Oyster’s Trail: Resurgence of Infrastructure Linked to Ransomware and Cybercrime Actors

Published: 2024-12-12 · Archived: 2026-04-05 21:47:51 UTC

TABLE OF CONTENTS

After a period of dormancy, the Oyster backdoor--linked to threat actors such as **Vanilla Tempest**, **Vice Society**, and **Rhysida**-has recently resurfaced. Over the past week, our continuous monitoring efforts have uncovered a set of fresh domains and servers, suggesting renewed attacks may be in the works.

Findings include:

- **Registration Patterns**: Most domains are registered through NameCheap, and Let's Encrypt TLS certificates are used to protect communications.
- **Shared Hosting**: One of the IPs revealed connections to 20 additional servers sharing SSH keys, all belonging to the Global-Data System IT Corporation ASN.

In this post, we detail the observed domains and infrastructure, highlighting the links and patterns that may assist defenders in hunting for similar activity and strengthening their detection capabilities.

Oyster Backdoor Overview

Also known as Broomstick and CleanUpLoader, Oyster first appeared in July 2023. The backdoor collects host details and communicates with its command-and-control (C2) server via TLS, using encoded HTTP data to transfer information securely. Contact is established with the C2 through an initial HTTP POST request to several endpoints, usually starting with /api.

In June 2024, Rapid7 identified a malvertising campaign leveraging trojanized installers for popular software like Google Chrome and Microsoft Teams to deliver the Oyster backdoor.

In July, we outlined a method to identify Oyster infrastructure based on web pages simply containing the word "Soon." The post also lists several IOCs, including domains and a JARM fingerprint based on the Let's Encrypt certs used, plus an HTTP response hash for defenders to do their own hunting.

In October, the Insikt Group linked CleanUpLoader, a variant of the Oyster backdoor, to ITG23, a Russian cybercriminal group tracked by Recorded Future. Their analysis further details the malware's operational tactics and supporting infrastructure.

Recent Observations

Within the Hunt app, we are tracking three IP addresses detected as part of the Oyster backdoor infrastructure:

- 185.196.10[.]179 (first observed 28 Nov)
- 193.109.120[.]240 (first observed 05 Dec)
- 91.236.230[.]11 (first observed 05 Dec)

On 06 December, researchers at TRAC posted on X about two IP addresses and three domains they linked to Vanilla Tempest. According to our scans, we assess those domains resolve to 91.236.230[.]11 and 185.196.10[.]179. This overlap reinforces our findings that the infrastructure identified by both our team and TRAC is likely tied to Oyster.

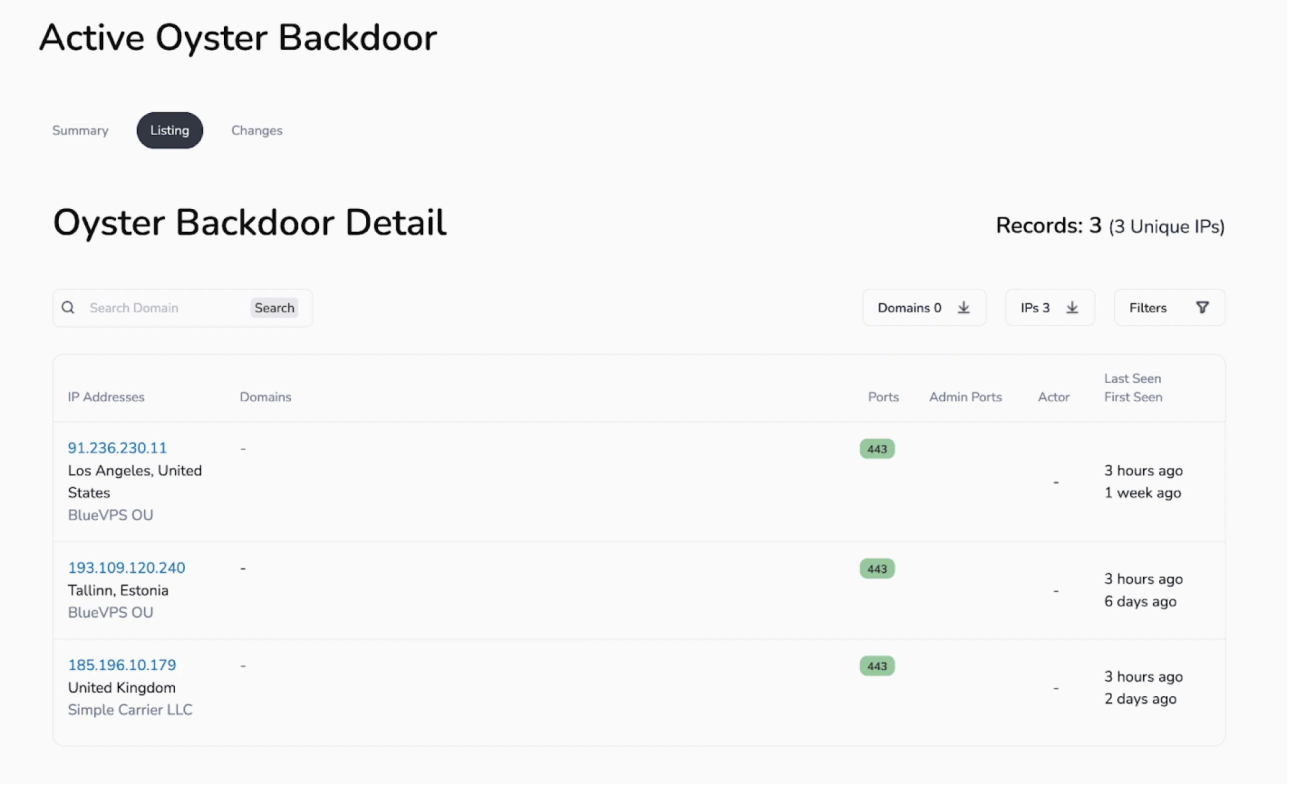

Figure 1: Listing of current Oyster backdoor infrastructure in Hunt.

While TRAC's post provides valuable context, we shift our focus to a third IP, 193.109.120[.]240, and its associated domain. Hosted on the BlueVPS OU network, this server has ports 80 and 443 open for HTTP/S and port 56777 configured for SSH, as shown in Figure 2. The IP resolves to a single domain, `cloudignitetech[.]com`, registered via NameCheap.

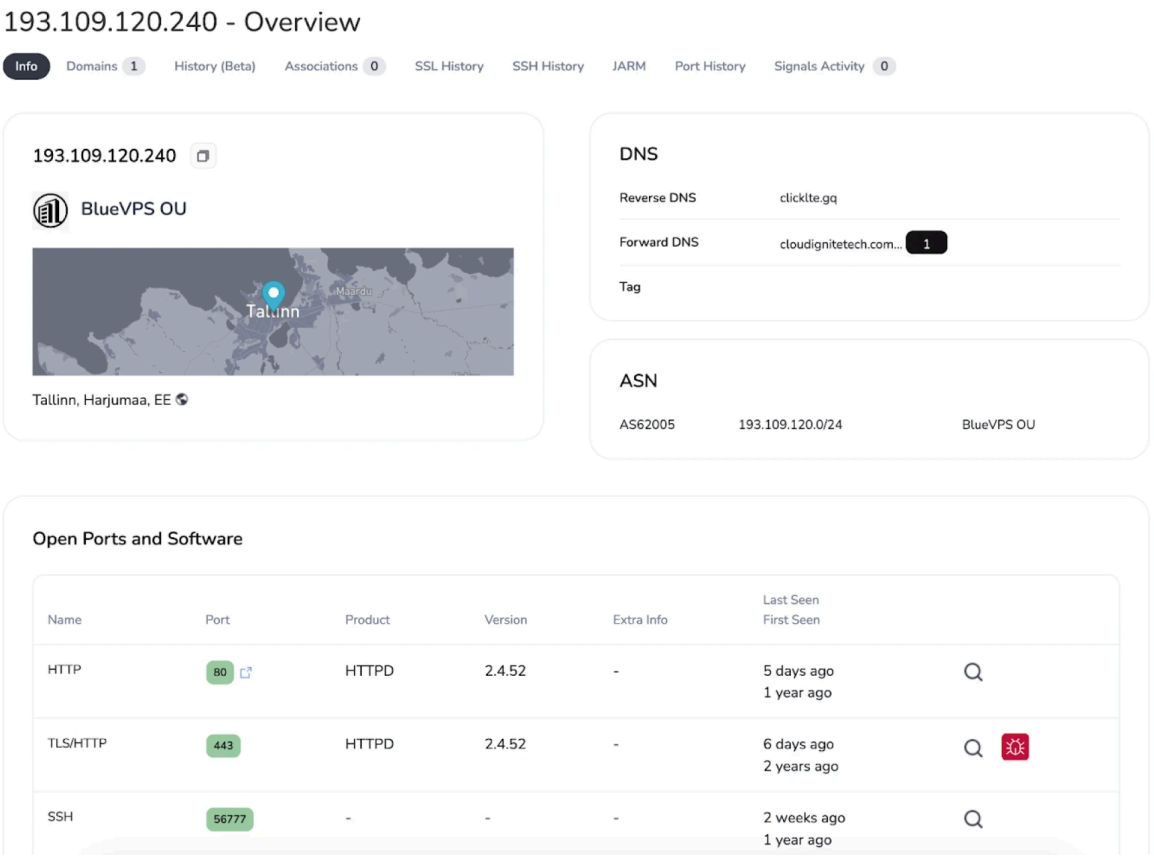

Figure 2: IP overview in Hunt.

In line with our previous blog post, the server's JARM fingerprint and web page displaying "**Soon**" have proven useful in tracking associated infrastructure. Below is an example of the HTML source retrieved from port 443, which demonstrates these distinct characteristics:

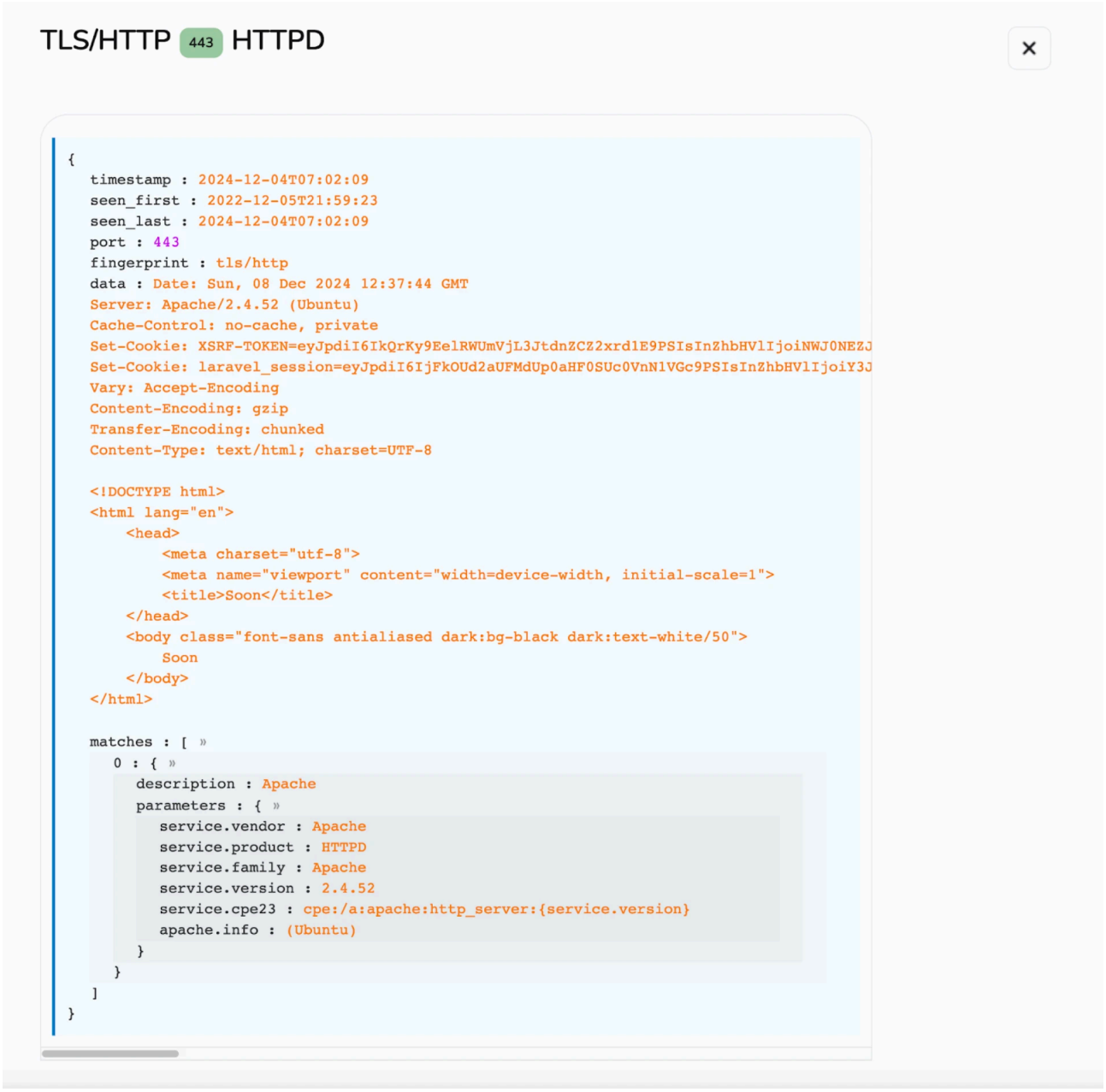

Figure 3: HTML details on port 443 showing the 'Soon' title linked to Oyster malware (Hunt).

A Let's Encrypt certificate (SHA256: **795AD205EA6D324FDC0E1E81BC3E89A813A45070F1D4B30214E4B79359EE5A3A**) using the same domain as the Common Name, was also found.

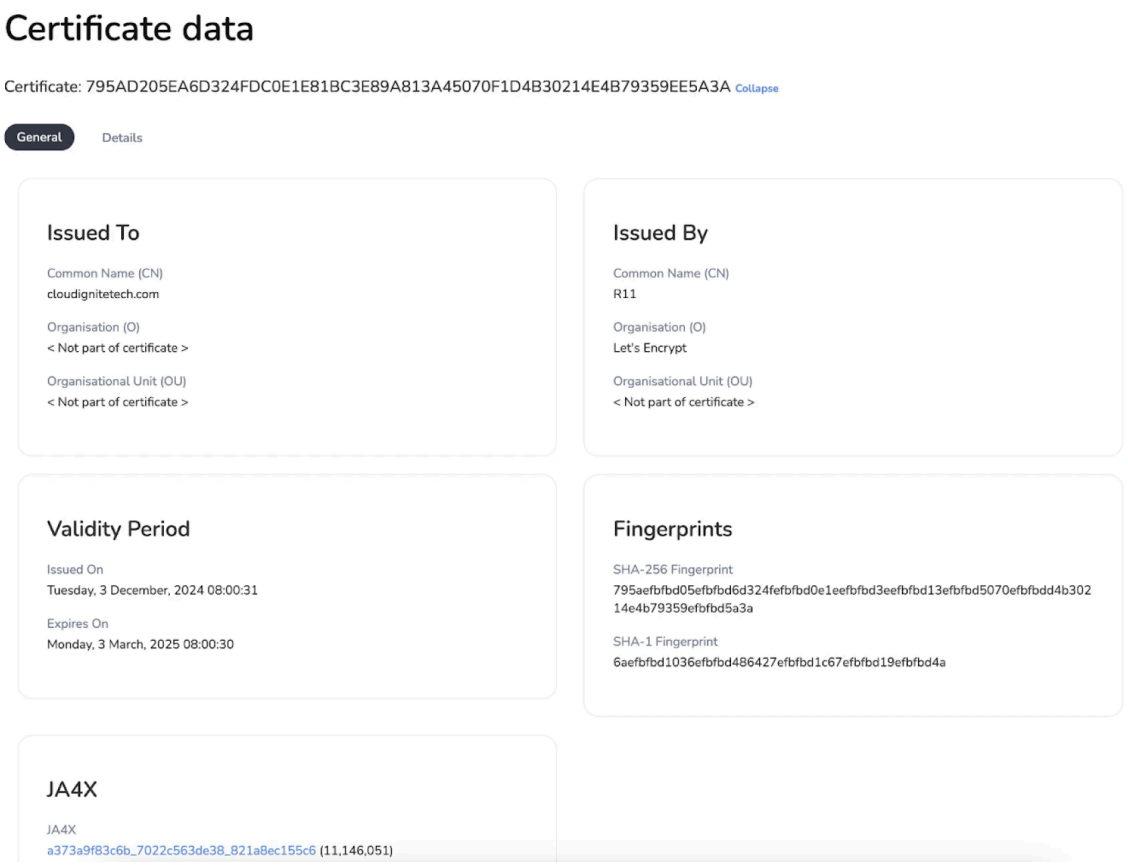

Figure 4: Screenshot of the TLS certificate data for the IP in Hunt.

Pivot!

Stepping back to analyze 185.196.10[.]179 in Hunt, our scans identified 20 associations with other IPs through shared SSH keys (Fingerprint: **05cfec94a6d9ab710f6dc6c4287408f4e71a4770d5b5b8e81b0552e1e91b7a33**).

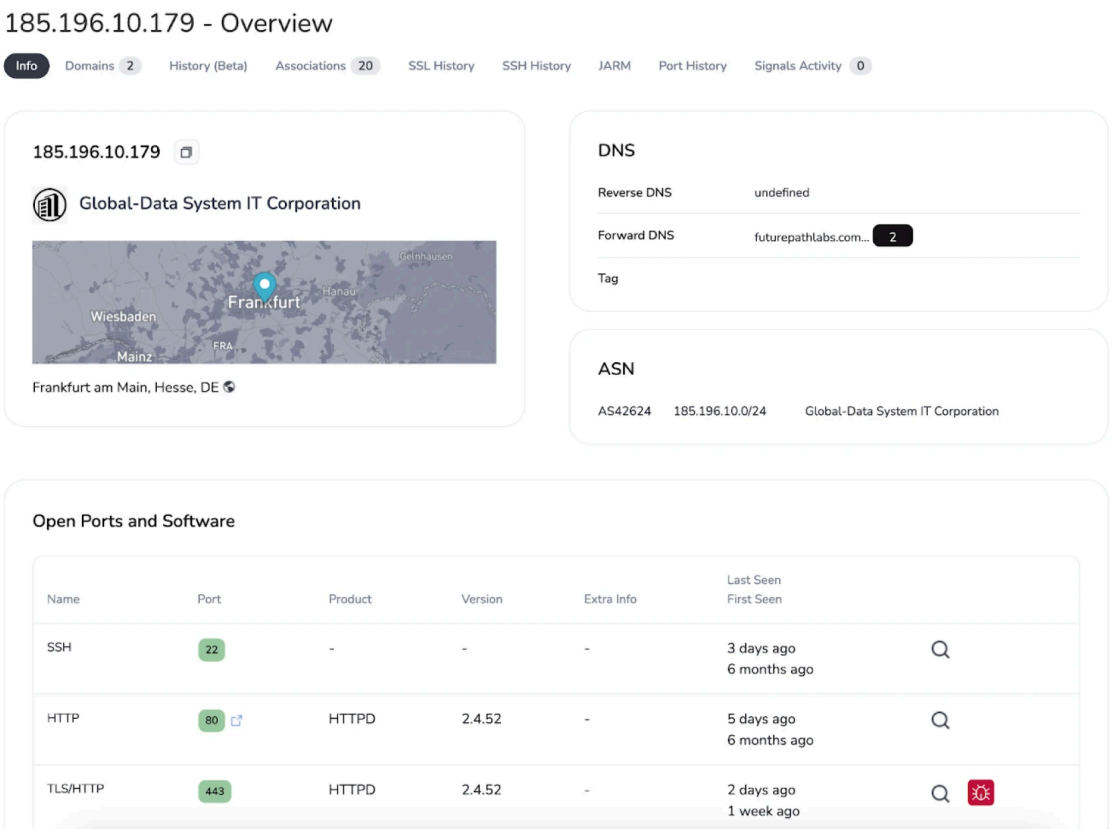

Figure 5: IP overview of 185.196.10[.]179, which shows the 'Associations' tab with the number 20 beside it (Hunt).

The IPs in question are clustered within the same ASN, with several resolving to domains similar to those discussed above. While these overlaps are compelling, they do not conclusively indicate malicious intent. The observed connections could result from server misconfigurations, the deployment of shared images containing embedded SSH keys, or even different actors unknowingly reusing a leaked key.

A full list of IPs and domains (based on our visibility) can be found at the end of this post.

Conclusion

This blog post has outlined key findings on new infrastructure associated with the Oyster backdoor, including three IPs identified in Hunt, a unique domain, and connections revealed through shared SSH keys. To support defenders in identifying similar threats, we continuously refine and update our detection rules, ensuring the latest information on command-and-control servers is readily available.

Network Observables

IP Address	Hosting Country	ASN	Domain(s)	Notes
91.236.230[.]11	US	BlueVPS OU	greensolutionshub[.]net	Detected by Hunt

IP Address	Hosting Country	ASN	Domain(s)	Notes
185.196.10[.]179	UK	Global-Data System IT Corporation	futurepathlabs[.]com kisppy[.]net	Detected by Hunt
193.109.120[.]240	EE	BlueVPS OU	cloudignitetech[.]com	Detected by Hunt
185.196.10[.]182	DE	Global-Data System IT Corporation	lido.fi-nft[.]app	Shared SSH keys w/ 185.196.10[.]179 + below
185.196.11[.]195	DE	Global-Data System IT Corporation	N/A	
185.196.10[.]97	DE	Global-Data System IT Corporation	jfhgfh.duckdns[.]org johnwest-cars[.]co.uk	
185.196.11[.]197	DE	Global-Data System IT Corporation	razer-boost[.]com	
185.208.159[.]112	DE	Global-Data System IT Corporation	N/A	
185.196.10[.]81	DE	Global-Data System IT Corporation	zojanink[.]pw	
185.196.11[.]60	DE	Global-Data System IT Corporation	N/A	
185.196.11[.]62	DE	Global-Data System IT Corporation	N/A	
185.196.10[.]174	DE	Global-Data System IT Corporation	N/A	
185.196.11[.]49	DE	Global-Data System IT	N/A	

IP Address	Hosting Country	ASN	Domain(s)	Notes
		Corporation		
185.196.10[.]172	DE	Global-Data System IT Corporation	N/A	
185.196.10[.]173	DE	Global-Data System IT Corporation	gemen[.]asia	
185.196.11[.]198	DE	Global-Data System IT Corporation	1k+	
185.196.10[.]177	DE	Global-Data System IT Corporation	N/A	
185.196.11[.]194	DE	Global-Data System IT Corporation	anumalisa[.]com menjamili[.]com	
185.196.11[.]105	DE	Global-Data System IT Corporation	N/A	
185.196.11[.]59	DE	Global-Data System IT Corporation	N/A	
185.196.10[.]221	DE	Global-Data System IT Corporation	N/A	
185.196.11[.]196	DE	Global-Data System IT Corporation	aramex.i-order[.]shop aramex.o-blank[.]site gumtreever.i-order[.]shop	
185.196.11[.]57	DE	Global-Data System IT Corporation	N/A	

Source: https://hunt.io/blog/oysters-trail-resurgence-infrastructure-ransomware-cybercrime