INTRINSEC

Innovative by design

VAIZ, FDN3, TK-NET: A nebula of Ukrainian networks engaged in brute force and password spraying attacks

Cyber Threat Intelligence

August 2025

@Intrinsec @Intrinsec Blog Website

Table of contents

1. Key findings

- Between June and July 2025, Ukraine-based autonomous system **FDN3 – AS211736**, allocated by the entity *FOP Dmytro Nedilskyi*, was used to launch multiple hundreds of thousands of brute force and **password spraying attacks** against **SSL VPN** and **RDP** devices, over a period of up to three days.

- We believe with a high level of confidence that *FDN3* is part of a **wider abusive infrastructure** composed of two other Ukrainian networks, ***VAIZ-AS*** (AS61432) and ***ERISHENNYA-ASN*** (AS210950), and a Seychelles based autonomous system named ***TK-NET*** (AS210848). Those were all allocated in August 2021 and often exchange IPv4 prefixes with one another to **evade blocklisting** and continue hosting abusive activities.

- Strong partnership and ramifications with other criminal entities could be established. This includes **Ecatel**'s front network in Seychelles "*IP Volume Inc.*" (AS202425), used as the main transit provider for most of the autonomous that compose this abusive infrastructure and also used to launch the same types of attacks at the same period through prefixes rented by *VAIZ-AS*. There is also ***Virtualine***, a bulletproof hosting solution managing a network registered in the United States, *KPROHOST LLC* (AS214940), which **exchanged prefixes** with *FDN3*.

- Despite being reannounced by a new network, the prefixes continue to emit the same type and high levels of attacks. It may means that a **common administrator** could be operating all the networks while also moving them to **evade blocklisting** and **attribution**.

2. Introduction

In a private report released in May 2025, we described how a group of multiple networks allocated in August 2021 and based in Ukraine and Seychelles were used for a common motive of **spam emission**, **network attacks** and **malware command-and-control hosting**.[1] Thus the entire infrastructure, composed of **AS61432**, **AS210848**, and **AS210950**, was added to Spamhaus' blocklist.

Later in June, some of the IPv4 prefixes announced by those abusive networks, and more specifically by *TK-NET* (AS210848), were moved to a **Ukrainian** autonomous system created at the **same time** in August 2021 and named *FDN3* (AS211736). This network's configuration is **highly similar** to *TK-NET*, where all prefixes are routed by *IP Volume Inc* (AS202425), an autonomous system managed by the unfamous **abusive hosting provider** *Ecatel*.[2] Smaller links with other criminal entities operating in bulletproof hosting solutions were also discovered.

The attacks originating from these prefixes continued right after being announced by *FDN3*. Consisting of massive **brute force** and **password spraying** campaigns launched simultaneously through various

[1] Intrinsec tactical report. "*VAIZ PARTNER & E-RISHENNYA: Ukrainian networks emitting aggressive scans through shell companies*". May 2025.

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

IPs against exposed **SSL VPN** and **RDP** assets. The peak of some of those attacks could last over a period of up to three days.

Password spraying

As a reminder, a password spraying attack attempts to access a large volume of accounts with a few commonly used passwords. By contrast, brute force attacks attempt to gain unauthorized access to a single account by guessing the password – often using large lists of potential passwords.[3]

Ransomware-as-a-Service organisations such as the newly created "*GLOBAL GROUP*" continue to **heavily rely on these techniques** to gain initial accesses on corporate networks, as reported by *EclecticIQ* in a recent report from July 15, stating: "*The actor [GLOBAL GROUP] shows clear interest in brute-forcing or exploiting enterprise VPN appliances (Fortinet, Palo Alto, Cisco), aiming to gain initial entry at the network perimeter […] these enable high-privilege initial access and rapid ransomware deployment, often bypassing traditional EDR solutions."*[4]

Earlier in March, the same editor reported on ***Black Basta***'s activities, another ransomware group engaged in bruteforce and password spraying attacks through a custom framework named BRUTED, stating: "*The BRUTED framework target various remote-access and VPN solutions […] to gain initial access to victim networks*."[5] The IPs hosting the framework were all announced by *Proton66* (AS198953), a Russian bulletproof hosting solution that we widely covered in a report released in November 2024.[6]

Along those finds, the *DFIR Report* released on June 30th details of an intrusion that occurred in late November 2024, in which a threat actor operating for the ransomware group "*Ransomhub*" gained a foothold in the target's network through a "*password spray attack against an exposed RDP server*".[7]

[3] *https://www.kaspersky.com/resource-center/definitions/what-is-password-spraying*

[4] *https://blog.eclecticiq.com/global-group-emerging-ransomware-as-a-service*

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

[6] *Intrinsec tactical threat report. "PROSPERO & Proton66: Uncovering the links between bulletproof networks". November 2024.*

[7] *https://thedfirreport.com/2025/06/30/hide-your-rdp-password-spray-leads-to-ransomhub-deployment/*

3. TOV VAIZ PARTNER and E-RISHENNYA

The first company, "***TOV VAIZ PARTNER***", allocated its own autonomous system **AS61432** in May 2021. It currently announces a single prefix: **185.156.72**[.]**0/24**. The servers seem to currently be sold on the website "ntup[.]net".

The second company, "***TOV E-RISHENNYA***", allocated its autonomous system **AS210950** three months later, in August 2021. It used two announces two prefixes: **45.143.201**[.]**0/24** and **185.193.89**[.]**0/24**. Both networks are listed on Spamhaus' blocklist.[8]

Despite having their own autonomous systems, a major part of their prefixes are announced on a Seychelles-based autonomous system named *Telkom Internet LTD* - **210848**, allocated at the same time, in August 2021.[9] This network shares all its peering agreements with *IP Volume Inc.* – **202425**, a company based in Seychelles and created by **Ecatel**'s owners, infamous for running an extensively abusive bulletproof hosting service in the Netherlands since 2005.[10]

IP Volume Inc. | Ecatel

Considered "*one of [The Netherlands']most criticized hosting businesses*" according to The New York Times[11], 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.[12]

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**.[13]

In addition to IP Volume Inc, Ecatel's directors created another company in the Netherlands named "*FiberXpress BV*"[14], 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.[15]

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*.

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

[9] *https://bgp.tools/as/210848*

[10] *https://www.nrc.nl/nieuws/2021/04/02/the-cesspool-of-the-internet-is-to-be-found-in-a-village-in-north-holland-a4038369*

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

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

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

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

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

The table below summarizes all the prefixes announced by the two organisations. Despite having sometimes different registrant names, they all share a common abuse contact address: "erishennya.res@gmail[.]com" (ACRO41012-RIPE).[16]

IPv4 prefix	Company	ASN
185.156.73[.]0/24	*TOV E-RISHENNYA*	210848
185.156.74[.]0/24	*TOV VAIZ PARTNER*	210848
185.193.88[.]0/24	*TOV E-RISHENNYA*	210848
31.43.191[.]0/24	*FOP Dmytro Nedilskyi*	210848
92.63.197[.]0/24	*Korotkij Denis Aleksandrovich*	210848
92.63.196[.]0/24	*TOV VAIZ PARTNER*	202425
185.156.72[.]0/24	*TOV VAIZ PARTNER*	61432
45.143.201[.]0/24	*Vitaliy Khnykin*	200195

Source: Hurricane Electric.

Since March 2025, *E-RISHENNYA*'s autonomous system AS210950, moved all its prefixes to known abusive and bulletproof networks. **185.193.89**[.]**0/24** is now announced by *GLOBAL CONNECTIVITY SOLUTIONS LLP* – **AS215540**, an AS based in the UK but managed by the same Russian individual as gir.network (AS207713). We have already investigated this AS regarding its use by Russian intrusions sets such as **UAC-0050**, **UAC-0006** and **UAC-0010** (Gamaredon).[17] The other prefix, **45.143.201**[.]**0/24**, is now announced by *Verasel, Inc.* – **AS2100195**, an autonomous systems based in Seychelles partially routed by *IP Volume inc.* – **AS20425**.[18] This specific prefix used to also be announced by *TOV VAIZ PARTNER* -AS61432 until November 2021.

The current registrant of the prefix now announced by *Verasel Inc.* is the same name as an older and now offline network based in Russia named *IP Khnykin Vitaliy Yakovlevich* – **AS44636**. It used to announce prefix **185.156.72**[.]**0/24**, now announced by *TOV VAIZ PARTNER* (*cf. figure 1*). It could therefore indicate that this Russian entity could still be operating despite deallocating its autonomous system.

[16] *https://apps.db.ripe.net/db-web-ui/lookup?source=ripe&key=ORG-VP68-RIPE&type=organisation*

[17] *https://www.intrinsec.com/wp-content/uploads/2025/03/TLP-CLEAR-From-espionage-to-PsyOps-Tracking-operations-and-infrastructure-of-UACs-in-2025-EN-1.pdf*

[18] *https://bgp.he.net/AS200195#_asinfo*

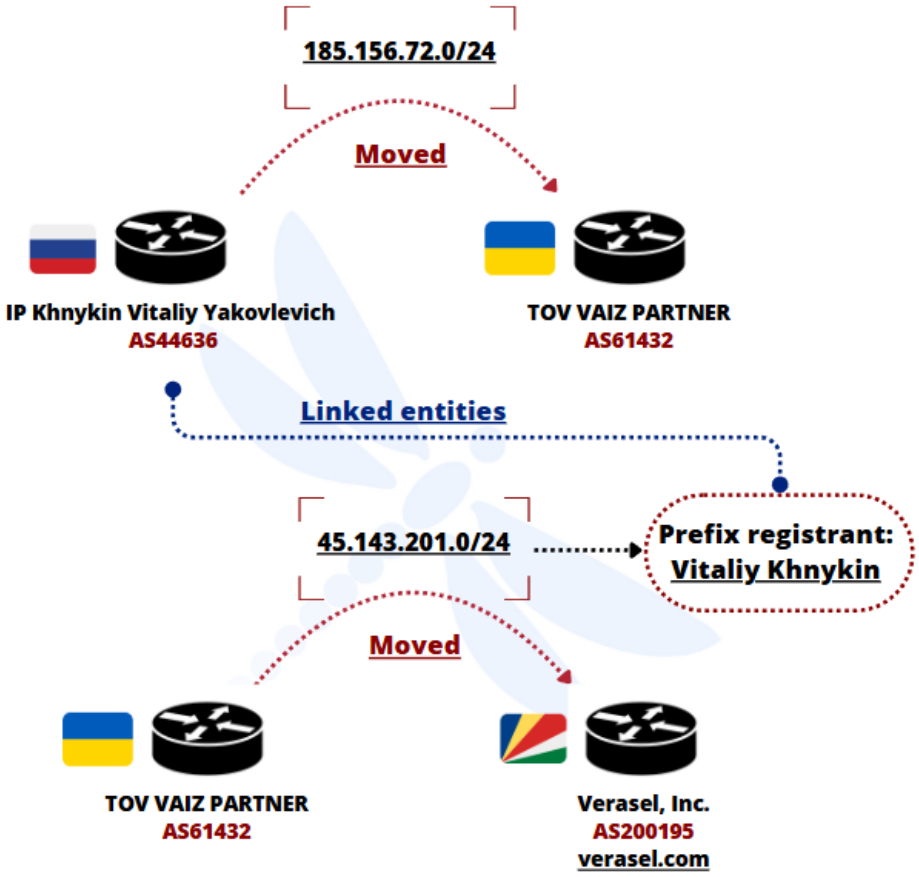

Figure 1. Layout summarizing the links shared between the above-mentioned entities.

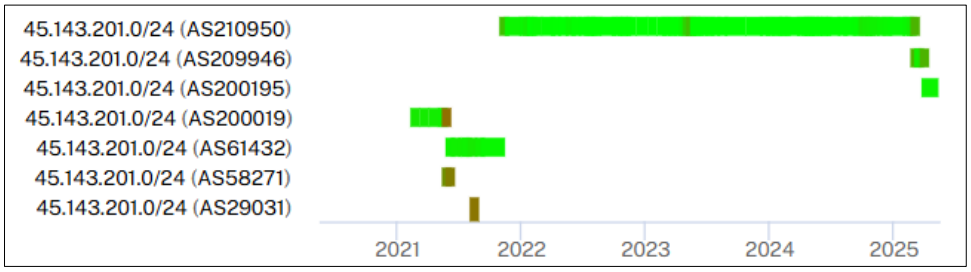

Figure 2. Timeline of autonomous systems that once announced prefix 45.143.201[.]0/24. Source: RIPEstat.

Overall, the entirety of prefixes that were moved from these two Ukrainian companies' autonomous systems are now announced by bulletproof and abusive networks fronted by shell companies (*cf. figure 3*).

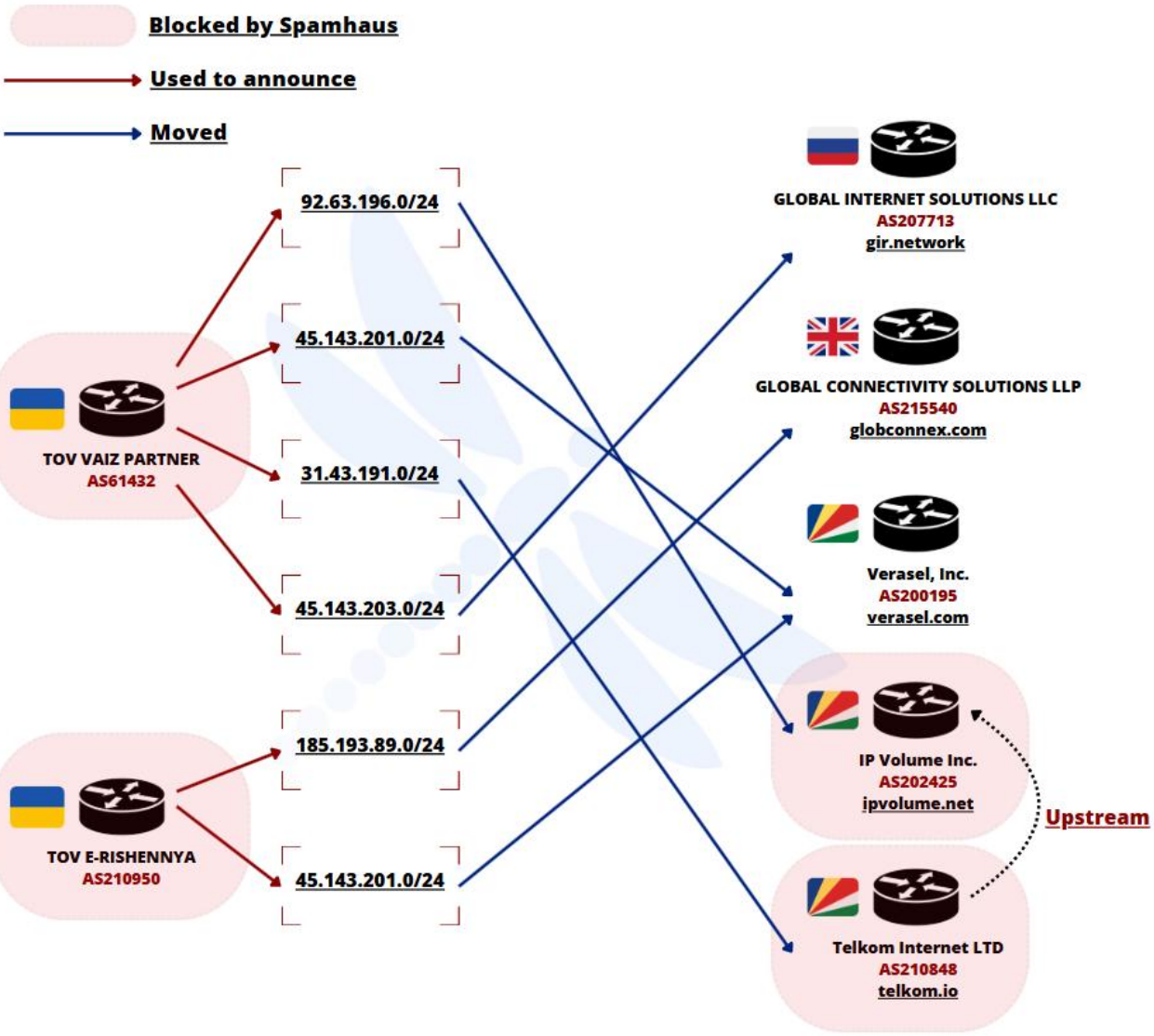

Figure 3. Layout of the prefixes movements that originated from AS61432 and AS210950.

In a tweet from July 2021, user "*@bad_packets*" mentions that "*All prefixes formerly announced by AS47981, are now routed through AS61432 [TOV VAIZ PARTNER]*", and that "*all traffic from these netblocks [45.143.203[.]0/24]*" should be blocked.[19] Inducing that even the previous announcer of that prefix was already using it for malicious intents. The tweet also indicates that *TOV VAIZ PARTNER* was located in Russia in 2021, before being reallocated to Ukraine (*cf. figure 4*).[20]

2021-07-08T15:15:08+00:00	VAIZ-AS ITBks892, RU
2022-12-01T14:15:37+00:00	VAIZ-AS ITBks892, UA

Figure 4. BGP update for AS61432.

[19] *https://x.com/bad_packets/status/1419898419385016320*

[20] *https://bgpranking.circl.lu/asn*

Regarding the network that previously announced the prefix, *Romanenko Stanislav Sergeevich* - **AS47981** (FOPSERVER, UA), it was described it as the network that launched the most attacks in April 2021, based on an intelligence report released by RedPiranha.[21] Those attacks came only three months before AS47981 moved its prefix to *TOV VAIZ PARTNER*.

3.1. Older Russian network, SibirInvest

Three of the prefixes announced by *Telkom Internet LTD*, and one by *TOV VAIZ PARTNER*, were previously announced by another Russian network, *SibirInvest OOO* – **AS44446**. Again in 2021, "*@bad_packets*" mentioned in a tweet to "*drop all traffic from AS44446 [SibirInvest]*". Interestingly, as for *Telkom Internet LTD*, this network shared all its peering agreements with *IP Volume Inc.* – **AS202425**. The front company created in Seychelles by Ecatel's owners to pursue their bulletproof hosting activities through an offshore and untraceable entity. (*cf. chapter 3.*).[22] [23]

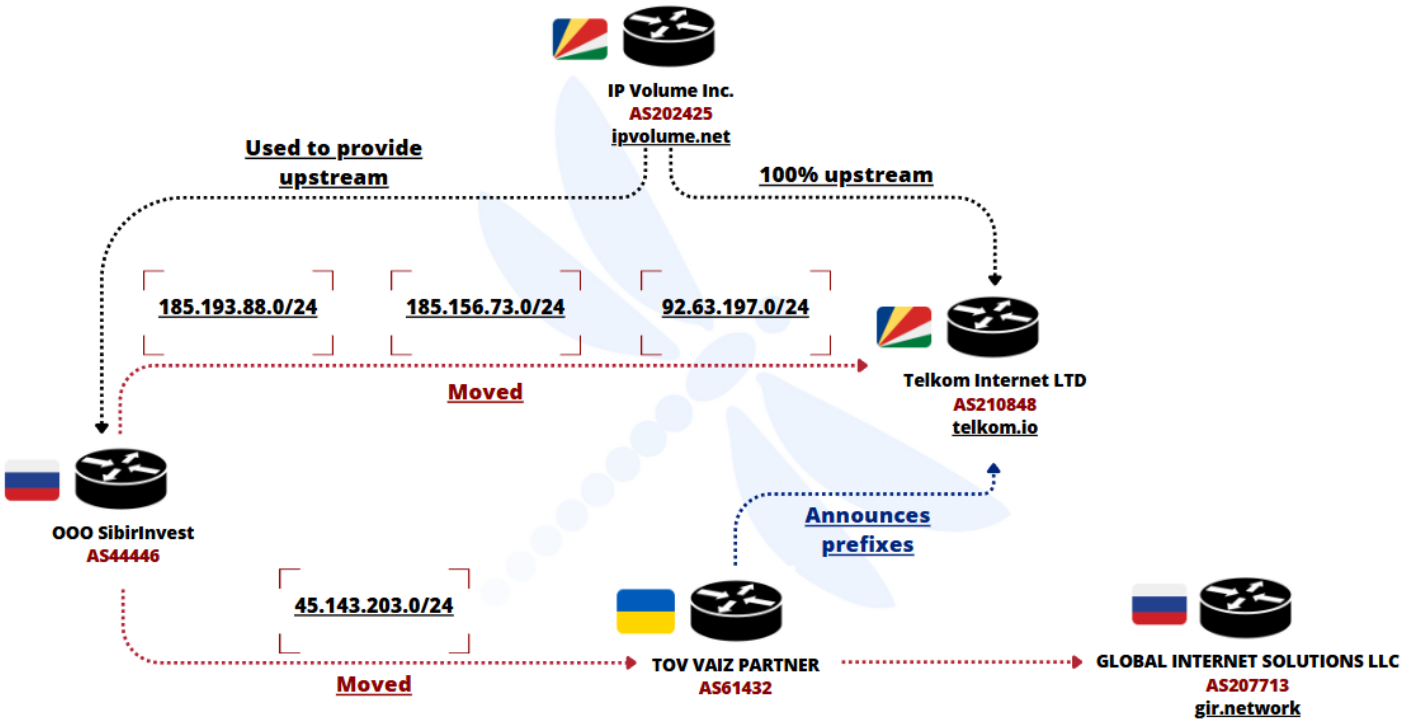

Figure 5. Layout of IPv4 prefixes movements originating from AS44446 and the links shared between each entities.

[21] *https://redpiranha.net/news/threat-intelligence-report-12th-april-18th-april-2021*

[22] *https://x.com/GoldenCSO/status/1494064524453896195*

[23] *https://community.ipfire.org/t/finding-out-what-an-attacker-aims-at/5687*

3.2. Russian registrant, ITDELUXE

All prefixes share a common registrant: ORG-VP68-RIPE[24], maintained by "ITDELUXE-MNT", a Russian company based in Novosibirsk. The email account of the owner, a certain Igor Vorozhtsov, notably created an account on the underground forum *Exploit*—leading to the hypothesis that his presence on the forum was **not fortuitous**.

Despite being moved to new autonomous systems, the prefix would still display those information.[25]

```
organisation:    ORG-VP68-RIPE
org-name:        TOV VAIZ PARTNER
country:         UA
org-type:        OTHER
address:         KIEV, ADAMA MIRKEVICHA 9-22
e-mail:          erishennya.res@gmail[.]com
e-mail:          d64897768@gmail[.]com
abuse-c:         ACRO41012-RIPE
mnt-ref:         ITDELUXE-MNT
mnt-by:          ITDELUXE-MNT
created:         2021-05-08T18:11:03Z
last-modified:   2024-08-02T03:40:14Z
source:          RIPE
```

```
mntner:          ITDELUXE-MNT
descr:           Maintainer for IT DELUXE objects
admin-c:         IV568-RIPE
tech-c:          IV568-RIPE
upd-to:          vigorv@mail[.]ru
mnt-nfy:         vigorv@mail[.]ru
auth:            PGPKEY-C396EEA0
auth:            SSO# Filtered
auth:            SSO# Filtered
auth:            SSO# Filtered
auth:            MD5-PW# Filtered
mnt-by:          ITDELUXE-MNT
created:         2008-01-17T14:43:00Z
last-modified:   2016-06-16T11:50:11Z
source:          RIPE# Filtered
```

Additionally, an *as-set* of the same name "AS-ITDELUXE" was created in 2016 with a unique member being a Russian autonomous system: **AS44636**[26]**.** This network used to announce prefix **185.156.72**[.]**0/24**, now announced by *TOV VAIZ PARTNER* – **AS61432**. At that time, this previous network was already using the prefix for spamming purposes. A tweet from October 2020, posted by @bgpstream, notably declares that the prefix was hijacked by NTSERVICE-AS, the upstream of *TOV VAIZ PARTNER*.[27]

[24] *https://apps.db.ripe.net/db-web-ui/lookup?source=ripe&key=ORG-VP68-RIPE&type=organisation*

[25] *https://bgp.he.net/net/45.143.203.0/24#_rdap*

[26] *https://bgp.he.net/irr/as-set/AS-ITDELUXE*

[27] *https://x.com/bgpstream/status/1312233834084212737*

3.3. Network spam stats

3.3.1. Telkom Internet LTD

As we previously mentioned, the main autonomous system announcing most of the prefix owned by those two Ukrainian companies is an autonomous system based in Seychelles named *Telkom Internet LTD* – AS210848, routed by *IP Volume Inc.* – AS202425.

In early April 2025, our various honeypots recorded a total of 27,831 network attacks emitted by IPs announced by AS210848. The following table lists the IPs that were most noisy.

Source IP	Count
92.63.197[.]145	7,110
92.63.197[.]236	7,050
185.193.88[.]223	2,735
185.193.88[.]178	2,535
185.193.88[.]229	2,327
92.63.197[.]210	2,236
92.63.197[.]167	2,050
185.156.73[.]222	1,725

Source: Intrinsec.

As one can notice on the following chart (*cf. figure 6*), the peak of attacks lasted for about a week (from the 6th of April to the 12th).

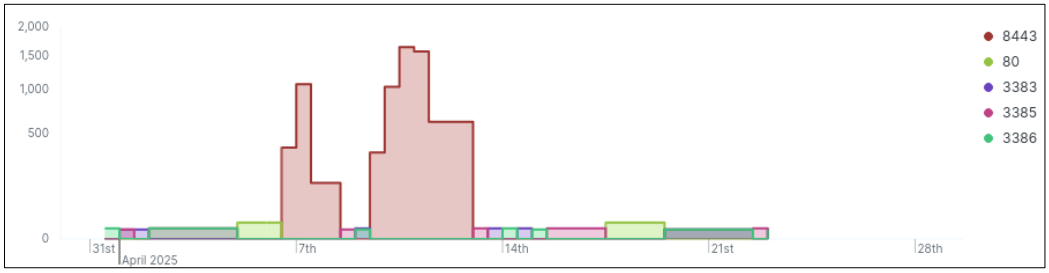

Figure 6. Chart of the number of attacks that targeted our honeypots, distributed by destination port and originating from AS210848 in April 2025.

The same could be observed through SANS' honeypot's metrics. In early May (May 4th), out of the 10 IPs that most hit SANS' honeypot on port 5555, seven were announced by either *TOV E-RISHENNYA* (185.193.88[.]0/24) or *TOV VAIZ PARTNER* (92.63.196[.]0/24). Those attacks also lasted for around a week.

Source IP	AS	Count
185.193.88[.]229	*Telkom Internet LTD* – AS210848	36,777
185.193.88[.]178	*Telkom Internet LTD* – AS210848	34,094
92.63.196[.]152	*IP Volume inc* – AS202425	32,652
185.193.88[.]223	*Telkom Internet LTD* – AS210848	32,341
92.63.196[.]179	*IP Volume inc* – AS202425	32,202
80.82.65[.]127	*IP Volume inc* – AS202425	28,571
92.63.196[.]249	*IP Volume inc* – AS202425	14,833
92.63.196[.]251	*IP Volume inc* – AS202425	7,583

Source: SANS Technology Institute.

3.3.2. IP Volume Inc, Ecatel

IP Volume Inc., the network enabling all of this malicious traffic by routing the prefixes announced by AS210848, and by also directly announcing IPs for both Ukrainian companies, is well known by our service for operating such activities. In a recent investigation on **BtHoster**, a bulletproof hosting service that manages two autonomous systems: *Skynet Network Ltd* - **AS214295**, and *Inside Network LTD* - **AS215476**, we notably described how Skynet Network shared 51% of its peering agreements with *IP Volume Inc*[28]. A clear sign that threat actors tend to easily create internet connectivity partnerships with *Ecatel*'s offshore company.

For example, in April 2025, **420,516 network attacks** emitted by *IP Volume Inc.* were recorded on our various honeypots. They all came from a common prefix: **89.248.163**[.]**0/24**, managed by a sketchy organisation "recyber[.]net", that declares on its website to be a "*project [that] assists researchers, universities and other educational instutions*." Nonetheless, in 2022, Radware already described the organization as "*anonymous*", "*non-communicative*" and therefore could not be confirm as benign.[29]

Source IP	Count
89.248.163[.]145	24,426
89.248.163[.]139	24,290
89.248.163[.]157	24,270
89.248.163[.]162	24,200
89.248.163[.]134	24,056
89.248.163[.]152	24,043
89.248.163[.]160	23,857
89.248.163[.]163	23,849
89.248.163[.]148	23,773
89.248.163[.]171	23,752

Source: Intrinsec.

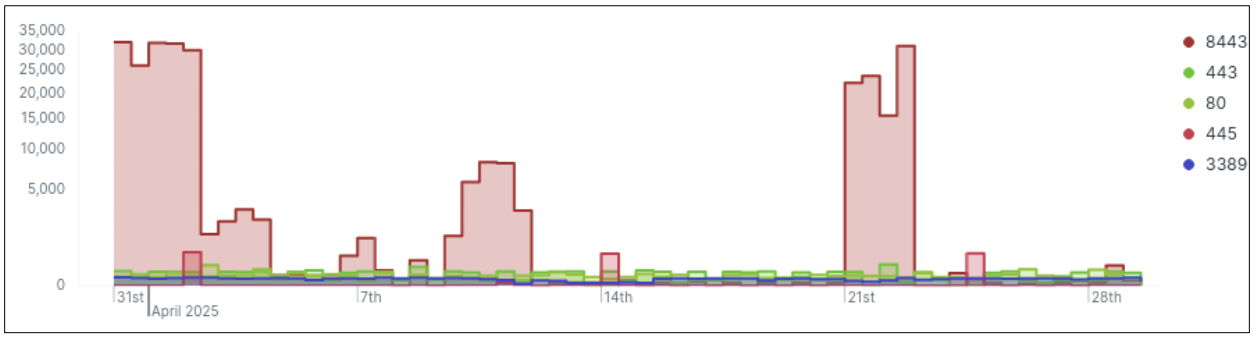

Figure 7. Chart of the number of attacks that targeted our honeypots, distributed by destination port and originating from AS202425 in April 2025.

[28] Intrinsec private report. "*BtHoster networks: Identifying noisy ISPs emitting high levels of malicious traffic*". March 2025.

[29] *https://www.radware.com/security/ddos-threats-attacks/threat-advisories-attack-reports/internet-noise-is-taxing-online-services-and-businesses/*

4. FDN3, FOP Dmytro Nedilskyi

Last but not least, allocated in August 2021 under AS number 211736, *FDN3* now announces four IPv4 prefixes, totalling **1,024** unique IPs. So far, neither the network nor its prefixes are present in Spamhaus' blocklist.

IPv4 prefix	Description
185.156.73[.]0/24	*TOV E-RISHENNYA*
31.43.185[.]0/24	*FOP Dmytro Nedilskyi*
88.210.63[.]0/24	*FOP Dmytro Nedilskyi*
92.63.197[.]0/24	*Korotkij Denis Aleksandrovich*

Source: Hurricane Electric.

As mentioned in the introduction, the network got recently activated, as three out of four prefixes were announced on June 18, 2025 (*cf. figure 1*).

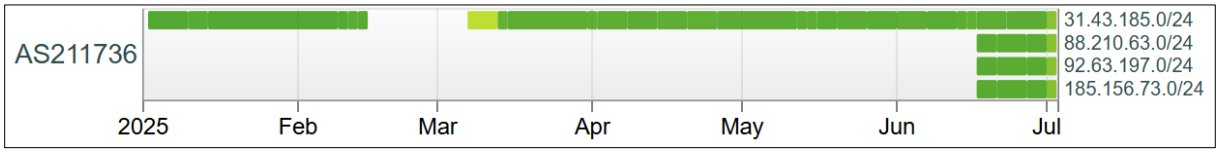

Figure 8. Timeline of IPv4 prefixes announced by AS211736.

4.1. Connections with Virtualine's shell networks

One of those recently acquired prefix, **88.210.63**[.]**0/24**, was indeed used for brute force and password spraying operations on VPN assets during a campaign that lasted **three days**, from July 6 to July 8, with **1,332,374** hits recorded on our honeypots (*cf. figure 2*).

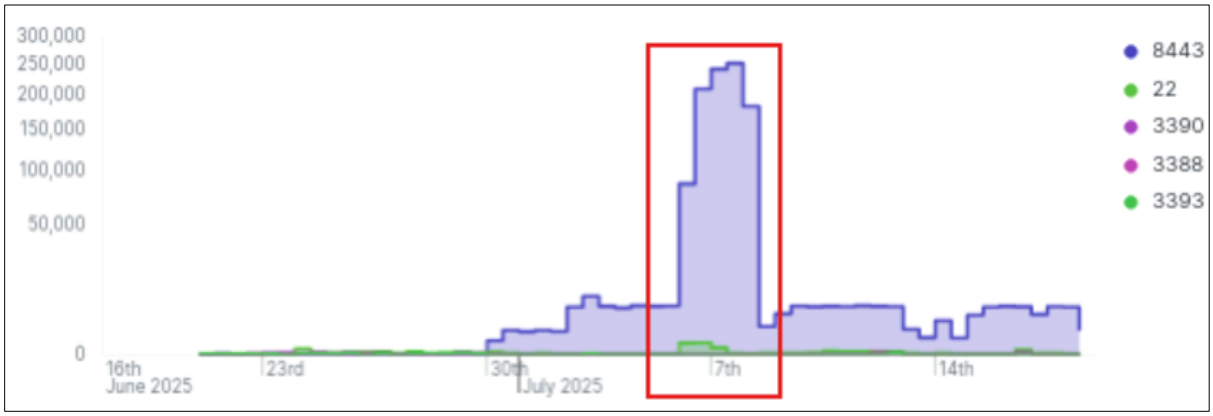

Figure 9. Chart of the number of attacks that targeted our honeypots, distributed by destination port and originating from AS211736, between June and July 2025.

As observed in the table below, we recorded around the same number of attacks for each IPs that were used in the attack, hinting they were precisely activated at the same time. This data can be corroborated with observations made by reporters regarding those IPs in this timeline on *AbuseIPDB*.[30]

[30] *https://www.abuseipdb.com/check-block/88.210.63.0/24*

The majority being related to SSL VPN and RDP bruteforce and password spraying attempts like we saw.[31]

Source IP	Count
88.210.63[.]21	113,406
88.210.63[.]28	111,081
88.210.63[.]23	110,527
88.210.63[.]24	110,354
88.210.63[.]29	109,954
88.210.63[.]25	109,915
88.210.63[.]27	109,551
88.210.63[.]22	109,064
88.210.63[.]26	108,762
88.210.63[.]30	108,634

Source: Intrinsec.

This specific prefix was previously announced by *KRPOHOST LLC* – AS214940, an abusive autonomous system based in the United States part of the infrastructure of shell networks managed by bulletproof hosting provider ***Virtualine***.

Virtualine

KPROHOST LLC (AS214940) and *Railnet LLC* (AS214943) are two US-based companies that both allocated their autonomous systems in May 2024, later added to Spamhaus' blocklist for the abusive content they host. In addition, they share prefixes and get routed by the same sketchy upstream providers like *Pfcloud UG* - AS51396 (*cf. figure 3*).

They are used as the legal front for a **bulletproof hosting provider** named "**Virtualine**". This service is advertised on the usual Russian-speaking forums such as *XSS* or *Exploit*. On those forums, Virtualine's administrator does not hesitate to explain to other users that their network can be used for illegal activities such as **phishing**, **carding**, **mail spam**, and **port scanning**. *KPROHOST LLC* is indeed often used to send hundreds of malspam campaigns, host malware C2s, and phishing pages.[32]

Similarly, *Railnet LLC* notably served as a favoured solution for **Russia-aligned intrusion sets** such as **UAC-0050** and **UAC-0006**, by hosting **Smokeloader** and other malware C2 used for their **hybrid operations** against **Ukraine** and its **allies**.[33]

Furthermore, they share a common legal registered agent, *Whitelabel Networks, LLC,* based in **Israel** and owned by a certain Daniel Mishayev.[34] Interestingly, five other autonomous systems related to *Whitelabel Networks LLC* are present in Spamhaus' blocklist, AS213828, AS213992, 215460, AS215436 and AS214497.[35]

[31] *https://www.abuseipdb.com/check/88.210.63.21*

[32] Intrinsec private report. "*Review of recent malspam campaigns launched through a newly born network*". December 2024.

[33] Intrinsec tactical threat report. "*From espionage to PsyOps: Tracking operations and bulletproof providers of UACs in 2025*". March 2025.

[34] *https://kyprofile.com/company/1360765*

[35] *https://x.com/spamhaus/status/1901992907680178453*

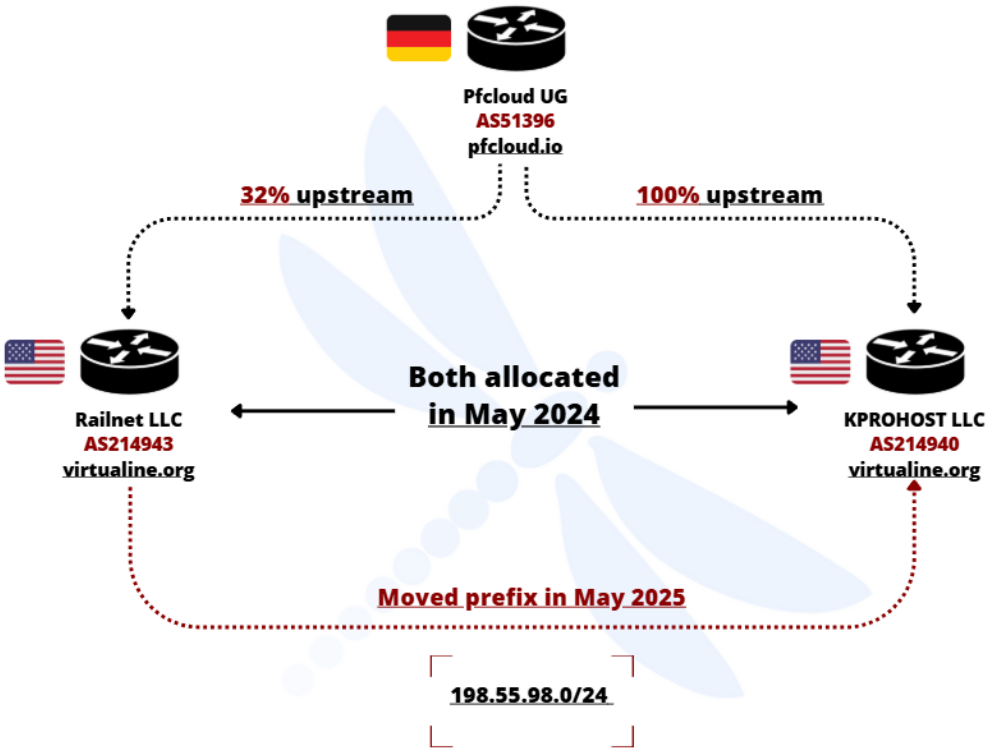

Figure 10. Layout of elements shared between AS214943 and AS214940.

Railnet is the current upstream provider[36] of a Turkish bulletproof hosting provider named *VSVK Onderhoud B.V.* - AS213511.[37] In April 2025, Spamhaus discovered the autonomous system's name to be usurped from a legitimate Dutch company of the same name.[38] This manipulation was orchestrated to use the front of a pre-existing real company in order to look less suspicious.

Interestingly, *Railnet* was previously routed by two legitimate Turkish networks, AS214466 and AS48678, the same providers as AS213511, before moving to *Aurologic* – AS30823, and *Pfcloud UG* – AS51396, two transit providers that tend to overlook the activities hosted by the networks they agree to peer with.[39] Additionally, those previous connections with Turkish entities could make us believe with a medium level of confidence that like AS213511, the administrator behind this bulletproof hosting service could be Turkish.

[36] *https://bgp.he.net/AS213511#_peers*

[37] *https://check.spamhaus.org/results/?query=SBL681135*

[38] *https://x.com/spamhaus/status/1914643262360465417*

[39] *https://check.spamhaus.org/sbl/listings/aurologic.com/*

4.2. Continuing the spam, TK-NET

The two other prefixes that *FDN3* announced in June, **92.63.197**[.]**0/24** and **185.156.73**[.]**0/24**, were previously announced by yet another abusive network named *Telkom Internet LTD* (TK-NET) – AS210848, also created in August 2021 and based in Seychelles. It currently announces three /24 prefixes for three distinctive abusive Ukrainian networks, *TOV VAIZ PARTNER* (AS61432),[40] *TOV E-RISHENNYA* (AS210950), and of course, *FOP Dmytro Nedilskyi* (*FDN3* - AS211736).[41] In a previous investigation released in May 2025, we described their relationships and the malicious traffic they emit.[42]

Back when they were announced by *TK-NET*, the prefixes were already used to operate the same type of attacks, composed of brute force and password spraying like we currently see, but also malware command-and-control hosting and phishing pages. Shortly after being announced by *FDN3*, they resumed on hosting and emitting the same type of malicious activities (*cf. figure 4*).

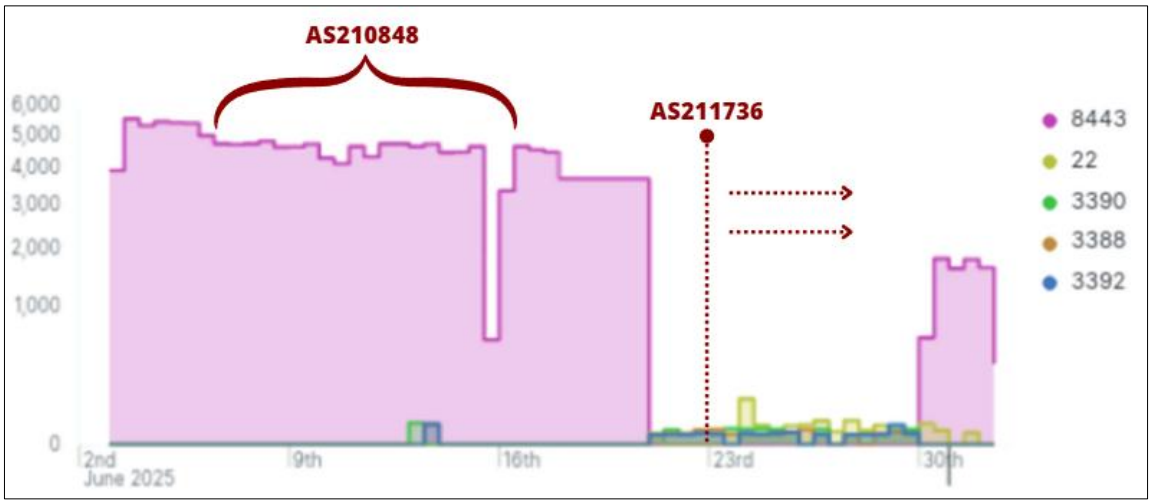

Figure 11. Chart of the number of attacks that targeted our honeypots, distributed by destination port and originating from prefixes announced first by AS210848 and after by AS211736, between June and July 2025.

TK-NET shares similarities with FDN3 (*cf. figure 5*). Both were created in August 2021, shared prefixes, and get entirely routed by IP Volume Inc. - AS202425, the front company based in Seychelles used by *Ecatel*'s creators.[43]

[40] *https://check.spamhaus.org/results/?query=SBL648356*

[41] *https://bgp.he.net/AS210848#_prefixes*

[42] Intrinsec tactical threat report. "*VAIZ PARTNER & E-RISHENNYA: Ukrainian networks emitting aggressive scans through shell companies*". May 2025.

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

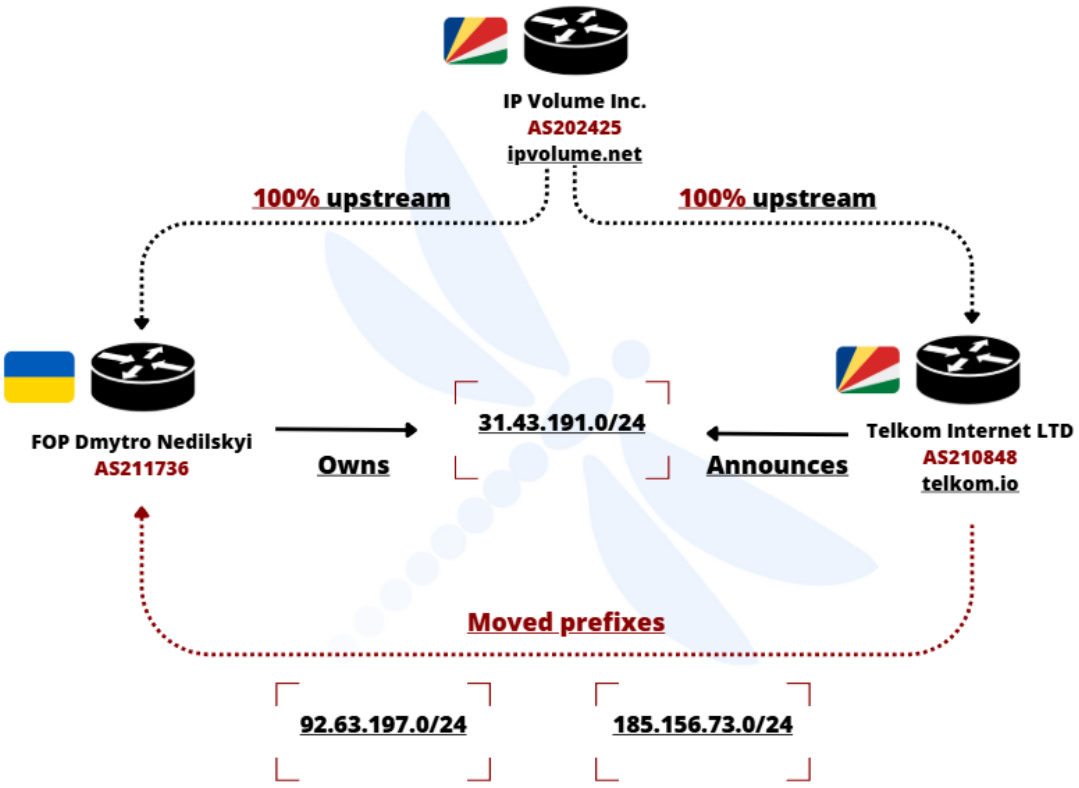

Figure 12. Layout of network elements shared between FDN3 - AS211736 and TK-NET - AS210848.

All those strong similarities, including their configuration, the content they host, and their creation date, led us to assess with a high level of confidence the previously mentioned autonomous systems to be operated by a common bulletproof hosting administrator (*cf. figure. 6*).

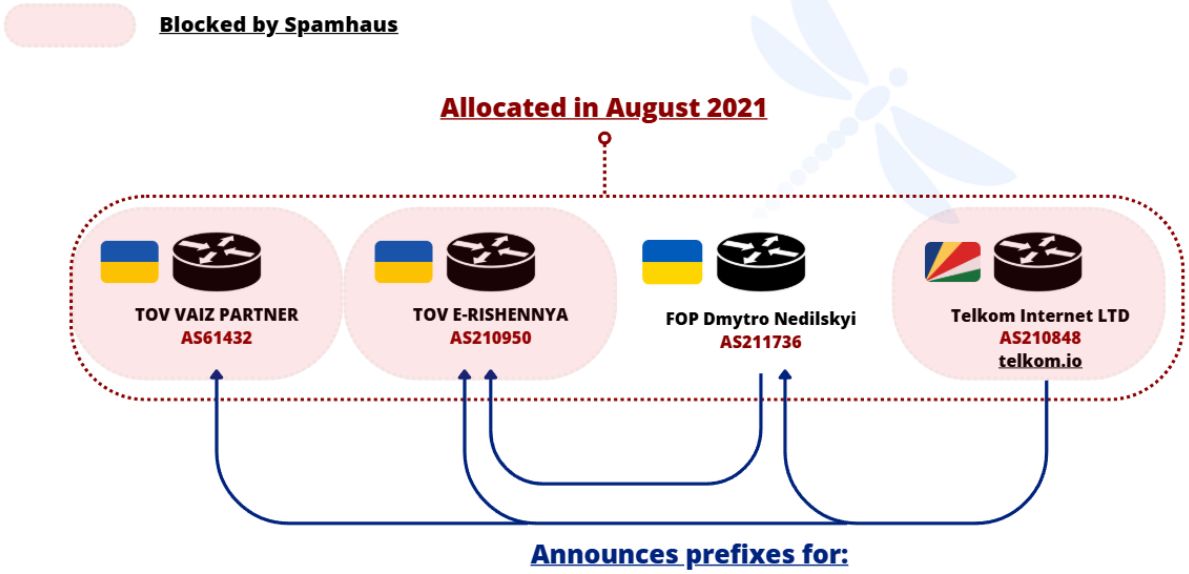

Figure 13. Layout of networks elements shared between FDN3 - AS211736, and TK-NET - AS210848.

4.3. Maintained by Alex Host

According to *FDN3*'s Whois information, the maintainer of the network "ORG-FDN3-RIPE", is a certain "ru-alexgroup-1-MNT".[44] The RIPE lookup for this maintainer links to their website, "kvmka[.]ru",[45] linked to the Russian company "*Alex Host LLC*" (ООО "АЛЕКС ГРУПП"). In an investigation released in July 2024 by *Qurium*, a Swedish NGO specialised in digital forensic, they highlighted how *Alex Host* had previously maintained other bulletproof hosting providers like *TNSECURITY* in late July 2023, notably used at the time to host Doppelganger's infrastructure.[46] Connections with such networks again leaves little doubts on the nature of this present infrastructure.

Registrant
In the WHOIS information for an autonomous system, the field "*mnt-by*" refers to the entity responsible for maintaining the registration information. "*mnt-by*" stands for "maintained by" and indicates the maintainer object, which could be an individual or organization authorized to make changes to the record in the database. This ensures that only authorized users can update the information related to the autonomous system.[47]

- organisation: **ORG-FDN3-RIPE**
- org-name: FOP Dmytro Nedilskyi
- country: UA
- org-type: OTHER
- descr: FOP Dmytro Nedilskyi
- address: Ukraine, Dnipro, st. Odynkivska, build. 25
- phone: +380635062303
- admin-c: DN4442-RIPE
- tech-c: DN4442-RIPE
- abuse-c: AR62526-RIPE
- mnt-by: FDN3-MNT
- mnt-ref: FDN3-MNT
- mnt-ref: **ru-alexgroup-1-MNT**
- created: 2021-01-12T19:51:05Z
- last-modified: 2022-12-01T16:25:35Z
- source: RIPE # Filtered

- mntner: **ru-alexgroup-1-MNT**
- descr: Startup maintainer
- admin-c: AF16214-RIPE
- tech-c: AF16214-RIPE
- upd-to: **abuse@kvmka[.]ru**
- auth: SSO# Filtered
- auth: SSO# Filtered
- mnt-by: ru-alexgroup-1-MNT
- created: 2020-12-09T11:01:37Z
- last-modified: 2024-04-22T08:45:15Z
- source: RIPE# Filtered

[44] *https://bgp.he.net/AS211736#_whois*
[45] *https://apps.db.ripe.net/db-web-ui/lookup?source=ripe&key=ru-alexgroup-1-MNT&type=mntner*
[46] *https://www.qurium.org/alerts/exposing-the-evil-empire-of-doppelganger-disinformation/*
[47] *https://docs.db.ripe.net/entire-documentation-HTML.html*

5. Korotkij Denis Aleksandrovich

5.1. Bulgarian spam networks, ROZA-AS

Back on prefix 92.63.197[.]0/24, that was moved from *TK-NET* to *FDN3* in late June, the registered entity displayed is another Ukrainian name:" *Korotkij Denis Aleksandrovich".* This name could be found in the description of an older prefix, 45.143.200[.]0/24, announced at the time by *ROZA-AS* (AS212283),[48] a Bulgarian autonomous system deemed malicious by *Spamhaus*. It then moved to *GCS-AS* (AS215540), a known Russian bulletproof hosting provider.[49] Such movements highlight the actor's tendencies to look for abusive networks to host its prefixes, enabling the continuity of their malicious activities.

5.1.1. SS-Net

Regarding *ROZA-AS*' nature, and its connections with other criminal networks, prefixes like 83.222.190[.]0/24 and 83.222.191[.]0/24, were moved in early 2025 to *SS-Net* (AS204428), a Bulgarian front network administrated by **4Vendeta**, yet another abusive entity operating in the bulletproof hosting business. In a previous investigation that we publicly released in May 2025, we notably described how those Bulgarians networks could be linked to **Bthoster**, a BPH provider advertised on Russian-speaking underground forums.[50]

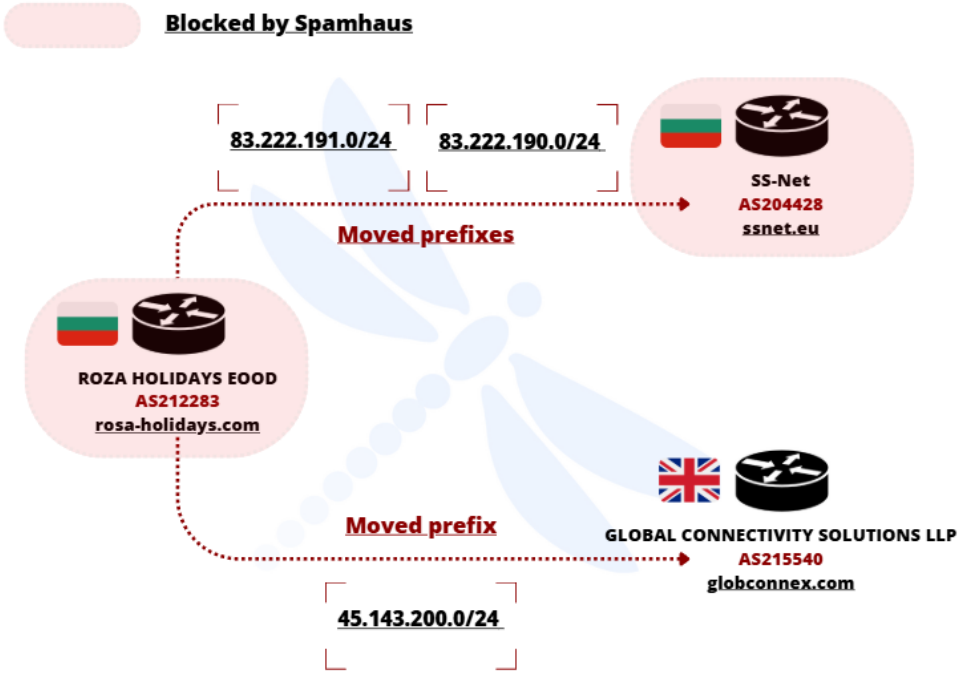

Figure 14. Layout of network elements shared between the above-mentioned entities.

[48] *https://www.pdflibr.com/AS212283*

[49] Intrinsec tactical threat report. "*From espionage to PsyOps: Tracking operations and bulletproof providers of UACs in 2025*". March 2025.

[50] Intrinsec tactical threat report. "*BtHoster: Identifying noisy networks emitting malicious traffic through masscan servers*". May 2025.

Those two prefixes continue to be used for password spraying and bruteforce purposes on RDP assets. The following table provides the number of hits that were recorded on our honeypots and emitted from those IP ranges, between June 7 and July 7, 2025.

Source IP	Count
83.222.191[.]178	55,284
83.222.191[.]130	12,937
83.222.190[.]190	11,668
83.222.191[.]42	8,308
83.222.191[.]150	4,003
83.222.191[.]94	3,996

Source: Intrinsec.

6. Amadey hosting

In addition to extensive abusing scans and bruteforce, a trove of command-and-control panels for **Amadey**, a malware sold on Russian-speaking underground forums that acts as both a loader and a stealer, could be found on the related networks.

Amadey C2	ASN	Active bots recorded
185.156.72[.]61	61432	*Offline*
185.156.72[.]96	61432	126
185.156.72[.]97	61432	122
185.156.72[.]89	48693	*Offline*
176.46.157[.]60	215310	*Offline*
31.43.185[.]30	211736	*Offline*
66.63.187[.]111	214943	3 (2,818 offlines)
94.154.35[.]25	214943	79
45.141.233[.]196	214943	64
213.209.150[.]166	214943	43

7. Conclusion

This investigation once again highlights a common phenomenon of offshore ISPs such as *IP Volume Inc.* **enabling smaller bulletproof networks through peering agreements and prefix hosting** overall. Thanks to their offshore location such as Seychelles, which provides anonymity to the owners of those companies, the malicious activities perpetrated though those networks cannot be directly imputed to them. We can be led to believe that such opaque montages will continue to be created and prosper in the long run if the jurisdiction of those locations keeps on covering those entities.

Furthermore, we described how **abusive networks could easily rebrand and evade** traces of their previous activities by **creating new autonomous systems and shell companies** on which their previous prefixes would be transferred. This demonstrates again the importance of contextualising and mapping those networks to get a better overview of their infrastructure in order to efficiently block them. Gathering blocklists provided by trusted sources such as Spamhaus constitutes a strong first step to deal with that matter.

Completely cutting communications with such networks can prevent from initial access attempts through scanned exposed assets and bruteforce attempts, command-and-control communications, or being exposed to phishing pages hosted on those ISPs.

8. Actionable content

8.1. Indicators of compromise

Value	Type	Description
210848	ASN	*Telkom Internet LTD*
202425	ASN	*IP Volume inc*
61432	ASN	*TOV VAIZ PARTNER*
210950	ASN	*TOV E-RISHENNYA*
211736	ASN	*FOP Dmytro Nedilskyi*
185.156.72[.]96	IPv4	Amadey C2
185.156.72[.]196	IPv4	Amadey C2
185.156.72[.]39	IPv4	Amadey C2
31.43.185[.]33	IPv4	Brute force / password spraying
31.43.185[.]38	IPv4	Brute force / password spraying
31.43.185[.]67	IPv4	Brute force / password spraying
31.43.185[.]4	IPv4	Brute force / password spraying
31.43.185[.]89	IPv4	Brute force / password spraying
31.43.185[.]41	IPv4	Brute force / password spraying
185.156.73[.]154	IPv4	Brute force / password spraying
92.63.197[.]236	IPv4	Brute force / password spraying
92.63.197[.]77	IPv4	Brute force / password spraying
92.63.197[.]79	IPv4	Brute force / password spraying
92.63.197[.]23	IPv4	Brute force / password spraying
185.156.73[.]67	IPv4	Brute force / password spraying
83.222.191[.]178	IPv4	Brute force / password spraying
83.222.191[.]130	IPv4	Brute force / password spraying
83.222.190[.]190	IPv4	Brute force / password spraying
83.222.191[.]42	IPv4	Brute force / password spraying
83.222.191[.]150	IPv4	Brute force / password spraying
83.222.191[.]94	IPv4	Brute force / password spraying
88.210.63[.]21	IPv4	Brute force / password spraying
88.210.63[.]28	IPv4	Brute force / password spraying
88.210.63[.]23	IPv4	Brute force / password spraying
88.210.63[.]24	IPv4	Brute force / password spraying
88.210.63[.]29	IPv4	Brute force / password spraying
88.210.63[.]25	IPv4	Brute force / password spraying
88.210.63[.]27	IPv4	Brute force / password spraying
88.210.63[.]22	IPv4	Brute force / password spraying
88.210.63[.]26	IPv4	Brute force / password spraying
88.210.63[.]30	IPv4	Brute force / password spraying
88.210.63[.]63	IPv4	Brute force / password spraying
88.210.63[.]88	IPv4	Brute force / password spraying
88.210.63[.]2	IPv4	Brute force / password spraying
88.210.63[.]3	IPv4	Brute force / password spraying

88.210.63[.]4	IPv4	Brute force / password spraying
88.210.63[.]7	IPv4	Brute force / password spraying
88.210.63[.]8	IPv4	Brute force / password spraying
88.210.63[.]9	IPv4	Brute force / password spraying
88.210.63[.]10	IPv4	Brute force / password spraying
88.210.63[.]11	IPv4	Brute force / password spraying
88.210.63[.]12	IPv4	Brute force / password spraying
88.210.63[.]16	IPv4	Brute force / password spraying
88.210.63[.]17	IPv4	Brute force / password spraying
88.210.63[.]18	IPv4	Brute force / password spraying

8.2. Recommendations

- Monitor and block all traffic from/to any IP address announced by the above-mentioned autonomous systems and organisations.
- Consider implementing the block-lists provided by Spamhaus regarding malicious networks and prefixes they detect:
    - *https://www.spamhaus.org/drop/drop.txt*
    - *https://www.spamhaus.org/drop/asndrop.json*

9. Sources

- *https://www.nrc.nl/nieuws/2021/04/02/the-cesspool-of-the-internet-is-to-be-found-in-a-village-in-north-holland-a4038369*
- *https://nl.wikipedia.org/wiki/IP_Volume*
- *https://www.intrinsec.com/wp-content/uploads/2025/03/TLP-CLEAR-From-espionage-to-PsyOps-Tracking-operations-and-infrastructure-of-UACs-in-2025-EN-1.pdf*
- *https://www.qurium.org/alerts/exposing-the-evil-empire-of-doppelganger-disinformation/*
- *https://thedfirreport.com/2025/06/30/hide-your-rdp-password-spray-leads-to-ransomhub-deployment/*
- *https://blog.eclecticiq.com/global-group-emerging-ransomware-as-a-service*
- *https://blog.eclecticiq.com/inside-bruted-black-basta-raas-members-used-automated-brute-forcing-framework-to-target-edge-network-devices*