DarkPeony's Trail: Certificate Patterns Point to Sustained Campaign Infrastructure

Published: 2024-11-21 · Archived: 2026-04-05 15:12:16 UTC

TABLE OF CONTENTS

In a recent blog post, we discussed SSL/TLS certificates tied to suspected **PlugX** command and control (C2) nodes, which featured recurring use of 'AES' in the organizational unit field. Building on this, we've also identified two additional suspicious certificates on the same infrastructure linked to domains likely used to download or communicate with malware.

These findings, alongside domain registration patterns, align closely with the infrastructure previously reported by NTT as being associated with DarkPeony. The group's repeated use of similar certificates and servers indicates a sustained operational tempo, enabling us to track this cluster of activity consistently over time.

This post will explore these network observables and provide context to assist defenders in proactively identifying future infrastructure before it becomes operationalized.

DarkPeony?

DarkPeony is a suspected Chinese cyber-espionage group known for targeting government and military organizations. As highlighted in NTT's report, the group was observed deploying PlugX malware in its campaigns, targeting entities across Myanmar, the Philippines, Mongolia, and Serbia.

The group primarily leverages infrastructure providers in Hong Kong, with **CTG Server Ltd**. and **ChangLian Network Technology Co**. being the most frequently observed networks. NameCheap and NameSilo are used to register domains, while CloudFlare nameservers are employed, likely in an attempt to conceal activity from researchers.

The domain `buyinginfo[.]org` was listed as one of the PlugX C2 servers in the report and became our starting point for looking for similar DarkPeony infrastructure. We identified the IP address linked to the above domain as `103.107.105[.]81`. As shown in Figure 1, the server uses three certificates of importance to our research: (2) CloudFlare and (1) TrustAsia Technologies, Inc.

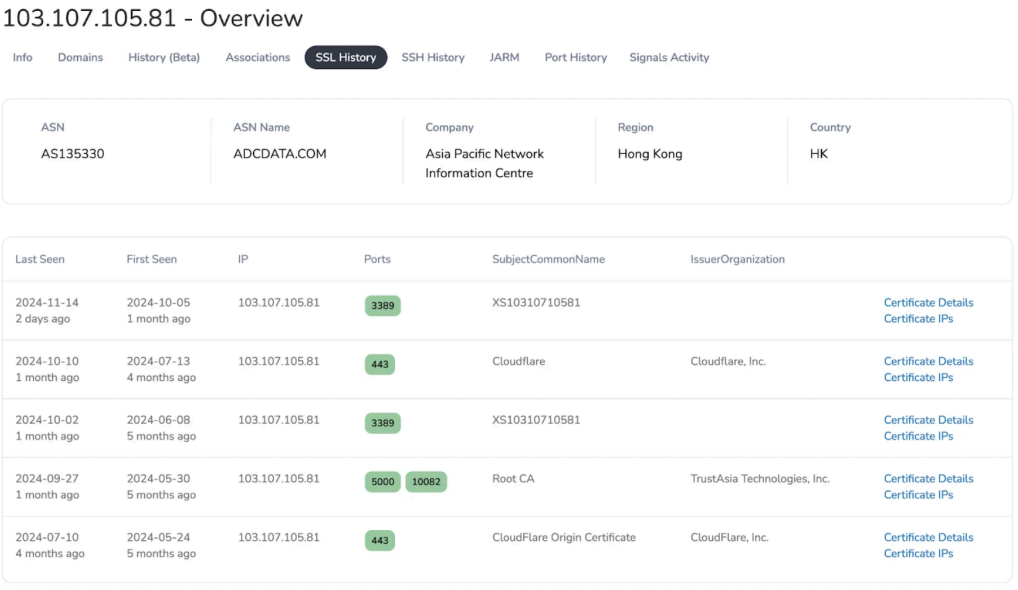

Figure 1: SSL History overview of 103.107.105.81 (Hunt).

Checking out the details for the certificate first seen on 2024-05-24, we see a DNS name of buyinginfo[.]org and the wildcard subdomain, *.buyinginfo[.]org.

IssuerOrganizationalUnit	CloudFlare Origin SSL Certificate Authority
IssuerLocality	San Francisco
IssuerProvince	California
IssuerStreetAddress	
IssuerPostalCode	
IssuerSubjectSerialNumber	
PolicyIdentifiers	
SignatureAlgorithm	SHA256-RSA
UnhandledCriticalExtensions	
UnknownExtKeyUsage	
KeyUsage	
ExtKeyUsage	['ClientAuth','ServerAuth']
PermittedDNSDomainsCritical	
PermittedDNSDomains	
PermittedEmailAddresses	
PermittedURIDomains	
PermittedIPRanges	
ExcludedDNSDomains	
ExcludedEmailAddresses	
ExcludedURIDomains	
ExcludedIPRanges	
BasicConstraintsValid	1
CRLDistributionPoints	,http://crl.cloudflare.com/origin_ca.crl,
DNSNames	*.buyinginfo.org buyinginfo.org

Figure 2: Certificate details showing the domain name from the NTT report (Hunt).

Our blog post about PlugX from last month identified a cluster of five servers suspected to be linked with PlugX activity. Each of these servers utilized a certificate featuring the letters "AES" in the Organizational Unit field, suggesting a potential marker for the infrastructure used by this actor.

Please revisit the prior post for a more detailed examination and the Advanced Search query used. Figure 3 below shows the results of running the query at that time.

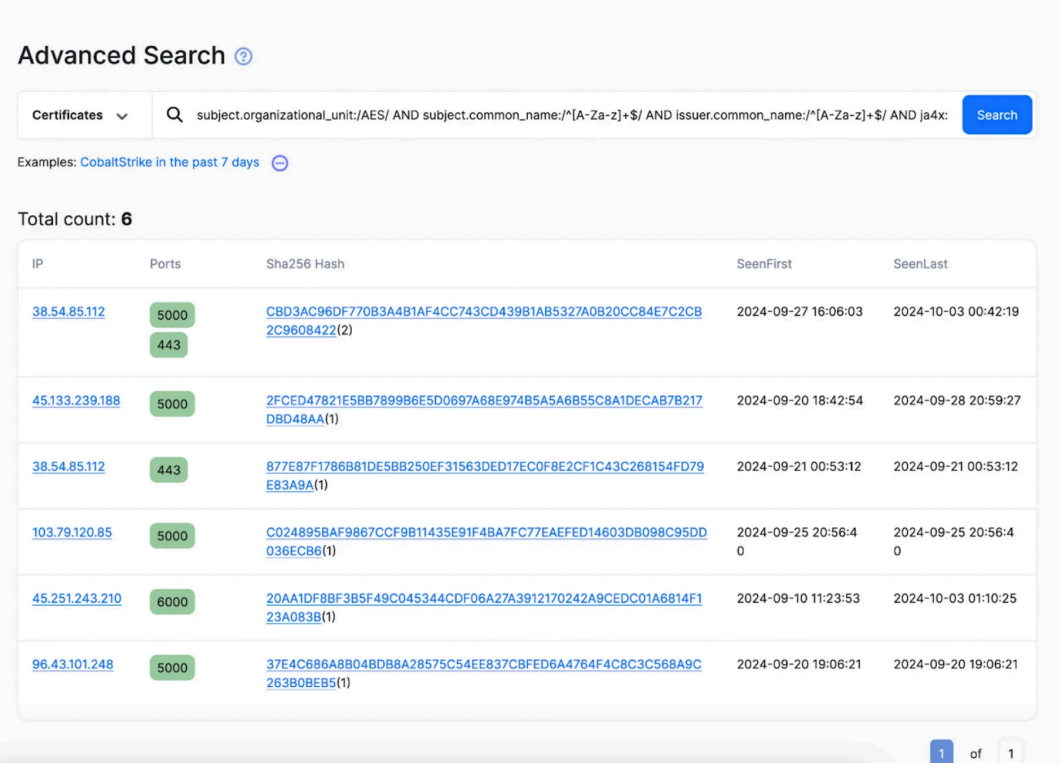

Figure 3: Advanced Search query results for the certificates containing "*AES*."

Focusing on the certificates of `96.43.101[.]248`, we noticed a CloudFlare (CF) certificate we hadn't dug into previously. Using well-known services can greatly hinder analysis, allowing the infrastructure to blend in with benign servers.

Techniques like these have been seen in other operations, such as those targeting government mail servers. We'll touch on a probable query that will allow us to get around this temporary roadblock later.

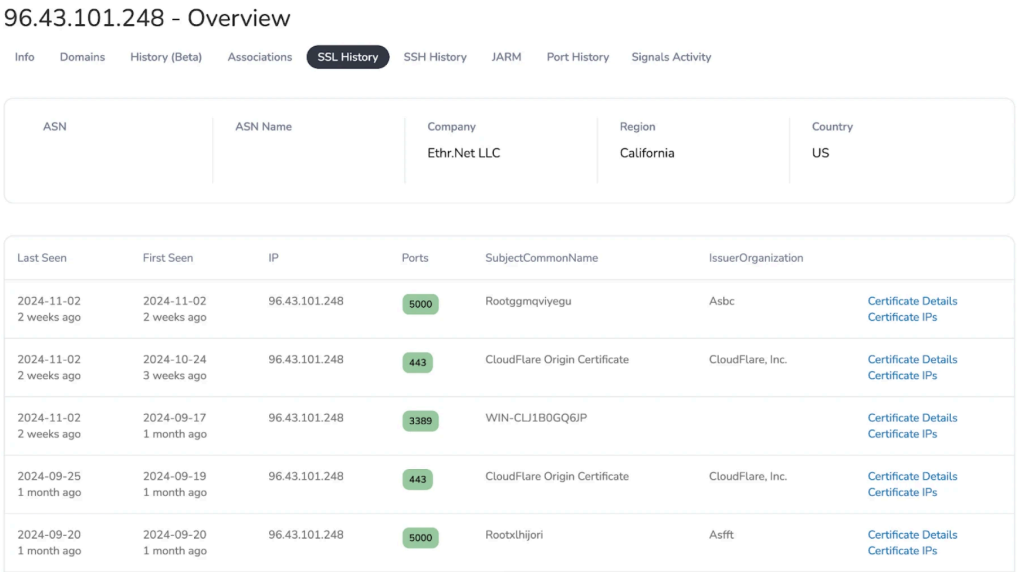

Figure 4: SSL History for the subject IP illustrates the AES and CloudFlare certs (Hunt).

Interestingly, the most recent certificate (SHA-256: **130c463eefbfbdc2b33eefbfbd18efbfbd030819e3abbc08efbfbd5342efbfbd77efbfbd01efbfbd**) from the above screenshot contains the domain name `vabercoach[.]com`.

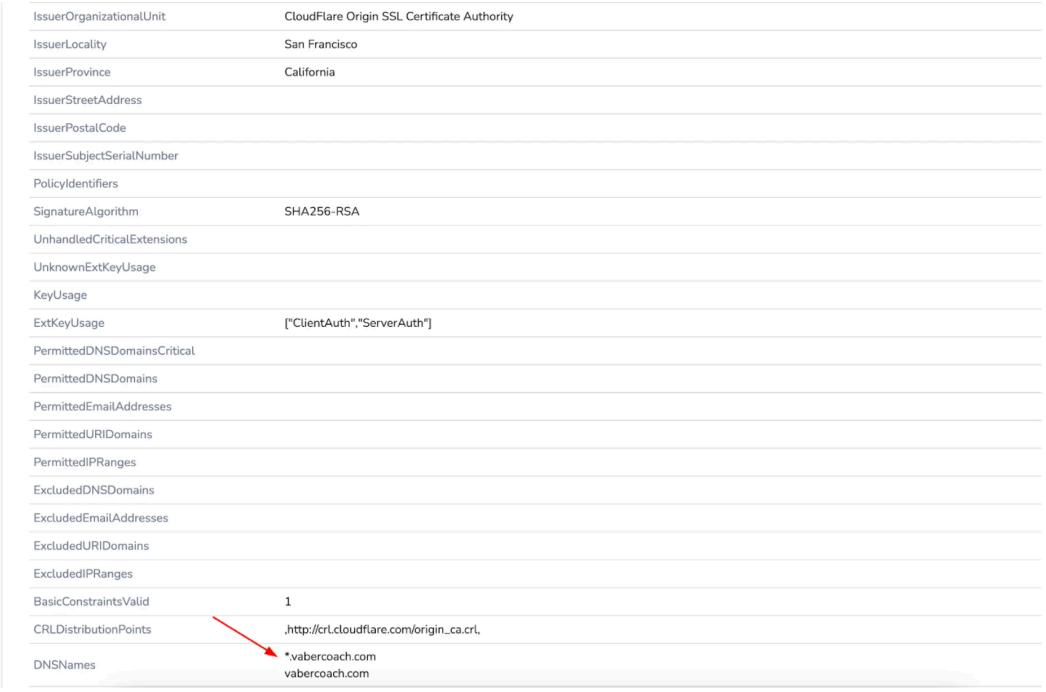

Figure 5: Certificate details for 96.43.101[.]248 (Hunt).

Clicking on the "Certificate IPs' button, we find our first pivot, a single IP address sharing this same certificate: 223.26.52[.]245.

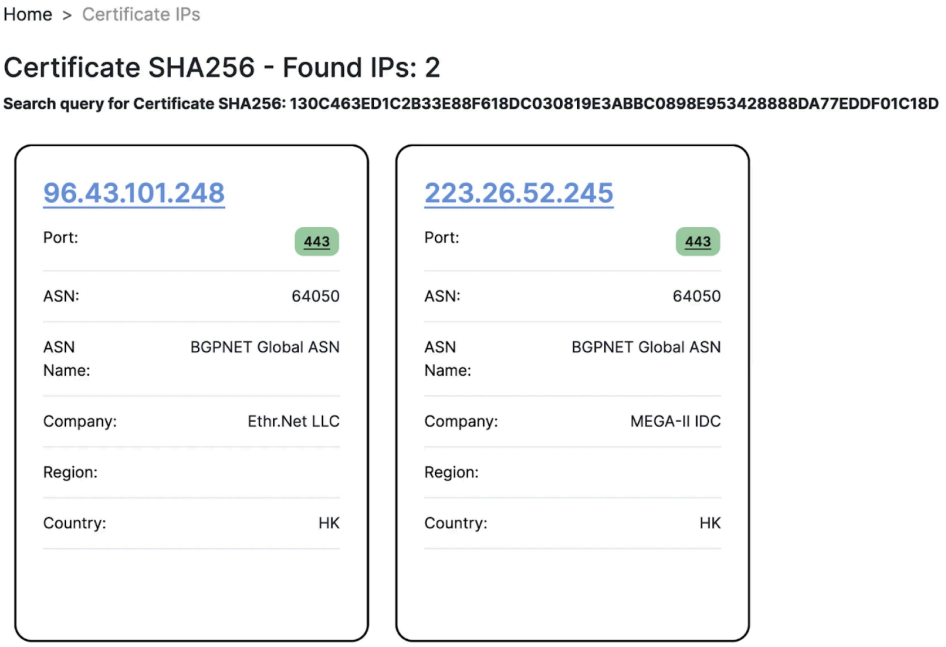

Figure 6: Screenshot of the shared certificate IPs (Hunt).

Our investigation into vabercoach[.]com led us to various sandboxes, including VirusTotal and Hatching Triage, and sources like X/Twitter, which revealed a malicious file named 'Meeting Invitation.msc' (SHA-256: **397afb74746b2fe01abc63789412b38f44ceb234a278a04b85b2bb5b4e64cc8c**) communicating with the domain.

Notably, the same file name was observed in the Operation ControlPlug campaign, as documented by NTT.

The screenshot below (Figure 7) illustrates network traffic from Hatching Triage. It shows calls to the domain's endpoint/unit and activity involving an additional domain, `loginge[.]com`.

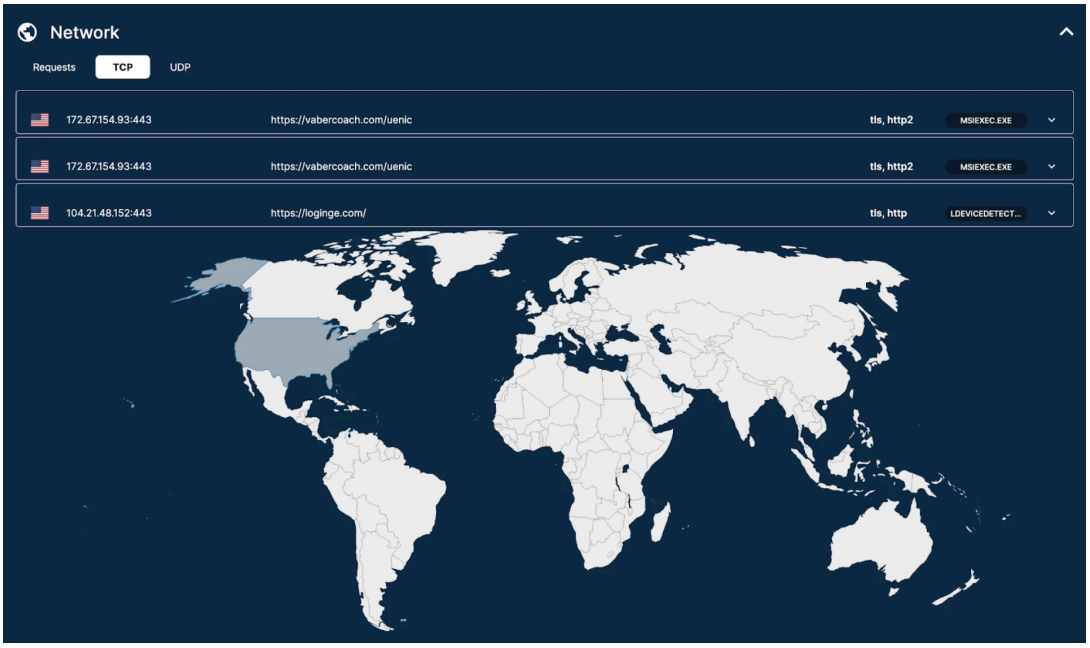

Figure 7: The network portion of the analysis of 'Meeting Invitation.msc' (Triage).

Note: The domains in the above figure resolve to CloudFlare allocated network space, thus hiding the true IP address.

Before diving into the remainder of the servers linked to DarkPeony, below is a pseudo-query that may assist in identifying additional CloudFlare certificates with minimal false positives. The following criteria should serve as a starting point for analysts seeking to expand their investigation and include ASNs as they are found:

JARM Fingerprint: "2ad2ad0002ad2ad22c2ad2ad2ad2ad703dc1bf20eb9604decefea997eabff7" AND **Subject Common Name**:"CloudFlare Origin Certificate" AND **ASN**:"152194, 137443"

The above could be enhanced to include port 443, which the certificate uses almost exclusively. Keep in mind that if the actor(s) changes the port in the future, we will need to adjust accordingly.

Additional Links

We'll continue our findings by featuring the 'AES' and CloudFlare certificates and identify any domains associated with the IPs. Unfortunately, we have not found any additional malware samples communicating with or referenced by the below.

Our first server, `146.66.215[.]19` stands out as an anomaly compared to the rest of the infrastructure. This IP address is provided by Datacamp Limited, located in Great Britain. Figure 8 shows the hosted certificates.

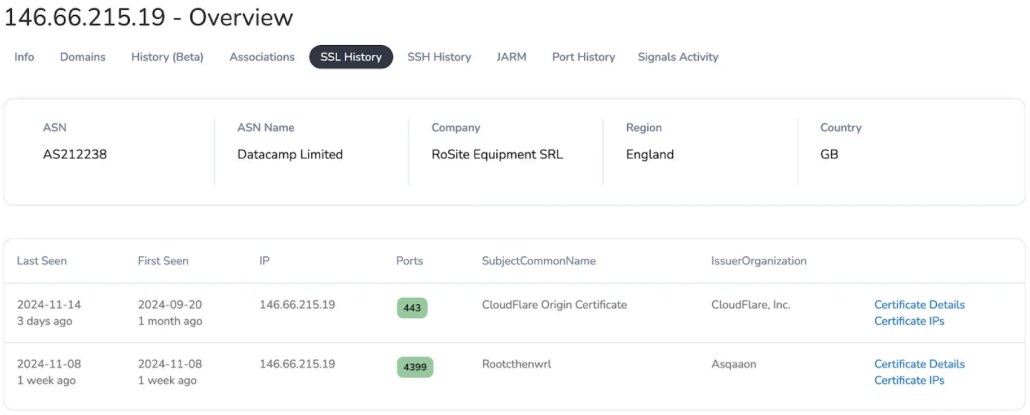

Figure 8: SSL History overview for 146.66.215[.]19 (Hunt).

`councilofwizards[.]com` is the single domain linked to this server using CloudFlare services.

45.32.105[.]184

Another server, `45.32.105[.]184`, is provided by Vultr Holdings, LLC, located in Singapore. The domain associated with this CloudFlare certificate, `thelocaltribe[.]com` follows the same patterns noted earlier in this analysis.

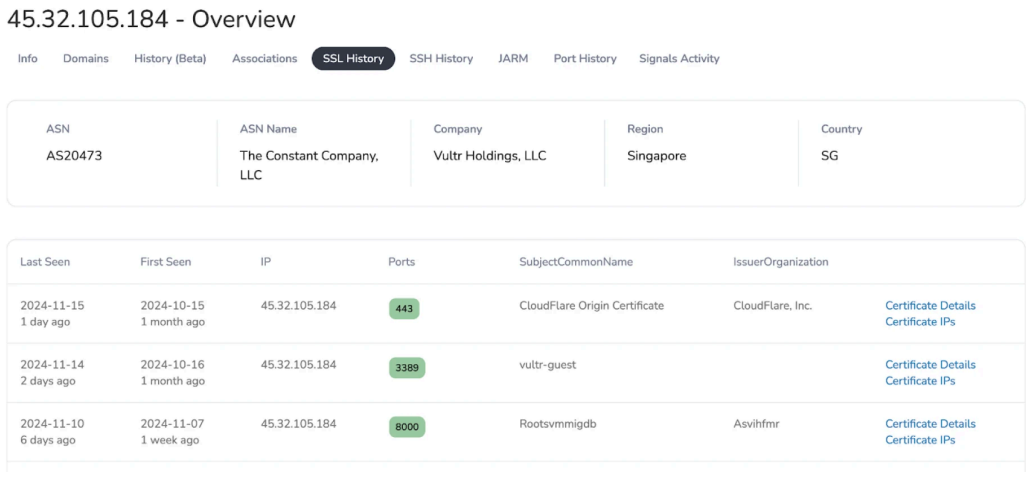

Figure 9: Screenshot of the certificate overview for 45.32.105[.]184 (Hunt).

Time For Something Different?

149.104.2[.]160

Hosted by XNNET LLC in Hong Kong, `149.104.2[.]160` presents a different characteristic. Unlike the previously mentioned servers, this IP does not use the 'AES' certificate but instead uses CloudFlare and another cert commonly reported as used by other threat actors to deploy malware like PlugX.

The certificate fields contain the following:

- **Subject Common Name**: Root CA
- **Subject Country**: US
- **Subject Organization**: TrustAsia Technologies, Inc.
- **Subject Organizational Unit**: Domain Validated SSL
- **Subject City**: Seattle
- **Subject State**: Washington.

Domain for CF cert on 149.104.2[.]160: `smldatacenter[.]com`

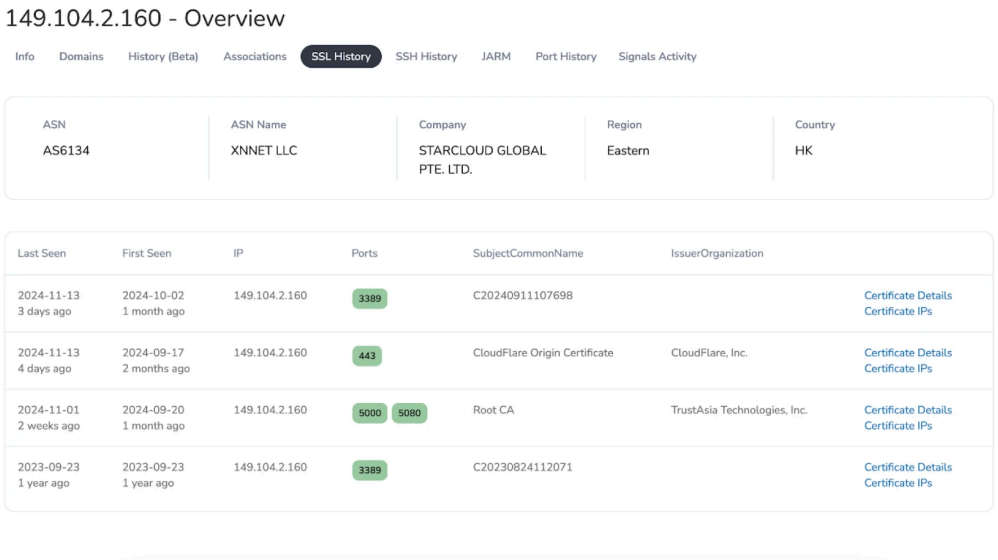

Figure 10: SSL History for 149.104.2[.]160 (Hunt).

202.91.36[.]213

Our final IP we'll cover also uses the CF and TrustAsia certificates at `202.91.36[.]213`, hosted on ChangLian Network Technology Co., Limited.

`kentscaffolders[.]com` is the domain linked to the CloudFlare cert on this server.

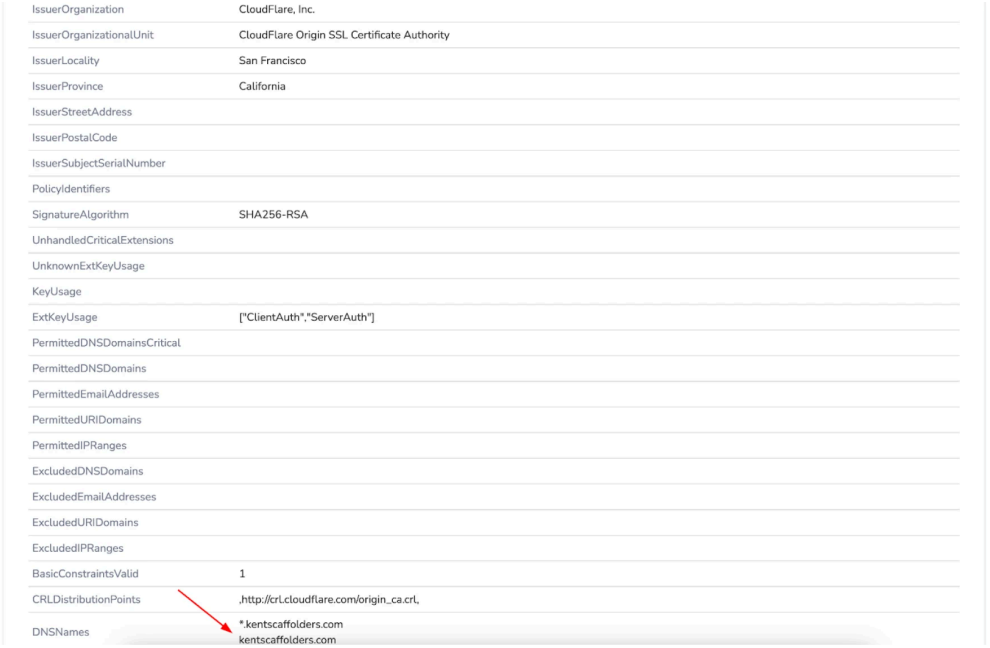

Figure 11: Certificate fields showing the kentscaffolders[.]com domain name (Hunt).

Honorable mention: Rounding out the above IPs using the CF & TrustAsia certificates is 223.26.52[.]208 on the CTG Server Limited network. The second domain seen earlier communicating with the malicious .msc file, loginge[.]com, is listed as a DNS name for the CloudFlare certificate.

Conclusion

In this post, we expanded on previously observed IPs/domains linked to DarkPeony, highlighting their continued use of certificate and domain registration practices to obfuscate malicious activity using legitimate services. The threat actor uses wildcard certificates with domains protected by CloudFlare to conceal the actual IP addresses and facilitate malware communication, effectively complicating tracking efforts.

Our focus was on the most recent IP addresses linked to this infrastructure. These elements provide valuable insights into the actor's constant operations. Security teams are encouraged to leverage these indicators to proactively hunt for emerging infrastructure as it appears, allowing for earlier detection and disruption of DarkPeony's activities.

Network Observables

IP Address	Country	ASN	Certs/Hash
103.107.105[.]81	HK	ADCDATA.COM	**CloudFlare**: 708D60B51595D2CDB313E40E9215E3857D931AC9368F308B4FC3244C75BB2 **TrustAsia**: D64C9AAA5447427AA5DEB13FF80FF1D73B8C074F1666AB452A80E0BD458
96.43.101.248	US	Ethr.Net LLC	**AES**: 994260498E6BDAD93AF7052C99CC7A894A0B9D509BCF28391399F0BBF41F **CloudFlare**: 130C463ED1C2B33E88F618DC030819E3ABBC0898E953428888DA77EDDF01
223.26.52.245	HK	CTG Server Limited	**CloudFlare**: 130C463ED1C2B33E88F618DC030819E3ABBC0898E953428888DA77EDDF01
146.66.215.19	GB	Datacamp Limited	**AES**: B9949EF3D7FED686ECAF04CC9EBEBC55FB7594C94F51E9794AB7BC4BB32 **CloudFlare**: 3BCBED98FAF9C8ADDAEDF04DBBB04D0BF457190DBC98E5548183EEEAC

IP Address	Country	ASN	Certs/Hash
45.32.105.184	SG	The Constant Company	**AES**: A0097944D47F7174231CE7A38A3C25CC51D9E9A70D5574CE04AA427EE6A3 **CloudFlare**: 05D9D2785E08FED0BD3BE97BD267CD56752381A5F032FE8D140A9A0AE54I
149.104.2.160	HK	XNNET LLC	**CloudFlare**: EEB4AE9ACC598DE874257A70941EDDA377C9EF45E7F3059C8C5D28778F87 **TrustAsia**: 2F35B0A119A7CA8204F4D158ABCDC90163B0F19F968367C685ED3A86258C4
202.91.36.213	HK	ChangLian Network Technology Co., Limited	**CloudFlare**: 6D14946DB325352CF82161B5AA1BB3442F6B980269A0CDBFEDB1311DC795 **TrustAsia**: F888DA96249AEA874229554A433EE3E5AB2483D400EF10C20FDA4118149F4
223.26.52[.]208	HK	CTG Server Limited	**CloudFlare**: 366e5abec0c2495720223e0438996ebff3d3596fd516e5a06d9c908c7c2 **TrustAsia**: 6CFB62E5FEAE0DE193B3F04B47E534A95BDE79FBE3B74E582233F341C510I

Source: https://hunt.io/blog/darkpeony-certificate-patterns