Their code was used to hack Sony and create 'WannaCry.' Meet the 'Lazarus Group'

May 19 2017, by Matt Pearce, Los Angeles Times

Credit: George Hodan/Public Domain

On Feb. 4, 2016, as employees left work to enjoy their weekends, the central bank of Bangladesh began firing off dozens of transfer orders to the Federal Reserve Bank of New York, asking to remove money from its accounts - almost $1 billion.

It was a heist. The robbers hadn't walked in with guns or tunneled into a

vault to get the money. They'd hijacked the bank's computer systems to access an international financial network, SWIFT, which shunts around billions of dollars a day. The invisible thieves made off with $81 million before officials halted the geyser of cash.

The attack's audacity, and the weaknesses it exposed, stunned bankers and financial regulators. Months later, cybersecurity researchers concluded that it was yet another notch in the belt of one of the most destructive hacker collectives on the internet, the "Lazarus Group," accused of previously being behind the devastating 2014 Sony Pictures Entertainment hack and other attacks - and accused of working for North Korea.

Now, the Lazarus Group has been tentatively linked to another audacious attack for cash, raising the question of whether North Korea has started sticking up internet users while carrying out its very public standoff with the United States.

Hundreds of thousands of computers have been hijacked in the last week by a virus called "WannaCry," which freezes files on computers and demands a ransom for their release. It's called ransomware, and it's a new spin on old-fashioned stickups: Pay up with bitcoin, the digital currency, or lose the files forever.

WannaCry spread to at least 150 nations over last weekend, including the U.S., shutting down hospitals in Britain and hijacking terminal screens at train stations in Germany, probably causing billions of dollars in damage. The virus was initially notable because it was an adaptation of a cybertool to hack Windows that had been developed by, and then stolen from, the U.S. National Security Agency.

But as analysts and investigators began picking apart WannaCry for forensic clues - the digital equivalent of dusting for prints - a

cybersecurity researcher at Google named Neel Mehta found something in an older version of the virus. It was just a few lines of code, but it has appeared only in one other known place: hacking tools created by the Lazarus Group. Word spread rapidly among researchers.

The connection to the Lazarus Group so far is only tentative, researchers caution, suggesting that it's possible the code was inserted as a "false flag" to throw off investigators. Officials in Europe and the U.S., still in the beginning stages of their investigations, have not named the Lazarus Group or North Korea as a suspect.

But "with a group like Lazarus, where we have a long history," said Eric Chien, a technical director at the Mountain View, Calif.-based internet security firm Symantec, "I would suspect that within a couple of weeks we should be able to rule them in or rule them out."

The hacker group was identified and given a name in a collaborative investigation published in February 2016 called "Operation Blockbuster," which was undertaken by several cybersecurity companies seeking to examine the perpetrators of the 2014 Sony hack.

Within the world of cybercrime, the Sony attack was highly unusual. The hackers struck as the studio was about to release "The Interview," a Seth Rogen and James Franco comedy whose plot centers on a plan to assassinate North Korea's leader, Kim Jong Un.

Hackers calling themselves "Guardians of Peace" launched a multi-pronged assault on Sony, destroying company files, demanding ransom, publishing embarrassing emails and salary information online and leaking unreleased films. The U.S. government blamed North Korea, and the "Guardians of Peace" disappeared.

Later, the "Operation Blockbuster" coalition began to examine data from

the attack published by the U.S. government. What it found surprised the coalition: The Sony hack was far from being a one-off attack.

"We saw things dating back years and years and years," said Peter LaMontagne, the former CEO of Novetta, the American firm that led the coalition.

Just as scientists examining DNA look for a creature's ancestors, the researchers linked code and processes used by the Sony hackers to a series of earlier attacks.

A 2009 distributed denial-of-service attack on American and South Korean websites. A 2011 attack that tried to shut down South Korean network broadcast companies and banks. A 2012 attack on a right-wing South Korean newspaper. The attackers seemed to be well resourced, clever and dogged, coming back again and again.

That's how researchers came up with "Lazarus Group," an allusion to the biblical figure who rises from the dead.

"We came up with that name because we kept seeing unique chunks of code appearing/reappearing in new malware strains," former Novetta technical director Andre Ludwig wrote in an email. He called it "one of the driving factors that enabled us to identify so many families of malware and make hard technical links between them all."

The backwaters of the internet are filled with agitators, spies and fraudsters. The most high-profile attacks of the last year have apparently involved Russia, which was accused of hacking Democrats and publishing their emails to sway the presidential election toward Donald Trump.

But the Lazarus hackers have stood out not for doing one thing, but for

doing everything.

"We tend to see cybergroups falling into categories and staying in their lanes," LaMontagne said. "You have hacktivists who have sort of a political agenda, and everything they do is geared to messaging. You have folks that are very focused on making money. ... Then, thirdly, we have pure foreign intelligence cyberespionage."

With the Sony hack, for example, LaMontagne said, Lazarus was "delving into all three." And the group's ambition seems unbounded.

"The scale of Lazarus operations is shocking," the Russia-based cybersecurity firm Kaspersky Lab said in a report on the Lazarus Group's activities, likening its production to "a factory of malware." "All this level of sophistication is something that is not generally found in the cybercriminal world. It's something that requires strict organization and control at all stages of the operation."

After the Novetta report came out in early 2016, the hackers remained busy and trackable. (The Bangladesh heist took place before the release of the report, but Lazarus was not linked to the attack until later.)

"Lazarus Group has been active constantly," said Chien of Symantec. "We constantly see them, doing little things here and there, but you only hear in the news the big event that happens."

Industry researchers later linked Lazarus hackers to the 2016 Bangladesh bank heist and a financial system attack in Poland in 2017. Top U.S. security officials have dropped hints that they think North Korea might be behind the financial attacks in addition to the Sony hack, citing private-sector research work.

"If that attribution is true ... that means a nation-state is robbing banks,"

NSA Deputy Director Richard Ledgett said during an Aspen Institute panel in March. "That's a big deal, in my opinion."

"Do you believe there are nation-states now robbing banks?" a moderator asked Ledgett.

"I do," Ledgett replied.

The WannaCry ransomware would be an unusual development, should North Korea end up being implicated - an instance of a nation trying to steal money from foreign users, both governmental and private.

Yet even though WannaCry is designed to steal money, it's doing a very poor job of it, raising less than $80,000 worth of bitcoin from a tiny percentage of the virus's hundreds of thousands of victims. The payments were arranged to go to easily trackable accounts. Experts initially thought it was the work of amateurs.

"This piece of ransomware has a lot of bugs in it, a lot of weird things that other ransomware doesn't have in it," Chien said. "There's actually no way (for the hackers) to determine who paid and who didn't pay," meaning that the chances of getting your files unlocked after paying a ransom "is very, very low."

Others have speculated that, if WannaCry is the work of North Korea, maybe the attackers just wanted to test out its disruptive capabilities for future political attacks - a motive that would not be outside the realm of possibility for the Lazarus Group.

"There's definitely no ceiling on their ambition," Chien said. "They may come up with an idea and say, 'Let's go do it.'"