

Experts in network security monitoring and network forensics



[NETRESEC](#) | [Products](#) | [Training](#) | [Resources](#) | [Blog](#) | [About Netresec](#)

[NETRESEC](#) » [Blog](#)

Erik Hjelmvik,
Monday, 04 January 2021 21:11:00 (UTC/GMT)

Finding Targeted SUNBURST Victims with pDNS

Our [SunburstDomainDecoder](#) tool can now be used to identify SUNBURST victims that have been explicitly targeted by the attackers. The only input needed is passive DNS (pDNS) data for avsvmcloud.com subdomains.

Companies and organizations that have installed trojanized a SolarWinds Orion update containing the SUBURST backdoor will send DNS queries for seemingly random subdomains of avsvmcloud.com. Some of these DNS queries actually contain the victim's internal AD domain encoded into the subdomain, as explained in our blog post [Reassembling Victim Domain Fragments from SUNBURST DNS](#).

Three Stages of SUNBURST Backdoor Operation

Most SUNBURST victims were luckily not targeted by the attackers. This means that the backdoor never made it past "STAGE1" of the infection process. Nevertheless, the attackers did choose to proceed to "STAGE2" with some victims. As explained in FireEye's blog post [SUNBURST Additional Technical Details](#), the "C2 coordinator" can proceed to the next stage by responding with a DNS A record pointing to an IP address within any of these three ranges:

Recent Posts

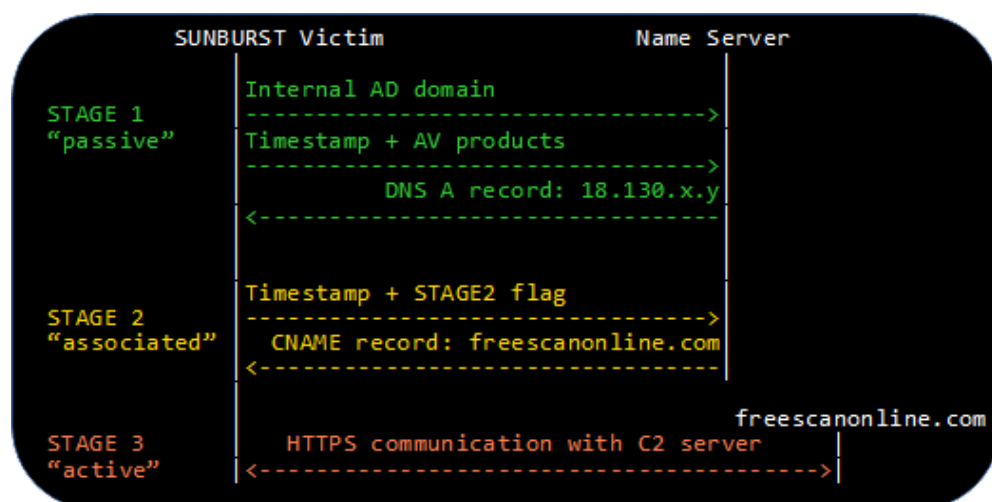
- » [VoIP tab in NetworkMiner Professional](#)
- » [Browsers tab in NetworkMiner Professional](#)
- » [Files tab in NetworkMiner Professional](#)
- » [Hosts tab in NetworkMiner Professional](#)
- » [Opening capture files with NetworkMiner Professional](#)
- » [Video Tutorial: Installing NetworkMiner Professional](#)
- » [CapLoader 1.9.7 Released](#)
- » [How to Inspect TLS Encrypted Traffic](#)

- 18.130.0.0/16
- 99.79.0.0/16
- 184.72.0.0/15

According to FireEye's "Diagram of actor operations and usage of SUNBURST", the decision to proceed to the next stage is based upon whether or not the victim's internal AD domain is "interesting to attack".

Note: "STAGE2" is referred to as "associated mode" in FireEye's blog post.

SUNBURST backdoors that have entered STAGE2 will allow CNAME records in DNS responses to be used as new C2 domains.



We have discovered that the SUNBURST backdoor actually uses a single bit in the queried avsvmcloud.com subdomain in order to flag that it has entered STAGE2 and is accepting new C2 domains in CNAME records. This bit is called [flag](#), [ext](#) or [dnssec](#) in the malicious SUNBURST implant and can be extracted from DNS queries that have an encoded timestamp, such as those indicating [which security products that are installed](#).

Detecting STAGE2 DNS Requests

Our [SunburstDomainDecoder](#) tool has now been updated to include a "STAGE2" tag in the output for DNS queries containing this stage 2 flag. This means that organizations like national CERTs, who perform incident response coordination and victim notification, can now use

Blog Archive

- » [2024 Blog Posts](#)
- » [2023 Blog Posts](#)
- » [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](#)

[Video blog posts](#)

News Feeds

- » [Google News](#)
- » [FeedBurner](#)
- » [RSS Feed](#)

SunburstDomainDecoder in order to identify and notify **targeted** SUNBURST victims that have entered STAGE2.

Here's the output we get when feeding SunburstDomainDecoder with Bambenek's [uniq-hostnames.txt](#) passive DNS data and only displaying lines containing "STAGE2":

```
SunburstDomainDecoder.exe < uniq-hostnames.txt | findstr STAGE2
22334A7227544B1E 2020-09-29T04:00:00.000000Z,STAG
E2 5qbtj04rcbp3tiq8bo6t
FC07EB59E028D3EE 2020-06-13T09:00:00.000000Z,STAG
E2 6a57jk2ba1d9keg15cbg
1D71011E992C3D68 2020-06-11T22:30:00.000000Z,STAG
E2 7sbvaemscs0mc925tb99
F90BDDDB47E495629 2020-06-13T08:30:00.000000Z,STAG
E2 gq1h856599gqh538acqn
DB7DE5B93573A3F7 2020-06-20T02:30:00.000000Z,STAG
E2 ihvpgv9psvq02ffo77et
3C327147876E6EA4 2020-07-22T17:00:00.000000Z,STAG
E2 k5kcubuassl3alrf7gm3
3C327147876E6EA4 2020-07-23T18:30:00.000000Z,STAG
E2 mhdosoksaccf9sni9icp
1D71011E992C3D68 central.pima.gov,STAGE2
DB7DE5B93573A3F7 coxnet.cox.com,STAGE2,WindowsDefe
nder
F90BDDDB47E495629 central.pima.gov,STAGE2
```

Most of these subdomains are listed in FireEye's [Indicator_Release_NBIs.csv](#) file as having CNAME pointers to other SUNBURST C2 domains like: freescanonline[.]com, deftsecurity[.]com and thedoccloud[.]com. But the first domain, with GUID 22334A7227544B1E, was actually not part of FireEye's IOC data.

Even more STAGE2 domains and GUID values can be found by analyzing other passive DNS resources, such as [this passive DNS dump on pastebin](#) by [Rohit Bansal](#).

```
curl -s https://pastebin.com/raw/6EDgCKxd | Sunbur
stDomainDecoder.exe | findstr STAGE2
E258332529826721 2020-07-18T05:00:00.000000Z,STAG
E2 1dbecfd99ku6fi2e5fjb
```



NETRESEC on X /
Twitter: [@netresec](#)



NETRESEC on
Mastodon: [@netresec@infosec.exchange](#)

```
2039AFE13E5307A1 2020-05-30T14:30:00.000000Z,STAG
E2 4n4vte5gmor7j9lpegsf
22334A7227544B1E 2020-09-29T04:00:00.000000Z,STAG
E2 5qbtj04rcbp3tiq8bo6t
FC07EB59E028D3EE 2020-06-13T09:00:00.000000Z,STAG
E2 6a57jk2ba1d9keg15cbg
1D71011E992C3D68 2020-06-11T22:30:00.000000Z,STAG
E2 7sbvaemscs0mc925tb99
1D71011E992C3D68 2020-06-11T22:30:00.000000Z,STAG
E2 7sbvaemscs0mc925tb99
F90BDDDB47E495629 2020-06-13T08:30:00.000000Z,STAG
E2 gq1h856599gqh538acqn
F90BDDDB47E495629 2020-06-13T08:30:00.000000Z,STAG
E2 gq1h856599gqh538acqn
DB7DE5B93573A3F7 2020-06-20T02:30:00.000000Z,STAG
E2 ihvpgv9psvq02ffo77et
DB7DE5B93573A3F7 2020-06-20T02:30:00.000000Z,STAG
E2 ihvpgv9psvq02ffo77et
3C327147876E6EA4 2020-07-23T18:30:00.000000Z,STAG
E2 mhdosoksaccf9sni9icp
```

After removing the domains already present in [FireEye's IOC](#) we're left with the following FQDN's that have been requested by SUNBURST backdoors in STAGE2:

- 1dbecfd99ku6fi2e5fjb.appsync-api.us-east-1.avsvmcloud.com
- 4n4vte5gmor7j9lpegsf.appsync-api.eu-west-1.avsvmcloud.com
- 5qbtj04rcbp3tiq8bo6t.appsync-api.us-east-1.avsvmcloud.com

Update January 7, 2021

Paul Vixie kindly [shared his SunburstDomainDecoder output](#) on Twitter yesterday. Paul's results show that the victim with GUID FC07EB59E028D3EE, which corresponds to the "6a57jk2ba1d9keg15cbg.appsync-api.eu-west-1.avsvmcloud[.]com" CNAME entry in [FireEye's IOC](#), was Pima County. This means that 3C327147876E6EA4 is the only GUID among the CNAME records published by FireEye that cannot yet be tied to a victim organization. Paul's data also reveals two new STAGE2 victim GUIDs (65A28A36F24D379D and 8D2267C5A00796DA).

Update January 12, 2021

With help of SunburstDomainDecoder 1.9 and [passive DNS data from Dancho Danchev](#) we've been able to verify that Palo Alto have installed the maliocous SUNBURST backdoor and that it entered into STAGE2 opreration on September 29, 2020. Palo Alto's CEO Nikesh Arora [has confirmed](#) that they were hit by SUNBURST (or "SolarStorm" as they call it).

Update January 25, 2021

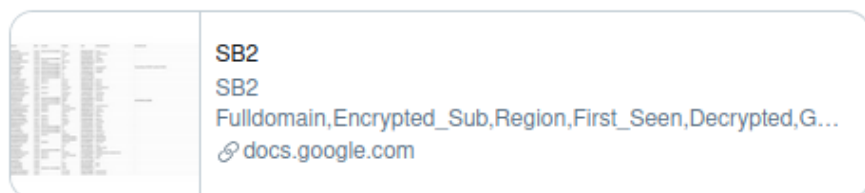
On December 17 [VriesHd tweeted a link to a Google Docs spreatsheet](#) containing aggregated SUNBURST DNS request data.



Kira 2.0
@VriesHd

...

Might be helpfull with the SolarWinds/SUNBURST data to combine one another, so here's all the data (subdomain, region, first seen date, decrypted DGA) that I'm personally aware of in a Google sheet atm. Feel free to comment with new or updated information



9:49 PM · Dec 17, 2020 · Twitter Web App

One month later VriesHd made some [substatial additions](#) to the ["SB2" spreadsheet](#), which by then contained several new STAGE2 victims. We have since then actively been trying to [reach out to the targeted organizations](#), either directly or through CERT organizations, who perform incident response coordination and help with the victim notification process. VriesHd's passive DNS collection has now been incorporated into the SUNBURST STAGE2 Victim Table below.

Targeted SUNBURST Victims

Here's a summary of the STAGE2 beacons from SUNBURST victims that can be extracted from publicly available data:

| GUID | avsvmcloud.com Subdomain | Timestamp (UTC) | AD Domain |
|------------------|---------------------------|---------------------|-----------------------------|
| FF1E34A864BCE106 | dh1usc8287hr46bi a74a | 2020-05-14 14:30 | nsanet.local |
| E5E2AD2B6DE697D6 | 70fov85qclvubqhf9 vlh | 2020-05-16 19:30 | cisco.com |
| FF1E34A864BCE106 | 2die0g7i5kgkki628 gaj | 2020-05-18 11:30 | nsanet.local |
| 3E8DF7FF13FC8D38 | 7hpaqi751fqoei2fd v8m | 2020-05-18 16:30 | HQ.FIDELIS |
| FF1E34A864BCE106 | tsem12v1rn620hatf ol2 | 2020-05-20 14:30 | nsanet.local |
| FF1E34A864BCE106 | a0hmuovel2400sf vf6n | 2020-05-20 16:30 | nsanet.local |
| 0C1A5A27B297FE46 | k0biaol9fc84ummf n7vi | 2020-05-26 11:30 | vgn.viasatg sd.com |
| A887B592B7E5B550 | m4apr0vu9qnomtu n3b9t | 2020-05-26 20:00 | WincoreWin dows.local |
| 2039AFE13E5307A1 | 4n4vte5gmor7j9lp egsf | 2020-05-30 14:30 | suk.sas.com |
| 06A4EA63C80EE24A | 9q5jifedn8aflr4ge3 nu | 2020-05-31 12:00 | scc.state.va. us |
| 9850F550BD1010F2 | gth7uravpvaapoi8 6834 | 2020-05-31 20:00 | lagnr.chevr ontexaco.net |
| E5E2AD2B6DE697D6 | 8k56mm0b876uvf 5e7rd3 | 2020-06-01 19:00 | cisco.com |
| 2039AFE13E5307A1 | laog1ushfp80e3f18 cjg | 2020-06-03 01:30 | suk.sas.com |
| 06A4EA63C80EE24A | ntlcvjppqc57t9kb8ac 75 | 2020-06-03 23:30 | scc.state.va. us |

| | | | |
|--------------------------|--------------------------|---------------------|----------------------|
| 1D71011E 992C3D68 | 7sbvaemscs0mc92 5tb99 | 2020-06-11 22:30 | central.pim a.gov |
| F90BDDDB4 7E495629 | gq1h856599gqh53 8acqn | 2020-06-13 08:30 | central.pim a.gov |
| FC07EB59 E028D3EE | 6a57jk2ba1d9keg1 5cbg | 2020-06-13 09:00 | central.pim a.gov |
| 58314193 3D242B0D | f25k66k5hu68fneu 7ocd | 2020-06-16 06:00 | logitech.loc al |
| 52CE2BAF D69B2D0E | f2co92njkm9od5eu 7btg | 2020-06-16 18:30 | fc.gov |
| FACC72E2 207CD69F | rkspr9a19fl8r5ipgg i1 | 2020-06-17 01:00 | fox.local |
| 3256C1BC AF74B5FC | p0a7jjdp4eq9o2vo k1mt | 2020-06-18 07:00 | ng.ds.army. mil |
| 92DC5436 D54898C D | lusq9mg6j1e3jii5f6 6o | 2020-06-18 17:30 | ddsn.gov |
| DB7DE5B9 3573A3F7 | ihvpgv9psvq02ffo7 7et | 2020-06-20 02:30 | coxnet.cox.c om |
| 59956D68 7A42F160 | o49qi0qbfm37o6ju l639 | 2020-06-23 06:00 | wctc.msft |
| 123EDA14 721C3602 | p5iokg3v9tntqcbo7 7p2 | 2020-06-29 08:30 | scc.state.va. us |
| 123EDA14 721C3602 | 84v0j8kkbvqf8ntt4 o9f | 2020-06-30 10:30 | scc.state.va. us |
| 2F52CFFC D8993B63 | 0tvuasje2vc2i2413 m6i | 2020-07-01 16:30 | mgt.srb.eur opa* |
| 65A28A36 F24D379D | 7u32o0m6ureci8h5 eo6k | 2020-07-02 01:00 | |
| 2F52CFFC D8993B63 | en1clufg22h2uca2 7ro3 | 2020-07-03 06:00 | mgt.srb.eur opa* |
| 2F52CFFC D8993B63 | s2r15kp335mnlq65 i6ce | 2020-07-03 09:00 | mgt.srb.eur opa* |

| | | | |
|--------------------------|--------------------------|---------------------|-----------------------|
| DB4013D DA16F6A 40 | up1vj67jjj9tpvceu7 ak | 2020-07-08 01:00 | los.local |
| 123EDA14 721C3602 | l0vos8o9m5p3m8o f7g96 | 2020-07-10 22:00 | scc.state.va. us |
| E5E2AD2B 6DE697D6 | 8kr7r16da442u75e gv1s | 2020-07-15 14:00 | cisco.com |
| A13731B1 7632C726 | ttj6cro8jm6cfma8n oo7 | 2020-07-17 12:30 | phpds.org |
| E5E2AD2B 6DE697D6 | gh1so69rl1sgrgf38 gr5 | 2020-07-17 15:00 | cisco.com |
| E2583325 29826721 | 1dbecfd99ku6fi2e5 fjb | 2020-07-18 05:00 | |
| 123EDA14 721C3602 | epm95unblvj984s2 ovqh | 2020-07-22 11:00 | scc.state.va. us |
| 3C327147 876E6EA4 | k5kcubuassl3alrf7g m3 | 2020-07-22 17:00 | corp.qualy s.com |
| 3C327147 876E6EA4 | mhdosoksaccf9sni9 icp | 2020-07-23 18:30 | corp.qualy s.com |
| F2C9AC93 206ABF47 | onpqb88oq440lq8 2p7lb | 2020-07-24 05:00 | jpso.gov |
| 123EDA14 721C3602 | 0qthjq50jbdvnjq16 o8f | 2020-07-27 17:00 | scc.state.va. us |
| 123EDA14 721C3602 | gu6r7k260p6afq3ti cso | 2020-07-28 17:30 | scc.state.va. us |
| 936F78AB 73AA3022 | i4d2krbn2f92jo3uj 8r9 | 2020-08-04 05:00 | ggsg-us.cisc o.com |
| 936F78AB 73AA3022 | et2gu9tg5ckrsvaj5 bom | 2020-08-05 06:00 | ggsg-us.cisc o.com |
| 22334A72 27544B1E | 5qbtj04rcbp3tiq8b o6t | 2020-09-29 04:00 | paloaltonet works* |

SUNBURST STAGE2 Victim Table

Sources: [John Bambenek](#), [Joe Słowik](#), [Rohit Bansal](#), [Dancho](#)

[*Danchev*](#), [*Paul Vixie*](#), [*FireEye*](#) and [*VriesHd*](#).

Identifying More SUNBURST STAGE2 Victims

Companies and organizations with access to more passive DNS resources will hopefully be able to use SunburstDomainDecoder to identify additional targeted SUNBURST victims that have progressed to STAGE2.

Download SunburstDomainDecoder

Our tool SunburstDomainDecoder is released under a Creative Commons [CC-BY](#) license, and can be downloaded here:

<https://www.netresec.com/files/SunburstDomainDecoder.zip>

You can also read more about SunburstDomainDecoder in our blog post [Reassembling Victim Domain Fragments from SUNBURST DNS](#).

Posted by Erik Hjelmvik on Monday, 04 January 2021
21:11:00 (UTC/GMT)

Tags: [#Netresec](#) [#pDNS](#) [#SUNBURST](#) [#SolarWinds](#)
[#Solorigate](#) [#SunburstDomainDecoder](#) [#SolarStorm](#)
[#STAGE2](#) [#avsvmcloud](#) [#C2](#)

Short URL: <https://netresec.com/?b=2113a6a>

[NETRESEC](#) | [Contact Us](#) | [Privacy](#) | [X](#) | [Mastodon](#) | [RSS](#) | [News Feed](#)