Exclusive: Suspected Chinese hackers used SolarWinds bug to spy on U.S. payroll agency – sources

reuters.com/article/us-cyber-solarwinds-china/exclusive-suspected-chinese-hackers-used-solarwinds-bug-to-spy-on-u-s-payroll-agency-sources-idUSKBN2A22K8

Christopher Bing, Jack Stubbs, Raphael Satter, Joseph Menn

Banks
Updated

By Christopher Bing, Jack Stubbs, Raphael Satter, Joseph Menn

6 Min Read

WASHINGTON (Reuters) - Suspected Chinese hackers exploited a flaw in software made by SolarWinds Corp to help break into U.S. government computers last year, five people familiar with the matter told Reuters, marking a new twist in a sprawling cybersecurity breach that U.S. lawmakers have labeled a national security emergency.

Two people briefed on the case said FBI investigators recently found that the National Finance Center, a federal payroll agency inside the U.S. Department of Agriculture, was among the affected organizations, raising fears that data on thousands of government

employees may have been compromised.

The software flaw exploited by the suspected Chinese group is separate from the one the United States has accused Russian government operatives of using to compromise up to 18,000 SolarWinds customers, including sensitive federal agencies, by hijacking the company's Orion network monitoring software.

Security researchers have previously said a second group of hackers was abusing SolarWinds' software at the same time as the alleged Russian hack, but the suspected connection to China and ensuing U.S. government breach have not been previously reported.

Reuters was not able to establish how many organizations were compromised by the suspected Chinese operation. The sources, who spoke on condition of anonymity to discuss ongoing investigations, said the attackers used computer infrastructure and hacking tools previously deployed by state-backed Chinese cyberspies.

A USDA spokesman said in an email "USDA has notified all customers (including individuals and organizations) whose data has been affected by the SolarWinds Orion Code Compromise."

In a follow-up statement after the story was published, a different USDA spokesman said the NFC was not hacked and that "there was no data breach related to Solar Winds" at the agency. He did not provide further explanation.

The Chinese foreign ministry said attributing cyberattacks was a "complex technical issue" and any allegations should be supported with evidence. "China resolutely opposes and combats any form of cyberattacks and cyber theft," it said in a statement.

SolarWinds said it was aware of a single customer that was compromised by the second set of hackers but that it had "not found anything conclusive" to show who was responsible. The company added that the attackers did not gain access to its own internal systems and that it had released an update to fix the bug in December.

FILE PHOTO: SolarWinds Corp. banner hangs at the New York Stock Exchange (NYSE) on the IPO day of the company in New York, U.S., October 19, 2018. REUTERS/Brendan McDermid

In the case of the sole client it knew about, SolarWinds said the hackers only abused its software once inside the client's network. SolarWinds did not say how the hackers first got in, except to say it was "in a way that was unrelated to SolarWinds."

The FBI declined to comment.

Although the two espionage efforts overlap and both targeted the U.S. government, they were separate and distinctly different operations, according to four people who have investigated the attacks and outside experts who reviewed the code used by both sets of hackers.

While the alleged Russian hackers penetrated deep into SolarWinds network and hid a “back door” in Orion software updates which were then sent to customers, the suspected Chinese group exploited a separate bug in Orion’s code to help spread across networks they had already compromised, the sources said.

‘EXTREMELY SERIOUS BREACH’

The side-by-side missions show how hackers are focusing on weaknesses in obscure but essential software products that are widely used by major corporations and government agencies.

“Apparently SolarWinds was a high value target for more than one group,” said Jen Miller-Osborn, the deputy director of threat intelligence at Palo Alto Networks’ Unit42.

Former U.S. chief information security officer Gregory Touhill said separate groups of hackers targeting the same software product was not unusual. “It wouldn’t be the first time we’ve seen a nation-state actor surfing in behind someone else, it’s like ‘drafting’ in NASCAR,” he said, where one racing car gets an advantage by closely following another’s lead.

The connection between the second set of attacks on SolarWinds customers and suspected Chinese hackers was only discovered in recent weeks, according to security analysts investigating alongside the U.S. government.

Reuters could not determine what information the attackers were able to steal from the National Finance Center (NFC) or how deep they burrowed into its systems. But the potential impact could be “massive,” former U.S. government officials told Reuters.

The NFC is responsible for handling the payroll of multiple government agencies, including several involved in national security, such as the FBI, State Department, Homeland Security Department and Treasury Department, the former officials said.

Records held by the NFC include federal employee social security numbers, phone numbers and personal email addresses as well as banking information. On its website, the NFC says it “services more than 160 diverse agencies, providing payroll services to more than 600,000 Federal employees.”

“Depending on what data were compromised, this could be an extremely serious breach of security,” said Tom Warrick, a former senior official at the U.S Department of Homeland Security. “It could allow adversaries to know more about U.S. officials, improving their ability

to collect intelligence.”

Reporting by Christopher Bing and Raphael Satter in Washington, Joseph Menn in San Francisco, and Jack Stubbs in London; Additional reporting by Brenda Goh in Shanghai; Editing by Jonathan Weber and Edward Tobin

Our Standards: The Thomson Reuters Trust Principles.