Active Exploitation of SolarWinds Software Potentially Affecting HPH Sector

Executive Summary

On 13 December 2020, FireEye and SolarWinds released security advisories detailing a highly-skilled and highly-targeted, manual supply chain attack on the SolarWinds Orion Platform network management system that leverages software updates to deploy a backdoor to victim organizations. SolarWinds Orion is an IT performance monitoring platform that helps organizations manage and optimize their IT infrastructure. The actors behind this campaign have likely gained access to numerous public and private organizations around the world starting as early as Spring 2020. Signatures to detect this threat are available and mitigations are detailed in this alert and should be prioritized.

Analysis

This supply chain compromise can allow attackers to gain access to victim organizations via Trojanized updates in the SolarWinds Orion Platform. While the attacker's post compromise activity leverages multiple techniques to evade detection and obscure their activity, there are also opportunities for detection. FireEye is tracking this threat actor as UNC2452 and news outlets suggest that APT29, also known as Cozy Bear, is behind the campaign.

Alert

On 13 December 2020, FireEye and SolarWinds released security advisories detailing active exploitation of SolarWinds Orion Platform software versions 2019.4 through 2020.2.1, released between March 2020 and June 2020. According to FireEye, SolarWinds.Orion.Core.BusinessLayer.dll is a SolarWinds digitally-signed component of the Orion software framework that contains a backdoor that communicates via HTTP to third party servers. This Trojanized version of the Orion plug-in has been given the names SUNBURST by FireEye and Solorigate by Microsoft. After an initial dormant period of up to two weeks, it retrieves and executes commands, called "Jobs", that include the ability to transfer files, execute files, profile the system, reboot the machine, and disable system services. The malware masquerades its network traffic as the Orion Improvement Program (OIP) protocol and stores reconnaissance results within legitimate plugin configuration files allowing it to blend in with legitimate SolarWinds activity. The backdoor uses multiple obfuscated blocklists to identify forensic and anti-virus tools running as processes, services, and drivers.

Patches, Mitigations & Workarounds:

FireEye has released an Advisory with additional details as well as signatures to detect this threat actor and supply chain attack in the wild found on its public GitHub page with detection rules in multiple languages including Snort, Yara, IOC, ClamAV. Additional mitigations include the following:

- Ensure that SolarWinds servers are isolated / contained until a further review and investigation is conducted. This should include blocking all Internet egress from SolarWinds servers.
- If SolarWinds infrastructure is not isolated, consider taking the following steps:
  - Restrict scope of connectivity to endpoints from SolarWinds servers, especially those that would be considered Tier 0 / crown jewel assets
  - Restrict the scope of accounts that have local administrator privileged on SolarWinds servers.
  - Block Internet egress from servers or other endpoints with SolarWinds software.
- Consider (at a minimum) changing passwords for accounts that have access to SolarWinds servers / infrastructure. Based upon further review / investigation, additional remediation measures may be required.
- If SolarWinds is used to manage networking infrastructure, consider conducting a review of network device configurations for unexpected / unauthorized modifications. Note, this is a proactive measure due to the scope of SolarWinds functionality, not based on investigative findings.

SolarWinds recommends upgrading to Orion Platform version 2020.2.1 HF 1 as soon as possible. An additional hotfix release, 2020.2.1 HF 2 is anticipated to be made available Tuesday, December 15, 2020 and SolarWinds recommends updating to HF 2 once released as this both replaces the compromised component and provides several additional security enhancements.

References

Emergency Directive 21-01: Mitigate SolarWinds Orion Code Compromise
https://cyber.dhs.gov/ed/21-01/
Active Exploitation of SolarWinds Software (13 December 2020)
https://us-cert.cisa.gov/ncas/current-activity/2020/12/13/active-exploitation-solarwinds-software
Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor (13 December 2020)
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
SolarWinds, SolarWinds Security Advisory (13 December 2020)
https://www.solarwinds.com/securityadvisory
SolarWinds, SolarWinds' Customers
https://www.solarwinds.com/company/customers
Washington Post, Russian Government Spies are Behind a Broad Hacking Campaign That Has Breached US Agencies and a Top Cyber Firm (13 December 2020)
https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html
Russian Hackers Broke Into Federal Agencies, U.S. Officials Suspect. (13 December 2020)
https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html
Wall Street Journal, U.S. Agencies Hacked in Foreign Cyber Espionage Campaign Linked to Russia (13 December 2020)
https://www.wsj.com/articles/agencies-hacked-in-foreign-cyber-espionage-campaign-11607897866
Microsoft, Behavior:Win32/Solorigate.C!dha (12 December 2020)
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Behavior:Win32/Solorigate.C!dha&ThreatID=2147771132&ranMID=24542&ranEAID=J84DHJLQkR4&ranSiteID=J84DHJLQkR4-P2Jx3ThWWP0JOzpI3p2MgA&epi=J84DHJLQkR4-P2Jx3ThWWP0JOzpI3p2MgA&irgwc=1&OCID=AID2000142_aff_7593_1243925&tduid=%28ir__3mcmiihf29kfq2uqkk0sohzn3m2xsqgxwup3yqgm00%29%287593%29%281243925%29%28J84DHJLQkR4-P2Jx3ThWWP0JOzpI3p2MgA%29%28%29&irclickid=_3mcmiihf29kfq2uqkk0sohzn3m2xsqgxwup3yqgm00
FireEye, Public GitHub – FireEye Mandiant SunBurst Countermeasures (13 December 2020)
https://github.com/fireeye/sunburst_countermeasures