Rare Watermark Links Cobalt Strike 4.10 Team Servers to Ongoing Suspicious Activity

Published: 2024-12-03 · Archived: 2026-04-06 00:11:33 UTC

TABLE OF CONTENTS

Hunt researchers recently uncovered a cluster of suspicious infrastructure using Cobalt Strike's latest version, **4.10**, released in July 2024. Despite efforts to disrupt unauthorized use, malicious actors continue to exploit the tool's post-exploitation features for nefarious purposes. According to our scan data, these servers are highlighted by a unique watermark shared by only five other IPs across the internet.

Notably, the domains associated with the team servers (which first showed in our scans on **19 November**) impersonate well-known brands, suggesting a targeted approach to deceive users, possibly through phishing. This post presents our analysis, including detailed examinations of the IP addresses, domains, and beacon configurations involved.

A New Version & Watermark 688983459

Cobalt Strike 4.10 introduced several enhancements to improve cybersecurity practitioners' efficiency. These updates offer improved flexibility, greater control, and improved evasion techniques, which, while intended for legitimate security testing, can also be leveraged by malicious actors.

Below are three of the most impactful (in our opinion) features introduced:

- **BeaconGate**: Enables operators to route Beacon's Windows API calls through a customizable interface, enhancing evasion strategies.
- **Postex Kit**: Provides a comprehensive set of post-exploitation tools designed to enhance system interaction after initial access.
- **Sleepmask-VS**: Introduces an updated sleep masking mechanism that hides Beacon's activity during idle periods, reducing detection risks.

Watermarks Explained

In Cobalt Strike, a watermark is a unique identifier embedded within the software, and its payloads are linked to a specific license/customer. While watermarks assist in linking activity to specific operators when seen across different instances, their effectiveness is limited due to the ease of spoofing and the widespread availability of leaked or pirated versions.

Low-prevalence watermarks may indicate activity not widely recognized by defenders, such as emerging malicious campaigns. Conversely, red team exercises may be more apt to keep default values, which could also result in rarely seen watermarks.

Watermark **688983459** was identified during our research into Cobalt Strike team servers. This identifier, only seen by our scanners across 7 other IP addresses, seemed like a worthy candidate to dive into and analyze further. This discovery led us to infrastructure using the latest version of Cobalt Strike as well as domains and configuration patterns, which we will discuss below.

Infrastructure Analysis

Beyond the shared watermark, the servers exhibit additional commonalities. All team servers are hosted in the United States within Amazon's network infrastructure, except for one utilizing Microsoft's services.

Additionally, the cluster shares network port configurations, specifically using port 80 for the Cobalt Strike team server. We'll quickly cover the beacon configuration, which can be viewed by clicking on the "i" button next to any detected team server in Hunt.

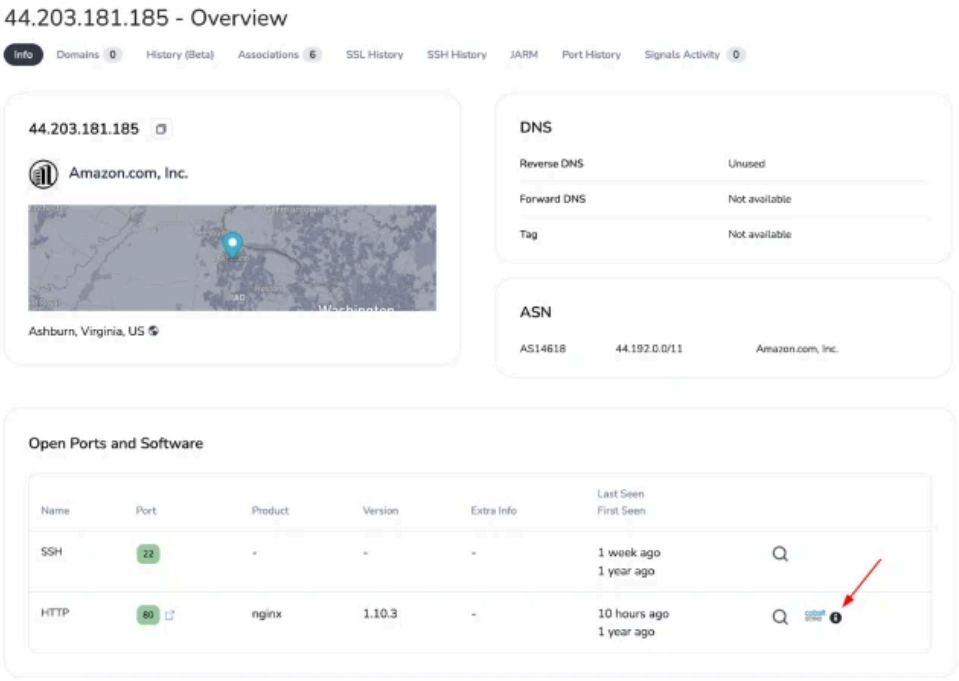


Figure 1: Screenshot showing the "i" button which allows users to quickly view beacon configurations without downloading them in Hunt.

Similarities between IP addresses, such as shared SSH keys, IoCs from reports, certificates, config, and redirects, are all available to quickly pivot on under the "Associations" tab in Hunt.

We found servers sharing the same config by drilling down into the aforementioned tab, uncovering six additional IPs, as seen in Figure 2 below.

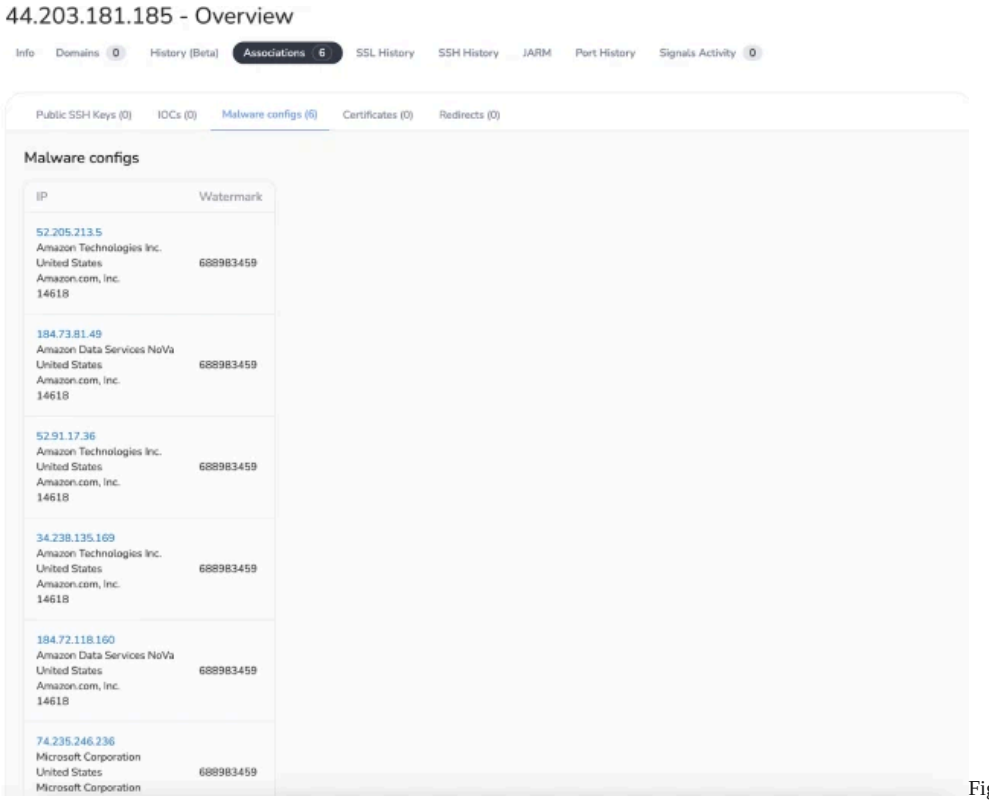
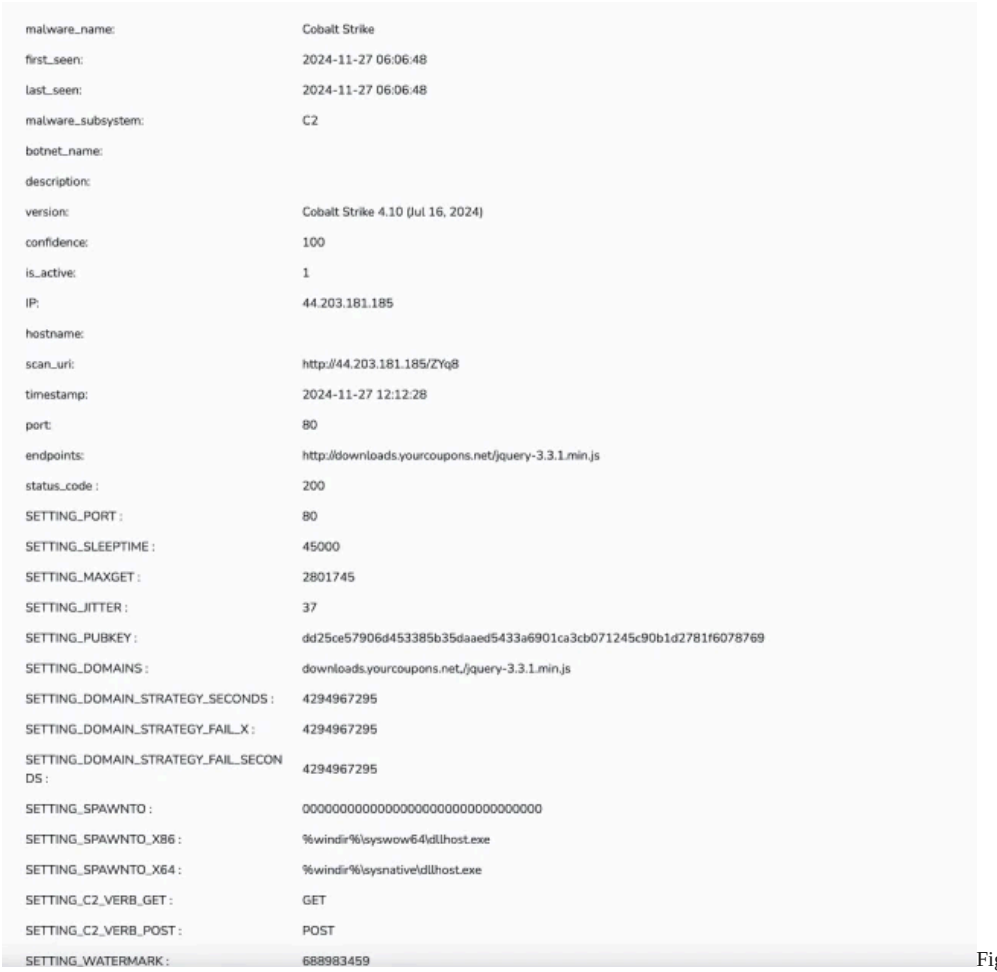


Figure 2: Associations tab showing six additional IP addresses sharing the same watermark (Hunt).

Another data point that assists in clustering suspicious infrastructure is the public key, which is also embedded within the beacon configuration. In our research, **dd25ce57906d453385b35daaed5433a6901ca3cb071245c90b1d2781f6078769**, was shared across all 7 servers. Below are some of the more interesting config fields starting with IP address 44.203.181[.]185.

- endpoint: `http://downloads.yourcoupons[.]net/jquery-3.3.1.min.js`
- SETTING_USERAGENT : Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
- SETTING_SUBMITURI : /jquery-3.3.2.min.js

Figure 3 below displays an example config from our first server.



malware_name:	Cobalt Strike
first_seen:	2024-11-27 06:06:48
last_seen:	2024-11-27 06:06:48
malware_subsystem:	C2
botnet_name:	
description:	
version:	Cobalt Strike 4.10 (Jul 16, 2024)
confidence:	100
is_active:	1
IP:	44.203.181.185
hostname:	
scan_uri:	http://44.203.181.185/ZYq8
timestamp:	2024-11-27 12:12:28
port:	80
endpoints:	http://downloads.yourcoupons.net/jquery-3.3.1.min.js
status_code :	200
SETTING_PORT :	80
SETTING_SLEEPTIME :	45000
SETTING_MAXGET :	2801745
SETTING_JITTER :	37
SETTING_PUBKEY :	dd25ce57906d453385b35daaed5433a6901ca3cb071245c90b1d2781f6078769
SETTING_DOMAINS :	downloads.yourcoupons.net,/jquery-3.3.1.min.js
SETTING_DOMAIN_STRATEGY_SECONDS :	4294967295
SETTING_DOMAIN_STRATEGY_FAIL_X :	4294967295
SETTING_DOMAIN_STRATEGY_FAIL_SECONDS :	4294967295
SETTING_SPAWNTO :	00000000000000000000000000000000
SETTING_SPAWNTO_X86 :	%windir%\syswow64\dllhost.exe
SETTING_SPAWNTO_X64 :	%windir%\sysnative\dllhost.exe
SETTING_C2_VERB_GET :	GET
SETTING_C2_VERB_POST :	POST
SETTING_WATERMARK :	688983459

Figure 3: Example beacon configuration including endpoints, user-agent, and submituri fields in Hunt.

So as not to bore you with multiple repetitive screenshots, we'll list the remaining IP addresses in the table below.

IP Address	ASN	Resolving Domain	Domain in Config	First Seen
34.238.135[.]169	Amazon Technologies Inc.	api.toptechmanagementgroup[.]com downloads.toptechmanagementgroup[.]com	downloads.toptechmanagementgroup[.]com	2024-11-26
52.91.17[.]36	Amazon Technologies Inc.	N/A	downloads.abyanfinancial[.]com	2024-11-25
52.205.213[.]5	Amazon Technologies Inc.	downloads.uscga[.]co	Same	2024-11-25
74.235.246[.]236	Microsoft Corporation	public.open-dns[.]uk	Same	2024-11-19

IP Address	ASN	Resolving Domain	Domain in Config	First Seen
184.72.118[.]160	Amazon Data Services NoVa	N/A	downloads.my-icecream[.]com	2024-11-25
184.73.81[.]49	Amazon Data Services NoVa	dev-monitor.upsideapp[.]com	downloads.helpsdeskmicrosoft[.]com	2024-11-25

After reviewing the domains in the table above, it's pretty clear this cluster of infrastructure is geared towards brand impersonation. Domain names like `downloads.helpsdeskmicrosoft[.]com` and `public.open-dns[.]uk` mimic legitimate organizations, likely aiming to blend in with network traffic.

Others, such as `downloads.uscga[.]co` and `downloads.abyanfinancial[.]com`, suggest possible targeting of specific sectors or entities.

During our research into this group of IPs, we could not identify any recent TLS certificates associated with the servers, indicating the infrastructure may still be in the early stages of development, or the operators are purposefully not using certificates to evade further scrutinization.

Downloading Beacons

We were able to extract a handful of payloads from the above team servers, which offered a chance for further analysis. Analyzing these beacons allows security professionals to develop detection signatures, understand operator TTPs, and possibly identify additional infrastructure previously unknown.

While a detailed examination of the payloads is beyond the scope of this post, we are sharing the SHA-256 hashes below and encourage the community to dig into these samples and analyze any shellcode or malicious artifacts.

Reminder: It's not uncommon for red teamers or malicious network operators to serve benign files in an attempt to protect the Team Server.

Team Server	SHA-256	File Size
52.205.213[.]5	ae352f86b470dfa999f3d50394876209d19bc06af2e246758f150f55eaa2a787	273.09 KB
44.203.181[.]185	d884ccc9aa3b1d1a018d7cb4a1d80da7142e934178ef0fc6faff7b1f1f7fa6c1	273.09 kB
34.238135[.]169	889e4f388ac6fd9d5f1025ed32276eb0fef2717c8d387fb82d5a8438bbe6025e	273.07 KB
184.73.81[.]49	a2ed422d92f5963468c9e3c615754dc7e31acd51b7372386d7694747bc2d9897	273.08 KB
184.72.118[.]160	e2a82f971d011675ad387beb2ef943824b2e62e3aab5f9ef79516c11693a6636	273.07 KB

One More Thing: A Curious Cluster with Watermark 1

Before wrapping up this post, we wanted to briefly highlight another small cluster of team servers we observed using a watermark of **1**. This value has typically been associated with cracked or leaked versions of Cobalt Strike.

In 2020, Amnesty International reported that the FinSpy spyware targeting macOS and Linux systems employed the same watermark. We see no links between this case and FinSpy, however adding historical context can assist in highlighting the /potential significance of findings.

Given that this group of servers varies greatly by version and other factors, we'll quickly detail some of the more interesting servers, and provide the rest at the end of this post..

IP Address: 113.250.188[.]15

- ASN: Chongqing Telecom
- Cobalt Strike Version: 4.3
- endpoints: `113.250.188[.]15/en_US/all.js`
- User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; InfoPath.1)
- PUBKEY: 2be79284671f4a3d7aa1158731c3ac3e499bfb1ca637e237e04acdd91a3e67c4

IP Address: 36.137.91[.]198

- ASN: China Mobile Communications Group Co., Ltd.
- Cobalt Strike Version: 4.2
- endpoints: `http://36.137.91[.]198:18443/cx`
- User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; Win64; x64; Trident/6.0; MATMJS)
- PUBKEY: 713cb0954ca69d973628c711744046d0b9dc7f6036175184389b31bd8ddbd7e3

IP Address: 85.208.110[.]57

- ASN: STARK INDUSTRIES SOLUTIONS LTD
- Cobalt Strike Version: 4.2
- Endpoints: `https://www.googleadservices[.]org:63221/pagead/conversion/16521530460`
- User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36 Vivaldi/3.7aa.
- PUBKEY: 02a621ddce14572cb2ded37edc76ce3d93cf78b46feec2d318bb1c4afaf609da
- TLS Certificate: CloudFlare SHA-256 Fingerprint: 8860015325A7DFA7DE7BBC6CE0C4600B3109577836E3F0116F223AB5F7A85490

Conclusion

Our threat hunting efforts led us to infrastructure leveraging the latest version of Cobalt Strike, all connected by the unique watermark 688983459. Utilizing the associations tab in Hunt, we quickly identified similar IPs, and additional analysis of similar ports, and domains impersonating well-known brands, points to a coordinated operation defenders should be on the lookout for.

We also discovered a separate group of servers using the watermark 1, historically associated with known malicious activity. While the intent behind this cluster remains unclear-whether it represents legitimate red team exercises or actions by malicious actors-it underscores the importance of vigilance. Monitoring both commonly used and rare watermarks is essential for detecting and mitigating threats in all their forms.

Watermark 1 Cluster

IP Address	ASN	Domain(s)	Miscellaneous
47.120.38[.]194	Hangzhou Alibaba Advertising Co.,Ltd.	mggbest[.]top	Cobalt Strike 4.2
91.196.70[.]155	EstNOC OY	N/A	"Microsoft" TLS Certificate SHA-256: 8A172E2F0CA849799E0B25CD0EB89D32020EECF30599D951C4E8ECB82

IP Address	ASN	Domain(s)	Miscellaneous
83.229.127[.]233	LUCIDACLOUD LIMITED	N/A	Cobalt Strike 4.2
124.222.201[.]108	Shenzhen Tencent Computer Systems Company Limited	N/A	Cobalt Strike 4.2
139.196.126[.]3	Hangzhou Alibaba Advertising Co.,Ltd.	N/A	Cobalt Strike 4.2
