Hack attacks, explained

August 30 2013, by Christina Pazzanese

After the Syrian Electronic Army disrupted The New York Times' website for nearly a day, Harvard's Jonathan L. Zittrain discussed how institutions will have to react in order to protect themselves. Credit: Stephanie Mitchell/Harvard Staff Photographer

Computer network hackers calling themselves the Syrian Electronic Army earlier this week disrupted *The New York Times*' website for nearly a day and electronic publishing on the Twitter social network for several hours. Also targeted were the Huffington Post and other media outlets.

These cyber attacks, which involved hijacking the companies' domain names by altering their numeric addresses, which in turn prevented visitors from seeing the websites, are just the most recent in a series of strikes on news organizations, including The Washington Post, The Associated Press, and the Financial Times, in the past few months.

To better understand the attacks, Gazette staff writer Christina Pazzanese asked Harvard's Jonathan L. Zittrain to comment by email on what happened and how institutions will have to react in order to protect themselves from future disruptions. Zittrain is a professor of law at Harvard Law School and the Harvard Kennedy School, and a professor of computer science at the School of Engineering and Applied Sciences. He is also co-founder of Harvard's Berkman Center for Internet & Society.

GAZETTE: Who is the Syrian Electronic Army?

ZITTRAIN: It appears to be a confederation of computer hackers who support the Syrian government. How much the Syrian state actively supports it is not known, which is a common problem in trying to understand groups of this sort.

GAZETTE: It doesn't sound especially difficult to initiate a Domain Name System (DNS) attack. What's involved?

ZITTRAIN: A distributed-denial-of-service attack is common, in part because it's easy to hijack many of the less-than-secure PCs connected to the Internet and use them to help overwhelm a website. There are even marketplaces in buying access to such PCs, so aggressors need not themselves be hackers. Websites like The New York Times tend to be well "bunkerized" against such attacks.

But there can be other forms of disrupting access, such as reconfiguring a site's domain name so that it points elsewhere—that's what happened here. That could be catastrophic for a bank whose customers are used to logging in at a given name, unaware that the name is now taking them to a new site, and it can also make a real statement for those who try to visit a news site that has been diverted. It's not supposed to be that easy to do. I imagine someone either hacked the password for the NYT's account with its domain name registrar, compromised the registrar's systems overall, or managed to "sweet talk" the registrar into doing a password recovery.

GAZETTE: If it is fairly simple to do, does that make it potentially more of a threat to a greater variety of institutions than a server breach?

ZITTRAIN: Both are threats. Rerouting DNS could also entail rerouting all of the company's incoming email if it's attached to the same domain. That could be terrible!

GAZETTE: Are these website disruptions happening more frequently now, and, if so, why?

ZITTRAIN: Yes, disruptions are happening more frequently, perhaps because they're seen as having more impact. As more people use the Internet, more people will be affected by a blockage.

GAZETTE: What can organizations do to protect themselves from this kind of attack?

ZITTRAIN: StopBadware.org is an example of a nonprofit that began at the Berkman Center that's now standalone. It provides webmasters with

advice on keeping their sites safe.

GAZETTE: What kinds of systemic changes need to happen to prevent vandals from disrupting global businesses?

ZITTRAIN: Over the longer term, the ideal will be to come up with security strategies that don't entail every site huddling under the umbrella of a couple massive Web-hosting providers. One set of thoughts on this topic is here.

GAZETTE: What are the free-speech implications of attacks targeting media outlets like The New York Times, The Washington Post, and the Financial Times?

ZITTRAIN: There's actually a divide in the broader hacker community about denial-of-service attacks. Some see it possible to do "properly" as a form of digital sit-in. Others think it's a bad idea, full stop: that information should flow freely, regardless of source.

This story is published courtesy of the Harvard Gazette*, Harvard University's official newspaper. For additional university news, visit* Harvard.edu.

Provided by Harvard University

Citation: Hack attacks, explained (2013, August 30) retrieved 21 June 2024 from https://phys.org/news/2013-08-hack.html