US Treasury and Commerce department email systems reportedly hacked

Kevin Reed
15 December 2020

Major US news outlets reported on Sunday that hackers had broken into the US Treasury and Commerce department computer systems and were monitoring internal email activity for months without detection. Unidentified experts and government officials “familiar with the matter” were quick to conclude that the hackers were “believed to be” working for Russian intelligence.

Among the first to report the hack was Reuters, which wrote that their sources “feared the hacks uncovered so far may be the tip of the iceberg,” and that “the hack is so serious it led to a National Security Council meeting at the White House on Saturday.”

Reuters reported that US government officials have not said much publicly about the hack other than the acknowledgment by the Commerce Department that “there was a breach at one of its agencies and that they asked the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI to investigate.”

John Ullyot, Deputy Assistant to the President, Senior Director for Strategic Communications at the National Security Council, told Reuters the agency was “taking all necessary steps to identify and remedy any possible issues related to this situation.”

The report went on to say that the hack appears to have taken place when software updates from government IT service provider SolarWinds had been tampered with in what is known as a “supply chain attack.” The technology platform—which serves US government customers “across the executive branch, the military, and the intelligence services”—was attacked with malicious code embedded “in the body of legitimate software updates.”

The Austin, Texas-based SolarWinds issued a statement late on Sunday acknowledging it had “experienced a highly sophisticated, manual supply chain attack” on its Orion platform software. On Monday, the firm stated that fewer than 18,000 of its 300,000 customers had software compromised by the hack.

The SolarWinds hack did not involve stealing usernames and passwords, a common technique used to gain widespread access to secure systems. Instead, once the hackers were in the SolarWinds network management software through the updates breach, they were able to insert counterfeit “tokens,” essentially electronic indicators that provide an assurance to Microsoft, Google or other providers about the identity of the computer system to which its email systems are communicating.

The *New York Times* reported that the Trump administration acknowledged the hack on Sunday and said it was carried out “on behalf of a foreign government—almost certainly a Russian intelligence agency, according to federal and private experts.”

The *Times* wrote that the Commerce Department agency affected by the hack “appeared to be the National Telecommunications and Information Administration, which helps determine policy for internet-related issues, including setting standards and blocking imports and exports of technology that is considered a national security risk.”

The *Washington Post* was categorical in its report that “Russian government hackers breached the Treasury and Commerce departments, along with other U.S. government agencies, as part of a global espionage campaign that stretches back months.” The *Post* claimed that Russian hackers “known by the nicknames APT29 or Cozy Bear, are part of that nation’s foreign intelligence service, the SVR,” according to “people familiar with the intrusions, who spoke on the condition of anonymity because of the sensitivity of the matter.”

The Russian government, communicating through its embassy in Washington, DC, denied that the Moscow government was engaged in hacking and said it “does not conduct offensive operations in the cyber domain.” In a Facebook post, the embassy said, “attempts of the US media to blame Russia for hacker attacks on US governmental bodies” were unfounded.

The hack of Treasury and Commerce department email communications comes less than a week after the National Security Agency (NSA)—an intelligence organization specializing in international cyberespionage—issued a warning about “Russian state-sponsored actors” who were exploiting systems used widely by the US government.

Although no details about the nature of the exploits were provided at that time, several days later the cybersecurity company FireEye announced that state-sponsored hackers had breached its servers and stolen some of its tools used to find vulnerabilities in government systems. A subsequent FireEye investigation named the Russian intelligence agency SVR as well as the hackers Cozy Bear and APT29.

FireEye is used by US government agencies, including the Department of Homeland Security and the branches of US intelligence, to test the security of their system with a battery of hacking techniques that the company maintains in a database. According to the *New York Times* report, the hackers who breached FireEye stole the firms “red team” tools and likely used these methods to hijack the SolarWinds Orion platform software updates.

While no evidence has been provided that the hacking was carried out by Russian intelligence, the fact that the top-level computer system used by the White House, the NSA, the Pentagon, the State Department and the Department of Justice—along with that of the top 10 telecommunications companies—has been broken into and was monitored for weeks without anyone knowing about it is a devastating revelation.

Jake Williams, a former NSA hacker and president of the cybersecurity firm Rendition Infosec, told the Associated Press, “I suspect that there’s a number of other (federal) agencies we’re going to hear from this week that have also been hit.”