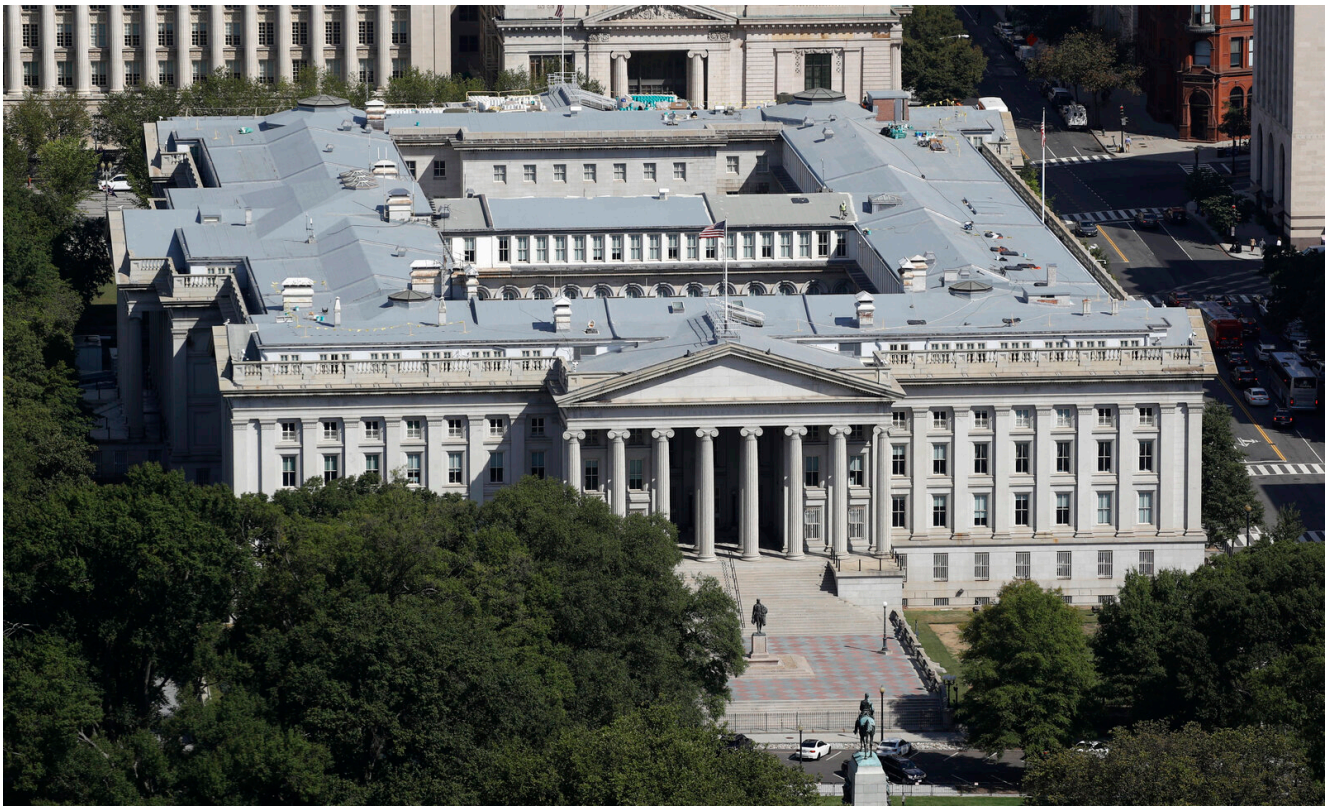
Russia Suspected In Major Cyberattack On U.S. Treasury, Commerce Departments



The U.S. Treasury Department, shown here in 2019, has been hacked along with the U.S. Commerce Department, according to reports. Russia is suspected but denies involvement. The U.S. government has acknowledged a breach and says it is investigating to make a full assessment. – Patrick Semansky/AP

Updated at 10:22 a.m. ET

Russian hackers working for the Kremlin are believed to be behind an attack into U.S. government computer systems at the departments of Treasury and Commerce that may have lasted months before it was detected, according to U.S. officials and media reports.

The hackers reportedly broke into the email systems at those two government departments, but the full extent of the breach was not immediately clear as U.S.

officials scrambled to make an assessment. There are concerns that hackers may have penetrated other government departments and perhaps many private companies as well.

The Commerce Department, the National Security Council and the Department of Homeland Security all acknowledged the intrusion in brief statements but provided no details.

“We can confirm there has been a breach in one of our bureaus,” the Commerce Department said.

“We have been working closely with our agency partners regarding recently discovered activity on government networks,” said NSC spokesman John Ullyot.

The U.S. government did not name Russia or any other actor as being responsible.

Reuters first reported the story on Sunday, and subsequent reports identified Russia’s foreign intelligence service, the SVR, as the most likely culprit.

Russia’s SVR, the rough equivalent to the CIA in the U.S., was blamed for major hacks in 2014-15 that involved unclassified email systems at the White House, State Department and the Joint Chiefs of Staff.

Russia on Monday denied any involvement in the latest reported breach.

Emergency directive

Meanwhile, the U.S. Cybersecurity and Infrastructure Security Agency (CISA), which is part of Homeland Security, issued an emergency directive calling on all federal civilian agencies to review their computer networks for signs of the compromise. The statement also said agencies should disconnect from SolarWinds Orion products immediately.

SolarWinds has government contracts, including with the military and intelligence services, and also works with many large private companies. The attackers are believed to have used a “supply chain attack” method that embeds malicious code into legitimate software updates.

“The compromise of SolarWinds’ Orion Network Management Products poses

unacceptable risks to the security of federal networks," CISA's acting Director Brandon Wales said in a statement. "Tonight's directive is intended to mitigate potential compromises within federal civilian networks, and we urge all our partners — in the public and private sectors — to assess their exposure to this compromise."

SolarWinds, based in Austin, Texas, put out its own statement saying it was aware that its systems were experiencing a "highly sophisticated, manual supply chain attack" on specific versions of its Orion platform software released between March and June of this year.

"We have been advised this attack was likely conducted by an outside nation-state and intended to be a narrow, extremely targeted, and manually executed attack, as opposed to a broad, system-wide attack," the company said.

Kevin Thompson, SolarWinds' president and CEO, said the company was working with the FBI, the U.S. intelligence community and other law enforcement agencies to investigate.

Tech companies respond

Two other tech companies, Microsoft and FireEye, also weighed in.

Microsoft said in a blog post late Sunday, "We believe this is nation-state activity at significant scale, aimed at both the government and private sector."

The Commerce Department and the Treasury Department use the Microsoft Office 365 platform, Reuters and The New York Times reported Sunday.

FireEye reported last week that hackers, also believed to be Russians, stole the company's key tools used to test vulnerabilities in the computer networks of its customers, which include government agencies.

FireEye said in a blog post late Sunday night that it had identified "a global campaign that introduces a compromise into the networks of public and private organizations through the software supply chain."

Speaking in Moscow last Friday, Kremlin spokesman Dmitry Peskov dismissed allegations that Russia was involved in the FireEye hack.

“I want to remind you that it was President (Vladimir) Putin who proposed that the American side agree and conclude agreements (with Russia) on cybersecurity,” Peskov said, adding that Washington had ignored the offer.

“If there have been attacks for many months, and the Americans could not do anything about it, it is probably not worth immediately, groundlessly blaming the Russians. We didn’t have anything to do with it,” he said.

NPR’s national security correspondent Greg Myre contributed to this report.

Source:
https://www.npr.org/2020/12/14/946163194/russia-suspected-in-months-long-cyber-attack-on-federal-agencies

[Disclaimer]