CYBER THREAT INTELLIGENCE REPORT

WWW.CSFI.US

January 8th, 2021

TLP:WHITE information may be distributed without restrictions,
subject to copyright controls.

“To provide Cyber Warfare awareness, guidance, and security solutions through collaboration, education, volunteer work, and training to assist the US Government, US Military, Commercial Interests, and International Partners."

CSFI CYBER NUGGETS (SolarWinds)

Quick Facts and Attribution:

- Solarwinds has around 300,000 customers globally.
- Backdoor installed into Orion software update via SolarWinds hack.
- Security researcher Vinoth Kumar told Reuters that, last year, he alerted the company that anyone could access SolarWinds' update server by using the password "solarwinds123" - Source: Reuters.
- Hackers working for the Russian SVR (per Bruce Schneier's article) - Source: The Guardian.
- At least 32 US federal agencies purchased SolarWinds Orion software following 2006.
- **Actor**: UNC2452 (Intrusion campaign named by FireEye).
- **Malware**: SUNBURST Backdoor.
- **SolarWinds.Orion.Core.BusinessLayer.dll** is a SolarWinds digitally-signed component of the Orion software framework that contains a backdoor that communicates via HTTP to third party servers.
- **Motive:** Intelligence collections

"This work indicates that an Advanced Persistent Threat (APT) actor, likely Russian in origin, is responsible for most or all of the recently discovered, ongoing cyber compromises of both government and non-governmental networks," the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA) said in a joint statement.

Russia, however, denied any involvement in the operation on December 13, stating it "does not conduct offensive operations in the cyber domain." - Source: The Hacker News

CISA.GOV Report link: https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure

CSFI aggregated and correlated relevant profiles and entities from social media and select apps (including deep/dark web). CSFI monitored many other combinations of keywords.

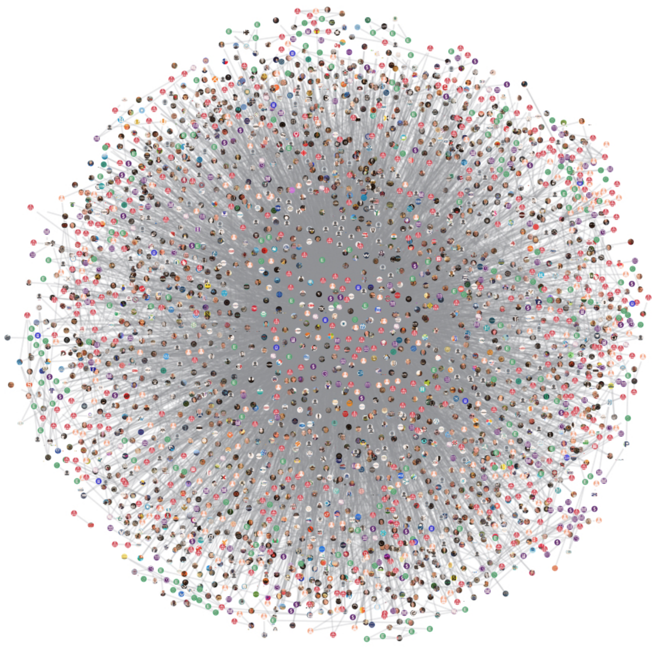
CSFI COLLECTIONS EFFORT

The following keywords were collected, aggregated and correlated by CSFI via well-coordinated collections operations:

- **Файлы взлома Орион** (DEC 31 2020 - DEC 22 2020)
  - 148 posts
  - 17 locations (reliable coordinates)
- **#solarwinds** (JAN 3 2021 - JAN 7 2021)
  - 10,000 captured posts across many social media platforms and search engines 2158 locations across the globe (reliable coordinates)
  - 2627 Users and groups of interest
  - 5952 Photos
  - 222 Videos

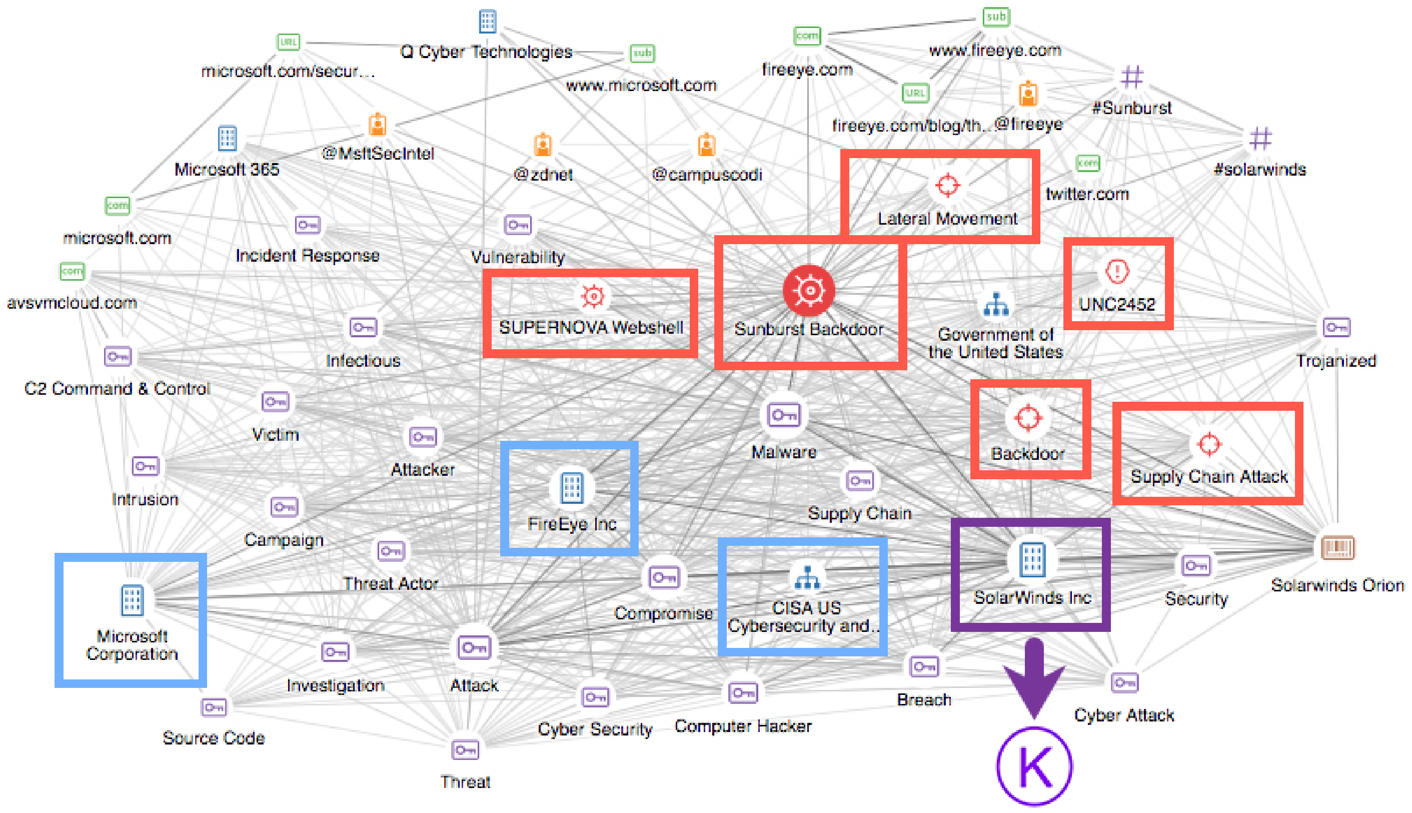
NOTE: Washington, DC, and the UK showed the most significant concentration of activity around #solarwinds. Coordinates can only be measured if users have their devices with Geolocation turned on. Russian sources reposted shared leaked FTP credentials belonging to SolarWinds. Exe files could be uploaded via leaked credentials. ***Most Russian apps/users had their Geolocation feature turned off when posting via social media during our research.***

CSFI found 2991 social media groups and authors of interest posting on the SolarWind hack. These are individuals or groups who are likely to hold most information on the topic. Each unique node can be analyzed in detail for further investigation.



> "All available intelligence sources, methods, technologies, and databases should be continuously exploited in an effort to analyze and determine the current situation of the adversary and other relevant actors."
> *~Joint Publication 2-01.3*

CONNECTING DOTS



THREAT ACTORS IN FOCUS

APT29 (Уютный мишка)

APT29 is thought to be a threat group operated under the control of the Russian state. APT29 is believed to have started operating since 2008 and associated to the Russian government. APT29 has been blamed for several high-profile attacks, such as the recent attacks against corona vaccine development and the attacks on the DNC in 2016. The latter was implicated alongside another Kremlin-linked hacker group, APT28. APT has traditionally focused on foreign government intelligence. However, the shift on stealing intellectual property through the Covid-19 vaccines' attacks and the FireEye hacking tool is the first of its kind from this group. MITRE: APT29 also known as Cozy Bear.

MITRE's breakdown: https://attackevals.mitre-engenuity.org/APT29/

Crowdstrike: https://www.crowdstrike.com/blog/who-is-cozy-bear/

APT29 uses a variety of techniques which have been outlined by MITRE here:
https://attack.mitre.org/groups/G0016/

APT29 Evaluation: Detection Categories: https://attackevals.mitre-engenuity.org/APT29/detection-categories.html

SVR (Служба внешней разведки)

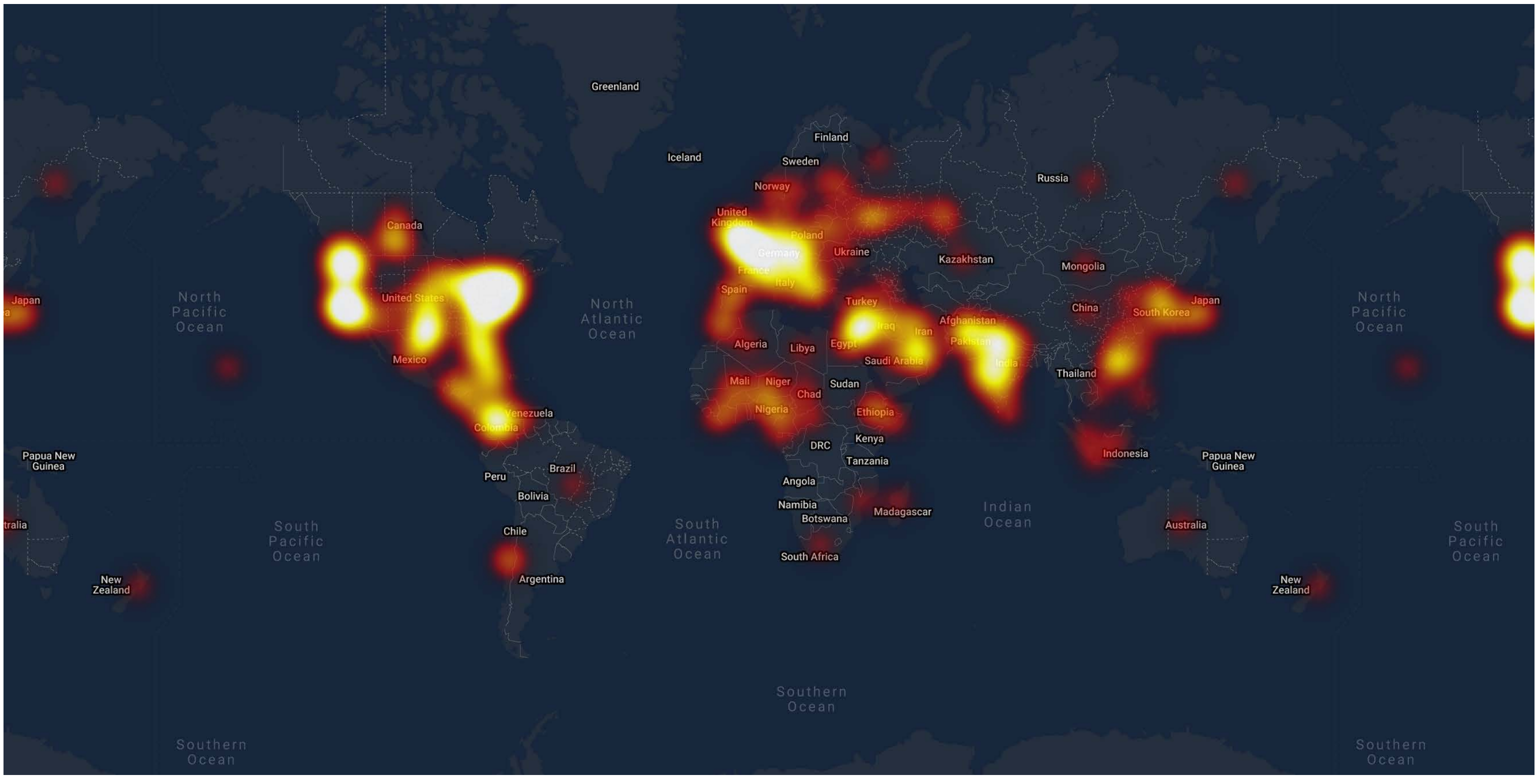
SVR is the Foreign Intelligence Service of the Russian Federation. SVR is Russia's external intelligence and espionage agency as opposed to Federal Security Services (FSB). SVR focuses on collecting intelligence, conducting espionage, performing surveillance in foreign countries considered adversarial, and having a variety of HUMINT officers that use diplomatic and covert officer covers. The SVR also gives some of its assets to reinforcing pro-Russian movements in Europe. The SVR works in parallel with the Main Directorate of the General Staff of the Armed Forces of the Russian Federation, referred to as the GRU.

There are varying opinions on whether APT29 is associated with SVR or FSB. Recorded Future:
https://www.recordedfuture.com/russian-apt-toolkits/

Source(s):
https://themoscowproject.org/explainers/russias-three-intelligence-agencies-explained/
https://www.brookings.edu/wp-content/uploads/2018/03/fp_20180316_future_political_warfare.pdf
https://www.exabeam.com/information-security/who-is-apt29/

The NYTimes does not name either the SVR or FSB:
https://www.nytimes.com/2020/12/08/technology/fireeye-hacked-russians.html

SUNBURST BACKDOOR NEWS DISSEMINATION HOT SPOTS



IOCs AND COUNTERMEASURES

TEARDROP and BEACON malware was used in the SolarWinds update. FireEye has provided two **Yara rules to detect TEARDROP** which is available on their GitHub repository: https://github.com/fireeye/sunburst_countermeasures/commit/722f5f82852a6ad00263c7721ac8f62eb2cb49ec

Defenders should look for the following alerts from FireEye HX: MalwareGuard and WindowsDefender:

Process Information
file_operation_closed
file-path*: “c:\\windows\\syswow64\\netsetupsvc.dll
actor-process:
pid: 17900

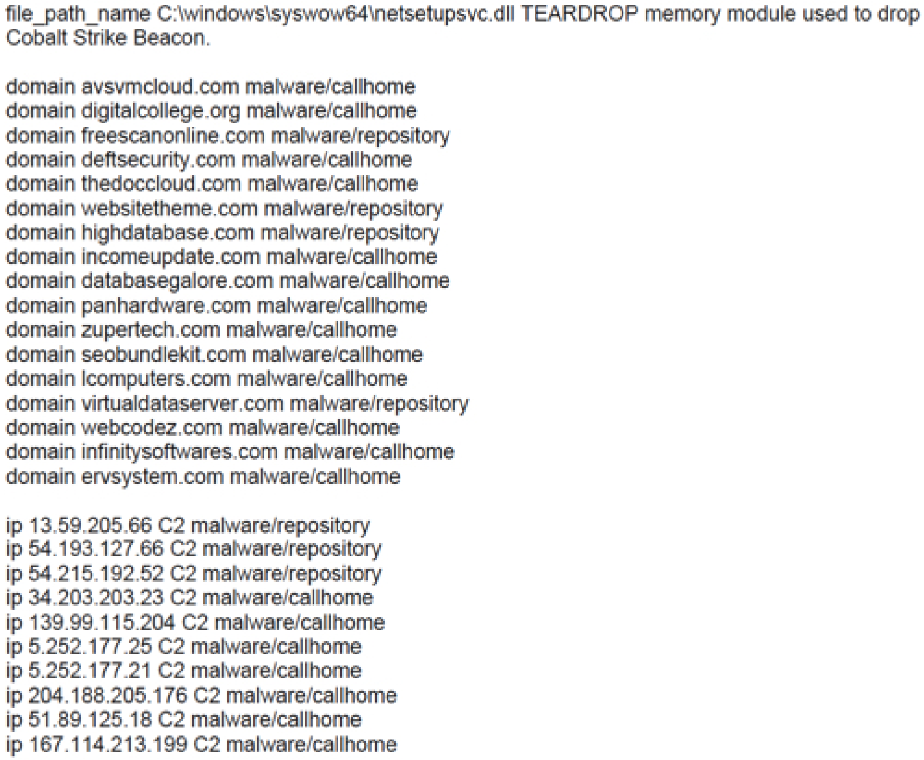
Window’s defender Exploit Guard log entries: (Microsoft-Windows-Security-Mitigations/KernelMode event ID 12)

Process”\Device\HarddiskVolume2\Windows\System32\svchost.exe” (PID XXXXX) would have been blocked from loading the non-Microsoft-signed binary

‘\Windows\SysWOW64\NetSetupSvc.dll’

Attacker Hostnames Match Victim Environment

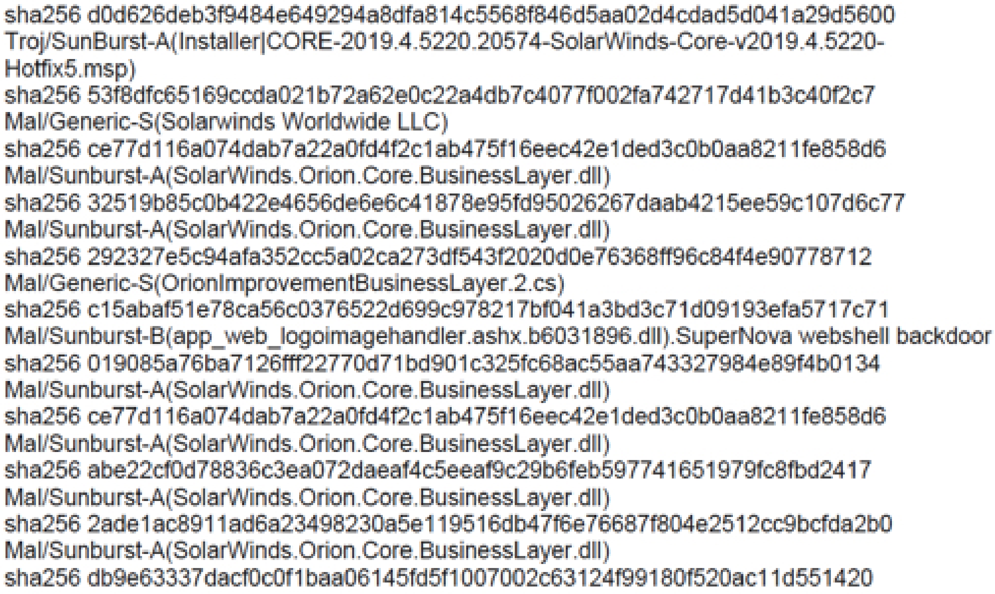
IOCS FROM SOLARWINDS ATTACK



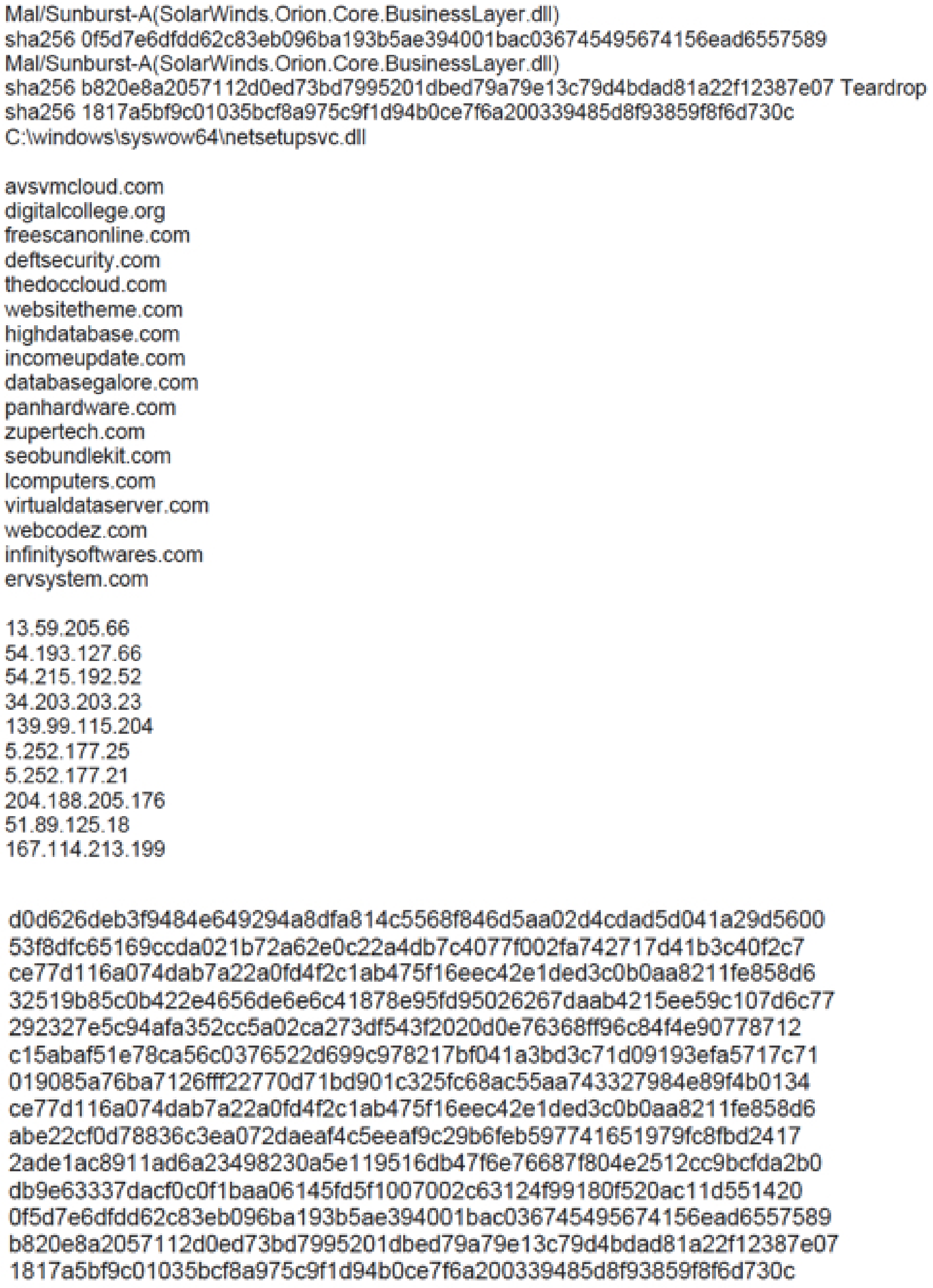
file_path_name C:\windows\syswow64\netsetupsvc.dll TEARDROP memory module used to drop Cobalt Strike Beacon.

domain avsvmcloud.com malware/callhome
domain digitalcollege.org malware/callhome
domain freescanonline.com malware/repository
domain deftsecurity.com malware/callhome
domain thedoccloud.com malware/callhome
domain websitetheme.com malware/repository
domain highdatabase.com malware/repository
domain incomeupdate.com malware/callhome
domain databasegalore.com malware/callhome
domain panhardware.com malware/callhome
domain zupertech.com malware/callhome
domain seobundlekit.com malware/callhome
domain lcomputers.com malware/callhome
domain virtualdataserver.com malware/repository
domain webcodez.com malware/callhome
domain infinitysoftwares.com malware/callhome
domain ervsystem.com malware/callhome

ip 13.59.205.66 C2 malware/repository
ip 54.193.127.66 C2 malware/repository
ip 54.215.192.52 C2 malware/repository
ip 34.203.203.23 C2 malware/callhome
ip 139.99.115.204 C2 malware/callhome
ip 5.252.177.25 C2 malware/callhome
ip 5.252.177.21 C2 malware/callhome
ip 204.188.205.176 C2 malware/callhome
ip 51.89.125.18 C2 malware/callhome
ip 167.114.213.199 C2 malware/callhome



sha256 d0d626deb3f9484e649294a8dfa814c5568f846d5aa02d4cdad5d041a29d5600
Troj/SunBurst-A(Installer|CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp)
sha256 53f8dfc65169ccda021b72a62e0c22a4db7c4077f002fa742717d41b3c40f2c7
Mal/Generic-S(Solarwinds Worldwide LLC)
sha256 ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6
Mal/Sunburst-A(SolarWinds.Orion.Core.BusinessLayer.dll)
sha256 32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77
Mal/Sunburst-A(SolarWinds.Orion.Core.BusinessLayer.dll)
sha256 292327e5c94afa352cc5a02ca273df543f2020d0e76368ff96c84f4e90778712
Mal/Generic-S(OrionImprovementBusinessLayer.2.cs)
sha256 c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71
Mal/Sunburst-B(app_web_logoimagehandler.ashx.b6031896.dll).SuperNova webshell backdoor
sha256 019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134
Mal/Sunburst-A(SolarWinds.Orion.Core.BusinessLayer.dll)
sha256 ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6
Mal/Sunburst-A(SolarWinds.Orion.Core.BusinessLayer.dll)
sha256 abe22cf0d78836c3ea072daeaf4c5eeaf9c29b6feb597741651979fc8fbd2417
Mal/Sunburst-A(SolarWinds.Orion.Core.BusinessLayer.dll)
sha256 2ade1ac8911ad6a23498230a5e119516db47f6e76687f804e2512cc9bcfda2b0
Mal/Sunburst-A(SolarWinds.Orion.Core.BusinessLayer.dll)
sha256 db9e63337dacf0c0f1baa06145fd5f1007002c63124f99180f520ac11d551420



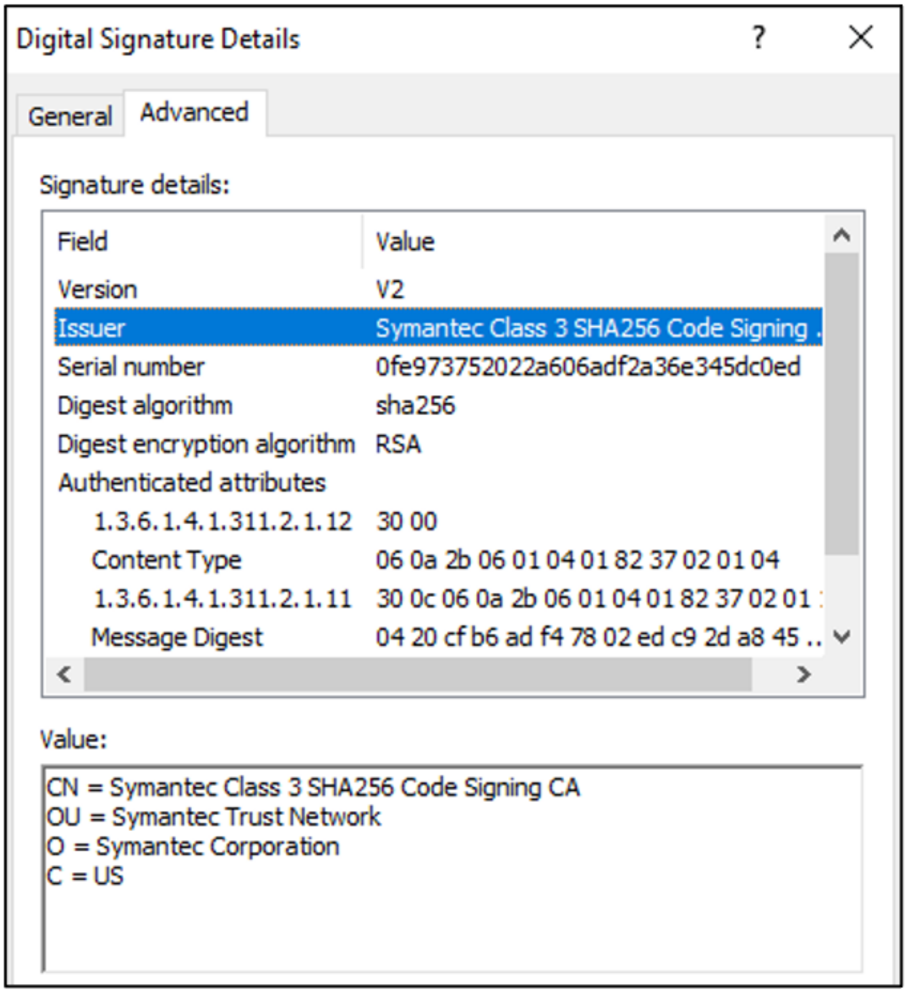
```
Mal/Sunburst-A(SolarWinds.Orion.Core.BusinessLayer.dll)
sha256 0f5d7e6dfdd62c83eb096ba193b5ae394001bac036745495674156ead6557589
Mal/Sunburst-A(SolarWinds.Orion.Core.BusinessLayer.dll)
sha256 b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07 Teardrop
sha256 1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c
C:\windows\syswow64\netsetupsvc.dll

avsvmcloud.com
digitalcollege.org
freescanonline.com
deftsecurity.com
thedoccloud.com
websitetheme.com
highdatabase.com
incomeupdate.com
databasegalore.com
panhardware.com
zupertech.com
seobundlekit.com
lcomputers.com
virtualdataserver.com
webcodez.com
infinitysoftwares.com
ervsystem.com

13.59.205.66
54.193.127.66
54.215.192.52
34.203.203.23
139.99.115.204
5.252.177.25
5.252.177.21
204.188.205.176
51.89.125.18
167.114.213.199

d0d626deb3f9484e649294a8dfa814c5568f846d5aa02d4cdad5d041a29d5600
53f8dfc65169ccda021b72a62e0c22a4db7c4077f002fa742717d41b3c40f2c7
ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6
32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77
292327e5c94afa352cc5a02ca273df543f2020d0e76368ff96c84f4e90778712
c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71
019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134
ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6
abe22cf0d78836c3ea072daeaf4c5eeaf9c29b6feb597741651979fc8fbd2417
2ade1ac8911ad6a23498230a5e119516db47f6e76687f804e2512cc9bcfda2b0
db9e63337dacf0c0f1baa06145fd5f1007002c63124f99180f520ac11d551420
0f5d7e6dfdd62c83eb096ba193b5ae394001bac036745495674156ead6557589
b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07
1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c
```

TACTICS, TECHNIQUES, AND PROCEDURES (TTPs)

MITRE evaluated 58 of 60 in scope Enterprise ATT&CK techniques across 10 ATT&CK tactics including 12 techniques for privilege escalation, 13 techniques for credential access and nine techniques for lateral movement (LINK): https://www.exabeam.com/information-security/who-is-apt29/

How was the SolarWinds Malware Deployed?

The malware was deployed as part of an update from SolarWinds' own servers and was digitally signed by a valid digital certificate bearing their name. This strongly points to a supply chain attack. The certificate was issued by Symantec with serial number 0fe973752022a606adf2a36e345dc0ed.



Signature details:

Field	Value
Version	V2
Issuer	Symantec Class 3 SHA256 Code Signing .
Serial number	0fe973752022a606adf2a36e345dc0ed
Digest algorithm	sha256
Digest encryption algorithm	RSA
Authenticated attributes	
1.3.6.1.4.1.311.2.1.12	30 00
Content Type	06 0a 2b 06 01 04 01 82 37 02 01 04
1.3.6.1.4.1.311.2.1.11	30 0c 06 0a 2b 06 01 04 01 82 37 02 01
Message Digest	04 20 cf b6 ad f4 78 02 ed c9 2d a8 45 ..

Value:

CN = Symantec Class 3 SHA256 Code Signing CA
OU = Symantec Trust Network
O = Symantec Corporation
C = US

Source: SANs.org

TACTICAL THREAT HUNTING

CSFI would like to recommend blue teams to deploy **Security Onion for threat hunting** by implementing **Zeek, Kolide and osquery**. Threat hunters are able to issue create multiple commands and run them against multiple hosts within the network.

This is a query for a Solarwinds hack hunting:

SELECT * from hash where directory like 'C:\Program Files\Solarwinds\%' or directory like 'C:\Program Files (x86)\Solarwinds\%'

AND md5 = ' **PASTE MD5 here** '

C:\Program Files\Solarwinds\ and C:\Program Files (x86)\Solarwinds\ are Solarwind Orion's default installation directories (but, it may be installed on the other location/path).

The query needs to paste the relevant MD5 and run.

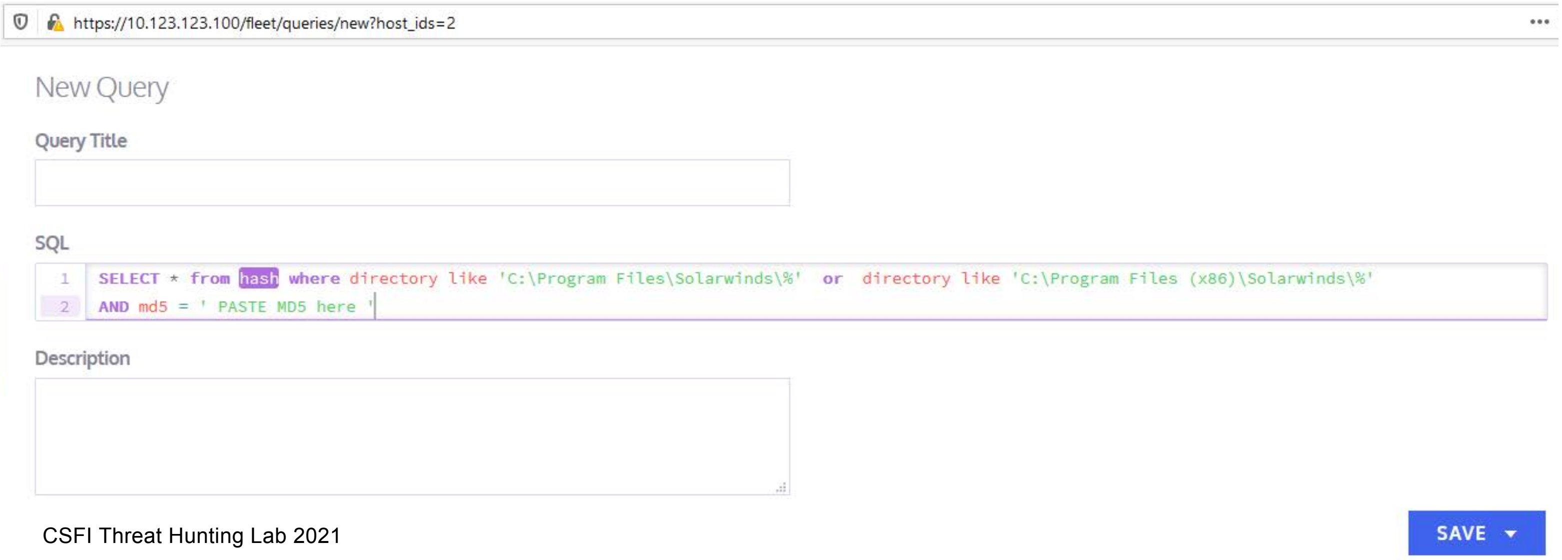
IOC list - https://us-cert.cisa.gov/ncas/alerts/aa20-352a

Query sample with one of the Solarwinds IOCs -

SELECT * from hash where directory like 'C:\Program Files\Solarwinds\%' or directory like 'C:\Program Files (x86)\Solarwinds\%'

AND md5 = '610ec1ab7701b410df1e309240343cdf'

NOTE: Please feel free to email contact@csfi.us if your organization would like CSFI's assistance with threat hunting.



```
SELECT * from hash where directory like 'C:\Program Files\Solarwinds\%'  or  directory like 'C:\Program Files (x86)\Solarwinds\%'
AND md5 = ' PASTE MD5 here '
```

CSFI Threat Hunting Lab 2021

CSFI OPERATIONAL SPONSORS

The Importance of Cyber Threat Intelligence can improve security effectiveness when appropriately used. CTI can facilitate better-informed security and business decisions and eventually enable organizations to take crucial action to defend their users, data, and reputation against adversaries. The CSFI CTI Report focuses on a *rapid tactical threat intelligence* used to considerably improve current security controls and methods to improve incident response.

Silobreaker offers all CSFI members a 30-day complimentary access to support their threat intelligence initiatives. For more information, please visit www.silobreaker.com or email darrell.johnston@silobreaker.com.

For more information about Cobwebs Web Intelligence (WEBINT) solutions, please visit https://cobwebs.com or email John.Ohare@cobwebs.com.

A special thanks for those who serve in silence and to all of our CSFI CTI volunteers! Please feel free to contact CSFI at contact@csfi.us if your organization would like to become a CSFI Operational Sponsor, or as CSFI GOLD SPONSOR.

CSFI Operational Sponsors provide operational support through the donation of vital collaborative services and technologies.

CSFI

Digitally signed by CSFI
Date: 2021.01.08 15:49:29 -05'00'