CYBER DEFENSE INTELLIGENCE

CYBER Defense Briefing

WATCH LIVE BRIEFING (RECORDED)

CYBER DEFENCE INTELLIGENCE CENTER

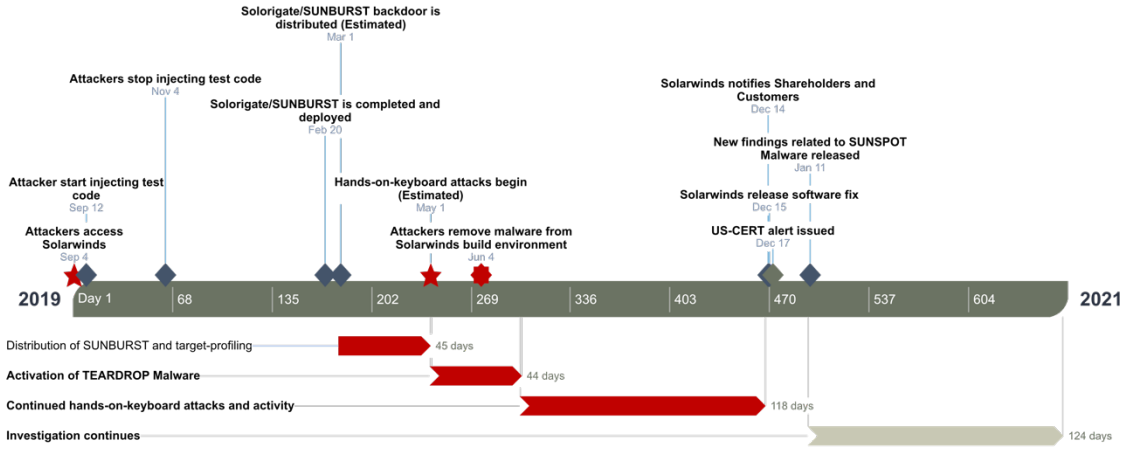
January 26, 2021

SolarWinds Hack

SCOPE: This intelligence briefing affects all Industry Segments and Organizations.

Attack Description and Timeline

SolarWinds, a US-based technology company, announced in December 2020 that they had been targeted in a sophisticated cyber-attack. The attack leveraged the SolarWinds Orion platform to allow the Threat Actor (TA) to extend the attack to SolarWinds' customers. These customers included numerous US Government agencies, including DHS (Department of Homeland Security) and the US Treasury Department. The attack also potentially impacted thousands of private organizations including FireEye (Cybersecurity Firm). Initial indications attribute the attack to Russian hackers but this has not yet been confirmed.



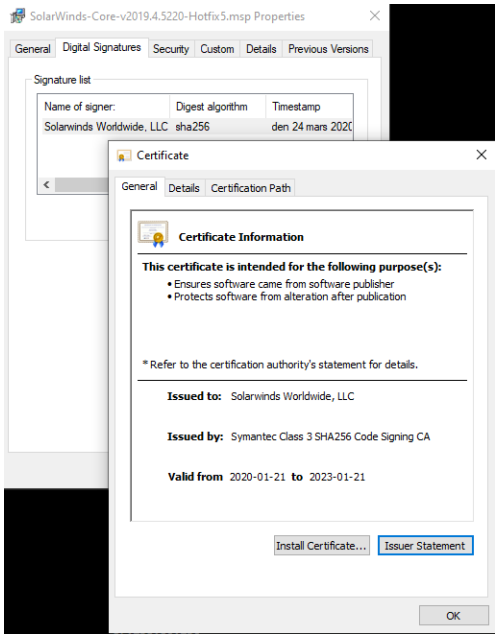
Solorigate Timeline

Source: Pillar Technology Partners

Attack Methodology

The SolarWinds attack was a sophisticated operation that started with a supply chain attack. These types of campaigns leverage the trust between organizations to further the attack and extend their reach into additional organizations. In this attack, the Threat Actors injected malicious code into the SolarWinds Orion platform. This platform was then deployed by SolarWinds customers allowing the Threat Actor to bypass security

controls and gain footholds into these companies. The Orion update that customers downloaded was properly digitally-signed by SolarWinds.



Source: FireEye

The malicious code set ("SUNBURST"/"SOLORIGATE" and "SUPERNOVA") created a backdoor into the systems using TEARDROP malware. The malicious code established persistence as well as implementing advanced defense evasion techniques. The backdoor also monitored the systems for security specific dlls and executables which could potentially detect its presence and avoided running if these dlls had been detected. Once established, the backdoor began conducting reconnaissance of the environment to identify opportunities for lateral movement.

The backdoor also connected to C2 (Command and Control) Servers to send the targeting information gathered to the Threat Actor. This information was then leveraged as part of a secondary attack where the Threat Actor began to conduct follow-on attacks and exfiltrate compromised data including compromised credentials, additional system compromises and privilege escalations. Microsoft's 365 Defender Research Team identified that the Threat Actors "went out of their way" to ensure that the backdoor they initially installed in the SolarWinds Orion network monitoring platform was separated "as much as possible" from Cobalt Strike loader which was used in the secondary attack.

The Microsoft Defender Research Team stated that the attackers believed that if Cobalt Strike (BEACON) - a legitimate penetration testing tool - was detected in an infected system, the victim would not notice the connection to the SolarWinds Orion backdoor.

The Microsoft 365 Defender Research Team report also discusses several previously unknown tactics, techniques and procedures the attackers used, including varying names

and folders as well as creating unique Cobalt Strike Dynamic Link Library loaders for each attack.

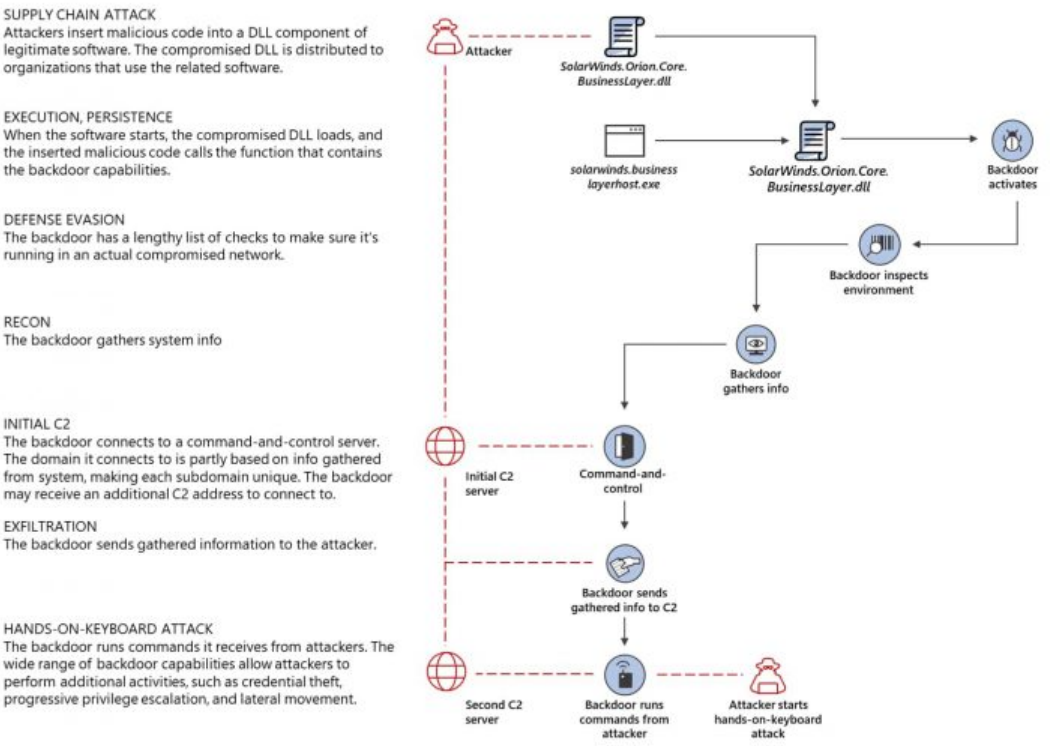


IMAGE: Microsoft Corporation

MITRE ATT&CK Techniques

The following techniques have been identified in the SolarWinds attack methodology.

ID	Description
T1012	Query Registry
T1027	Obfuscated Files or Information
T1057	Process Discovery
T1070.004	File Deletion
T1071.001	Web Protocols

T1071.004	Application Layer Protocol: DNS
T1083	File and Directory Discovery
T1105	Ingress Tool Transfer
T1132.001	Standard Encoding
T1195.002	Compromise Software Supply Chain
T1518	Software Discovery
T1518.001	Security Software Discovery
T1543.003	Windows Service
T1553.002	Code Signing
T1568.002	Domain Generation Algorithms
T1569.002	Service Execution
T1584	Compromise Infrastructure

Impacts

The long-term impacts of the attack remain to be seen, but initial estimates are that the loss of sensitive data was devastating. SolarWinds has indicated that it has 300,000+ Orion customers, of which approximately 18,000 customers downloaded the affected version. Further analysis indicates that anywhere from 50 to 500 hundred of those customers were targeted for secondary "advanced" attacks. However, many of these companies are third-party service provider technology companies which have extended reach and administrative controls into their customers' data.

Amongst the customers targeted for the secondary attacks, many were US Government agencies including US departments of Commerce, Defense, Energy, Homeland Security, State, the Treasury, and Health. The extent of data compromise is still unknown, but at this point, it is assumed that sensitive and classified information was accessed and

possibly exfiltrated. In addition to the US Government targets, the list of identified organizations included banks, foreign governments, universities, and technology companies.

Large technology service providers such as Mimecast, coordinated their internal investigations and collaborated with other organizations to identify, remediate and notify their affected customers. They have also developed remediation instructions for their customers.

Attack Attribution

Attribution for the attack is still being debated. FireEye has attributed the attack to an unknown attacker identified as UNC2452 (Also known as "Dark Halo"). FireEye has not attributed this attack to Russian bad actors at this point.

The US Intelligence services have attributed the attack to a Russian State-funded APT Group known as APT29 ("Cozy Bear"). There are also indications that APT41 (Chinese Nation-State Actor) could have been involved.

At this time, it is difficult to definitively attribute the attack to a single group. The level of sophistication, quality of code and funding required to conduct this type of operation do indicate that it is likely a Nation-State, foreign service backed effort.

Actions

Protection from attacks like the SolarWinds hack involve many dimensions of a well-run security program. A strong security program will increase the likelihood that an attack such as this can be discovered more quickly**,** and thereby, receive prompt attention reducing the incident's impact. However, the level of sophistication of this attack overwhelmed even expert security firms. Nonetheless, strong foundational elements and constant monitoring will improve your defense against this and any other type of attack.

- Implement a strong **vulnerability management** and **patching process** to ensure that inherent weaknesses in systems and devices are identified, analyzed, and closed.
- Deploy **next-gen Endpoint protection** that not only identifies resident and dormant viruses and malware during system scans via signature, but also stops actions taken by executables when they execute in memory.
- Design a **"Defense-in-depth" architecture** which leverages tools that provide "Intelligent Overlap" in their detection and protection capabilities.
- Implement a strong **monitoring capability** that gathers telemetry from systems and devices and can correlate events into alerts.
- Ensure that your vendors have a strong security program by implementing a **vendor management process** that assesses and audits vendors' security capabilities and actions.
- Conduct **proactive "Threat Hunting"** exercises to identify Indicators of Compromise and suspicious activities before they can become an attack.

- Stay engaged with **Threat Intelligence** services to ensure that your team has the "latest and greatest" OSINT (open-source intelligence) information.
- FireEye / Mandiant has developed a PowerShell script called **Azure AD Investigator** that searches your Microsoft Office365 Directory for Solorigate Indicators of Compromise.

Prepared by the Cyber Defense Coalition Intelligence Center Analysis Team.
For live discussion on this briefing and how to prevent sophisticated attacks such as SolarWinds, join us for the Cyber Defense Intelligence Forum January 29, 2021 at noon or watch a replay of this session.

WATCH LIVE BRIEFING (RECORDED)

REGISTER FOR FUTURE CDI LIVE BRIEFINGS