SolarWinds Supply Chain Attack

Notable Observations & Defensive Strategy Against Novel Malwares

Introduction

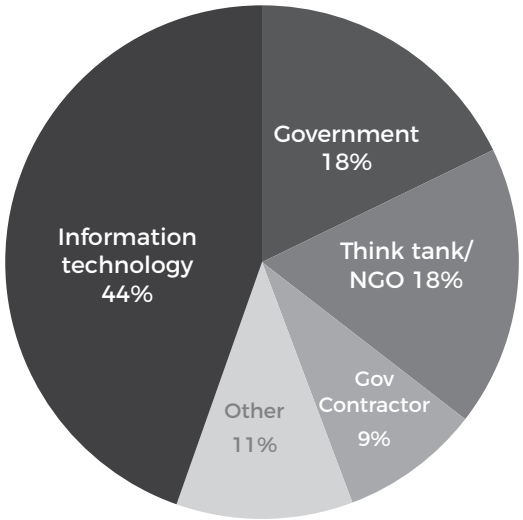
In the year 2020, the onset of the pandemic disrupted supply chains worldwide with rapid digitization, ramping up cyber risks associated with supply chains. As this narrative was getting stronger, the final weeks of an already challenging year exposed a supply chain vulnerability of nearly global importance. In December 2020, SolarWinds Inc., leading provider of IT monitoring and management solutions for enterprises, disclosed that it has fallen prey to a widespread supply chain attack trojanizing its Orion business software updates.

FireEye & CrowdStrike who have been supporting SolarWinds in its investigation reported that the attackers deployed a novel malicious tool, SUNSPOT (hasn't been attributed to any known adversary), into the build environment of Orion's platform to inject SUNBURST backdoor.[1] The said trojanized software updates may have been installed by as many as 17,000 customers.[2] However, the attackers were only interested in a few hundreds of these customers who received secondary payloads, such as the post-exploitation tool named Teardrop. The initial list of victims not only included the U.S government, but other consulting and technology firms in North America, Europe, Asia and the Middle East as shown in the chart below:

SolarWinds Hack Victims by sector

44% of victims were in the Information Technology sector, including software firms, IT Services, and equipment providers.

US Government targets are involved in Finance, National Security, Health, and Telecommunications, while the government contractor victims primarily support defence and national security organisations.

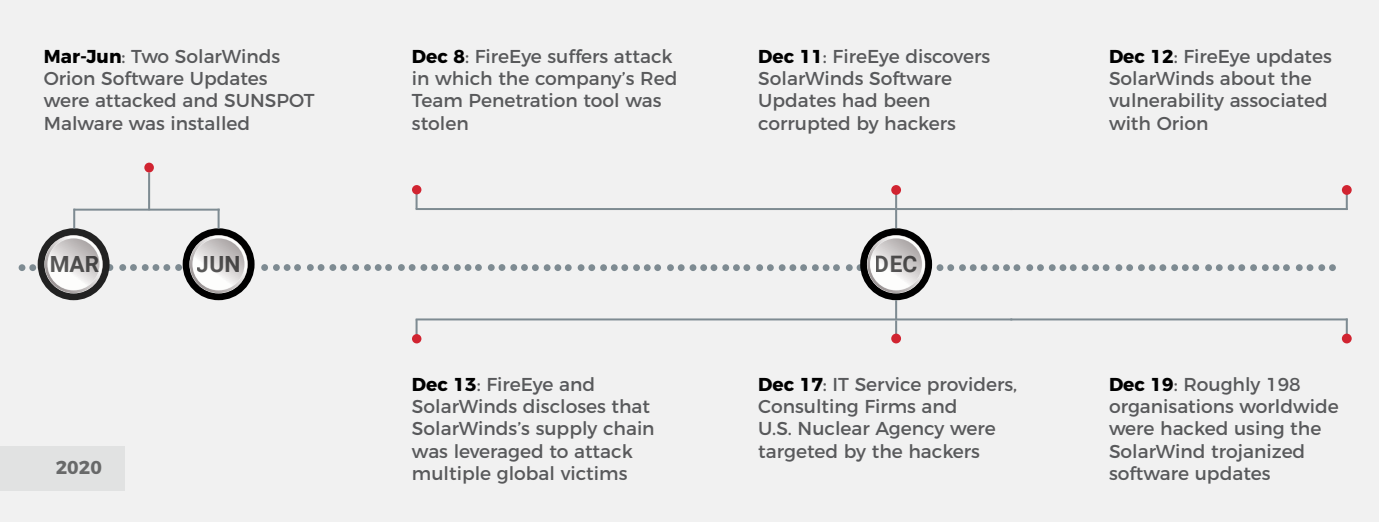


Source: Microsoft (https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/)

At ColorTokens, we think it's critical to step back and analyse the attack phases & ramifications of such a highly evasive attack campaign. Hence, our experts have combined all the findings to help you assess your potential vulnerability to the SolarWinds attack and to advise on next steps.

Trends Observed in the SolarWinds Hack

Although FireEye uncovered the scope of this sophisticated supply chain attack in December 2020, SolarWinds in its recent blogpost revealed that the malware SUNSPOT may have been inserted into the update packages of its customers in between March 2020 and June 2020. Since then, the highly skilled attackers have successfully managed to evade the standard forensic and antivirus methods used by SolarWinds, other private companies and the federal government. The campaign that's currently ongoing has the following timeline, connecting the dots between FireEye's discovery of the attack and SolarWind's original hack:[3]



Russian cybercriminals are suspected to have used SolarWinds Orion software updates to install the SUNBURST backdoor on enterprise users' IT systems and networks, causing a serious attack of unprecedented proportions. FireEye's findings revealed that the backdoor communicates with third-party servers via HTTP, after an initial dormant period following deployment. Once the malware activates, it is able to gather data as it traverses compromised networks as legitimate lateral traffic without getting detected, and it even "stores reconnaissance results within legitimate plug-in configuration files."[4]

*Affected Products

Orion Platform versions 2019.4 HF 5, 2020.2 with no hotfix installed, or with 2020.2 HF 1, including: Application Centric Monitor (ACM), Database Performance Analyzer Integration Module* (DPAIM*), Enterprise Operations Console (EOC), High Availability (HA), IP Address Manager (IPAM), Log Analyzer (LA), Network Automation Manager (NAM), Network Configuration Manager (NCM), Network Operations Manager (NOM), Network Performance Monitor (NPM), NetFlow Traffic Analyzer (NTA), Server & Application Monitor (SAM), Server Configuration Monitor (SCM), Storage Resource Monitor (SRM), User Device Tracker (UDT), Virtualization Manager (VMAN), VoIP & Network Quality Manager (VNQM), Web Performance Monitor (WPM)

*Note: Recent as of December 31,2020, 3PM CST

Threat Vectors and Detection Opportunities

Hackers behind this widespread campaign use a variety of threat vectors to masquerade their footprints while they move laterally. Hence, if you are using the above mentioned SolarWinds Software, the below section will help you find some potential opportunities for detection:

- **TEARDROP and BEACON Malware:** In at least one of the SUNBURST samples that have been recovered, the attackers deployed a previously unseen memory-only dropper (dubbed TEARDROP) to deploy Cobalt Strike BEACON.
- **Attacker Hostnames Match Victim Environment:** The threat actors matched the hostnames of their command-and-control infrastructure with the victim's environment's hostname to blend into the environment and avoid suspicion.
- **Lateral Movement Using Different Credentials:** Once the attackers gained access to the network, they moved laterally using credentials that are different from those used for remote access.
- **Temporary File Replacement and Temporary Task Modification:** Using a temporary file replacement technique, the attackers manipulated scheduled tasks to execute their tools and then returned the scheduled task to its original configuration. Once legitimate remote access was achieved, they also removed any trace of Backdoors.

General Detection and Protection Measures

As the campaign is currently ongoing, these are the precautionary measures recommended by SolarWinds, to stay ahead of evolving attack vectors:[5]

- SolarWinds has asked customers using the product Orion Platform v2020.2 with no hotfix or 2020.2 HF 1 to upgrade to Orion Platform version 2020.2.1 HF 2 as soon as possible to ensure the security of your environment. This version is currently available here
- SolarWinds has asked customers using the product Orion Platform v2019.4 HF 5 to update to 2019.4 HF 6, which is available for download here
- The hotfix release 2020.2.1 HF 2 is now available in the SolarWinds Customer Portal at https://customerportal.solarwinds.com/. It is recommended to update to the 2020.2.1 HF 2, as the 2020.2.1 HF 2 release replaces the compromised component and provides several additional security enhancements.
- Please follow the guidelines available here for securing your Orion Platform instance, if an immediate upgrade hasn't been performed.
- In case, the SolarWinds infrastructure isn't isolated, block domain and subdomain of avsvmcloud[.]com at perimeter level and restrict scope of connectivity to endpoints (Tier 0/Crown Jewel Assets) from SolarWinds servers

ColorTokens Applies Proactive Protection Throughout the Attack Lifecycle

According to the latest "2020 State of the Software Supply Chain" report released by Sonatype, the so-called "next-generation" supply chain attacks have surged by 430% in the past year. As the adversaries are getting craftier and imposing an unprecedented level of risks, the world should look to specialised coverage that is indispensable to cybersecurity protection against evolving cyber-attacks.

Based on Zero Trust Architecture, ColorTokens' Xtended Zero Trust Platform, comprising Xshield & Xprotect, defends organizations against the most sophisticated cyber-attacks. The various attacks phases involved in SolarWinds Exploit and ColorTokens' approach to blocking them are described below:

Pre-Attack Stages	ColorTokens Coverage
Payload Delivery: A software update component of SolarWinds was embedded with a backdoor that connects to third party servers through HTTP	**Xshield** with **Xassure** Breach Protection service can prevent and detect such exploits of trusted sources and outbound access
Reconnaissance: After 2 weeks in dormant state the malware started unpacking the payload and collecting data on the network by masquerading as genuine network traffic	**Xshield** blocks unauthorized communication between systems
Payload Installation: Post installation of the trojanised updated file, the malware attempts to connect with C2 domains, mimicking as genuine SolarWinds connection	**Xassure** Breach Protection service prevents attack patterns leveraging **Microsoft Windows** genuine and trusted processes

Post-Attack Stages	
Beaconing: Network connections made to attacker machines masquerading as internal machines. All the destinations were within the geo locations of the targeted organization	**Xshield** prevents such connections. **Xassure** Breach Protection service detects Domain Generation Algorithms to prevent beacons
Lateral Movement: Lateral movement using different credentials and compromising other systems on the network	**Xshield** automatically prevents unauthorised communication between systems
Hide digital footprints: Temporary file replacement technique to remotely execute utilities	**Xprotect** with its advanced rule rings can prevent attacks around command lines executions

Mitigation Recommendations

FireEye's analysis of SUNBURST revealed extensive use of lateral movement to propagate and infect other systems. Further, the lack of proactive process-based controls allowed further attacks on infected systems. As new threat information continues to emerge, ColorTokens recommends customers to undertake the following mitigation strategies to defend against further risks from this and other sophisticated cyberattacks:

- Ring-fence any 3rd party servers and internal critical applications to prevent unauthorized communications between systems and reduce propagation via lateral movement.
- Ensure your endpoints are protected to prevent hackers from launching legitimate applications and processes from within malicious code.
- Implement continuous monitoring security practices that look for attack patterns exploiting trusted processes and prevent further connections and beacons.

Applying security hygiene and east-west segmentation along with endpoint and server hardening can be effective techniques to reign in spiraling complex segments that promote unseen lateral movement. Such attacks depend on network complexity and lack of east-west controls to move laterally from system to system. Micro-segmentation that automatically prevents communication between systems that do not otherwise communicate significantly reduces the propagation possible via lateral movement.

To learn more about how we can help you assess your security risk posture and implement defensive strategies against sophisticated supply chain attacks, request a ColorTokens customized demo.

To understand more about our solutions, visit https://colortokens.com/products/xtended-zero-trust-platform/

References

[1]https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
[2]https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/
[3]https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/
[4]https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
[5]https://www.solarwinds.com/securityadvisory