The New York Times | https://nyti.ms/2qlBmPd

U.S.

# In Computer Attacks, Clues Point to Frequent Culprit: North Korea

点击查看本文中文版

By NICOLE PERLROTH and DAVID E. SANGER MAY 15, 2017

SAN FRANCISCO — Intelligence officials and private security experts say that new digital clues point to North Korean-linked hackers as likely suspects in the sweeping ransomware attacks that have crippled computer systems around the world.

The indicators are far from conclusive, the researchers warned, and it could be weeks, if not months, before investigators are confident enough in their findings to officially point the finger at Pyongyang's increasingly bold corps of digital hackers. The attackers based their weapon on vulnerabilities that were stolen from the National Security Agency and published last month.

Security experts at Symantec, which in the past has accurately identified attacks mounted by the United States, Israel and North Korea, found early versions of the ransomware, called WannaCry, that used tools that were also deployed against Sony Pictures Entertainment, the Bangladesh central bank last year and Polish banks in February. American officials said Monday that they had seen the same similarities.

All of those attacks were ultimately linked to North Korea; President Barack Obama formally charged the North in late 2014 with destroying computers at

Sony in retaliation for a comedy, "The Interview," that envisioned a C.I.A. plot to kill Kim Jong-un, the country's leader.

The computer code used in the ransomware bore some striking similarities to the code used in those three attacks. That code has not been widely used, and has been seen only in attacks by North Korean-linked hackers. Researchers at Google and Kaspersky, a Moscow-based cybersecurity firm, confirmed the coding similarities.

Those clues alone are not definitive, however. Hackers often borrow and retrofit one another's attack methods, and government agencies are known to plant "false flags" in their code to throw off forensic investigators.

"At this time, all we have is a temporal link," said Eric Chien, an investigator at Symantec who was among the first to identify the Stuxnet worm, the American- and Israeli-led attacks on Iran's nuclear program, and North Korea's effort to steal millions from the Bangladeshi bank. "We want to see more coding similarities," he said, "to give us more confidence."

The new leads about the source of the attacks came as technology executives raised an alarm about another feature of the attacks: They were based on vulnerabilities in Microsoft systems that were found by the N.S.A. and apparently stolen from it.

In a blog post on Microsoft's website over the weekend, Brad Smith, the company's president, asked what would happen if the United States military lost control of "some of its Tomahawk missiles" and discovered that a criminal group was using them to threaten a damaging strike. It was a potent analogy, and an unusually public airing of the newest split in the Silicon Valley-Washington divide.

Over the past few months, it has become clear that the intelligence community's version of Tomahawks — the "vulnerabilities" the N.S.A. and C.I.A. have spent billions of dollars to develop to break into foreign computers and foil Iranian nuclear programs or North Korean missiles — are being turned against everyday computer users around the world.

"We have seen vulnerabilities stored by the C.I.A. show up on WikiLeaks," Mr. Smith wrote, "and now this vulnerability stolen from the N.S.A. has affected

customers around the world."

The N.S.A.'s tools were published last month by a hacking group calling itself the Shadow Brokers, which enabled hackers to bake them into their ransomware, which then spread rapidly through unpatched Microsoft computers, locking up everything in its wake.

There is no evidence that the North Koreans were involved in the actual theft of the N.S.A. hacking tools. There are many theories, but the favorite hypothesis among intelligence officials is that an insider, probably a contractor, stole the information, much as Edward J. Snowden lifted a different trove of information from the N.S.A. four years ago.

But hackers quickly seized on the published vulnerabilities to wreak havoc on computer systems that were not "patched" in recent months, after the N.S.A. quietly told Microsoft about the flaw in their systems. The damage wreaked in recent days could well escalate into the billions of dollars, security experts say, particularly now that any criminal, terrorist or nation state has the ability to tease the tools apart and retrofit them into their own hacking tools.

Not surprisingly, government officials say it is not entirely their fault. They will not confirm or deny what Mr. Smith says outright: That these "vulnerabilities" come out of America's growing cyberarsenal. At a news conference at the White House on Monday, Thomas Bossert, President Trump's Homeland Security adviser, told reporters, "This was not an exploit developed by the N.S.A. to hold organizations ransom," he said. "This was a vulnerability exploit that was part of a much larger tool put together by the culpable parties."

"The provenance of the underlying vulnerability is not of as much concern to me," Mr. Bossert said, stepping around the delicate question of the N.S.A.'s role.

The weapons used in the attacks that started Friday, government officials insist, were cobbled together from many sources. And the fault, they argue, lies with whoever turned them into weapons — or maybe with Microsoft itself, for not having a system in place to make sure that when they issue a patch that neutralizes such attacks, everyone around the world takes the time to fix their systems. Or with the victims, who failed to run their security updates made

available two months ago, or who continue to use so-called “legacy” software that Microsoft no longer supports.

When asked about the source of the attack, Mr. Bossert said on Monday, “We don’t know.” He told reporters at the White House. “Attribution can be difficult. I don’t want to say we have no clues. But I stand assured that the best and brightest are working on this hack.”

As Mr. Bossert was speaking to reporters, yet another N.S.A. hacking tool, very similar to the one used in the weekend’s ransomware attacks, was being retrofitted by cybercriminals and put up for sale on the underground dark web. In private hacking forums, cybercriminals were discussing how to develop more than a dozen other N.S.A. hacking tools for criminal use.

Another round of attacks using the N.S.A. tools could well affect another big issue that the Obama administration debated and never resolved when it left office: whether the government can demand that all companies assure that investigators can “unlock” encrypted communications. Before he was fired last week, James B. Comey, the F.B.I. director, often complained that the government was “going dark,” and that intelligence agencies and local police departments needed a way to crack the encrypted mobile conversations of terrorists or kidnappers.

But the N.S.A.’s loss of its own hacking tools has undercut that argument, executives say. If the N.S.A. and the C.I.A. cannot keep their hacking tools locked up, companies like Apple are asking, why should Americans trust them with the keys to unlock every private communication and bank transfer? Won’t those leak, too, meaning that hackers, blackmailers and thieves will all have access to everyone’s private email, health records and financial transactions?

Nine years ago, the White House created a process for deciding what unpatched holes to disclose to manufacturers like Microsoft and its competitors, and which to keep in its arsenal.

That process was refined by Mr. Obama and in 2015, Adm. Michael Rogers, the director of the NSA, said the agency had shared 91 percent of the zero-days it had discovered that year. A zero-day is a previously undisclosed flaw that leaves computer users with zero days to fix the vulnerability.

But Michael Daniel, the White House cybercoordinator in the Obama administration, noted, “We still don’t have a good rating system for vulnerabilities in terms of their severity. Not all zero-days are created equal,” he said.

The N.S.A.’s wormlike tool was leaked online by the Shadow Brokers last month.

“What happened with the Shadow Brokers in this case is equivalent to a nuclear bomb in cyberspace,” said Zohar Pinhasi, a former cybersecurity intelligence officer for the Israeli military, now the chief executive of MonsterCloud, which helps mitigate ransomware attacks. “This is what happens when you give a tiny little criminal a weapon of mass destruction. This will only go bigger. It’s only the tip of the iceberg.”

***Correction: May 17, 2017***

An article on Tuesday about hints that hackers linked to North Korea may have been involved in recent ransomware attacks misspelled the given name of the country’s leader in some copies. He is Kim Jong-un, not Kim Jung-un.

Nicole Perlroth reported from San Francisco, and David E. Sanger from Washington.

*Get politics and Washington news updates via Facebook, Twitter and in the Morning Briefing newsletter.*

A version of this article appears in print on May 16, 2017, on Page A1 of the New York edition with the headline: In Computer Attacks, Clues Point to Frequent Culprit: North Korea.