From: [redacted] </O=ITHAKA/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=[redacted]>
Sent: Monday, December 27, 2010 4:36 PM
To: [redacted]@ithaka.org>; [redacted] <[redacted]@ithaka.org>
Cc: [redacted]@ithaka.org>
Subject: RE: MIT Abuse Recurrence

Thanks [redacted],

That's right. We often see an abuse uptick toward the end of semesters and during holiday breaks, it is expected. We also saw a smallish pattern on Saturday in which 5 different institutions got blocked for 300 downloads at similar times 8:30 am, 1:30 pm, 5 pm etc. No question that it was the same person.

I blocked the offending IPs manually for about 12 hours. It did not recur. This is what we look for and expect during the "off-times".

But, alas, the MIT user(s) also found some spare time and resource as well.

[redacted]

From: [redacted]
Sent: Monday, December 27, 2010 4:30 PM
To: [redacted]
Cc: [redacted]
Subject: RE: MIT Abuse Recurrence

Interesting that the last time this happened was Columbus Day weekend. Looks like our friend likes to hit when folks tend to be out.

From: [redacted]
Sent: Monday, December 27, 2010 3:03 PM
To: [redacted]
Cc: [redacted]
Subject: Re: MIT Abuse Recurrence

Thanks [redacted]. I also emailed [redacted] this morning and just got the bounce message.

Will let you know if/when I hear from [redacted].

[redacted]

Sent from my iPad

On Dec 27, 2010, at 1:45 PM, "[redacted]" <[redacted]@ithaka.org> wrote:

> Good Afternoon,
>
> By way of a follow up, we have not heard from MIT. I tried to reach [redacted] directly, but their voicemail is on stating that the libraries are closed and all library employees are on budget mandated furlow until January 3rd.

We are trying to reach our tech contact there. No additional activity has surfaced since [redacted] put an end to it around 9 PM last night.

I have the raw data the [redacted] grabbed and am asking [redacted] to give us a summary similar to the others [redacted] has produced re: MIT.

Best,

[redacted]

From: [redacted]
Sent: Sunday, December 26, 2010 11:31 PM
To: [redacted]
Cc: [redacted]
Subject: MIT Abuse Recurrence

Good Evening,

I sent the email below a short time ago to inform MIT that the excessive activity returned this afternoon around 12:30 PM. [redacted] noticed the activity around 9:00 PM when checking on MDC for something else. The activity did not hit our download thresholds and does not appear to have affected other user's experience.

[redacted] is reporting that we sent them 152,824 PDF requests. [redacted] also speculates about the amount of content, just pure volume, makes it hard to imagine what is going on. 87 GBs of PDFs this time, that's no small feat, requires organization. The script itself isn't very smart, but the activity is organized and on purpose.

Attempts to identify the user revealed that the computer and network were up to date with patches and didn't have known side doors to hack. [redacted] does believe that [redacted] could trace the IP back to a specific building, which you will see included in my email to MIT.

I intend to call [redacted] first thing in the morning. Not sure if all of their staff are off this week or not, but I want to reach out directly and try and work with them to accomplish the most immediate concern, Identifying the user(s) responsible.

Finally, we do have the proposed login required solution ready, but we had no window to test on both ends after the 12.18 release and had planned to implement it with them in mid-January, once successful testing could be accomplished. And, for clarity, this solution continues to be a stressed as a separate workflow from identify the user(s) responsible and secure the content garnered.

Best,

[redacted]

From: [redacted]
Sent: Sunday, December 26, 2010 11:02 PM

To: [redacted]
Cc: [redacted]
Subject: MIT Abuse Recurrence

Good Evening,

We have identified activity this evening around 9:00 pm that resembles the abuse of the JSTOR archive previously reported on 9/25-9/26 and 10/9 of this year.

The activity is originating from 18.55.6.240, and we believe that it may be from the Dorrance Building on the MIT campus. We will be suspending the Class C range 18.55.6.* and monitoring closely for additional activity, suspending access as necessary.

We are requesting that every effort be made to identify the individuals responsible and to ensure that the content taken in this incident and those previously mentioned is secured and deleted. A detailed report of the activity and the content acquired will follow.

[redacted]
[redacted]
JSTOR | Portico

[redacted]@ithaka.org
[redacted]