

US banks hit by more than a week of cyberattacks (Update)

September 28 2012, by Raphael Satter

U.S. banks have been buffeted by more than a week of powerful cyberattacks, but the mystery surrounding their perpetrators lingers.

One expert said Friday that he was suspicious of claims of responsibility purportedly made by Islamists angry at an anti-Muslim movie made in the United States, explaining that the widely-circulated Internet postings might have been an attempt to deflect attention from the true culprit.

"In the intelligence world, we call that a 'false flag,'" said Mike Smith, whose Web security company Akamai has helped analyze some of the attacks.

The postings, published to the Web earlier this month, suggested that an obscure Islamist group had taken revenge on American financial institutions for the "Innocence of Muslims," a low-budget U.S. film that ridiculed Muhammad, revered by Muslims as the last of God's prophets.

Since then at least half a dozen banks—including the Bank of America, JPMorgan Chase, and Citigroup—have witnessed traffic surges and disruptions. Not all have confirmed they were the victims of an online onslaught, but such surges are a hallmark of denial-of-service attacks, which work by drowning target websites with streams of junk data.

Such attacks are fairly common and generally don't compromise sensitive data or do any lasting damage. Still, they can be a huge headache for companies that rely on their websites to interact with

customers.

Most say the recent spate of attacks has been unusually powerful. PNC bank, which was hit on Thursday, has never seen such a strong surge in traffic, spokesman Fred Solomon said in a telephone interview. Smith said he estimated the flow of data at 60 to 65 gigabits per second.

Smith said the profile and power of the attack made it an unlikely fit for the religious youth that the Internet postings called upon to join in the anti-U.S. campaign. He explained that politically-motivated hackers—often called hacktivists—usually flood the Web with appeals for support and post links to software that can turn followers' personal computers into crude cyberweapons.

Twitter and online chat rooms then explode with activity, as casual supporters pile in to coordinate attacks.

"You're not seeing that with this particular set of attacks," Smith said. "At the same time ... the attack traffic is fairly homogeneous. It's not this wide cornucopia of attacks that's coming at you that you see with a hacktivist attack."

So who is behind the campaign?

Cybercriminals often use denial-of-service attacks to shake down smaller websites, but major U.S. banks make unlikely targets for a protection racket.

Could a state actor be at play? U.S. Senator Joe Lieberman, without offering any proof, said he believed the assaults were carried out by Iran in retaliation for tightened economic sanctions imposed by the United States and its allies.

Smith demurred when asked who could be behind the campaign, although he said there were "only a handful of groups out there that have the technical ability or incentive" to carry it out.

In any case, the online attacks appeared to be easing. Solomon, the PNC bank spokesman, said while traffic remained heavy Friday the flow was gradually returning to normal.

Doug Johnson, with the American Bankers Association, echoed that assessment.

"I believe it's tapering off," he said.

Copyright 2012 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

Citation: US banks hit by more than a week of cyberattacks (Update) (2012, September 28) retrieved 21 September 2024 from <https://phys.org/news/2012-09-banks-week-cyberattacks.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--