Case Study

SUNBURST

Mapping Malicious Activity Using Farsight Historical Passive DNS

A Post-Attack Analysis of the Scale and Scope of the SUNBURST Compromise

DomainTools

INTRODUCTION

By studying the investigation into the SUNBURST attack, this case study demonstrates how cyber analysts can easily and quickly examine and visualize the scale of a malware attack—whether during or after the incident—using Farsight DNSDB passive DNS data and Maltego. It also takes a close look at the attack pattern of SUNBURST and provides insights into the malware's behavior.

About the SolarWinds SUNBURST Supply Chain Compromise

In December 2020, cyber threat analysis company FireEye discovered a global supply chain attack trojanizing SolarWinds Orion business software updates in order to distribute the malware named SUNBURST. The sophisticated attack affected public and private organizations—18,000 SolarWinds customers, including almost all Fortune 500 companies, government agencies, and government contractors—since as early as Spring 2020 and has resulted in network lateral movement and data theft by adversaries.

The SUNBURST Attack Flow

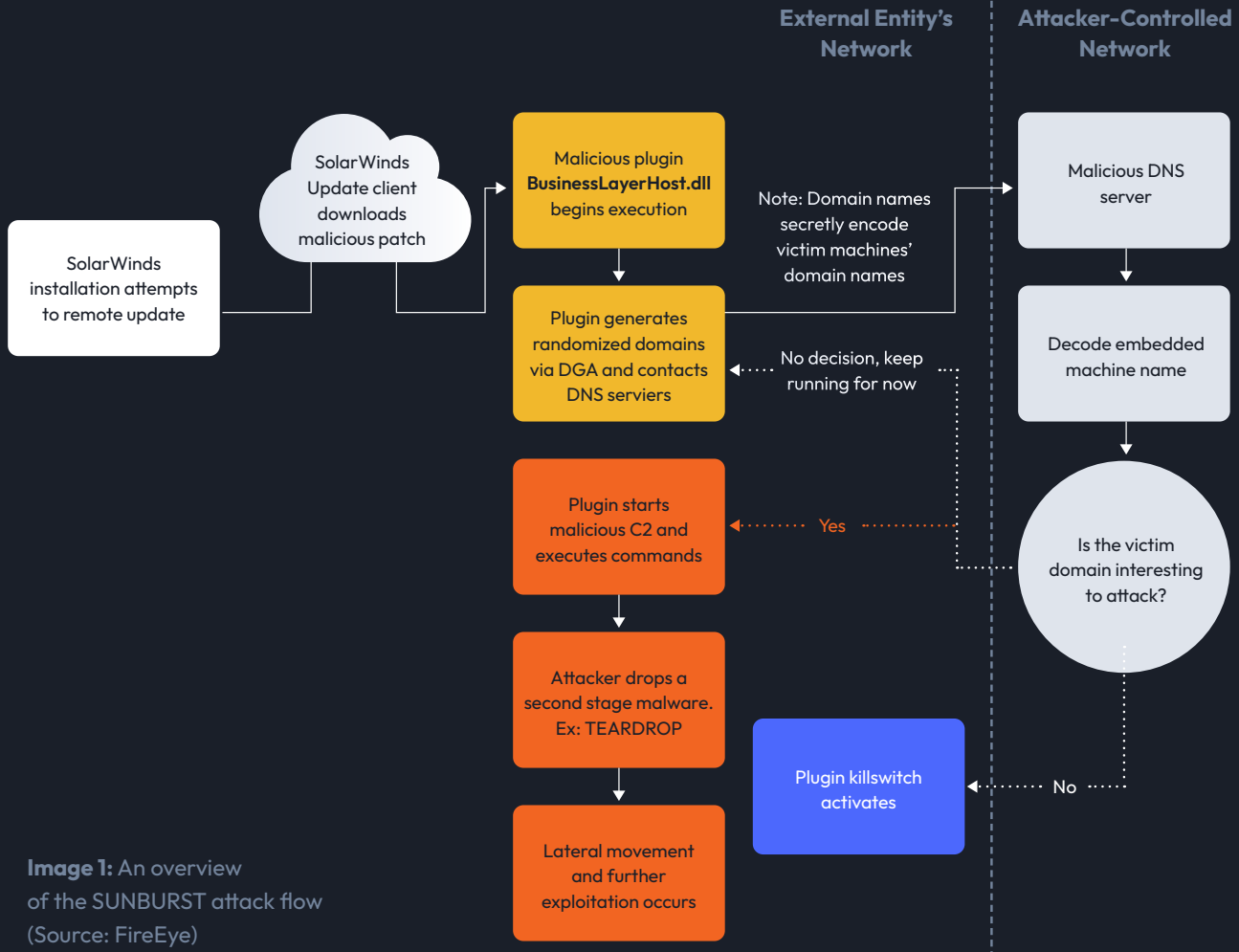

Image 1: An overview of the SUNBURST attack flow (Source: FireEye)

1. Initial Access

The attackers installed a malicious Dynamic Link Library file in a SolarWinds update package, which infected the end-users' machines and posed a backdoor when executed.

2. Command and Control

Once executed, the malware, using a Domain Generation Algorithm (DGA), generated a seemingly randomized domain that encoded the compromised computer's domain name. The malware then used DNS to resolve the domain to an IP address, which helped decide whether the compromised computer was a valuable target. Depending on the subnet the subdomain resolved to (see in the table below), the malware would either connect to a final C2 server, continue beaconing, activate a kill-switch for termination, or transition from active to passive mode.

Connect to Final C2 Server through DNS CNAME Response				
18.130.0.0/16	99.79.0.0/16	184.72.0.0/15		
Continue Beaconing				
8.18.144.0/23	18.130.0.0/16	71.152.53.0/24	99.79.0.0/16	87.238.80.0/21
199.201.117.0/24	184.72.0.0/15			
Terminate (Kill switch)				
10.0.0.0/8	fc00:: - fe00::	96.31.172.0/24	172.16.0.0/12	fec0:: - ffc0::
131.228.12.0/22	192.168.0.0/16	144.86.226.0/24	ff00:: - ff00::	224.0.0.0/3
20.140.0.0/15				
Transition from Active to Passive Mode				
41.84.159.0/24	74.114.24.0/21	154.118.140.0/24	217.163.7.0/24	

3. Lateral Movement & Exfiltration

If the malware connected to a final C2 server, the attackers would drop a second stage malware and further exploitation would occur to exfiltrate data from the compromised network.

SUNBURST Attack Scope Analysis Using Maltego and Farsight DNSDB

After being discovered, Microsoft has taken over the domain used by SUNBURST— avsvmcloud[.]com—and resolved it to 20.140.0[.]1. If SUNBURST now attempts to connect to its C2 coordinator using a subdomain of avsvmcloud[.]com, the kill-switch will be activated instead. Subsequently, without historical passive DNS data it is also no longer possible to investigate the hostnames generated with the DGA, the infected victims, the attack pattern observed, and the IP resolved from avsvmcloud[.]com's subdomains.

Using historical DNS data, investigators can still identify which subdomains were resolved to which IP addresses in relation to the SUNBURST attack. Furthermore, using Farsight's Flexible Search Transforms in Maltego, analysts can retrieve not only specific domains and IP addresses, but also any domain matching a specific pattern.

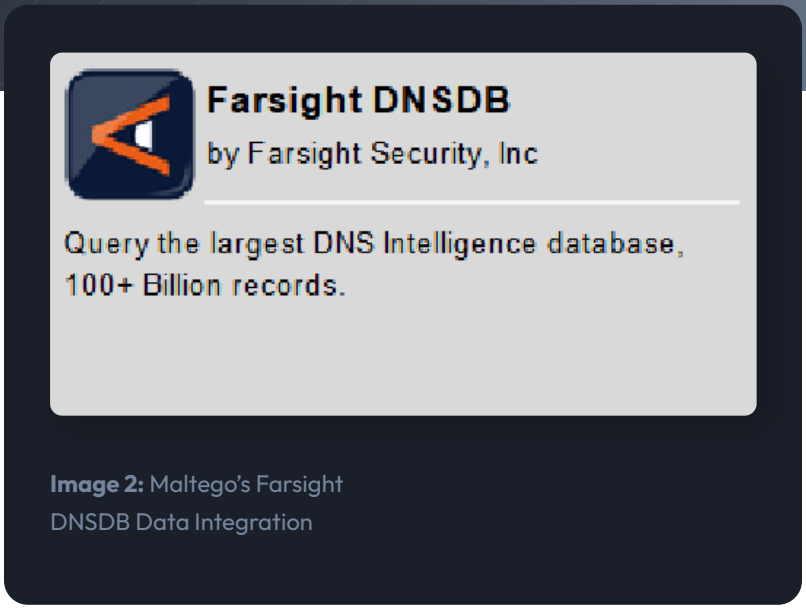

Image 2: Maltego's Farsight DNSDB Data Integration

In this case study, we demonstrate how to combine Maltego's link analysis capability and Farsight DNSDB passive DNS historical data to retrieve the historical domain and IP address data and analyze the potential scope of the SUNBURST attack.

About the new Farsight DNSDB Transforms

Farsight has deployed updates to the Farsight DNSDB Transform Hub item. The transforms have been re-named to be more intuitive and better in-line with Maltego transform naming conventions.

The new transforms leverage the DNSDB API version 2, increasing the level of error reporting detail provided to the user when something doesn't go as planned. DNSDB Flexible Search transforms also are now included in the hub item. Just create a Phrase entity with either a regular expression string or file-glob style pattern. The new transforms will enable you to perform complex partial string searches in Farsight DNSDB. To take advantage of these new capabilities, simply update the Farsight DNSDB hub item in your Maltego client.

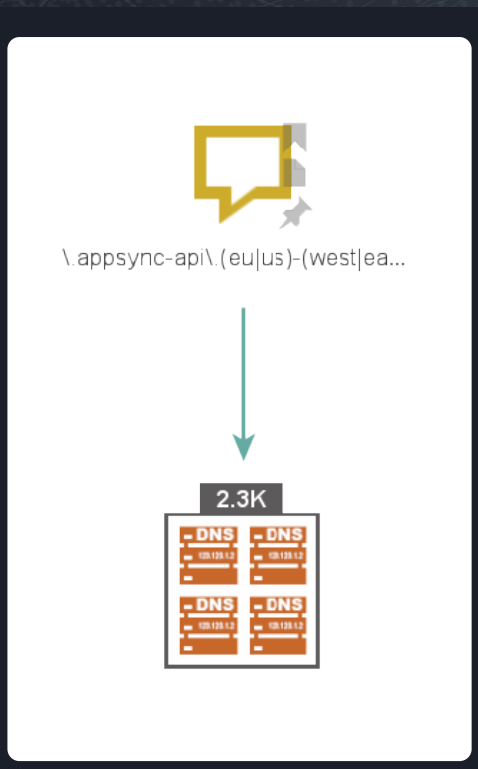

Image 3: Retrieving DNS names associated with the domain generated by the SUNBURST malware

First, we input a known the pattern known to be used by SUNBURST's DGA as a regular expression (regex) into Phrase Entities on the Maltego graph:

```
\.appsync-api\.(eu|us)-(west|east)-(1|2)\.avsvmcloud\.com\.$
```

We ran the Search DNS Names (Regex) [DNSDB] Transform from the Farsight DNSDB data integration to retrieve all the DNS queries matching this pattern. The DNS names returned were resolved at some point in the past and most probably the majority of them, at least before Microsoft seized the domain, created by SUNBURST malware attempting to communicate to a C2 server after having infected a host.

With the DNS name records in hand, we could go ahead and delete the initial Phrase Entities used to perform the search. Next, we looked into the IP addresses these FQDNS resolved to by running the To DNS Records [DNSDB] in order to see what the C2 coordinator instructed the malware to do next.

Since Microsoft has seized the domain and resolved it to the 20.140.0[.]1 IP address which activates the kill-switch, a large number of the DNS Names Entities connect to this particular IP address. If a DNS name only resolved to this particular IP address, it is safe to assume that the communication happened after Microsoft seized the domain, and some names might have been also artificially made by the curious security researchers.

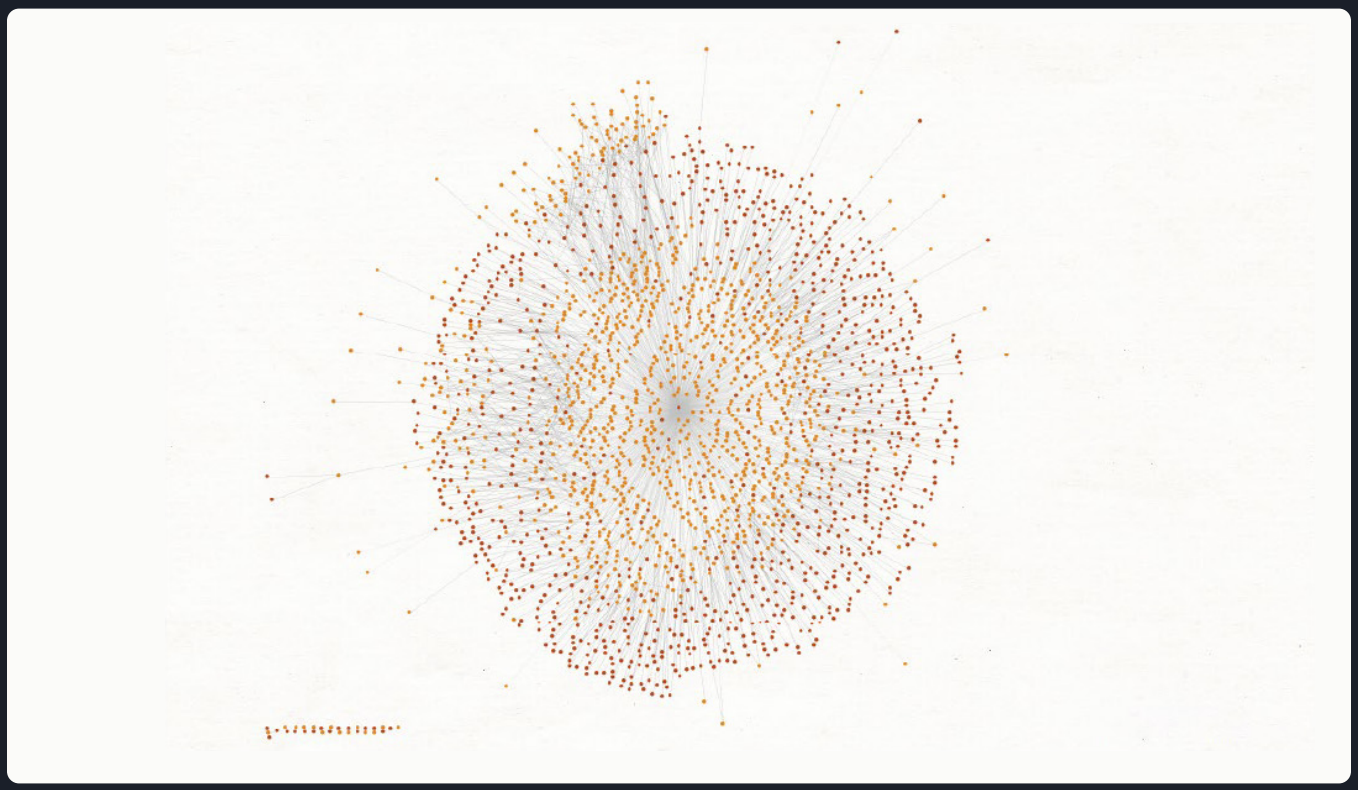

Image 4: Resolving the DNS names to IP addresses

For this case study, we will look at C2 communications that occurred before Microsoft's action and possibly also before the SolarWinds compromise was public knowledge. To do so, we exclude the DNS Name Entities that only linked to the 20.140.0[.]1 IP Address Entity.

To better analyze the rest of the graph, we used the Ball Size by Links (Incoming) Viewlet to enlarge the data node sizes based on the number of incoming links they have. Note that the 20.140.0[.]1 IP Address Entity has the most incoming links (and therefore resolutions). This is likely due to the fact that even if some FQDNs (Fully Qualified Domain Name) resolved to other IP addresses, they would eventually be resolved to this IP if the malware continued beaconing.

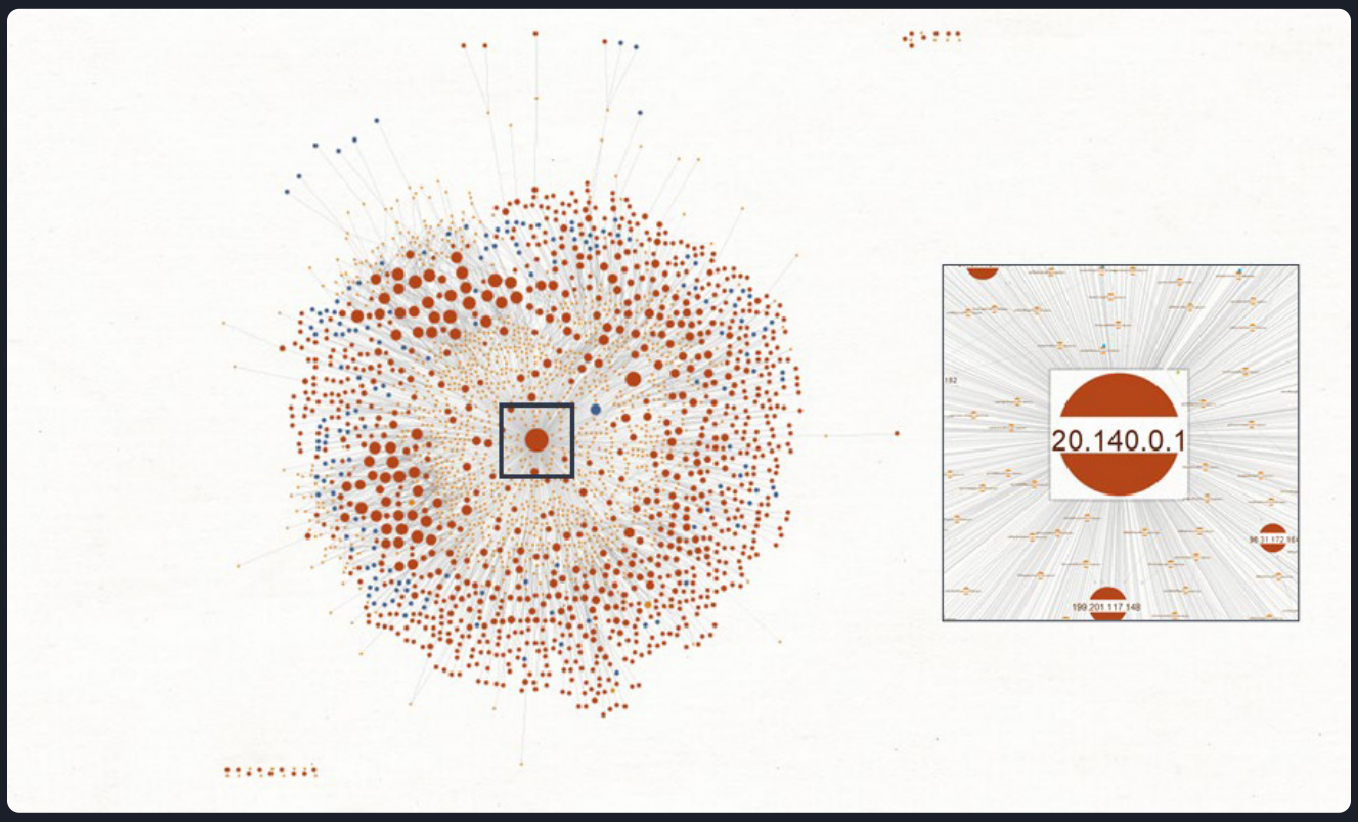

Image 5: The 20.140.0[.]1 IP address has the most DNS name links because Microsoft seized the avsvmcloud[.]com domain

We can now easily find certain IP addresses and the related DNS names in the graph and copy the data points onto a new graph to investigate further.

As shown in the image below, four DNS names resolved to the 18.130.0.0/16 subnet. If the malware received a CNAME response immediately after being resolved to this subnet, it will connect to its final C2 server

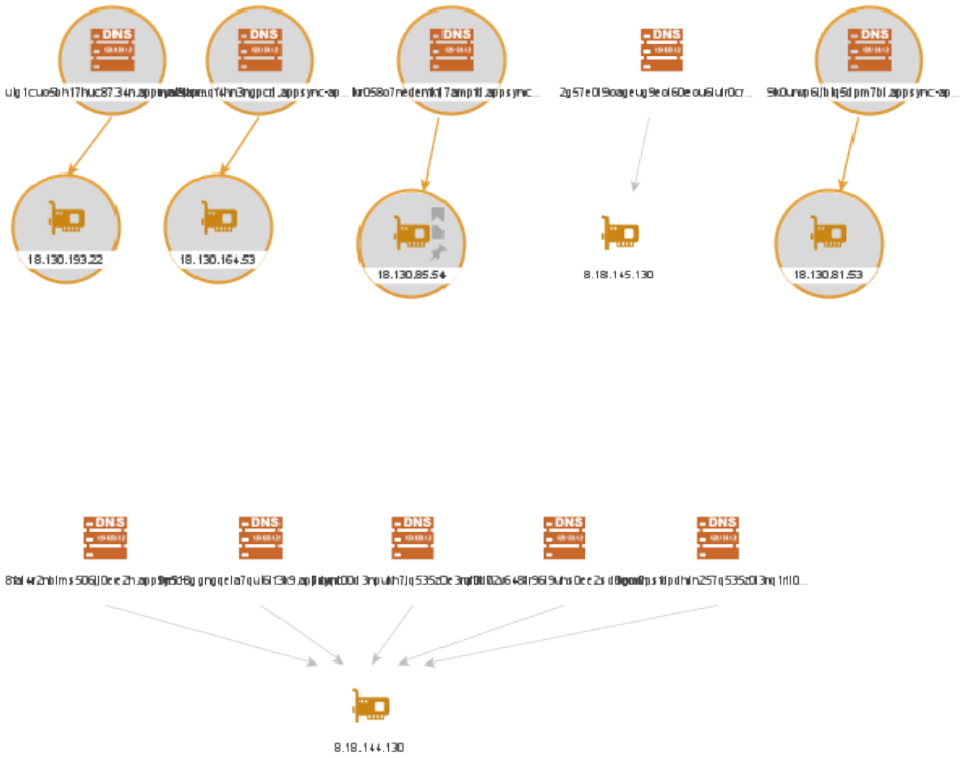

Image 6: DNS names resolving to IP addresses known to result in the malware possibly establishing connection with the final C2 servers

We could continue to check the individual IP addresses against the block list provided at the beginning of this case study to understand where each FQDNS was redirected to, but it would consume excessive time and effort. Instead, we could divide the IP addresses into netblocks using the To Netblock [Using whois info] Transform.

While the netblocks will not exactly map the ranges defined in the block list, given enough distance between the range of each netblock, we can expect that the resulting grouping will only belong to one of the function groups of the malware.

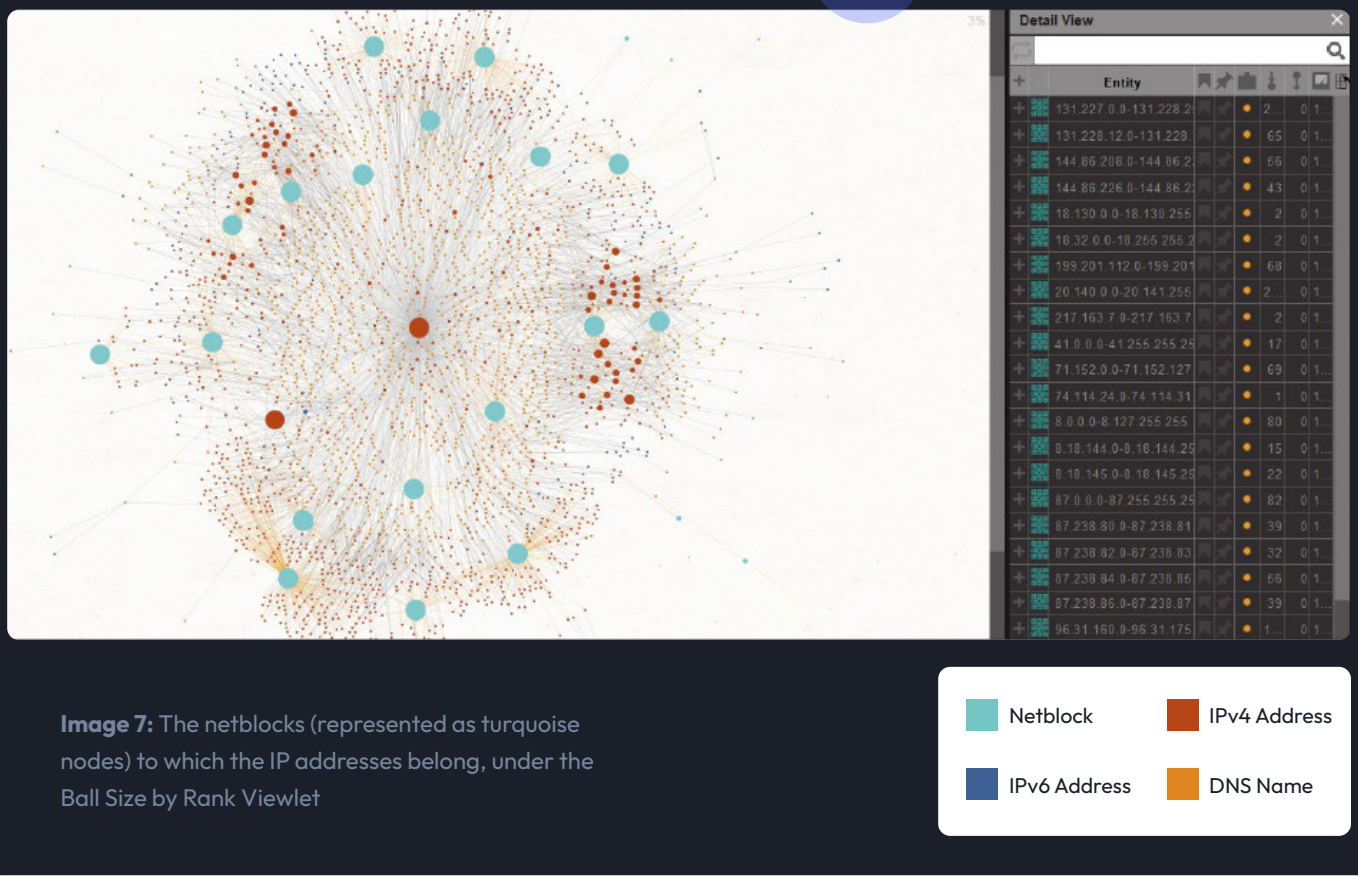

Image 7: The netblocks (represented as turquoise nodes) to which the IP addresses belong, under the Ball Size by Rank Viewlet

With the netblock information, we can quickly select the Netblock Entity as well as the IP addresses and DNS names pointing to that Netblock Entity for deeper inspection.

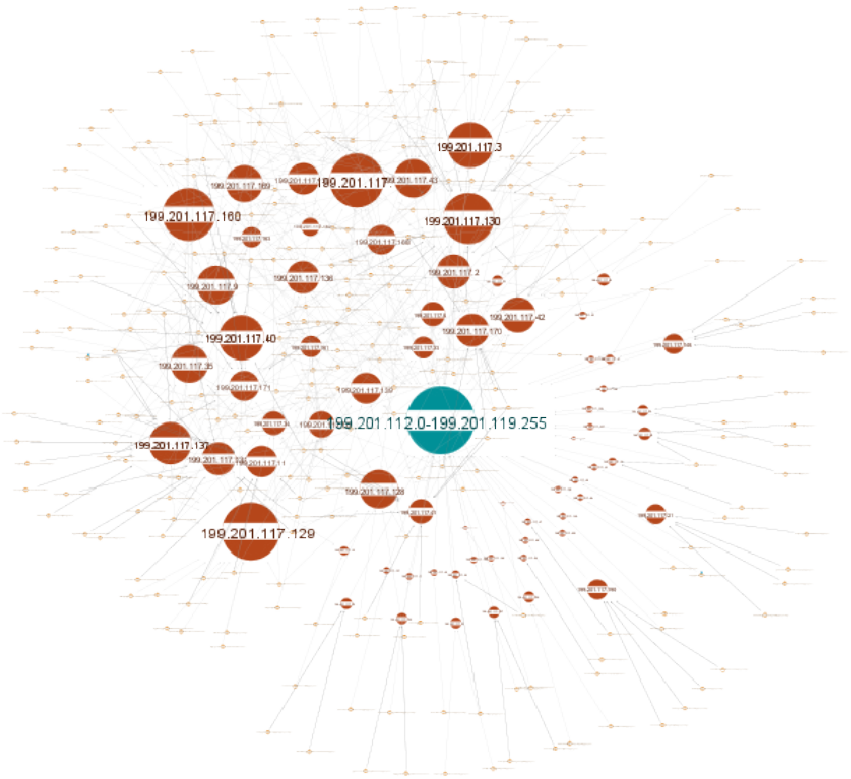

Image 8: The Netblock Entity 199.201.112.0-199.201.119.255 and relevant IP addresses which resulted to the malware continuing beaconing according to the hard-coded list of IP address blocks

Identifying Other Potential C2 Servers

Up until now in our investigation, we specifically looked at the infrastructure connected to the avsvmcloud[.]com domain. Knowing the pattern used by the DGA, we can take one step further and try to identify other potential C2 servers using the input as above, but including other than than avsvmcloud[.]com domains:

- \.appsync-api\.(eu|us)-(west|east)-(1|2)\.

The DNS name Flexible Search Regex query will help discover DNS names that fit the same patterns and might be relevant to the SUNBURST attack, but in other domains.

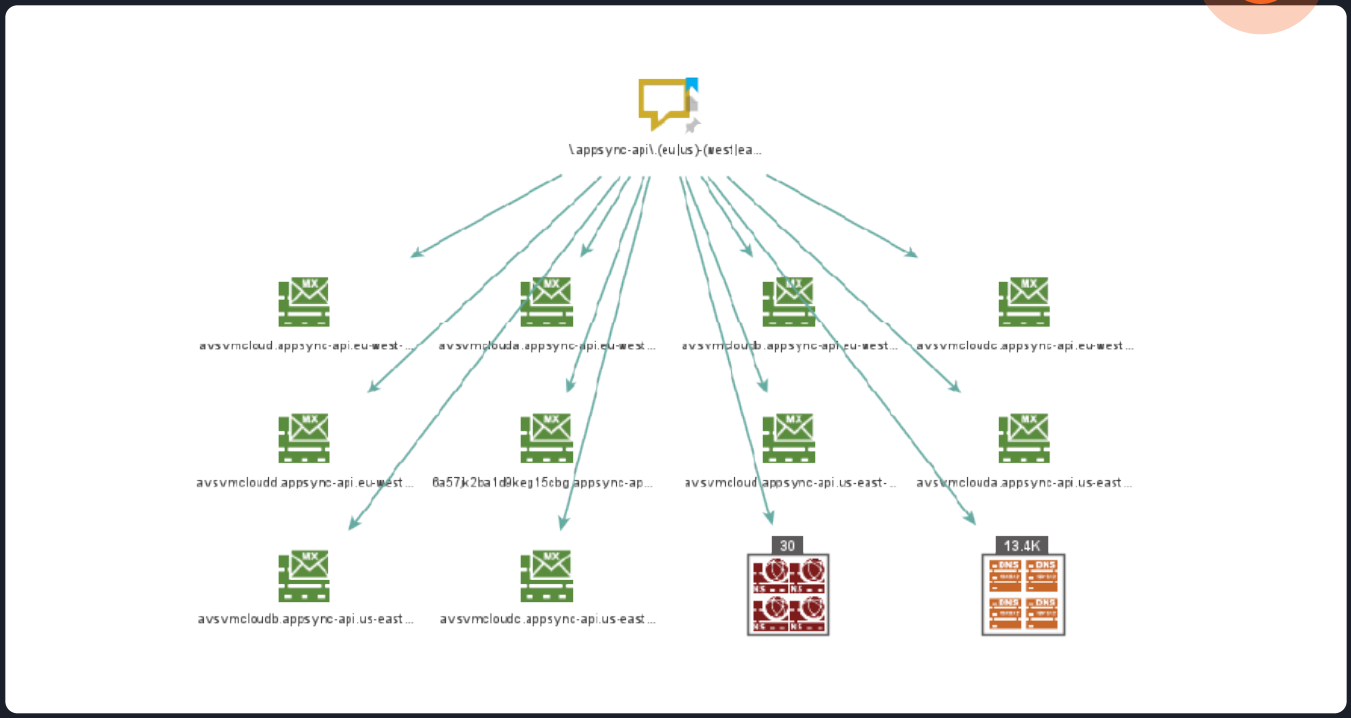

Image 9: Identifying other potntial DNS names and C2 servers based on the attack pattern

SUMMARY

As you can see, we have identified additional FQDN in other domains that fit the pattern used by adversaries in this compromise. From this point on, we have all the information needed to explore and analyze the SUNBURST attack in greater detail.

Enrich Your Network Analysis with Farsight Passive DNS Data and Maltego Now

We hope this case study helps you understand how cyber security analysts and operation teams can leverage Farsight DNSDB's passive DNS data in combination with Maltego to retrieve historical infrastructure data for attack analysis and identify key intelligence based on an attack pattern.

Getting Started is Easy: Try Our Free Trial for Farsight Transforms!

Farsight Transforms are available for both community and commercial Maltego users with a free trial. You can get started immediately without an API key or registration, or sign up to the 30-day free trial for more query allowance.

To access the full solution, a Maltego commercial license and a Farsight DNSDB subscription are required. Learn more about the access information on our Data Partner page here.

If you want to learn more about how Maltego can reduce time for your cybersecurity operations, schedule a personalized demo with us today!

For more information about Maltego's solution and other whitepapers and case studies, visit Maltego.com. For more information about Farsight DNSDB, other passive DNS solutions and to access more resources from Farsight, please visit our webpage for Farsight DNSDB.

About DomainTools

DomainTools is the global leader for internet intelligence and the first place security practitioners go when they need to know. The world's most advanced security teams use our solutions to identify external risks, investigate threats, and proactively protect their organizations in a constantly evolving threat landscape.

Learn more about how to connect the dots on malicious activity at domaintools.com or follow us on Twitter: @domaintools.

Farsight DNSDB