US agencies, companies secure networks after huge hack

14 December 2020, by Ben Fox and Frank Bajak

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 and private companies rushed Monday to secure their computer networks following the disclosure of a sophisticated and long-running cyber-espionage intrusion suspected of being carried out by Russian hackers.

The full extent of the damage is not yet clear. But the potential threat was significant enough that the Department of Homeland Security's cybersecurity unit directed all federal agencies to remove compromised network management software and thousands of companies were expected to do the same.

What was striking about the operation was its potential scope as well as the manner in which the perpetrators managed to pierce cyber defenses and gain access to email and internal files at the Treasury and Commerce departments and potentially elsewhere.

The intrusion was stark evidence of the vulnerability of even supposedly secure government networks, even after well-known previous attacks.

"It's a reminder that offense is easier than defense and we still have a lot of work to do," said Suzanne Spaulding, a former U.S. cybersecurity official who is now a senior adviser at the Center for Strategic and International Studies.

The identity of the perpetrator remained unclear. A U.S. official, speaking on condition of anonymity because of an ongoing investigation, told The Associated Press on Monday that Russian hackers are suspected.

The Washington Post, citing unnamed sources, said the attack was carried out by Russian government hackers who go by the nicknames APT29 or Cozy Bear and are part of that nation's foreign intelligence service.

The intrusion came to light after a prominent cybersecurity firm, FireEye, determined it had been breached and alerted that foreign governments and major corporations were also compromised. The company did not say who it suspected, though many experts believed Russia was responsible given the level of skill involved.

A FireEye senior vice president, Charles Carmakal said the company was aware of "dozens of incredibly high-value targets that have been compromised" by the hackers and was "pro-actively helping a number of organizations respond to their intrusions."

He said he expects many more to learn in coming days that they, too, were hacked.

U.S. authorities acknowledged that federal agencies were affected by the breach on Sunday, providing few details. The Cybersecurity and Infrastructure Security Agency, known as CISA, said in an unusual directive that the widely used network software SolarWinds had been compromised and should be removed from any system using it.

The national cybersecurity agencies of Britain and Ireland issued similar alerts.

SolarWinds is used by hundreds of thousands of organizations around the world, including most Fortune 500 companies and multiple U.S. federal agencies. The perpetrators were able to embed malware in a security update issued by the company, based in Austin, Texas. Though SolarWinds estimated 18,000 customers were infected, most of the malware was not activated.

When it was, the hackers could impersonate system administrators and have total access to the infected networks.

Carmakal said the highly disciplined hackers—though they made few mistakes in masking their presence in networks—only chose targets with highly coveted information because every time they activate the tool remotely the likelihood of detection increases.

"Quite honestly, my heart sank when I saw some of the details, just the amount of information they could potentially have if they are reading everyone's emails and they are accessing sensitive files within places like Treasury or Commerce," said Ben Johnson, a former National Security Agency cyber-engineer who is now chief technology officer of software security firm Obsidian.

SolarWinds has said its customers include 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, along with the top U.S. telecommunications and accounting firms.

National Security Council spokesman John Ullyot said Monday that the Trump administration was working with CISA, U.S. intelligence agencies, the FBI and government departments affected by the intrusion to coordinate a response.

"It's obviously incredibly significant and widespread," said Chris Painter, who coordinated cyber-policy at the State Department during the Obama administration. "How much was compromised? How much was exfiltrated? There are lots of open questions now."

Kremlin spokesman Dmitry Peskov said Monday that Russia had "nothing to do with" the hack.

"Once again, I can reject these accusations," Peskov told reporters. "If for many months the Americans couldn't do anything about it, then, probably, one shouldn't unfoundedly blame the Russians for everything."

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.

Cybersecurity experts said the goal of the months-long effort appeared to be espionage and not profit or inflicting damage.

In terms of scale alone, the operation seems similar to the 2105 Office of Personnel Management hack that authorities blame on the Chinese government, said Ben Buchanan, a Georgetown University cyber-espionage expert.

"These operators are experienced and capable, adept at finding a systemic weakness and then exploiting it quietly for months," said Buchanan, author of "The Hacker and The State."

Members of Congress were pressing the government for more information. "If reports are true and state-sponsored hackers successfully snuck malware-riddled software into scores of federal government systems, our country has suffered a massive national security failure that could have ramifications for years to come," said Sen. Ron Wyden, an Oregon Democrat who is a prominent voice on cyber issues.

If it was carried out by a foreign government, and the U.S. has the proof, then it becomes a question of what to do about it.

Some obvious options would include expelling diplomats of the offending country, imposing sanctions or filing criminal charges for cyber-espionage, steps that Washington and the European Union have taken against Russia in the past.

"I'm sure that the departments like NSA and Cyber Command are coming up with options, that the Treasury Department is looking at sanction options, that the State Department is looking for how they will send a strong signal," Spaulding said. "Whether they will get approval for all these things from the White House remains to be seen."

In the meantime, SolarWinds and its many private-sector clients were working to close any breaches and repair the damage.

The company said in a financial filing that it believed fewer than 18,000 customers installed the compromised product update earlier this year.

"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.