INTRINSEC

Innovative by design

# BtHoster: Identifying noisy networks emitting malicious traffic through masscan servers

Cyber Threat Intelligence

May 2025

@Intrinsec @Intrinsec Blog Website

# Table of contents

# 1. Key findings

- By analysing the networks that most hit our honeypots, we found two autonomous systems named *Skynet Network Ltd* (**AS214295**) and *Inside Network LTD* (**AS215476**), that we assess with a high level of confidence to be operated by the bulletproof hosting provider **BtHoster**. This provider notably offers pre-configured **masscan** servers. Both networks are based in the United Kingdom, registered by what we believe to be **shell companies**.

- Those two networks happen to transit their traffic through a **common upstream provider** named *UAB Host Baltic* (**AS209605**) based in Lithuania. Digging into the IPs of this network, we observed the presence of hundreds of **Mirai variants** and other malwares C2s such as **RisePro**, **Cobalt Strike**, **Remcos**, **Moobot**, and **HookBot**.

- Multiple IPv4 prefixes previously announced by an **Iranian network** were dispatched to those abusive networks based in the UK and on an additional one in **Serbia**. On March 5, a security analyst on *X* reported that all those networks were involved in **BGP** and **bruteforce attacks**. The description and geolocation of the previous Iranian autonomous system prefixes were kept on the new ones, making it look like the attacks came from Iran.

- A company based in Cyprus named *IT HOSTLINE LTD* (**AS44559**) known to be a partner of *Stark Industries Solutions* and managed by the operator of **Proxyline**, is providing IPv4 prefixes to abusive networks such as *Aeza International*(**AS210644**), *Global Internet Solutions*(**207713**), and *Global Connectivity Solutions*(**215540**).

# 2. Introduction

Between February and March 2025, our various honeypots received an increasing number of attacks originating from IPs announced by small autonomous systems composed of only a few IPv4 prefixes such as *Skynet Network Ltd* – **AS214295**. In addition to **bruteforce attacks** and **massive scanning**, various **Mirai botnets** and other malware command-and-control servers were found to be hosted on those networks.

By searching for information regarding the nature of those autonomous systems and the companies running them, we discovered that some of them were only **rebrands of a known bulletproof hosting provider named btHoster** that created those new entities to **evade bad reputation** and **blocklists**. This provider notably offers pre-configured **masscan** servers with a routing capacity up to **1300kpps** (Kilo Packets Per Second), matching with the high volume of aggressive networks attacks that we observed on our honeypots originating from the autonomous systems that it operates. Such infrastructures tend to be used by most threat actors, such as **IABs** looking for initial accesses in corporate network through exposed and vulnerable assets. For example, *ElectricIQ* recently reported

on members of the ransomware group **Black Basta** using *Proton66 OOO* - **AS198953**, a bulletproof provider based in Russia, to host mass internet scanning and automated brute forcing frameworks.[1]

As usual, the actors operating these businesses first create a regular company in their country of origin, that will later be blacklisted as the malicious content hosted on their network increases. They then open a **shell company in the United Kingdom** or an offshore country such as Seychelles, to register a new autonomous system. The IPv4 prefixes from their older network are then transferred. Depending on their financial capacities, such networks can sometimes announce new prefixes to completely erase all traces of the malicious activities hosted on their previous network.

As for any autonomous systems, their traffic needs to transit through bigger ISPs to access the internet. We notably found their provider to be based in Lithuania and named *UAB Host Baltic* – **AS209605**. This provider is indeed used by those smaller bulletproof networks for its upstream capacities.

With this report, we aim at providing an in-depth analysis of these networks, notably on how their infrastructure is operated, and their ramifications that could enable the finding of additional malicious networks in order to entirely block them.

# 3. Mapping the network through the upstream

## 3.1. UAB Host Baltic

As mentioned in the introduction, *UAB Host Baltic* (AS209605) is a hosting provider based in Lithuania currently announcing seven IPv4 prefixes[2] with servers located in the *BALT-IX* datacenter.[3]

This autonomous system's IPs have been particularly active in **brute force** and **aggressive scanning attacks**. In the last 30 days only, between February and March 2025, around **62,779** attacks were launched to our various honeypots by IPs originating from *UAB Host Baltic*'s network.

The table below displays the 10 IPs originating from **AS209605** that targeted the most our honeypots, between February and March 2025.

| Source IP | Count |
|---|---|
| 141.98.10[.]108 | 7,954 |
| 141.98.11[.]98 | 4,927 |
| 141.98.11[.]27 | 4,469 |
| 141.98.11[.]205 | 4,159 |
| 141.98.11[.]128 | 3,597 |
| 141.98.11[.]112 | 3,199 |
| 141.98.11[.]175 | 2,275 |
| 91.224.92[.]10 | 780 |
| 141.98.11[.]88 | 386 |
| 141.98.11[.]89 | 292 |

*Source: Intrinsec.*

[1] *https://blog.eclecticiq.com/inside-bruted-black-basta-raas-members-used-automated-brute-forcing-framework-to-target-edge-network-devices*

[2] *https://bgp.he.net/AS209605#_prefixes*

[3] *https://bgp.he.net/AS209605#_ix*

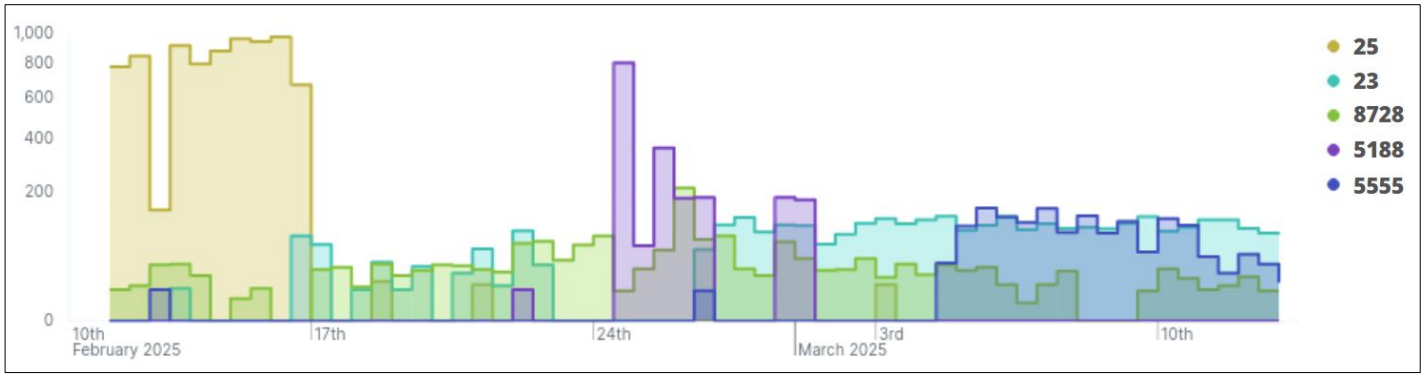



*Figure 1. Chart of the number of attacks that targeted our honeypots, distributed by destination port and originating from AS209605 between February and March 2025.*

Regarding other malicious content that could be found on this network, we discovered that it had been used to launch spamming campaigns deploying the **XLoader** malware amongst others throughout 2024.[4] Additionally, the network happens to host hundreds of **Mirai** botnets.[5]

## 3.2. Inside Network LTD

*UAB Host Baltic* provides upstream transit to two smaller networks, starting with *Inside Network LTD* (**AS215476**), an autonomous system based in the United Kingdom[6] and allocated in February 2024 that announces a single IPv4 prefix: **77.90.185**[.]**0/24**.[7] When visiting the company's website "**insidenetwork**[.]**info**", the users are invited to contact the provider on Telegram through the account "**bthosterltd**". This autonomous system appears in spamhaus' blocklist.[8]

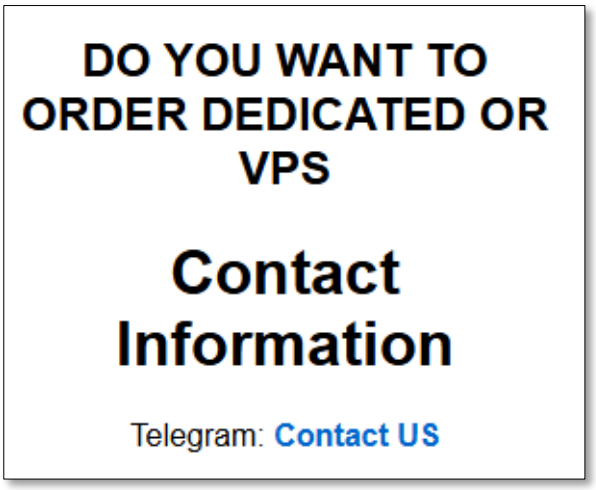



*Figure 2. Landing page of insidenetwork[.]info.*

[4] *https://bazaar.abuse.ch/sample/20e1e86085b3f02e2d3c2ac50e45c181f161cc070beafc10a3bf30ca5dfec771/*

[5] *https://urlhaus.abuse.ch/feeds/asn/209605*

[6] *https://find-and-update.company-information.service.gov.uk/company/15432172*

[7] *https://bgp.he.net/AS215476*

[8] *https://www.spamhaus.org/drop/asndrop.json*

### 3.2.1. BtHoster LTD

This Telegram account happens to be the contact of a known bulletproof provider named "**BtHoster**", that used to operate an autonomous system of the same name: *BtHoster LTD* – **AS198465**, also registered in the United Kingdom.[9] The single prefix announced by *Inside Network* was previously announced by this autonomous system.

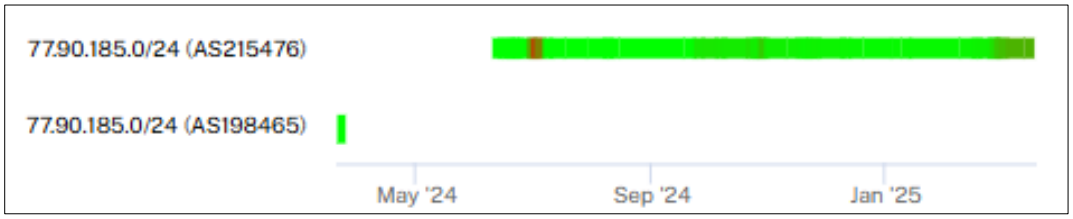



*Figure 3. Timeline of autonomous systems that announced the prefix 77.90.185[.]0/24. Source: RIPEstat.*

On underground forums, BtHoster advertises the bulletproof nature of his business stating that activities such as "*scan / brute / cracking*" are allowed to be operated on its servers. Additionally, pre-configured masscan servers can be rented with routing capacities maxing 1300kpps.

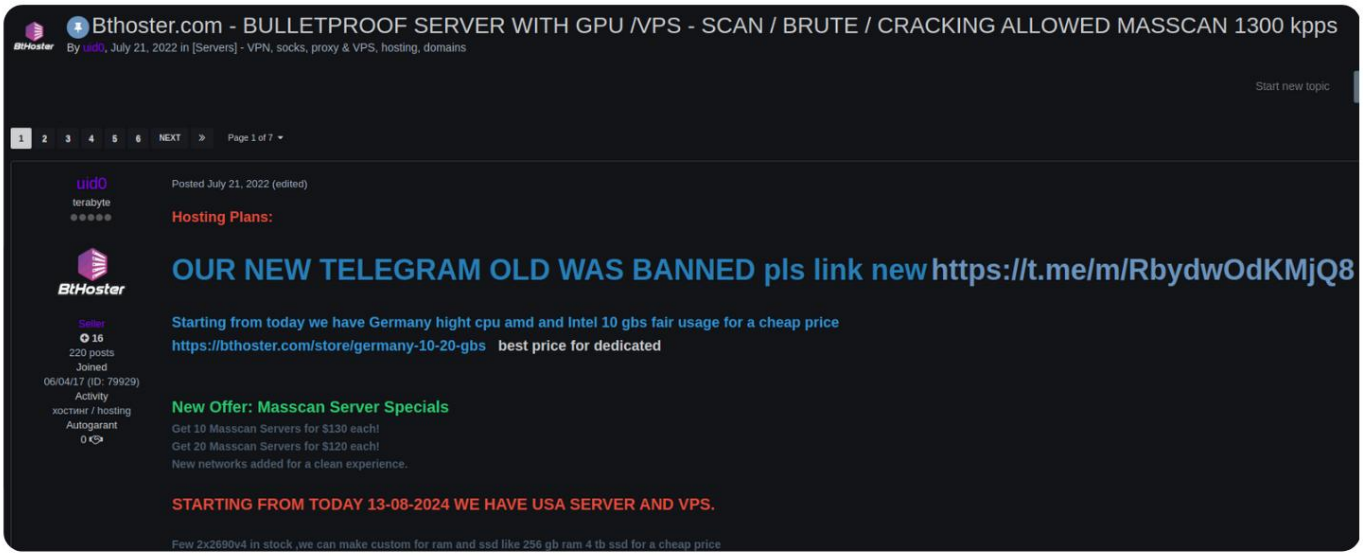



*Figure 4. Advertisement for hosting solution "BtHoser" on an underground Russian-speaking forum. Source: Exploit.*

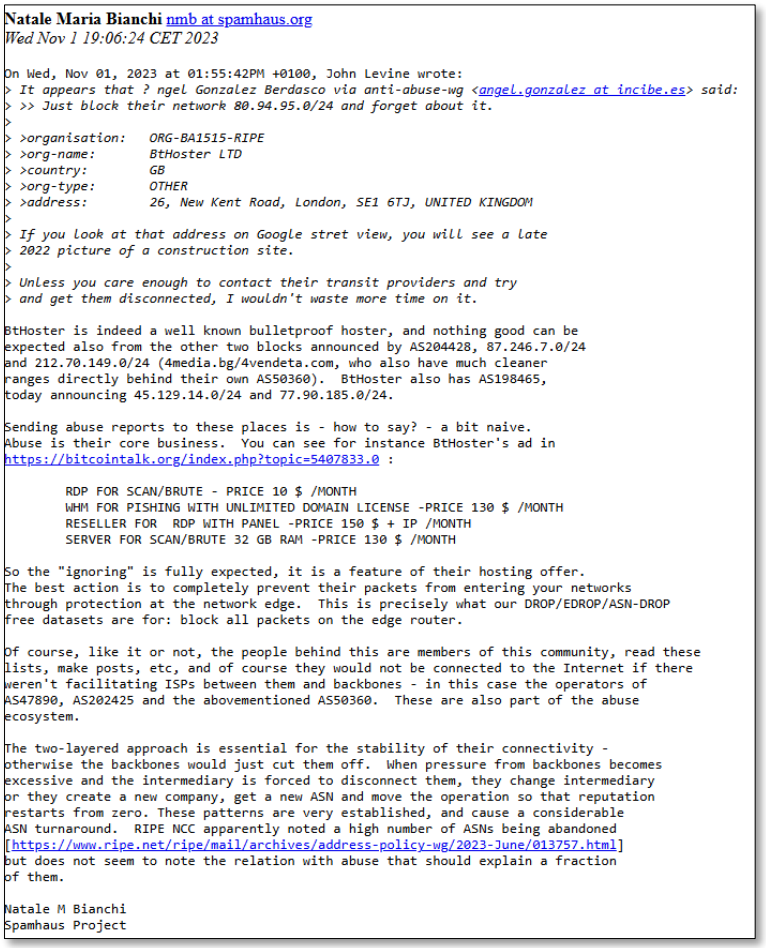
Their website "bthoster[.]com", was once hosted on *UAC Host Baltic*'s network in 2022,[10] hinting that BtHoster's administrator has been favouring this provider in addition to using it for its upstream capacities.

[9] *https://find-and-update.company-information.service.gov.uk/company/14487799/*

[10] *https://www.virustotal.com/gui/ip-address/141.98.11.127*

### 3.2.2. SS-Net, 4Media Ltd., 4Vendeta

A mail exchange from November 2023 between a member of the Spanish Instituto Nacional de Ciberseguridad and a Spamhaus member, already mentioned the malicious nature of BtHoster[11], stating that "*the best action is to completely prevent their packets from entering your networks*". At the time, BtHoster used an IPv4 prefix announced by *SS-Net* – **AS204428**, [12] a network that, according to Spamhaus, also provides bulletproof capacities, and was added to their block list.[13]



**Natale Maria Bianchi** nmb at spamhaus.org
*Wed Nov 1 19:06:24 CET 2023*

On Wed, Nov 01, 2023 at 01:55:42PM +0100, John Levine wrote:
> *It appears that ? ngel Gonzalez Berdasco via anti-abuse-wg <angel.gonzalez at incibe.es> said:*
> *>> Just block their network 80.94.95.0/24 and forget about it.*
>
> *>organisation: ORG-BA1515-RIPE*
> *>org-name: BtHoster LTD*
> *>country: GB*
> *>org-type: OTHER*
> *>address: 26, New Kent Road, London, SE1 6TJ, UNITED KINGDOM*
>
> *If you look at that address on Google stret view, you will see a late*
> *2022 picture of a construction site.*
>
> *Unless you care enough to contact their transit providers and try*
> *and get them disconnected, I wouldn't waste more time on it.*

BtHoster is indeed a well known bulletproof hoster, and nothing good can be expected also from the other two blocks announced by AS204428, 87.246.7.0/24 and 212.70.149.0/24 (4media.bg/4vendeta.com, who also have much cleaner ranges directly behind their own AS50360). BtHoster also has AS198465, today announcing 45.129.14.0/24 and 77.90.185.0/24.

Sending abuse reports to these places is - how to say? - a bit naive. Abuse is their core business. You can see for instance BtHoster's ad in https://bitcointalk.org/index.php?topic=5407833.0 :

RDP FOR SCAN/BRUTE - PRICE 10 $ /MONTH
WHM FOR PISHING WITH UNLIMITED DOMAIN LICENSE -PRICE 130 $ /MONTH
RESELLER FOR RDP WITH PANEL -PRICE 150 $ + IP /MONTH
SERVER FOR SCAN/BRUTE 32 GB RAM -PRICE 130 $ /MONTH

So the "ignoring" is fully expected, it is a feature of their hosting offer. The best action is to completely prevent their packets from entering your networks through protection at the network edge. This is precisely what our DROP/EDROP/ASN-DROP free datasets are for: block all packets on the edge router.

Of course, like it or not, the people behind this are members of this community, read these lists, make posts, etc, and of course they would not be connected to the Internet if there weren't facilitating ISPs between them and backbones - in this case the operators of AS47890, AS202425 and the abovementioned AS50360. These are also part of the abuse ecosystem.

The two-layered approach is essential for the stability of their connectivity - otherwise the backbones would just cut them off. When pressure from backbones becomes excessive and the intermediary is forced to disconnect them, they change intermediary or they create a new company, get a new ASN and move the operation so that reputation restarts from zero. These patterns are very established, and cause a considerable ASN turnaround. RIPE NCC apparently noted a high number of ASNs being abandoned [https://www.ripe.net/ripe/mail/archives/address-policy-wg/2023-June/013757.html] but does not seem to note the relation with abuse that should explain a fraction of them.

Natale M Bianchi
Spamhaus Project

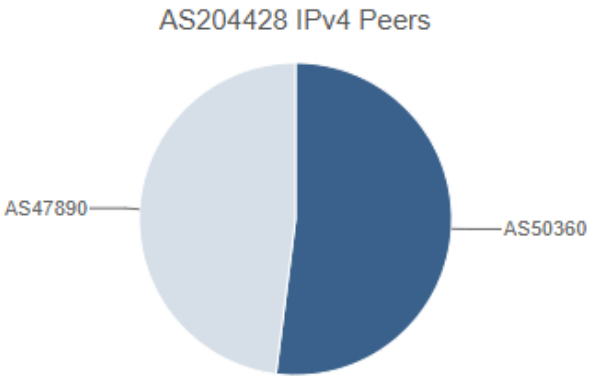
*Figure 5. Snippet of the mail exchange. Source: RIPE.*

Based in Bulgaria, *SS-Net* shares 48% of its peering agreements with *UNMANAGED LTD* – **AS47890**, another British bulletproof hosting provider that placed itself on the 4th position of autonomous systems that most attacked our honeypots, with more than **1 million network attacks** launched. The other 52% are shared with *Tamatiya EOOD* – **AS50360**, also based in Bulgaria and operated by a hosting provider named **4Vendeta**.

[11] *https://www.ripe.net/ripe/mail/archives/anti-abuse-wg/2023-November/006519.html*

[12] *https://bgp.he.net/AS204428*

[13] *https://www.spamhaus.org/drop/asndrop.json*




| ASN | Name |
|---|---|
| AS50360 | Tamatiya EOOD |
| AS47890 | UNMANAGED LTD |

*Figure 6. Pie chart of the percentage of load shared with the above-mentioned autonomous systems and AS204428. Source: Hurricane Electric.*

We assess with a high level of confidence that 4Vendeta also operates *SS-Net*. The two companies indeed share the same mail server **195.230.24**[.]**20**, resolving both their websites "4vendeta[.]com" and "ssnet[.]eu".[14] This IP resolves the domain of another Bulgarian company named *4Media Ltd.*, also operating its own autonomous system **AS202325**, and benefits from *Tamatiya EOOD*'s upstream.

We recently came across *4Media Ltd.* during an investigation into the set known as *Shadow Syndicate*, attributed by Group-IB in late 2023.[15] This intrusion set appears to heavily rely, for European hosting providers within ASNs that are part of the AS-set AS-Tamatiya, on a Bulgarian network cluster of 22 ASNs that includes **AS202325**, as well as several bulletproof hosters (BPHs) operated from Russia (we will publish further details in a separate analysis).

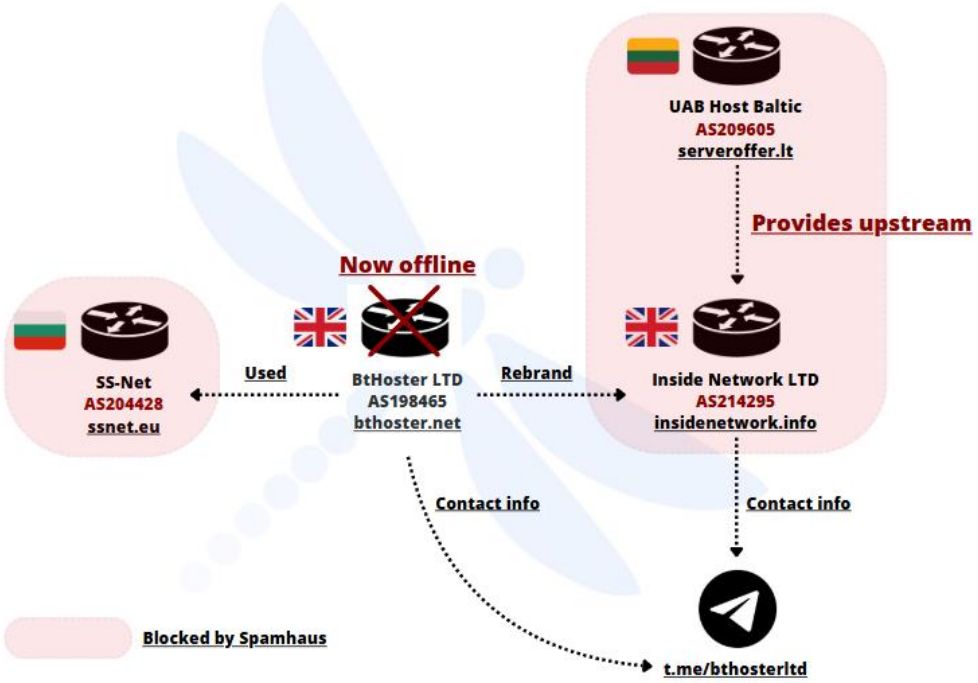



*Figure 7. Layout summarizing the links between the above-mentioned autonomous systems.*

[14] *https://www.virustotal.com/gui/ip-address/195.230.24.20*
[15] https://www.group-ib.com/blog/shadowsyndicate-raas/

Again, SS-Net was particularly noisy with around **61,724** networks attacks targeted at our honeypots between February 17th and March 17th, 2025. The table below displays the 10 IPs that targeted the most our honeypots originating from **AS204428**.

| Source IP | Count |
|---|---|
| 80.94.95[.]240 | 21,028 |
| 83.222.190[.]190 | 16,003 |
| 83.222.191[.]42 | 8,502 |
| 80.94.95[.]112 | 4,268 |
| 83.222.191[.]130 | 2,361 |
| 83.222.191[.]70 | 1,928 |
| 83.222.191[.]182 | 1,720 |
| 83.222.191[.]162 | 1,599 |
| 83.222.191[.]178 | 1,404 |
| 83.222.190[.]46 | 999 |

*Source: Intrinsec.*

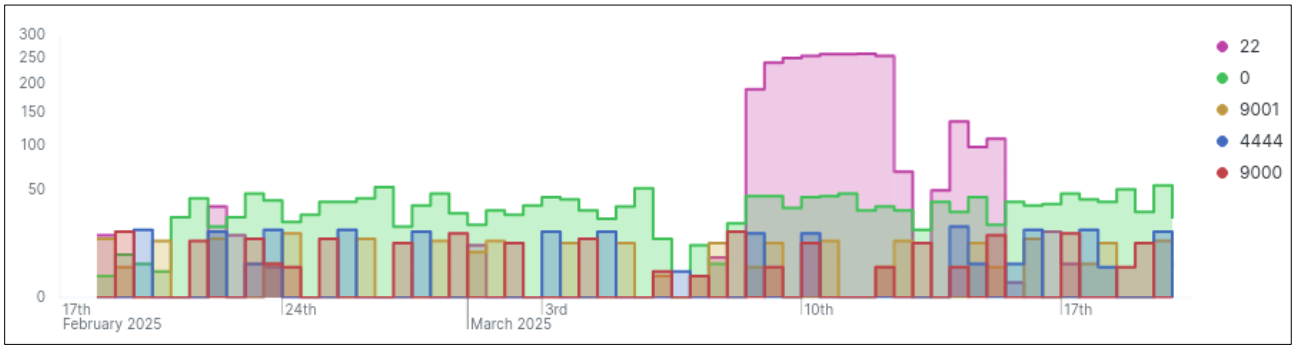



*Figure 8. Chart of the number of attacks that targeted our honeypots, distributed by destination port and originating from AS204428 between February and March 2025.*

## 3.3. Skynet Network Ltd

The second autonomous system that benefits from UAB Host Baltic's upstream capacities is named *Skynet Network Ltd* – **AS214295** and also based in the United Kingdom.[16] With only three IPv4 prefixes of 256 IPs each,[17] Skynet Network still managed to place itself as the 9th position of autonomous systems that most targeted our honeypots in the last 30 days with more than a million network attacks recorded.

| ASN | AS | Count |
|---|---|---|
| 135905 | *VIETNAM POSTS AND TELECOMMUNICATIONS GROUP* | 40,376,796 |
| 16276 | *OVH SAS* | 12,943,886 |
| 53062 | *ALT|GGNET TELECOM BACKBONE* | 1,777,355 |
| **47890** | ***Unmanaged Ltd*** | **1,398,688** |

[16] *https://find-and-update.company-information.service.gov.uk/company/12308008/*

[17] *https://bgp.he.net/AS214295*

| | | |
|---|---|---|
| 14061 | *DigitalOcean, LLC* | 1,321,749 |
| **214943** | ***Railnet LLC*** | **1,237,016** |
| 135834 | *Multicraft Digital Tech* | 1,186,230 |
| 37963 | *Hangzhou Alibaba Advertising Co.,Ltd.* | 1,053,648 |
| **214295** | ***Skynet Network Ltd*** | **1,035,019** |
| 138754 | *Kerala Vision Broad Band Private Limited* | 921,465 |

*Source: Intrinsec*

The table below displays the 10 IPs that targeted the most our honeypots originating from **AS214295**, between February 9th and March 10th, 2025.

| Source IP | Count |
|---|---|
| 194.0.234[.]26 | 42,081 |
| 45.142.193[.]47 | 32,893 |
| 45.142.193[.]56 | 32,803 |
| 45.142.193[.]50 | 32,774 |
| 45.142.193[.]83 | 32,756 |
| 45.142.193[.]244 | 32,611 |
| 45.142.193[.]72 | 32,575 |
| 45.142.193[.]46 | 32,544 |
| 45.142.193[.]43 | 32,541 |
| 45.142.193[.]67 | 32,527 |

*Source: Intrinsec*

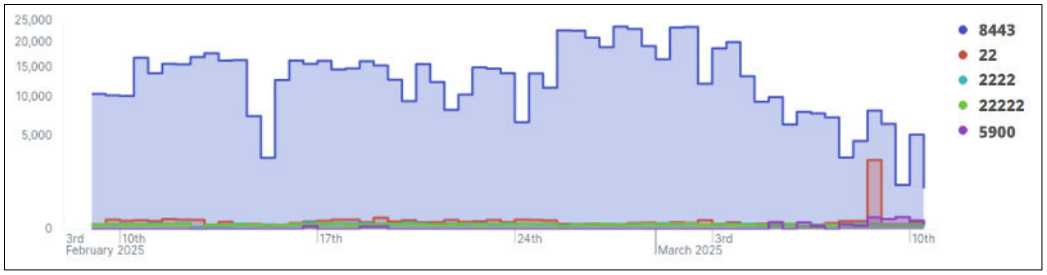
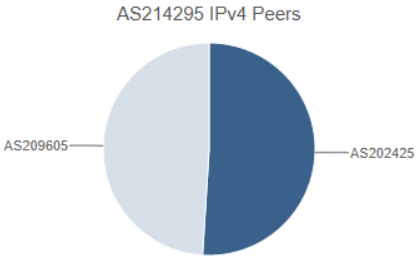



*Figure 9. Chart of the number of attacks that targeted our honeypots, distributed by destination port and originating from AS214295 between February and March 2025.*

*Skynet Network* does not share all its peering agreements with *UAB Host Baltic*. 51% of them are shared with *IP Volume Inc.* – **AS202425**, an autonomous system based in Seychelles and operated by *Ecatel*'s administrators.




| ASN | Name |
|---|---|
| AS202425 | IP Volume inc |
| AS209605 | UAB Host Baltic |

*Figure 10. Pie chart of the percentage of load shared with the above-mentioned autonomous and AS214295. Source Hurricane Electric.*

**IP Volume Inc. | Ecatel**

Considered "*one of [The Netherlands']most criticized hosting businesses*" according to The New York Times[18], Ecatel was founded in 2005 by two Dutch nationals. The company was registered in Kent (United Kingdom) with its headquarters in The Hague. In 2011, the company got into an argument with the data centre in Alphen aan de Rijn where they rented servers. Thereupon, they decided to start their own data centre called **DataOne** in Wormer.[19]

In December 2015, IP addresses from Ecatel moved to a new company registered in Seychelles named *Quasi Network*, which later changed to "*IP Volume Inc*". In 2020, the Ministry of Justice and Security of the Netherlands published a ranking of Dutch hosting companies with the most child pornography on their servers. With 4,500 out of 175,000 verified reports, IP Volume Inc ranked **second**.[20]

In addition to IP Volume Inc, Ecatel's directors created another company in the Netherlands named "*FiberXpress BV*"[21], associated to the autonomous system **AS57717**. *IP Volume Inc* obtains upstream from this network by sharing **74.5**% of its peering agreements. Overall, the autonomous system manages **1,792 IPv4**. The address of the company is the same as their datacentre in Wormer, where all of their other Dutch companies are also located.[22]

By analysing the various contents hosted on *FiberXpress BV*, we discovered a trove of domains that were part of a large network of fake websites distributing copies of cracked software or video games. In some cases, those websites switched from being hosted on *IP Volume Inc* to *FiberXpress BV*.

Furthermore, we often stumble upon *IP Volume Inc*. to be the main provider of routing capacities to smaller bulletproof hosting networks such as *Telkom Internet LTD* – **AS210848**.

### 3.3.1. Limited Network and the Iranian connection

Regarding the prefixes announced by *Skynet Network*, **194.0.234**[.]**0/24** is said to be managed by the company *Atis Omran Sevin PSJ* located in Iran. We assess with a medium level of confidence that this description was the one provided by the previous autonomous system of the same name that announced this prefix, only to be intentionally spoofed by the current AS announcing it. A second prefix is said to be owned by *Limited Network Ltd.*, another company based in the UK,[23] operating its own autonomous system **AS213790**.[24]

| IPv4 prefix | Company |
|---|---|
| 194.0.234[.]0/24 | Atis Omran Sevin PSJ |
| 45.142.193[.]0/24 | Limited Network LTD |
| 87.120.93[.]0/24 | Audit Data |

*Source: Hurricane Electric*.

[18] *https://www.nytimes.com/interactive/2019/12/22/us/child-sex-abuse-websites-shut-down.html*

[19] *https://nl.wikipedia.org/wiki/IP_Volume*

[20] *https://www.nrc.nl/nieuws/2020/10/08/vier-bedrijven-hosten-overgrote-deel-kinderporno-a4015235*

[21] *https://www.dnb.com/business-directory/company-profiles.fiberxpress_bv.98ecba6e933249d62edbcef242871a0f.html*

[22] Intrinsec private report. "*Mapping Ecatel ramifications & bulletproof networks fronted by offshore companies*". October 2024.

[23] *https://find-and-update.company-information.service.gov.uk/company/16076447/*

[24] *https://bgp.he.net/AS213790*

The now offline company's website "limitednetwork[.]xyz" was hosted on **77.90.185**[.]**19**,[25] an IP announced by *Inside Network Ltd* – AS215476, the British company operated by BtHoster. As for *Inside Network*'s website, the users visiting *Limited network*'s website would be invited to contact BtHoster's telegram account for any requests. Based on this find, we can assess with a high level of confidence that BtHoster also operates *Limited Network Ltd* – **AS213790**, and by extension, *Skynet Network Ltd* – **AS214295**, that announces prefixes for *Limited Network*. Additionally, the high number of aggressive scanning attacks emitted from *Skynet Network* matches with the masscan servers provided by BtHoster, thus hinting furthermore that *Skynet Network* could be operated by BtHoster.


*Figure 11. Landing page of limitednetwork[.]xyz(left), landing page of insidenetwork[.]info(right).*

Limited Network's IPs also emit thousands of network attacks. In the last 30 days, around **55,295** of them were launched at our various honeypots. All attacks originated from the single IPv4 prefix announced by Limited Network '**185.93.89**[.]**0/24**'.

| Source IP | Count |
|---|---|
| 185.93.89[.]120 | 35,581 |
| 185.93.89[.]108 | 12,840 |
| 185.93.89[.]118 | 6,874 |

*Source: Intrinsec.*

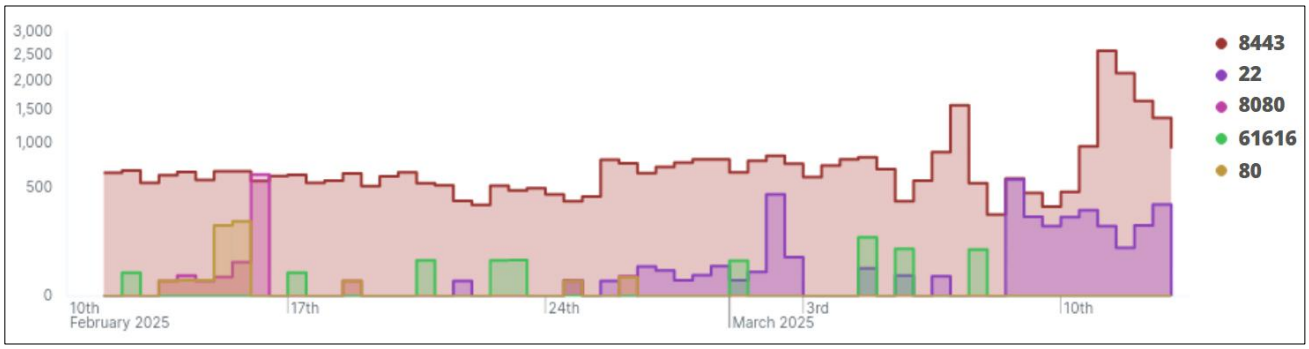



*Figure 12. Chart of the number of attacks that targeted our honeypots, distributed by destination port and originating from AS213790 between February and March 2025.*

[25] *https://www.virustotal.com/gui/domain/limitednetwork.xyz/*

Curiously, this prefix's description displays the same Iranian company "**Atis Omran Sevin PSJ**" that was found in one of *Skynet Network*'s prefixes.[26] Once again, we can assess with a medium level of confidence that those descriptions were not changed intentionally to spoof the geolocation of the company in Iran.

This Iranian hosting provider previously managed its own autonomous systems (**AS58192**, **AS48214**, **AS52209, AS15828**, lordvps[.]net, khatibi[.]org, almaseabi[.]net) which are now all offline. All IPv4 prefixes were then reannounced by other autonomous system, including the prefix **81.30.107**[.]**0/24**, now announced by *CIPHER OPERATIONS DOO BEOGRAD* – **AS215930**, a company based in Serbia.

### 3.3.2. CIPHER OPERATIONS DOO BEOGRAD

Announcing five IPv4 prefixes of 256 IPs each,[27] this network's upstream is *Tele Asia Limited* – **AS133398**, the same company providing upstream to *UAB host Baltic,* and that also appears to host hundreds of Mirai variants[28]. Their network is currently listed in Spamhaus' block list,[29] and provides no website. We assess with a high level of confidence that It was listed for being a rebrand of a bulletproof hosting provider based in Iran that previously managed the autonomous system *Robat Blue Diamond Network Co., Ltd.* – **AS15828**. They notably both share the same contact address: "spaceshipnetworks@yandex[.]com". When it was still announcing IPs, this network was also peered with *Tele Asia Limited*.

### 3.3.3. BGP Hijack, ASN shifts, prefix movements

On March 5th, 2025, Jo Provost, a security analyst, posted a message on *X* that mentioned some of these networks.[30] In his tweet, he notably mentions how *CIPHER OPERATIONS DOO BEOGRAD*(**AS215930**), *UAB Host Baltic*(**AS209605**), and *Amwaj Alkhyr*(**AS44947**), announced a common IPv4 prefix **81.30.107**[.]**0/24**. According to him, this operation can be associated to **BGP hijacking**.[31]

Such attack could allow attackers to:

- Hijack unencrypted data (MITM, phishing, espionage)
- Launch attacks while masking origin
- Misattribute blame to other countries

[26] *https://bgp.he.net/AS213790#_prefixes*

[27] *https://bgp.he.net/AS215930*

[28] *https://urlhaus.abuse.ch/feeds/asn/133398*

[29] *https://www.spamhaus.org/drop/asndrop.json*

[30] *https://x.com/sansmotdepasse/status/1897102087001141657*

[31] *https://www.ripe.net/media/documents/BGP_hijacking_brief_guide_on_protecting_BGP_from_bad_actors_b117eaf3-243d-4a95_xjDDZAc.pdf*

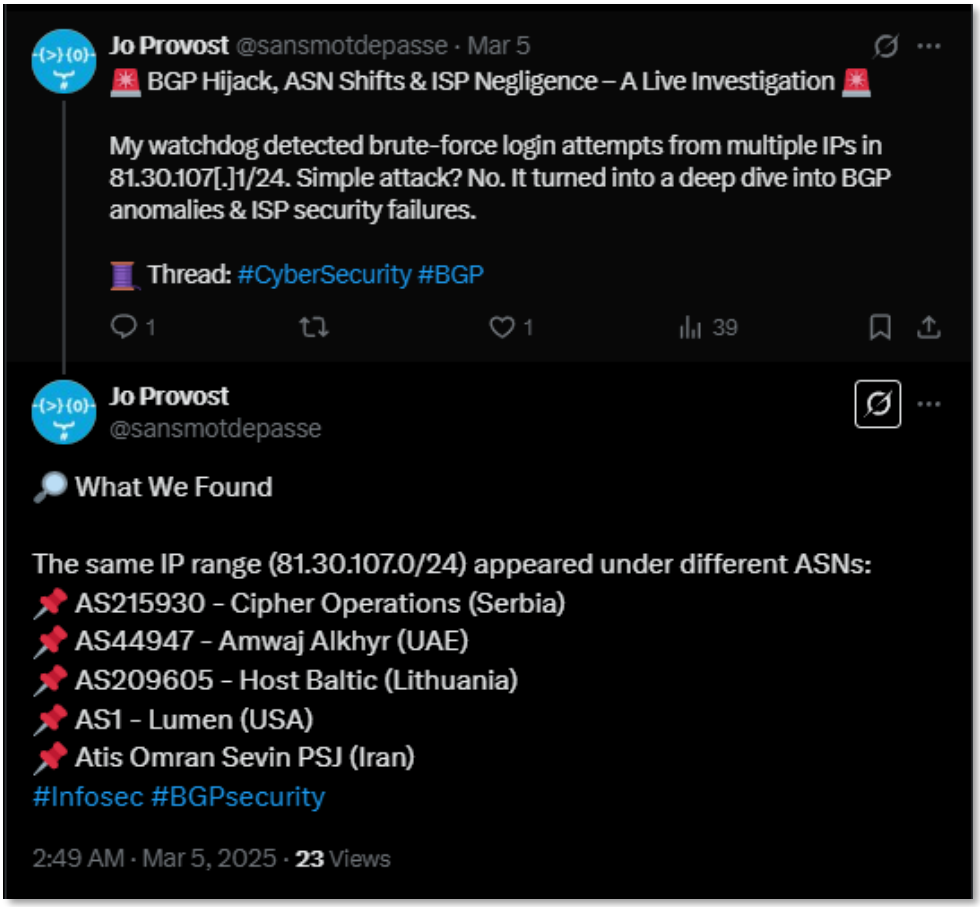



*Figure 13. Tweet dating from March 5, 2025, posted by Jo Provost on X.*

The following layout (*cf. figure 14*) aims at summarizing all the elements linking the previously mentioned entities.

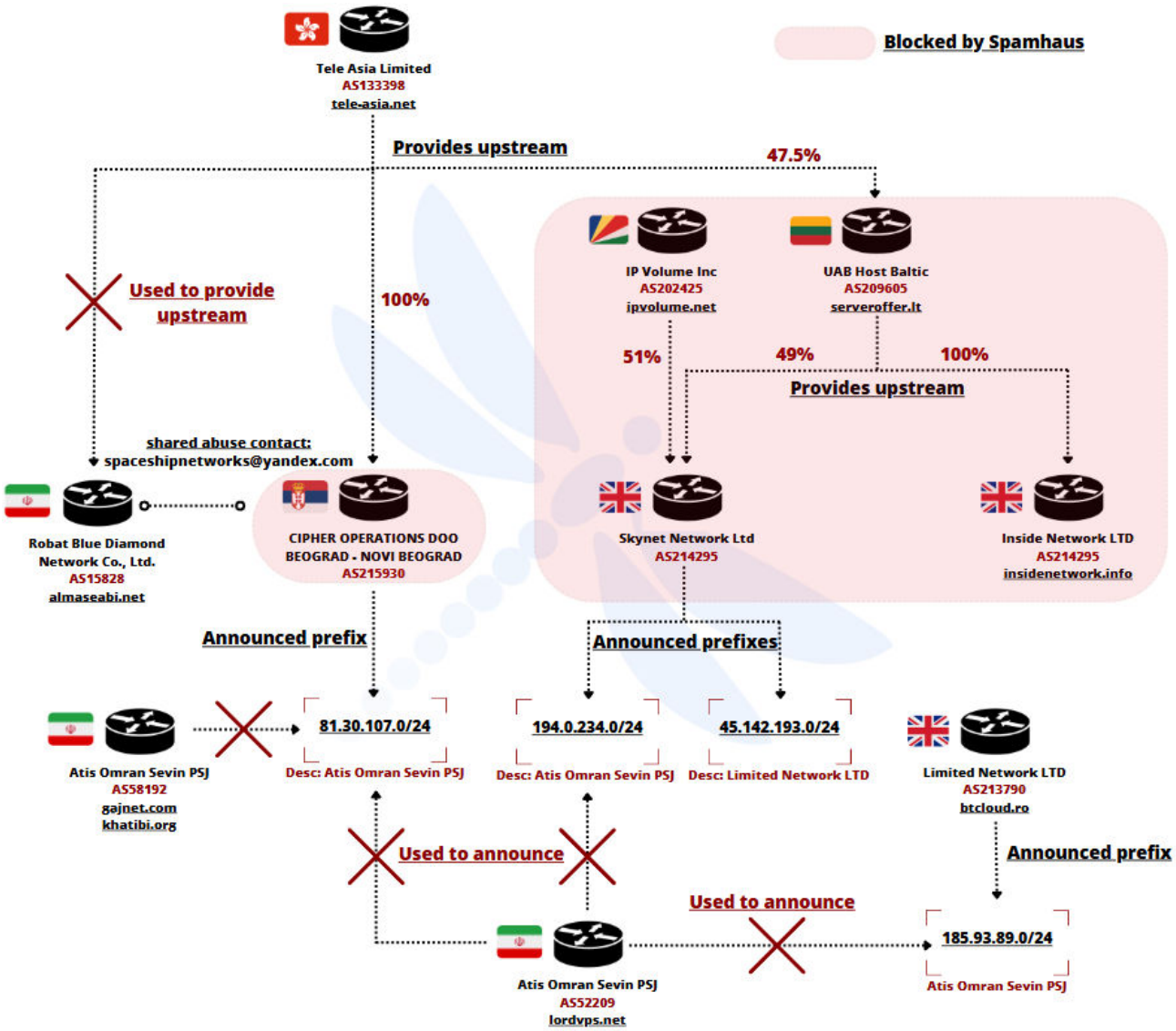



*Figure 14. Layout summarizing all the network links found between each autonomous system we mentioned.*

### 3.3.4. Middle network and proxy provider

One of the networks involved in this BGP anomaly, *Amwaj Alkhyr*(**AS44947**), based in Dubai, has also kept the description of prefixes previously announced by the Iranian company "**Atis Omran Sevin PSJ**".[32] As for the other networks, we can be led to believe that it was done unintentionally, or to spoof the company. Nonetheless, in 2024, most of the prefixes announced by *Amwaj Alkhyr* were moved to abusive autonomous such as *Aeza International Ltd.* – **AS210644** along the Serbian network that we previously encountered (**AS215930**) involved in the BGP hijacking incident. Those elements reinforce the hypothesis of this network being operated for sketchy motives.

[32] *https://bgp.he.net/AS44947#_prefixes*

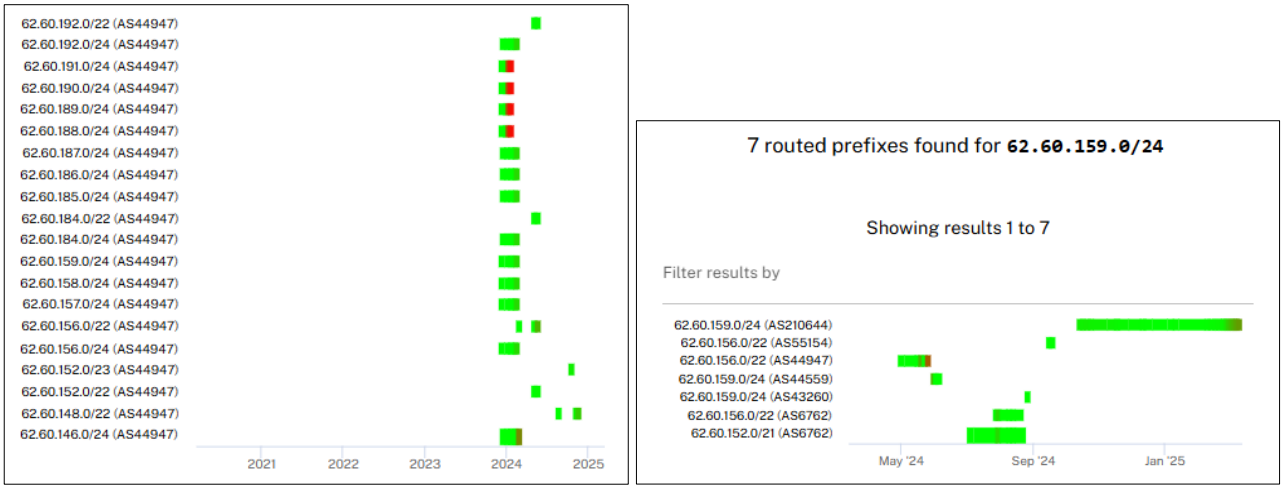



*Figure 15. Timeline of IPv4 prefixes announced by Amwaj Alkhyr – AS44947(left), and movements of prefix 62.60.159[.]0/24(right). Source: RIPEstat*

We noticed that most prefixes first moved to a network based in Cyprus named *IT HOSTLINE LTD* – **AS44559**, managed by an Uzbek individual.[33] This person notably operates the proxy businesses "**Proxyline**, **Spaceproxy**, and **Farmproxy.ru**", that get most of their IPs from the Russian bulletproof provider *Stark Industries Solutions Ltd.* – **AS44477**, with which his network shares all its peering agreements.[34] As mentioned by Brian Krebs in an article from May 2024: "*investigation into Stark Industries reveals it is being used as a global proxy network that conceals the true source of cyberattacks and disinformation campaigns against enemies of Russia*".[35] *Stark Industries* also owns a couple of prefixes on another network managed by the same individual, this time located in the UK and named *HOST TELECOM LTD* (**AS214238**).[36] Based on the pictures posted on his *Instagram* account (*figure 16*), his proxy businesses seem to have been quite successful.

[33] *https://i-cyprus.com/company/614368*

[34] *https://bgp.he.net/AS44559#_peers*

[35] *https://krebsonsecurity.com/2024/05/stark-industries-solutions-an-iron-hammer-in-the-cloud/*

[36] *https://bgp.he.net/AS214238#_prefixes*

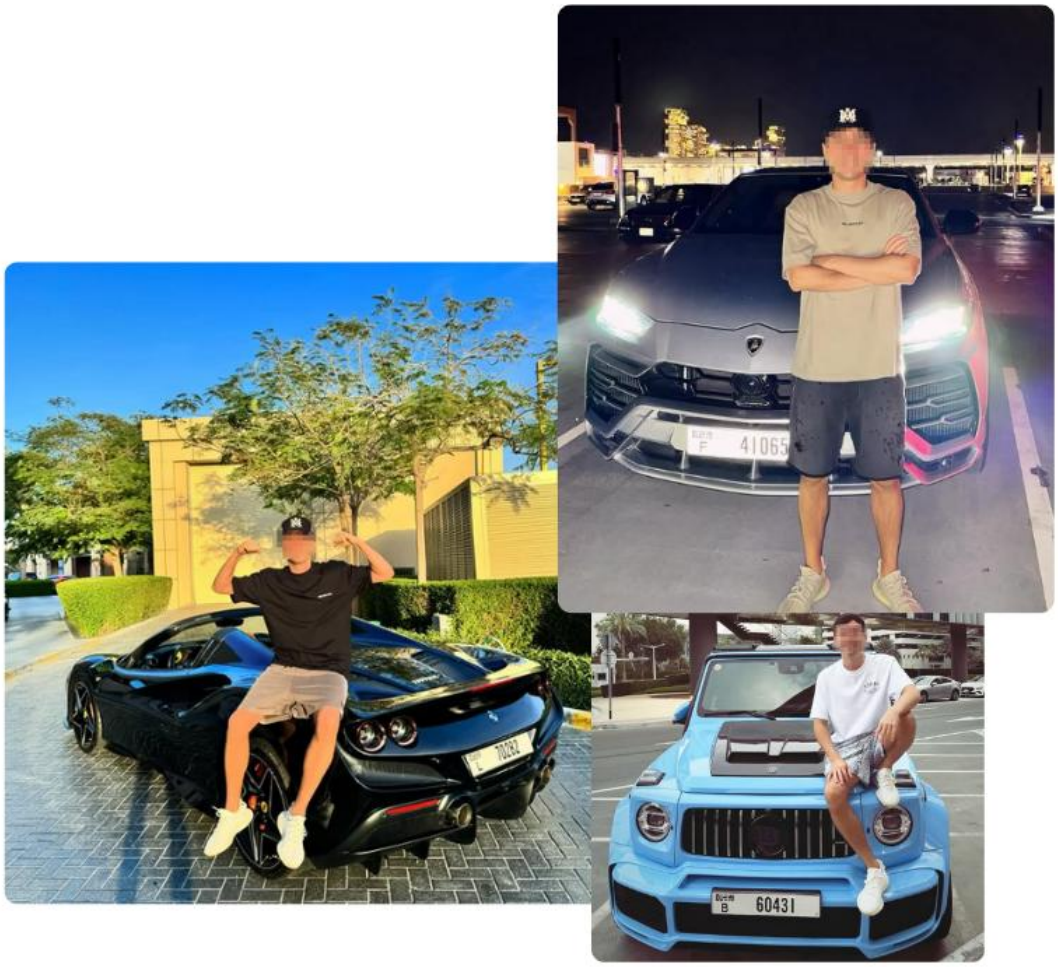


*Figure 16. Pictures of the administrator of Proxyline. Source: Instagram.*

His company IT HOSTLINE LTD has been providing IPv4 prefixes to other abusive networks based in Russia. For example, *GLOBAL INTERNET SOLUTIONS LLC* – **AS207713** (also known as **GIR**) and *GLOBAL CONNECTIVITY SOLUTIONS LLP (AS215540)*, two front companies used the bulletproof hosting provider "**4vps.su**". Both networks are often used by Russian state sponsored intrusion sets such as **Gamaredon** (UAC-0010),[37]**Doppelgänger**,[38]**NoName057(16)** (DDoSia project),[39] and both **UAC-0050** and **UAC-0006**, as we previously reported in February 2025.[40] Additionally, the owner of these networks has been linked to ransomware operations in the past.[41]

[37] *https://www.rnbo.gov.ua/files/2023_YEAR/CYBERCENTER/Gamaredon_activity.pdf*

[38] *https://www.qurium.org/alerts/exposing-the-evil-empire-of-doppelganger-disinformation/*

[39] *https://blog.sekoia.io/noname05716-ddosia-project-2024-updates-and-behavioural-shifts/*

[40] Intrinsec "*From espionage to PsyOps: Tracking operations and infrastructure of UACs in 2025".* March 2025.

[41] *https://medium.com/@danchodanchev/dancho-danchevs-round-up-of-russia-based-high-profile-ransomware-cybercriminals-ed1bf5a38b8f*

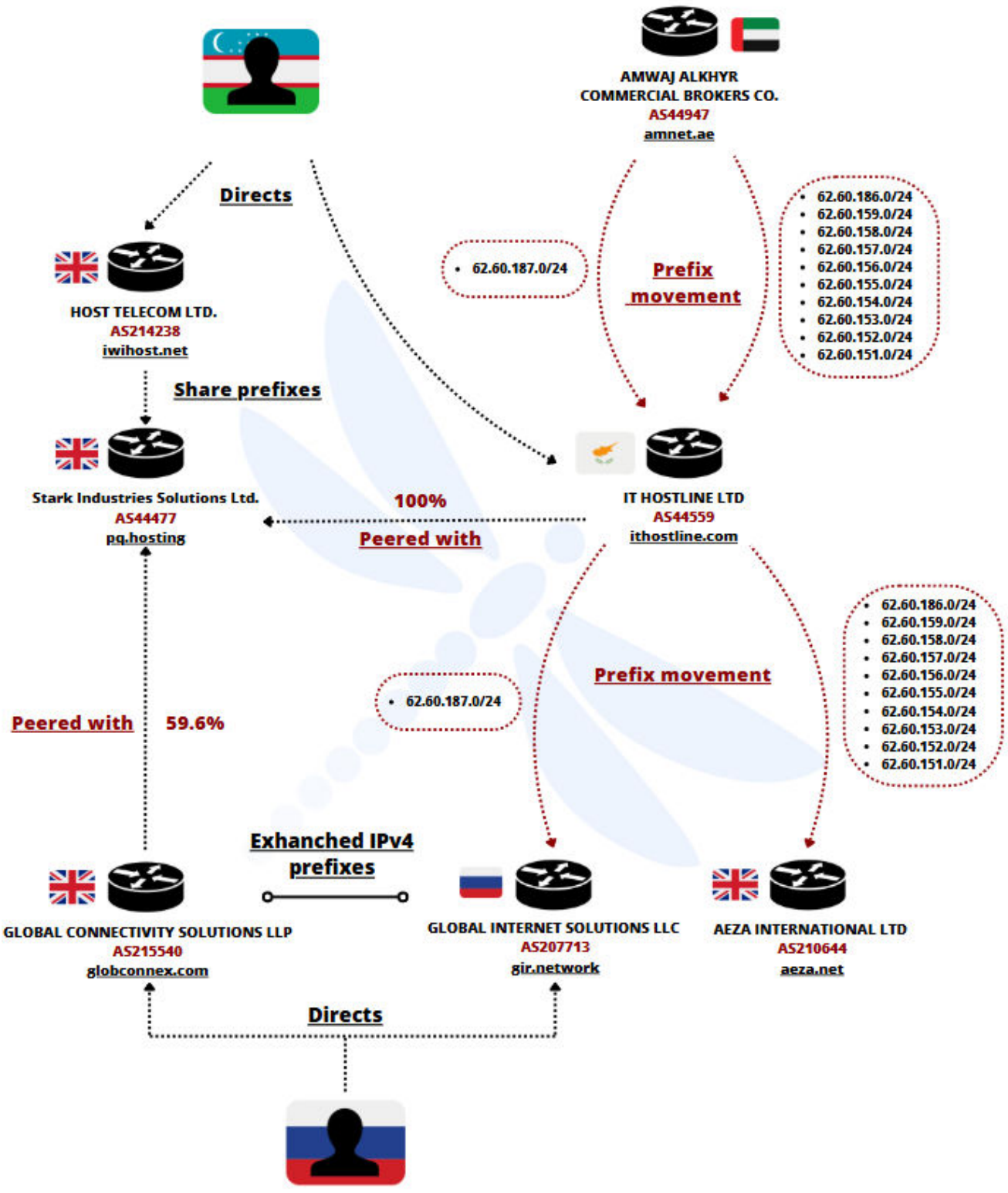



*Figure 17. Layout of the links that could be established between the above-mentioned individuals and autonomous systems.*

# 4. Conclusion

Networks displaying high levels of spam and malicious network activities overall can sometimes be the tree hiding the forest. With only a couple of IP prefixes, the quantity of attacks they emit can sometimes **surpass** the ones launched from regular ISPs abused by malicious clients.
**Tracking their network infrastructure** and relations to other entities represent a **key element** to **anticipate future threats and intrusion sets** that will most certainly **use these bulletproof hosting providers for their operations**.
Due to the vast quantity of malicious networks like these, blocklists operated by trusted sources such as Spamhaus tend to present **holes in their nets**, some of them managing to evade being added to the list. This implies that security analysts must **actively monitor network movements** related to those infrastructure to **detect rebrands** in different offshore locations through new shell companies.
Overall, blocking bulletproof networks is crucial to prevent against **initial access attempts** operated through phishing or compromised exposed assets by **ransomware operators** or **IABs** in general that could have been **brute forced** or **scanned** using these networks.

# 5. Actionable content

## 5.1. Indicators of compromise

| Value | Type | Description |
|---|---|---|
| 209605 | ASN | *UAB Host Baltic* |
| 214295 | ASN | *SKYNET NETWORK LTD* |
| 213790 | ASN | *Limited Network LTD* |
| 215476 | ASN | *Inside Network LTD* |
| 204428 | ASN | *SS-Net* |
| 47890 | ASN | *UNMANAGED LTD* |
| 202325 | ASN | *4Media Ltd.* |
| 50360 | ASN | *Tamatiya EOOD* |
| 202425 | ASN | *IP Volume Inc* |
| 215930 | ASN | *CIPHER OPERATIONS DOO BEOGRAD - NOVI BEOGRAD* |
| 215540 | ASN | *GLOBAL CONNECTIVITY SOLUTIONS LLP* |
| 207713 | ASN | *GLOBAL INTERNET SOLUTIONS LLC* |

## 5.2. Recommendations

- Monitor all traffic from/to any IP address belonging to above-mentioned autonomous systems and organisations.
- Incorporate the IOCs from this report into your Threat Intelligence platform and/or communicate them to your SOC to anticipate and detect these threats.

# 6. Appendices

## 6.1. Spamhaus blocked ASNs

| ASN | AS name | Blocked by spamhaus |
|---|---|---|
| 209605 | *UAB Host Baltic* | Yes |
| 214295 | *SKYNET NETWORK LTD* | Yes |
| 215240 | *Silent Connection Ltd.* | Yes |
| 215476 | *Inside Network LTD* | Yes |
| 204428 | *SS-Net* | Yes |
| 202325 | *4Media Ltd.* | No |
| 50360 | *Tamatiya EOOD* | No |
| 47890 | *UNMANAGED LTD* | No |
| 202425 | *IP Volume Inc* | Yes |
| 215930 | *CIPHER OPERATIONS DOO BEOGRAD - NOVI BEOGRAD* | Yes |
| 213790 | *Limited Network LTD* | No |
| 215540 | *GLOBAL CONNECTIVITY SOLUTIONS LLP* | No |
| 207713 | *GLOBAL INTERNET SOLUTIONS LLC* | No |

*Source:* Spamhaus

# 7. Sources


- *https://www.ripe.net/ripe/mail/archives/anti-abuse-wg/2023-November/006519.html*
- *https://x.com/sansmotdepasse/status/1897102089618383112*
- *https://x.com/banthisguy9349/status/1783401854925210002*
- *https://www.ripe.net/media/documents/BGP_hijacking_brief_guide_on_protecting_BGP_from_bad_actors_b117eaf3-243d-4a95_xjDDZAc.pdf*
- *https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/*
- *https://medium.com/bugs-that-bite/bthoster-please-stop-this-ip-address-f8e9dcdf7c51*
- *https://krebsonsecurity.com/2024/05/stark-industries-solutions-an-iron-hammer-in-the-cloud/*
- *https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-003.pdf*
- *https://www.qurium.org/alerts/exposing-the-evil-empire-of-doppelganger-disinformation/*
- *https://www.rnbo.gov.ua/files/2023_YEAR/CYBERCENTER/Gamaredon_activity.pdf*
- *https://www.esentire.com/blog/nitrogen-campaign-2-0-reloads-with-enhanced-capabilities-leading-to-alphv-blackcat-ransomware*