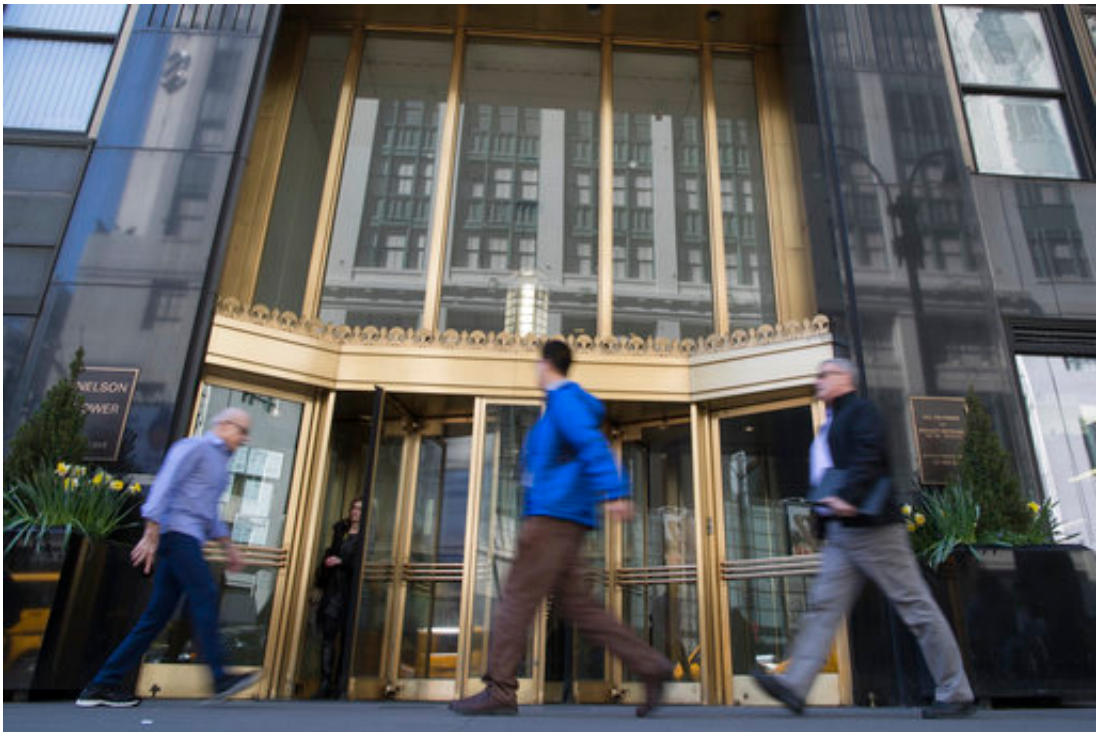
New leak suggests NSA penetrated Mideast banking networks

April 14 2017, by Raphael Satter



Pedestrians make their way past the building that houses the New York office of EastNets in Midtown, Manhattan, N.Y., Friday, April 14, 2017. A new set of documents purportedly lifted from the U.S. National Security Agency suggests that American spies have burrowed deep into the Middle East's financial network, apparently compromising the Dubai office of the anti-money laundering and financial services firm EastNets. The company said Friday that the documents were dated and denied that any customer data had been affected. (AP Photo/Mary Altaffer)

A new set of documents purportedly lifted from the U.S. National Security Agency suggests that American spies have burrowed deep into the Middle East's financial network, apparently compromising the Dubai office of the anti-money laundering and financial services firm EastNets. The company said Friday the documents were dated and denied that any customer data had been affected.

TheShadowBrokers, which startled the security experts last year by releasing some of the NSA's hacking tools, has recently resumed pouring secrets into the public domain. In a first for TheShadowBrokers, the data include PowerPoint slides and purported target lists, suggesting the group has access to a broader range of information than previously known.

"This is by far the most brutal dump," said Comae Technologies founder Matt Suiche, who has closely followed the group's disclosures and initially helped confirm its connection to the NSA last year. In a blog post , he said it appeared that thousands of employee accounts and machines from EastNets' offices had been compromised and that financial institutions in Kuwait, Bahrain and the Palestinian territories had been targeted for espionage.

In a statement , EastNets said there was "no credibility" to the allegation that its customers' details had been stolen.

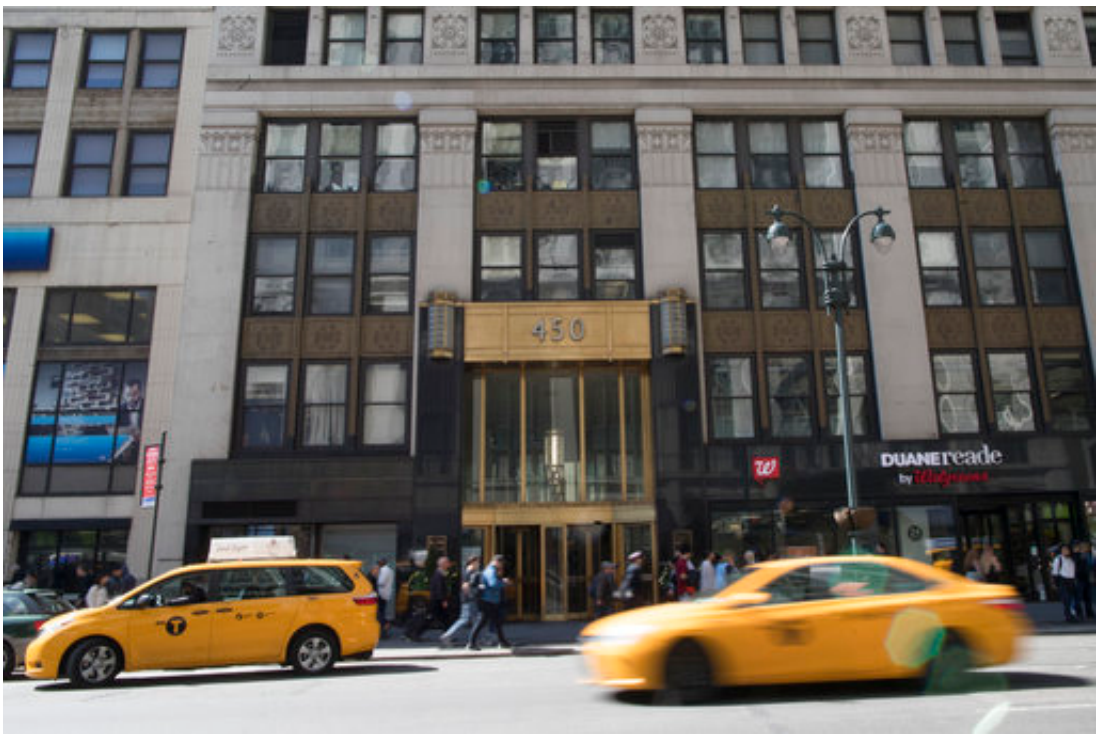
The company, which acts as a "service bureau" connecting customers to the financial world's electronic backbone, SWIFT, said the ShadowBrokers documents referred to a "low-level internal server" that had since been retired and that a "complete check" of its systems had turned up no evidence of any compromise.

The denial drew skepticism from those who'd reviewed the files.

"Eastnets' claim is impossible to believe," said Kevin Beaumont, who was one of several experts who spent Friday combing through the documents and trying out the code. He said he'd found password dumps, an Excel spreadsheet outlining the internal architecture of the company's server and one file that was "just a massive log of hacking on their organization."

SWIFT, based in Belgium, released a less categorical statement, saying, "we understand that communications between these service bureaus and their customers may previously have been accessed by unauthorized third parties." It said there was no evidence its own network had been compromised.

Repeated messages seeking clarification from EastNets went unreturned.



Traffic makes it's way past the building that houses the New York office of EastNets in Midtown, Manhattan, N.Y., Friday, April 14, 2017. A new set of

documents purportedly lifted from the U.S. National Security Agency suggests that American spies have burrowed deep into the Middle East's financial network, apparently compromising the Dubai office of the anti-money laundering and financial services firm EastNets. The company said Friday that the documents were dated and denied that any customer data had been affected. (AP Photo/Mary Altaffer)

Beaumont said there was bad news in the release for Microsoft as well. He said the malicious code published Friday appeared to exploit previously undiscovered weaknesses in older versions of its Windows operating system—the mark of a sophisticated actor and a potential worry for many of Windows' hundreds of millions of users.

The opinion was seconded by Matthew Hickey of Prestbury, England-based cybersecurity company Hacker House.

"It's an absolute disaster," Hickey said in an email. "I have been able to hack pretty much every Windows version here in my lab using this leak."

Microsoft said in a statement that it is reviewing the leak and "will take the necessary actions to protect our customers." It declined to elaborate.

The NSA, which did not respond to emails, has previously shown interest in targeting SWIFT, according to documents leaked by former intelligence contractor Edward Snowden, and Suiche said other documents in the release suggested an effort to monitor the world's financial transactions that went beyond EastNets.

"I'll bet it's not the only SWIFT service bureau that's been compromised," he said.