WHITE PAPER

SolarWinds: Anatomy of a Supersonic Supply Chain Attack

Venafi

Introduction

The attack on SolarWinds and JetBrains has ushered in a new generation of software supply chain attacks. While supply chain attacks are not new, this attack is already one of the most wide-reaching and sophisticated cyberattacks ever seen.

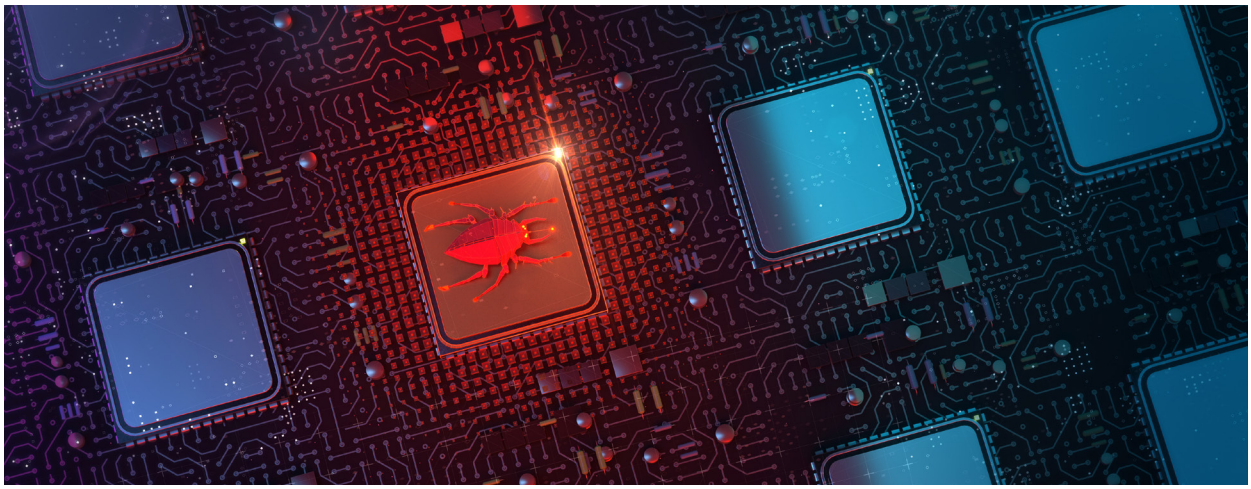
The attack required extremely high levels of sophistication, stealth and painstaking planning of every detail in order to avoid detection. It involves compromises of multiple companies, including many of the top U.S. software companies, which were then used to gain backdoors to the customers of these organizations. The ultimate targets were carefully selected, and the attacks targeting them were carefully tailored using multiple tools and a range of novel attack methods.

One common element used repeatedly throughout the entire attack lifecycle was the leverage of legitimate and trusted machine identities. These critical security assets, which include code signing keys and certificates used to sign code as well as SAML tokens, allowed attackers to maintain a low profile, bypass security controls, pivot across networks and gain trusted access to key assets. The massive compromises resulting from the SolarWinds/JetBrains attack would not have been possible without the successful use of forged or compromised machine identities that allowed the adversaries to elevate privileges, access data and services and maintain a low profile for the entire attack lifecycle.

Using legitimate, trusted machine identities allowed the attackers who had gained access to SolarWinds' software build environment to sign a poisoned software update that was released to over 18,000 SolarWinds customers around the globe. At this time there is no direct evidence that the attackers used SolarWinds' code signing materials to sign other malware or tools, but this remains a possibility. Taking into consideration the adversaries' level of sophistication, it is possible SolarWinds' code signing materials could have been stolen as part of the attack. If this is the case, these can used in future campaigns, or sold to other threat actors to poison future software updates.

The adversaries continued to target machine identities in the post-exploitation phase to hide in plain sight. Once they gained a foothold on the victims' networks, they managed to compromise SAML code signing certificates that helped them forge SAML tokens, which allowed them to authenticate against targeted resources, whether they were on premises or in the cloud. By leveraging these tokens, the attackers were able to appear legitimate to network detection tools and blend in with normal traffic, allowing them to remain undetected on networks for nearly a year.

The scope of this attack is still unfolding, but it's already clear that the attack's impact will send shock waves through the software development and cybersecurity industries. This attack clearly illustrates that enterprisewide machine identity management is an essential security control that cannot be neglected.



Attack Summary

On December 13, 2020, the first reports surfaced, revealing the details of one of the most notable supply chain attacks of the decade. Numerous organizations in the private and public sectors around the globe were hit by a well-planned attack using a sophisticated supply chain. The attack leveraged compromised network monitoring and management software from SolarWinds® Orion®. By successfully compromising the software build and code signing infrastructure, adversaries managed to deliver backdoored updates to thousands of SolarWinds customers.

Artifacts from the investigation confirmed that the source code of the Orion update was directly modified to include the SUNBURST backdoor, which was digitally signed and delivered through the company's software release system. The modification to the update was very lightweight, making it easily overlooked. SUNBURST was added to the update by another malware, dubbed SUNSPOT, that replaced one of the source code files during the build process with another version containing the backdoor.

The fact that the update was digitally signed with a valid SolarWinds certificate enabled broad distribution of the malicious code to; it also raised no flags from security detection controls. As a result of the compromise of this software update, the backdoor infiltrated the networks of 18,000 SolarWinds customers—around 80% of the Fortune 500, including giant corporations like Microsoft, Cisco, Intel Nvidia, Belkin, FireEye and Deloitte—as well as numerous U.S. government departments and agencies.

The adversaries chose their victims carefully and tailored world-class capabilities to specific victims. Although the backdoor was delivered to all SolarWinds Orion customers, the adversaries clearly cherry-picked the targets that were most beneficial to them. They also leveraged their positions on compromised networks to expand to interconnected companies that were not SolarWinds customers. In addition to getting a peak at the software source code of other prominent software companies such as Microsoft, the attackers also attempted to infiltrate dozens of SolarWinds partners, like CrowdStrike, using resellers' access.

Once a victim's network was infected, the adversaries continued their quest for machine identities. By targeting the SAML token-signing certificate, they were able to forge SAML tokens so they could impersonate highly privileged user accounts, mostly of key IT and security personnel. These compromised machine identities allowed them to authenticate against any resources, while blending in with normal network traffic to avoid raising suspicion.

The same adversary is also accused of compromising TeamCity, a widely-used CI/CD tool by JetBrains, in order to use it as a pathway for the attack on SolarWinds Orion and other software companies. Currently, there aren't enough details about the TeamCity compromise to determine exactly what happened or whether this assertion is true, but if JetBrains were, in fact, compromised, that would make it a holy grail of supply chain attacks.

Whether TeamCity was involved or not, the attack on SolarWinds is worrying CIOs and CISOs of every organization. The adversaries invested significant amounts of time and resources to ensure their malicious code was properly inserted into the software build process, while remaining undetected by the SolarWinds developers. Demonstrating high levels of sophistication and patience, the attackers consistently prioritized operational security. This made it possible for them to keep a low profile while causing massive breaches to companies all over the world. Without a doubt, this attack was the work of a nation-state APT (Advanced Persistent Threat) group believed to be associated with the Russian state.

While software supply chain attacks are not novel, the sophistication of this attack illustrates weakness in our software supply chain that leave us vulnerable to similar attacks. The delivery of a backdoor that is digitally signed by a globally known software developer is extremely difficult to defend against. This style of attack enables the adversary to hide in plain sight and gain access to a broad range of other systems, as well as the machine identities required to access sensitive data and services. Software supply chain attacks have made high-profile organizations including U.S. government agencies and tech giants like Microsoft, which previously had been out of reach to attackers, the ultimate victims. In many cases, the ultimate target of these attacks were two or three organizations removed from the initial compromise.

Future attacks using these strategies and tools are inevitable. Securing the software supply chain, including the code signing infrastructure as well all other machine identities, must be part of the security profile of every company that operates a service or develops software. This is the only way to protect customers and maintain integrity and trust.

Attack Details

SolarWinds

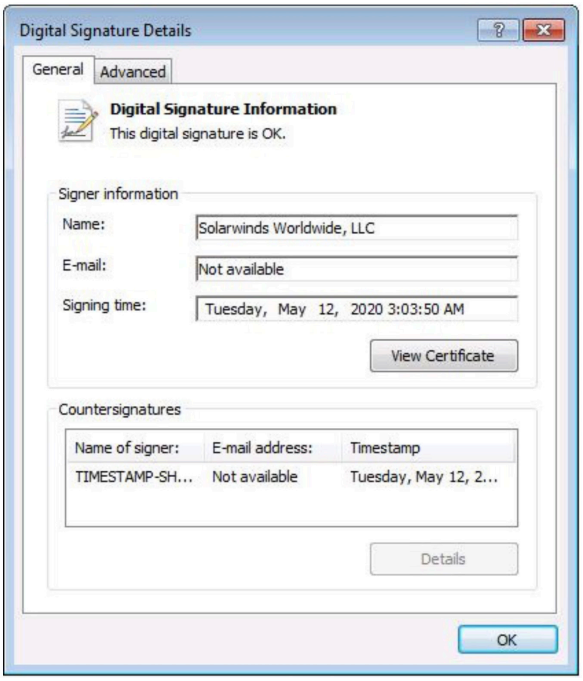
Researchers believe the attackers were preparing for the attack for a long period of time, patiently waiting and testing their approaches. Analysis of the source code of the specific component targeted, *SolarWinds.Orion.Core.BusinessLayer.dll*, shows that the adversaries were inserting empty classes in it as early as October 2019 as a proof of concept. These efforts illustrate the extent of planning and testing the attackers completed before they included the poisoned payload into the build process. In addition to other precautions, the modification to the DLL was very lightweight and was designed to be easily overlooked; it used a similar class name, *OrionImprovementBusinessLayer*, to blend in with the rest of the code.

Further analysis of the artifacts reveal that the malicious file ultimately built with the Orion software build system was compiled only once and was modified at the source code level. It is still unclear how the adversaries managed to compromise the build machine, but it is certain that the build infrastructure was compromised (see SUNSPOT section).

It is also clear that the adversaries were able to force the signing system to sign malicious code, so the digital signing system was definitely compromised. SUNBURST was added to the DLL, compiled and digitally signed using a SolarWinds certificate issued by Symantec between March and May 2020. The fact that the DLL containing the backdoor was digitally signed enabled the adversaries to both elevate privileges and keep a low profile at the same time.

The attack was so successful that the backdoor dubbed SUNBURST was inserted to the DLL in versions 2019.4 HF 5 through 2020.2.1 and remained available on SolarWinds' website even after the disclosure of the attack.

While no public evidence has been presented yet that SolarWinds certificates were used to sign other malware and tools, this option should not be excluded. All certificates and keys on the build systems should be revoked preemptively to avoid further compromise.



SolarWinds digital signature on the backdoored software

Timeline

August 2019	first domain registration
September 2019	the earliest suspicious activity on SolarWinds internal systems
October 2019	first modification of the SolarWinds Orion software update
December 2019	DGA domain acquired
February 2020	SSL certificate acquired
February 2020	SUNSPOT compiled
March – May 2020	weaponization: SUNBURST is added to SolarWinds Orion software update
June 2020	adversary removes SUNBURST from SolarWinds environment
December 8, 2020	FireEye reports on red team tool stolen in an attack
December 12, 2020	SolarWinds is informed of the compromise
December 13, 2020	FireEye reports on SolarWinds supply chain attack
December 14, 2020	SolarWinds releases security advisory
December 14, 2020	Volexity reports on Dark Halo exploiting a vulnerability Microsoft Exchange Control Panel
December 15, 2020	Reports of government agencies hit by the attack, such as the Commerce and Treasury Departments; the Department of Homeland Security (DHS), the National Institutes of Health and the State Department
December 17, 2020	DHS's CISA and NSA release alerts on VMware vulnerability used to forge SAML tokens as part of the SolarWinds attack; attributing the attack to Cozy Bear
December 17, 2020	Microsoft announces that it was breached in the SolarWinds attack and that 40 customers were targeted through it
December 31, 2020	Microsoft says the attacker viewed source code
January 6, 2021	The New York Times report on JetBrains TeamCity targeted in SolarWinds attack
January 11, 2021	CrowdStrike releases analysis of SolarWinds Build server and SUNSPOT
January 11, 2021	Kaspersky reports similarities with Kazaur and Turla

Primary Backdoor Capabilities

Hands-on-Keyboard and Command and Control Capabilities

SUNBURST has a long list of functions and capabilities, all designed to allow attackers hands-on-keyboard access to perform various actions.

Once delivered to the victim's network, SUNBURST completes a long list of checks and tasks, such as confirming the victim's identity, collecting system information and disabling security tools.

After a period of inactivity of between 12 to 14 days, the malware enables remote connections from the internal network to third-party servers using HTTP connections, implementing sophisticated functionality to communicate with its operators' infrastructure. These connections are used to determine its command and control (C&C) domain server using a Domain Generation Algorithm (DGA) to construct and resolve a subdomain of avsvmcloud[.]com. The adversary utilizes the DGA subdomain to vary the DNS response to victims to control the targeting of the malware (see DGA section).

Once the command and control connection is established, the backdoor is open and the adversary has hands-on-keyboard capabilities to execute commands, transfer and execute files, profile the system, reboot the machine and disable system services.

To remain as stealthy as possible, SUNBURST blends in with legitimate SolarWinds activity by hiding its network traffic in the Orion Improvement Program (OIP) protocol and storing all reconnaissance results within legitimate plugin configuration files.

Elevated Privileges and Forged SAML Tokens

Leveraging the administrative privileges obtained during the backdoor delivery, the adversaries were able to access the victim's global administrator account and their trusted SAML token-signing certificate. Typically, this certificate is stored on the server that provides the SAML federation capabilities, making it accessible to anyone with administrative rights on that server. The SAML certificate can typically be accessed either from storage or by reading memory.

Using the token-signing certificate, Microsoft reported that the adversaries could forge SAML tokens for any existing user or account in the organization, including highly privileged accounts. These capabilities then allowed the attackers to bypass multifactor authentication for various services. In Microsoft's case, the adversaries mostly targeted key IT and security personnel with privileged administrative accounts.

Using the SAML tokens created by the compromised token-signing certificate, the adversaries could authenticate against any on-premises resource and any cloud environment configured to trust tokens signed with the compromised SAML token-signing certificate. By impersonating existing applications that use the same permissions, the unauthorized access blended in with normal network traffic and the security controls did not raise any red flags.

DGA (Domain Name Generation Algorithm) and Victim Selection

Among the lengthy list of SUNBURST functions and capabilities, the backdoor applies logic to determine which subsequent actions should be taken based on the victim. Because a large portion of Orion customers around the world had been infected with the backdoor, the adversary needed these sophisticated capabilities to determine which of the compromised organizations were the desired targets for the attack, and to tailor subsequent steps to that organization.

For this purpose, the adversary implemented a Domain Name Generation Algorithm (DGA) using a DNS query containing an encoded value of the internal domain name of the compromised organization. Once decoded, the adversaries were able to obtain the internal name of the victim and choose the next steps to fit the targeted organization.

Based on the decoded internal names, researchers found indications that Mediatek, the Ministry of Health in Australia and Banc Central (an IT security service for banks) were targeted by the attack. This has not been confirmed by public reports.

The list of U.S. federal agencies and departments affected by SUNBURST include the Pentagon, the National Institutes of Health, the Department of Commerce, the Department of Homeland Security, the State Department, the Department of the Treasury and the Department of Energy as well as many state and local governments. The private companies and organizations hit by SUNBURST include Belkin, Cisco, Intel, Nvidia, VMware Microsoft, FireEye and Deloitte.

A more comprehensive list of confirmed victims can be found here.

The SUNBURST samples recovered by FireEye delivered different payloads. In one instance, the attackers deployed a new, in-memory dropper, dubbed TEARDROP, to deploy Cobalt Strike BEACON, which uses HTTP, HTTPS or DNS requests to beacon back to the operator. TEARDROP does not have code overlap with any previously seen malware and is believed to be used to execute a customized Cobalt Strike BEACON.

Initial Access: SUNSPOT—the Implant on SolarWinds Orion Build System

A few weeks after the disclosure of the attack, CrowdStrike was chosen to work closely with SolarWinds on the incident response. CrowdStrike provided an analysis of the SolarWinds software build server and provided more insight into how the SUNBURST backdoor was added to the Orion source code. According to the researchers, the adversaries used another malware, dubbed SUNSPOT, to insert the backdoor into the software builds of the SolarWinds Orion product. SUNSPOT monitored running processes involved in compilation of the Orion product and replaced one of the source files with a poisoned version that included the SUNBURST backdoor. SUNSPOT included several safeguards designed to prevent the Orion software builds from failing, which had the potential to alert developers of the adversaries' presence in the build environment.

SUNSPOT operators also maintained persistence by creating a scheduled task set to execute when the host booted. This task was likely built on 2020-02-20 11:40:02, according to the build timestamp found in the binary.

The design of the malware suggests that the adversaries invested significant effort to ensure the code was properly inserted and remained undetected. The attackers also prioritized sophisticated operational security to avoid raising any alarms on the build environment.

Second Access Vector: VMware Vulnerability and SAML Tokens

As the information about the attack was unfolding, there were also new reports indicating that U.S. federal government agencies had been targeted using the SolarWinds backdoor in combination with two additional exploits in VMware and Microsoft. DHS's Cybersecurity and Infrastructure Security Agency (CISA) released an advisory on December 17th on the SolarWinds attack, noting that CISA had evidence of additional exploit vectors beyond the Orion backdoor. The advisory also mentioned that the adversaries used the SUNBURST backdoor in the Orion update to gain initial access to the local networks and then exploited a VMWare vulnerability (CVE-2020-4006) to perform federated login through Microsoft Active Directory Federation Services (ADFS).

The advisory specifically noted that adversaries managed to compromise the SAML token-signing certificate (another mission-critical machine identity) using elevated Active Directory privileges. In the Microsoft report mentioned above, the adversaries used the token-signing certificate to create valid tokens for specific services in order to access resources in hosted environments, such as email, and then exfiltrate data via authorized application programming interfaces (APIs).

An earlier advisory from the NSA on December 7 observed malicious activity involving the VMware vulnerability. This activity led to the installation of a web shell and generation of SAML tokens that were sent to Microsoft ADFS, granting the threat actors access to protected data. On December 17th, the NSA released a more detailed advisory explaining how the VMware vulnerability was being used to forge SAML tokens; this advisory specifically referenced the SolarWinds compromise.

While it is not yet confirmed that these two cases are related, reports associate these two attacks with the same APT group attributed to Russia. Undisclosed sources specifically attribute the attacks on SolarWinds and VMware to the Russian APT group dubbed Cozy Bear. At this point, in the timeline this attribution was not confirmed by the security community (see Attribution section).

JetBrains' TeamCity as the Entry Point?

A month after the attack was disclosed, The New York Times reported that American intelligence agencies and private security specialists were investigating the potential role of JetBrains, a widely-used Czech software development company with research labs in Russia and over 300,000 customers, in the SolarWinds supply chain compromise.

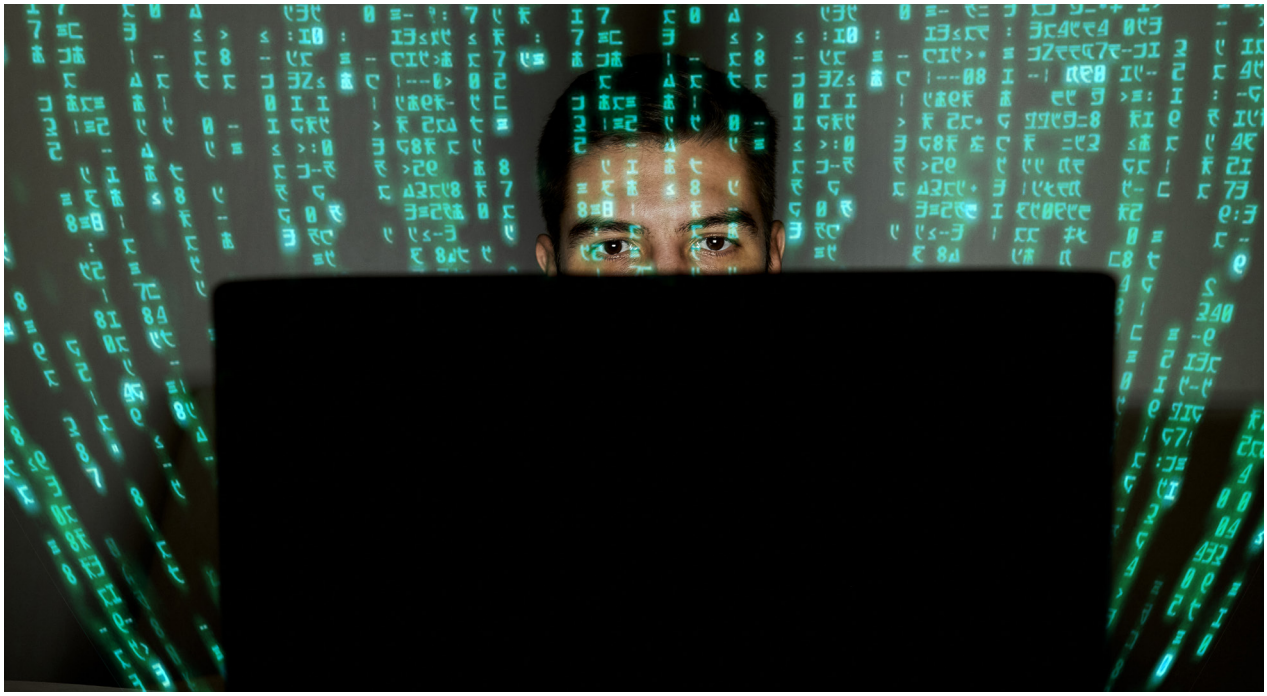
According to the report, JetBrains software was breached by the Russian adversaries to plant the backdoor in SolarWinds Orion software. The report also alleges that JetBrains was used to deliver the same backdoor to an unspecified number of additional technology companies. The report specifically mentioned an investigation of JetBrains' Continuous Integration and Continuous Delivery (CI/CD) Tool, TeamCity, which is used by developers to automate building, testing and deploying software.

By compromising TeamCity, or exploiting gaps in the way developers use the tool, cybersecurity experts explained that the adversaries were able to plant backdoors in the software of JetBrains' customers. According to the report, it is unclear whether the adversaries exploited a vulnerability in TeamCity or they were able to exploit its users via stolen credentials or vulnerabilities in unpatched or outdated software.

According to JetBrains CEO, Maxim Shafirov, the company was not informed by the U.S. government nor by SolarWinds that its software was under investigation, nor was it aware of any compromise or vulnerabilities in their product. According to Shafirov, TeamCity is only available as a self-hosted, standalone application. This means that the installation, configuration and maintenance of their software, including security and access, are the responsibility of the end user and not JetBrains.

A spokesperson for SolarWinds explained that the company used TeamCity as part in its software development environment but noted they hadn't seen any evidence linking the Orion compromise to the TeamCity product.

More information on this attack continues to be uncovered. If it turns out that JetBrains was indeed compromised and used to access the SolarWinds network, the level of sophistication in this attack will increase dramatically, making it the holy grail of supply chain attacks. It will also be one of the largest breaches of U.S. networks to date.



Attribution and Related Campaigns

A review of the artifacts and details of the attack make it clear that the adversaries are highly sophisticated and trained; this attack is, without a doubt, the work of a nation-state APT group. Furthermore, the group demonstrated patience and prioritized operational security over impact, maintaining a low profile for nearly a year, throughout the attack lifecycle.

FireEye and other security companies involved in analyzing the attack have not yet pointed to any specific, known nation-state actors from their threat library. Instead, they referred to it as an unknown group using one of the following aliases:

- UNC2452 (FireEye)
- SolarStorm (Unit42)
- StellarParticle (CrowdStrike)
- Solorigate (Microsoft)
- Dark Halo (Volexity).

Cozy Bear (APT29)

A few days after the disclosure in mid-December, several media reports cited government sources who reported that the group behind the SolarWinds and VMware attacks was the Russian-backed APT group dubbed Cozy Bear (or APT29). This group is believed to be part of the Russian Federal Security Service (FSB), and they are responsible for multiple, severe attacks around the world.

Turla

In January, Russian-based security company Kaspersky found overlaps between SUNBURST and another backdoor known as Kazuar, which was first reported by Palo Alto Networks in 2017. Kazuar was linked by Palo Alto with Turla, another infamous Russian APT group. Although Kaspersky has evidence that Kazuar was used along with other tools associated with Turla, the company did not directly attribute the SolarWinds attack to the same group.

Conclusion

The attack on SolarWinds and JetBrains marks a new era of supply chain attacks. While supply chain attacks have been around for years, this attack is different. The adversaries potentially compromised a developer tool to infiltrate the network of another software vendor and then get inside high-profile organizations that previously were out of reach. They probed SolarWinds' environment and the developers' awareness for months before weaponizing their software update with malicious code. Then they remained undetected for many months by blending in and mimicking the developers' coding style and naming standards.

Legitimate and trusted machine identities enabled the adversaries to gain initial access and remain undetected throughout the entire attack lifecycle. By compromising the code signing system, the group was able to compromise the code signing system and force it to sign a malicious code that was delivered to the entire SolarWinds customer base. While there is no direct evidence yet that the group used SolarWinds code signing materials to sign other malware or tools, this remains a strong possibility. It wouldn't be shocking to discover that the code signing machine identities used in this attack had been stolen and end up being used in future ones. To avoid any further exploitation, all SolarWinds' machine identities used in the affected environment should be considered compromised and preemptively revoked.

The attackers' quest for machine identities did not stop there. In the post exploitation phase, after gaining a foothold on the victims' network, the adversaries targeted SAML code signing certificates that would allow them to forge SAML token access to resources of interest, whether these resources were on premises or in the cloud. Leveraging trusted access to existing high-profile accounts and critical applications, the group was able to hide in plain sight.

By tailoring its world-class capabilities to its targets, the group cherry-picked the victims that would be most beneficial to them and leveraged machine identities on the compromised network to reach to the web of interconnected organizations through supply or delivery chains. In this way, the adversaries were able to extend their reach beyond SolarWinds' customers to their customers' customers.

Already, the list of targets and victims raises many questions regarding the motivation behind this attack. Whether it is for cyberespionage or monetization, this attack has already had a massive impact on companies and users all over the world, and this may just be the tip of the iceberg at this point. Whether TeamCity—which is used by developers all over the world—was compromised or not, the level of access gained by the adversaries could have global implication that are yet to be fully understood.

The global implications of this attack are profound, but the immediate implications for every organization are also critical. Every organization should be implementing zero-trust networking principles and role-based access controls to every application and server on their network. Uusers should not automatically be able to access every device or application on enterprise networks, and most organizations already have robust sets of security controls in place to prevent this. Every organization now needs to extend these same principles to machines; servers and applications need the same kinds of limitations. This requires a robust machine identity management program that provides centralized visibility and intelligence over machine identities—the approximate equivalent of usernames and passwords—along with robust automation that enables organizations to respond within minutes to a machine identity compromise.

Trusted by

5 OF THE 5 Top U.S. Health Insurers
5 OF THE 5 Top U.S. Airlines
3 OF THE 5 Top U.S. Retailers
3 OF THE 5 Top Accounting/Consulting Firms
4 OF THE 5 Top Payment Card Issuers
4 OF THE 5 Top U.S. Banks
4 OF THE 5 Top U.K. Banks
4 OF THE 5 Top S. African Banks
4 OF THE 5 Top AU Banks

Venafi is the cybersecurity market leader in machine identity management, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to-machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access. **To learn more, visit venafi.com**