US agencies hacked in monthslong global cyberspying campaign

December 14 2020, by Eric Tucker, Frank Bajak and Matt O'brien

The U.S. Treasury Department building viewed from the Washington Monument, Wednesday, Sept. 18, 2019, in Washington. Hackers got into computers at the U.S. Treasury Department and possibly other federal agencies, touching off a government response involving the National Security Council. Security Council spokesperson John Ullyot said Sunday, Dec. 13, 2020 that the government is aware of reports about the hacks. (AP Photo/Patrick Semansky, file)

U.S. government agencies were ordered to scour their networks for malware and disconnect potentially compromised servers after authorities learned that the Treasury and Commerce departments were hacked in a monthslong global cyberespionage campaign discovered when a prominent cybersecurity firm learned it had been breached.

In a rare emergency directive issued late Sunday, the Department of Homeland Security's cybersecurity arm warned of an "unacceptable risk" to the executive branch from a feared large-scale penetration of U.S. government agencies that could date back to mid-year or earlier.

"This can turn into one of the most impactful espionage campaigns on record," said cybersecurity expert Dmitri Alperovitch.

The hacked cybersecurity company, FireEye, would not say who it suspected—many experts believe the operation is Russian given the careful tradecraft—and noted that foreign governments and major corporations were also compromised.

News of the hacks, first reported by Reuters, came less than a week after FireEye disclosed that nation-state hackers had broken into its network and stolen the company's own hacking tools.

The apparent conduit for the Treasury and Commerce Department hacks—and the FireEye compromise—is a hugely popular piece of server software called SolarWinds. It is used by hundreds of thousands of organizations globally, including most Fortune 500 companies and multiple U.S. federal agencies that will now be scrambling to patch up their networks, said Alperovitch, the former chief technical officer of the cybersecurity firm CrowdStrike.

The DHS directive—only the fifth since they were created in 2015—said U.S. agencies should immediately disconnect or power down any machines running the impacted SolarWinds software.

FireEye, without naming any specific targets, said in a blog post that its investigation into the hack of its own network had identified "a global campaign" targeting governments and the private sector that, beginning in the spring, had slipped malware into a SolarWinds software update. Neither the company nor the U.S. government publicly identified Russian state-backed hackers as responsible.

The malware gave the hackers remote access to victims' networks, and Alperovitch said SolarWinds grants "God-mode" access to a network, making everything visible.

"We anticipate this will be a very large event when all the information comes to light," said John Hultquist, director of threat analysis at FireEye. "The actor is operating stealthily, but we are certainly still finding targets that they manage to operate in."

On its website, SolarWinds says it has 300,000 customers worldwide, including all five branches of the U.S. military, the Pentagon, the State Department, NASA, the National Security Agency, the Department of Justice and the White House. It says the 10 leading U.S. telecommunications companies and top five U.S. accounting firms are also among customers.

FireEye said it had confirmed infections in North America, Europe, Asia and the Middle East, including in the health care and oil and gas industry—and had been informing affected customers around the world in the past few days. It's customers include federal, state and local governments and top global corporations.

It said that malware that rode the SolarWinds update did not seed self-propagating malware—like the NotPetya malware blamed on Russia that caused more than $10 billion in damage globally—and that any actual infiltration of an infected organization required "meticulous planning and manual interaction."

That means it's a good bet only a subset of infected organizations were being spied on by the hackers. Nation-states have their cyberespionage priorities, which include COVID-19 vaccine development.

On Sunday, Russia's U.S. embassy described as "unfounded" in a post on its Facebook page the "attempts of the U.S. media to blame Russia for hacker attackes on U.S. governmental bodies."

The Treasury Department referred requests for comment to the National Security Council, whose spokesman, John Ullyot, said the government was "taking all necessary steps to identify and remedy any possible issues related to this situation."

The government's Cybersecurity and Infrastructure Security Agency said it was working with other agencies to help "identify and mitigate any potential compromises." The FBI said it was engaged in a response but declined to comment further.

President Donald Trump last month fired the director of CISA, Chris Krebs, after Krebs vouched for the integrity of the presidential election and disputed Trump's claims of widespread electoral fraud.

In a tweet Sunday, Krebs said "hacks of this type take exceptional tradecraft and time," adding that he believed that its impact was only beginning to be understood.

Federal agencies have long been attractive targets for foreign hackers looking to gain insight into American government personnel and policymaking.

Hackers linked to Russia, for instance, were able to break into the State Department's email system in 2014, infecting it so thoroughly that it had to be cut off from the internet while experts worked to eliminate the infestation. A year later, a hack at the U.S. government's personnel office blamed on China compromised the personal information of some 22 million current, former and prospective federal employees, including highly sensitive data such as background investigations.

The intrusions disclosed Sunday included the Commerce Department's agency responsible for internet and telecommunications policy. A spokesperson confirmed a "breach in one of our bureaus" and said "we have asked CISA and the FBI to investigate."

Austin, Texas-based SolarWinds confirmed Sunday a "potential vulnerability" related to updates released between March and June for software products called Orion that help monitor networks for problems.

"We believe that this vulnerability is the result of a highly-sophisticated, targeted and manual supply chain attack by a nation state," said SolarWinds CEO Kevin Thompson said in a statement. He said it was working with the FBI, FireEye and intelligence community.

FireEye announced on Tuesday that it had been hacked, saying foreign state hackers with "world-class capabilities" broke into its network and stole tools it uses to probe the defenses of its thousands of customers. The hackers "primarily sought information related to certain government customers," FireEye CEO Kevin Mandia said in a statement, without naming them.

Former NSA hacker Jake Williams, the president of the cybersecurity firm Rendition Infosec, said FireEye surely told the FBI and other federal partners how it had been hacked and they determined that Treasury had been similarly compromised.

"I suspect that there's a number of other (federal) agencies we're going to hear from this week that have also been hit," Williams added.

FireEye responded to the Sony and Equifax data breaches and helped Saudi Arabia thwart an oil industry cyberattack—and has played a key role in identifying Russia as the protagonist in numerous aggressions in the burgeoning netherworld of global digital conflict.

Mandia said there was no indication they got customer information from the company's consulting or breach-response businesses or threat-intelligence data it collects.

© 2020 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed without permission.

Citation: US agencies hacked in monthslong global cyberspying campaign (2020, December 14) retrieved 20 April 2024 from
https://techxplore.com/news/2020-12-agencies-hacked-monthslong-global-cyberspying.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.