SUNBURST: SolarWinds' Supply-Chain Attack

By Intel 471

Published: 2026-04-01 · Archived: 2026-04-05 18:29:20 UTC

Threat Detection Packages

SUNBURST Known Malicious DNS Activity

- Splunk
- Elastic Lucene
- Elastic DSL

SUNBURST Suspicious Processes for SolarWinds Orion Software

- Splunk
- Elastic Lucene
- Elastic DSL

SUNBURST Named Pipe Indicator

- Splunk
- Elastic Lucene
- Elastic DSL

Introduction

Last week

FireEye

shared that

they

experienced

unauthorized access and theft of their

offensive security

tools

used

by their red team

, by a sophisticated state-sponsored adversary

.

Although the theft of these sophisticated tools will

have

an impact on future attacks carried out by the adversary, how they accessed the tools was

a much bigger problem. Over the weekend FireEye

shared more details of their compromise and broke the news

that

they fell victim to a supply-chain attack involving

the

IT services

company SolarWinds

. FireEye reported the SolarWinds Orion software update had a backdoor injected into its code

,

which SolarWinds believed to have been included in updates

released between March and June 2020

. It should be noted,

h

owever

,

that

some researchers

have

report

ed

seeing activity as early as late 2019

.

The backdoor was dubbed SUNBURST by FireEye.

[hubspot type=cta portal=7924572 id=ec572148-ebc2-449f-8ccc-0353bc94df5e]

This supply-chain attack still

has an

unknown impact

. According to SolarWinds' website their customer

s

include

many

U.S. Government agencies, as well as

a significant

percentage

of the Fortune 500.

According to

a recent filing

with the

US

Securities and Exchange Commission

(SEC)

it is

estimate

d that at least 18,000 installed the

malicious

update

.

Due to the nature of the attack, including the supply-chain compromise,

the

actor’s extreme attention to detail and operational security, as well as the high-profile targets who were successfully compromised as a result of the attack,

it is suspected that it was conducted by a nation-state sponsored group.

Volexity

researchers

have

attributed this

attack to a threat actor under the name of Dark Halo

, whom they have been tracking since late 2019

.

SUNBURST, the implant delivered via the backdoored SolarWinds Orion update,

was found in one of the DLL files contained in the update, specifically

“

SolarWinds

.Orion.Core.BusinessLayer.dll

”

.

According to

FireEye

, the backdoor has a dormant period of up to two weeks, and then will attempt to resolve a subdomain of

avsvmcloud

[

.

]com

, which

will return a

DNS

CNAME record

pointing

to a

c

ommand

and

c

ontrol

(C2)

domain. We go into detail on the functionality of SUNBURST

in our

Cyborg Labs Threat Hunt

Deep Dive

,

in which we review the SolarWinds supply-chain compromise, and examine the SUNBURST implant and how it behaves in an environment.

UPDATE: 17 December 2020

We are releasing 3 threat detection packages that will allow organizations to detect SUNBURST activity in their environment.

Threat Detection Packages

SUNBURST Known Malicious DNS Activity

Splunk

```
(query_type IN ("CNAME","A") AND (query="*avsvmcloud.com" OR answer="*avsvmcloud.com")) OR
(query_type="A" AND query IN ("deftsecurity.com","freescanonline.com", "thedoccloud.com", "websitetheme.com",
"highdatabase.com", "incomeupdate.com", "databasegalore.com", "panhardware.com", "zupertech.com",
"freescanonline.com", "deftsecurity.com", "thedoccloud.com"))
| stats values(_time) as occurrences count by src, query, query_type, answer
| convert ctime(occurrences)
```

Elastic Lucene

```
((dns.question.name:"/.*avsvmcloud\\.com/" or dns.answer.name:"/.*avsvmcloud\\.com/") and
(dns.question.type:"/[Cc][Nn][Aa][Mm][Ee]|[Aa]/" or dns.answer.type:"/[Cc][Nn][Aa][Mm][Ee]|[Aa]/")) or
(dns.question.name:("deftsecurity.com" or "freescanonline.com" or "thedoccloud.com" or "websitetheme.com" or
"highdatabase.com" or "incomeupdate.com" or "databasegalore.com" or "panhardware.com" or "zupertech.com" or
"freescanonline.com" or "deftsecurity.com" or "thedoccloud.com") and (dns.question.type:"/[Aa]/" or
dns.answer.type:"/[Aa]/"))((dns.question.name:"/.*avsvmcloud\\.com/" or dns.answer.name:"/.*avsvmcloud\\.com/")
and (dns.question.type:"/[Cc][Nn][Aa][Mm][Ee]|[Aa]/" or dns.answer.type:"/[Cc][Nn][Aa][Mm][Ee]|[Aa]/")) or
(dns.question.name:("deftsecurity.com" or "freescanonline.com" or "thedoccloud.com" or "websitetheme.com" or
"highdatabase.com" or "incomeupdate.com" or "databasegalore.com" or "panhardware.com" or "zupertech.com" or
"freescanonline.com" or "deftsecurity.com" or "thedoccloud.com") and (dns.question.type:"/[Aa]/" or
dns.answer.type:"/[Aa]/"))
```

Elastic DSL

```
{ "bool": { "should": [ { "bool": { "must": [ { "query_string": { "fields": [ "dns.question.type", "dns.answer.type" ],
"query": "/[Cc][Nn][Aa][Mm][Ee]|[Aa]/" } }, { "query_string": { "fields": [ "dns.question.name", "dns.answers.name"
], "query": "/.*avsvmcloud\\.com/" } } ] } }, { "bool": { "filter": [ { "terms": { "dns.question.name": [
"deftsecurity.com", "freescanonline.com", "thedoccloud.com", "websitetheme.com", "highdatabase.com",
"incomeupdate.com", "databasegalore.com", "panhardware.com", "zupertech.com", "freescanonline.com",
"deftsecurity.com", "thedoccloud.com" ] } } ], "must": [ { "query_string": { "fields": [ "dns.answer.type",
"dns.question.type" ], "query": "/[Aa]/" } } ] } } ] }
}
```

SUNBURST Suspicious Processes for SolarWinds Orion Software

Splunk

```
index=sysmon sourcetype="sysmon:xml" ParentImage = "SolarWinds.BusinessLayerHost.exe" AND NOT Image IN
("*\\SolarWinds\\Orion\\APM\\APMServiceControl.exe",
"*\\SolarWinds\\Orion\\ExportToPDFCmd.Exe","*\\SolarWinds.Credentials\\SolarWinds.Credentials.Orion.WebApi.exe",
"*\\SolarWinds\\Orion\\Topology\\SolarWinds.Orion.Topology.Calculator.exe", "*\\SolarWinds\\Orion\\Database-
Maint.exe", "*\\SolarWinds.Orion.ApiPoller.Service\\SolarWinds.Orion.ApiPoller.Service.exe",
"*\\Windows\\SysWOW64\\WerFault.exe")
| stats values(_time) as occurrences, values(Image) as ChildProcesses, values(CommandLine) as CommandLines
count by host, ParentImage
| convert ctime(occurrences)
```

Elastic Lucene

```
parent.process.executable:"/.*[Ss][Oo][Ll][Aa][Rr][Ww][Ii][Nn][Dd][Ss]\\.[Bb][Uu][Ss][Ii][Nn][Ee][Ss]+[Ll][Aa]
[Yy][Ee][Rr][Hh][Oo][Ss][Tt]\\.[Ee][Xx][Ee]/" and not
(process.executable:"/.*\\\\Windows\\\\SysWOW64\\\\WerFault\\.exe/" OR
process.executable:"/.*\\\\SolarWinds\\.Orion\\.ApiPoller\\.Service\\\\SolarWinds\\.Orion\\.ApiPoller\\.Service\\.exe/"
or process.executable:"/.*\\\\SolarWinds\\\\Orion\\\\Database-Maint\\.exe/" or
process.executable:"/.*\\\\SolarWinds\\\\Orion\\\\Topology\\\\SolarWinds\\.Orion\\.Topology\\.Calculator\\.exe/" or
process.executable:"/.*\\\\SolarWinds\\\\Orion\\\\ExportToPDFCmd\\.exe/" or
process.executable:"/.*\\\\SolarWinds\\\\Orion\\\\APM\\\\APMServiceControl\\.exe/" or
process.executable:"/.*\\\\SolarWinds.Credentials\\\\SolarWinds\\.Credentials\\.Orion\\.WebApi\\.exe/")
```

Elastic DSL

```
{ "bool": { "must": [ { "query_string": { "query": "/.*[Ss][Oo][Ll][Aa][Rr][Ww][Ii][Nn][Dd][Ss]\\.[Bb][Uu][Ss][Ii]
[Nn][Ee][Ss]+[Ll][Aa][Yy][Ee][Rr][Hh][Oo][Ss][Tt]\\.[Ee][Xx][Ee]/", "fields": [ "process.parent.executable" ] } } ],
"must_not": [ { "query_string": { "query": "/.*\\\\SolarWinds\\\\Orion\\\\APM\\\\APMServiceControl\\.exe/", "fields":
[ "process.executable" ] } }, { "query_string": { "query": "/.*\\\\SolarWinds\\\\Orion\\\\ExportToPDFCmd\\.exe/",
"fields": [ "process.executable" ] } }, { "query_string": { "query":
"/.*\\\\SolarWinds\\\\Orion\\\\Topology\\\\SolarWinds\\.Orion\\.Topology\\.Calculator\\.exe/", "fields": [
"process.executable" ] } }, { "query_string": { "query": "/.*\\\\SolarWinds\\\\Orion\\\\Database-Maint\\.exe/", "fields":
[ "process.executable" ] } }, { "query_string": { "query":
"/.*\\\\SolarWinds\\.Orion\\.ApiPoller\\.Service\\\\SolarWinds.Orion\\.ApiPoller\\.Service\\.exe/", "fields": [
"process.executable" ] } }, { "query_string": { "query": "/.*\\\\Windows\\\\SysWOW64\\\\WerFault\\.exe/", "fields": [
"process.executable" ] } }, { "query_string": { "query":
"/.*\\\\SolarWinds.Credentials\\\\SolarWinds\\.Credentials\\.Orion\\.WebApi\\.exe/", "fields": [ "process.executable" ]
} } ] }
}
```

SUNBURST Named Pipe Indicator

Splunk

```
index=sysmon sourcetype=sysmon:xml (EventID=17 OR EventID=18) PipeName="583da945-62af-10e8-4902-
a8f205c72b2e"
```

| stats values(_time) as occurrences, values(EventID) as eventID, values(PipeName) as pipeName count by host
| convert ctime(occurrences)

Elastic Lucene

event.code:("17" or "18") and file.name:"583da945-62af-10e8-4902-a8f205c72b2e"

Elastic DSL

{ "bool": { "must": [{ "query_string": { "query": "17", "fields": ["event.code"] } }, { "query_string": { "query": "18", "fields": ["event.code"] } }, { "query_string": { "query": "583da945-62af-10e8-4902-a8f205c72b2e", "fields": ["file.name"] } }] }
}

Cyborg Security's research and development team has built dozens of threat detection packages for the SUNBURST implant and additional malicious behaviours described by FireEye. These packages come tailored to your unique environment and can be immediately downloaded and deployed. You can find these detections, in addition to all known indicators of compromise (IOC), on the HUNTER platform.

[hubspot type=cta portal=7924572 id=ae832f8f-83db-4b26-8f4d-f37f258623e2]
