

From: [REDACTED] </O=ITHAKA/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=[REDACTED]>
Sent: Monday, October 11, 2010 12:47 PM
To: [REDACTED]@ithaka.org>
Cc: [REDACTED]@ithaka.org>; [REDACTED]@ithaka.org>; [REDACTED]@Ithaka.org>; [REDACTED] <[REDACTED]@ithaka.org>; [REDACTED] <[REDACTED]@ithaka.org>; [REDACTED] <[REDACTED]@ithaka.org>
Subject: Update: JSTOR & MIT

Afternoon Update,

Still no word from MIT, but I suspect it will come shortly. That said, and wanting to be prepared, if there are any details or contingencies for reinstatement, we should be developing those now. They will likely come back and say it's taken care of again. They may or may not offer a reason. An immediate recurrence is highly unlikely, whether they have truly taken care of it or not, so it will be hard to solicit proof.

If I were forced to guess, I think they will report back that they identified a compromised User Name and Password and a bunch of referring access from IPs around the globe (typically some combination of China, Russia, and a smattering of Eastern European, Asian and South American origins). Some schools think that blocking those referring IPs is sufficient, which it is not, but isn't a bad addition. Hackers generally use Open Proxies to fake their actual location and can find an alternate Open Proxy to use quite readily. Only changing the password or disabling the offending Username and Password is an acceptable solution.

In cases like these, we ask them to confirm that the identity responsible has been dealt with, we also ask that they confirm deletion of harvested content, but if it is from a referring IP abroad, this user could be anyone/anywhere.

Anyway, if there are special requests or requirements to gain reinstatement, we should have them at the ready.

Thanks,

[REDACTED]

-----Original Message-----

From: [REDACTED]
Sent: Monday, October 11, 2010 11:04 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: Re: Extreme robotic activity of JSTOR at MIT

Thanks [REDACTED].

There was one Facebook post at midnight, a normal user from MIT (at least via his profile he lists the MIT Network in Facebook), having trouble. I have not responded, wanting to give MIT at least the morning to touch base. Still no word from MIT.

Looping in [REDACTED] I brought then up to speed last night.

[REDACTED]
[REDACTED]

██████████@ithaka.org
██████████

On Oct 11, 2010, at 10:40 AM, ██████████@ithaka.org> wrote:

> Good to see this response. I fully understand our need to be down until this is remedied, but I'm also mindful of the potential loss of goodwill from innocent MIT users who rely on us. Has ██████████ received any inquiries on this front?

>
> -----Original Message-----

> From: ██████████
> Sent: Sunday, October 10, 2010 9:43 PM
> To: ██████████
> Subject: Fw: Extreme robotic activity of JSTOR at MIT

>
> Fyi
>
> ----- Original Message -----

> From: ██████████ [mailto:██████████@MIT.EDU]
> Sent: Sunday, October 10, 2010 08:15 PM
> To: ██████████
> Cc: ██████████ <██████████@mit.edu>; ██████████ <██████████@mit.edu>
> Subject: RE: Extreme robotic activity of JSTOR at MIT

> Thank you, ██████████ Your action was entirely appropriate, and I appreciate your courtesy in letting me know. It is infuriating that MIT's security appears unable to stop this pattern. We will redouble our efforts to solve the problem. --██████████

>
>
> _____
> From: ██████████@ithaka.org]
> Sent: Saturday, October 09, 2010 11:15 PM
> To: ██████████
> Subject: Extreme robotic activity of JSTOR at MIT

> Dear ██████████

>
> I wanted to let you know about an extreme step we have taken this evening. Our staff have blocked access to JSTOR from MIT. This is a highly unusual step and one we do not take lightly. We have had to do so because someone is systematically attempting to download large parts of the JSTOR database from within MIT's IP range. They use robots to open a session, download a PDF, open a new session, download another PDF, and keep repeating at a high rate. Not only is this a problem because it is beyond the terms of the license, but the downloading is so extensive that it impacts other users and has even brought some of our servers down. We worked through a similar incident at MIT three weeks ago and thought that the activity was being done by a visiting scholar who had left. But it has started again at an even faster rate. I am not writing you to complain about the activity; I just wanted you to be aware of the extreme step we have taken and why.

>
> Our staff have communicated with your staff and will be working to get MIT access back up just as soon as possible.

> I'll keep you posted as I hear more.

> Best regards,

> ██████████