Little-known SolarWinds gets scrutiny over hack, stock sales

December 16 2020, by Matt O'brien

This Tuesday, Aug. 4, 2009, file photo shows the United States Chamber of Commerce building in Washington. Elite cyber spies have spent months secretly exploiting SolarWinds software to peer into computer networks, putting many of the company's highest-profile customers in national governments, including the U.S. Treasury and Commerce departments, and Fortune 500 companies on high alert. (AP Photo/Manuel Balce Ceneta, File)

Before this week, few people were aware of SolarWinds, a Texas-based

software company providing vital computer network monitoring services to major corporations and government agencies worldwide.

But the revelation that elite cyber spies have spent months secretly exploiting SolarWinds' software to peer into computer networks has put many of its highest-profile customers in national governments and Fortune 500 companies on high alert. And it's raising questions about whether company insiders knew of its security vulnerabilities as its biggest investors sold off stock.

Founded in 1999 by two brothers in Tulsa, Oklahoma, ahead of the feared turn-of-the-millennium Y2K computer bug, the company's website says its first product "arrived on the scene to help IT pros quell everyone's world-ending fears."

This time, its products are the ones instilling fears. The company on Sunday began alerting about 33,000 of its customers that an "outside nation state"—widely suspected to be Russia—injected malicious code into some updated versions of its premier product, Orion. The ubiquitous software tool, which helps organizations monitor the performance of their computer networks and servers, had become an instrument for spies to steal information undetected.

"They're not a household name the same way that Microsoft is. That's because their software sits in the back office," said Rob Oliver, a research analyst at Baird who has followed the company for years. "Workers could have spent their whole career without hearing about SolarWinds. But I guarantee your IT department will know about it."

Now plenty of other people know about it, too. One of SolarWinds' customers, the prominent cybersecurity firm FireEye, was the first to detect the cyberespionage operation, and began notifying other victims. Among other revealed spying targets were the U.S. departments of

Treasury and Commerce.

But the Trump administration has been silent on what other agencies were breached. And that wasn't sitting well with some members of Congress.

"Stunning," tweeted Sen. Richard Blumenthal, a Connecticut Democrat. He said a Senate Armed Services Committee classified briefing Tuesday "on Russia's cyberattack left me deeply alarmed, in fact downright scared. Americans deserve to know what's going on."

"Declassify what's known & unknown," he demanded.

The Department of Homeland Security directed all federal agencies to remove the compromised software on Sunday night and thousands of companies were expected to do the same. The Pentagon said in a statement Wednesday that it had so far found "no evidence of compromise" on its classified and unclassified networks from the "evolving cyber incident."

The NSA, DHS and FBI briefed the House Intelligence Committee Wednesday on what was widely considered a serious intelligence failure, and Democratic Sen. Dick Durbin told CNN "this is virtually a declaration of war by Russia on the United States, and we should take that seriously."

Among business sectors scrambling to protect their systems and assess potential theft of information were the electric power industry, defense contractors and telecommunications firms.

The breach took the air out of SolarWinds, which is now based in the hilly outskirts of Austin, Texas. The compromised product accounts for nearly half the company's annual revenue, which totaled $753.9 million

over the first nine months of this year. Its stock has plummeted 23% since the beginning of the week.

Moody's Investors Service said Wednesday it was looking to downgrade its rating for the company, citing the "potential for reputational damage, material loss of customers, a slowdown in business performance and high remediation and legal costs."

SolarWinds' longtime CEO, Kevin Thompson, had months earlier indicated that he would be leaving at the end of the year as the company explored spinning off one of its divisions. The SolarWinds board appointed his replacement, current PulseSecure CEO Sudhakar Ramakrishna, on Dec. 7, according to a financial filing, a day before FireEye first publicly revealed the hack on its own system and two days before the change of CEOs was announced.

It was also on Dec. 7 that the company's two biggest investors, Silver Lake and Thoma Bravo, which control a majority stake in the publicly traded company, sold more than $280 million in stock to a Canadian public pension fund. The two private equity firms in a joint statement said they "were not aware of this potential cyberattack" at the time they sold the stock. FireEye disclosed the next day that it had been breached.

The hacking operation began at least as early as March when SolarWinds customers who installed updates to their Orion software were unknowingly welcoming hidden malicious code that could give intruders the same view of their corporate network that in-house IT crews have. 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.

FireEye said Wednesday that it had identified a "killswitch" that prevents the malware used by the hackers from operating. But while that

disables the original backdoor, it won't remove intruders from systems where they created different ways of remotely accessing victimized networks.

SolarWinds executives declined interviews through a spokesperson, who cited an ongoing investigation into the hacking operation that involves the FBI and other agencies.

Thompson's last few weeks at the helm are likely to be spent responding to frightened customers, some of them rankled about marketing tactics that might have made a target of SolarWinds and its highest-profile clients.

The company earlier this week took down a web page that boasted of dozens of its best-known customers, from the White House, Pentagon and the Secret Service to the McDonald's restaurant chain and Smithsonian museums. The Associated Press is among customers, though the news agency said it did not use the compromised Orion products.

SolarWinds estimated in a financial filing that about 18,000 customers had installed the compromised software. And while that made them vulnerable to spy operations, security experts say its unlikely the hackers penetrated the vast majority. Spies tend to have narrow interest in such operations. Dozens of "high-value targets" in government and industry were compromised, said FireEye, without naming them. It said it has confirmed infections in North America, Europe, Asia and the Middle East to governments, consulting firms and the health care, technology, telecommunications and oil and gas industries—and has been informing affected organizations around the world.

Stanford University cybersecurity expert Alex Stamos said there aren't nearly enough qualified threat hunters globally to scour potentially

infected organizations for hidden malware from the operation.

"We are going to be reaping an 'iron harvest' of second-stage malware for years from this one," he tweeted, a reference to unexploded World War II bombs that continue to be found in Europe three-quarters of century later.