SolarWinds

Supply Chain Attack

CYTEX™

Whitepaper

1. Introduction

The recent Solarwinds and FireEye breach is one of the most elaborate cybersecurity compromises in recent memory. This attack was unprecedented in both its sophistication and scale. Approximately 18,000 Solarwinds customers are known to have been affected. The list of the impacted customers includes a large number of government agencies and numerous Fortune 500 enterprises.

The Solarwinds cyberattack is also significant because it used a data supply chain to gain access infiltrate the target agencies. A separate but less publicized supply chain attack occurred this past summer where the donor data from the major hospitals in the US was stolen following a ransomware attack at BlackBaud hosting services. In the BlackBaud attack, none of the hospitals were directly targeted and many were unaware that their information had been compromised. All of the affected hospitals had to issue breach notifications to comply with the HIPAA breach notification rules while BlackBaud was not required to do so. Many of the publicly traded hospitals also had to file an 8-K with the SEC to report on the breach. Both Solarwinds and FireEye have also filed 8-K reports outlining the security incidents involving their products[1] [2].

Affected hospitals, Solarwinds & FireEye had to file 8-K reports

2. SolarWinds Orion Attack

Solarwinds has disclosed that their system may have been compromised as early as October 2019, when state sponsored cyber criminals gained access to its network management system. The cyber criminals injected a non-malicious file into the Solarwinds system as a test run to see if the file would go undetected.

[1] https://investors.fireeye.com/node/14776/html
[2] https://investors.solarwinds.com/financials/sec-filings/default.aspx

In the actual attack, the cybercriminals replaced a dynamically linked file "solarwinds.orion.core.businesslayer.dll" that contained the malware. The attacker's likely chose SolarWind's Orion platform because it is widely used by IT staff to monitor network devices and servers. Since this software requires elevated user permissions to run, once compromised, it enabled the attackers to latterly move between systems, reshape the traffic, and install additional identity tokens without being noticed.

After the malicious program was installed, the tainted version of the SolarWinds Orion plug-in masqueraded network traffic as the Orion Improvement Program (OIP) protocol to communicate with its command-and-control center to download and execute malicious commands. The malicious commands included file transfers, file execution, disabling system services, and network reconnaissance. The command center was hosted at "asvsmcloud.com" and the attackers used VPN servers in the same country to obfuscate IP addresses and evade detection. The malicious program communicated with the command center using HTTP and the command center responded through DNS CNAME fields that provided further information on which domain to contact for the next set of commands to execute. The bot used a DAG subdomain generation algorithm to generate a list of domains[3]. The malware's capability to generate subdomains to vary DNS request is interesting but once discovered, it was also easy to sinkhole it from spreading.

3. Credential Compromise

The genesis of the Sunburst/Orion/Solarwinds attack was due to a compromised credential. The attackers either used a known password or a credential authentication bypass to gain access to the Solarwinds development environment, where they were able to introduce the infected dll file.

[3] https://pastebin.com/b6f2rkBP

4. Endpoint Failure

None of the device agents and virus programs at the affected sites were able to identify the infected Orion dll file. This was primarily because SolarWinds had provided guidance to exclude its runtime binaries from the virus scanning list for improved performance[4].

5. Detection

The following forensics steps can identify if an organization has been breached:

- Check your current and historical DNS traffic to see if any queries are directed to avsvmcloud[.]com
    - If there are DNS queries to avsvmcloud[.]com, check the responses to see if a CNAME is returned
- Check if there are any DNS queries or connection to the known endpoints[5].
- Are there any unexpected DNS queries from the SolarWinds products in the past few months?
- Did SolarWinds make any HTTP/HTTPS requests to sites that can't be explained?

Additionally, the following steps can mitigate the damage until a thorough investigation is completed to assess the damage.

- 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.

[4] https://support.solarwinds.com/SuccessCenter/s/article/Files-and-directories-to-exclude-from-antivirus-scanning-for-Orion-Platform-products?language=en_US
[5] https://github.com/fireeye/sunburst_countermeasures

    - 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.

6. Prevention

The following sections provide some recommendation on developing preventive measures to thwart future cyberattacks.

6.1. Data Supply Chain

The recent data supply chain attacks have shown that enterprises need to be vigilant and pay attention to their security posture beyond the perimeter. Organizations need to be aware of their vendor's trust worthiness, which can be performed with this five-stage process model:

1. Inventory all data partners
2. Prioritize data vendors and partners according to business needs
3. Assess the data partners and conduct vulnerability assessments, data custodianship analysis, and regulatory compliance checks
4. Assign a risk and impact score to after each partner analysis
5. Conduct regular evaluations and determine the frequency by partner's risk, importance, and impact score

6.2. DNS Monitoring

DNS monitoring should be a part of every enterprise's security arsenal. Active DNS monitoring and filtering can reveal malware connections to its command and control, cut down on phishing site visits, identify malicious domains, and enforce usage policies.

In the Solarwinds attack, the installed malware also generated DGA subdomains that were used to connect to its command center and extract new command instructions. Once the DGA subdomains were identified, FireEye and Microsoft security teams worked together to create a sinkhole by preventing all of the DNS traffic from avsvmcloud[.]com to a list of blocklist IP addresses.

6.3. Authentication Controls

NSA issued an advisory about the abuse of authentication mechanisms[6]. The advisors warned that malicious actors are abusing trust in federated authentication environments to access protected data in the cloud. This requires defenders to use different detection techniques because traditional intrusion detection would not likely discover the techniques, tactics, and procedures that were used to gain access. To defend against these attacks, organizations must pay attention to their Single-Sign-On configuration and harden the on premise or federated identity services. By consolidating identity and access management services in the organizations can relieve themselves from the burden of having to manage an on-premise service and gain more of the protections offered by the cloud service.

6.4. Monitor Cloud Workloads

NSA also offered suggestion to continuously and proactively monitor the cloud workloads. The NSA advisory offers recommendations[7] to harden Azure authentication and authorization configuration in accordance with Microsoft guidance on securing privileged access, enforcement of multi-factor authentication, and guidance on disabling legacy access to the authentication configuration.

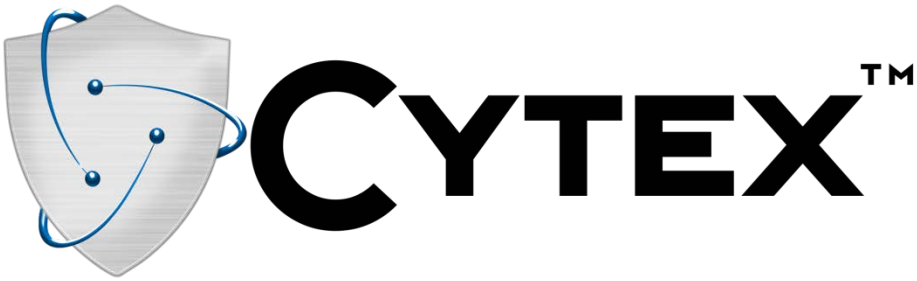
Even though the NSA advisory is focused on Azure cloud infrastructure, the recommendations can be adapted to other workload configuration in Amazon AWS and Google Cloud Services.

[6] https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2451159/nsa-cybersecurity-advisory-malicious-actors-abuse-authentication-mechanisms-to/#pop4744190
[7] https://media.defense.gov/2020/Dec/17/2002554125/-1/-1/0/AUTHENTICATION_MECHANISMS_CSA_U_OO_198854_20.PDF

7. Cytex

Cytex is an innovative suite of applications designed for the SMB market. Cytex readily provides all of the recommended protection and preventive measures to help SMB secure their infrastructure:

- Data supply chain
  - Monitor and assess data partner and vendor risks
  - Score vendors according to risk and impact
- DNS monitoring
  - Malicious domain detection and blocking
  - Phishing domain detection and blocking
  - DAG subdomain detection
  - Policy enforcement
  - Traffic shaping to isolate domains
- Authentication controls
  - Control access to on-premise and cloud applications with SSO
  - Support for multifactor authentication
  - Streamline user onboarding and offboarding
- Cloud workload monitoring
  - Monitor and identify misconfigured cloud workload configurations
  - Continuously monitor cloud workloads for configuration changes
  - Assess workloads using recommended best practices
  - Support for AWS, Azure, and Google Cloud



All-in-One solution for SMB data protection & compliance

Learn more at cytex.io
Follow us on Twitter @cytexsmb >> Watch us at YouTube Cytexsmb