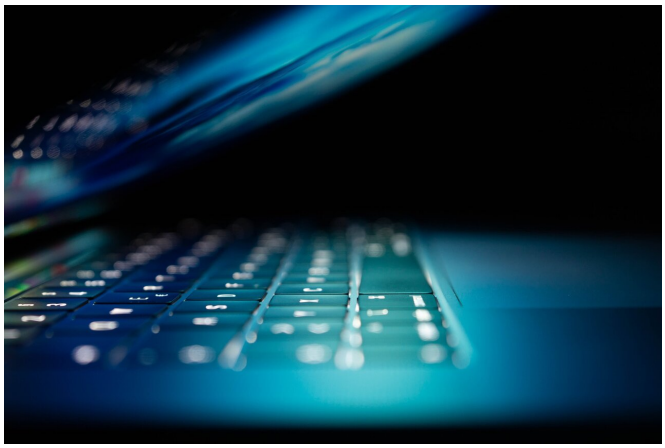
SolarWinds breach could reshape cybersecurity practices

4 January 2021, by Kara Carlson



Credit: Unsplash/CC0 Public Domain

As investigations continued into the massive data breach linked to Austin-based software company SolarWinds, experts say the attack could lead to long-term changes in cybersecurity policies and procedures for government entities and private companies alike.

News of the cyberattack broke on Dec. 13, with Reuters news service reporting that a sophisticated hacking group backed by a foreign government might have stolen information from U.S. government agencies, including email traffic. The breach appears to have affected nearly every level of government, as well as potentially hundreds of private companies.

As many as 18,000 SolarWinds customers—out of a total of 300,000—might have been running SolarWinds software containing a vulnerability that allowed hackers to penetrate various networks.

The Homeland Security Department's Cybersecurity and Infrastructure Security Agency has called the hack a grave risk to government and private networks, and experts say the damage will be difficult to detect and undo.

So far, the investigation has revealed a number of high-profile targets of the attack, including the Department of Treasury, Homeland Security, the Department of Energy and Microsoft.

While federal government officials have yet to say who they believe is responsible, The Washington Post, citing unnamed sources, reported that 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.

Daniel Ives, an analyst with Wedbush Securities, said the attack is the among the largest breaches in U.S history, and that it could take years to fully understand the full extent of the attack, which has "broad ramifications" going forward, he said.

"This scale, the scope of this attack is jaw-dropping," Ives said. "I think how pervasive potentially (the hackers) got within the confines of the government and enterprises is a major wakeup call."

SolarWinds finds itself caught in the middle of an escalating cyberwar and a broader scale of supply chain attacks, in which another company could have just as likely ended up the target, Ives said. SolarWinds, which makes network and IT management software, has more than 3,000 global employees. It was founded in 1999 and moved to Central Texas in 2006.

The hackers are believed to have made their way into a number of systems by tampering with an update server of the SolarWinds network management systems. Through it, the hackers were able to gain remote access and insert malicious code that hitched a ride on a software update.

SolarWinds has released a number of software updates to patch the problem. Reuters also reported a possible second breach around the same time in the SolarWinds system, which also has since been patched.

In a written statement, the company said it is working closely with federal law enforcement and intelligence agencies to investigate the attack and whether it was backed by a foreign government. The company said it is also working with third-party cybersecurity experts.

"We are solely focused on helping the industry and our customers understand and mitigate this attack, and quickly released hotfix updates to customers that we believe will close the vulnerability. While our investigation is ongoing, we are committed to being transparent with our customers and will continue taking all appropriate steps to protect them," the company said.

Widespread implications

The attack could have widespread implications for the cybersecurity industry at large, as companies and the government have become increasingly reliant on online and cloud systems. Gartner, an organization that researches technology industry trends, predicted cybersecurity spending would reach about $123.8 billion this year.

Ives said the number of cyberattacks are growing, as is their level of sophistication.

"It speaks to a cyberwar, cyberespionage, that's been going on for a number of years but it's continuing to get ratcheted up," Ives said.

Ives said this particular breach is a concern for both the amount of time it might have gone undetected and its pervasiveness. It's a "nightmare situation," he said.

"SolarWinds was the target of this attack. The next attack it could be another software," Ives said. " As much as this is a black eye for the industry, I think it's more the fear of what this means in terms of a supply chain attack, going through the front door versus the back door."

Ives said he also thinks SolarWinds has the ability to bounce back and recover its reputation after the attack. He said the company has worked fast and been transparent throughout the aftermath of the attack.

"This is going to be a chapter in history in terms of the supply chain book," Ives said. "But SolarWinds didn't get to where they are today by not being aggressive and a global brand in terms of IT management software. It's a dark chapter, but it's how they navigate that chapter."

'Like bed bugs'

Cybersecurity experts said it's not possible to fully know yet if all the hackers' access points have been removed from the systems they breached, on both the government and business level.

"It's a little bit like bed bugs," said David Springer, an Austin-based lawyer for Bracewell LLP who specializes in securities litigation including cybersecurity counseling and policy. "You can do a lot to try to eradicate them, but sometimes the problem gets so bad, and they're just so into everything you kind of have to just burn your mattress. And that's kind of where we find ourselves here."

Springer said it has become clear that once in these systems, the hackers moved around the network and breached a number of systems.

"Fixing SolarWinds is preventing another attack to get in that way, but it doesn't do anything to take the hackers off the network. They're already there, and now have enabled multiple other entry and exit points," Springer said.

Springer said the breach has renewed conversations about cybersecurity and better steps for transparency, security and securing networks. That includes supply chain security and making sure that when the government or large corporations acquire software or updates, there is increased transparency about what's in that software package, and having the ability to audit what's in there to ensure it hasn't been altered, he said. There's also a renewed focus on internal

security programs.

"A lot of times, historically, you view securing a network as a perimeter defense. The vast majority of defending you do is at the perimeter. You're just trying to keep that guy out of your network. But then once something is happening inside your network, it's kind of presumed to be OK," Springer said. "Within a network, there's not a ton of security internally. There's definitely a renewed focus on within network."

From a government perspective, Springer said he expects there to be stricter security mandates considered for the vendors that government agencies use.

"There needs to be a maintained focus on ensuring ... that the private companies are doing the right things from a security point of view, that it doesn't become the way that attackers are going to constantly get into government networks, just by penetrating these people were supplying software to it," Springer said.

The same applies to private companies. Ives predicted the average company will be spending more on cybersecurity in the next year, a pattern that has only been sped up by the breach.

"Security has to stay one step ahead of the bad actors," Ives said. "In this case, it didn't. I think the industry learns from it, adjusts and just gets further blockades going forward, both within the confines of an organization as well as within the cloud."