ISAC - United Against Ransomware

Back to Blog

Threat Intelligence 45 min readNovember 13, 2025

Infrastructure AnalysisDFIRAttributionDPRK

Cross-Chain TxDataHiding Crypto Heist: A Very Chainful Process (Part 3)

In collaboration with: Bridewell

Deep dive into the adversary infrastructure, operational security measures, and attribution analysis of the DPRK-linked campaign, revealing infrastructure fingerprints, C2 clusters, and connections to known threat groups.

Yashraj Solanki

Contributors: Gavin Knapp, Joshua Penny, Ellis Stannard, Tammy Harper

Share:

Executive Summary

Crystal Intelligence to investigate a cryptocurrency and data theft attempt via a private weaponised GitHub repository. What initially appeared to be a standard phishing campaign, quickly evolved into something far more sophisticated—a multi-layered attack leveraging novel blockchain-based command-and-control infrastructure and cross-platform malware designed to compromise development environments at scale.

Part 1 of this series delves into the sophisticated nature of a potentially attributed DPRK campaign where novel tradecraft such as Cross-Chain TxDataHiding techniques combined with the subsequent creation of a takedown-proof Command and control (C2) infrastructure. Part2 continues with a holistic analysis of the core malicious payloads with a complete view into the entire kill chain.

Part 3 aims to expand on the findings from parts 1 and 2 with a focus on the infrastructure leveraged by the threat actor during the campaign which can support attribution during the later stages. Through the understanding of the operational infrastructure, we aim to uncover other related clusters through our analysis, using infrastructure fingerprinting and wider open-source intelligence in order to explore potentially related campaigns.

Bridewell to conduct the comprehensive infrastructure analysis and attribution assessment detailed in this report. Bridewell's expertise in threat infrastructure tracking and OPSEC analysis was instrumental in developing the infrastructure fingerprints and cluster analysis presented here. We extend our sincere thanks to the Bridewell team for their invaluable contributions to this research effort and their commitment to advancing the cybersecurity community's understanding of sophisticated threat actor infrastructure.

It is worth noting that as efforts are made to reduce bias while correlating our infrastructure findings with what is known from parts 1 and 2, any attribution made during this part is kept independent to the previous parts. Only where correlation is required, the relevant connections are retrieved and built upon. With all infrastructure tracking engagements, no prior attribution assessments influence our analysis in order to deliver an unbiased, independent evaluation.

Should you have any information that can potentially support or refute our analysis, please feel free to reach out to us at Ransom-ISAC. As and where assumptions or estimates are made to fill the gaps in our analysis, they have been stated clearly so that the reader is aware.

Infrastructure Analysis

This section will explore the adversary infrastructure in detail to provide insights into some of the Operational Security (OPSEC) measures taken by the adversary during the intrusion to impair attribution. We shall start with a recap of the main types of infrastructure found in the previous part and the known IP addresses.

Intrusion C2 Channels

There are primarily two types of C2 channels previously identified based on the type of C2 mechanism and the different payloads distributed. The Python dropper communicating on a HTTP API C2 channel over port 27017 and the Loader/RAT communicating over both HTTP API and socket.io channels on C2 ports 27017 and 443 respectively. The two types of C2 channel are as follows:

- **HTTP API:** `http://[server]:27017`
- **Command Socket:** `http://[server]:443` (WebSocket via socket.io)

These C2 channels are also responsible for hosting payloads found during the various stages of the infection chain in addition to the conventional C2 capabilities such as remote commands execution and data exfiltration.

Note: For the purpose of our analysis, it is not required to treat the infrastructure differently based on the payloads since the two types of channels are sufficient for building infrastructure fingerprints. For more information on the implementation of the C2 channels by the malware, please check out part 2.

Analysis from parts 1 and 2 identified **4** unique C2 IP addresses discovered either, directly through tracing the complex infection chain or, configured as alternate/fallback hard-coded values in the malicious payloads acting as a fail safe mechanism in the event the primary channel is not able to establish connection with patient zero.

C2 IP Addresses	C2 Port	C2 Channel Type	Malware
23.27.20[.]143	27017	HTTP API	Python Dropper
136.0.9[.]8	27017, 443	HTTP API, socket.io	Loader/RAT
166.88.4[.]2	27017, 443	HTTP API, socket.io	Loader/RAT
23.27.202[.]27	27017, 443	HTTP API, socket.io	Loader/RAT

C2 Components

Note: There is discrepancy in the first seen dates for the listed C2s and those identified later as an outcome of the infrastructure fingerprinting efforts. This is due to the interval of the C2 services and ports crawled by the internet scanners which has inadvertently created blind spots. The earliest date from the selection of internet scanners was considered, these should be treated as estimates only.

The section is divided into two sub-sections based on the type of leveraged C2 channel.

Dropper C2: HTTP API

Let's begin our analysis with the IP address `23.27.20[.]143` - identified during the intrusion. The reason to select this IP address is it's prevalence in the previously conducted intrusion analysis and the standalone focus on HTTP API as a C2 channel. We will explore socket.io as a C2 at a later point.

- **Source IP address:** `23.27.20[.]143`
- **Source Location:** United Kingdom
- **Primary C2 Port:** 27017
- **Alternate C2 Port:** 5432
- **Status:** ACTIVE
- **First C2 Configuration Seen:** 6th August 2025

Through the use of internet scanners, the following HTTP header configuration was identified and associated with the source IP address.

```
HTTP/1.1 404 Not Found
Access-Control-Allow-Origin: *
Cache-Control: no-store, no-cache, must-revalidate
Connection: keep-alive
Content-Type: text/html; charset=utf-8
Date: Fri, 31 Oct 2025 00:23:35 GMT
Expires: Sat, 26 Jul 1997 05:00:00 GMT
Keep-Alive: timeout=15,max=100
Last-Modified: Fri, 31 Oct 2025 00:23:35 GMT
Pragma: no-cache
Server: EmbedIO/3.5.2
Content-Length: 0
```

Note: The above header configuration was obtained using an internet scanner and is different from the HTTP response captured during the original intrusion analysis. The fundamental difference resides in the HTTP status code, content length and encoding that would have influenced the fingerprint creation.

One of the possible reasons behind this mismatch could be, how the operator had set up the infrastructure to improve their OPSEC and prevent the various internet scanners from crawling that would rely on default options, modules and/or user agents to probe the IP addresses.

Common HTTP API C2 Characteristics

With respect to IP address leveraging the HTTP API C2 channel, all four C2 IP addresses have the following characteristics in common:

1. HTTP Header Configuration

Server and version: `EmbedIO/3.5.2`

EmbedIO is a lightweight open-source web server by Unosquare which is available for users to download from the GitHub. The server is built for .NET Framework and .NET Core with the latest version 3.5.2 that released in November 2022. Some of the key features include:

- Cross-platform: tested on multiple OS and runtimes
- Extensible: Write your own modules
- Create REST APIs quickly with the out-of-the-box Web API module
- WebSockets support
- Create GUIs for Windows services or Linux daemons

The cross platform capability of the server is on par with the payloads designed for the intrusion. The modular and light weight nature along with the convenience of creating GUIs makes it a lucrative choice for an adversary. From an infrastructure tracking standpoint, currently, at the time of writing this, there are only 300 servers deployed in the wild with this specific version of EmbedIO which can be considered rare.

2. HTTP Header Setting - Expires Field

The value `Expires: Sat, 26 Jul 1997 05:00:00 GMT` in the HTTP header appears to stand out. The value is clearly older than today's date. The significance of using an Expires header that has a past value is an older (HTTP/1.0) method for controlling the cache. This is contradicting since the HTTP method above is HTTP/1.1. The more modern (HTTP/1.1) has a more effective way to prevent caching by using the *Cache-Control* header which is already being used in the above HTTP header with the correct parameters *Cache-Control: no-store, no-cache, must-revalidate*. If a modern browser sees both, it will obey *Cache-Control* and ignore *Expires*.

Additionally, the specific use of this exact date value is probably inspired from an older PHP documentation that referenced it as an example. Also, the day and date combination does not logically add up, the correct day is Monday for that date, not Saturday. There are roughly 20,000 servers with this date value, which is low and a vast majority of them use HTTP/1.1. This past date setting (even on the HTTP/1.1 method) is likely and deliberately set by the operator for backward compatibility to ensure that even very old clients or proxies that don't understand *Cache-Control* will still see the past *Expires* date and know not to cache the content.

3. HTTP Header Setting - Keep Alive

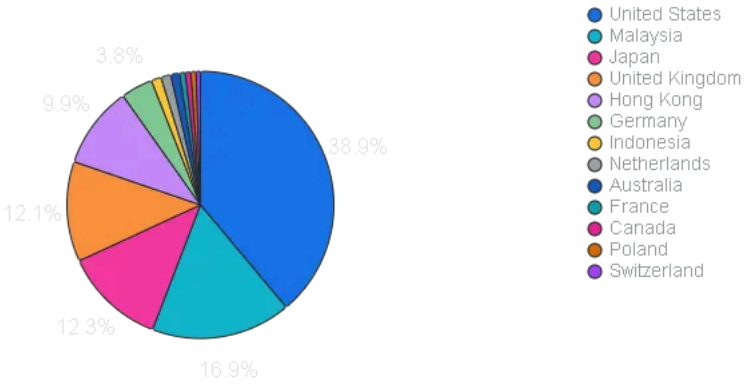
Keep-Alive: `timeout=15,max=100` value in the HTTP header is set to ensure that victims always make a new request to the server when interacting with it. From an operator's perspective, it is defining the limits for the C2 beaconing time intervals opting for a persistent connection with the C2. The specific parameters are set to let the server know to only keep a connection open for a window of **15 seconds** after the last response is sent.

If the client does not send a new request within that defined time frame, the server will close the connection to free up the resources. Also, the server will allow a maximum of **100 total requests** to be sent over a single connection after which an existing connection is closed and a new one is required. At the time of writing this, 50,000 servers globally are configured with this setting.

4. Hosted Infrastructure

Autonomous System Number (ASN): AS149440

Organisation Name: Evoxt Enterprise



The organisation has a 3 year old autonomous system (AS) for its network infrastructure, which allows it to provision its own network routing. It also provides virtual machines, or Virtual Private Servers (VPS), with a focus on low-cost and high-performance options. The ASN is primarily hosting servers located in the US with global presence extending to Malaysia, Japan, UK, Hong Kong and Germany to name a few.

Threat actors often use such dedicated VPS to host their C2s giving them a more granular control over the infrastructure. It is also common for threat actors to spin up their infrastructure in the same region as the victims to avoid any network traffic from being dropped due to geo-blocking. In a later section *ASN Overview*, we will sift through wider open-source intelligence to share sightings of known malware and threat groups that have used this ASN in the past.

The operator's choice to select this ASN could also be based on the overall good reputation. While there is evidence of historic malicious activity associated with this ASN, in general, this ASN is not widely flagged as a malicious network due to the overall low spam activity (less than 1%) in addition to not being listed on major, widespread blacklists. Abuse databases also show very few reports, with most being several years old and having a low confidence of abuse.

5. Network Ports Used

The primary port used for C2 is the TCP port **27017** which is a default port used by MongoDB databases to establish connection with the clients. The same HTTP headers configuration was also found on a different TCP port **5432** which can be treated as an alternate port for C2 that is typically used for PostgreSQL databases.

At this point, Despite observing only two ports under the same IP address, the threat actor's apparent preference for database-designated ports is noteworthy, especially considering the targets are developers.

6. Common Services, Ports and Configs

By considering the services, their ports and broader configuration, we can determine consistency between the already identified C2 servers, by logging volatility of the services. Furthermore, these can be combined with other meta data such as `First Seen` and `Last Seen` dates (active status) for the servers to provide a better clustering criteria based on such service statistics.

Concept of Service Hibernation Score (SHS)

From the duration, the `First Seen` C2 configuration was recorded and up until the `last seen` date, the calculation is based on the number of unique services observed divided by the number of times they have been changed/updated, we can derive what is informally known as **service hibernation score**. The primary significance of the score is to broadly understand the consistency of services configured on the infrastructure which can help assess if the same operators are still using the infrastructure or not.

For instance, if a server during its active period (time interval between first and last seen dates) had 5 unique services which were altered a total of 15 times, the calculated score would be (5 divided by 15) 0.33. Higher the SHS score, more consistent the services are. It is also important to understand that the accuracy of the score itself is highly influenced by the scanning interval of those services since it relies on the frequency of the services changed/updated.

C2 IP Addresses	C2 Port	Other Active Services	Other Ports	SHS
23.27.20[.]143	**27017**, 5432	**RDP, WINRM**	**3389, 5985**	0.034
136.0.9[.]8	**27017**, 443	**RDP, WINRM**, DCERPC, NETBIOS, SMB, Unknown	**3389, 5985**	0.050

C2 IP Addresses	C2 Port	Other Active Services	Other Ports	SHS
166.88.4[.]2	**27017**, 443	**RDP, WINRM**, DCERPC, NETBIOS, SMB, Unknown	**3389, 5985**, 135, 139, 445, 17500	0.049
23.27.202[.]27	**27017**, 443	**RDP, WINRM**, DCERPC, NETBIOS, SMB	**3389, 5985**, 135, 139, 445	0.041

Note: Please see that the above C2 port is still referring to HTTP based API channel and not socket.io. We will cover socket.io separately to avoid any confusion and hence port 443 is ignored.

While it is not specifically known, it can also be assessed with low confidence that the operators are using RDP to remotely access their C2 server with an assumption that the victim C2 connection (HTTP based API channel) terminates at C2 server and thereby not used by operator workstations.

7. RDP TLS Certificate Common Name (CN)

All IP addresses mentioned above have the issuer/subject CN of `EV-4A6OE6M0E2D` on their RDP TLS certificate. Currently, there are a 300 servers with the same CN.

Clustering Assessment Criteria

To recap, the following common factors were considered to split the resultant IP addresses obtained from the infrastructure fingerprint. The criteria is based on the following factors and further divided into low, medium and high confidence ratings. The factors are also listed in the increasing order of their significance:

- HTTP method and status code
- HTTP headers configuration
- Server and version used
- Hosted ASN
- Hosted C2 port
- Service hibernation score (SHS)
- RDP TLS certificate CN

Note: The confidence level is subject to change as we explore other relevant attributes in the subsequent sections such as **C2 URL paths, communicating payloads** and **hard-coded values** seen in the payloads.

Infrastructure Fingerprints

Upon consideration of the above attributes, an initial infrastructure fingerprint was constructed.

FINGERPRINT 1: `server="EmbedIO" && header="Expires: Sat, 26 Jul 1997 05:00:00 GMT" && header="HTTP/1.1 404 Not Found" && header="Content-Length: 0"`

Fingerprint 1 results in **11** unique IP addresses (inclusive of the **4** identified previously). These IP addresses are divided based on the clustering assessment criteria. For the purpose of attribution, all IP addresses were considered irrespective of their active status. The results are also classified as clusters based on common ASNs, and similar C2 ports (those seen associated with databases).

Results of Fingerprint 1:

Clusters	Confidence	IP Addresses	ASN	ASN Name	First Seen	Last Seen	C2 Ports
Cluster-1	HIGH	**23.27.20[.]143**	149440	Evoxt Enterprise	Sep 2025	ACTIVE	**27017**, 5432
Cluster-1	HIGH	**136.0.9[.]8**	149440	Evoxt Enterprise	Sep 2025	ACTIVE	**27017**
Cluster-1	HIGH	**166.88.4[.]2**	149440	Evoxt Enterprise	Sep 2025	ACTIVE	**27017**
Cluster-1	HIGH	**23.27.202[.]27**	149440	Evoxt Enterprise	Sep 2025	ACTIVE	**27017**
Cluster-1	HIGH	**23.27.120[.]142**	149440	Evoxt Enterprise	Oct 2025	ACTIVE	**27017**

Clusters	Confidence	IP Addresses	ASN	ASN Name	First Seen	Last Seen	C2 Ports
Cluster-1	HIGH	**154.91.0[.]103**	149440	Evoxt Enterprise	Feb 2025	Mar 2025	**27017**, 5432, 1433
Cluster-2	MEDIUM	**85.239.62[.]36**	62240	Clouvider Limited	May 2025	June 2025	27017
Cluster-2	MEDIUM	**85.239.60[.]213**	62240	Clouvider Limited	Feb 2025	Feb 2025	27017, 80
Cluster-3	LOW	**91.99.83[.]196**	24940	Hetzner Online GmbH	June 2025	June 2025	8080
Cluster-3	LOW	**37.27.108[.]244**	24940	Hetzner Online GmbH	June 2025	June 2025	8080
Cluster-3	LOW	**57.128.212[.]19**	16276	OVH SAS	May 2025	May 2025	8080

Notable Observations

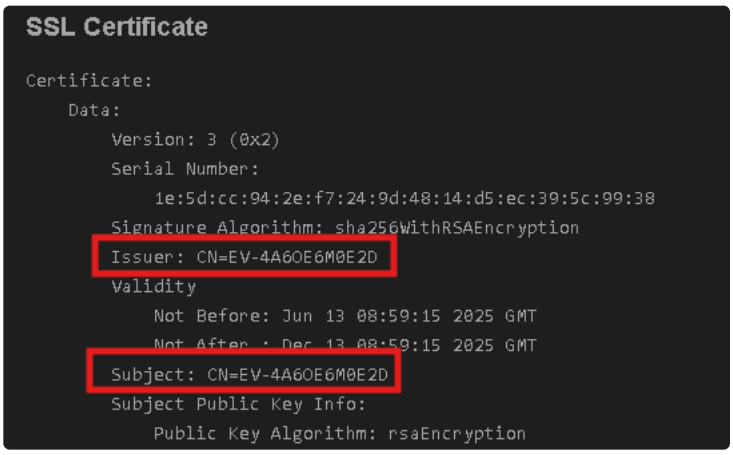
New C2 Ports

In addition to the discovered primary C2 ports, the list now includes, 27017, 5432, 1433, 8080 and 80. It is evident that the last two; 8080 and 80 are deviations from the initial assessment that the selected C2 ports were based on databases (it could also be possible that these ports only used for testing after which, they were migrated to the other ports). However, the inclusion of TCP port **1433** is able to compensate on the assessment made since it is the default port for Microsoft SQL servers.

ASN Groupings

- **Cluster-1** follows the common pattern of hosted ASN linked to original 4 C2 IP addresses which instills confidence to this cluster
- **Cluster-2** can be seen associated with a completely different ASN *Clouvider Limited*
- **Cluster-3** is a grouping of two different ASNs (Hetzner and OVH) which were not seen in other clusters. Both ASNs are known for having a bad reputation for hosting malicious infrastructure

RDP TLS Certificate CN



While it is not mentioned in the table above, all IP addresses linked to Cluster-1 (not just the 4 original ones) have the same RDP TLS Certificate CN `EV-4A6OE6M0E2D`. Currently, there are over 1500 servers with this RDP TLS certificate with a vast majority belonging to Evoxt.

However, Cluster-2 has a common RDP TLS certificate CN pattern of `PACKERP-XXXXXXX`. Historically, there are only **17** IP addresses that have this CN pattern on RDP port 3389, each ending with a unique alphanumeric characters of fixed length. One the other hand, Cluster-3 has no RDP service linked to it.

Based on the recent last seen dates on the IP addresses, it might be worth tracking these under a separate cluster which may provide insights in the near future as to who is setting up such remote access. Of the 17 IP addresses, 9 were hosted in Russia and hosted on ASN-62005 **BlueVPS OU**. A vast majority of these are still active at the time of writing this.

Based on the common ASN (BlueVPS OU) and the RDP TLS certificate CN `PACKERP-XXXXXXX`, another cluster under the name **Cluster-X-RDP** was created to track operators setting up such remote access to the C2 servers in the near future.

Fingerprint 2: `(asn="62005" || asn="49392") && cert="PACKERP-" && port="3389"`

Cluster-X-RDP

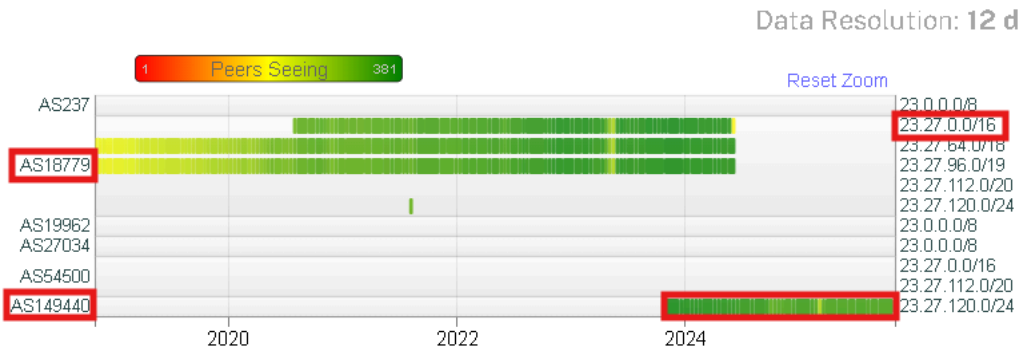
IP Addresses	First Seen	Last Seen
91.242.241[.]31	Nov 2024	ACTIVE
91.242.241[.]170	Apr 2025	ACTIVE
91.242.241[.]117	Apr 2025	ACTIVE
91.242.241[.]122	May 2025	ACTIVE
91.242.241[.]15	Dec 2024	ACTIVE
91.242.241[.]174	Nov 2024	ACTIVE
91.242.241[.]55	Nov 2024	Jun 2025
91.242.241[.]183	Dec 2024	ACTIVE
62.106.66[.]151	Dec 2024	Sep 2025
45.129.199[.]127	Apr 2025	ACTIVE
45.86.231[.]67	Jan 2025	ACTIVE

Another pattern we observed is that many active IP addresses were hosted on a different ASN-49392 **LLC Baxet** prior to being hosted on *BlueVPS*. Based on that observed infrastructure pattern, it can be forecasted that IP address `91.242.241[.]55` with last seen date of June 2025 will be hosted on BlueVPS in the near future.

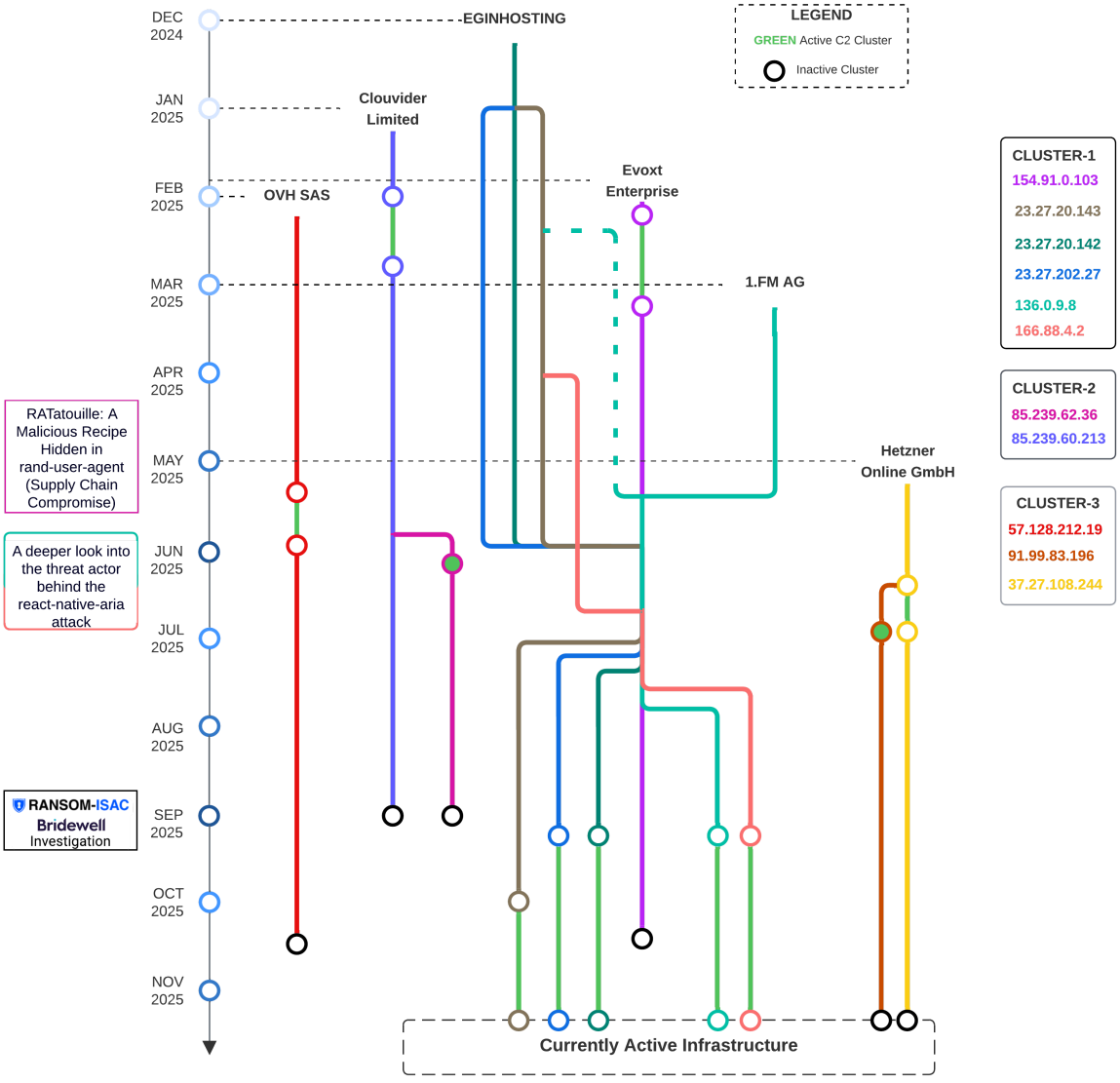
Hosting Timeline Analysis

Clusters 1,2 and 3 have a notable pattern pertaining to the choice of ASN selected for their operations. The selection of *Evoxt Enterprise* for Cluster 1 as the preferred ASN combined with other infrastructure attributes is unique enough to track the cluster.

Prior to using that ASN, the set of IP addresses from cluster 1 were observed on a different ASN **EDINHOSTING**. To determine when the shift in the ASNs occurred, we leveraged the routing history for IP addresses in clusters 1,2 and 3.



The diagram below may assist with better visualisation of the hosted infrastructure changes. The green lines and circles indicate the actual time frame when the infrastructure was observed exhibiting C2 properties. Green-filled circles were used to showcase a shorter time span in comparison to the green lines.



The left side of the diagram maps open-source reporting to the C2 indicators. We shall build upon those references in the later sections. From the diagram, it can be deduced that some cluster IP addresses have a longer active C2 behaviour while others such as `85.239.62[.]36` and `57.128.212[.]19` were short lived (green-filled circles). Also, IP addresses in cluster 1 have a consistent pattern of previously being hosted on a different ASN compared to the one observed during the intrusion.

Alternate HTTP Status Code: OPSEC 302 Redirection

Note: It is worth reiterating that we mainly considered the HTTP status *404 Not Found* because this is what was observed on multiple internet scanners during the active timeline of the intrusion we were investigating.

However, during part 2 of the series (as mentioned under 302 Response (Easter Egg) section), while tracing the infection chain through different stages, an alternate **HTTP 302 Found** response was discovered where the perceived objective was to redirect unintended victims to a different location (in our scenario, to a specific GitHub link).

However, during part 2 of the series (as mentioned under 302 Response (Easter Egg) section), while tracing the infection chain through different stages, an alternate **HTTP 302 Found** response was discovered where the perceived objective was to redirect unintended victims to a different location (in our scenario, to a specific GitHub link).

Threat actors implement such redirections to ensure network traffic is directed to those that it is intended for, in order to bypass potential analysis through automated bots, sandbox environments and other means where default parameters are used to contact adversary infrastructure.

This is yet another added method to improve adversary's OPSEC but also provides with an opportunity to fingerprint this unique redirection. The ports **8080** and **8094** leveraged for redirection could also be indicative of potential logging activity which can be generally assessed as the adversary conducting counter intelligence on those analysts attempting to track their kill chain.

The primary infrastructure fingerprint (clusters 1,2 and 3) can be modified slightly to accommodate this redirection mechanism used by the threat actors by simply changing the HTTP status code which also gives rise to a new **Cluster-X-302** that results in **11** unique IP addresses, all **based in Russia** and under the same ASN **PJSC Megafon**.

Although, all 11 IP addresses originating from Cluster-X-302 are historic (not actively seen in 2025), these IP addresses could have been part of previously set up infrastructure that was probably used during the early stages and then disposed. We are likely to not see this cluster in the future. It is still worth recording this cluster for when we look into wider OSINT to check for any potential indicator overlap despite the cluster likely burnt and never to be used again.

Fingerprint 3: `server="EmbedIO/3.5.2" && banner="HTTP/1.1 302 Found Expires: Sat, 26 Jul 1997 05:00:00 GMT"`

Key Characteristics

- **OPSEC:** HTTP 302 Redirect
- **Hosted ports:** 8080, 8094
- **Location:** Russia, hosted on ASN 31213, PJSC Megafon
- **Attributes:** server, keep-alive date, content length and expiry date is same as clusters 1,2 and 3

Other Metadata

First Seen X-302 IP address: 6th Nov 2024

Last Seen X-302 IP address: 31st Dec 2024

Eagle Portal

Cluster-X-302

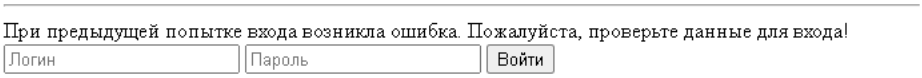
IP Addresses	First Seen	Last Seen
78.25.123[.]242	Dec 2024	Mar 2025
78.25.123[.]66	Nov 2024	Sep 2025
78.25.122[.]218	Nov 2024	Sep 2025
78.25.109[.]155	Nov 2024	Mar 2025
78.25.108[.]249	Nov 2024	Oct 2025
78.25.111[.]63	Dec 2024	Mar 2025

IP Addresses	First Seen	Last Seen
78.25.121[.]187	Nov 2024	Mar 2025
78.25.123[.]153	Nov 2024	Mar 2025
78.25.123[.]240	Nov 2024	Dec 2024
78.25.123[.]249	Nov 2024	ACTIVE
85.26.218[.]114	Nov 2024	ACTIVE

Currently, only `85.239.60[.]213` from Cluster-2 overlaps with activity timeline for this cluster. Also, for all IP addresses listed above, specifically on ports **8080** and **8094** (where the redirects were found), we also identified a web page what appears to be a login page with a Russian title **"Орлан 2.0 (веб-интерфейс)"** which translates to **Orlan 2.0 (web interface)**. All login pages have the same JavaScript likely used to track web cookies for the login page. Currently, the exact significance of **Orlan 2.0** is not known.

NOTE: The `js_md5` value is `736dd2e77c190d2eb418338f49dda10e`

Below is the view of the HTML content, without rendering images, other CSS element:



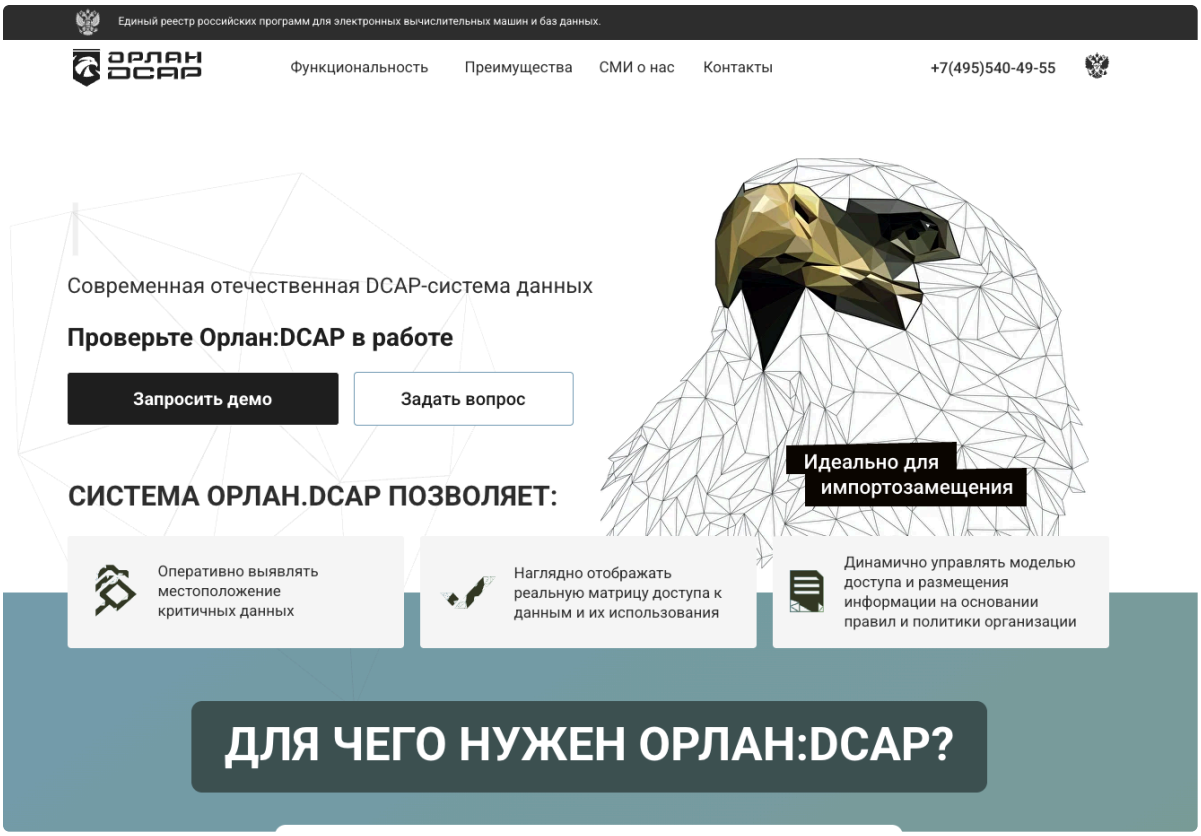
Note: It can be assessed that the naming convention for the login page could have possibly be inspired from an upgraded strike version of the Orlan-10 able to carry four high-explosive fragmentation projectiles was reportedly used in the 2022 Russian invasion of Ukraine which could potentially hint towards pro-Russian stance.

According to the Oryx website, at least 208 Orlan-10, 19 **Orlan-20**, and 16 Orlan-30 have been shot down as of February 12 2025, including by a UK-supplied Martlet missile. A version called Moskit is used for EW. However, this assessment should be considered low confidence at best due to lack of direct evidence supporting it.

Note: **Орлан (or Orlan) directly translates to 'eagle' in English.**

A plausible hypothesis with moderate-to-high confidence is that the "Орлан 2.0 (веб-интерфейс)" login pages observed across Cluster-X-302 infrastructure represent legitimate licensed deployments of Orlan Security's DCAP system (**https://orlan-security.ru**) being operationally employed by DPRK threat actors to systematically prioritise and optimise large-scale data exfiltration operations.

Given the DPRK attribution and the actor's established modus operandi focussed on data collection, DPRK operators may be deploying legitimate Orlan:DCAP licences on compromised victim networks to automate the identification of high-value data targets. Rather than manually searching through terabytes of victim data, the DCAP system would automatically scan and classify all unstructured data across compromised file servers, identify files containing intellectual property, financial records, trade secrets, and source code, and generate prioritised target lists showing which files are most sensitive based on content analysis using Orlan's built-in neural networks and pattern matching technologies. This would enable DPRK actors to maximise intelligence and financial value whilst minimising bandwidth consumption and detection risk—directly supporting known operational priorities including cryptocurrency exchange data theft, intellectual property exfiltration for state economic advancement, and financial fraud operations.

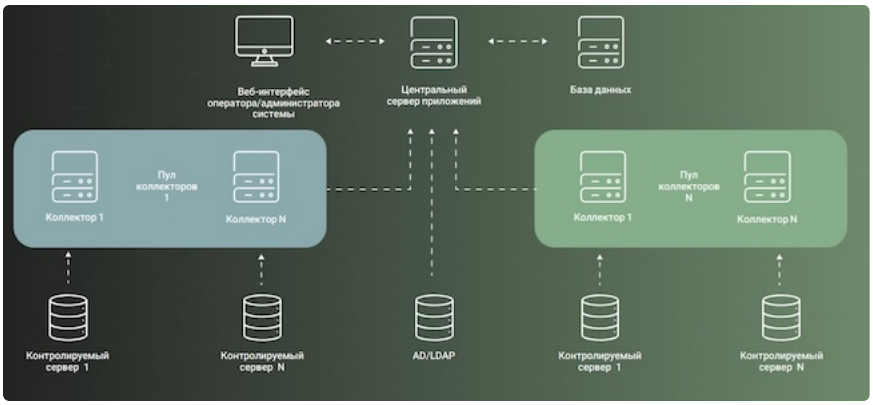


Source: https://orlan-security.ru/

DCAP stands for Data-Centric Audit and Protection - a security system that automatically discovers, classifies, and monitors unstructured data (files, emails, documents) across an organisation to identify where sensitive information is stored, who can access it, and what they're doing with it. DCAPs appear to be a hybrid of Data Loss Prevention (DLP) and Asset Inventory, popular within Russia.

Rather than manually searching through terabytes of victim data, the DCAP system would automatically scan and classify all unstructured data across compromised file servers, identify files containing intellectual property, financial records, trade secrets, and source code, and generate prioritised target lists showing which files are most sensitive based on content analysis using Orlan's built-in neural networks and pattern matching technologies.

The architecture diagram of Orlan:DCAP shows (in Russian):



Source: https://www.anti-malware.ru/analytics/Market_Analysis/DCAP-DAG-2025#part67

Components:

- **Веб-интерфейс оператора/администратора системы** = Web interface for operator/administrator of the system (top left - the login page from above)
- **Центральный сервер приложения** = Central application server (top center)
- **База данных** = Database (top right)
- **Пул коллекторов** = Pool of collectors (the agents - shown in boxes labeled "Коллектор 1" and "Коллектор N")
- **Контролируемый сервер** = Controlled/monitored server (bottom - showing multiple servers being monitored)

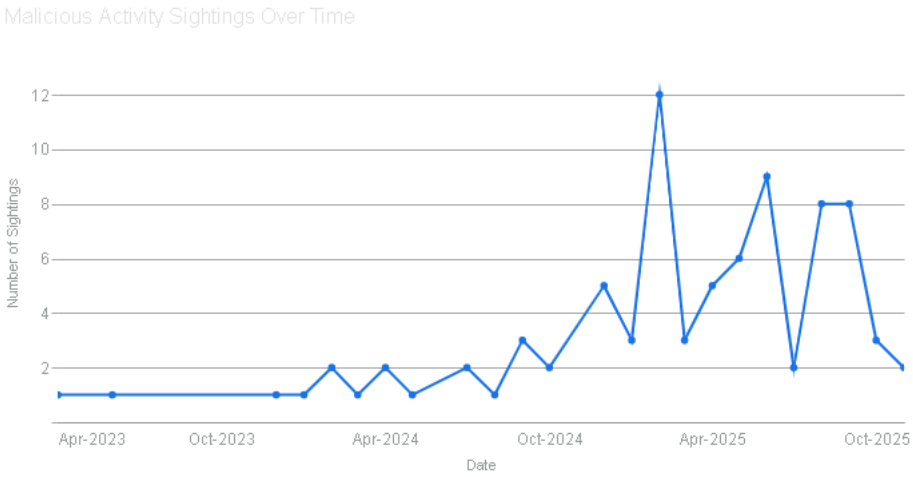
- **AD/LDAP** = Active Directory/LDAP (center bottom)

The operational workflow would involve: initial compromise of target organisations, deployment of legitimate Orlan:DCAP agents (which appear as authorised security software and evade detection), automated scanning and classification of the victim's entire data repository, DPRK operators accessing the centralised web interfaces (observed on ports 8080/8094) to review classification results, and executing targeted exfiltration focussing on pre-identified sensitive data.

ASN Analysis and Wider OSINT

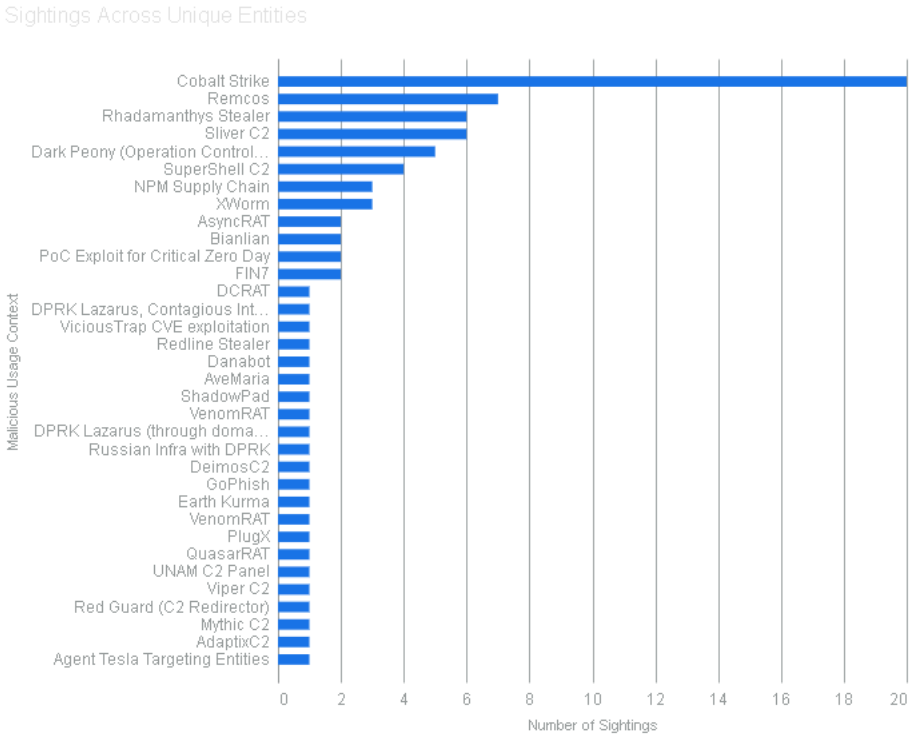
The ASN of choice for primary infrastructure (clusters 1,2 and 3) observed during the intrusion is **Evoxt Enterprise** (ASN: AS149440). This section aims to correlate any available open-source intelligence surrounding the usage of this ASN with any known malware or threat actors in addition to sharing external references where such documented intrusions/campaigns have been observed.

The IP address ranges were enumerated via the ASNs and then used to extract sightings into known reporting. Where possible, validation checks were conducted to ensure that the IP addresses actually belonged to the ASN when it was referenced in public reports.

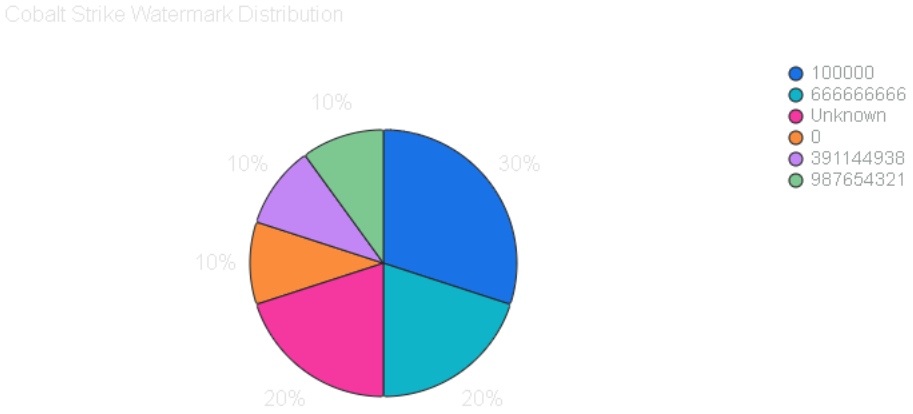


Key Observations:

A total of **84** unique sightings of malware and known threat groups were identified using this ASN over the last three years. The distribution is split between Offensive Security Tools (OST), commodity malware, custom malware used by nation states, CVEs exploitation and other reported campaigns.



Majority of the sightings were for Cobalt Strike C2 framework spanning across different Cobalt Strike Watermarks.



- 0 - The most common watermark, widely associated with cracked versions of Cobalt Strike
- 100000 - No attribution to known groups or operators
- 666666666 - A fixed value often associated with pirated copies
- 987654321 - A fixed value often associated with pirated copies
- 391144938 - Observed in reporting related to various Chinese nation state groups, such as Viper's Nest

Known Threat Groups

Group Name	Country Origin	Description
Dark Peony	China	Also known as RedDelta, the group has been active since at least 2012 and has focused on Southeast Asia and Mongolia. The group has routinely adapted its targeting in response to global geopolitical events. They evolved its infection chain multiple times since mid-2023.

Group Name	Country Origin	Description
FIN7	Russia	FIN7 is a financially-motivated threat group that has been active since 2013. FIN7 has targeted the retail, restaurant, hospitality, software, consulting, financial services, medical equipment, cloud services, media, food and beverage, transportation, pharmaceutical, and utilities industries in the United States.
Lazarus	DPRK	Lazarus Group is a North Korean state-sponsored cyber threat group attributed to the Reconnaissance General Bureau (RGB). Lazarus Group has been active since at least 2009. North Korea's cyber operations have shown a consistent pattern of adaptation, forming and reorganising units as national priorities shift.
Moonstone Sleet	DPRK	Moonstone Sleet is a North Korean-linked threat actor executing both financially motivated attacks and espionage operations. The group previously overlapped significantly with another North Korean-linked entity, Lazarus Group, but has differentiated its tradecraft since 2023.
APT29	Russia	APT29 is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR). They have operated since at least 2008, often targeting government networks in Europe and NATO member countries, research institutes, and think tanks.
Earth Kurma	Unknown	Earth Kurma is an APT group targeting government and telecommunications sectors in Southeast Asia, with a primary focus on data exfiltration. They employ advanced custom malware, including rootkits like KRNRAT and MORIYA, and utilise cloud storage services for exfiltration.

_V-Selected C2: SocketIO

So far we have discussed the HTTP API C2 channel (also known as the Dropper C2 from part 2 of the series), in this section we shall explore and build upon the secondary C2 infrastructure leveraging WebSocket via socket.io (also known as the _V-selected C2 from part 2).

It is also worth mentioning that there are some overlapping properties between the two C2 mechanisms. Hence, an attempt is made to cover only those aspects of socket.io C2 that were not previously mentioned in order to develop some unique insights into the utilised infrastructure.

Out of the 4 original IP addresses found during the intrusion analysis, **3** of them qualify as socket.io C2 on TCP port **443**.

- `23.27.202[.]27`
- `136.0.9[.]8`
- `166.88.4[.]2`

HTTP Headers

Revisiting the internet scanners and probing those HTTP response headers that are related to port 443, the following HTTP headers were identified during the C2 activity timeline:

```
HTTP/1.1 404 Not Found
Content-Security-Policy: default-src 'none'
X-Content-Type-Options: nosniff
Content-Type: text/html; charset=utf-8
Content-Length: 139
Date: REDACTED
Connection: keep-alive
Keep-Alive: timeout=5
```

The above headers on their own are not enough to create an infrastructure fingerprint. However, a couple of anomalies were recognised that may assist in an improved development of the fingerprint.

Infrastructure Fingerprint

While conventionally TCP port 443 is for HTTPS protocol, HTTP is being used for the C2 based on the absence of SSL certificate. By combining conventional HTTPS ports (such as port 443) with the listed specific headers in addition to checking for absence of SSL certificate, the following fingerprint was developed:

Fingerprint 4: `"HTTP/1.1 404 Not Found Content-Security-Policy: default-src 'none' X-Content-Type-Options: nosniff Content-Type: text/html; charset=utf-8 Content-Length: 139 Date: " "Connection: keep-alive Keep-Alive: timeout=5" has_ssl:false port:443 !tag:cloud`

The newly formed **Cluster-4** provides total of 18 IP addresses which were reduced down to **8** unique IP addresses by excluding those IP addressed that were hosted on cloud.

Additionally, half of resultant IP addresses had `Error` as their HTML title while the other half did not. It was decided to avoid using a filter based on HTML title in order to capture a broader set of results that can be used to check for indicator overlap with external reporting.

Alternatively, the above fingerprint can be made broader to capture more IP addresses while increasing risk of false positives. This can be done by including other ports that *could* implement HTTPS but typically don't. For example, adding the alternate port for HTTPS, port 8443 would have significantly increased the number of results.

Cluster-4

IP Addresses	ASN	Cluster Inclusion
136.0.9[.]8	Evoxt Enterprise	Part of Cluster 1
23.27.202[.]27	Evoxt Enterprise	Part of Cluster 1
166.88.4[.]2	Evoxt Enterprise	Part of Cluster 1
23.27.120[.]142	Evoxt Enterprise	Part of Cluster 1
181.117.128[.]64	AMX Argentina	NEW
183.101.157[.]30	Korea Telecom	NEW
195.122.31[.]246	VAKS, KOOPERATIVA SABIEDRIBA	NEW
202.155.8[.]173	CV. Rumahweb Indonesia	NEW

C2 URL paths

Both, the dropper and _V-Select C2s have the following URL paths:

HTTP API: `http://[server]:27017`

- `/verify-human/[version]` - Logging/telemetry
- `/u/f` - File upload endpoint
- `/snv` - endpoint name snv
- `/$/boot` - Python dropper
- `/$/z1` - Python Stealer

Command Socket: `http://[server]:443` (WebSocket via socket.io)

/socket.io/

Socket.io URLs

Full socket.io URL Structure: `http://[server_ip]:TCP_port/socket.io/?EIO=4&transport=polling&t=[0-9a-z]{8}`

- TCP_Port - port number, in our case, it is set to 443 (also port 3306 was seen on a different IP address) for the _V-Selected C2s
- EIO - Engine,IO version number which is equal to 4, the latest version of the protocol
- transport - The supported transport mechanism that is set to polling state, the other alternative state is Websocket
- t - Socket.io implements cache busting with a timestamp parameter in the query string. If you assign `timestampParam` a value of `ts` then the key for the timestamp would be `ts`, it defaults to `t` if no value is assigned.

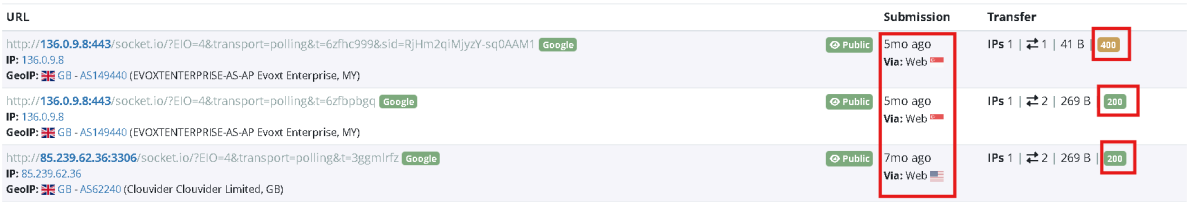
There is also a `sid` (Session ID) parameter that is mandatory for socket.io connections only after the session is established. Hence, if and only the server accepts connection, it will then respond with an `open` packet that contains this `sid` parameter embedded inside the JSON-encoded payload. The `sid` is required on *every* polling request *except* the very first one.

Here is a breakdown on the steps taken to establish a socket.io connection:

1. Initial Handshake: Client sends a request to server with defined `EIO` and transport parameters
2. Server Response: After receiving the handshake, server responds and creates a new session including the population of the `sid`.
3. All subsequent polling: Must now include the `sid` received from server after the initial handshake. Failure in appending the `sid` will result in a HTTP 400 error.

The common characteristics from the URL structure were leveraged (with inclusion of port 3306) to enumerate URL paths matching the criteria.

Search query (In-scope Ports): `(page.url:":443" OR page.url:":3306") AND page.url:"/socket.io/?EIO=4&transport=polling"`



Based on the results, only `136.0.9[.]8` (Cluster-1) was identified on port 443 and `85.239.62[.]36` (Cluster-2) on port 3306.

Other experimental ports such as 8000,8080, 8094, 1433 5432 and 27017 were also attempted which provided no significant results with the exception of new IP addresses `45.138.16[.]208` on port 8080 and `154.216.19[.]19` on port 8000.

While investigating these two newly identified IP addresses, they appear to be outliers, although both are flagged as malicious on VirusTotal. Nevertheless, they will be useful to check for indicator overlap at a later point.

As seen in the above snippet, there are primarily two HTTP responses from the C2 servers.

HTTP Status 200:

hxxp://**136.0.9[.]8[:]443**/socket.io/?EIO=4&transport=polling&t=
```
<head><meta name="color-scheme" content="light dark"></head><body><pre style="word-wrap: break-word; white-space: pre-wrap;">0{"sid":"MGy81qf5krq0sJA0AAI5","upgrades":["websocket"],"pingInterval":25000,"pingTimeout":60000,"maxPayload":10000000}
</pre></body>
```

hxxp://**85.239.62[.]36[:]3306**/socket.io/?EIO=4&transport=polling&t=
```
<head><meta name="color-scheme" content="light dark"></head><body><pre style="word-wrap: break-word; white-space: pre-wrap;">0{"sid":"qUGGniX8EH05h-GZAGBQ","upgrades":["websocket"],"pingInterval":25000,"pingTimeout":60000,"maxPayload":10000000}
</pre></body>
```

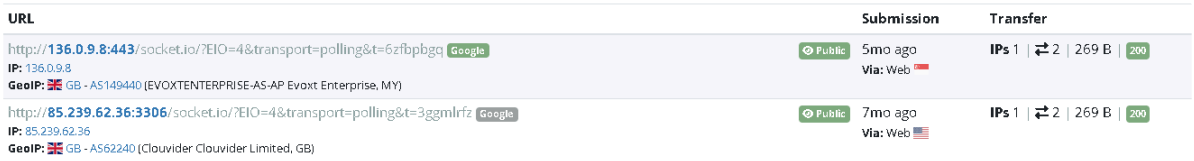
Breakdown of the parameters:

- **`"sid": "xxxxxxxxxxxxxxxxxxx"`**
  This is the **Session ID** we discussed. The server has just generated this unique ID for the client. Your client must now include this `sid` in all future requests for this session.
- **`"upgrades": ["websocket"]`**
  - This is the server telling the client, it is currently using HTTP polling, but can **support upgrading** the connection to `websocket`.
  - A Socket.IO client will see this and immediately try to establish a new, faster, more efficient WebSocket connection.
- **`"pingInterval": 25000`**
  This is the **heartbeat interval** in milliseconds. The server will send a "ping" packet to the client every 25 seconds to make sure it's still alive.
- **`"pingTimeout": 60000`**
  This is the **timeout** in milliseconds. If the client doesn't respond to a "ping" with a "pong" packet within 60 seconds, the server will assume the client has disconnected and will close the session.
- **`"maxPayload": 10000000`**
  This is the maximum size of a data packet (in bytes) that the server will accept (10,000,000 bytes, or ~10 MB).

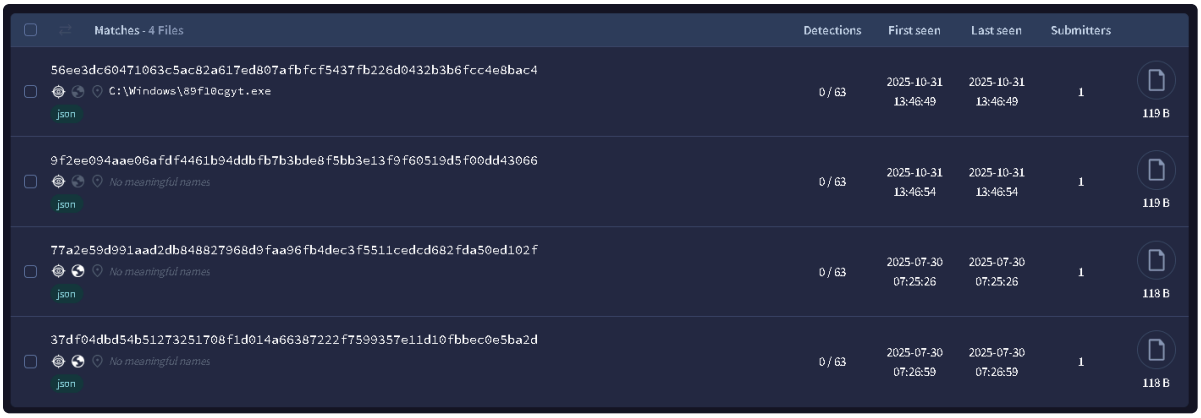
HTTP Status 400:
```
<head><meta name="color-scheme" content="light dark"><meta charset="utf-8"></head><body><pre>{"code":1,"message":"Session ID unknown"}</pre><div class="json-formatter-container"></div></body>
```

An alternate hunting opportunity would have been to check the DOM for the specific values of `pingInterval`, `pingTimeout` and `maxPayload` which was tested and yields the same results. The Document Object Model (DOM) is essentially an API for HTML and XML documents that is responsible for defining elements as objects, and created as a tree of objects when a page loads.

Search query (DOM Content): `text.content:"pingInterval\":25000" AND text.content:"pingTimeout\":60000" AND text.content:"maxPayload\":10000000"`



Search query (JSON Response): `content:{3a 32 35 30 30 30 2c 22 70 69 6e 67 54 69 6d 65 6f 75 74 22 3a 36 30 30 30 30 2c 22 6d 61 78 50 61 79 6c 6f 61 64 22 3a 31 30 30 30 30 30 30 30}`

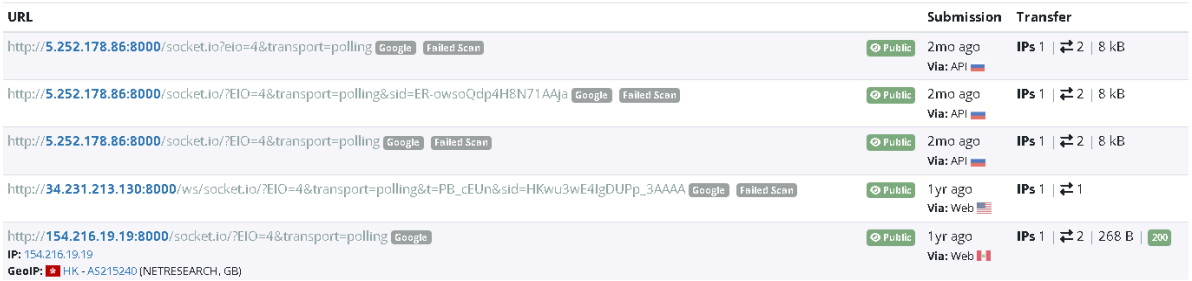


The below are SHA256 hashes of the JSON responses extracted from the successful HTTP responses from the servers:

- `56ee3dc60471063c5ac82a617ed807afbfcf5437fb226d0432b3b6fcc4e8bac4`
- `9f2ee094aae06afdf4461b94ddbfb7b3bde8f5bb3e13f9f60519d5f00dd43066`
- `77a2e59d991aad2db848827968d9faa96fb4dec3f5511cedcd682fda50ed102f`
- `37df04dbd54b51273251708f1d014a66387222f7599357e11d10fbbec0e5ba2d`

A new IP address `23.131.92[.]195` was identified that was observed interacting with the bottom two SHA256 hashes listed above. It does not match the URL structure and is using HTTPS instead of the HTTP ones observed earlier and hence is another outlier. There are other broader hunting opportunities where we can simply check for the wider URL patterns and then filter on those IP addresses with HTTP status codes 200 and 400.

Search query (Extended Ports): `(page.url:":8000" OR page.url:":8080") AND page.url:"/socket.io/?EIO=4&transport=polling"`



The three newly discovered IP addresses from HTTP 200 status code are all low confidence in terms of lacking relevance to the socket.io C2s:

`45.138.16[.]208`

`154.216.19[.]19`

`23.131.92[.]195`

Note: `45.138.16[.]208` and `23.131.92[.]195` were identified on VirusTotal since they were not scanned through urlscan.io.

There were also URLs which had failed scanned status, these are low-confidence and are listed below:

`5.252.178[.]86` HTTP socket on port 8000

`34.231.213[.]130` HTTP socket on port 8000

For the 400 code, the following were identified (only the newly discovered ones are mentioned):

- `191.96.53[.]163` HTTP based socket.io on port 5000
- `34.250.221[.]219` HTTPS based socket.io

Other urlscan.io queries:

Search query (HTTP Status 200): `page.url:"/socket.io/?EIO=4&transport=polling" AND page.status:200`

Search query (HTTP Status 400): `page.url:"/socket.io/?EIO=4&transport=polling" AND page.status:400`

Note: Both search queries require filtering on IP addresses used in the URLs to filter down the raw results from the queries.

HTTP API URLs

- `/verify-human/[version]` - Logging/telemetry
- `/u/f` - File upload endpoint
- `/snv` - endpoint name snv
- `/$/boot` - Python dropper
- `/$/z1` - Python Stealer

Search Query: `entity:url url:"27017" (url:"/verify-human/" or url:"/u/f" or url:"/snv" or url:"/$/boot" or url:"/$/z1" )`

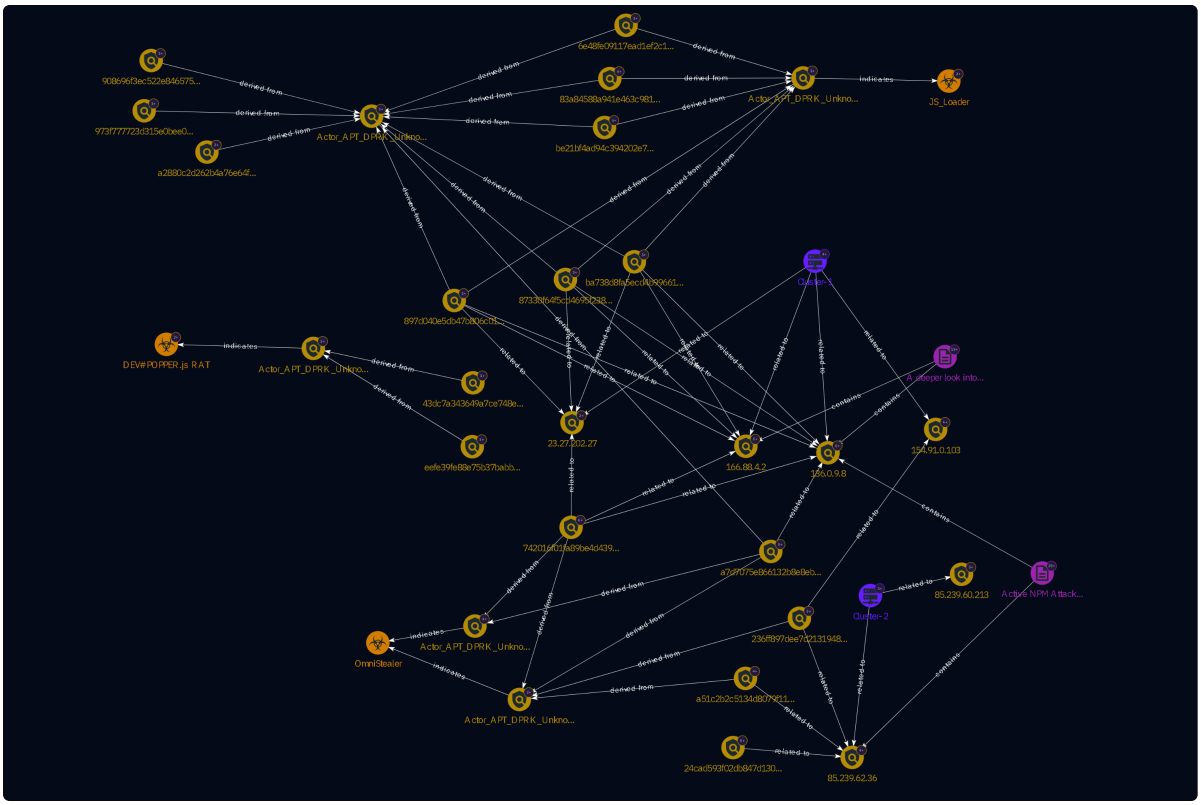
Unique IP addresses `136.0.9.8`,`23.27.20.143`,`85.239.62.36` were identified which belong to clusters 1 and 2. A variation of the search query was tested to accommodate for the alternate C2 ports 5432, 1433 and 8080 where no results were found.

Communicating Payloads with Infrastructure

During part 2 of the series, we developed five YARA rules to track the core payloads observed during the intrusion. These rules are listed below for reference and are available on our GitHub.

- Actor_APT_DPRK_Unknown_MAL_Script_PY_Stealer_Unknown_Strings_1_1Oct25
- Actor_APT_DPRK_Unknown_MAL_Script_PY_Stealer_Unknown_Strings_2_Oct25
- Actor_APT_DPRK_Unknown_MAL_Script_JS_Loader_Unknown_Strings_Oct25
- Actor_APT_DPRK_Unknown_MAL_Script_JS_RAT_Unknown_Strings_Oct25
- Actor_APT_DPRK_Unknown_MAL_Indicators_Strings_Oct25

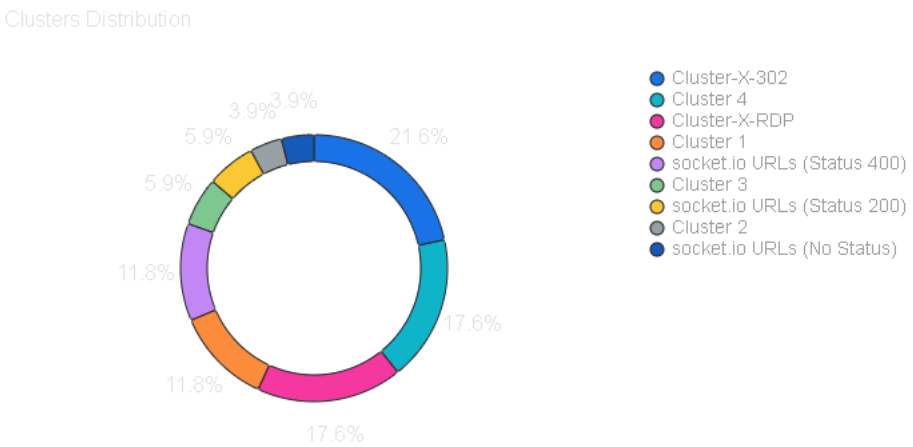
To better illustrate the relationships between the infrastructure clusters, payloads matching YARA and the rules themselves, please see the graph below.



Attribution

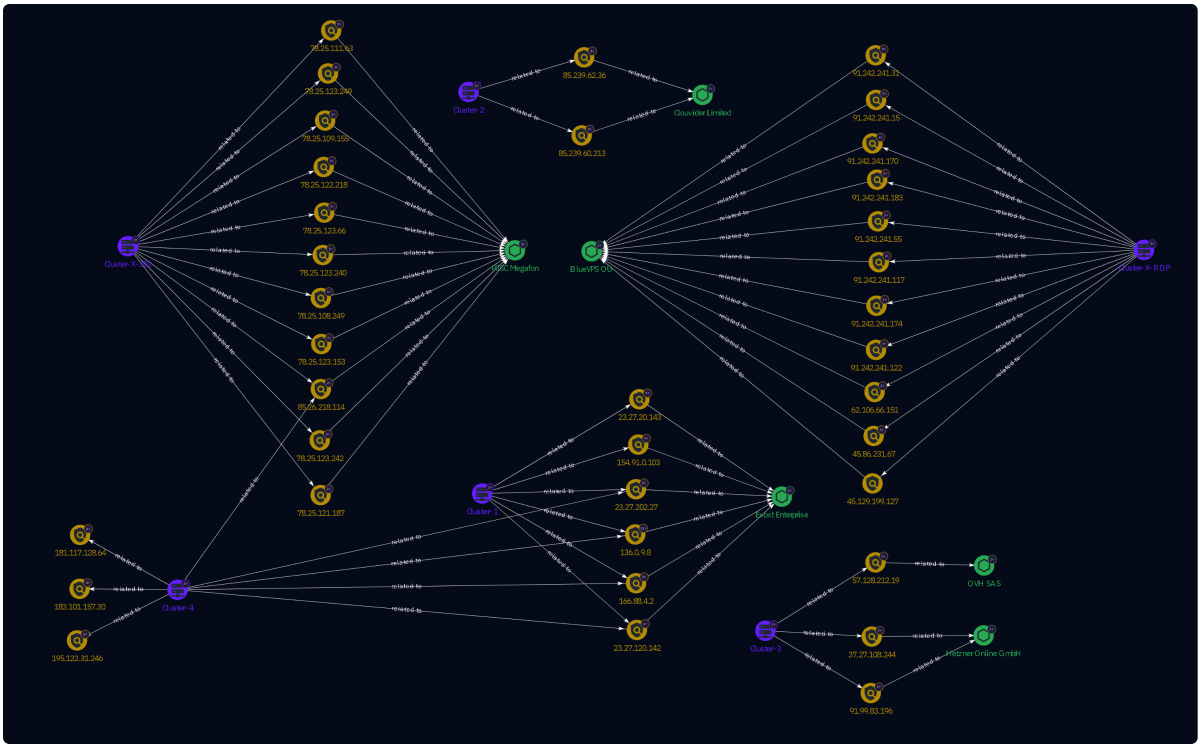
This section contains information that is used to summarise and conclude our assessment on attribution to the intrusion activity with respect to the infrastructure leveraged. Our findings from the intrusion and wider pivoting while building the clusters is complemented with the use of open-source reporting associated with our observed activity.

Clusters Overview



Cluster Name	Cluster Size	Confidence	Description
Cluster 1	6	HIGH	HTTP API C2 channel hosted on ASN Evoxt Enterprise
Cluster 2	2	MEDIUM	HTTP API C2 channel hosted on ASN Clouvider Limited

Cluster Name	Cluster Size	Confidence	Description
Cluster 3	3	LOW	HTTP API C2 channel hosted on other ASNs and port numbers
Cluster 4	9	HIGH	Socket.io C2 Channel over port 443 and 3306
Cluster-X-RDP	9	MEDIUM	Remote Access Infrastructure used to set up C2s for the intrusion
Cluster-X-302	11	MEDIUM	OPSEC redirection method used with HTTP 302



Key Indicators Overlap

All IP addresses from the defined clusters were used to search for any references in the past open-source reporting:

Cluster Name	Indicator	Source
Cluster 1, Cluster 4	136.0.9[.]8	Aikido - React Native Aria Supply Chain Attack
Cluster 1, Cluster 4	166.88.4[.]2	Aikido - React Native Aria Supply Chain Attack
Cluster 2	85.239.62[.]36	Aikido - RAT Supply Chain Compromise

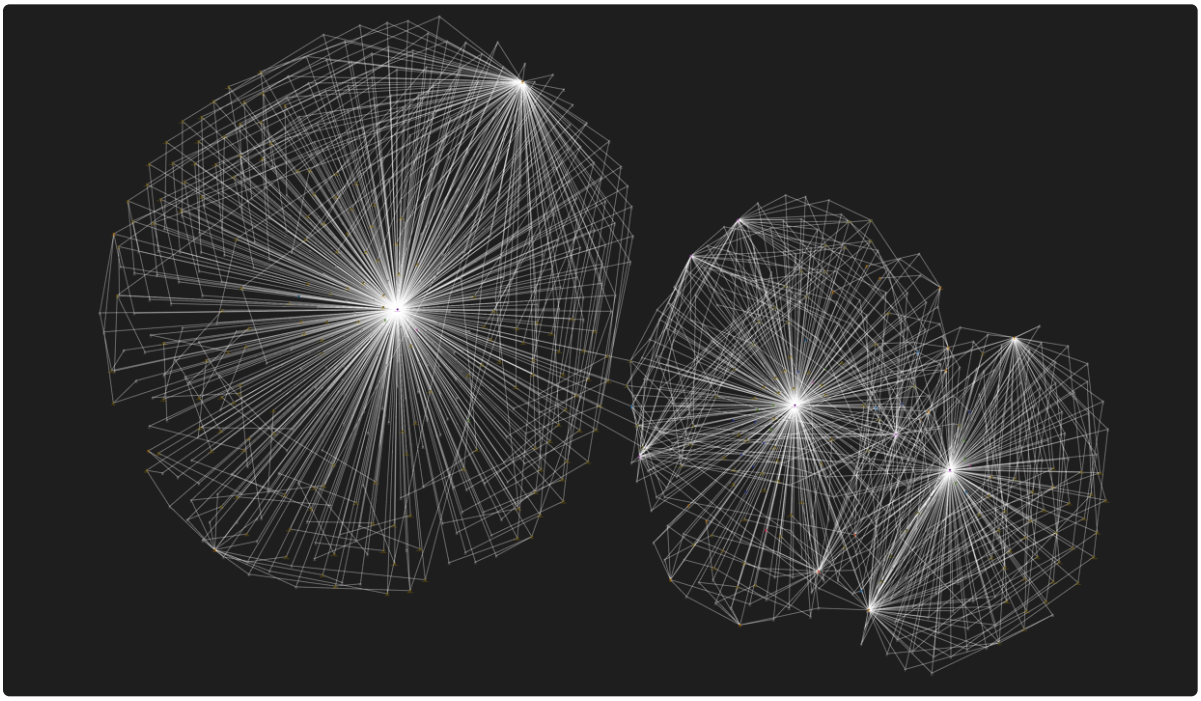
`136.0.9[.]8`, `166.88.4[.]2` and `85.239.62[.]36` were all mentioned in two separate blogs by Aikido who initially identified a campaign in May 2025 where threat actors compromised popular NPM packages. The observed initial access vector for the campaign was an NPM developer's token being compromised and then used to make malicious changes to NPM package GitHub repositories.

It is worth mentioning that between the two blogs shared by Aikido, they referenced three IP addresses and there is a positive match on all three with what was seen during cluster developments which can suggest that the intrusion we observed is likely related to the campaign covered by Aikido. They also commented on `85.239.62[.]36` around when it was potentially activated in Feb 2025 which is insightful since it belongs to Cluster 2.

Aikido did not make attribution to known threat groups. However, they suspect on basis of the sophistication in the infection chain that it is likely a state-sponsored operation. Interestingly, based on the Russian hosting ASN observed on `85.239.62[.]36`, they are leaning towards a Russian APT behind the operations which is also one of our stronger hypothesis.

Close Proximity Reporting

The following reports have been picked based on their closer proximity reporting interval that is in line with what we have seen with the intrusion timeline and were also selected based on the tradecraft described which we deemed is similar to the intrusion under consideration.



Note: Graph produced by OpenCTI STIX

There is some considerable overlap between sources based on the TTPs, targeting and payloads used including:

- **Cisco Talos -** Beavertail and Ottercookie
- **Google (GTIG) -** UNC5142 Leverages Etherhiding
- **ESET -** Deceptive Development

Conclusion

The primary focus of part 3 was to closely analyse and develop fingerprints for the payload and C2 infrastructure sighted during the intrusion. Based on our current findings, we were able to develop and divide the infrastructure clusters with differing degrees of confidence.

Based on the clusters identified from intrusion analysis and wider pivoting, it is assessed with low to medium confidence that there are two distinct threat actors working with one another that are actively or passively involved in the intrusion. Their participation is based on their involvement during setting up the infrastructure used for the intrusion and then the subsequent usage of the infrastructure itself during the intrusion.

Based on the timeline, geolocation and the remote access facilitated by the operators prior to the intrusion, it can be assessed with low confidence that the pre-attack infrastructure is being facilitated in Russia to then later be used by a DPRK aligned threat cluster. Involvement of Russia in the earlier stages is based on the RDP TLS certificate **PACKERP-XXXXXXXX** that was initially discovered with IP addresses in Cluster-2 and later used to create Cluster-X-RDP.

Historic reporting has suggested that IP address blocks in Russia were used as egress nodes for cybercrime activities aligned with **North Korea (Famous Chollima)**. Vast majority of ASNs linked to the IP addresses mentioned in the article are on *Stark Industries* while others include *Evoxt Enterprise* (ASN associated with Cluster-1) and *Zapbytes Technologies*.

While we have seen overlap in key indicators from clusters 1 and 2 with the campaign covered by Aikido, they did not make any attribution to known threat groups over the observed campaign. However, based on the indicator overlap, it can be assessed with moderate to high confidence that the intrusion we observed is likely part of the campaign despite it lacking attribution.

A plausible hypothesis that can be assessed with moderate-to-high confidence for the "Орлан 2.0 (веб-интерфейс)" login pages observed across Cluster-X-302 infrastructure represent legitimate licensed deployments of Orlan Security's DCAP system (https://orlan-security.ru) being operationally employed by DPRK threat actors to systematically prioritise and optimise large-scale data exfiltration operations.

Given the DPRK attribution and the actor's established modus operandi focused on data collection, DPRK operators may be deploying legitimate Orlan:DCAP licences on compromised victim networks to automate the identification of high-value data targets. This would enable DPRK actors to maximise intelligence and financial value whilst minimising bandwidth consumption and detection risk—directly supporting known operational priorities including cryptocurrency exchange data theft, intellectual property exfiltration for state economic advancement, and financial fraud operations.

At this point, there is not enough evidence as such to suggest attribution towards a known specific threat group and we shall continue to monitor the clusters in the near future to determine if connections exist to known threat groups and/or campaigns.

If you have any additional supporting information on the IP addresses listed in the clusters, please feel free to reach out to Ransom-ISAC at .

Part 4

Our next analysis will be covering dedicated blockchain infrastructure and cryptocurrency tracking. Through comprehensive blockchain analysis, we'll trace the flow of stolen funds across multiple chains and reveal the financial infrastructure underpinning this campaign. Such a siloed approach ensures that unintended biases are reduced to the best of our analytical abilities, providing an independent view of the threat actor's financial operations.

In Part 4, we'll expose the wallet networks, fund routing patterns, and laundering techniques used to monetise this sophisticated attack chain. From initial theft to final destination, discover how DPRK threat actors move and obfuscate stolen cryptocurrency at scale.

Acknowledgements

Bridewell and Crystal Intelligence for their invaluable contributions to this investigation. Special recognition goes to the Bridewell team for their expertise in infrastructure analysis and attribution assessment that formed the foundation of Part 3. We also wish to thank Crystal Intelligence for bringing this case to our attention and their continued partnership throughout the investigation. Finally, we're grateful to all individuals and organisations who have reached out requesting assistance or sharing intelligence—your collaboration strengthens our collective defense against sophisticated threat actors and advances the broader cybersecurity community's understanding of evolving threats.

Indicators of Compromise (IOCs)

1. ASN IOCs (High-Medium Degree of Confidence)

IP Address	First Seen	Malware/Activity
23.26.237.237	Nov-25	Rhadamanthys Stealer
23.26.237.117	Oct-25	Rhadamanthys Stealer
23.27.24.90	Oct-25	Sliver C2
23.27.168.222	Oct-25	Rhadamanthys Stealer
136.0.141.91	Sep-25	Rhadamanthys Stealer
136.0.141.245	Sep-25	Rhadamanthys Stealer
166.88.117.240	Sep-25	Remcos
23.27.124.91	Sep-25	Remcos
156.227.0.60	Sep-25	Rhadamanthys Stealer
96.126.191.167	Sep-25	Xworm

IP Address	First Seen	Malware/Activity
108.165.147.181	Sep-25	SuperShell C2
216.173.65.45	Sep-25	Remcos
166.88.194.123	Aug-25	Cobalt Strike (Watermark: 0)
23.27.163.245	Aug-25	VenomRAT
23.27.169.64	Aug-25	DCRAT
23.27.24.227	Aug-25	GoPhish
166.88.132.69	Aug-25	Remcos
166.0.132.184	Aug-25	Sliver C2
38.211.230.55	Jun-25	Remcos
23.27.201.30	Jun-25	Sliver C2
166.88.61.58	Jun-25	AdaptixC2
166.88.114.78	May-25	Sliver C2
166.88.100.85	May-25	Cobalt Strike (Watermark: 391144938)
23.27.48.77	May-25	Remcos
166.88.95.137	May-25	Mythic C2
23.27.48.113	Apr-25	Red Guard (C2 Redirector)
166.88.14.137	Apr-25	Cobalt Strike (Watermark: 391144938)
216.173.64.63	Feb-25	XWorm
166.88.90.22	Feb-25	AsyncRAT
23.27.169.4	Feb-25	Viper C2

IP Address	First Seen	Malware/Activity
166.88.98.221	Feb-25	Cobalt Strike (Watermark: 0)
23.27.240.252	Feb-25	Cobalt Strike (Watermark: 666666666)
23.27.48.179	Feb-25	Cobalt Strike (Watermark: 666666666)
166.88.141.40	Feb-25	Cobalt Strike (Watermark: 666666666)
23.27.48.4	Jan-25	Cobalt Strike (Watermark: 987654321)
23.27.12.214	Dec-24	SuperShell C2
23.27.201.57	Dec-24	UNAM C2 Panel
156.235.89.227	Dec-24	Sliver C2
23.27.240.237	Dec-24	Cobalt Strike
45.194.27.99	Oct-24	Sliver C2
166.88.57.117	Sep-24	SuperShell C2
136.0.11.193	Sep-24	Cobalt Strike (Watermark: 100000)
23.27.244.39	Aug-24	Remcos
172.121.5.230	Apr-24	Cobalt Strike (Watermark: 100000)
166.88.132.139	Feb-24	QuasarRAT
166.88.97.138	Aug-25	PlugX
166.88.61.35	Jul-25	China Aligned Espionage, Cobalt Strike (Watermark: 100000)
166.88.96.120	Jun-25	Cobalt Strike (Watermark: 100000)
166.88.4.2	Jun-25	NPM Supply Chain
166.88.2.90	Aug-25	Dark Peony (Operation Controlplug)

IP Address	First Seen	Malware/Activity
166.88.194.53	Apr-25	Earth Kurma
166.88.61.53	Apr-25	Russian Infra with DPRK
166.88.117.11	Apr-25	Dark Peony (Operation Controlplug)
166.88.35.203	Mar-25	Dark Peony (Operation Controlplug)
166.88.2.184	Mar-25	Cobalt Strike (Watermark: 666666666)
166.88.14.52	Dec-24	Cobalt Strike (Watermark: 987654321)
166.88.14.44	Mar-25	Xworm
166.88.101.20	Feb-25	DeimosC2
166.88.99.15	Feb-25	Cobalt Strike (Watermark: Unknown)
166.88.55.54	Feb-25	Cobalt Strike (Watermark: Unknown)
166.88.132.39	Nov-25	DPRK Lazarus, Contagious Interview
166.88.159.187	Jun-25	FIN7
166.88.159.37	Oct-24	FIN7
193.57.57.121	Jan-25	Cobalt Strike (Watermark: 100000)
198.105.127.98	May-24	DPRK Lazarus (through domain resolution)
198.105.127.124	May-25	PoC Exploit for Critical Zero Day
223.165.6.30	Jul-24	VenomRAT
38.211.230.5	Jul-25	Dark Peony (Operation Controlplug)
38.246.73.120	Jun-25	Dark Peony (Operation Controlplug)
45.195.76.82	Feb-24	Cobalt Strike (Watermark: 100000)

IP Address	First Seen	Malware/Activity
45.195.76.26	Dec-23	ShadowPad
50.114.5.82	Sep-24	Supershell
91.218.183.90	Apr-23	Cobalt Strike (Threat Actor (QUARTERRIG (APT29))
103.179.142.121	Jun-23	AveMaria
136.0.3.250	Jan-25	AsyncRAT
136.0.3.71	Mar-24	Bianlian
136.0.3.240	Jan-24	Bianlian
136.0.8.169	Feb-25	Danabot
136.0.9.8	Jun-25	NPM Supply Chain (Ports: 27017 and 3306)
142.111.77.196	Jul-24	DPRK Moonsleet NPM
154.81.220.233	Feb-25	Redline Stealer
155.254.60.160	May-25	ViciousTrap CVE exploitation
156.227.0.187	Apr-24	Agent Tesla Targeting Entities
156.236.76.90	Jun-25	PoC Exploit for Critical Zero Day

2. All Clusters IOCs (Low Degree of Confidence)

Cluster Name	First Seen	Indicator
Cluster-1	Sep 2025	**23.27.20[.]143**
Cluster-1	Sep 2025	**136.0.9[.]8**
Cluster-1	Sep 2025	**166.88.4[.]2**
Cluster-1	Sep 2025	**23.27.202[.]27**
Cluster-1	Oct 2025	23.27.120[.]142

Cluster Name	First Seen	Indicator
Cluster-1	Feb 2025	154.91.0[.]103
Cluster-2	May 2025	85.239.62[.]36
Cluster-2	Feb 2025	85.239.60[.]213
Cluster-3	June 2025	91.99.83[.]196
Cluster-3	June 2025	37.27.108[.]244
Cluster-3	May 2025	57.128.212[.]19
Cluster-X-RDP	Nov 2024	91.242.241[.]31
Cluster-X-RDP	Apr 2025	91.242.241[.]170
Cluster-X-RDP	Apr 2025	91.242.241[.]117
Cluster-X-RDP	May 2025	91.242.241[.]122
Cluster-X-RDP	Dec 2024	91.242.241[.]15
Cluster-X-RDP	Nov 2024	91.242.241[.]174
Cluster-X-RDP	Nov 2024	91.242.241[.]55
Cluster-X-RDP	Dec2024	91.242.241[.]183
Cluster-X-RDP	Dec 2024	62.106.66[.]151
Cluster-X-RDP	Apr 2025	45.129.199[.]127
Cluster-X-RDP	Jan 2025	45.86.231[.]67
Cluster-X-302	Dec 2024	78.25.123[.]242
Cluster-X-302	Nov 2024	78.25.123[.]66
Cluster-X-302	Nov 2024	78.25.122[.]218

Cluster Name	First Seen	Indicator
Cluster-X-302	Nov 2024	78.25.109[.]155
Cluster-X-302	Nov 2024	78.25.108[.]249
Cluster-X-302	Dec 2024	78.25.111[.]63
Cluster-X-302	Nov 2024	78.25.121[.]187
Cluster-X-302	Nov 2024	78.25.123[.]153
Cluster-X-302	Nov 2024	78.25.123[.]240
Cluster-X-302	Nov 2024	78.25.123[.]249
Cluster-X-302	Nov 2024	85.26.218[.]114
Cluster-4	Sep 2025	136.0.9[.]8
Cluster-4	Sep 2025	23.27.202[.]27
Cluster-4	Sep 2025	166.88.4[.]2
Cluster-4	Oct 2025	23.27.120[.]142
Cluster-4	Mar 2025	181.117.128[.]64
Cluster-4	Oct 2025	183.101.157[.]30
Cluster-4	Nov 2025	195.122.31[.]246
Cluster-4	Nov 2025	202.155.8[.]173
socket.io URL (Status 200)	Sep 2025	45.138.16[.]208
socket.io URL (Status 200)	Sep 2024	154.216.19[.]19
socket.io URL (Status 200)	Jul 2025	23.131.92[.]195
socket.io URL (No Status)	Nov 2022	5.252.178[.]86

Cluster Name	First Seen	Indicator
socket.io URL (No Status)	Unknown	34.231.213[.]130
socket.io URL (Status 400)	May 2024	191.96.53[.]163
socket.io URL (Status 400)	May 2023	34.250.221[.]219

3. File Hashes (High Degree of Confidence)

YARA Rule Name	SHA256 Hash
Actor_APT_DPRK_Unknown_MAL_Script_PY_Stealer_Unknown_Strings_1_1Oct25	742016f01fa89be4d43916d5d2349c8d86dc89f096302501ec2
Actor_APT_DPRK_Unknown_MAL_Script_PY_Stealer_Unknown_Strings_1_1Oct25	a7d7075e866132b8e8eb87265f7b7fab0e9f6dd7f748445a18f
Actor_APT_DPRK_Unknown_MAL_Script_PY_Stealer_Unknown_Strings_2_Oct25	236ff897dee7d21319482cd67815bd22391523e37e0452fa23(
Actor_APT_DPRK_Unknown_MAL_Script_PY_Stealer_Unknown_Strings_2_Oct25	742016f01fa89be4d43916d5d2349c8d86dc89f096302501ec2
Actor_APT_DPRK_Unknown_MAL_Script_PY_Stealer_Unknown_Strings_2_Oct25	a7d7075e866132b8e8eb87265f7b7fab0e9f6dd7f748445a18f
Actor_APT_DPRK_Unknown_MAL_Script_PY_Stealer_Unknown_Strings_2_Oct25	24cad593f02db847d1302ee7c486d0756708521d5ae69faa9d
Actor_APT_DPRK_Unknown_MAL_Script_PY_Stealer_Unknown_Strings_2_Oct25	a51c2b2c5134d8079f11a22bd0621d29b10e16aefa4174b516
Actor_APT_DPRK_Unknown_MAL_Script_JS_Loader_Unknown_Strings_Oct25	be21bf4ad94c394202e7b52a1b461ed868200f0f03b3c85449
Actor_APT_DPRK_Unknown_MAL_Script_JS_Loader_Unknown_Strings_Oct25	87330f64f5cd4695f2385f87c9fffffee26d5ad2637665f1cd5d7fc
Actor_APT_DPRK_Unknown_MAL_Script_JS_Loader_Unknown_Strings_Oct25	ba738d8fa5ecd4b996612dde6cd4516cbe7116305661521ffcf
Actor_APT_DPRK_Unknown_MAL_Script_JS_Loader_Unknown_Strings_Oct25	83a84588a941e463c981083555a2e7814887fa8816e7cca5af
Actor_APT_DPRK_Unknown_MAL_Script_JS_Loader_Unknown_Strings_Oct25	6e48fe09117ead1ef2c10a3db614217184fc300ac70ee902f67
Actor_APT_DPRK_Unknown_MAL_Script_JS_Loader_Unknown_Strings_Oct25	897d040e5db47b806c01eb2a1a056ca49b10e0aa4985f84d2l
Actor_APT_DPRK_Unknown_MAL_Script_JS_RAT_Unknown_Strings_Oct25	eefe39fe88e75b37babb37c7379d1ec61b187a9677ee5d0c86
Actor_APT_DPRK_Unknown_MAL_Script_JS_RAT_Unknown_Strings_Oct25	43dc7a343649a7ce748e4c2f94bcb6064199507cfd9f064a2d4
Actor_APT_DPRK_Unknown_MAL_Indicators_Strings_Oct25	908696f3ec522e846575061e90747ddf29fccab0e5936459749

YARA Rule Name	SHA256 Hash
Actor_APT_DPRK_Unknown_MAL_Indicators_Strings_Oct25	897d040e5db47b806c01eb2a1a056ca49b10e0aa4985f84d2
Actor_APT_DPRK_Unknown_MAL_Indicators_Strings_Oct25	be21bf4ad94c394202e7b52a1b461ed868200f0f03b3c85449
Actor_APT_DPRK_Unknown_MAL_Indicators_Strings_Oct25	6e48fe09117ead1ef2c10a3db614217184fc300ac70ee902f67
Actor_APT_DPRK_Unknown_MAL_Indicators_Strings_Oct25	87330f64f5cd4695f2385f87c9ffffee26d5ad2637665f1cd5d7fc
Actor_APT_DPRK_Unknown_MAL_Indicators_Strings_Oct25	83a84588a941e463c981083555a2e7814887fa8816e7cca5af
Actor_APT_DPRK_Unknown_MAL_Indicators_Strings_Oct25	ba738d8fa5ecd4b996612dde6cd4516cbe7116305661521ffcf
Actor_APT_DPRK_Unknown_MAL_Indicators_Strings_Oct25	a2880c2d262b4a76e64fd29a813f2446ecbd640f378714aa57
Actor_APT_DPRK_Unknown_MAL_Indicators_Strings_Oct25	973f777723d315e0bee0fb9e81e943bb3440be7d2de7bf5824
Actor_APT_DPRK_Unknown_MAL_Indicators_Strings_Oct25	a7d7075e866132b8e8eb87265f7b7fab0e9f6dd7f748445a18f

Continue Reading