SolarWinds – An Overview

Supply Chain Attack, Concerns, and Remediation

Author: Tushar Nandwana, Information Technology Risk Control
Published: February 2021

Executive Summary

The compromise of the SolarWinds Orion Network Configuration Manager Update (referred to as Orion onward) has been in the news since its discovery in December 2020. The impact of this cyberattack on a software supply chain (attacking a vendor's software update build) is quite extensive and poses a significant risk for the downstream customers. The sophistication of the attack and the organizations that were ultimately targeted is astonishing and terrifying. However, this is only the tip of the iceberg. How deeply an organization has been compromised or what intellectual property was exfiltrated is yet to be fully determined. What is clear is that the ramifications of this cyberattack are far reaching and it may take years to fully understand the complete impact of it.

This article provides a short summary of the history of this threat, information on why this threat should be a concern to all, and guidance on third-party resources to aid with education and remediation on this matter. In an effort to be overly cautious, we recommend that you review and consider the numerous corrective actions noted in this article and those suggested by well-known security firms and the Department of Homeland Security directive 21-01. This situation remains dynamic and will continue to evolve over time.

The Malware

Before reviewing the events that led to the attack and subsequent compromise from the Orion update, let's review the various pieces of malware that were involved in this process:

- Sunspot – The malware used by the threat actor (TA) to insert Sunburst/Solorigate into SolarWinds build or development platform.
- Sunburst/Solorigate – The malicious backdoor code that was inserted into the development build of the Orion product update. The TA took time to understand SolarWinds' build cycle and blended and aligned the malware into Orion's build, so that it was imperceptible to the SolarWinds' developers. It appears to be one of the most complex and sophisticated cyberattacks in history. SolarWinds has not been able to verify the identity of the TA. However, due to its sophistication, it is likely to be the work of a nation state.
- Teardrop – The second stage payload that is dropped by the Sunburst/Solorigate backdoor into the victim's systems infected with the Orion update. TA then used Teardrop to deploy Cobalt Strike (a malware penetration testing tool) attack kits into applicable network environments.
  Supernova – Another sophisticated backdoor discovered in the Orion platform. It allows TA to carry out malicious activity while staying completely hidden. The critical concern here is that Supernova appears to be deployed by a completely different TA group than the one that compromised Orion.

- Raindrop – Another dropper malware detected during the SolarWinds investigation. It too had a payload of Cobalt Strike, but unlike Teardrop, it was not deployed by the initial Sunburst backdoor. Rather, it was found to be present on some networks where a computer had already been compromised by Sunburst.

What Happened?

- SolarWinds noted that TA first compromised its software development environment (build) on September 4, 2019. They believe the attack vector was either through a credential compromise (maybe through an employee's compromised email) and/or access through a third-party app that had a zero day vulnerability. This remains under investigation.
- TA started to inject test code and do trial runs on September 12, 2019 and completed testing by November 4, 2019. TA was making sure that the inserted malicious code was imperceptible to SolarWinds' development group when it was being compiled. For technical information on how this was done, refer to the CrowdStrike analysis.
- On Feb 20, 2020, the Sunburst malware backdoor is compiled and deployed with the Orion update, which was released as Hotfix 5 DLL or 2019.4 HF 5 on March 26, 2020. The compromised updates were digitally signed and pushed out to 18,000 customers over several months in 2020. TA removed the backdoor from Orion in June 2020.
- Although the Orion update was uploaded by 18,000 organizations, research indicates that the TA was interested in a limited number of these organizations. The TA was focused on specific government entities such as Department of Commerce, Energy, Homeland Security, Defense, Justice, and major Fortune 500 firms such as FireEye, Microsoft, Palo Alto, Cisco, Qualys, Nvidia, Intel and numerous others.
- Some of the remarkable features of Sunburst backdoor that enabled it and the TA to avoid detection while roaming through the victim's network and exfiltrating data include:
    - Staying dormant for two weeks after initial Orion update to avoid being detected on scans the victim would run to check for anomalous behavior.
    - Not operating if it found:
        - Certain environments or in certain systems (such as a virtual environment) because the TA likely assumed that it was a security analyst's computer.
        - Security products from CrowdStrike, CyberArk, Panda, Cybereason, Kaspersky, Logrythm and Dell Secureworks. The TA likely assumed that customers using these products were more sophisticated.
        - Specific IP addresses as they were trying to remain undetected.
    - Navigating the environment to determine security products in use and disabling some security features in the victim's system.
    - Checking for specific running processes and either disabling or modifying audit logs and time stamps.
    - Hiding exfiltrated data in DNS (domain name system) traffic which looked like communication traffic from the Orion platform.
    - Using IP addresses within the same country for command and control (C2) server communications.
    - Creating Custom Domain names back to the C2 server so that a discovery in one company would not impact others that are compromised.
    - Most importantly, using Golden SAML (Security Assertion Markup Language) attack technique to allow TA to fully bypass multifactor authentication controls in place, and thereby allow the TA ready and persistent access to any SAML enabled cloud service including AWS (Amazon Web Services)

and Office 365 cloud environments. This is a direct effort to gain access to cloud services where the TA likely assumed the victim stored their most important data.

- The TA group was quite stealthy and maintained a high level of operational security at all stages of the attack – from the initial break-in into SolarWinds when they injected the malware, to operating without being detected after being deployed through the Orion update, secretly communicating with the C2 servers, second stage malware deployment and finally data exfiltration. Due to the level of resources needed to develop the malware, and to maintain stealth and persistence for nine months, the TA group has the likely indications of being a nation state. Their goal appears to be government and corporate espionage through the exfiltration of sensitive information and intellectual property, while NOT inflicting damage so as to avoid detection for as long as possible.

What if you are affected by the Orion update?

- By now, you should hopefully have unplugged the affected devices and/or applied the necessary patches to Orion as released by SolarWinds. Refer to the Remediation section.
- Preserve your logs for all systems so they can be used later to investigate - specifically those from the date of compromise in early 2020.
- Follow the various remediation strategies suggested by DHS, FireEye, CrowdStrike, Sygnia, Volexity and others. These are noted at the end of this paper.
- Even after patching and remediation, if you were running the compromised version you should carry out a forensic investigation of your network environment to confirm that the TA did not inject any other backdoors or malware into your network environment, or exfiltrated any proprietary data.
- Consider an extended detection (using the aforementioned logs) and response solution to review past events and look for malicious activity, such as unexplained account creation.

Why should it concern me if I don't use SolarWinds Orion?

- Development Tools
  - The software development and build process used by SolarWinds is common throughout the software industry. As such, research notes that the methods and techniques used against them could be readily repurposed against many other major software providers to compromise their software builds. This can greatly harm the software update supply chain process and those organizations that rely upon it.
  - If you deploy software to your customers, use this as a lesson and decide how to improve your code development and secure delivery of your software.
- Other Threats
  - DHS' CISA (Cybersecurity and Infrastructure Security Agency) believes that the TA group also used multiple other infection vectors in addition to the Orion backdoor (Sunburst) to infiltrate other companies during 2020.
  - Malwarebytes, a firm that did NOT use SolarWinds products, disclosed in January 2021 that the same TA group had gained access to some of their internal company emails by exploiting a dormant email protection product with privileged access into their Office 365 environment.
  - This TA group has used techniques to bypass a victim's multi- factor authentication system to access cloud-hosted applications.
  - This TA group may have used other vectors not yet discovered.

What more should you consider?

- Third-party software suppliers
  - Be more aware of software updates from your software vendors/suppliers as they may have been potentially exploited.
  - Contact your third parties that you rely on (especially those that have your Non Public information) to review and determine if they were susceptible to the Orion attack and if so, ascertain their remediation and internal review activities.
  - Consider obtaining third-party risk assessments on your suppliers from TPRM (third party risk management) vendors such as BitSight, Security Scorecard, Risk Recon or others.
- Educate yourself
  - TA groups may have potentially compromised your network using the other techniques and tactics noted above. It would be in your best interest to consider conducting a deeper investigation of your network to look for many of the telltale signatures characteristic of this TA group.

Contact Us

To learn more about how Intact Technology can help you manage online and other technology risks, please contact Dan Bauman, VP of Risk Control at dbauman@intactinsurance.com or 262-951-1455.

References & Resources

- Education
  - SolarWinds – Ongoing Investigation
  - CISA – Advisory
  - FireEye – Blog
  - Microsoft – Blog
  - Krebs on Security – SolarWinds, What Hit Us could Hit Others
  - Dark Reading – 7 Things We Know So Far
  - Crowdstrike – Technical Analysis
  - Malwarebytes – Blog
  - MITRE ATT&CK – Knowledge Base of Adversary Attack and Techniques

- Patching & Remediation
  - SolarWinds – Security Advisory
  - Department of Homeland Security – Emergency Directive
  - Crowdstrike – Tool to identify and mitigate risks in Azure Active Directory
  - FireEye
    - How to detect and remediate
    - Hardening and Remediation Strategies for Microsoft 365
  - Microsoft – Solorigate Resource Center
  - Volexity – Responding to the SolarWinds Breach
  - Sygnia – Golden SAML Advisory