Bulletproof Hosting Hunt

By Vasilis Orlof

Published: 2025-04-04 · Archived: 2026-04-05 17:45:23 UTC

It all started with a simple follow up on another Lumma infection. I wanted to find and automate a quick way to get hunting leads for infra that is not hidden behind CDNs but I think I might have found a Bulletproof hosting provider.

Lumma continues to be in the top 5 malware families [1] [2] , which means high sample availability on malware reporting platforms and a great starting point for a hunt! Starting from the latest Lumma samples, we can expand to additional malicious infrastructure, including phishing, impersonation mininng and various malware.

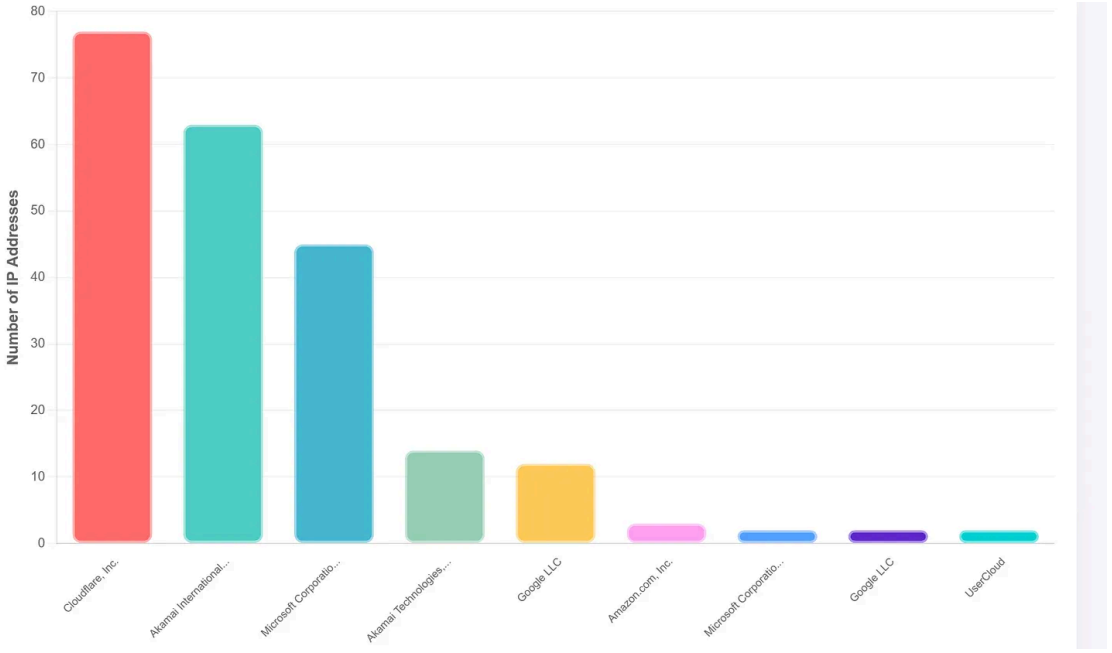
Using abuse.ch API to retrieve samples from the last week (of this writing), returns 100 results between 15-22/7. With the latest hashes in hand we can start our analysis.

```
Summary:
- Date range: 2025-07-15 to 2025-07-22
- Total Lumma Stealer samples: 100
- Samples from last 7 days: 100
- Hashes saved to file: hashes.txt

Daily breakdown:
  2025-07-22: 8 samples
  2025-07-21: 24 samples
  2025-07-20: 33 samples
  2025-07-19: 21 samples
  2025-07-18: 13 samples
  2025-07-17: 1 samples

First 10 hashes from the last 7 days:
 1. 71cc7cf1ed7faf62ad3dfbdde26a2a257044b50fa2446347490fad24403f0f7f
 2. 628035c14718c064036edf3cd0fe349007bc37d22cca740f4880e2cde3a78bc7
 3. 903b077014c4652752cff3db65e05572096fbb16386b4c7ac10c5d951bf4bbf0
 4. ad8d2d36547bb6c3fd44a137948dae585b9c66f7f3e6c36adcb0fd1f6a130a37
 5. bccf2951c42b748568df470bdd739f93fb1a0c95540806cd042dc18a92572007
 6. 2144207c1a122498f32c574d7f7be0238a2a5424188443bd5e980ed7097b6176
 7. 1687172d191ac95ddddbd7174f1ff6faf5a750dd03927c503ba7c2940eaf4706
 8. c95f4d81c8a30ed33e4f4651f526437c2a90aa11409eaa9ccf8b367f63db8e4e
 9. bb308a71fd2b233c79cd03fa937335bd69d22283c0925c998bed53e28e547425
10. 3af5ee1e1472fe3b73fb2f207c5250e4f6941caa6ab1969768ed641abfd64f2d
... and 90 more in the file
```

First, let's grab any communicating IPs. Using VT API we can see that the malicious files are communicating with 292 IPs. Now that we have our IPs, we'll group them and try to filter out dead end pivots. What I mean by that is, since most of the domains associated with Lumma are usually hidden behind CDN like Cloudflare, Akamai etc, we'll filter those out as it's nearly impossible to pivot.



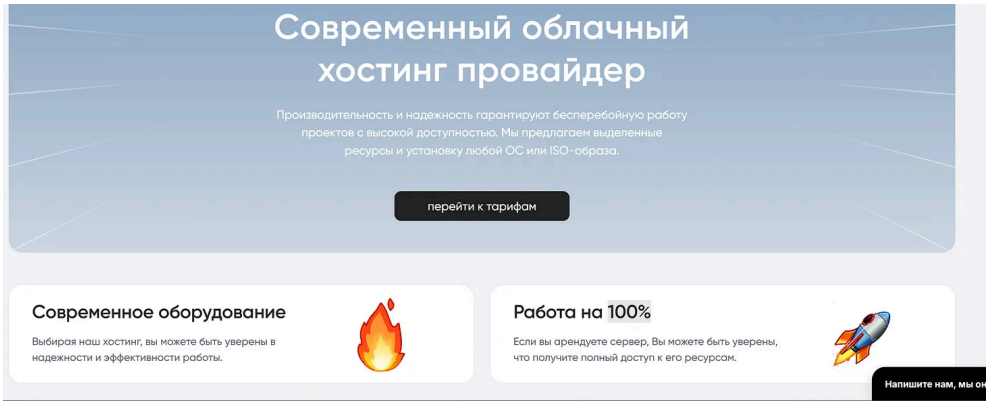
After filtering the IPs and ASN, we are left with 10 unique IPs spread across 10 unique ASN so there is no immediate pattern in the grouping.

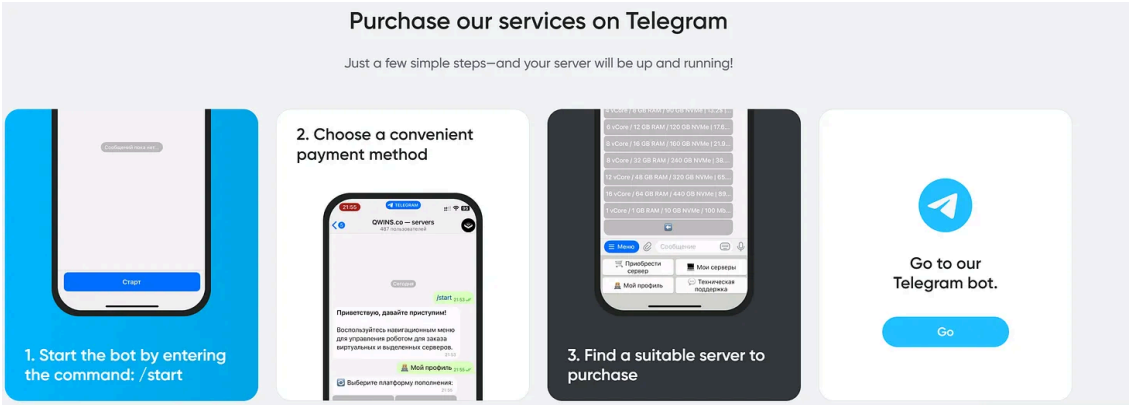
```
 141.98.6.34 - AS213702, Qwins LTD
185.215.113.51 - AS51381, (ELITETEAM-PEERING-AZ1 1337TEAM PEERING AZ1)
144.172.115.212 - AS14956, ROUTERHOSTING
167.160.161.12 - AS214943, Railnet LLC
```

```
104.251.123.89 - AS14315, 1GSERVERS, LLC
146.70.100.103 - AS9009, M247 Europe SRL
176.46.152.39 - AS214351, FEMO IT SOLUTIONS LIMITED
198.54.117.242 - AS22612, Namecheap, Inc.
45.134.26.137 - AS198953 ,Proton66 OOO
92.38.145.145 - AS199524, G-Core Labs S.A.
```

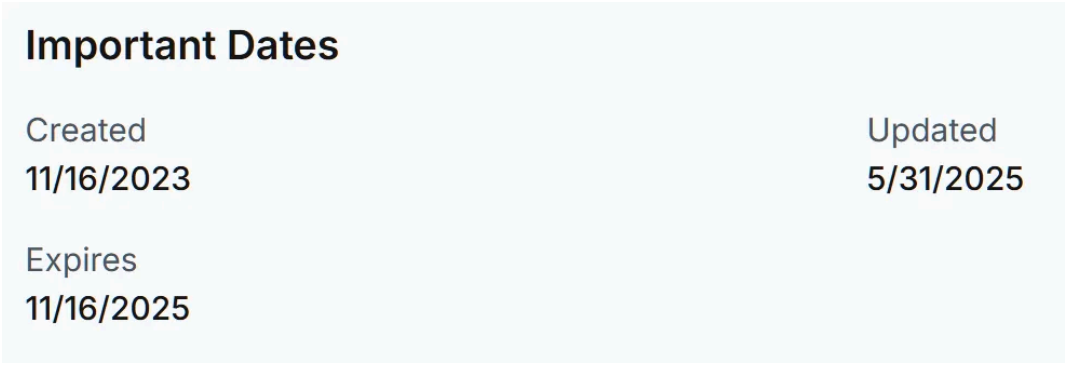
Starting with 141.98.6.34 part of the AS213702 owned by QWINS LTD we find a very interesting Russian operated hosting provider offering VPS and dedicated servers at very low prices (starting around 2$ per month), while also offering services directly through their Telegram bot.

Servers can be deployed in Russia, Germany, Finland, Netherlands, Estonia





The company was incorporated on 11 November 2024 in the UK and had “Kristina Konstantinova” as acting director from the date of incorporation until April 2025 (6 months exactly). The company domain was registered one year earlier on Nov 2023



Important Dates

Created
11/16/2023

Updated
5/31/2025

Expires
11/16/2025

KONSTANTINOVA, Kristina

Correspondence address
71-75, Shelton Street, London, England, WC2H 9JQ

Role	Date of birth	Appointed on	Resigned on
RESIGNED **Director**	**June 1990**	**11 November 2024**	**11 April 2025**

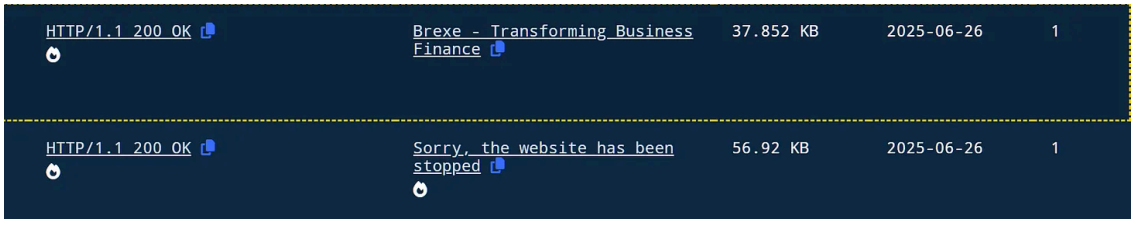
Nationality	Country of residence	Occupation
Estonian	**Estonia**	**Director And Company Secretary**

The company was renamed on April 2025 to “QUALITY IT NETWORK SOLUTIONS LIMITED”.

Previous company names

Name	Period
QWINS LTD	11 Nov 2024 - 14 Apr 2025

Reviewing the aforementioned IP, we can see that around the end of June, a site impersonating “Brex” financial services was hosted on it.



HTTP/1.1 200 OK	Brexe - Transforming Business Finance	37.852 KB	2025-06-26	1
HTTP/1.1 200 OK	Sorry, the website has been stopped	56.92 KB	2025-06-26	1

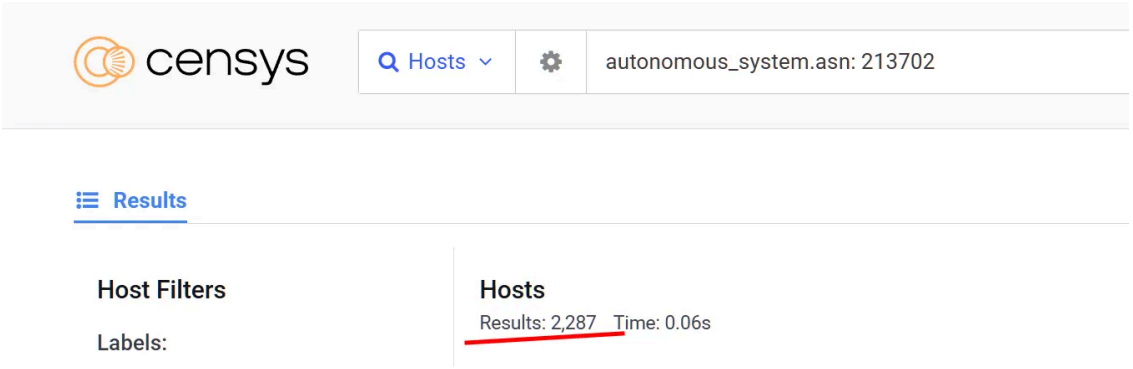
In addition, we see many malicious files (exe,zip,rar,etc.), associated mainly with infostealers and trojans recently communicating with the same IP meaning it is used by either multiple threat actors or a single actor involved in many attacks.

Scanned	Detections	Type	Name
2025-07-22	44 / 72	Win32 EXE	NewTeam.exe
2025-07-13	45 / 71	Win32 EXE	WeweChat.exe
2025-07-13	21 / 71	Win32 EXE	main.exe
2025-07-17	43 / 72	Win32 EXE	AsyncioInjector_v2.1.exe
2025-07-20	27 / 72	Win32 EXE	2025-07-20_8a4cd14cf51f2e0be689ddbe94347140_dosia_frostygoop_ghostlocker_knight_luca-stealer_poet-rat_quasar-rat_sliver_snatch
2025-07-22	0 / 60	RAR	Activate Installer v.2025 (PASS 2025).rar
2025-07-19	36 / 72	Win32 EXE	NvidiaAppSetupInt
2025-07-19	45 / 72	Win32 EXE	2025-07-19_686ed8d3e1e24d4161592628a49ccb30_black-basta_cobalt-strike_luca-stealer
2025-07-18	36 / 70	Win32 EXE	1main.exe
2025-07-09	21 / 72	Win32 EXE	2025-07-09_3910eef191054beeac73275848a13366_black-basta_cobalt-strike_luca-stealer_satacom_vidar
2025-07-15	45 / 72	Win32 EXE	2025-07-15_bdd0c17813ba1a7f7963cf02c42c8ace_black-basta_cobalt-strike_luca-stealer_satacom_vidar
2025-07-05	45 / 72	Win32 EXE	33034d4449a2e10559915f6ed6705f52f6b91427967737 6b9a23b5299b130528
2025-07-01	14 / 65	ZIP	ptoakddd.zip
2025-07-21	16 / 65	ZIP	Set-up.zip
2025-07-14	45 / 72	Win32 EXE	3c7e7e899aeabaddb4eaa26c29b043b7e89696283436 85c9704d8c595da78162
2025-07-18	45 / 72	Win32 EXE	2025-07-16_9f54a0ad760dfd257c7603764394277b_black-basta_cobalt-strike_luca-stealer_satacom_vidar
2025-07-11	22 / 71	Win32 EXE	testuser_test.exe

This hosting provider seems promising, so let’s spend some more time investigating the ASN before pivoting to other networks.

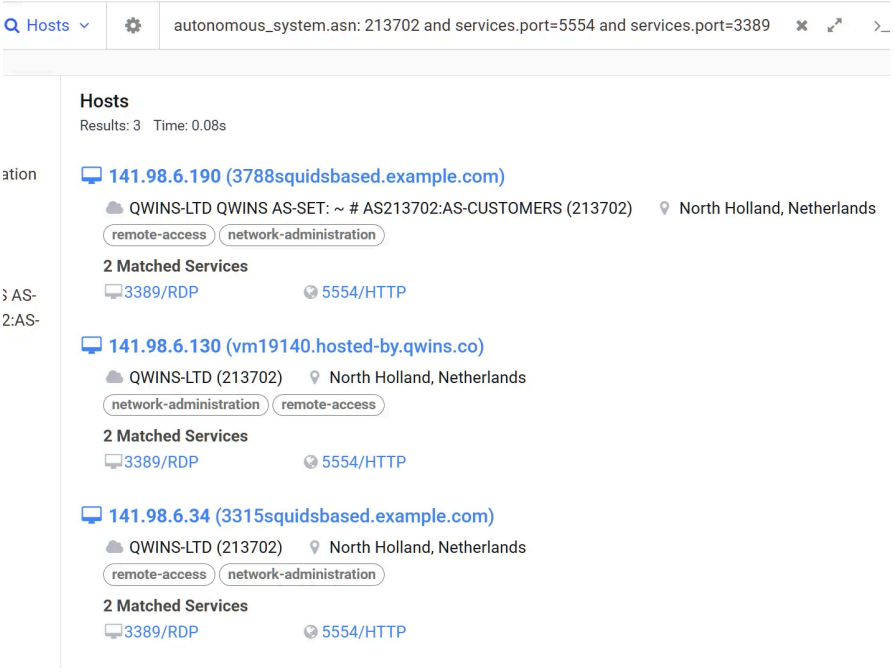
Our hypothesis is that ASN 213702 is being used by threat actors and by now, we can say with high confidence that the IP 141.98.6.34 is hosting malicious payloads and is used as C2 infrastructure.

Moving over to Censys, we see that there are about 2.3K hosts in that ASN.



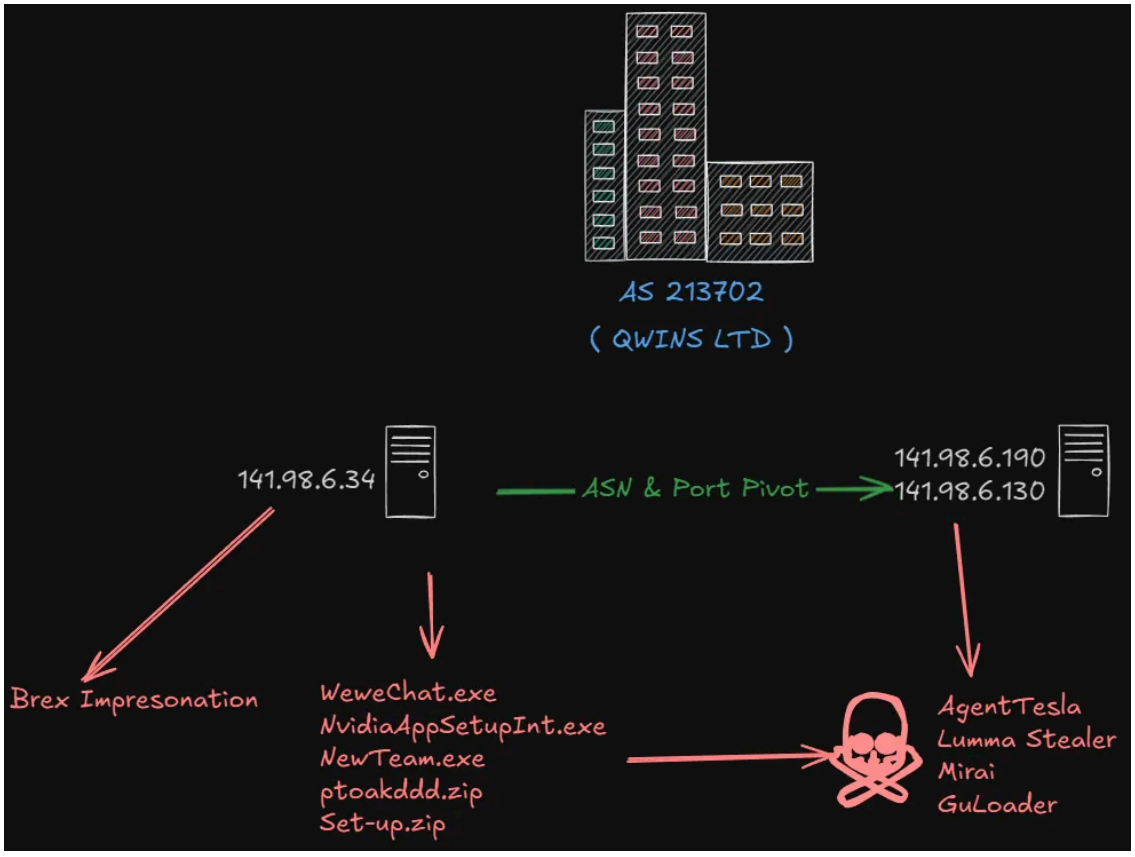
We can narrow it down by filtering for hosts that match the attributes of our IP, which leaves us with just 3 hosts which also seem to share the same self signed cert.

```
autonomous_system.asn: 213702 and services.port=5554 and services.port=3389
```



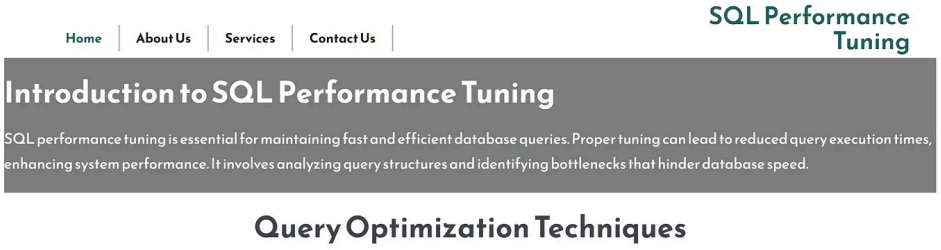

```
 141.98.6.190
141.98.6.130
141.98.6.34
```

The above IPs have been linked with malware, specifically with trojans and loaders and infostealers (makoob, guloader, agenttesla) and have been active around the same time, in combination with the services and self signed certificates, I would say it's safe to cluster those 3 IPs together.

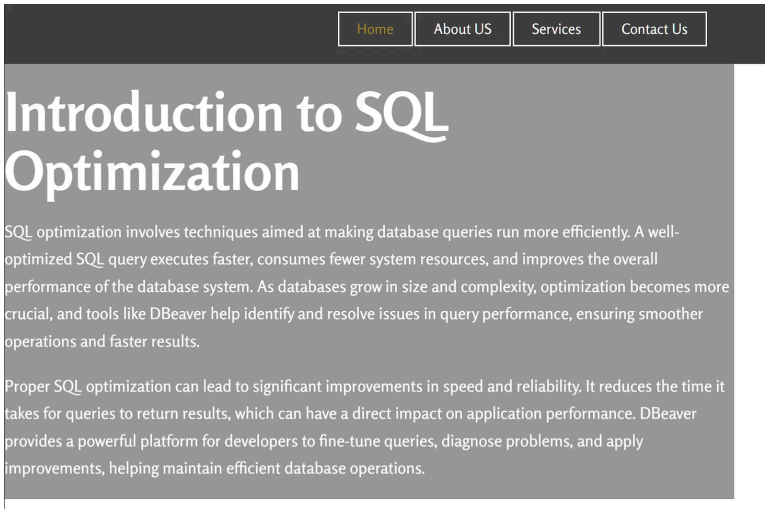


Our next pivot comes from domains hosted on our newly found cluster that trying to impersonate the database tool DBeaver.

”dbeaver.it[.]com” & “dbeaver-pro.[s]ite” are hosted on that cluster and they claim to perform SQL perfomance optimization.



dbeaver-pro[.]site



dbeaver.it[.]com

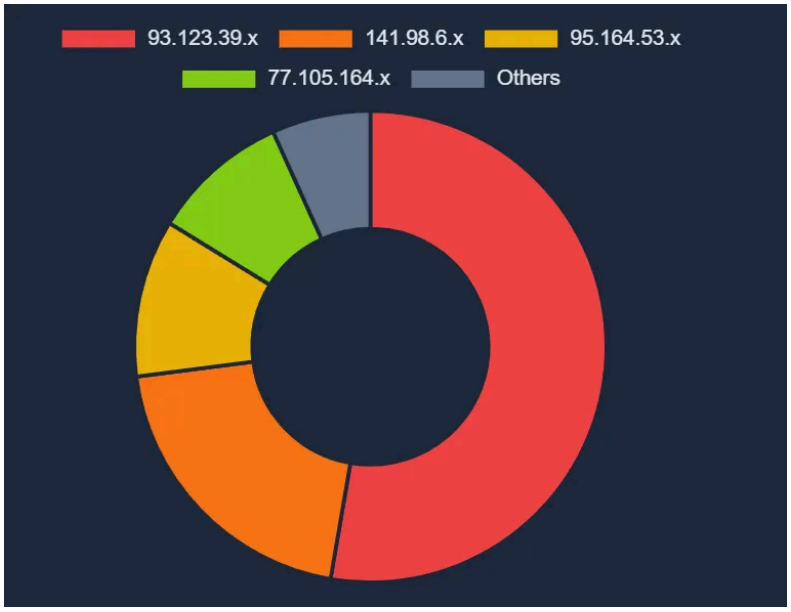
dbeaver-pro[.]site leads us to our next IP target 141.98.6.81, this IP has association mainly with botnets (mirai, quackbot, qbot, condi and more).

It’s clear now, that many malicious activities take place in this ASN, since it’s a relatively small network hosting around 3K IPs, let’s try to group the malicious activity per network and map out in more detail what kind of activities originate from these networks.

As Number	As Name	CIDR Range
213702	QWINS LTD	45.67.202.0/24
213702	QWINS LTD	77.105.164.0/24
213702	QWINS LTD	84.21.189.0/24
213702	QWINS LTD	93.123.39.0/24
213702	QWINS LTD	95.164.12.0/24
213702	QWINS LTD	95.164.53.0/24
213702	QWINS LTD	95.164.55.0/24
213702	QWINS LTD	95.164.123.0/24
213702	QWINS LTD	95.164.250.0/24
213702	QWINS LTD	141.98.6.0/24
213702	QWINS LTD	185.238.191.0/24
213702	QWINS LTD	195.66.27.0/24

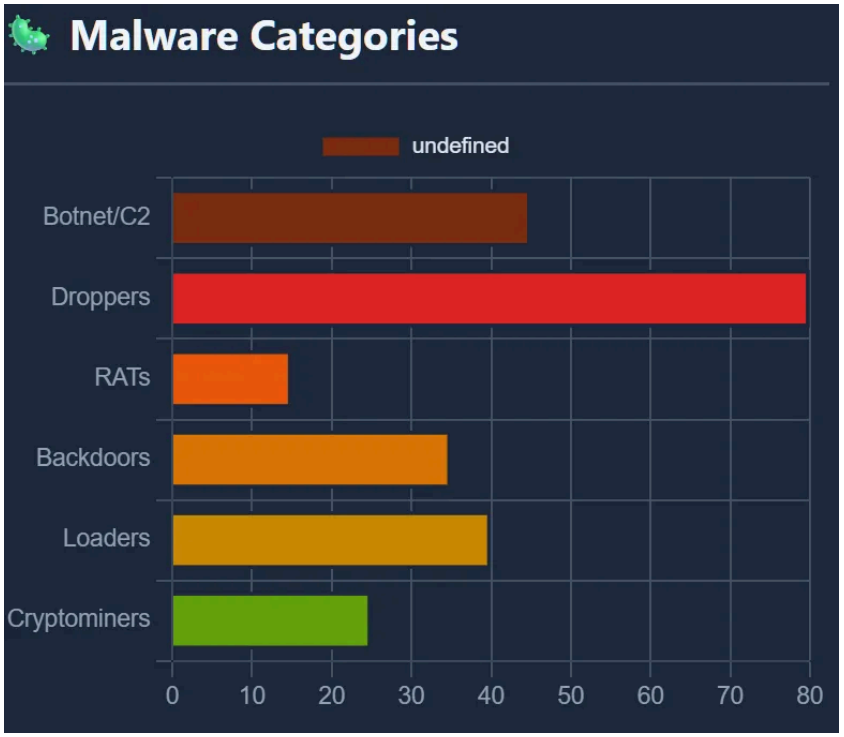
To keep the IoC as fresh as possible, I only focused on the last 30 days. Grabbed all the hashes, IPs and URLs that were flagged as malicious on these networks and analyzed the results.

Most of the activity is originating from networks 93.123.39.0/24 and 141.98.6.0/24



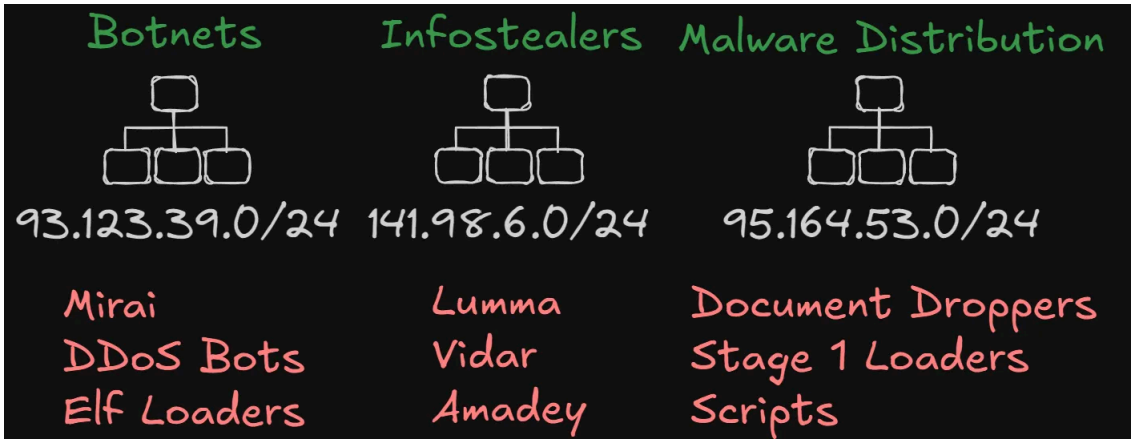
Based on the hashes found communicating and/or hosted on the networks, most of the malware is categorized as Droppers but as you can see, there is a huge variety of malware like botnet, rats, cryptominers, infostealers, targeting multiple architectures (Windows/Linux x86/x86_64, ARM, Mips). Specifically, I found a big concentration on the following malware.

Amadey Botnet
Mirai Botnet
Zapchast Trojan
Lumma
Vidar
DarkGate



We previously found that phishing websites and social engineering originated from the networks too, which is consistent with the initial access via document droppers (pdf, doc,zip).

Further reviewing the findings leads to additional clustering based on the malware communication.



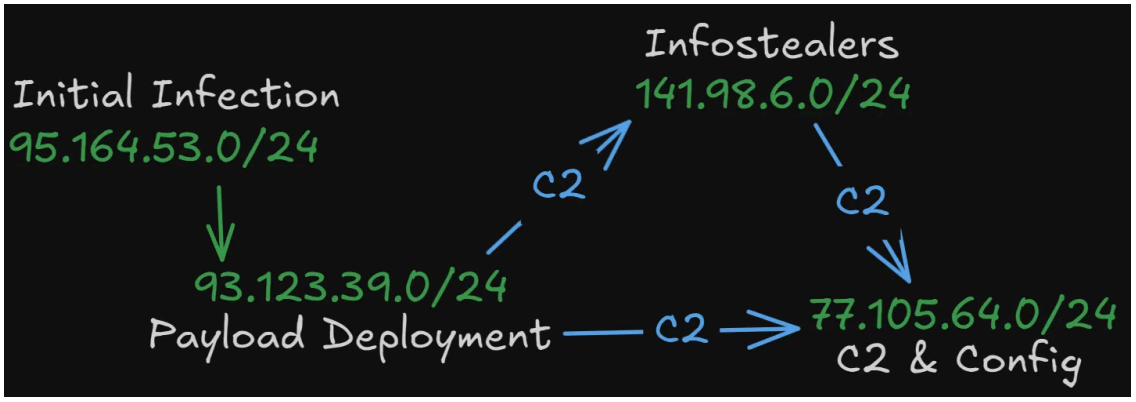
In this network, we find 39 malicious IPs spreading over than 120 payloads mainly associated with botnets, DDoS infra and C2 usually on port 666

We can find around 15 flagged IPs, hosting over 45 samples. Mainly infostealers like Amadey, Lumma and Vidar and probably C2 infra.

Found many files that look like initial payload distribution and malware hosting. It could be serving as the entry point for infection chains, hosting document droppers, and first stage loaders.

The above findings can be somewhat verified if we follow the flow of the malicious files/hashes. We can see that many droppers on the 95.164 network lead to payloads on the 93.123 network and many stealers from the 141.98

communicate the 77.105 network which I interpreted as C2 communication and data exfil.



To summarize, I think we found a very interesting hosting provider that requires further investigation, I can't say with certainty if this is or isn't a BPH but I can definitely say that there are some troubling signs.
In any case, this is all I have for now. I will follow up on some of the leads and see what other connections might appear.
If anyone has previously worked on that please reach out.
As always, I hope you are all safe and healthy. Thanks and take care!

Full IoC list

Linkedin

X

Source: https://intelinsights.substack.com/p/bulletproof-hosting-hunt