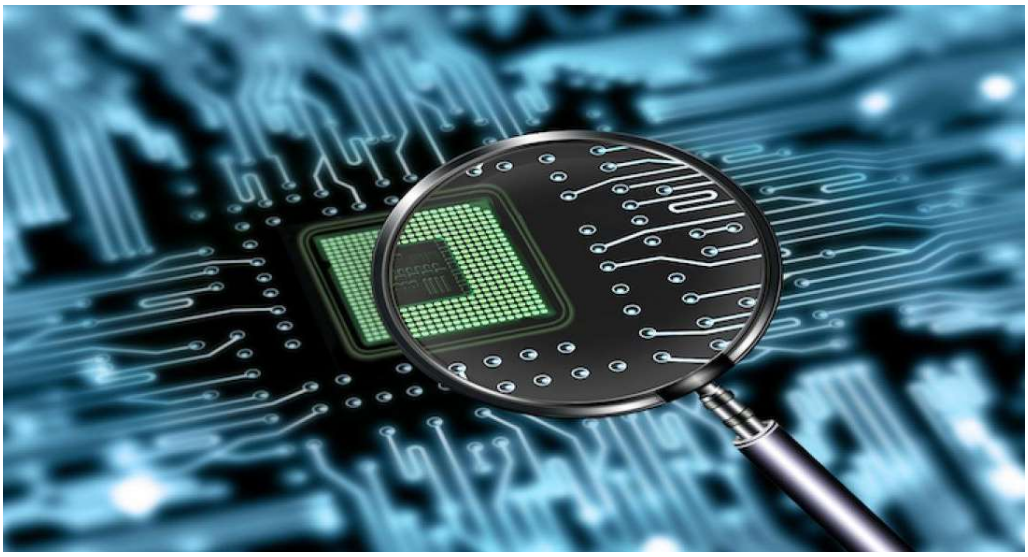
Back

SolarWinds SUNBURST Attack Explained: What Really Happened?



July 28, 2021 | Yana Blachman

Targeting high-profile organizations directly is incredibly difficult, requires a lot of time and effort, and often takes a long time to yield fewer results. Why? Large-scale organizations, such as the government, are well-funded, well-protected, and have entire teams working tremendously hard to maintain the latest security software protecting their network.

To compensate, attackers have to shift up stream to the software supply chain to find a

Download the whitepaper.

What were SUNBURST's exact capabilities?

The culprits managed to target software vendor SolarWinds by targeting Orion, its network monitoring and management tool. They compromised one of Orion's build servers and inserted a backdoor in one of the update's modules. The backdoored update, which was digitally signed, was delivered to roughly 18,000 SolarWinds customers (including Fortune 500 Companies) and was available on their website. FireEye, a cybersecurity company, alerted SolarWinds about the backdoor dubbed SUNBURST and only a few days after the report the backdoor was removed.

Since the backdoor was delivered to such a large amount of Orion's customers, it raised the risk bar for the attacker and forced them to make it as unnoticeable as possible. The change to Orion's update module was very lightweight and could easily go unnoticed. Also, for defense evasion, the backdoor would be inactive at first. After a couple weeks it would make DNS requests and upload data that would help identify the victims and machines of high interest to target and give the attackers hands-on-keyboard access to the compromised machines. After the connection to the command and control servers was established, it would download a second stage malware. This was delivered to a small amount of Orion customers that were of interest for cyber-espionage purposes.

Who were the SUNBURST victims, and how were they compromised?

The ultimate targets of this attack were very carefully chosen. Among the 18,000 customers that installed the update were US agencies including parts of the Pentagon, the Department of Homeland Security, the State Department, the Department of Energy, the National Nuclear Security Administration, and the National Treasury. Also included on the list of targets were FireEye, Microsoft, Cisco, Intel, and Deloitte, the California Department of State Hospitals, and Kent State University.

The fact that the update was digitally signed and originated from a trusted source enabled the attackers to gain access to such high-profile targets and hide in plain sight. This is precisely why supply chain attacks are notoriously difficult to detect. They abuse the trust we rely on to safely navigate the internet—a degree of trust is necessary when it comes to software vendors.

Unfortunately, the supply chain attack did not end here.

Microsoft confirmed that the attackers used vendor access to infiltrate 40 additional organizations that weren't even SolarWinds' customers. These targets included MalwareBytes, Palo Alto Networks, Mimecast, and Crowdstrike. In the case of Mimecast, a Mimecast-issued certificate that was used to authenticate some of the company's products to Microsoft 365 Exchange Web Services had been compromised and used for further exploitation, allowing the attackers to intercept traffic, or possibly infiltrate customers' Microsoft 365 Exchange Web Services, and steal private information.

Machine identities were the main cause behind the SUNB

See Popular Tags

Audit	6 tags
Backdoor	27 tags
Cloud	45 tags
Code Signing	53 tags
Current Events	4 tags
Data Breach	37 tags
Development Fund	58 tags
DevOps	89 tags
Ecosystem	22 tags
Encryption	187 tags
IoT	21 tags
Machine Identity Management	96 tags
Mobile	11 tags
Outages	48 tags
PKI	118 tags

code-signing and signature verification in the build pipeline.

What enabled the attackers to get to their targets in the first place was a digitally signed software and the use of a trusted machine identity, which was the SolarWinds code signing certificate.

Plus, after the initial access, the attackers were after cryptographic keys to secure access to systems across the whole organization. Using the elevated privileges achieved by the initial Orion compromise, they were able to steal a SAML token-signing certificate and forge SAML tokens for any existing users and accounts and authenticate against any on-prem and any cloud resource in that environment.

By using authorized and legitimate machine identities they were able to blend in with normal traffic without raising any red flags. They hid in plain sight for months.

What is so unique about the SolarWinds SUNBURST attack?

This was by no means the first supply chain attack, and it surely won't be the last. What makes this instance stand out what the level of stealth and patience demonstrated by the attackers, and that they had the foresight to prioritize operational security over rushing into action.

The scope and impact of this event are still unfolding, but it's clear that it will send shock waves through the software development and the cybersecurity industries. This should serve as a wake up call to all companies, as no industry is immune. Source code, content distribution, and every part of the software development pipeline must be secured.

If your organization is lagging behind, you can start your digital transformation right now. Venafi CodeSign Protect secures your code signing private keys, automates approval workflows, and maintains an irrefutable record of all code-signing activities.

Related Posts

- Venafi Machine Identity Threat Model
- Linux Foundation Launches sigstore to Combat Open-Source Supply Chain Attacks
- Why Automate the Deployment of Your Digital Certificates? [SolarWinds]
- How You Can Become a Machine Identity Threats Pro!

Like this blog? We think you will love this.

Security News	109 tags
SHA-1	8 tags
SSH	75 tags
SSL/TLS	169 tags
Threat Intelligence	208 tags