SolarWinds Orion and UNC2452 – Summary and Recommendations

trustedsec.com/blog/solarwinds-orion-and-unc2452-summary-and-recommendations/

By Nick Gilberti in Incident Response, Incident Response & Forensics December 14, 2020

In the wake of recent revelations regarding a supply chain compromise of the SolarWinds Orion platform by a nation-state actor, and subsequent targeting of private sector and government organizations by said actor, the TrustedSec Incident Response team is releasing the following summary and guidance. This guidance reflects information from industry counterparts as well as recommendations derived from internal experience. To reiterate, this document represents a consolidation of the vast number of useful resources and information being shared by the community; it is intended to provide a convenient source of information and guidance as the situation develops, not to label existing research as our own.

For the purposes of this discussion, we will be referring to the threat actor dubbed “UNC2452” by FireEye and the corresponding malware identified as “SUNBURST,” which has capabilities to deliver a memory-only dropper named “TEARDROP,” which in turn has been observed delivering Cobalt Strike Beacon and other malware.

Highlights

- UNC2452 has been observed leveraging a supply chain compromise to serve backdoored updates for the SolarWinds Orion Platform software.
    - As such, the initial access vector into a target environment is the Orion software itself, rather than "traditional" access vectors such as RDP or phishing.
- Compromised builds of the SolarWinds Orion Platform include versions 2019.4 HF 5 through 2020.2.1, released between March 2020 and June 2020.
    - The malicious update is digitally signed by SolarWinds and has been publicly available since March 2020.
- The threat actor has implemented extensive measures to blend their activity with legitimate SolarWinds behavior, with the goal of evading detection.
- The threat actor has been observed conducting a variety of post-exploitation activities to act on objectives and establish long-term access, including:
    - Adding or modifying federation trusts in Azure AD to accept tokens signed with actor-owned certificates;
    - Adding x509 keys/password credentials to OAuth Applications or Service Principals, often with the goal of reading mail content from Exchange Online services; and
    - Leveraging memory-only droppers to deploy Cobalt Strike BEACON and potentially other backdoors.

Recommendations Related to SolarWinds Orion Product

- Upgrade to Orion Platform version 2020.2.1 HF 1 as soon as possible. [1]
    - Directions for checking which version of the Orion Platform you are using can be found here: https://support.solarwinds.com/SuccessCenter/s/article/Determine-which-version-of-a-SolarWinds-Orion-product-I-have-installed?language=en_US
    - To check which hotfixes you have applied, go here: https://support.solarwinds.com/SuccessCenter/s/article/Verify-hotfixes-that-have-been-installed?language=en_US
    - If you cannot upgrade immediately, follow guidelines available here for hardening your Orion Platform instance:

https://www.solarwinds.com/-/media/solarwinds/swdcv2/landing-pages/trust-center/resources/secure-configuration-in-the-orion-platform.ashx?rev=32603e0c87d84085b081f99a33fe5f4d&hash=62A998B9753957D82BC0F07005D38368

- Namely, ensure your Orion Platform installation is placed behind a firewall, disable Internet access to the Orion Platform, and limit the ports and connections only to what is necessary.
    - SolarWinds expects to release an additional hotfix (2020.2.1 HF 2) on Tuesday, December 15, 2020.
        - This hotfix will replace the compromised software component and provide additional security enhancements.
    - Microsoft recommends considering disabling SolarWinds in your environment entirely, “until you are confident that you have a trustworthy build free of injected code.”
- 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 privileges on SolarWinds servers; and
    - 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.

Recommendations for General Investigation and Hunting

- Block and cross-reference the list of command-and-control endpoints provided in the Indicators of Compromise resources below with remote access logs to identify unauthorized access.
    - Attacker IP addresses will likely be in the same country as the target organization.
    - Use geolocation data to identify instances of “impossible travel,” i.e., if an account logged in from a distance after logging in nearby.
- UNC2452 has been observed mimicking victim hostnames in their command-and-control infrastructure[2]. Querying Internet scanning services such as Shodan for internal hostnames may reveal attacker infrastructure used against your organization.
- Check for a single system authenticating to multiple systems with multiple accounts.
    - This may be difficult without sufficient visibility into network and host-based activity.
- Several antivirus and Endpoint Detection and Response (EDR) products have now implemented detections for the “SUNBURST” malware. Ensuring that anti-virus and EDR data sources are up to date is critical.

Recommendations for Hardening Active Directory[3]

- Ensure that user accounts with administrative rights follow best practices, including the use of privileged access workstations, Just-In-Time/Just-Enough-Admin, and strong authentication.
    - Reduce the number of users that are members of highly privileged Directory Roles, like Global Administrator, Application Administrator, and Cloud Application Administrator.
- Monitor your Active Directory environment for anomalous activity and protect sensitive credentials.
    - Ensure that service accounts and service principals with administrative rights use high entropy secrets, certificates, and are stored securely.
    - Monitor for changes to secrets used for service accounts and service principals as part of your security monitoring program.
    - Monitor for anomalous use of service accounts.
        - Microsoft Azure AD indicates session anomalies, as does Microsoft Cloud App Security, if in use.
- Reduce attack surface by removing/disabling unused or unnecessary applications and service principals.
    - Reduce permissions on active applications and service principals, especially applications with AppOnly permissions.

Indicators of Compromise

Refer to the FireEye GitHub repository for the latest Indicators of Compromise and signatures:

https://github.com/fireeye/sunburst_countermeasures

References and Suggested Reading

[1] https://www.solarwinds.com/securityadvisory

[2] https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

[3] https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/

For a full Incident Response playbook on responding to the Sunburst backdoor, see “SolarWinds Backdoor (Sunburst) Incident Response Playbook” by TrustedSec’s Incident Response Team.