Unmasking Adversary Infrastructure: How Certificates and Redirects Exposed Earth Baxia and PlugX Activity

hunt.io/blog/unmasking-adversary-infrastructure-how-certificates-and-redirects-exposed-earth-baxia-and-plugx-activity

TABLE OF CONTENTS

Introduction

Tracking adversary infrastructure often starts with subtle clues. In this case, unconventional certificates and unique HTTP redirect headers led us to two distinct malicious networks. One network was linked to Earth Baxia, a threat actor identified by Trend Micro believed to be from China, while the other appears to be connected to **PlugX**, based on our telemetry.

While these two infrastructures were tracked independently and are not connected, following these basic indicators helped us map out clusters of servers likely used in network intrusions.

This post details the steps taken to uncover and track these networks.

Identifying Earth Baxia Infrastructure

After reviewing the Trend Micro report, we analyzed the IOCs to identify any additional infrastructure potentially linked to Earth Baxia. Our research uncovered Cloudflare certificates with **Subject Alternative Name** (SAN) domains resembling those mentioned in the blog post. SANs are extensions within SSL/TLS certificates that list additional domain names, or IP addresses a certificate can secure beyond the primary domain.

CloudFlare certificate:

```
SubjectCommonName: CloudFlare Origin Certificate\
SubjectOrganization: CloudFlare, Inc.\
SubjectOrganizationalUnit: CloudFlare Origin CA

Issuer Country: US\
IssuerOrganization: CloudFlare, Inc.\
IssuerOrganizationalUnit: CloudFlare Origin SSL Certificate Authority\
IssuerLocality: San Francisco

DNSNames: *.viet-tel[.]site\
viet-tel[.]site
```

An example of one of the Cloudflare certificates found at 203.25.119[.]28.

We also discovered several self-signed certificates falsely claimed to have been issued by **Microsoft**, adding to the suspicious nature of the infrastructure. Over the same period, many servers hosting these certificates were also observed to serve the Cloudflare certificates mentioned above. Combined with the HTTP redirects, which we'll mention shortly, these indicators pointed to a small but distinct cluster of **12** likely malicious servers, all of which we attribute to Earth Baxia based on our visibility.

The complete list of the IPs, domains, and redirect URLs is included at the end of this post.

"Microsoft" self-signed certificate:

```
SubjectCommonName: bing[.]com\
SubjectCountry: US\
SubjectOrganization: Microsoft Corporation\
SubjectOrganizationalUnit: Microsoft IT\
SubjectLocality: Redmond\
SubjectProvince: Washington

Issuer data: same as above
```

This cert was also seen at 203.25.119[.]28 during the same period.

The HTTP 301 redirects we observed were primarily over ports **443 and 8443**, directing users to well-known legitimate websites like the **FBI, NASA, and eBay** homepages. This technique was likely used to create an illusion of benign activity, blending malicious behavior into what seemed like standard traffic patterns.

Attackers often leverage open-source redirector tools such as RedGuard or RedWarden to obscure the actual location of command-and-control (C2) servers and evade detection by researchers. However, in this case, there was no evidence that either of these tools was employed, suggesting a custom header was used to achieve a similar effect.

```
HTTP/1.1  301 Moved Permanently\
Date: Wed, 2 Oct 2024  08:25:21 GMT **Value varies\
Content-Type: text/html\
Content-Length: 106 **Value varies
```

HTTP 301 redirect used in Earth Baxia malicious servers.

The selection of the redirect URLs used appears strategic, focusing on high-profile organizations in the **defense, intelligence, and software sectors.** These choices suggest that the attacker(s) aimed to blend into environments where military or government-related traffic is commonplace.

Noteworthy Redirect URLs:

- **www[.]jdf.mil[.]jm**: This domain belongs to the Jamaica Defence Force (JDF), Jamaica's official military organization.
- **www[.]sap[.]com**: Redirects to the official website of SAP, a global leader in enterprise software solutions.
- **www[.]mil[.]ru**: The official website of the Russian Ministry of Defense, frequently targeted or spoofed in various campaigns.
- **www[.]mi6.gov[.]uk**: This domain redirects to the UK's Secret Intelligence Service (SIS), commonly referred to as MI6, which uses the official domain sis.gov[.]uk.
- **www[.]pao.af[.]mil**: A spoof of the Public Affairs Office of the United States Air Force. Visiting this domain results in an HTTP 400 error.

```
<html><head><meta http-equiv="refresh" content="0; url=https://www.jdf.mil[.]jm"></head><body></body></html
```

Redirect URL hosted at **203.55.176[.]207:8443**

Identifying PlugX Servers Through Anomalous Certificates and Redirects

While hunting for unusual SSL/TLS certificates, our research team came across a small set of servers, some identified as PlugX C2 nodes. A notable pattern emerged among these IPs--the letters "**AES**" appeared consistently in the Subject Organizational Unit field of the certificates.

Examples of the certificates we encountered are below.

```
SubjectCommonName: Rootxlhijori\
SubjectCountry: yo\
SubjectOrganization: Asfft\
SubjectOrganizationalUnit: AES\
SubjectLocality: nmdmkivk\
SubjectProvince: Lostxoxk
```

An example certificate for 96.43.101[.]248.

```
SubjectCommonName: Rootabmxucet\
SubjectCountry: qy\
SubjectOrganization: Asxee\
SubjectOrganizationalUnit: tnkkAES\
SubjectLocality: esfzhk\
SubjectProvince: Losududrj
```

Suspicious certificated hosted at 45.133.239[.]188.

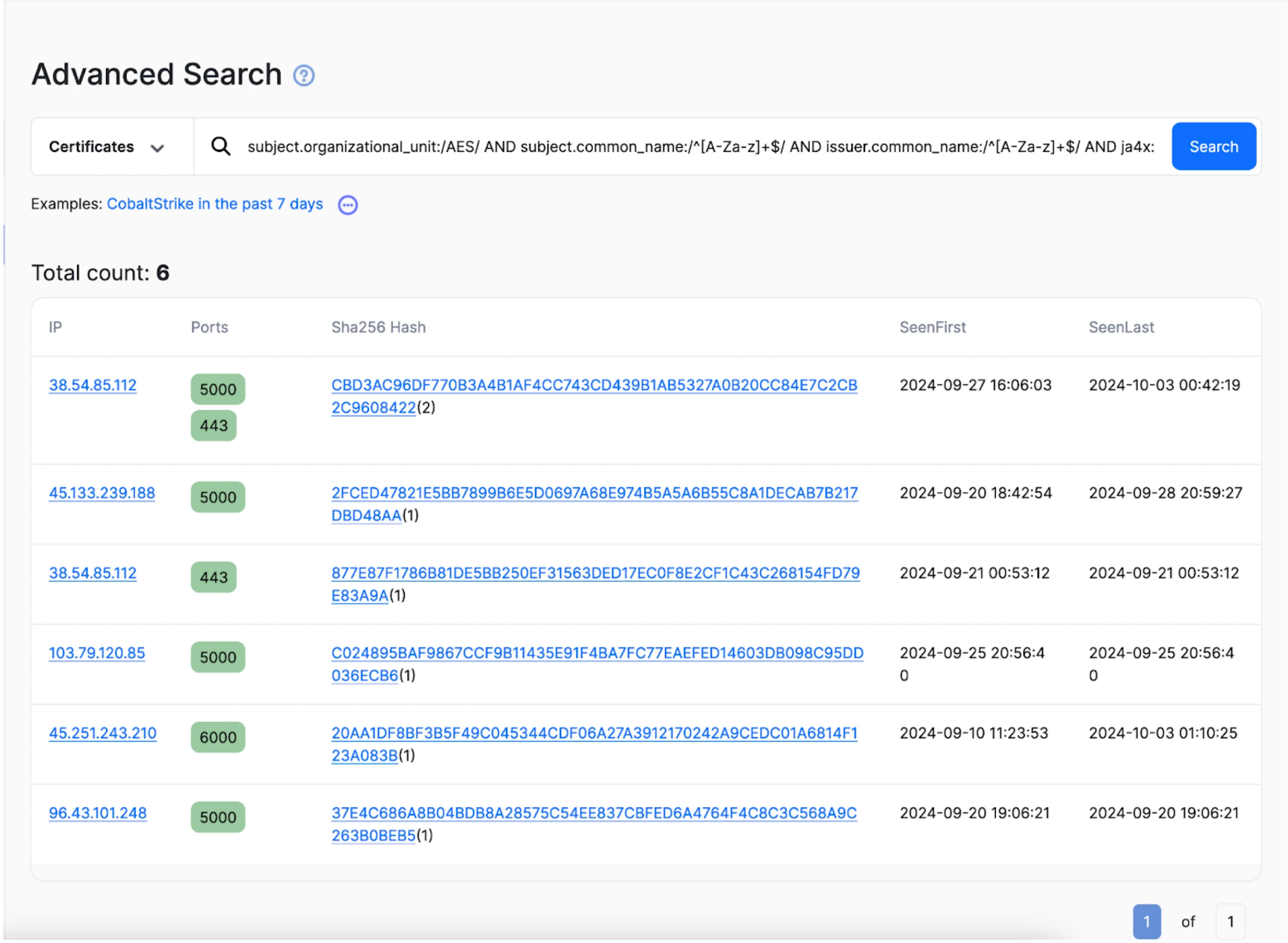
We developed a Hunt Advanced Search query targeting servers with similar certificate characteristics to narrow our analysis. This resulted in **5** unique IP addresses, indicating a cluster of infrastructure tied to PlugX operations.

```
subject.organizational_unit:/AES/ AND subject.common_name:/^[A-Za-z]+$/ AND issuer.common_name:/^[A-Za-z]+$/
AND ja4x:c9d784bbb12e_c9d784bbb12e_795797892f9c
```

Advanced Search query for PlugX linked certificates.

The query is designed to filter for certificates where the OrganizationalUnit field contains 'AES' and both the Subject CommonName and Issuer CommonName contain only alphabetical characters.

Additionally, the query looks for a specific **JA4X** fingerprint. The screenshot below shows our findings.



`subject.organizational_unit:/AES/ AND subject.common_name:/^[A-Za-z]+$/ AND issuer.common_name:/^[A-Za-z]+$/ AND ja4x:`

Total count: **6**

IP	Ports	Sha256 Hash	SeenFirst	SeenLast
38.54.85.112	5000 443	CBD3AC96DF770B3A4B1AF4CC743CD439B1AB5327A0B20CC84E7C2CB2C9608422(2)	2024-09-27 16:06:03	2024-10-03 00:42:19
45.133.239.188	5000	2FCED47821E5BB7899B6E5D0697A68E974B5A5A6B55C8A1DECAB7B217DBD48AA(1)	2024-09-20 18:42:54	2024-09-28 20:59:27
38.54.85.112	443	877E87F1786B81DE5BB250EF31563DED17EC0F8E2CF1C43C268154FD79E83A9A(1)	2024-09-21 00:53:12	2024-09-21 00:53:12
103.79.120.85	5000	C024895BAF9867CCF9B11435E91F4BA7FC77EAEFED14603DB098C95DD036ECB6(1)	2024-09-25 20:56:40	2024-09-25 20:56:40
45.251.243.210	6000	20AA1DF8BF3B5F49C045344CDF06A27A3912170242A9CEDC01A6814F123A083B(1)	2024-09-10 11:23:53	2024-10-03 01:10:25
96.43.101.248	5000	37E4C686A8B04BDB8A28575C54EE837CBFED6A4764F4C8C3C568A9C263B0BEB5(1)	2024-09-20 19:06:21	2024-09-20 19:06:21

Figure 1: Query results for suspicious PlugX certificates. Search conducted on 03 October (Hunt Link)

Four of the five results in Figure 1 had ports already detected as PlugX on the Hunt platform:

- 38.54.85[.]112 -- Ports: 443, 5000
- 45.133.239[.]188 -- Port: 5000
- 45.251.243[.]210 -- Port: 6000
- 96.43.101[.]248 -- Port: 5000

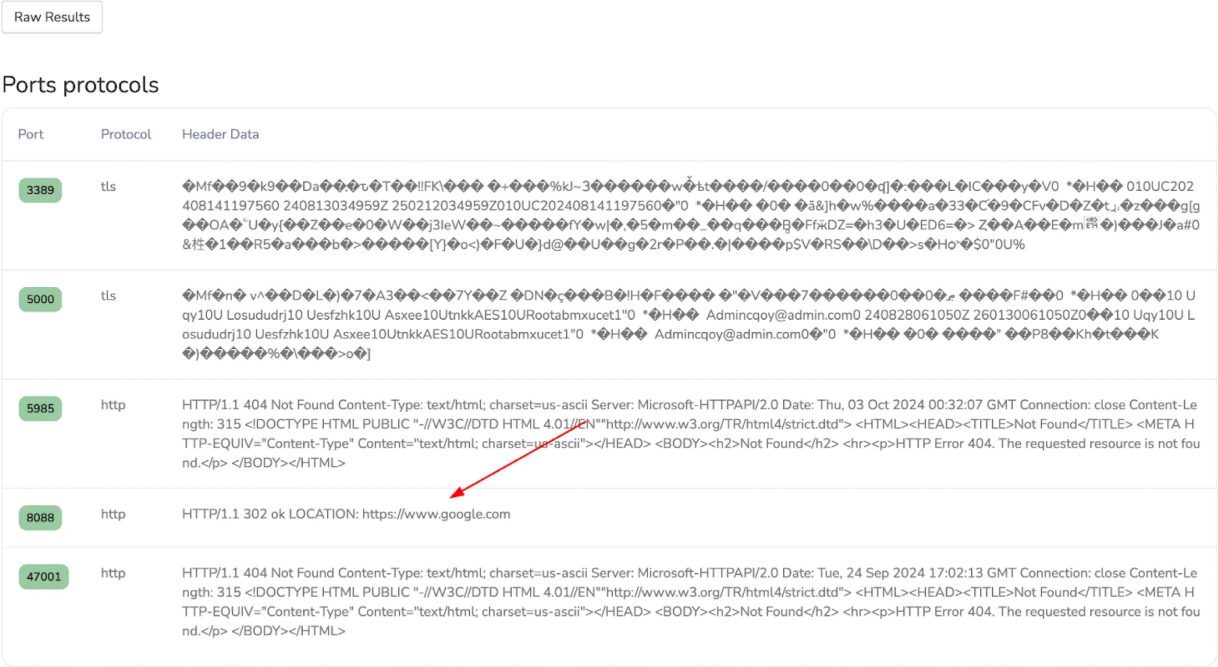
After identifying the IPs tied to the suspicious certificates, we also observed HTTP 302 redirects. These redirects were consistently seen on ports 80 and 8088, commonly used for unencrypted HTTP traffic. In this case, all the redirects pointed to the same domain: **https://www.google.com**.

An example of the redirect header is as follows:

```
HTTP/1.1  302 ok\
LOCATION: https://www.google.com
```

The lowercase "ok" in the status code is unusual. It could indicate hastily constructed, or custom HTTP responses likely meant to mimic legitimate headers while slightly deviating from standard HTTP formatting.

Also, notice the all-caps "LOCATION" header and the redirection to Google.



Ports protocols

Port	Protocol	Header Data
3389	tls	�Mf��9�k9��Da��.�τ�T��!!FK\��� �+���%kJ~3������w�ьt����/����0���0�q]�:���L�IC���y�V0 *�H�� 010UC202408141197560 240813034959Z 250212034959Z010UC202408141197560�"0 *�H�� �0� �ā&]h�w%����a�33�C�9�CFv�D�Z�t.�z���g[g��OA�ˁU�y{��Z��e�0�W��j3leW��~�����fY�w|�,�5�m��_��q���Ḇ�FfӂDZ=�h3�U�ED6=�> Z��A��E�m�)���J�a#0&栍�1��R5�a���b�>�����[Y}�o<)�F�U�}d@��U��g�2r�P��.�|����p$V�RS��\D��>s�Ho�$0"0U%
5000	tls	�Mf�n� v^��D�L�)�7�A3��<��7Y��Z �DN�ç���B�!H�F���� �"�V���7�������0���0�ع ����F#��0 *�H�� 0��10 Uqy10U Losududrj10 Uesfzhk10U Asxee10UtnkkAES10URootabmxucet1"0 *�H�� Admincqoy@admin.com0 240828061050Z 260130061050Z0��10 Uqy10U Losududrj10 Uesfzhk10U Asxee10UtnkkAES10URootabmxucet1"0 *�H�� Admincqoy@admin.com0�"0 *�H�� �0� ����" ��P8��Kh�t���K�)�����%�\���>o�]
5985	http	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Thu, 03 Oct 2024 00:32:07 GMT Connection: close Content-Length: 315 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd"> <HTML><HEAD><TITLE>Not Found</TITLE> <META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD> <BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>
8088	http	HTTP/1.1 302 ok LOCATION: https://www.google.com
47001	http	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Tue, 24 Sep 2024 17:02:13 GMT Connection: close Content-Length: 315 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd"> <HTML><HEAD><TITLE>Not Found</TITLE> <META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD> <BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Figure 2: Custom HTTP 302 response at **45.133.239[.]188** (Hunt Link).

Conclusion

In this investigation, we uncovered two distinct clusters of malicious infrastructure. The first, tied to **Earth Baxia**, revealed suspicious certificates and HTTP 301 redirects that pointed users to trusted sites like the FBI homepage, suggesting an attempt to obscure malicious activity.

The second set of servers, potentially linked to a more extensive **PlugX** campaign, was identified by anomalous certificates containing the "AES" string and HTTP 302 redirects to Google. These minor yet significant anomalies in certificates and headers helped us identify and track this infrastructure, offering valuable insights for further investigation and defense.

Monitoring indicators like those discussed above lets defenders pinpoint suspicious infrastructure early on, allowing them to uncover malicious activity before an attack is fully underway. This proactive approach gives security teams a valuable head start in preventing potential threats from escalating.

Earth Baxia Network Observables

IP Address	ASN	Certificate	Domain(s)	Redirect URL	Host Country	Last Seen

IP Address	ASN	Certificate	Domain(s)	Redirect URL	Host Country	Last Seen
18.162.111[.]155	Amazon.com, Inc.	Cloudflare & Microsoft	visualstudio-microsoft[.]com	https://www.dropbox[.]com	HK	2024-09-28
43.239.249[.]243	xTom Japan Co., Ltd.	Cloudflare & Microsoft	index.caihongyun[.]cc SAN: taipeilivecenter[.]online oca[.]pics	https://www.pao.af[.]mil	JP	2024-09-26
45.76.153[.]76	The Constant Company, LLC	Cloudflare & Microsoft	promociin.com api.promociin[.]com kallpod-asia.kallfly[.]com api.s2.baxtool[.]ru SAN: islot[.]ink	https://www.mi6.gov[.]uk	SG	2024-10-02
45.153.129[.]96	Cloudie Limited	Cloudflare & Microsoft	51xiatian[.]cc app.51xiatian[.]cc www.youke2[.]top SAN: s3-microsoft[.]com	https://www.ebay[.]com	HK	2024-10-02
96.9.213[.]142	Datacamp Limited	Cloudflare & Microsoft	SAN: trendmicrotech[.]com	https://www.mil[.]ru	SG	2024-09-26
96.9.212[.]181	Datacamp Limited	Cloudflare & Microsoft	SAN: naver-info[.]store skt-info[.]online	https://www.ups[.]com	SG	2024-09-24
103.199.16[.]232	365 Online technology joint stock company	Cloudflare	N/A	N/A	VN	2024-10-02
128.199.126[.]48	DigitalOcean, LLC	Let's Encrypt	SAN: xhq.yidaplays[.]ink	https://www.sap[.]com	SG	2024-09-28
172.93.189[.]206	Gigabit Hosting Sdn Bhd	Cloudflare	N/A	https://www.wikipedia[.]org	HK	2024-09-29
172.93.189[.]209	Gigabit Hosting Sdn Bhd	Cloudflare & Microsoft	SAN: s3bucket-azure[.]online	https://www.google[.]com	HK	2024-10-02
203.25.119[.]28	Gigabit Hosting Sdn Bhd	Cloudflare & Microsoft	SAN: viet-tel[.]site	https://www.fbi[.]gov	HK	2024-09-21
203.55.176[.]207	Datacamp Limited	Cloudflare & Microsoft	SAN: transfer-server[.]store	https://www.jdf.mil[.]jm	SG	2024-10-01

TABLE OF CONTENTS

Introduction

Tracking adversary infrastructure often starts with subtle clues. In this case, unconventional certificates and unique HTTP redirect headers led us to two distinct malicious networks. One network was linked to Earth Baxia, a threat actor identified by Trend Micro believed to be from China, while the other appears to be connected to **PlugX**, based on our telemetry.

While these two infrastructures were tracked independently and are not connected, following these basic indicators helped us map out clusters of servers likely used in network intrusions.

This post details the steps taken to uncover and track these networks.

Identifying Earth Baxia Infrastructure

After reviewing the Trend Micro report, we analyzed the IOCs to identify any additional infrastructure potentially linked to Earth Baxia. Our research uncovered Cloudflare certificates with **Subject Alternative Name** (SAN) domains resembling those mentioned in the blog post. SANs are extensions within SSL/TLS certificates that list additional domain names, or IP addresses a certificate can secure beyond the primary domain.

CloudFlare certificate:

```
SubjectCommonName: CloudFlare Origin Certificate\
SubjectOrganization: CloudFlare, Inc.\
SubjectOrganizationalUnit: CloudFlare Origin CA

Issuer Country: US\
IssuerOrganization: CloudFlare, Inc.\
IssuerOrganizationalUnit: CloudFlare Origin SSL Certificate Authority\
IssuerLocality: San Francisco

DNSNames: *.viet-tel[.]site\
viet-tel[.]site
```

An example of one of the Cloudflare certificates found at 203.25.119[.]28.

We also discovered several self-signed certificates falsely claimed to have been issued by **Microsoft**, adding to the suspicious nature of the infrastructure. Over the same period, many servers hosting these certificates were also observed to serve the Cloudflare certificates mentioned above. Combined with the HTTP redirects, which we'll mention shortly, these indicators pointed to a small but distinct cluster of **12** likely malicious servers, all of which we attribute to Earth Baxia based on our visibility.

The complete list of the IPs, domains, and redirect URLs is included at the end of this post.

"Microsoft" self-signed certificate:

```
SubjectCommonName: bing[.]com\
SubjectCountry: US\
SubjectOrganization: Microsoft Corporation\
SubjectOrganizationalUnit: Microsoft IT\
SubjectLocality: Redmond\
SubjectProvince: Washington

Issuer data: same as above
```

This cert was also seen at 203.25.119[.]28 during the same period.

The HTTP 301 redirects we observed were primarily over ports **443 and 8443**, directing users to well-known legitimate websites like the **FBI, NASA, and eBay** homepages. This technique was likely used to create an illusion of benign activity, blending malicious behavior into what seemed like standard traffic patterns.

Attackers often leverage open-source redirector tools such as RedGuard or RedWarden to obscure the actual location of command-and-control (C2) servers and evade detection by researchers. However, in this case, there was no evidence that either of these tools was employed, suggesting a custom header was used to achieve a similar effect.

```
HTTP/1.1  301 Moved Permanently\
Date: Wed, 2 Oct 2024  08:25:21 GMT **Value varies\
Content-Type: text/html\
Content-Length: 106 **Value varies
```

HTTP 301 redirect used in Earth Baxia malicious servers.

The selection of the redirect URLs used appears strategic, focusing on high-profile organizations in the **defense, intelligence, and software sectors**. These choices suggest that the attacker(s) aimed to blend into environments where military or government-related traffic is commonplace.

Noteworthy Redirect URLs:

- **www[.]jdf.mil[.]jm**: This domain belongs to the Jamaica Defence Force (JDF), Jamaica's official military organization.
- **www[.]sap[.]com**: Redirects to the official website of SAP, a global leader in enterprise software solutions.
- **www[.]mil[.]ru**: The official website of the Russian Ministry of Defense, frequently targeted or spoofed in various campaigns.
- **www[.]mi6.gov[.]uk**: This domain redirects to the UK's Secret Intelligence Service (SIS), commonly referred to as MI6, which uses the official domain sis.gov[.]uk.
- **www[.]pao.af[.]mil**: A spoof of the Public Affairs Office of the United States Air Force. Visiting this domain results in an HTTP 400 error.

```
<html><head><meta http-equiv="refresh" content="0; url=https://www.jdf.mil[.]jm"></head><body></body></html
```

Redirect URL hosted at **203.55.176[.]207:8443**

Identifying PlugX Servers Through Anomalous Certificates and Redirects

While hunting for unusual SSL/TLS certificates, our research team came across a small set of servers, some identified as PlugX C2 nodes. A notable pattern emerged among these IPs--the letters "**AES**" appeared consistently in the Subject Organizational Unit field of the certificates.

Examples of the certificates we encountered are below.

```
SubjectCommonName: Rootxlhijori\
SubjectCountry: yo\
SubjectOrganization: Asfft\
SubjectOrganizationalUnit: AES\
SubjectLocality: nmdmkivk\
SubjectProvince: Lostxoxk
```

An example certificate for 96.43.101[.]248.

```
SubjectCommonName: Rootabmxucet\
SubjectCountry: qy\
SubjectOrganization: Asxee\
SubjectOrganizationalUnit: tnkkAES\
SubjectLocality: esfzhk\
SubjectProvince: Losududrj
```

Suspicious certificated hosted at 45.133.239[.]188.

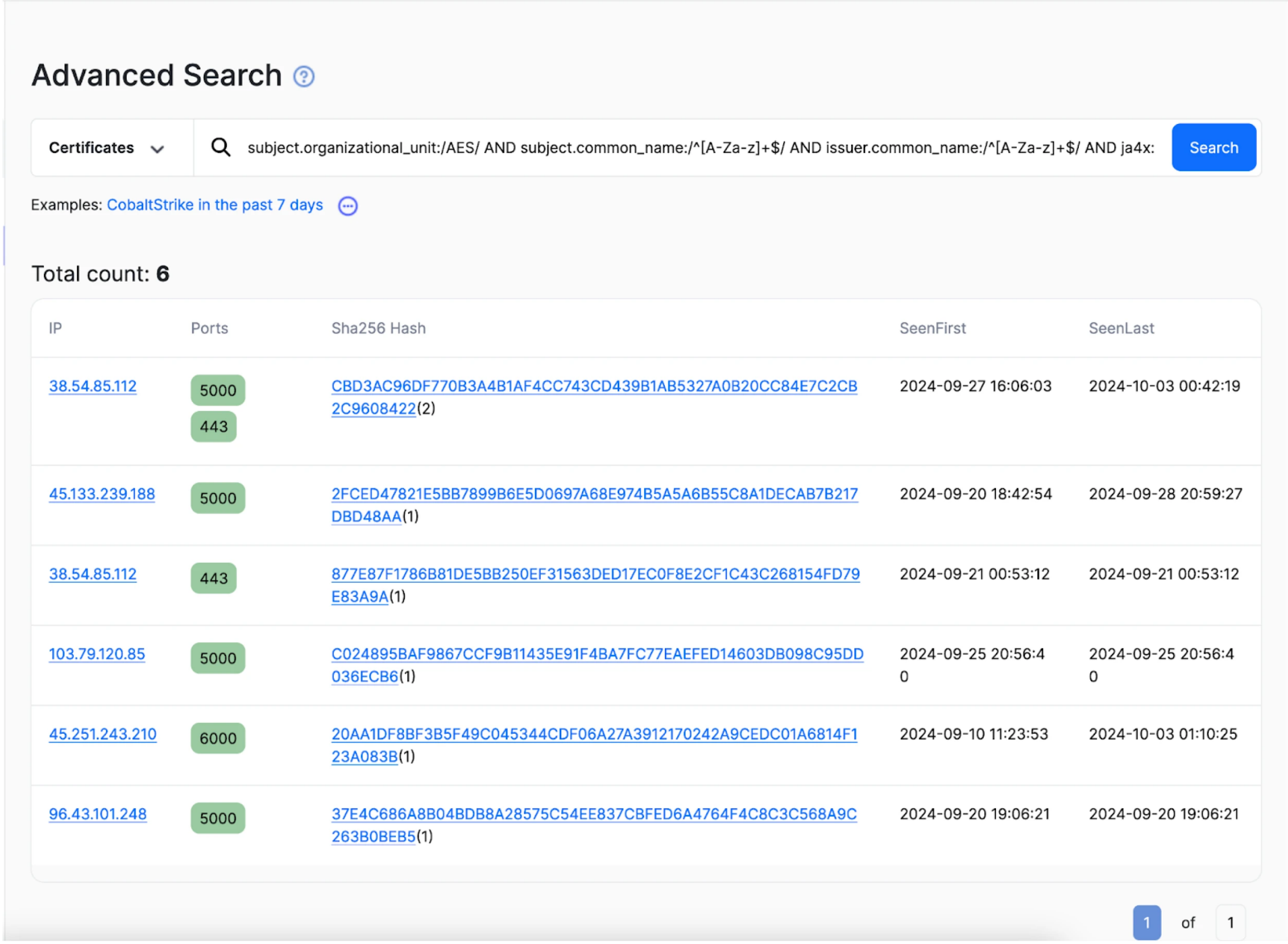
We developed a Hunt Advanced Search query targeting servers with similar certificate characteristics to narrow our analysis. This resulted in **5** unique IP addresses, indicating a cluster of infrastructure tied to PlugX operations.

```
subject.organizational_unit:/AES/ AND subject.common_name:/^[A-Za-z]+$/ AND issuer.common_name:/^[A-Za-z]+$/
AND ja4x:c9d784bbb12e_c9d784bbb12e_795797892f9c
```

Advanced Search query for PlugX linked certificates.

The query is designed to filter for certificates where the OrganizationalUnit field contains 'AES' and both the Subject CommonName and Issuer CommonName contain only alphabetical characters.

Additionally, the query looks for a specific **JA4X** fingerprint. The screenshot below shows our findings.



Advanced Search

subject.organizational_unit:/AES/ AND subject.common_name:/^[A-Za-z]+$/ AND issuer.common_name:/^[A-Za-z]+$/ AND ja4x:

Total count: **6**

IP	Ports	Sha256 Hash	SeenFirst	SeenLast
38.54.85.112	5000 443	CBD3AC96DF770B3A4B1AF4CC743CD439B1AB5327A0B20CC84E7C2CB2C9608422(2)	2024-09-27 16:06:03	2024-10-03 00:42:19
45.133.239.188	5000	2FCED47821E5BB7899B6E5D0697A68E974B5A5A6B55C8A1DECAB7B217DBD48AA(1)	2024-09-20 18:42:54	2024-09-28 20:59:27
38.54.85.112	443	877E87F1786B81DE5BB250EF31563DED17EC0F8E2CF1C43C268154FD79E83A9A(1)	2024-09-21 00:53:12	2024-09-21 00:53:12
103.79.120.85	5000	C024895BAF9867CCF9B11435E91F4BA7FC77EAEFED14603DB098C95DD036ECB6(1)	2024-09-25 20:56:40	2024-09-25 20:56:40
45.251.243.210	6000	20AA1DF8BF3B5F49C045344CDF06A27A3912170242A9CEDC01A6814F123A083B(1)	2024-09-10 11:23:53	2024-10-03 01:10:25
96.43.101.248	5000	37E4C686A8B04BDB8A28575C54EE837CBFED6A4764F4C8C3C568A9C263B0BEB5(1)	2024-09-20 19:06:21	2024-09-20 19:06:21

Figure 1: Query results for suspicious PlugX certificates. Search conducted on 03 October (Hunt Link)

Four of the five results in Figure 1 had ports already detected as PlugX on the Hunt platform:

- 38.54.85[.]112 -- Ports: 443, 5000
- 45.133.239[.]188 -- Port: 5000
- 45.251.243[.]210 -- Port: 6000
- 96.43.101[.]248 -- Port: 5000

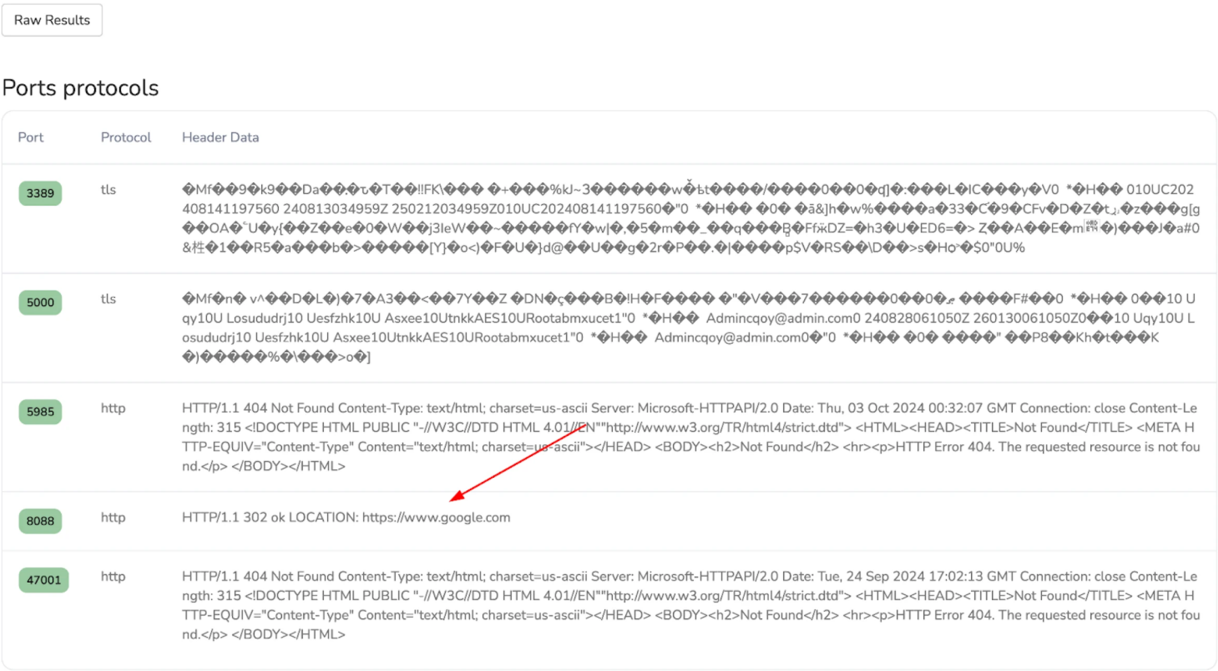
After identifying the IPs tied to the suspicious certificates, we also observed HTTP 302 redirects. These redirects were consistently seen on ports 80 and 8088, commonly used for unencrypted HTTP traffic. In this case, all the redirects pointed to the same domain: **https://www.google.com**.

An example of the redirect header is as follows:

```
HTTP/1.1  302 ok\
LOCATION: https://www.google.com
```

The lowercase "ok" in the status code is unusual. It could indicate hastily constructed, or custom HTTP responses likely meant to mimic legitimate headers while slightly deviating from standard HTTP formatting.

Also, notice the all-caps "LOCATION" header and the redirection to Google.



Ports protocols

Port	Protocol	Header Data
3389	tls	�Mf��9�k9��Da��.�ττ�T��!!FK\��� �+���%kJ~3������w�̌ьt����/����0���0�q]�:���L�IC���y�V0 *�H�� 010UC202408141197560 240813034959Z 250212034959Z010UC202408141197560�"0 *�H�� �0� �ā&]h�w%����a�33�C�9�CFv�D�Z�t.,�z���g[g ��OA�ˁU�y{��Z��e�0�W��j3IeW��~�����fY�w|�,�5�m��_��q���Ḇ�FfжDZ=�h3�U�ED6=�> Z��A��E�m㇍�)���J�a#0 &栍�1��R5�a���b�>�����[Y}�o<)�F�U�}d@��U��g�2r�P��.�|����p$V�RS��\D��>s�Ho˃�$0"0U%
5000	tls	�Mf�n� v^��D�L�)�7�A3��<��7Y��Z �DN�ç���B�!H�F���� �"�V���7�������0���0�.ع ����F#��0 *�H�� 0��10 Uqy10U Losududrj10 Uesfzhk10U Asxee10UtnkkAES10URootabmxucet1"0 *�H�� Admincqoy@admin.com0 240828061050Z 260130061050Z0��10 Uqy10U Losududrj10 Uesfzhk10U Asxee10UtnkkAES10URootabmxucet1"0 *�H�� Admincqoy@admin.com0�"0 *�H�� �0� ����" ��P8��Kh�t���K �)�����%�\���>o�]
5985	http	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Thu, 03 Oct 2024 00:32:07 GMT Connection: close Content-Length: 315 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd"> <HTML><HEAD><TITLE>Not Found</TITLE> <META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD> <BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>
8088	http	HTTP/1.1 302 ok LOCATION: https://www.google.com
47001	http	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Tue, 24 Sep 2024 17:02:13 GMT Connection: close Content-Length: 315 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd"> <HTML><HEAD><TITLE>Not Found</TITLE> <META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD> <BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Figure 2: Custom HTTP 302 response at **45.133.239[.]188** (Hunt Link).

Conclusion

In this investigation, we uncovered two distinct clusters of malicious infrastructure. The first, tied to **Earth Baxia**, revealed suspicious certificates and HTTP 301 redirects that pointed users to trusted sites like the FBI homepage, suggesting an attempt to obscure malicious activity.

The second set of servers, potentially linked to a more extensive **PlugX** campaign, was identified by anomalous certificates containing the "AES" string and HTTP 302 redirects to Google. These minor yet significant anomalies in certificates and headers helped us identify and track this infrastructure, offering valuable insights for further investigation and defense.

Monitoring indicators like those discussed above lets defenders pinpoint suspicious infrastructure early on, allowing them to uncover malicious activity before an attack is fully underway. This proactive approach gives security teams a valuable head start in preventing potential threats from escalating.

Earth Baxia Network Observables

IP Address	ASN	Certificate	Domain(s)	Redirect URL	Host Country	Last Seen
18.162.111[.]155	Amazon.com, Inc.	Cloudflare & Microsoft	visualstudio-microsoft[.]com	https://www.dropbox[.]com	HK	2024-09-28
43.239.249[.]243	xTom Japan Co., Ltd.	Cloudflare & Microsoft	index.caihongyun[.]cc SAN: taipeilivecenter[.]online oca[.]pics	https://www.pao.af[.]mil	JP	2024-09-26

IP Address	ASN	Certificate	Domain(s)	Redirect URL	Host Country	Last Seen
45.76.153[.]76	The Constant Company, LLC	Cloudflare & Microsoft	promociin.com api.promociin[.]com kallpod-asia.kallfly[.]com api.s2.baxtool[.]ru SAN: islot[.]ink	https://www.mi6.gov[.]uk	SG	2024-10-02
45.153.129[.]96	Cloudie Limited	Cloudflare & Microsoft	51xiatian[.]cc app.51xiatian[.]cc www.youke2[.]top SAN: s3-microsoft[.]com	https://www.ebay[.]com	HK	2024-10-02
96.9.213[.]142	Datacamp Limited	Cloudflare & Microsoft	SAN: trendmicrotech[.]com	https://www.mil[.]ru	SG	2024-09-26
96.9.212[.]181	Datacamp Limited	Cloudflare & Microsoft	SAN: naver-info[.]store skt-info[.]online	https://www.ups[.]com	SG	2024-09-24
103.199.16[.]232	365 Online technology joint stock company	Cloudflare	N/A	N/A	VN	2024-10-02
128.199.126[.]48	DigitalOcean, LLC	Let's Encrypt	SAN: xhq.yidaplays[.]ink	https://www.sap[.]com	SG	2024-09-28
172.93.189[.]206	Gigabit Hosting Sdn Bhd	Cloudflare	N/A	https://www.wikipedia[.]org	HK	2024-09-29
172.93.189[.]209	Gigabit Hosting Sdn Bhd	Cloudflare & Microsoft	SAN: s3bucket-azure[.]online	https://www.google[.]com	HK	2024-10-02
203.25.119[.]28	Gigabit Hosting Sdn Bhd	Cloudflare & Microsoft	SAN: viet-tel[.]site	https://www.fbi[.]gov	HK	2024-09-21
203.55.176[.]207	Datacamp Limited	Cloudflare & Microsoft	SAN: transfer-server[.]store	https://www.jdf.mil[.]jm	SG	2024-10-01