

Robust Indicators of Compromise for SUNBURST

 netresec.com/

January 11, 2021

Erik Hjelmvik

,

Monday, 11 January 2021 10:30:00 (UTC/GMT)



There has been a great deal of confusion regarding what network based Indicators of Compromise (IOC) SolarWinds Orion customers can use to self assess whether or not they have been targeted after having installed a software update with the SUNBURST backdoor. Many of the published IOCs only indicate that a backdoored SolarWinds Orion update has been installed, but the question that many security teams are trying to answer is whether or not the installed backdoor has been used by the threat actor.

Dont trust everything you read!

There is a widespread misunderstanding that receiving a so-called “NetBios” DNS A record (for example an address in 8.18.144.0/23) in response to a *.avsvmcloud.com DNS query would mean that you’ve been targeted. Our analysis of the decompiled SUNBURST code and passive DNS data show that that receiving a “NetBios” response does not necessarily mean that the client has been targeted. Unfortunately this misunderstanding has lead to various sensationalist stories being published with long lists of companies and organizations that are claimed to be “singled out by the hacking group for the second stage of the attack”, “explicitly selected by the SolarWinds hackers for further activities” or “breached via SolarWinds and then specifically targeted by the hackers for additional internal compromise”.

Another common misunderstanding is that clients sending *.avsvmcloud.com DNS queries with encoded timestamps, and optionally a list of installed/running AV products, have been actively targeted. Our analysis of the decompiled SUNBURST code show that the timestamped “Pings” or AV service status reports get exfiltrated in DNS traffic after the client’s internal AD domain has been sent, but before the perpetrators decide whether or not they want to activate the backdoor.

Indicators of a Targeted Attack

So what network based IOC’s can incident responders, blue teams and SOC analysts use in order to see if they have been targeted by the SUNBURST operators?

The following network based events indicate that a client has been actively targeted and the SUNBURST backdoor has progressed beyond the initial mode of operation:

- Received a DNS A record for an *.avsvmcloud.com query, that points to an IP address in any of the following three networks: 18.130.0.0/16, 99.79.0.0/16 or 184.72.0.0/15
- Sent an *.avsvmcloud.com DNS query with the STAGE2 flag encoded in the subdomain.
- Received a CNAME record for a query to *.avsvmcloud.com

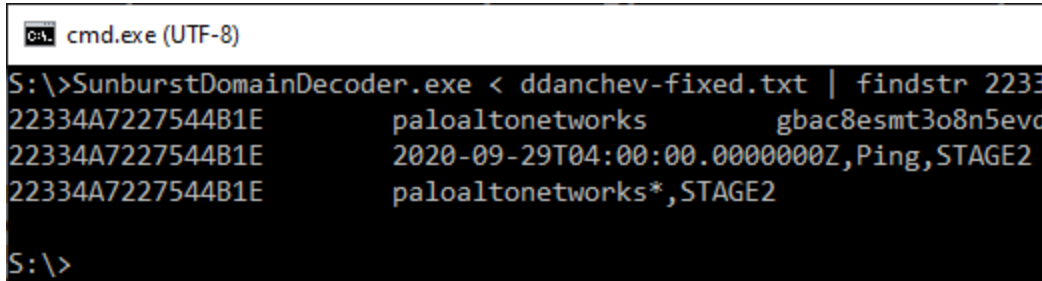
These three indicators are DNS based, so organizations will need to have a full historical backlog of DNS transactions ranging back to April 2020 in order to use them reliably. Another network based IOC is HTTPS communication to one of the known STAGE3 C2 domains. However, please note that the C2 domain list might not be complete. It is even possible that a unique C2 domain is used for each victim. Nevertheless, here’s a list of the SUNBURST STAGE3 C2 domains we are currently aware of:

- avsvmcloud[.]com
- databasegalore[.]com
- deftsecurity[.]com
- digitalcollege[.]org
- freescanonline[.]com
- globalnetworkissues[.]com
- highdatabase[.]com
- incomeupdate[.]com
- kubecoloud[.]com
- lcomputers[.]com
- mobilnweb[.]com
- panhardware[.]com
- seobundlekit[.]com
- solartrackingsystem[.]net
- thedoccloud[.]com
- virtualwebdata[.]com

- [webcodez\[.\]com](#)
- [websitesheme\[.\]com](#)
- [zupertech\[.\]com](#)

Palo Alto was a Targeted SUNBURST Victim

We can now verify that Palo Alto was among the targeted SUNBURST victims, because their DNS request for "5qbtj04rcbp3tiq8bo6t.appsync.api.us.east.1.avsvmcloud.com" contains an encoded STAGE2 flag. The attack took place on September 29 at around 04:00 UTC, according to the timestamp that was also encoded into the avsvmcloud subdomain.



```
cmd.exe (UTF-8)
S:\>SunburstDomainDecoder.exe < ddanchev-fixed.txt | findstr 2233
22334A7227544B1E      paloaltonetworks      gbac8esmt3o8n5evd
22334A7227544B1E      2020-09-29T04:00:00.0000000Z,Ping,STAGE2
22334A7227544B1E      paloaltonetworks*,STAGE2
S:\>
```

Image: Parsing passive DNS data from Dancho Danchev with SunburstDomainDecoder v1.9 and filtering on GUID "22334A7227544B1E".

Palo Alto's CEO Nimesh Arora has confirmed that they were hit by SUNBURST (or "SolarStorm" as they call it), but they don't provide much details. Here's what Nimesh wrote on December 17:

Recently, we experienced an attempt to download Cobalt Strike on one of our IT SolarWinds servers. [...]

We thought this was an isolated incident, however, on Dec. 13, we became aware that the SolarWinds software supply chain was compromised and it became clear that the incident we prevented was an attempted SolarStorm attack.

Our SUNBURST STAGE2 Victim Table has now been updated to include Palo Alto along side the other targeted victims.

Posted by Erik Hjelmvik on Monday, 11 January 2021 10:30:00 (UTC/GMT)

Tags: [#SUNBURST](#) [#SolarWinds](#) [#SolarStorm](#) [#avsvmcloud](#) [#STAGE2](#) [#DNS](#) [#CNAME](#) [#avsvmcloud.com](#) [#Cobalt Strike](#) [#DNS](#) [#FireEye](#)

Recent Posts

» [Real-time PCAP-over-IP in Wireshark](#)

» [Emotet C2 and Spam Traffic Video](#)

- » [Industroyer2 IEC-104 Analysis](#)
- » [NetworkMiner 2.7.3 Released](#)
- » [PolarProxy in Windows Sandbox](#)
- » [PolarProxy 0.9 Released](#)

Blog Archive

- » [2022 Blog Posts](#)
- » [2021 Blog Posts](#)
- » [2020 Blog Posts](#)
- » [2019 Blog Posts](#)
- » [2018 Blog Posts](#)
- » [2017 Blog Posts](#)
- » [2016 Blog Posts](#)
- » [2015 Blog Posts](#)
- » [2014 Blog Posts](#)
- » [2013 Blog Posts](#)
- » [2012 Blog Posts](#)
- » [2011 Blog Posts](#)

[List all blog.posts](#)



NETRESEC on Twitter

Follow [@netresec](#) on twitter:

- » twitter.com/netresec