Targeting Process for the SolarWinds Backdoor

netresec.com/

February 17, 2021

Erik Hjelmvik

,

Wednesday, 17 February 2021 20:22:00 (UTC/GMT)

The SolarWinds Orion backdoor, known as SUNBURST or Solorigate, has been analyzed by numerous experts from Microsoft, FireEye and several anti-virus vendors. However, we have noticed that many of the published reports are either lacking or incorrect in how they describe the steps involved when a client gets targeted by the threat actors. We have therefore decided to publish this writeup, which is based on the analysis we did of the SolarWinds backdoor when creating our SunburstDomainDecoder tool.

UPDATE March 1, 2021

Fixed errors in the Stage 2 beacon structure and added a CyberChef recipe link.

avsvmcloud.com DNS queries are not DGA related

The DNS communication between the backdoored SolarWinds Orion clients and the authoritative name server for avsvmcloud.com is not caused by a Domain Generation Algorithm (DGA), it's actually a fully functional two-way communication C2 channel. The clients encode information, such as the internal AD domain and installed security applications into the DNS queries and the DNS responses from the name server are used to instruct the clients to continue beaconing, stop beaconing or to target a client by proceeding to what we call Stage 2 operation. Thus, the authoritative name server for avsvmcloud.com was actually the C2 server for Stage 1 and 2 operation of the SolarWinds backdoor.

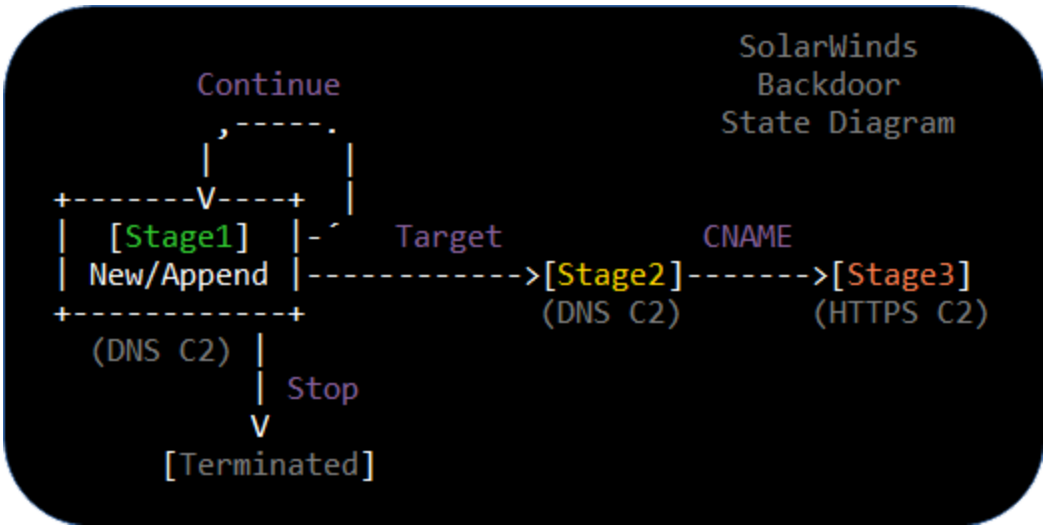

Image: SolarWinds Backdoor State Diagram

Command: Continue Beaconing

The default response from the name server is the "Continue Beaconing" command, which indicates that the threat actors have not yet decided if the SolarWinds client is of interest for further activity. Receiving a DNS A record in any of the following net ranges instructs the SolarWinds backdoor to continue beaconing:

- 8.18.144.0/23
- 71.152.53.0/24
- 87.238.80.0/21
- 199.201.117.0/24

In "Stage 1" operation the SUNBURST client starts out in the "New" mode where it exfiltrates the internal AD domain name. The AD domain data is often split into multiple DNS queries to reduce the length of each DNS query. The client later proceeds to the "Append" mode when the full AD domain has been exfiltrated. In "Append" mode the client transmits a list of installed or running security applications to the DNS C2 server, as we have described in our Extracting Security Products from SUNBURST DNS Beacons blog post. The client remains in Append mode until it gets either terminated or targeted.

Note: It is also possible to reset a client back to the "New" mode with a so-called "Ipx" command, but that is out of scope for this blog post.

Command: Stop Beaconing

The stop beaconing command terminates the DNS beaconing, so that the client no longer retrieves any commands from the C2 server. The C2 communication is stopped after receiving a DNS DNS A or AAAA record in any of the following ranges:

- 20.140.0.0/15
- 96.31.172.0/24

- 131.228.12.0/22
- 144.86.226.0/24
- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16
- 224.0.0.0/3
- fc00:: - fe00::
- fec0:: - ffc0::
- ff00::

Command: Target Client

A SUNBURST client that has been "targeted" will change a flag called rec.dnssec in the source code from false to true. We call this flag the "Stage 2" flag, which must be set in order for the client to accept a CNAME record and proceed to Stage 3. Symantec refer to the Stage 2 flag as "a bit flag representing whether the previous DNS response successfully contained partial or full instructions to start the secondary HTTP communication channel".

A DNS A record in any of the following three IP ranges can be used to set the "Stage 2" flag:

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

The state of the Stage 2 flag is actually signaled in the avsvmcloud.com DNS queries, which is how we managed to identify the AD domains of 23 targeted organizations just by analyzing SUNBURST DNS queries.

Stage 2 DNS Request Structure

The structure of the SUNBURST DNS queries in Stage 1 is pretty well described by Prevasio and Symantec, so we will not cover those in this blog post. Instead we will focus specifically on the structure of the DNS queries transmitted in Stage 2 operation, where the clients request a CNAME record from the name server.

As we have explained previously the exfiltrated data gets base32 encoded, using the custom alphabet "ph2eifo3n5utg1j8d94qrvbmk0sal76c", in order to ensure that only valid domain name characters are used in the DNS beacons.

The structure of the Stage 2 request, before it gets base32 encoded and appended as an avsvmcloud.com subdomain, looks like this:

Field	Size	Description

XOR Key	8 bits	A value between 0x01 and 0x7F used to XOR encrypt the rest of the data.
GUID	64 bits	Client ID encrypted using 16 bit rotating XOR with the last 15 bits of *Timestamp* and the *Stage 2 flag*.
Packet Type	4 bits	A value of 0x1, could in theory be 0x2 but that's very unlikely.
Timestamp	19 bits	Number of 30 minute periods since start of 2010 (UTC).
Stage 2 Flag	1 bit	A flag set to "1" in Stage 2 operation, otherwise "0".

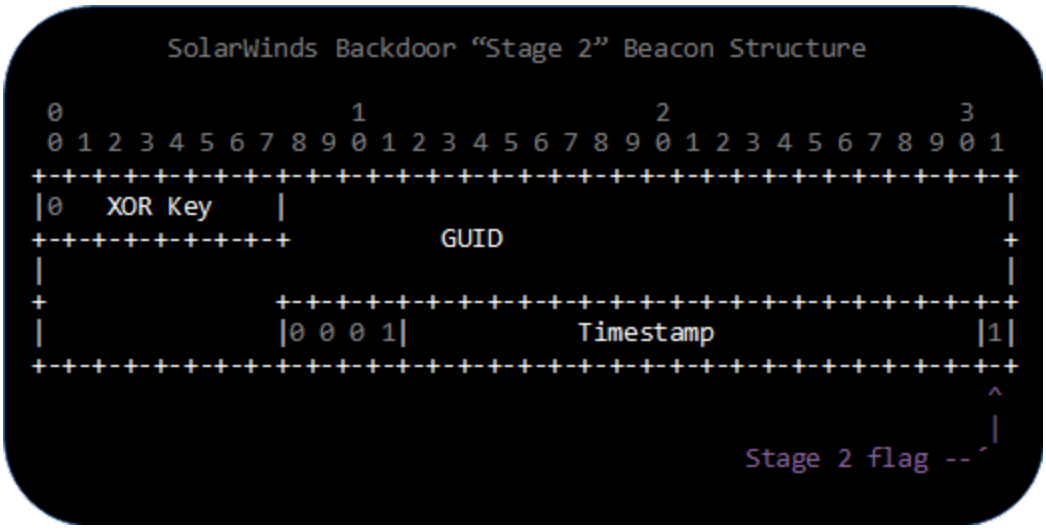

Image: Stage 2 beacon structure of the SolarWinds backdoor

The base32 encoding not only uses a custom alphabet, it also employs a reversed endianess and byte order compared to "normal" implementations. We have created a CyberChef recipe that performs this custom base32 decoding, so that the structure can be verified more easily. A list with 45 different Stage 2 avsvmcloud.com subdomains can be found in our Finding Targeted SUNBURST Victims with pDNS blog post. Feel free to replace the input to our CyberChef recipe with any of those subdomains.

Sleep Timers

The DNS responses from the name server not only controls how the SolarWinds backdoor should transition between the various stages, it also controls for how long the backdoor should wait before sending the next DNS beacon.

The delay is assigned by AND-ing the last octet of the received IP address with bitmask 0x54. The result from the AND operation is then used to select a sleep interval in the table below, within which the client picks a random number of minutes to sleep.

AND Result	Name	Sleep Interval
0x00	1 hour	30-120 minutes

0x04	4 hours	240-300 minutes
0x10	8 hours	480-600 minutes
0x14	1 day	1440-1560 minutes
0x40	3 days	4320-5760 minutes
0x44	1 week	10020-10140 minutes
0x50	2 weeks	20100-20220 minutes
0x54	1 month	43140-43260 minutes

An exception to the table above is clients that have entered Stage 2, which will only wait one to three minutes before requesting a CNAME.

Example DNS C2 for a Non-Targeted Client

Below is an example of DNS queries and responses from a SUNBURST client that wasn't targeted by the threat actors. These particular queries and responses come from a post on SolarWinds' community forum.

- 2020-07-04 00:03 UTC
  Query: if9prvp9o36mhihw2hrs260g12eu1 ⇒ AD domain "omeros.local"
  Response: 8.18.145.139 ⇒ sleep 1h, then **Continue**
- 2020-07-04 01:08 UTC
  Query: hnhb3v1b37dvv09icg0edp0 ⇒ Carbon Black is running
  Response: 8.18.145.62 ⇒ sleep 1 day, then **Continue**
- 2020-07-05 01:15 UTC
  Query: ea99hr2sfen95nkjlc5g ⇒ Nothing new to report
  Response: 8.18.144.150 ⇒ sleep 1 day, then **Continue**
- 2020-07-06 02:42 UTC
  Query: 707gigk9vbc923hf27fe ⇒ Nothing new to report
  Response: 8.18.145.151 ⇒ sleep 1 day, then **Continue**
- 2020-07-07 03:52 UTC
  Query: 6eivqct649pcg0g16ol4 ⇒ Nothing new to report
  Response: 20.140.84.127 ⇒ **Stop** DNS beacon

Note: Queried domain names in this list are subdomains of appsync-api.eu-west-1.avsvmcloud.com.

Example DNS C2 for a Targeted Client

*Disclaimer: We have very few DNS queries and responses for targeted victims, hence the transactions below are improvised based on data from VriesHd, Joe Słowik and FireEye. Please view these transactions as an example of what the communication **might** look like for a targeted victim rather than what actually happened to this particular target.*

- 2020-06-11 04:00 UTC
  Query: r8stkst71ebqgj66ervisu10bdohu0gt ⇒ AD domain, part 1 "central.pima.g"
  Response: 8.18.144.1 ⇒ Sleep 1h, then **Continue**
- 2020-06-11 05:00 UTC
  Query: ulfmcf44qd58t9e82w ⇒ AD domain, part 2 "ov"
  Response: 8.18.144.2 ⇒ Sleep 1h, then **Continue**
- 2020-06-11 06:00 UTC
  Query: p50jllhvhmoti8mpbf6p2di ⇒ Nothing to report
  Response: 8.18.144.16 ⇒ Sleep 8h, then **Continue**
- 2020-06-11 14:00 UTC
  Query: (?) ⇒ Nothing new to report
  Response: 8.18.144.17 ⇒ Sleep 8h, then **Continue**
- 2020-06-11 22:35 UTC
  Query: j5uqlssr1hfqnn8hkf172mp ⇒ Nothing to report
  Response: 184.72.181.52 ⇒ **Target** client for Stage 2 operation (1-3 minutes sleep)
- 2020-06-11 22:37 UTC
  Query: 7sbvaemscs0mc925tb99 ⇒ Client in Stage 2 operation, requesting CNAME
  Response: deftsecurity.com ⇒ **CNAME** for Stage 3 HTTPS C2 server

Note: Queried domains in this list are subdomains of appsync-api.us-west-2.avsvmcloud.com.

Conclusions

We hope this blog post clears up any misunderstandings regarding the targeting process of the SolarWinds backdoor and highlights the significance of the Stage 2 flag.

We warmly welcome any feedback or questions you might have regarding this writeup, please feel free to contact us or reach out to us through Twitter.

Posted by Erik Hjelmvik on Wednesday, 17 February 2021 20:22:00 (UTC/GMT)

Tags: #SolarWinds #backdoor #SUNBURST #Solorigate #FireEye #Microsoft #CNAME #STAGE2 #Stage 2 #DNS #avsvmcloud.com #C2 #CyberChef #ASCII-art

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