Sunburst Hack: Best Practices, Identifying And Mitigating - Check Point Blog

By etal

Published: 2020-12-21 · Archived: 2026-04-20 02:13:13 UTC

Introduction

During the closing weeks of 2020 a Cyber Security attack became one of the main headline news stories of what had already been a news-rich year. Attributed to a campaign that began months earlier, the information security teams of government agencies and private organizations quickly shifted their focus to a vulnerability in the SolarWinds Orion solution, which could open a backdoor into organizational communications networks. Dubbed Sunburst, this incident called into question the trustworthiness of the primary technology tools that organizations use to manage their corporate technology resources.

As with any security incident, security practitioners would initially focus on identifying signs of potential Sunburst activities in their networks and systems. From there they would prioritize immediate remediation activities. Once these initial efforts were complete, security teams would need to consider broader structural changes to their security programs.

This blog provides information intended to assist with these primary phases and is structured according to the following flow:

1. A summary of the Sunburst breach
2. Network mitigations
3. Host remediation
4. Additional considerations
5. Potential considerations for longer-term security improvements, including guidance on DevOps, Endpoint and cloud environments, according to the Zero-Trust Architecture framework

Some of the recommendations included in this blog apply to what was known about the Sunburst event at the time of writing. Check Point will update the document as more information becomes available.

Individuals interested in speaking with Check Point about Sunburst and other security topics are invited to interact with their account teams and to contact Check Point via the contact details listed on its public website at: https://www.checkpoint.com/

About the Sunburst event

On the 8th of December 2020, FireEye, a US-based Cyber Security company, notified the market that it was attacked by what the company believed was a nation-state actor who gained access to some of FireEye's Red Team tools.

Five days later, on the 13th of December 2020, reporting in major US news outlets indicated that US government agencies had been breached in what appeared to be a complex Cyber Attack, and on that same day the US Cyber & Infrastructure Security Agency (CISA) issued an emergency directive to all US Federal civilian agencies to "review their networks for indicators of compromise and disconnect or power down SolarWinds Orion products immediately."

The CISA notification was followed by a SolarWinds filing with the Securities and Exchange Commission (SEC). That filing noted that SolarWinds was made aware of a "cyberattack that inserted a vulnerability within its Orion monitoring products which, if present and activated, could potentially allow an attacker to compromise the server on which the Orion products run."

SolarWinds Orion

SolarWinds Orion is an enterprise software suite that includes performance and application monitoring and network configuration management. SolarWinds Orion is used to monitor and manage on-premise and hosted infrastructures. To provide SolarWinds Orion with the necessary visibility into this diverse set of technologies, it is common for network administrators to configure SolarWinds Orion with pervasive privileges, making it a valuable target for adversary activity.

According to the Cybersecurity and Infrastructure Security Agency (CISA), the SolarWinds Orion export, Sunburst, was a supply chain attack that compromised and impacted several U.S. government agencies, critical infrastructure entities. The incident also affected private sector organizations using an advanced persistent threat (APT) attack that started in March 2020.

According to the CISA's analysis, the threat actor added a malicious version of the binary solarwinds.orion.core.businesslayer.dll into the SolarWinds software lifecycle, which was then signed by a legitimate SolarWinds code signing certificate.

The compromised binary, once installed, calls out to a victim-specific avsvmcloud.com domain using a protocol designed to mimic legitimate SolarWinds protocol traffic. After the initial check-in, the hacker can use the Domain Name System (DNS) response to selectively send back new domains or IP addresses for interactive command and control traffic (C&C).

SolarWinds Orion typically uses a significant number of highly privileged accounts to perform normal business functions. Successful compromise of one of these systems can therefore enable further action. Consequently, entities that observe traffic from their SolarWinds Orion devices to avsvmcloud.com should not immediately conclude that the hacker leveraged the SolarWinds Orion backdoor. Instead, additional investigation is needed into whether the SolarWinds Orion device engaged in further unexplained communications.

According to the CISA advisory, the following SolarWinds Orion products were impacted:

- Orion Platform 2019.4 HF5, version 2019.4.5200.9083
- Orion Platform 2020.2 RC1, version 2020.2.100.12219
- Orion Platform 2020.2 RC2, version 2020.2.5200.12394
- Orion Platform 2020.2, 2020.2 HF1, version 2020.2.5300.12432

Broader significance of the incident

Among the next steps that the attacker took after establishing the initial foothold was to compromise the Security Assertion Markup Language (SAML) signing certificate using escalated Active Directory privileges. Once this was accomplished, the hacker created unauthorized but valid tokens (token id) and presented them to services that trust SAML tokens from the environment. These tokens can then be used to access resources in hosted environments, such as email, for data investigation and exfiltration via authorized application programming interfaces (APIs).

SAML is used by many business applications, including:

- SaaS Applications that requires SAML for single-sign-on (Business Applications, Email Services e.g.)
- File storage services (such as SharePoint, OneDrive for Business)
- Kubernetes and Containers environments that requires Active directory

These types of solutions are important for espionage and data collection efforts. Access to email and file repositories provides visibility into troves of interesting communications and content.

MITRE ATT&CK® Techniques used in Sunburst attack

The MITRE ATT&K® framework helps provide context to the Sunburst campaign. The following represent known tactics and techniques:

- Query Registry [T1012]
- Obfuscated Files or Information [1027]
- Obfuscated Files or Information: Steganography [T1027.003]
- Process Discovery [T1057]
- Indicator Removal on Host: File Deletion [T1070.004]
- Application Layer Protocol: Web Protocols [T1071.001]
- Application Layer Protocol: DNS [T1071.004]
- File and Directory Discovery [T1083]
- Ingress Tool Transfer [T1105]

- Data Encoding: Standard Encoding [T1132.001]
- Supply Chain Compromise: Compromise Software Dependencies and Development Tools [[T1195.001]
- Supply Chain Compromise: Compromise Software Supply Chain [T1195.002]
- Software Discovery [T1518]
- Software Discovery: Security Software Discovery [T1518.001]
- Create or Modify System Process: Windows Service [T1543.003]
- Subvert Trust Controls: Code Signing [T1553.002]
- Dynamic Resolution: Domain Generation Algorithms [T1568.002]
- System Services: Service Execution [T1569.002]
- Compromise Infrastructure [T1584]

Security practitioners interested in reviewing comprehensive lists of indicators of compromise can find them in multiple online publications. The CISA alert referenced below is one such example.

This event continues to evolve and researchers are providing updated information on a regular basis. The following sources provide relevant background:

- Check Point blog post: https://blog.checkpoint.com/2020/12/16/solarwinds-sunburst-attack-what-do-you-need-to-know/
- CISA alert (AA20-352A): https://us-cert.cisa.gov/ncas/alerts/aa20-352a
- FireEye research: https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
- Microsoft publication: https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/

Mitigations in the network

An appropriate first step in identifying presence of malicious activity within the corporate environment is to analyze network traffic for potential attack indications. Relevant functions that can assist in this effort include: signature and heuristic analysis of potential malware, identification of outbound command and control traffic involved in the attack process and intrusion prevention signatures for signs of potential exploit. The easiest way to leverage such capabilities is to activate protections within security technologies operating in the network.

Check Point gateways include an array of technologies that can assist with network-level remediation and investigation efforts. Customers with gateways (physical and virtual) who are licensed for Next Generation Firewall (NGFW), Next Generation Threat Prevention (NGTP) or Next Generation Threat Prevention and SandBlast (SNBT or what was previously known as NGTX) need only update their protection packages or activate automatic updating to protect their networks from elements of the Sunburst attack:

Protection	**Software Blade**	**License Bundle**
Trojan.Win32.SUNBURST.TC.XXX	Anti-Virus	NGTP/SNBT
HackTool.Wins.FE_RT.A<XX>	Threat Emulation	SNBT

Backdoor.Win32.SUNBURST.XX	Anti-Bot	NGTP/SNBT
Backdoor.Win32.Beacon.<A-H>	Anti-Bot	NGTP/SNBT
Sunburst Backdoor Suspicious Traffic (CPAI-2020-1309)	IPS	NGFW/NGTP/SNBT

Check Point will continue to update its indicators and to add more identifiers as they become available. These will be added to Check Point's ThreatCloud platform on a real-time basis.

Automated event analysis

Critical to Sunburst remediation efforts is the ability to find evidence of impact quickly. Automated event analysis tools play an important role in such investigative efforts. Check Point makes this possible with its InfinitySOC solution.

Check Point researchers have integrated publicly available Sunburst indicators as well as proprietary intelligence data into InfinitySOC. Administrators can leverage the cloud-based platform to search for Sunburst indicators within network, cloud and endpoint environments. The solution also provides event investigation tools to drill-down into findings to validate and plan remediation steps.

In the following screenshot we see identified Sunburst indicators with their corresponding addresses, associated risk levels attack family association. In addition we see timeline charts that represent the number of connections to the Sunburst indicators.

Information on InfinitySOC is available via Check Point's website

Automated Sunburst logging

The logging and reporting functions built-in to Check Point's management suite have also been updated to search for Sunburst indicators. Organizations can leverage their existing management platforms to query log data for the

known indicators.

Security CheckUp

Customers who do not employ Check Point network protections or are not licensed for these capabilities can leverage a quick assessment process called Security CheckUp. This process does not impact production traffic.

To perform a Security CheckUp, an organization would work with a Check Point engineer to install a security gateway on a mirror port or elsewhere in the network. Once in-place, the activated device will immediately generate event data associated with the Sunburst attack and other threats.

Information on how to run a Security CheckUp is available on the Check Point website

The host: a primary target

As covered in multiple descriptions of the Sunburst attack (see section “About the Sunburst event” above), a primary vector used in this attack was a vulnerability that was inserted into the SolarWinds Orion platform, specifically vulnerable versions noted earlier in this document. The installation of these updates on the server included a file, SolarWinds.Orion.Core.BusinessLayer.dll, backdoor that the attacker would use to connect to the server and initiate additional changes. As with any security incident targeting a server or computer, such changes might include modification to directories and files or configuration elements. Depending on where an attacker is in her or his timeline, such changes can become indicators of an attack in progress. Or, if an attacker was insufficiently adept at cleaning her or his tracks, these modification can also be used to identify if a machine was compromised.

While certainly standard practice, it is important to note that organizations should never take the protection of servers and computers for granted. Thus, even though this specific attack would have bypassed traditional server-level access control and malware prevention, the success of this attack does not mean that best practices based on least privilege and host-based threat prevention are no longer relevant. Indeed, in some ways, these sort of events remind us that fundamental security controls are more important today than ever before.

Threat hunting

A crucial first step in identifying affected machines is to establish visibility into events affecting servers and computers. These would include changed files, activated processes, changes to system registry and network activity entering and leaving potentially impacted machines.

Organizations should also perform full forensics evaluation of an Orion server's storage devices, which can only be performed after taking the server offline.

Check Point provides powerful solution to assist with assessment efforts of threats targeting servers and computers. The company's SandBlast Agent includes a unique Threat Hunting capability that provides detailed visibility into infected assets and correlates such activity with the MITRE ATT&CK™ Framework. The solution also include attack diagnostics and remediation capabilities that enable administrators and incident response teams to triage and resolve attacks quickly.

Activating Threat Hunting is a very simple process. An administrator would open the user interface, access either the "Threat Prevention" or "Forensics" tabs of the "Policy" section and toggle the "Threat Hunting" switch to "On." From there the only additional required step is to save the policy change and install it on the management server.

Once this change has been made, SandBlast Agents operating within the environment will populate data into the Threat Hunting interface, which administrators can use to hunt for related events.

As shown in the screenshot below, and since the initial announcement of the Sunburst attack, Check Point has updated the pre-defined queries of the Threat Hunting solution to look for Sunburst indicators automatically. This

is intended to simplify the search for indicators of Sunburst activity and to enable organizations to rapidly determine risk levels and define remediation plans.

Information on SandBlast Agent is available on the Check Point public website at: https://www.checkpoint.com/products/advanced-endpoint-protection/. Customers interested in activating the Threat Hunting capabilities of the solution can follow the simple steps outlined in the document entitled, "SandBlast Agent Threat Hunting Onboarding," which is available on Check Point SecureKnowledge repository (SK: 170052).

Additional considerations

Organizations impacted by the Sunburst incident reported malicious activity targeting Security Assertion Markup Language (SAML) use cases. It is therefore critical to consider a series of practical changes to SAML practices, including:

1. Strengthen credentials by enforcing multi-factor authentication for users and devices
    1. Avoid long SAML token durations, for example to a time-limit of no longer than one hour
    2. Monitor tokes for identical timestamps, which would indicate abnormal behavior
    3. Look for tokens that have associated logins with user accounts within an hour of the token's initial generation
2. Monitor all services for unusual sign-ins, changes to tokens or keys
    1. Considering the nature of the Sunburst attack, potentially pay special attention to Office365
3. Reset/replace/re-issue all sensitive API key integrations, such as those leveraged by multi-factor, SAML integrations, website configuration files and others
4. Look for network specific artifacts, especially API calls that reference cloud assets and services

Should the SolarWinds Orion solution continue to be used, it is imperative that organizations:

1. Reset all credentials used by or stored in SolarWinds software

2. Treat all hosts monitored by the SolarWinds Orion monitoring software as compromised by threat actors and assume that further persistence mechanisms have been deployed
3. Rebuild hosts monitored by the SolarWinds Orion monitoring software using trusted sources

Coverage of the Sunburst incident suggested that cloud-based services were among the primary targets of the threat actors. As organizations move more services to cloud, it is becoming increasingly important to understand potential risks to Infrastructure as a Service (IaaS) implementations.

Cloud security posture management (CSPM) solutions can be beneficial to quickly identify potential deviance from best practice. They include out-of-the-box regulatory compliance and best practice assessment tools. These review configuration settings within cloud systems and highlight areas of concern in how applications and services interact within cloud environments.

The Check Point CloudGuard CSPM offering provides a rich array of such assessment frameworks, including automated assessments based on the Azure CIS Foundation v. 1.1.0, including inspections for multi-factor authentication and other critical identity and access management (IAM) considerations.

Information on Check Point's CSPM offering is available online

Going forward: lessons learned and next steps

Security incidents present an opportunity to reevaluate and improve information security programs comprehensively. They show us threat vectors that we previously might have overlooked and raise awareness across the organization to the need to improve existing or implement new controls.

In light of the critical nature of the Sunburst attack, Check Point recommends that organizations take a number of steps that potentially can be beneficial in reducing future risk, including:

1. Security Architecture – consider aligning security programs to the Zero-Trust model, which embraces macro and micro segmentation of network to block lateral malware movement (East-West) within the network, data center domain and cloud
2. Advanced Threat Prevention – all environments should be protected with deep packet inspection technologies and protections for persistent and complex threat vectors, which would include Next Generation firewalling to protect network segments and workloads in the virtual fabrics (e.g. VMWare, Public IaaS)
3. Cloud workload protection – Kubernetes/Container nodes should be protected with (Cloud Workload Protection Platform (CWPP) functions, such as: network access control, Anti-Bot, CloudBots, Anti-Virus and Sandboxing
4. DevSecOps – ensure that software development environments are assured by a security posture management solution (CSPM) along with CI/CD pipeline development processes that incorporate threat hunting analysis and source code scanning, including library verification when downloaded from external resources
5. Endpoint – as a main target and attack vector, endpoint security should be viewed within the context of Zero Trust Network Access (ZTNA) and endpoint protections need to be enriched with next generation protections

The following sections provide additional detail on elements of the above recommendations.

Architectural considerations

Considering the lateral movement elements of the Sunburst attack, an assessment of existing network segmentation practices would be very relevant. This would include ensuring that network-level access control enforces segmentation according to the principles of least privilege. Core functions and critical data repositories should be firewalled from other parts of the network with strict rules that limit user, network and application access only to the bare minimum of resources. In addition, traffic flows should be controlled to prevent access from Internet-connected systems, even those that require periodic connections to vendor software updates.

For organizations that have moved much, or are in the process of moving their services to Azure-specific instances, Check Point recommends a security architecture approach that leverages multiple layers of protection. This approach incorporates:

- Advanced threat prevention across the environments and between Azure and private data centers
- Macro and micro-segmentation within the Azure IaaS functions
- Access control according to a hub and spoke design
- Centralized security policy management within the cloud or on premise
- Cloud security posture management
- Cloud-delivered threat prevention for user traffic to SaaS applications and general Internet traffic
- API-level inspection for rogue connections and embedded threats
- Automated forensics of host and user events and threats

The below diagram summarizes the above points into a network topology. More information on this design recommendation is available on the Check Point webiste's best practices section, at: https://www.checkpoint.com/architecture/security-best-practices/**.**

Cloud Native Application Protection Platform

Besides countermeasures to detect and mitigate challenges presented by attacks such as Sunburst, organizations should also consider augmenting their methods for ensuring code integrity. With the possibility of “Copy Cat” attacks and the accelerated development timelines associated with cloud technologies and CI/CD practices, the risk of future Supply Chain attacks making their way into new software packages is especially relevant.

The diagram below, which was proposed by Gartner, provides a unified overview with multiple security control areas. The concept building blocks are Cloud Security Posture Management, Cloud Workload Protection Platform and Cloud Network Security.

CI/CD pipeline security

These recommendations can also be applied to the CI/CD pipeline. Code-level vulnerabilities can be identified through code analysis, containers can be assessed with associated elements, such as the libraries used in the development process, and application monitoring can be performed with advanced automated methods.

Sunburst teaches us that attackers can maintain persistence for extended periods of time. It therefore is increasingly important to consider control plane protections. These mechanisms could be implemented with admission controllers and runtime engines, which include advanced and modern technologies such as Machine Learning and Artificial Intelligence for behavioral analysis.

The suggested approach incorporates:

- Secure application development: ensure proper logging, static, dynamic and interactive application security testing (SAST/DAST/IAST) of code and dependencies
- Configuration and settings: implement reliable secrets management (ConfigMaps only for insecure data, secret resources for sensitive information/credentials), mount secrets as volumes and not environment variables
- Governance: Use pod security policies (disable privileges, use read-only file systems), enforce network policies, use Role-Based Access Control (RBAC)
- Posture management: reference CIS Kubernetes Benchmark, NIST.SP.800-190 and others

Suggested Architecture for Kubernetes environments

With corporate systems quickly moving to container-based approaches, the need for cloud native protection strategies has become more critical. Check Point recommends considering a Zero-Trust approach to protecting Kubernetes environments. Following this approach would isolate development, testing and production environments, including limiting and inspecting traffic between services (namespaces) as much as possible.

The security organization needs to play a role in cloud and agile development. It needs to ensure that standards apply and that protections exist for risky communications. DevOps and DevSecOps partner with security to manage platforms and application tiers

Organizations interested in working with Check Point on understanding a secure transition cloud-driven technology strategies can participate in the company’s unique security architecture workshop program.

Information on this unique service can be obtained through their Check Point account team or online at: https://www.checkpoint.com/support-services/security-workshop/.
Customer can also reference more detailed architectural recommendations on the Check Point best practice site, at: https://www.checkpoint.com/architecture/security-best-practices/.

Summary

While much about the SolarWinds Sunburst and related attack activities remain unknown, available information suggests the involvement of a highly capable nation-state actor who was able to build a Supply Chain attack that impacted many high profile organizations.

The tactics employed by the threat actor successfully bypassed the security precautions of sophisticated security teams. Nevertheless, this event serves as an opportunity for security practitioners to leverage the event to learn lessons and identify opportunities to improve security strategies.

Outlined in previous pages were practical steps that organizations can take to identify and mitigate the effects of a Sunburst incident. The guidelines above remind us that the traditional security practices of least privilege and segmentation can reduce the potential impact of even the most advanced attacks. In addition, automated analysis and advanced threat prevention techniques arm us with new capabilities to identify potential attacks and respond to them more quickly than ever before.