

Twenty-three SUNBURST Targets Identified

Erik Hjelmvik

Monday, 25 January 2021 08:25:00 (UTC/GMT)

Remember when Igor Kuznetsov and Costin Raiu announced that two of the victims in [FireEye's SUNBURST IOC list](#) were *****net.***.com** and **central.***.gov** on Kaspersky's [Securelist blog in December](#)? Reuters later [reported](#) that these victims were Cox Communications and Pima County.

We can now reveal that the internal AD domain of **all** SUNBURST deployments in FireEye's IOC list can be extracted from publicly available DNS logs [published by twitter user VriesHd](#), a.k.a. "Kira 2.0", with help of our [SunburstDomainDecoder](#) tool. The data published by VriesHd is the most complete SUNBURST DNS collection we've seen, with over 35.000 avsvmcloud.com subdomains! Here is FireEye's IOC table completed with our findings:

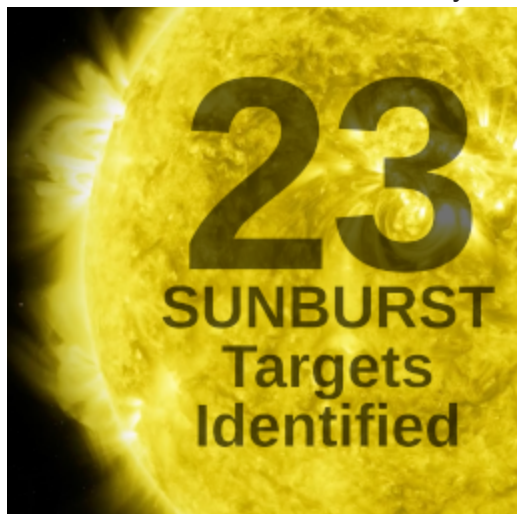
Leaked AD Domain	Sunburst C2 FQDN	Stage 2 CNAME	Timestamp (UTC)
central.pima.gov	6a57jk2ba1d9keg15cbg.appsync-api.eu-west-1.avsvmcloud.com	freescanonline[.]com	2020-06-13 09:00
central.pima.gov	7sbvaemscs0mc925tb99.appsync-api.us-west-2.avsvmcloud.com	deftsecurity[.]com	2020-06-11 22:30
central.pima.gov	gq1h856599gqh538acqn.appsync-api.us-west-2.avsvmcloud.com	thedoccloud[.]com	2020-06-13 08:30
coxnet.cox.com	ihvpgv9psvq02ffo77et.appsync-api.us-east-2.avsvmcloud.com	freescanonline[.]com	2020-06-20 02:30
corp.qualys.com	k5kcubuassl3alrf7gm3.appsync-api.eu-west-1.avsvmcloud.com	thedoccloud[.]com	2020-07-22 17:00
corp.qualys.com	mhdosoksaccf9sni9icp.appsync-api.eu-west-1.avsvmcloud.com	thedoccloud[.]com	2020-07-23 18:30

Victims Targeted with SUNBURST Stage 2 Backdoor

It was not just the victims listed in FireEye's IOC that were specifically targeted by the SUNBURST operators. As explained in our [Finding Targeted SUNBURST Victims with pDNS](#) blog post, the "STAGE2" flag in SUNBURST's DNS beacons can be used to reveal additional organizations that were singled out as interesting targets by the threat actors.

We'd like to stress that the majority of all companies and organizations that have installed a backdoored SolarWinds Orion update were never targeted by the threat actors. This means the these SUNBURST backdoors never made it past what we call "Stage 1 operation", where the backdoor encodes the internal AD domain name and [installed security products](#) into DNS requests. SUNBURST backdoors in Stage 1 operation cannot accept any commands from the C2 server without first progressing into Stage 2 operation. We estimate that about 99.5% of the installed SUNBURST backdoors never progressed into [Stage 2 operation](#).

Here is the full list of internal AD domain names from the SUNBURST deployments in VriesHd's DNS data that actually did enter Stage 2 operation according to our analysis:



- central.pima.gov ([confirmed](#))
- cisco.com ([confirmed](#))
- corp.qualys.com ([confirmed](#))
- coxnet.cox.com ([confirmed](#))
- ddsn.gov
- fc.gov
- fox.local
- ggsg-us.cisco.com ([confirmed](#))
- HQ.FIDELIS ([confirmed](#))
- jpsa.gov
- lagnr.chevrontexaco.net
- logitech.local
- los.local
- mgt.srb.europa* ([confirmed](#))
- ng.ds.army.mil

- nsanet.local (not the NSA)
- paloaltonetworks* (confirmed)
- phpds.org
- scc.state.va.us (confirmed)
- suk.sas.com
- vgn.viasatgsd.com
- wctc.msft
- WincoreWindows.local

Our SUNBURST STAGE2 Victim Table has now been updated with additional details about the STAGE2 signaling from these SUNBURST implants, including timestamps, avsvmcloud.com subdomains and GUID values.

Initial Microsoft Targeting FAIL

The last two entries in the AD domain list above are interesting, since they both hint that the targeted entity might be Microsoft.


The data that gets exfiltrated in DNS beacons during SUNBURST's initial stage is the internal domain the SolarWinds Orion PC is connected to and a list of installed security products on that PC. These domain names, security products and possibly also the victims' public IP addresses, was the data available to the attackers when they decided which ones they wanted to proceed to Stage 2 with and thereby activate the HTTPS backdoor built into SUNBURST.

The threat actors were probably surprised when they realized that "WincoreWindows.local" was in fact a company in West Virginia that manufactures high quality windows and doors.



The threat actors later found another backdoored SolarWinds Orion machine connected to a domain called "wctc.msft", which also sounds like it could be Microsoft. Below is a table outlining relevant events for these two SUNBURST deployments that can be extracted from VriesHd's [SB2 spreadsheet](#) with [SunburstDomainDecoder](#).

Target ID	Beaconed Data	Date
A887B592B7E5B550	AD domain part 1: "WincoreW"	
A887B592B7E5B550	AD domain part 2: "indows.local"	
A887B592B7E5B550	AV Products: [none]	2020-05-22
<p>🙄 <i>Threat actor decision: Target victim</i> A887B592B7E5B550</p>		
A887B592B7E5B550	STAGE2 request for new C2 server in CNAME	2020-05-26
<p>🙄 <i>Threat actor decision: These aren't the droids we're looking for</i></p>		
59956D687A42F160	AD domain: "wctc.msft"	

59956D687A42F160	AV Products: [none]	2020-06-20
59956D687A42F160	Ping	2020-06-21
59956D687A42F160	Ping	2020-06-22
 <i>Threat actor decision: Target victim 59956D687A42F160</i>		
59956D687A42F160	STAGE2 request for new C2 server in CNAME	2020-06-23

Microsoft have been public about being hit by SUNBURST (or "Solorigate" as they call it), so we can assume that the threat actors eventually located a backdoored SolarWinds Orion installation in their networks.

Victim Notification

We spent the previous week reaching out to targeted companies and organizations, either directly or through CERT organizations. From what we understand many of these organizations were already aware that they had been targeted victims of SUNBURST, even though they might not have gone public about the breach.

The Ethical Dilemma

We have no intentions to shame the organizations that have installed a backdoored SolarWinds Orion update, regardless if they were targeted by the threat actor or not. In fact, the supply chain security problem is an extremely difficult one to tackle, even for companies and organizations with very high security standards. This could have happened to anyone!

However, since multiple passive DNS logs and SUNBURST victim lists have been circulating through publicly available channels for over a month, we felt that it was now acceptable to publicly write about the analysis we've been doing based on all this data. We'd also like to thank everyone who has helped collect and share passive DNS data, including John Bambenek, Joe Slowik, Rohit Bansal, Dancho Danchev, Paul Vixie and VriesHd. This open data has been crucial in order to develop and verify our SunburstDomainDecoder tool, which has been leveraged by numerous incident response teams to perform forensic analysis of DNS traffic from their SolarWinds Orion deployments.

More Credits

We'd like to thank CERT-SE and all other computer emergency response organizations that have helped us with the task of notifying organizations that were identified as targeted. We would also like to applaud companies and organizations like FireEye, Palo Alto Networks,

[Fidelis Cybersecurity](#), [Microsoft](#), the [U.S. Department of Energy](#) and the [U.S. Federal Courts](#) for being transparent and publicly announcing that the SUNBURST backdoor had been used in an attempt to compromise their networks.

Posted by Erik Hjelmvik on Monday, 25 January 2021 08:25:00 (UTC/GMT)

Tags: [#SUNBURST](#) [#FireEye](#) [#Solorigate](#) [#Microsoft](#) [#SolarWinds](#) [#FireEye](#) [#CNAME](#) [#STAGE2](#) [#DNS](#) [#Passive DNS](#) [#avsvmcloud.com](#) [#pDNS](#) [#Microsoft](#)

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