

From: [REDACTED] </O=ITHAKA/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=[REDACTED]>
Sent: Monday, December 27, 2010 7:04 AM
To: [REDACTED]@ithaka.org>
Cc: [REDACTED]@ithaka.org>; [REDACTED] <[REDACTED]@ithaka.org>
Subject: Re: MIT Abuse Recurrence

Thanks,

I think it is fine to send along. I have the report from [REDACTED] and will send it along to you all when i get in and to MIT in advance of my call to [REDACTED].

I will also make the Abuse Team aware of the incident.

[REDACTED]
[REDACTED]
JSTOR | Portico

[REDACTED]@ithaka.org
[REDACTED]

On Dec 27, 2010, at 6:40 AM, [REDACTED] <[REDACTED]@ithaka.org> wrote:

I don't have a problem with it being sent, if I recall the message correctly. But good idea for [REDACTED] to take another look at it.

From: [REDACTED]
Sent: Monday, December 27, 2010 12:33 AM
To: [REDACTED]
Subject: Re: MIT Abuse Recurrence

Yes, this is a real concern and MIT needs to demonstrate real care here.

I will email [REDACTED] in the morning.

Does anyone have any problem with me forwarding [REDACTED] initial report. If so, please edit it to a form that you are comfortable with me forwarding.

Thanks

[REDACTED]

From: [REDACTED]
Sent: Sunday, December 26, 2010 11:41 PM

To: [REDACTED]
Cc: [REDACTED]
Subject: RE: MIT Abuse Recurrence

They have not. I spoke with [REDACTED] briefly prior to the release and emphasized our concern and tried to communicate our unwillingness to "let it go" in any sense of the phrase.

I might just be irked because I am up dealing with this person on a Sunday night, but I am starting to feel like they need to get a hold of this situation and right away or we need to offer to send them some help (read FBI).

[REDACTED]

From: [REDACTED]
Sent: Sunday, December 26, 2010 11:34 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: MIT Abuse Recurrence

Thanks for this update, [REDACTED]. It is very troubling.

Following your call a couple of weeks ago with MIT, did they offer any further insight on the previous activity?

██████████

From: ██████████
Sent: Sunday, December 26, 2010 11:31 PM
To: ██
Cc: ██████████
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. ██████████ 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.

██████████ is reporting that we sent them 152,824 PDF requests. ██████████ 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. ██████████ does believe that ██████████ could trace the IP back to a specific building, which you will see included in my email to MIT.

I intend to call ██████████ 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,

██████████

From: ██████████
Sent: Sunday, December 26, 2010 11:02 PM
To: '██████████'
Cc: ██████████
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]

JSTOR | Portico

[REDACTED]@ithaka.org

[REDACTED]