Cybersecurity

SolarWinds Adviser Warned of Lax Security Years Before Hack

By Ryan Gallagher
December 21, 2020, 10:01 AM CST

- Cybersecurity researchers also cite several security lapses
- Texas company's software targeted by suspected Russian hackers

Photographer: TRIPPLAAR KRISTOFFER/SIPA/AP

A former security adviser at the IT monitoring and network management company SolarWinds Corp. said he warned management of cybersecurity risks and laid out a plan to improve it that was ultimately ignored.

In a 23-page PowerPoint presentation reviewed by Bloomberg News, Ian Thornton-Trump recommended to company executives in 2017 that SolarWinds appoint a senior director of cybersecurity, and said he told them that "the survival of the company depends on an

internal commitment to security."

The following month, he terminated his relationship with the company, saying he believed its leadership wasn't interested in making changes that would have "meaningful impact."

Thornton-Trump, as well as a former SolarWinds software engineer who talked to Bloomberg News, said that given the cybersecurity risks at the company, they viewed a major breach as inevitable. Their concerns about SolarWinds are shared by several cybersecurity researchers, who discovered what they described as glaring security lapses at the company, whose software was used in a suspected Russian hacking campaign.

"My belief is that from a security perspective, SolarWinds was an incredibly easy target to hack," said Thornton-Trump, now the chief information security officer at threat intelligence firm Cyjax Ltd.

Last week, the Austin, Texas-based SolarWinds found itself at the center of the largest cybersecurity attack in recent memory. Suspected Russian hackers breached the internal networks of at least 200 customers, including U.S. government agencies and an as-yet-unknown number of private companies, a cybersecurity firm and people familiar with the investigation told Bloomberg.

In an operation that cybersecurity experts have described as exceedingly sophisticated and hard to detect, the hackers installed malicious code in updates to SolarWinds's widely used Orion software, which was sent to as many as 18,000 customers.

Read More: At Least 200 Victims Identified in Suspected Russian Cyber-Attack

The malicious code provided the hackers access to the customers' computer networks and, as clients around the world continue to comb their systems for signs of the Russian hackers, the list of victims is expected to grow.

In a statement posted on the SolarWinds website on Friday, Kevin Thompson, the company's chief executive officer, said that the company's top priority was "to ensure that our and our customers' environments are secure."

"Security and trust in our software are the foundations of our commitment to our customers," he said. "We strive to implement and maintain appropriate safeguards, processes, and procedures designed to protect our customers."

'Collaborating Closely'

Responding to Bloomberg News' questions about the 2017 presentation and other security issues identified by researchers, a SolarWinds spokesperson said in a statement, "Our top priority is our work with our customers, our industry partners and government agencies to determine whether a foreign government orchestrated this attack, best understand its full scope, and to help address any customer needs that develop. We are doing this work as quickly and transparently as possible. There will be plenty of time to look back and we plan to do that in a similarly transparent way."

In addition, the company said it is collaborating with law enforcement and "will continue gathering all relevant information to ensure an incident like this does not happen again."

Thornton-Trump was working at LogicNow, a U.K.-based cloud computing company, when it was acquired by SolarWinds in June 2016. With nearly two decades of experience in cybersecurity, Thornton-Trump said he helped LogicNow build its brand in the security market.

The security adviser delivered the 2017 PowerPoint to at least three SolarWinds executives, on both the marketing and technology sides of the company, he said.

Thornton-Trump said that in his experience SolarWinds didn't put enough investment into building a cybersecurity culture within the company. In an email explaining his reasons for leaving that he sent to a SolarWinds executive on May 15, 2017, which was seen by Bloomberg

News, Thornton-Trump said that he'd "lost faith in the leadership" of the company, who he said appeared "unwilling to make the corrections" he believed were necessary to continue support for the security brand he had built at LogicNow.

"There was a lack of security at the technical product level, and there was minimal security leadership at the top," Thornton-Trump said in an interview. "We knew in 2015 that hackers were looking for any route into a business. But SolarWinds did not adapt. That's the tragedy. There were plenty of lessons to learn, but SolarWinds wasn't paying attention to what was going on."

About two months after Thornton-Trump left SolarWinds, the company recruited Tim Brown, a former chief technology officer at Dell Security, to take on the position of vice president of security architecture. In an interview with a trade publication last year, Brown said that he was working to secure SolarWinds's systems from attack. "We test our incident response process every day -- in case something happens to us from the outside that is major," he said. "We have been lucky, and it's great." When companies are hacked, Brown added, it was often their own fault. "If you look at the attacks that have been successful, most of them have been silly mistakes," he said.

A former SolarWinds employee, who worked as a software engineer at one of the company's U.S. offices, said SolarWinds appeared to prioritize the development of new software products over internal cybersecurity defenses. The employee, who requested anonymity due to having signed a non-disclosure agreement, said it wasn't uncommon for some of the company's computer systems to be operating out-of-date web browsers and operating systems, which could make them more vulnerable to hackers.

Cybersecurity researchers also said they've discovered flaws with SolarWinds's security practices.

One of them, Vinoth Kumar, said he notified SolarWinds in 2019 that the password to one of its servers had leaked online. The password, according to Kumar, was "solarwinds123." SolarWinds told Kumar that the password had been visible due to a "misconfiguration," and removed it.

In addition, until recently SolarWinds advised its customers on its website to disable virus scanning for Orion platform products so those products could run more efficiently, according to several cybersecurity researchers who posted about it on Twitter. The SolarWinds's web

page has subsequently been removed from public view.

Jake Williams, a former hacker for the U.S. National Security Agency who is now president of cybersecurity firm Rendition Infosec, said technology companies such as SolarWinds that build and produce computer code often "don't do security well."

"Security is a cost center, not a profit center," Williams said. "I think that probably has a lot to do with it. An underlying problem at SolarWinds has probably crept in through some missing security best practice."

Even if SolarWinds had robust cybersecurity practices, however, it might not have deterred the alleged Russian hackers, who U.S. authorities described as highly skilled, patient and well resourced, demonstrating "complex tradecraft" in their attacks.

"The reality is that sophisticated threat actors, no matter how good the defenses, will eventually succeed," said Costin Raiu, director of global research and analysis at the cybersecurity firm Kaspersky. "If the cost justifies the effort, the breach will happen."

Success in Obscurity

Though it isn't a household name, SolarWinds's software is popular in IT departments in the U.S. and elsewhere, with more than 320,000 customers, providing technology that monitors the performance of computers within a network. Company officials appear to be content with maintaining a low profile. "We operate behind the scenes," said John Pagliuca, president of SolarWinds's managed service providers division, during an October earnings call. "We've thrived under relative obscurity."

Since it was founded in 1999, SolarWinds and its partners have been awarded contracts with the U.S. government worth more than $230 million, according to sales records reviewed by Bloomberg News. Its software is ubiquitous among federal government agencies. The U.S. military, the FBI, the Secret Service, the National Nuclear Security Administration, Veterans Affairs, and the Department of Homeland Security are among those to have purchased SolarWinds's software, the records show.

The software had been approved for use in the U.S. government. In August 2019, for instance, a version of the Orion software was signed off for use by the Defense Information Systems

Agency, which tests software for cybersecurity issues.

According to SolarWinds, its Orion platform generates 45% of the company's revenue.

Disclosure of the attack came at the end of a year with several financial milestones for SolarWinds. In the second quarter, the company closed the largest commercial deal in its history, and its annual revenue was expected to top $1 billion for the first time, according to its third-quarter results.

Despite the economic uncertainty caused by the Covid-19 pandemic, sales were growing, according to company records.

SolarWinds gained a foothold in the government marketplace many years ago because it was regarded as "idiot proof," and was the first software of its kind, said Williams, the former NSA hacker. "Orion is to network management systems what Kleenex is to tissue," he said. "Other products are laughably complex and bad by comparison. It was the first actually easy-to-use network management system, and took off like wildfire as a result."

After 14 years at SolarWinds, Thompson, the CEO, is due to retire on Dec. 31. Participating in his final earnings call in October, he said his farewells to colleagues and investors, not realizing what was on the horizon. "We're still the best story in software," Thompson said. "Keep believing, as there's still a lot of special things left to accomplish at SolarWinds."

In the past week, since the suspected Russian hack was first reported, shares in SolarWinds have shed 40% of their value, closing Friday at $14.18 to round out a five-day losing streak. Friday's 19% decline was the biggest one-day decline since October 2018.

In this article

SWI
SOLARWINDS CORP
15.91 USD ▼ -0.21 -1.30%

TWTR
TWITTER INC
54.96 USD ▲ +0.32 +0.59%

DELL
DELL TECHN-C

73.30 USD ▲ +0.24 +0.33%

AONE
ONE - CLASS A
10.50 USD ▼ -0.01 -0.05%