SECURONIX™

Securonix Threat Research:

Detecting SolarWinds/ SUNBURST/ECLIPSER Supply Chain Attacks

Oleg Kolesnikov, Den Iuzvyk
Securonix Threat Research Team
Created: December 8, 2020
Last Updated: January 12, 2021

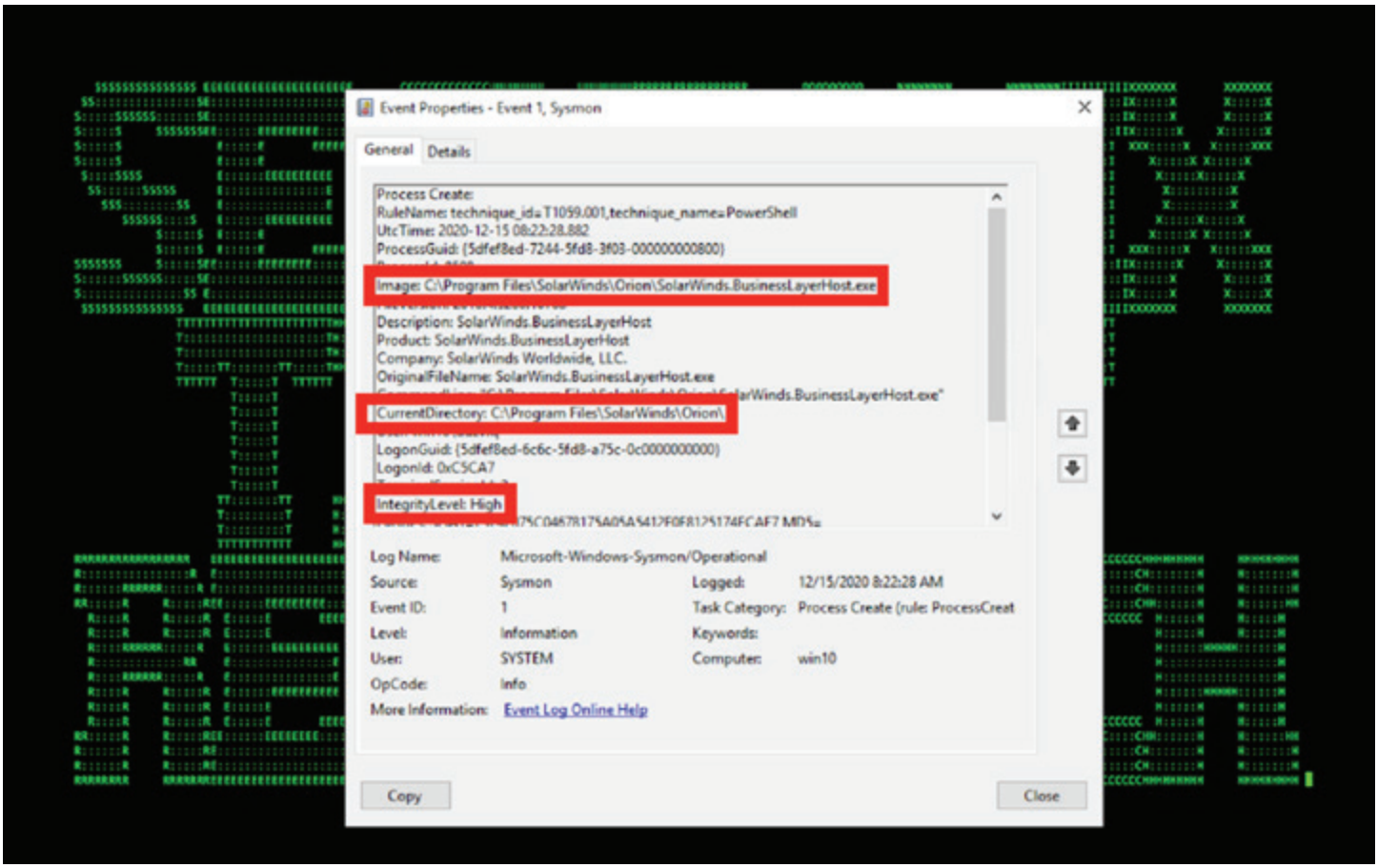
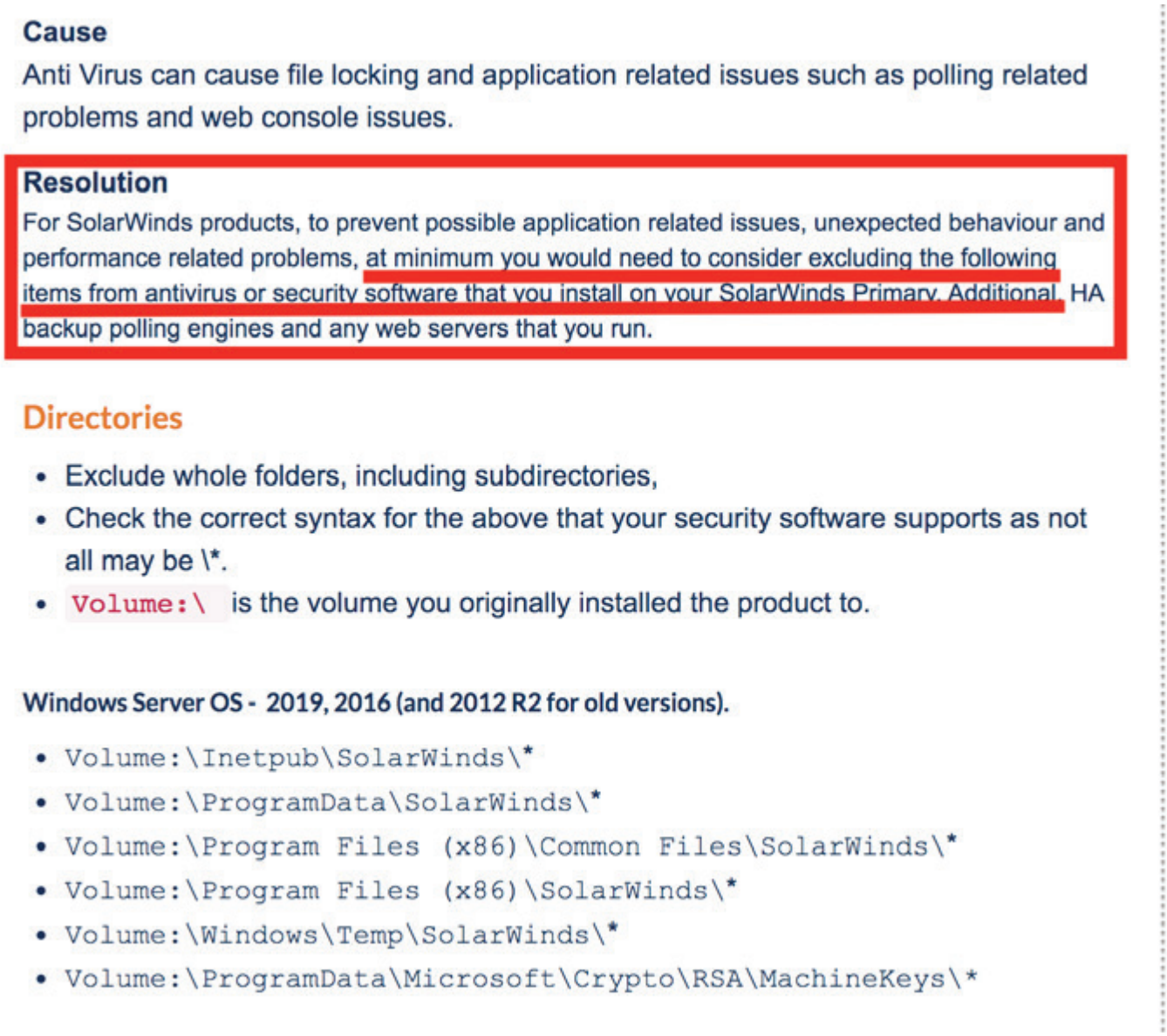


Figure 1: Example of Trojanized SolarWinds With Embedded Malicious Payload Activity in Logs

The Securonix Threat Research (STR) team has been actively investigating the critical ongoing SolarWinds Orion/SUNBURST supply chain attacks (monitored by STR as ECLIPSER) with some of the recent victims being one of the leading security vendors [1] as well as a number of US government entities and other victims targeted as part of attacks involving the compromised SolarWind Orion IT software [5,7].

Below is a summary of what we currently know about the high-profile SolarWinds Orion/ ECLIPSER attacks and our recommendations on some possible Securonix predictive indicators/ security analytics to increase your chances of detecting the current/future variants of the attacks involving the stolen tools as well as leveraging some of the known and unknown associated attack vectors/CVEs.

Update - January 12, 2021 - According to our latest analysis results and the publicly available details, there is a possibility that the SUNBURST/ECLIPSER breach involved a *broader/multi-stage* supply chain attack with potentially some of the tertiary supply chain vendor (JetBrains) build process components, such as, e.g. TeamCity CI/CD with some additional malicious implants possibly leveraging a variant of SUNSPOT [20] to enable backdooring of the main supply chain vendor target (SolarWinds).



Cause

Anti Virus can cause file locking and application related issues such as polling related problems and web console issues.

Resolution

For SolarWinds products, to prevent possible application related issues, unexpected behaviour and performance related problems, at minimum you would need to consider excluding the following items from antivirus or security software that you install on your SolarWinds Primary, Additional, HA backup polling engines and any web servers that you run.

Directories

- Exclude whole folders, including subdirectories,
- Check the correct syntax for the above that your security software supports as not all may be *.
- `Volume:\` is the volume you originally installed the product to.

Windows Server OS - 2019, 2016 (and 2012 R2 for old versions).

- `Volume:\Inetpub\SolarWinds\*`
- `Volume:\ProgramData\SolarWinds\*`
- `Volume:\Program Files (x86)\Common Files\SolarWinds\*`
- `Volume:\Program Files (x86)\SolarWinds\*`
- `Volume:\Windows\Temp\SolarWinds\*`
- `Volume:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\*`

Figure 2: Attackers Taking Advantage of EDR/AV Monitoring Blind Spot - SolarWinds Advisory Recommending Excluding SolarWinds Components From EDR/AV Monitoring To Prevent Application-Related Issues [6,8]

Summary

Attack Vector(s): A covert multi-stage supply-chain attack with a longer breakout time/operational tempo (likely started prior to 2020) reportedly carried out by a nation-state-sponsored actor using a trojanized digitally-signed SolarWinds Orion IT monitoring component payload (SolarWinds.Orion.Core.BusinessLayer.dll)[5] and actively taking advantage of EDR/AV blind spots (See Figure 2)[6,8].

Figure 3: Example of One of SolarWinds Orion Attacks Victim's Red Team Tools (KeeFarce) Reportedly Stolen by Attackers in Action

Impact: 18,000+ customers of SolarWinds believed to have been likely exposed as victims through compromised updates, including some major U.S. government (U.S. Treasury and Commerce, etc.), consulting (a leading US-based security company–FireEye/over 60 Red Team Tools (RTT) stolen by the MTA, etc.), technology, telecom, and other entities across North America, Europe, Asia, and the Middle East.

Some Examples of Observed ATT&CK Techniques:

- T1195.002 Supply Chain Compromise
- T1568.002 Dynamic Resolution: Domain Generation Algorithms
- T1497.003 Virtualization/Sandbox Evasion: Time Based Evasion
- T1027.003 Obfuscated Files or Information: Steganography
- T1041 Exfiltration Over C2 Channel
- T1583.003 Acquire Infrastructure: Virtual Private Server
- T1071.001 Application Layer Protocol: Web Protocols
- T1569.002 System Services: Service Execution
- T1070.004 Indicator Removal on Host: File Deletion
- T1057 Process Discovery
- T1036.003 Masquerading: Rename System Utilities

- T1021 Remote Services
- T1036.004 Masquerading: Masquerade Task or Service
- T1101.001 Password guessing
- T1101.003 Password spraying
- T1078 Inappropriately secured administrative credentials
- T1133 External remote access services
- T1053.005 Scheduled Task

*** Note that there were some new MITRE ATT&CK procedures and technique variants observed as part of the attacks. Some of the new procedural variations of techniques included, for instance, T1070 Indicator Removal on Host. In addition, some techniques were used as part of an expanded tscope such as T1098.001 Account Manipulation: Additional Cloud Credentials; there were also some new sub-techniques not yet published as part of ATT&CK, including T1606.002 Forge Web Credentials: SAML Tokens, and others [13].

Red Team Tools (RTT) Impact: From the analysis of the RTT stolen from one of the victims [1]:
>40% of the stolen RTT are either publicly available security tools or based on publicly available security tools (see Figure 3).
~40% of stolen RTT are developed internally by FireEye.
>15% of stolen RTT are difficult to identify because the details shared are very limited. Based on the details available, there is a high probability most of the tools are modified versions of the publicly available tools [3].

Scope: According to the sources familiar with the investigation, the breaches observed, including the recently disclosed attack stealing internal adversary/red team tools from a victim company (FireEye), are currently believed to be a part of a broader attack campaign leveraging a relatively sophisticated supply chain attack using SolarWinds Orion with a nation-state-sponsored malicious threat actor (MTA) taking advantage of compromised Solarwinds dev/prod. digital certificates (from March-May 2020) to sign a malicious trojanized update for SolarWinds® Orion® Platform software builds for versions 2019.4 HF 5 and 2020.2 with no hotfix or 2020.2 HF 1 & leveraging stolen SAML token signing certificate [7,10].

Update - In addition to the SUNBURST/ECLIPSER supply chain attacks, there's been reports of additional malware referred to by some sources as SUPERNOVA. According to the available details [15], the malware is not part of the SUNBURST/ECLIPSER supply chain attacks and was instead separately placed on the targets using an SolarWinds Orion API zero-day authentication bypass vulnerability (CVE-2020-10148). The attacks reportedly involved using the vulnerabilities to install a custom unsigned trojanized DLL web shell implant "app_web_logoimagehandler.ashx.b6031896.dll" that was targeted to be used with the SolarWinds Orion product [15] (See Figure 6.1)..

Zero-day Exploits: According to one of the victims targeted by the malicious attackers (FireEye), *no zero-day exploits* were stolen. However, there were 16 CVE associated with the stolen RTT.

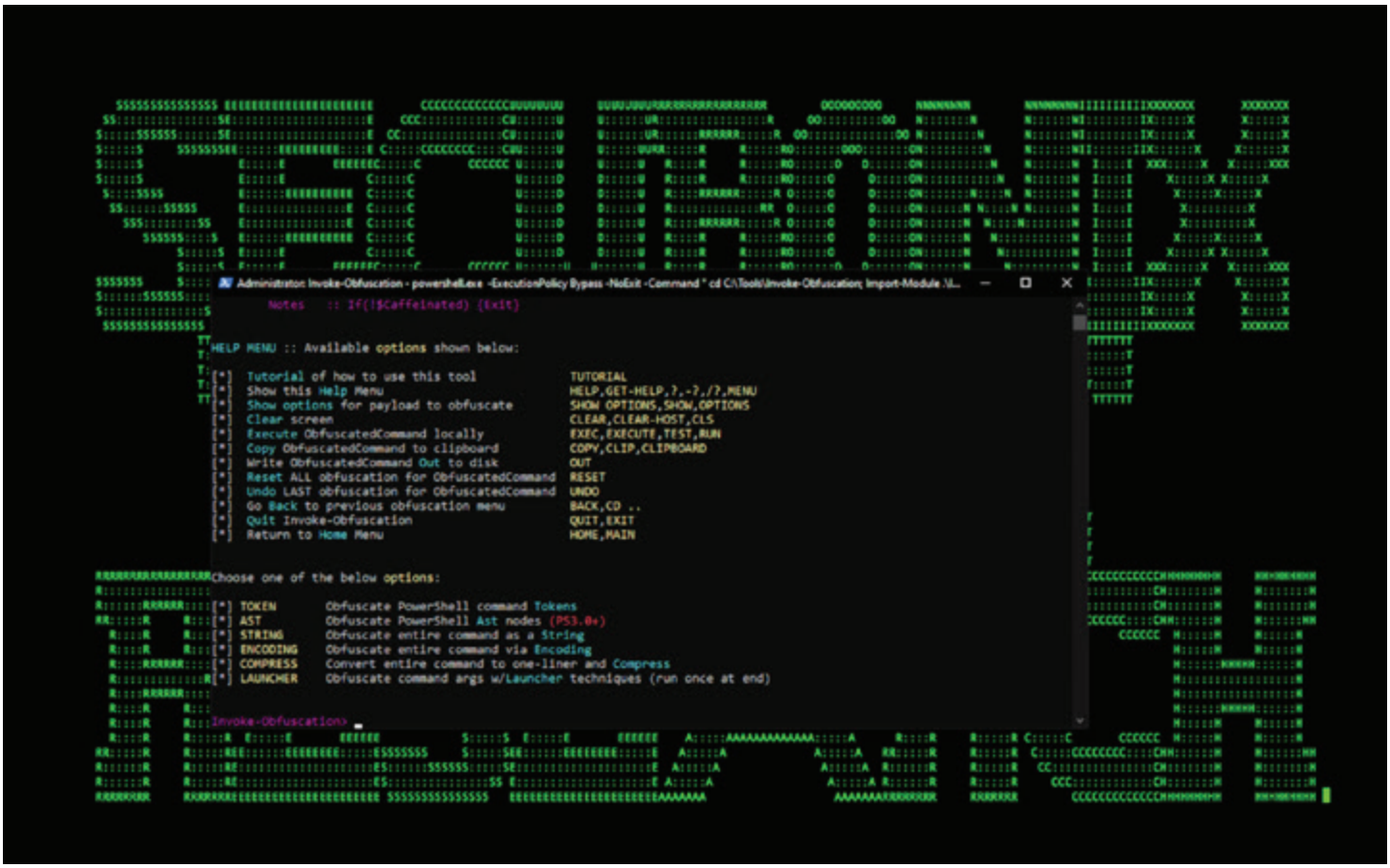


Figure 4: Example of a Variant of One of Victim's Stolen Red Team Tools Available as Part of Public Sources (Rubeus)

Some of the Key Artifacts Observed:

e1ebab8ed84dc10b95a1f68c812ecbf6d8f350f8
5e643654179e8b4cfe1d3c1906a90a4c8d611cea
fd15760abfc0b2537b89adc65b1ff3f072e7e31c
2f1a5a7411d015d01aaee4535835400191645023
395da6d4f3c890295f7584132ea73d759bd9d094
75af292f34789a1c782ea36c7127bf6106f595e8
d130bd75645c2433f88ac03e73395fba172ef676
ebe711516d0f5cd8126f4d53e375c90b7b95e8f2
0548eedb3d1f45f1f9549e09d00683f3a1292ec5
1b476f58ca366b54f34d714ffce3fd73cc30db1a
2dafddbfb0981c5aa31f27a298b9c804e553c7bc
e70b6be294082188cbe0089dd44dbb86e365f6a2
393702fab1c5d09d9f94e8a63114746d
e18a6a21eb44e77ca8d739a72209c370
56ceb6d0011d87b6e4d7023d7ef85676
846e27a652a5e1bfbd0ddd38a16dc865

3e329a4c9030b26ba152fb602a1d5893
02af7cec58b9a5da1c542b5a32151ba1
2c4a910a1299cdae2a4e55988a2f102e
f6d07f3d81dcea99b27462d100414917
2b3445e42d64c85a5475bdbc88a50ba8c013febb53ea97119a11604b7595e53d
6e4050c6a2d2e5e49606d96dd2922da480f2e0c70082cc7e54449a7dc0d20f8d
92bd1c3d2a11fc4aba2735d9547bd0261560fb20f36a0e7ca2f2d451f1b62690
a25cadd48d70f6ea0c4a241d99c5241269e6faccb4054e62d16784640f8e53bc
a3efbc07068606ba1c19a7ef21f4de15d15b41ef680832d7bcba485143668f2d
a58d02465e26bdd3a839fd90e4b317eece431d28cab203bbdde569e11247d9e2
ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c
b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07
b8a05cc492f70ffa4adcd446b693d5aa2b71dc4fa2bf5022bf60d7b13884f666
ffdbdd460420972fd2926a7f460c198523480bc6279dd6cca177230db18748e8
c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71
019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134
c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77
c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71
cc082d21b9e880ceb6c96db1c48a0375aaf06a5f444cb0144b70e01dc69048e6
ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6
d0d626deb3f9484e649294a8dfa814c5568f846d5aa02d4cdad5d041a29d5600
d3c6785e18fba3749fb785bc313cf8346182f532c59172b69adfb31b96a5d0af
dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b
e0b9eda35f01c1540134aba9195e7e6393286dde3e001fce36fb661cc346b91d
eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed
0f5d7e6dfdd62c83eb096ba193b5ae394001bac036745495674156ead6557589
1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c
20e35055113dac104d2bb02d4e7e33413fae0e5a426e0eea0dfd2c1dce692fd9
*.avsvmcloud\.com
*.lcomputers\.com
*.webcodez\.com
13.57.184.217
13.59.205.66
18.217.225.111
18.220.219.143
196.203.11.89
3.16.81.254
3.87.182.149
3.87.182.149
34.219.234.134

54.193.127.66
54.215.192.52

Added January 11:

0548eedb3d1f45f1f9549e09d00683f3a1292ec5
1b476f58ca366b54f34d714ffce3fd73cc30db1a
2dafddbfb0981c5aa31f27a298b9c804e553c7bc
e70b6be294082188cbe0089dd44dbb86e365f6a2
02af7cec58b9a5da1c542b5a32151ba1
fd15760abfc0b2537b89adc65b1ff3f072e7e31c
20e35055113dac104d2bb02d4e7e33413fae0e5a426e0eea0dfd2c1dce692fd9
2b3445e42d64c85a5475bdbc88a50ba8c013febb53ea97119a11604b7595e53d
0f5d7e6dfdd62c83eb096ba193b5ae394001bac036745495674156ead6557589
1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c
6e4050c6a2d2e5e49606d96dd2922da480f2e0c70082cc7e54449a7dc0d20f8d
92bd1c3d2a11fc4aba2735d9547bd0261560fb20f36a0e7ca2f2d451f1b62690
a3efbc07068606ba1c19a7ef21f4de15d15b41ef680832d7bcba485143668f2d
a58d02465e26bdd3a839fd90e4b317eece431d28cab203bbdde569e11247d9e2
b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07
b8a05cc492f70ffa4adcd446b693d5aa2b71dc4fa2bf5022bf60d7b13884f666
cc082d21b9e880ceb6c96db1c48a0375aaf06a5f444cb0144b70e01dc69048e6
e0b9eda35f01c1540134aba9195e7e6393286dde3e001fce36fb661cc346b91d
ffdbdd460420972fd2926a7f460c198523480bc6279dd6cca177230db18748e8
ervsystem\.com
infinitysoftwares\.com
mobilnweb\.com
5f40b59ee2a9ac94ddb6ab9e3bd776ca
c45c9bda8db1d470f1fd0dcc346dc449839eb5ce9a948c70369230af0b3ef168

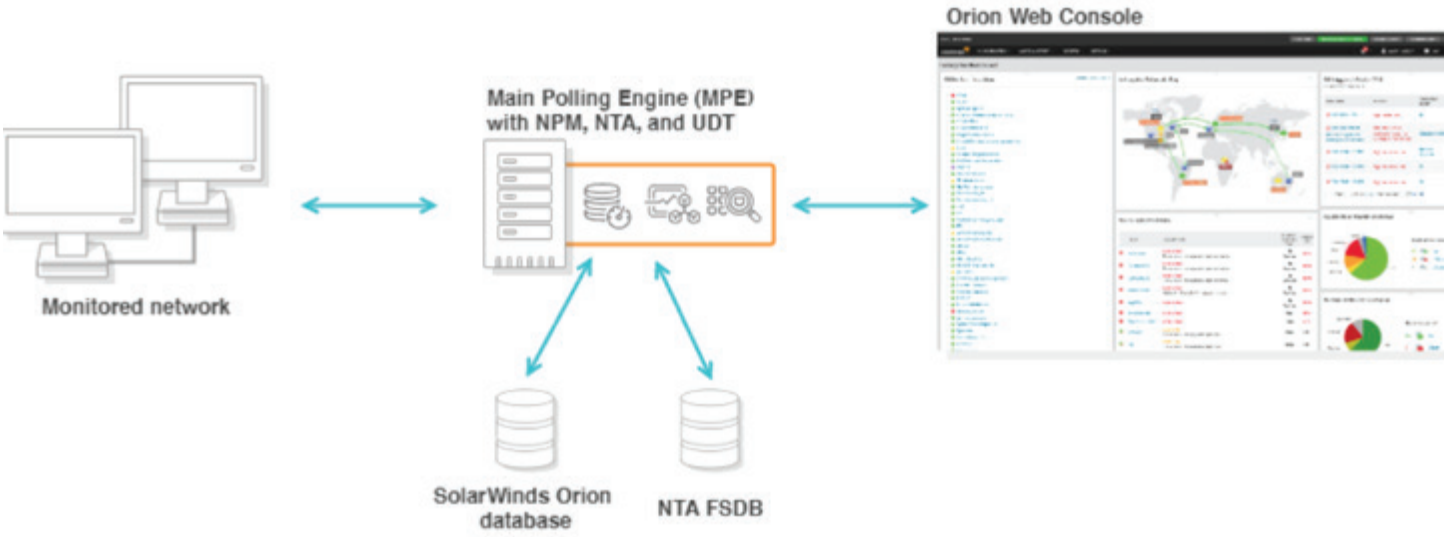


Figure 5: Example of a "Watcher" - SolarWinds Orion Monitoring Architecture

Critical SolarWinds ECLIPSER aka SUNBURST aka Solorigate Attacks - Blue Team Highlights

Detection Highlight #1 - Importance of "Watching the Watchers" (WOW) Detections

SolarWinds Orion (SO) is one of the common "Watcher" products that can be used to help IT/ops monitor the health and performance of an infrastructure.

At the same time, there often is very limited/no security monitoring done of the orgs' "Watcher" products themselves, whether on a network, security, or in the cloud.

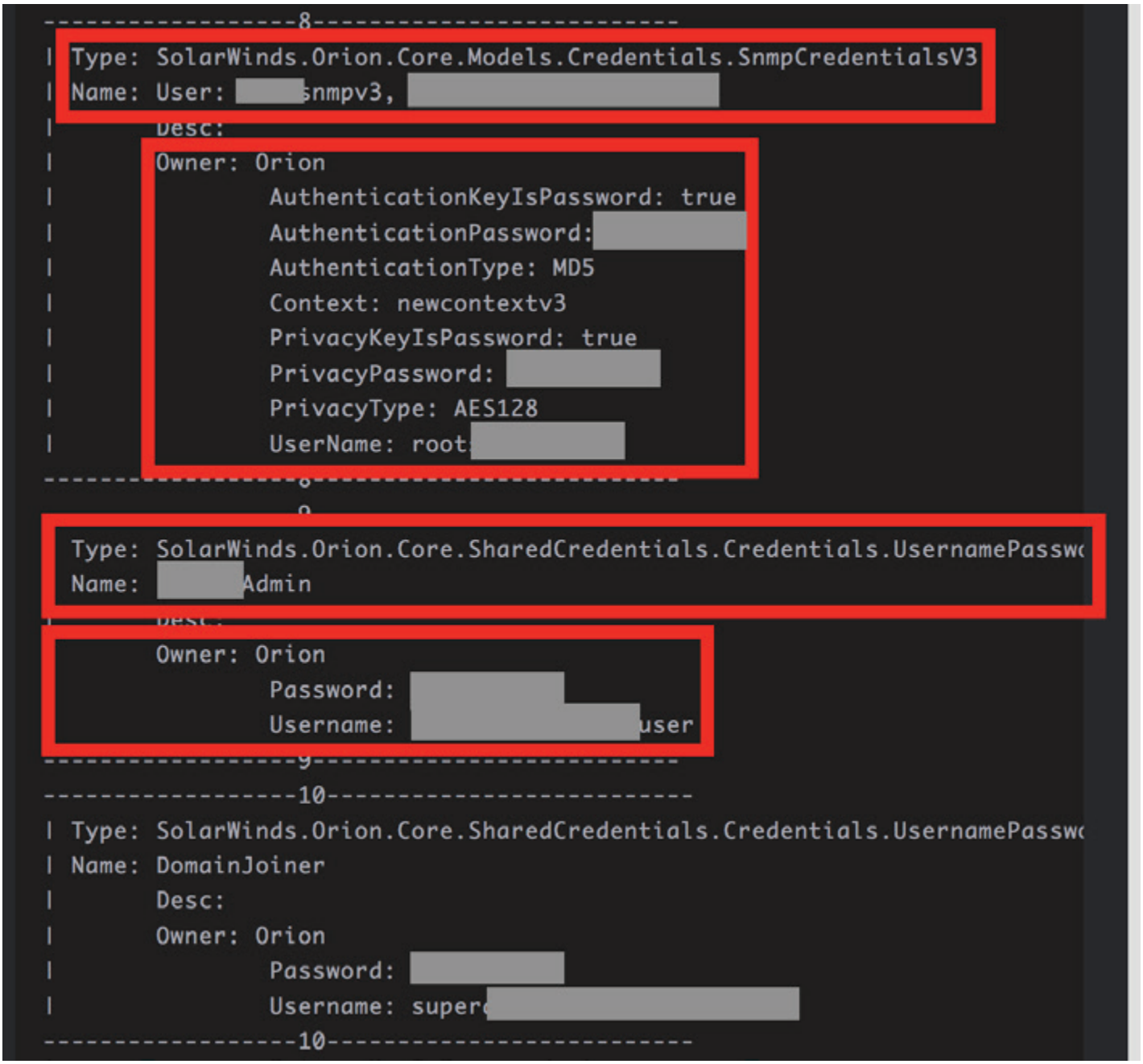


Figure 6: Sensitive Details Likely Dumped by Attackers Directly From SolarWinds Orion DB

As we've seen with the critical SO attacks, this lack of monitoring can represent a significant security detection gap that can be effectively exploited by attackers.

This is particularly critical in light of the fact that SO stored sensitive credentials in its internal DB that can be dumped, e.g. using open source tools such as SolarFlare from mubix [11], and others.

This type of credential dumping was also likely leveraged by the attackers as part of the lateral movement within the victims' networks and potentially means that a number of other SO-controlled components might have been compromised (see Figure 6).

In order to address this major detection gap, it is critical to include the WOW detection use cases and security monitoring as part of your detection-in-depth strategy.

This includes security monitoring of your IT/Ops tools, your network appliance and edge devices, your virtual and cloud services, the related cloud/applications/logs, et al.

For some examples of the relevant detections, please see below.

Detection Highlight #2 - AV/EDR Blind Spots and Importance of Diversifying Your Telemetry (DYT)

Another important highlight from the latest attacks targeting SO relates to how effectively the attackers exploited the common *AV/EDR blind spots*.

Specifically, as shown in Figure 2, AV/EDR was explicitly recommended by the vendor/SO to be *disabled* to prevent application-related issues.

This approach is not uncommon across many vendors/organizations with some of the products often just added to whitelists with minimal SOC deconflicting/investigations.

This was combined with some additional EDR evasion/covertness w/relatively higher level of opsec behaviors [10] enabling attackers to remain undetected/evade EDR longer.

One of the key takeaways from these attacks is the importance of not relying on a single telemetry source such as EDR, NTA, logs, etc.

To detect the modern attacks, it is critical to be able to leverage multiple diversified telemetry (DYT) data sources as part of your detections, e.g. your IT/Ops tools, your network appliance and edge devices, your endpoints, your critical servers, firewall/proxies, virtual and cloud services, the related cloud/applications/logs, etc.

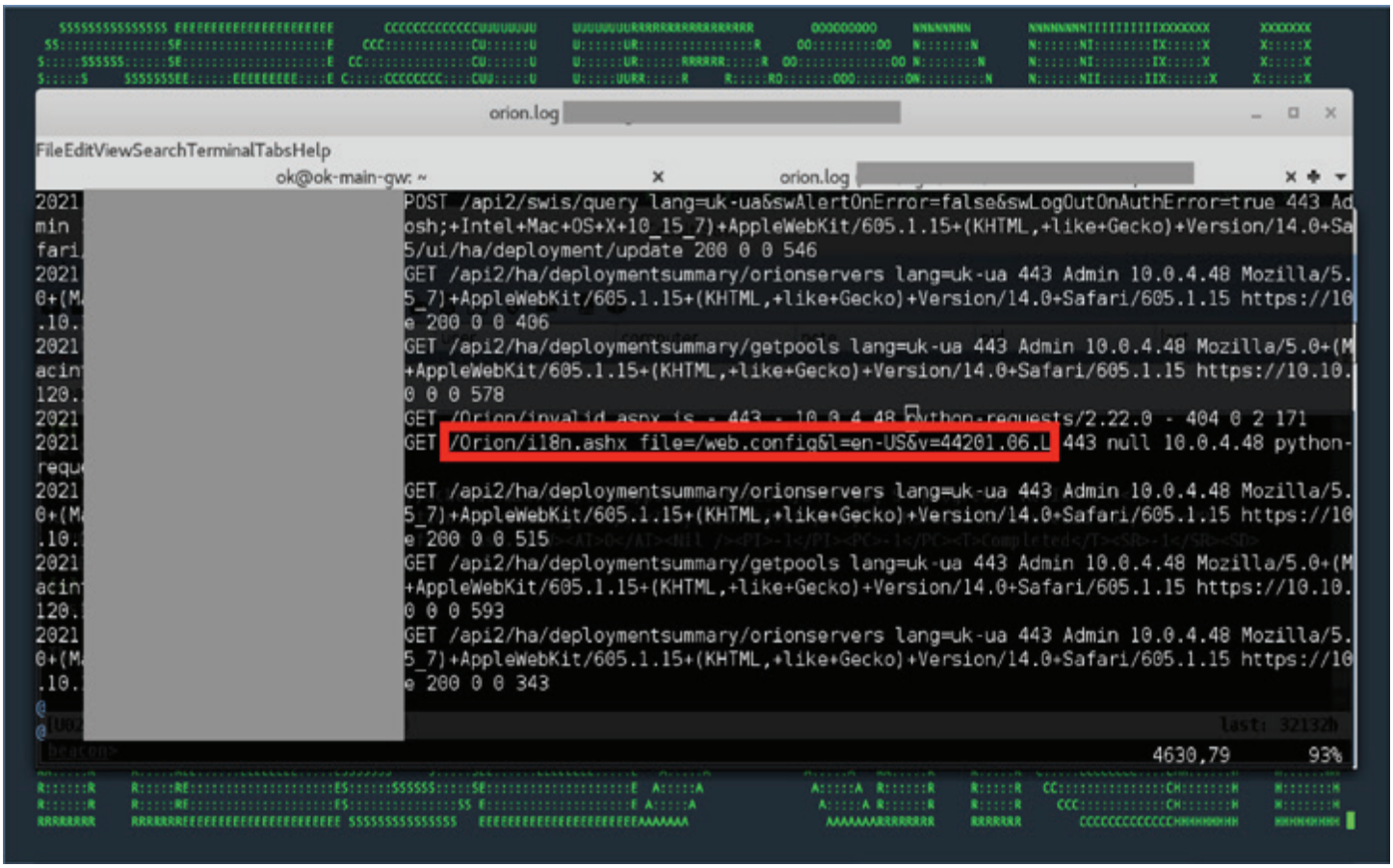


Figure 6.1: SUPERNOVA - Some Examples of Additional SolarWinds Exploitation Attempts In Logs

Detection - Sample Spotter Search Queries - SolarWinds/ECLIPSER Malicious Activity

Please find below some examples of the trivial Spotter queries to assist with initial threat hunting/ retrohunting/identifying some possible attack behaviors based on the details above.

Note: Because of the rapidly changing attack landscape, the recommendation is not to rely on static IOAs/queries and to implement the use cases/predictive indicators for the best possible protection (see next section).

Proxy
rg_functionality = “Web Proxy” and destinationhostname not contains “.solarwinds.com” and (RequestUrl contains “/swip/upd/SolarWinds.CortexPlugin.Components.xml” or RequestUrl contains “/swip/Events” or RequestUrl contains “swip/Upload.ashx”)

Named Pipes
rg_functionality = “Endpoint Management Systems” and (baseeventid=17 or baseeventid=18) and filepath contains “583da945-62af-10e8-4902-a8f205c72b2e”

Process Monitoring
rg_functionality =”Endpoint Management Systems” AND (oldfilename CONTAINS “SolarWinds.BusinessLayerHost.exe” or oldfilename CONTAINS “SolarWinds.BusinessLayerHostx64.exe”) AND (filename IS NOT NULL AND filename !=”-”) | RARE filename

Cloud/AzureAD - New Credential Added by Admin/App Owner to An Application/SP
rg_functionality = “MicrosoftAzureActiveDirectoryAuditLogs” AND customstring3 IN (“Add service principal”, “Certificates and secrets management”)
AND eventoutcome CONTAINS “success” AND (InitiatedBy.user.userPrincipalName CONTAINS “@” OR InitiatedBy.app.displayName CONTAINS “@”)
AND (keyEvents CONTAINS “KeyIdentifier=” AND keyEvents CONTAINS “KeyUsage=Verify”)
AND keyEvents.displayName CONTAINS “KeyDescription”
AND (keyEvents.oldValue = “[]” OR keyIdentifier != keyIdentifierOld)
AND keyUsage = “Verify”

Cloud/AzureAD - Users Signing Into AzureAD via PS Accessing Non-AD Resources [10]
rg_functionality = “MicrosoftAzureSigninLogs” AND AppId CONTAINS “1b730954-1685-4b74-9bfd-dac224a7b894” AND TokenIssuerType CONTAINS “AzureAD”
AND ResourceIdentity != “00000002-0000-0000-c000-000000000000” eventoutcome = 0
rg_functionality = “Microsoft Windows” AND destinationprocessname ENDS WITH “powershell.exe”
AND (
resourcecustomfield1 CONTAINS ‘powershell -nop -w hidden -enc ‘
OR resourcecustomfield1 CONTAINS ‘powershell -nop -exec bypass -enc ‘
)

rg_functionality = “Microsoft Windows” AND destinationprocessname NOT ENDS WITH “msbuild.exe” AND resourcecustomfield1 NOT CONTAINS ‘msbuild’
AND (
resourcecustomfield1 CONTAINS ‘noconsolelogger’
OR resourcecustomfield1 CONTAINS ‘noconlog’
)

rg_functionality = “Microsoft Windows” AND destinationprocessname ENDS WITH “dism.exe”
AND (
resourcecustomfield1 CONTAINS “/Mount-Wim”
OR resourcecustomfield1 CONTAINS “/WimFile:”
OR resourcecustomfield1 CONTAINS “/MountDir:”
OR resourcecustomfield1 CONTAINS “/LogPath:NUL”
OR resourcecustomfield1 CONTAINS “/index:1”
)]

Process Hashes [4]
rg_functionality = “Endpoint Management Systems” AND baseeventid=7 AND sourceProcessName CONTAINS “svchost.exe” AND destinationProcessName ENDS WITH “NetSetupSvc.dll”
rg_functionality = “Endpoint Management Systems” AND (baseeventid=1 OR baseeventid = 4688) AND filehash in (“b91ce2fa41029f6955bff20079468448”,”02af7cec58b9a5da1c542b5a32151ba1”,”2c4a910a1299cdae2a4e55988a2f102e”,”846e27a652a5e1bfbd0ddd38a16dc865”,”4f2eb-62fa529c0283b28d05ddd311fae”,”56ceb6d0011d87b6e4d7023d7ef85676”)

Proxy C2 [4]
rg_functionality = “Web Proxy” and RequestUrl in (“panhardware.com”,”databasegalore.com”,”avsvmcloud.com”,”freescanonline.com”,”thedoccloud.com”,”deftsecurity.com”)

Some Trivial SO-related Process Insights For Threat Hunting
“rg_functionality = “”Endpoint Management Systems”” AND (baseeventid=1 OR baseeventid = 4688) AND sourceprocessname=””solarwinds.businesslayerhost.exe””
AND destinationProcessName NOT ENDS WITH “”\SolarWinds\Orion\ExportToPDFCmd.exe””
AND destinationProcessName NOT ENDS WITH “”\SolarWinds.Credentials\SolarWinds.Credentials.Orion.WebApi.exe””
AND destinationProcessName NOT ENDS WITH “”\SolarWinds\Orion\Topology\SolarWinds.Orion.Topology.Calculator.exe””
AND destinationProcessName NOT ENDS WITH “”\SolarWinds\Orion\\Database-Maint.exe””
AND destinationProcessName NOT ENDS WITH “”\SolarWinds.Orion.ApiPoller.Service\SolarWinds.Orion.ApiPoller.Service.exe””
AND destinationProcessName NOT ENDS WITH “”\Windows\SysWOW64\WerFault.exe”

rg_functionality = “Endpoint Management Systems” AND sourceprocessname ENDS WITH “SolarWinds.BusinessLayerHost.exe” AND destinationprocessname ENDS WITH “powershell.exe”
rg_functionality = “Endpoint Management Systems” AND sourceprocessname

ENDS WITH “SolarWinds.BusinessLayerHost.exe” AND
destinationprocessname ENDS WITH “cmd.exe” AND resourcecustomfield1
CONTAINS “echo”
rg_functionality = “Endpoint Management Systems” AND sourceprocessname
ENDS WITH “Microsoft.IdentityServer.ServiceHost.exe” AND
(destinationprocessname ENDS WITH “werfault.exe” OR
destinationprocessname ENDS WITH “csc.exe”) AND resourcecustomfield1
NOT CONTAINS “nameId”
rg_functionality = “Endpoint Management Systems” AND
destinationpocessname ENDS WITH “csrss.exe” AND filepath NOT STARTS
WITH “C:\Windows\System32”
rg_functionality = “Endpoint Management Systems” AND
destinationpocessname NOT ENDS WITH “adfind.exe” AND
resourcecustomfield1 CONTAINS “ -h “ AND resourcecustomfield1 CONTAINS
“ -f “ AND ((resourcecustomfield1 CONTAINS “name=” AND
resourcecustomfield1 CONTAINS “Domain Admins” AND resourcecustomfield1
CONTAINS “member” AND resourcecustomfield1 CONTAINS “-list”) OR
(resourcecustomfield1 CONTAINS “objectcategory=”)

rg_functionality = “Windows Powershell” AND baseeventid = 4104 and
message CONTAINS “ComObject” AND message CONTAINS “Schedule.Service”
AND message CONTAINS “Microsoft\Windows\SoftwareProtectionPlatform”
AND message CONTAINS “RegisterTaskDefinition” AND message CONTAINS
“EventCacheManager.exe” AND message CONTAINS “ONSTART”
Cloud/AzureAD - Users Signing Into AzureAD via PS Accessing Non-AD
Resources [10]

rg_functionality = “MicrosoftAzureSigninLogs” AND AppId CONTAINS
“1b730954-1685-4b74-9bfd-dac224a7b894” AND TokenIssuerType CONTAINS
“AzureAD”
AND ResourceIdentity != “00000002-0000-0000-c000-000000000000” eventoutcome = 0

filehash NOT NULL AND filehash in
(“ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6”,
“0f5d7e6dfdd62c83eb096ba193b5ae394001bac036745495674156ead6557589”,
“e0b9eda35f01c1540134aba9195e7e6393286dde3e001fce36fb661cc346b91d”,

“20e35055113dac104d2bb02d4e7e33413fae0e5a426e0eea0dfd2c1dce692fd9”,
“2b3445e42d64c85a5475bdbc88a50ba8c013febb53ea97119a11604b7595e53d”,
“a3efbc07068606ba1c19a7ef21f4de15d15b41ef680832d7bcba485143668f2d”,
“92bd1c3d2a11fc4aba2735d9547bd0261560fb20f36a0e7ca2f2d451f1b62690”,
“a58d02465e26bdd3a839fd90e4b317eece431d28cab203bbdde569e11247d9e2”,
“cc082d21b9e880ceb6c96db1c48a0375aaf06a5f444cb0144b70e01dc69048e6”)

filehash NOT NULL AND filehash in
(“0f5d7e6dfdd62c83eb096ba193b5ae394001bac036745495674156ead6557589”,”e0b9e
da35f01c1540134aba9195e7e6393286dde3e001fce36fb661cc346b91d”,”20e35055113dac10
4d2bb02d4e7e33413fae0e5a426e0eea0dfd2c1dce692fd9”,”2b3445e42d64c85a5475bdb
c88a50ba8c013febb53ea97119a11604b7595e53d”,”a3efbc07068606ba1c19a7ef21f4de15
d15b41ef680832d7bcba485143668f2d”,”92bd1c3d2a11fc4aba2735d9547bd0261560fb2
0f36a0e7ca2f2d451f1b62690”,”a58d02465e26bdd3a839fd90e4b317eece431d28cab203bb
dde569e11247d9e2”,”cc082d21b9e880ceb6c96db1c48a0375aaf06a5f444cb0144b70
e01dc69048e6”
ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6
0f5d7e6dfdd62c83eb096ba193b5ae394001bac036745495674156ead6557589
e0b9eda35f01c1540134aba9195e7e6393286dde3e001fce36fb661cc346b91d
20e35055113dac104d2bb02d4e7e33413fae0e5a426e0eea0dfd2c1dce692fd9
2b3445e42d64c85a5475bdbc88a50ba8c013febb53ea97119a11604b7595e53d
a3efbc07068606ba1c19a7ef21f4de15d15b41ef680832d7bcba485143668f2d
92bd1c3d2a11fc4aba2735d9547bd0261560fb20f36a0e7ca2f2d451f1b62690
a58d02465e26bdd3a839fd90e4b317eece431d28cab203bbdde569e11247d9e2
cc082d21b9e880ceb6c96db1c48a0375aaf06a5f444cb0144b70e01dc69048e6
0f5d7e6dfdd62c83eb096ba193b5ae394001bac036745495674156ead6557589
e0b9eda35f01c1540134aba9195e7e6393286dde3e001fce36fb661cc346b91d
20e35055113dac104d2bb02d4e7e33413fae0e5a426e0eea0dfd2c1dce692fd9
2b3445e42d64c85a5475bdbc88a50ba8c013febb53ea97119a11604b7595e53d
a3efbc07068606ba1c19a7ef21f4de15d15b41ef680832d7bcba485143668f2d
92bd1c3d2a11fc4aba2735d9547bd0261560fb20f36a0e7ca2f2d451f1b62690
a58d02465e26bdd3a839fd90e4b317eece431d28cab203bbdde569e11247d9e2
cc082d21b9e880ceb6c96db1c48a0375aaf06a5f444cb0144b70e01dc69048e6

Detection - Sample Spotter Search Queries - Related Attack Vectors/CVEs

Please find below some examples of the trivial Spotter queries to assist with detection of some of the related CVEs disclosed [1].

Note: Because of the rapidly changing attack landscape, the recommendation is not to rely on static IOAs/queries and to implement the use cases/predictive indicators for the best possible protection (see next section).

Some sample Spotter search queries to assist with detection of the use of the relevant attack vectors/CVEs disclosed by some of the victims, e.g. FireEye, are as follows:

CVE-2019-11510
rg_functionality = “Web Proxy” and RequestUrl CONTAINS “?/dana/html5acc/guacamole/”

CVE-2018-13379
rg_functionality = “Web Proxy” and RequestUrl contains “/remote/fgt_lang?lang=/../../../..//////////dev/cmdb/sslvpn_websession”

CVE-2020-1472
resourcegroupname= “”zeek”” AND sourcetype=bro:rpc:json operation IN (NetrServerReqChallenge, NetrServerAuthenticate3, NetrServerPasswordSet2)
| STATS count by sourceaddress
| where count > 100”

CVE-2019-11580
rg_functionality = “Web Proxy” and RequestUrl CONTAINS “/crowd/plugins/servlet/exp?cmd=”

CVE_2019-19781
rg_functionality = “Web Proxy” and RequestUrl CONTAINS “/../vpns/” or RequestUrl CONTAINS “/vpns/cfg/smb.conf” or (RequestUrl CONTAINS “/vpns/portal/scripts/” and RequestUrl CONTAINS “.pl”)

CVE-2020-10189
rg_functionality = “Endpoint Management Systems” AND (baseeventid=1 OR baseeventid = 4688) AND sourceprocessname ENDS WITH “DesktopCentral_Server\ jre\bin\java.exe” and (destinationprocessname ENDS WITH “cmd.exe” or destinationprocessname ENDS WITH “powershell.exe” or destinationprocessname ENDS WITH “bitsadmin.exe”)

and others.

Detection - Sample Spotter Search Queries - Red Team Tools

Please find below some examples of the trivial Spotter queries to assist with initial threat hunting/ identifying some behaviors associated with the stolen RTT [4].

Note: Because of the rapidly changing attack landscape, the recommendation is not to rely on static IOAs/queries and to implement the use cases/predictive indicators for the best possible protection (see next section).

rg_functionality = “”Endpoint Management Systems”” AND baseeventid = 7 AND filepath ENDS WITH “”libvlc.dll”

rg_functionality = “Microsoft Windows” AND filename IN (‘\PIPE\OIPC_CNTAOSMGR_PIPE_2218EBAB_63F8_##E4_930C_AF69E78928AF’, ‘\PIPE\OIPC_OFC_AS_PIPE_2218EBAB_63F8_49E4_93##_AF69E79928AF’, ‘\Device\Mup\’)

“rg_functionality = “Microsoft Windows” AND destinationprocessname ENDS WITH “powershell.exe” AND (additionaldetails1 CONTAINS ‘powershell -nop -w hidden -enc ‘ OR additionaldetails1 CONTAINS ‘powershell -nop -exec bypass -enc ‘)

rg_functionality = “Microsoft Windows” AND destinationprocessname NOT ENDS WITH “msbuild.exe” AND additionaldetails1 NOT CONTAINS ‘msbuild’ AND (OR additionaldetails1 CONTAINS ‘noconsolelogger’ OR additionaldetails1 CONTAINS ‘noconlog’) AND (sourceprocessname NOT ENDS WITH ‘\bin\nact.exe’ OR sourceprocessname NOT ENDS WITH ‘\MSBuild\15.0\Bin\amd64\Tracker.exe’ OR sourceprocessname NOT ENDS WITH ‘\Program Files\dotnet\dotnet.exe’)

rg_functionality = “Endpoint Management Systems” AND baseeventid = 7 AND (filepath ENDS WITH “anything. cpl” OR filepath ENDS WITH “\anything.dll”)

rg_functionality = “Endpoint Management Systems” AND baseeventid = 7 AND (filepath ENDS WITH “anything. cpl” OR filepath ENDS WITH “\anything.dll”)

rg_functionality = “Endpoint Management Systems” AND baseeventid = 7 AND filepath ENDS WITH ‘“ibvlc.dll”

rg_functionality = “Endpoint Management Systems” AND baseeventid = 7 AND filepath ENDS WITH “X32BRIDGE.dll”

rg_functionality = “Microsoft Windows” AND destinationprocessname ENDS WITH “excolorcplcavator.exe” AND (sourceprocessname ENDS WITH “cscript.exe” OR sourceprocessname ENDS WITH “wscript.exe” OR sourceprocessname ENDS WITH “MSHTA.exe” OR sourceprocessname ENDS WITH “winword.exe” OR sourceprocessname ENDS WITH “excel. exe”)

rg_functionality = “Microsoft Windows” AND (destinationprocessname ENDS WITH “colorcpl.exe” OR destinationprocessname ENDS WITH “colorcpl.exe”) AND (sourceprocessname ENDS WITH “cscript.exe” OR sourceprocessname ENDS WITH “wscript.exe” OR sourceprocessname ENDS WITH “MSHTA.exe”)

“rg_functionality = “”Microsoft Windows”” AND (destinationprocessname ENDS WITH “”colorcpl. exe”” OR destinationprocessname ENDS WITH “”colorcpl.exe””) AND
AND (sourceprocessname ENDS WITH “”cscript.exe”” OR sourceprocessname ENDS WITH “”wscript.exe”” OR sourceprocessname ENDS WITH “”MSHTA.exe””)

rg_functionality = “Microsoft Windows” AND destinationprocessname ENDS WITH “dism.exe” AND (additionaldetails1 CONTAINS “/Mount-Wim” OR additionaldetails1 CONTAINS “/WimFile:” OR additionaldetails1 CONTAINS “/MountDir:” OR additionaldetails1 CONTAINS “/LogPath:NUL” OR additionaldetails1 CONTAINS “/index:1”)

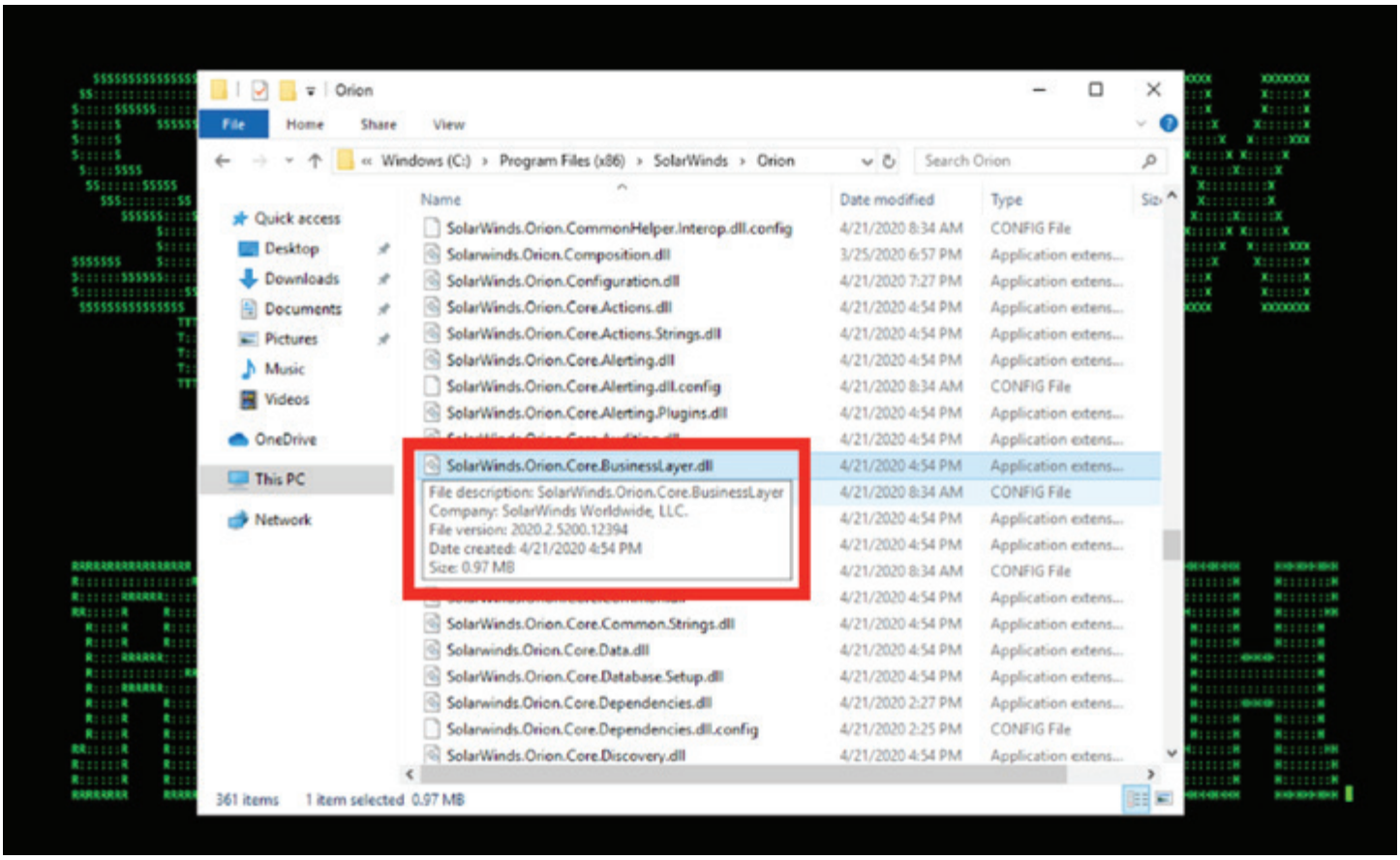


Figure 7: Example of Malicious Compromised DLL Loaded by the Target SolarWinds Instance

Detection – Securonix Behavior Analytics/Security Analytics

Here are some high-level examples of some of the relevant Securonix behavior analytics/predictive indicators to increase the chances of early detection of the malicious activity associated with the SolarWinds/ECLIPSER MTA including potential future variants of attacks:

- Watching the Watchers (WOW) - Possible Trojaned Vendor HTTP C2 Behavior Discrepancy Analytic
- Possible SolarWinds Orion DB Credential Dumping Using SOLARFLARE
- Possible ADPassHunt Malicious Payload Use Analytic
- Traffic to DGA Domains - Possible C2 Analytic
- Possible TEARDROP Malicious Payload Variant Analytic
- Possible Renamed LOL Helper Tool Payload Use By Malware Analytic
- Possible SUNSPOT Variant Dropped Artifact Analytic
- Rare WMI Exec Process Potential Lateral Movement Analytic
- Peak DNS IN A Request Volume For Source Analytic
- Possible Zerologon CVE-2020-1472 EP Computer Account Change Analytic

- Possible SolarWinds SUPERNOVA Auth Bypass Exploitation Analytic
- Possible Malicious .NET CSC.EXE Implant In-Memory Compilation Analytic
- Possible SolarWinds SUPERNOVA i18n Malicious Activity Analytic
- Watching the Watchers (WOW) - Possible Compromised Vendor Component Rare JA3 C2 Hash Analytic

and a number of others, including WOW-PXY1-ERI, WEL-TAR45-RUN, WOW-EDR1-ERI, WOW-EDR2-ERI, WOW-NTA1-ERI, EDR-SYM111-ERI, EDR-SYM112-RUN, DNS-BIN1-BPI, and others.

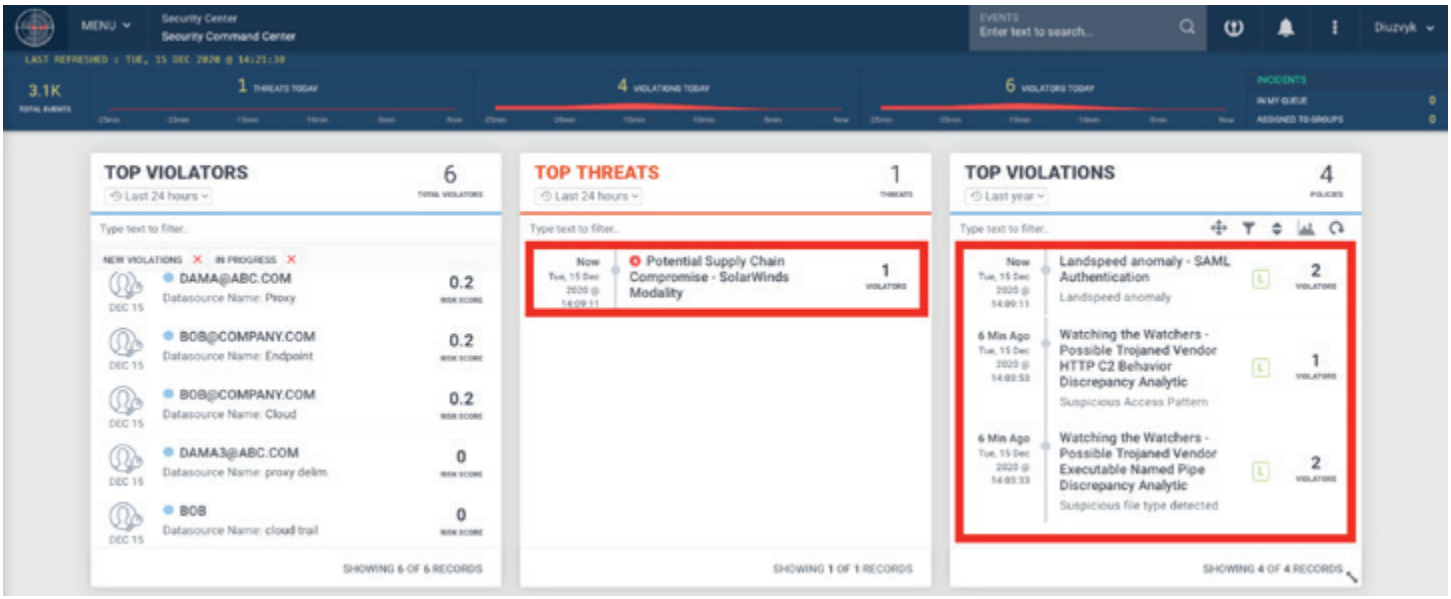


Figure 8: Example of SolarWinds/ECLIPSER Detection in Securonix Labs

Mitigation and Prevention - Securonix Recommendations

Here are some of the Securonix recommendations to help customers prevent and/or mitigate future attacks:

- Follow the mitigation guidance depending on your network categorization as specified in AA20-352A [18];
- If running the affected versions, conduct forensic analysis, and if accepting the risk of running the affected product, perform hardening as described in ED-21-01 [17];
- Consider performing an in-depth security review of your on-prem and cloud infrastructure for possible post-breach persistence vectors embedded by the attackers;
- In the event of a likely systemic identity compromise, consider performing a partial or full reconstitution of your IAM/trust services to mitigate the risks of reoccurrence;
- Proactively validate and configure the missing logging visibility/security monitoring to ensure that all the relevant logs, including:
    1. Remote access (VPN, RDP, SSH, et al.) logs
    2. Solarwinds platform/IIS logs

3. IDP/SP/Cloud access logs
4. Authentication/MFA logs
5. Endpoint (raw)/AD/server logs, NTA logs, etc.

are captured and stored for at least 180-270 days in a separate log capability;

- For all network devices (routers, switches, firewalls, etc.) managed by affected SolarWinds servers, consider auditing firmware and configurations for possible signs of subversion/ backdooring and resetting to a stable firmware, if feasible.

References

1. Kevin Mandia. FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community. December 8, 2020. https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html

2. Kolesnikov et al. Securonix Threat Research: Detecting High-Impact Targeted Cloud/MSP $14M+ Ryuk and REvil Ransomware Attacks. January 3, 2020. https://www.picussecurity.com/resource/blog/techniques-tactics-procedures-utilized-by-fireeye-red-team-tools.

3. Özarslan et al. Tactics, Techniques and Procedures (TTPs) Utilized by FireEye's Red Team Tools. December 10, 2020. https://www.picussecurity.com/resource/blog/techniques-tactics-procedures-utilized-by-fireeye-red-team-tools.

4. Fireeye Countermeasures. December 8, 2020. https://github.com/fireeye/red_team_tool_countermeasures.

5. Fireeye. Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor. December 13, 2020. https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html.

6. Solarwinds. Files and directories to exclude from antivirus scanning for Orion Platform products (AV exceptions and exclusions). https://support.solarwinds.com/SuccessCenter/s/article/Files-and-directories-to-exclude-from-antivirus-scanning-for-Orion-Platform-products?language=en_US

7. Christopher Bing. Reuters - Suspected Russian hackers spied on U.S. Treasury emails - sources. December 13, 2020. https://www.reuters.com/article/us-usa-cyber-treasury-exclsuive/exclusive-u-s-treasury-breached-by-hackers-backed-by-foreign-government-sources-idINKBN28N0PG

8. Ozarslan. December 15, 2020. Tactics, Techniques, and Procedures (TTPs) Used in the SolarWinds Breach. https://www.picussecurity.com/resource/blog/ttps-used-in-the-solarwinds-breach.

9. John Lambert. Important steps for customers to protect themselves from recent nation-state cyberattacks. December 13, 2020. https://blogs.microsoft.com/on-the-issues/2020/12/13/customers-protect-nation-state-cyberattacks/

10. MSRC. Customer Guidance on Recent Nation-State Cyber Attacks. December 13, 2020. https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/.

11. Mubix. SolarFlare Release: Password Dumper for SolarWinds Orion. December 13, 2020. https://malicious.link/post/2020/solarflare-release-password-dumper-for-solarwinds-orion/.

12. Brain Krebs. U.S. Treasury, Commerce Depts. Hacked Through SolarWinds Compromise. December 14, 2020. https://krebsonsecurity.com/2020/12/u-s-treasury-commerce-depts-hacked-through-solarwinds-compromise/.

13. Damien Cash et al. Dark Halo Leverages SolarWinds Compromise to Breach Organizations. December 14, 2020. https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/.

14. Malone M. et al. Identifying UNC2452-Related Techniques for ATT&CK. January 6, 2020. https://medium.com/mitre-attack/identifying-unc2452-related-techniques-9f7b6c7f3714

15. SolarWinds. SolarWinds Security Advisory. December 31, 2020. https://www.solarwinds.com/securityadvisory

16. Perlroth N. et al. Widely Used Software Company May Be Entry Point for Huge U.S. Hacking. January 6, 2021. https://www.nytimes.com/2021/01/06/us/politics/russia-cyber-hack.html.

17. FBI, CISA, ODNI, NSA. Joint Statement. January 5, 2021. https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure.

18. CISA. Supplemental Guidance v3. January 6, 2021. https://cyber.dhs.gov/ed/21-01/#supplemental-guidance-v3

19. CISA. Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations. January 7, 2021. https://us-cert.cisa.gov/ncas/alerts/aa20-352a

20. Crowdstrike. SUNSPOT: An Implant in the Build Process. January 12, 2021. https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/

About Securonix

Securonix is redefining SIEM for today's hybrid cloud, data-driven enterprise. Built on big data architecture, Securonix delivers SIEM, UEBA, SOAR, Security Data Lake, NTA, and vertical-specific applications as a pure SaaS solution with unlimited scalability and no infrastructure cost. Securonix reduces noise, prioritizes high fidelity alerts, and detects and responds to advanced insider and cyber threats with behavioral analytics technology that pioneered the UEBA category.

Contact Securonix

www.securonix.com
info@securonix.com | (310) 641-1000


SECURONIX™