6-The New York Times-Malware Case

Malware Case Is Major Blow for the N.S.A.

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

139

Read in app

The National Security Agency in Maryland. The weekend's ransomware attack is only the latest in a series of trials for the agency.Credit…Patrick Semansky/Associated Press

By Scott Shane

May 16, 2017

WASHINGTON — Since August, when a mysterious group calling itself the Shadow Brokers announced that it was auctioning off highly classified National Security Agency hacking tools, a low-grade panic has seized the nation's largest intelligence agency. *[Worry]*

In April, when the Shadow Brokers dumped dozens of the agency's software exploits on the web, free to criminals and foreign spies alike, the clock began ticking toward inevitable calamity. And since Friday, the agency has watched as malicious software based on its creations spread across the world, shutting down hospitals, disrupting rail traffic and spurring frustration and chaos in some 150 countries. *[Disappointment]*

“For half a century, N.S.A. pried into other people’s secrets,” said Amy B. Zegart, a Stanford University professor who studies intelligence agencies. “Now they’re suddenly sitting ducks who have their secrets stolen and used around the world.” *[Anger]*

The weekend’s ransomware attack is only the latest in a series of trials for the agency. In 2005, the revelation by The New York Times that the National Security Agency was eavesdropping inside the United States without court orders set off a yearslong debate over American privacy and led to new legal limits on surveillance. In 2013, Edward J. Snowden gave journalists hundreds of thousands of N.S.A. documents he had taken as a contractor, igniting a global debate over the agency’s targeting of allies as well as foes. Last August, shortly after the Shadow Brokers’ debut, a veteran intelligence contractor named Harold T. Martin III was charged with walking out of the National Security Agency and other agencies with a staggering 50 terabytes of confidential data.

Michael V. Hayden, the director of the National Security Agency from 1999 to 2005, said he had defended it for years in debates over civil liberties. “But I cannot defend an agency having powerful tools if it cannot protect the tools and keep them in its own hands, *[Disappointment]*” he said. He said the loss of the so-called malware, and the damage it has caused, “poses a very serious threat to the future of the agency.” *[Worry]*

The latest nightmare for the agency, which is responsible for eavesdropping, code breaking and cyberespionage, appears to be far from over. Early Tuesday, a post purportedly from the Shadow Brokers announced that it was starting a sort of hack-of-the-month club.

“TheShadowBrokers is launching new monthly subscription model,” said the post, in the faux broken English that the group has repeatedly used in public statements. “Is being like wine of month club. Each month peoples can be paying membership fee, then getting members only data dump each month. What members doing with data after is up to members.”

Image

Harold T. Martin III was charged last year with walking out of the National Security Agency and other agencies with a staggering 50 terabytes of confidential data.Credit…Deborah Shaw

The mocking tone — the post's title, "OH LORDY! Comey Wanna Cry Edition," referred to President Trump's firing of the F.B.I. director , James B. Comey, and the ransomware known as WannaCry — could not disguise the deadly serious nature of the threat. Software experts said that the group's dump of N.S.A. tools in April included additional exploits that are "wormable" — meaning they could spread rapidly, like the ransomware attack — and that it might well have more N.S.A. malware it has not yet released. *[Worry]*

In an especially painful development for the agency, some specialists detected evidence that North Korea might have carried out the attack, meaning an adversary had turned American weapons against American allies and innocent parties *[Anger, Disappointment]*. From British hospitals to the American shipping company FedEx, older computers using Microsoft Windows locked up, with a demand of $300 or more to unlock the files on each machine. (The National Security Agency did not respond to a request for comment. *[Deny]*)

Michael Sulmeyer, a former top Pentagon policy official who now runs the cybersecurity program at Harvard's Kennedy School, said the Shadow Brokers episode was a "disaster" for the National Security Agency that underscored how the stakes of leaks from the agency had changed.

"Ten years ago, the costs were fairly low for things going wrong at N.S.A.," Mr. Sulmeyer said. Then, he said, leaks could cut off important sources of intelligence, but today the agency wields powerful malicious software. "Now," he said, "there's a risk for public safety." *[Worry]*

The agency has spent hundreds of millions in taxpayer dollars to develop an arsenal of stealthy software tools to break into foreign computer networks and gather intelligence. When it lost control of those exploits, it was a less lethal version of the Air Force awakening one morning to find many fighter jets missing — and then learning that the fighters were randomly strafing cities around the globe *[Disappointment]*.

The Shadow Brokers saga began in mid-August with a cryptic announcement on Pastebin.com of an online auction of hacking tools taken from what the post called the Equation Group, a tech industry name for the National Security Agency's hacking division, officially called Tailored Access Operations. A few samples were listed to encourage bids.

"We auction best files to highest bidder," the note said.

The announcement created a scramble in the intelligence world to assess the damage and to find the source. There were at least three theories: that Russian hackers had somehow swiped the tools from the agency or a contractor; that N.S.A. operators had inadvertently left them unguarded on a "staging server" used to conduct espionage; or that a disgruntled insider had leaked or sold the malware.

The last scenario — an insider leak from among the 35,000 N.S.A. employees and thousands more contractors — is now in the lead, officials say. About the time the leak hunt began, the F.B.I. arrested Mr. Martin, a veteran intelligence contractor who had worked at the National Security Agency, including in its Tailored Access Operations unit. An N.S.A. employee was arrested in 2015 but never identified, according to officials who spoke on the condition of anonymity. That employee's possible role in leaks remains unclear.

Mr. Martin was not charged with sharing the tools. It is uncertain what charges have been filed against the second person.

The Shadow Brokers found few bidders for their stolen wares. They offered a few more announcements, including screenshots of computer code, without stirring up sales.

Then, in March, apparently after being tipped off by the National Security Agency, Microsoft offered customers a patch that would protect against some of the N.S.A. exploits. *[Rebuild]* Fearing that the window for using the stolen malware was closing, on April 14, the Shadow Brokers simply dumped a list of dozens of the N.S.A. files on github.com, a site for programmers. The group gave the password to find the malware on a cloud site, Yandex Disk, and issued an announcement on steemit.com.

“Is being too bad nobody deciding to be paying theshadowbrokers for just to shutup and going away,” the notice said. “TheShadowBrokers rather being getting drunk with McAfee,” an apparent reference to the antivirus company, “on desert island with hot babes.”

When he saw the files, Sven Dietrich, who teaches computer security at the John Jay College of Criminal Justice in New York, told his class that it was only a matter of time before the escaped N.S.A. malware began doing damage. *[Worry]*

“It’s too tempting to have nation-state level exploits available for free on the web,” he said.

BinaryEdge, a Zurich cybersecurity company, began picking up machines around the world infected with an N.S.A. exploit called DoublePulsar. The total reached 106,000 on April 21; 244,000 on April 25; 429,000 on April 27.

“It was a prewarning of what was to come,” said Tiago Henriques, the chief executive of BinaryEdge. Using another exploit, called EternalBlue, attackers began targeting vulnerable machines with a self-replicating software “worm” that locked files and posted a ransom demand.

Even the April release of N.S.A. exploits is not close to exhausted, according to several cyberspecialists. On the underground dark web, they said, another N.S.A. tool has been weaponized and offered for sale, and hackers are discussing how to use another dozen agency exploits.

But Mr. Henriques did have a kind of compliment for the work of the National Security Agency, now under siege.

“These tools were beautifully made,” he said. “Hard to detect and easy to use. They were pretty much point and shoot. Even under the circumstances, you have to appreciate good engineering.” *[Positive]*