Trend data on the SolarWinds Orion compromise

By Malavika Balachandran TadeuszJesse Kipp

Published: 2020-12-16 · Archived: 2026-04-06 00:12:21 UTC

2020-12-16

2 min read

On Sunday, December 13, FireEye released a report on a sophisticated supply chain attack leveraging SolarWinds' Orion IT monitoring software. The malware was distributed as part of regular updates to Orion and had a valid digital signature.

One of the notable features of the malware is the way it hides its network traffic using a multi-staged approach. First, the malware determines its command and control (C2) server using a domain generation algorithm (DGA) to construct and resolve a subdomain of avsvmcloud[.]com.

These algorithmically generated strings are added as a subdomain of one of the following domain names to create a new fully-qualified domain name to resolve:

```
.appsync-api[.]eu-west-1[.]avsvmcloud[.]com.appsync-api[.]us-west-2[.]avsvmcloud[.]com.appsync-api[.]us-east-1[.]avsvmcloud[.]com.appsync-api[.]us-east-2[.]avsvmcloud[.]com
```

An example of such a domain name might look like: `hig4gcdkgjkrt24v6isue7ax09nksd[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com`

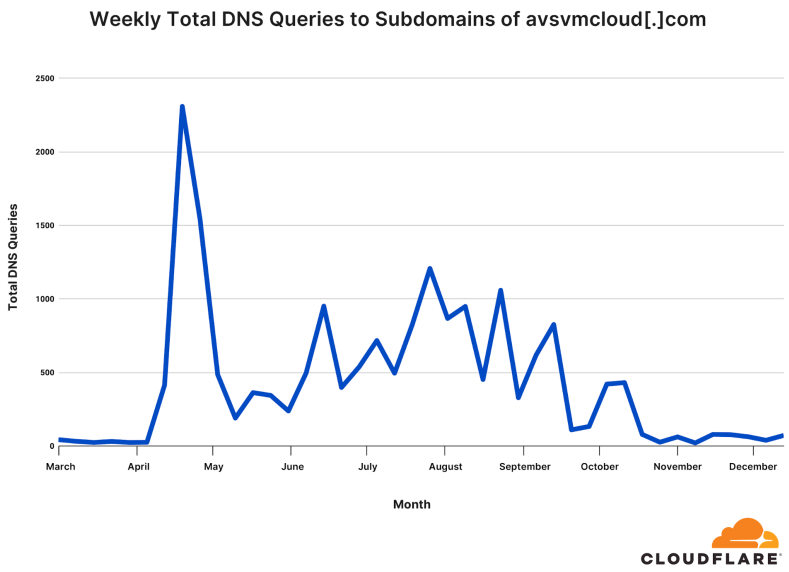
The DNS query response to a subdomain of one of the above will return a CNAME record that points to another C2 domain, which is used for data exfiltration. The following subdomains were identified as the C2 domains used for data exfiltration:

```
freescanonline[.]comdeftsecurity[.]comthedoccloud[.]comwebsitetheme[.]comhighdatabase[.]comincomeupdate[.]comdatabasegalore[.]companhard
```

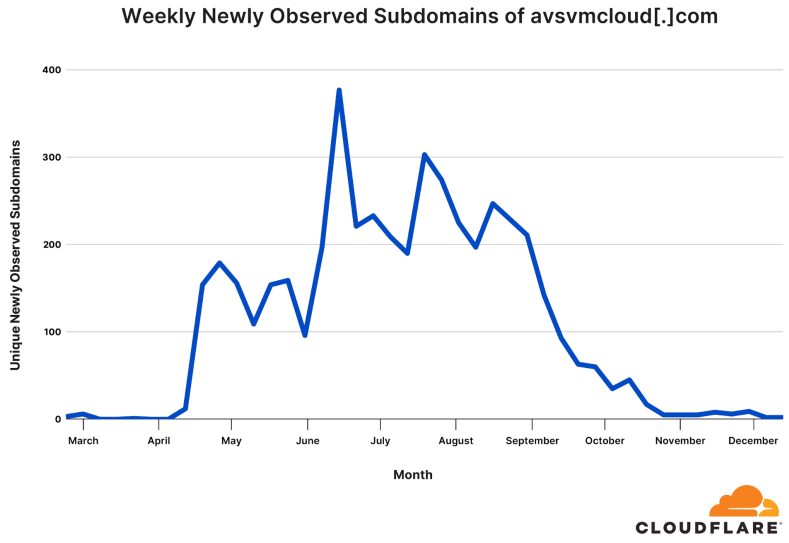
Malware activity seen on Cloudflare’s public DNS resolver 1.1.1.1

Using the published details about the network observables of the malware, we analyzed DNS query traffic to the identified malicious hostnames. Because 1.1.1.1 has a strong, audited privacy policy, we are unable to identify the source IP of users connecting to the malicious hostname — we can only see aggregated trends.

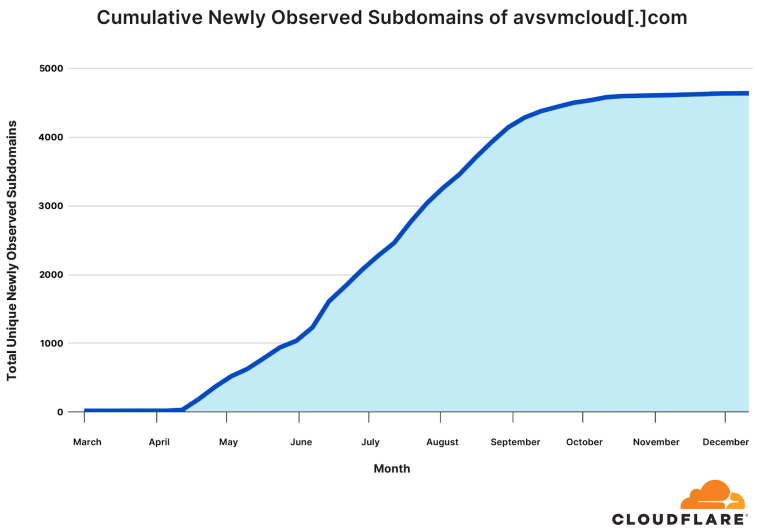
We first noticed a spike in DNS traffic through Cloudflare’s 1.1.1.1 resolver to avsvmcloud[.]com starting in April 2020:



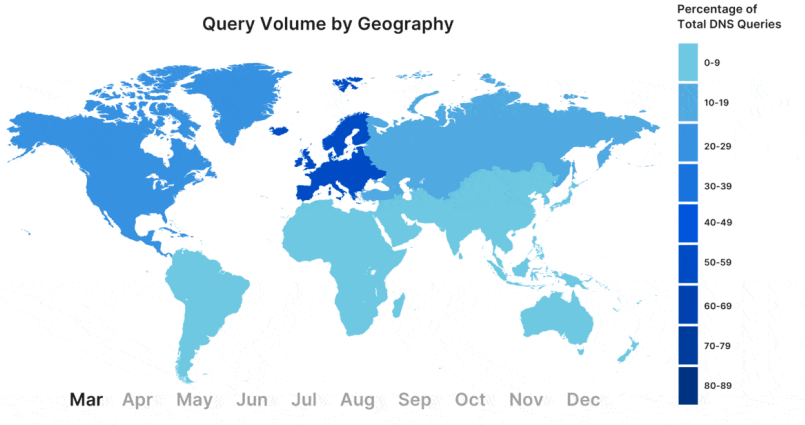
Reviewing the subdomain data, a specific pattern of DGA domains emerged as early as April. These subdomains followed a format, (e.g. {dga-string}[.]appsync-api[.]{region}[.]avsvmcloud[.]com). As time went on, the attackers added more unique subdomains. The graph below depicts the unique newly observed subdomains of avsvmcloud[.]com on a weekly basis.



As illustrated in the graphs, we noticed a major rise in activity over the summer, with total subdomains observed reaching steady state in September.



While the growth of unique names slowed down starting in October, the geographic distribution continued to change during the entire course of the attack. During the first few weeks of the attack, queries originated almost entirely from clients in North America and Europe. In May, the source of queries began to spread across the globe. By July, the queries began to cluster again, this time in South America, before returning to originate primarily from North America in November.



Protecting our customers from malicious activity

Cloudflare's 1.1.1.1 resolver has strict privacy protections, so we can only see trends of this attack. We cannot notify users that they might be compromised, because we intentionally do not know who those users are. For customers of Cloudflare Gateway, however, we can help them block these types of threats, and identify cases where they might be compromised.

Cloudflare Gateway consists of features that secure how users and devices connect to the Internet. Gateway's DNS filtering feature is built on the same technology that powers 1.1.1.1, and adds security filtering and logging.

Following the FireEye report, Cloudflare blocked access to the C2 domains used in this attack for customers using the "Malware" category in Gateway, as well as for customers using 1.1.1.1 for Families (1.1.1.2 & 1.1.1.3).

Our response team is working with customers to search logs for queries related to the malicious domains. Gateway customers can also download logs of their DNS query traffic and investigate on their own.

Cloudflare's connectivity cloud protects entire corporate networks, helps customers build Internet-scale applications efficiently, accelerates any website or Internet application, wards off DDoS attacks, keeps hackers at bay, and can help you on your journey to Zero Trust.

Visit 1.1.1.1 from any device to get started with our free app that makes your Internet faster and safer.

To learn more about our mission to help build a better Internet, start here. If you're looking for a new career direction, check out our open positions.

Cloudflare Zero TrustCloudflare GatewayZero TrustSecurityTrendsThreat Intelligence

Related posts

March 30, 2026 6:00 AM

Cloudflare Client-Side Security: smarter detection, now open to everyone

We are opening our advanced Client-Side Security tools to all users, featuring a new cascading AI detection system. By combining graph neural networks and LLMs, we've reduced false positives by up to 200x while catching sophisticated zero-day exploits....

By

-
-

March 12, 2026 5:00 AM

Announcing Cloudflare Account Abuse Protection: prevent fraudulent attacks from bots and humans

Blocking bots isn’t enough anymore. Cloudflare’s new fraud prevention capabilities — now available in Early Access — help stop account abuse before it starts....

By

-

March 12, 2026 5:00 AM

Announcing Cloudflare Account Abuse Protection: prevent fraudulent attacks from bots and humans

Blocking bots isn’t enough anymore. Cloudflare’s new fraud prevention capabilities — now available in Early Access — help stop account abuse before it starts....

By

-

March 11, 2026 1:00 PM

AI Security for Apps is now generally available

Cloudflare AI Security for Apps is now generally available, providing a security layer to discover and protect AI-powered applications, regardless of the model or hosting provider. We are also making AI discovery free for all plans, to help teams find and secure shadow AI deployments....

By

-
-
-
