SolarWinds Case Study

Georgetown County Government

SUNBURST

The SolarWinds Orion security breach, a.k.a. SUNBURST, impacted numerous U.S. government agencies, business customers and consulting firms. SUNBURST was a very sophisticated supply chain attack, which refers to a disruption in a standard process resulting in a compromised result with a goal of being able to attack subsequent users of the software.

SUNSPOT, the highly sophisticated and novel code was designed to inject the SUNBURST malicious code into the Orion Platform during the build process. SUNSPOT is not a new malware or attack, but instead a component of the SUNBURST cyberattack.

While SUNSPOT infection is part of the attack chain that allows for SUNBURST backdoor compromise, SUNSPOT has distinct host indicators of attack (including executables and related files), artifacts, and TTPs (tactics, techniques, and procedures).

SolarWinds

SolarWinds was the victim of a cyberattack that inserted a vulnerability (SUNBURST) within the Orion® Platform software builds for versions **2019.4 HF 5, 2020.2 unpatched**, and **2020.2 HF 1**, which, if present and activated, could potentially allow an attacker to compromise the server on which the Orion Platform products run. SUNBURST was very sophisticated supply chain attack, which refers to a disruption in a standard process resulting in a compromised result with a goal of being able to attack subsequent users of the software.

Based on the investigation, it appears that the code was intended to be used in a targeted way as its exploitation requires manual intervention. We've been advised that the sophistication and nature of SUNBURST indicates that it may have been conducted by an outside nation state, but SolarWinds has not verified the identity of the attacker.

Timeline

SolarWinds SUNBURST

Attack

September 4, 2019: A threat actor accessed SolarWinds. Source: SolarWinds blog, January 11, 2021.
september 12, 2019 through November 4, 2019: The threat actor injected test code and performed a trial run. Source: SolarWinds Blog, January 11, 2021.

December 2019: The hackers accessed at least one of SolarWinds' Office 365 accounts by December 2019, and then leapfrogged to other Office 365 accounts used by the company.

February 20, 2020: SUNBURST attack was compiled and deployed.
March 26, 2020: Hotfix 5 DLL available to customers.
June 4, 2020: Threat actor removes malware from build VMs.

Tuesday, December 8, 2020: FireEye Suffers Attack: FireEye discloses that state-sponsored hackers broke into FireEye's network and stole the company's Red Team penetration testing tools. **Source**: MSSP Alert.

Friday, December 11, 2020: During a FireEye breach investigation, FireEye discovers that SolarWinds Orion updates had been corrupted and weaponized by hackers.

Saturday, December 12, 2020: A FireEye executive advised SolarWinds CEO Kevin Thompson that Orion contained a vulnerability as the result of a cyberattack. **Source**: SolarWinds SEC filing.

Vulnerabilities

Overall Summary

The government has known about the vulnerabilities that allowed the SolarWinds attack since the birth of the internet—and chose not to fix them.

Supply Chain

The malware was embedded in a SolarWinds security update. When clients clicked on the update, they unwittingly downloaded malware, which allowed the hacker to monitor—and, in some cases, alter—data across the entire network. Orion's software, it turned out, was protected by a very flimsy password ("solarwinds123"). As has been the case all too often throughout the internet age, the watchword was efficiency, not security.

CISA Guidance

The CISA updated its guidance on the SolarWinds Orion vulnerability. Specifically, all federal agencies operating versions of the SolarWinds Orion platform other than those identified as "affected versions" are required to use at least SolarWinds Orion Platform version 2020.2.1HF2. The National Security Agency (NSA) has examined this version and verified that it eliminates the previously identified malicious code. Given the number and nature of disclosed and undisclosed vulnerabilities in SolarWinds Orion, all instances that remain connected to federal networks must be updated to 2020.2.1 HF2 by COB December 31, 2020.

3rd Party Vendor

All new hotfixes and patches have been released since SUNBURST was detected have undergone these new levels of scrutiny. SolarWinds is increasing existing actions and taking additional actions across the enterprise to further harden and improve the security of the environment and products:

- Increased hardening of build environment and build pipeline
- Auditing and surveillance
- Environmental reviews by third-party cybersecurity experts
- Release code penetration testing (pentesting)
- Increased scanning of downloadable bits
- Scanning and analysis of source code and build output
- Refreshing of all employee and contractor credentials and credential security and elevating access restriction
- Re-signing of all release code with new certificates

In addition, SW is elevating their ongoing architectural focus on continually improving the way they design, build, and support their products.

Costs

- American businesses and government agencies could be spending upward of $100 billion over many months
- Not only were at least four government departments targeted by the Kremlin hack — Commerce, Treasury, Homeland Security and Justice — but also thousands of top global corporations who were customers of SolarWinds, Cilluffo said. While government agencies appeared to be primary targets, "it doesn't mean the private sector isn't affected as well," he said.
- The SolarWinds attack exposed 18,000 clients of the software management company after they downloaded and installed a tainted software update that was infected with malware. The breach occurred sometime between March and June this year and wasn't discovered until cybersecurity research firm FireEye, which was attacked separately, revealed the SolarWinds breach in early December.
- Fewer than 10 U.S. agencies were potentially compromised by follow-on activity and the FBI and the intelligence agencies are "working to identify the non-government entities who also may be impacted," the statement said.
- On its now deleted customer list page, SolarWinds claimed that its clients included 425 of the Fortune 500 companies including Microsoft, Lockheed Martin and Ford Motor Co., as well as all "five branches of the U.S. military," the Pentagon, Justice Department, State Department, and the "Office of the President of the United States."

Prevention

- SolarWinds reviewed the architecture of the build environment, the privileged and non-privileged users that have access to the build environment, and the network surrounding the build environment.
- SolarWinds retained third-party cybersecurity experts to assist in an investigation of these matters, including whether the vulnerabilities were exploited as a point of any infiltration of any customer systems, and in the development of appropriate mitigation and remediation plans to help ensure future releases are protected.
- Deployed additional, robust threat protection and threat hunting software on all network endpoints, including a critical focus on development environments.
- Resetting credentials for all users in the corporate and product development domains, including resetting the credentials for all privileged accounts, and for all accounts used in building the Orion® Platform and related products.
- Consolidated remote and cloud access avenues for accessing the SolarWinds network and applications by enforcing multi-factor authentication (MFA).
- Moving to a completely new build environment with stricter access controls and deploying mechanisms to allow for reproducible builds from multiple independent pipelines.