GROUP-IB

← Blog

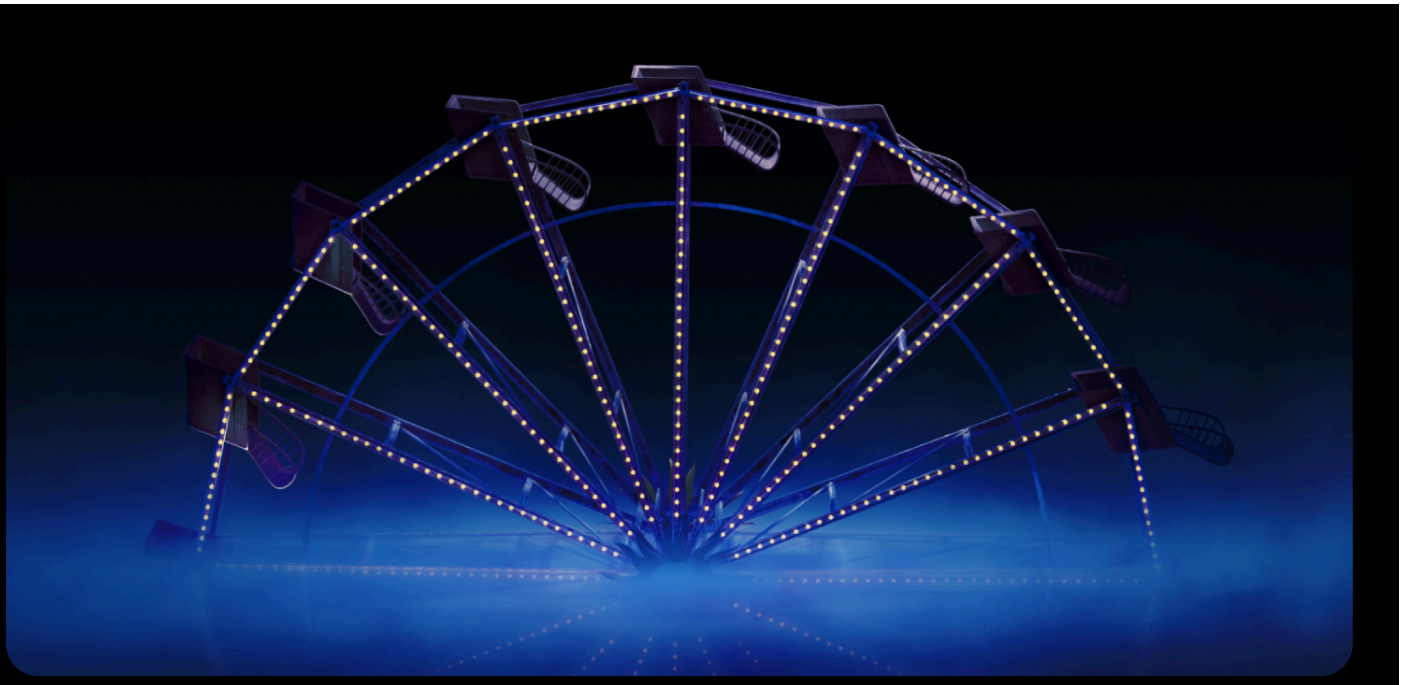
Eline Switzer

Threat Intelligence Analyst

Dusting for fingerprints: ShadowSyndicate, a new RaaS player?

No sleep until the Cybercrime Fighters Club is done with finding the answer as to who is behind this new ransomware-as-a-service affiliate.

September 26, 2023 · min to read · Threat Intelligence



Cybercrime Fighters Club RaaS ShadowSyndicate

Preface

In mid-May 2023, Group-IB began to receive highly positive feedback from the cybersecurity community regarding the publication of joint research. As a result, **Group-IB Threat Intelligence** analysts teamed up with **Joshua Penny** from **Bridewell**, Group-IB's long-standing MSSP partner in Europe, and threat researcher **Michael Koczwara** as part of Group-IB's new Cybercrime Fighters Club initiative to conduct a collaborative investigation into what we assert to be a new Ransomware-as-a-Service (RaaS) affiliate.

Acknowledgements: We would like to thank Nikita Rostovtsev for his contribution to this blog post.

Introduction

The **Ransomware-as-a-Service** (RaaS) market is a fast-moving one. Prominent RaaS or affiliate groups can form, wreak havoc, and disband all within a short period of time. In Hi-Tech Crime Trends 2022/2023, Group-IB Threat Intelligence's review of the top cyber threats, our researchers predicted

that the RaaS industry will continue to grow rapidly and that numerous new gangs would likely appear on the block. In this blog, we'll detail what we believe to be a new RaaS group that appears to operate differently from the rest: Enter **ShadowSyndicate.**

What is unusual about ShadowSyndicate (not to be confused with Shadow ransomware)? Well, it's incredibly rare for one Secure Shell (SSH) fingerprint to have such a complex web of connections with a large number of malicious servers. In total, **we found ShadowSyndicate's SSH fingerprint on 85 servers since July 2022**. Additionally, we can say with various degrees of confidence that the group has used **seven different ransomware families** over the course of the past year, making ShadowSyndicate notable for their versatility. At this stage, we are unable to confirm if ShadowSyndicate is a RaaS affiliate or an initial access broker, although based on our evidence, which we'll outline in this blog post, we believe that the threat actor is the former.

This blog post aims to provide an overview of the infrastructure leveraged by ShadowSyndicate and contains our preliminary conclusions; leaving avenues for further research into the group's identity open for exploration. As part of Group-IB's new Cybercrime Fighters Club program, this blog also serves as a key example of the value of knowledge exchange and joint research in the field of cybersecurity.

Join the Group-IB Cybercrime Fighters Club!

The global fight against cybercrime is a collaborative effort, and that's why we're looking to partner with industry peers to research emerging threats and publish joint findings on our blog. If you've discovered a breakthrough into a particular threat actor or a vulnerability in a piece of software, let us know, and we can mobilize all our necessary resources to dive deeper into the issue.

All contributions will be given appropriate credit along with the full backing of our social media team on Group-IB's Threat Intelligence Twitter page, where we regularly share our latest findings into threat actors' TTPs and infrastructure, along with our other social media accounts.

#LetsStopCybercrime #CybercrimeFightersClub

Key findings

The threat actor dubbed **ShadowSyndicate** uses the same Secure Shell (SSH) fingerprint on many servers (**85** at the time of writing).

ShadowSyndicate is a threat actor that works with various ransomware groups and affiliates of ransomware programs.

In its attacks, ShadowSyndicate used an “off-the-shelf” toolkit, including **Cobalt Strike**, **IcedID**, and **Sliver** malware.

At least **52 servers** with this SSH were used as a Cobalt Strike C2 framework.

ShadowSyndicate has been active since **July 2022.**

We can, with a strong degree of confidence, attribute ShadowSyndicate to **Quantum** ransomware activity in September 2022, **Nokoyawa** ransomware activity in October 2022, November 2022, and March 2023, as well as to **ALPHV** activity in February 2023.

With a low degree of confidence, we can attribute ShadowSyndicate to **Royal, Cl0p, Cactus**, and **Play** ransomware activity.

We found connections between ShadowSyndicate infrastructure and **Cl0p/Truebot**.

Summary

The SSH fingerprint **1ca4cbac895fc3bd12417b77fc6ed31d**, which is connected to various potentially malicious servers, was detected by multiple researchers. It was deployed on **85 IP servers** and most of them (at least 52) were tagged as **Cobalt Strike C2**.

We have dubbed the threat actor that uses the SSH fingerprint 1ca4cbac895fc3bd12417b77fc6ed31d **ShadowSyndicate** (previous name Infra Storm). This SSH fingerprint was first seen on **July 16, 2022** and it is still in use at the time of writing (September 2023).

Together we looked into any associated information we could find, with the aim of determining which cybercriminal groups used these servers.

At the start of our research, we established five hypotheses about ShadowSyndicate that we set out to prove. These hypotheses are as follows:

1. ShadowSyndicate is a hoster who set up the SSH fingerprint on their server.
2. ShadowSyndicate is a DevOps engineer that deploys servers and provides them to various threat actors.
3. ShadowSyndicate owns an underground service offering “bulletproof hosting” to cybercriminals.
4. ShadowSyndicate is an initial access broker that obtains initial access to victims themselves and then sells that access to other cybercrime groups.
5. ShadowSyndicate is a RaaS affiliate that uses various types of ransomware.

Although we have not reached a final verdict, all the facts obtained during our research suggest that **hypothesis E**, **that ShadowSyndicate is a RaaS affiliate that uses various types of ransomware**, is the most plausible.

Figure 1. Hosts related to ShadowSyndicate’s SSH fingerprint. Source: Group-IB Graph Network Analysis tool.

The full list of IP addresses used by the threat actor is as follows:

Table 1. List of IP addresses linked to ShadowSyndicate

	IP address	SSH first seen on host
1	45.227.253[.]20	2022.07.16
2	194.135.24[.]247	2022.08.11
3	5.188.86[.]227	2022.08.17
4	179.60.150[.]139	2022.08.23
5	179.60.146[.]51	2022.09.06
6	81.19.135[.]249	2022.09.11
7	179.60.146[.]52	2022.09.13
8	179.60.146[.]25	2022.09.14
9	45.227.253[.]30	2022.09.14

For the sake of convenience, we will refer to this list of servers as **List A**.

If we go back to our initial assumptions, option A (that ShadowSyndicate is a hoster who set up the SSH fingerprint on their servers) was rejected immediately because we discovered the existence of 18 different hosts in multiple countries.

We identified several server clusters presumably related to various threat actors. We also found their tools and some TTPs that they used. Some servers had been detected in previous attacks. The tools and malware used by the attackers included **Cobalt Strike, Sliver, IcedID, and Matanbuchus**.

Research

We conducted our research using Group-IB tools and data, reports by other vendors, the search engines **Shodan** and **Censys**, and OSINT.

Tools identified

Cobalt Strike

When analyzing the servers contained on List A, we came across **eight different Cobalt Strike watermarks**. A watermark is a license key for Cobalt Strike users. Adversaries can use cracked versions of Cobalt Strike, with the watermark changed to a value that is not unique, for example 12345678. In addition, threat actors can use special scripts to change a watermark to any value.

We have come across the following Cobalt Strike watermarks on servers from **List A**.

Table 2. Cobalt Strike watermarks on servers from List A.

Watermark	Unique hosts with watermark (data obtained by Group-IB)	Threat actors who used Cobalt Strike with this watermark	Details	Sources
12345	121	Royal, Cactus	In 2023, watermark 12345 was found to be used in attacks related to Royal and Cactus	Royal – Link Cactus – Link
305419776	151	Quantum, Nokoyawa	In April and September 2022, watermark 305419776 + sleeptime 60000 were found to be used in attacks involving Quantum ransomware. In October and November 2022, this	Quantum – Link 1 | Link 2 Nokoyawa – Link 1 | Link 2

It is noteworthy that, while analyzing Cobalt Strike configurations from servers on List A, we saw instances when an **identical configuration was deployed on two servers**, one of which is on List A and the second is not. In one case, both servers were on List A.

Cobalt Strike configuration pairs

As stated above, we came across identical configurations of Cobalt Strike on pairs of servers: the first is on list A and the second is not. In this section, we provide the relevant data. It will be useful for future attribution efforts.

Table 3. Servers with identical Cobalt Strike configurations

Pair no.	Configuration	Server #1 (Server on list A)	Server #2	Comment
1	2022-11-28 watermark 674054486, sleeptime 119588	194.135.24[.]246	194.135.24[.]253	Both servers are on List A
2	2022-10-01 watermark 206546002, sleeptime 60000, mysqlserver[.]org	179.60.146[.]25	146.70.116[.]20	Second server is not on List A
3	2023-01-21 watermark 674054486, sleeptime 57247, avdev[.]net	194.165.16[.]62	212.113.106[.]118	Second server is not on List A
4	2022-12-19 watermark 674054486, sleeptime 60216.	194.165.16[.]91	79.137.202[.]45	Second server is not on List A

Sliver

Sliver is an open-source penetration testing tool developed in the programming language Go. It's designed to be scalable and can be used by organizations of all sizes to perform security testing. Like Cobalt Strike and Metasploit, Sliver can be used by threat actors in real-life attacks. We found evidence of Sliver being used on servers from List A:

- 193.142.30[.]17 was connected to Sliver in May 2023
- 193.142.30[.]154 has been used as Sliver C2 since at least May 2023 and is still being used as of July 2023
- 194.135.24[.]241 was tagged by Group-IB as Sliver in January 2023

Sliver JARM certificates

```
00000000000000000043d43d00043de2a97eabb398317329f027c66e4c1b01
0000000000000000000000000000000000000000000000000000000000000000
```

References:

- Reference #1
- Reference #2
- Reference #3

IcedID

IcedID is a malware developed in 2017 as a banking Trojan with web injects. In recent years it has mostly been used in attack chains to deliver another payload, for example ransomware. IcedID was detected in attacks involving the following ransomware groups: **Karakurt, RansomEXX, Black Basta, Nokoyawa, Quantum**, **REvil**, **Xingteam**, and **Conti**.

The server 78.128.112[.]139 from List A (above) was detected in activity connected to the IcedID infection chain. It led to Quantum ransomware being deployed in September 2022. In this case, the initial vector of attack was MalSpam, which delivered a malicious ISO file.

The server 5.8.18[.]242 from List A was also detected in activity connected to the IcedID infection chain. This activity led to Nokoyawa being deployed in October 2022. In this case, the initial vector of attack was an Excel maldoc containing VBA macros which downloaded the IcedID payload.

Matanbuchus

Matanbuchus is a Malware-as-a-Service (MaaS) loader known since 2021. It is used to execute .exe payloads and for loading and executing shellcodes and malicious DLL files. It has been detected in phishing campaigns and it ultimately drops the Cobalt Strike post-exploitation framework on compromised machines.

The following servers from List A were potentially connected to Matanbuchus activity in February 2023:

- 45.182.189[.]105
- 45.182.189[.]106

Meterpreter

Meterpreter is a Metasploit payload that runs on the target system and supports the penetration testing process.

The server 179.60.150[.]151 was detected as Meterpreter C2 in March 2023.

Deployment of servers

Secure Shell (SSH) uses a fingerprint generated with a unique server host key so that a client can identify the server. We began our investigation after finding a set of servers with the same SSH key fingerprint.

Our initial assumption was that servers from **List A** were related to one hosting provider that used the same SSH for setting up servers. To confirm or disprove this theory, we checked information about the networks for servers from **List A,** which we have compiled in Table 4 (below).

Table 4. Network information of servers

	IP address	Country	Network name	Owner name
1	45.227.253[.]20	Panama	PA-DICO2-LACNIC	DirectWebH CORP
2	194.135.24[.]247	Czech Republic	CZ-RELCOM-19950206	Reliable Communications s.r.o.
3	5.188.86[.]227	Cyprus	CHANNEL-NET	Channelnet
4	179.60.150[.]139	Belize	BZ-MGLT-LACNIC	MAXWELL GROUP LTD
5	179.60.146[.]51	Costa Rica	CR-DASA3-LACNIC	DATASOLUTIONS S.A.
6	81.19.135[.]249	Seychelles	DIGICLOUD-NET	Alviva Holding Limited
7	179.60.146[.]52	Costa Rica	CR-DASA3-LACNIC	DATASOLUTIONS S.A.
8	179.60.146[.]25	Costa Rica	CR-DASA3-LACNIC	DATASOLUTIONS S.A.

The information in the above table indicates that the servers used by ShadowSyndicate do not have the same owner, allowing us to discount hypothesis A (that ShadowSyndicate is a hoster who set up the SSH fingerprint on their server). In fact, we identified 18 different server owners.

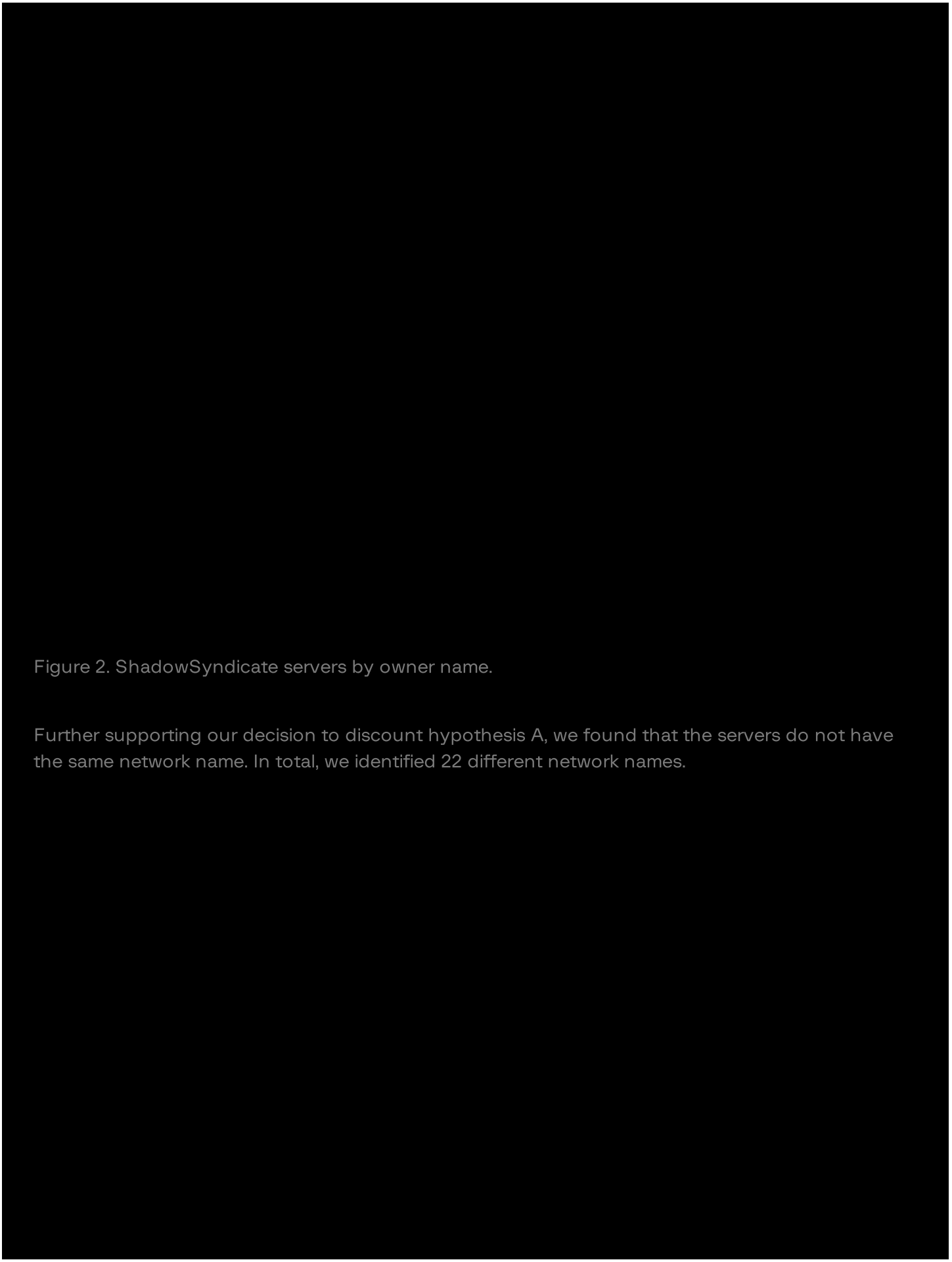


Figure 2. ShadowSyndicate servers by owner name.

Further supporting our decision to discount hypothesis A, we found that the servers do not have the same network name. In total, we identified 22 different network names.

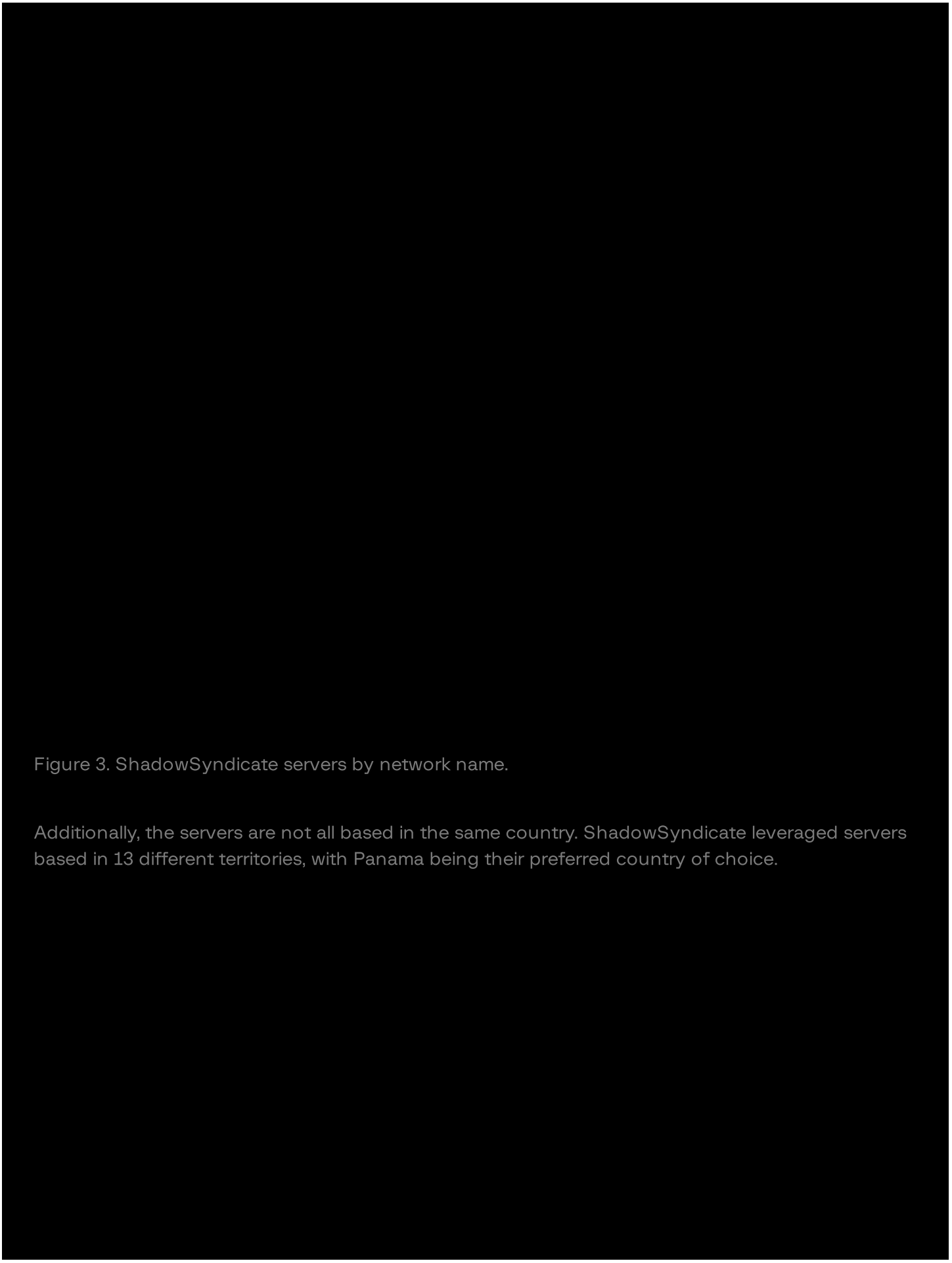


Figure 3. ShadowSyndicate servers by network name.

Additionally, the servers are not all based in the same country. ShadowSyndicate leveraged servers based in 13 different territories, with Panama being their preferred country of choice.

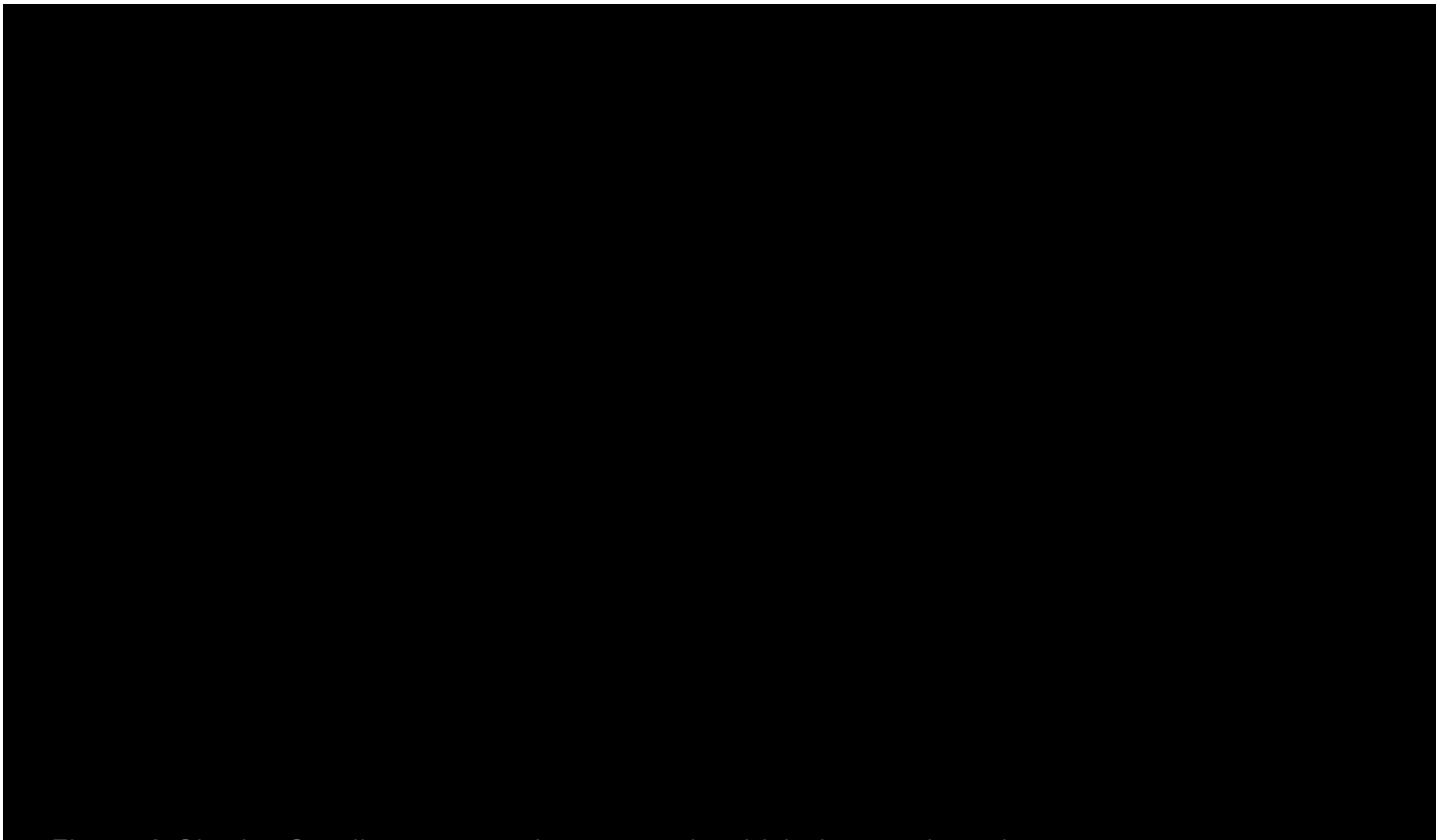


Figure 4. ShadowSyndicate servers by country in which they are based.

We have therefore reached the conclusion that servers from **List A** aren't related to one network and one hosting provider. Hypothesis A (above), which stated that 1ca4cbac895fc3bd12417b77fc6ed31d is the SSH on which the hoster was set up, **can therefore be rejected**.

On most **List A** servers, OpenSSH 8.2p1 was used. Further research uncovered connections with various ransomware families (for example **Trickbot, Nokoyawa, Royal, Ryuk, FIN7, ALPHV, and Cl0p**). Most of our findings connect ShadowSyndicate with ransomware activity, but unfortunately we didn't detect strong ties to a specific threat actor. As a result, **assumptions B, C, D, and E have yet to be fully discounted.**

Data attributed with a high degree of confidence

Several servers on **List A** were attributed to known attackers with a high degree of confidence. In the interests of brevity, we will not provide full Cobalt Strike configurations. However, we will provide some parameters if they are known (date of detection, watermark, sleeptime, Cobalt Strike C2

server) because certain combinations of these parameters could be unique and useful for attribution.

Connection with Quantum

Quantum ransomware was discovered in July 2021. Quantum presumably included members of Conti, a prolific cybercrime group that shut down its ransomware operations and dedicated leak site (DLS) more than a year ago. Quantum's DLS hasn't been updated since November 2022.

Table 5. Attribution of IP address 78.128.112[.]139 (found in List A).

IP address	Attribution
78.128.112[.]139	This Cobalt Strike server with watermark 305419776, sleeptime 60000 was detected in a Quantum ransomware attack in September 2022 – Link ISO file -> IceDID -> Cobalt Strike -> Quantum

Connection with Nokoyawa

Nokoyawa is a type of ransomware first discovered in February 2022. The origins of Nokoyawa can be traced back to another ransomware type called **Nemty**. Nokoyawa has been active since August 2023.

One of the Cobalt Strike servers from **List A** was detected in two connected Nokoyawa attacks in Q4 2022. These attacks have a lot in common with the Quantum attack described in the previous section. Another server from List A was detected in a Nokoyawa attack in April 2023.

Table 6. Attribution of IP address 5.8.18[.]242 (found in List A).

IP address	Cobalt Strike configurations and Attribution
5.8.18[.]242	Cobalt Strike with watermark 305419776, sleeptime 60000 was detected on a host on October 12, 2022. This Cobalt Strike server was detected in an attack involving Nokoyawa in October 2022 – Link

	Excel maldoc -> IceDID -> Cobalt Strike -> Nokoyawa It is important to note that the watermark, sleeptime, period of attack and TTPs are all similar to the Quantum attack described in the previous section. In November 2022 the same Cobalt Strike server 5.8.18[.]242 (with the same watermark 305419776, sleeptime 60000) was also used in attack involving Nokoyawa – Link Thread-Hijacked Email -> HTML Attachment -> ZIP -> ISO file -> IcedID -> Cobalt Strike -> Nokoyawa The SSH fingerprint 1ca4cbac895fc3bd12417b77fc6ed31d was detected on this server on October 11, 2022.

Table 7. Attribution of IP address 46.161.27[.]160 (found in List A).

46.161.27[.]160	Cobalt Strike with watermark 674054486 was detected on a host on March 27, 2023, with CS domain devsetgroup[.]com The domain devsetgroup.com was detected in an attack involving **Nokoyawa** – Link SSH fingerprint 1ca4cbac895fc3bd12417b77fc6ed31d was detected on this server on April 4, 2023.

Connection with ALPHV

ALPHV (aka **BlackCat**) is a ransomware operator group discovered in December 2021. It has been active since August 2023 and is one of the most active ransomware groups in history.

Let's have a closer look at the server pairs 5 and 6 in **Table 3 (found above)**. These server pairs had identical configurations of Cobalt Strike.

Table 8. Server pairs containing identical configurations of Cobalt Strike.

Cobalt Strike configuration	Server #1 (server on list A)	SSH first seen on server #1	Server #2
2023-01-31 watermark 674054486 sleeptime 60946 server devcloudpro[.]com	194.165.16[.]64	December 6, 2022	109.172.45.28

2023-01-29 watermark 674054486 sleeptime 58835 server uranustechsolution[.]com	194.165.16[.]90	January 29, 2023	109.172.45.77

Identical Cobalt Strike configurations (same watermark, sleeptime, Cobalt Strike domain and date of detection by Group-IB) were identified by Group-IB specialists in an incident response case related to an ALPHV attack that took place in February 2023. It should be noted that these configurations are unique and were seen only twice.

Servers from the attack involving ALPHV:

- 109.172.45[.]28
- 109.172.45[.]77

The evidence points to a strong connection with ALPHV ransomware.

Data attributed with a low degree of confidence

While checking List A servers using Group-IB data sources, we established that some servers were mapped as Ryuk, Conti, and Trickbot. However, these criminal groups no longer exist. Ryuk ceased to exist at the end of 2021, while Conti and Trickbot (which are connected) went dormant at the beginning of 2022.

Researchers believe that former members of these groups could be continuing with their criminal activity using the same infrastructure, but they might now operate individually or in other criminal groups. Unfortunately, at the time of writing we do not have reliable enough evidence to attribute them to existing threat actors — we can only make educated guesses.

We would also like to highlight unattributed servers with Cobalt Strike, presumably related to ransomware activity. Our assumptions of current attribution are based on Cobalt Strike watermarks detected in previous attacks conducted by ransomware groups and mentioned in other reports.

Our research shows that several watermarks could be detected on a single server, which complicates attribution but confirms our theory that ShadowSyndicate could be an affiliate who works with various RaaS groups.

Let's look into available information in more detail. Below we provide data with known Cobalt Strike watermarks and other tags which might help with attribution.

Table 9. Connections with Royal, Quantum, Cl0p, ALPHV, Nokoyawa, and Play

IP address	SSH first seen on host	Cobalt Strike configurations and possible attributions
45.227.253[.]20	July 16, 2022	May 16, 2023 watermark 1580103824 sleeptime 57297 domain qw.sveexec[.]comIn 2022, watermark 1580103824 was detected on a server related to Royal ransomware.In May 2023, watermark 1580103824 was detected in an attack related to Cl0p ransomware.
194.135.24[.]247	August 11, 2022	August 24, 2022 watermark 305419776 sleeptime 60000April 8, 2023 watermark 1580103824 sleeptime 60000In April and September 2022, watermark 305419776 + sleeptime 60000 was detected in attacks involving Quantum ransomware. In Q4 2022, this watermark also was detected in an attack involving Nokoyawa.In 2022, watermark

Table 10. Notable data found on servers

IP address	SSH first seen on host	Data found on server
158.255.2[.]245	July 20, 2023	May 24, 2022 The Cobalt Strike watermark is unknown. However, this server is connected to several domains registered on July 18, 2023: asapor[.]xyz

		asaporeg[.]xyz asaper[.]xyz assapaa[.]xyz aserpo[.]xyz
193.142.30[.]205	July 26, 2023	Cobalt Strike wasn't detected on this host. However, this server is connected to a domain registered on July 23, 2023: eastzonentp[.]com

Connections with Cl0p/Truebot infrastructure

During our research, we uncovered several potential connections between ShadowSyndicate and **Truebot/Cl0p** infrastructure. We identified a number of IP addresses attributed to Cl0p that we believe have changed ownership to ShadowSyndicate, as evidenced by the use of the ShadowSyndicate SSH key. These IP addresses have been linked to 4 out of 5 clusters that we have attributed to ransomware affiliates associated with **Cl0p** and **Black Basta** and to ex-ransomware groups such as **Ryuk**.

To show the association between Cl0p and ShadowSyndicate, below we present the IP addresses reused by both Cl0p clusters and ShadowSyndicate. We also compared hosting providers to try and determine whether the ShadowSyndicate threat actors previously operated as Cl0p affiliates.

Out of the **149 IP addresses** that we linked to Cl0p ransomware affiliates, we have seen, since August 2022, **12 IP addresses from 4 different clusters** changed ownership to ShadowSyndicate, which suggests that there is some potential sharing of infrastructure between these groups. Unfortunately, we could not verify the use of these IPs before they changed ownership to ShadowSyndicate, but they are now all used as C2 infrastructure for Cobalt Strike or Metasploit.

These IP addresses are as follows:

Table 11. IP addresses shared between Cl0p and ShadowSyndicate

IP	ShadowSyndicate SSH first seen	Usage
147.78.47[.]231	September 20, 2022	Cobalt Strike

179.60.146[.]51	September 6, 2022	Cobalt Strike
179.60.150[.]151	February 6, 2023	Meterpreter
194.135.24[.]241	November 12, 2022	Cobalt Strike
194.135.24[.]248	September 18, 2022	Cobalt Strike
45.227.252[.]247	November 16, 2022	Cobalt Strike
45.227.252[.]252	November 25, 2022	Cobalt Strike
45.227.255[.]189	October 7, 2022	Cobalt Strike

Figure 5: Data visualization of connections between ShadowSyndicate and Cl0p

These IPs can be attributed to Cl0p on account of their connection with clusters of infrastructure that were previously linked to Cl0p affiliates using SSH hash fingerprints.

The following SSH hashes represent select clusters of infrastructure predominantly linked to Cl0p:

SSH hashes:

- ddd9ca54c1309cde578062cba965571
- b54cce689e9139e824b6e51a84a7a103
- 9bd79ffaeb8de31c9813b3ce51b30488
- 5e21f8e88b007935710b2afc174f289
- 55c658703c07d6344e325ea26cf96c3
- 96ea77a1a901e38aac8b9d5772d3d765

Below we show how infrastructure was reused between Cl0p and ShadowSyndicate and we compare how hosting providers were selected. Although we cannot directly connect ShadowSyndicate to Cl0p with a high degree of confidence, the following observations are noteworthy and suggest some form of connection between the two groups.

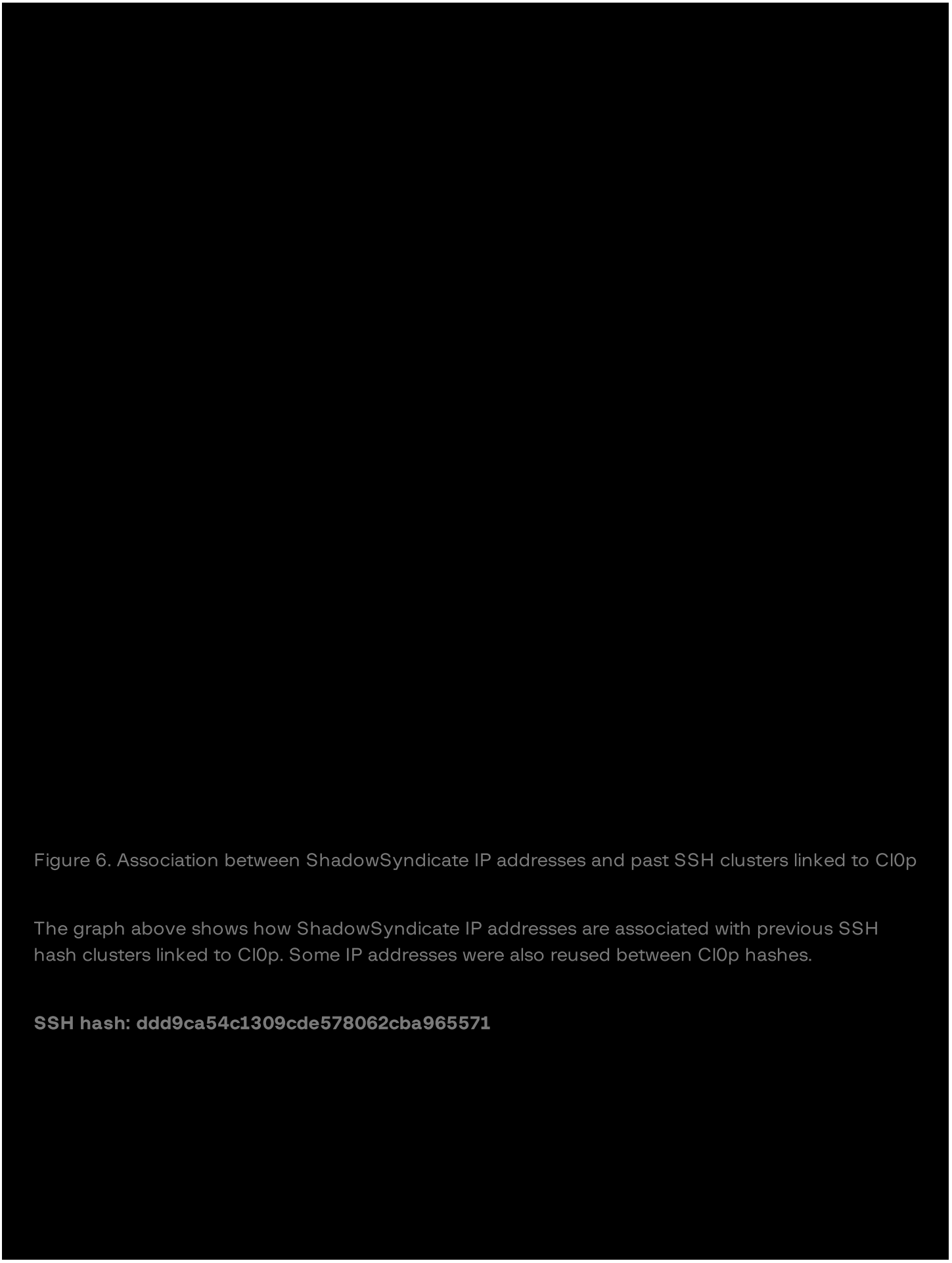


Figure 6. Association between ShadowSyndicate IP addresses and past SSH clusters linked to Cl0p

The graph above shows how ShadowSyndicate IP addresses are associated with previous SSH hash clusters linked to Cl0p. Some IP addresses were also reused between Cl0p hashes.

SSH hash: ddd9ca54c1309cde578062cba965571

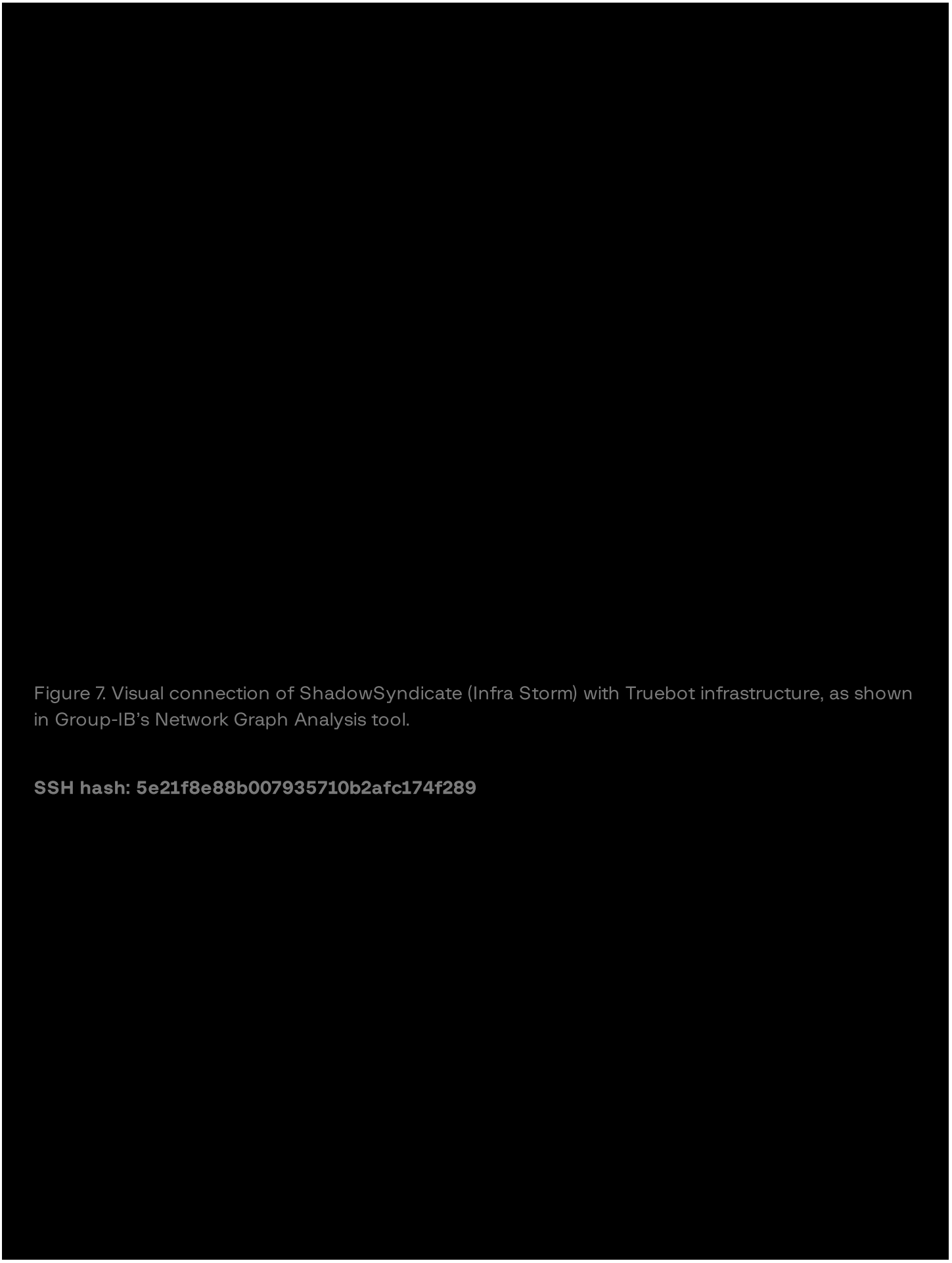


Figure 7. Visual connection of ShadowSyndicate (Infra Storm) with Truebot infrastructure, as shown in Group-IB's Network Graph Analysis tool.

SSH hash: 5e21f8e88b007935710b2afc174f289

Figure 8. Connection between ShadowSyndicate (Infra Storm) and SSH 5e21f8e88b007935710b2afc174f289

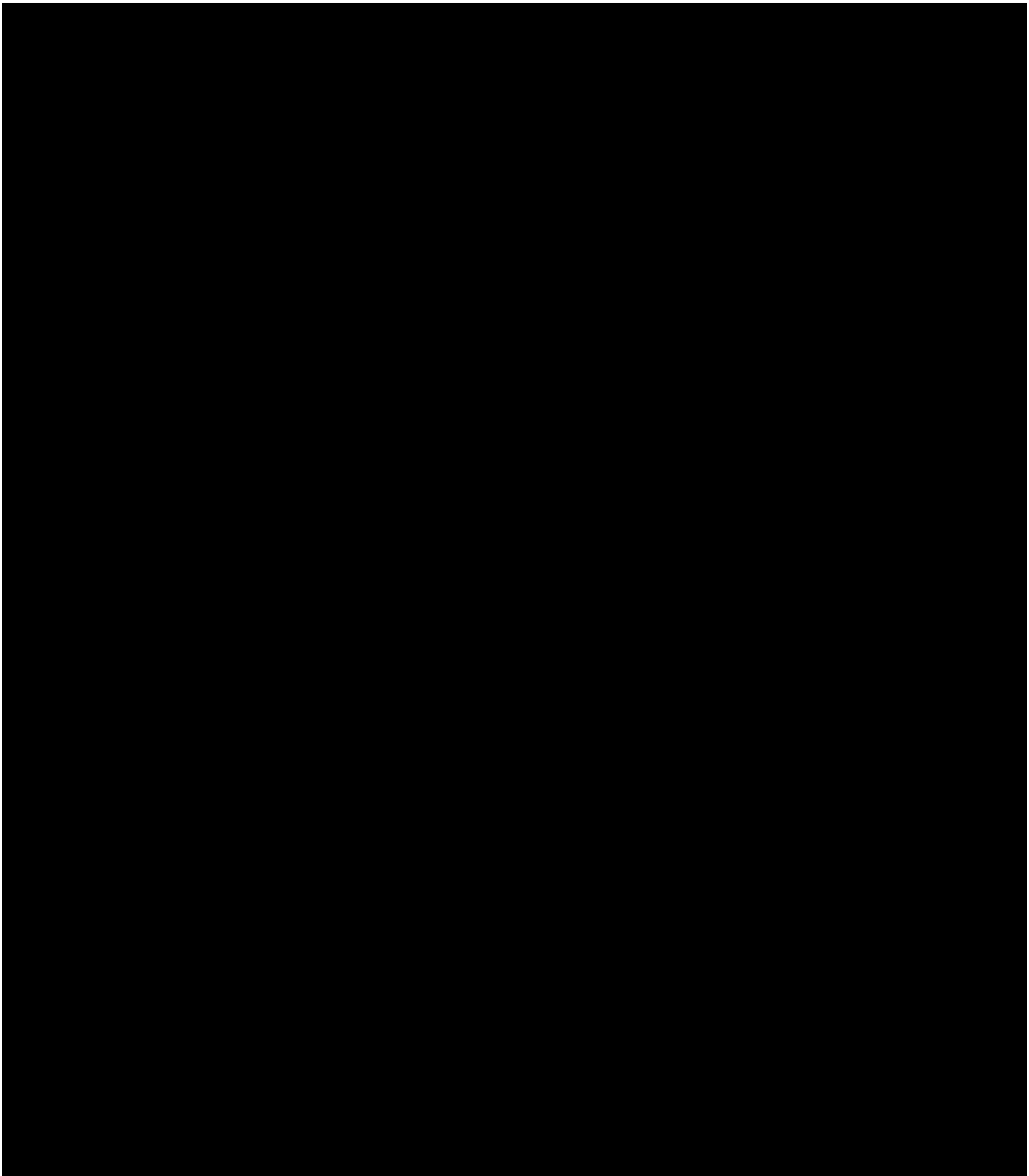


Figure 9. Comparison of hosting providers of ShadowSyndicate and Cl0p infrastructure

The above Figure 9 shows that while there is some limited crossover between the infrastructure used by both the two threat actors, the majority of the hosting providers leveraged by ShadowSyndicate have not been used by Cl0p previously.

Conclusions

Although we have not reached a final verdict, all the facts obtained during this joint research project suggest that the most plausible assumption is that ShadowSyndicate is an affiliate working with various RaaS.

Group-IB Threat Intelligence will continue to hunt for more information related to this particular threat actor, and as part of the Cybercrime Fighters Club initiative, we are open to collaboration with any researchers who also share our interest in fighting against cybercrime. We hope that with more research, we will be able to determine, in the near future, the threat actor's identity.

Join the Group-IB Cybercrime Fighters Club!

The global fight against cybercrime is a collaborative effort, and that's why we're looking to partner with industry peers to research emerging threats and publish joint findings on our blog. If you've discovered a breakthrough into a particular threat actor or a vulnerability in a piece of software, let us know, and we can mobilize all our necessary resources to dive deeper into the issue.

All contributions will be given appropriate credit along with the full backing of our social media team on Group-IB's Threat Intelligence Twitter page, where we regularly share our latest findings into threat actors' TTPs and infrastructure, along with our other social media accounts.

#LetsStopCybercrime #CybercrimeFightersClub

Join us now

Indicators of compromise

IP addresses

Domain names

Share this article

Found it interesting? Don't hesitate to share it to wow your friends or colleagues

Unified Risk Platform

Integrations

AI Cybersecurity Hub

Partners

Partner Program

MSSP and MDR Partner Program

Technology Partners

Partner Locator

Company

About Group-IB

Team

CERT-GIB

Careers

Internship

Academic Aliance

Sustainability

Media Center

Contact

Subscription plans

Services

Resource Center

Contact

APAC: +65 3159 3798

EU & NA: +31 20 226 90 90

MEA: +971 4 568 1785

info@group-ib.com

Subscribe to stay up to date with the latest cyber threat trends