Still digging and (b)(6), 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)(7)(

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)

Speaking with (b)(6),(b)(7)(C) just now about making sure we have (b)(6),(b)(7)(C) time as needed for the MIT evaluation currently underway and discovering that the IP addresses associated with these specific incidents have numerous additional days of mass downloading.

It would take some time to normalize against usual MIT usage, but at first glance, it is reasonably safe to assume from what (b)(6), and I covered that the individual responsible has already acquired the entire JSTOR corpus. Glad to have a call ASAP if you think it useful and I let (b)(6), know that I thought you might be calling him shortly after receiving this message for clarification. In light of this information, it would seem that we need to try and understand the full picture outside of the identified incidents going forward. Certainly our tack here merits some re-evaluation, both concerning this case and the potential for additional measures of prevention as we move forward. Also copying In(b)(6), at this juncture.

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

Thanks,

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

JSTOR | Portico

(b)(6),(b)(7)(C) ithaka.org

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, February 07, 2011 11:18 AM
To: (b)(6),(b)(7)(C) BOS); Extern (b)(6),(b) cambridgepolice.org
Subject: FW: MIT Update: It's worse than we know

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b)(7)(C) thaka.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: (b)(6),(b)(7)(C)
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),(b)(7)(C)

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 – 1,385,569
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) thaka.org>
Date: Fri, 28 Jan 2011 14:28:43 -0500
To: (b)(6),(b)(7)(C) thaka.org; (b)(6),(b)(7)(C) thaka.org>

Cc: (b)(6),(b)(7)(C) thaka.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 show's 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)(

From: (b)(6),(b)(7)(C) thaka.org>
Date: Fri, 28 Jan 2011 14:13:57 -0500
To: (b)(6),(b)(7)(C) thaka.org>
Cc: (b)(6),(b)(7)(C) thaka.org> (b)(6),(b)(7)(C) thaka.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)

Still digging and (b)(6) 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),

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

From: (b)(6),(b)(7)(C) cambridgepolice.org>
Sent: Wednesday, February 02, 2011 8:47 AM
To: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C) BOS)
Subject: RE: MIT Update: It's worse than we know

Got it

From: Heymann, Stephen (USAMA) [mailto: (b)(6),(b)(7)(C) usdoj.gov]
Sent: Wednesday, February 02, 2011 8:32 AM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C)
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: (b)(6),(b)(7)(C)
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),(b)(7)

From: (b)(6),(b)(7)(C)
Sent: Friday, January 28, 2011 2:50 PM
To: (b)(6),(b)(7)(C)
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 – 1,385,569
Reviews – 938,063
Misc – 459,457
News – 62,127
Editorial – 9,472

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); Externa (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:
Cc: (b)(6),(b)(7)(C)
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),(b)(7)(

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 – 1,385,569
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 show's all downloads and totals 2,834,826 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 these 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)(

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>
Cc: ithaka.org> (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)

Still digging and (b) (6), 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)(7)(

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

-----BEGIN PGP SIGNATURE-----
(b)(6),(b)(7)(C)

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

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Wednesday, January 26, 2011 8:34 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Follow-up questions with (b)(6),(b)(7)(C)

Any response from him on this?

From: (b)(6),(b)(7)(C) (BOS) [mailto: (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Wednesday, January 26, 2011 4:48 PM
To: (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C)
Subject: RE: Follow-up questions with

Let me know if either 4pm on Thursday or 1pm on Friday is a good time to have a conference call.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto: (b)(6),(b)(7)(C) MIT.EDU]
Sent: Monday, January 24, 2011 10:15 PM
To: (b)(6),(b)(7)(C) (BOS); External: (b)(6),(b) cambridgepolice.org; (b)(6),(b)(7)(C) usdoj.gov
Cc:
Subject: Re: Follow-up questions with (b)(6),(b)(7)(C)

Steve (b)(6), - The only time I've got available on Wednesday is after 4:00pm, due to an all-day commitment starting at 9am; it sounds like that might not work for Steve, but if it does, it works for me. Thursday is wide open all day, with only a hard-stop for me at 5:30pm. Friday also has me tied up 9am-3pm.

(b)(6), (b)(7)(C) - for tomorrow, does 3:00pm work for you to meet down in (b)(6), (b)(7)(C)? Per (b)(6), (b)(7)(C) comment last meeting, I'm thinking we can just furnish you with one of the duplicate drives that's already got the data on it (or we can clone one of those). (b)(6), is located here: (b)(6),(b)(7)(C)

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

Hope all are well and staying warm.

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

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

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Monday, January 24, 2011 10:15 PM
To: (b)(6),(b)(7)(C) BOS); External (b)(6),(b)(7)(C) cambridgepolice.org; (b)(6),(b)(7)(C) usdoj.gov
Cc:
Subject: Re: Follow-up questions with (b)(6),(b)(7)(C)

Steve (b)(6), . The only time I've got available on Wednesday is after 4:00pm, due to an all-day commitment starting at 9am; it sounds like that might not work for Steve, but if it does, it works for me. Thursday is wide open all day, with only a hard-stop for me at 5:30pm. Friday also has me tied up 9am-3pm.

(b)(6), (b)(7)(C) - for tomorrow, does 3:00pm work for you to meet down in (b)(6),(b)(7)(C) ? Per (b)(6), (b)(7)(C) comment last meeting, I'm thinking we can just furnish you with one of the duplicate drives that's already got the data on it (or we can clone one of those). (b)(6), (b)(7)(C) is located here: (b)(6),(b)(7)(C)

Hope all are well and staying warm.

Best,

(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C) Security Analyst
IT Security Systems & Services
MIT
(b)(6),(b)(7)(C)
PGP Fingerprint (b)(6),(b)(7)(C)

On Jan 24, 2011, at 6:25 PM (b)(6),(b)(7)(C) (BOS) wrote:

When would be a good time for you to have a conference call on Wednesday?

Also, if it works for you, I would like to drop by your office sometime tomorrow to get a copy of the packet data capture and the video surveillance file. When would be a good time?

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) usdoj.gov]
Sent: Monday, January 24, 2011 5:45 PM

On 10/12/10, the MIT Network and Information Security Team received an email from (b)(6),(b)(7)(C) stating that JSTOR informed her that excessive downloading came from IP address (b)(6),(b)(7)(C)

On 10/13/10, (b)(6),(b)(7)(C) traced the second occurrence of excessive unauthorized downloading to a computer registered on the network as "Grace Host" with an email of ghost42@mailinator.com, a NAC address of 0017f22cb074 and computer name of "ghost-laptop". (b)(6),(b)(7)(C) disabled the host registrations identified as bogus. (b)(6),(b)(7)(C) of Network Security and Support Services for MIT, notified (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C), the Director of MIT Operations and Infrastructure, that information indicated that the same unknown person appears to be using MIT guest registration from a wired connection in building 16.

On 11/29/10, the MIT Network and Information Security Team was notified by the MIT branch of the Institute of Electrical and Electronic Engineers that journal spidering has occurred on their site and it was tracked to the Student Information Processing Board XVM cluster, a group of computers that are shared and that anyone in the MIT community can use to host a Virtual Machine.

On 01/03/11, (b)(6),(b)(7)(C) received an email from (b)(6),(b)(7)(C) forwarded from (b)(6),(b)(7)(C) informing him that that the excessive downloading of journals had begun again.

On 01/04/11, (b)(6),(b)(7)(C) emailed (b)(6),(b)(7)(C) of Network Operations, and (b)(6),(b)(7)(C) mit.edu) (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) for Network and Infrastructure Services for MIT, asking them to further pinpoint the location of the computer downloading the journals. At 0808, (b)(6),(b) located a computer hidden by a box connected to a switch in a wire closet in the basement of building 16. The computer was also connected to an external hard drive. (b)(6),(b)(7) established a packet capture of the same switch the computer was found attached to.

(b)(6),(b)(7)(C) also provided SA (b)(6),(b)(7)(C) with a copy of historical network flow data concerning IP addresses (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) from 12/14/10 to 01/04/11 and DHCP log information for computers registered as ghost-macbook and ghost-laptop.

SA (b)(6),(b)(7)(C) contacted SA (b)(6),(b)(7)(C) (CID) at the CERT Coordination Center at the Software Engineering Institute at Carnegie Mellon University. SA (b)(6),(b) provided SA (b)(6),(b)(7)(C) with instructions to upload the data to the CERT drop box.

On 01/06/11, at approximately 1232, video surveillance showed the individual later identified as Swartz return to the wire closet and remove the netbook and external hard drive. Later, (b)(6),(b)(7)(C) of the MIT Police Department called (b)(6),(b)(7)(C) of the MIT Police Department and stated that he had located the suspect later identified as Swartz riding his bicycle on Massachusetts Avenue near the intersection with Lee Street in Cambridge, Massachusetts. (b)(6),(b)(7)(C) and SA (b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Tuesday, January 11, 2011 11:44 AM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b)(7)(C) cambridgepolice.org
Subject: RE: Confirming Interviews on Friday

Yes (b)(6),(b) is available. I should have made that clear in my earlier e-mail, but was focused on identifying the right IS&T people.

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

Office of the General Counsel
Massachusetts Institute of Technology
77 Massachusetts Avenue, Building (b)(6),(b)
Cambridge, MA 02139
tel: (b)(6),(b)(7)(C)
fax: 617-258-0267
(b)(6),(b)(7)(C) mit.edu

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) usdoj.gov]
Sent: Tuesday, January 11, 2011 10:06 AM
To: (b)(6),(b)(7)(C)
Cc: (BOS); (b)(6),(b)(7)(C)
Subject: RE: Confirming Interviews on Friday

(b)(5),(b)(7)(C) per EOUSA

Steve

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) MIT.EDU]
Sent: Tuesday, January 11, 2011 8:27 AM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C)
Subject: RE: Confirming Interviews on Friday

Steve –

Friday does work for us, although it might be easier to start at 11:00 (our conference room is booked from 9:30 to 11:00). Hopefully that's okay.

I have been in contact with the folks in IS&T and they came up with a slightly different list of names of people you'd probably want to speak with. They suggested (b)(6),(b)(7)(C) and (b)(6),(b)(7) they've advised me that (b)(6), would likely be able to provide the same information that (b)(6),(b)(7)(C) and (b)(6),(b)(7) could provide). Also (b)(6), (b)(6),(b)(7)(C) advised me that he probably can't provide much information beyond what you could get from (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) If you still want to speak to everyone, I'm sure we can make it work, but I just want to be sure we're being as efficient as possible. Let me know your thoughts.

We can hold the meeting in the Office of General Counsel conference room, located in room (b)(6),(b)(To get here, walk through the main entrance of 77 Massachusetts Avenue. You will enter a large lobby (known as Lobby 7) and see a long corridor directly in front of you (known as the Infinite Corridor). Follow the Infinite Corridor until you enter another large open lobby, known as Lobby 10 (you will see a large set of doors on the right that look out onto a large quad facing the Back Bay, called Killian Court). When you're in Lobby 10, there will be two elevators on your left (to further confuse things, you may see a sign that says "Lobby 13" with an arrow, but you're in Lobby 10 at that point). Take either of the elevators to the third floor. When you exit the elevators, immediately turn left and you will see a sign for the Office of the General Counsel. Follow the hallway until you see another sign for the entrance to the Office of the General Counsel.

I'm in meetings the bulk of today, so I will be somewhat inaccessible, but we can coordinate any additional details tomorrow.

(b)(6),(b)(7)(C)
Office of the General Counsel
Massachusetts Institute of Technology
77 Massachusetts Avenue, Building (b)(6),(b)(7)(C)
Cambridge, MA 02139
tel: (b)(6),(b)(7)(C)
fax: 617-258-0267
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) usdoj.gov]
Sent: Monday, January 10, 2011 4:30 PM
To: (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C) BOS);
Subject: Confirming Interviews on Friday

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

If you can make it work from your end, let's do the interviews on Friday beginning at 10:00 a.m. I anticipate (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) joining me. Tentatively, we would like to speak with the following five people in the order listed (as well as anyone else you may think useful or appropriate).

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

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

Office of the General Counsel
Massachusetts Institute of Technology
77 Massachusetts Avenue, Building (b)(6),(b)(7)(C)
Cambridge, MA 02139
tel: (b)(6),(b)(7)(C)
fax: 617-258-0267
(b)(6),(b)(7) mit.edu

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) usdoj.gov]
Sent: Monday, January 10, 2011 4:30 PM
To: (b)(6),(b)(7)(C)
Cc: (BOS); (b)(6),(b)(7)(C)
Subject: Confirming Interviews on Friday

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

If you can make it work from your end, let's do the interviews on Friday beginning at 10:00 a.m. I anticipate (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) joining me. Tentatively, we would like to speak with the following five people in the order listed (as well as anyone else you may think useful or appropriate).

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

per EOUSA

(b)(5),(b)(7)(C)

Thank you, Steve

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Tuesday, January 11, 2011 8:27 AM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(7)(C) BOS); External (b)(6),(b)(7)(C) cambridgepolice.org
Subject: RE: Confirming Interviews on Friday

Steve –

Friday does work for us, although it might be easier to start at 11:00 (our conference room is booked from 9:30 to 11:00). Hopefully that's okay.

I have been in contact with the folks in IS&T and they came up with a slightly different list of names of people you'd probably want to speak with. They suggested (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) they've advised me that (b)(6),(b)(7)(C) would likely be able to provide the same information that (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) could provide). Also, (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) advised me that he probably can't provide much information beyond what you could get from (b)(6),(b)(7)(C) (b)(6),(b)(7)(C). If you still want to speak to everyone, I'm sure we can make it work, but I just want to be sure we're being as efficient as possible. Let me know your thoughts.

We can hold the meeting in the Office of General Counsel conference room, located in room (b)(6),(b)(7)(C). To get here, walk through the main entrance of 77 Massachusetts Avenue. You will enter a large lobby (known as Lobby 7) and see a long corridor directly in front of you (known as the Infinite Corridor). Follow the Infinite Corridor until you enter another large open lobby, known as Lobby 10 (you will see a large set of doors on the right that look out onto a large quad facing the Back Bay, called Killian Court). When you're in Lobby 10, there will be two elevators on your left (to further confuse things, you may see a sign that says "Lobby 13" with an arrow, but you're in Lobby 10 at that point). Take either of the elevators to the third floor. When you exit the elevators, immediately turn left and you will see a sign for the Office of the General Counsel. Follow the hallway until you see another sign for the entrance to the Office of the General Counsel.

I'm in meetings the bulk of today, so I will be somewhat inaccessible, but we can coordinate any additional details tomorrow.

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

(b)(6),(b)(7)(C)
Office of the General Counsel
Massachusetts Institute of Technology
77 Massachusetts Avenue, Building (b)(6),(b)(7)(C)
Cambridge, MA 02139
tel: (b)(6),(b)(7)(C)
fax: 617-258-0267
(b)(6),(b)(7)(C) mit.edu

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) usdoj.gov]
Sent: Monday, January 10, 2011 4:30 PM

On 09/27/10 at approximately 1028, the MIT Network and Information Security Team receives an email from (b)(6),(b)(7)(C) the MIT (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) regarding excessive downloading from two IP addresses (b)(6),(b)(7)(C) and 18.55.6.215. JSTOR restores MIT access but blocks access to the identified IP addresses. (b)(6),(b)(7)(C) mit.edu), (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) Security Analyst discovers network registration for "Gary Host" used email address ghost@mailinator.com, a MAC address of 00235a735ffb and computer name "ghost-macbook" register on the network on 09/24/10. (b)(6),(b)(7)(C) disabled the computer registration.

On 10/09/10 at approximately 1115, (b)(6),(b)(7)(C) from JSTOR Operations Staff emails (b)(6),(b)(7)(C) the MIT (b)(6),(b)(7)(C) to inform her that MIT's access to JSTOR had been cut off again due to excessive downloading.

On 10/12/10, the MIT Network and Information Security Team received an email from (b)(6),(b)(7)(C) stating that JSTOR had told her the excessive downloading came from IP address (b)(6),(b)(7)(C)

On 10/13/10, (b)(6),(b)(7)(C) traced the second occurrence of excessive unauthorized downloading to a computer registered on the network as "Grace Host" with an email of ghost42@mailinator.com, a MAC address of 0017f22cb074 and computer name of "ghost-laptop". (b)(6),(b) disabled the host registrations identified as bogus. (b)(6),(b)(7)(C) a Manager of (b)(6),(b)(7)(C) for MIT notified (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) the (b)(6),(b)(7)(C) MIT Operations and Infrastructure that information indicates that the same unknown person appears to be using MIT guest registration from a wired connection in building 16.

On 11/29/10, the MIT Network and Information Security Team is notified by the MIT branch of the Institute of Electrical and Electronic Engineers that journal spidering is occurring on their site and it is tracked to the Student Information Processing Board XVM cluster, a group of computers that are shared and that anyone in the MIT community can host a Virtual Machine on.

On 11/30/10, the Virtual Machine downloading journals from JSTOR is taken offline.

On 01/03/11 at approximately 1440, (b)(6),(b)(7)(C) received an email fro (b)(6),(b)(7)(C) forwarded from (b)(6),(b)(informing him that that the excessive downloading of journals had begun again.

On 01/04/11 at approximately 0249, (b)(6),(b)(7) emails (b)(6),(b)(7)(C) the MIT (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) mit.edu) a (b)(6),(b)(7)(C) for Network and Infrastructure Services for MIT asking them to further pinpoint the location of the computer downloading the journals. At 0808 (b)(6),(b)(locates a computer hidden by a box connected to a switch in a wire closet in the basement of building 16. The computer is also connected to an external hard drive. (b)(6),(b)(establish a packet capture of the same switch the computer is found attached to.

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 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 in the basement of Building 16, the

Dorrance Building (77 Massachusetts Avenue, Cambridge, MA) which houses 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 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. 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 LUSAX0D0010011100E1601. The netbook matches the description of an Acer netbook (b)(6),(b)(7)(C) reported as stolen to MIT Police on 12/31/10. Network traffic indicated that the netbook was using two IP address (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 that 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.

Also on 01/04/11, at approximately 1526, the surveillance camera was able to record 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.

Also on 01/04/11, (b)(6),(b)(7)(C) provided SA (b)(6),(b)(7)(C) with a copy of historical network flow data concerning IP addresses (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) from 12/14/10 to 01/04/11 and DHCP log information for computers registered as ghost-macbook and ghost-laptop. SA (b)(6),(b)(7 contacted SA (b)(6),(b)(7)(C) (CID) at the CERT Coordination Center at the Software Engineering Institute at Carnegie Mellon University. SA (b)(6),(b)(7) provided SA (b)(6),(b) with instructions to upload the data to the CERT drop box.

On 01/06/11, at approximately 1232, video surveillance viewed the individual later identified as Swartz return to the wire closet and remove the netbook and external hard drive. At approximately 1411 (b)(6),(b)(7)(C) of the MIT police Department called (b)(6),(b)(7)(C) of the MIT Police and stated that he had located the suspect later identified as Swartz riding his bicycle on Massachusetts Avenue near the intersection with Lee Street in Cambridge Massachusetts. (b)(6),(b)(7)(C) and SA (b)(6),(b)(7 responded to Lee Street to assist (b)(6),(b)(7)(C) attempted to interview the Swartz however; Swartz jumped off of his bicycle and ran down Lee Street. (b)(6),(b)(7)(C) and SA (b)(6),(b)(7)(detained the suspect. An inventory of the backpack the suspect was wearing located a US passport in the name of Aaron Swartz. Swartz was transported by Cambridge Police to Cambridge Police headquarters to be booked for Breaking and Entering.

Also on 01/06/11, (b)(6),(b)(7)(C) checked the DHCP logs for computer registrations with containing the word ghost. Ghost-laptop is seen to be still active on the MIT network using the same MAC address as used on 01/04/11 to download journals. (b)(6),(b)(6),(b)(7)(C) mit.edu) an MIT Network Engineer, traces ghost-laptop on the network to building W20 on the 5th floor. MIT Building W20 is the Stratton Student Center. (b)(6),(b)(7)(C) and (b)(6),(b)(traveled to the Stratton Student Center and determined that the Network Drop Location ghost-laptop was connected to was in the Student Information Processing Board office, room 557. (b)(6),(b)(7)(contacted (b)(6),(b)(7)(C) to inform him that they believed they had traced the netbook to a room in the student center. SA (b)(6),(b)(7 met (b)(6),(b)(7 and (b)(6),(b)(7)(C) at the student center and found the Acer Aspire netbook and external hard

Thu 9/30/10 | pm (b)(6),(b)(7)(C) emails (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) to provide the facts of the event; mentions that (b)(6), and (b)(6),(b)(7) had spoken regarding possible solution utilizing authentication that's already available from the Libraries for JSTOR access; some logistics to work out.

Sat 10/9/10 | 11:15pm (b)(6),(b)(7) emails (b)(6), informing her MIT's JSTOR access has been cut off again due to extreme downloading.

Mon 10/11/10 | 7:44pm (b)(6),(b emails (b)(6), to strategize on preventing these types of abuses and raises issue of JSTOR sending in IP abuse information in timely manner vs. blocking all of MIT's access; suggests additional measures of blocking due to lack of IP info as VPN-based abuses of resources have been exploited in the past.

Tue 10/12/10 | 6:36am Security team receives email from (b)(6),(b regarding most recent JSTOR abuse; no IP address information yet to act on.

Tue 10/12/10 | 4:02pm Security team receives email from (b)(6),(b with logs and IP address information provided by JSTOR.
JSTOR access restored. Abuse coming from address (b)(6),(b)(7)(C)

Wed 10/13/10 | 6:34am (b)(6),(b)(7)(sends email to (b)(6),(and (b)(6),(b)(7) regarding more info on further bogus registration information.
Will press JSTOR to have brief technical conversation with JSTOR's folks. Suggests if our proxy solution already in place for other resources is utilized, it's possible that JSTOR can automatically push people through it who attempt to access JSTOR directly so a large behavior change doesn't inconvenience MIT community accessing JSTOR and there would be authentication to the resource.

Host registration committing download now shows Grace Host (ghost42@mailinator.com).

We saw Gary Host registered on 9/27 using MAC address 00235a735ffb (ghost-macbook).
We saw Grace Host registered on 10/9 using MAC address 0017f22eb074 (ghost-laptop).
We saw MAC addresses change, something that a person does typically to avoid being banned or tracked on network.
We saw ghost-macbook change to 00235a735ffc after being banned.

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

PGP public key ID (b)(6),(b)(7)(C) http://pgp.mit.edu

-----BEGIN PGP SIGNATURE-----
(b)(6),(b)(7)(C)

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

(b)(3):Rule 6E

per EOUSA

Thanks

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

From: (b)(6),(b)(7)(C) (BOS) [mailto: (b)(6),(b)(7)(C) ess.dhs.gov]
Sent: Thursday, January 06, 2011 2:09 PM
To: (b)(6),(b)(7)(C)
Subject: Re: Packet Capture

How could I get a copy of the network traffic?

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

Sent from Blackberry

From: (b)(6),(b)(7)(C) MIT.EDU>
To: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) mit.edu>
C (b)(6),(b)(7)(C) mit.edu> (b)(6),(b)(7)(C) mit.edu>
Sent: Wed Jan 05 17:01:53 2011
Subject: Packet Capture

(b)(3):Rule 6E

per EOUSA

Thank you

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

PGP Fingerprint: (b)(6),(b)(7)(C)

-----BEGIN PGP SIGNATURE-----
(b)(6),(b)(7)(C)

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

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Friday, January 07, 2011 1:18 AM
To: (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C) (BOS)
Subject: 1st hard drive from suspect

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

Just wanted to check in regarding potentially recovering the hard drive that was reported seen, on the video feed, being swapped out by the suspect on Tuesday; may/may not be moot at this point if he's already been bailed out, but I'd think that's where a lot of the JSTOR property might be sitting.

I'm super impressed with all the good work that went into this coming together. Hopefully it works like this most of the time for you all.

Best,
(b)(6),(b)(

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

PGP Fingerprint: (b)(6),(b)(7)(C)

-----BEGIN PGP SIGNATURE-----
(b)(6),(b)(7)(C)
-----END PGP SIGNATURE-----

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Thursday, January 06, 2011 4:17 PM
To: (b)(6),(b)(7)(C) 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: [004ce5e0c756] (from client
(b)(6),(b)(7) 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 (b)(6),(b)(7) 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 (b)(6),(b)(7) 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.

--

(b)(6),(b)(7)(C) Network Admin
Massachusetts Institute of Technology
(b)(6),(b) mit.edu

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

--

(b)(6),(b)(7)(C) Network Admin
Massachusetts Institute of Technology
mit.edu

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

(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. <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-----

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

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

From: (b)(6),(b)(7)(C) MIT.EDU>
To: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) mit.edu>
Cc: (b)(6),(b)(7)(C) mit.edu> (b)(6),(b)(7)(C) it.edu>
Sent: Wed Jan 05 17:01:53 2011
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)
Network & Infrastructure Services
Information Services and Technology (IS&T)
Massachusetts Institute of Technology
Room (b)(6),(b)(7)(C)
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.

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Thursday, January 06, 2011 3:22 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: RE: Packet Capture

Hi there,
I've setup a web server on the machine containing the files so you can download them. They are in a standard tcpdump format. The URL is

(b)(3):Rule 6E

We've got plenty of bandwidth over here, however, if downloading this much data is a problem for you I could put them on a SATA drive and bring them down to your office. Let me know.

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

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Thursday, January 06, 2011 2:09 PM
To: (b)(6),(b)(7)(C)
Subject: RE: Packet Capture

How could I get a copy of the network traffic?

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

Sent from Blackberry

From: (b)(6),(b)(7)(C) MIT.EDU>
To: (b)(6),(b)(7)(C) (BOS);(b)(6),(b)(7)(C) mit.edu>
Cc: (b)(6),(b)(7)(C) dmit.edu>;(b)(6),(b)(7)(C) mit.edu>
Sent: Wed Jan 05 17:01:53 2011
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)
Network & Infrastructure Services
Information Services and Technology (IS&T)
Massachusetts Institute of Technology
Room (b)(6),(b)(7)(C)
Cambridge, MA 02139

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C)MIT.EDU]
Sent: Thursday, January 06, 2011 9:37 AM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b)(7)(C) cambridgepolice.org
Cc: (b)(6),(b)(7)(C)
Subject: MIT - BU 16

All,

I am going to suggest that we take the laptop and hard drive offline today. I think the amount of network traffic captured is sufficient and would like to remove the laptop to see if he comes back to retrieve it. I will be able to put some people there for a short time in an attempt to ID.

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

The open questions will be if we decide to take it offline, is this something I can do with instruction or will I need help? Also, do we want to have the new drive printed?

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

From: (b)(6),(b)(7)(C)
Sent: Wednesday, January 05, 2011 5:02 PM
To: (b)(6),(b)(7)(C) (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)
Network & Infrastructure Services
Information Services and Technology (IS&T)
Massachusetts Institute of Technology
Room (b)(6),(b)(7)(C)
Cambridge, MA 02139
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C) mit.edu

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Thursday, January 06, 2011 1:11 PM
To: (b)(6),(b)(7)(C) BOS (b)(6),(b)(7)(C) External-
(b)(6),(b)(7)(C) cambridgepolice.org
Cc: (b)(6),(b)(7)(C)
Subject: RE: When to pull laptop

(b)(6),(b)(7)(C) called me. He left a message with (b)(6), We saw the port go down at 12:32pm today. I'm going to look at the video archive. Did someone take this down intentionally ?

(b)(6),(b)(7)(C)
(b)(6),(b)(7)(- Network Operations
Massachusetts Institute of Technology
77 Massachusetts Ave, Room (b)(6),(b)(7)(C)
Cambridge, MA 02139
Phone: (b)(6),(b)(7)(C)
Email (b)(6),(MIT.edu

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) uscs.dhs.gov]
Sent: Thursday, January 06, 2011 10:59 AM
To: (b)(6),(b)(7)(C) cambridgepolice.org
Cc: (b)(6),(b)(7)(C)
Subject: When to pull laptop

What time works for you to pull the laptop and external? I am in my Boston office now. I could be there in 15. I would like to keep the surveillance camera running because I think he will come back when he notices the laptop is offline. Is there any chance we could dust for prints again before we pull the laptop since we know he came back?

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b)(7)(C) MIT.EDU]
Sent: Thursday, January 06, 2011 9:37 AM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b)(7)(C) cambridgepolice.org
Cc: (b)(6),(b)(7)(C)
Subject: MIT - Bld 16

All,

I am going to suggest that we take the laptop and hard drive offline today. I think the amount of network traffic captured is sufficient and would like to remove the laptop to see if he comes back to retrieve it. I will be able to put some people there for a short time in an attempt to ID.

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

The open questions will be if we decide to take it offline, is this something I can do with instruction or will I need help? Also, do we want to have the new drive printed?

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

From: (b)(6),(b)(7)(C)
Sent: Wednesday, January 05, 2011 5:02 PM
To: (b)(6),(b)(7)(C) [redacted].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)
- Network & Infrastructure Services
Information Services and Technology (IS&T)
Massachusetts Institute of Technology
Room (b)(6),(b)(7)(C)
Cambridge, MA 02139
(b)(6),(b)(7)(C)
(b)(6),(b) mit.edu

From: (b)(6),(b)(7)(C) >cambridgepolice.org>
Sent: Thursday, January 06, 2011 11:20 AM
To: (b)(6),(b)(7)(C) MIT.EDU'
Cc: (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) BOS)
Subject: Re: MIT - Bld 16

(b)(6),(that is certainly your call and sounds good (b)(6),(b)(will be responding either way.

From: (b)(6),(b)(7)(C) MIT.EDU>
To: (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)
Sent: Thu Jan 06 11:17:02 2011
Subject: RE: MIT - Bld 16

(b)(6),(b)(7)(We can bag, tag and deliver if that works. I am thinking that if we are leaving the camera up, we should be in and out rather quickly incase the suspect ventures by. I would imagine (b)(6), could process it in her lab.

(b)(6),

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) cambridgepolice.org]
Sent: Thursday, January 06, 2011 11:13 AM
To: (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C) usss.dhs.gov'; (b)(6),(b)(7)(C) @comcast.net'; (b)(6),(b)(7)(C) usss.dhs.gov'
Subject: Fw: MIT - Bld 16

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

The thread below has the status of the investigation to date.

As I am on a day off today I would request that CPD Crime Scene personnel hook up with SA (b)(6),(b)(7)(C) and process the newest external hard drive for prints that the suspect left the other day after we cleared the scene.

As you'll notice from the thread, the operation is being shut down and we will continue the investigation just not with the computer hooked up and downloading data.

(b)(6),(b)(7)(C) cell phone number is (b)(6),(b)(7)(C)

(b)(6), and (b)(6) can you call (b)(6),(b)(7)(C) and hook up with her and (b)(6), (b)(7)

Respectfully Submitted,

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

From: (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) (BOS) usss.dhs.gov>
To: (b)(6),(b)(7)(C) MIT.EDU> (b)(6),(b)(7)(C) mit.edu> (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C) mit.edu> (b)(6),(b)(7)(C) mit.edu> (b)(6),(b)(7)(C) mit.edu> (b)(6),(b)(7)(C) (b)(6),(b)(7)(C BOS (b)(6),(b)(7)(C) usss.dhs.gov>
Sent: Thu Jan 06 10:00:07 2011
Subject: RE: MIT - Bld 16

The open questions will be if we decide to take it offline, is this something I can do with instruction or will I need help? Also, do we want to have the new drive printed?

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

From: (b)(6),(b)(7)(C)
Sent: Wednesday, January 05, 2011 5:02 PM
To: (b)(6),(b)(7)(C) (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)
Network & Infrastructure Services
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) mit.edu

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Wednesday, January 05, 2011 5:02 PM
To: (b)(6),(b)(7)(C) [BOS] (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)
Network & Infrastructure Services
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) mit.edu