Unraveling Network Infrastructure Linked to the SolarWinds Hack

domaintools.com/resources/blog/unraveling-network-infrastructure-linked-to-the-solarwinds-hack

Background

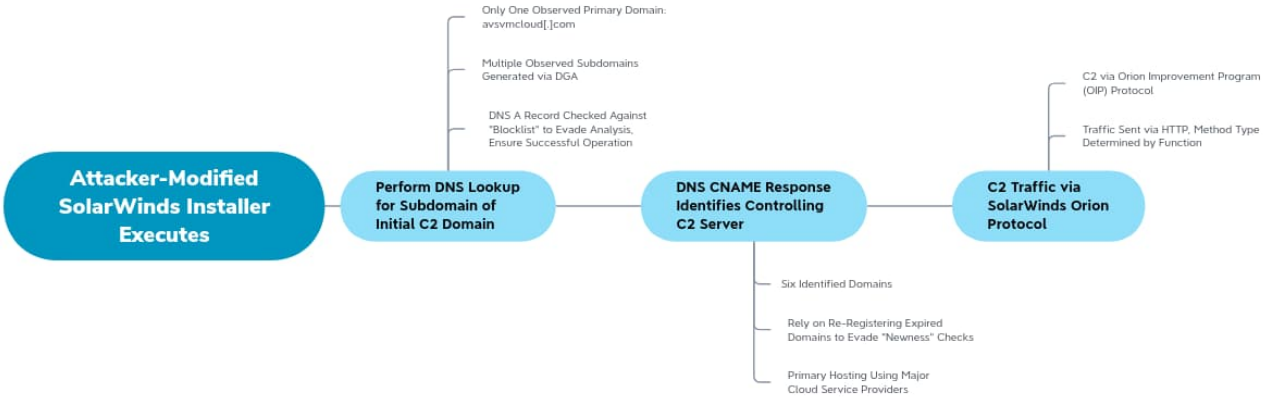
On 13 December 2020, multiple media reports emerged first identifying network intrusions at several US government agencies. Subsequent reporting indicated these intrusions, along with a previously-identified breach at information security giant FireEye, were linked to a compromise at IT management and remote monitoring software provider SolarWinds.

FireEye and Microsoft followed up media reporting with in-depth technical reports on a complex supply chain attack focusing on SolarWinds' Orion IT monitoring software. The attack focuses on a malicious Dynamic Linked Library (DLL) included in the legitimate Orion installer package, referred to as SUNBURST or Solorigate by FireEye and Microsoft, respectively. Network defenders, threat researchers, and other interested parties are strongly encouraged to review the linked reports from FireEye and Microsoft to understand these campaigns in detail.

However, as part of the overall intrusion via the compromise at SolarWinds, several interesting network-based observations emerge. This includes both behaviors related to the Command and Control (C2) activity of SUNBURST and the characteristics of the network infrastructure used to facilitate the campaign.

Observed Command and Control Behavior

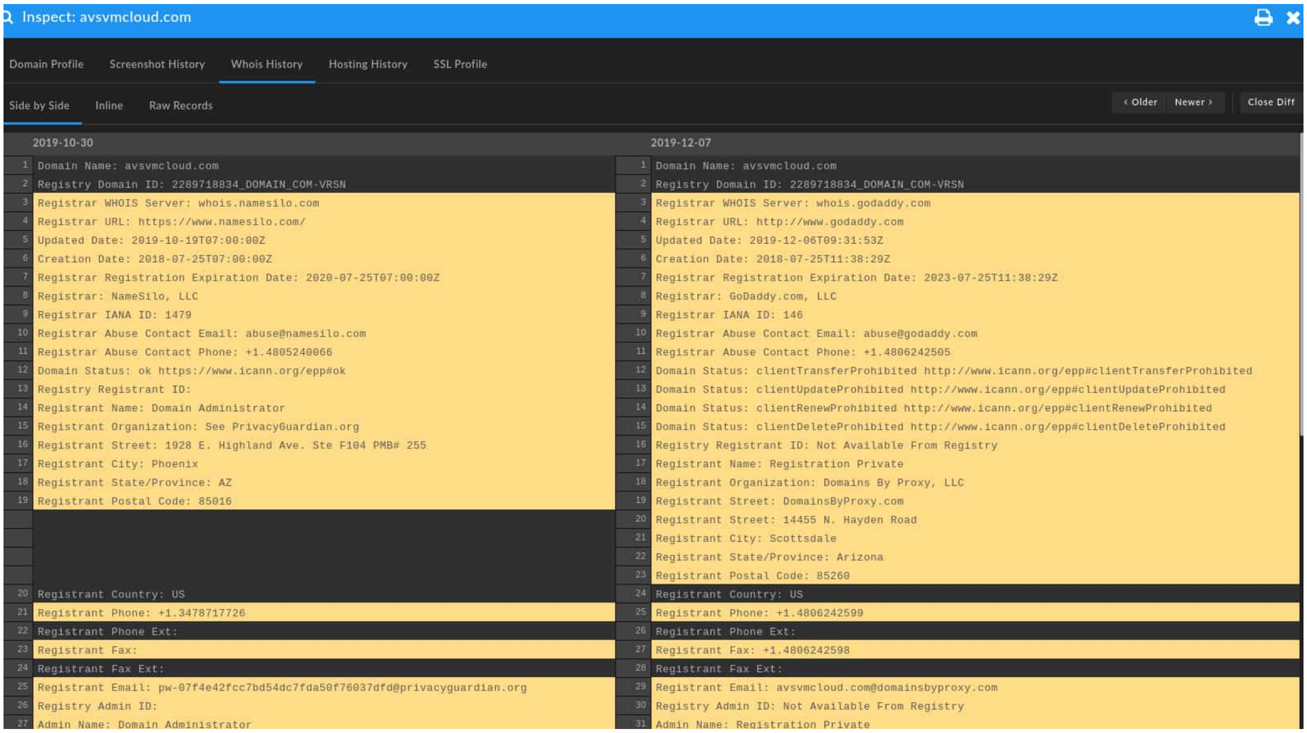
SUNBURST uses a complex, multi-staged mechanism for identifying a controlling C2 server, and performing subsequent communication. This is summarized in the following chart.


Attacker-Modified SolarWinds Installer Executes
Perform DNS Lookup for Subdomain of Initial C2 Domain
Only One Observed Primary Domain: avsvmcloud[.]com
Multiple Observed Subdomains Generated via DGA
DNS A Record Checked Against "Blocklist" to Evade Analysis, Ensure Successful Operation
DNS CNAME Response Identifies Controlling C2 Server
Six Identified Domains
Rely on Re-Registering Expired Domains to Evade "Newness" Checks
Primary Hosting Using Major Cloud Service Providers
C2 Traffic via SolarWinds Orion Protocol
C2 via Orion Improvement Program (OIP) Protocol
Traffic Sent via HTTP, Method Type Determined by Function

C2 behavior is first dependent on resolving a subdomain of the first-stage C2 domain:

```
Avsvmcloud[.]com
```

The primary domain is interesting, as it first appears long before the Spring 2020 timeframe when SUNBURST is believed to have started (Spring 2020), in July 2018. A closer view of Whois history via DomainTools Iris shows a noticeable change in the domain in late 2019:



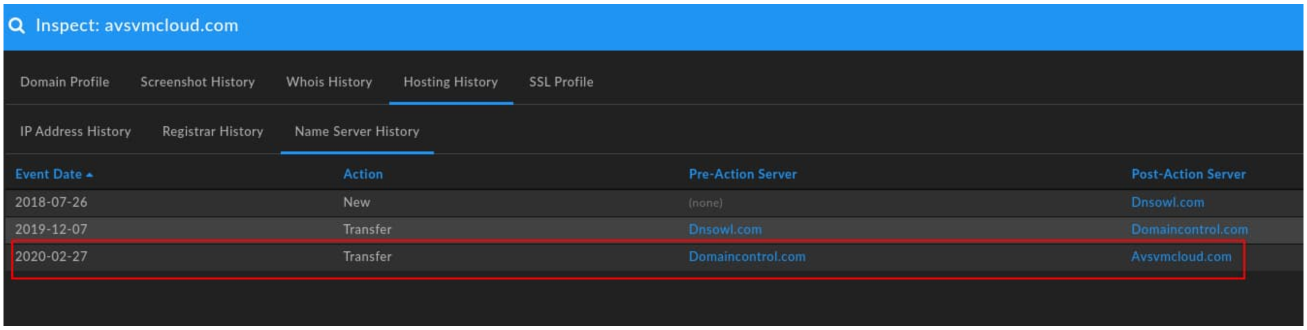
2019-10-30

```
Domain Name: avsvmcloud.com
Registry Domain ID: 2289718834_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2019-10-19T07:00:00Z
Creation Date: 2018-07-25T07:00:00Z
Registrar Registration Expiration Date: 2020-07-25T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: ok https://www.icann.org/epp#ok
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: See PrivacyGuardian.org
Registrant Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Registrant City: Phoenix
Registrant State/Province: AZ
Registrant Postal Code: 85016




Registrant Country: US
Registrant Phone: +1.3478717726
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: pw-07f4e42fcc7bd54dc7fda50f76037dfd@privacyguardian.org
Registry Admin ID:
Admin Name: Domain Administrator
```

2019-12-07

```
Domain Name: avsvmcloud.com
Registry Domain ID: 2289718834_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2019-12-06T09:31:53Z
Creation Date: 2018-07-25T11:38:29Z
Registrar Registration Expiration Date: 2023-07-25T11:38:29Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Registration Private
Registrant Organization: Domains By Proxy, LLC
Registrant Street: DomainsByProxy.com
Registrant Street: 14455 N. Hayden Road
Registrant City: Scottsdale
Registrant State/Province: Arizona
Registrant Postal Code: 85260
Registrant Country: US
Registrant Phone: +1.4806242599
Registrant Phone Ext:
Registrant Fax: +1.4806242598
Registrant Fax Ext:
Registrant Email: avsvmcloud.com@domainsbyproxy.com
Registry Admin ID: Not Available From Registry
Admin Name: Registration Private
```

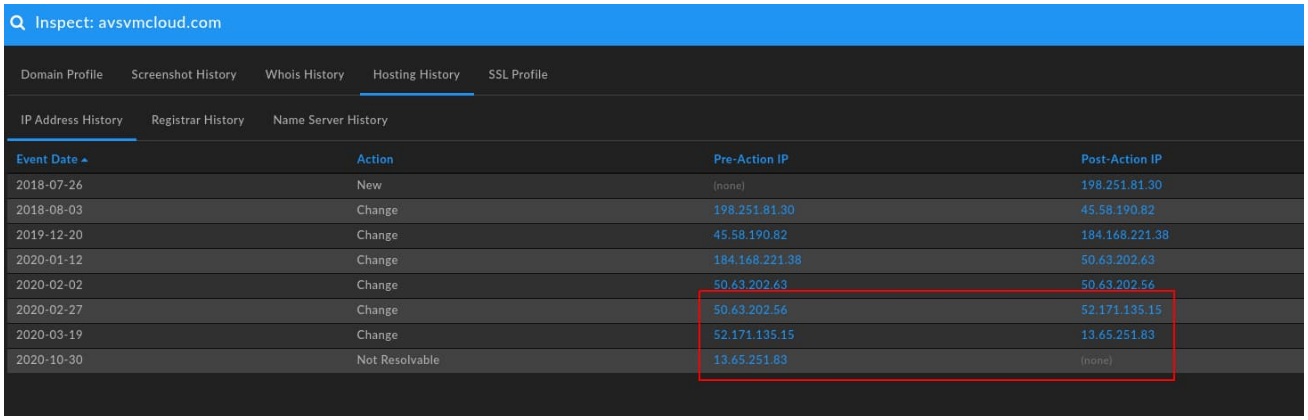
Initially, the domain was registered via Namecheap with PrivacyGuardian anonymization, but then shifted to completely different services (GoDaddy and Domains by Proxy) in December 2019. This change in registration information is reflected in hosting and related characteristics:



Event Date ▲	Action	Pre-Action Server	Post-Action Server
2018-07-26	New	(none)	Dnsowl.com
2019-12-07	Transfer	Dnsowl.com	Domaincontrol.com
2020-02-27	Transfer	Domaincontrol.com	Avsvmcloud.com

The two images above capture alterations in hosting and authoritative name server:

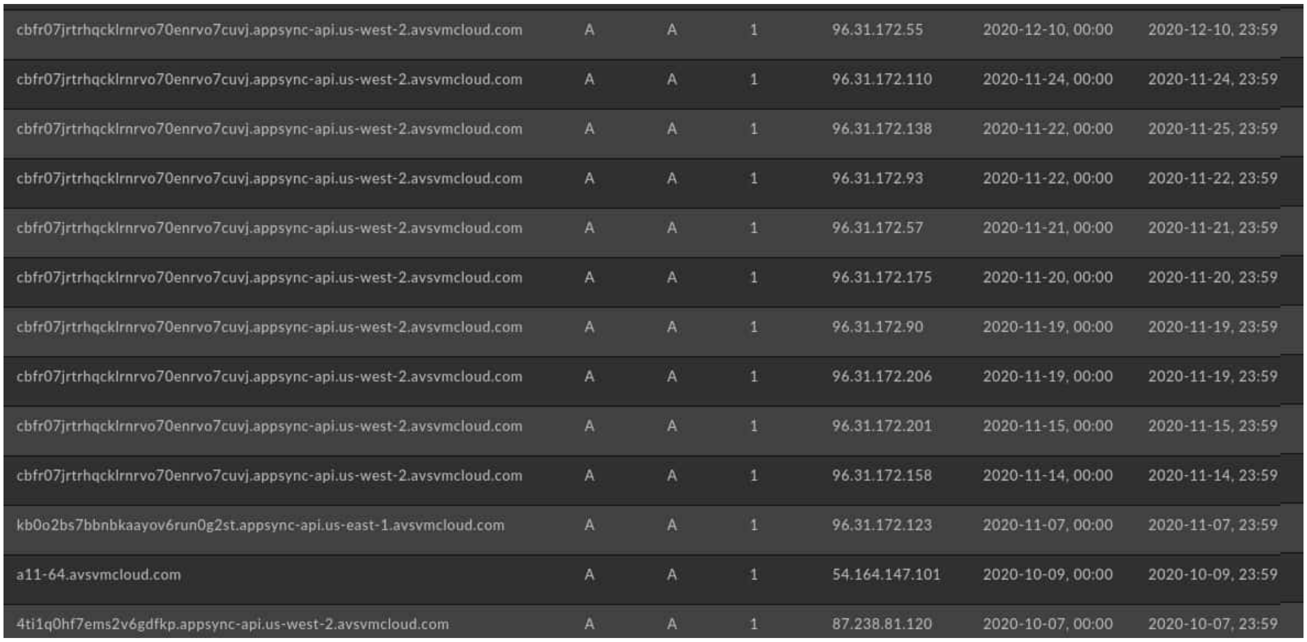
- The domain shifted to GoDaddy parking infrastructure on 20 December 2019, roughly the same time as the change in registration.
- The domain remains on GoDaddy parking infrastructure until 27 February 2020, when it shifts to Microsoft cloud hosting (52.171.135[.]15, then 13.65.251[.]83)
- At the same time hosting shifts to Microsoft, the domain changes authoritative name server to self-hosting at Avsvmcloud[.]com.



Event Date ▲	Action	Pre-Action IP	Post-Action IP
2018-07-26	New	(none)	198.251.81.30
2018-08-03	Change	198.251.81.30	45.58.190.82
2019-12-20	Change	45.58.190.82	184.168.221.38
2020-01-12	Change	184.168.221.38	50.63.202.63
2020-02-02	Change	50.63.202.63	50.63.202.56
2020-02-27	Change	50.63.202.56	52.171.135.15
2020-03-19	Change	52.171.135.15	13.65.251.83
2020-10-30	Not Resolvable	13.65.251.83	(none)

The primary domain ceases to resolve to an IP address on 30 October 2020.

While the primary domain ceases to resolve on 30 October 2020, subdomains remained active through early December 2020 as shown in DomainTools Passive DNS (pDNS) data:



cbfr07jrtrhqcklrnrvo70enrvo7cuvj.appsync-api.us-west-2.avsvmcloud.com	A	A	1	96.31.172.55	2020-12-10, 00:00	2020-12-10, 23:59
cbfr07jrtrhqcklrnrvo70enrvo7cuvj.appsync-api.us-west-2.avsvmcloud.com	A	A	1	96.31.172.110	2020-11-24, 00:00	2020-11-24, 23:59
cbfr07jrtrhqcklrnrvo70enrvo7cuvj.appsync-api.us-west-2.avsvmcloud.com	A	A	1	96.31.172.138	2020-11-22, 00:00	2020-11-25, 23:59
cbfr07jrtrhqcklrnrvo70enrvo7cuvj.appsync-api.us-west-2.avsvmcloud.com	A	A	1	96.31.172.93	2020-11-22, 00:00	2020-11-22, 23:59
cbfr07jrtrhqcklrnrvo70enrvo7cuvj.appsync-api.us-west-2.avsvmcloud.com	A	A	1	96.31.172.57	2020-11-21, 00:00	2020-11-21, 23:59
cbfr07jrtrhqcklrnrvo70enrvo7cuvj.appsync-api.us-west-2.avsvmcloud.com	A	A	1	96.31.172.175	2020-11-20, 00:00	2020-11-20, 23:59
cbfr07jrtrhqcklrnrvo70enrvo7cuvj.appsync-api.us-west-2.avsvmcloud.com	A	A	1	96.31.172.90	2020-11-19, 00:00	2020-11-19, 23:59
cbfr07jrtrhqcklrnrvo70enrvo7cuvj.appsync-api.us-west-2.avsvmcloud.com	A	A	1	96.31.172.206	2020-11-19, 00:00	2020-11-19, 23:59
cbfr07jrtrhqcklrnrvo70enrvo7cuvj.appsync-api.us-west-2.avsvmcloud.com	A	A	1	96.31.172.201	2020-11-15, 00:00	2020-11-15, 23:59
cbfr07jrtrhqcklrnrvo70enrvo7cuvj.appsync-api.us-west-2.avsvmcloud.com	A	A	1	96.31.172.158	2020-11-14, 00:00	2020-11-14, 23:59
kb0o2bs7bbnbkaayov6run0g2st.appsync-api.us-east-1.avsvmcloud.com	A	A	1	96.31.172.123	2020-11-07, 00:00	2020-11-07, 23:59
a11-64.avsvmcloud.com	A	A	1	54.164.147.101	2020-10-09, 00:00	2020-10-09, 23:59
4ti1q0hf7ems2v6gdfkp.appsync-api.us-west-2.avsvmcloud.com	A	A	1	87.238.81.120	2020-10-07, 00:00	2020-10-07, 23:59

With the above, we have some initial observations related to this campaign:

1. Primary C2 infrastructure was acquired and initially provisioned in December 2019 using an existing but likely expired domain that superficially resembles a domain for cloud hosting services.
2. Hosting, name server, and other items necessary for operational use were established on 27 February 2020.
3. If Avsvmcloud[.]com is the only primary C2 domain, the SUNBURST campaign was operational no earlier than 27 February 2020, with a significant change in aspect on 30 October 2020.

Yet, operations do not end here. Provided the subdomain of Avsvmcloud[.]com resolves to a value not in an internally-stored blocklist of IP address ranges, C2 behavior looks for a returned Canonical Name (CNAME) record. This value is used for subsequent C2 activity, sent via HTTP but using the Orion Improvement Program format to "blend in" to network communications. Observed domains linked to second-stage C2 include the following items:

Domain	Create Date	IP Address	ISP	Registrar
databasegalore[.]com	2019-12-14	5.252.177.21	MivoCloud SRL	NAMECHEAP INC
deftsecurity[.]com	2019-02-11	13.59.205.66	Amazon Technologies Inc.	NAMESILO, LLC
freescanonline[.]com	2014-08-14	54.193.127.66	Amazon.com Inc.	NAMECHEAP INC

Domain	Create Date	IP Address	ISP	Registrar
highdatabase[.]com	2019-03-07	139.99.115.204	OVH Singapore Pte. Ltd	NAMESILO, LLC
incomeupdate[.]com	2016-10-02	5.252.177.25	MivoCloud SRL	NameCheap, Inc.
panhardware[.]com	2019-05-30	204.188.205.176	SharkTech	NameSilo, LLC
thedoccloud[.]com	2013-07-07	54.215.192.52	Amazon.com Inc.	NameSilo, LLC
virtualwebdata[.]com	2014-03-22	18.217.225.111	Amazon Technologies Inc.	NameSilo, LLC
websitetheme[.]com	2006-07-28	18.253.52.187	Amazon Technologies Inc.	NAMESILO, LLC
zupertech[.]com	2016-08-16	51.89.125.18	OVH SAS	NameSilo, LLC

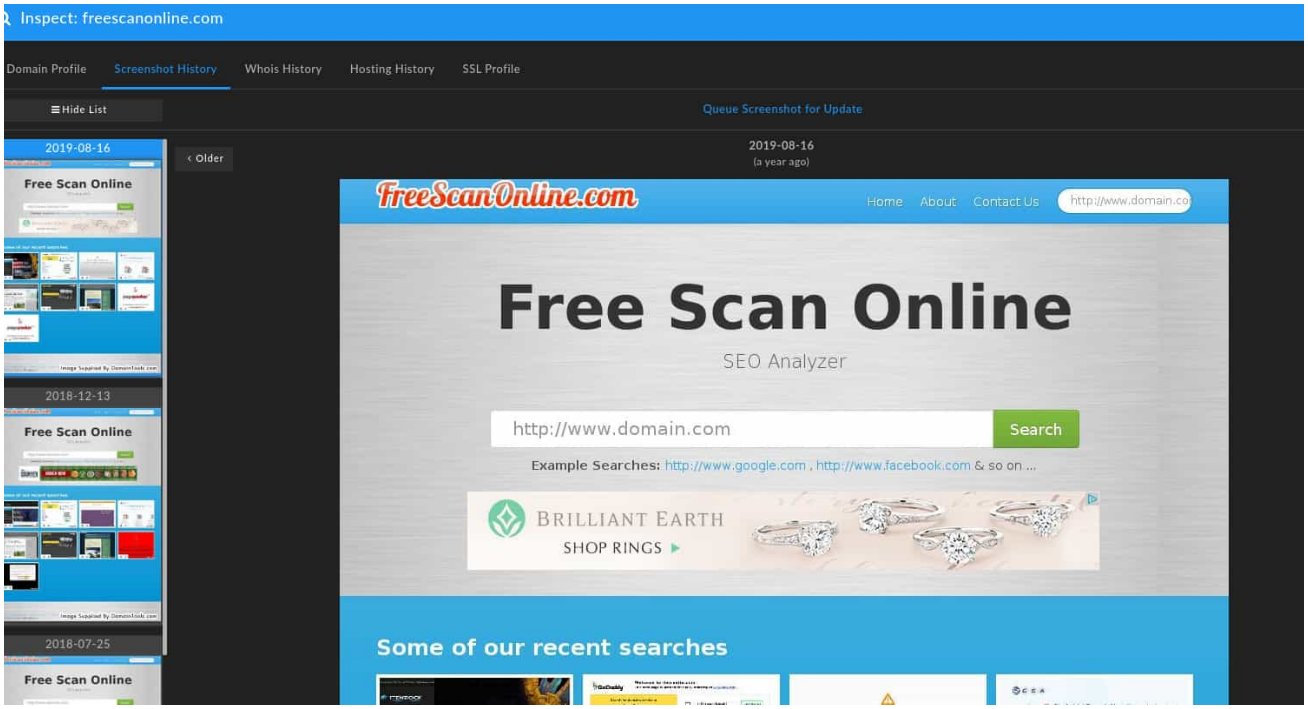
Understanding Network Infrastructure

Based on the dataset of eleven domains—one initial C2 item that works to resolve a second C2 domain for adversary use—we can derive several lessons about the responsible adversary and their infrastructure tendencies.

First and foremost, the adversary relies overwhelmingly on cloud-based providers such as Amazon and Microsoft for hosting purposes, with smaller or less-reputable providers also used for the second-stage C2 domains. While not well reflected in the pattern of second-stage domains, pDNS information for subdomain resolutions on Avsvmcloud[.]com show an overwhelming use of major cloud providers in returned responses, captured in DomainTools Iris output here. This hosting tendency makes infrastructure pivoting difficult, but also presents problems for defenders as such infrastructure can be shared by additional, non-malicious entities or reallocated quickly to other parties which muddies forensic analysis.

Second, naming themes as one component of domain characteristics show a tendency toward technology or IT service names. Although somewhat difficult to track and filter, identifying naming themes in new, previously unobserved network traffic can serve as a way to flag suspicious infrastructure for follow-on investigation. Looking for “technology adjacent” domains newly resolving can serve as a tripwire for possible malicious activity.

Third, the domains in question appear to represent a combination of likely adversary created (such as Databasegalore[.]com, which was created roughly the same time Avsvmcloud[.]com was provisioned), opportunistic re-registration of existing domains, and possible compromise of legitimate infrastructure. In the second case, Deftsecurity[.]com changes registrar and privacy provider in February 2019 despite existing for several years prior indicating likely re-registration by the adversary. More concerning are cases such as Freescanonline[.]com, which appears to have been a legitimate site for Search Engine Optimization (SEO) analysis as late as August 2019:



Of note, this domain was resolving to 108.179.242[.]236 until mid-February 2020, when it shifted to Amazon hosting inline with other network items observed in this campaign. This item therefore is somewhat ambiguous, either representing adversary take-over (given how recently it appears to have been used for legitimate purposes) or opportunistic re-registration on expiration.

Overall, the attacker leveraged domains with some degree of “history” behind them to evade filters or algorithms that flag network infrastructure due to “newness”. By having several months of creation time before either taking control over or modifying hosting for use in the SUNBURST campaign between December 2019 and March 2020 (based on analysis of DomainTools data), the attacker could build a false sense of trust in the network infrastructure used to potentially evade some security solutions and analysis.

Lessons for Defenders

Overall, the SUNBURST campaign represents a highly complex, operationally savvy, and technically patient campaign. As detailed by FireEye and Microsoft, this extends to subsequent lateral movement operations within victim networks, which relied overwhelmingly on capturing credentials within victim environments and mimicking user activity to evade detection. We as network defenders are thus presented with an exceptionally difficult attack to detect, defeat, and recover from—or are we?

As documented in this posting, there are a number of network observables that are critical to attacker success for C2 purposes as part of SUNBURST operations. While certainly not without its own difficulties, Network Security Monitoring (NSM) and DNS analysis can identify new, unusual, or outright suspicious network communication patterns.

Monitoring is even more powerful when tracking external communications is combined with internal system awareness to quickly disposition what hosts are communicating to outside entities. In the case of the SolarWinds Orion software, identifying traffic from this service or its hosting device to new, unusual domains—even if using communication patterns similar to Orion telemetry—can rapidly identify connections that are abnormal and worth further scrutiny.

While much work would remain to properly disposition the event in question and discover something as complex and evasive as a malicious, signed update package, at least initial detection that something is “wrong” can be readily achieved. Next steps would require further analysis, review of system behaviors and configurations, and subsequent investigation—but at a minimum defenders are now alert and aware that something is amiss within the monitored environment.

Conclusion

The SUNBURST campaign represents a uniquely distressing intrusion event with implications for multiple industries and network operators. The ubiquity of SolarWinds in large networks, combined with the potentially long dwell time of intrusions facilitated by this compromise, mean victims of this campaign need not only recover their SolarWinds instance, but may need to perform widespread password resets, device recovery, and similar restoration activity to completely evict an intruder.

While this is concerning and unfortunate for the present circumstances, future supply chain attacks—as this will not be the last such incident to impact network defenders and operators—can be met with and detected by aggressive NSM and communication visibility. So long as even the most complex backdoor or implant requires communication to or instructions from a controlling entity, defenders have opportunities to detect and disrupt operations. Through continuous monitoring of network traffic and an understanding of what hosts are communicating, defenders can leverage attacker weaknesses and dependencies to overcome these otherwise daunting challenges.

Read our next blog in series on the SolarWinds Supply Chain Incident.

Read More