Mapping Suspected KEYPLUG Infrastructure: TLS Certificates, GhostWolf, and RedGolf/APT41 Activity

Update: Changes in 'Support_1024' Certificate Field

Since our initial analysis, the 'Support_1024' field, which previously stood out in KeyPlug-related activity, has now been incorporated into WolfSSL's standard server PEM file (server.pem) published on GitHub. As a result, certificate-based detection methods that relied on this field are no longer a reliable indicator of KeyPlug infrastructure.However, we are continuing to track GhostWolf activity using additional methods beyond TLS certificate indicators, ensuring that our detection remains robust despite this change.

Tracking the infrastructure threat actors use is essential in identifying their operations, past and present, and gaining insights into their operational preferences. Defenders and researchers can trace attacks and anticipate future activity by analyzing the digital breadcrumbs left behind on servers, such as TLS certificates and server configurations.

In March 2023, Recorded Future's Insikt Group published a report detailing a cluster of network infrastructure associated with KEYPLUG, which they attributed to a suspected Chinese state-sponsored actor tracked by the company as RedGolf. The group is also referred to as APT41, BARIUM, and Earth Baku, among other aliases. Insikt Group uses the designation "GhostWolf" to describe this particular infrastructure set.

Building on these findings, we examined the IP addresses in the report's IoC section to identify pivots and uncover evidence of ongoing activity. Our research revealed overlaps with recently reported operations, including KEYPLUG activity targeting Italian organizations in mid-2024. This post will shed light on how looking into historical TLS certificates can uncover renewed activity by the original threat actor or attempts by another group seeking to imitate their operations.

Historical Context and the Anomaly

Our starting point in researching this activity relied on the IoC section of the report mentioned above. which listed 39 IPs associated with the GhostWolf infrastructure. We queried each IP in the Hunt app to identify commonalities that would aid in tracking more recent servers. One key data point surfaced again and again: the presence of a wolfSSL certificate found under the SSL History tab.

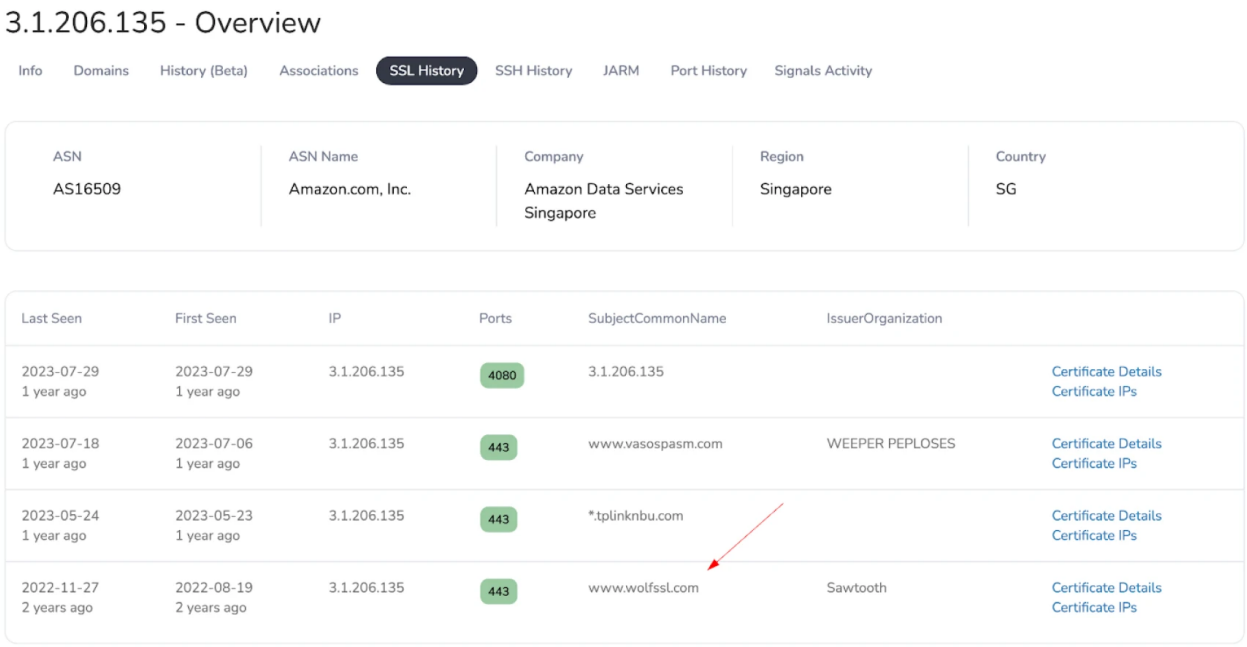

Figure 1: The certificate that started our research into this infrastructure. (Hunt)

wolfSSL is a lightweight, open-source SSL/TLS library designed for secure communications, particularly in embedded systems and RTOS environments. The certificate identified as belonging to the GhostWolf cluster closely mirrors the example certificates provided on the wolfSSL GitHub repository. Specifically, the server administrator opted for the 1024-bit version, although larger key sizes like 2048-bit are also available.

The example certificate hosted in the repo is displayed below.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            59:52:6b:92:1a:25:8f:1b:ee:4c:51:9c:47:2f:ff:ff:9d:43:29:47
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = Montana, L = Bozeman, O = Sawtooth, OU = Consulting_1024, CN = www.wolfssl.com, emailAddress = info@wolfssl.com
        Validity
            Not Before: Dec 18 21:25:29 2024 GMT
            Not After : Sep 14 21:25:29 2027 GMT
        Subject: C = US, ST = Montana, L = Bozeman, O = Sawtooth, OU = Consulting_1024, CN = www.wolfssl.com, emailAddress = info@wolfssl.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:cd:ac:dd:47:ec:be:b7:24:c3:63:1b:54:98:79:
                    e1:c7:31:16:59:d6:9d:77:9d:8d:e2:8b:ed:04:17:
                    b2:c6:eb:e4:9b:91:be:31:50:62:97:58:b5:7f:29:
                    de:b3:71:24:0b:bf:97:09:7f:26:dc:2d:ec:a8:2e:
                    b2:64:2b:7a:2b:35:19:2d:a2:80:cb:99:fd:94:71:
                    1b:23:8d:54:db:2e:62:8d:81:08:2d:f4:24:72:27:
                    6c:f9:c9:8e:db:4c:75:ba:9b:01:f8:3f:18:f4:e6:
                    7f:fb:57:94:92:cc:88:c4:b4:00:c2:aa:d4:e5:88:
                    18:b3:11:2f:73:c0:d6:29:09
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                D3:22:8F:28:2C:E0:05:EE:D3:ED:C3:71:3D:C9:B2:36:3A:1D:BF:A8
            X509v3 Authority Key Identifier:
                keyid:D3:22:8F:28:2C:E0:05:EE:D3:ED:C3:71:3D:C9:B2:36:3A:1D:BF:A8
                DirName:/C=US/ST=Montana/L=Bozeman/O=Sawtooth/OU=Consulting_1024/CN=www.wolfssl.com/emailAddress=info@wolfssl.com
                serial:59:52:6B:92:1A:25:8F:1B:EE:4C:51:9C:47:2F:FF:FF:9D:43:29:47
            X509v3 Basic Constraints:
                CA:TRUE
```

Figure 2: Snippet of ca-cert.pem for the wolfSSL library. (GitHub)

If you look too quickly, you may think the fields of the malicious certificate are identical to those in the above screenshot. However, a subtle but critical difference in the Organizational Unit (OU) fields is visible upon closer inspection. The legitimate example certificate uses "Consulting_1024" for both the Issuer and Subject, while the servers found by Insikt Group change this field to "**Support_1024**."

NotBefore	2021-02-10 19:49:53
NotAfter	2023-11-07 19:49:53
SubjectKeyId	efbfbd3c35efbfbd740e23efbfbd29efbfbd09efbfbd16efbfbd7c
SubjectCommonName	www.wolfssl.com
SubjectCountry	US
SubjectOrganization	wolfSSL
SubjectOrganizationalUnit	Support_1024
SubjectLocality	Bozeman
SubjectProvince	Montana
SubjectStreetAddress	
SubjectPostalCode	
SubjectSubjectSerialNumber	
IssuerCommonName	www.wolfssl.com
IssuerCountry	US
IssuerOrganization	Sawtooth
IssuerOrganizationalUnit	Consulting_1024
IssuerLocality	Bozeman
IssuerProvince	Montana
IssuerStreetAddress	
IssuerPostalCode	
IssuerSubjectSerialNumber	
PolicyIdentifiers	
SignatureAlgorithm	SHA256-RSA

Figure 3: "Support_1024" OU field differentiating from the example certificate. (Hunt)

This small configuration change not only modifies the certificate's original SHA-256 hash but also produces a distinct JA4X fingerprint. As we'll discuss in the next section, these characteristics, combined

with other indicators, allow us to identify newly deployed servers while filtering out those associated with the legitimate testing certificate.

Leveraging Hunt for TLS Certificate Analysis

Now that we've explored the GhostWolf infrastructure and the unique certificate configuration that led to our findings let's examine how Hunt's SSL History tools--specifically "Certificate IPs"--enable a deeper understanding of related servers and help build our search queries.

Pivoting With Certificate IPs

Revising the initial screenshot, users can click the **Certificate IPs** button next to a certificate of their choice to view a detailed history. For example, the certificate in question with SHA-256 hash **4C1BAA3ABB774B4C649C87417ACAA4396EBA40E5028B43FADE4C685A405CC3BF** is currently associated with `122` IP addresses according to our scan data.

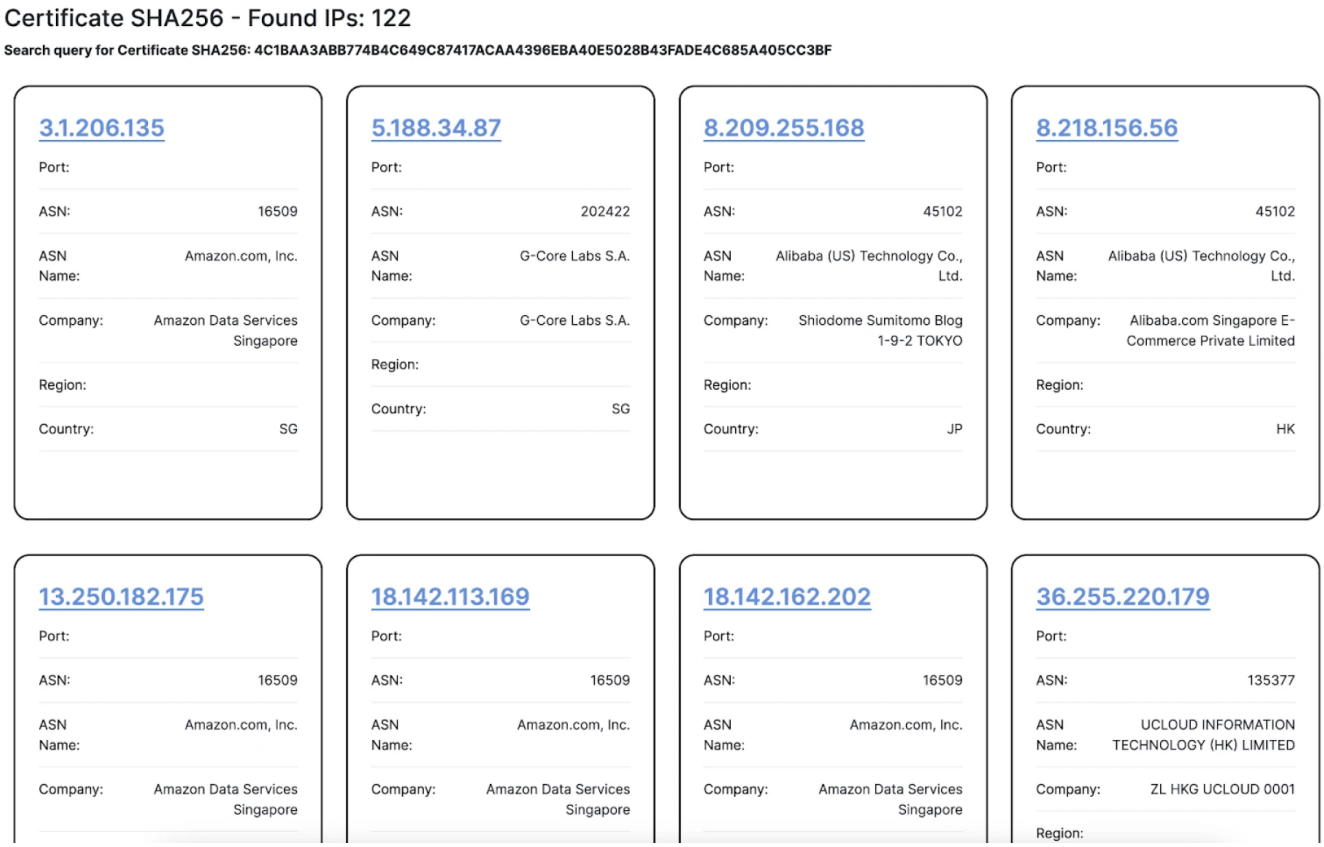

Figure 4: Snippet of the returned IPs sharing the same suspicious certificate. (Hunt)

The historical data includes many IPs from the RedGolf report, confirming that this hash is likely linked to the reported KEYPLUG activity and validating our approach to tracking this infrastructure.

If you haven't already, we highly recommend reading the entire PDF produced by the Insikt Group to learn additional insights into hosting provider preferences and server locations.

We won't be analyzing all 122 results here. Instead, later in this post, we will focus on the most recent IPs returned from our query, along with a small group of closely assigned servers overlapping with an indicator noted in Yoroi's 2024 blog post.

JA4X Fingerprints

When creating queries to search for adversary infrastructure, relying on a single data point is insufficient and a waste of time. To further refine the returned results, we'll turn to JA4X, integrated within the Hunt app on the certificate data page.

If you're unfamiliar with JA4X, it's part of the JA4+ suite and an extension of the JA3 TLS fingerprinting method, designed to create more precise fingerprints by including additional metadata. This enhancement improves the detection of malicious or anomalous connections.

Examining the data for this certificate, we found that only **41** servers shared the JA4X fingerprint `c9d784bbb12e_c9d784bbb12e_83900cc62ac7`. This suggests a significant degree of similarity in how these servers are configured or managed, indicating they are under the control of the same threat actor.

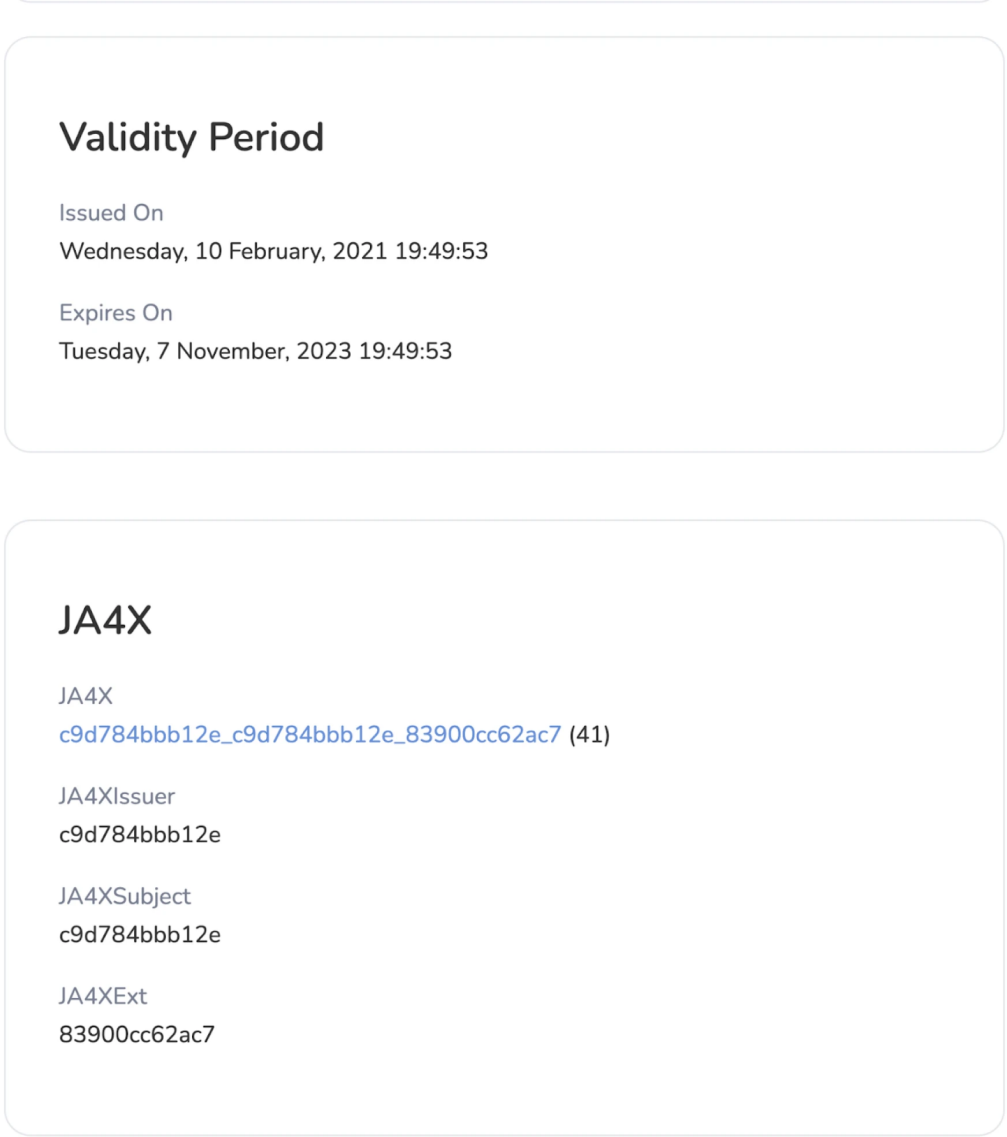

Figure 5: Screenshot of the JA4X fingerprint and issued/expired dates. (Hunt)

At this point, we have identified multiple unique indicators tied to the certificate, including:

- The anomalous **OU field**: `Support_1024`.
- The **SHA-256 hash** of the certificate.
- The **JA4X fingerprint**: `c9d784bbb12e_c9d784bbb12e_83900cc62ac7`.

The more precise and targeted our query is, the more effectively we can narrow down results to a manageable set for further investigation. In the next section, we'll use Hunt's Advanced Search feature to see how many servers are still active.

Ongoing Activity

With all the necessary data points identified, we can now craft a search query to pinpoint likely GhostWolf servers that are still active. Given that we have both a JA4X fingerprint and an SHA-256 hash, we'll use JA4X for this search, as it provides more granular insights into handshake behavior, cipher suites, and other specific configuration details. Additionally, we'll include certificates with the Organizational Unit (OU) field set to Support_1024, as this appears to be a consistent marker for this cluster of IP addresses.

Using Hunt's Advanced Search feature, we crafted the following query in SQL syntax:

```
ja4x:c9d784bbb12e_c9d784bbb12e_83900cc62ac7
AND
subject.organizational_unit:"Support_1024"
```

The above resulted in just six IP addresses, with the earliest detection by our network scans dating back to 2023.

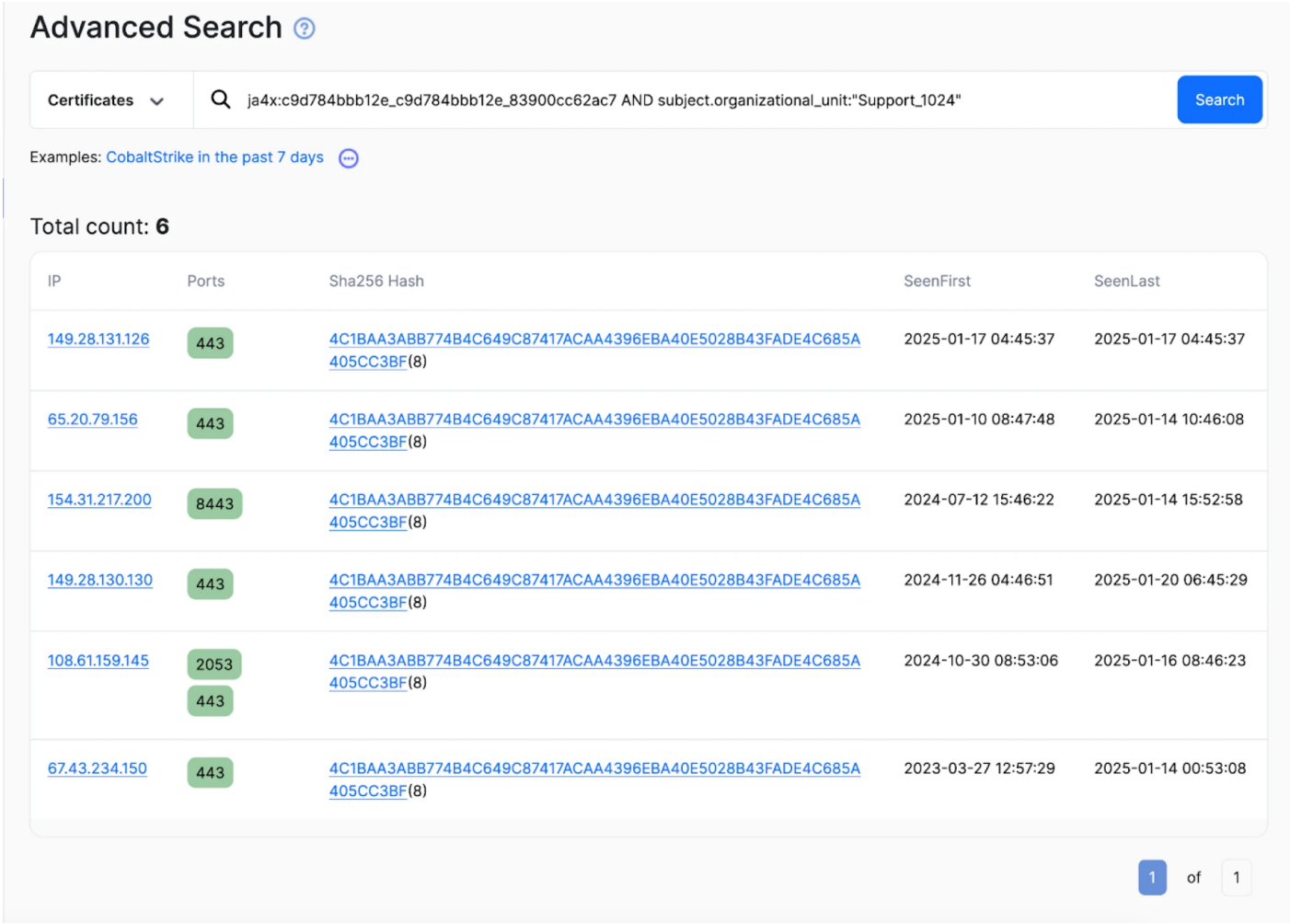

Figure 6: Advanced Search results in Hunt for the Support_1024 certificate.

Recent Activity and Observations

A few of the servers in the above figure were deployed within the past week, while others have remained active for varying durations. Port 443, usually HTTPS, is the most popular.

Public reporting on KEYPLUG highlights its support for various protocols, including HTTP/S, TCP, WSS, and KCP over UDP. For the servers running on port 443, scan data revealed responses of either **TLS** or **TCPWRAPPED**. Further examination of port history indicates that some IPs also hosted WebSocket or raw TCP servers during overlapping periods.

Hosted on port 8443 of ``154.31.217[.]200```, is what we believe (thanks to discussions with friends of Hunt) to be an HTTPS-based KEYPLUG C2 server that we have been tracking for some time.

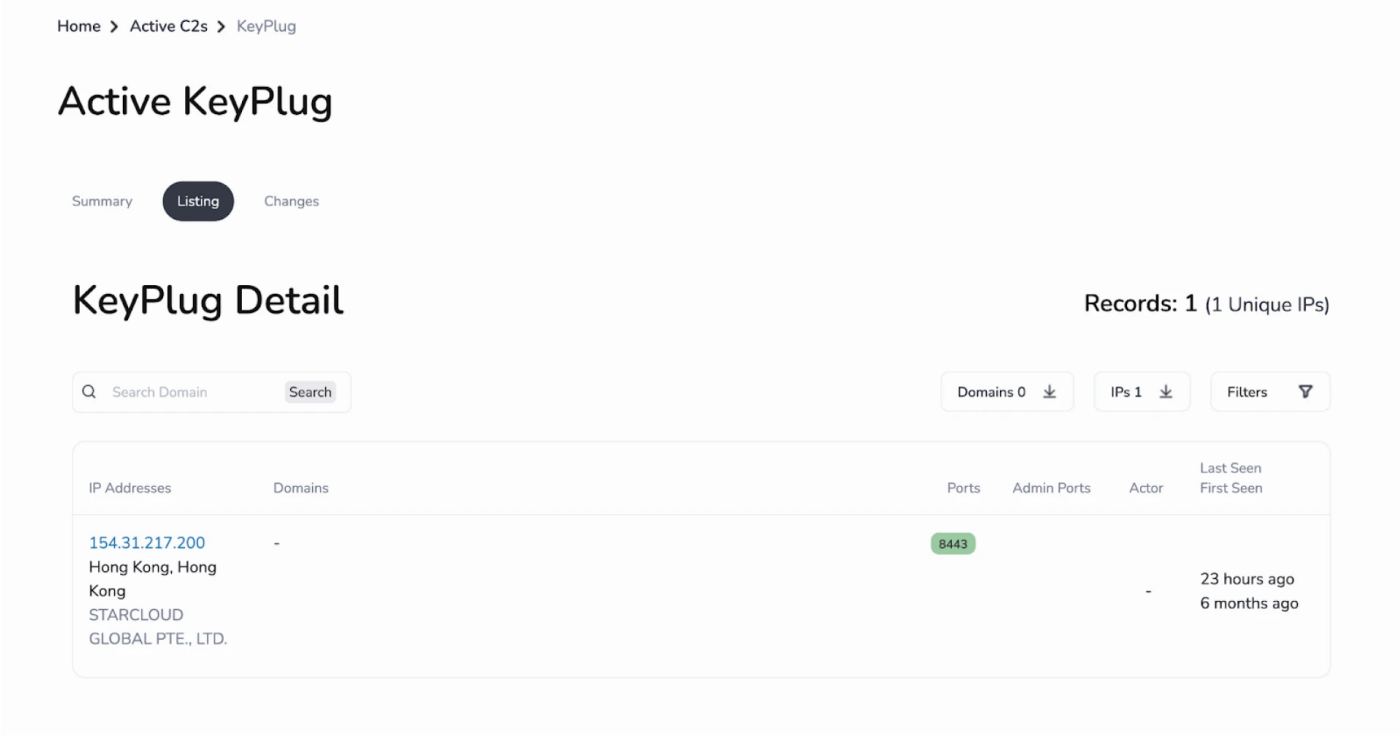

Figure 7: Screenshot of Hunt Active C2s page for KEYPLUG.

Table 1 below depicts the hosting provider and geolocation information for the six IPs identified in our query:

IP Address	Hosting Provider	Location
149.28.131[.]126	The Constant Company, LLC	SG
65.20.79[.]156	The Constant Company, LLC	IN
154.31.217[.]200	Nebula Global LLC	HK
149.28.130[.]130	The Constant Company, LLC	SG
108.61.159[.]145	The Constant Company, LLC	US
67.43.234[.]150	GloboTech Communications	CA

Table 1: Advanced Search results.

In May 2024, Yoroi published a blog post on a suspected APT41 intrusion into Italian organizations, noting an IoC for IP address `67.43.234[.]146:443` communicating over the QUIC protocol. This is a closely assigned server to one of the results above in Table 1, 67.43.234[.]150. Reviewing the SSL History Certificate IPs in Hunt revealed two additional adjacent IPs- `67.43.234[.]147` and `67.43.234[.]148`-active from March 27, 2023, to December 23, 2024.

This pattern of connected servers assigned in close groups aligns with reporting on GhostWolf infrastructure as a common acquisition method.

While we, unfortunately, have no malware samples available to confirm direct connections between the IPs in the table and those mentioned in Yoroi's post, the overlaps and similarities to the acknowledged GhostWolf server warrant further investigation and monitoring.

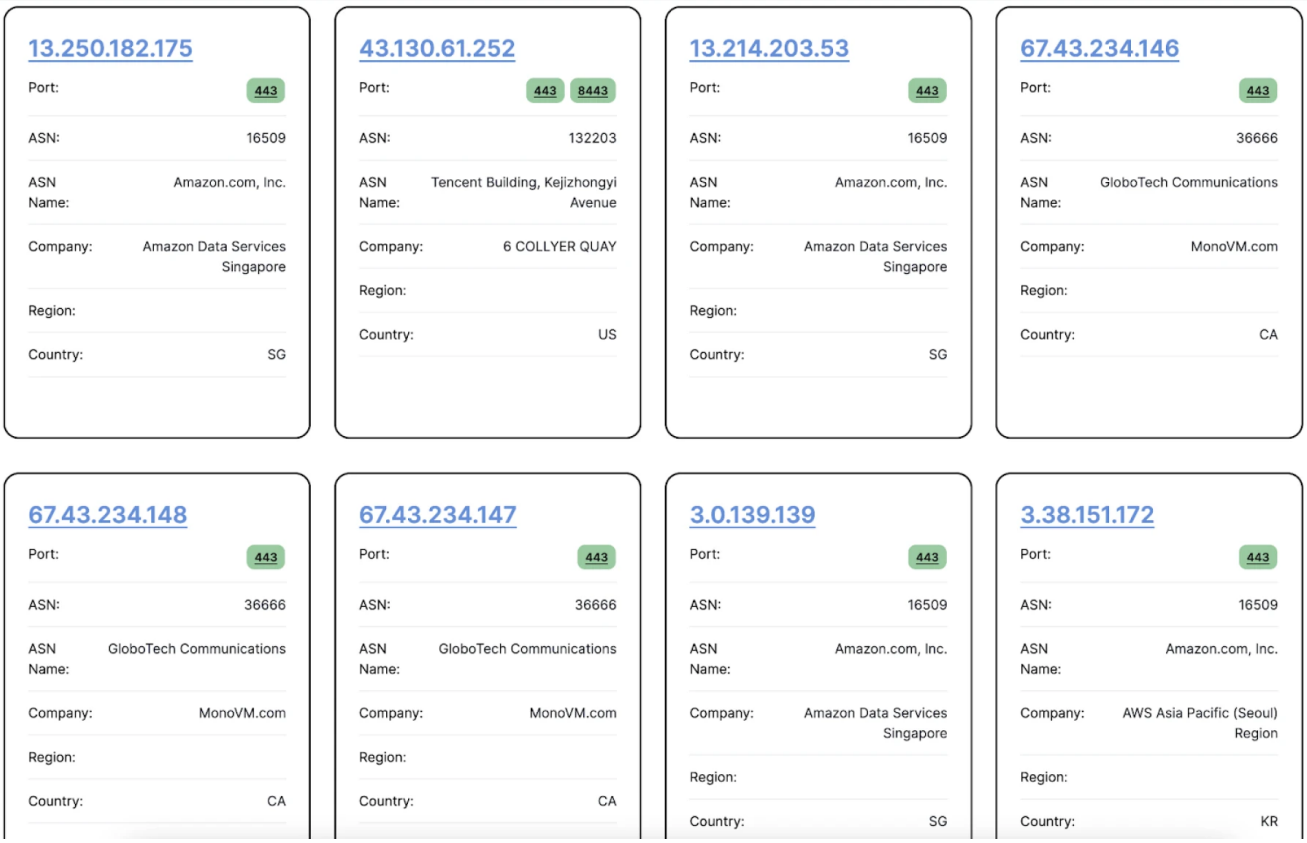

Figure 8: Screenshot of historical associations showing closely assigned IP addresses overlapping with previous reporting. (Hunt)

A GhostWolf Variant?

While investigating additional servers associated with the JA4X fingerprint, we identified another certificate (SHA-256 Fingerprint: `3d4a60efbfbd4d3eefbfbd62efbfbd0d51efbfbd53efbfbd1a6731efbfbd7fefbfbd1174efbfbd`) on `114.55.6[.]216`, which remains active at the time of writing. Unlike the other certificates using Support_1024, this one resembles the example certificate on the wolfSSL GitHub repo. However, the Issued On date and time are identical to our findings above, suggesting a possible connection.

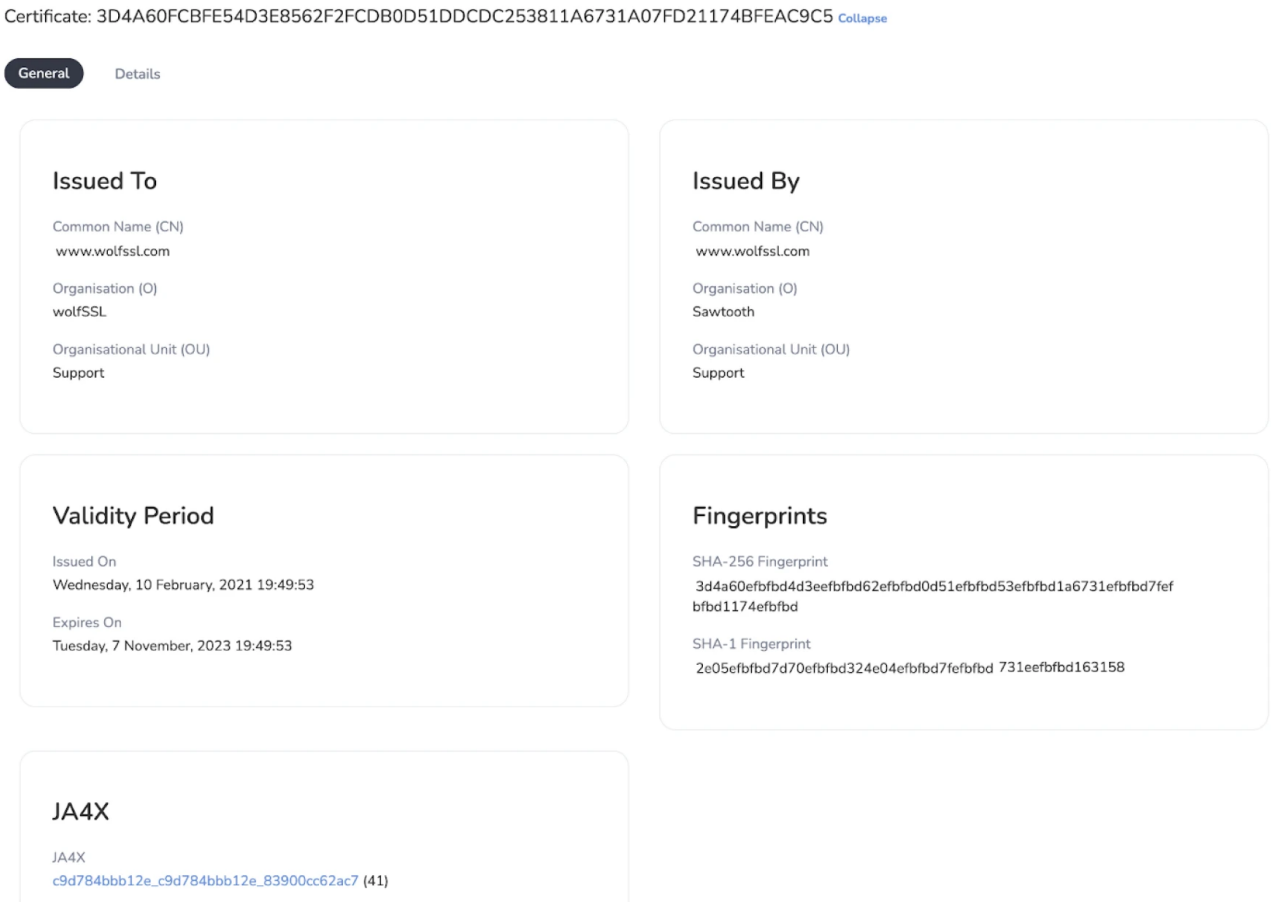

Figure 9: Screenshot of certificate data showing Issued On overlaps with previous findings. (Hunt)

Although we cannot conclusively link this server to RedGolf activity, its hosting provider, geographic location (Aliyun Computing Co., LTD, CN), and observed port usage align with previously reported command and control infrastructure.

As we've seen throughout this blog post, analysis of TLS certificates, no matter how old, and their associated fingerprints can reveal potential connections worth investigating. Below, we'll summarize our findings and outline key takeaways for continued research and defense.

Conclusion

The reuse of modified certificate and server configurations over extended periods, coupled with consistent hosting provider preferences and consecutive IP assignments, suggests the ongoing activity of this threat actor. Whether this infrastructure is tied to RedGolf/APT41 or another group with access to the certificates remains uncertain. Still, the patterns observed and the recency of new servers being spun up warrant closer attention.

The above underscores the value of tracking certificates within your environments for defenders. Recommendations include:

- Monitoring environments for certificates with unusual or suspicious fields, such as altered Organizational Unit (OU) values or unexpected issue dates.

- Incorporating TLS fingerprinting methods like the JA4+ suite into detection workflows to identify suspicious patterns in network traffic.

These basic steps can assist users in detecting suspicious infrastructure more effectively, even when threat actors attempt to blend in the noise.

Network Observables and Indicators of Compromise (IOCs)

IP Address	Hosting Provider	Location
149.28.131[.]126	The Constant Company, LLC	SG
65.20.79[.]156	The Constant Company, LLC	IN
154.31.217[.]200	Nebula Global LLC	HK
149.28.130[.]130	The Constant Company, LLC	SG
108.61.159[.]145	The Constant Company, LLC	US
67.43.234[.]150	GloboTech Communications	CA
114.55.6[.]216	Aliyun Computing Co., LTD	CN

Historical Network Observables and IOCs

IP Address	Hosting Provider	Location
18.142.162[.]202	Amazon Data Services Singapore	SG
8.209.255[.]168	Shiodome Sumitomo Blog 1-9-2 TOKYO	JP
3.1.206[.]135	Amazon Data Services Singapore	SG
8.218.156[.]56	Alibaba.com Singapore E-Commerce Private Limited	HK
47.92.204[.]81	Aliyun Computing Co., LTD	CN
43.201.51[.]16	Amazon.com, Inc.	KR
45.137.10[.]37	XNNET LLC	HK
103.226.155[.]96	Shenzhen Katherine Heng Technology Information Co., Ltd.	HK
103.234.96[.]167	Shenzhen Katherine Heng Technology Information Co., Ltd.	HK
173.209.62[.]186	MonoVM.com	CA
173.209.62[.]188	MonoVM.com	CA
173.209.62[.]189	MonoVM.com	CA
173.209.62[.]190	MonoVM.com	CA
202.79.173[.]220	CTG Server Ltd.	HK
202.79.173[.]228	CTG Server Ltd.	HK
209.141.36[.]195	BuyVM Services	US
36.255.220[.]179	ZL HKG UCLOUD 0001	HK
13.250.182[.]175	Amazon Data Services Singapore	SG
18.142.113[.]169	Amazon Data Services Singapore	SG
5.188.34[.]87	G-Core Labs S.A.	SG
38.55.24[.]53	KURUN CLOUD INC	US
202.79.173[.]211	CTG Server Ltd.	HK
39.106.32[.]186	Aliyun Computing Co., LTD	CN
8.213.131[.]120	Alibaba.com Singapore E-Commerce Private Limited	KR
209.141.36[.]195	BuyVM Services	US
18.143.183[.]217	Amazon Data Services Singapore	SG

IP Address	Hosting Provider	Location
18.163.6[.]115	Amazon Data Services Hong Kong	HK
54.151.200[.]128	Amazon Data Services Singapore	SG
13.214.160[.]122	Amazon Data Services Singapore	SG
43.130.61[.]252	6 COLLYER QUAY	US
13.214.203[.]53	Amazon Data Services Singapore	SG
3.0.139[.]139	Amazon Data Services Singapore	SG
3.38.151[.]172	AWS Asia Pacific (Seoul) Region	KR
13.209.204[.]54	AWS Asia Pacific (Seoul) Region	KR
173.209.62[.]187	MonoVM.com	CA
13.228.200[.]171	Amazon Data Services Singapore	SG
45.137.10[.]166	XNNET LLC	HK
13.124.47[.]148	AWS Asia Pacific (Seoul) Region	KR
139.180.211[.]30	SGP_VULTR_CUST	SG
8.219.191[.]81	Alibaba.com Singapore E-Commerce Private Limited	SG
51.79.177[.]23	OVH Singapore PTE. LTD	SG
88.218.192[.]22	XNNET LLC	HK
15.168.60[.]114	Amazon Data Services Osaka	JP
103.244.148[.]80	Shenzhen Katherine Heng Technology Information Co., Ltd.	HK
67.43.228[.]18	GloboTech Communications	CA
67.43.228[.]19	GloboTech Communications	CA
67.43.228[.]20	GloboTech Communications	CA
67.43.228[.]21	GloboTech Communications	CA
67.43.228[.]22	GloboTech Communications	CA
45.148.244[.]220	Perviy TSOD LLC	RU
202.182.121[.]16	TYO_VULTR_CUST	JP
154.12.87[.]168	Cogent Communications	US
13.214.172[.]25	Amazon Data Services Singapore	SG
103.226.155[.]98	Shenzhen Katherine Heng Technology Information Co., Ltd.	HK
64.176.50[.]30	The Constant Company, LLC	JP
64.176.51[.]12	The Constant Company, LLC	JP
65.20.84[.]44	Vultr Holdings LLC	IN
65.20.78[.]204	Vultr Holdings LLC	IN
47.245.60[.]81	ALICLOUD-JP	JP
8.222.243[.]185	Alibaba.com Singapore E-Commerce Private Limited	SG
139.180.153[.]109	The Constant Company, LLC	SG
139.180.213[.]58	The Constant Company, LLC	SG
45.32.101[.]56	The Constant Company, LLC	SG
103.146.230[.]130	Sichuan Zhonghe Network Technology Co., Ltd.	HK
67.43.234[.]149	MonoVM.com	CA
103.146.230[.]165	Sichuan Zhonghe Network Technology Co., Ltd.	HK
47.245.99[.]137	Alibaba.com LLC	US
8.222.220[.]3	Alibaba.com Singapore E-Commerce Private Limited	SG
103.146.230[.]183	Sichuan Zhonghe Network Technology Co., Ltd.	HK
65.20.79[.]14	Vultr Holdings LLC	IN

IP Address	Hosting Provider	Location
158.247.234[.]25	The Constant Company, LLC	KR
205.185.121[.]28	FranTech Solutions	US
43.249.36[.]84	LeaseWeb Asia Pacific - Hong Kong	HK
66.42.49[.]65	SGP_VULTR_CUST	SG
158.247.245[.]229	The Constant Company, LLC	KR
139.180.188[.]174	SGP_VULTR_CUST	SG
65.20.70[.]52	Vultr Holdings LLC	IN
158.247.203[.]247	The Constant Company, LLC	KR
154.92.16[.]198	Guangzhou Yisu Cloud Limited	HK
207.148.71[.]45	SGP_VULTR_CUST	SG
45.76.150[.]120	Vultr Holdings, LLC	SG
158.247.253[.]114	The Constant Company, LLC	KR
139.180.145[.]193	SGP_VULTR_CUST	SG
139.180.189[.]81	SGP_VULTR_CUST	SG
64.176.83[.]46	The Constant Company, LLC	SG
158.247.251[.]91	The Constant Company, LLC	KR
45.32.125[.]90	Vultr Holdings, LLC	SG
65.20.69[.]6	Vultr Holdings, LLC	IN
45.77.34[.]88	Vultr Holdings, LLC	SG
65.20.78[.]223	Vultr Holdings, LLC	IN
139.84.175[.]197	The Constant Company, LLC	IN
111.180.200[.]74	CHINANET HUBEI PROVINCE NETWORK	CN