THREAT INTELLIGENCE REPORT

ShadowSyndicate: A Global Ransomware-as-a-Service Player?

Authors:

Eline Switzer
Threat Intelligence Analyst, Group-IB

Joshua Penny
Senior Threat Intelligence Analyst, Bridewell

Michael Koczwara
Threat Researcher

Bridewell | GROUP-IB

Contents

Introduction

Ransomware-as-a-Service (RaaS) is a recent development that has made ransomware even more prolific over the last few years. In simple terms, a ransomware operator will write software that allows low-skills actors (known as affiliates) to launch their own ransomware campaigns. There is no need for these affiliates to be able to code or have much technical expertise, they can simply rely on the ransomware products provided by these vendors.

In many ways, the RaaS ecosystem is comparable to how modern tech companies operate and consume software as a service (SaaS) products. While there are any number of affiliates looking for the right RaaS product to help them operate their own ransomware campaigns, the ecosystem is upheld by a number of major players who supply RaaS. These groups find success in forming, selling their product and disbanding quickly – helping them evade identification.

At Bridewell CTI, we've been conducting research, in collaboration with Group-IB and independent researcher Michael Koczwara, into a new, major player in the RaaS ecosystem. In this report, we'll share our findings on this player, known as ShadowSyndicate, to uncover how they operate and what they're doing differently to conventional RaaS groups. We'll also be looking at the infrastructure they've leveraged and share indicators of compromise (IoCs) you should be aware of.

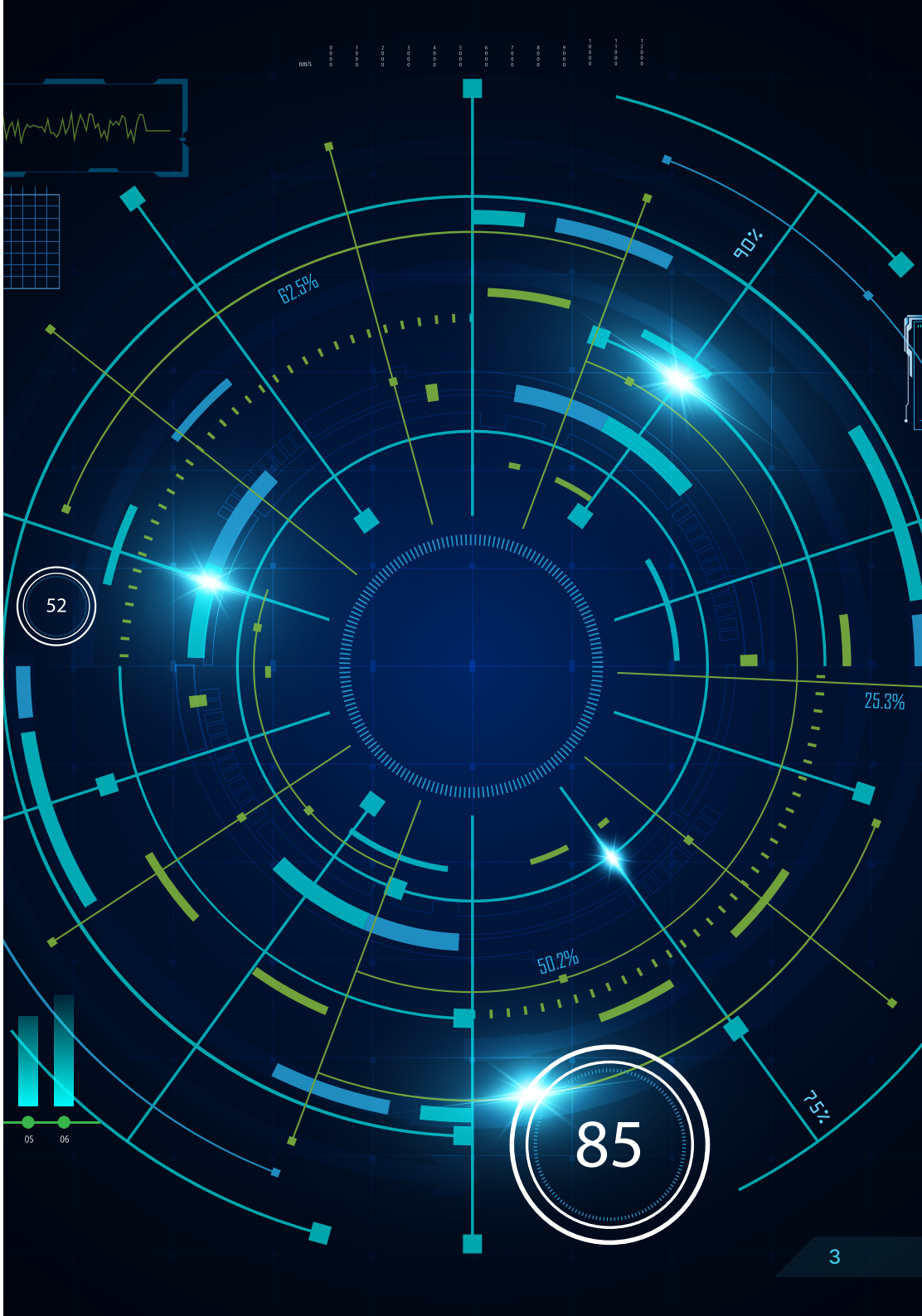
ShadowSyndicate: What Do You Need to Know?

ShadowSyndicate is unique when compared to other RaaS players. To start, it is unusual for a single Secure Shell (SSH) fingerprint to have such a complex web of connections with so many 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, we believe that the threat actor is the former. You can find more information on our hypotheses, evidence and conclusions later in this report.

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 and 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 (August 2023).

Together, we looked into any associated information we could find, with the aim of determining which cyber criminal 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:

a) ShadowSyndicate is a hoster who set up the SSH fingerprint on their server.

b) ShadowSyndicate is a DevOps engineer that deploys servers and provides them to various threat actors.

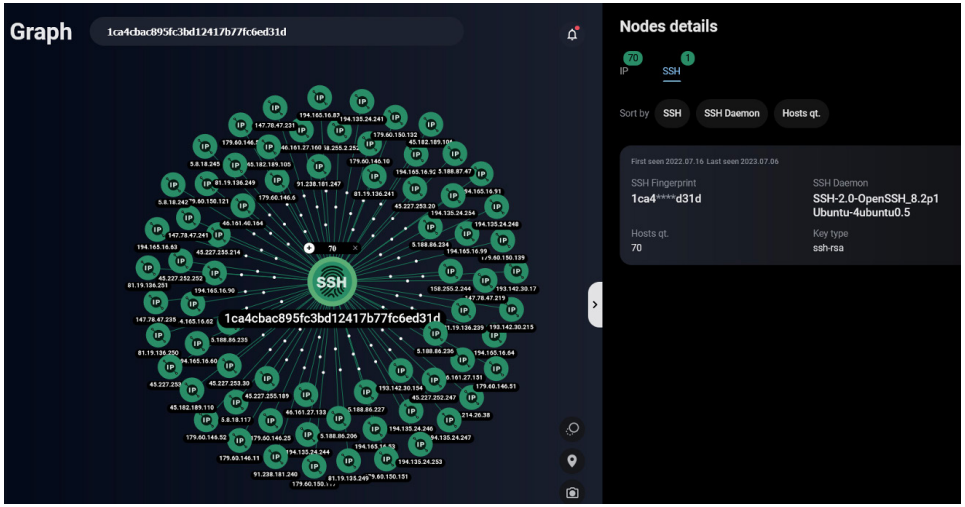
c) ShadowSyndicate owns an underground service offering “bulletproof hosting” to cyber criminals.

d) ShadowSyndicate is an initial access broker that obtains initial access to victims themselves and then sells that access to other cyber crime groups.

e) 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.

IP Addresses

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
10	194.165.16[.]53	2022.09.17
11	194.135.24[.]248	2022.09.18
12	45.227.253[.]29	2022.09.20
13	147.78.47[.]231	2022.09.20
14	194.165.16[.]83	2022.09.30
15	5.188.86[.]235	2022.09.30
16	5.8.18[.]117	2022.10.02
17	45.227.255[.]189	2022.10.07
18	5.8.18[.]242	2022.10.11
19	194.135.24[.]241	2022.11.12
20	45.227.252[.]247	2022.11.16
21	194.165.16[.]92	2022.11.22
22	147.78.47[.]241	2022.11.24
23	45.227.252[.]252	2022.11.25
24	5.8.18[.]245	2022.11.26
25	194.135.24[.]246	2022.11.28
26	194.165.16[.]63	2022.12.02
27	179.60.150[.]117	2022.12.05
28	194.165.16[.]64	2022.12.06
29	194.165.16[.]91	2022.12.19
30	194.135.24[.]253	2023.01.02
31	194.165.16[.]60	2023.01.02
32	81.19.136[.]250	2023.01.23
33	194.165.16[.]99	2023.01.24

IP Addresses

	IP address	SSH first seen on host
34	194.165.16[.]62	2023.01.24
35	81.19.136[.]249	2023.01.24
36	194.165.16[.]90	2023.01.29
37	179.60.150[.]151	2022.12.20
38	45.182.189[.]105	2023.02.09
39	45.182.189[.]106	2023.02.09
40	46.161.27[.]151	2023.02.13
41	81.19.136[.]239	2023.02.16
42	158.255.2[.]244	2023.03.12
43	179.60.146[.]6	2023.03.20
44	194.135.24[.]254	2023.04.04
45	46.161.27[.]160	2023.04.04

	IP address	SSH first seen on host
46	194.135.24[.]244	2023.04.04
47	158.255.2[.]252	2023.04.04
48	46.161.40[.]164	2023.04.05
49	179.60.146[.]10	2023.04.11
50	179.60.146[.]5	2023.04.11
51	88.214.26[.]38	2023.04.12
52	81.19.136[.]241	2023.04.13
53	179.60.150[.]121	2023.04.18
54	179.60.146[.]11	2023.04.18
55	91.238.181[.]240	2023.04.19
56	193.142.30[.]215	2023.04.21
57	179.60.150[.]132	2023.04.29

	IP address	SSH first seen on host
58	45.182.189[.]110	2023.05.09
59	81.19.136[.]251	2023.05.11
60	45.227.255[.]214	2023.05.12
61	5.188.86[.]206	2023.05.12
62	147.78.47[.]235	2023.05.16
63	147.78.47[.]219	2023.05.16
64	91.238.181[.]247	2023.05.17
65	5.188.86[.]236	2023.05.22
66	193.142.30[.]17	2023.05.22
67	193.142.30[.]154	2023.05.22
68	5.188.86[.]234	2023.05.22
69	46.161.27[.]133	2023.06.08

IP Addresses

	IP address	SSH first seen on host
70	5.188.87[.]47	2023.06.27
71	158.255.2[.]245	2023.07.20
72	179.60.150[.]125	2023.07.20
73	141.98.82[.]201	2023.07.20
74	78.128.112[.]139	Unknown (relevant on July 20, 2023)
75	193.29.13[.]202	Unknown (relevant on July 20, 2023)
76	78.128.112[.]207	Unknown (relevant on July 20, 2023)
77	193.29.13[.]148	Unknown (relevant on July 20, 2023)
78	193.142.30[.]205	2023.07.26
79	81.19.135[.]229	2023.08.17
80	193.142.30[.]211	Unknown (relevant on August 24, 2023)
81	45.227.252[.]229	Unknown (relevant on August 24, 2023)

	IP address	SSH first seen on host
82	193.142.30[.]37	Unknown (relevant on August 24, 2023)
83	78.128.11[.]220	Unknown (relevant on August 24, 2023)
84	5.188.87[.]54	Unknown (relevant on August 24, 2023)
85	5.188.87[.]41	2023.08.26

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 19 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 - Tools Identified

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

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.

Research - Tools Identified

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 watermark and the same sleeptime were also found to be used in attacks involving Nokoyawa.	Quantum – Link 1 | Link 2 Nokoyawa – Link 1 | Link 2
206546002	236	Royal, Quantum, Play	In late 2022, watermark 206546002 was found to be used in attacks related to Royal ransomware. Detected in attacks involving Quantum and Play.	Royal – Link Quantum, Play – Link
587247372	22	ALPHV, Play (likely)	In 2023, it was used in an attack involving ALPHV. Identified in an attack likely related to Play ransomware in March 2023.	Play (likely attack) – Link ALPHV – Link

Research - Tools Identified

Table 2 Continued. 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
1580103824	517	Cl0p, Possibly Royal	In May 2023, this watermark was detected in an attack related to Cl0p ransomware. In May 2022 this watermark was detected on server related to Royal In 2022, this watermark was detected in connection with IcedID and Gootloader malware.	Cl0p – Link: server 5.188.206[.]78 Royal – Link: server 139.60.161[.]69 with Cobalt Strike C2 anbush[.]com GitHub (IcedID) – Link Red Canary (Gootloader) – Link
674054486	187	ALPHV, Nokoyawa	In 2023, watermark 674054486 was detected in attacks related to ALPHV and Nokoyawa.	Nokoyawa – Link ALPHV - Group-IB Incident Response Engagement, February 2023
426352781	1068	Royal	In 2022, watermark 426352781 was observed in attacks related to Royal ransomware.	CISA – Link
668694132	43	Unknown		

It is noteworthy that, while analysing 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.

Research - Tools Identified

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, cmdatabase[.]com	194.165.16[.]91	79.137.202[.]45	Second server is not on List A

Research - Tools Identified

Table 3 Continued. Servers with identical Cobalt Strike configurations.

Pair no.	Configuration	Server #1 (Server on list A)	Server #2	Comment
5	2023-01-31 watermark 674054486, sleeptime 60946, devcloudpro[.]com	194.165.16[.]64	109.172.45[.]28	Second server is not on List A
6	2023-01-29 watermark 674054486, sleeptime 58835, uranustechsolution[.]com	194.165.16[.]90	109.172.45[.]77	Second server is not on List A
7	2022-11-12 watermark 674054486, sleeptime 57421	194.165.16[.]92	212.224.88[.]71	Second server is not on List A

Research - Tools Identified

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 organisations 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
00000000000000000000000000000000000000000000000000000000000000

References:

https://twitter.com/MichalKoczwara/status/1591326977457258497?s=20
https://twitter.com/MichalKoczwara/status/1591750513238118401?s=20
https://twitter.com/MichalKoczwara/status/1645002394734845956

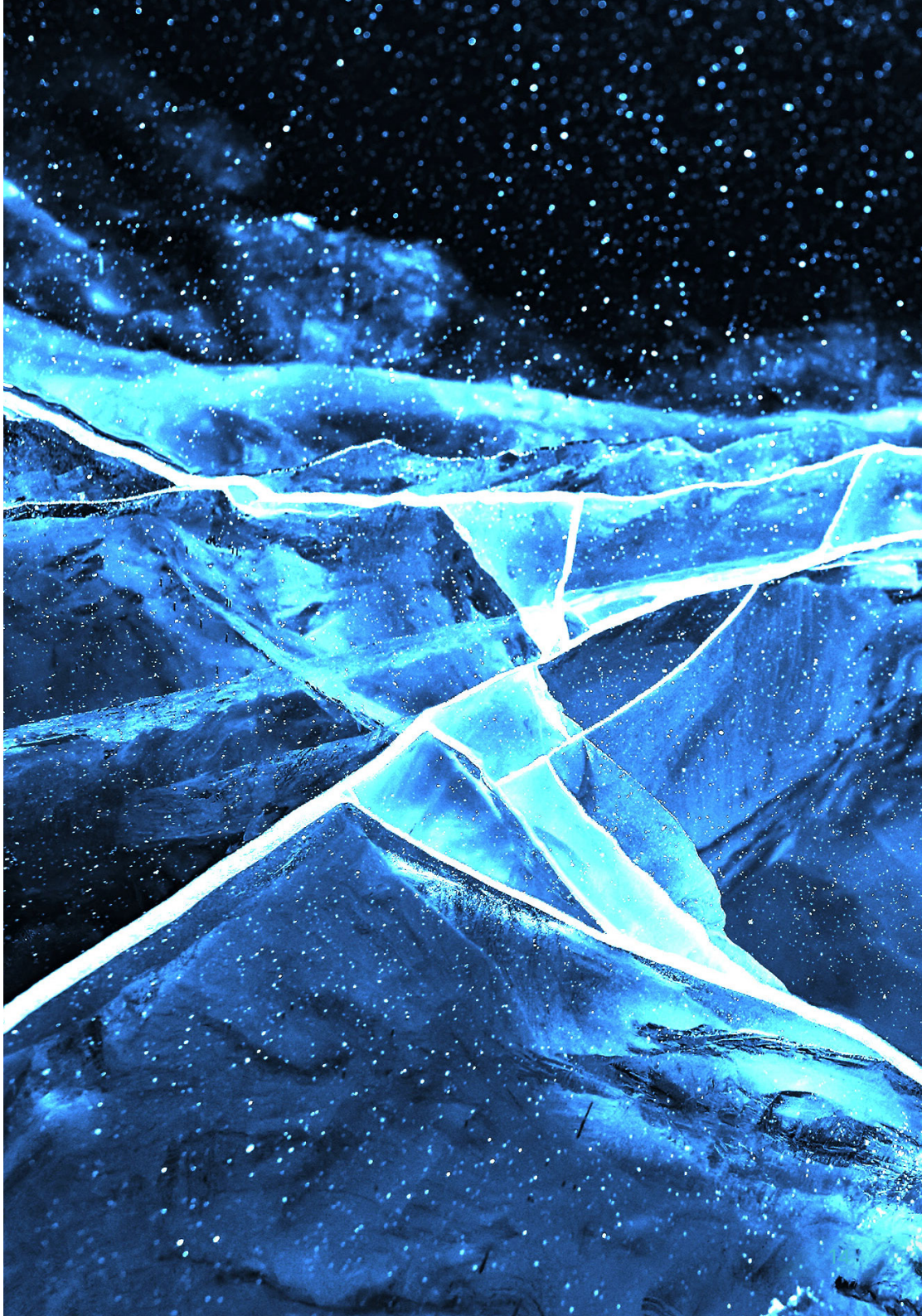
Research - Tools Identified

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.



Research - Tools Identified

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

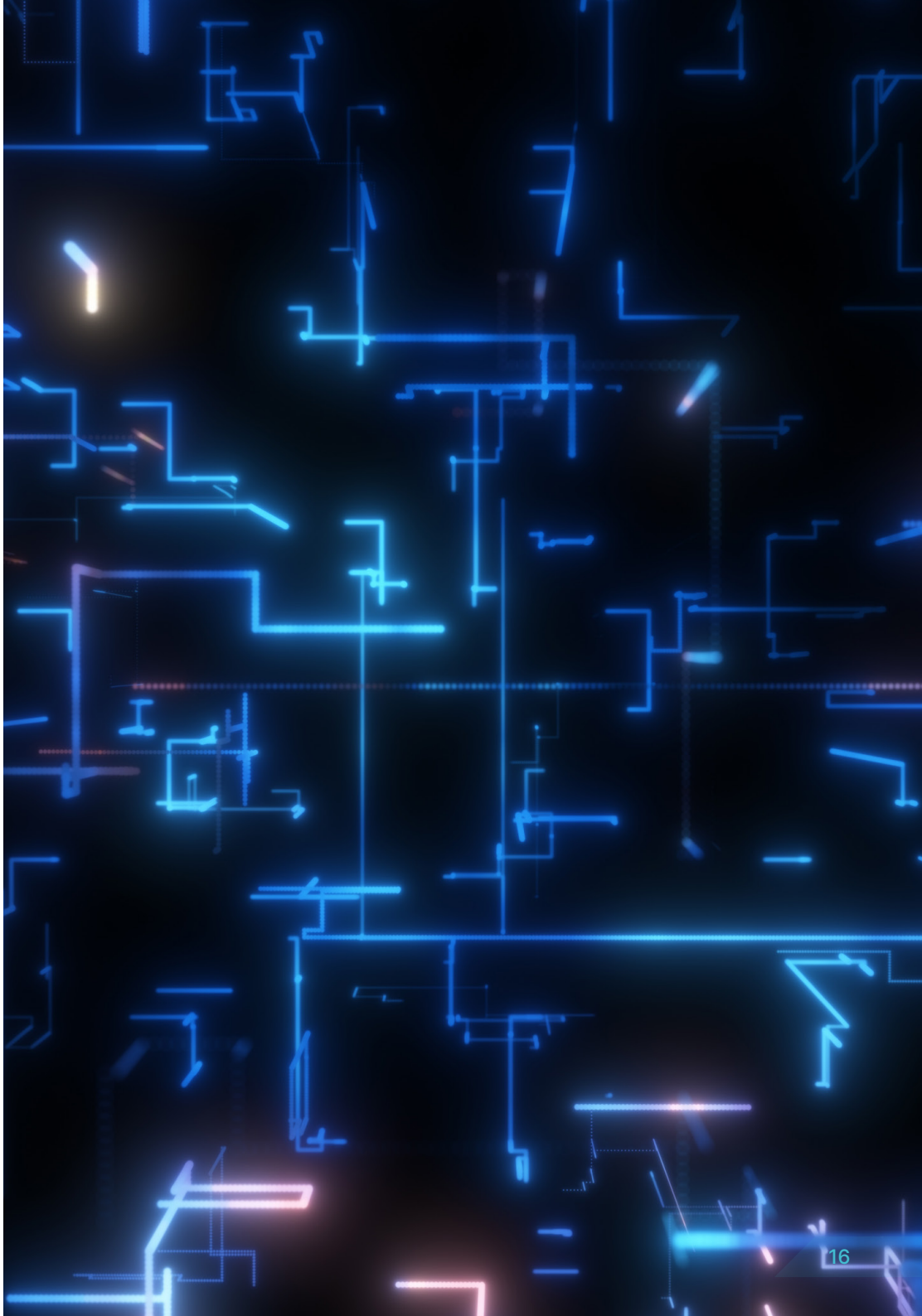
45.182.189[.]106

Research - Tools Identified

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.



Research - 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.
9	45.227.253[.]30	Panama	PA-DICO2-LACNIC	DirectWebH CORP
10	194.165.16[.]53	Panama	PA-FLYSERVERS	Flyservers S.A.
11	194.135.24[.]248	Czech Republic	CZ-RELCOM-19950206	Reliable Communications s.r.o.
12	45.227.253[.]29	Panama	PA-DICO2-LACNIC	DirectWebH CORP
13	147.78.47[.]231	Panama	GLOBALHOST-CUSTOMER-NET	END-CLIENTS-FOR-VPS-VDS

Research - Deployment of Servers

Table 4 Continued. Network information of servers.

	IP address	Country	Network Name	Owner Name
14	194.165.16[.]83	Panama	PA-FLYSERVERS	Flyservers S.A.
15	5.188.86[.]235	Cyprus	CHANNEL-NET	Channelnet
16	5.8.18[.]117	Cyprus	CLOUDBS-EUNET	Cloud VPS and Hosting Solutions
17	45.227.255[.]189	Panama	PA-OICO-LACNIC	Okpay Investment Company
18	5.8.18[.]242	Cyprus	CLOUDBS-EUNET	Cloud VPS and Hosting Solutions
19	194.135.24[.]241	Czech Republic	CZ-RELCOM-19950206	Reliable Communications s.r.o.
20	45.227.252[.]247	Honduras	HN-DGSA-LACNIC	DATA GRANDE S.A.
21	194.165.16[.]92	Panama	PA-FLYSERVERS	Flyservers S.A.
22	147.78.47[.]241	Panama	GLOBALHOST-CUSTOMER-NET	END-CLIENTS-FOR-VPS-VDS
23	45.227.252[.]252	Honduras	HN-DGSA-LACNIC	DATA GRANDE S.A.
24	5.8.18[.]245	Cyprus	CLOUDBS-EUNET	Cloud VPS and Hosting Solutions
25	194.135.24[.]246	Czech Republic	CZ-RELCOM-19950206	Reliable Communications s.r.o.
26	194.165.16[.]63	Panama	PA-FLYSERVERS	Flyservers S.A.
27	179.60.150[.]117	Belize	BZ-MGLT-LACNIC	MAXWELL GROUP LTD
28	194.165.16[.]64	Panama	PA-FLYSERVERS	Flyservers S.A.
29	194.165.16[.]91	Panama	PA-FLYSERVERS	Flyservers S.A.
30	194.135.24[.]253	Czech Republic	CZ-RELCOM-19950206	Reliable Communications s.r.o.

Research - Deployment of Servers

Table 4 Continued. Network information of servers.

	IP address	Country	Network Name	Owner Name
31	194.165.16[.]60	Panama	PA-FLYSERVERS	Flyservers S.A.
32	81.19.136[.]250	Seychelles	DIGICLOUD-NET136	Alviva Holding Limited
33	194.165.16[.]99	Panama	PA-FLYSERVERS	Flyservers S.A.
34	194.165.16[.]62	Panama	PA-FLYSERVERS	Flyservers S.A.
35	81.19.136[.]249	Seychelles	DIGICLOUD-NET136	Alviva Holding Limited
36	194.165.16[.]90	Panama	PA-FLYSERVERS	Flyservers S.A.
37	179.60.150[.]151	Belize	BZ-MGLT-LACNIC	MAXWELL GROUP LTD
38	45.182.189[.]105	Panama	PA-DASA4-LACNIC	DATAHOME S.A.
39	45.182.189[.]106	Panama	PA-DASA4-LACNIC	DATAHOME S.A.
40	46.161.27[.]151	Netherlands	Megaholdings-net	VPS and Shared Hosting pool
41	81.19.136[.]239	Seychelles	DIGICLOUD-NET136	Alviva Holding Limited
42	158.255.2[.]244	Russian Federation	RU-SERVER-V-ARENDY-20111114	LLC "Server v arendy"
43	179.60.146[.]6	Costa Rica	CR-DASA3-LACNIC	DATASOLUTIONS S.A.
44	194.135.24[.]254	Czech Republic	CZ-RELCOM-19950206	Reliable Communications s.r.o.
45	46.161.27[.]160	Netherlands	Megaholdings-net	VPS and Shared Hosting pool
46	194.135.24[.]244	Czech Republic	CZ-RELCOM-19950206	Reliable Communications s.r.o.
47	158.255.2[.]252	Russian Federation	RU-SERVER-V-ARENDY-20111114	LLC "Server v arendy"

Research - Deployment of Servers

Table 4 Continued. Network information of servers.

	IP address	Country	Network Name	Owner Name
48	46.161.40[.]164	Moldova	ankas-net	net for ankas
49	179.60.146[.]10	Costa Rica	CR-DASA3-LACNIC	DATASOLUTIONS S.A.
50	179.60.146[.]5	Costa Rica	CR-DASA3-LACNIC	DATASOLUTIONS S.A.
51	88.214.26[.]38	Seychelles	FCLOUD-NET	FutureNow Incorporated
52	81.19.136[.]241	Seychelles	DIGICLOUD-NET136	Alviva Holding Limited
53	179.60.150[.]121	Belize	BZ-MGLT-LACNIC	MAXWELL GROUP LTD
54	179.60.146[.]11	Costa Rica	CR-DASA3-LACNIC	DATASOLUTIONS S.A.
55	91.238.181[.]240	Martinique	ONEHOST-NET	VDS&VPN services
56	193.142.30[.]215	Russian Federation	BATTERFLYAIMEDIA-NET	Batterflyai Media ltd.
57	179.60.150[.]132	Belize	BZ-MGLT-LACNIC	MAXWELL GROUP LTD
58	45.182.189[.]110	Panama	PA-DASA4-LACNIC	DATAHOME S.A.
59	81.19.136[.]251	Seychelles	DIGICLOUD-NET136	Alviva Holding Limited
60	45.227.255[.]214	Panama	PA-OICO-LACNIC	Okpay Investment Company
61	5.188.86[.]206	Cyprus	CHANNEL-NET	Channelnet
62	147.78.47[.]235	Panama	GLOBALHOST-CUSTOMER-NET	END-CLIENTS-FOR-VPS-VDS
63	147.78.47[.]219	Panama	GLOBALHOST-CUSTOMER-NET	END-CLIENTS-FOR-VPS-VDS
64	91.238.181[.]247	Martinique	ONEHOST-NET	VDS&VPN services

Research - Deployment of Servers

Table 4 Continued. Network information of servers.

	IP address	Country	Network Name	Owner Name
65	5.188.86[.]236	Cyprus	CHANNEL-NET	Channelnet
66	193.142.30[.]17	Russian Federation	BATTERFLYAIMEDIA-NET	Batterflyai Media ltd.
67	193.142.30[.]154	Russian Federation	BATTERFLYAIMEDIA-NET	Batterflyai Media ltd.
68	5.188.86[.]234	Cyprus	CHANNEL-NET	Channelnet
69	46.161.27[.]133	Netherlands	Megaholdings-net	VPS and Shared Hosting pool
70	5.188.87[.]47	Cyprus	CHANNEL-NET	Channelnet
71	158.255.2[.]245	Russian Federation	RU-SERVER-V-ARENDY-20111114	LLC "Server v arendy"
72	179.60.150[.]125	Belize	BZ-MGLT-LACNIC	MAXWELL GROUP LTD
73	141.98.82[.]201	Panama	VDSLINE-NET	Flyservers S.A.
74	78.128.112[.]139	Bulgaria	DOTDASH-NET	VPS and Shared Hosting pool
75	193.29.13[.]202	Romania	HOSTING-NETWORK	VPS & shared hosting pool
76	78.128.112[.]207	Bulgaria	DOTDASH-NET	VPS and Shared Hosting pool
77	193.29.13[.]148	Romania	HOSTING-NETWORK	VPS & shared hosting pool
78	193.142.30[.]205	Russian Federation	BATTERFLYAIMEDIA-NET	Batterflyai Media ltd.
79	81.19.135[.]229	Seychelles	DIGICLOUD-NET	Alviva Holding Limited
80	193.142.30[.]211	Russian Federation	BATTERFLYAIMEDIA-NET	Batterflyai Media ltd.
81	45.227.252[.]229	Honduras	HN-DGSA-LACNIC	DATA GRANDE S.A.

Research - Deployment of Servers

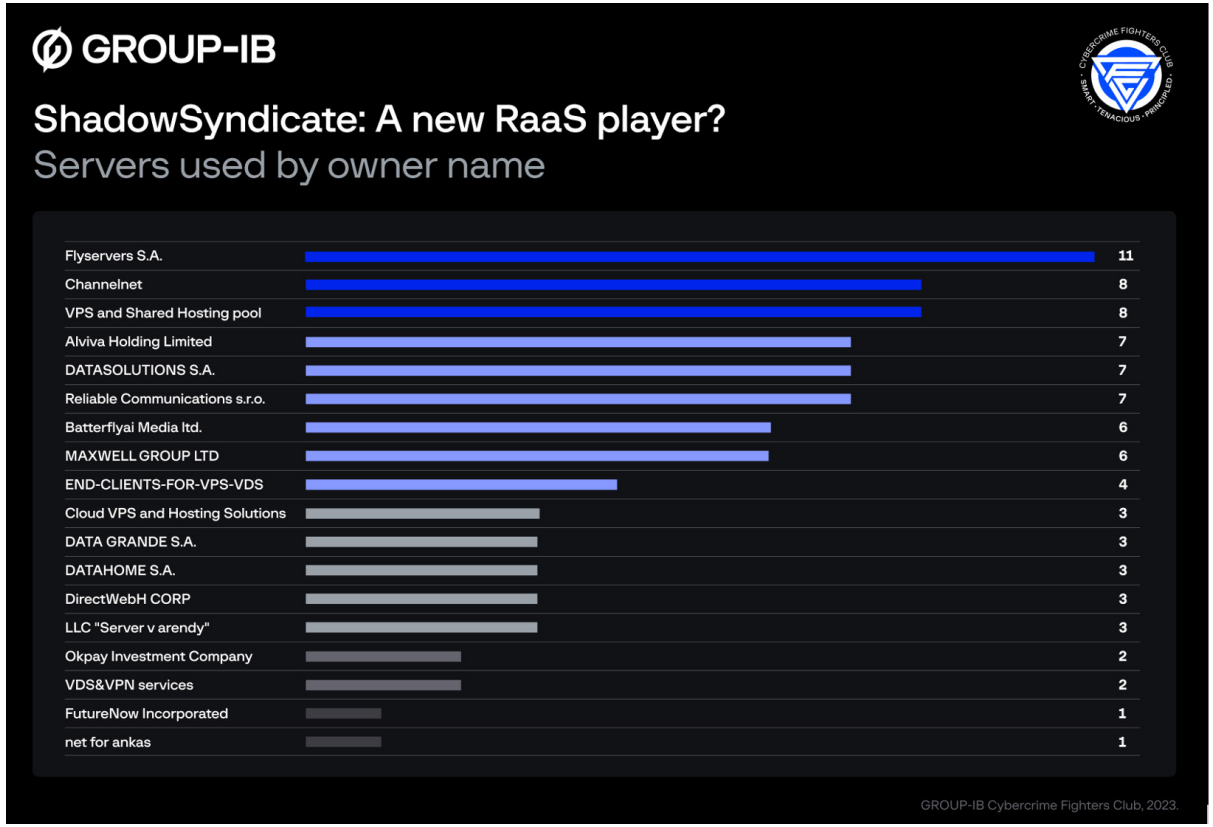
Table 4 Continued. Network information of servers.

	IP address	Country	Network Name	Owner Name
82	193.142.30[.]37	Russian Federation	BATTERFLYAIMEDIA-NET	Batterflyai Media ltd.
83	78.128.11[.]220	Bulgaria	DOTDASH-NET	VPS and Shared Hosting pool
84	5.188.87[.]54	Cyprus	CHANNEL-NET	Channelnet
85	5.188.87[.]41	Cyprus	CHANNEL-NET	Channelnet

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.

Research - Deployment of Servers

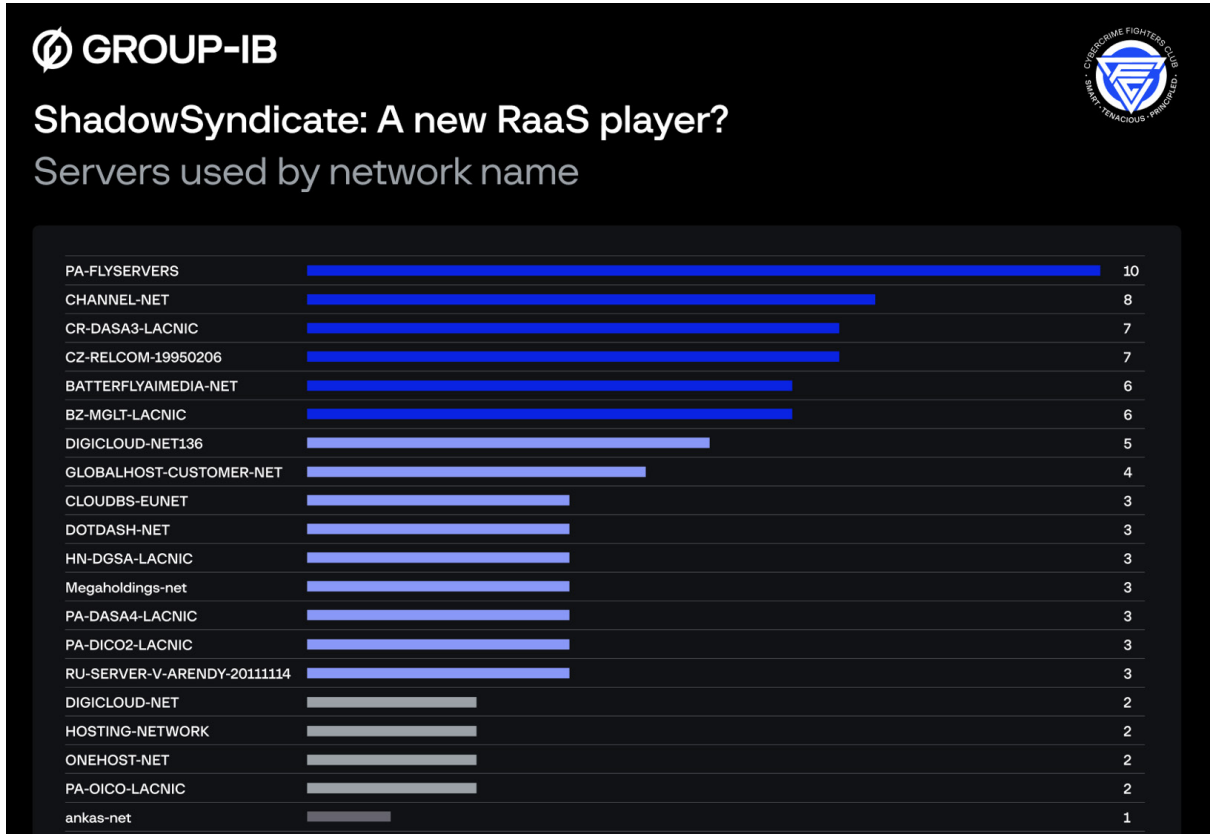
Figure 2. ShadowSyndicate servers by owner name.



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.

Research - Deployment of Servers

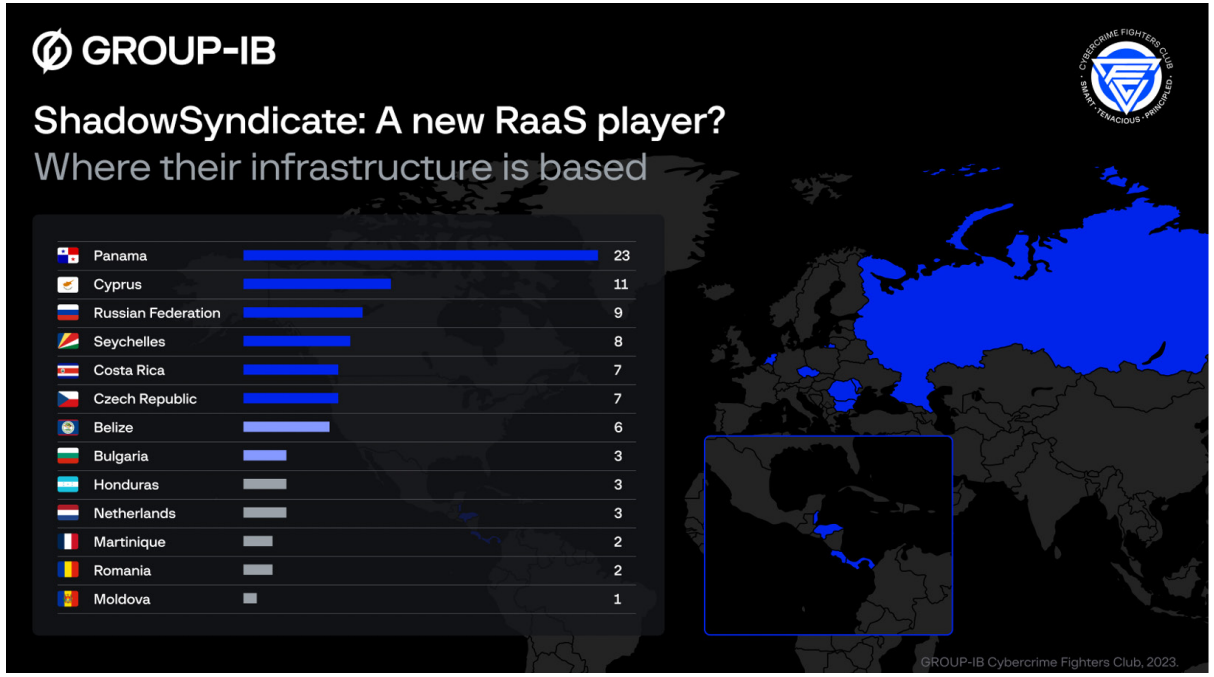
Figure 3. ShadowSyndicate servers by network name.



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.

Research - Deployment of Servers

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 samples (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**.

Research - 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

Research - Data Attributed With a High Degree of Confidence

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.

Research - Data Attributed With a High Degree of Confidence

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

IP address	Attribution
46.161.27[.]1	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.

Research - Data Attributed With a High Degree of Confidence

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 on page 11). 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.

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.

Data Attributed With a Low Degree of Confidence

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[.]com In 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 60000 April 8, 2023 watermark 1580103824 sleeptime 60000 In 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 1580103824 was detected on a server related to Royal ransomware. In May 2023, watermark 1580103824 was detected in an attack related to Cl0p ransomware.

Data Attributed With a Low Degree of Confidence

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

IP address	SSH first seen on host	Cobalt Strike configurations and possible attributions
5.188.86[.]227	August 17, 2022	March 21, 2023 watermark 674054486 sleeptime 86137 domain psychologymax[.]com April 10, 2023 watermark 587247372 sleeptime 64864 domain mirrordirectory[.]com April 27, 2023 watermark 587247372 sleeptime 60000 domain msf-sql[.]com In 2023, watermark 674054486 was detected in attacks related to ALPHV and Nokoyawa. In 2023, watermark 587247372 was used in an attack involving ALPHV, and in March 2023 in an attack possibly related to Play ransomware

Data Attributed With a Low Degree of Confidence

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

IP address	SSH first seen on host	Cobalt Strike configurations and possible attributions
179.60.146[.]25	September 14, 2022	October 1, 2022 watermark 206546002 sleeptime 60000 domain mysqlserver[.]org March 27, 2023 watermark 674054486 sleeptime 58376 domain opentechcorp[.]net In late 2022, watermark 206546002 was detected in attacks related to Royal ransomware. In 2022, it was detected in attacks involving Quantum and Play. In 2023, watermark 674054486 was detected in attacks related to ALPHV and Nokoyawa.
45.227.253[.]30	September 14, 2022	August 11, 2022 watermark 206546002 sleeptime 60000 September 14, 2022 watermark 305419776 sleeptime 60000 domain windosupdate[.]net In late 2022, watermark 206546002 was detected in attacks related to Royal ransomware. In 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.

Data Attributed With a Low Degree of Confidence

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

IP address	SSH first seen on host	Cobalt Strike configurations and possible attributions
194.165.16[.]53	September 17, 2022	September 17, 2022 watermark 206546002 sleeptime 56957 domain maximumservers[.]net In late 2022, watermark 206546002 was detected in attacks related to Royal ransomware. In 2022, it was detected in attacks involving Quantum and Play.
194.135.24[.]248	September 18, 2022	September 19, 2022 watermark 305419776 sleeptime 60000 In April and September 2022, watermark 305419776 + sleeptime 60000 were detected in attacks involving Quantum ransomware. In Q4 2022, this watermark also was detected in an attack involving Nokoyawa.
147.78.47[.]231	September 20, 2022	September 19, 2022 watermark 1580103824 sleeptime 60000 In 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.
194.165.16[.]83	September 30, 2022	October 1, 2022 watermark 668694132 sleeptime 61118 domain ipulsecloud[.]com

Data Attributed With a Low Degree of Confidence

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

IP address	SSH first seen on host	Cobalt Strike configurations and possible attributions
5.188.86[.]235	September 30, 2022	September 30, 2022 watermark 305419776 sleeptime 60000 March 15, 2023 watermark 674054486 sleeptime 85087 domain herbswallow[.]com March 31, 2023 watermark 587247372 sleeptime 45000 domain d4ng3r.s01kaspersky[.]com April 5, 2023 watermark 587247372 sleeptime 45000 domain cache01.micnosoftupdate[.]com April 11, 2023 watermark 587247372 sleeptime 45000 msupd.wimdowupdate[.]com April 12, 2023 watermark 587247372 sleeptime 45000 upd232.windowservicecentar[.]com

Data Attributed With a Low Degree of Confidence

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

IP address	SSH first seen on host	Cobalt Strike configurations and possible attributions
5.188.86[.]235	September 30, 2022	In April and September 2022, watermark 305419776 + sleeptime 60000 were detected in attacks involving Quantum ransomware. In Q4 2022, this watermark also was detected in an attack involving Nokoyawa. In 2023, watermark 674054486 was detected in attacks related to ALPHV and Nokoyawa. Domain d4ng3r.s01kaspersky[.]com and watermark 587247372 were detected in an attack possibly related to Play ransomware.
5.8.18[.]117	October 2, 2022	October 1, 2022 watermark 206546002 sleeptime 60000 In late 2022, watermark 206546002 was detected in attacks related to Royal ransomware. In 2022, it was detected in attacks involving Quantum and Play.
194.135.24[.]241	November 12, 2022	July 24, 2022 watermark 206546002 sleeptime 60000 November 15, 2022 watermark 12345 sleeptime 38142 domain paloaltocloud[.]online In late 2022, watermark 206546002 was detected in attacks related to Royal ransomware. In 2022, it was detected in attacks involving Quantum and Play. In 2023, watermark 12345 was detected in attacks related to Royal and Cactus.

Data Attributed With a Low Degree of Confidence

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

IP address	SSH first seen on host	Cobalt Strike configurations and possible attributions
45.227.252[.]247	November 16, 2022	November 17, 2022 watermark 305419776 sleeptime 60000 December 21, 2022 watermark 426352781 sleeptime 60000 In April and September 2022, watermark 305419776 + sleeptime 60000 were detected in attacks involving Quantum ransomware. In Q4 2022, this watermark was also detected in an attack involving Nokoyawa. In 2022, watermark 426352781 was detected in attacks related to Royal ransomware.
194.165.16[.]92	November 22, 2022	November 12, 2022 watermark 674054486 sleeptime 57421 In 2023, watermark 674054486 was detected in attacks involving ALPHV and Nokoyawa.
45.227.252[.]252	November 25, 2022	November 25, 2022 watermark 305419776 sleeptime 60000 In April and September 2022, watermark 305419776 + sleeptime 60000 were detected in attacks involving Quantum ransomware. In Q4 2022, this watermark was also detected in an attack involving Nokoyawa.

Data Attributed With a Low Degree of Confidence

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

IP address	SSH first seen on host	Cobalt Strike configurations and possible attributions
5.8.18[.]245	November 26, 2022	Cobalt Strike November 26, 2022 watermark 206546002 + sleeptime 60000 In late 2022, watermark 206546002 was detected in attacks related to Royal ransomware.
194.135.24[.]246	November 28, 2022	Cobalt Strike March 10, 2023 watermark 674054486 + sleeptime 119588 In 2023, watermark 674054486 was detected in attacks involving ALPHV and Nokoyawa.
179.60.150[.]117	December 5, 2022	April 29, 2022 watermark 206546002 sleeptime 60000 December 5, 2022 watermark 674054486 domain esoftwareupdates[.]com In April 2022, a Group-IB hunting rule attributed this IP address to FIN7 (according to a unique SSL certificate). In late 2022, watermark 206546002 was detected in attacks related to Royal ransomware. In 2022, it was detected in attacks involving Quantum and Play. In 2023, watermark 674054486 was detected in attacks related to ALPHV and Nokoyawa.

Data Attributed With a Low Degree of Confidence

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

IP address	SSH first seen on host	Cobalt Strike configurations and possible attributions
194.165.16[.]91	December 19, 2022	October 26, 2022 watermark 426352781 sleeptime 28 December 19, 2022 watermark 674054486 sleeptime 60216, domain cmdatabase[.]com In 2022, watermark 426352781 was detected in attacks related to Royal ransomware. In 2023, watermark 674054486 was detected in attacks related to ALPHV and Nokoyawa.
179.60.150[.]151	December 20, 2022	December 20, 2022 watermark 674054486 sleeptime 61156 In 2023, watermark 674054486 was detected in attacks related to ALPHV and Nokoyawa.
194.135.24[.]253	January 2, 2023	January 3, 2023 watermark 674054486 sleeptime 119588 In 2023, watermark 674054486 was detected in attacks related to ALPHV and Nokoyawa.

Data Attributed With a Low Degree of Confidence

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

IP address	SSH first seen on host	Cobalt Strike configurations and possible attributions
194.165.16[.]60	January 2, 2023	June 23, 2022 watermark 305419776 sleeptime 60000 January 28, 2023 watermark 206546002 sleeptime 60000 In April and September 2022, watermark 305419776 + sleeptime 60000 were detected in attacks involving Quantum ransomware. In Q4 2022, this watermark was also detected in an attack involving Nokoyawa. In late 2022, watermark 206546002 was detected in attacks related to Royal ransomware.
194.165.16[.]62	January 24, 2023	January 19, 2023 watermark 674054486 sleeptime 57247 domain avdev[.]net In 2023, watermark 674054486 was detected in attacks related to ALPHV and Nokoyawa.
179.60.146[.]6	March 20, 2023	March 19, 2023 watermark 674054486 sleeptime 63826 domain powersupportplan[.]com In 2023, watermark 674054486 was detected in attacks related to ALPHV and Nokoyawa.

Data Attributed With a Low Degree of Confidence

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

IP address	SSH first seen on host	Cobalt Strike configurations and possible attributions
179.60.146[.]10	April 11, 2023	April 11, 2023 watermark 674054486 sleeptime 56209 domain aerosunelectric[.]com In 2023, watermark 674054486 was detected in attacks related to ALPHV and Nokoyawa.
179.60.146[.]5	April 11, 2023	2023-04-11 watermark 674054486 sleeptime 58845 domain expotechsupport[.]com In 2023, watermark 674054486 was detected in attacks related to ALPHV and Nokoyawa.
179.60.146[.]11	April 18, 2023	April 18, 2023 watermark 674054486 sleeptime 64535 domain webtoolsmedia[.]com In 2023, watermark 674054486 was detected in attacks related to ALPHV and Nokoyawa.
91.238.181[.]240	April 19, 2023	April 19, 2023 watermark 674054486 sleeptime 63427 domain settingdata[.]com In 2023, watermark 674054486 was detected in attacks related to ALPHV and Nokoyawa.

Data Attributed With a Low Degree of Confidence

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

IP address	SSH first seen on host	Cobalt Strike configurations and possible attributions
5.188.86[.]206	May 12, 2023	Cobalt Strike May 17, 2023 watermark 12345 sleeptime 60000 In 2023 watermark 12345 was observed in attacks related to Royal and Cactus.
147.78.47[.]235	May 16, 2023	May 17, 2023 watermark 1580103824 sleeptime 55713 In May 2023, watermark 1580103824 was detected in an attack related to Cl0p ransomware.
147.78.47[.]219	May 16, 2023	May 29, 2023 watermark 1580103824 sleeptime 59800 domain qw.vm3dservice[.]com In May 2023, watermark 1580103824 was detected in an attack related to Cl0p ransomware.
91.238.181[.]247	May 17, 2023	2023-05-16 watermark 587247372 domain situotech[.]com In 2023, watermark 587247372 was detected in attacks related to Play and Royal ransomware.

Data Attributed With a Low Degree of Confidence

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

IP address	SSH first seen on host	Cobalt Strike configurations and possible attributions
46.161.27[.]133	June 8, 2023	May 2023 watermark 580103824 domain qw.sortx2[.]com In May 2023, watermark 1580103824 was detected in an attack related to Cl0p ransomware.
5.188.87[.]47	June 27, 2023	June 27, 2023 watermark 1580103824 sleeptime 60037 domain dsvchost[.]com In May 2023, watermark 1580103824 was detected in an attack related to Cl0p ransomware.
193.29.13[.]148	Unknown (relevant on July 20, 2023)	May 25, 2023 watermark 674054486 In 2023, watermark 674054486 was detected in attacks related to ALPHV and Nokoyawa.

Data Attributed With a Low Degree of Confidence

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
81.19.135[.]229	August 17, 2023	Cobalt Strike wasn't detected on this host. However, this server is connected to several domains registered on August 16, 2023: etgtgvtgttefeer[.]xyz egetrgertgegege[.]xyz egetrgertgeb[.]xyz egetrgertgebrtgf[.]xyz egetrgertgegegevgvyub[.]xyz
5.188.87[.]41	August 26, 2023	Cobalt Strike wasn't detected on this host in 2022 and 2023. It was detected in September 2021. However, this server is connected to a domain registered on August 22, 2023: svchostsreg[.]com

Data Attributed With a Low Degree of Confidence

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** change 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:

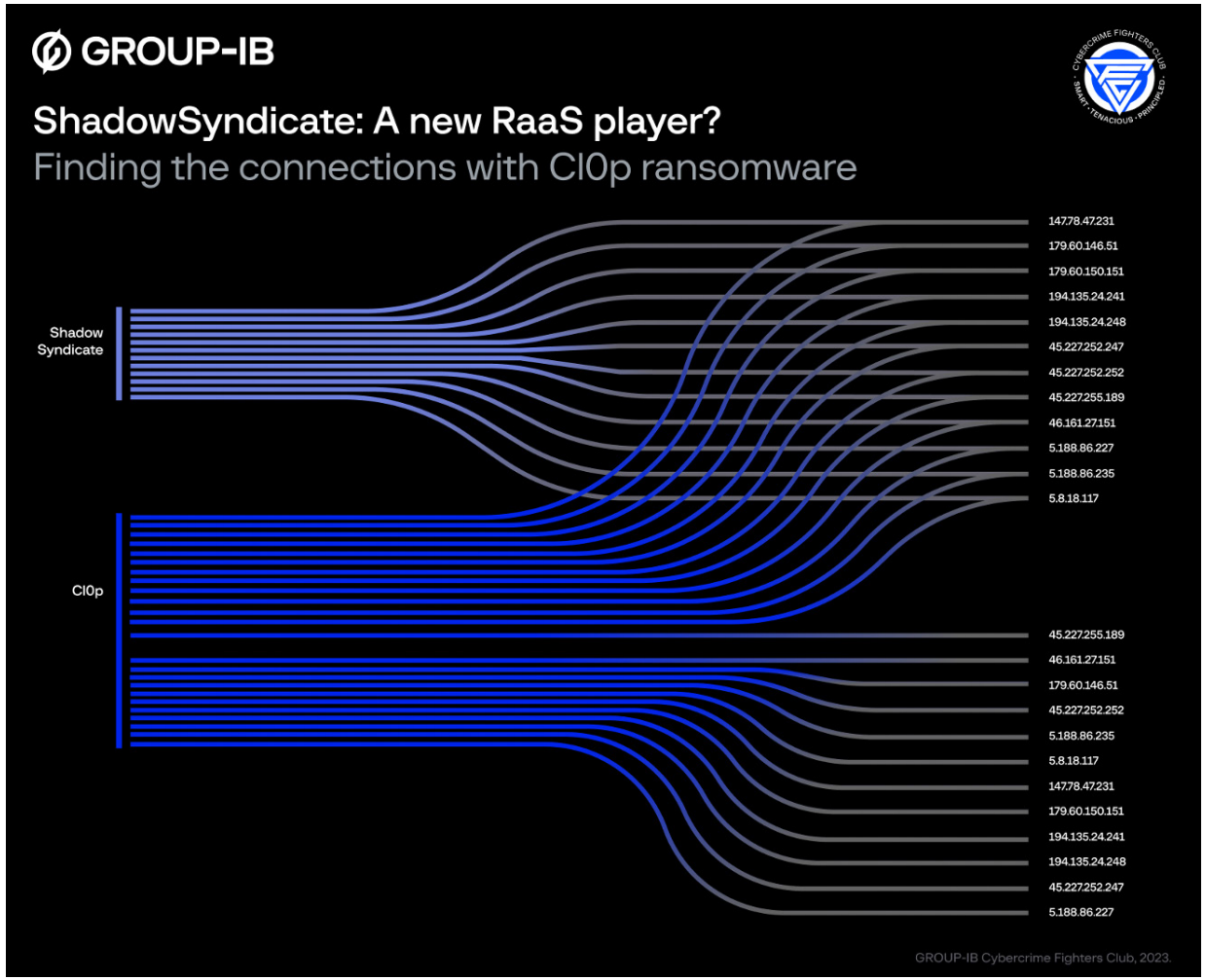
Table 11. IP addresses shared between Cl0p and ShadowSyndicate

IP address	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

IP address	ShadowSyndicate SSH first seen	Usage
45.227.252[.]252	November 25, 2022	Cobalt Strike
45.227.255[.]189	October 7, 2022	Cobalt Strike
46.161.27[.]151	February 13, 2023	Cobalt Strike/Metasploit
5.188.86[.]227	August 17, 2022	Cobalt Strike
5.188.86[.]235	October 26, 2022	Cobalt Strike
5.8.18[.]117	October 2, 2022	Cobalt Strike

Data Attributed With a Low Degree of Confidence

Figure 5: Data visualization of connections between ShadowSyndicate and Cl0p



Data Attributed With a Low Degree of Confidence

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

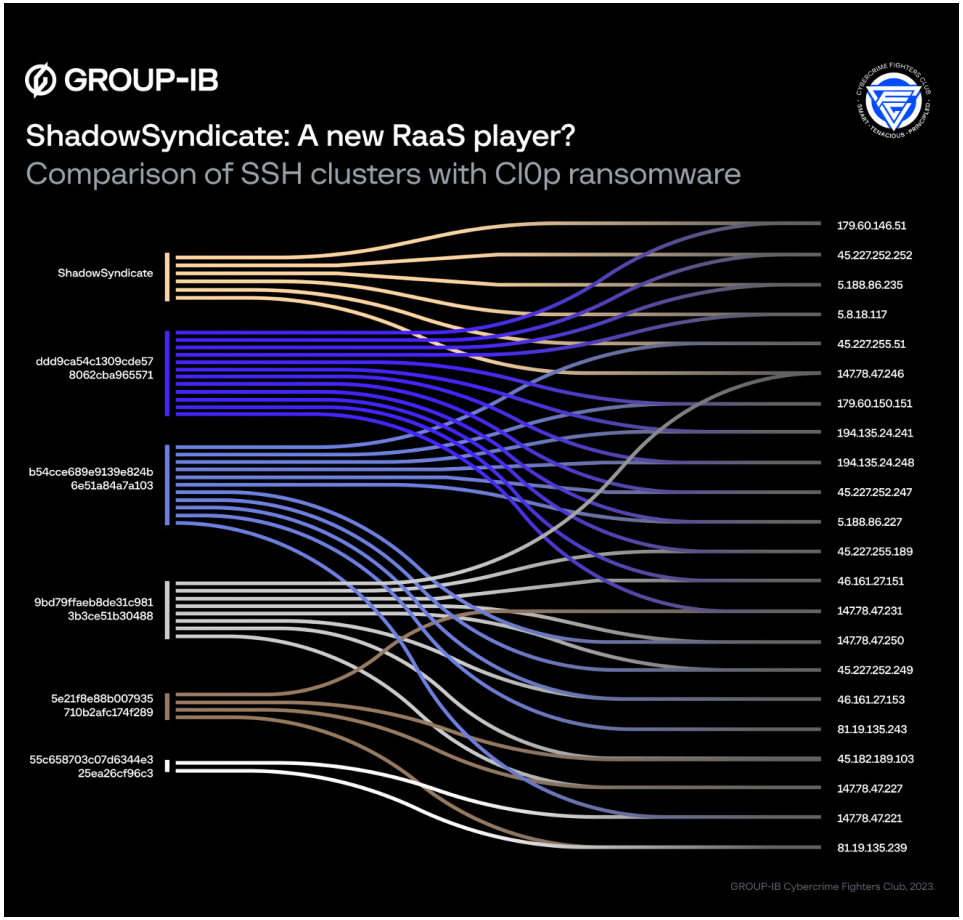
5e21f8e88b007935710b2afc174f289

55c658703c07d6344e325ea26cf96c3

96ea77a1a901e38aac8b9d5772d3d765

In Figure 6, 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 shows how ShadowSyndicate IP addresses are associated with previous SSH hash clusters linked to Cl0p. Some IP addresses were also reused between Cl0p hashes.

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



Data Attributed With a Low Degree of Confidence

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

SSH hash: ddd9ca54c1309cde578062cba965571

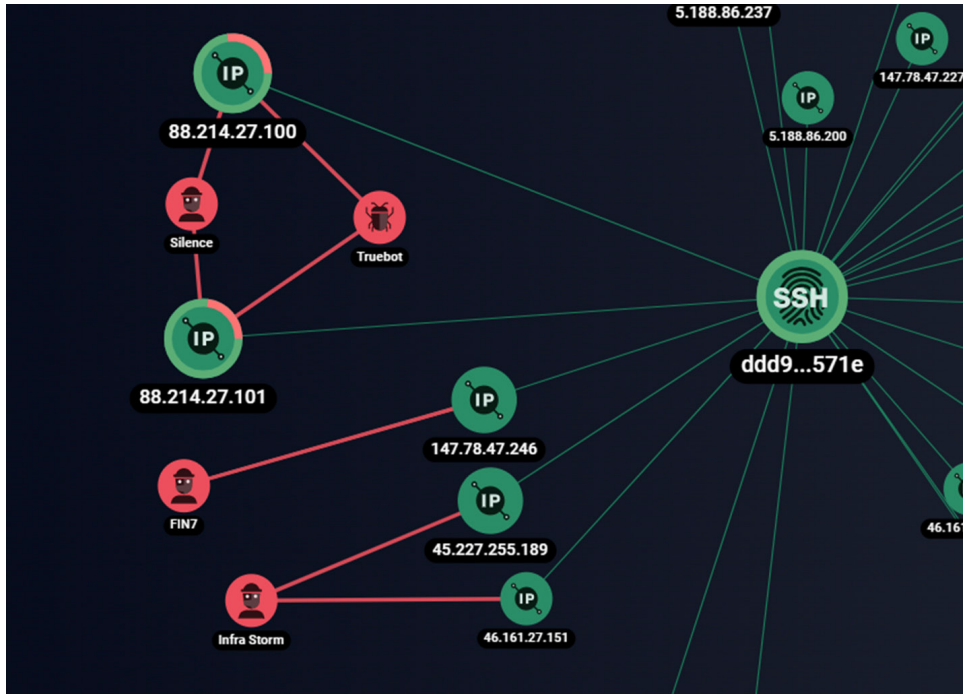
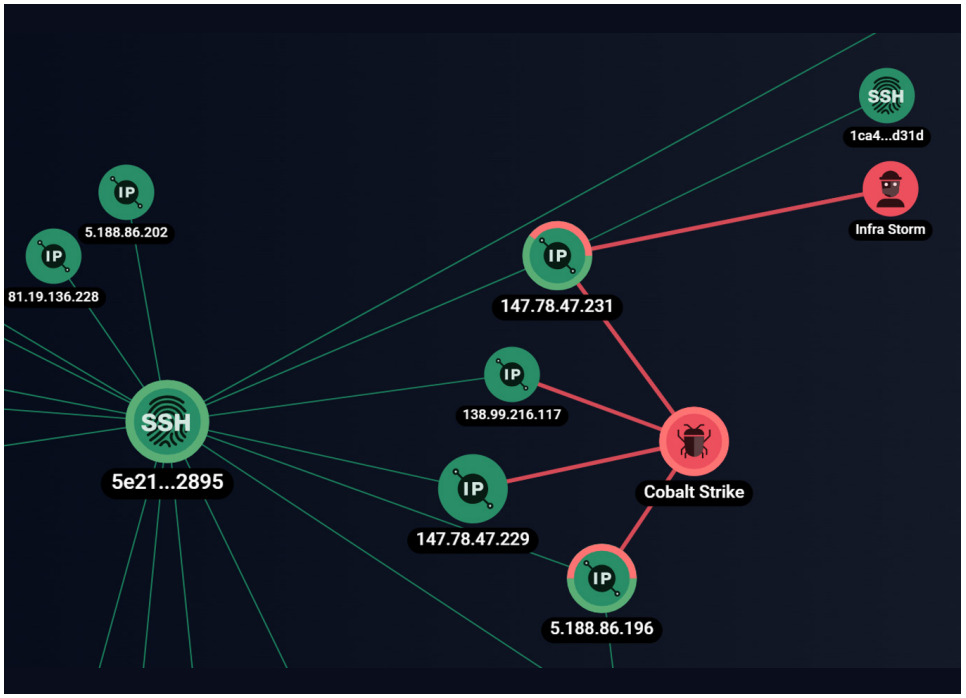


Figure 8. Connection between ShadowSyndicate (Infra Storm) and SSH 5e21f8e88b007935710b2afc174f289

SSH hash: 5e21f8e88b007935710b2afc174f289



Data Attributed With a Low Degree of Confidence

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

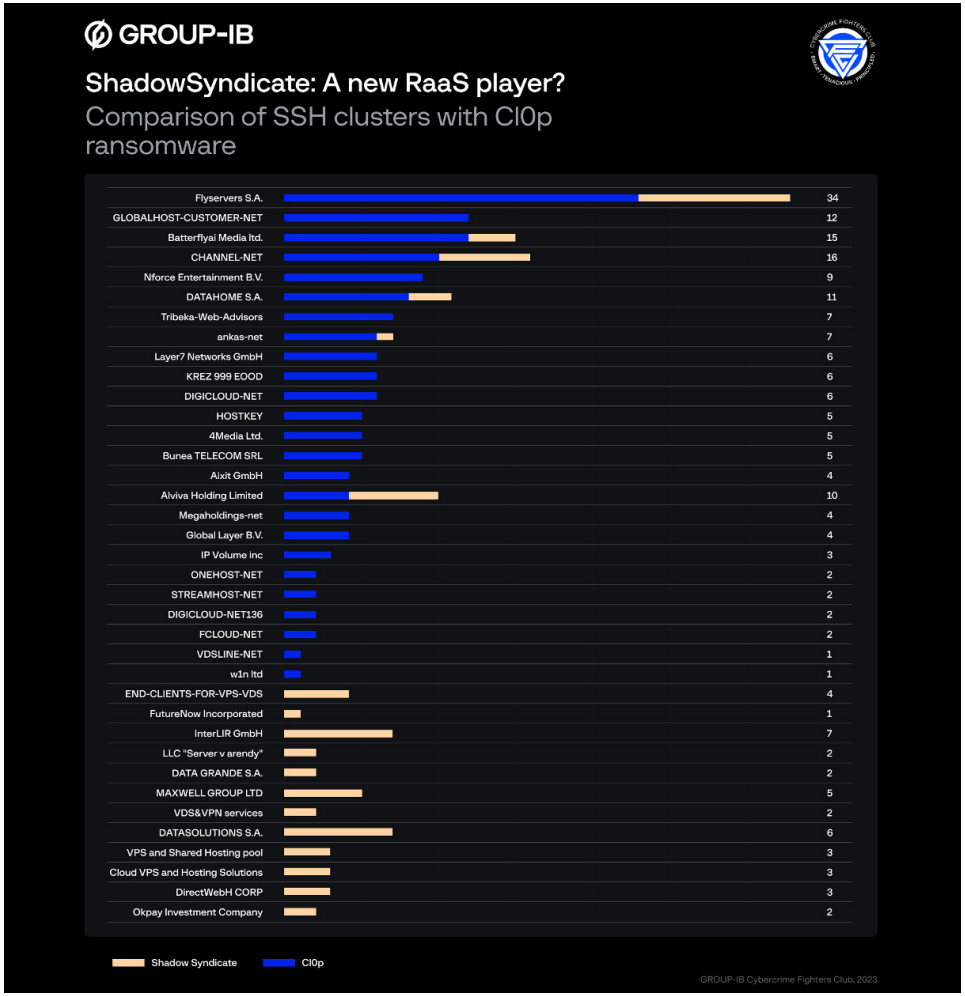


Figure 9 shows that while there is some limited crossover between the infrastructure used by both the two threat actors, the majority of the hosting providers leveraged by ShadowSyndicate have not been used by Cl0p previously.

Conclusions

Based on our research, the most plausible assumption we can make about ShadowSyndicate is that they're an affiliate working with various RaaS groups. However, we have not reached a final verdict, and this may change as we uncover further information in the coming months. As we continue to work with Group-IB and Michael Koczwara, we hope to conduct more research and uncover this threat actor's identity.

To stay up to date with any future developments, as well as see our future CTI reports, follow us on X and LinkedIn.

- https://twitter.com/bridewellsec
- https://www.linkedin.com/company/bridewellsec/mycompany/

Indicators of Compromise

IP addresses

109.172.45[.]28
109.172.45[.]77
141.98.82[.]201
146.70.116[.]20
147.78.47[.]219
147.78.47[.]231
147.78.47[.]235
147.78.47[.]241
158.255.2[.]244
158.255.2[.]245
158.255.2[.]252
179.60.146[.]10
179.60.146[.]11
179.60.146[.]25
179.60.146[.]5
179.60.146[.]51
179.60.146[.]52
179.60.146[.]6
179.60.150[.]117
179.60.150[.]121
179.60.150[.]125
179.60.150[.]132
179.60.150[.]139
179.60.150[.]151
193.142.30[.]154
193.142.30[.]17
193.142.30[.]205
193.142.30[.]215
193.29.13[.]148
193.29.13[.]202
194.135.24[.]241
194.135.24[.]244
194.135.24[.]246
194.135.24[.]247
194.135.24[.]248
194.135.24[.]253
194.135.24[.]254
194.165.16[.]53
194.165.16[.]60
194.165.16[.]62
194.165.16[.]63
194.165.16[.]64
194.165.16[.]83
194.165.16[.]90
194.165.16[.]91
194.165.16[.]92
194.165.16[.]99
212.113.106[.]118
212.224.88[.]71
45.182.189[.]105
45.182.189[.]106
45.182.189[.]110
45.227.252[.]247
45.227.252[.]252
45.227.253[.]20
45.227.253[.]29
45.227.253[.]30
45.227.255[.]189
45.227.255[.]214
46.161.27[.]133
46.161.27[.]151
46.161.27[.]160
46.161.40[.]164
5.188.86[.]206
5.188.86[.]227
5.188.86[.]234
5.188.86[.]235
5.188.86[.]236
5.188.87[.]47
5.8.18[.]117
5.8.18[.]242
5.8.18[.]245
78.128.112[.]139
78.128.112[.]207
79.137.202[.]45
81.19.135[.]249
81.19.136[.]239
81.19.136[.]241
81.19.136[.]249
81.19.136[.]250
81.19.136[.]251
88.214.26[.]38
91.238.181[.]240
91.238.181[.]247
81.19.135[.]229
193.142.30[.]211
45.227.252[.]229
193.142.30[.]37
78.128.112[.]220
5.188.87[.]54
5.188.87[.]41

Indicators of Compromise

Domain names

aerosunelectric[.]com
asaper[.]xyz
asapor[.]xyz
asaporeg[.]xyz
aserpo[.]xyz
assapaa[.]xyz
avdev[.]net
cache01.micnosoftupdate[.]com
cmdatabase[.]com
d4ng3r.s01kaspersky[.]com
devcloudpro[.]com
devsetgroup[.]com
dsvchost[.]com
eastzonentp[.]com
esoftwareupdates[.]com
expotechsupport[.]com
herbswallow[.]com
ipulsecloud[.]com
maximumservers[.]net
msupd.wimdowupdate[.]com
mysqlserver[.]org
opentechcorp[.]net
paloaltocloud[.]online
powersupportplan[.]com
qw.sortx2[.]com
qw.sveexec[.]com
qw.vm3dservice[.]com
settingdata[.]com
situotech[.]com
upd232.windowservicecentar[.]com
uranustechsolution[.]com
webtoolsmedia[.]com
windosupdate[.]net
etgtgvtgttefeer[.]xyz
egetrgertgegege[.]xyz
egetrgertgeb[.]xyz
egetrgertgebrtgf[.]xyz
egetrgertgegegevgvyub[.]xyz
svchostsreg[.]com

Bridewell

+44 (0)3303 110 940

hello@bridewell.com

bridewell.com

GROUP-IB

+65 3159-3798

info@group-ib.com

group-ib.com