10-6

BJC
2 People
Access

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

Chronology of Events

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C)]
Sent: Wednesday, January 05, 2011 11:23 AM
To: (b)(6),(b)(7)(C)
Subject: Unauthorized Activity on the MIT network

(b)(5)

On 01/04/11 Detective (b)(6),(b)(7)(C) of the Cambridge Police Department and a member of the New England Electronic Crimes Task Force received a call from the (b)(6),(b)(7)(C) of Massachusetts Institute of Technology Police that an unauthorized computer had been found in a wire closet on MIT grounds and Network Traffic suggested that the computer was being used to download technical journals. The computer was found in a wire closet of in the basement of Building 16, the Dorrance Building (77 Massachusetts Avenue) which has MIT Biological (b)(6),(b)(7)(C) Engineering Department

for MIT stated that on 01/03/11 the library had notified him that someone was downloading large numbers of journals from the library without authorization. Large amounts of unauthorized downloading was first noticed by the library on 09/29/10 and on 11/23/10 there was another incident of excessive downloading. From 01/09/11 to 01/04/11, (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) was able to trace the activity to a particular switch in the wire closet (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) when to examine the wire closet he found the unauthorized computer connected to the switch. An external hard drive was connected to the netbook. The netbook was an Acer Aspire One with a serial number LUSAX0D001001100E1601. The netbook matches the description of an Acer netbook (b)(6),(b)(7)(C) reported as stolen to MIT Police on 12/31/10. The netbook appeared to be using two IP addres (b)(6),(b)(7)(C) which are IP address belonging to MIT. Use of NMap showed that the netbook had port 22 and 8092 open. Port 22 is the default port for SSH (Secure Shell network protocol) and port 8092 that is often associated with TCP (Transmission Control Protocol) traffic. Cambridge Police processed the scene for prints. Stickers on the outside of the netbook showed that it was originally loaded with Windows 7 starter edition but an examination of the screen indicated that the current operating system was Ubuntu, a type of Linux. The login screen showed a computer name of "ghost-laptop" with the user "Gene Host" logged in. The login screen had a password. All efforts to bypass the login screen were futile (b)(6),(b)(7)(C) started a wireshark packet capture of traffic on the switch around 9AM on 01/04/11 and the packet capture is continuing (b)(6),(b)(7)(C) provided SA (b)(6),(b)(7)(C) with a copy of flow traffic on the network. The flow traffic is currently being uploaded to the CERT dropbox. MIT decided to leave the netbook running in place with the hopes of capturing more network traffic to show if a suspect was controlling the netbook through a SSH channel and if the network traffic can show where the suspect is controlling the netbook from. MIT placed a camera in the wire closet to observe if the suspect returns for the netbook. MIT also established an alarm to notify MIT if the netbook is removed from the network. The technical journals being downloaded have a monetary value. All MIT students have access to view the journals but are limited as to how much they can download and anyone outside of MIT including students after they graduate have to pay a substantial subscription to access the files. The price for downloading one file can vary from $200.00 to $3,000.00. Total value of the downloaded files could be in excess of $50,000.00.

At 1526 on 01/04/11 this individual came back and appears to be replacing the external drive:

July 16 Scifinder
9/29 JSTOR
10/12 Meeting
11/23 excessive downloading

1/3/11 (b)(6),(b)(7)(C) report to make
(b)(6),(b)(7)(C) track to physical Room
(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) tracks activity to switch
(b)(6),(b)(7)(C) comes to look and sees drive

Started logging at ≈0900 1/4/11

Saw ping from china

Different MAC Addresses have been used

Has 2 IP on Same MAC
possible virtual interface
1/3/11 - 1/4/11

port: 22 8092
PCP
NMAP,

(b)(6),(b)(7)(C) } Internal IP } Publicly Access

httpd

1/6/10

Suspect Aaron Swartz taken into custody

Aaron H Swartz
DOB 8 NOV 1986
Passport 029801374

Passport is By Paperwork

(b)(6),(b)(7)(C)

659

work a Affidavit

Run SSN

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) on BOP for Search

(b)(6),(b)(7)(C) 1374 on Cambridge PD Booking

Call (b)(6),(b)(7)(C)

Call

Lvl or Hwy

(b)(6),(b)(7)(C)

1/19/11 Conf Call

Hey mann

Hey mann talked to (b)(6),(b)(7)(C)

yesterday 1/18/11

about direct contact w/ MIT

Re out (b)(6),(b)(7)(C)

on traffic out

SSH Comand link established

(b)(6),(b)(7)(C) = BOP SSN = Account

IC Social

(b)(6),(b)(7)(C)

D15Doc10 (FW MIT Update It's worse than we know).txt

From: Heymann, Stephen (USAMA) [(b)(6),(b)(7)(C)@usdoj.gov]
Sent: Wednesday, February 02, 2011 8:32 AM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b)(7)(C)@cambridgepolice.org
Subject: FW: MIT Update: It's worse than we know

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C)@ithaka.org]
Sent: Friday, January 28, 2011 3:05 PM
To: Heymann, Stephen (USAMA)
Subject: FW: MIT Update: It's worse than we know

… and this too.

From: (b)(6),(b)(7)(C)
Sent: Friday, January 28, 2011 3:02 PM
To: (b)(6),(b)(7)(C)
Cc:
Subject: RE: MIT Update: It's worse than we know

I do know from (b)(6),(b)(7)(C) initial analysis that the downloading was done systematically using sequential increases in our stable URLs. That is, get stable URL 12345, get stable URL 12346, 12347, 12348 and so on.

This tells us a few things. One, that the previous activity was similar to the pattern (b)(6) is seeing. That is, not targeted towards types. Two, it lends credence to an entire corpus grab approach. Don't care what it is I am getting, just get me the next one.

(b)(6)

From: (b)(6),(b)(7)(C)
Sent: Friday, January 28, 2011 2:50 PM
To:
Cc: (b)(6),(b)(7)(C)
Subject: Re: MIT Update: It's worse than we know

This doesn't appear to be targeted towards research articles or any particular titles, collections, or disciplines.
For the 2.8 million in Nov and Dec, the breakdown by article type is:
Research articles - 1,335,569
Reviews - 938,063
Misc - 459,457
News - 62,127
Editorial - 9,472

Those numbers more or less correlate to the corpus as a whole. I'd say the he was going after everything.

From: (b)(6),(b)(7)(C)@ithaka.org>
Date: Fri, 28 Jan 2011 14:28:43 -0500
To: (b)(6),(b)(7)(C)@ithaka.org>, (b)(6),(b)(7)(C)@ithaka.org>
Cc: (b)(6),(b)(7)(C)@ithaka.org>
Subject: Re: MIT Update: It's worse than we know

Attached are 2 screen shots depicting PDF download activity from MIT for November and December. One shows all downloads and totals 2,854,824 for the 2 months. The other filters out downloads from the 3 IP's that look to be associated with the download abuse (b)(6),(b)(7)(C)

and totals 17,865
for the 2 Month period. Recognizing that some legitimate downloads may have occurred from the 3 filtered
IP's, it would still be safe to say that about 2.8 million illegal downloads occurred during November and
December. We know that some illegal downloading occurred prior to November and into January. I don't
have those numbers yet. But looking at the graph you can see that some pretty aggressive downloading was
taking place the last week of Dec (over 100k.day). It seems likely this extended into January for some period of
time. It wouldn't be much of a stretch to say that as much of a million or more additional downloads may have
occurred that are not reflected on this chart. I expect to have January data available for review by Monday.
I'll also start loading Oct and Sept numbers as well to complete the picture.

(b)(6),
(b)(7)(C

From: (b)(6),(b)(7)(C) ithaka.org>
Date: Fri, 28 Jan 2011 14:13:57 -0500
To: (b)(6),(b)(7)(C) ithaka.org>(b)(6),(b)(7)(C) Ithaka.org>
Cc: (b)(6),(b)(7)(C) ithaka.org>,
Subject: RE: MIT Update: It's worse than we know

So, with September and October, what does the number look like? Still looking like the entire corpus?

From: (b)(6),(b)(7)(C)
Sent: Friday, January 28, 2011 2:10 PM
To:
Cc: (b)(6),(b)(7)(C)
Subject: RE: MIT Update: It's worse than we know

(b)(6),(b)(7)(C)

(b)
Still digging and (6),(b is going to pass along a screen shot of what he is seeing for November and
December. It appears as though the activity was less impactful in November, but just these two
months ballpark ~2 million + PDFs over their normal usage. (b)(6),(is also seeking out data prior and since
for review.

(b)
(6),(b

From: (b)(6),(b)(7)(C)
Sent: Friday, January 28, 2011 1:53 PM
To: (b)(6),(b)(7)(C)
Cc:
Subject: RE: MIT Update: It's worse than we know

I will call in a moment.

From: (b)(6),(b)(7)(C)
Sent: Friday, January 28, 2011 1:43 PM
To: (b)(6),(b)(7)(C)
Cc:
Subject: MIT Update: It's worse than we know
Importance: High

Hi (b)(6),(b)(7)
(C)

DISDoc11 (Fw Updated Timeline of JSTOR-related events from September through today).txt

From: (b)(6),(b)(7)(C) cambridgepolice.org]
Sent: Friday, January 07, 2011 2:31 PM
To: (b)(6),(b)(7)(C) usdoj.gov'; (b)(6),(b)(7)(C) usdoj.gov'; (b)(6),(b)(7)(C)
(BOS); (b)(6),(b)(7)(C) (BOS)
Subject: Fw: Updated: Timeline of JSTOR-related events from September through today

From: (b)(6),(b)(7)(C) MIT.EDU>
To: (b)(6),(b)(7)(C)
Sent: Fri Jan 07 13:47:09 2011
Subject: Fw: Updated: Timeline of JSTOR-related events from September through today
(b)(6),(b)(7)(C) - Not sure this public knowledge, but I wanted you to have this info.

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) plant.mit.edu]
Sent: Friday, January 07, 2011 8:46 AM
To: (b)(6),(b)(7)(C)
Subject: Fw: Updated: Timeline of JSTOR-related events from September through today

(b)(6),(b)(7)(C)

FYI.

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) MIT.EDU]
Sent: Friday, January 07, 2011 7:24 AM
To: (b)(6),(b)(7)(C)
Subject: Fwd: Updated: Timeline of JSTOR-related events from September through today

Sent from my iPhone

Begin forwarded message:
From: (b)(6),(b)(7)(C) mit.edu>
Date: January 7, 2011 3:46:04 AM EST
To: (b)(6),(b)(7)(C) mit.edu> (b)(6),(b)(7)(C) mit.edu>
Subject: Updated: Timeline of JSTOR-related events from September through today
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Timeline of JSTOR-related events

People involved:

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)
JSTOR Operations Staff
Cambridge Police Detective
United States Secret Service Special Agent
MIT (b)(6),(b)(7)(C) and
MIT (b)(6),(b)(7)(C)
MIT
MIT Campus Police (b)(6),(b)(7)(C)
MIT Detective
MIT (b)(6),(b)(7)(C)
MIT

two open ports are discovered on netbook, both allowing for remote access. Strategy is determined for continual monitoring of traffic to/from the netbook. Camera is set up; (b)(6),(b) and (b)(6),(b) restore scene to original condition as it had been discovered.

~2:30pm — Paths diverge; (b)(6),(b) and SA (b)(6),(b)(7)(C) return to N42.

~3:00pm — (b)(6),(b)(7) and (b)(6),(b)(7)(speak with (b)(6),(b)(7)(C) to verify specific data to be turned over to Secret Service is within scope of investigation and poses no legal risks. (b)(6),(b)(7)(C) provides SA (b)(6),(b)(7)(C) with historical network flow data concerning (b)(6),(b)(7)(C) & (b)(6),(dating from 12/14 until present and relevant DHCP log information from prior occurrences of ghost-macbook and ghost-laptop JSTOR downloading incidents (from Sept. and Oct.).

~3:00pm — Scene is restored to the way it was found and all involved clear out from building 16.

3:26pm — Suspect is seen on camera entering network closet, noticeably unaware of what had occurred all morning. He's observed swapping out the external hard disk drive with a different one. He left before police could arrive. On his way out, the suspect shuts off the lights. As this will hurt video quality and possibly work against the motion activation of the camera, (b)(6),(b)(7)(C) returns to closet and turns lights back on.

~4:00pm — SA (b)(6),(b)(7)(C) leaves campus; (b)(6),(b)(7)(calls (b)(6),(b) to inquire if he needs anything further. (b)(6),(b) is waiting to hear of location to transmit captured network traffic to for further analysis.

Thu 01/06/11 | 12:32pm — Suspect enters network closet while covering his face with bike helmet, presumably thinking video cameras may be in hallway. Once inside and with the door closed, he hurriedly removes his netbook, hard drive, and network cable and stows them in his backpack. While leaving, he covers his face again with the helmet and is out within 2 minutes with not enough time for police to respond to the area quickly enough to apprehend.

2:15pm — (b)(6),(b)(7)(C) at home, calls (b)(6),(b) seeing 2nd IP address that had been used by laptop, (b)(6),(b)(7)(C) in use on the 4th floor of building 16. (b)(6) verifies location of IP address. The MAC address was different, however the

D15Doc11 (Pw Updated Timeline of JSTOR-related events from September through today).txt

office, room 557.

3:42pm (b)(6),(b)(7)(C) calls Det. (b)(6),(b)(7)(C) to request police presence prior to the group entering the SIPB offices to check the room for the netbook.

4:00pm Det. (b)(6),(b)(7)(C) and SA (b)(6),(b)(7)(C) arrive outside W20 room 557. The students present are asked by Det. (b)(6),(b)(7)(C) if they saw anyone drop off a silver laptop computer; they all respond they'd only been there ~15-20 minutes and had seen no computer. The room is searched by all -- (b)(6),(b)(7)(locates the laptop, neatly placed under a table in a corner abutting a filing cabinet. The netbook is plugged in to a network jack about 6 feet away and is sitting on an external hard drive, attached, the same way it had been when in building 16.

(b)(6),(b)(7)(C) dons gloves and proceeds to examine the netbook. It appeared to be in a halfway shutdown state and all attempts to access a terminal on the machine were unsuccessful. It was determined that there was no feasible way to do live forensics on the computer in an attempt to capture a snapshot of current memory. The laptop is shutdown and bagged as evidence. SA (b)(6),(b)(7)(C) placed a call to the Cambridge police to inquire about getting another fingerprint exam for the netbook.

4:45pm The group returns to W92 and meets with (b)(6), to debrief.

5:30pm (b)(6),(b)(7)(C) and (b)(6), go to (b)(6),(b)(7)(C) office to join a conference call with (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) to brief them on the technical details of the work, the staff involved and sequence of events which enabled the group to locate the netbook. The call was concluded ~6:00.

A rough approximation of MIT's staff's time spent on incident since September: 160 hours in aggregate.

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

IT Security Systems & Services, IS&T
MIT
(b)(6),(b)(7)(C)

PGP public key ID: 9E62D0E6 | http://pgp.mit.edu
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.8 (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

-----END PGP SIGNATURE-----

From: [redacted] [redacted]MIT.EDU]
Sent: Thursday, January 06, 2011 4:17 PM
To: [redacted] (BOS)
Subject: Laptop Movement

After returning from Building 16, I checked radius logs and found the

following entries:

perimeter:
Thu Jan 6 12:42:08 2011 : Auth: Login OK: [004ce5a0c756] (from client [redacted] port 50023 cli 00-4C-E5-A0-C7-56)
tangent:
Thu Jan 6 13:26:52 2011 : Auth: Login OK: [00-4C-E5-A0-C7-56] (from client [redacted].14 port 7 cli 00-4C-E5-A0-C7-56)
sector:
Thu Jan 6 13:28:55 2011 : Auth: Login OK: [00-4C-E5-A0-C7-56] (from client [redacted] port 7 cli 00-4C-E5-A0-C7-56)

Suspect connected in Building 4, then W20. I checked the switch in W20 and found it still active.
We arrived at W20 and traced the jacks to a drop in W20-557. MIT Police detectives arrived and found the laptop in question. Scene is being processed.

--

[redacted]
[redacted] Network Admin
Massachusetts Institute of Technology
[redacted]mit.edu [redacted]

[redacted]
[redacted] Network Admin
Massachusetts Institute of Technology
[redacted]mit.edu [redacted]

disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it. <LaptopDude.jpg><12-32-40.jpg><12-32-41.jpg><12-32-48.jpg><12-34-03-2.jpg><12-34-03-3.jpg><12-34-03.jpg><12--32-17.jpg>

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.8 (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

-----END PGP SIGNATURE-----

D15Doc26 (Re grace host and ghost macbook registration email).txt

From: (b)(6),(b)(7)(C) @MIT.EDU]
Sent: Wednesday, February 02, 2011 3:13 PM
To: (b)(6),(b)(7)(C) (BOS)
CC: External (b)(6),(b)(7) cambridgepolice.org
Subject: Re: grace host and ghost macbook registration email

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Host Lookup

visitor registration
name: Gary Host
email: ghost42@mailinator.com
phone:
days remaining: 4
last expiration date: 13-Oct-2010
MAC address: 00235a735ffc
status: inactive
comment:
please include
contact info (b)(6),(b)(7)(C)
record last updated by mit.edu at Wed Oct 13 06:54:22 2010 EDT

- From the DHCP logs:

dhcplogger/dhcp-20101009.gz:Oct 8 23:02:05 installer dhcpd: DHCPACK on 18.55.7.48 to 00:23:5a:73:5f:fc (ghost-laptop) via (b)(6),(b)(7)(C) dhcplogger/dhcp-20101009.gz:Oct 8 23:13:49 installer dhcpd: DHCPACK on (b)(6),(b)(7)(C) to 00:17:f2:2c:b0:74 (ghost-macbook) via eth0

On Feb 2, 2011, at 1:04 PM, (b)(6),(b)(7)(C) (BOS) wrote:

> Do remember what email was used on 10/08/10 when ghost macbook and Grace Host was registered?
> (b)(6),(b)(7)(C)
>
> U.S. Secret Service
> Boston Field Office
> (b)(6),(b)(7)(C)
>
>
>
> All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.8 (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

-----END PGP SIGNATURE-----

From: (b)(6),(b)(7)(C)
Sent: Wednesday, January 05, 2011 6:48 AM
Subject: FW: Building 16

Follow Up Flag: Follow up
Flag Status: Flagged

Suspect as of yet unidentified.

From: (b)(6),(b)(7)(C) [mailto:(b)(6), (b)(7)(C)@MIT.EDU]
Sent: Tuesday, January 04, 2011 3:51 PM
To: (b)(6),(b)(7)(C)
Subject: FW: Building 16

(b)(6),(here are the screenshots from the camera setup on the laptop at MIT. Looks like he added a drive, but it is still on the network.

(b)(6), (b)(7)(

We did not get the call until he left the room.

From: (b)(6),(b)(7)(C)
Sent: Tuesday, January 04, 2011 3:48 PM
To: (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C)
Subject: Building 16

Here are screenshots from 3:26pm

(b)(6), (b)(7)(

(b)(6),(b)(7)(C)

Information Services & Technology, MIT

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) @mit.edu

(b)(6),(b)(7)(C)

Begin forwarded message:

From: (b)(6),(b)(7)(C) (b)(6),(b)(7)(C)@mit.edu>
Date: January 4, 2011 3:46:18 PM EST
To: @mit.edu>

(b)(6),(b)(7)(C)

I am following up a couple of possible ID's this morning and will get back to you on my success (or not).

(b)(5)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

From:
Sent: Wednesday, January 05, 2011 5:02 PM
To: (b)(6),(b)(7)(C) usss.dhs.gov (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C)
Subject: Packet Capture

Hi there,
I have collected about 70G of network traffic so far with about 98% of which is the JSTOR journal downloads. I've done some initial checking of the capture and I don't see anything that identifies a command and control channel. I was just wondering what the next step is.

Thank you

(b)(6),(b)(7)(C)
Information Services and Technology (IS&T)
Massachusetts Institute of Technology
Room (b)(6),(b)(7)
Cambridge, MA 02139
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C) mit.edu

Case continued in Boston.

DETAILS OF INVESTIGATION:

On 01/04/11, Detective (b)(6),(b)(7)(C) of the Cambridge Police Department and a member of the New England Electronic Crimes Task Force, received a call from (b)(6),(b)(7)(C) @MIT.EDU) of the Massachusetts Institute of Technology Police Department, informing him that an unauthorized computer had been found in a wire closet on MIT grounds and Network Traffic suggested that the computer was being used to download expensive technical journals without authorization. The computer was found in a wire closet of the basement of Building 16, the Dorrance Building (77 Massachusetts Avenue, Cambridge, MA) which houses the MIT Biological Engineering Department.

Also on 01/04/11, SA (b)(6),(b)(7)(C), Detective (b)(6),(b)(7)(C) and Detective (b)(6),(b)(7)(C) of the Boston Police Department, traveled to MIT and met with (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) @mit.edu) of the MIT Police, (b)(6),(b)(7) and (b)(6),(b)(in the basement of building 16. Criminalist (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) from Cambridge Police processed the scene for prints. The netbook found connected to the switch in the wire closet in the basement of building 16 was an Acer Aspire One with a serial number LUSAX0D001001100E1601. Network traffic indicated that the netbook was using two IP addresses (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) which are both IP addresses belonging to MIT. Use of NMap showed that the netbook had port 22 and 8092 open. Port 22 is the default port for SSH (Secure Shell network protocol) and port 8092 is often associated with TCP (Transmission Control Protocol) traffic. A surveillance camera was placed in the wire closet to record anyone returning for the netbook.

Continuing on 01/04/11, at approximately 1526, the surveillance camera recorded a white male later identified as Aaron Swartz (DOB 11/08/86) enter the wire closet. Based on the surveillance video, Swartz appeared to replace the external hard drive with a new one and take the old hard drive with him.

Further on 01/04/11, (b)(6),(b)(7)(C) was able to provide SA (b)(6),(b)(7)(C) with the following timeline:

On 09/26/10, (b)(6),(b)(7)(C) the MIT (b)(6),(b)(7)(C) received an email from (b)(6),(b)(7)(C) the JSTOR (b)(6),(b)(7)(C) stating that at 0800 excessive downloading of journals had been detected from MIT and that all of MIT access to JSTOR would be blocked. JSTOR converts printed scholarly journals into electronic form and stores them in a central archive that can be accessed by libraries and institutions such as MIT.

On 09/27/10, the MIT Network and Information Security Team received an email from (b)(6),(b)(7)(C) the MIT (b)(6),(b)(7)(C) Scholarly Publishing and Licensing, regarding excessive downloading from two IP addresses (b)(6),(b)(7)(C) and 18.55.6.215. JSTOR restored MIT access but blocked access to the identified IP addresses. (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) @mit.edu), (b)(6),(b)(7)(C) Analyst, discovered network registration for "Gary Host" with email address ghost@mailinator.com, a MAC address of 00235a735ffb and

Information Services and Technology (IS&T)
Massachusetts Institute of Technology
Room (b)(6),(b)(7)
Cambridge, MA 02139
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C) mit.edu

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.