SolarWinds Backdoor (Sunburst) Incident Response Playbook

trustedsec.com/blog/solarwinds-backdoor-sunburst-incident-response-playbook/

By TrustedSec in Incident Response, Incident Response & Forensics, Research, Security Remediation, Security Testing & Analysis, Technical Counter Surveillance Measures, Threat Hunting

December 17, 2020

Over the last several days, TrustedSec has received queries on the best ways to contain, eradicate, and remediate the SolarWinds backdoor (aka #solarigate aka Sunburst). The TrustedSec Incident Response team has put together a playbook of recommended actions to provide some level of assurance that your organization is no longer affected by the backdoor.

This is almost the worst-case scenario for many organizations: an advanced, state-sponsored actor (may have) had an undetected backdoor into your network for months. Even worse, the system(s) that backdoor was on had full access to your environment. Due to this, as many others in the industry have stated, organizations have to assume they have been fully breached. Therefore, the following playbook operates under this assumption.

Two (2) notes before we get started:

1. Even if you have already taken steps to respond, we recommend looking through this list. There may be something you did not think of.
2. Do not blindly take all the actions below. Every organization must perform their own due diligence of determining what the effects of the actions below are and to ensure that the organization is OK with those effects.

Investigation

The investigation should take place concurrent to the containment, eradication, and recovery processes. SolarWinds Orion servers should be forensically preserved, if possible, to allow forensic examination. This includes:

- Obtaining live response data, including RAM
- Imaging and hashing the disk
- Saving any network logs (e.g., firewall, NetFlow) of the servers before they are rolled out
- Exporting any centralized logs from the servers before they are rolled out

Since every organization's internal visibility is different, rather than providing a list of tasks to perform when investigating, we have compiled a list of questions that should be answered. For any questions that cannot be answered, organizations should determine what can be put in place in the future to sufficiently answer those questions. Timeframes for all questions should be for as long as your organization has had SolarWinds Orion deployed, going back to March 2020.

User Activity

The accounts mentioned below include both accounts used by SolarWinds Orion to perform its monitoring and management, which are stored within SolarWinds, and local accounts in the Orion server operating system.

- Did accounts authenticate (successful or failed) to any systems or applications that they should not have?

  If you do not have logs that go back that far, you will have to perform a search across locally stored logs in your environment.
- Did accounts receive authentication attempts (successful or failed) from external locations, especially those they have not logged in from before (e.g., on the VPN)?
- Have accounts set off impossible travel alerts?
- Are any suspicious OAUTH applications allowed Mail.Read or Mail.ReadWrite permissions (or excessive permissions) within Office 365?

Network Activity

- Have any systems connected to known command and control (C2) domains or IP addresses?
- Have any systems connected to the DNS sinkhole IP address (20.140.0.1)?
- Have the servers connected to any other external domains or IP addresses?
- Have the servers connected to any internal systems they should not have?
- Have the servers connected to any internal systems at odd times or days?
- Have any new federation trusts been added to existing Azure tenants?

Endpoint Activity

- Is the backdoor Dynamic-Link Library (DLL) still present on the Orion servers?
- Is the backdoor DLL on any other servers? (Hint: Use FireEye Yara signatures or hashes of DLLs to search.)
- Is there any indication of suspicious activity on the Orion servers?
- Is there any indication of suspicious activity on any systems/applications whose credentials were held within the Orion servers?
- Are there any suspicious ASEPs on the servers or remote access software?
- Were any accounts added or reenabled on the Orion servers or any systems or applications to which Orion had administrative access?
- Have all network device configuration files to which Orion had access been validated?
- Have security software (anti-virus, Endpoint Detection and Response (EDR)) detected any suspicious activity or malware on systems?

Post-Exploitation Activity

- Has any post-exploitation activity been detected on any system?

  FireEye reports state that Cobalt Strike has been used as a post-exploitation payload. (https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html) Known files include c:\windows\syswow64\netsetupsvc.dll.
- Has your organization's domain been leaked in RDP SSL certificates online? (Hint: Check Shodan.)

Containment

Containment is the process of stopping the spread of or preventing further damage from an attack.

1. Quarantine the SolarWinds Orion servers that have the backdoor DLL so they cannot communicate with any other network or system. Possible options include:
   1. NULL-routing their IP addresses
   2. Placing the Orion servers in their own network with no access to any other systems or the Internet
   3. Utilizing EDR to contain the systems
   4. Shutting down the servers

      If you go this route, be sure to grab live response forensic data first—it is better to have it and not need it than vice versa.

2. Disable any accounts utilized by SolarWinds Orion to access other devices or communicate in your network. These include:
    1. Orion platform service account
    2. SQL database service account
    3. Any accounts used for application/system/WMI monitoring from Orion
    4. Accounts used by Orion to email/send alerts
    5. SNMP community strings
3. Block network communication to the known C2 domains and IP addresses for all systems. Possible options include:
    1. DNS sinkhole domains
    2. Block IP addresses at firewalls
    3. Block domains and IP addresses in proxy servers
    4. Turn on Sunburst-related IPS signatures
4. Block all Internet access for SolarWinds Orion servers.
5. Configure alerting for any system accessing known Indicators of Compromise (IoCs) of Sunburst or the use of any user ID that has been disabled. This should be done for both endpoint and network monitoring.

Eradication

Eradication is the process of removing an attacker or affected system from an environment.

1. Change passwords for any account used by SolarWinds Orion. User sturdyerde posted an excellent method to do this on SolarWinds' community forum. (https://thwack.solarwinds.com/t5/NPM-Discussions/When-you-have-to-change-all-passwords-for-the-Orion-monitoring/td-p/613340)
2. Change any shared passwords for accounts that were on the SolarWinds Orion servers. This includes shared local account passwords or service accounts on the system.
3. Change the passwords or community strings that are stored within Orion to perform monitoring.
4. If this was not done in the containment phase, remove the Orion servers from the network.

Note that instead of changing passwords for accounts, some reports have suggested that it is faster and easier to create new accounts and remove the old accounts used in and by SolarWinds Orion.

Recovery

Recovery is the act of bringing systems back to normal operations.

1. Back up the SolarWinds configuration and database.
    1. Information on how to do this should be in the SolarWinds Orion documentation.
2. Rebuild the operating system from a known good golden image.
3. Install SolarWinds version 2020.2.1 HF 2. (https://www.solarwinds.com/securityadvisory)
4. Ensure security and endpoint visibility onto the server.
5. Restore the data from the backed-up configuration and database.
6. Verify the cryptographic hashes of the SolarWinds.Orion.Core.BusinessLayer.dll file installed to ensure that the backdoor DLL is no longer present.
    1. Hashes can be found in the Microsoft customer guidance.

Alternatively, it may not be possible to completely rebuild the server from scratch, although this is our preferred and recommended method. If you cannot do this, perform the following:

1. Back up the SolarWinds configuration and database.
2. Install the hotfix for SolarWinds Orion 2020.2.1 HF 2.
3. Ensure security and endpoint visibility into the servers.
4. Verify the cryptographic hashes of the SolarWinds.Orion.Core.BusinessLayer.dll file installed to ensure that the backdoor DLL is no longer present.

If you take the restore approach rather than the rebuild approach, you still need to perform containment and eradication procedures!

Regardless of which approach is taken, the following recovery activities also need to occur:

1. Remove any temporary containment measures that were put into place.
2. Ensure endpoint and network alerting is configured for the following:
    1. Presence of any known IoCs
    2. Use of accounts in a suspicious manner (e.g., a SolarWinds service account trying to log in to the VPN)
3. Ensure all network and endpoint security software is up to date on signatures, including those related to Sunburst.

References to Lists of Known Indicators

- https://github.com/fireeye/sunburst_countermeasures
- https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/