT detected a large number of e-mail messages with PDF attachments from " [redacted]

b7-E

Current Status

29 Jun: CIRT contacted the IT Service Center and confirmed that the user of the workstation is located in a different bureau. CIRT was informed that the IT Service Center will reassign the ticket to the correct ISSO.

Status History

16 Jun: CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
17 Jun: The IT Service Center has provided a reference number for this event.
18 Jun: CIRT requested a status update from the ISSO via e-mail.
19 Jun: The IT Service Center informed CIRT that the ticket has been assigned to the appropriate point of contact, and remediation is in progress.
20 Jun: The IT Service Center resent the initial e-mail to the correct ISSO.
22 Jun: CIRT requested a status update from the IT Service Center via e-mail and phone.
23 Jun: CIRT requested additional information regarding the physical location of the user.
24 Jun: CIRT requested a status update from the IT Service Center via e-mail.
25 Jun: CIRT requested a status update from the IT Service Center via e-mail and phone. The IT Service Center will re-open this ticket and forward the initial request to the correct ISSO.
26 Jun: CIRT requested a status update from the IT Service Center via e-mail and phone.

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Malicious Code directed towards an internal machine

Ticket Number: [redacted]	**Location.** [redacted]

E

b7E

Date and Time Ticket Created: 06/25/2009 0636 GMT	**Affected Bureau:** AF
Event Description CIRT detected malware being directed towards a DoS workstation and attempting to download an executable file.	
Current Status **29 Jun: CIRT received updated ISSO contact information and resent the initial notification to the correct contact.**	
Status History **25 Jun:** CIRT requested that the ISSO search for specific files and perform an antivirus scan. **26 Jun:** CIRT requested a status update via e-mail from the ISSO.	

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: E-mail – Malicious Payload (Code, Attachment, Link)

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/25/2009 0914 GMT	**Affected Bureau:** EAP
Event Description CIRT was notified of a suspicious e-mail, possibly containing malicious code, targeting multiple users. [redacted]	
Current Status **29 Jun: CIRT requested a status update from the ISSO, the RSO, and the IPO via e-mail.**	
Status History **25 Jun:** CIRT requested a status update from the ISSO via e-mail. **25 Jun:** CIRT requested that the ISSO determine if the users had received the e-mail and if the e-mail has been opened or deleted. CIRT also requested that the ISSO identify any additional recipients of the e-mail if it has been forwarded. CIRT requested that the ISSO [redacted] **26 Jun:** CIRT requested a status update from the ISSO via e-mail.	

b7E

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Malicious Code directed towards an internal machine

BM ✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/25/2009 0849 GMT	**Affected Bureau:** DOM

E
375

Event Description CIRT detected the download of a malicious executable to a DoS workstation.
Current Status **29 Jun: CIRT requested a status update from the ISSO via e-mail and phone.**
Status History **25 Jun:** CIRT requested that the ISSO disconnect the workstation from the network and reimage the operating system. **26 Jun:** CIRT requested a status update from the ISSO via e-mail.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/29/2009 1115 GMT	**Affected Bureau:** WHA
Event Description CIRT detected a DoS workstation communicating with a malicious website and possibly downloading a malicious executable.	
Current Status **29 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.**	
Status History **N/A - New Event**	

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/29/2009 1213 GMT	**Affected Bureau:** WHA
Event Description CIRT detected a DoS workstation communicating with a malicious website and possibly downloading a malicious executable.	
Current Status **29 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.**	
Status History **N/A - New Event**	

DECLASSIFIED

575
E

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Malicious Code directed towards an internal machine

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/20/2009 0744 GMT	**Affected Bureau:** DOM

Event Description
CIRT detected the download of an executable from a suspected phishing site.

Final Action
27 Jun: The ISSO informed CIRT that no unauthorized software or malicious code was found on the machine. A virus scan was performed with negative results and the machine contains all of the latest patches from Patch Management.

Status History
22 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.
23 Jun: CIRT requested a status update from the ISSO via e-mail.
24 Jun: CIRT has resent the initial request to the IT Service Center.
25 Jun: CIRT requested a status update via telephone. The ticket has been assigned to a DSD technician
26 Jun: CIRT requested a status update from the IT Service Center via e-mail and phone.

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/24/2009 0944 GMT	**Affected Bureau:** EAP

Event Description
CIRT detected a DoS workstation downloading a suspicious executable file from a website.

Final Action
29 Jun: The ISSO informed CIRT that no malicious or unauthorized files were found. Antivirus definitions are up-to-date, and a scan was successfully completed with negative results. The computer is current with all of the latest patches from IRM Patch Management.

Status History
24 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.
25 Jun: CIRT requested a status update from the ISSO via e-mail.
26 Jun: CIRT requested a status update from the ISSO via e-mail.

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Virus/Worm on an internal machine

b7E

Ticket Number [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/29/2009 1147 GMT	**Affected Bureau:** DOM
Event Description CIRT detected malware being directed towards a DoS workstation and attempting to download an executable file.	
Final Action **29 Jun: CIRT was unable to confirm that a full version of the executable was downloaded. The website is no longer active, and traffic records do not indicate that a working executable was received.**	
Status History **N/A - New Event**	

BM ✓

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/29/2009 1223 GMT	**Affected Bureau:** EAP
Event Description CIRT detected a malicious executable directed at a DoS workstation	
Final Action **29 Jun: CIRT determined that the file was not a malicious executable, and that the entire file was never fully downloaded. The workstation was not compromised.**	
Status History **N/A - New Event**	

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Information Security Issue (violation or infraction)

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/29/2009 0857 GMT	**Affected Bureau:** DOM
Event Description CIRT was notified of a PII Event.	
Final Action **29 Jun: This ticket has been referred to US-CERT and the Privacy Team.**	
Status History **N/A - New Event**	

E

Appendix B – Compliance & Vulnerability Scanning Statistics

b7E

DECLASSIFIED

VULNERABILITY TOTALS:

Total Critical Vulnerabilities: 9,462
Total High Vulnerabilities: 549,814

TOP 10 CRITICAL VULNERABILITIES

Vulnerability	CVSS Score	Count
[redacted]	10.00	1289
[redacted]	10.00	1152
[redacted]	10.00	938
[redacted]	10.00	800
[redacted]	10.00	654
[redacted]	10.00	525
[redacted]	10.00	504
[redacted]	10.00	429
[redacted]	10.00	377
[redacted]	10.00	309

b7E

TOP 10 HIGH VULNERABILITIES

Vulnerability	CVSS Score	Count
[redacted]	9.30	29224
[redacted]	7.00	28837
[redacted]	9.30	26570
[redacted]	9.30	26486
[redacted]	9.30	26284
[redacted]	9.30	18683
[redacted]	9.30	14029
[redacted]	9.30	13974
[redacted]	9.30	8920
[redacted]	9.30	8881

b7E

DECLASSIFIED

E

b7E

DECLASSIFIED

Top 10 Most Common Vulnerabilities

Vulnerability	CVSS Score	Count
[redacted]	9.30	29224
[redacted]	7.00	28837
[redacted]	9.30	26570
[redacted]	9.30	26486
[redacted]	9.30	26284
[redacted]	5.10	23667
[redacted]	9.30	18683
[redacted]	9.30	14029
[redacted]	9.30	13974
[redacted]	9.30	8920

b7E

Top 10 Compliance Failures

Configuration Setting		Count
[redacted]		63865
[redacted]		63497
[redacted]		63495
[redacted]		56771
[redacted]		46055
[redacted]		34325
[redacted]		29829
[redacted]		29709
[redacted]		29694
[redacted]		29691

b7E

DECLASSIFIED

Appendix C – DoS Cyber Condition (CyberCon) Levels

CyberCon Level	Tripwires	Actions
Significant cyber attacks are currently occurring	• Degradation, denial, or destruction of systems • Highly sophisticated attacks • Major tensions within country / significant catastrophic events • ***DoS is unable to execute its diplomatic mission*** • ***Widespread or focused attacks targeting vulnerabilities within the enterprise require an immediate coordinated response.*** • ***Network infrastructure throughput is severed.*** • ***Common network services are disrupted.*** • ***Sensitive information in the enterprise is at high risk of compromise.***	• Disconnection of Internet connectivity • Task Force initialization • Documented Remediation Steps completed and verified prior to re-connection
HIGH Significant cyber attacks are imminent or moderate attacks are occurring	• Widespread malicious activity • Intelligence indicates targeted activity • Increase in sophisticated recon and probes • Heightened tensions within country or major event • ***DoS must resort to alternative communications means to execute its diplomatic mission*** • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at moderate risk of compromise.***	• Initiate Management Team briefings • Three-times-a-day notification to pre-determined recipient list • Additional sniffers deployed as needed • Authorize limited OT for analysts

UNCLASSIFIED

ELEVATED **Moderate cyber attacks are imminent**	• Increased risk • Limited malicious activity • Intelligence indicates general threats • Specific incidents reported and under review • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at some risk of compromise.***	• Ensure protective measures implemented • Increase backups, audits, etc. • Verify response action plans & staff ready • Document changes in cyber security posture
GUARDED **Nuisance cyber attack activity is present**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Potential malicious activity within the enterprise may be handled thorough routine channels and procedures.*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.*** • ***Existing countermeasures are likely to be adequate to counter this threat***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures
LOW **Nuisance cyber attack activity is expected**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Automated response is sufficient to counter potential malicious activity within the enterprise*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures

DECLASSIFIED

Appendix D – Intranet Web Links of Interest

UNCLASSIFIED

Within the Office of Computer Security

- **Awareness**
  Periodic Update: http://cs.ds.state.gov/ETPA/ETPA_03.cfm
- **Computer Incident Response Team (CIRT)**
  Periodic Update: http://cs.ds.state.gov/CIRT/CIRT_08.cfm
- **Cyber Threat Analysis Division (CTAD)**
  Daily Read File: http://source.ds.state.sgov.gov (ClassNet)
  Tactical Awareness: http://cs.ds.state.gov/CTAD/CTAD_07.cfm
- **The Office of Computer Security**
  Periodic Update: http://cs.ds.state.gov/index.cfm
- **Compliance and Vulnerability Scanning**
  Periodic Update: http://cs.ds.state.gov/index.cfm

Outside of the Office of Computer Security

- **Cyber Security Incident Program**
  Periodic Update: http://csip.ds.state.gov
- **Enterprise Network Management**
  Periodic Update: http://enm.irm.state.gov
- **The Office of Information Assurance**
  Periodic Update: http://ia.irm.state.gov/
- **Patch Management**
  Periodic Update: http://enm.irm.state.gov/nlm/patch/Default.htm
- **Virus Incident Response Team (VIRT)**
  Periodic Update: http://sysintegweb.irm.state.gov/si/AntiVirus.html

The CIRT welcomes all constructive feedback to the daily Cyber Security Brief. If you have feedback for the CSB, please send it to CIRT@state.gov

DECLASSIFIED

P
013
b7E
E

Cyber Security Brief

United States Department of State
Bureau of Diplomatic Security
as of June 30, 2009-1400 EST

July 1, 2009

Current DoS Cyber Threat Condition

GUARDED

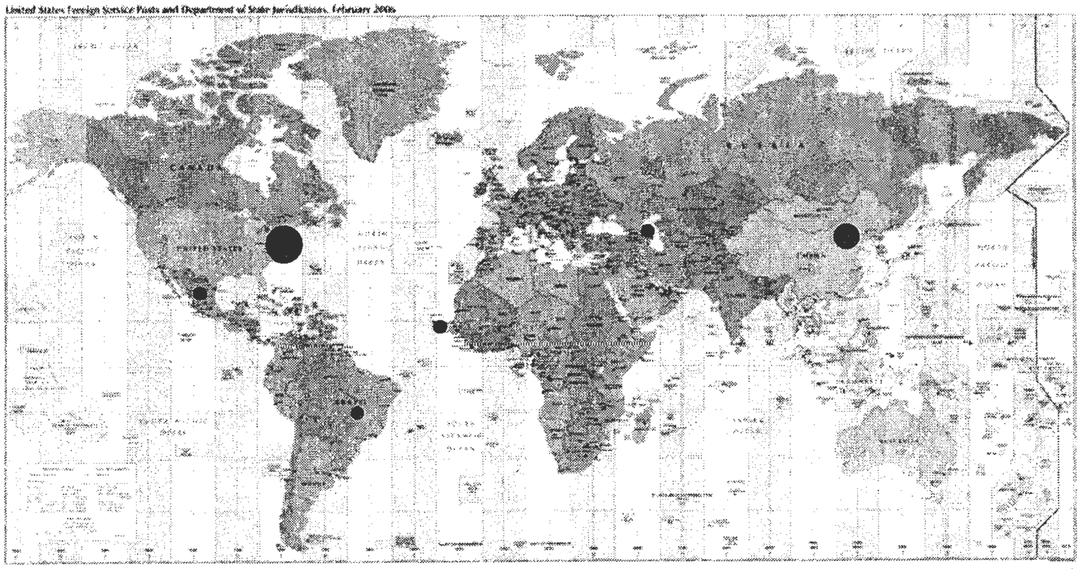
No change from last reported condition

Nuisance cyber attack activity is present

Executive Summary

1. CIRT
    - Nothing substantial to report
2. CTAD Daily Read File
    - (U) The Lucky Sploit Toolkit

Geographic Distribution of Computer Incident Response Team (CIRT) Events


United States Foreign Service Posts and Department of State Jurisdictions, February 2006

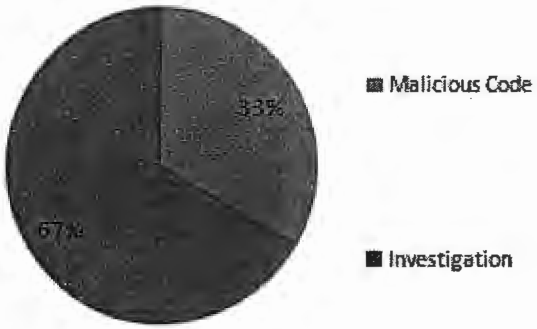
Legend: • *1 event* ● *2 events* ● *3+ events*

DECLASSIFIED

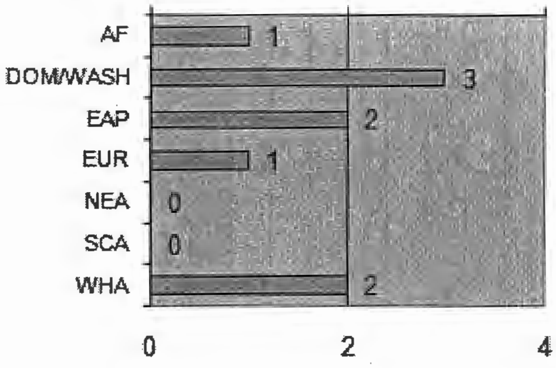
DECLASSIFIED

Open CIRT Events: 6 **Closed CIRT Events:** 3

CIRT Events by US-CERT Category



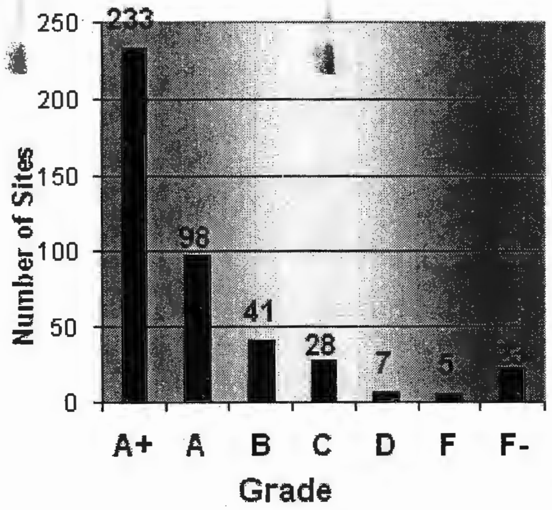
CIRT Events by Bureau



Firewall Block Request Summary

- Nothing substantial to report

Enterprise Risk Score Grade Distribution



Computer Incident Response Team (CIRT)

- Nothing substantial to report

DECLASSIFIED

Personally identifiable information (PII) loss reported

- Nothing substantial to report

DECLASSIFIED

Classified spillage incident(s) reported to CIRT and referred to DS/IS/APD

- Nothing substantial to report

US-CERT Coordination

- Nothing substantial to report

Compliance & Vulnerability Scanning

- *See Appendix B for statistics*

Cyber Threat Analysis Division (CTAD)

DAILY READ FILE: (U) The Lucky Sploit Toolkit

Key Highlights: (classified content - see CTAD Daily Read File on ClassNet for details)

(U) Source Paragraph: "Over the past few months SphosLabs have been seeing a relatively new kit being used by attackers in drive-by downloads to infect victims with malware [malicious software]. The kit is known as LuckySploit . . . It is a kit that enables attackers to construct malicious sites in order to hit victims with exploits and infect them with malware. Like many previous kits (Mpack, Firepack, Icepack, El Fiesta and the like), the pages it creates contain heavily obfuscated JavaScript in an attempt to evade detection and blocking. However, unlike previous kits, LuckySploit (or at least the recent version of it) also uses encryption."
Source: Sophos Labs blog (http://www.sophoscom), "Not so lucky (sploit) mass defacement," 10 March 2009

***Virus Incident Response Team (VIRT) Statistics** (as of midnight eastern time)*

Spam Blocked at Perimeter:
Previous day: 1,420,693
Month to date - June: 32,269,525
Year to date for 2009: 282,060,622

Virus Blocked at Perimeter:
Previous day:122
Month to date - June:7,922
Year to date for 2009: 28,037

Cyber Security News Headlines

The New Cybersecurity Licensing Proposal at a Glance *[Source: gcn.com]*
Cyber Security, the Nuclear Threat and You *[Source: computerworld.com]*

E

b7E

DECLASSIFIED

Appendix A –CIRT Event Summaries

Legend:	*Open Events: 6*	*Closed Events: 3*

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: E-mail - Malicious Payload (Code, Attachment, Link)

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 2052 GMT	**Affected Bureau:** DOM

Event Description

CIRT detected a large number of e-mail messages with PDF attachments from " [redacted] er.

b7E

Current Status

30 Jun: CIRT requested a status update from the IT Service Center via e-mail

Status History

16 Jun: CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
17 Jun: The IT Service Center has provided a reference number for this event.
18 Jun: CIRT requested a status update from the ISSO via e-mail.
19 Jun: The IT Service Center informed CIRT that the ticket has been assigned to the appropriate point of contact, and remediation is in progress.
20 Jun: The IT Service Center resent the initial e-mail to the correct ISSO.
22 Jun: CIRT requested a status update from the IT Service Center via e-mail and phone.
23 Jun: CIRT requested additional information regarding the physical location of the user.
24 Jun: CIRT requested a status update from the IT Service Center via e-mail.
25 Jun: CIRT requested a status update from the IT Service Center via e-mail and phone. The ITSC will re-open this ticket and forward the initial request to the correct ISSO.
26 Jun: CIRT requested a status update from the IT Service Center via e-mail and phone.
29 Jun: CIRT contacted the IT Service Center and confirmed that the user of the workstation is located in a different bureau. CIRT was informed that IT Service Center will reassign the ticket to the correct ISSO.

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: E-mail - Malicious Payload (Code, Attachment, Link)

Ticket Number: [redacted]	**Location:** [redacted]

b7E

DECLASSIFIED

Date and Time Ticket Created: 06/25/2009 0914 GMT	**Affected Bureau:** EAP
Event Description CIRT was notified of a suspicious e-mail, possibly containing malicious code, targeting multiple users [redacted]	
Current Status **30 Jun: CIRT requested a status update from the ISSO via e-mail and phone.**	
Status History **25 Jun:** CIRT requested that the ISSO determine if the users had received the e-mail and if the e-mail has been opened or deleted. CIRT also requested that the ISSO identify any additional recipients of the e-mail if it has been forwarded. CIRT requested that the ISSO [redacted] **26 Jun:** CIRT requested a status update from the ISSO via e-mail. **29 Jun:** CIRT requested a status update from the ISSO, the RSO, and the IPO via e-mail.	

b7E

b7E

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/30/2009 1335 GMT	**Affected Bureau:** DOM
Event Description CIRT was notified of a suspicious e-mail, possibly containing malicious code. This event [redacted]	
Current Status **30 Jun: CIRT requested that the ISSO ship the user's hard drive to TASO for analysis.**	
Status History **N/A - New Event**	

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: E-mail - Phishing

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/30/2009 0800 GMT	**Affected Bureau:** EAP
Event Description CIRT detected a possible phishing e-mail, originating from various sources, containing a [redacted]	
Current Status **30 Jun: CIRT is validating if any users have had access to this shared mailbox.**	

b7E

DECLASSIFIED

57E
E

Status History **N/A - New Event**

DECLASSIFIED

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Malicious Code directed towards an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/29/2009 1213 GMT	**Affected Bureau:** WHA
Event Description CIRT detected a DoS workstation communicating with a malicious website and possibly downloading a malicious executable.	
Current Status **30 Jun: CIRT requested a status update from the ISSO via e-mail.**	
Status History **29 Jun:** CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.	

BM ✓

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Virus/Worm on an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/30/2009 1022 GMT	**Affected Bureau:** EUR
Event Description CIRT detected a DoS workstation communicating with a website possibly containing a PDF with malicious code.	
Current Status **30 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.**	
Status History **N/A - New Event**	

BM ✓

DECLASSIFIED

b7E
E

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Malicious Code directed towards an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/25/2009 0636 GMT	**Affected Bureau:** AF

BM ✓

Event Description
CIRT detected malware being directed towards a DoS workstation and attempting to download an executable file.

Final Action
30 Jun: The ISSO informed CIRT that no evidence of malware was found on the workstation.

Status History
25 Jun: CIRT requested that the ISSO search for specific files and perform an antivirus scan.
26 Jun: CIRT requested a status update via e-mail from the ISSO.
29 Jun: CIRT received updated ISSO contact information and resent the initial notification to the correct contact.

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Virus/Worm on an internal machine

Ticket Number: [redacted]	**Location** [redacted]
Date and Time Ticket Created: 06/29/2009 1115 GMT	**Affected Bureau:** WHA

BM ✓

Event Description
CIRT detected a DoS workstation communicating with a malicious website and possibly downloading a malicious executable.

Final Action
30 Jun: The ISSO informed CIRT that no unauthorized software or malicious code was found on the machine. A virus scan was performed with negative results and the machine contains all of the latest patches from Patch Management.

Status History
29 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

DECLASSIFIED

E
b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Non-event

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/25/2009 0849 GMT	**Affected Bureau:** DOM

Event Description
CIRT detected the download of a malicious executable to a DoS workstation.

Final Action
30 Jun: The ISSO informed CIRT that a virus scan was completed with negative results. The machine is missing two patches which will be added. The hard drive will be replaced.

Status History
25 Jun: CIRT requested that the ISSO disconnect the workstation from the network and reimage the operating system.
26 Jun: CIRT requested a status update from the ISSO via e-mail.
29 Jun: CIRT was informed by the ISSO that the hard drive is scheduled to be replaced.

b7E
E

Appendix B – Compliance & Vulnerability Scanning Statistics

DECLASSIFIED

VULNERABILITY TOTALS:

Total Critical Vulnerabilities: 9,569
Total High Vulnerabilities: 550,426

TOP 10 CRITICAL VULNERABILITIES

Vulnerability	CVSS Score	Count
[redacted]	10.00	1356
[redacted]	10.00	1152
[redacted]	10.00	951
[redacted]	10.00	800
[redacted]	10.00	664
[redacted]	10.00	531
[redacted]	10.00	504
[redacted]	10.00	428
[redacted]	10.00	378
[redacted]	10.00	317

b2E

TOP 10 HIGH VULNERABILITIES

Vulnerability	CVSS Score	Count
[redacted]	9.30	29349
[redacted]	7.00	29005
[redacted]	9.30	26842
[redacted]	9.30	26757
[redacted]	9.30	26553
[redacted]	9.30	18937
[redacted]	9.30	14245
[redacted]	9.30	14190
[redacted]	9.30	8886
[redacted]	9.30	8848

b7E

DECLASSIFIED

b7E

Top 10 Most Common Vulnerabilities

Vulnerability	CVSS Score	Count
[redacted]	9.30	29349
[redacted]	7.00	29005
[redacted]	9.30	26842
[redacted]	9.30	26757
[redacted]	9.30	26553
[redacted]	5.10	23778
[redacted]	9.30	18937
[redacted]	9.30	14245
[redacted]	9.30	14190
[redacted]	9.30	8886

b7E

Top 10 Compliance Failures

Configuration Setting	Count
[redacted]	63874
[redacted]	63506
[redacted]	63504
[redacted]	56779
[redacted]	46046
[redacted]	34328
[redacted]	29840
[redacted]	29720
[redacted]	29704
[redacted]	29702

b7E

Appendix C – DoS Cyber Condition (CyberCon) Levels

CyberCon Level	Tripwires	Actions
[illegible] **Significant cyber attacks are currently occurring**	• Degradation, denial, or destruction of systems • Highly sophisticated attacks • Major tensions within country / significant catastrophic events • ***DoS is unable to execute its diplomatic mission*** • ***Widespread or focused attacks targeting vulnerabilities within the enterprise require an immediate coordinated response.*** • ***Network infrastructure throughput is severed.*** • ***Common network services are disrupted.*** • ***Sensitive information in the enterprise is at high risk of compromise.***	• Disconnection of Internet connectivity • Task Force initialization • Documented Remediation Steps completed and verified prior to re-connection
HIGH **Significant cyber attacks are imminent or moderate attacks are occurring**	• Widespread malicious activity • Intelligence indicates targeted activity • Increase in sophisticated recon and probes • Heightened tensions within country or major event • ***DoS must resort to alternative communications means to execute its diplomatic mission*** • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at moderate risk of compromise.***	• Initiate Management Team briefings • Three-times-a-day notification to pre-determined recipient list • Additional sniffers deployed as needed • Authorize limited OT for analysts

DECLASSIFIED

ELEVATED **Moderate cyber attacks are imminent**	• Increased risk • Limited malicious activity • Intelligence indicates general threats. • Specific incidents reported and under review • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at some risk of compromise.***	• Ensure protective measures implemented • Increase backups, audits, etc. • Verify response action plans & staff ready • Document changes in cyber security posture
GUARDED **Nuisance cyber attack activity is present**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Potential malicious activity within the enterprise may be handled thorough routine channels and procedures.*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.*** • ***Existing countermeasures are likely to be adequate to counter this threat***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures
LOW **Nuisance cyber attack activity is expected**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Automated response is sufficient to counter potential malicious activity within the enterprise*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures

Appendix D – Intranet Web Links of Interest

UNCLASSIFIED

Within the Office of Computer Security

- **Awareness**
  Periodic Update: http://cs.ds.state.gov/ETPA/ETPA_03.cfm
- **Computer Incident Response Team (CIRT)**
  Periodic Update: http://cs.ds.state.gov/CIRT/CIRT_08.cfm
- **Cyber Threat Analysis Division (CTAD)**
  Daily Read File: http://source.ds.state.sgov.gov (ClassNet)
  Tactical Awareness: http://cs.ds.state.gov/CTAD/CTAD_07.cfm
- **The Office of Computer Security**
  Periodic Update: http://cs.ds.state.gov/index.cfm
- **Compliance and Vulnerability Scanning**
  Periodic Update: http://cs.ds.state.gov/index.cfm

Outside of the Office of Computer Security

- **Cyber Security Incident Program**
  Periodic Update: http://csip.ds.state.gov
- **Enterprise Network Management**
  Periodic Update: http://enm.irm.state.gov
- **The Office of Information Assurance**
  Periodic Update: http://ia.irm.state.gov/
- **Patch Management**
  Periodic Update: http://enm.irm.state.gov/nlm/patch/Default.htm
- **Virus Incident Response Team (VIRT)**
  Periodic Update: http://sysintegweb.irm.state.gov/si/AntiVirus.html

The CIRT welcomes all constructive feedback to the daily Cyber Security Brief. If you have feedback for the CSB, please send it to CIRT@state.gov

P 014
b7E
E

Cyber Security Brief

DECLASSIFIED

United States Department of State
Bureau of Diplomatic Security
as of July 1, 2009-1400 EST

July 2, 2009

Current DoS Cyber Threat Condition

GUARDED

No change from last reported condition

Nuisance cyber attack activity is present

Executive Summary

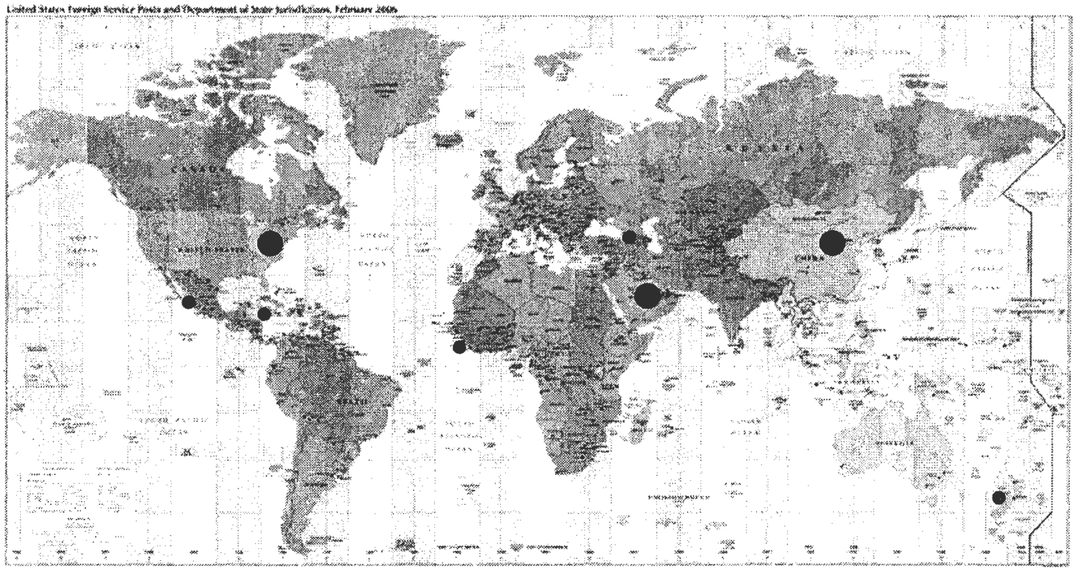
1. **CIRT**
   - Random PDF exploit attack [redacted]

b7E

2. **CTAD Daily Read File**
   - (U) Republic of Korea Information Security

3. **PII Loss Reported**
   - Two passport applications missing

Geographic Distribution of Computer Incident Response Team (CIRT) Events

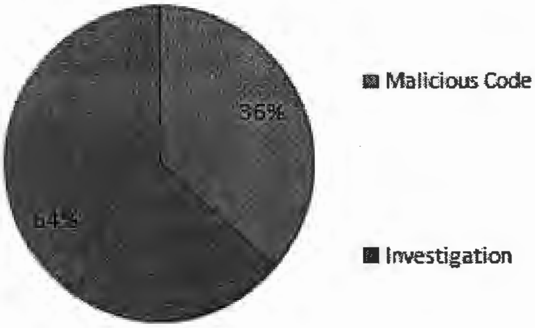

United States Foreign Service Posts and Department of State Jurisdictions, February 2006

Legend: ● *1 event* ● *2 events* ● *3+ events*

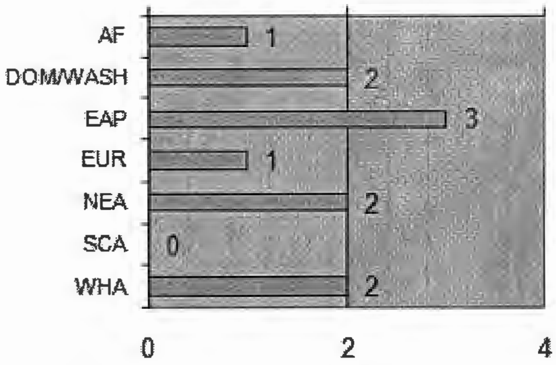
Open CIRT Events: 6 **Closed CIRT Events: 5**

DECLASSIFIED

CIRT Events by US-CERT Category



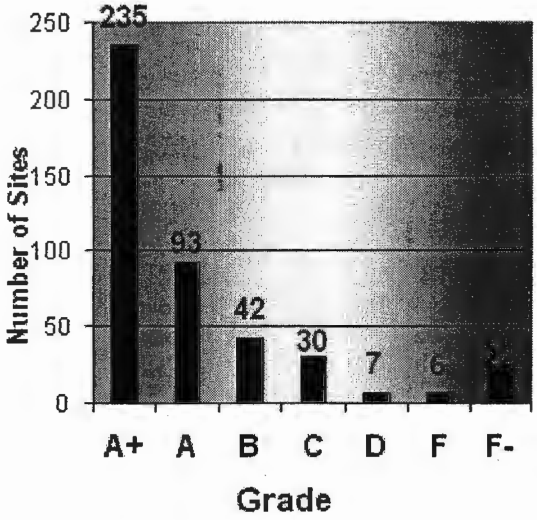
CIRT Events by Bureau



Firewall Block Request Summary

- Nothing substantial to report

Enterprise Risk Score Grade Distribution



Computer Incident Response Team (CIRT)

- Individual tickets will be referenced in the next Cyber Security Brief,

Classified spillage incident(s) reported to CIRT and referred to DS/IS/APD

- Nothing substantial to report

C03145587030

Personally identifiable information (PII) loss reported

- Two passport applications mailed from a postal acceptance facility in the Philadelphia Passport Agency region to the Lindberg Postal Distribution Center cannot be located at this time.

US-CERT Coordination

- Nothing substantial to report

<u>Compliance & Vulnerability Scanning</u>

- *See <u>Appendix B</u> for statistics*

<u>Cyber Threat Analysis Division (CTAD)</u>

DAILY READ FILE: (U) Republic of Korea Information Security

Key Highlights: (classified content - see CTAD Daily Read File on ClassNet for details)

(U) Source Paragraph: "South Korea's defense networks are attacked an average of 15,000 times a day by hackers and hit with viruses another 80,000 times, the top military intelligence agency said Tuesday [16 June]. The figure represents a 20-percent increase compared to last year, the Defense Security Command (DSC) said in a statement."
Source: CIA, Open Source Center, "South Korean Defense Networks Under Increasing cyber Attack: Military Intel Agency (U)," 16 June 2009.

<u>Virus Incident Response Team (VIRT) Statistics</u> *<u>(as of midnight eastern time)</u>*

Spam Blocked at Perimeter:	**Virus Blocked at Perimeter:**
Previous day: **1,420,693**	Previous day:**122**
Month to date - June: **32,269,525**	Month to date - June:**7,922**
Year to date for 2009: **282,060,622**	Year to date for 2009: **28,037**

<u>Cyber Security News Headlines</u>

<u>U.S. Official: Cybersecurity Plans Not Just Talk</u> *[Source: internetnews.com]*
<u>A Bustling Week for Cyber Justice</u> *[Source: washingtonpost.com]*
<u>Cyber Command Faces Urgent Agenda</u> *[Source: gcn.com]*

E

b7E

Appendix A –CIRT Event Summaries

DECLASSIFIED

Legend:	*Open Events: 6*	*Closed Events: 5*

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Malicious Code directed towards an internal machine

L

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/01/2009 1241 GMT	**Affected Bureau:** NEA
Event Description CIRT detected a malicious executable being directed at a DoS workstation.	
Current Status **1 Jul: CIRT requested that the ISSO search for specific files and reimage the operating system if the files are found.**	
Status History **N/A - New Event**	

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: E-mail - Malicious Payload (Code, Attachment, Link)

L

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/25/2009 0914 GMT	**Affected Bureau:** EAP
Event Description CIRT was notified of a suspicious e-mail, possibly containing malicious code, targeting multiple users. [redacted]	
Current Status **1 Jul: The ISSO informed CIRT that examination of this event is ongoing.**	
Status History **25 Jun:** CIRT requested that the ISSO determine if the users had received the e-mail and if the e-mail has been opened or deleted. CIRT also requested that the ISSO identify any additional recipients of the e-mail if it has been forwarded. CIRT requested that the ISSO [redacted] **26 Jun:** CIRT requested a status update from the ISSO via e-mail.	

b7E

b7E

DECLASSIFIED

E
b7E

29 Jun: CIRT requested a status update from the ISSO, the RSO, and the IPO via e-mail.
30 Jun: CIRT requested a status update from the ISSO via e-mail and phone.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/30/2009 1335 GMT	**Affected Bureau:** DOM

✓

Event Description
CIRT was notified of a suspicious e-mail, possibly containing malicious code. This event [redacted]

b7E

Current Status
1 Jul: CIRT requested a status update from the ISSO via e-mail.

Status History
30 Jun: CIRT requested that the ISSO ship the user's hard drive to TASO for analysis.

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: E-mail – Phishing

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/30/2009 0800 GMT	**Affected Bureau:** EAP

✓

Event Description
CIRT detected a possible phishing e-mail, originating from various sources, containing a [redacted]

b7E

Current Status
1 Jul: The ISSO informed CIRT that examination of this event is ongoing.

Status History
30 Jun: CIRT requested that the ISSO determine if the users had received the e-mail and if the e-mail has been opened or deleted. CIRT also requested that the ISSO identify any additional recipients of the e-mail if it has been forwarded. CIRT requested that the ISSO [redacted]

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Malicious Code directed towards an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/01/2009 1151 GMT	**Affected Bureau:** NEA

✓

E
b7E

Event Description CIRT detected a malicious executable being directed at a DoS workstation.
Current Status **1 Jul: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.**
Status History **N/A - New Event**

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Spyware/Trojan on an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/01/2009 0626 GMT	**Affected Bureau:** EAP
Event Description An ISSO notified CIRT of an e-mail with a malicious PDF attachment which was successfully quarantined [redacted]	
Current Status **1 Jul: CIRT requested that the ISSO search the workstation for specific files and reimage the workstation if the files are found.**	
Status History **N/A - New Event**	

b7E

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: E-mail - Phishing

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/01/2009 1347 GMT	**Affected Bureau:** WHA
Event Description CIRT detected a malicious e-mail directed at a DoS workstation.	
Final Action **1 Jul: Analysis of the workstation did not show the presence of the malicious code, and the workstation was not observed to be calling out to the known malicious**	

E
b7E

site/domain.
Status History **N/A - New Event**

DECLASSIFIED

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Malicious Code directed towards an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/29/2009 1213 GMT	**Affected Bureau:** WHA
Event Description CIRT detected a DoS workstation communicating with a malicious website and possibly downloading a malicious executable.	
Final Action **1 Jul: The ISSO examined the workstation and found no evidence of malware.**	
Status History **29 Jun:** CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management. **30 Jun:** CIRT requested a status update from the ISSO via e-mail.	

BM ✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/30/2009 1022 GMT	**Affected Bureau:** EUR
Event Description CIRT detected a DoS workstation communicating with a website possibly containing a PDF with malicious code.	
Final Action **1 Jul: The ISSO informed CIRT that the files in question were not found on the machine. A virus scan was performed with negative results and the machine contains all of the latest patches from Patch Management.**	
Status History **30 Jun:** CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.	

BM ✓

DECLASSIFIED

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Information Security Issue (violation or infraction)

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/01/2009 0800 GMT	**Affected Bureau:** DOM

BM ✓

Event Description
Personally Identifiable Information (PII) may have been breached or disclosed to unauthorized third parties.

Final Action
1 Jul: This ticket has been referred to US-CERT and the Privacy Office.

Status History
N/A - New Event

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Operational/Approved Activity

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/01/2009 1013 GMT	**Affected Bureau:** AF

BM ✓

Event Description
CIRT received a report of an unauthorized logon attempt to access a DoS server.

Final Action
1 Jul: CIRT notified the ISSO that the account accessing the e-mails is part of the validation process for e-mail archives.

Status History
N/A - New Event

E
b2

Appendix B – Compliance & Vulnerability Scanning Statistics

DECLASSIFIED

Vulnerability Totals:

Total Critical Vulnerabilities: 9,793
Total High Vulnerabilities: 578,830

Top 10 Critical Vulnerabilities

b7E

Vulnerability	CVSS Score	Count
[redacted]	10.00	1508
[redacted]	10.00	1131
[redacted]	10.00	959
[redacted]	10.00	800
[redacted]	10.00	675
[redacted]	10.00	557
[redacted]	10.00	504
[redacted]	10.00	429
[redacted]	10.00	388
[redacted]	10.00	310

Top 10 High Vulnerabilities

b7E

[redacted]	CVSS Score	Count
[redacted]	9.30	31142
[redacted]	7.00	30869
[redacted]	9.30	28455
[redacted]	9.30	28401
[redacted]	9.30	28196
[redacted]	9.30	20259
[redacted]	9.30	14895
[redacted]	9.30	14841
[redacted]	9.30	9672
[redacted]	9.30	9515

DECLASSIFIED

E

DECLASSIFIED

Top 10 Most Common Vulnerabilities

Vulnerability	CVSS Score	Count
[redacted]	9.30	31142
[redacted]	7.00	30869
[redacted]	9.30	28455
[redacted]	9.30	28401
[redacted]	9.30	28196
[redacted]	5.10	24206
[redacted]	9.30	20259
[redacted]	9.30	14895
[redacted]	9.30	14841
[redacted]	9.30	9672

b7E

Top 10 Compliance Failures

Configuration Setting	Count
[redacted]	63944
[redacted]	63576
[redacted]	63573
[redacted]	56854
[redacted]	46090
[redacted]	34398
[redacted]	29948
[redacted]	29828
[redacted]	29812
[redacted]	29810

b7E

Appendix C – DoS Cyber Condition (CyberCon) Levels

CyberCon Level	Tripwires	Actions
Significant cyber attacks are currently occurring	• Degradation, denial, or destruction of systems • Highly sophisticated attacks • Major tensions within country / significant catastrophic events • ***DoS is unable to execute its diplomatic mission*** • ***Widespread or focused attacks targeting vulnerabilities within the enterprise require an immediate coordinated response.*** • ***Network infrastructure throughput is severed.*** • ***Common network services are disrupted.*** • ***Sensitive information in the enterprise is at high risk of compromise.***	• Disconnection of Internet connectivity • Task Force initialization • Documented Remediation Steps completed and verified prior to re-connection
HIGH **Significant cyber attacks are imminent or moderate attacks are occurring**	• Widespread malicious activity • Intelligence indicates targeted activity • Increase in sophisticated recon and probes • Heightened tensions within country or major event • ***DoS must resort to alternative communications means to execute its diplomatic mission*** • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at moderate risk of compromise.***	• Initiate Management Team briefings • Three-times-a-day notification to pre-determined recipient list • Additional sniffers deployed as needed • Authorize limited OT for analysts

ELEVATED **Moderate cyber attacks are imminent**	• Increased risk • Limited malicious activity • Intelligence indicates general threats • Specific incidents reported and under review • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at some risk of compromise.***	• Ensure protective measures implemented • Increase backups, audits, etc. • Verify response action plans & staff ready • Document changes in cyber security posture
GUARDED **Nuisance cyber attack activity is present**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Potential malicious activity within the enterprise may be handled thorough routine channels and procedures.*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.*** • ***Existing countermeasures are likely to be adequate to counter this threat***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures
LOW **Nuisance cyber attack activity is expected**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Automated response is sufficient to counter potential malicious activity within the enterprise*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures

Appendix D – Intranet Web Links of Interest

DECLASSIFIED

Within the Office of Computer Security

- **Awareness**
  Periodic Update: http://cs.ds.state.gov/ETPA/ETPA_03.cfm
- **Computer Incident Response Team (CIRT)**
  Periodic Update: http://cs.ds.state.gov/CIRT/CIRT_08.cfm
- **Cyber Threat Analysis Division (CTAD)**
  Daily Read File: http://source.ds.state.sgov.gov (ClassNet)
  Tactical Awareness: http://cs.ds.state.gov/CTAD/CTAD_07.cfm
- **The Office of Computer Security**
  Periodic Update: http://cs.ds.state.gov/index.cfm
- **Compliance and Vulnerability Scanning**
  Periodic Update: http://cs.ds.state.gov/index.cfm

Outside of the Office of Computer Security

- **Cyber Security Incident Program**
  Periodic Update: http://csip.ds.state.gov
- **Enterprise Network Management**
  Periodic Update: http://enm.irm.state.gov
- **The Office of Information Assurance**
  Periodic Update: http://ia.irm.state.gov/
- **Patch Management**
  Periodic Update: http://enm.irm.state.gov/nlm/patch/Default.htm
- **Virus Incident Response Team (VIRT)**
  Periodic Update: http://sysintegweb.irm.state.gov/si/AntiVirus.html

The CIRT welcomes all constructive feedback to the daily Cyber Security Brief. If you have feedback for the CSB, please send it to CIRT@state.gov

DECLASSIFIED

E

P

b7E

015

Cyber Security Brief

DECLASSIFIED

United States Department of State
Bureau of Diplomatic Security
as of June 24, 2009-1400 EST

June 25, 2009

Current DoS Cyber Threat Condition

GUARDED

No change from last reported condition

Nuisance cyber attack activity is present

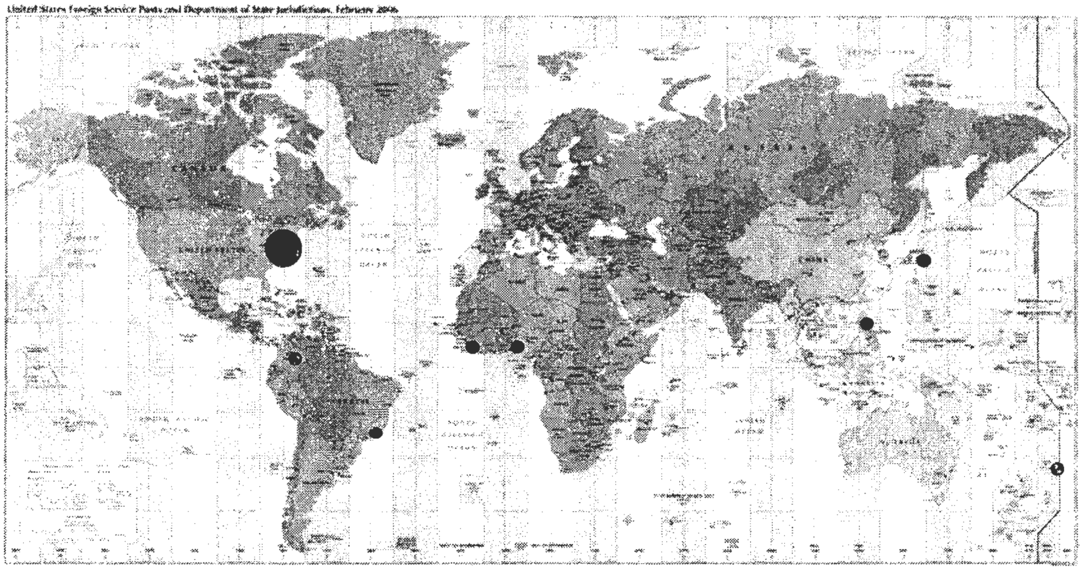
Executive Summary

1. **<u>CIRT</u>**
    - CIRT is awaiting the ISSOs' responses and remediation confirmations on the remaining spear-phishing attack notifications.

2. **<u>CTAD Daily Read File</u>**
    - (U) People's Republic of China (PRC) Information Dominance

<u>Geographic Distribution of Computer Incident Response Team (CIRT) Events</u>

United States Foreign Service Posts and Department of State Jurisdictions, February 2006



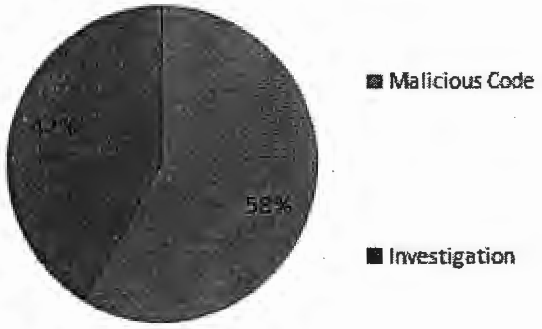
Legend: • *1 event* ● *2 events* ⬤ *3+ events*

DECLASSIFIED

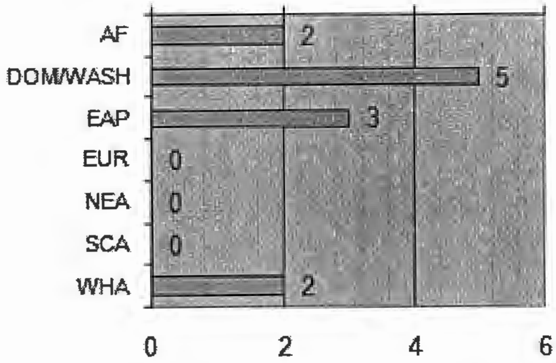
DECLASSIFIED

Open CIRT Events: 5 Closed CIRT Events: 7

CIRT Events by US-CERT Category



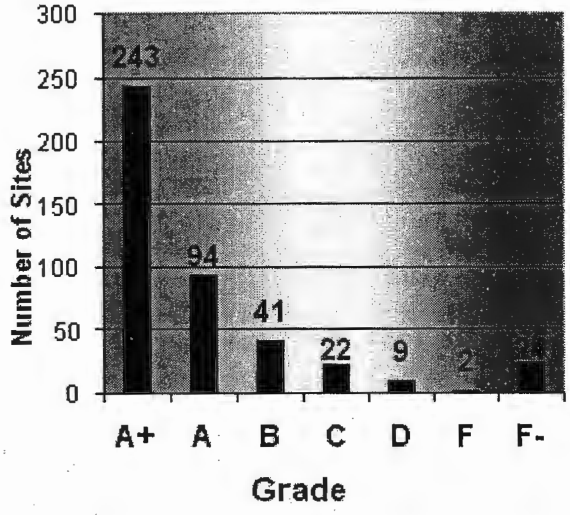
CIRT Events by Bureau



Firewall Block Request Summary

- Nothing substantial to report

Enterprise Risk Score Grade Distribution



Computer Incident Response Team (CIRT)

- CIRT is awaiting the ISSOs' responses and remediation confirmations on the remaining spear-phishing attack notifications of e-mails with a malicious PDF attachment. Due to the large number of tickets generated by this event, these tickets are presented in table format

DECLASSIFIED

Personally identifiable information (PII) loss reported

- Nothing substantial to report

Classified spillage incident(s) reported to CIRT and referred to DS/IS/APD

- Nothing substantial to report

US-CERT Coordination

- Nothing substantial to report

<u>Compliance & Vulnerability Scanning</u>

- *See <u>Appendix B</u> for statistics*

<u>Cyber Threat Analysis Division (CTAD)</u>

DAILY READ FILE: (U) People's Republic of China (PRC) Information Dominance

Key Highlights: (classified content)

Source Paragraph: (classified content)

<u>Virus Incident Response Team (VIRT) Statistics</u> *<u>(as of midnight eastern time)</u>*

Spam Blocked at Perimeter:	Virus Blocked at Perimeter:
Previous day: 1,791,238	Previous day:122
Month to date - June: 22,716,578	Month to date - June:7,253
Year to date for 2009: 272,507,675	Year to date for 2009: 27,368

<u>Cyber Security News Headlines</u>

<u>Military Command Is Created for Cyber Security</u> *[Source: wsj.com]*
<u>What's Ahead for WH Cybersecurity 'Czar'</u> *[Source: federalnewsradio.com]*
<u>Cybersecurity is Everyone's Problem</u> *[Source: dailytech.com]*

E

DECLASSIFIED

Appendix A – CIRT Event Summaries

b7E

Legend:	Open Events: 5	Closed Events: 7

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Malicious Code directed towards an internal machine

[redacted] CIRT detected a large number of e-mail messages [redacted]

b7E

Ticket Number	Location	Bureau	Date Opened	Awaiting Post Response	Post is Remediating	Date Closed
[redacted]	[redacted]	WHA/US	06-12-09			06-24
[redacted]	[redacted]	EAP	06-12-09		Yes	
[redacted]	[redacted]	AF	06-12-09			06-24

b7E

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: E-mail - Malicious Payload (Code, Attachment, Link)

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 2052 GMT	**Affected Bureau:** DOM

Event Description
CIRT detected a large number of e-mail messages with PDF attachments from " [redacted]

b7E

Current Status
24 Jun: CIRT requested a status update from the IT Service Center via e-mail.

Status History
16 Jun: CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened,

[illegible]

b7E

CIRT requested that the ISSO re-image the operating system.
17 Jun: The IT Service Center has provided a reference number for this event.
18 Jun: CIRT requested a status update from the ISSO via e-mail.
19 Jun: The IT Service Center informed CIRT that the ticket has been assigned to the appropriate point of contact, and remediation is in progress.
20 Jun: The IT Service Center resent the initial e-mail to the correct ISSO.
22 Jun: CIRT requested a status update from the IT Service Center via e-mail and phone.
23 Jun: CIRT requested additional information regarding the physical location of the user.

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Malicious Code directed towards an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/20/2009 0744 GMT	**Affected Bureau:** DOM

Event Description
CIRT detected the download of an executable from a suspected phishing site.

Current Status
24 Jun: CIRT has resent the initial request to the IT Service Center.

Status History
22 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.
23 Jun: CIRT requested a status update from the ISSO via e-mail.

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Unauthorized Software Downloaded to a DoS machine

Ticket Number: [redacted]	**Location** [redacted]
Date and Time Ticket Created: 06/22/2009 1230 GMT	**Affected Bureau:** AF

Event Description
CIRT detected the download of a malicious executable to a DoS workstation.

Current Status
24 Jun: The ISSO informed CIRT that the workstation is being examined and an update will be provided upon its completion.

Status History

b7E

22 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.
23 Jun: The ISSO informed CIRT that he is currently examining this event.

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Virus/Worm on an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/24/2009 0944 GMT	**Affected Bureau:** EAP

✓

Event Description
CIRT detected a DoS workstation downloading suspicious executable file from a website.

Current Status
24 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

Status History
N/A - New Event

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Malicious Code directed towards an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/19/2009 1148 GMT	**Affected Bureau:** DOM

✓

Event Description
CIRT detected a DoS workstation communicating with a suspicious website and possibly downloading a r [redacted]

b7E

Final Action
24 Jun: The ISSO informed CIRT that he will have the PC re-imaged.

Status History
19 Jun: CIRT requested that the ISSO search for specific files and reimage the operating system if the files are found.
20 Jun: The ISSO informed CIRT that he is currently examining this event. A virus scan has

E

b7E

been performed with negative results. The workstation will be reimaged as a precaution. **22 Jun:** CIRT requested a status update from the ISSO via e-mail. **23 Jun:** The ISSO informed CIRT that he is still examining this event.

Ticket Number [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/22/2009 1419 GMT	**Affected Bureau:** WHA
Event Description CIRT detected a malicious executable file directed at a DoS workstation.	
Final Action **24 Jun: The ISSO informed CIRT that no unauthorized files or software were detected and a full virus scan was performed with negative results. The workstation was removed from the network and will be reimaged.**	
Status History **22 Jun:** CIRT requested that the ISSO disconnect the workstation from the network and reimage the operating system. **23 Jun:** CIRT requested a status update from the ISSO via e-mail.	

Ticket Number: [redacted]	**Location** [redacted]
Date and Time Ticket Created: 06/24/2009 0511 GMT	**Affected Bureau:** EAP
Event Description CIRT detected an executable download of unauthorized software on a DoS machine.	
Final Action **24 Jun: The ISSO informed CIRT that the workstation was successfully reimaged.**	
Status History **N/A - New Event**	

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Non-event

Ticket Number: [redacted]	**Location** [redacted]
Date and Time Ticket Created: 06/23/2009 1445 GMT	**Affected Bureau:** DOM
Event Description CIRT was informed by US-CERT of a DoS workstation(s) that is communicating with an external entity.	

E
b 7E

Final Action **24 Jun: The results of malware analysis did not locate any malicious activity or threats to the DoS network.**
Status History **N/A - New Event**

UNCLASSIFIED

Ticket Number:	**Location:**
Date and Time Ticket Created: 06/24/2009 1021 GMT	**Affected Bureau:** WHA
Event Description CIRT detected a DoS workstation communicating with a malicious website and possibly downloading a malicious executable.	
Final Action **24 Jun: The ISSO informed CIRT that the machine was scanned; there was no evidence of malicious activity and no viruses were found on the workstation.**	
Status History **N/A - New Event**	

UNCLASSIFIED

E

b7E

DECLASSIFIED

Appendix B – Compliance & Vulnerability Scanning Statistics

VULNERABILITY TOTALS:

Total Critical Vulnerabilities: 8,779

Total High Vulnerabilities: 505,083

TOP 10 CRITICAL VULNERABILITIES

b7E

Vulnerability	CVSS Score	Count
[redacted]	10.00	1228
[redacted]	10.00	1153
[redacted]	10.00	958
[redacted]	10.00	803
[redacted]	10.00	597
[redacted]	10.00	484
[redacted]	10.00	460
[redacted]	10.00	375
[redacted]	10.00	274
[redacted]	10.00	226

TOP 10 HIGH VULNERABILITIES

b7E

Vulnerability	CVSS Score	Count
[redacted]	9.30	27439
[redacted]	7.00	26879
[redacted]	9.30	24677
[redacted]	9.30	24632
[redacted]	9.30	24440
[redacted]	9.30	17225
[redacted]	9.30	12863
[redacted]	9.30	12820
[redacted]	9.30	8061
[redacted]	9.30	8027

E

b7E

DECLASSIFIED

Top 10 Most Common Vulnerabilities

Vulnerability	CVSS Score	Count
[redacted]	9.30	27439
[redacted]	7.00	26879
[redacted]	9.30	24677
[redacted]	9.30	24632
[redacted]	9.30	24440
[redacted]	5.10	23418
[redacted]	9.30	17225
[redacted]	9.30	12863
[redacted]	9.30	12820
[redacted]	9.30	8061

b7E

Top 10 Compliance Failures

Configuratio [redacted]		Count
[redacted]		63209
[redacted]		62859
[redacted]		62852
[redacted]		56103
[redacted]		53678
[redacted]		45527
[redacted]		33748
[redacted]		29497
[redacted]		29436
[redacted]		29419

b7E

DECLASSIFIED

Appendix C – DoS Cyber Condition (CyberCon) Levels

CyberCon Level	Tripwires	Actions
Significant cyber attacks are currently occurring	• Degradation, denial, or destruction of systems • Highly sophisticated attacks • Major tensions within country / significant catastrophic events • ***DoS is unable to execute its diplomatic mission*** • ***Widespread or focused attacks targeting vulnerabilities within the enterprise require an immediate coordinated response.*** • ***Network infrastructure throughput is severed.*** • ***Common network services are disrupted.*** • ***Sensitive information in the enterprise is at high risk of compromise.***	• Disconnection of Internet connectivity • Task Force initialization • Documented Remediation Steps completed and verified prior to re-connection
HIGH **Significant cyber attacks are imminent or moderate attacks are occurring**	• Widespread malicious activity • Intelligence indicates targeted activity • Increase in sophisticated recon and probes • Heightened tensions within country or major event • ***DoS must resort to alternative communications means to execute its diplomatic mission*** • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at moderate risk of compromise.***	• Initiate Management Team briefings • Three-times-a-day notification to pre-determined recipient list • Additional sniffers deployed as needed • Authorize limited OT for analysts

Appendix D – Intranet Web Links of Interest

DECLASSIFIED

Within the Office of Computer Security

- **Awareness**
  Periodic Update: http://cs.ds.state.gov/ETPA/ETPA_03.cfm
- **Computer Incident Response Team (CIRT)**
  Periodic Update: http://cs.ds.state.gov/CIRT/CIRT_08.cfm
- **Cyber Threat Analysis Division (CTAD)**
  Daily Read File: http://source.ds.state.sgov.gov (ClassNet)
  Tactical Awareness: http://cs.ds.state.gov/CTAD/CTAD_07.cfm
- **The Office of Computer Security**
  Periodic Update: http://cs.ds.state.gov/index.cfm
- **Compliance and Vulnerability Scanning**
  Periodic Update: http://cs.ds.state.gov/index.cfm

Outside of the Office of Computer Security

- **Cyber Security Incident Program**
  Periodic Update: http://csip.ds.state.gov
- **Enterprise Network Management**
  Periodic Update: http://enm.irm.state.gov
- **The Office of Information Assurance**
  Periodic Update: http://ia.irm.state.gov/
- **Patch Management**
  Periodic Update: http://enm.irm.state.gov/nlm/patch/Default.htm
- **Virus Incident Response Team (VIRT)**
  Periodic Update: http://sysintegweb.irm.state.gov/si/AntiVirus.html

The CIRT welcomes all constructive feedback to the daily Cyber Security Brief. If you have feedback for the CSB, please send it to CIRT@state.gov

DECLASSIFIED

P 016
b7E
E

Cyber Security Brief

DECLASSIFIED

United States Department of State
Bureau of Diplomatic Security
as of June 25, 2009-1400 EST

June 26, 2009

Current DoS Cyber Threat Condition

GUARDED

No change from last reported condition

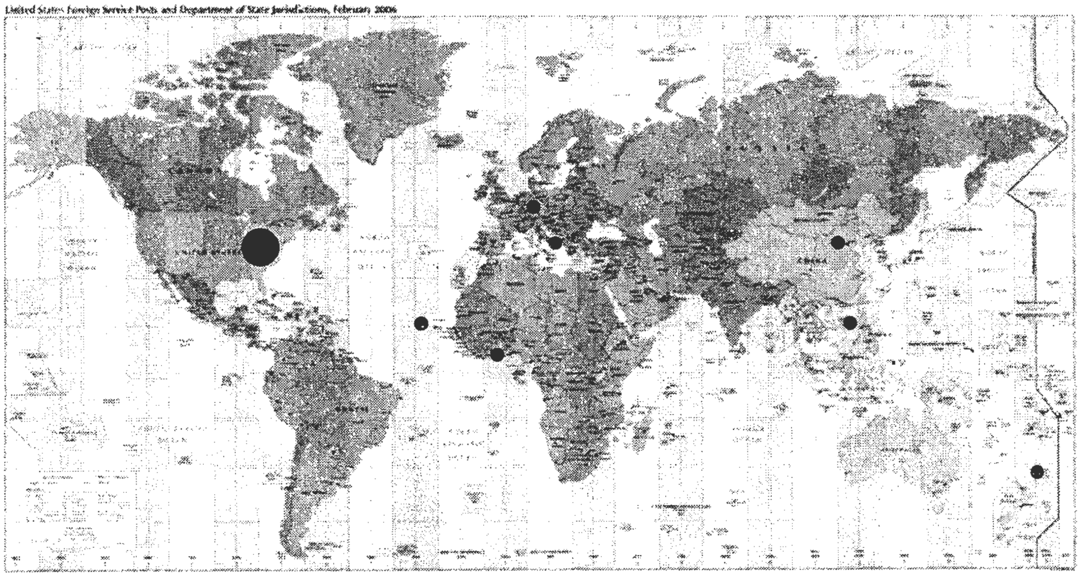
Nuisance cyber attack activity is present

Executive Summary

1. **CIRT**
    - The RCSO in Frankfurt, Germany reported several OpenNet+ computers running an unauthorized commercial application
    - Embassy Beijing ECON personnel targets of spear phishing attack

2. **CTAD Daily Read File**
    - (Classified content – See ClassNet for details)

Geographic Distribution of Computer Incident Response Team (CIRT) Events


United States Foreign Service Posts and Department of State Jurisdictions, February 2006

Legend: • *1 event* ● *2 events* ⬤ *3+ events*

DECLASSIFIED

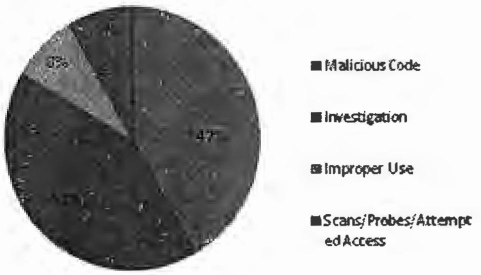
E

Open CIRT Events: 7 **Closed CIRT Events: 5**

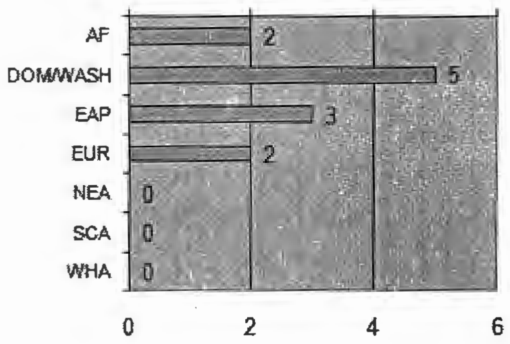
b7E

DECLASSIFIED

CIRT Events by US-CERT Category



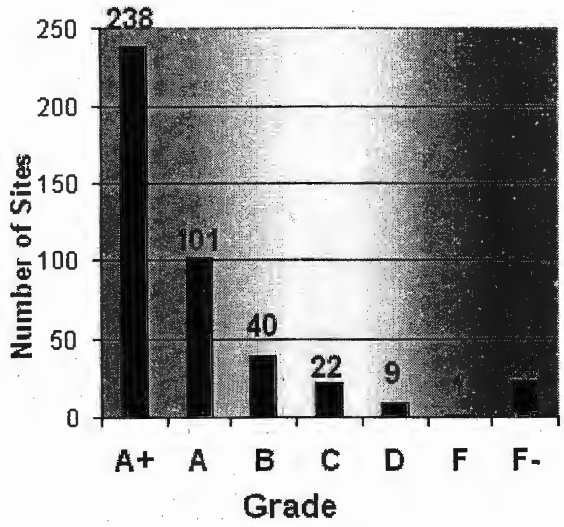
CIRT Events by Bureau



Firewall Block Request Summary

- Nothing substantial to report

Enterprise Risk Score Grade Distribution



Computer Incident Response Team (CIRT)

- The RCSO in Frankfurt, Germany reported several

b7E

E

- CIRT was notified that multiple DoS users in Beijing's ECON office were recipients [redacted]

b7E

DECLASSIFIED

Personally identifiable information (PII) loss reported

- Nothing substantial to report

Classified spillage incident(s) reported to CIRT and referred to DS/IS/APD

- Nothing substantial to report

US-CERT Coordination

- Nothing substantial to report

Compliance & Vulnerability Scanning

- *See Appendix B for statistics*

Cyber Threat Analysis Division (CTAD)

DAILY READ FILE: (Classified content – See CTAD Daily Read File on ClassNet for details)

***Virus Incident Response Team (VIRT) Statistics** (as of midnight eastern time)*

Spam Blocked at Perimeter:	**Virus Blocked at Perimeter:**
Previous day: **1,809,554**	Previous day:**83**
Month to date - June: **26,339,537**	Month to date - June:**7,508**
Year to date for 2009: **276,130,634**	Year to date for 2009: **27,623**

Cyber Security News Headlines

IT Customers Warned of Spying Attempts by Vendors *[Source: computerworld.com]*
Cyber Commander's Dual-Hat Job *[Source: govinfosecurity.com]*
Defending IT: Words from the New Military Cyber Commander *[Source: govinfosecurity.com]*

b7E

E

Appendix A –CIRT Event Summaries

UNCLASSIFIED

Legend:	*Open Events: 7*	*Closed Events: 5*

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: E-mail - Malicious Payload (Code, Attachment, Link)

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 2052 GMT	**Affected Bureau:** DOM

Event Description

CIRT detected a large number of e-mail messages with PDF attachments from " [redacted]

b7E

Current Status

25 Jun: CIRT requested a status update from the IT Service Center via e-mail and phone. The ITSC will re-open this ticket and forward the initial request to the correct ISSO.

Status History

16 Jun: CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
17 Jun: The IT Service Center has provided a reference number for this event.
18 Jun: CIRT requested a status update from the ISSO via e-mail.
19 Jun: The IT Service Center informed CIRT that the ticket has been assigned to the appropriate point of contact, and that remediation is in progress.
20 Jun: The IT Service Center resent the initial e-mail to the correct ISSO.
22 Jun: CIRT requested a status update from the IT Service Center via e-mail and phone.
23 Jun: CIRT requested additional information regarding the physical location of the user.
24 Jun: CIRT requested a status update from the IT Service Center via e-mail.

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Malicious Code directed towards an internal machine

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/25/2009 0636 GMT	**Affected Bureau:** AF

UNCLASSIFIED

b7E

E

Event Description CIRT detected malware being directed towards a DoS workstation and attempting to download an executable file.	
Current Status **25 Jun: CIRT requested that the ISSO search for specific files and perform an antivirus scan.**	
Status History **N/A - New Event**	

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: E-mail - Malicious Payload (Code, Attachment, Link)

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/25/2009 0914 GMT	**Affected Bureau:** EAP
Event Description CIRT was notified of a suspicious e-mail, possibly containing malicious code, targeting multiple users. This event consisted of [redacted]	
Current Status **25 Jun: CIRT requested that the ISSO determine if the users received the e-mail and if the e-mail has been opened or deleted. CIRT also requested that the ISSO identify any additional recipients if the e-mail has been forwarded. CIRT requested that the** [redacted]	
Status History **N/A - New Event**	

b7E

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Malicious Code directed towards an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/20/2009 0744 GMT	**Affected Bureau:** DOM
Event Description CIRT detected the download of an executable from a suspected phishing site.	
Current Status **25 Jun: CIRT requested a status update via telephone. The ticket has been assigned to a DSD technician.**	

b7E

E

Status History
22 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.
23 Jun: CIRT requested a status update from the ISSO via e-mail.
24 Jun: CIRT has resent the initial request to the IT Service Center.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/25/2009 0849 GMT	**Affected Bureau:** DOM

Br ✓

Event Description
CIRT detected the download of a malicious executable to a DoS workstation

Current Status
25 Jun: CIRT requested that the ISSO disconnect the workstation from the network and reimage the operating system.

Status History
N/A - New Event

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Unauthorized Software Downloaded to a DoS machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/22/2009 1230 GMT	**Affected Bureau:** AF

Br ✓

Event Description
CIRT detected the download of a malicious executable to a DoS workstation.

Current Status
25 Jun: CIRT requested a status update from the IT Service Center via e-mail and phone.

Status History
22 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.
23 Jun: The ISSO informed CIRT that he is currently examining this event.
24 Jun: The ISSO informed CIRT that the workstation is being examined and an update will be provided upon completion.

DECLASSIFIED

b7E
E

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Virus/Worm on an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/24/2009 0944 GMT	**Affected Bureau:** EAP

b6 ✓

Event Description
CIRT detected a DoS workstation downloading a suspicious executable file from a website.

Current Status
25 Jun: CIRT requested a status update from the ISSO via e-mail.

Status History
24 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Malicious Code directed towards an internal machine

JAVASCRIPT SHELLCODE DETECTED: CIRT detected a large number of e-mail messages [redacted]

b7E

Ticket Number	Location	Bureau	Date Opened	Awaiting Post Response	Post is Remediating	Date Closed
[redacted]	[redacted]	EAP	06-12-09			06-25

US-CERT Category: CAT 4 (Improper Use)
Event Type Confirmed: Configuration Issue

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/25/2009 0813 GMT	**Affected Bureau:** EUR

b6 ✓

Event Description
CIRT was notified of suspicious network activity from a number [redacted]

b7E

b7E

b7E E

[redacted]

Final Action
25 Jun: CIRT implemented [redacted]

b7E

Status History
N/A - New Event

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Malicious Code directed towards an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/25/2009 0836 GMT	**Affected Bureau:** DOM

Event Description
CIRT detected the download of a malicious executable to a DoS workstation.

Final Action
25 Jun: CIRT requested that the ISSO disconnect the workstation from the network and reimage the operating system. The ISSO did not find any malicious files on the workstation. As a precaution, the hard drive will be removed and replaced.

Status History
N/A - New Event

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/25/2009 0820 GMT	**Affected Bureau:** DOM

Event Description
CIRT detected the download of a malicious executable onto a DoS workstation.

Final Action
25 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management. The ISSO reported that no unauthorized files were found on the workstation, the results of a virus scan were negative, and all patches are current.

Status History
N/A - New Event

b2E

E

DECLASSIFIED

US-CERT Category: CAT 6 (Scans/Probes/Attempted Access)
Event Type Confirmed: Unauthorized Hardware connected to a DoS network

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/25/2009 0802 GMT	**Affected Bureau:** EUR
Event Description CIRT was notified of possible unauthorized attempts to connect to a server.	
Final Action **25 Jun: The ISSO informed CIRT that an unauthorized laptop was located and removed from the network.**	
Status History **N/A - New Event**	

✓

b7E

E

Appendix B – Compliance & Vulnerability Scanning Statistics

DECLASSIFIED

Vulnerability Totals:

Total Critical Vulnerabilities: 8,818

Total High Vulnerabilities: 504,937

Top 10 Critical Vulnerabilities

Vulnerability	CVSS Score	Count
[redacted]	10.00	1195
[redacted]	10.00	1154
[redacted]	10.00	956
[redacted]	10.00	806
[redacted]	10.00	599
[redacted]	10.00	495
[redacted]	10.00	459
[redacted]	10.00	375
[redacted]	10.00	281
[redacted]	10.00	241

b7E

Top 10 High Vulnerabilities

[redacted]	CVSS Score	Count
[redacted]	9.30	27444
[redacted]	7.00	26894
[redacted]	9.30	24805
[redacted]	9.30	24730
[redacted]	9.30	24538
[redacted]	9.30	17337
[redacted]	9.30	12869
[redacted]	9.30	12825
[redacted]	9.30	8029
[redacted]	9.30	7998

b7E

DECLASSIFIED

b7E
E

DECLASSIFIED

Top 10 Most Common Vulnerabilities

Vulnerability	CVSS Score	Count
[redacted]	9.30	27444
[redacted]	7.00	26894
[redacted]	9.30	24805
[redacted]	9.30	24730
[redacted]	9.30	24538
[redacted]	5.10	23727
[redacted]	9.30	17337
[redacted]	9.30	12869
[redacted]	9.30	12825
[redacted]	9.30	8029

b7E

Top 10 Compliance Failures

Configuration Setting	Count
[redacted]	63426
[redacted]	63063
[redacted]	63056
[redacted]	56271
[redacted]	53824
[redacted]	45738
[redacted]	34073
[redacted]	29613
[redacted]	29531
[redacted]	29511

b7E

DECLASSIFIED

DECLASSIFIED

Appendix C – DoS Cyber Condition (CyberCon) Levels

CyberCon Level	Tripwires	Actions
Significant cyber attacks are currently occurring	• Degradation, denial, or destruction of systems • Highly sophisticated attacks • Major tensions within country / significant catastrophic events • ***DoS is unable to execute its diplomatic mission*** • ***Widespread or focused attacks targeting vulnerabilities within the enterprise require an immediate coordinated response.*** • ***Network infrastructure throughput is severed.*** • ***Common network services are disrupted.*** • ***Sensitive information in the enterprise is at high risk of compromise.***	• Disconnection of Internet connectivity • Task Force initialization • Documented Remediation Steps completed and verified prior to re-connection
HIGH **Significant cyber attacks are imminent or moderate attacks are occurring**	• Widespread malicious activity • Intelligence indicates targeted activity • Increase in sophisticated recon and probes • Heightened tensions within country or major event • ***DoS must resort to alternative communications means to execute its diplomatic mission*** • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at moderate risk of compromise.***	• Initiate Management Team briefings • Three-times-a-day notification to pre-determined recipient list • Additional sniffers deployed as needed • Authorize limited OT for analysts

DECLASSIFIED

ELEVATED **Moderate cyber attacks are imminent**	• Increased risk • Limited malicious activity • Intelligence indicates general threats • Specific incidents reported and under review • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at some risk of compromise.***	• Ensure protective measures implemented • Increase backups, audits, etc. • Verify response action plans & staff ready • Document changes in cyber security posture
GUARDED **Nuisance cyber attack activity is present**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Potential malicious activity within the enterprise may be handled thorough routine channels and procedures.*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.*** • ***Existing countermeasures are likely to be adequate to counter this threat***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures
LOW **Nuisance cyber attack activity is expected**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Automated response is sufficient to counter potential malicious activity within the enterprise*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures

Appendix D – Intranet Web Links of Interest

DECLASSIFIED

Within the Office of Computer Security

- **Awareness**
  Periodic Update: http://cs.ds.state.gov/ETPA/ETPA_03.cfm
- **Computer Incident Response Team (CIRT)**
  Periodic Update: http://cs.ds.state.gov/CIRT/CIRT_08.cfm
- **Cyber Threat Analysis Division (CTAD)**
  Daily Read File: http://source.ds.state.sgov.gov (ClassNet)
  Tactical Awareness: http://cs.ds.state.gov/CTAD/CTAD_07.cfm
- **The Office of Computer Security**
  Periodic Update: http://cs.ds.state.gov/index.cfm
- **Compliance and Vulnerability Scanning**
  Periodic Update: http://cs.ds.state.gov/index.cfm

Outside of the Office of Computer Security

- **Cyber Security Incident Program**
  Periodic Update: http://csip.ds.state.gov
- **Enterprise Network Management**
  Periodic Update: http://enm.irm.state.gov
- **The Office of Information Assurance**
  Periodic Update: http://ia.irm.state.gov/
- **Patch Management**
  Periodic Update: http://enm.irm.state.gov/nlm/patch/Default.htm
- **Virus Incident Response Team (VIRT)**
  Periodic Update: http://sysintegweb.irm.state.gov/si/AntiVirus.html

The CIRT welcomes all constructive feedback to ~~the daily~~ Cyber Security Brief. If you have feedback for the CSB, please send it to CIRT@state.gov

P ~~0~~ 017
D7E
E

Cyber Security Brief

DECLASSIFIED

United States Department of State
Bureau of Diplomatic Security
as of June 26, 2009-1400 EST

June 29, 2009

Current DoS Cyber Threat Condition

GUARDED

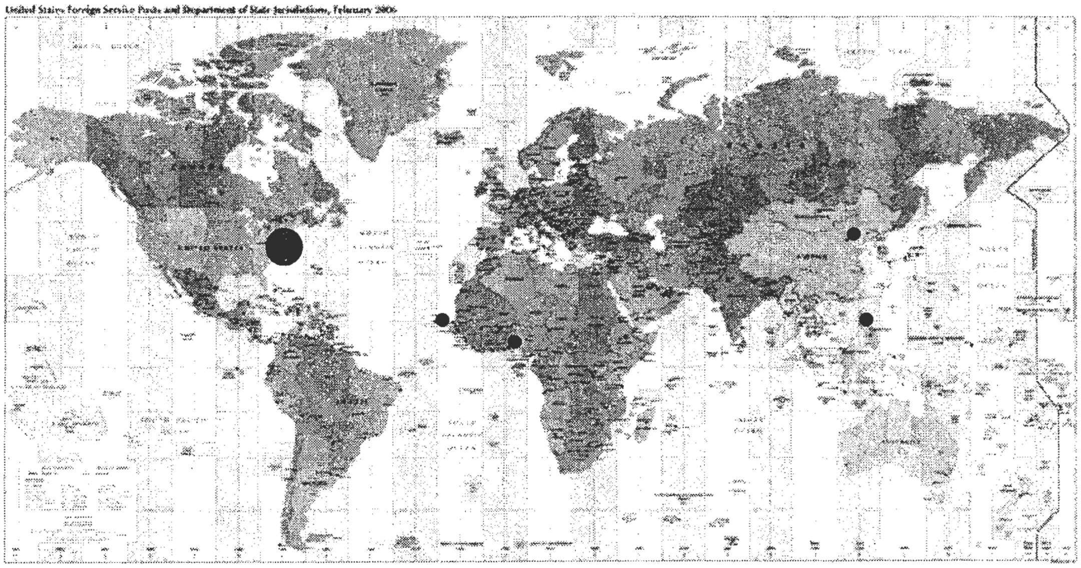
No change from last reported condition

Nuisance cyber attack activity is present

Executive Summary

1. <u>CIRT</u>
   - CIRT is currently reviewing a potentially hostile Spam message that targeted Department users
2. **<u>CTAD Daily Read File</u>**
   - (classified content)
3. **<u>Personally identifiable information loss reported</u>**
   - Unauthorized access to passport record of high profile individual/celebrity
4. **<u>Classified Spillage incident reported</u>**
   - A classified spillage reported in Washington, DC

<u>Geographic Distribution of Computer Incident Response Team (CIRT) Events</u>


United States Foreign Service Posts and Department of State Jurisdictions, February 2006

Legend: • *1 event* ● *2 events* ⬤ *3+ events*

DECLASSIFIED

b7E

E

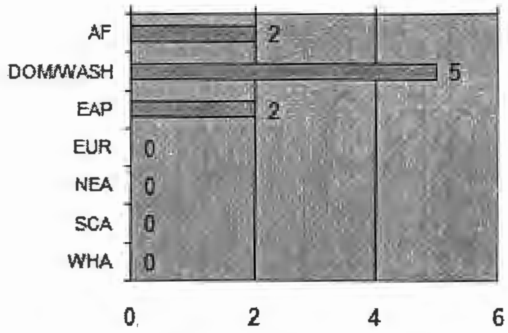
Open CIRT Events: 7

Closed CIRT Events: 2

DECLASSIFIED

CIRT Events by US-CERT Category

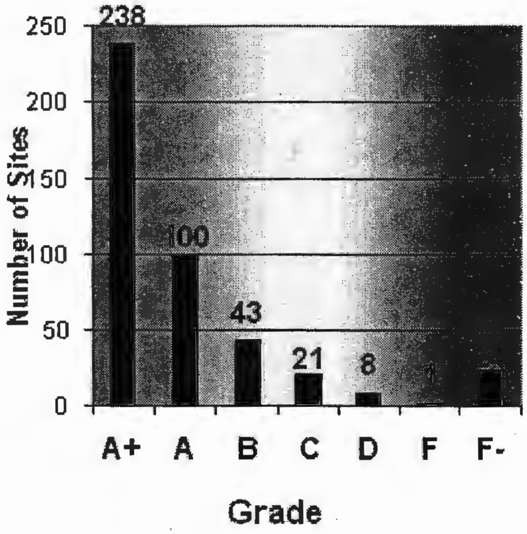
CIRT Events by Bureau



Firewall Block Request Summary

- Nothing substantial to report

Enterprise Risk Score Grade Distribution



Computer Incident Response Team (CIRT)

- CIRT is currently reviewing a [redacted]

b7E

Personally identifiable information (PII) loss reported

- CIRT was informed that unauthorized access to the PIERS passport record of a high profile individual/celebrity may have occurred. This event has been referred to US-CERT and the Privacy Team.

Classified spillage incident(s) reported to CIRT and referred to DS/IS/APD

- An incident of classified spillage in Washington, DC was reported to CIRT and has been referred to DS/APD.

US-CERT Coordination

- Nothing substantial to report

Compliance & Vulnerability Scanning

- *See Appendix B for statistics*

Cyber Threat Analysis Division (CTAD)

DAILY READ FILE: (Classified content – See CTAD Daily Read File on ClassNet for details)

Virus Incident Response Team (VIRT) Statistics *(as of midnight eastern time)*

Spam Blocked at Perimeter:	Virus Blocked at Perimeter:
Previous day: **1,423,892**	Previous day:**113**
Month to date - June: **27,763,429**	Month to date - June:**7,621**
Year to date for 2009: **277,554,526**	Year to date for 2009: **27,736**

Cyber Security News Headlines

Wide-Ranging Changes Might be Sought for Cybersecurity *[Source: nextgov.com]*
British Intelligence Agencies to Step Up Security over Cyber-Attack Threats *[Source: guardian.co.uk]*
Ex-DHS Cyber Chief Tapped as President of ICANN *[Source: washingtonpost.com]*

b7E
E

UNCLASSIFIED

Appendix A – CIRT Event Summaries:

Legend:	*Open Events: 7*	*Closed Events: 2*

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: E-mail – Malicious Payload (Code, Attachment, Link)

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/16/2009 2052 GMT	**Affected Bureau:** DOM

b7E

Event Description

CIRT detected a large number of e-mail messages with PDF attachments from " [redacted]

b7E

Current Status

26 Jun: CIRT requested a status update from the IT Service Center via e-mail and phone.

Status History

16 Jun: CIRT requested that the ISSO determine if the suspicious message had been received and if the message had been opened or deleted. If the message was opened, CIRT requested that the ISSO re-image the operating system.
17 Jun: The IT Service Center has provided a reference number for this event.
18 Jun: CIRT requested a status update from the ISSO via e-mail.
19 Jun: The IT Service Center informed CIRT that the ticket has been assigned to the appropriate point of contact, and remediation is in progress.
20 Jun: The IT Service Center resent the initial e-mail to the correct ISSO.
22 Jun: CIRT requested a status update from the IT Service Center via e-mail and phone.
23 Jun: CIRT requested additional information regarding the physical location of the user.
24 Jun: CIRT requested a status update from the IT Service Center via e-mail.
25 Jun: CIRT requested a status update from the IT Service Center via e-mail and phone. The ITSC will re-open this ticket and forward the initial request to the correct ISSO.

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Malicious Code directed towards an internal machine

Ticket Number: [redacted]	**Location:** [redacted]

b7E

b7E
E

Date and Time Ticket Created: 06/25/2009 0636 GMT	**Affected Bureau:** AF

DECLASSIFIED

Event Description
CIRT detected malware being directed towards a DoS workstation and attempting to download an executable file.

Current Status
26 Jun: CIRT requested a status update via e-mail from the ISSO.

Status History
25 Jun: CIRT requested that the ISSO search for specific files and perform an antivirus scan.

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: E-mail - Malicious Payload (Code, Attachment, Link)

Bm ✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/25/2009 0914 GMT	**Affected Bureau:** EAP

b7E

Event Description
CIRT was notified of a suspicious e-mail, possibly containing malicious code, targeting multiple users. [redacted]

Current Status
26 Jun: CIRT requested a status update from the ISSO via e-mail.

Status History
25 Jun: CIRT requested a status update from the ISSO via e-mail.
25 Jun: CIRT requested that the ISSO determine if the users had received the e-mail and if the e-mail has been opened or deleted. CIRT also requested that the ISSO identify any additional recipients if the e-mail has been forwarded. CIRT requested that the ISSO verify [redacted]

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Malicious Code directed toward internal machine

Bm ✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/20/2009 0744 GMT	**Affected Bureau:** DOM

Event Description
CIRT detected the download of an executable from a suspected phishing site.

DECLASSIFIED

b75
E

Current Status
26 Jun: CIRT requested a status update from the IT Service Center via e-mail and telephone.

Status History
22 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.
23 Jun: CIRT requested a status update from the ISSO via e-mail.
24 Jun: CIRT has resent the initial request to the IT Service Center.
25 Jun: CIRT requested a status update via telephone. The ticket has been assigned to a DSD technician.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/25/2009 0849 GMT	**Affected Bureau:** DOM

Bm ✓

Event Description
CIRT detected the download of a malicious executable to a DoS workstation

Current Status
26 Jun: CIRT requested a status update from the ISSO via e-mail.

Status History
25 Jun: CIRT requested that the ISSO disconnect the workstation from the network and reimage the operating system.

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Unauthorized Software Downloaded to a DoS machine

Ticket Number [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/22/2009 1230 GMT	**Affected Bureau:** AF

Bm ✓

Event Description
CIRT detected the download of a malicious executable to a DoS workstation.

Current Status
26 Jun: The ISSO informed CIRT that the workstation was reimaged and is awaiting the user's return in July. The ISSO requested that the ticket be placed in pending status.

Status History
22 Jun: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

E
b7G

23 Jun: The ISSO informed CIRT that he is currently examining this event.
24 Jun: The ISSO informed CIRT that the workstation is being examined and an update will be provided upon completion.
25 Jun: CIRT requested a status update from the IT Service Center via e-mail and phone.

DECLASSIFIED

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Virus/Worm on an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/24/2009 0944 GMT	**Affected Bureau:** EAP
Event Description CIRT detected a DoS workstation downloading a suspicious executable file from a website.	
Current Status **26 Jun: CIRT requested a status update from the ISSO via e-mail.**	
Status History **24 Jun:** CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management. **25 Jun:** CIRT requested a status update from the ISSO via e-mail.	

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Information Security Issue (violation or infraction)

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/26/2009 1221 GMT	**Affected Bureau:** DOM
Event Description Personally Identifiable Information (PII) may have been breached or disclosed to unauthorized third parties.	
Final Action **26 Jun: This ticket has been referred to US-CERT and the Privacy Office**	
Status History **N/A - New Event**	

Ticket Number: [redacted]	**Location:** [redacted]

DECLASSIFIED

Date and Time Ticket Created: 06/26/2009 1351 GMT	**Affected Bureau:** DOM
Event Description CIRT was notified of a Classified Spillage	
Final Action **26 Jun: CIRT has referred this classified spillage to DS-ADP.**	
Status History **N/A - New Event**	

DECLASSIFIED

E

b7E

Appendix B – Compliance & Vulnerability Scanning Statistics

Vulnerability Totals:

Total Critical Vulnerabilities: 9,241
Total High Vulnerabilities: 518,769

Top 10 Critical Vulnerabilities

Vulnerability	CVSS Score	Count
[redacted]	10.00	1211
[redacted]	10.00	1154
[redacted]	10.00	955
[redacted]	10.00	807
[redacted]	10.00	614
[redacted]	10.00	498
[redacted]	10.00	494
[redacted]	10.00	431
[redacted]	10.00	375
[redacted]	10.00	292

b7E

Top 10 High Vulnerabilities

Vulnerability	CVSS Score	Count
[redacted]	9.30	27907
[redacted]	7.00	27327
[redacted]	9.30	25259
[redacted]	9.30	25184
[redacted]	9.30	24992
[redacted]	9.30	17491
[redacted]	9.30	13195
[redacted]	9.30	13151
[redacted]	9.30	8292

b7E

b7E

QuickTime	[redacted]	9.30	8259

DECLASSIFIED

Top 10 Most Common Vulnerabilities

Vulnerability	CVSS Score	Count
[redacted]	9.30	27907
[redacted]	7.00	27327
[redacted]	9.30	25259
[redacted]	9.30	25184
[redacted]	9.30	24992
[redacted]	5.10	23612
[redacted]	9.30	17491
[redacted]	9.30	13195
[redacted]	9.30	13151
[redacted]	9.30	8292

b7E

Top 10 Compliance Failures

Configuration Setting	Count
[redacted]	63768
[redacted]	63393
[redacted]	63392
[redacted]	56634
[redacted]	54249
[redacted]	45983
[redacted]	34562
[redacted]	29764
[redacted]	29645
[redacted]	29628

b7E

Appendix C – DoS Cyber Condition (CyberCon) Levels

CyberCon Level	Tripwires	Actions
Significant cyber attacks are currently occurring	• Degradation, denial, or destruction of systems • Highly sophisticated attacks • Major tensions within country / significant catastrophic events • ***DoS is unable to execute its diplomatic mission*** • ***Widespread or focused attacks targeting vulnerabilities within the enterprise require an immediate coordinated response.*** • ***Network infrastructure throughput is severed.*** • ***Common network services are disrupted.*** • ***Sensitive information in the enterprise is at high risk of compromise.***	• Disconnection of Internet connectivity • Task Force initialization • Documented Remediation Steps completed and verified prior to re-connection
HIGH **Significant cyber attacks are imminent or moderate attacks are occurring**	• Widespread malicious activity • Intelligence indicates targeted activity • Increase in sophisticated recon and probes • Heightened tensions within country or major event • ***DoS must resort to alternative communications means to execute its diplomatic mission*** • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at moderate risk of compromise.***	• Initiate Management Team briefings • Three-times-a-day notification to pre-determined recipient list • Additional sniffers deployed as needed • Authorize limited OT for analysts

DECLASSIFIED

ELEVATED **Moderate cyber attacks are imminent**	• Increased risk • Limited malicious activity • Intelligence indicates general threats • Specific incidents reported and under review • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at some risk of compromise.***	• Ensure protective measures implemented • Increase backups, audits, etc. • Verify response action plans & staff ready • Document changes in cyber security posture
GUARDED **Nuisance cyber attack activity is present**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Potential malicious activity within the enterprise may be handled thorough routine channels and procedures.*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.*** • ***Existing countermeasures are likely to be adequate to counter this threat***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures
LOW **Nuisance cyber attack activity is expected**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Automated response is sufficient to counter potential malicious activity within the enterprise*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures

DECLASSIFIED

Appendix D – Intranet Web Links of Interest

UNCLASSIFIED

Within the Office of Computer Security

- **Awareness**
  Periodic Update: http://cs.ds.state.gov/ETPA/ETPA_03.cfm
- **Computer Incident Response Team (CIRT)**
  Periodic Update: http://cs.ds.state.gov/CIRT/CIRT_08.cfm
- **Cyber Threat Analysis Division (CTAD)**
  Daily Read File: http://source.ds.state.sgov.gov (ClassNet)
  Tactical Awareness: http://cs.ds.state.gov/CTAD/CTAD_07.cfm
- **The Office of Computer Security**
  Periodic Update: http://cs.ds.state.gov/index.cfm
- **Compliance and Vulnerability Scanning**
  Periodic Update: http://cs.ds.state.gov/index.cfm

Outside of the Office of Computer Security

- **Cyber Security Incident Program**
  Periodic Update: http://csip.ds.state.gov
- **Enterprise Network Management**
  Periodic Update: http://enm.irm.state.gov
- **The Office of Information Assurance**
  Periodic Update: http://ia.irm.state.gov/
- **Patch Management**
  Periodic Update: http://enm.irm.state.gov/nlm/patch/Default.htm
- **Virus Incident Response Team (VIRT)**
  Periodic Update: http://sysintegweb.irm.state.gov/si/AntiVirus.html

The CIRT welcomes all constructive feedback to the daily Cyber Security Brief
If you have feedback for the CSB, please send it to CIRT@state.gov

T 019
b7E E

Cyber Security Brief

DECLASSIFIED

United States Department of State
Bureau of Diplomatic Security
as of July 2, 2009-1400 EST

July 6, 2009

Current DoS Cyber Threat Condition

GUARDED

No change from last reported condition

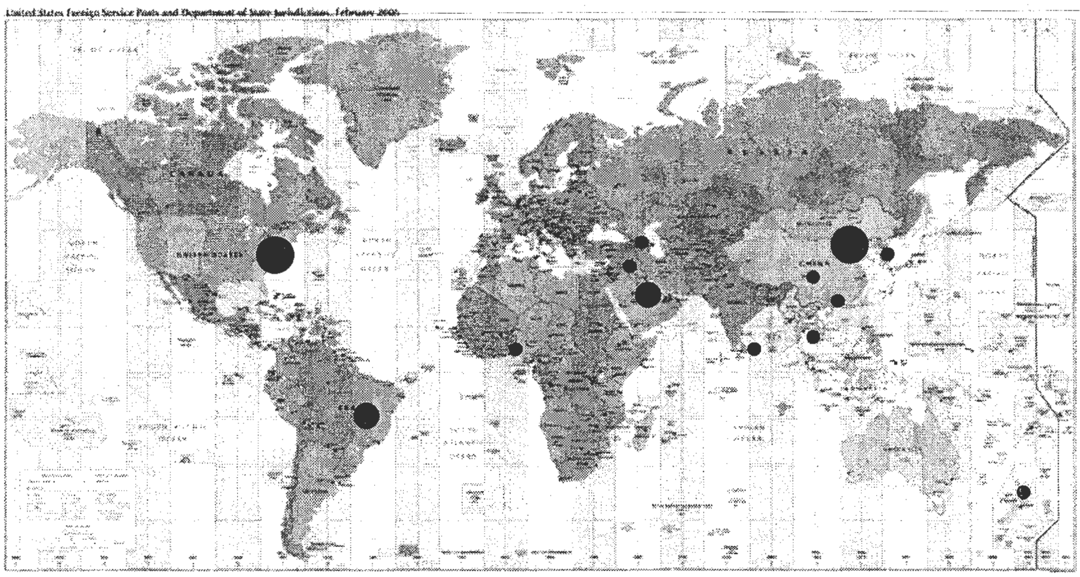
Nuisance cyber attack activity is present

Executive Summary

1. CIRT
   - Large scale phishing attack targeting multiple seemingly unrelated Department of State employees

2. CTAD Daily Read File
   - (U) Instant Messaging Malware on the Rise, Again

Geographic Distribution of Computer Incident Response Team (CIRT) Events


United States Foreign Service Posts and Department of State Jurisdictions, February [illegible]

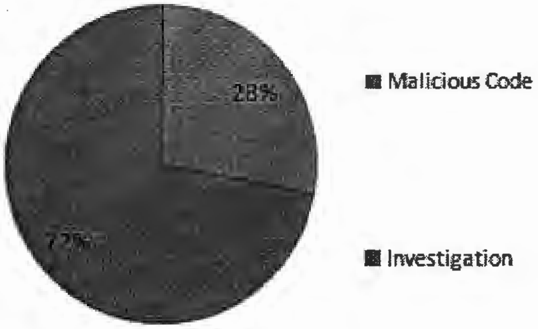
Legend: • *1 event* ● *2 events* ⬤ *3+ events*

DECLASSIFIED

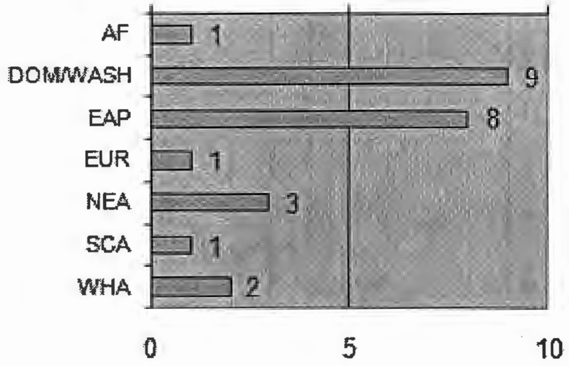
Open CIRT Events: 19 **Closed CIRT Events: 6**

DECLASSIFIED

CIRT Events by US-CERT Category



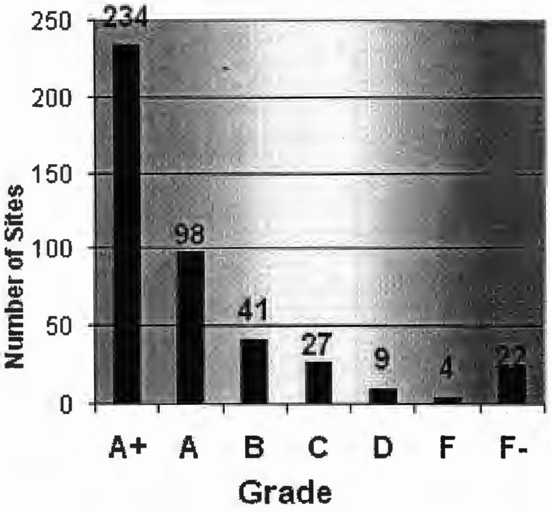
CIRT Events by Bureau



Firewall Block Request Summary

- Nothing substantial to report

Enterprise Risk Score Grade Distribution



Computer Incident Response Team (CIRT)

- CIRT detected a large scale spear phishing campaign targeting DoS employees, both stateside and abroad. CIRT is in the process of contacting the affected users. Due to the large number of tickets generated, these tickets are presented in table format. CIRT anticipates that there will be more tickets opened in the next several days.

Personally identifiable information (PII) loss reported

- Nothing substantial to report

E

b7E

Classified spillage incident(s) reported to CIRT and referred to DS/IS/APD

- Nothing substantial to report

DECLASSIFIED

US-CERT Coordination

- Nothing substantial to report

Compliance & Vulnerability Scanning

- *See Appendix B for statistics*

Cyber Threat Analysis Division (CTAD)

DAILY READ FILE: (U) Instant Messaging Malware on the Rise, Again

(U) Key Highlights:

- *MessageLabs research indicates that IM malware has increased in the last six months*
- *Analysts predict that 1 in 80 IM users will receive a malicious IM each month*
- *The rise in malware could be correlated to recent advancements in CAPTCHA breaking*
- *DoS personnel are reminded that Web-based and locally loaded installation of IM clients and Chat software are prohibited on Department computers*

b7E

***Virus Incident Response Team (VIRT) Statistics** (as of midnight eastern time)*

Spam Blocked at Perimeter:	Virus Blocked at Perimeter:
Previous day: **1,263,747**	Previous day:**89**
Month to date - July: **1,263,747**	Month to date - July:**89**
Year to date for 2009: **284,798,882**	Year to date for 2009: **34,250**

Cyber Security News Headlines

White House Pledges to Stay On Top of Cybersecurity *[Source: fiercegovernmentit.com]*
Cybersecurity Plan Means New Jobs *[Source: govinfosecurity.com]*
Justice Tech a Big Winner in Senate Spending Bill *[Source: fcw.com]*

DECLASSIFIED

b7E

Appendix A –CIRT Event Summaries

DECLASSIFIED

Legend:	*Open Events: 19*	*Closed Events: 6*

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Malicious Code directed towards an internal machine

[redacted] CIRT detected a large number of e-mail messages [redacted]

b7E

Ticket Number	Location (# of Users)	Bureau	Date Opened	Awaiting Post Response	Post is Remediating	Date Closed
[redacted]	[redacted]	EAP	7-02			
[redacted]	[redacted]	EAP	7- 02			
[redacted]	[redacted]	EAP	7-02			
[redacted]	[redacted]	SCA	7-02			
[redacted]	[redacted]	NEA	7-02			
[redacted]	[redacted]	DOM	7-02			
[redacted]	[redacted]	WHA	7-02			7-02
[redacted]	[redacted]	EAP	7-02			
[redacted]	[redacted]	DOM	7-02			
[redacted]	[redacted]	DOM	7-02			
[redacted]	[redacted]	DOM	7-02			
[redacted]	[redacted]	DOM	7-02			
[redacted]	[redacted]	EAP	7-02			
[redacted]	[redacted]	DOM	7-02			

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Email - Malicious Payload (Code, Attachment, Link)

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/25/2009 0914 GMT	**Affected Bureau:** EAP

Event Description
CIRT was notified of a suspicious e-mail, possibly containing malicious code, targeting

DECLASSIFIED

E

multiple users. This event consisted [redacted] DECLASSIFIED
Current Status **2 Jul: CIRT is awaiting a response from the ISSO.**
Status History **25 Jun:** CIRT requested that the ISSO determine if the users had received the e-mail and if the e-mail has been opened or deleted. CIRT also requested that the ISSO identify any additional recipients of the e-mail if it has been forwarded. CIRT requested that the ISSO [redacted] **26 Jun:** CIRT requested a status update from the ISSO via e-mail. **29 Jun:** CIRT requested a status update from the ISSO, the RSO, and the IPO via e-mail. **30 Jun:** CIRT requested a status update from the ISSO via e-mail and phone. **1 Jul:** CIRT requested a status update from the ISSO via e-mail and phone.

b7E

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: E-mail - Phishing

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/30/2009 0800 GMT	**Affected Bureau:** EAP
Event Description CIRT detected a possible phishing e-mail, originating from various sources, containing a [redacted]	
Current Status **2 Jul: The ISSO informed CIRT that a status update is forthcoming.**	
Status History **30 Jun:** CIRT requested that the ISSO determine if the users had received the e-mail and if the e-mail has been opened or deleted. CIRT also requested that the ISSO identify any additional recipients of the e-mail if it has been forwarded. CIRT requested that the ISSO [redacted] **1 Jul:** The ISSO informed CIRT that examination of this event is ongoing.	

b7E

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Malicious Code directed towards an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/01/2009 1151 GMT	**Affected Bureau:** NEA

DECLASSIFIED

b7E

Event Description CIRT detected a malicious executable being directed at a DoS workstation.
Current Status **2 Jul: CIRT requested a status update from the ISSO via e-mail.**
Status History **1 Jul:** CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/02/2009 1422 GMT	**Affected Bureau:** DOM
Event Description CIRT detected a malicious executable file being directed at DoS workstation.	
Current Status **2 Jul: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.**	
Status History **N/A - New Event**	

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/02/2009 1346 GMT	**Affected Bureau:** WHA
Event Description CIRT detected a malicious executable directed at a DoS workstation.	
Current Status **2 Jul: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.**	
Status History **N/A - New Event**	

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Spyware/Trojan on an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/01/2009 0626 GMT	**Affected Bureau:** EAP

✓

b7E

Event Description
An ISSO notified CIRT of an e-mail with a malicious PDF attachment which was successfully quarantined [redacted]

Current Status
2 Jul: CIRT requested a status update from the ISSO via e-mail.

Status History
1 Jul: CIRT requested that the ISSO search the workstation for specific files and reimage the operating system if the files are found.

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Malicious Code directed towards an internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/22/2009 1230 GMT	**Affected Bureau:** AF

✓

Event Description
CIRT detected the download of a malicious executable to a DoS workstation.

Final Action
2 Jul: This event had been pending awaiting the user's return. The ISSO reported that workstation has been re-imaged.

Status History
June 22-July 2: Remediation pending.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/02/2009 0917 GMT	**Affected Bureau:** DOM

✓

b7E

Event Description
US-CERT detected DoS workstations [redacted]

Final Action

b7E

2 Jul: The traffic was analyzed and nothing malicious was found.

DECLASSIFIED

Status History
N/A - New Event

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/01/2009 1241 GMT	**Affected Bureau:** NEA

Event Description
CIRT detected a malicious executable being directed at a DoS workstation.

Final Action
2 Jul: The ISSO informed CIRT that no unauthorized files or software was discovered on the workstation. The machine contains the latest patches from Patch Management.

Status History
1 Jul: CIRT requested that the ISSO search for specific files and reimage the operating system if the files are found.

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Non-event

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/02/2009 1010 GMT	**Affected Bureau:** EUR

Event Description
CIRT received notification from the systems manager about server crashes.

Final Action
2 Jul: These events were found to be caused by E & V Scanning activities.

Status History
N/A - New Event

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/30/2009 1335 GMT	**Affected Bureau:** DOM

Event Description
CIRT was notified of a suspicious e-mail, possibly containing malicious code. This event

b7E

Final Action **2 Jul: The ISSO informed CIRT that the hard drive has been shipped to TASO.**	
Status History **30 Jun:** CIRT requested that the ISSO ship the user's hard drive to TASO for analysis. **1 Jul:** CIRT requested a status update from the ISSO via e-mail.	

b7E

E

Appendix B – Compliance & Vulnerability Scanning Statistics

Vulnerability Totals:

Total Critical Vulnerabilities: 9,544

Total High Vulnerabilities: 575,804

Top 10 Critical Vulnerabilities

Vulnerability	CVSS Score	Count
[redacted]	10.00	1514
[redacted]	10.00	1131
[redacted]	10.00	956
[redacted]	10.00	796
[redacted]	10.00	703
[redacted]	10.00	553
[redacted]	10.00	506
[redacted]	10.00	391
[redacted]	10.00	313
[redacted]	10.00	284

b7E

Top 10 High Vulnerabilities

[redacted]	CVSS Score	Count
[redacted]	9.30	31104
[redacted]	7.00	30704
[redacted]	9.30	28374
[redacted]	9.30	28321
[redacted]	9.30	28123
[redacted]	9.30	20191
[redacted]	9.30	14944
[redacted]	9.30	14886
[redacted]	9.30	9579
[redacted]	9.30	9425

b7E

UNCLASSIFIED

b7E

E

DECLASSIFIED

Top 10 Most Common Vulnerabilities

Vulnerability	CVSS Score	Count
[redacted]	9.30	31104
[redacted]	7.00	30704
[redacted]	9.30	28374
[redacted]	9.30	28321
[redacted]	9.30	28123
[redacted]	5.10	24360
[redacted]	9.30	20191
[redacted]	9.30	14944
[redacted]	9.30	14886
[redacted]	9.30	9579

b7E

Top 10 Compliance Failures

Configuration Setting	Count
[redacted]	63783
[redacted]	63421
[redacted]	63418
[redacted]	56740
[redacted]	45972
[redacted]	34297
[redacted]	29873
[redacted]	29753
[redacted]	29736
[redacted]	29734

b7E

DECLASSIFIED

DECLASSIFIED

Appendix C – DoS Cyber Condition (CyberCon) Levels

CyberCon Level	Tripwires	Actions
Significant cyber attacks are currently occurring	• Degradation, denial, or destruction of systems • Highly sophisticated attacks • Major tensions within country / significant catastrophic events • ***DoS is unable to execute its diplomatic mission*** • ***Widespread or focused attacks targeting vulnerabilities within the enterprise require an immediate coordinated response.*** • ***Network infrastructure throughput is severed.*** • ***Common network services are disrupted.*** • ***Sensitive information in the enterprise is at high risk of compromise.***	• Disconnection of Internet connectivity • Task Force initialization • Documented Remediation Steps completed and verified prior to re-connection
HIGH **Significant cyber attacks are imminent or moderate attacks are occurring**	• Widespread malicious activity • Intelligence indicates targeted activity • Increase in sophisticated recon and probes • Heightened tensions within country or major event • ***DoS must resort to alternative communications means to execute its diplomatic mission*** • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at moderate risk of compromise.***	• Initiate Management Team briefings • Three-times-a-day notification to pre-determined recipient list • Additional sniffers deployed as needed • Authorize limited OT for analysts

DECLASSIFIED

ELEVATED **Moderate cyber attacks are imminent**	• Increased risk • Limited malicious activity • Intelligence indicates general threats • Specific incidents reported and under review • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at some risk of compromise.***	• Ensure protective measures implemented • Increase backups, audits, etc. • Verify response action plans & staff ready • Document changes in cyber security posture
GUARDED **Nuisance cyber attack activity is present**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Potential malicious activity within the enterprise may be handled thorough routine channels and procedures.*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.*** • ***Existing countermeasures are likely to be adequate to counter this threat***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures
LOW **Nuisance cyber attack activity is expected**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Automated response is sufficient to counter potential malicious activity within the enterprise*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures

Appendix D – Intranet Web Links of Interest

DECLASSIFIED

b7E

Within the Office of Computer Security

- **Awareness**
  Periodic Update: http://cs.ds.state.gov/ETPA/ETPA_03.cfm
- **Computer Incident Response Team (CIRT)**
  Periodic Update: http://cs.ds.state.gov/CIRT/CIRT_08.cfm
- **Cyber Threat Analysis Division (CTAD)**
  Daily Read File: http://source.ds.state.sgov.gov (ClassNet)
  Tactical Awareness: http://cs.ds.state.gov/CTAD/CTAD_07.cfm
- **The Office of Computer Security**
  Periodic Update: http://cs.ds.state.gov/index.cfm
- **Compliance and Vulnerability Scanning**
  Periodic Update: http://cs.ds.state.gov/index.cfm

Outside of the Office of Computer Security

- **Cyber Security Incident Program**
  Periodic Update: http://csip.ds.state.gov
- **Enterprise Network Management**
  Periodic Update: http://enm.irm.state.gov
- **The Office of Information Assurance**
  Periodic Update: http://ia.irm.state.gov/
- **Patch Management**
  Periodic Update: http://enm.irm.state.gov/nlm/patch/Default.htm
- **Virus Incident Response Team (VIRT)**
  Periodic Update: http://sysintegweb.irm.state.gov/si/AntiVirus.html

The CIRT welcomes all constructive feedback to the daily Cyber Security Brief. If you have feedback for the CSB, please send it to CIRT@state.gov

DECLASSIFIED

U14

0198 b7E

E

Cyber Security Brief

DECLASSIFIED

United States Department of State
Bureau of Diplomatic Security
as of July 6, 2009-1400 EST

July 7, 2009

Current DoS Cyber Threat Condition

GUARDED

No change from last reported condition

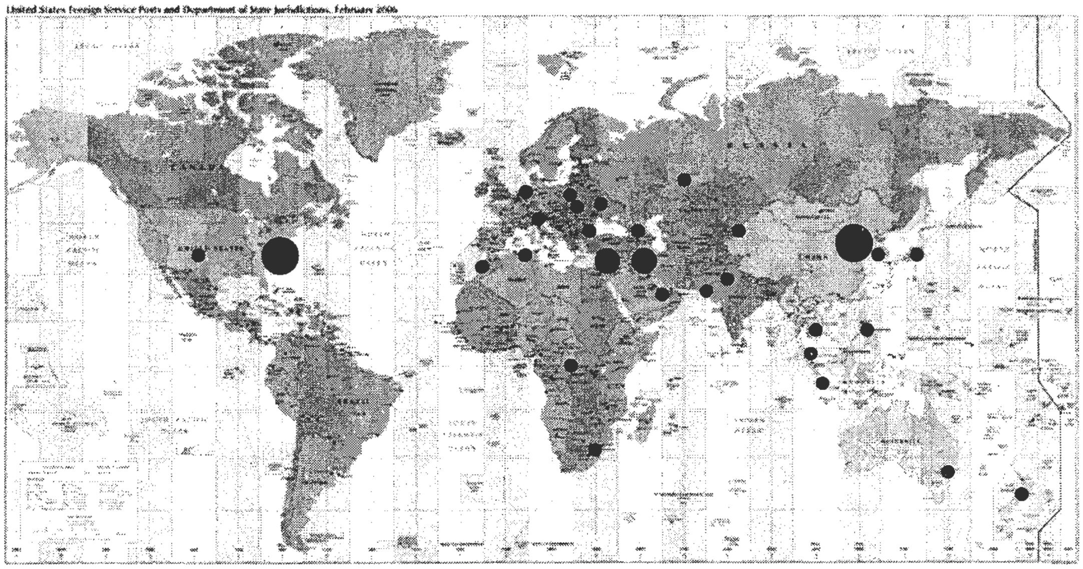
Nuisance cyber attack activity is present

Executive Summary

1. **CIRT**
   - Electrical fire at SA-20 causes evacuation and building electrical shut-down
   - CIRT continues to notify DoS ISSO's due to a large scale phishing attack

2. **CTAD Daily Read File**
   - *(Not available due to SA-20 power outage)*

Geographic Distribution of Computer Incident Response Team (CIRT) Events


United States Foreign Service Posts and Department of State Jurisdictions, February 2006

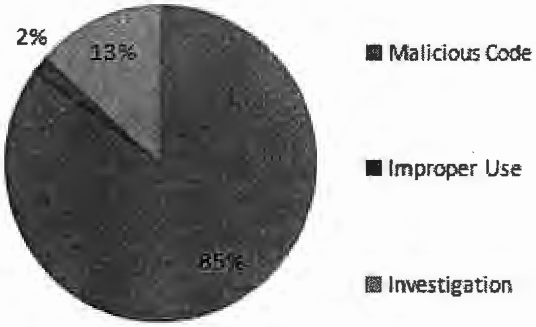
Legend: ● *1 event* ● *2 events* ● *3+ events*

DECLASSIFIED

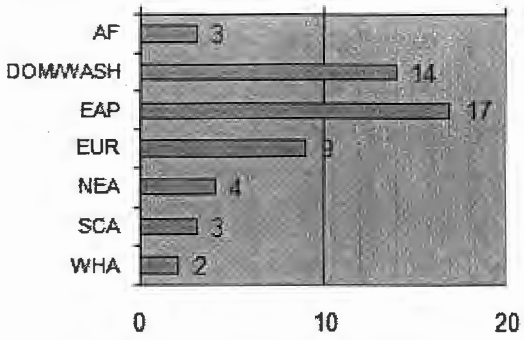
DECLASSIFIED

Open CIRT Events: 38 **Closed CIRT Events:** 14

CIRT Events by US-CERT Category



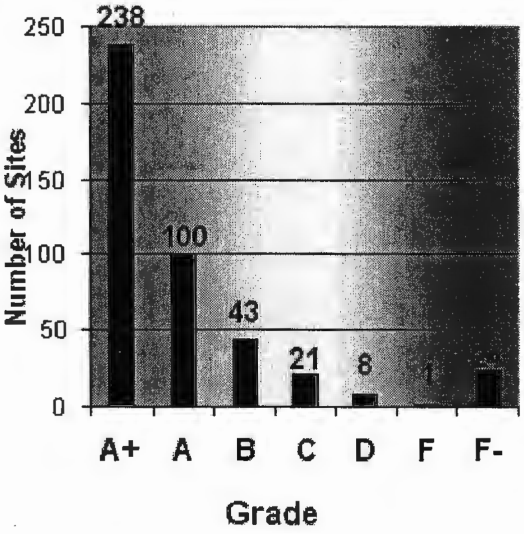
CIRT Events by Bureau



Firewall Block Request Summary

- Nothing substantial to report

Enterprise Risk Score Grade Distribution



DECLASSIFIED

Computer Incident Response Team (CIRT)

- An electrical fire at SA-20 in Arlington, VA required an evacuation of the facility for the day, along with powering down the majority of the electrical systems. A number of CIRT systems were effected (file & print servers, web servers) but CIRT remains operational at SA-26 in Beltsville, MD.

Personally identifiable information (PII) loss reported

- Nothing substantial to report

Classified spillage incident(s) reported to CIRT and referred to DS/IS/APD

- Nothing substantial to report

US-CERT Coordination

- Nothing substantial to report

Compliance & Vulnerability Scanning

- *Not available due to SA-20 power outage.*

Cyber Threat Analysis Division (CTAD)

- *Not available due to SA-20 power outage*

***Virus Incident Response Team (VIRT) Statistics** (as of midnight eastern time)*

Spam Blocked at Perimeter
Previous day: 950,283
Month to date – July: 5,455,080
Year to date for 2009: **288,990,215**

Virus Blocked at Perimeter
Previous day: 5
Month to date – July: 181
Year to date for 2009: **28,297**

Cyber Security News Headlines

NSA to participate in US cybersecurity [Source: wikinews.com]
Cyber Command Launched. US Strategic Command to Oversee Offensive [Source: dissidentvoice.org]
About Face: Obama to Proceed with Bush-Era Cybersecurity Plan [Source: .commondreams.org]

E

DECLASSIFIED

b7E

Appendix A – CIRT Event Summaries

Legend:	*Open Events: 38*	*Closed Events: 14*

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Email - Malicious Payload (Code, Attachment, Link)

b7C

Ticket Number	Location	Bureau	Open Date	Awaiting Post Response	Post is Remediating	Closed Date/Time
[redacted]	[redacted]	EAP	6/30/09		Yes	
[redacted]	[redacted]	EAP	7/2/09	Yes		
[redacted]	[redacted]	SCA	7/2/09		Yes	
[redacted]	[redacted]	DOM	7/2/09	Yes		
[redacted]	[redacted]	EAP	7/2/09	Yes		
[redacted]	[redacted]	DOM	7/2/09	Yes		
[redacted]	[redacted]	DOM	7/2/09	Yes		
[redacted]	[redacted]	DOM	7/2/09	Yes		
[redacted]	[redacted]	DOM	7/2/09		Yes	
[redacted]	[redacted]	EUR	7/2/09	Yes		
[redacted]	[redacted]	NEA	7/2/09		Yes	
[redacted]	[redacted]	SCA	7/2/09		Yes	
[redacted]	[redacted]	EUR	7/2/09		Yes	
[redacted]	[redacted]	EUR	7/2/09	Yes		
[redacted]	[redacted]	EUR	7/2/09		Yes	
[redacted]	[redacted]	EAP	7/3/09	Yes		
[redacted]	[redacted]	EAP	7/3/09	Yes		
[redacted]	[redacted]	EAP	7/3/09	Yes		
[redacted]	[redacted]	AF	7/3/09		Yes	
[redacted]	[redacted]	EUR	7/3/09	Yes		
[redacted]	[redacted]	EUR	7/3/09	Yes		
[redacted]	[redacted]	EAP	7/3/09	Yes		
[redacted]	[redacted]	EUR	7/3/09	Yes		
[redacted]	[redacted]	EAP	7/3/09		Yes	

E

b2
b7E

Ticket Number	Location	Bureau	Open Date	Awaiting Post Response	Post is Remediating	Closed Date/Time
[redacted]	[redacted]	EAP	7/3/09	Yes		
[redacted]	[redacted]	EUR	7/3/09	Yes		
[redacted]	[redacted]	EAP	7/3/09	Yes		
[redacted]	[redacted]	DOM	7/3/09	Yes		
[redacted]	[redacted]	DOM	7/3/09	Yes		
[redacted]	[redacted]	DOM	7/3/09		Yes	
[redacted]	[redacted]	DOM	7/3/09	Yes		
[redacted]	[redacted]	DOM	7/3/09	Yes		
[redacted]	[redacted]	DOM	7/3/09		Yes	
[redacted]	[redacted]	EAP	7/2/09			7/6/09
[redacted]	[redacted]	EAP	7/2/09			7/6/09
[redacted]	[redacted]	NEA	7/2/09			7/3/09
[redacted]	[redacted]	EAP	7/2/09			7/6/09
[redacted]	[redacted]	DOM	7/2/09			7/5/09
[redacted]	[redacted]	WHA	7/2/09			7/3/09
[redacted]	[redacted]	EAP	7/2/09			7/6/09
[redacted]	[redacted]	DOM	7/2/09			7/3/09
[redacted]	[redacted]	DOM	7/3/09			7/6/09
[redacted]	[redacted]	AF	7/3/09			7/6/09
[redacted]	[redacted]	EAP	7/3/09			7/6/09
[redacted]	[redacted]	EUR	7/3/09			7/6/09
[redacted]	[redacted]	NEA	7/3/09			7/6/09

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Email - Malicious Payload (Code, Attachment, Link)

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/25/2009 0914 GMT	**Affected Bureau:** EAP

Event Description
CIRT was notified [redacted]

b7E

E

b7E

Current Status
6 Jul: CIRT contacted Post for a status update. The ISSO informed CIRT that he will send an update later today.

Status History
25 Jun: CIRT requested that the ISSO determine if the users had received the e-mail and if the e-mail has been opened or deleted. CIRT also requested that the ISSO identify any additional recipients of the e-mail if it has been forwarded. CIRT requested that the ISSO [redacted]
26 Jun: CIRT requested a status update from the ISSO via e-mail.
29 Jun: CIRT requested a status update from the ISSO, the RSO, and the IPO via e-mail.
30 Jun: CIRT requested a status update from the ISSO via e-mail and phone.
1 Jul: CIRT received notification from the ISSO that they have received the ticket and have begun working the event.
2 Jul: CIRT requested a status update from the ISSO via e-mail.
3 Jul: Awaiting update from the ISSO on Tuesday due to July 4th Holiday.

b7C

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Email - Phishing

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/30/2009 0800 GMT	**Affected Bureau:** EAP

✓

Event Description
CIRT detected [redacted] originating from various sources.

b7E

Current Status
6 Jul: CIRT requested a status update from the ISSO via e-mail.

Status History
30 Jun: CIRT requested that the ISSO determine if the users had received the e-mail and if the e-mail has been opened or deleted. CIRT also requested that the ISSO identify any additional recipients of the e-mail if it has been forwarded. CIRT requested that the ISSO [redacted]
1 Jul: The ISSO informed CIRT that examination of this event is ongoing.
2 Jul: The ISSO informed CIRT that a status update is forthcoming.
3 Jul: Awaiting update from the ISSO on Tuesday due to July 4th Holiday.

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Malicious Code directed toward internal machine

Ticket Number: [redacted]	**Location:** [redacted]

✓

b7E
E

Date and Time Ticket Created: 07/01/2009 1451 GMT	**Affected Bureau:** NEA

Event Description
CIRT detected the download of a malicious executable to a DoS workstation.

Current Status
6 Jul: CIRT requested a status update from the ISSO via e-mail.

Status History
1 Jul: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.
2 Jul: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.
3 Jul: Awaiting update from the ISSO on Tuesday due to July 4th Holiday.

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Spyware/Trojan on internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/01/2009 0626 GMT	**Affected Bureau:** EAP

Event Description
An ISSO notified CIRT [redacted] n e-mail with a malicious PDF attachment.

b7E

Current Status
6 Jul: CIRT requested a status update from the ISSO via e-mail.

Status History
1 Jul: CIRT requested that the ISSO search the workstation for specific files and reimage the operating system if the files are found.
2 Jul: CIRT requested a status update from the ISSO via e-mail.
3 Jul: Awaiting update from the ISSO on Tuesday due to July 4th Holiday.

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Suspicious/Abnormal traffic

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/05/2009 2014 GMT	**Affected Bureau:** AF

I

Event Description CIRT was notified by US-CERT [redacted] to a suspicious website that may be malicious in nature.
Current Status **6 Jul: CIRT requested a status update from the ISSO via e-mail.**
Status History **5 Jul:** CIRT sent out the initial email to the ISSO on the high side.

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Unauthorized Hardware connected to DOS network

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/03/2009 0325 GMT	**Affected Bureau:** SCA
Event Description CIRT was notified by an ISSO [redacted]	
Current Status **6 Jul: CIRT requested a status update from the ISSO via e-mail.**	
Status History **3 Jul:** CIRT requested a status update from the ISSO via e-mail.	

✓

b7E

US-CERT Category: CAT 4 (Improper Usage)
Event Type Confirmed: Unauthorized Software Downloaded to DOS machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/02/2009 1346 GMT	**Affected Bureau:** WHA
Event Description CIRT detected the download of a malicious executable to a DoS workstation.	
Final Action **6 Jul: ISSO reported that the executable was not found on the workstation. Also the workstation is up to date on patches** [redacted]	
Status History **2 Jul:** CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the	

✓

b7E

workstation is up-to-date with all of the latest patches from IRM Patch Management.
3 Jul: Awaiting update from ISSO on Tuesday due to July 4th Holiday.

Appendix B – Compliance & Vulnerability Scanning Statistics

- Not available due to power outage at SA-20.

DECLASSIFIED

Appendix C – DoS Cyber Condition (CyberCon) Levels

CyberCon Level	Tripwires	Actions
Significant cyber attacks are currently occurring	• Degradation, denial, or destruction of systems • Highly sophisticated attacks • Major tensions within country / significant catastrophic events • ***DoS is unable to execute its diplomatic mission*** • ***Widespread or focused attacks targeting vulnerabilities within the enterprise require an immediate coordinated response.*** • ***Network infrastructure throughput is severed.*** • ***Common network services are disrupted.*** • ***Sensitive information in the enterprise is at high risk of compromise.***	• Disconnection of Internet connectivity • Task Force initialization • Documented Remediation Steps completed and verified prior to re-connection
HIGH **Significant cyber attacks are imminent or moderate attacks are occurring**	• Widespread malicious activity • Intelligence indicates targeted activity • Increase in sophisticated recon and probes • Heightened tensions within country or major event • ***DoS must resort to alternative communications means to execute its diplomatic mission*** • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at moderate risk of compromise.***	• Initiate Management Team briefings • Three-times-a-day notification to pre-determined recipient list • Additional sniffers deployed as needed • Authorize limited OT for analysts

UNCLASSIFIED

ELEVATED **Moderate cyber attacks are imminent**	• Increased risk • Limited malicious activity • Intelligence indicates general threats • Specific incidents reported and under review • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at some risk of compromise.***	• Ensure protective measures implemented • Increase backups, audits, etc. • Verify response action plans & staff ready • Document changes in cyber security posture
GUARDED **Nuisance cyber attack activity is present**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Potential malicious activity within the enterprise may be handled thorough routine channels and procedures.*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.*** • ***Existing countermeasures are likely to be adequate to counter this threat***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures
LOW **Nuisance cyber attack activity is expected**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Automated response is sufficient to counter potential malicious activity within the enterprise*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures

Appendix D – Intranet Web Links of Interest

UNCLASSIFIED

Within the Office of Computer Security

- **Awareness**
  Periodic Update: http://cs.ds.state.gov/ETPA/ETPA_03.cfm
- **Computer Incident Response Team (CIRT)**
  Periodic Update: http://cs.ds.state.gov/CIRT/CIRT_08.cfm
- **Cyber Threat Analysis Division (CTAD)**
  Daily Read File: http://source.ds.state.sgov.gov (ClassNet)
  Tactical Awareness: http://cs.ds.state.gov/CTAD/CTAD_07.cfm
- **The Office of Computer Security**
  Periodic Update: http://cs.ds.state.gov/index.cfm
- **Compliance and Vulnerability Scanning**
  Periodic Update: http://cs.ds.state.gov/index.cfm

Outside of the Office of Computer Security

- **Cyber Security Incident Program**
  Periodic Update: http://csip.ds.state.gov
- **Enterprise Network Management**
  Periodic Update: http://enm.irm.state.gov
- **The Office of Information Assurance**
  Periodic Update: http://ia.irm.state.gov/
- **Patch Management**
  Periodic Update: http://enm.irm.state.gov/nlm/patch/Default.htm
- **Virus Incident Response Team (VIRT)**
  Periodic Update: http://sysintegweb.irm.state.gov/si/AntiVirus.html

The CIRT welcomes all constructive feedback to the daily Cyber Security Brief. If you have feedback for the CSB, please send it to CIRT@state.gov

020 b7E
E

Cyber Security Brief

DECLASSIFIED

United States Department of State
Bureau of Diplomatic Security
as of July 7, 2009-1400 EST

July 8, 2009

Current DoS Cyber Threat Condition GUARDED **No change from last reported condition**

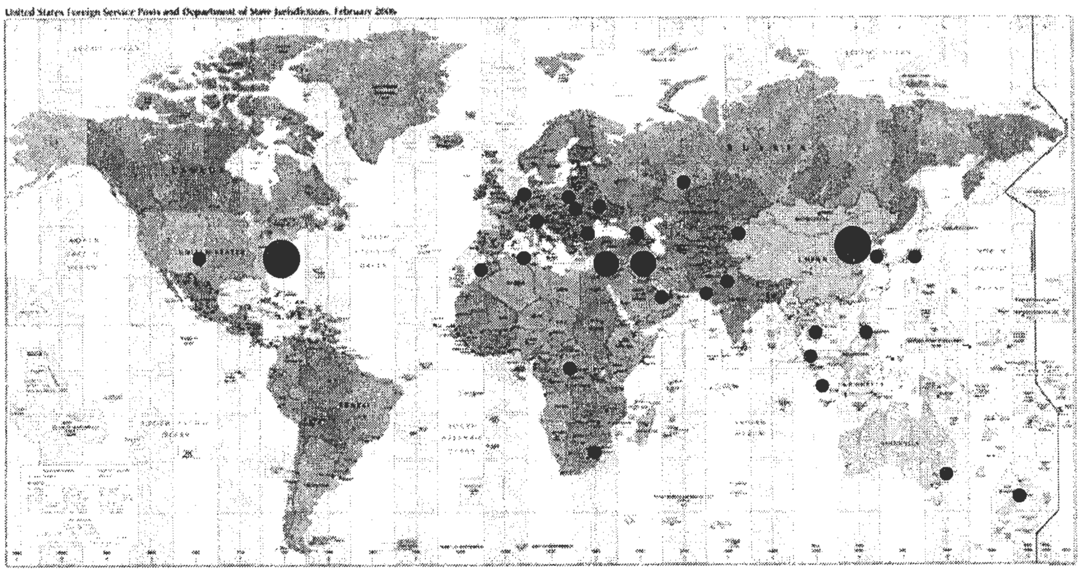
Nuisance cyber attack activity is present

Executive Summary

1. CIRT
   - US-CERT notification [redacted] CTAD provided
   - CIRT continues to await the ISSO's responses concerning the large scale phishing attack
2.
3. CTAD Daily Read File
   - *(Not available due to facility issues at SA-20 in Arlington, VA)*

b7E

Geographic Distribution of Computer Incident Response Team (CIRT) Events


United States Foreign Service Posts and Department of State Jurisdictions, February 2006

Legend: ● *1 event* ● *2 events* ● *3+ events*

DECLASSIFIED

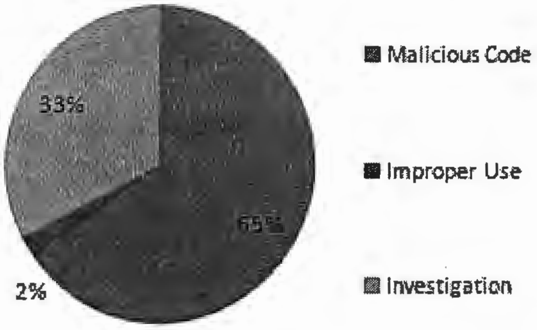
E

b7E

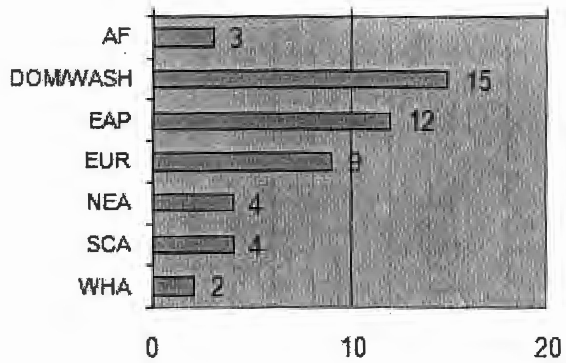
DECLASSIFIED

Open CIRT Events: 29 **Closed CIRT Events: 20**

CIRT Events by US-CERT Category



CIRT Events by Bureau

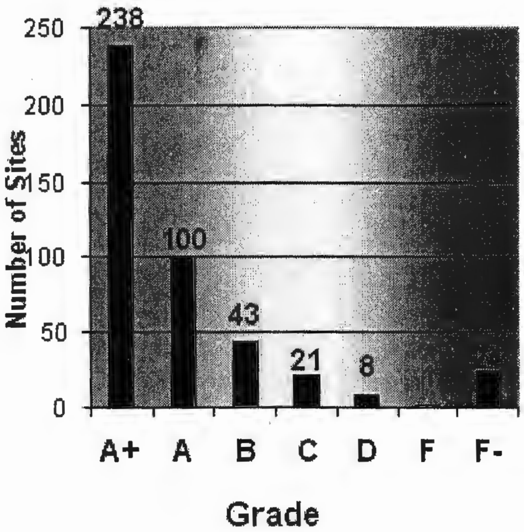


Firewall Block Request Summary

- [redacted]

b7E

Enterprise Risk Score Grade Distribution



Computer Incident Response Team (CIRT)

- US-CERT notified CERT of a Distributed Denial of Service attack targeting multiple [redacted]

b7E

DECLASSIFIED

b7E

E

Personally identifiable information (PII) loss reported

- CIRT was notified of one missing passport from the National Passport Center that was held for further information cannot be located at this time.
- CIRT was notified of one missing passport from the Miami Passport Agency that was held for further information cannot be located at this time.

Classified spillage incident(s) reported to CIRT and referred to DS/IS/APD

- CIRT was notified of a class spillage. The event was reported to APD.

US-CERT Coordination

- US-CERT notified CERT of a Distributed Denial of Service attack targeting multiple

b7E

Compliance & Vulnerability Scanning

- *Not available due to facility issues at SA-20 in Arlington*

Cyber Threat Analysis Division (CTAD)

- *Not available due to facility issues at SA-20 in Arlington, VA*

***Virus Incident Response Team (VIRT) Statistics** (as of midnight eastern time)*

Spam Blocked at Perimeter
Previous day: 1,223,158
Month to date – July: 6,678,238
Year to date for 2009: **290,213,373**

Virus Blocked at Perimeter
Previous day: 71
Month to date – July: 252
Year to date for 2009: **28,368**

Cyber Security News Headlines

DHS to host industry day for Security LOB *[source: federalnewsradio.com]*
Port Security Needs Federal Funding *[source: wciv.com]*
The upcoming Gartner Information Security Summit 2009 UK *[source: net-security.org]*

Appendix A –CIRT Event Summaries

DECLASSIFIED

b7E

Legend:	Open Events: 29	Closed Events: 20

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Email - Malicious Payload (Code, Attachment, Link)

b7E

Ticket	Location	Bureau	Open Date	Awaiting Post Response	Post is Remediating	Close Date
[redacted]	[redacted]	EAP	6/30/2009		Yes	
[redacted]	[redacted]	EAP	7/2/2009	Yes		
[redacted]	[redacted]	DOM	7/2/2009	Yes		
[redacted]	[redacted]	DOM	7/2/2009	Yes		
[redacted]	[redacted]	DOM	7/2/2009	Yes		
[redacted]	[redacted]	DOM	7/2/2009	Yes		
[redacted]	[redacted]	SCA	7/2/2009		Yes	
[redacted]	[redacted]	EAP	7/3/2009	Yes		
[redacted]	[redacted]	EAP	7/3/2009	Yes		
[redacted]	[redacted]	EAP	7/3/2009	Yes		
[redacted]	[redacted]	EUR	7/3/2009	Yes		
[redacted]	[redacted]	EAP	7/3/2009		Yes	
[redacted]	[redacted]	EAP	7/3/2009	Yes		
[redacted]	[redacted]	EUR	7/3/2009	Yes		
[redacted]	[redacted]	DOM	7/3/2009	Yes		
[redacted]	[redacted]	DOM	7/3/2009		Yes	
[redacted]	[redacted]	DOM	7/3/2009	Yes		
[redacted]	[redacted]	DOM	7/3/2009		Yes	
[redacted]	[redacted]	EAP	7/2/2009			7/6/2009
[redacted]	[redacted]	EAP	7/2/2009			7/6/2009
[redacted]	[redacted]	SCA	7/2/2009			7/7/2009
[redacted]	[redacted]	EAP	7/2/2009			7/7/2009
[redacted]	[redacted]	DOM	7/2/2009			7/6/2009
[redacted]	[redacted]	EAP	7/2/2009			7/6/2009
[redacted]	[redacted]	EUR	7/2/2009			7/7/2009
[redacted]	[redacted]	NEA	7/2/2009			7/7/2009
[redacted]	[redacted]	EAP	7/2/2009			7/6/2009

E

Ticket Number	Location	Bureau	Open Date	Awaiting Post Response	Post is Remediating	Close Date
[redacted]	[redacted]	EUR	7/2/2009			7/7/2009
[redacted]	[redacted]	EUR	7/2/2009			7/7/2009
[redacted]	[redacted]	EUR	7/2/2009			7/7/2009
[redacted]	[redacted]		7/3/2009			7/6/2009
[redacted]	[redacted]	AF	7/3/2009			7/7/2009
[redacted]	[redacted]	EUR	7/3/2009			7/7/2009
[redacted]	[redacted]	EUR	7/3/2009			7/7/2009
[redacted]	[redacted]	EAP	7/3/2009			7/7/2009
[redacted]	[redacted]	AF	7/3/2009			7/6/2009
[redacted]	[redacted]	EAP	7/3/2009			7/6/2009
[redacted]	[redacted]	EUR	7/3/2009			7/6/2009
[redacted]	[redacted]	NEA	7/3/2009			7/6/2009
[redacted]	[redacted]	EAP	7/3/2009			7/7/2009
[redacted]	[redacted]	DOM	7/3/2009			7/7/2009
[redacted]	[redacted]	DOM	7/3/2009			7/7/2009

b7E

[redacted] US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Email - Phishing

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/30/2009 0800 GMT	**Affected Bureau:** EAP

BM ✓

Event Description

CIRT detected a possible phishing email [redacted]

b7E

Current Status

7 Jul: CIRT requested a status update from the ISSO via e-mail and phone.

Status History

30 Jun: CIRT requested that the ISSO determine if the users had received the e-mail and if the e-mail has been opened or deleted. CIRT also requested that the ISSO identify any additional recipients of the e-mail if it has been forwarded. CIRT requested that the ISSO [redacted]

✓

1 Jul: The ISSO informed CIRT that examination of this event is ongoing.
2 Jul: The ISSO informed CIRT that a status update is forthcoming.
3 Jul: Awaiting update from the ISSO on Tuesday due to July 4th Holiday.

DECLASSIFIED

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Malicious Code directed toward internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/07/2009 1012 GMT	**Affected Bureau:** NEA
Event Description CIRT identified a DoS workstation that downloaded a rogue Anti-Virus application.	
Current Status **7 Jul: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.**	
Status History **N/A - New Event**	

✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/07/2009 1138 GMT	**Affected Bureau:** EUR
Event Description CIRT identified a DoS workstation that downloaded a [redacted]	
Current Status **7 Jul: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.**	
Status History **N/A - New Event**	

✓

b7E

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/07/2009 1156 GMT	**Affected Bureau:** NEA
Event Description CIRT identified a DoS workstation that downloaded a rogue Anti-Virus application.	
Current Status **7 Jul: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch**	

✓

b7E

Management.
Status History **N/A - New Event**

DECLASSIFIED

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/07/2009 1210 GMT	**Affected Bureau:** AF
Event Description CIRT identified a DoS workstation that downloaded [redacted]	
Current Status **7 Jul: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.**	
Status History **N/A - New Event**	

BM ✓

b7E

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/07/2009 1329 GMT	**Affected Bureau:** WHA
Event Description CIRT identified a DoS workstation that downloaded a rogue Anti-Virus application.	
Current Status **7 Jul: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.**	
Status History **N/A - New Event**	

BM ✓

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/07/2009 1335 GMT	**Affected Bureau:** WHA
Event Description CIRT identified a DoS workstation that downloaded [redacted]	
Current Status **7 Jul: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and**	

BM ✓

b7E

b7E

E

verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

DECLASSIFIED

Status History
N/A - New Event

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/07/2009 1337 GMT	**Affected Bureau:** DOM

On ✓

Event Description
CIRT identified a DoS workstation that downloaded [redacted]

b7E

Current Status
7 Jul: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

Status History
N/A - New Event

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Suspicious/Abnormal traffic

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/05/2009 2014 GMT	**Affected Bureau:** AF

On ✓

Event Description
CIRT was notified by the US-CERT of [redacted] to a suspicious website that may be malicious in nature.

b7E

Current Status
7 Jul: CIRT requested a status update from the ISSO via e-mail.

Status History
5 Jul: CIRT sent out the initial email to the ISSO on ~~the high side.~~
6 Jul: CIRT received an update from the ISSO. [redacted]

b7E

DECLASSIFIED

b7E
E

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Unauthorized Hardware connected to DOS network

Ticket Number: 12571	**Location:** [redacted]
Date and Time Ticket Created: 07/03/2009 0325 GMT	**Affected Bureau:** SCA

✓

Event Description
CIRT was notified by an ISSO [redacted]

b7E

Current Status
7 Jul: CIRT requested a status update from the ISSO via e-mail.

Status History
3 Jul: CIRT requested a status update from the ISSO via e-mail.
6 Jul: CIRT requested a status update from the ISSO via e-mail.

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Email - Malicious Payload (Code, Attachment, Link)

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/25/2009 0914 GMT	**Affected Bureau:** EAP

✓

Event Description
CIRT was notified by an ISSO [redacted]

b7E

Final Action
7 Jul: The ISSO notified CIRT that the message had been deleted by the user and not opened.

Status History
25 Jun: CIRT requested that the ISSO determine if the users had received the e-mail and if the e-mail has been opened or deleted. CIRT also requested that the ISSO identify any additional recipients of the e-mail if it has been forwarded. CIRT requested that the ISSO [redacted]
26 Jun: CIRT requested a status update from the ISSO via e-mail.
29 Jun: CIRT requested a status update from the ISSO, the RSO, and the IPO via e-mail.
30 Jun: CIRT requested a status update from the ISSO via e-mail and phone.
1 Jul: CIRT received notification from the ISSO that they have received the ticket and have begun working the event.
2 Jul: CIRT requested a status update from the ISSO via e-mail.
3 Jul: Awaiting update from the ISSO on Tuesday due to July 4th Holiday.

b7E

E

b7E

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Malicious Code directed toward internal machine

Ticket Number: [redacted]	**Location** [redacted]
Date and Time Ticket Created: 07/01/2009 1151 GMT	**Affected Bureau:** NEA

Event Description
CIRT detected the download of a malicious executable to a DoS workstation.

Final Action
7 Jul: The ISSO informed CIRT that no malicious or unauthorized files were found. Antivirus definitions are up-to-date, and a scan was successfully completed with negative results. The computer is current with all of the latest patches from IRM Patch Management.

Status History
1 Jul: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.
2 Jul: CIRT requested a status update from the ISSO via e-mail.
3 Jul: Awaiting update from the ISSO on Tuesday due to July 4th Holiday.

US-CERT Category: CAT 4 (Improper Usage)
Event Type Confirmed: Internet Browsing

Ticket Number [redacted]	**Location** [redacted]
Date and Time Ticket Created: 07/07/2009 1102 GMT	**Affected Bureau:** SCA

Event Description
CIRT was notified of suspicious web surfing activity that may have been inappropriate adult material.

Final Action
7 Jul: The ISSO notified CIRT that the material was not explicit adult material.

Status History
N/A - New Event

DECLASSIFIED

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Information Security Issue (Violation or Infraction)

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/06/2009 1557 GMT	**Affected Bureau:** DOM
Event Description Personally Identifiable Information (PII) may have been breached or disclosed to unauthorized third parties.	
Final Action **7 Jul: This event has been referred to US-CERT and the Privacy Team.**	
Status History **N/A - New Event**	

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/06/2009 1630 GMT	**Affected Bureau:** DOM
Event Description Personally Identifiable Information (PII) may have been breached or disclosed to unauthorized third parties.	
Final Action **7 Jul: This event has been referred to US-CERT and the Privacy Team.**	
Status History **N/A - New Event**	

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/06/2009 1841 GMT	**Affected Bureau:** DOM
Event Description CIRT was notified of a Classified Spillage.	
Final Action **7 Jul: This event was referred to the APD Team.**	
Status History **N/A - New Event**	

DECLASSIFIED

Appendix B – Compliance & Vulnerability Scanning Statistics

- *Not available due to facility issues at SA-20 in Arlington, VA*

DECLASSIFIED

DECLASSIFIED

Appendix C – DoS Cyber Condition (CyberCon) Levels

CyberCon Level	Tripwires	Actions
Significant cyber attacks are currently occurring	• Degradation, denial, or destruction of systems • Highly sophisticated attacks • Major tensions within country / significant catastrophic events • ***DoS is unable to execute its diplomatic mission*** • ***Widespread or focused attacks targeting vulnerabilities within the enterprise require an immediate coordinated response.*** • ***Network infrastructure throughput is severed.*** • ***Common network services are disrupted.*** • ***Sensitive information in the enterprise is at high risk of compromise.***	• Disconnection of Internet connectivity • Task Force initialization • Documented Remediation Steps completed and verified prior to re-connection
HIGH **Significant cyber attacks are imminent or moderate attacks are occurring**	• Widespread malicious activity • Intelligence indicates targeted activity • Increase in sophisticated recon and probes • Heightened tensions within country or major event • ***DoS must resort to alternative communications means to execute its diplomatic mission*** • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at moderate risk of compromise.***	• Initiate Management Team briefings • Three-times-a-day notification to pre-determined recipient list • Additional sniffers deployed as needed • Authorize limited OT for analysts

ELEVATED **Moderate cyber attacks are imminent**	• Increased risk • Limited malicious activity • Intelligence indicates general threats • Specific incidents reported and under review • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at some risk of compromise.***	• Ensure protective measures implemented • Increase backups, audits, etc. • Verify response action plans & staff ready • Document changes in cyber security posture
GUARDED **Nuisance cyber attack activity is present**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Potential malicious activity within the enterprise may be handled thorough routine channels and procedures.*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.*** • ***Existing countermeasures are likely to be adequate to counter this threat***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures
LOW **Nuisance cyber attack activity is expected**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Automated response is sufficient to counter potential malicious activity within the enterprise*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures

DECLASSIFIED

Appendix D – Intranet Web Links of Interest

Within the Office of Computer Security

DECLASSIFIED

- **Awareness**
  Periodic Update: http://cs.ds.state.gov/ETPA/ETPA_03.cfm
- **Computer Incident Response Team (CIRT)**
  Periodic Update: http://cs.ds.state.gov/CIRT/CIRT_08.cfm
- **Cyber Threat Analysis Division (CTAD)**
  Daily Read File: http://source.ds.state.sgov.gov (ClassNet)
  Tactical Awareness: http://cs.ds.state.gov/CTAD/CTAD_07.cfm
- **The Office of Computer Security**
  Periodic Update: http://cs.ds.state.gov/index.cfm
- **Compliance and Vulnerability Scanning**
  Periodic Update: http://cs.ds.state.gov/index.cfm

Outside of the Office of Computer Security

- **Cyber Security Incident Program**
  Periodic Update: http://csip.ds.state.gov
- **Enterprise Network Management**
  Periodic Update: http://enm.irm.state.gov
- **The Office of Information Assurance**
  Periodic Update: http://ia.irm.state.gov/
- **Patch Management**
  Periodic Update: http://enm.irm.state.gov/nlm/patch/Default.htm
- **Virus Incident Response Team (VIRT)**
  Periodic Update: http://sysintegweb.irm.state.gov/si/AntiVirus.html

The CIRT welcomes all constructive feedback to the daily Cyber Security Brief. If you have feedback for the CSB, please send it to CIRT@state.gov

T 021
b7E

Cyber Security Brief

United States Department of State
Bureau of Diplomatic Security
as of July 8, 2009-1400 EST

July 9, 2009

Current DoS Cyber Threat Condition

GUARDED

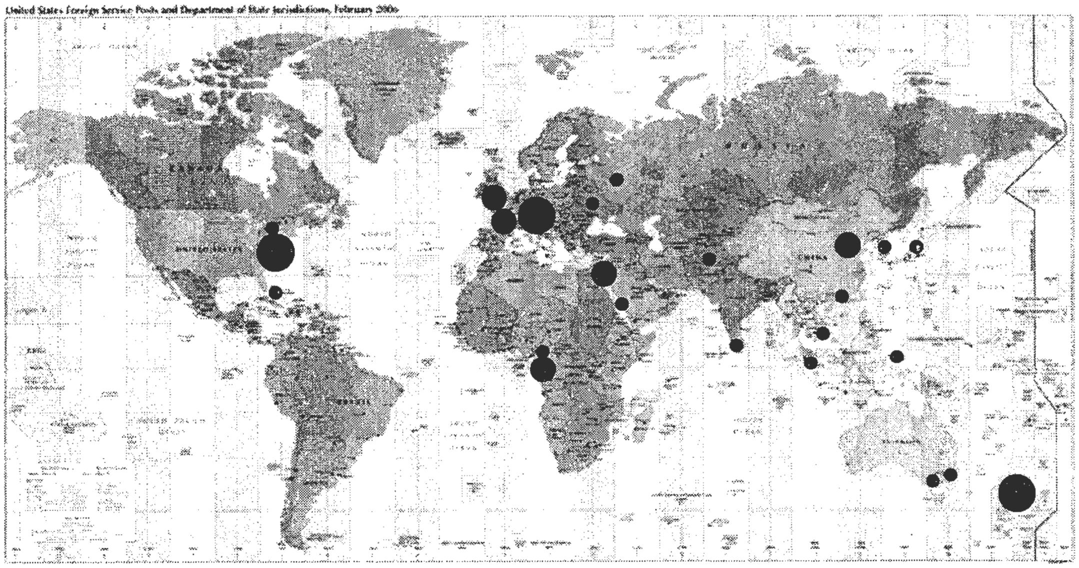
No change from last reported condition

Nuisance cyber attack activity is present

Executive Summary

1. **CIRT**
   - CIRT continues to await the ISSO's responses concerning the large scale phishing attack
2. **CTAD Daily Read File**
   - USG Personnel Targeted Through Social Networking Sites

Geographic Distribution of Computer Incident Response Team (CIRT) Events


United States Foreign Service Posts and Department of State Jurisdictions, February 2006

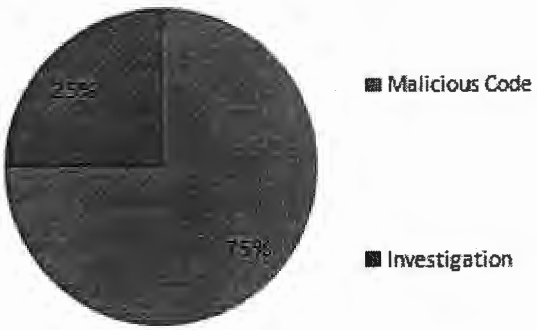
Legend: • *1 event* ● *2 events* ⬤ *3+ events*

DECLASSIFIED

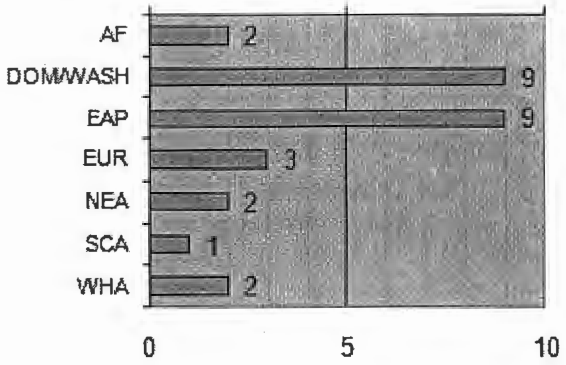
DECLASSIFIED

Open CIRT Events: 17 **Closed CIRT Events:** 11

CIRT Events by US-CERT Category



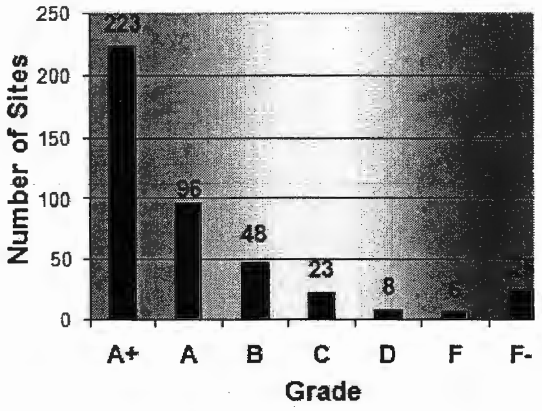
CIRT Events by Bureau



Firewall Block Request Summary

- Nothing significant to report

Enterprise Risk Score Grade Distribution



Computer Incident Response Team (CIRT)

- Nothing significant to report

Personally identifiable information (PII) loss reported

- Nothing significant to report

Classified spillage incident(s) reported to CIRT and referred to DS/IS/APD

- Nothing significant to report

US-CERT Coordination

- Nothing significant to report

DECLASSIFIED

b7E

Compliance & Vulnerability Scanning

- *Not available due to facility issues at SA-20 in Arlington, VA*

Cyber Threat Analysis Division (CTAD)

Daily Read File: USG Personnel Targeted Through Social Networking Sites

Key Highlights: (classified content - see CTAD Daily Read File on ClassNet for details)

b7E

Virus Incident Response Team (VIRT) Statistics *(as of midnight eastern time)*

Spam Blocked at Perimeter	Virus Blocked at Perimeter
Previous day: 1,223,158	Previous day: 71
Month to date – July: 6,678,238	Month to date – July: 252
Year to date for 2009: **290,213,373**	Year to date for 2009: **28,368**

Cyber Security News Headlines

Obama Administration Plans to Use NSA to Defend Civilian Agency Networks *[source: foxnews.com]*
Cybersecurity: Obama's Next Big-Ticket Agenda Item *[source: 247wallst.com]*
U.S. Wants Privacy in New Cybersecurity *[source: sci-tech-today.com]*

DECLASSIFIED

DECLASSIFIED

E

b7E

Appendix A –CIRT Event Summaries

Legend:	Open Events: 17	Closed Events: 11

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Email - Malicious Payload (Code, Attachment, Link)

b7E

Ticket Number	Location	Bureau	Open Date	Awaiting Post Response	Post is Remediating	Close Date
[redacted]	[redacted]	EAP	7/2/2009	Yes		
[redacted]	[redacted]	DOM	7/2/2009		Yes	
[redacted]	[redacted]	DOM	7/2/2009	Yes		
[redacted]	[redacted]	DOM	7/2/2009	Yes		
[redacted]	[redacted]	DOM	7/2/2009	Yes		
[redacted]	[redacted]	SCA	7/2/2009		Yes	
[redacted]	[redacted]	EAP	7/3/2009	Yes		
[redacted]	[redacted]	EAP	7/3/2009		Yes	
[redacted]	[redacted]	DOM	7/3/2009		Yes	
[redacted]	[redacted]	DOM	7/3/2009		Yes	
[redacted]	[redacted]	DOM	7/3/2009		Yes	
[redacted]	[redacted]	EAP	6/30/2009			7/8/2009
[redacted]	[redacted]	SCA	7/2/2009			7/7/2009
[redacted]	[redacted]	EAP	7/2/2009			7/7/2009
[redacted]	[redacted]	EUR	7/2/2009			7/7/2009
[redacted]	[redacted]	NEA	7/2/2009			7/7/2009
[redacted]	[redacted]	EUR	7/2/2009			7/7/2009
[redacted]	[redacted]	EUR	7/2/2009			7/7/2009
[redacted]	[redacted]	EUR	7/2/2009			7/7/2009
[redacted]	[redacted]	EAP	7/3/2009			7/7/2009
[redacted]	[redacted]	EAP	7/3/2009			7/8/2009
[redacted]	[redacted]	EAP	7/3/2009			7/7/2009
[redacted]	[redacted]	EUR	7/3/2009			7/7/2009
[redacted]	[redacted]	EUR	7/3/2009			7/7/2009
[redacted]	[redacted]	EAP	7/3/2009			7/7/2009
[redacted]	[redacted]	EUR	7/3/2009			7/8/2009
[redacted]	[redacted]	EAP	7/3/2009			7/8/2009
[redacted]	[redacted]	EUR	7/3/2009			7/8/2009

E

Ticket Number	Location	Bureau	Open Date	Awaiting Post Response	Post is Remediating	Close Date
[redacted]	[redacted]	EAP	7/3/2009			7/7/2009
[redacted]	[redacted]	DOM	7/3/2009			7/7/2009
[redacted]	[redacted]	DOM	7/3/2009			7/7/2009
[redacted]	[redacted]	DOM	7/3/2009			7/7/2009
[redacted]	[redacted]	EAP	7/7/2009			7/8/2009

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Email - Phishing

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 06/30/2009 0800 GMT	**Affected Bureau:** EAP

✓

Event Description
CIRT detected a possible phishing email [redacted] nating from various sources.

✓

Current Status
8 Jul: CIRT requested a status update from the ISSO via e-mail and phone.

b7E

Status History

30 Jun: CIRT requested that the ISSO determine if the users had received the e-mail and if the e-mail has been opened or deleted. CIRT also requested that the ISSO identify any additional recipients of the e-mail if it has been forwarded. CIRT requested that the ISSO [redacted]

1 Jul: The ISSO informed CIRT that examination of this event is ongoing.
2 Jul: The ISSO informed CIRT that a status update is forthcoming.
3 Jul: Awaiting update from ISSO on Tuesday due to July 4th Holiday.
6 Jul: CIRT requested a status update from the ISSO via e-mail and phone.
7 Jul: CIRT requested a status update from the ISSO via e-mail and phone.

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Malicious Code directed toward internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/07/2009 1138 GMT	**Affected Bureau:** EUR

✓

Event Description
CIRT identified a DoS workstation that downloaded a [redacted]

b7E

b7E

Current Status
8 Jul: CIRT requested a status update from the ISSO via e-mail.

Status History
7 Jul: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/07/2009 1210 GMT	**Affected Bureau:** AF

Event Description
CIRT identified a DoS workstation that downloaded a [redacted]

b7E

Current Status
8 Jul: CIRT requested a status update from the ISSO and the A/ISSO via e-mail.

Status History
7 Jul: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/07/2009 1335 GMT	**Affected Bureau:** WHA

Event Description
CIRT identified a DoS workstation that downloaded [redacted]

b7E

Current Status
8 Jul: CIRT requested a status update from the ISSO via e-mail.

Status History
7 Jul: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

Ticket Number [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/07/2009 1337 GMT	**Affected Bureau:** DOM

Event Description
CIRT identified a DoS workstation that downloaded [redacted]

b7E

Current Status
8 Jul: The Consular Affairs helpdesk notified CIRT that the ticket has been assigned to

b7E

a Field Technician for remediation.
Status History **7 Jul:** CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

UNCLASSIFIED

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Suspicious/Abnormal traffic

Ticket Number: [redacted]	**Location** [redacted]
Date and Time Ticket Created: 07/05/2009 2014 GMT	**Affected Bureau:** AF
Event Description CIRT was notified by US-CERT [redacted] a suspicious website that may be malicious in nature.	
Current Status **8 Jul: CIRT is attempting to corroborate the details surrounding this event with DS counterparts, but has been unable to do so, due to facility issues at SA-20.**	
Status History **5 Jul:** CIRT sent out the initial email to the ISSO on the high side. **6 - 7Jul:** CIRT is attempting to corroborate the details surrounding this event with DS counterparts, but has been unable to do so, due to facility issues at SA-20.	

b7E

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Email - Malicious Payload (Code, Attachment, Link)

Ticket Number: [redacted]	**Location** [redacted]
Date and Time Ticket Created: 07/07/2009 1012 GMT	**Affected Bureau:** NEA
Event Description CIRT identified a DoS workstation that downloaded a [redacted]	
Final Action **8 Jul: ISSO reported to CIRT that no unauthorized files were found on the workstation and a virus scan resulted in negative results.**	
Status History **7 Jul:** CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the	

b7E

[illegible]

b7E

workstation is up-to-date with all of the latest patches from IRM Patch Management.

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Malicious Code directed toward internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/01/2009 0626 GMT	**Affected Bureau:** EAP

Event Description
An ISSO notified CIRT of [redacted] an e-mail with a malicious PDF attachment. [redacted]

b7E

Final Action
8 Jul: The ISSO removed the email from the user's mailbox and checked the workstation to ensure it was clean.

Status History
1 Jul: CIRT requested that the ISSO search the workstation for specific files and reimage the operating system if the files are found.
2 Jul: CIRT requested a status update from the ISSO via e-mail.
3 Jul: Awaiting update from ISSO on Tuesday due to July 4th Holiday.
6 Jul: CIRT requested a status update from the ISSO via e-mail.
7 Jul: CIRT requested a status update from the ISSO via e-mail.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/07/2009 1156 GMT	**Affected Bureau:** NEA

Event Description
CIRT identified a DoS workstation that downloaded [redacted]

b7E

Final Action
8 Jul: The ISSO reported that the workstation has been removed from the network and is being re-imaged.

Status History
7 Jul: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/07/2009 1329 GMT	**Affected Bureau:** WHA

Event Description CIRT identified a DoS workstation that downloaded [redacted]
Final Action **8 Jul: The ISSO informed CIRT that the malicious files were found and removed. Antivirus definitions are up-to- date, and a scan was successfully completed with negative results. The computer is current with all of the latest patches from IRM Patch Management.**
Status History **7 Jul:** CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.

b7E

Appendix B – Compliance & Vulnerability Scanning Statistics

- *Not available due to facility issues at SA-20 in Arlington, VA*

UNCLASSIFIED

DECLASSIFIED

Appendix C – DoS Cyber Condition (CyberCon) Levels

CyberCon Level	Tripwires	Actions
Significant cyber attacks are currently occurring	• Degradation, denial, or destruction of systems • Highly sophisticated attacks • Major tensions within country / significant catastrophic events • ***DoS is unable to execute its diplomatic mission*** • ***Widespread or focused attacks targeting vulnerabilities within the enterprise require an immediate coordinated response.*** • ***Network infrastructure throughput is severed.*** • ***Common network services are disrupted.*** • ***Sensitive information in the enterprise is at high risk of compromise.***	• Disconnection of Internet connectivity • Task Force initialization • Documented Remediation Steps completed and verified prior to re-connection
HIGH **Significant cyber attacks are imminent or moderate attacks are occurring**	• Widespread malicious activity • Intelligence indicates targeted activity • Increase in sophisticated recon and probes • Heightened tensions within country or major event • ***DoS must resort to alternative communications means to execute its diplomatic mission*** • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at moderate risk of compromise.***	• Initiate Management Team briefings • Three-times-a-day notification to pre-determined recipient list • Additional sniffers deployed as needed • Authorize limited OT for analysts

DECLASSIFIED

UNCLASSIFIED

ELEVATED **Moderate cyber attacks are imminent**	• Increased risk • Limited malicious activity • Intelligence indicates general threats • Specific incidents reported and under review • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at some risk of compromise.***	• Ensure protective measures implemented • Increase backups, audits, etc. • Verify response action plans & staff ready • Document changes in cyber security posture
GUARDED **Nuisance cyber attack activity is present**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Potential malicious activity within the enterprise may be handled thorough routine channels and procedures.*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.*** • ***Existing countermeasures are likely to be adequate to counter this threat***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures
LOW **Nuisance cyber attack activity is expected**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Automated response is sufficient to counter potential malicious activity within the enterprise*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures

DECLASSIFIED

Appendix D – Intranet Web Links of Interest

DECLASSIFIED

Within the Office of Computer Security

- **Awareness**
  Periodic Update: http://cs.ds.state.gov/ETPA/ETPA_03.cfm
- **Computer Incident Response Team (CIRT)**
  Periodic Update: http://cs.ds.state.gov/CIRT/CIRT_08.cfm
- **Cyber Threat Analysis Division (CTAD)**
  Daily Read File: http://source.ds.state.sgov.gov (ClassNet)
  Tactical Awareness: http://cs.ds.state.gov/CTAD/CTAD_07.cfm
- **The Office of Computer Security**
  Periodic Update: http://cs.ds.state.gov/index.cfm
- **Compliance and Vulnerability Scanning**
  Periodic Update: http://cs.ds.state.gov/index.cfm

Outside of the Office of Computer Security

- **Cyber Security Incident Program**
  Periodic Update: http://csip.ds.state.gov
- **Enterprise Network Management**
  Periodic Update: http://enm.irm.state.gov
- **The Office of Information Assurance**
  Periodic Update: http://ia.irm.state.gov/
- **Patch Management**
  Periodic Update: http://enm.irm.state.gov/nlm/patch/Default.htm
- **Virus Incident Response Team (VIRT)**
  Periodic Update: http://sysintegweb.irm.state.gov/si/AntiVirus.html

The CIRT welcomes all constructive feedback to the daily Cyber Security Brief. If you have feedback for the CSB, please send it to CIRT@state.gov

ck

DECLASSIFIED

E P b7E

022

Cyber Security Brief

DECLASSIFIED

United States Department of State
Bureau of Diplomatic Security
as of July 9, 2009-1400 EST

July 10, 2009

Current DoS Cyber Threat Condition

GUARDED

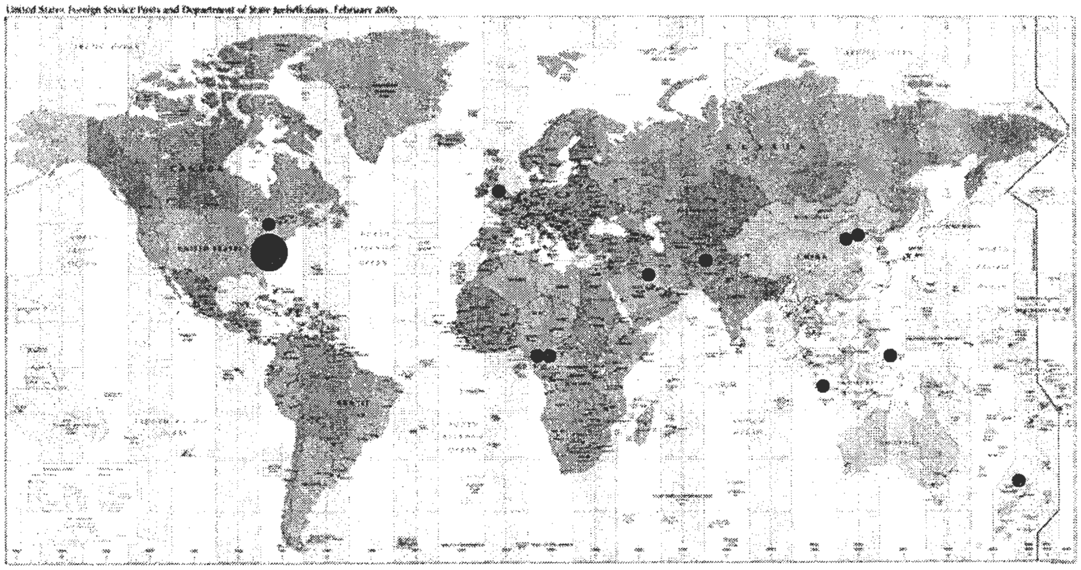
No change from last reported condition

Nuisance cyber attack activity is present

Executive Summary

1. **CIRT**
   - Nothing significant to report
2. **CTAD Daily Read File**
   - Global Efforts to Create Centralized Cyber Security Commands

Geographic Distribution of Computer Incident Response Team (CIRT) Events

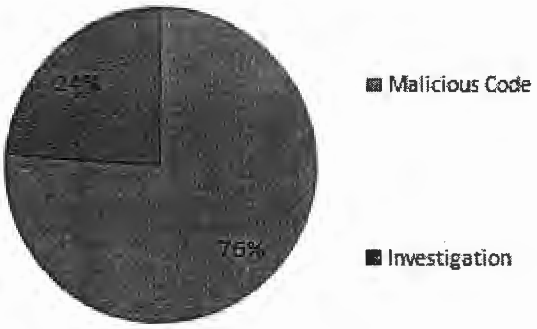

United States Foreign Service Posts and Department of State Jurisdictions, February 2009

Legend: ● *1 event* ● *2 events* ● *3+ events*

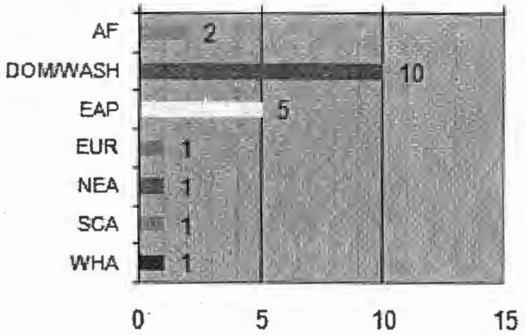
DECLASSIFIED

***Open CIRT Events*: 11** ***Closed CIRT Events*: 10**

CIRT Events by US-CERT Category



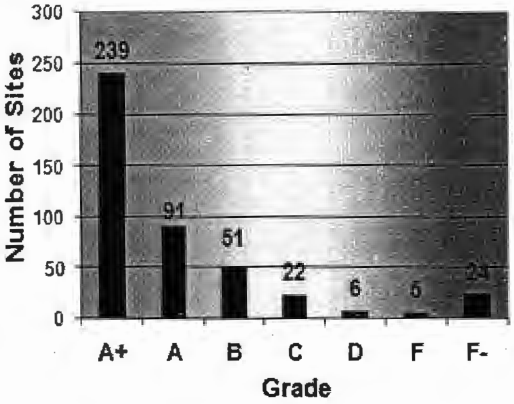
CIRT Events by Bureau



Firewall Block Request Summary

- Nothing significant to report

Enterprise Risk Score Grade Distribution



Computer Incident Response Team (CIRT)

- Nothing significant to report

Personally identifiable information (PII) loss reported

- One passport application mailed from postal acceptance facility in the Philadelphia Passport Agency region to the Lindbergh Postal Distribution Center cannot be located at this time.

Classified spillage incident(s) reported to CIRT and referred to DS/IS/APD

- Nothing significant to report

US-CERT Coordination

- Nothing significant to report.

DECLASSIFIED

Compliance & Vulnerability Scanning

- *See Appendix B for statistics*

Cyber Threat Analysis Division (CTAD)

CTAD Daily Read File:

Global Efforts to Create Centralized Cyber Security Commands

Key Highlights:

- *USCYBERCOM is being established for the coordination of defense CNO.*
- *The RoK plans to establish a cyber command by 2012.*
- *The OK's GCHQ will host a CSOC for real-time analysis for cyber activity in September.*
- *PRC officials apparently perceive USCYBERCOM as a means to initiate a cyber arms race.*

Source Paragraph: "Defense Secretary Robert Gates today [23 June 2009] approved the creation of a unified U.S. Cyber command [USCYBERCOM] to oversee the protection of military networks against cyber threats… The plans are due by Sept. 1 and need to include the new command's mission, roles and responsibilities, reporting structures and accountability measures, Gates said. The new command will most likely be headquartered in Fort Meade, MD. And will reach initial operating capabilities by October, and full capability by October 2010…"

Source: Computerworld (http://www.computerworld.com), "Defense Secretary Gates approves creation of U.S. Cyber command," Date of Source: 23 June 2009

Virus Incident Response Team (VIRT) Statistics (as of midnight eastern time)

Spam Blocked at Perimeter
Previous day: 1,223,158
Month to date – July: 6,678,238
Year to date for 2009: **290,213,373**

Virus Blocked at Perimeter
Previous day: 71
Month to date – July: 252
Year to date for 2009: **28,368**

Cyber Security News Headlines

US officials eye North Korea in cyber attack *[source: associated press]*
IU cybersecurity expert: Recent cyberattacks a 'wake-up call' *[source: iu.edu]*
Third State Department snooper sentenced *[source: computerworld.com]*

DECLASSIFIED

b7E

E

Appendix A – CIRT Event Summaries

Legend:	Open Events: 11	Closed Events: 10

US-CERT Category: CAT 3 (Malicious Code)
Event Type Suspected: Email - Malicious Payload (Code, Attachment, Link)

Ticket Number	Location	Bureau	Open Date	Awaiting Post Response	Post is Remediating	Close Date
[redacted]	[redacted]	EAP	07/02/09		Yes	
[redacted]	[redacted]	DOM	07/02/09	Yes		
[redacted]	[redacted]	DOM	07/02/09		Yes	
[redacted]	[redacted]	EAP	07/03/09	Yes		
[redacted]	[redacted]	EAP	07/03/09	Yes		
[redacted]	[redacted]	DOM	07/03/09		Yes	
[redacted]	[redacted]	DOM	07/03/09			07/09/09
[redacted]	[redacted]	DOM	07/02/09			07/09/09
[redacted]	[redacted]	SCA	07/02/09			07/09/09
[redacted]	[redacted]	EAP	06/30/09			07/08/09
[redacted]	[redacted]	DOM	07/02/09			07/08/09
[redacted]	[redacted]	DOM	07/03/09			07/08/09
[redacted]	[redacted]	EUR	07/03/09			07/08/09
[redacted]	[redacted]	EUR	07/03/09			07/08/09

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Malicious Code directed toward internal machine

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/07/2009 1335 GMT	**Affected Bureau:** WHA
Event Description CIRT identified a DoS workstation that downloaded [redacted]	
Current Status **9 Jul: CIRT received updated ISSO contact information and resent the initial**	

b7E

b7C
E

notification to the correct contact.

DECLASSIFIED

Status History
7 Jul: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.
8 Jul: CIRT requested a status update from the ISSO via e-mail.

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/07/2009 1337 GMT	**Affected Bureau:** DOM

b7C

Event Description
CIRT identified a DoS workstation that downloaded [redacted]

Current Status
9 Jul: CIRT requested an update from the Consular Affairs helpdesk, who informed CIRT that the ticket is still in progress.

Status History
7 Jul: CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management.
8 Jul: The Consular Affairs helpdesk notified CIRT that the ticket has been assigned to a Field Technician for remediation.

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Suspicious/Abnormal traffic

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/05/2009 2014 GMT	**Affected Bureau:** AF

b7E

Event Description
CIRT was notified by the US-CERT [redacted] suspicious website that may be malicious in nature.

Current Status
9 Jul: CIRT is attempting to corroborate the details surrounding this event with DS counterparts, but has been unable to do so, due to facility issues at SA-20.

Status History
5 Jul: CIRT sent out the initial email to the ISSO on the high side.
6 Jul - 8 Jul: CIRT is attempting to corroborate the details surrounding this event with DS counterparts, but has been unable to do so, due to facility issues at SA-20.

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Suspected: Unauthorized Hardware connected to DOS network

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/09/2009 0758 GMT	**Affected Bureau:** NEA
Event Description CIRT detected [redacted]	
Current Status **9 Jul: CIRT requested that the ISSO locate the system associated with the network activity and remove it from the network.** [redacted]	
Status History **N/A - New Event**	

b7E

b7E

E b7E

US-CERT Category: CAT 3 (Malicious Code)
Event Type Confirmed: Malicious Code directed toward internal machine

Ticket Number: [redacted] **Location:** [redacted] BM ✓

Date and Time Ticket Created: 06/30/2009 0800 GMT **Affected Bureau:** EAP

Event Description
CIRT detected a possible phishing email containing [redacted] originating from various sources. b7E

Final Action [redacted] b7E

Status History

30 Jun: CIRT requested that the ISSO determine if the users had received the e-mail and if the e-mail has been opened or deleted. CIRT also requested that the ISSO identify any additional recipients of the e-mail if it has been forwarded. CIRT requested that the ISSO [redacted] b7E

1 Jul: The ISSO informed CIRT that examination of this event is ongoing.
2 Jul: The ISSO informed CIRT that a status update is forthcoming.
3 Jul: Awaiting update from ISSO on Tuesday due to July 4th Holiday.
6 Jul: CIRT requested a status update from the ISSO via e-mail and phone.
7 Jul: CIRT requested a status update from the ISSO via e-mail and phone..
8 Jul: CIRT requested a status update from the ISSO via e-mail and phone.

Ticket Number: [redacted] **Location:** [redacted] BM ✓

Date and Time Ticket Created: 07/09/2009 1149 GMT **Affected Bureau:** DOM

Event Description
CIRT was notified by US-CERT of a potential phishing attack targeting the Department of State. The phishing attack consisted of an email with a malicious PDF attachment.

Final Action
9 Jul: CIRT was unable to locate any network activity that correlated with the traffic reported by US-CERT.

Status History
N/A - New Event

Ticket Number: [redacted] **Location:** [redacted] BM ✓

E b7E

Date and Time Ticket Created: [redacted]	**Affected Bureau** [redacted]
Event Description CIRT identified a DoS workstation that downloaded [redacted]	
Final Action **9 Jul: The ISSO informed CIRT that no malicious or unauthorized files were found. Antivirus definitions are up-to-date, and a scan was successfully completed with negative results. The computer is current with all of the latest patches from IRM Patch Management.**	
Status History **7 Jul:** CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management. **8 Jul:** CIRT requested a status update from the ISSO via e-mail.	

DECLASSIFIED

b7E

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/07/2009 1210 GMT	**Affected Bureau:** AF
Event Description CIRT identified a DoS workstation that downloaded [redacted]	
Final Action **9 Jul: The ISSO informed CIRT that the malicious files were found and removed. Antivirus definitions are up-to- date, and a scan was successfully completed with negative results. The computer is current with all of the latest patches from IRM Patch Management.**	
Status History **7 Jul:** CIRT requested that the ISSO search for specific files and remove the files if they are found. CIRT also requested that the ISSO perform an antivirus scan and verify that the workstation is up-to-date with all of the latest patches from IRM Patch Management. **8 Jul:** CIRT requested a status update from the ISSO and the A/ISSO via e-mail.	

b7E

US-CERT Category: CAT 6 (Investigation)
Event Type Confirmed: Information Security Issue (violation or infraction)

Ticket Number: [redacted]	**Location:** [redacted]
Date and Time Ticket Created: 07/09/2009 1238 GMT	**Affected Bureau:** DOM
Event Description Personally Identifiable Information (PII) may have been breached or disclosed to unauthorized third parties.	

UNCLASSIFIED

Final Action

9 Jul: This event was referred to US-CERT and the Privacy Team.

Status History

N/A - New Event

DECLASSIFIED

E

DECLASSIFIED

Appendix B – Compliance & Vulnerability Scanning Statistics

Vulnerability Totals:

Total Critical Vulnerabilities:	9,322
Total High Vulnerabilities:	564,989

Top 10 Critical Vulnerabilities

Vulnerability	CVSS Score	Count
[redacted]	10.00	1558
[redacted]	10.00	1131
[redacted]	10.00	929
[redacted]	10.00	792
[redacted]	10.00	640
[redacted]	10.00	506
[redacted]	10.00	464
[redacted]	10.00	393
[redacted]	10.00	294
[redacted]	10.00	287

b7E

Top 10 High Vulnerabilities

[redacted]	CVSS Score	Count
[redacted]	9.30	30940
[redacted]	7.00	30573
[redacted]	9.30	28221
[redacted]	9.30	28170
[redacted]	9.30	27976
[redacted]	9.30	19934
[redacted]	9.30	14633
[redacted]	9.30	14614
[redacted]	9.30	9560
[redacted]	9.30	9410

b7E

DECLASSIFIED

E

DECLASSIFIED

Top 10 Most Common Vulnerabilities

Vulnerability	CVSS Score	Count
[redacted]	9.30	30940
[redacted]	7.00	30573
[redacted]	9.30	28221
[redacted]	9.30	28170
[redacted]	9.30	27976
[redacted]	5.10	24804
[redacted]	9.30	19934
[redacted]	9.30	14633
[redacted]	9.30	14614
[redacted]	9.30	9560

b7E

Top 10 Compliance Failures

Configuration Setting	Count
[redacted]	63530
[redacted]	63158
[redacted]	63152
[redacted]	56443
[redacted]	45948
[redacted]	34229
[redacted]	29742
[redacted]	29621
[redacted]	29605
[redacted]	29600

b7E

DECLASSIFIED

Appendix C – DoS Cyber Condition (CyberCon) Levels

CyberCon Level	Tripwires	Actions
[redacted] **Significant cyber attacks are currently occurring**	• Degradation, denial, or destruction of systems • Highly sophisticated attacks • Major tensions within country / significant catastrophic events • ***DoS is unable to execute its diplomatic mission*** • ***Widespread or focused attacks targeting vulnerabilities within the enterprise require an immediate coordinated response.*** • ***Network infrastructure throughput is severed.*** • ***Common network services are disrupted.*** • ***Sensitive information in the enterprise is at high risk of compromise.***	• Disconnection of Internet connectivity • Task Force initialization • Documented Remediation Steps completed and verified prior to re-connection
HIGH **Significant cyber attacks are imminent or moderate attacks are occurring**	• Widespread malicious activity • Intelligence indicates targeted activity • Increase in sophisticated recon and probes • Heightened tensions within country or major event • ***DoS must resort to alternative communications means to execute its diplomatic mission*** • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at moderate risk of compromise.***	• Initiate Management Team briefings • Three-times-a-day notification to pre-determined recipient list • Additional sniffers deployed as needed • Authorize limited OT for analysts

DECLASSIFIED

ELEVATED **Moderate cyber attacks are imminent**	• Increased risk • Limited malicious activity • Intelligence indicates general threats • Specific incidents reported and under review • ***Attacks targeting vulnerabilities within the enterprise may require a coordinated response.*** • ***Network infrastructure throughput is noticeably diminished.*** • ***Common network services are partially disrupted.*** • ***Sensitive information in the enterprise is at some risk of compromise.***	• Ensure protective measures implemented • Increase backups, audits, etc. • Verify response action plans & staff ready • Document changes in cyber security posture
GUARDED **Nuisance cyber attack activity is present**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Potential malicious activity within the enterprise may be handled thorough routine channels and procedures.*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.*** • ***Existing countermeasures are likely to be adequate to counter this threat***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures
LOW **Nuisance cyber attack activity is expected**	• No significant malicious activity • Network operating within "acceptable risk" range • Incident detection and response capability normal • ***Automated response is sufficient to counter potential malicious activity within the enterprise*** • ***Network infrastructure throughput is normal.*** • ***Common network services are not impaired*** • ***Sensitive information in the enterprise is at slight risk of compromise.***	• Maintain regular security monitoring, scanning, & remediation operations • Verify status of protective measures

Appendix D – Intranet Web Links of Interest

UNCLASSIFIED

Within the Office of Computer Security

- **Awareness**
  Periodic Update: http://cs.ds.state.gov/ETPA/ETPA_03.cfm
- **Computer Incident Response Team (CIRT)**
  Periodic Update: http://cs.ds.state.gov/CIRT/CIRT_08.cfm
- **Cyber Threat Analysis Division (CTAD)**
  Daily Read File: http://source.ds.state.sgov.gov (ClassNet)
  Tactical Awareness: http://cs.ds.state.gov/CTAD/CTAD_07.cfm
- **The Office of Computer Security**
  Periodic Update: http://cs.ds.state.gov/index.cfm
- **Compliance and Vulnerability Scanning**
  Periodic Update: http://cs.ds.state.gov/index.cfm

Outside of the Office of Computer Security

- **Cyber Security Incident Program**
  Periodic Update: http://csip.ds.state.gov
- **Enterprise Network Management**
  Periodic Update: http://enm.irm.state.gov
- **The Office of Information Assurance**
  Periodic Update: http://ia.irm.state.gov/
- **Patch Management**
  Periodic Update: http://enm.irm.state.gov/nlm/patch/Default.htm
- **Virus Incident Response Team (VIRT)**
  Periodic Update: http://sysintegweb.irm.state.gov/si/AntiVirus.html

The CIRT welcomes all constructive feedback to the ~~daily Cy~~ber Security Brief. If you have feedback for the CSB, please send it to CIRT@state.gov