Seychelles, Seychelles, on the C(2) Shore

team-cymru.com/post/seychelles-seychelles-on-the-c-2-shore

S2 Research Team September 30, 2022

An overview of a bulletproof hosting provider named ELITETEAM.

Introduction: What is “Bulletproof Hosting” (BPH)?

Bulletproof hosting (BPH) is a type of service offered by hosting providers that allows operators unrestricted and unregulated use of their paid infrastructure. Usually, these providers ignore abuse complaints, giving threat actors an ideal platform to conduct various malicious activities.

BPH providers prefer to operate in jurisdictions that have lenient laws against such conduct. Due to the different laws in different countries, this creates a significant gray area that allows BPH providers to claim immunity to what their customers (threat actors) host.

In addition to malicious activities, some of the other services enabled / hosted by BPH providers include online gambling, the sharing of copyrighted materials, misinformation, etc.

A number of online monikers are associated with individuals involved in the provision of BPH services, and include; Yalishanda, BraZZZerS, MoreneHost, and Vicetemple.

Executive Summary

- ELITETEAM, a bulletproof hosting provider registered in the Republic of Seychelles, is associated with multiple malicious campaigns.
- Multiple distinct clusters of threat activity were noted, operating from IP addresses within a netblock associated with ELITETEAM.
- Each threat cluster had seemingly different “goals”, from directly stealing banking information to deploying ransomware and crypto miners. With a diverse range of targets, and notable differences in attacker TTPs.
- Evidence was identified, based on AS announcements, linking ELITETEAM to another known Russian bulletproof hosting provider.

ELITETEAM Netblock Summary

ELITETEAM owns four different ASNs as “1337TEAM LIMITED”: **AS39770**, **AS60424**, **AS56873**, and **AS51381,** but mainly operates from **AS51381**, which is associated with netblock **185.215.113.0/24.**

Looking at the WHOIS data related to this netblock, an address in Seychelles is provided:

```
organisation:   ORG-LA1589-RIPE
org-name:       1337TEAM LIMITED
country:        SC
org-type:       LIR
address:        Global Gateway 8, Rue de la Perle office "1337TEAM LIMITED"
address:        0000
address:        Providence
address:        SEYCHELLES
phone:          +248
language:       EN
remarks:        CERTs, LEAs and Gov Agents - please use email: legal (dog) eliteteam.to
remarks:        For non-automatic abuses - please use email: abuse-request (dog) eliteteam.to
remarks:        We have very strict NO SPAM tolerance policy and carefully review any abuse,
exclude spammers emails
remarks:        Spammers: ban-me-please@eliteteam.to <-- send email here if you want permanent
banning on our mail server
```

Figure 1: ELITETEAM WHOIS Data

The address “Global Gateway 8, Rue de la Perle office “1337TEAM LIMITED”, Seychelles” was previously disclosed in documents commonly referred to as the Panama Papers and Offshore Leaks, indicating that ELITETEAM may use Seychelles as a front for their operations, whilst controlling them from another location.

Infrastructure Summary

The identified malicious infrastructure, hosted via ELITETEAM and discussed in this blog post, is divided into three different clusters, as follows:

- Cluster 1: Malvertising and info-stealing
- Cluster 2: Phishing
- Cluster 3: Skimming

Cluster 1

The first cluster, and currently the most active one, was previously observed (since December 2020), targeting victims through exploitation of the Log4Shell (CVE-2021-44228) vulnerability. However, since around February 2022, we have observed a switch to the use of

malvertising campaigns, using ‘fake’ software as a lure, leading to the installation of the Amadey malware on victim machines.

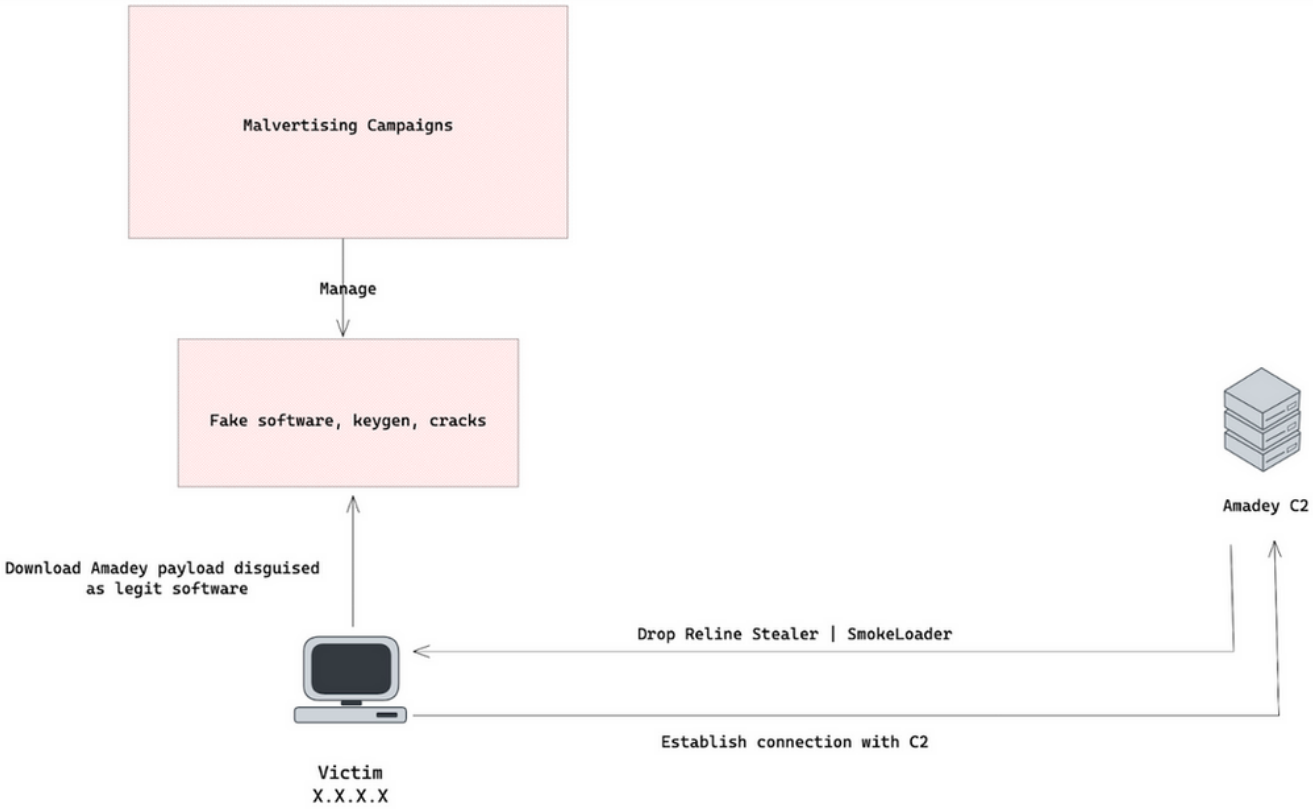

Figure 2: Malvertising Campaign

Following the initial installation of Amadey, depending on the version number of the malware, (3.08 through to 3.21 was observed in this cluster) one of two payloads are then dropped; Redline stealer, or Smokeloader. It appears the initial goal of the threat actors is the theft of victim information / credentials, however further payloads were also observed being dropped, including Djvu ransomware and crypto miners.

During this investigation, we focused our research on five Amadey C2 servers:

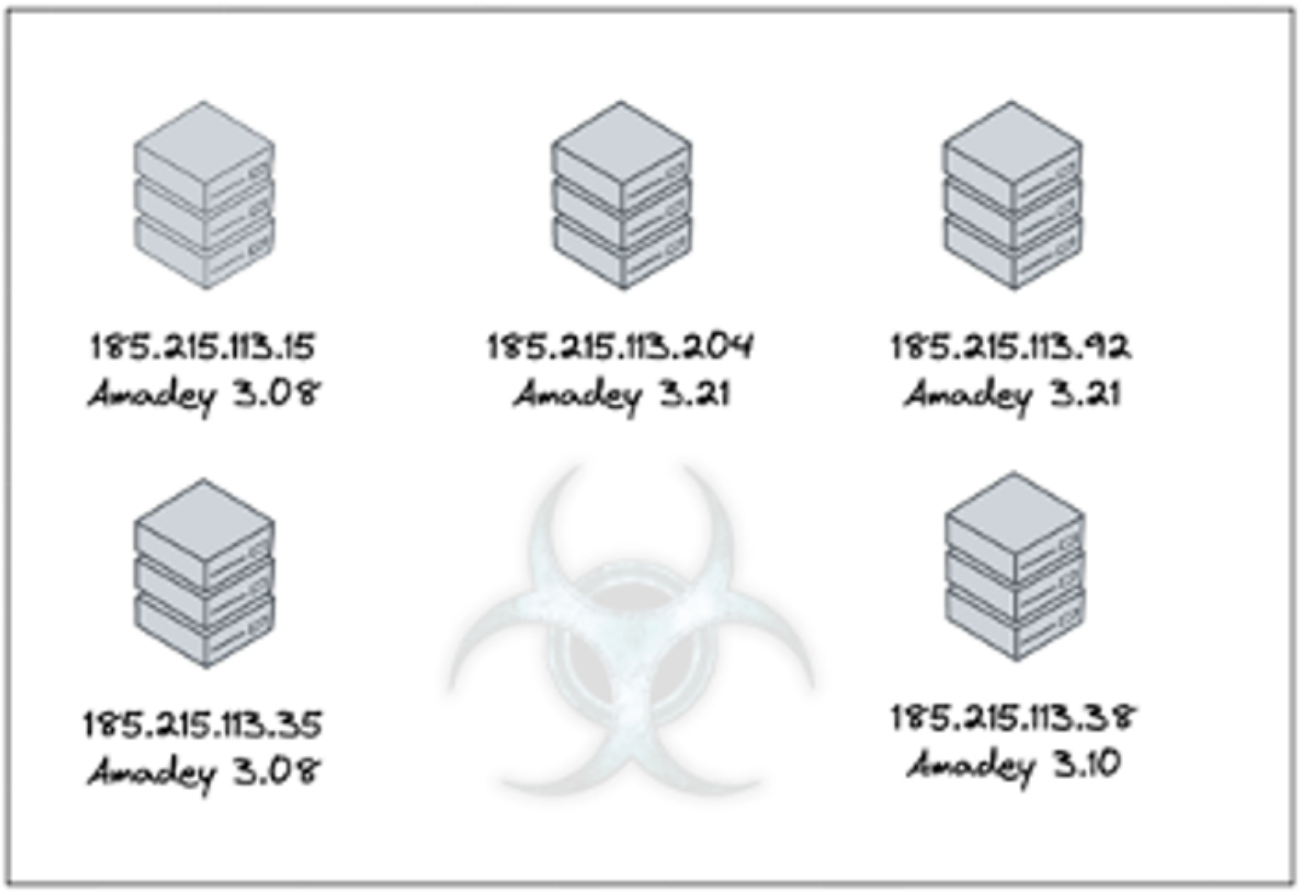

Figure 3: Amadey C2 Servers

Note: For reasons unknown, this cluster hosts multiple different versions of Amadey, all of which are currently in use in attacks.

Pivoting on URL strings associated with the Amadey C2 servers (Figure 2), we were able to identify a list of tasks hosted on **185.215.113.92** (Amadey version 3.21).

Юниты/Билды:	Адрес:	Тип:	Архитектура:	Сохранить в:	Лимит:	Получено:	Успешно:	Ошибки загрузки:	Ошибки запуска:	Прогресс:	Успех:
*	https://bitbucket.org/usasoftwar...	EXE файл (диск)	Все	%Tmp%	10000	1184	716	24	27	11.8%	7.2%
*	https://bitbucket.org/usasoftwar...	EXE файл (диск)	Все	%Tmp%	10000	1184	698	60	18	11.8%	7%

Figure 4: Tasks Hosted on 185.215.113.92

The payloads associated with these tasks appeared to be hosted on a Bitbucket account named ‘USASoftwareDevelopment’.

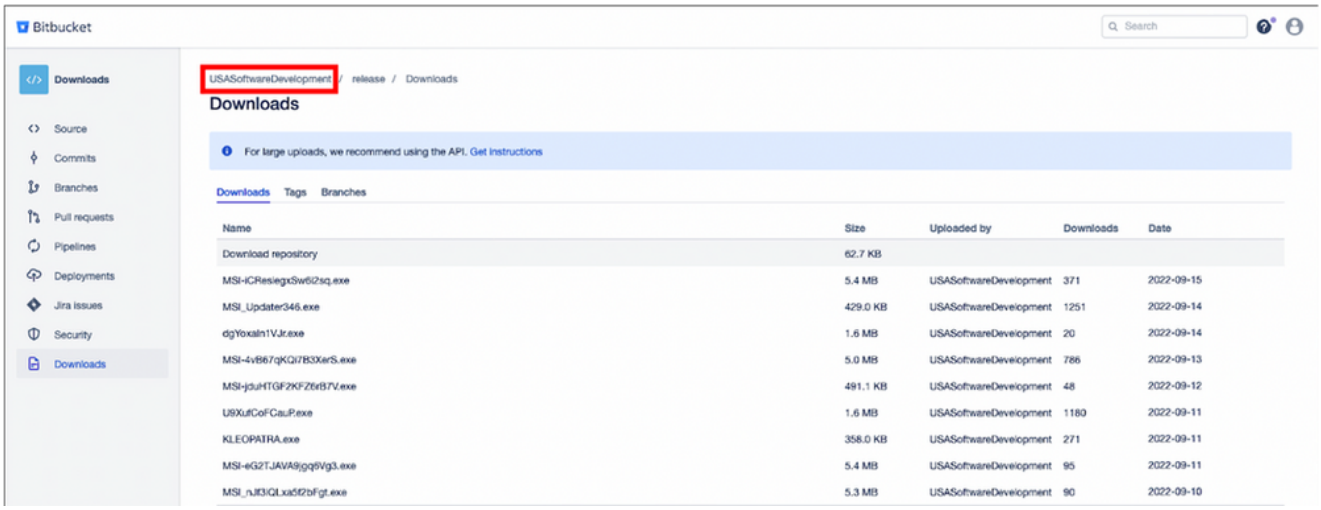

Figure 5: USASoftwareDevelopment Bitbucket Account

Analysis of these payloads identify them as Redline stealer executables (botnet: IMHOTEP), which are likely loaded onto victim systems to facilitate data theft and systems reconnaissance. Data from victim systems is then exfiltrated to **185.215.113.217**.

Note: The number of downloads recorded against each payload provides a further indication to the scale of this activity.

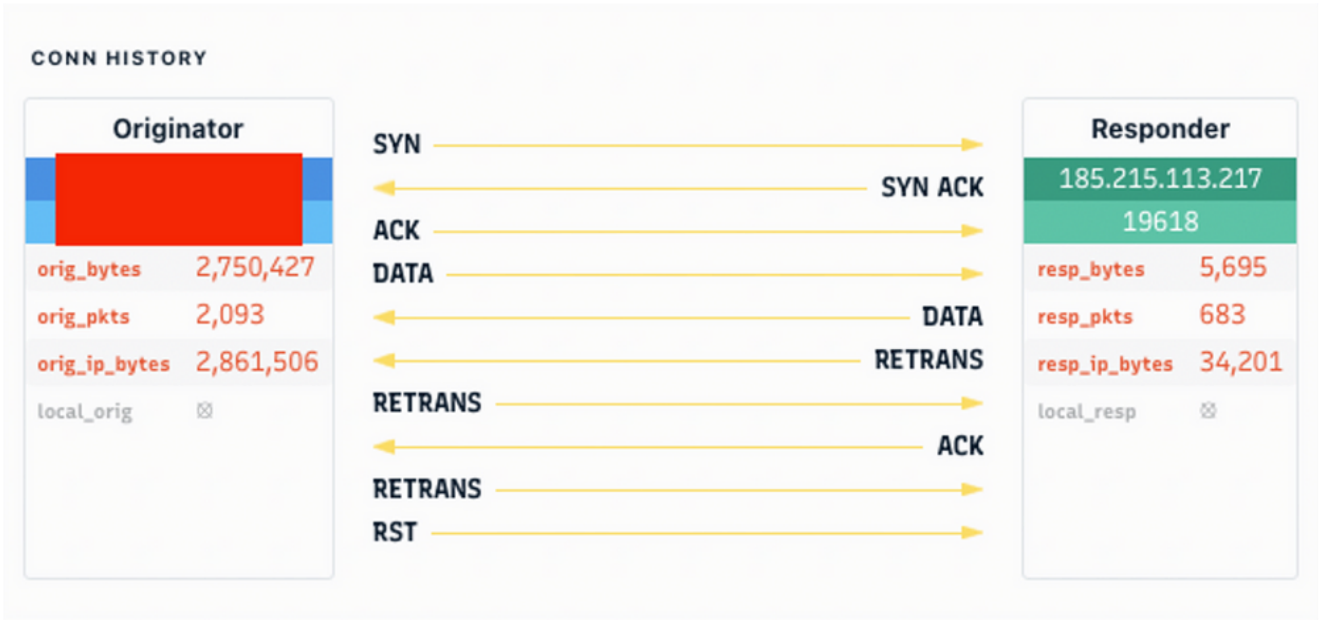

Figure 6: Data Exfiltration to 185.215.113.217

Similar findings were also observed for **185.215.113.205**, which was not initially identified as an Amadey C2 server.

For unit:	Url:	PE type:	Arc:	Folder:	Limit:	Received:	Launched:	Download errors:	Launch errors:	Progress:	Success:
•	https://bitbucket.org/alex222111...	EXE (m)	All	memory	1000000	1994	1473	0	138	0.2%	0.1%
•	https://bitbucket.org/alex222111...	EXE (m)	All	memory	1000000	2007	1705	0	85	0.2%	0.2%

Figure 7: Tasks Hosted on 185.215.113.205

In this case, the payloads were hosted on a different Bitbucket account ('Alex'), but again all of the samples analyzed were identified as Redline stealer. Of note, data exfiltration for these payloads was to **65.21.133.231** (assigned to AS24940 - Hetzner Online GmbH).

Figure 8: Data Exfiltration to 65.21.133.231

Examining threat telemetry for **65.21.133.231**:47430, it is apparent that this particular campaign became active on 20 August 2022, and to date has seen at least 500 victims. The observed victims were dispersed globally, with the highest concentrations in Brazil, India, and South Africa, based on IP geo-location data.

Finally, a third Bitbucket account (named 'mrssoprano666') was identified, again associated with **185.215.113.92**.

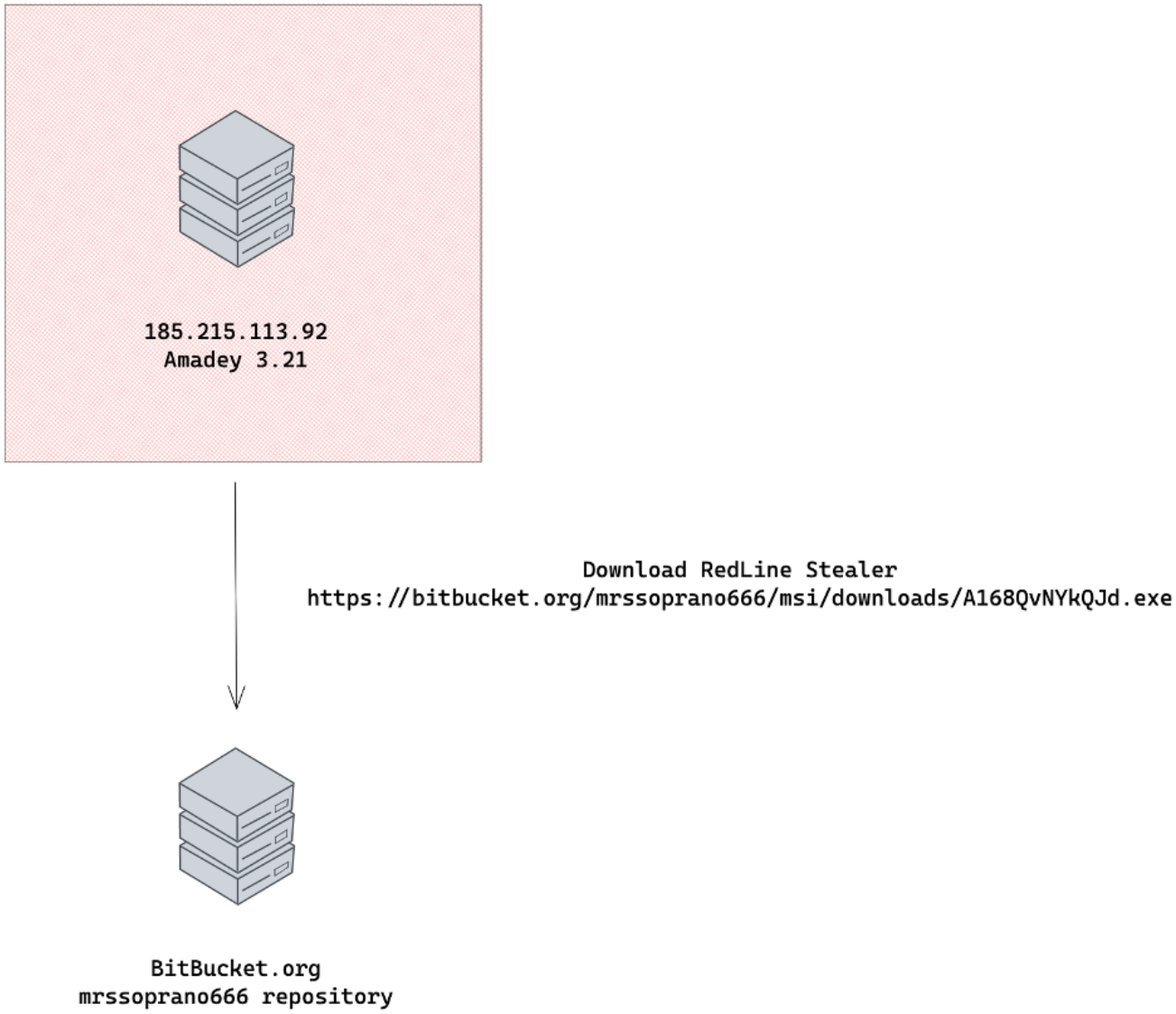

Figure 9: ‘mrssoprano666’ Bitbucket Account

In this case, we pay witness to a potential “career” change. We identified a user called ‘mrssoprano666’ on an underground Russian-language forum, offering ‘physical’ services associated with fraudulent activity. These services included answering telephone calls, making calls to victims (posing as a bank or shop), and the rerouting of parcels.

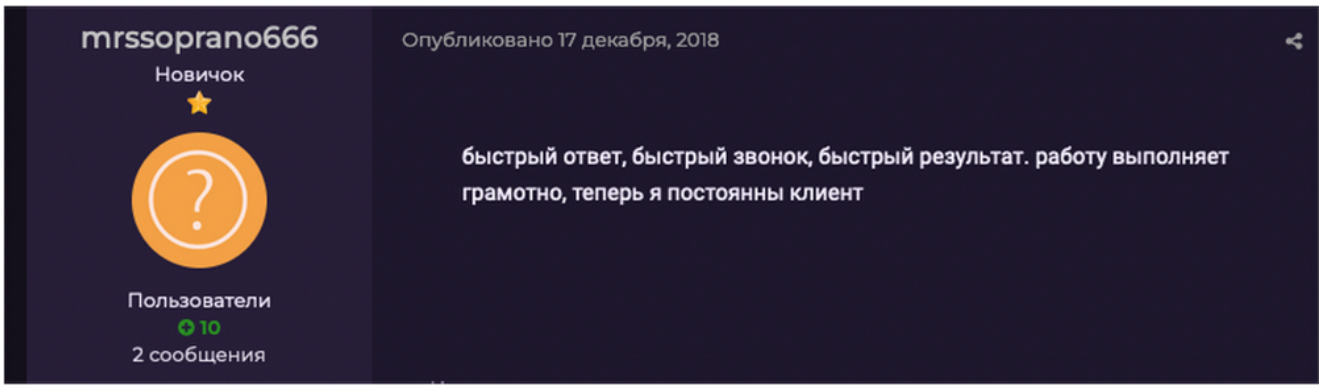

Figure 10: Forum Post by ‘mrssoprano666’

Based on the timeline of activity on this forum, it appears that the user ‘mrssoprano666’ disappeared in 2020 (having advertised their services since 2018) before subsequently re-appearing as a cybercrime affiliate this year.

Cluster 2

The second cluster is mainly used to conduct phishing campaigns, with a particular focus on the spoofing of investment and cryptocurrency platforms. This cluster is highly active, particularly considering AS51381 only accounts for 256 IP addresses, ranking 8th place in Interisle’s Phishing Landscape 2021 behind much larger ASs.

Rank	AS Name	AS number	# Routed IPv4 Addresses	Phishing attacks	Phishing Attack Score ▼
1	AWEX - Hostinger International Limited	204915	768	13,186	**171,692.7**
2	WEEBLY	27647	2,112	10,701	**50,667.6**
3	PIHL-AS - Private Internet Hosting LTD	213058	704	1,714	**24,346.6**
4	IDNIC-JALANET-AS-ID PT. Jupiter Jala Arta	131775	2,304	3,446	**14,956.6**
5	WIX_COM - Wix.com Ltd.	58182	1,024	1,219	**11,904.3**
6	BEON-AS-ID PT. Beon Intermedia	55688	2,560	2,589	**10,113.3**
7	NAMECHEAP-NET	22612	62,208	55,903	**8,986.5**
8	ELITETEAM-PEERING-AZ1 - 1337TEAM LIMITED	51381	256	208	**8,125.0**

Figure 11: Phishing Landscape 2021 Rankings

Three IPs are used to host phishing sites:

- **185.215.113.100**
- Observed most recently in a campaign targeting Polish Credit-Agricole users.
- **185.215.113.201**
- Used as a Redline Stealer C2 until April 2022

- Switched to phishing purposes in June 2022
- **185.215.113.206**

As noted previously, there is a financial flavor to this cluster, in one campaign we observed the targeting of Fidelity customers, in an attempt to steal credentials.

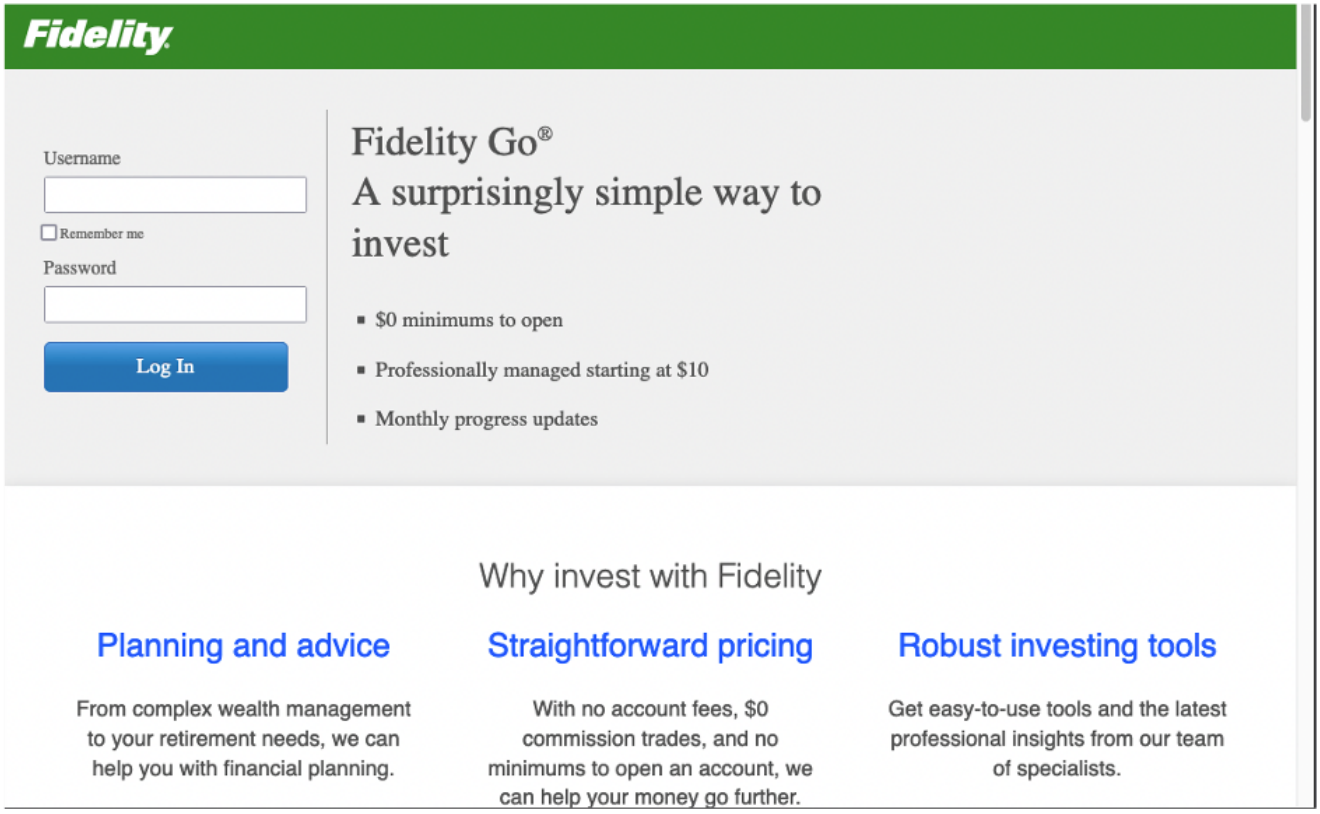

Figure 12: Phishing Page Targeting Fidelity

Interestingly, there was also a second stage to this attack; usually attackers are simply seeking credentials, but in this case it appears the attackers wanted to double up on the opportunity. Once a user had entered their credentials, they were directed to download a file called ‘Fidelity Protect Services’. This is a completely fictitious product offering from Fidelity, but continues to be a highly convincing part of the scam.

Figure 13: Fidelity Protect Services

The file (hosted at cv19alert[.]com/fidelityprotect.exe) was not available for download at the time of our investigation. However, a copy was uploaded to Virustotal on 28 June 2022 by a user in the United States (MD5: 4532b0d0ca6330bf73e0d6f76f8cf35b).

Analysis of the sample identifies it as a Raccoon Stealer V2 payload, with the timeline aligning with the malware first being spotted in the wild (and initially referred to as RecordBreaker based on User Agent strings).

In the first stage, the malware pushes the ‘machineId’ and username to the C2 server, along with the ‘configId’ (RC4 key).

```
POST / HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=utf-8
User-Agent: record
Host: 104.193.255.48
Content-Length: 94
Connection: Keep-Alive
Cache-Control: no-cache
machineId=90059c37-1320-41a4-b58d-2b75a9850d2f|admin&configId=356547cff73a46df
87e3a788a4dad168
```

Figure 14: Initial POST Request

The RC4 key is used to decrypt the location of the C2 server, in this case 104.193.255.48 (AS14576 - HOSTING SOLUTIONS).

```
→ python3 script.py 2008-70-0x0000000000400000-0x0000000000412000-memory.dmp
[+] found possible encrypted c2 b'Vt1vhIj/lgMHRvWdG1dfmD3zJrLUng==' at 0xd460
[+] found possible rc4 key b'356547cff73a46df87e3a788a4dad168' at 0xd43c
[>] decrypted c2: b'http://104.193.255.48/'
```

Figure 15: Decrypted C2 Server

Unfortunately the C2 was offline at the time of our investigation, so we were not able to retrieve the full configuration of the malware.

Cluster 3

The third cluster is connected to credit and debit card skimming activity, with the earliest observations occurring in November 2021.

A campaign associated with this cluster was previously reported on by the Sucuri research team, which noted:

- Compromise of the victim website, with an attempt to load a malicious JavaScript file.
- Website visitors met with an unwarranted prompt for credit card information.
- Spoofing of the legitimate domain ‘api.jquery.com’; the attackers used a similar domain ‘apiujquery[.]com’.

- C2 server used to serve the secondary payload, allowing for JavaScript injections into pages when certain keywords were triggered, e.g., ‘checkout’, ‘my-account’, ‘order’.
- C2 server located at **51.178.8.230** (AS16276 - OVH).

At some stage after the publication of this blog, the C2 server was moved to **185.215.113.5**.

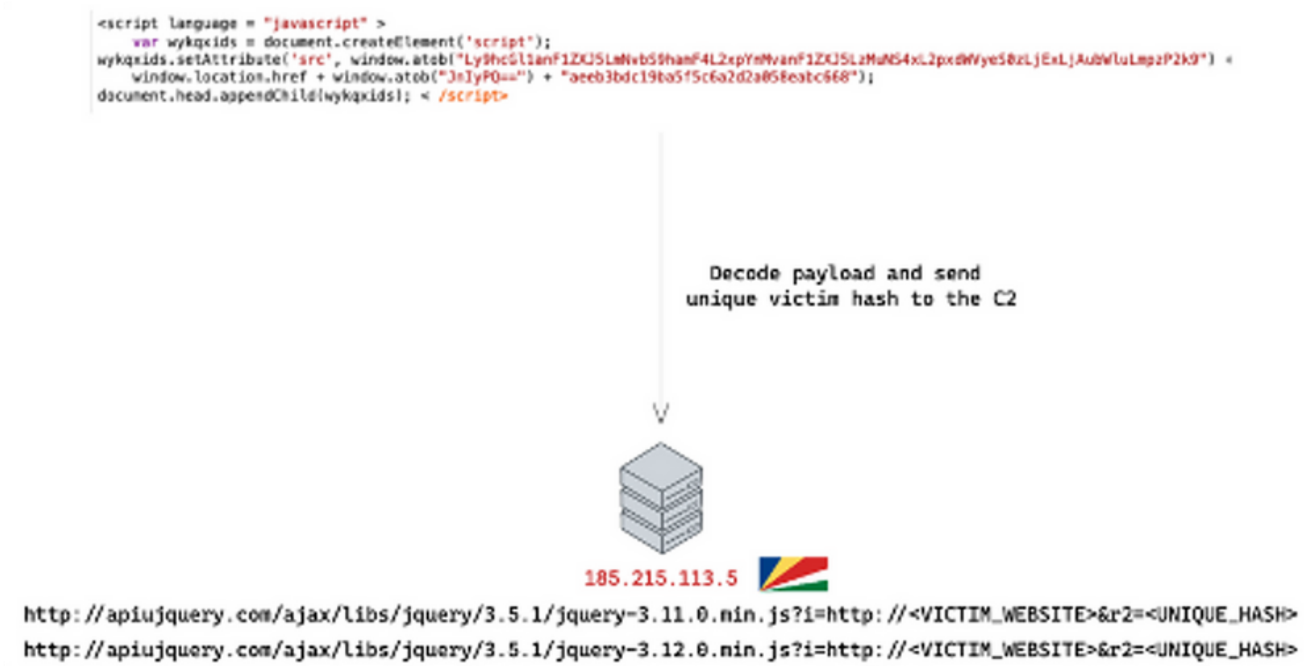

Figure 16: Current Campaign C2 Details

Based on our threat telemetry for **185.215.113.5**, we have observed at least 50 unique victims connecting to the C2 server over the past three months.

Reviewing the current campaign, it appears very similar to the one reported on nearly a year ago. The first JavaScript injection payload sends a unique hash to the C2 to register and identify the victim on the admin side.

However, some updates to the second stage payload have been noted. Firstly, the ‘triggered words’ list has been updated to include several more keywords.

Figure 17: Triggered Words List

Secondly, an additional C2 server was identified, hosted on **185.215.113.20**. Both the initial and the 'new' C2 server share the same SSH Server Host Key value.

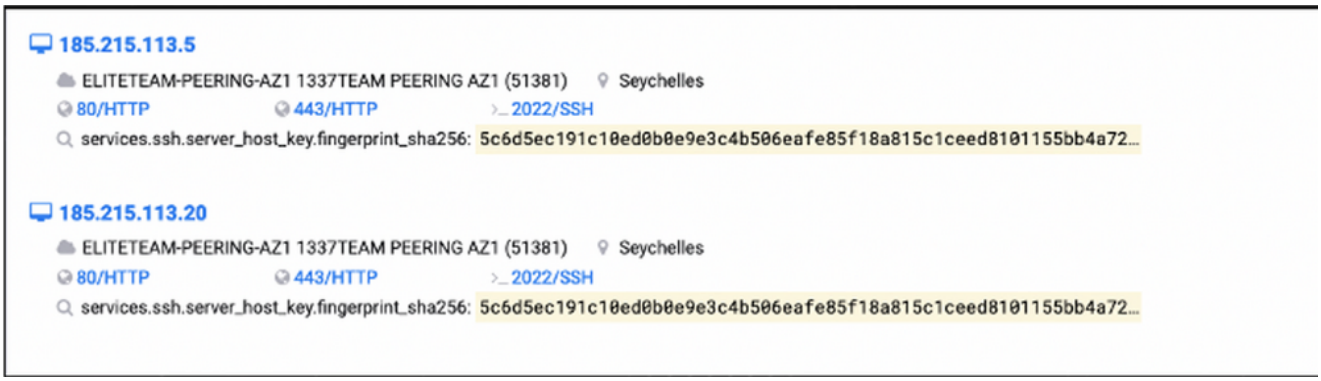

Figure 18: SSH Server Host Key Match

The current IOCs for this campaign are therefore as follows:

- apiujquery[.]com | **185.215.113.5**
- C2: http://apiujquery[.]com/ajax/libs/jquery/3.5.1/jquery-3.12.0.min.js?i
- apigstatic[.]com | **185.215.113.20**
- C2: https://apigstatic[.]com/ajax/libs/jquery/5.1.7/jquery-7.41.3.min.js?i

Big Picture

Big Picture - Summary of Infrastructure

Zooming out from the clusters already discussed, a significant number of IPs within the **185.215.113.0/24** netblock have been linked to malicious activity in the recent past. With 110~ IPs categorized as malicious within VirusTotal over the past 90 days, and 80~ IPs associated with entries made to ThreatFox within the past year.

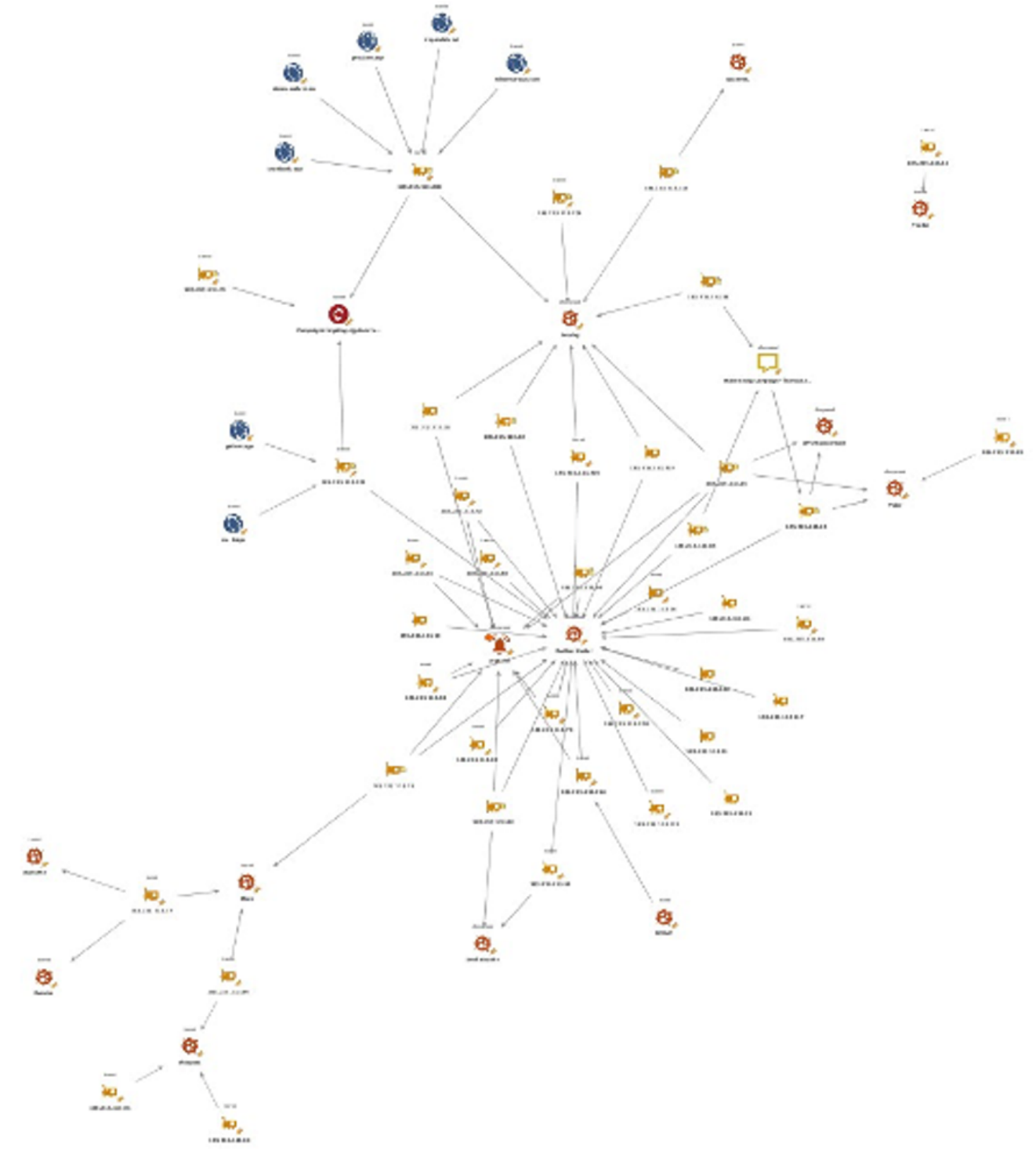

Figure 19: Malicious Activity Cluster within AS51381

Big Picture - AS Details

ELITETEAM have been highlighted in the past by other researchers, identifying them as malicious / BPH providers. To quote Spamhaus in their botnet report from 2021 “[ELITETEAM] is a bulletproof hosting company purporting to be located in Seychelles. In reality, they more than likely operate out of Russia.”

In late 2020, when the ASs were first allocated to ELITETEAM, they were initially declared as Russian before being updated to reflect their status as Seychellois, as is the case today.

Timestamp	ASN Description
2018-04-13T15:15:40+00:00	CTEZTI-AS National University Lviv Politechnika, PL
2020-09-02T07:14:59+00:00	-Reserved AS-, ZZ
2020-11-13T02:15:02+00:00	AS-, ZZ
2020-11-13T14:15:02+00:00	,
2020-11-14T15:15:01+00:00	ELITETEAM, RU
2020-11-20T14:15:05+00:00	ELITETEAM, SC
2020-11-26T14:15:05+00:00	ELITETEAM-AZ1, SC
2020-11-27T14:15:04+00:00	ELITETEAM-PEERING-AZ1, SC
2021-06-26T21:15:09+00:00	ELITETEAMPEERINGAZ1, SC
2021-06-27T00:15:10+00:00	ELITETEAM-PEERING-AZ1, SC
2022-03-07T14:15:26+00:00	ELITETEAM-PEERING-AZ1 1337TEAM PEERING AZ1, SC

Timestamp	ASN Description
2018-04-13T15:15:40+00:00	PROLOGICS-AS, RU
2020-09-02T07:14:59+00:00	-Reserved AS-, ZZ
2020-11-16T02:15:06+00:00	AS-, ZZ
2020-11-16T14:15:02+00:00	,
2020-11-17T14:15:00+00:00	ELITETEAM, RU
2020-11-19T14:15:05+00:00	ELITETEAM, SC
2020-11-26T14:15:05+00:00	ELITETEAM-AZ3, SC
2020-11-27T14:15:04+00:00	ELITETEAM-PEERING-AZ3, SC
2021-06-26T21:15:09+00:00	ELITETEAMPEERINGAZ3, SC
2021-06-27T00:15:10+00:00	ELITETEAM-PEERING-AZ3, SC

Figure 20: ASN Description Information for AS51381 and AS60424

Digging deeper into the details surrounding the ASs assigned to ELITETEAM, looking at information such as netblock announcements and peering, we were able to establish further ties to Russia.

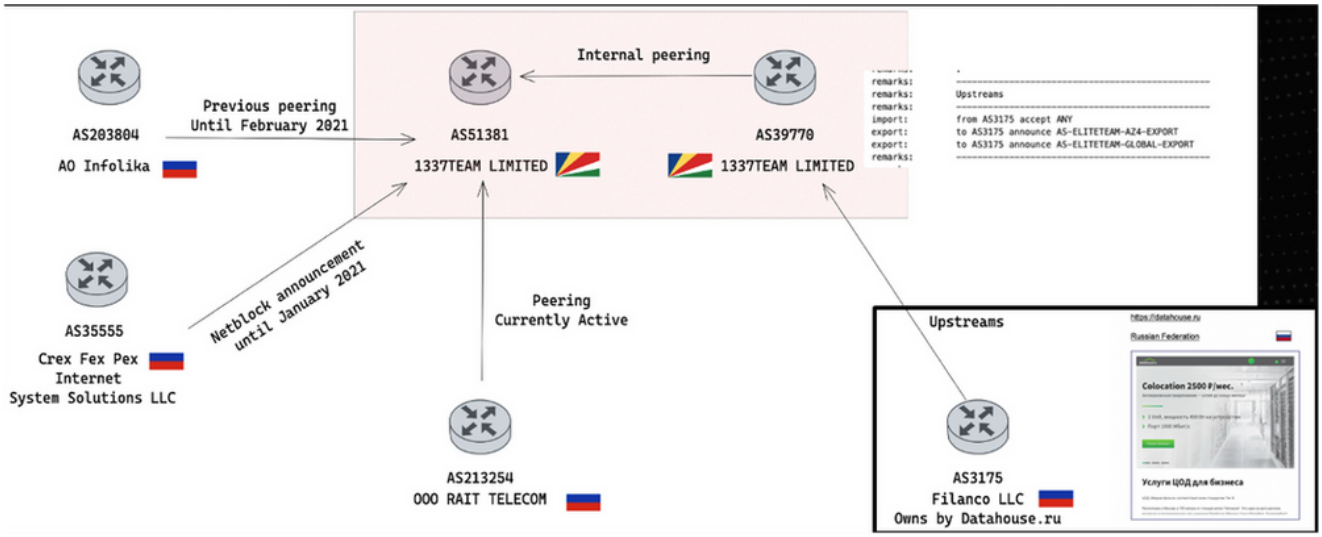

Figure 21: ELITETEAM Peers

Indeed, all ASs connected to the ELITETEAM infrastructure are owned by Russian entities:

- AS3555 | Crex Fex Pex Internet System Solutions LLC | Announcing AS51381 until January 2021

- AS203804 | AS Infolika | Peer until February 2021

Details of the above activity have been disclosed previously by Valery Reiss-Marchive when discussing the Egregor ransomware.

- AS213254 | OOO RAIT TELECOM | Peer until August 2022
- AS49612 | DDOS-GUARD LTD | Current peer as of September 2022
- AS3175 | Filanco LLC | Owned by Datahouse.ru, another Russian BPH provider for which ELITETEAM is an upstream peer

AS213254 (OOO RAIT TELECOM) was seized by US law enforcement (ICE - Homeland Security Investigations) in early September 2022 and is currently no longer visible on the routing table.

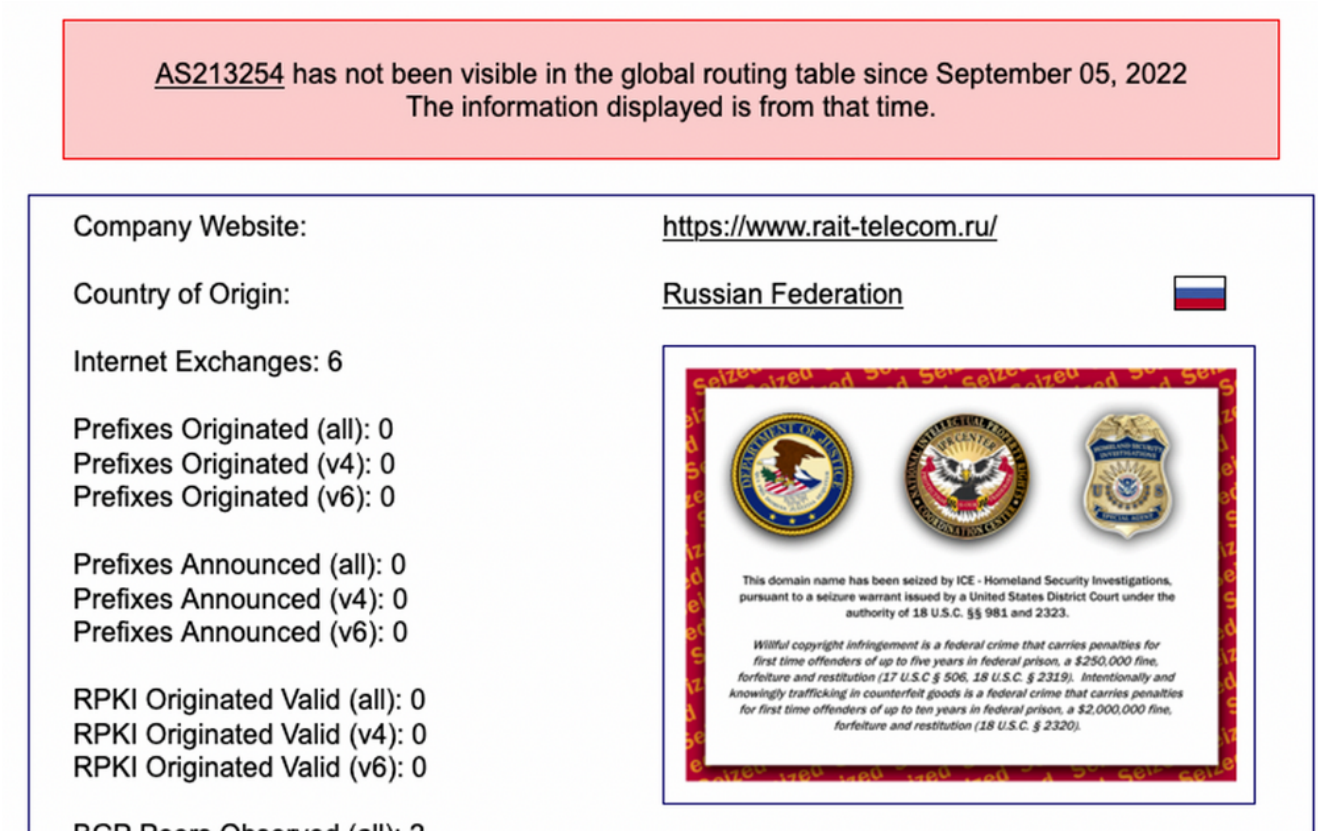

Figure 22: US Law Enforcement Takedown of AS213254

It is possible that at some stage in the chain the operators were aware of the law enforcement action, as there was a migration observed in August 2022, where for a period both AS213254 and AS49612 were observed as peers for AS51381.

Conclusion

As outlined throughout this blog, ELITETEAM enables malicious activity on a significant scale, allowing threat actors to operate with impunity against global targets, who in some cases appear to be individuals with surplus funds with which to invest or experiment with digital currencies, and in others just your average Joe Public. We have observed varying campaigns and TTPs, indicating diverse usage of ELITETEAM's services by threat actors of varying skill sets. It is not often sound advice to say, "block all connections to a /24", but in respect of the infrastructure assigned to ELITETEAM, overwhelming evidence compels us to suggest this to be the case.

All the data and information we have researched points to ELITETEAM being Russian / Russian-speaking, operating behind a shell organization in Seychelles. We have reason to believe that Datahouse, RU is connected to ELITETEAM and worthy of further investigation.

Figure 23: Obi Wan Kenobi Encountering ELITETEAM

IOCs

Netblock:

185.215.113[.]0/24

Amadey C2s on 2022/09/21:

185.215.113[.]15

185.215.113[.]92

185.215.113[.]204

185.215.113[.]35

185.215.113[.]114

185.215.113[.]205

Phishing IPs:

185.215.113[.]100

185.215.113[.]201

185.215.113[.]206

Phishing domains:

agricole-sms[.]org

ermac[.]icu

bonus-agricole[.]pl

releyfi-login.comebien[.]app

releyfi-login.flipflop[.]app

relayfi-login.zenquickcash[.]net

scipost-xmeta[.]org

geekgirlacademy[.]com

icepapers[.]com

hoamelgar[.]com

williamsaraujo[.]com

zspacelab[.]net

cv19alert[.]com

Skimmer IPs:

185.215.113[.]5

185.215.113[.]20

Skimmer domains:

apiujquery[.]com

apigstatic[.]com

File sharing websites used to drop payloads:

uploadgram[.]me

mediafire[.]com

pu-file[.]com

hero-files[.]com

RedLine Stealer payloads:

00580a4220102211f07bb54041d6f49c6995b86948fbfaf98c720e7fdfd4214c

0258c677f58e13433e8aea350caa1f4643ce4fe24be6d28278915176572af3ca

02b0b5d59068e9f00daa7ee2d4c3027e902c32038868f5de00b710ab7c7e9182

016da58a917c5aad423db3c50cc75e351e62926c0e0c8e00a5c1de0ec6fc84af

00649bad6081d82108bbde63efaab243b0d5f5f95dc99f9c46fa5ecd74c584b4

02f1627f1a3e2f8531e2217ed28e420b717355ef15ca42bd9734b356f2bb2285

76f4e8c50ece719c504376db8e131a8afcf8307e21ec864439452ac66f1da7ff

09de0dca1123d58508f85013bfd94c764b9d0ba45bd556b7e5b9f81df471eed8

3b4140faaa3828375888ca2ff1152fdf46529175ee49931ad8a20f52e0cdb058

13f672297f1efe6a3eb73b8d3d7f2fa89117feef14a61054ccbde74a07ae2ef0

4f3d55a6d73b630dfae91b89f98643462862a2b0264867752b802d0c1a8729e4

Amadey payloads:

e49833410fea53f166523cc960fc7d60ddfcf60d0fc2024e68dbabab27ce8313

232a7888f79f09c47258df130cbf4e854c7a5e0af0a534e5d918bbe7b4a9cd5a

53463b214577f4ea17e629a8516b21584ceaef323880a7660b2ec6015a0da617

7bc6a9edc592553dcb9250d70816f511d43a998f95f4e0b2a347dc2b66f897c4

b9fa703b80c7d124148f64ae3474f1f2b01a42cd1ed6871be2bb6c9d15ecf871

134ed27da9f9e727a3e6b4c551655d93f4e18969836ae94f0d59ddae09bbd0d1

f6740bc4e0f17e6642dcb7343e768b0ff357c4b62508de0db21553014c3fb231

Detection mechanisms

IDS Rules:

- MALWARE-CNC Win.Trojan.Redline variant outbound request detected
- ET DROP Spamhaus DROP Listed Traffic Inbound group 22
- ET DROP Spamhaus DROP Listed Traffic Inbound group 21
- ET MALWARE Amadey CnC Check-In
- ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download
- MALWARE-CNC Win.Trojan.Amadey botnet outbound connection

Other Considerations:

Monitor external assets and endpoints for connections to the netblock assigned to ELITETEAM, in addition to the phishing and C2 IPs provided above.