2-The New York Times-Hacking Group Claims N.S.A

Hacking Group Claims N.S.A. Infiltrated Mideast Banking System

Send any friend a story

As a subscriber, you have 10 gift articles to give each month. Anyone can read what you share.

Give this article

Read in app

The National Security Agency campus in Fort Meade, Md. The agency has the target of leaks from a hacking group that calls itself the Shadow Brokers.Credit…Patrick Semansky/Associated Press

By Nicole Perlroth

April 15, 2017

For the past few months, an elite hacking group calling itself the Shadow Brokers has sporadically leaked sensitive data from the National Security Agency. On Friday, just when its leaks had appeared to slow, the group released what appears to be its most damaging leak so far: a trove of highly classified hacking tools used to break into various Microsoft systems, along with what it said was evidence that the N.S.A. had infiltrated the backbone of the Middle East's banking infrastructure.

The timing of the leaks coincides with the United States' recent shift in policy in Syria, which has escalated the conflict with the Syrian government's main backer, Russia. The Shadow Brokers wrote in broken English in an online post , which cited the American missile attack on a Syrian air base among other reasons for the leak, that after a hiatus, it had

returned to leaking because it was upset that President Trump was abandoning “the peoples who getting you elected.”

Among the leaks on Friday was an extensive list of PowerPoint and Excel documents that, if authentic, indicate that the N.S.A. has successfully infiltrated EastNets , a company based in Dubai that helps to manage transactions in the international bank messaging system called Swift .

Swift, short for the Society for Worldwide Interbank Financial Telecommunication, is used by about 11,000 banks to transfer money from one country to another. The vast majority of those banks rely on Swift service bureaus, like EastNets, the largest bureau in the Middle East, to handle their transactions. The latest leaks suggest that, by hacking EastNets, the N.S.A. may have successfully hacked, or at minimum targeted, computers inside some of the biggest banks in the Middle East, including ones in Abu Dhabi and Dubai in the United Arab Emirates; Kuwait; Qatar; Syria; Yemen; and the Palestinian territories. Among the leaked documents was a now-patched N.S.A. road map to hacking Swift’s back-end infrastructure, which could be used by cybercriminals in the future.

This would not be the first time that United States intelligence agencies have been accused of hacking into Middle Eastern banks. In 2012, security researchers discovered that a computer virus had infiltrated thousands of computers, many inside Lebanese banks . Unlike cybercriminals, who target banks to maximize financial profit, the attackers had monitored the financial transactions of a targeted list of clients of Lebanese banks, which experts said had been used as financial conduits for the Syrian government and Hezbollah, the Lebanese militant group and political party.

The digital crumbs from that attack suggested, cybersecurity experts said, that the virus was the work of the same attackers behind Stuxnet , the computer attack that destroyed the centrifuges in an Iranian nuclear facility and that has been attributed to the United States and Israel.

It is also not the first time a country has been accused of infiltrating the Swift banking system. Federal prosecutors are investigating North Korea’s possible role in a Swift hack that resulted in the theft of $81 million from the central bank of Bangladesh in February 2016 . Security researchers

found that traces of code used in the Bangladesh theft had been used in a destructive cyberattack against Sony in 2014, which the Obama administration and security experts blamed North Korean hackers for carrying out.

The United States is leading inquiries into North Korea's possible involvement in the Swift theft. If legitimate, the leaks suggesting that the N.S.A. has also infiltrated the Swift system leave the United States in an awkward position.

The N.S.A. did not respond to requests for comment. *[Deny]*

The Shadow Brokers first emerged in August, when the group leaked a list of what it said were N.S.A. hacking tools. Initially, some suspected the materials came from an N.S.A. insider gone rogue. But the Shadow Brokers leaks continued even after the F.B.I. arrested an N.S.A. contractor who they believed was stockpiling and potentially leaking the agency's hacking tools . *[Deny]*

Another theory, advanced by security experts and even by Edward J. Snowden , the former N.S.A. contractor who leaked highly classified agency documents and is now living in Russia, is that the Shadow Brokers is a part of the same Russian groups behind the hacking that occurred during the American presidential campaign last year. Some security researchers raised the possibility that the leaks were a warning to American intelligence officials that the Russians had stolen the very tools the American intelligence community could deploy in a counterattack on Russia for its involvement in the pre-election breaches.

The group resumed its leaks after the United States carried out airstrikes targeting Syria, Russia's ally. In a post on April 8, the group said Mr. Trump had abandoned those who helped get him elected. "The ShadowBrokers is losing faith in you," it said, adding, "Is appearing you are abandoning 'your base,' 'the movement,' and the peoples who getting you elected."

On Friday, EastNets denied that it had been hacked. In a statement , the company said its Swift service bureau runs on a separate secure network that cannot be reached over the public internet. The company said the

leaked documents that claimed its computers had been compromised referred to an old server that the bureau had retired in 2013.

“While we cannot ascertain the information that has been published, we can confirm that no EastNets customer data has been compromised in any way,” Hazem Mulhim, EastNets’ chief executive, said in the statement.

But the latest Shadow Brokers leak claims otherwise. One Excel spreadsheet lists what appears to be thousands of stolen credentials belonging to compromised employees and technology administrators at EastNets offices around the globe. Another shows a list of what the group said was computer addresses that have been hacked or targeted by N.S.A. analysts, with the corresponding bank they belong to. Among those listed as having been successfully “implanted,” or infected with spyware, are Noor Bank, Tadhamon International Islamic Bank, Al Quds Bank for Development and Investment, Arcapita Bank and the Kuwait Fund for Arab Economic Development.

None of the documents suggest that the N.S.A. used its access to steal funds. Instead, it appears that the agency was seeking to track the financial movements of certain Middle Eastern bank clients, ostensibly to gain insight into potential terrorist groups or government officials.

The Shadow Brokers’ latest data release also includes a listing of what seemed to be N.S.A. hacking tools, so-called exploits, that allowed the agency to invisibly break into computers and servers running Microsoft Windows. The exploits appear to affect every recent version of Microsoft Windows except its Windows 10 software.

But in a statement issued on Friday, Microsoft said it had already patched its software to protect users from many of the exploits listed in the leaks. Phillip Misner, Microsoft’s principal security group manager, said that of the exploits listed in the Shadow Broker leaks, only three had not been patched, but that none of those three worked on any of Microsoft’s supported software, which includes Windows 7 and up.

Technology companies typically credit security researchers who turn over problems in their software. But in a somewhat mysterious departure from

that procedure, Microsoft did not say how it had learned of the exploits before their release by the Shadow Brokers on Friday.