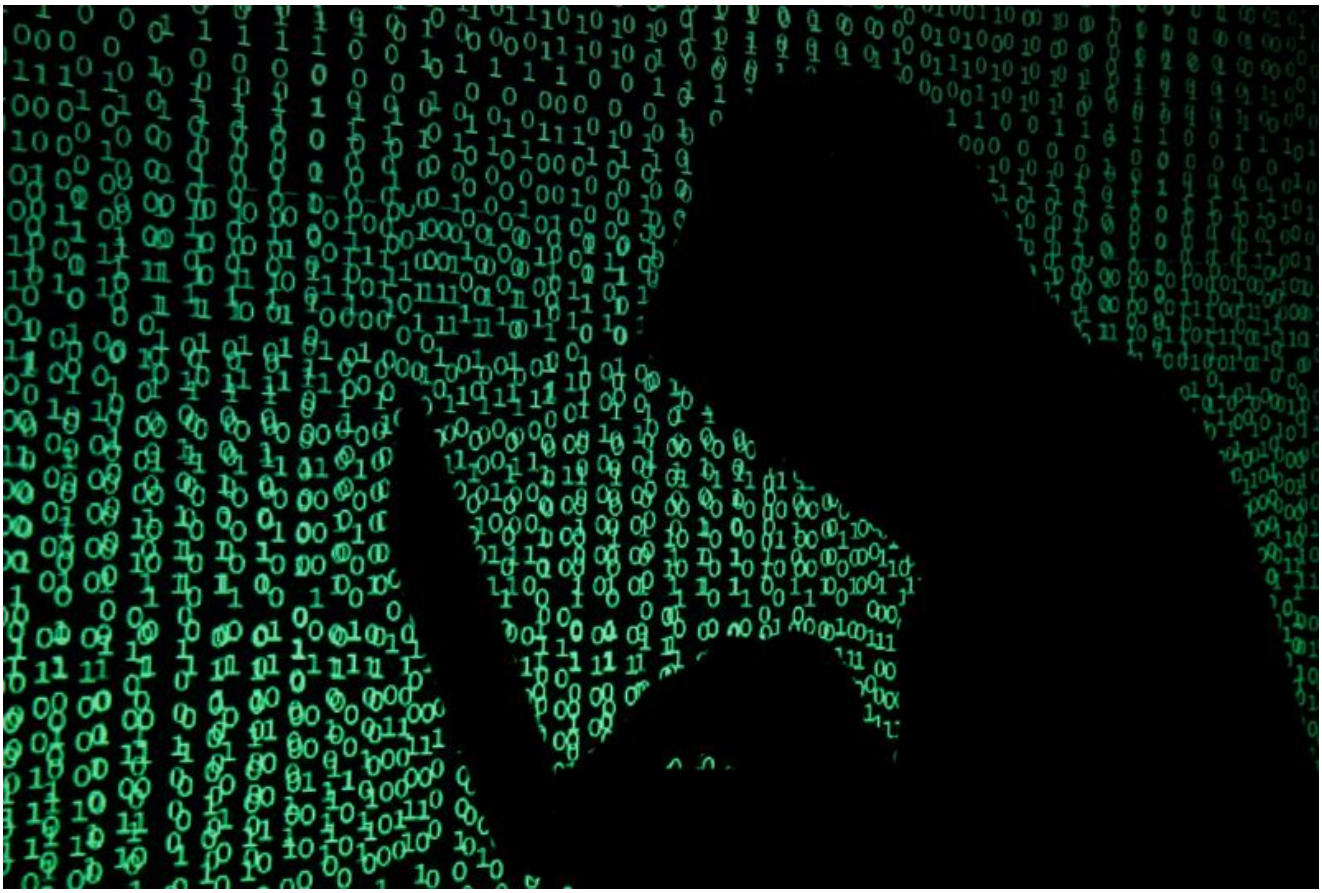
Suspected Russian hackers spied on U.S. Treasury emails - sources

reuters.com/article/us-usa-cyber-treasury-exclsuive/suspected-russian-hackers-spied-on-u-s-treasury-emails-sources-idUSKBN28N0PG

Christopher Bing



Technology News
Updated

By Christopher Bing

5 Min Read

WASHINGTON (Reuters) - Hackers believed to be working for Russia have been monitoring internal email traffic at the U.S. Treasury and Commerce departments, according to people familiar with the matter, adding they feared the hacks uncovered so far may be the tip of the iceberg.

FILE PHOTO: A hooded man holds a laptop computer as cyber code is projected on him in this illustration picture taken on May 13, 2017. REUTERS/Kacper Pempel/Illustration

The hack is so serious it led to a National Security Council meeting at the White House on Saturday, said one of the people familiar with the matter.

U.S. officials have not said much publicly beyond the Commerce Department confirming there was a breach at one of its agencies and that they asked the Cybersecurity and Infrastructure Security Agency and the FBI to investigate.

National Security Council spokesman John Ullyot added that they “are taking all necessary steps to identify and remedy any possible issues related to this situation.”

The U.S. government has not publicly identified who might be behind the hacking, but three of the people familiar with the investigation said Russia is currently believed to be responsible for the attack. Two of the people said that the breaches are connected to a broad campaign that also involved the recently disclosed hack on FireEye, a major U.S. cybersecurity company with government and commercial contracts.

In a statement posted here to Facebook, the Russian foreign ministry described the allegations as another unfounded attempt by the U.S. media to blame Russia for cyberattacks against U.S. agencies.

The cyber spies are believed to have gotten in by surreptitiously tampering with updates released by IT company SolarWinds, which serves government customers across the executive branch, the military, and the intelligence services, according to two people familiar with the matter. The trick - often referred to as a “supply chain attack” - works by hiding malicious code in the body of legitimate software updates provided to targets by third parties.

In a statement released late Sunday, the Austin, Texas-based company said that updates to its monitoring software released between March and June of this year may have been subverted by what it described as a “highly-sophisticated, targeted and manual supply chain attack by a nation state.”

The company declined to offer any further detail, but the diversity of SolarWind’s customer base has sparked concern within the U.S. intelligence community that other government agencies may be at risk, according to four people briefed on the matter.

Related Coverage

SolarWinds says on its website that its customers include most of America’s Fortune 500 companies, the top 10 U.S. telecommunications providers, all five branches of the U.S. military, the State Department, the National Security Agency, and the Office of President of the United States.

‘HUGE CYBER ESPIONAGE CAMPAIGN’

The breach presents a major challenge to the incoming administration of President-elect Joe Biden as officials investigate what information was stolen and try to ascertain what it will be used for. It is not uncommon for large scale cyber investigations to take months or years to complete.

“This is a much bigger story than one single agency,” said one of the people familiar with the matter. “This is a huge cyber espionage campaign targeting the U.S. government and its interests.”

Hackers broke into the NTIA’s office software, Microsoft’s Office 365. Staff emails at the agency were monitored by the hackers for months, sources said.

A Microsoft spokesperson did not respond to a request for comment. Neither did a spokesman for the Treasury Department.

The hackers are “highly sophisticated” and have been able to trick the Microsoft platform’s authentication controls, according to a person familiar with the incident, who spoke on condition of anonymity because they were not allowed to speak to the press.

“This is a nation state,” said a different person briefed on the matter.

The full scope of the breach is unclear. The investigation is still its early stages and involves a range of federal agencies, including the FBI, according to three of the people familiar with the matter.

A spokesperson for the Cybersecurity and Infrastructure Security Agency said they have been “working closely with our agency partners regarding recently discovered activity on government networks. CISA is providing technical assistance to affected entities as they work to identify and mitigate any potential compromises.”

The FBI and U.S. National Security Agency did not respond to a request for comment.

There is some indication that the email compromise at NTIA dates back to this summer, although it was only recently discovered, according to a senior U.S. official.

Reporting by Christopher Bing, Jack Stubbs, Joseph Menn, and Raphael Satter; Editing by Chris Sanders, Daniel Wallis and Diane Craft

Our Standards: The Thomson Reuters Trust Principles.