Extracting Security Products from SUNBURST DNS Beacons

netresec.com/

December 29, 2020

Erik Hjelmvik

,

Tuesday, 29 December 2020 09:38:00 (UTC/GMT)

The latest version of our SunburstDomainDecoder (v1.7) can be used to reveal which endpoint protection applications that are installed on trojanized SolarWinds Orion deployments. The security application info is extracted from DNS queries for "avsvmcloud.com" subdomains, which is used by SUNBURST as a beacon and C2 channel.

Here's an example showing that City of Kingston, Ontario, Canada were running Windows Defender on their trojanized SolarWinds deployment back in June:

```
C:\> SunburstDomainDecoder.exe < uniq-hostnames.txt | findstr F9A9387F7D252842
F9A9387F7D252842 2020-06-16T00:00:00.0000000Z,
WindowsDefender_RUNNING,WindowsDefender_STOPPED lt5ai41qh5d53qoti3mkmc0
F9A9387F7D252842 on.ca olc62cocacn7u2q22v02eu
F9A9387F7D252842 2020-06-17T00:00:00.0000000Z q94idf4sjbem0rait7gv
F9A9387F7D252842 city.kingston. r1qshoj05ji05ac6eoip02jovt6i2v0c
F9A9387F7D252842 city.kingston.on.ca
```

The "F9A9387F7D252842" value is the victim's unique SUNBURST GUID. See our blog post Reassembling Victim Domain Fragments from SUNBURST DNS for more info about how the GUID value is encoded into the DNS traffic.

You can also run SunburstDomainDecoder in Linux, with help of Mono, like this:

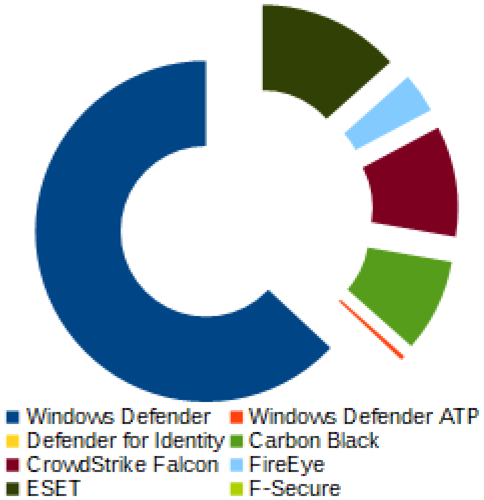
```
$ mono SunburstDomainDecoder.exe < uniq-hostnames.txt | grep 76330B4D49BF7EC4
76330B4D49BF7EC4 LABELMAR e8fh1ravufms0qpt00gudir2951udivf
>76330B4D49BF7EC4 2020-05-30T12:30:00.0000000Z,
ESET_RUNNING,ESET_STOPPED gp27ssesmvnpkgff7rc0eok
76330B4D49BF7EC4 nde5gaefm oiltaoj08jjd8h12vnr4tur5h
76330B4D49BF7EC4 LABELMARKET.ES
```

The file "uniq-hostnames.txt" is a publicly available SUNBURST passive DNS repository created by Bambenek Consulting.

Security Product Statistics

It is also possible to use the passive DNS data shared by Bambenek, Joe Słowik and others to compute statistics of which security products that are popular among SolarWinds' customers.

Application	Count
Windows Defender	150
Windows Defender ATP	1
MS Azure ATP / Defender for Identity	0
Carbon Black	21
CrowdStrike Falcon	25
FireEye	9
ESET	32
F-Secure	0



It is worth mentioning that SUNBURST does not report status for several other major endpoint protection vendors, such as Kaspersky, McAfee, Symantec, Sophos or Trend Micro.

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 Tuesday, 29 December 2020 09:38:00 (UTC/GMT)

Tags: #SunburstDomainDecoder #SUNBURST #SolarWinds #Solorigate #DNS #Windows Defender #Carbon Black #FireEye #ESET #F-Secure #C2 #beacon

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