The SolarWinds Orion SUNBURST Supply-chain Attack - Trulysuper

By siteadmin

Published: 2020-12-16 · Archived: 2026-04-05 13:24:39 UTC

UPDATE 2020-12-19 23:20 UTC: updated results table

UPDATE 2020-12-21 15:37 UTC: updated section on C2 infrastructure based on current findings
UPDATE 2020-12-22 17:04 UTC: added link to Invoke-SunburstDecoder
UPDATE 2020-12-22 22:48 UTC: added section: Disabling security services and avoiding detection
UPDATE 2020-12-23 17:33 UTC: updated results table
UPDATE 2021-01-26 13:00 UTC: clarified some of the statements about targeted organizations, as they are only assumptions.

This post provides a list of internal names of organizations that had the SUNBURST backdoor installed, as well as which of these organizations have indications of having proceeded to the second stage of the attack, where further internal compromise might have taken place.

Summary

The recent SolarWinds Orion hack is part of a cyber attack that is one of the most severe in history.

A supply chain attack leveraged SolarWinds Orion updates to deliver a backdoor to potentially 18,000 SolarWinds customers. The attack was highly sophisticated.

The infected systems in the various compromised organizations were configured to probe the threat actor systems to request instructions.

Truesec Threat Intelligence analyzed the malware, as well as historical network data, to determine some of the affected organizations that the threat actor might have explicitly selected for further activities, where it is possible that further internal compromise took place. These assumptions are based on historical network data (passive DNS) and the logic within the malware when handling certain responses.

While this is likely only a small part of the scope of the attack, it provides indications on the type of organizations that were potentially the real targets of the attack.

Some names stand out, such as ggsg-us.cisco (**Cisco GGSG**), us.deloitte.co (**Deloitte**), nswhealth.net (**NSW Ministry of Health in Australia**), **banccentral.com** (service supplier of IT and security for banks), and many others.

The impact of this attack is likely to be of gigantic proportions. The full extent of this breach will most likely never be communicated to the public, and instead will be restricted to trusted parts of the intelligence community.

Introduction

A supply chain attack leveraged SolarWinds to deliver malicious software updates to their customers (approximately 18.000 potentially affected customers according to SolarWinds). The update installed a sophisticated backdoor giving the threat actor the ability to access selected targets and proceed with further activities inside the compromised organizations.

It is believed that the attack was carried out by a nation-state actor, likely APT29 a.k.a. Cozy Bear, i.e. Russian Intelligence.

FireEye and Microsoft initially published reports[1][2] describing some of the inner workings of the backdoor. A second, more detailed, post was later published by FireEye[15]. The backdoor is remarkably sophisticated and is worth a long technical description, while only some of its functionalities and characteristics are described in this article.

Truesec Threat Intelligence analyzed the backdoor as well as historical network data to identify patterns revealing possible victims.

Due to the nature of the attack, a large number of organizations around the world have been affected by the backdoor, while likely only a smaller number were specifically selected and targeted by the threat actor to conduct additional internal compromise (phase 2).

Technical Background

The threat actor was able to inject a backdoor in the Solarwinds Orion software by modifying the source code of an existing plugin, which was then signed by Solarwinds and published as part of an update available on the SolarWinds website. SolarWinds published an advisory[3] specifying the versions affected.

The malicious update has been available for several months and there are indications of breaches as early as March 2020. One of the identified malicious updates was hosted at the following URL:

```
hxxps://downloads.solarwinds[.]com/solarwinds/CatalogResources/Core/2019.4/2019.4.5220.20574/SolarWinds-Core-
```

The update package was properly digitally-signed, as shown below.

Figure 1 – Malicious Solarwinds Orion update containing SUNBURST backdoor

The backdoor code was made part of the following digitally-signed Orion component:

```
SolarWinds.Orion.Core.BusinessLayer.dll
```

This DLL is also signed.

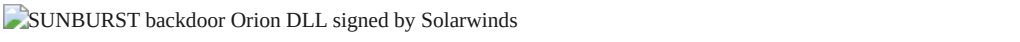

Figure 2 – Malicious Solarwinds Orion DLL containing SUNBURST backdoor

The backdoor implements sophisticated functionality to communicate with the threat actor infrastructure and applies logic to determine what actions should be taken.

As a large number of Orion servers around the world have been infected with the backdoor, the threat actor had to have a way to determine which organization was contacting the attack infrastructure to be able to select the real target of this attack. This logic is partially explained below. For details see the FireEye article [15].

The hacked servers that received the Solarwinds backdoor periodically probe the threat actor infrastructure with a DNS query like the following:

```
<DGA_value>.appsync-api.eu-west-1[.]avsvmcloud[.]com
```

where <DGA_value> is computed with a DomainName Generation Algorithm and contains an encoded version of the internal Active Directory name of the infected server. The threat actor server decodes the information in the DNS requests and uses the internal domain name of the organization to determine what instructions to send back.

Truesec reversed the backdoor and identified a set of IP address ranges that, when received as part of the DNS response, will determine the actions taken by the backdoor code. Part of this code is illustrated in the figure below.

Figure 3 – Reversed SUNBURST backdoor showing IP ranges used to determine next actions

The **AddressFamily** field determines what the backdoor should do next, which can be roughly summarized as follows:

Atm or ImpLink : Terminate (killswitch).

Ipx : Go to initial state and keep polling.

NetBios: Start or continue second stage. Can initialize an HTTP backdoor channel used to collect additional information and deploy a second stage malware (specified by the threat actor at the time of instructions, and therefore specific to the target).

We can therefore assume that if the initial probe was answered with an address of type **NetBios**, the threat actor had configured the backdoor to move to the second stage, which is where additional malware can be deployed to possibly perform additional internal compromise.

Given the number of affected organizations, it is still likely that a large number of victims with indications of stage 2, as described here, were later filtered out by the threat actor (not deemed worthy of further attack).

Identifying Internal Names of Victims

The DomainName Generation Algorithm described earlier, used to create a DNS query containing an encoded value of the internal domain name of the compromised organization, can be reversed.

RedDrip Team published a report[4] and a script[5] to decode the DGA part of the DNS requests, therefore allowing to retrieve the cleartext value of the internal domain name of the hacked server that made the request.

For example, if a compromised server makes the following request to the threat actor server:

```
ciepcqqog816s6urtt6t0kf60ceo6e20.appsync-api.us-east-2.avsvmcloud[.]com
```

This can be decoded to obtain the following internal name of the victim:

```
ggsg-us.cisco
```

This means that having records of performed DNS requests to avsvmcloud[.]com will reveal the internal names of the compromised organizations.

The SUNBURST backdoor uses the following three parameters to create a “Host Id” used in the DNS requests:

- MAC address of the network interface
- Internal domain name that the machine is joined to
- Machine Guid from **HKEY_LOCAL_MACHINESOFTWAREMicrosoftCryptographyMachineGuid**

Since the DGA values from DNS requests can be decoded, if you have a DNS request and you want to see if it was generated from a certain machine, you only need to know MAC address, internal domain name, and machine Guid.

This can be extremely helpful during investigations to determine if a machine had a communicating SUNBURST backdoor on it. We wrote a PowerShell script that can be used for this, based on the great work by Erik Hjelmvik, Netresec.

Identifying Threat Actor Instructions

The next step was to obtain historical records of DNS requests, **including the response**. We obtained some of the available historical data[6].

The sample data contains 1528 DNS requests to avsvmcloud[.]com and their responses.

When filtered for requests matching the DGA algorithm syntax, we have requests with dates ranging from early April to December 2020.

This is an example of such request and response:

```
date : 2020-04-19 08:24:26
last_seen : 2020-04-19 08:24:27
qtype : 1
domain : avsvmcloud.com
qname : q8bps26mocuq6re4dutru70ct2w.appsync-api.us-east-1.avsvmcloud.com
value_ip : 8.18.144.138
type : ip
_key : 0e8ab64d5f5aff04fea862f4f72fcf1d04c3d377
value : 8.18.144.138
```

From this data we can determine that on April 19th, a request was made that decodes to the internal name **pageaz.gov**, and received as response 8.18.144.138, which according to the backdoor logic explained earlier maps to address type **NetBios**, meaning that the threat actor might have deployed an HTTP backdoor in this environment.

Command and Control Infrastructure

By analyzing the IP addresses returned when instructing infected servers to establish an HTTP backdoor, we can identify the following blocks.

IP block	Registered Organization (WHOIS information)
184.72.0.0 / 255.254.0.0	Amazon.com, Inc.
71.152.53.0 / 255.255.255.0	Amazon.com, Inc.
8.18.144.0 / 255.255.254.0	Amazon Inc.
87.238.80.0 / 255.255.248.0	Amazon Data Services Ireland DUB3 Datacentre
18.130.0.0 / 255.255.0.0	Amazon Technologies Inc.
99.79.0.0 / 255.255.0.0	Amazon Data Services Canada
199.201.117.0 / 255.255.255.0	Traiana, Inc

Table 1 – List of IP blocks used when instructing systems to establish an HTTP backdoor, mapped to WHOIS information

These IP blocks are **not** used to establish the HTTP connection. Instead, if a CNAME record is contained in the response, that is the address used as C2 address for the new HTTP channel. FireEye listed the CNAME responses that they have observed as part of their indicators of compromise[9]. These are also reported below for convenience:

```
freescanonline[.]com
deftsecurity[.]com
freescanonline[.]com
thedoccloud[.]com
```

We initially thought that the A records in the blocks above were the C2 addresses, which would also make sense as almost all are part of the Amazon infrastructure and threat actors often use cloud providers to host their attack infrastructure. This would have also meant that the block belonging to **Traiana, Inc** could potentially be under the control of the threat actor.

Truesec Threat Intelligence observed a large number of DNS responses from the threat actor server providing different IP addresses in the range 199.201.117.0/24 for the next stage.

At this point in time, it does not seem that these IP blocks were under the control of the threat actor, but were instead deliberately used as part of the logic within the backdoor.

Putting the Pieces Together

We have decoded the DGA parts of the requests to identify internal domain names of compromised organizations, correlated that with the responses received from the threat actor server, and mapped them with the hardcoded list of IP ranges in the backdoor code.

This gives us a (partial) list of breached organizations, and which ones had the SUNBURST backdoor configured for the second stage of the attack where further internal compromise might have taken place.

Note that some of the names are truncated. Further analysis is ongoing to determine if this can be improved.

The results are summarized at the bottom of this post. This list contains the decoded values of internal domain names. We can therefore only **assume** that they belong to an organization based on the name of the domains and publicly available information.

Some of the internal names stand out, such as ggsg-us.cisco (**Cisco GGSG**), us.deloitte.co (**Deloitte**), nswhealth.net (**NSW Ministry of Health in Australia**), **banccentral.com** (service supplier of IT and security for banks), and many others.

Disabling Security Services and Avoiding Detection

The backdoor keeps an eye on a number of processes, services, and device drivers. It simply avoids running if any of the following 137 processes are detected on the system.

```
apimonitor-x64
apimonitor-x86
autopsy64
autopsy
autoruns64
autoruns
autorunsc64
autorunsc
binaryninja
blacklight
cutter
de4dot
debugview
diskmon
dnsd
dnspy
dotpeek32
dotpeek64
dumpcap
exeinfope
fakedns
fakenet
ffdec
fiddler
fileinsight
floss
gdb
hiew32
idaq64
idaq
idr
ildasm
ilspy
jd-gui
lordpe
officemalscanner
ollydbg
pdfstreamdumper
pe-bear
pebrowse64
peid
pe-sieve32
pe-sieve64
pestudio
peview
pexplorer
ppee
ppee
procdump64
procdump
processhacker
procexp64
procexp
```

```
procmon
prodiscoverbasic
py2exedecompiler
r2agent
rabin2
radare2
ramcapture64
ramcapture
reflector
regmon
resourcehacker
retdec-ar-extractor
retdec-bin2llvmir
retdec-bin2pat
retdec-config
retdec-fileinfo
retdec-getsig
retdec-idr2pat
retdec-llvmir2hll
retdec-macho-extractor
retdec-pat2yara
retdec-stacofin
retdec-unpacker
retdec-yarac
rundotnetdll
sbiesvc
scdbg
scylla_x64
scylla_x86
shellcode_launcher
solarwindsdiagnostics
sysmon64
sysmon
tcpdump
tcpvcon
tcpview
vboxservice
win32_remote
win64_remotex64
windbg
windump
winhex64
winhex
winobj
wireshark
x32dbg
x64dbg
xwforensics64
xwforensics
redcloak
avgsvc
avgui
avgsvca
avgidsagent
avgsvcx
avgwdsvcx
avgadminclientservice
afwserv
avastui
avastsvc
aswidsagent
```

```
aswidsagenta
aswengsrv
avastavwrapper
bccavsvc
psanhost
psuaservice
psuamain
avp
avpui
ksde
ksdeui
tanium
taniumclient
taniumdetectengine
taniumendpointindex
taniumtracecli
taniumtracewebsocketclient64
```

The second check is a list of 8 services matched by process names. The backdoor searches for the services and keeps track of the status of the services. Additionally, it changes the security descriptor of the service registry key and the start parameter. The service is never stopped by the backdoor and it looks like it simply waits until the machine restarts for the service to change state. The state of the services is recorded and stored in the DLL config file using the parameter **RetryWatcherPostpone**

The list of services is the following:

```
msmpeng
mssense
cavp
cb
csfalconservice
csfalconcontainer
xagt
xagtnotif
ekrn
eguiproxy
egui
fsgk32st
fswebuid
fsgk32
fsma32
fssm32
fnrb32
fsaua
fsorsp
fsav32
```

The backdoor **avoids tampering with the start parameter of the WinDefend service** and only changes the service key security descriptor.

The third check is performed to detect 17 specific device drivers. This check behaves the same way as the check for processes and will make sure that the backdoor aborts if any of the following drivers are detected.

```
cybkerneltracker.sys
atrsdfw.sys
eaw.sys
rvsavd.sys
dgdmk.sys
sentinelmonitor.sys
hexisfsmonitor.sys
```

```
groundling32.sys
groundling64.sys
safe-agent.sys
crexecprev.sys
psepfilter.sys
cve.sys
brfilter.sys
brcow_x_x_x_x.sys
lragentmf.sys
libwamf.sys
```

Based on this analysis, we can conclude that the detection of any of the specified **processes** or **device drivers** will always alter the execution path of the backdoor and **discontinue the execution**. While the detection of the listed services will only alter the execution path if a change in the status was detected.

Note that for services running as protected services, changing the service registry start parameter is not possible while the service is running. This applies to services related to any antimalware with ELAM capabilities like the Windows Defender.

The Backdoor does not try to avoid the listed antivirus, antimalware, and EDR service. For unknown reasons, it tries to keep track of the status of these services.

Impact of the Attack

The target organizations, the threat actor sophistication, and the amount of time between the initial breach and the discovery strongly indicates an impact of gigantic proportions.

It is highly likely that a massive amount of highly confidential information belonging to government organizations, medical institutions, cybersecurity, the financial industry, etc. has been leaked. It is also highly likely that software and systems have been compromised and that the modus operandi of the SolarWinds breach can be repeated in future campaigns.

More information will be disclosed during the upcoming months but the full extent of this breach will most likely never be communicated to the public, and instead will be restricted to trusted parts of the intelligence community.

Results of the Analysis

Decoded Internal Name	Possible Organization (may be inaccurate)*	Observed Message	First Seen
f.gnam		2nd stage	2020-04-04
corp.stratusnet	Stratus Networks	2nd stage	2020-04-17
pageaz.gov	City of Page	2nd stage	2020-04-19
tx.org		2nd stage	2020-04-19
newdirections.kc		2nd stage	2020-04-21
christieclinic.com	Christie Clinic Telehealth	2nd stage	2020-04-22
osb.local		2nd stage	2020-04-28
MOC.local		2nd stage	2020-04-30
ehtuh-		2nd stage	2020-05-01
resprod.com	Res Group (Renewable energy company)	2nd stage	2020-05-06
barrie.ca	City of Barrie	2nd stage	2020-05-13
te.nz	TE Connectivity (Sensor manufacturer)	2nd stage	2020-05-13
fisherbartoninc.com	The Fisher Barton Group (Blade Manufacturer)	2nd stage	2020-05-15

sdch.local	South Davis Community Hospital	2nd stage	2020-05-18
internal.jtl.c		2nd stage	2020-05-19
mnh.rg-law.ac.il	College of Law and Business, Israel	2nd stage	2020-05-26
RPM.loca		2nd stage	2020-05-28
CIRCU		2nd stage	2020-05-30
magnoliaisd.loc	Magnolia Independent School District	2nd stage	2020-06-01
fidelitycomm.lo	Fidelity Communications (ISP)	2nd stage	2020-06-02
fidelitycomm.local		2nd stage	2020-06-02
corp.stingraydi	Stingray (Media and entertainment)	2nd stage	2020-06-03
keyano.local	Keyano College	2nd stage	2020-06-03
friendshipstatebank.com		2nd stage	2020-06-06
ghsmain1.ggh.g		2nd stage	2020-06-09
ieb.go.id		2nd stage	2020-06-12
nswhealth.net	NSW Health	2nd stage	2020-06-12
city.kingston.on.ca	City of Kingston, Ontario, Canada	2nd stage	2020-06-15
servitia.intern		2nd stage	2020-06-16
CONSOLID		2nd stage	2020-06-17
corp.ptci.com	Pioneer Telephone Scholarship Recipients	2nd stage	2020-06-19
ironform.com	Ironform (metal fabrication)	2nd stage	2020-06-19
digitalsense.co	Digital Sense (Cloud Services)	2nd stage	2020-06-24
ggsg-us.cisco	Cisco GGSG	2nd stage	2020-06-24
CentralY		2nd stage	2020-06-24
signaturebank.l	Signature Bank	2nd stage	2020-06-25
signaturebank.local		2nd stage	2020-06-25
Aerial.l		2nd stage	2020-06-26
mountsinai.hosp	Mount Sinai Hospital	2nd stage	2020-07-02
pqcorp.com	PQ Corporation	2nd stage	2020-07-02
mountsinai.hospital	Mount Sinai Hospital, New York	2nd stage	2020-07-02
banccentral.com	BancCentral Financial Services Corp.	2nd stage	2020-07-03
fhc.local		2nd stage	2020-07-06
isi		2nd stage	2020-07-06
gxw		2nd stage	2020-07-07
kcpl.com	Kansas City Power and Light Company	2nd stage	2020-07-07
lufkintexas.net	Lufkin (City in Texas)	2nd stage	2020-07-07
sm-group.local	SM Group (Distribution)	2nd stage	2020-07-07

cys.local	CYS Group (Marketing analytics)	2nd stage	2020-07-10
escap.org		2nd stage	2020-07-10
ftsillapachecasi		2nd stage	2020-07-10
oslerhc.org	William Osler Health System	2nd stage	2020-07-11
wrbaustralia.ad	W. R. Berkley Insurance Australia	2nd stage	2020-07-11
dufferincounty.on.ca	Dufferin County, Ontario, Canada	2nd stage	2020-07-17
fmtn.ad	City of Farmington	2nd stage	2020-07-21
htwanmgmt.local		2nd stage	2020-07-22
pcsco.com	Professional Computer Systems	2nd stage	2020-07-23
COTESTDE		2nd stage	2020-07-25
camcity.local	Adult Webcam	2nd stage	2020-07-28
usd373.org	Newton Public Schools	2nd stage	2020-08-01
Ameri		2nd stage	2020-08-02
sfsi.stearnsban	Stearns Bank	2nd stage	2020-08-02
ville.terrebonn	Ville de Terrebonne	2nd stage	2020-08-02
Amerisaf		2nd stage	2020-08-02
chc.dom		2nd stage	2020-08-04
FWO.IT		2nd stage	2020-08-05
azlcyy		2nd stage	2020-08-07
itps.uk.net	ITPS (IT Services)	2nd stage	2020-08-11
bhq.lan		2nd stage	2020-08-18
prod.hamilton.	Hamilton Company	2nd stage	2020-08-19
BCC.loca		2nd stage	2020-08-22
aiwo		2nd stage	2020-08-24
cosgroves.local	Cosgroves (Building services consulting)	2nd stage	2020-08-25
moncton.loc	City of Moncton	2nd stage	2020-08-25
ad001.mtk.lo	Mediatek	2nd stage	2020-08-26
cds.capilanou.	Capilano University	2nd stage	2020-08-27
csnt.princegeor	City of Prince George	2nd stage	2020-09-18
int.ncahs.net		2nd stage	2020-09-23
CIMBM		2nd stage	2020-09-25
netdecisions.lo	Netdecisions (IT services)	2nd stage	2020-10-04
.sutmf		Wait	2020-06-25
mixonhill.com	Mixon Hill (intelligent transportation systems)	Terminate	2020-04-29
yorkton.cofy	Community Options for Families & Youth	Terminate	2020-05-08

ies.com	IES Communications	Terminate	2020-06-11
spsd.sk.ca	Saskatoon Public Schools	Terminate	2020-06-12
cow.local		Terminate	2020-06-13
KS.LOCAL		Terminate	2020-07-10
bcofsa.com.ar	Banco de Formosa	Terminate	2020-07-13
ansc.gob.pe	GOB (Digital Platform of the Peruvian State)	Terminate	2020-07-25
bop.com.pk	The Bank of Punjab	Terminate	2020-07-31
airquality.org		Terminate	2020-08-09
dokkenengineerin		Terminate	2020-08-19
3if.2l		Terminate	2020-08-20
rbe.sk.ca	Regina Public Schools	Terminate	2020-08-20
ni.corp.natins		Terminate	2020-10-24
phabahamas.org	Public Hospitals Authority, Caribbean	Terminate	2020-11-05
insead.org	INSEAD Business School	Terminate	2020-11-07
deniz.denizbank	DenizBank	Terminate	2020-11-14
bi.corp		Terminate	2020-12-14
ccscurriculum.c		Unknown	2020-04-18
bisco.int	Bisco International (Adhesives and tapes)	Unknown	2020-04-30
atg.local		Unknown	2020-05-11
internal.hws.o		Unknown	2020-05-23
grupobazar.loca		Unknown	2020-06-07
xnet.kz	X NET (IT provider in Kazakhstan)	Unknown	2020-06-09
ush.com		Unknown	2020-06-15
publiser.it		Unknown	2020-07-05
us.deloitte.co	Deloitte	Unknown	2020-07-08
n2k		Unknown	2020-07-12
e-idsolutions.	IDSolutions (video conferencing)	Unknown	2020-07-16
xijtt-		Unknown	2020-07-21
ETC1.local		Unknown	2020-08-01
ninewellshospita		Unknown	2020-08-21
ABLE.local		N/A	N/A
acmedctr.ad		N/A	N/A
ad.azarthritis.com	Arizona Arthritis & Rheumatology Associates	N/A	N/A
ad.library.ucla.edu		N/A	N/A
ad.optimizely.	Optimizely, Software Company	N/A	N/A

admin.callidusc		N/A	N/A
aerioncorp.com	Aerion Corporation	N/A	N/A
agloan.ads		N/A	N/A
ah.org		N/A	N/A
AHCCC		N/A	N/A
allegronet.co.		N/A	N/A
alm.brand.dk		N/A	N/A
amalfi.local		N/A	N/A
americas.phoeni		N/A	N/A
amr.corp.intel		N/A	N/A
apu.mn		N/A	N/A
ARYZT		N/A	N/A
b9f9hq		N/A	N/A
BE.AJ		N/A	N/A
belkin.com	Belkin International	N/A	N/A
bk.local		N/A	N/A
bmrn.com		N/A	N/A
bok.com		N/A	N/A
BrokenArrow.Local		N/A	N/A
btb.az		N/A	N/A
c4e-internal.c		N/A	N/A
calsb.org		N/A	N/A
casino.prv		N/A	N/A
cda.corp		N/A	N/A
central.pima.gov	Pima County, Arizona	N/A	N/A
cfsi.local		N/A	N/A
ch.local		N/A	N/A
ci.dublin.ca.us	Dublin, California	N/A	N/A
cisco.com	Cisco	N/A	N/A
cityofsacramento	City of Sacramento	N/A	N/A
clinicasierravista.org	Clinica Sierra Vista	N/A	N/A
corp.dvd.com		N/A	N/A
corp.sana.com	Sana Biotechnology	N/A	N/A
COWI.Net		N/A	N/A
coxnet.cox.com		N/A	N/A

CRIHB.NET		N/A	N/A
cs.haystax.local		N/A	N/A
csa.local		N/A	N/A
csci-va.com		N/A	N/A
csqsxh		N/A	N/A
DCCAT.DK		N/A	N/A
deltads.ent		N/A	N/A
detmir-group.ru		N/A	N/A
dhhs-ad.		N/A	N/A
digitalreachinc.com		N/A	N/A
dmv.state.nv.us		N/A	N/A
dotcomm.org		N/A	N/A
ebe.co.roanoke.va.us		N/A	N/A
ecobank.group	Ecobank	N/A	N/A
ecocorp.local		N/A	N/A
epl.com		N/A	N/A
fa.lcl		N/A	N/A
fortsmithlibrary.org		N/A	N/A
fremont.lamrc.net		N/A	N/A
FSAR.LOCAL		N/A	N/A
ftfcu.corp		N/A	N/A
FVF.locam		N/A	N/A
gksm.local		N/A	N/A
gloucesterva.net		N/A	N/A
glu.com		N/A	N/A
gnb.local		N/A	N/A
gncu.local		N/A	N/A
gsf.cc		N/A	N/A
gyldendal.local		N/A	N/A
helixwater.org	Helix Water District	N/A	N/A
hgvc.com		N/A	N/A
HQ.RE-wwgi2xnl		N/A	N/A
ia.com		N/A	N/A
inf.dc.net		N/A	N/A
ingo.kg		N/A	N/A

innout.corp		N/A	N/A
int.lukoil-international.uz	Lukoil	N/A	N/A
intensive.int		N/A	N/A
its.iastate.ed		N/A	N/A
jarvis.lab		N/A	N/A
LABELMARKET.ES		N/A	N/A
lasers.state.la.us		N/A	N/A
milledgeville.local	milledgeville, Georgia	N/A	N/A
mutualofomahabank.com	Mutual of Omaha Bank	N/A	N/A
nacr.com		N/A	N/A
ncpa.loc		N/A	N/A
neophotonics.co	NeoPhotonics Corporation	N/A	N/A
net.vestfor.dk		N/A	N/A
nih.if		N/A	N/A
nvidia.com	Nvidia	N/A	N/A
on-pot		N/A	N/A
orient-express.com	Orient Express	N/A	N/A
paloverde.local		N/A	N/A
rai.com		N/A	N/A
rccf.ru		N/A	N/A
repsrv.com		N/A	N/A
ripta.com		N/A	N/A
roymerlin.com		N/A	N/A
rs.local		N/A	N/A
rst.atlantis-pak.ru		N/A	N/A
SamuelMerritt.edu	Samuel Merritt University	N/A	N/A
sbywx3		N/A	N/A
sc.pima.gov		N/A	N/A
scif.com		N/A	N/A
SCMRI.local		N/A	N/A
scroot.com		N/A	N/A
seattle.interna		N/A	N/A
securview.local		N/A	N/A
SFBALLET		N/A	N/A
SF-Libra		N/A	N/A

siskiyous.edu	College of the Siskiyous, California	N/A	N/A
sjhsagov.org		N/A	N/A
Smart		N/A	N/A
smes.org		N/A	N/A
sos-ad.state.nv.us		N/A	N/A
sro.vestfor.dk		N/A	N/A
staff.technion.ac.il		N/A	N/A
superior.local		N/A	N/A
swd.local		N/A	N/A
taylorfarms.com		N/A	N/A
thajxq		N/A	N/A
thoughtspot.int		N/A	N/A
tr.technion.ac.il		N/A	N/A
tv2.local		N/A	N/A
uis.kent.edu		N/A	N/A
uncity.dk		N/A	N/A
uont.com		N/A	N/A
vantagedatacenters.local	Vantage Data Centers	N/A	N/A
viam-invenient		N/A	N/A
vms.ad.varian.com		N/A	N/A
voceracommunications.com	Vocera Communications	N/A	N/A
vsp.com		N/A	N/A
WASHOE.W		N/A	N/A
weioffice.com		N/A	N/A
wfhf1.hewlett.		N/A	N/A
woodruff-sawyer		N/A	N/A
xdxinc.net		N/A	N/A
y9k.in		N/A	N/A
zeb.i8		N/A	N/A
zippertubing.com	Zippertubing	N/A	N/A

* *The organization names are assumptions based on the decoded internal names and may be inaccurate.*

---

[1] https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

[2] https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/

[3] https://www.solarwinds.com/securityadvisory

[4] https://mp.weixin.qq.com/s/v-ekPFtVNZG1W7vWjcuVug

[5] https://github.com/RedDrip7/SunBurst_DGA_Decode

[6] https://github.com/bambenek/research/tree/main/sunburst

[7] https://www.cls-group.com/partnerships/traiana-inc/

[8] http://www.traiana.com

[9] https://github.com/fireeye/sunburst_countermeasures/blob/main/indicator_release/Indicator_Release_NBIs.csv

[10] https://github.com/Truesec/sunburst-decoder

[11] https://www.netresec.com/?page=Blog&month=2020-12&post=Reassembling-Victim-Domain-Fragments-from-SUNBURST-DNS

[12] https://gist.githubusercontent.com/IISResetMe/d61a2263c617959eda2682e94f8df8b1/raw/ebc9e675c961c2c3f5b8dbb3c2ee1c83f6181731/de

[13] https://gist.githubusercontent.com/IISResetMe/d61a2263c617959eda2682e94f8df8b1/raw/ebc9e675c961c2c3f5b8dbb3c2ee1c83f6181731/ma detectors.txt

[14] https://gist.githubusercontent.com/IISResetMe/d61a2263c617959eda2682e94f8df8b1/raw/ebc9e675c961c2c3f5b8dbb3c2ee1c83f6181731/de drivers.txt

[15] https://www.fireeye.com/blog/threat-research/2020/12/sunburst-additional-technical-details.html

---

For additional information and discussions on this topic, Truesec has recently published the following video where we discuss nation-state actors in relation to the SolarWinds SUNBURST hack.

Truesec Tech Talk – SolarWinds SUNBURST breach and how nation-state actors operate

I was interviewed by Andy Syrewicze at Altaro on the SolarWinds SUNBURST attack and what IT service providers can and should do. You can watch the video interview below and you can also read Andy's post here.

Video Interview – Solarwinds Hack Fallout
