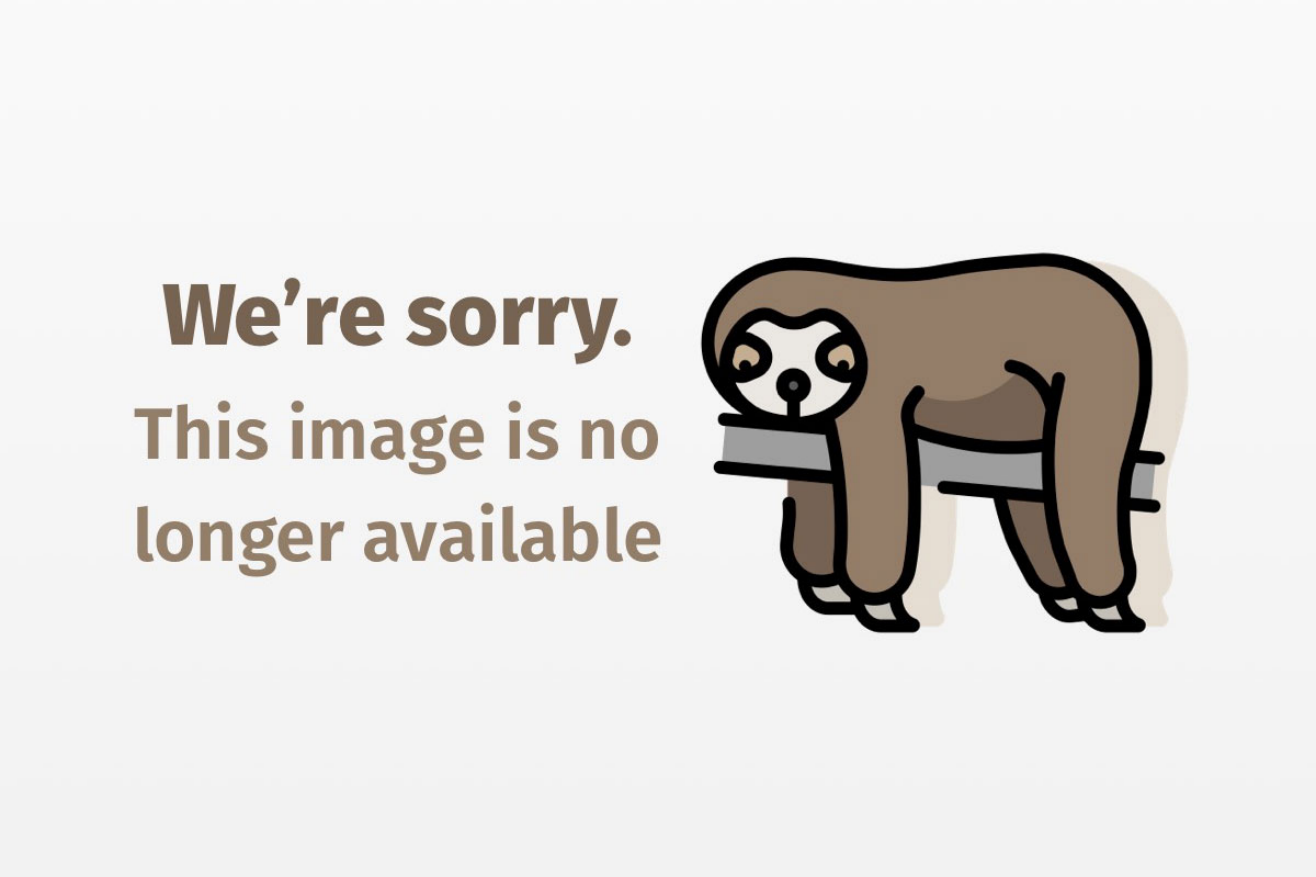
New NSA leak may expose its bank spying, Windows exploits

csoonline.com/article/3190055/new-nsa-leak-may-expose-its-bank-spying-windows-exploits.html

By Michael Kan



A hacking group has released suspected U.S. government files that show the National Security Agency may have spied on banks across the Middle East.

Numerous Windows hacking tools are also among the new batch of files the Shadow Brokers dumped Friday. In recent months, the mysterious group has been releasing hacking tools allegedly taken from the NSA, and security researchers say they actually work.

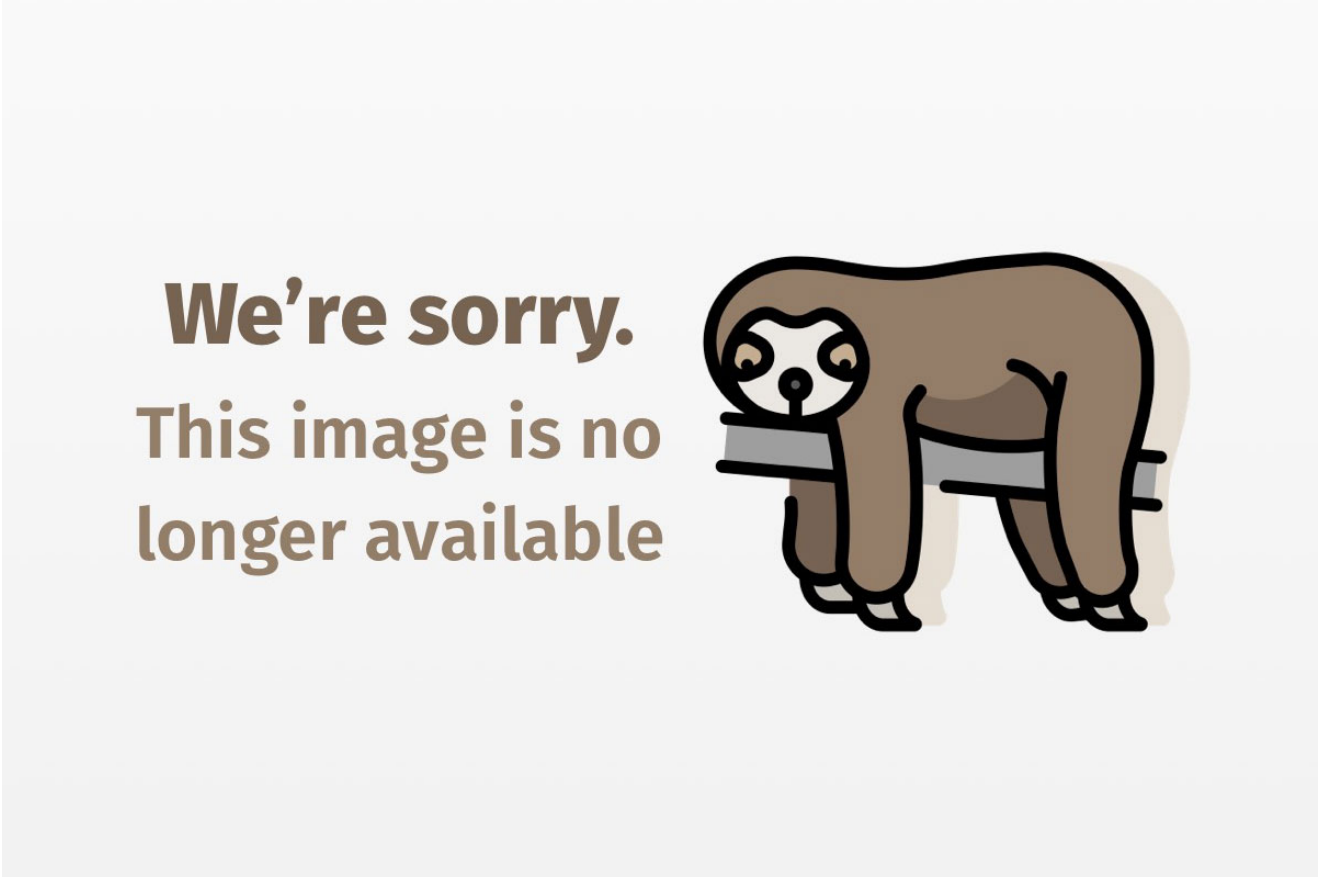
Friday's leak includes an archive describing the internal architecture at EastNets, a Dubai-based anti-money laundering company that also offers services related to SWIFT, the financial banking network.

The leaked files show the NSA was allegedly targeting EastNets in Dubai, Belgium, and Egypt.

Among the documents is a PowerPoint presentation designated as top secret. It mentions “ongoing collection” from servers owned by financial institutions in the United Arab Emirates, Yemen, Kuwait, Palestine, and Bahrain.

The files appear to include logs from 2013 that show the NSA was also targeting oil and investment companies across the Middle East.

If the files are real, the exposed information represents a threat to the SWIFT network, said Matt Suiche, founder of security firm Comae Technologies, who has been looking over the leaked files.



Shadow brokers

A slide from a powerpoint presentation allegedly taken from the NSA.

“This is the first time to date that so much information had been published on how a SWIFT Service Bureau actually works and its internal infrastructure,” he wrote in a blog post.

However, EastNets called reports that it had been hacked “totally false and unfounded.” The company has checked its servers and found no compromise or any vulnerabilities.

“The photos shown on Twitter, claiming compromised information, is about pages that are outdated and obsolete, generated on a low-level internal server that is retired since 2013,” the company said in a statement.

The group behind the leak, the Shadow Brokers, didn't clearly explain why they dumped the files. But in addition to the documents, the hackers also released what appears to be an arsenal of Windows-based hacking tools -- some of which target previously unknown vulnerabilities.

"This isn't a data dump, this is a damn Microsoft apocalypse," tweeted a security researcher who goes by the name Hacker Fantastic.

Researchers are still pouring over the leaked documents, but they've noticed the tools target Windows XP, Windows Server 2003, Windows 7 and 8, among other software products such as Lotus Notes, now called IBM Notes. Any hackers can now download the tools and learn from them.

On Friday, Microsoft also said it was still studying the leak, and it "will take the necessary actions to protect our customers."

In a short posting written in broken English, the Shadow Brokers warned on Friday they had more files to dump.

Earlier this month, the group reappeared after a hiatus and wrote a blog post criticizing U.S. President Donald Trump for ordering an airstrike in Syria and "abandoning" his voters.

"Maybe if all surviving WWIII, theshadowbrokers be seeing you next week," the group wrote on Friday.

Security researchers say the group's latest leak is the most damaging one to date. "It's a huge slap on the face of NSA," said Bulgarian antivirus expert Vesselin Bontchev in an email.

Tell us what you think. Leave a comment on our Facebook page.