BlueTeam CheatSheet * SolarWinds Events* | Last updated: 2020-12-24 1334 UTC

By 262588213843476

Archived: 2026-04-05 23:51:58 UTC

SolarWinds Supply-chain Compromises

Detections

General

- This section aims to provide the detections released by security companies to detect the malwares / files linked to SolarWinds supply-chain compromise events. We kindly remind you that this detections signatures could / will evolve in the next days, stays updated by checking the vendors resources to have the last information.

Warning

- SolarWinds in a support article now removed, asked the organizations to exclude SolarWinds products paths of the anti-virus scans. If it is an understandable practice to not impact SolarWinds products functions, the following detections will not work if the installation paths exclusions are not removed first.

Security Products

FireEye

- Their indicators (Network and File hashes) are available on their GitHub repository . There are also detections rules for Snort, Yara, IOC & ClamAV formats.
- Their products rules covering the detection:
    - APT_Backdoor_MSIL_SUNBURST_1
    - APT_Backdoor_MSIL_SUNBURST_2
    - APT_Backdoor_MSIL_SUNBURST_3
    - APT_Backdoor_MSIL_SUNBURST_4
    - APT.Backdoor.MSIL.SUNBURST
    - SUNBURST SUSPICIOUS FILEWRITES (METHODOLOGY)
    - SUNBURST SUSPICIOUS URL HOSTNAME (METHODOLOGY)
    - SUNBURST SUSPICIOUS CHILD PROCESSES (METHODOLOGY)
    - SUNBURST COMPROMISE INDICATORS
    - APT_Webshell_MSIL_SUPERNOVA_2
    - APT_Webshell_MSIL_SUPERNOVA_1

    - APT_HackTool_PS1_COSMICGALE_1
    - APT_Dropper_Raw64_TEARDROP_1
    - APT_Dropper_Win64_TEARDROP_2
    - Backdoor.BEACON

Sources

- Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor
- FireEye Github dedicated repo

Microsoft

- Microsoft detects the threat with Windows Defender signatures available with detection release 1.329.368.0 or higher.

Detection for backdoored SolarWinds.Orion.Core.BusinessLayer.dll files:

- Trojan:MSIL/Solorigate.BR!dha

Detection for Cobalt Strike fragments in process memory and stops the process:

- Trojan:Win32/Solorigate.A!dha
- Behavior:Win32/Solorigate.A!dha

Detection for the second-stage payload, a cobalt strike beacon that might connect to infinitysoftwares[.]com:

- Trojan:Win64/Solorigate.SA!dha

Detection for the PowerShell payload that grabs hashes and SolarWinds passwords from the database along with machine information:

- Trojan:PowerShell/Solorigate.H!dha

Sources

- Microsoft Security Response Center - Solorigate Resource Center
- Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers

Symantec

- Tools associated with these IOCs will be detected and blocked on machines running Symantec Endpoint products .

File-based protection:

- Backdoor.Sunburst
- Backdoor.Sunburst!gen1
- Backdoor.SuperNova
- Backdoor.Teardrop

Network-based protection:

- System Infected: Trojan.Backdoor Activity 244

Sources

- Sunburst: Supply Chain Attack Targets SolarWinds Users

Kaspersky

- Kaspersky products protect against this threat and detect it with the following names:

- Backdoor.MSIL.Sunburst.a
- Backdoor.MSIL.Sunburst.b
- HEUR:Trojan.MSIL.Sunburst.gen
- HEUR:Backdoor.MSIL.Sunburst.gen
- Backdoor.MSIL.Sunburst.b

- Kaspersky Behavior Detection component detects activity of the trojanized library a:

- PDM:Trojan.Win32.Generic.

- Kaspersky IoA Tag "Sunburst"

- Kaspersky Anti-Targeted Attack Platform detects Sunburst traffic with a set of IDS rules with the following verdicts:

- Trojan.Sunburst.HTTP.C&C
- Backdoor.Sunburst.SSL.C&C
- Backdoor.Sunburst.HTTP.C&C
- Backdoor.Sunburst.UDP.C&C
- Backdoor.Beacon.SSL.C&C
- Backdoor.Beacon.HTTP.C&C
- Backdoor.Beacon.UDP.C&C

Source

- How we protect our users against the Sunburst backdoor

MalwareBytes

- MalwaresBytes released its signatures with a blog post , watch the following:
- Backdoor.Sunburst
- Backdoor.WebShell

Sources

- SolarWinds advanced cyberattack: What happened and what to do now

McAfee

- Coverage for all known binaries used in this attack will be covered in the 4287 V3 DATs (ENS) and the 9835 V2 DATs (VSE, Web Gateway) to be released on December 14, 2020, and in GTI for cloud-connected systems.
- The Extra.DAT contains more generic detection capabilities tentatively scheduled to be included in the 4288 V3 DATs (ENS) and the 9836 V2 DATs (VSE). These DATs are to be released on December 15, 2020.
- The detection name for threats in this attack is "HackTool-Leak.c" before the 4288 V3 DATs (ENS) and the 9836 V2 DATs (VSE, Web Gateway). After these DATs, the detection name for threats in this attack is Trojan-Sunburst.
- For customers who cannot update DATs or who are not using On-Access Scanning / On-Demand Scanning, Exploit Prevention coverage can be configured using the following Expert Rules. The Rule content is also available in the attached Sunburst_Expert_Rules.zip.

Sources:

- KB93861: McAfee coverage for SolarWinds Sunburst Backdoor
- SUNBURST Malware and SolarWinds Supply Chain Compromise
- MVISION Insights Campaign: SolarWinds Supply Chain Attack Affecting Multiple Global Victims With SUNBURST Backdoor

Sophos

- Sophos has an article regarding the playbook for incident response that includes good knowledge on how to use the Sophos tools.
- Their detections signatures are the following ones:
    - Troj/SunBurst-A.CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp
    - Mal/Generic-S.Solarwinds Worldwide LLC
    - Troj/Agent-BGGA.SolarWinds.Orion.Core.BusinessLayer.dll
    - Troj/Agent-BGGB.SolarWinds.Orion.Core.BusinessLayer.dll
    - Troj/Agent-BGFZ.SolarWinds.Orion.Core.BusinessLayer.dll
    - Mal/Generic-S.OrionImprovementBusinessLayer.2.cs
    - Troj/Agent-BGGC+Mal/Generic-S.app_web_logoimagehandler.ashx.b6031896.dll
    - Mal/Sunburst-A

Sources

- Incident response playbook for responding to SolarWinds Orion compromise
- Sophos GitHub info

SentinelOne

- Following the SolarWinds supply chain attack:

- SentinelOne's Singularity Cloud blocks all reported IOCs
- All SentinelOne customers have access to a new hunting pack which includes custom Deep Visibility hunting queries for the latest SUNBURST and FireEye breach IOCs

Source

- FireEye/SolarWinds: Taking Action and Staying Protected

Palo Alto networks

Cortex XDR

- Cortex XDR customers are protected using the product's WildFire integration, as well as through Local Analysis, the Password Theft Protection module, and the Behavioral Threat Protection (BTP) engine. Protections are continually being evaluated, developed, and deployed for Cortex XDR.

Cortex XDR Managed Threat Hunting

- Our Cortex XDR Managed Threat Hunting Team (MTH) has proactively searched all Cortex XDR Pro customer logs to identify potentially impacted organizations and provide them an assessment of their risk.

WildFire (NGFW security subscription)

- Gap analysis and threat hunting leveraging the FireEye-provided Yara signatures and observables has enabled Unit 42 researchers to identify potential malware samples that we are now analyzing, building and deploying protections for within WildFire.

App-ID

- Using the NGFW's Logs, a customer can get quick situational awareness of layer-7 application data in their environment. Customers looking for SolarWinds activity in their environment could do this from Panorama or NGFW under the Monitor tab and search through Traffic or Unified logs for "(app eq solarwinds)or(app eq solarwinds-rmm)or(app eq solarwinds-msp-manager)or(app eq solarwinds-agent)or(app eq solarwinds-npm)or(app eq solarwinds-sam)or(app eq solarwinds-msp-anywhere)". This could also be viewed in the ACC Network Activity tab and filter by Application. This can be made into a routine check through custom reporting.

AutoFocus

- AutoFocus customers can track SolarStorm's activity in the tags SolarStorm , SUPERNOVA and SUNBURST .

IoT Security (NGFW security subscriptions)

- The IoT Security subscription has the capability of identifying SolarWinds servers. These devices are being added to the IoT Security user portal UI, and the Device-ID attribute will be pushed to PAN-OS. These devices will be displayed to users as "SolarWinds Network Management Device" within the IoT Security user portal UI. In PAN-OS, users will see the Device-ID attribute "Profile" = "SolarWinds Network Management Device". This feature will be enabled for all IoT Security customers this week.

Threat Prevention DNS Security (NGFW security subscriptions)

- Threat Prevention and DNS Security provide protection against C2 beacons and associated traffic. Protections are continually being evaluated, developed, and deployed for Threat Prevention subscription.

URL Filtering (NGFW security subscription)

- As of the time of writing, associated infrastructure described in this blog have accurate verdicts of malware.

Sources

- Threat Brief: SolarStorm and SUNBURST Customer Coverage

Checkpoint

- Check Point covers this threat with the following Threat Prevention products:

Anti-Virus:

- Trojan.Win32.SUNBURST.TC.XXX

Threat emulation:

- HackTool.Wins.FE_RT.A

Anti-Bot:

- Backdoor.Win32.SUNBURST.XX
- Backdoor.Win32.Beacon.

IPS:

- Sunburst Backdoor Suspicious Traffic

Sources

- Check Point response to SolarWinds supply chain attack

Cisco

- Cisco SNORT users are protected by using the following signatures:
  - SIDs 56660-56668
- Cisco also released an informational security advisory to help its customers in the response in case of compromise of Cisco equipment.

Sources

- Threat Advisory: SolarWinds supply chain attack
- SolarWinds Orion Platform Supply Chain Attack

Fortinet

- FortiGuard Labs has AV coverage in place for publicly available samples as:
  - W32/Agent.1BA1!tr
  - W32/Sunburst.A!tr
  - MSIL/Agent.102E!tr
  - MSIL/Agent.C865!tr
  - MSIL/Agent.8448!tr
  - MSIL/Agent.5676!tr
- FortiGuard Labs has released a revised IPS signature that will detect SUNBURST activity which was released in IPS definitions set (16.981):
  - FireEye.Red.Team.Tool

FortiEDR

- For FortiEDR protections, all published IOC's were added to our Cloud intelligence and will be blocked if executed on customer systems.

Web Filtering client

- All network IOC's are blocked by the Web Filtering client.

Sources

- Supply Chain Attack on SolarWinds Orion Platform Affecting Multiple Organizations Worldwide (APT29)

Trend Micro

General

- The malicious files associated with this attack are already detected by the appropriate Trend Micro products as:
    - Backdoor.MSIL.SUNBURST.A
    - Trojan.MSIL.SUPERNOVA.A

Trend Micro XDR

- Trend Micro XDR customers benefit from all detection capabilities of the underlying products such as Apex One. In addition, depending on their data collection time range, XDR customers may be able to sweep for IOCs retroactively if there was potential activity in this range to help in investigation. Some auto-sweeping rules related to this incident have already been enabled for XDR customers.

Trend Micro Cloud One - Workload Security and Deep Security Rules

- In addition to the anti-malware patterns listed above (for customers that utilize the anti-malware module), Trend Micro has released the following rules that helps to block some of the known domains and malicious traffic:
    - Rule 1010669 - Identified Malicious Domain – SolarWinds
    - Rule 1010675 - Identified HTTP Backdoor Win32.Beaconsolar.A Runtime Detection
    - Rule 1010676 - Identified HTTP Trojan.MSIL.Sunburst.A Traffic Request

TippingPoint

- Customers that use Trend Micro TippingPoint technologies also can utilize the following ThreatDV filters:
    - 38626 : HTTP: Trojan.MSIL.Sunburst.A Runtime Detection
    - 38627 : HTTP: Backdoor.Win32.Beaconsolar.A Runtime Detection

Trend Micro Deep Discovery

- The following Deep Discovery Inspector (DDI) rule has been released for this threat in the latest pattern:
    - 4491: DNS_SUNBURST_RESPONSE_SB
- Customers utilizing Deep Discovery technologies such as DDI and Deep Discovery Analyzer (DDAN) may find it useful to use the capabilities of the platform to help investigate potential lateral movement and other detections within the environment.

Sources

- SECURITY ALERT: Sunburst (SolarWinds) Targeted Attack Detection and Investigation with Trend Micro Products

SIEM cheat sheet

IBM QRadar

- IBM employee, Gladys Koska, published a very exhaustive blog post named “SUNBURST indicator detection in QRadar“ detailing how, using QRadar, you can detect the SolarWinds threats:

Sources

- SUNBURST indicator detection in QRadar

Splunk

- Splunk employee, Ryan Kovar, released a blog post named “Using Splunk to Detect Sunburst Backdoor” detailing some requests that can be useful to detect SolarWinds events.

Sources

- Using Splunk to Detect Sunburst Backdoor

Errors, typos, something to say ?

- Feel free to report any mistake directly below in the comment or in DM on Twitter @SwitHak

---