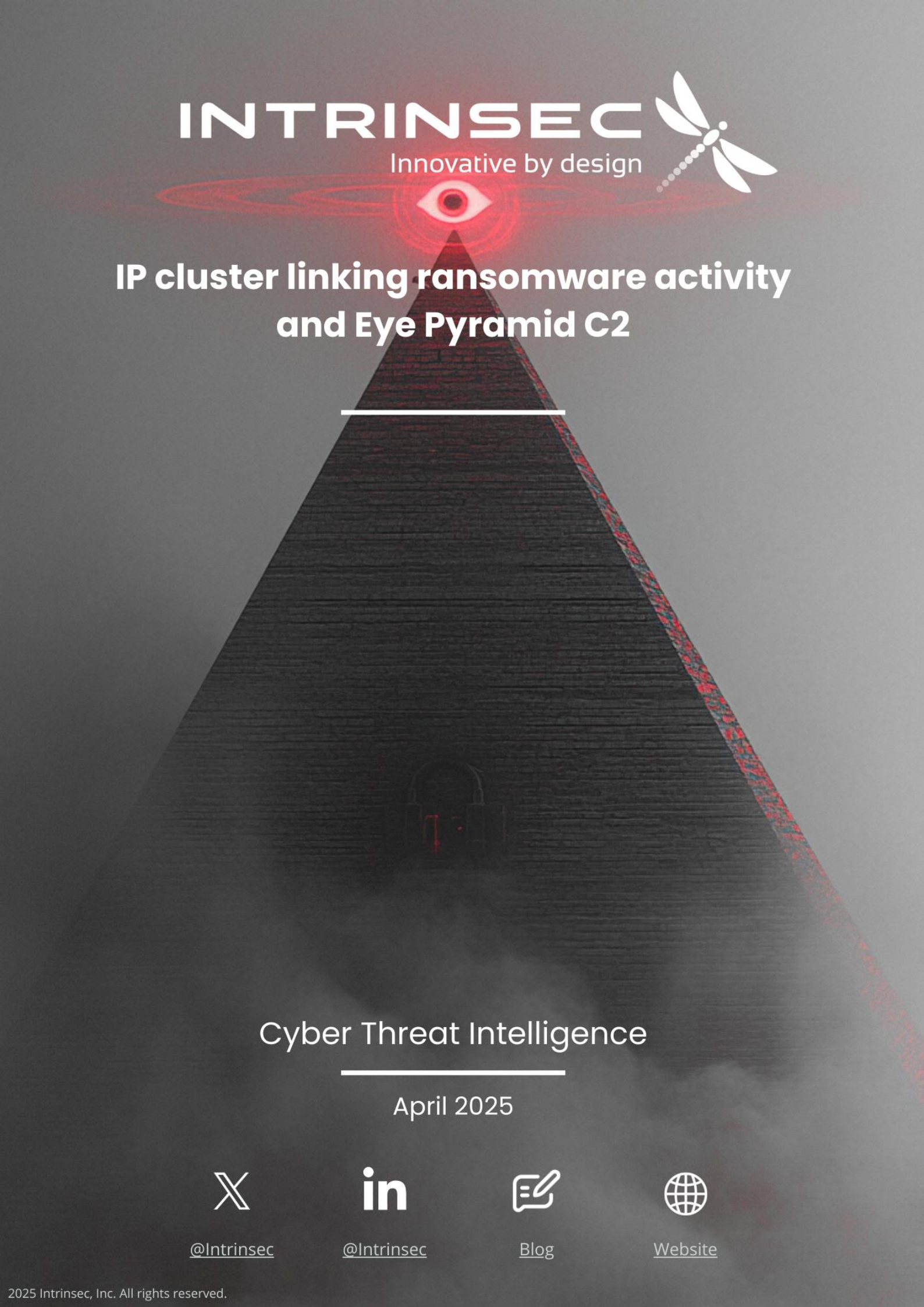


INTRINSEC

Innovative by design

IP cluster linking ransomware activity and Eye Pyramid C2

Cyber Threat Intelligence

April 2025

@Intrinsec @Intrinsec Blog Website

Table of contents

1. Key findings

In this report are presented:

- Pivots on infrastructure associated to a **Python backdoor used by RansomHub**, as exposed by GuidePoint Security. These pivots enabled us to discover infrastructure close to this one, related to the offensive tool **Eye Pyramid**.
- Explanations on the open-source tool Eye Pyramid and details on the recent IP addresses that started to **expose a banner** associated with the tool, since **17 January 2025**. Some of these IP addresses are related to additional payloads such as **Cobalt Strike, Sliver, Rhadamanthys and the ransomware Rhysida**. A number of these IP addresses are hosted on known bulletproof hosting providers such as **Limenet**, **Aeza** and **Railnet**.
- A JSON file was discovered which enabled us to link these infrastructure and IP addresses used previously by ransomware operations such as **Rhysida, Vice Society** and **BlackCat**. This JSON file was identified as being a default error response of Eye Pyramid servers. It could indicate similarity in the configuration of the servers of these clusters of activity.

2. Introduction

Ransomware operations often leverage offensive tools for post-compromise exploitation and lateral movement into compromised networks. They can rely on legitimate red-teaming tool such as Cobalt Strike, Metasploit or Sliver, but can also develop custom tools. In this manner, GuidePoint security recently gave insight into a Python backdoor used by RansomHub, after initial infections.

Our analysis started here, as we discovered an offensive tool by pivoting on the infrastructure associated with the Python backdoor. This offensive tool named "Eye Pyramid" leverages Python to deploy other offensive tools and/or payloads directly in memory. It was open sourced on GitHub in 2022, but we only discovered several IP addresses associated with this tool since mid-January 2025. Some of them are related to other malicious payloads such as Cobalt Strike, Sliver, Rhadamanthys and the ransomware Rhysida.

Eye Pyramid was identified in a case disclosed by The DFIR Report in December 2024[1], which ties this case to a threat actor associated with Fog ransomware. As this tool is effective and can be linked to potential ransomware delivery, as exposed by DFIR Report and in this analysis, it is important to document new infrastructure associated with it and better prepare defenses.

[1] https://thedfirreport.com/2024/12/02/the-curious-case-of-an-egg-cellent-resume/

Find below a summary of our findings on this rogue infrastructure:

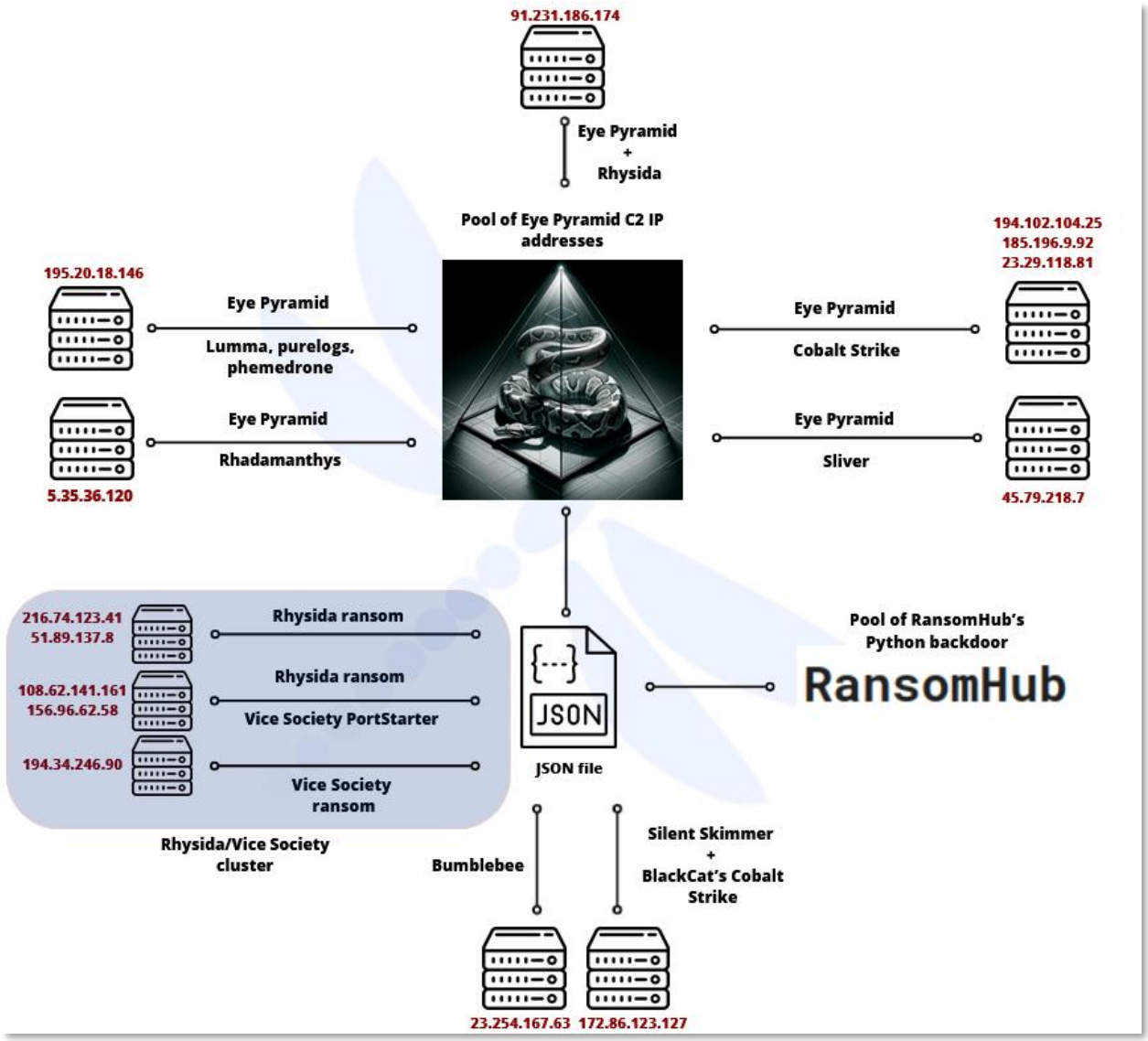


Figure 1: Overview of the rogue infrastructure.

3. RansomHub's Python backdoor C2

On 15 January 2025, GuidePoint Security[2] published an article on the use of a Python backdoor by RansomHub affiliates, to maintain access to compromised endpoints. The access was then used to deploy the ransomware RansomHub on the impacted network. In their article, the company also confirms findings observed by Reliaquest, were SocGholish infections were seen prior to RansomHub compromises. The IP address 92.118.112[.]208[3] is listed in GuidePoint's article as being related to the Python backdoor and was mentioned 11 months prior in Reliaquest's article[4] as being related to SocGholish.

This infection chain from SocGholish to RansomHub corresponds to observations made by Cyber New Jersey[5] and Microsoft[6], where RansomHub infections were seen after compromises by SocGholish infections linked to TA569 (Mustard Tempest).

In GuidePoint's article, several C2 IP addresses leveraged by RansomHub operators for their Python backdoor were given. By querying some of them on Shodan, we noticed that they exposed the same banner on ports 8000 and 443. Using the hash of this banner, we can pivot and discover additional IP addresses. We noticed that there are 26 IP addresses, so 12 more than the 14 IP addresses mentioned in GuidePoint's article. To note, this number fluctuates based on scans made by Shodan's engine.

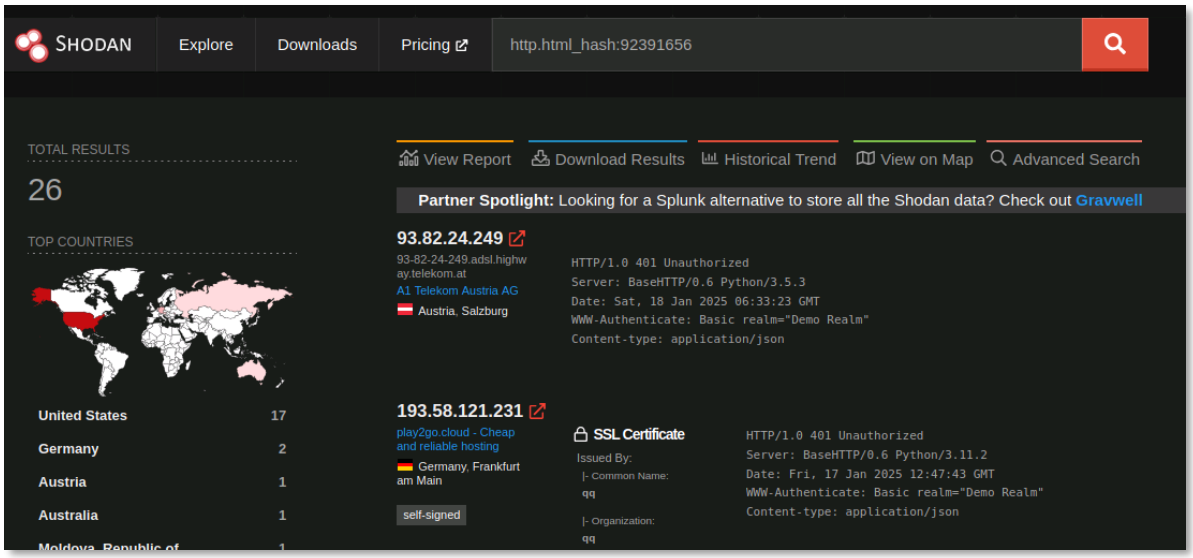


Figure 2: Results of the query on the banner's hash. Source: https://www.shodan.io/search?query=http.html_hash%3A92391656&page=1

[2] https://www.guidepointsecurity.com/blog/ransomhub-affiliate-leverage-python-based-backdoor/
[3] https://www.virustotal.com/gui/ip-address/92.118.112.208/
[4] https://reliaquest.com/blog/common-malware-loaders/
[5] https://www.cyber.nj.gov/Home/Components/News/News/1448/214
[6] https://thehackernews.com/2024/07/scattered-spider-adopts-ransomhub-and.html

4. Eye Pyramid C2

We noted that banners exposed by these new IP addresses were a bit different than the one exposed by the python backdoor IP addresses. The difference resides in the declared authentication method. For the python backdoor, it is ***"WWW-Authenticate: Basic realm="auth""*** while it is ***"WWW-Authenticate: Basic realm="Demo Realm""*** in the new IP addresses.

After checking these new IP addresses on Virus Total, we noticed that most of them were tagged as being related to "**Eye Pyramid C2**". To note, this tool should **not be confused** with malware in .NET named "Eye Pyramid", reported on in 2017 and active since 2014[7].

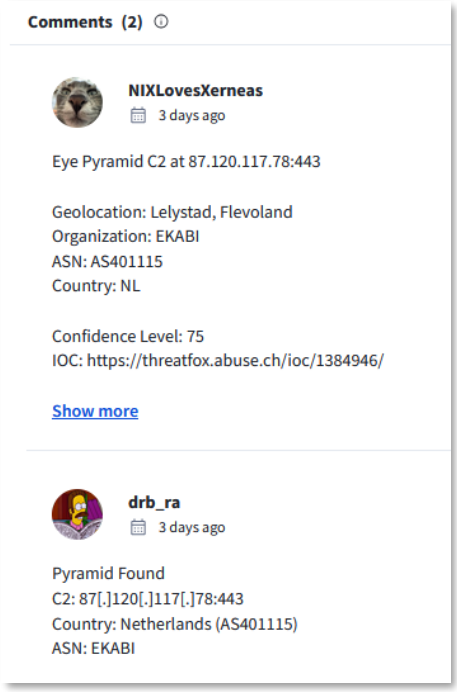


Figure 3: IP address flagged as being related to Eye Pyramid by the community. Source: https://www.virustotal.com/gui/ip-address/87.120.117.78/community

Eye Pyramid C2 is an open-source C2 framework available on GitHub[8]. It was developed by the user "**naksin**" more than two years ago and presented at Defcon[9]. It is a tool written in Python that **facilitates EDR bypassing**. It is composed of:

- A Python HTTP/S server that can **deliver encrypted files**.
- Python modules that can **load in-memory** dependencies of offensive tooling such as **Bloodhound, secretsdump, LaZagne, Pythonnet, DonPAPI, pythonmemorymodule, paramiko, pproxy**.

[7] https://malpedia.caad.fkie.fraunhofer.de/details/win.eye_pyramid
[8] https://github.com/naksyn/Pyramid
[9] https://www.naksyn.com/edr%20evasion/2022/09/01/operating-into-EDRs-blindspot.html

- Fixed Python dependencies (zip files) that can be **imported in memory**.
- Python cradle that can **download, decrypt and execute** in memory Pyramid modules.

The tool is effective as it abuses the fact that Python.exe is a legitimate signed binary that does not provide visibility on Python dynamic code and is usually not blocked or restricted. As such, Eye Pyramid can **carry out offensive tasks** and deploy other tools/payloads from within the legitimate python.exe process. Since **17 January 2025**, IP addresses associated with the tool started to become detected and reported on Abuse by the user "drb_ra"[10].

As further confirmation that these new IP addresses are associated with Eye Pyramid, we found the content of the banner exposed by the IP addresses on Shodan, with mentions of "**Demo Realm**", in the **default server code** of Eye Pyramid on GitHub. As such, we can confirm that IP addresses exposing the banner we queried on Shodan, with mentions of "demo realm" are **associated with Eye Pyramid**, while IP addresses exposing the same banner only changing the mention to "auth" are **associated with RansomHub's python backdoor**.

```
def do_HEAD(self):
        self.send_response(200)
        self.send_header('Content-type', 'application/json')
        self.end_headers()

def do_AUTHHEAD(self):
        self.send_response(401)
        self.send_header(
                'WWW-Authenticate', 'Basic realm="Demo Realm"')
        self.send_header('Content-type', 'application/json')
        self.end_headers()
```

Figure 4: Server response found on the code of the GitHub project. Source: https://github.com/naksyn/Pyramid/blob/main/Server/pyramid.py

[10] https://threatfox.abuse.ch/browse/malware/win.eye_pyramid/

Overall, IP addresses mentioning “demo-realm” are:

IP address	Threat	AS
93.82.24[.]249	Eye Pyramid C2	AS 8447 (Telekom Austria)
193.58.121[.]231	Eye Pyramid C2	AS 215439 (Play2go International Limited) communicates with malicious python script[11] detected as Pyramid
194.102.104[.]24	Eye Pyramid C2	AS 48753 (Ava Host Srl)
194.102.104[.]25	Eye Pyramid C2 and Cobalt Strike	AS 48753 (Ava Host Srl)
195.20.18[.]146	Eye Pyramid C2 and stealers	AS 48753 (Ava Host Srl)
87.120.117[.]78	Eye Pyramid C2	AS 401115 (EKABI)
23.29.118[.]81	Cobalt Strike	AS 29802 (HVC-AS)
146.70.87[.]141	Eye Pyramid C2	AS 9009 (M247 Europe SRL)
93.123.72[.]42	Eye Pyramid C2	AS 206264 (Amarutu Technology Ltd)
62.76.251[.]43	Eye Pyramid C2	AS 204582 (The Technical center of Internet Limited Liability Company)
45.79.218[.]7	Sliver C2	AS 63949 (Akamai Connected Cloud)
96.30.199[.]157	Not detected	AS 20473 (AS-VULTR)
45.86.231[.]115	Eye Pyramid C2	AS 62005 (BlueVPS OU)
77.239.96[.]169	Eye Pyramid C2	AS 210644 (AEZA INTERNATIONAL LTD)
91.231.186.174	Eye Pyramid C2 and Rhysida ransomware	AS 62240 (Clouvider Limited)
195.177.95[.]163	Eye Pyramid C2	AS 214943 (Railnet LLC)
185.196.9[.]92	Eye Pyramid C2 and Cobalt Strike	AS 42624 (Global-Data System IT Corporation)

11 https://www.virustotal.com/gui/file/7c97de6707fb63e1e61a3529ee54284dff6990d5c0fdb610f92eae28c9165820

4.1 Autonomous Systems

Some of these IP addresses are registered on interesting autonomous systems. For instance, the IP address 193.58.121[.]231[12] is hosted on AS 215439 (Play2go International Limited).

This AS is linked with the website play2go[.]cloud. It is interesting as it is advertised as a "Gaming hosting" solution but was abused to host Eye Pyramid C2 server components. The gaming hosting advertisement could also be a marketing posture to mask malicious activity and appear legitimate. However, we did not identify *a priori* bulletproof activities from this AS. We will continue to study it and provide information on it if we find such.

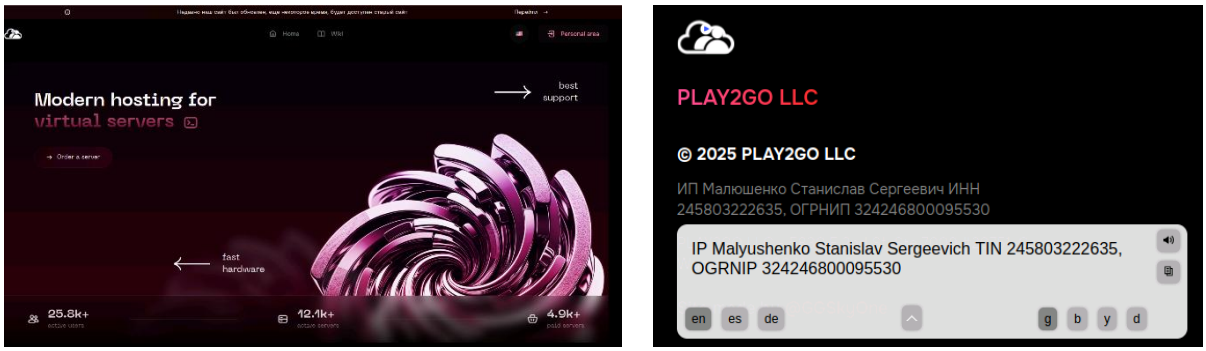


Figure 5: Home page of play2go cloud.

The IP address 87.120.117[.]78[13] is on **AS 401115 (EKABI)**. EKABI is a sub brand of Limenet, which we already analyzed in a private analysis shared to our clients.

EKABI | CrazyRDP

As a reminder, the bulletproof hosting provider **CrazyRDP**, that used to be fronted by the American company *Limenet*, recently changed its complete infrastructure in order to evade network blacklistings and overall bad reputation. Brand new IPs located in Bulgaria have been announced by autonomous systems fronted by American companies, including EKABI and four other autonomous systems: AS401116, AS401109, AS401120, and AS401110.

Indeed, CrazyRDP announced on September 30 a complete reinitialization of its IP range, and that all its clients would receive new IP addresses from these autonomous systems.

The malicious content that could be found on *Limenet* was indeed transferred to these newly created networks and is thus still online to this day.

IP address 77.239.96[.]169[14] is hosted on **AS 210644 (AEZA INTERNATIONAL LTD)**.

[12] https://www.virustotal.com/gui/ip-address/193.58.121.231/relations
[13] https://www.virustotal.com/gui/ip-address/87.120.117.78/relations
[14] https://www.virustotal.com/gui/ip-address/77.239.96.169/detection

Aeza International Ltd.

For several months, Intrinsec's CTI team has been noticing the recrudescence of a variety of malware command-and-control servers being hosted on the same Autonomous System named *Aeza International Ltd.* (**AS210644**). This service has been growing since 2021 under a different name *Aeza Group Ltd*. (**AS216246**). Before creating the company, the founder of Aeza was involved in another Russian bulletproof hosting provider named "MskHost", which was hacked by hacktivists and eventually shut down by their creators.

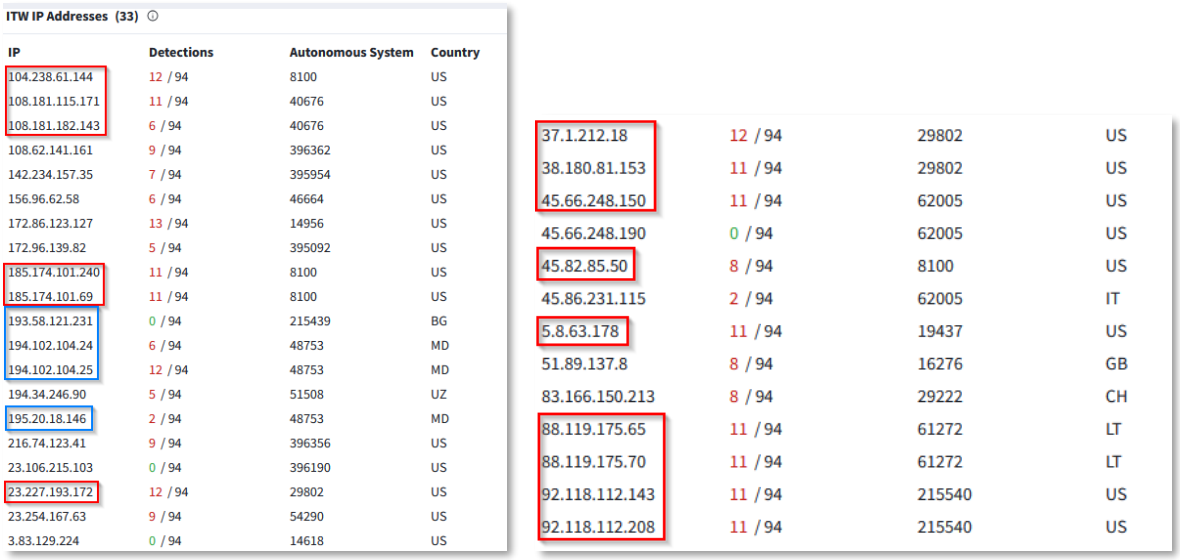
Major actors like **TA577** have been using this service for their campaigns and we believe that it will remain the case for both sophisticated and basic threat actors.

IP address 195.177.95[.]163[15] is hosted on **AS 214943 (Railnet LLC)** and IP address 212.87.222[.]84[16] is hosted on **AS 215540 (Global Connectivity Solutions Llp)**. Both autonomous systems will be analyzed in further analysis, to expose their bulletproof activities.

[15] https://www.virustotal.com/gui/ip-address/195.177.95.163/relations
[16] https://www.virustotal.com/gui/ip-address/212.87.222.84/relations

5. JSON file linking a cluster of ransomware C2s

Additionally, we found a JSON file that appears to be linked to both IP addresses of RansomHub's python backdoor, and to Eye Pyramid C2. This file communicates on VirusTotal with a bunch of IP addresses as shown in the screenshot below. Circled in red are IP addresses associated with the python backdoor, while in blue are IP addresses associated with Eye Pyramid.



ITW IP Addresses (33)

IP	Detections	Autonomous System	Country
104.238.61.144	12 / 94	8100	US
108.181.115.171	11 / 94	40676	US
108.181.182.143	6 / 94	40676	US
108.62.141.161	9 / 94	396362	US
142.234.157.35	7 / 94	395954	US
156.96.62.58	6 / 94	46664	US
172.86.123.127	13 / 94	14956	US
172.96.139.82	5 / 94	395092	US
185.174.101.240	11 / 94	8100	US
185.174.101.69	11 / 94	8100	US
193.58.121.231	0 / 94	215439	BG
194.102.104.24	6 / 94	48753	MD
194.102.104.25	12 / 94	48753	MD
194.34.246.90	5 / 94	51508	UZ
195.20.18.146	2 / 94	48753	MD
216.74.123.41	9 / 94	396356	US
23.106.215.103	0 / 94	396190	US
23.227.193.172	12 / 94	29802	US
23.254.167.63	9 / 94	54290	US
3.83.129.224	0 / 94	14618	US
37.1.212.18	12 / 94	29802	US
38.180.81.153	11 / 94	29802	US
45.66.248.150	11 / 94	62005	US
45.66.248.190	0 / 94	62005	US
45.82.85.50	8 / 94	8100	US
45.86.231.115	2 / 94	62005	IT
5.8.63.178	11 / 94	19437	US
51.89.137.8	8 / 94	16276	GB
83.166.150.213	8 / 94	29222	CH
88.119.175.65	11 / 94	61272	LT
88.119.175.70	11 / 94	61272	LT
92.118.112.143	11 / 94	215540	US
92.118.112.208	11 / 94	215540	US

Figure 6: IP addresses seen delivering the JSON file. Source: https://www.virustotal.com/gui/file/54477efe7ddfa471efdcc83f2e1ffb5687ac9dca2bc8a2b86b253cdbb5cb9c84/relations

When checking for the other IP addresses, we noticed that some of them were related to specific known threats:

IP address	Threat	AS
108.62.141[.]161	Rhysida ransomware[17] and Vice Society PortStarter tool[18]	AS 396362 (LEASEWEB-USA-NYC)
156.96.62[.]58	Rhysida ransomware[19] and Vice Society PortStarter tool[20]	AS 46664 (VDI-NETWORK)
194.34.246[.]90	Vice Society ransomware[21]	AS 51508 (Uzum Technologies FC LLC)

[17] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a
[18] https://news.sophos.com/en-us/2023/11/10/vice-society-and-rhysida-ransomware/
[19] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a
[20] https://news.sophos.com/en-us/2023/11/10/vice-society-and-rhysida-ransomware/
[21] https://us-cert.cisa.gov/ncas/alerts/aa22-249a

172.86.123[.]127	Silent Skimmer[22] and BlackCat's Cobalt Strike	AS 14956 (ROUTERHOSTING)
23.254.167[.]63	Bumblebee[23]	AS 54290 (HOSTWINDS)
172.96.139[.]82	Eye Pyramid C2[24]	AS 395092 (SHOCK-1)
212.87.222[.]84	Eye Pyramid C2	AS 215540 (Global Connectivity Solutions Llp)
142.234.157[.]35	Unknown	AS 395954 (LEASEWEB-USA-LAX)
216.74.123[.]41	Possibly Rhysida[25]	AS 396356 (LATITUDE-SH)
51.89.137[.]8	Possibly Rhysida[26]	AS 16276 (OVH SAS)
83.166.150[.]213	Havok and Meterpreter (potential Red Team)	AS 29222 (Infomaniak Network SA)

Overall, all these IP addresses appear related to malicious activity, and are linked to this unique JSON file. The content of the JSON file is the following:

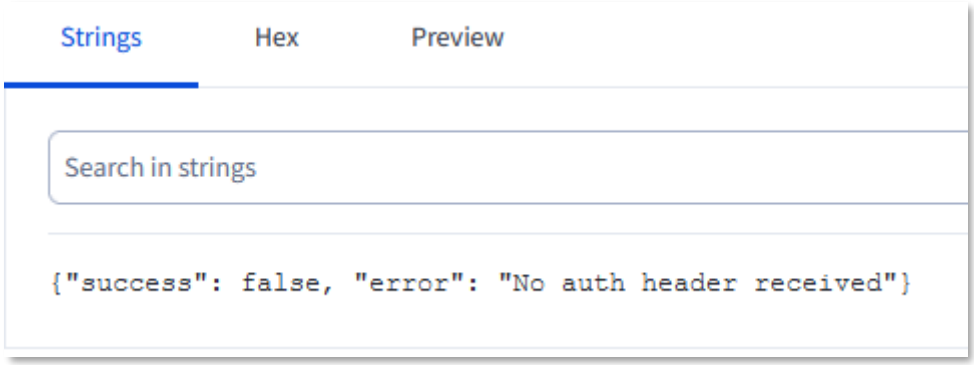


Figure 7: Content of the JSON file.

It corresponds to strings found in Eye Pyramid server's code on GitHub. Specifically, it is a server response error when there is no 'Authorization' in the header of a request to the server.

[22] https://unit42.paloaltonetworks.com/silent-skimmer-latest-campaign/
[23] https://0xtoxin.github.io/malware%20analysis/Bumblebee-DocuSign-Campaign/
[24] https://thedfirreport.com/2024/12/02/the-curious-case-of-an-egg-cellent-resume/
[25] https://www.guidepointsecurity.com/blog/update-from-the-ransomware-trenches/
[26] https://www.guidepointsecurity.com/blog/update-from-the-ransomware-trenches/

```
def do_GET(self):
        self.parsed_options=options
        key = self.server.get_auth_key()

        ''' Present frontpage with user authentication. '''
        if self.headers.get('Authorization') == None:
                self.do_AUTHHEAD()

                response = {
                        'success': False,
                        'error': 'No auth header received'
                }
```

Figure 8: Eye Pyramid's server response corresponding to the content of the JSON file: https://github.com/naksyn/Pyramid/blob/main/Server/pyramid.py

6. Additional Pivots

The IP address 195.20.18[.]146[27], associated recently with an Eye Pyramid C2, exposes an "Index of" with various files. On our OpenCTI instance, we noted that several files hosted on this server were related to stealers such as Lumma, Purelogs and Phemedrone.

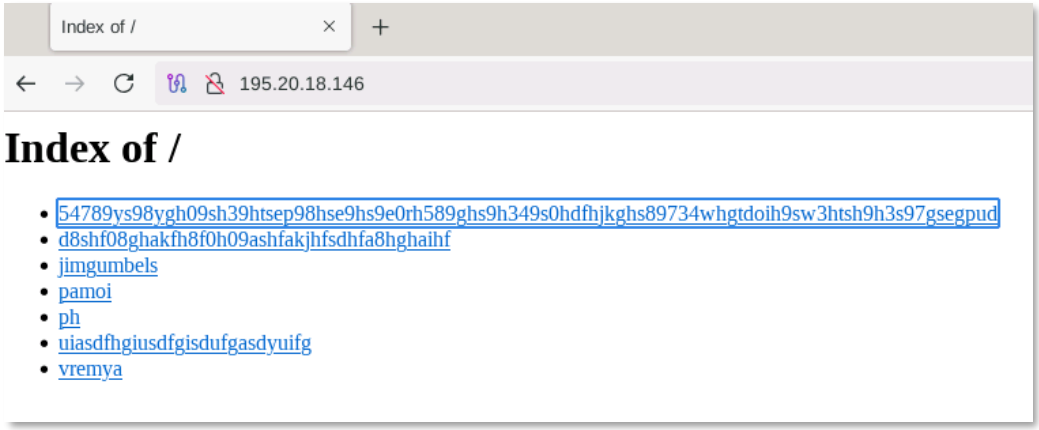


Figure 9: "Index of" on IP address 195.20.18[.]146.

6.1 SSL JARM

From the IP address 45.79.218[.]7, detected as related to Sliver and exposing the Eye Pyramid server response, the JARM of the SSL certificate (**3fd06c20d00000006c43d06c06c43d41226dd5dfc615dd4a96265559485910**) returns 3 additional IP addresses, which could indicate that they were setup by the same threat actor.

[27] https://www.virustotal.com/gui/ip-address/195.20.18.146/relations

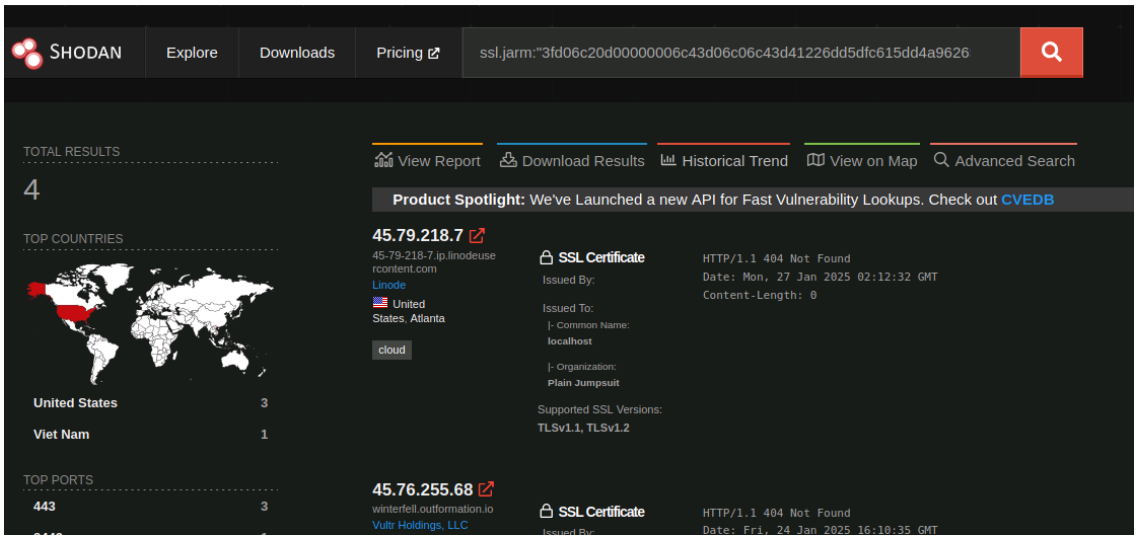


Figure 10: Results for the Shodan query on the ssl jarm. Source: https://www.shodan.io/search?query=ssl.jarm%3A%223fd06c20d00000006c43d06c06c43d41226dd5dfc615dd4a96265559485910%22.

Two of the three new IP addresses were detected as being related to Sliver C2, 45.76.255[.]68[28] and 61.28.233[.]21[29]. We suspect that this JARM may be associated with a malicious threat actor's infrastructure, which **leverages Sliver C2 and Eye Pyramid C2**.

JARM fingerprint

JARM is a **TLS server fingerprinting** application released as an open-source project by Salesforce[30]. The tool shares some similarities with the JA3 signatures, released by the same team, which passively examines network traffic collecting fingerprints from clients and servers alike.

The active constituent in JARM comes from its ability to **send 10 customized TLS ClientHello** packets to a target TLS server in the search for a unique set of responses; aggregating and hashing these in such a way as to create what is called a JARM fingerprint. JARM utilizes a **fuzzy hashing technique that concatenates** two consecutive 30-character and 32-character long blocks into one fixed-length crypto hash to produce a final 62-character fingerprint. The first block bears aspects like **TLS versions and ciphers chosen by the server** in response to each ClientHello packet sent by the client, whereas the second block represents a truncated **SHA256 hash of the server-side extensions**. As a result, individual servers can be quickly identified from a list of pre-compiled JARM fingerprints for a multitude of purposes.[31]

Network defenders and threat hunters can use JARM to **detect potentially malicious activity** threatening their environments.

[28] https://www.virustotal.com/gui/ip-address/45.76.255.68/relations
[29] https://www.virustotal.com/gui/ip-address/61.28.233.21/community
[30] https://engineering.salesforce.com/easily-identify-malicious-servers-on-the-internet-with-jarm-e095edac525a/
[31] https://securitytrails.com/blog/jarm-fingerprinting-tool

The IP address 96.30.199[.]157 also exposed an interesting SSL JARM (**2ad2ad0002ad2ad0000000000000009ae424f0795ef87e3214be6b18081e15**) that returned 24 IP addresses:

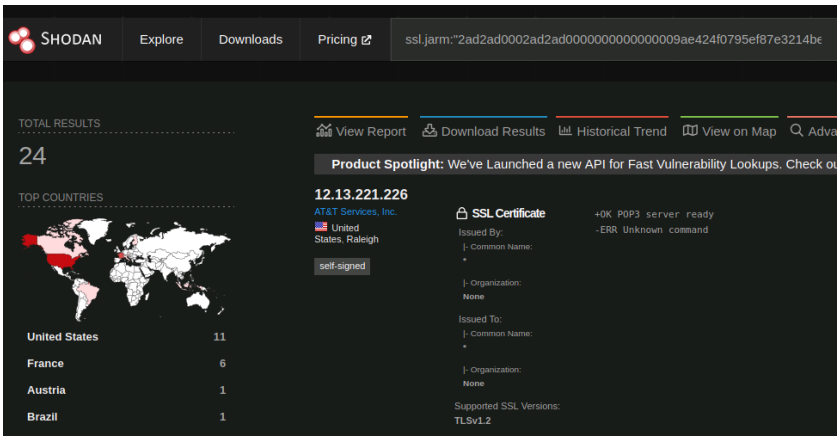


Figure 11: Results for the Shodan query on the ssl jarm. Source: https://www.shodan.io/search?query=ssl.jarm%3A%222ad2ad0002ad2ad0000000000000009ae424f0795ef87e3214be6b18081e15%22.

However, from this cluster we only noted 2 potentially malicious IP addresses, 185.206.146[.]56[32] and 47.96.137.203[33]. As such, we cannot classify this Jarm as pertinent and should not be used to track malicious infrastructure.

6.2 WIN-4NHED479K4N

We also came across the machine name **WIN-4NHED479K4N**, on IP address 87.120.112[.]252, which is associated with autonomous systems **Ekabi**, **Nybula**, **Cheapy Host** and **Zhongguanchun**. As a reminder, all of them are sub brands of the hosting provider **Limenet**. This machine name is still a significant indicator for detecting infrastructure related to this bulletproof hosting provider.

[32] https://www.virustotal.com/gui/ip-address/185.206.146.56/relations
[33] https://www.virustotal.com/gui/ip-address/47.96.137.203/relations

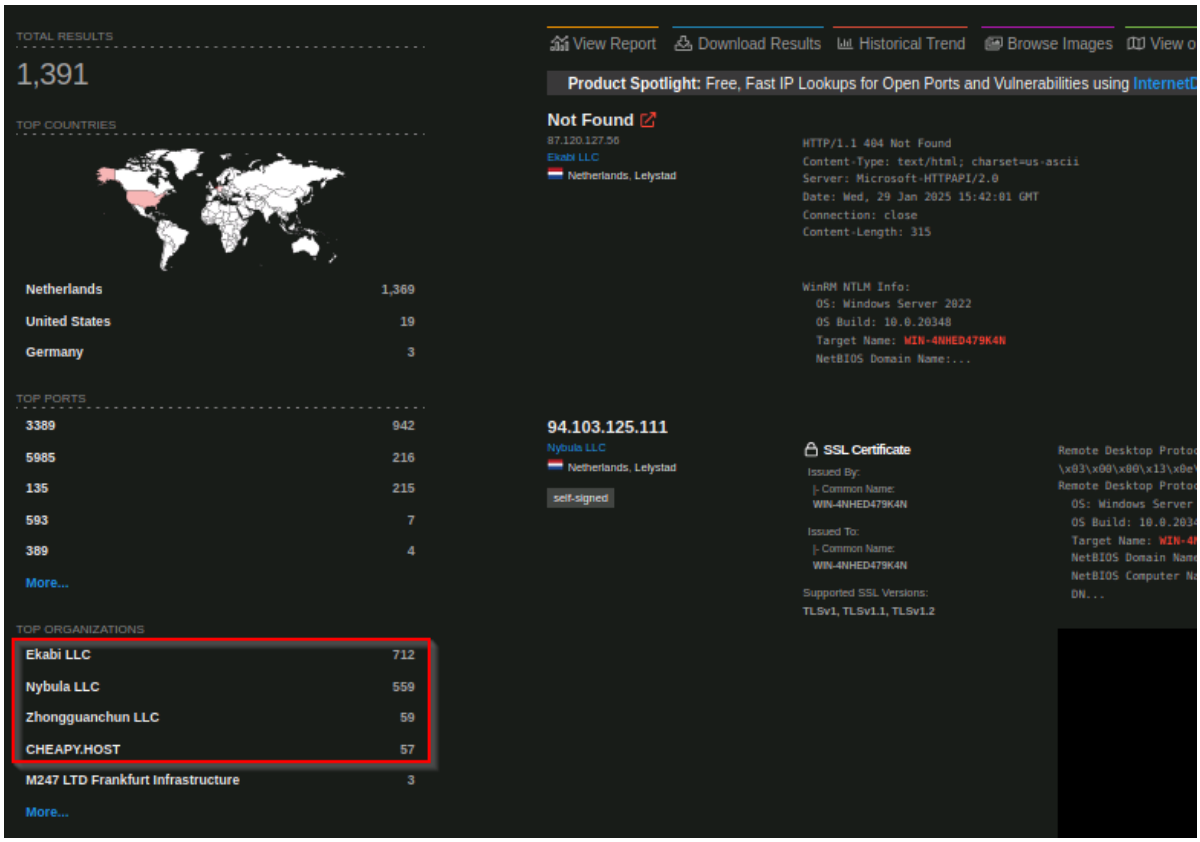


Figure 12: Results for the Shodan query on the machine name "WIN-4NHED479K4N", which shows its link to Limenet's infrastructure. Source: https://www.shodan.io/search?query=WIN-4NHED479K4N.

7. Conclusion

Post-compromise tools come in varied form but remain effective for attackers to move laterally on networks and deploy additional payloads. They are a tool of choice especially for ransomware operators, as they need to discover networks and infect multiple machines.

In this report, we analyzed infrastructure associated with the post-compromise tool Eye Pyramid C2, linked with a few additional payloads including ransomwares such as Rhysida, RansomHub and Vice Society.

Based on our findings, we can assess that at least one affiliate of Rhysida started using Eye Pyramid C2, maybe as a post-intrusion tool to deliver additional tools and its ransomware, elevate privileges and move laterally on compromised networks. A documented affiliate/cluster, who switched from Vice Society to Rhysida, was also related to this infrastructure via a specific JSON file. This file communicates only with IP addresses associated with Eye Pyramid, C2 of ransomwares and other threats. However, there is also a possibility that infrastructure from past compromise may have been shared and reused by other threat actors. A similarity in the server response from RansomHub's Python backdoor and the default Eye Pyramid server setup suggests that, at least on the server side, there may be a link between the python backdoor and code from Eye Pyramid.

Intrinsec CTI will continue to track this cluster of activity, which may further reveal links between various ransomwares and Eye Pyramid.

8. Actionable content

8.1. Indicators of compromise

Value	Type	Description
104.238.61.144	IPv4	RansomHub's python backdoor
108.181.115.171	IPv4	RansomHub's python backdoor
108.181.182.143	IPv4	RansomHub's python backdoor
172.210.82.245	IPv4	RansomHub's python backdoor
173.44.141.226	IPv4	RansomHub's python backdoor
185.174.101.240	IPv4	RansomHub's python backdoor
185.174.101.69	IPv4	RansomHub's python backdoor
23.227.193.172	IPv4	RansomHub's python backdoor
23.92.31.138	IPv4	RansomHub's python backdoor
37.1.212.18	IPv4	RansomHub's python backdoor
38.180.81.153	IPv4	RansomHub's python backdoor
45.66.248.150	IPv4	RansomHub's python backdoor
45.82.85.50	IPv4	RansomHub's python backdoor
5.8.63.178	IPv4	RansomHub's python backdoor
88.119.175.65	IPv4	RansomHub's python backdoor
88.119.175.70	IPv4	RansomHub's python backdoor
92.118.112.143	IPv4	RansomHub's python backdoor
92.118.112.208	IPv4	RansomHub's python backdoor (after SocGholish)
185.219.220.175	IPv4	RansomHub's python backdoor
155.138.253.99	IPv4	Eye Pyramid C2
23.29.118.81	IPv4	Cobalt Strike (2023)
93.82.24.249	IPv4	Eye Pyramid C2
193.58.121.231	IPv4	Eye Pyramid C2
194.102.104.24	IPv4	Eye Pyramid C2
194.102.104.25	IPv4	Eye Pyramid C2
195.20.18.146	IPv4	Eye Pyramid C2 and stealers
87.120.117.78	IPv4	Eye Pyramid C2
146.80.87.141	IPv4	Eye Pyramid C2
93.123.72.42	IPv4	Eye Pyramid C2
62.76.251.43	IPv4	Eye Pyramid C2
45.86.231.115	IPv4	Eye Pyramid C2
54.38.94.225	IPv4	Eye Pyramid C2
81.177.215.62	IPv4	Eye Pyramid C2
172.96.139.82	IPv4	Eye Pyramid C2 (seen by DFIRreport)
185.196.9.92	IPv4	Eye Pyramid C2 and Cobalt Strike
45.79.218.7	IPv4	Eye Pyramid C2 and Sliver C2

91.231.186.174	IPv4	Eye Pyramid C2 and Rhysida ransomware
195.177.95.163	IPv4	Eye Pyramid C2
188.23.170.151	IPv4	Eye Pyramid C2
195.208.25.141	IPv4	Eye Pyramid C2
179.60.147.67	IPv4	Eye Pyramid C2
212.87.222.84	IPv4	Eye Pyramid C2
198.134.107.41	Ipv4	Eye Pyramid C2
93.82.29.21	Ipv4	Eye Pyramid C2
45.76.255.68	IPv4	Sliver C2
61.28.233.21	IPv4	Sliver C2
67c6fd2b54382a5f399725d592543ff2eb54db8685966132f403110209f58db4	SHA256	Eye Pyramid module
108.62.141.161	IPv4	Rhysida ransomware
156.96.62.58	IPv4	Rhysida ransomware/ Vice society portstarter tool
194.34.246.90	IPv4	Vice Society ransomware
23.254.167.63	IPv4	Bumblebee C2
172.86.123.127	IPv4	Silent Skimmer
54477efe7ddfa471efdcc83f2e1ffb5687ac9dca2bc8a2b86b253cdbb5cb9c84	SHA256	1. JSON file communicating with malicious IPs

8.2. Recommendations

- Block the IOCs provided in the "Indicators of compromise" section of this analysis and subscribe to a CTI feed to obtain fresh IOCs related to Eye Pyramid C2 and ransomware threats. Intrinsec offers its own CTI feed to enhance your detection and response capabilities: https://www.intrinsec.com/en/cyber-threat-intelligence-feeds/
- Consider blocking the execution of "Python.exe" for users who do not need it. For further protection, block binaries and dlls signed by "Python Foundation", creating exceptions only for users who need to use Python.
- Apply a least privilege policy, limiting administrators access only to users who need it. Don't let administrators account on systems that don't need it.
- Delete unused accounts that could be exploited for compromise or post-exploitation.
- Train your employees to recognize phishing attempts, which may take the form of malicious emails containing files or links to malicious domains.
- Put in place a data backup policy. Backups serve as a safety net if files are encrypted. Store them offline or on separate networks to protect against lateral movement by attackers.
- Encrypt sensitive data and data at rest to prevent its leak in case of a ransomware compromise.
- Have a documented and tested emergency plan to act in case of a ransomware infection.

9. Sources

- https://threatfox.abuse.ch/browse/malware/win.eye_pyramid/
- https://www.naksyn.com/edr%20evasion/2022/09/01/operating-into-EDRs-blindspot.html
- https://news.sophos.com/en-us/2023/11/10/vice-society-and-rhysida-ransomware/
- https://www.guidepointsecurity.com/blog/ransomhub-affiliate-leverage-python-based-backdoor/
- https://www.reliaquest.com/blog/new-python-socgholish-infection-chain/
- https://thehackernews.com/2024/07/scattered-spider-adopts-ransomhub-and.html
- https://www.cyber.nj.gov/Home/Components/News/News/1448/214
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a
- https://www.guidepointsecurity.com/blog/update-from-the-ransomware-trenches/
- https://us-cert.cisa.gov/ncas/alerts/aa22-249a
- https://unit42.paloaltonetworks.com/silent-skimmer-latest-campaign/
- https://thedfirreport.com/2024/12/02/the-curious-case-of-an-egg-cellent-resume/
- https://0xtoxin.github.io/malware%20analysis/Bumblebee-DocuSign-Campaign/
- https://research.checkpoint.com/2023/the-rhysida-ransomware-activity-analysis-and-ties-to-vice-society/
- https://www.microsoft.com/en-us/security/blog/2022/10/25/dev-0832-vice-society-opportunistic-ransomware-campaigns-impacting-us-education-sector/