The Tech Established 1881 ONLINE EDITION

MIT's oldest and largest newspaper & the first newspaper published on the web

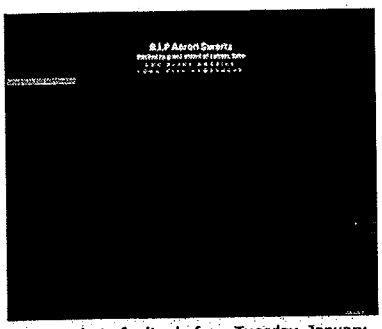
CORRECTION TO THIS ARTICLE:
The third paragraph of this article ambiguously states that "the hack and subsequent outages were due to a configuration change at EDUCAUSE." The configuration change refers to a compromise of MIT's account at EDUCAUSE, not (necessarily?) EDUCAUSE's databases. According to Garth Jordan, EDUCAUSES's vice president of operations, someone logged into MIT's account successfully on the first try, indicating that the person knew MIT's password when accessing the account. An email was sent to MIT's contact on record when the account was accessed.

MIT DNS hacked; traffic redirected

Emails sent to KAIST, other traffic redirected to Harvard

By Joanna Kao
ONLINE MEDIA EDITOR
January 23, 2013

MIT was hacked yesterday shortly before noon, with MIT URLs redirecting to a webpage claiming credit for the attack in remembrance of Aaron Swartz. MIT's email was also diverted.



A screenshot of mit.edu from Tuesday, January 22, after hackers re-directed MIT's home page in the name of Aaron Swartz.

As a result of the hack, people who tried to reach MIT over the Internet outside the MIT network were redirected to a hacked web page, and some emails may have been lost or delayed. The hack affected all names under mit.edu, such as *web.mit.edu*, *tech.mit.edu*, etc. Activity within MIT was not believed to be affected by this attack.

Article Tools
1 Comment
E-Mail
Print
Write the Editor
Post to Facebook
Share on Reddit

The hack and subsequent outages were due to a configuration change at EDUCAUSE, the registrar that provides information on all names that end in .edu. A registrar, which allows users to purchase domain names, also specifies the domain name system (DNS) servers for a domain, which convert domain names to IP addresses needed to actually load the page. It is unclear how the hackers gained control of MIT's information at EDUCAUSE.

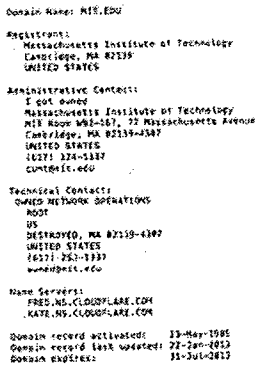
Because of the attack, the EDUCAUSE registry listed the name of the administrative contact for mit.edu as "I got owned," and the name servers were changed to CloudFlare servers, an external DNS provider.

Chronology

From 11:58 a.m. to 1:05 p.m., MIT's DNS was redirected from MIT's own servers to CloudFlare, where the hackers had configured servers to return a Harvard IP address for all mit.edu queries, except email. The Harvard machine returned a web page that showed "R.I.P. Aaron Swartz, Hacked by grand wizard of Lulzsec, Sabu, God bless America, Down with Anonymous." (see photo.) A continuously looping chiptunes version of the National Anthem also played. The hackers also signed their names ("hacked by aushok and tibitximer") over text from Aaron Swartz' blog post titled "Immoral" in the background.

Unlike previous attacks, which temporarily disabled some services, this attack had the potential to be much more severe. Email was specifically affected. Mail is normally received by one of nine different MIT servers; however today, mail that was sent between 11:58 a.m. and 1:05 p.m. was directed to a

ARTICLE IMAGES



machine at KAIST, Korea Advanced Institute of Science and Technology, meaning the attackers had complete control of emails successfully sent during that time. It is unclear what percentage of emails were successfully transmitted during this time. It is assumed that the machines at Harvard and KAIST were compromised and that Harvard and KAIST were not responsible for the attack.

Some time before 1 p.m., CloudFlare stopped directing non-email traffic to Harvard and sent it all to MIT's main web server, 18.9.22.69. All traffic to any part of MIT went to that server — for example, going to csail.mit.edu would return MIT's homepage, which is not normal behavior.

By 1:05 p.m. EDUCAUSE had corrected its listing of MIT's DNS servers, from CloudFlare back to MIT's own servers. However, any machines that accessed mit.edu during that hour could have cached the wrong mapping and would continue to refer all queries to CloudFlare for the next 48 hours.

At 4:20 p.m., with information from MIT, CloudFlare started returning the correct addresses for all mit.edu queries, except for email. By 7:15 p.m., CloudFlare removed the "mail.mit.edu" record, which referred to the machine handling MIT email at KAIST. It is unclear whether MIT email went to KAIST between 4:20 p.m. and 7:15 p.m.

This is not the first time MIT has been hacked since Swartz' death. On Sunday, Jan. 13, MIT experienced a network outage due to a DoS attack. And on Saturday, Jan. 19, MIT's email went down for 10 hours due to a "mail loop caused by a series of malformed email messages," according to the *MIT News Office*.

MIT spokeswoman Kimberly C. Allen said that Information Services & Technology became aware of an issue affecting mit.edu domain registration at 11:58 a.m. this morning. "IS&T was made aware of the problem via automated email from the domain registrar to MIT indicating that MIT's Domain Name Servers (DNS) had been changed. MIT's domain rights and the mit.edu domain were returned to MIT's control at 1:05 pm."

John A. Hawkinson contributed to this article.

A previous version of this article ran on the web at http://tech.mit.edu/V132/N62/hack.html.

View 1 comments on this article