EXPLAINER: How bad is the hack that targeted US agencies?

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

Hack attack. Wikipedia, CC BY-SA

Governments and major corporations worldwide are scrambling to see if they, too, were victims of a global cyberespionage campaign that penetrated multiple U.S. government agencies and involved a common

software product used by thousands of organizations. Russia, the prime suspect, denies involvement. Cybersecurity investigators said the hack's impact extends far beyond the affected U.S. agencies, which include the Treasury and Commerce departments, though they haven't disclosed which companies or what other governments were targeted.

___

WHAT HAPPENED?

The hack began as early as March when malicious code was snuck into updates to popular software that monitors computer networks of businesses and governments. The malware, affecting a product made by U.S. company SolarWinds, gave elite hackers remote access into an organization's networks so they could steal information. It wasn't discovered until the prominent cybersecurity company FireEye determined it had been hacked. Whoever broke into FireEye was seeking data on its government clients, the company said—and made off with hacking tools it uses to probe its customers' defenses.

"There's no evidence that this was meant to be destructive," said Ben Buchanan, Georgetown University cyberespionage expert and author of "The Hacker and The State." He called the campaign's scope, "impressive, surprising and alarming."

Its apparent monthslong timeline gave the hackers ample time to extract information from a lot of different targets. Buchanan compared its magnitude to the 2015 Chinese hack of the U.S. Office of Personnel Management, in which the records of 22 million federal employees and government job applicants were stolen.

FireEye executive Charles Carmakal said the company was aware of "dozens of incredibly high-value targets" compromised" by the hackers

and was helping "a number of organizations respond to their intrusions." He would not name any, and said he expected many more to learn in coming days that they, too, were infiltrated.

___

WHAT IS SOLARWINDS?

SolarWinds, of Austin, Texas, provides network-monitoring and other technical services to hundreds of thousands of organizations around the world, including most Fortune 500 companies and government agencies in North America, Europe, Asia and the Middle East.

Its compromised product, called Orion, accounts for nearly half SolarWinds' annual revenue. The company's revenue totaled $753.9 million over the first nine months of this year. Its centralized monitoring looks for problems in an organization's computer networks, which means that breaking in gave the attackers a "God-view" of those networks.

SolarWinds, whose stock fell 17% on Monday, said in a financial filing that it sent an advisory to about 33,000 of its Orion customers that might have been affected, though it estimated a smaller number of customers—fewer than 18,000—had actually installed the compromised product update earlier this year.

FireEye described the malware's dizzying capabilities—from initially lying dormant up to two weeks, to hiding in plain sight by masquerading its reconnaissance forays as Orion activity.

___

WAS MY WORKPLACE AFFECTED?

Neither SolarWinds nor U.S. cybersecurity authorities have publicly identified which organizations were breached. Just because a company or agency uses SolarWinds as a vendor doesn't necessarily mean they were vulnerable to the hacking. The malware that opened remote-access backdoors was injected into SolarWinds' Orion product updates released between March and June, but not every customer installed them.

The hackers would have also had to want to target the organization. Hacking on their level is expensive and the disciplined intruders only they chose targets with highly coveted information because the risk of being detected rose any time they activated the malware, said FireEye's Carmakal.

The so-called supply-chain method used to distribute the malware via SolarWinds' software recalled the technique Russian military hackers used in 2016 to infect companies that do business in Ukraine with the hard drive-wiping NotPetya virus—the most damaging cyberattack to date. In that case, the hackers inserted a self-propagating worm into a tax preparation software company's updates to infect its customers. In this case, any actual infiltration of an infected organization required "meticulous planning and manual interaction," according to FireEye.

—

WHO IS RESPONSIBLE?

SolarWinds said it was advised that an "outside nation state" infiltrated its systems with malware. Neither the U.S. government nor the affected companies have publicly said which nation state they think is responsible.

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. Russia said Monday it had "nothing to do with" the hacking.

"Once again, I can reject these accusations," Kremlin spokesman Dmitry 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."

Buchanan, the Georgetown expert, said the hackers were "adept at finding a systemic weakness and then exploiting it quietly for months." Supporting the consensus in the cyberthreat analysis community that Russians are responsible are the tactics, techniques and procedures used, which bear their digital fingerprints, said Brandon Valeriano, a Marine Corps University technology scholar.

___

WHAT CAN BE DONE TO PREVENT AND COUNTERACT SUCH HACKS?

Espionage does not its violate international law—and cyber defense is hard. But retaliation against governments responsible for egregious hacks happens. Diplomats can be expelled. Sanctions can be imposed. The Obama administration expelled Russian diplomats in retaliation for the meddling of Kremlin military hackers in Donald Trump's favor in the 2016 election. Cybersecurity "has not been a presidential priority" during the Trump administration and the outgoing president has been unable or unwilling to hold Russia to account for aggressive action in cyberspace, said Chris Painter, who coordinated cyberpolicy in the State Department during the Obama administration.

"I think that contributes to Russia's bravado," he said. The incoming Biden national security team has indicated it will be less tolerant, and is

expected to restore the position of the White House cybersecurity coordinator eliminated by Trump.

The greater White House cybersecurity focus will be crucial, industry experts say.

An advisory issued by Microsoft, which assisted FireEye in the hack response, said it had "delivered more than 13,000 notifications to customers attacked by nation states over the past two years and observed a rapid increase in (their) sophistication and operational security capabilities."