SOLARWINDS HACK

SolarWinds attack explained: And why it was so hard to detect

A group believed to be Russia's Cozy Bear gained access to government and other systems through a compromised update to SolarWinds' Orion software. Most organizations aren't prepared for this sort of software supply chain attack.

By Lucian Constantin
CSO Senior Writer, CSO

15 DECEMBER 2020 22:44 AEDT

The recent breach of major cybersecurity company FireEye by nation-state hackers was part of a much larger attack that was carried out through malicious updates to a popular network monitoring product and impacted major government organizations and companies. The incident highlights the severe impact software supply chain attacks can have and the unfortunate fact that most organizations are woefully unprepared to prevent and detect such threats.

A hacker group believed to be affiliated with the Russian government gained access to computer systems belonging to multiple US government departments including the US Treasury and Commerce in a long campaign that is believed to have started in March. The news triggered an emergency meeting of the US National Security Council on Saturday.

The attack involved hackers compromising the infrastructure of SolarWinds, a company that produces a network and applications monitoring platform called Orion, and then using that access to produce and distribute trojanized updates to the software's users. On a page on its website that was taken down after news broke out, SolarWinds stated that its customers included 425 of the US Fortune 500, the top ten US telecommunications companies, the top five US accounting firms, all branches of the US Military, the Pentagon, the State Department, as well as hundreds of universities and colleges worldwide.

The SolarWinds software supply chain attack also allowed hackers to access the network of US cybersecurity firm FireEye, a breach that was announced last week. Even though FireEye did not name the group of attackers responsible, the Washington Post reports it is APT29 or Cozy Bear, the hacking arm of Russia's foreign intelligence service, the SVR.

"FireEye has detected this activity at multiple entities worldwide," the company said in an advisory Sunday. "The victims have included government, consulting, technology, telecom and extractive entities in North America, Europe, Asia and the Middle East. We anticipate there are additional victims in other countries and verticals. FireEye has notified all entities we are aware of being affected."

The malicious Orion updates

The software builds for Orion versions 2019.4 HF 5 through 2020.2.1 that were released between March 2020 and June 2020 might have contained a trojanized component. However, FireEye noted in its analysis that each of the attacks required meticulous planning and manual interaction by the attackers.

The attackers managed to modify an Orion platform plug-in called SolarWinds.Orion.Core.BusinessLayer.dll that is distributed as part of Orion platform updates. The trojanized component is digitally signed and contains a backdoor that communicates with third-party servers controlled by the attackers. FireEye tracks this component as SUNBURST and has released open-source detection rules for it on GitHub.

"After an initial dormant period of up to two weeks, it retrieves and executes commands, called 'Jobs,' that include the ability to transfer files, execute files, profile the system, reboot the machine, and disable system services," the FireEye analysts said. "The malware masquerades its network traffic as the Orion Improvement Program (OIP) protocol and stores reconnaissance results within legitimate plugin configuration files allowing it to blend in with legitimate SolarWinds activity. The backdoor uses multiple obfuscated blocklists to identify forensic and anti-virus tools running as processes, services, and drivers."

The attackers kept their malware footprint very low, preferring to steal and use credentials to perform lateral movement through the network and establish legitimate remote access. The backdoor was used to deliver a lightweight malware dropper that has never been seen before and which FireEye has dubbed TEARDROP. This dropper loads directly in memory and does not leave traces on the disk. Researchers believe it was used to deploy a customized version of the Cobalt Strike BEACON payload. Cobalt Strike is a commercial penetration testing framework and post-exploitation agent designed for red teams that has also been adopted and used by hackers and sophisticated cybercriminal groups.

To avoid detection, attackers used temporary file replacement techniques to remotely execute their tools. This means they modified a legitimate utility on the targeted system with their malicious one, executed it, and then replaced it back with the legitimate one. A similar technique involved the temporary modification of system scheduled tasks by updating a legitimate task to execute a malicious tool and then reverting the task back to its original configuration.

"Defenders can examine logs for SMB sessions that show access to legitimate directories and follow a delete-create-execute-delete-create pattern in a short amount of time," the FireEye researchers said. "Additionally, defenders can monitor existing scheduled tasks for temporary updates, using frequency analysis to identify anomalous modification of tasks. Tasks can also be monitored to watch for legitimate Windows tasks executing new or unknown binaries."

This is some of the best operational security exhibited by a threat actor that FireEye has ever observed, being focused on detection evasion and leveraging existing trust relationships. However, the company's researchers believe these attacks can be detected through persistent defense and have described multiple detection techniques in their advisory.

SolarWinds advises customers to upgrade to Orion Platform version 2020.2.1 HF 1 as soon as possible to ensure they are running a clean version of the product. The company also plans to release a new hotfix 2020.2.1 HF 2 on Tuesday that will replace the compromised component and make additional security enhancements.

The US Department of Homeland Security has also issued an emergency directive to government organizations to check their networks for the presence of the trojanized component and report back.

No easy solution

Software supply-chain attacks are not a new development and security experts have been warning for many years that they are some of the hardest type of threats to prevent because they take advantage of trust relationships between vendors and customers and machine-to-machine communication channels, such as software update mechanisms that are inherently trusted by users.

Back in 2012, researchers discovered that the attackers behind the Flame cyberespionage malware used a cryptographic attack against the MD5 file hashing protocol to make their malware appear as if it was legitimately signed by Microsoft and distribute it through the Windows Update mechanism to targets. That wasn't an attack where the software developer itself, Microsoft, was compromised, but the attackers exploited a vulnerability in the Windows Update file checking demonstrating that software update mechanisms can be exploited to great effect.

In 2017, security researchers from Kaspersky Lab uncovered a software supply-chain attack by an APT group dubbed Winnti that involved breaking into the infrastructure of NetSarang, a company that makes server management software, which allowed them to distribute trojanized versions of the product that were digitally signed with the company's legitimate certificate. That same group of attackers later broke into the development infrastructure of Avast subsidiary CCleaner and distributed trojanized versions of the program to over 2.2 million users. Last year, attackers hijacked the update infrastructure of computer manufacturer ASUSTeK Computer and distributed malicious versions of the ASUS Live Update Utility to users.

"I don't know of any organization that incorporates what a supply chain attack would look like in their environment from a threat modeling perspective," David Kennedy, former NSA hacker and founder of security consulting firm TrustedSec, tells CSO. "When you look at what happened with SolarWinds, it's a prime example of where an attacker could literally select any target that has their product deployed, which is a large number of companies from around the world, and most organizations would have no ability to incorporate that into how they would respond from a detection and prevention perspective. This is not a discussion that's happening in security today."

While software that is deployed in organizations might undergo security reviews to understand if their developers have good security practices in the sense of patching product vulnerabilities that might get exploited, organizations don't think about how that software could impact their infrastructure if its update mechanism is compromised, Kennedy says. "It's something that we're still very immature on and there's no easy solution for it, because companies need software to run their organizations, they need technology to expand their presence and remain competitive, and the organizations that are providing this software don't think about this as a threat model either."

Kennedy believes it should start with software developers thinking more about how to protect their code integrity at all times but also to think of ways to minimize risks to customers when architecting their products.

"A lot of times you know when you're building software, you think of a threat model from outside in, but you don't always think from inside out," he said. "That's an area a lot of people need to be looking at: How do we design our architecture infrastructure to be more resilient to these types of attacks? Would there be ways for us to stop a lot of these attacks by minimizing the infrastructure in the [product] architecture? For example, keeping SolarWinds Orion in its own island that allows communications for it to function properly, but that's it. It's good security practice in general to create as much complexity as possible for an adversary so that even if they're successful and the code you're running has been compromised, it's much harder for them to get access to the objectives that they need."

Companies, as users of software, should also start thinking about applying zero-trust networking principles and role-based access controls not just to users, but also to applications and servers. Just as not every user or device should be able to access any application or server on the network, not every server or application should be able to talk to other servers and applications on the network. When deploying any new software or technology into their networks, companies should ask themselves what could happen if that product gets compromised because of a malicious update and try to put controls in place that would minimize the impact as much as possible.

It's likely that the number of software supply-chain attacks will increase in the future, especially as other attackers see how successful and wide ranging they can be. The number of ransomware attacks against organizations exploded after the WannaCry and NotPetya attacks of 2017 because they showed to attackers that enterprise networks are not as resilient as they thought against such attacks. Since then many cybercrime groups have adopted sophisticated techniques that often put them on par with nation-state cyberespionage actors.

Ransomware gangs have also understood the value of exploiting the supply chain and have started hacking into managed services providers to exploit their access into their customers' networks. NotPetya itself had a supply chain component because the ransomware worm was initially launched through the backdoored software update servers of an accounting software called M.E.Doc that is popular in Eastern Europe.

Both organized crime and other nation-state groups are looking at this attack right now as "Wow, this is a really successful campaign," Kennedy said. From a ransomware perspective, if they simultaneously hit all the organizations that had SolarWinds Orion installed, they could have encrypted a large percentage of the world's infrastructure and made off with enough money that they wouldn't have ever had to work again. "They probably know their sophistication level will need to be increased a bit for these types of attacks, but it's not something that is too far of a stretch, given the progression we're seeing from ransomware groups and how much money they're investing in development. So, I definitely think that we can see this with other types of groups [not just nation states] for sure."

More on cyberattacks:

- **Recent cyberattacks show disturbing trends**
- **11 types of hackers and how they will harm you**
- **5 signs you've been hit with an APT**

Next read this

- *The 10 most powerful cybersecurity companies*
- *7 hot cybersecurity trends (and 2 going cold)*
- *The Apache Log4j vulnerabilities: A timeline*
- *Using the NIST Cybersecurity Framework to address organizational risk*
- *11 penetration testing tools the pros use*

Lucian Constantin is a senior writer at CSO, covering information security, privacy, and data protection.

Follow

7 hot cybersecurity trends (and 2 going cold)