Shadow syndicate infrastructure illumination

Cyber Threat Intelligence

July 2025

@Intr @Intrinsec Blog Website

Table of contents

1. Key findings

We found a new heuristic allowing us to keep tracking the attack infrastructure of the infamous ShadowSyndicate known to leverage a wide range of top-tier Ransomware-as-service.

- ShadowSyndicate used the same Secure Shell (SSH) fingerprint on many servers (138 at the time of writing). It matches a previous TTP reported by GroupIB in September 2023
- ShadowSyndicate works with numerous ransomware groups and affiliates of ransomware programs including RansomHub
- We found connections between ShadowSyndicate infrastructure and Cl0p/Truebot substantiating previous findings of GroupIB
- We found connections between ShadowSyndicate infrastructure and Citrix Bleed attack infrastructure that spread Lockbit ransomware
- We assess with moderate confidence that ShadowSyndicate has access to a network of private bulletproof hosters (BPHs) in Europe that exhibit traits of Intelligence Agencies hosting (IAH)
- The global resilience against takedowns is ensured via a high level of imbrication of those BPHs, registered in offshore jurisdiction, spanning different countries but operated from Russia. We found links of interests with the Kremlin for some of them
- BPHs are blurring lines by appearing as VDS | VPS | VPN | (residential) proxy platforms and even sometimes an additional obfuscation layer via a DDOS protection provider
- With lower confidence, we found a hack and leak operation targeting Hunter Biden, the son of the former President of the United States, seeking to influence 2024 presidential elections. The goal is to weaken representative governments perceived as democracies and weaken unaligned candidates with the Kremlin's interests. Using proxies such as ransomware programs and/or an IAB shields from prosecution in return for "plausible deniability for state-backed cyber operations
- We found connections between ShadowSyndicate infrastructure and Amos Stealer infrastructure (moderate confidence) as well as though with lower confidence, with ToneShell backdoor

As of this writing, the attack infrastructure remains active, with threat actors continuously scanning for vulnerabilities and distributing new malicious payloads to victims.

We would like to express our sincere appreciation for our collaboration with Group-IB, for their peer reviewing, insightful discussions, and valuable contributions. The opportunity to cross-correlate data using their telemetry has been especially valuable, enabling us to validate findings and enhance the overall accuracy and depth of our analysis. This partnership underscores the importance of collective intelligence in tackling today's complex threat landscape.

N.B. Names of persons and organisations within this presentation are included for completeness. No implication of guilt or association should be implied.

2. Introduction

ShadowSyndicate (aka Infra Storm GroupIB) is a recent intrusion set reportedly active since July 2022. It has demonstrated the use of multiple top tier **Ransomware-as-a-Service** (RaaS) brands such as **AlphaV/Blackcat, Lockbit, Play, Royal, Cl0p, Cactus and Ransomhub**. **GroupIB** in 2023 conjectured that **ShadowSyndicate** is more likely a **new Ransomware-as-a-Service** (RaaS) affiliate rather than an **Initial access broker** (IAB).

Overlaps were also found with **TrickBot**, **Ryuk/Conti, FIN7**, and TrueBot (also known as Silence.Downloader) malware operations (linked to the **Silence group** overlapping **infamous Russian intrusion set Evil Corp** directed by **FSB** to conduct cyberespionage against NATO allies).

3. Infrastructure analysis

The investigation started from the sharing of two scanning ips from a trusted circle (91.238.181.225 and 5.188.86.]169). We rapidly found that **both ips shared the same SSH key**, which triggered this investigation. Shodan (b5:4c:ce:68:9e:91:39:e8:24:b6:e5:1a:84:a7:a1:03) provided at that time 47 matching servers with this fingerprint while Fofa collected even a higher number of related servers (143 or **136 after data deduplication**).

After we pivoted on each of them, we now present the results of our investigations.

3.1. Overlaps with tracked intrusion sets

We have detected that ShadowSyndicate attack infrastructure does overlap with other tracked infrastructures belonging to:

- Top tier ransomware ecosystem
  - Lockbit V3.0 Citrix bleed campaign [**moderate overlap**]
  - Cl0p/Evilcorp/Truebot [**moderate overlap**]
  - Cicada3301 [**weak overlap**]
  - Black Basta [**weak overlap**]
- Fake homebrew [**strong overlap**]
- DecoyDog (PuppyRAT with C2 over DNS) [**weak overlap**]
- Foreign Information Manipulation and Interference (FIMI) [**weak overlap**]

3.1.1. Lockbit 3.0 attack campaigns on Citrix Bleed

As far as Lockbit last known attack infrastructure upon the well-known **Citrix bleed campaign** is concerned we found such commonalities that we'd like to highlight.

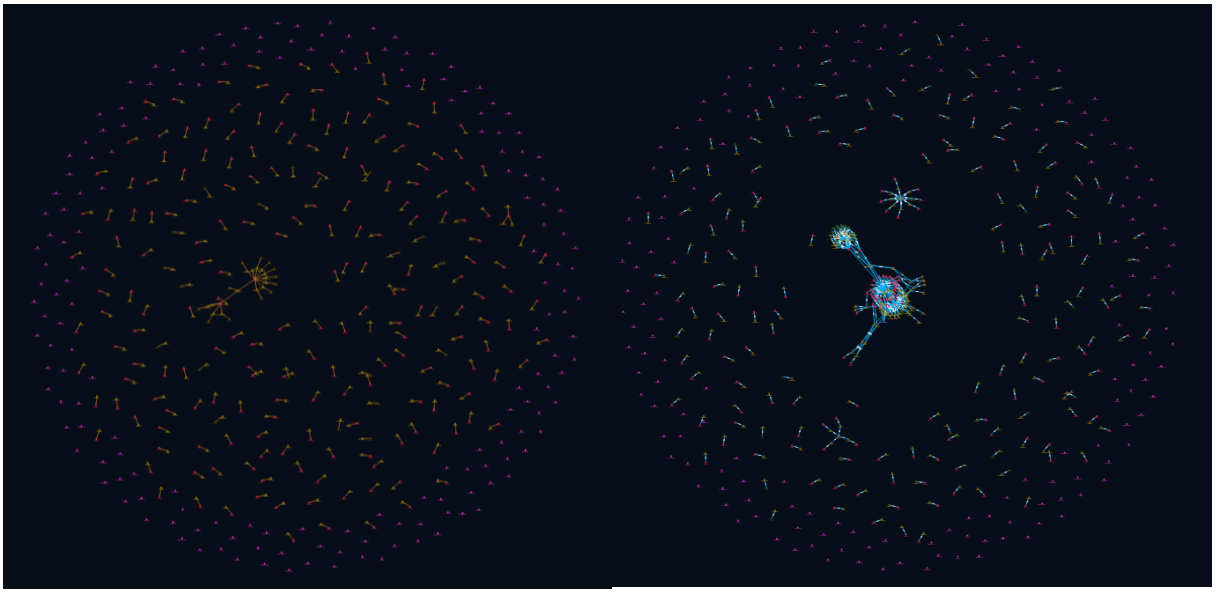


*Figure 1. Left: attack infrastructure before enrichment and cross-correlation with our intel database in Opencti. Right: after cross-correlation and analysis. Lockbit 3.0 attack infrastructure allowed Ransomware Affiliates to exploit **CVE 2023–4966 Citrix Bleed** Vulnerability and encrypt a wide range of victims around October 2023.*

In the figure above one can see an overlap with known entities in our Opencti database with the **offensive framework Cobalt strike**. A stronger overlap is encountered with **ShadowSyndicate** intrusion sets and its two known SSH cryptographic keys.

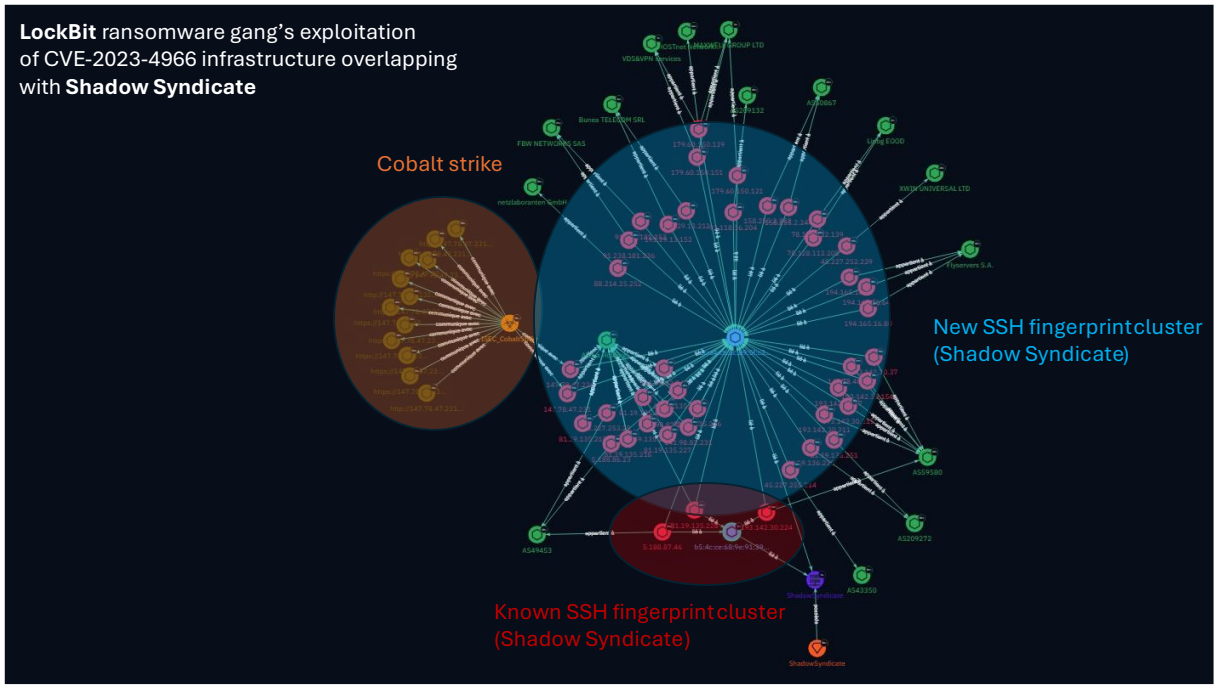


Figure 2 A moderate overlap of about forty IP addresses is encountered between Citrix Bleed attack campaign and ShadowSyndicate infrastructure that we track via two SSH cryptographic keys.

For two IPs of the **ShadowSyndicate infrastructure**, we found **Cobalt strike beacons at the same timeframe** that were linked to **the Citrix bleed exploit attack campaign** where **Lockbit ransomware** was chiefly deployed by affiliates(but also **Threeam**).

- 147.78.47[.]226 26/12/2023 to 28/12/2023 & 147.78.47.231 15/10/2023 28/12/2023
  - 1580103824
    - **UAC-0056** (aka: Bleeding Bear, DEV-0586, EMBER BEAR, FROZENVISTA, Lorec Bear, Lorec53, Nascent Ursa, Nodaria, Saint Bear, Storm-0587, TA471, UNC2589, Cadet Blizzard). **GRU affiliated actor** conducting **cyberespionage-sabotage operations against Ukraine/Georgia since 2021** (whispergate, Free civilian defacements, …).
    - **ShadowSyndicate**
    - **Cl0p ransomware** (targeting Cleo secure file sharing for business)**.** This campaign aligns with known TTPs of the infamous Russian intrusion set Evil Corp. The latter is likely directed by FSB to conduct cyberespionage against NATO allies. Evilcorp is known to have breached in early 2023 hundreds of entity with a supply chain attack exploiting flaws in the **MOVEit file sharing tool**
    - Blacksuit ransomware as reported on December 2023 by DFIR report. See our previous report (3am in the ransoming, 4eeb0f78-29fb-496a-964b-1bab21f962c3) explaining that Zeon ransomware became Royal and, even more recently, Blacksuit, which worked (still works?) with Evilcorp via Baddie.
  - 391144938 9/12/2023-26/12/2023
    - 2024: GroupIB associated this watermark with a specific server JARM to Hsharada servers. HsHarada ransomware exploited proxyshell vuln escalation privileges. This attack campaign targets healthcare and healthcare-adjacent organizations. According to CISA (Feb 2025) the operator of this ransomware does not exfiltrate data and rotate their ransomware executable payloads with names including Ghost, Cring, Crypt3r, Phantom, Strike, Hello, Wickrme, Rapture and HsHarada. TTPs and victimology is in line with **UAC-0056** (low confidence).
    - Aug 2023: China-nexus threat actors reported by:
      - SentinelOne (BRONZE STARLIGHT). BRONZE STARLIGHT also known as DEV-0401 or SLIME34) is a suspected Chinese 'ransomware' group whose main goal appears to be espionage rather than financial gain, though using ransomware as means for distraction or misattribution (*e.g.,* Lockbit 2.0 in April 2022)
      - Recorded Future (RedHotel). Red Hotel (aka Earth Lusca) overlap also with another campaign where threat actors exploited multiple CVEs against **zimbra Collaboration Suite** (reported by the CISA on early 2023)

This finding is substantiated by *"a strong connection between **LockBit** and the previously reported **ShadowSyndicate**"* published by Joshua Penny, Michael Koczwara. Their report published around November 2023 analysed IOCs provided by Boeing in a joint CISA/FBI/ACSC report that was a victim of the **Citrix bleed attack campaign**.

3.1.2. Cicada3301 RaaS program (Blackcat/ALPHV' rebrand?)

We found that at least one IP address (*c.g.,* 91.238.181[.]238, hosting provider called VDS&VPN services) was **overlapping with** the **ShadowSyndicate attack infrastructure** and **an exfiltration server used by affiliates of a recent RaaS program known as Cicada3301**.

Cicada3301 was first observed in June 2024 and developed in **Rust** language as it is for some other brands such as the defunct Hive, Blackcat/ALPHV RansomExx, Qilin (Agenda), and Luna. Another important aspect is that **Cicada3301 operators** in February 2024 **sought to exploit ScreenConnect vulnerabilities**, (CVE-2024-1708 and CVE-2024-1709). The same vulnerabilities were also extensively exploited according to Trendmicro by other top tier ransomware such as **BlackBasta** (overlapping with attack infrastructure of **ShadowSyndicate**) and **Bl00dy** ransomware.

As far as **Bl00dy** ransomware is concerned, affiliates *"employed leaked builders from both **Conti** and **LockBit Black (aka LockBit 3.0)**"* and exploited *"**various zero-day vulnerabilities**, including a **PaperCut** software vulnerability"* according to Trendmicro.

As **Blackcat/ALPHV** is one of a few ransomware known to have also used **ESXi ransomware written in Rust** and shown **several commonalities with Cicada3301** such as in the code, the encryption/decryption mechanisms, naming conventions, it's been conjectured that **Cicada3301** could be a rebrand. This hypothesis is substantiated by the timeline where the rebrand would have occurred right after the **Blackcat/ALPHV**' exit scam.

An interesting point discussed by Truesec is a potential teaming up of the defunct **Blackcat/ALPHV** program with the **botnet Brutus** (used to conduct a broad automated campaign **via VPN brute-force/password spraying attacks**, including **ScreenConnect**). This resonates with the BlackBasta's leaked internal chat logs that showed that this group also used Brutus botnet, dubbed **BRUTED**, to breach in enterprises since 2023.

According to Unit42 the **IP address was flagged for Cobalt Strike activity** (watermark: 674054486). This watermark **could be linked to other ransomware groups such as Bashful Scorpius** (aka **Nokoyawa**) and Ambitious Scorpius (aka **ALPHV/BlackCat**) in 2023. Unit42 added that an affiliate who deployed **BlackCat ransomware** in March 2022 exposed victims' data throughout **Cicada3301**.

3.1.3. Chinese and North Korea state sponsored APTs

While pivoting on the IP address 193.29.13[.]167 (AS42397, **Bunea TELECOM SRL**) we found a communicating malware via Threatbook named 65103ed62bf26e5b_ea77654.msi identified as **Alien** (sha256: 65103ed62bf26e5bab1b56756771bc129d2c6ff6a419cab858d29d0ff233bef2, on 2024-09-19 02:01:36).

This sample is **a MSI file** that first submitted from **Russia** at 2024-09-18 22:40:41 UTC on VT. From behaviour panel from VT one can directly spot at **a suspicious communicating domain name** with the malware (POST command) as well **as a download endpoint** (GET command of Loader_TM.dll) as shown in the figure below:

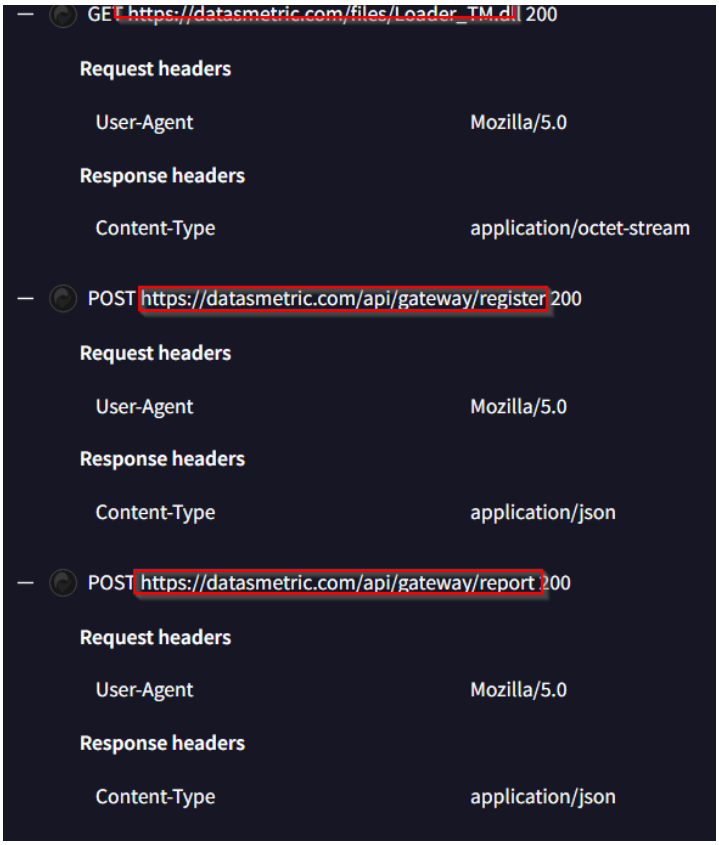
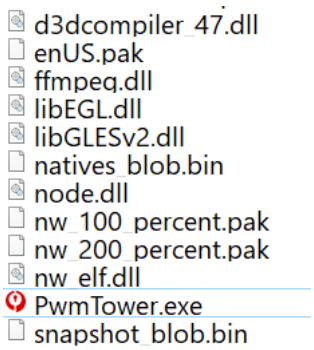


Figure 3 C&C endpoints of the MSI file unveiled by dynamic analyses of sandboxes provided by VT. A file named Loader_TM.dll might be of interest to analyze as a second stage.

Thanks to threatbook we found that the downloaded file *Loader_TM.dll* holds the following sha256:

9a2da32d2dc364059878a43322d9f56c372d710544edb47258564556de698030 (not known in the VT database). By investigating the **MSI file** properties, we found that it **was signed** with a **legitimate certificate** named **SCANDI LLC** (issuer:GlobalSign GCC R45 EV CodeSigning CA 2020) with the associated serial number 1f02bc9533123645610f5914 being valid between 7-08-02023 and 7-08-2024.

By pivoting on the issuer name **SCANDI LLC** we found that the researcher @RussianPanda9xx on X (ex-twitter) reported on the same finding. The tweet mentions an analysis of Chris Duggan reporting on a signed MSI file being undetected at that time (18th October 2024), which seems to be the same.



Uncompressing the MSI file unveiled several files with .dll, .bin, .pak and .exe extensions as shown in the figure below.

Figure 4 Files embedded in the MSI file once extracted locally. One can spot at PwmTower.exe binary file with the sha256 hash 4fe0aa609df4df49317733445194b27e77c42aea5d16108ef28b0c4f2e4f38b2 (legitimate security tool).

Now that we have a better idea of the overall behaviour of the MSI package that points to a side-loading of a malicious DLL named nw_elf.dll, we delved into its actual code via a reverse engineering analysis.

The first request that the binary sends is: *hxxps://datasmetrics.]com/files/Loader_TM.dll* that should deliver a second stage. **However, the domain is currently down and the second DLL cannot be retrieved.**

1. *Overlaps with Toneshell Backdoor*

We found a **low** to **moderate overlap of the discovered TTPs related to the malicious MSI package** and a **recent report published by Unit42** unveiling an undocumented variant of the backdoor named **ToneShell** (discovered by Trendmicro in Nov 2022, aka bespoke stagers).

The following **ToneShell backdoor** process tree was described by Unit42, which follows three stages as shown in the figure below.

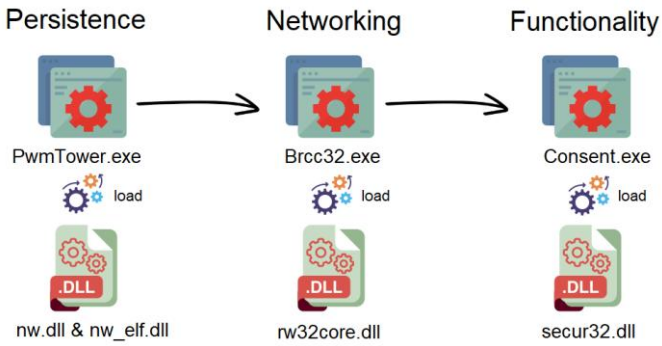


Figure 5 Screenshot taken from Unit42. Toneshell backdoor process tree.

Unit42 underlined that no other known APTs than **Stately Taurus (Mustang Panda, BRONZE PRESIDENT, TA416, RedDelta and Earth Preta)**, a **Chinese state-sponsored group**, has used **ToneShell** backdoors (including its variants). Unit 42 has observed the group **gathering information on targets in and around the Southeast Asia region** since at least 2012. ESET researchers then detected an overlapping malicious cluster of activity but with "distinct organizational and technical differences" compared to **Stately Taurus.** ESET assessed this cluster of activity, dubbed **CeranaKeeper**, as a new **China-aligned** intrusion set.

Moreover in our case, one can observe the choice of embedding legitimate DLLs (**ffmpeg.dll**, **d3dcompiler_47.dll**) that could recall a **well-known supply chain attack** against **3CX Desktop App** allegedly conducted in late March 2023 by a **north Korean APT** according to GTAG from Google; This attack **could resemble the TTPs witnessed for ToneShell** as it also used **the DLL side loading technique** from a malicious MSI package and both targeted Windows and MacOS platforms.

We further found that the name of the DLL **nw_elf.dll** is described as **nwjs** and likely related issue on **Github** that was already published in **2018** from the **nwjs project.** This issue mentions DLLs missing version field correspond to the tree of files we observed with (ffmpeg.dll, node.dll, nw.dll, nw_elf.dll and nw.exe). We conjecture that **mimicking this project could be used as a lure in the early stages of the kill chain to appear as legitimate desktop apps based on JavaScript**.

However, we must underline that such **legitimate and unused files that we discovered upon our analysis could have been planted as a false flag** by the intrusion set. In contrast, **the use of Toneshell could have been conducted by a north Korean APT to point fingers towards China**. Another likely scenario would be that, if previous attribution were valid, ToneShell could be used by other nation-state actors beyond China.

According to Unit 42 the **first stage of ToneShell backdoor** aims at **establishing persistence** depending on the process' privileges upon execution. **Stage 2 and three provide C2 network** using

pipes and **functionality components**. The capabilities of **ToneShell** are **designed for cyberespionage** that includes:

- Executing commands
- File system interaction
- Downloading and uploading files
- Keylogging
- Screen capturing

The domain datasmetric[.]com was first resolved for 5 months (from 2024-02-27 to 2024-08-07 according to securitytrails) by the IP address 193.228.128[.]158, which belongs to the **rogue Russian**. **ASN *GLOBAL CONNECTIVITY SOLUTIONS LLP*** *(AS215540)*. The latter is indeed **a front company that relied on the bulletproof hosting provider** "**4vps.su**". This network is being used by **Russian state sponsored intrusion sets** that we covered in multiple recent analyses.

2. Infrastructure overlap with ToneShell backdoor, Rustdoor and Koi stealer

From 2024-08-07 till 2024-11-29, datasmetric[.]com was resolved by the IP address (193.29.13[.]167). This IP address also resolved a known malicious domain maconlineoffice[.]com around 2023-10-05 as shown in the figure below.

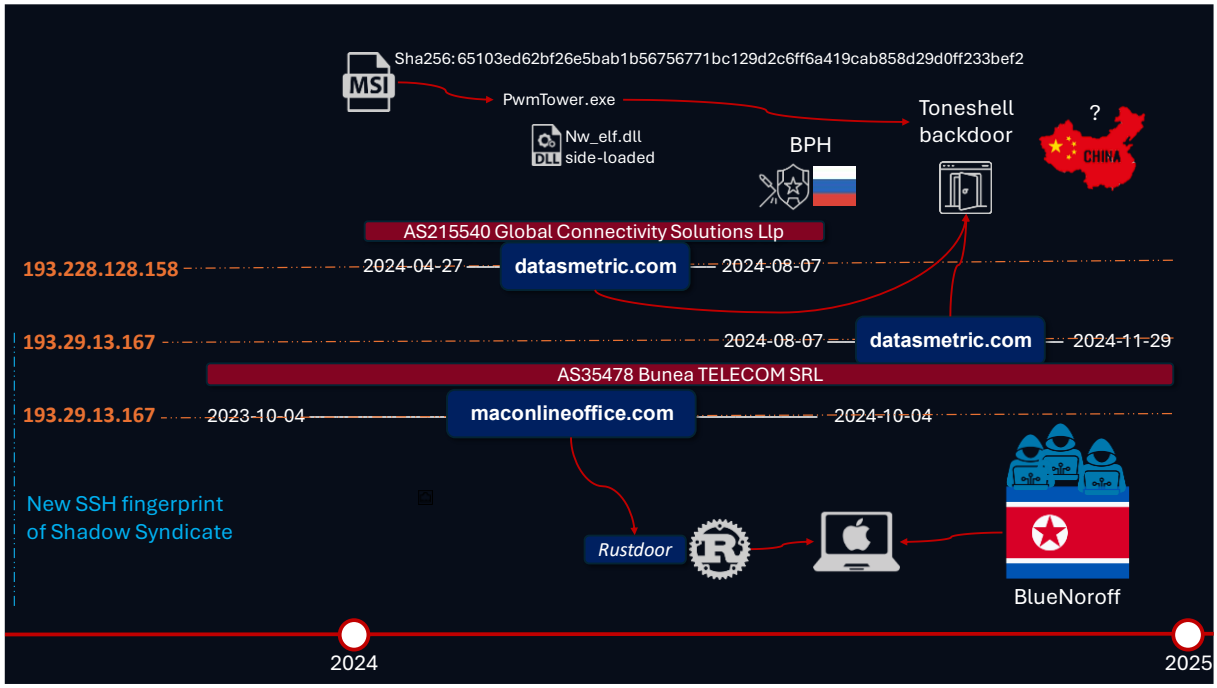


Figure 6 Links and dependencies of IPv4 address 193.29.13[.]127 to two state-sponsored APTs linked to North Korea (BlueNoroff) and China (ToneShell backdoor alleged to be a custom tool of Mustang Panda according to Unit42 and Trendmicro editors).

Beyond the previous overlap of threats on the same IP address, we found an overlap respectively of malware and network TTPs throughout **similarities in API endpoints** used by the two backdoors (Toneshell and the variant 2 of Rustdoor) as well as the **use of a common word "metric" to craft C2 domains** (datasmetric[.]com and apple-ads-metric[.]com). We have summarized such an overlap in the figure below.

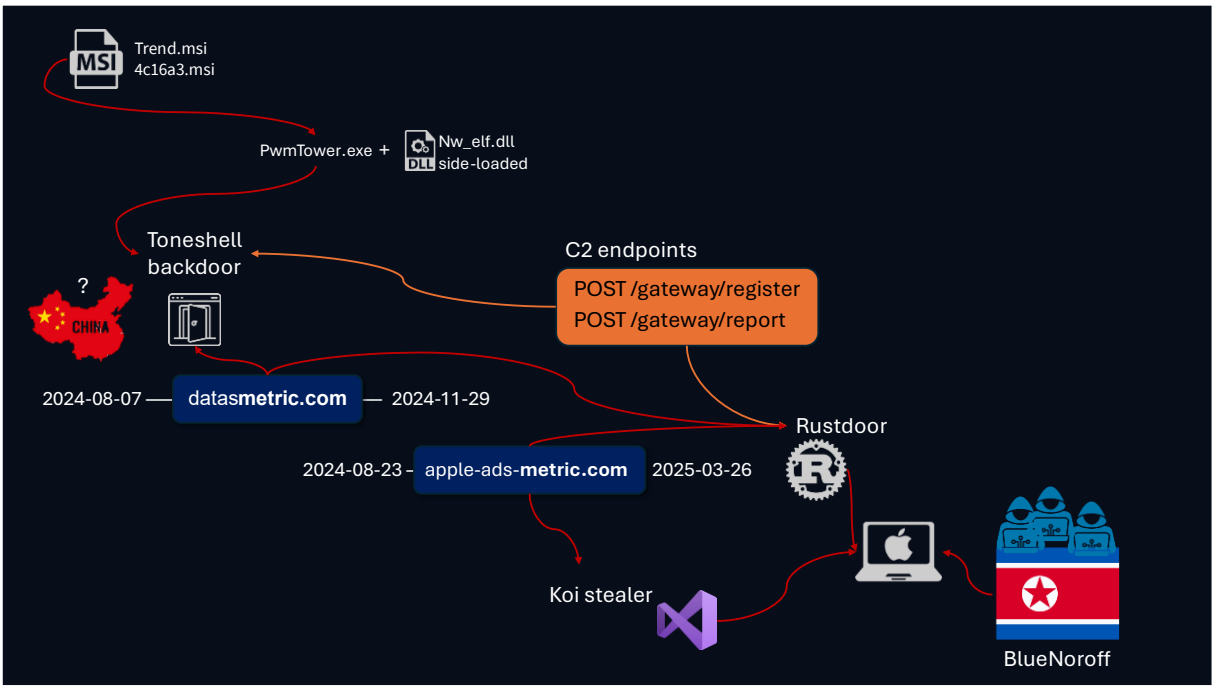


Figure 7 Attack infrastructure of ShadowSyndicate overlaps with Toneshell, Rustdoor and Koi stealer.

3. *North Korea APT actors and the Russian top tier ransomware ecosystem*

We then found in the literature the sha256 hash of the MSI (sha256:65103ed62bf26e5bab1b56756771bc129d2c6ff6a419cab858d29d0ff233bef2) reported by Chris Duggan in October 2024. He stated that this **MSI** was overlapping **the top tier ransomware ecosystem (Play, Cl0p)**, according to him, perhaps via an **Access Broker's ransomware network**.

As a reminder and underlined by **Chris Duggan**, it is known that **Play ransomware is only one of the many ransomware brands** used by the group **ShadowSyndicate**. Bitdefender in a recent report cited the work of Chris Duggan and mentioned that *"**macOS Backdoor artifacts and IOCs suggest a possible relationship with the BlackBasta and (ALPHV/BlackCat) ransomware operators**"*, and thus with North Korean threat actors suspected to usually use Rustdoor.

Two years before already, **Andariel** (aka Onyx Sleet, Jumpy Pisces) used **Maui** ransomware to also target U.S. hospitals and healthcare companies and was consequently disrupted by the US Justice Department. More precisely **Unit42** conjectured that members of **Andariel** were acting either as *"an **initial access broker** (IAB) or an affiliate of the **Play** ransomware group"*. To be recalled about Play ransomware are the notable similarities with **Quantum ransomware**, an offshoot of the **Conti ransomware group**. Besides, upon ransomware attacks **Andariel** settled persistence by *"spreading the open-source tool **Sliver** and their unique custom malware, **DTrack**, to other hosts via Server Message Block (**SMB**) protocol"*.

4. *Overlap with Atomic Stealer infrastructure & similarities with Rustdoor backdoor:*

While pivoting on several IPs such as 194.34.239[.]34 (**HOSTKEY B.V.**) or 185.232.67[.]14 (**Alviva Holding Limited, AS209132**) we found a recent blog post (January 2025) written by the researcher Cyb3rhawk reporting on **Atomic stealer (AKA Rod Stealer, AMOS, Atomic macOS Stealer.** The infrastructure of this malware **overlaps with the actual infrastructure under study as shown in the figure below**.

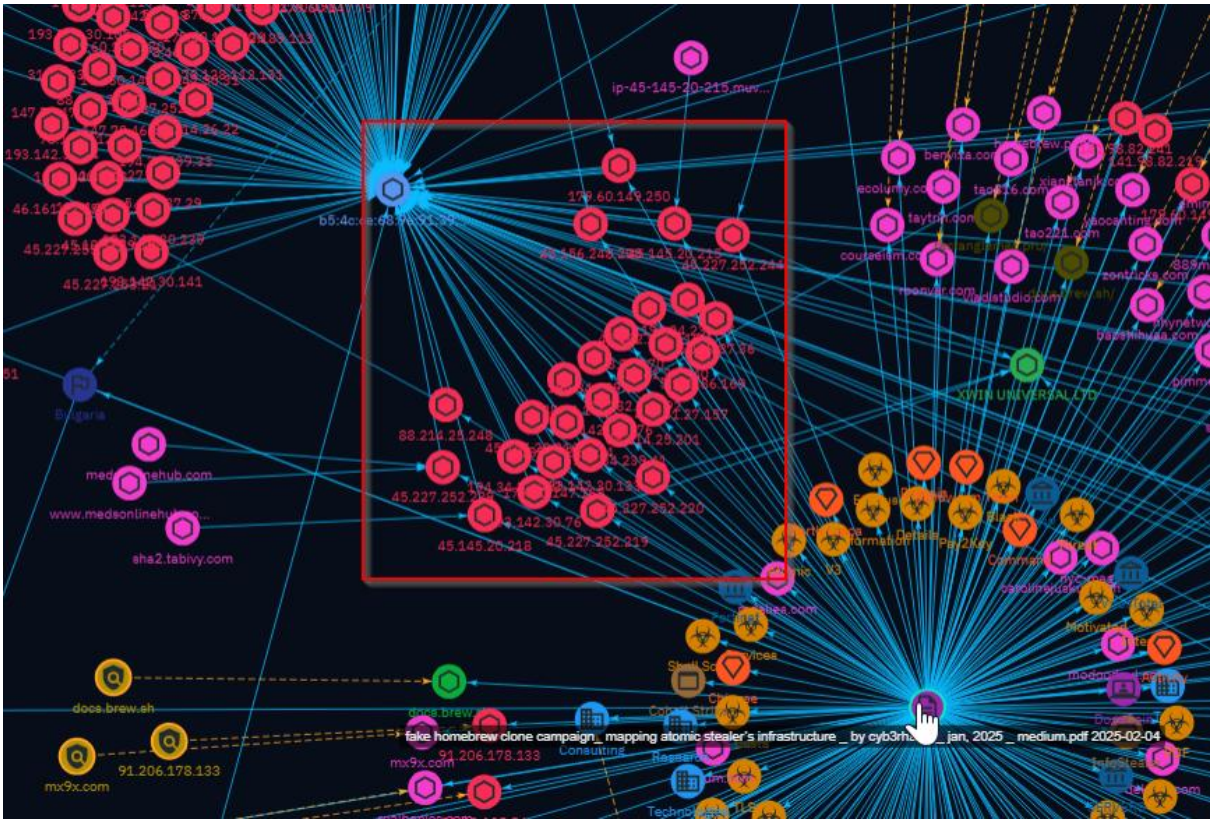
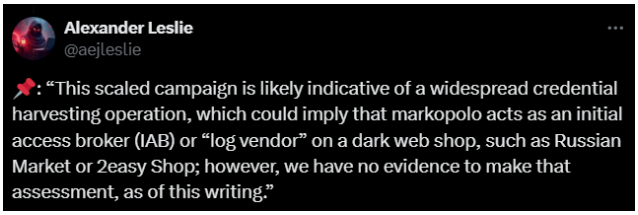


Figure 8 Strong overlap found between the infrastructure under study (ShadowSyndicate) and the one found in the literature reporting on Atomic stealer infrastructure. Screenshot taken from SaaS Intrinsec Opencti platform.



Atomic stealer was first discovered in April 2023. Recorded future unveiled in June 2024 that **Atomic stealer** is likely spread by the alias 'markopolo', an **IAB** spreading **StealC, Rhadamanthys** and **Atomic** via **Malicious Vortax installers on Windows and macOS**.

Figure 9 The image contains a statement by Alexander Leslie suggesting "markopolo" may act as an IAB or log vendor, though no evidence supports this claim at the time of writing for Russian Market or 2easy Shop. Screenshot taken from X (ex-twitter).

The vector of infection uses scam on social media (Vortax) paired with another older campaign targeting **Web3 gaming projects** masquerading as virtual meeting applications that primarily target cryptocurrency users. In terms of victimology, was detected by Kaspersky *"infections all around the world, with Russia and Brazil targeted the most heavily"*.
In the last campaign criminals used fake mac homebrew Google Ads to lure victims and **steal credentials, crypto wallets and browser data from compromised devices**. Here the fake ad redirected visitors to the fake counterpart's URL, brewe[.]sh (instead of brew.sh). The malicious domains were registered via **Dynadot Inc** (ISP JSC "Ukrtelecom", geolocated in **Ukraine**).

It is important to note that **Bitdefender** reported on **code similarities between the Apple Script block of the new variant of AMOS (Atomic stealer) and the 2nd variant of Rustdoor backdoor** presented in the previous paragraph. **Bitdefender** also uncovered that a **C2 communicating with this new variant was associated with Amadey** (5.42.65[.]114).

This IP address is mentioned in the recent chat leaks of **Blackbasta** and in a report of Recorded Future associated to **AMOS**. **Recorded Future** reported *"a multifaceted campaign, attributed to **Russian-speaking threat actors** likely located in the CIS, abusing a legitimate GitHub profile to impersonate legitimate software, such as 1Password, Bartender 5, and Pixelmator Pro, among others, and distribute various malware families focused on stealing personal information from unsuspecting victims".*
Via **Domaintools passive DNS** we found **another DNS** (loomfi[.]com) **linked to the same intrusion set**. This DNS was first seen 2025-01-18 and **hides** its genuine IP **behind Cloudflare CDN** while the 7th most abused US domain **registrar Dynadot Inc was used** for this domain.

The **DNS is flagged as malicious** by 6 antiviruses over 94 on Virustotal platform. **Two malicious payloads communicated with** the malicious **domain loomfi[.]com** around mid-**2024** as shown in the screenshot below (the first most abused US domain **registrar Namecheap** was used).

Communicating Files (2)

Scanned	Detections	Type	Name
2024-07-25	70 / 73	Win32 EXE	server
2024-07-21	63 / 72	Win32 DLL	RCX871C.tmp

Figure 10 Screenshot taken from Virustotal. Two PE32 binaries communicated with loomfi[.]com around mid-2024.

It turns out that both files could be associated **via crowdsourced Yara rules to Nitol malware**. This **malware** could be used as a **DDOS bot to install Amadey**, a downloader known since 2018 that we covered multiple times in previous analyses.

5. *DeepSeek LLM luring campaigns to spread Atomic stealer*

While pivoting on this IP address 81.19.135[.]228 (Org Alviva Holding Limited, no ASN) overlapping both the Lockbit Citrix bleed attack infrastructure and atomic stealer's infrastructure, we found a close campaign surfing on the new DeepSeek LLM to lure users.

Passive DNS Replication on VT **unveiled 128 malicious domains resolved to** 81.19.135[.]228 from 2024-12-06 to 2025-03-31. Four of those malicious domains were present in the github repository of esentire and related to **ClickFix style shell script** and **Atomic Stealer**.

As shown in the figure below, VT intelligence allowed us to analyse latest files that communicated with the IP address 81.19.135[.]228, which exhibit two patterns for the filenames of the Mach-0 files namely 'Open Gatekeeper Friendly' (see red boxes) and localfile~ .x64|arm64 (see blue boxes). The **bash script safeguard.sh** connects to the malicious URL https://escapeesrvclub[.]com/macshare[.]php (see yellow box).

Communicating Files (12)

Scanned	Detections	Type	Name
2025-03-25	32 / 63	Mach-O	localfile~.arm64
2025-03-29	33 / 64	Mach-O	Open Gatekeeper Friendly
2025-03-22	34 / 63	Mach-O	Open Gatekeeper Friendly
2025-02-12	1 / 61	Shell script	safeguard.sh
2025-01-30	28 / 62	Mach-O	localfile~.arm64
2025-03-29	33 / 64	Mach-O	localfile~.x64
2025-04-01	29 / 63	Mach-O	localfile~.x64
2025-02-09	29 / 62	Mach-O	Open Gatekeeper Friendly
2025-02-19	28 / 63	Mach-O	localfile~.x64
2025-04-01	28 / 63	Mach-O	localfile~.arm64
2025-03-22	31 / 63	Mach-O	localfile~.arm64
2025-03-22	29 / 61	Mach-O	Open Gatekeeper Friendly

Figure 11 Latest files that communicated with IP address 81.19.135[.]228 according to VT. One can observe two patterns for the filenames of the Mach-0 files namely 'Open Gatekeeper Friendly' and localfile~ (.x64|arm64). The bash script safeguard.sh connects to the malicious URL https://escapeesrvclub[.]com/macshare[.]php.

"Open Gatekeeper Friendly" named files (understand Apple's Gatekeeper bypass) was reported on X by MakwareHunterTeam in March 2025 underlining that the **malicious binary also downloaded a FUD archive "ledger.zip"** embedding a Fully UnDetectable (FUD) Mach-O file at that time. Right after, Moonlock Lab posted an analysis of the main Mach-O file triggering **a phishing page simulating a fake critical error coercing the user to fill in a seed phrase of 24 words to recover a Ledger Live account**. The **final goal here is to drain assets from a cold wallet** (here ledger but could also be trezor) that was **first detected by the Atomic infostealer**.

According to Moonlock Lab the **Mach-O is FUD thanks to encryption process** *"XORing each byte with a dynamically computed autogenerated key"*, which **resembles** the mechanism used in a sample identified as **Poseidon stealer** by @bruce_k3tta on X **with a panel mentioning** another potential Greek reference "**Odyssey**".

As far as **Poseidon stealer** is concerned, Malwarebytes mentioned the 27th of June 2024 that *"a large part of the code base being the same as its predecessor"*, namely **Atomic stealer** but *"added a few new features such as looting VPN configurations"*. **Malwarebytes** found that a threat actor with the alias **Rodrigo4** was **selling on XSS** (infamous underground **Russian-speaking forum**) the update from Atomic to alleged **Poseidon**. Flashpoint added that "Rodrigo4" or "Mr. Rodrigos" **engaged in conflicts with rival macOS stealer developers** on illicit forums (e.g., with co0per).

Poseidon Stealer was spread in late 2024 via **malicious Swiss government application** "AGOV access" and was also distributed through a **trojanized "Arc Browser"** served to victims (via **Google advertisements**).

While visiting escapeesrvclub[.]com resolving 81.19.135[.]228 (FLYSERVERS-ASN Flyservers S.A., PA, AS 209588, Russia) one can find a luring html content exhibiting successful deployment of a web site; others tagged it as a phishing alert and blockchain fraud.

Figure 12 Web content presented to a visitor of such domains seeking to mimic legitimate behaviours of a normal website freshly deployed (screenshot Intrinsec).

By pivoting on the ASN 209588 (**Flyservers S.A.**) on URLscan we found that previous domains found on VT also display the same web content as shown below (see orange overlay). A related campaign was reported on X using a **fake safeguard page and captcha** to deliver **Atomic stealer**, which **resonates** with the aforementioned safeguard.sh bash script.

We also found that **Boolka injecter** was **hosted by the same ASN since last summer**. This finding is interesting as we fallback to the same observation that GroupIB has published at that time while analysing the infrastructure of **ShadowSyndicate**.

According to GroupIB the landing page distributing Boolka *"served as a test run for a malware delivery platform based on BeEF framework"*, which matches the subdomain beef.softbyms.com that we found.

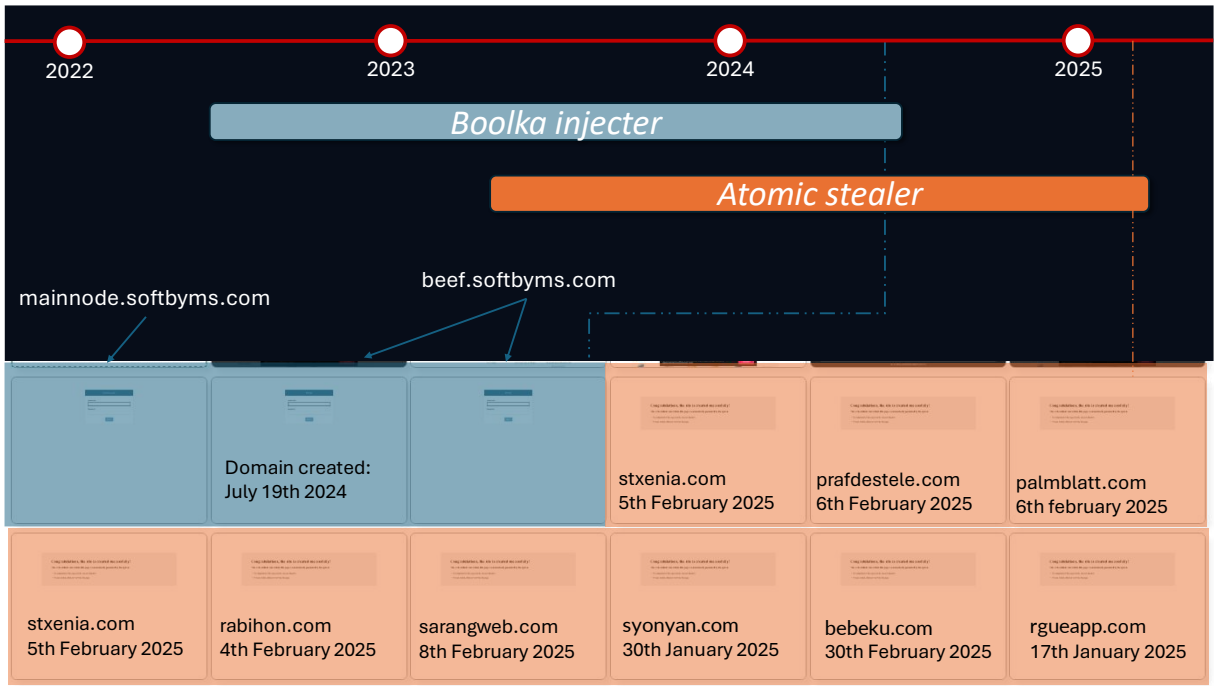


Figure 13 Recently observed screenshots of pages hosted on the ASN (AS209588 FLYSERVERS-ASN, PA).Screenshot taken from URLScan and enriched by Intrinsec. We found that Atomic stealer downloading servers from the beginning of this year and Boolka injecters in late of last year were both hosted by FLYSERVERS-ASN. (was moved to rogue Proton66 000 ASN at the time of writing). This threat appeared in June 2022 according to GroupIB.

It's important to note that **all IPs that belonged to Flyservers S.A., PA distributing Atomic stealer now belongs to Proton66 OOO, RU** that we already have covered in recent analyses (see report be9fdd75-

0299-49b9-8f39-71067e21b756, PROSPERO-AS : *Tracing the Links Between Anonymous Bulletproof Networks*).

In the paper of GroupIB about **Boolka** and as far as **ShadowSyndicate is concerned**, we found an important sentence *"at the moment it looks like the **aforementioned SSH belongs to some bulletproof hosting provider or VPN**"*.

Their new assessment comfort our findings of a wide range of threats (somewhat linked to **Kremlin interest, North Korea and even maybe China** via Toneshell backdoor) while spanning campaigns involving **APTs, botnets, stealers and even a FIMI operation**. It also resonates perfectly with our analysis of each encountered ASNs/ISPs at the ed of the document.

6. *Unknown APT uses DecoyDog: DNS tunnelling as C2*

Upon the analysis of the **ShadowSyndicate's attack infrastructure**, we encountered multiple times a known **multi-level malicious subdomain associated with DecoyDog DNS kit** for the following IP addresses:

- 91.238.181[.]225 (VDS&VPN services) AS49434 - FBW NETWORKS SAS, FR
- 194.34.239[.]33 (LLC "Server v arendy"), AS50867, HOSTKEY B.V., RU
- 194.34.239[.]38 (LLC "Server v arendy"), AS50867, HOSTKEY B.V., RU
- 88.214.25[.]201 (ThinkTech Technology Industrial CO. Limited) AS35042 Layer7 Networks GmbH
- 88.214.25[.]244 (ThinkTech Technology Industrial CO. Limited) AS35042 Layer7 Networks GmbH

As it turns out that we already encountered this malicious domain at least upon one analysis of **Killnet** group (we could not establish a link with DecoyDog kit), the malicious **DNS claudfront[.]net in conjunction with PupyRAT** recalled a past report of **Infoblox** about **the Decoy Dog toolkit** relying on those both unusual characteristics. Here is a reminder of the intelligence we already gathered and shared with our clients.

The domain claudfront[.]net **likely typo squats** the well-established domain **cloudfront.net** related to the legitimate content delivery network (**CDN**) service from **Amazon**. The amazon domain created 16 years ago could produce **close entropy in terms of DNS signature allowing attackers to keep surmise.**
This domain is of particular interest as it was discovered by Infoblox researchers that it was leveraged for C2 beaconing over DNS by **PupyRAT**.
PupyRAT, aka: Patpoopy, is a **"cross-platform, multi-function RAT and post-exploitation tool** mainly written in **Python**" according to its readme on Github. This RAT is particularly hard to detect by security solutions thanks to its **fileless nature and its encrypted C2 communications over DNS**. As it is open source, whenever encountered in attacks by defenders make it harder to identify as a discriminate TTP for attribution.
According to Infoblox both domains (cbox4.ignorelist[.]com and claudfront[.]net) were flagged in early April 2023 for anomalous beaconing while the C2 communication originated almost **exclusively from hosts in Russia**. The timeframe and the short period of hosting but also the pattern '9999' must be noted.

We plan to publish a dedicated investigation into the DecoyDog kit infrastructure at a later stage, as our understanding of this threat has recently evolved.

3.1.4. Foreign Information Manipulation and Interference: USA presidential election 2024

Next finding is an unexpected one as while pivoting on each IP addresses controlled by ShadowSyndicate we found in http headers a web server Nginx field "Location" as follows: "nginx:*.hunterlap.top" (194.34.239[.]33, AS 50867, Hostkey B.v.,). Besides, we also found two domains linked to **Decoydog toolkit infrastructure resolved to the given IP address** (see details in main text).

The *.hunterlap[.]top domain was seen in http headers on 194.34.239[.]33 earlier in 2024 (last seen on 2024-06-01) **but before the SSH fingerprint of ShadowSyndicate was initially spotted in December 2024**. This hinders to establish a direct connection between ShadowSyndicate and such a well-known foreign Information manipulation and interference of USA presidential election and could point to the use of the same infrastructure to conduct a broad range of operations.

The domain name "hunterlap[.]top" drawn our attention as it likely refers to the **famous US federal justice case known as *'Hunter Biden laptop controversy'***. We could confirm by retrieving screenshots taken by Domaintools that this domain was pointing to a "hack and leak" crime related to ***'Hunter Biden laptop controversy'*** that was claimed by **ShareBear** as shown in the figure below.

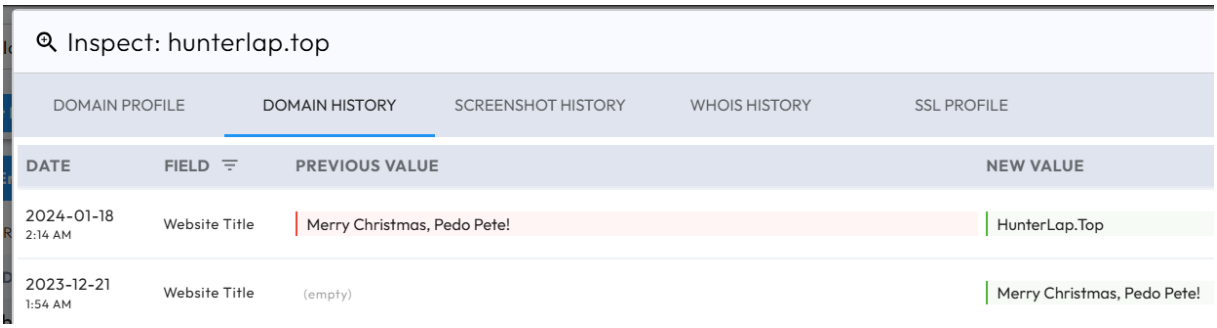


Figure 14 Screenshot taken from Domaintools exhibiting the web title change of hunterlap.top. The title of the website was changed once from "Merry Christmas Pedo Pete" to "HunterLap.Top" Laptop" the 2024-01-18.

The domain hunterlap[.]top was first seen by Domaintools 2023-12-01 and it was registered by **NameSilo LLC**. The domain hunterlap[.]top was first seen a year ago and last updated at 2024-01-17 while its genuine IP address **was hidden behind Cloudflare CDN**.

The '**Hunter Biden laptop** controversy' still defrays the chronicles since the **presidential elections of 2020 in the United States**. On April 9, 2025, Donald J. Trump issued a presidential memorandum titled *"Addressing Risks from Chris Krebs and Government Censorship."* The memorandum accuses **Christopher Krebs**, former director of the Cybersecurity and Infrastructure Security Agency (CISA), of misusing his authority to censor speech, particularly concerning the 2020 election and the COVID-19 pandemic. It specifically alleges that under Krebs' leadership, **CISA suppressed discussions about Hunter Biden's laptop by collaborating with major social media platforms** to censor related information.

In brief, emails were found in a **laptop** belonging to the **President's son** (**hunter Biden**), which was dropped off in April 2019 at a repair shop in Delaware, where the Biden family lives, and never

recovered. **Three weeks before the 2020 U.S. presidential election**, the [New York Post](#) **published a front-page article** featuring laptop emails that purported **to expose corruption linked to Joe Biden** in secret emails, the Democratic candidate and father of Hunter Biden.

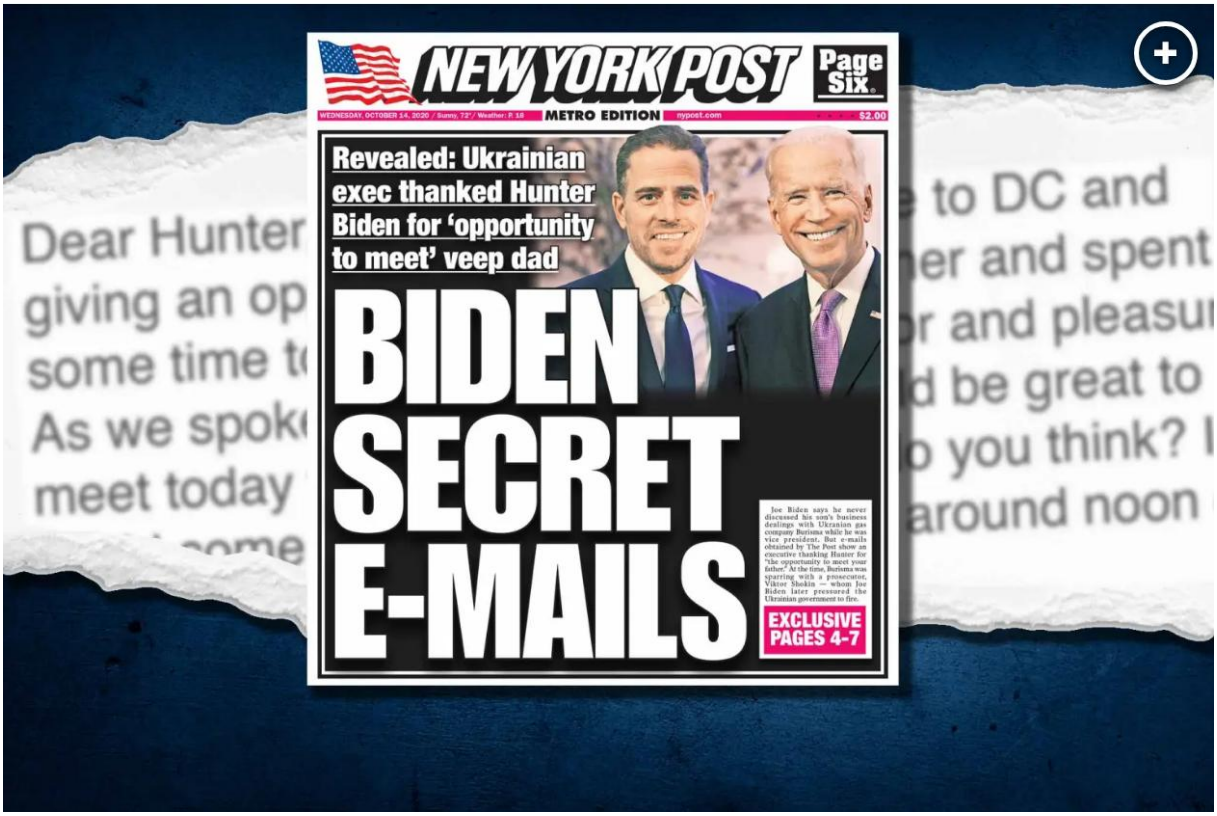


Figure 15 Image taken from the New York Post, a media owned News Corp, Rupert Murdoch's media empire. This article was published 3 weeks before the US presidential election that occurred in 2020.

News Corp, Rupert Murdoch's media empire—which includes outlets such as the **New York Post**—is widely recognized for having its editorial line steered to reflect his personal ideology, often described as **Europhobic, libertarian, climate-denier, and close to the Republican's party program**.
In 2011 **Murdoch was involved in a huge affair**, which led to the closure of the News of the World tabloid after **revelations of dubious and illegal journalistic practices** on thousands of celebrities, politicians and members of the royal family **by hacking/tapping their phones** (precedent to spyware nowadays used such as Pegasus). **Questionable payments to the Police and military officials**, in return for **story tipoffs** are investigated **by the FBI including the Murdoch's activities in Russia** via "*News Outdoor Russia*". This scandal not only shook public confidence in the media, but also exposed the close links between the press, the police/military and politics.
Murdoch's network consistently **backed Donald Trump** until the disappointing midterm election results in November 2022. Moreover, a **defamation trial revealed that Murdoch never subscribed to the idea of a Trump victory in the 2020** presidential race, even as his editorial teams propagated the former candidate's baseless claims **of a "stolen election" via Dominion systems**.

The **FBI seized the Hunter's Biden laptop**, but the repairer had made a copy of the hard drive, which was given to **advocate of Donald Trump Rudy Giuliani**, who passed it on to the **New York Post**. FBI then

covered up 51 ex-intelligence officials who wrongly suggested and then-candidate Joe Biden that the files came from Russia.

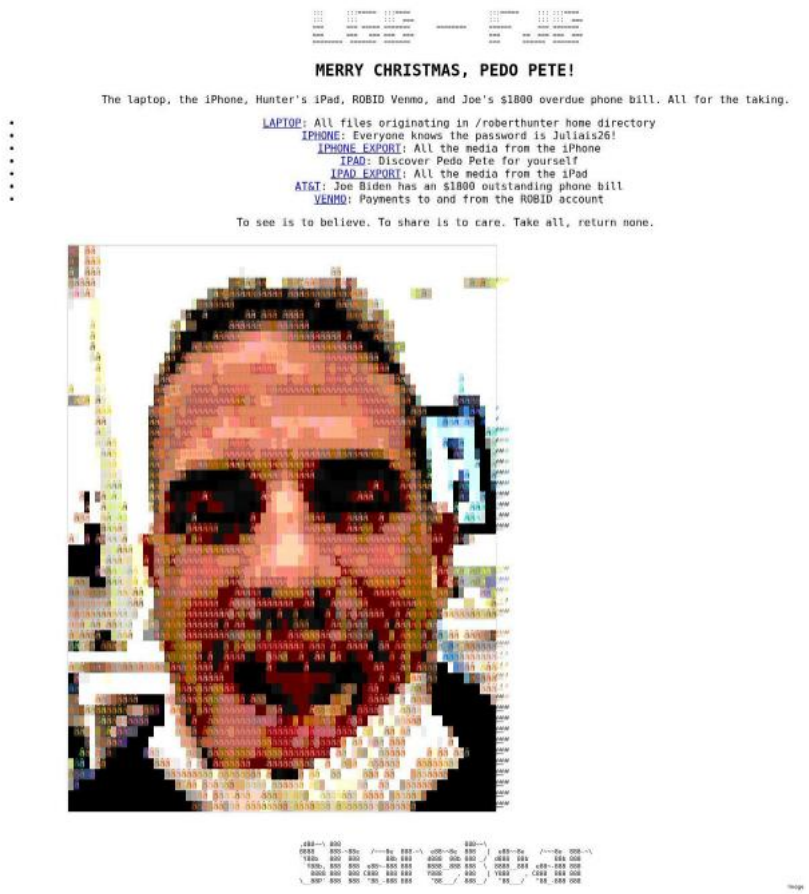


Figure 16 Screenshot taken by Domaintools on 2023-12-21. This website was up at least till 31 of May 2024 and leaked data found on the laptop of Hunter Biden, the son of Joe Biden running for US presidential elections against Donald trump in 2020. The title of the website LGB FJB corresponds to "anti Biden Ugly Xmax campaign's". Speculation had previously alleged the 'Pedo Peter' contact alias referred to Joe Biden after this contact was found on the Hunter's iPhone. The tree of leaked files can be retrieved via the wayback machine. The leak was claimed by a group named ShareBear.

It's important to note that **Hunter Biden** was a member of the Board of Directors of Burisma Holdings, one of **Ukraine's largest private natural gas producers**, from 2014 until his term expires in April 2019 that was accused of corruption and money-laundering.

The **New York Times** reported in May 2021 that federal investigators in Brooklyn had begun a criminal investigation late in **the Trump administration**. Possible efforts by several current and former **Ukrainian officials to spread unsubstantiated allegations about Joe Biden concerning corruption** were unveiled, attacking him by capillarity throughout its sun Hunter Biden. **GRU agents working in Ukraine** relayed this story seeking to **put the blame of Biden's sun scandal towards Ukraine**.

Pro trump accounts on social networks such as @Jozeecue have relayed the "hack and leak " crime to amplify the campaign. We found that this website was first posted on the infamous **4chan underground forum by an account alias named ShareBear** (posted on December 17, 2023, at 20:24:03 UTC, see figure below), which matches the alias found on the website hosted at hunterlap[.]top. This

post was soon after relayed and analysed on far-right website **8kun.net** (ex 8chan) by an anonymous source on December 19, 2023, at 22:12:57 UT.

Figure 17 Screenshot taken from Flashpoint intelligence platform where we found the original post sharing hunterlap.top leak site to the community. This post was relayed and analyzed on 8kun.net by an anonymous source the December 19, 2023, at 22:12:57 UTC.

Such **hack and leak operations are a hallmark largely abused by the Russian intelligence services** since at least 2007-2008 (against Estonia and the Georgian Republic), in particular by the Main Intelligence Directorate (GRU), to create a perception hack. More, recently on April 15, 2021, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) designated 16 entities and 16 Russian from the Federal Security Service (FSB), the Main Intelligence Directorate (GRU), and the Foreign Intelligence Service (SVR) involved in controlling disinformation outlets.

The Strategic Culture Foundation (SCF), a Russian online journal **linked to the SVR and the Ministry of Foreign Affairs**. Controlled by the SVR's Directorate MS (Active Measures), spread false narratives about **U.S. officials involved in the 2020 presidential election**. The journal published conspiracy theories and aims to disguise its Russian origins to make its disinformation more credible to readers.

As such, **news of a cyber intrusion leads** the public to question the reliability of election results to **weaken representative governments perceived as democracies**. Moreover, using **proxies such as IABs or ransomware groups shield from prosecution** in return for "plausible deniability for state-backed cyber operations.

N.B: Pivoting on the same DNS we found via Fofa only **another server exhibiting this time a Nginx web server** with the title "HunterLap.Top» hosted by OVH, Mumbai; 148.113.5.24 (AS16276, OVH). This server is known for having been offensive around 2023 (brute SSH and port scans). We found neither a direct link with the other server nor further intelligence about that server or screenshots that proved it hosted the same content about Hunter Biden.

3.2. An imbricated network of Russian Bulletproof hosters used by ShadowSyndicate

As tipped in a knowledge graph thanks to our Opencti database, we observed that several IP addresses were pointing to a few ASNs. Identify them is of paramount importance for building up defences and perhaps solve the mystery of **ShadowSyndicate**. We present in the figure below **the most frequently encountered ASNs related to the last SSH key of ShadowSyndicate**.

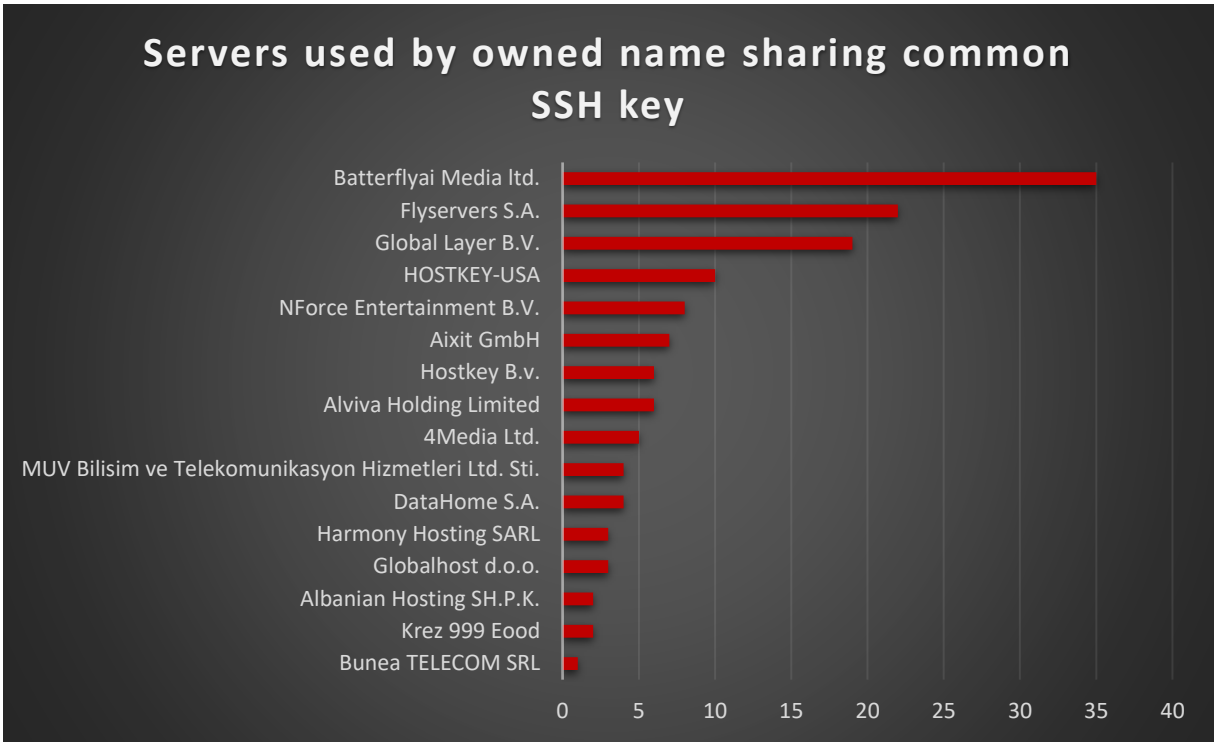


Figure 18 Servers owned named sharing common ssh key related to ShadowSyndicate in the literature. An owned server is not necessarily linked to known malicious activity but highly probable as an anticipation if not already.

It's important to note that overall, **some ASNs are consistent with the ones reported by GroupIB** for the previously known SSH key fingerprint related to ShadowSyndicate (*c.g.*, Flyservers S.A. , Batterflyai Media ltd., Alviva Holding Limited, DataHome S.A.,VDS&VPN services etc).
Since we track ShadowSyndicate from its last renewed SSH key we also observed stability for months (from December 2024 till 2nd of May 2025), which suggests infrastructural or operational continuity over time and thus a TTP that we can stick to that intrusion set.
We present hereby a first scheme summarizing the breakdown of each Autonomous System Numbers (ASN) we found to be leveraged by ShadowSyndicate.

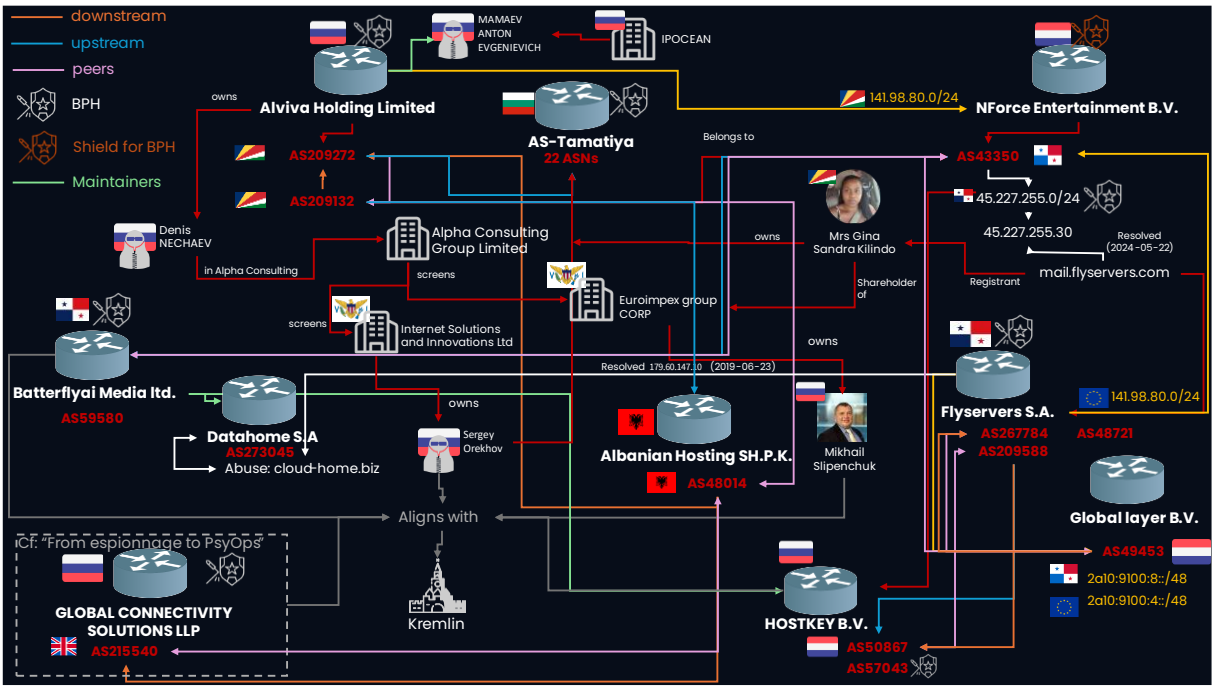


Figure 19 The figure illustrates a first fraction of the operators enabling ShadowSyndicate to leverage its attack infrastructure. We found a high degree of interconnected infrastructures through ASN ownership and routing relationships. Red lines represent downstream connections, blue lines indicate upstream providers, and purple lines show peer relationships. Entities marked with a shield and sword symbol are identified as bulletproof hosting (BPH) providers, while those with a flaming shield symbol are categorized as shields for BPH. Green lines denote network maintainers. National flags indicate the country of registration or operational origin, and resolved ips with dates pointing to historical associations. Individuals are linked to corporate entities through ownership, control, or shareholder roles.

The diagram presents a complex network of interconnected companies and autonomous systems (ASNs) involved in wide spectrum of malicious hosting operations. The AS-set AS-Tamatiya, a Bulgarian network cluster of 22 ASNs is detailed in the next figure.

Overall, we found a high degree of imbrication throughout peering, upstreams, downstreams, prefixes, DNS see to resolve IP belonging to another bulletproof AS being part of the same ecosystem (moderate confidence). The map also highlights obfuscation tactics such as layering ownership through multiple offshore jurisdictions such as Panama, Seychelles or us Virgin Islands and maintaining separate identities for infrastructure, registrants, and operators.

For instance, we found two ASNs to be present in the **Alpha Consulting leaks** as such that "Alpha Consulting Group Limited" screened "Euroimpex Group CORP" and "Internet Solutions and Innovations Ltd" while Mrs Gina Kilindo is the registrant of mail.flyservers[.]com. These entities are linked to various Russian oligarchs such as Mikhail Slipenchuk, Sergey Orekhov (perhaps Denis Nechaev ?).

Alviva Holding Limited, tied to the Seychelles, appears to be a key parent organization, owning AS209272 and AS209132, and is connected to **Nforce entertainment B.V.**, **AS-set Tamatiya**, **Alpha Consulting** and **IPOCEAN** located in **Russia** owned by MAMAEV Anton Evgenievich, who sells/rents highjacked IP spaces.

Several ASNs (e.g., AS48014, AS267784, AS209588, AS49453) appear to be downstream or peer networks. We already assessed in a previous analysis that Global Connectivity Solutions LLP (AS215540) aligns with Russian state interests (see main text).

We now focus on the AS-SET TAMATIYA tied to 22 underlying ASNs as presented in the scheme below.

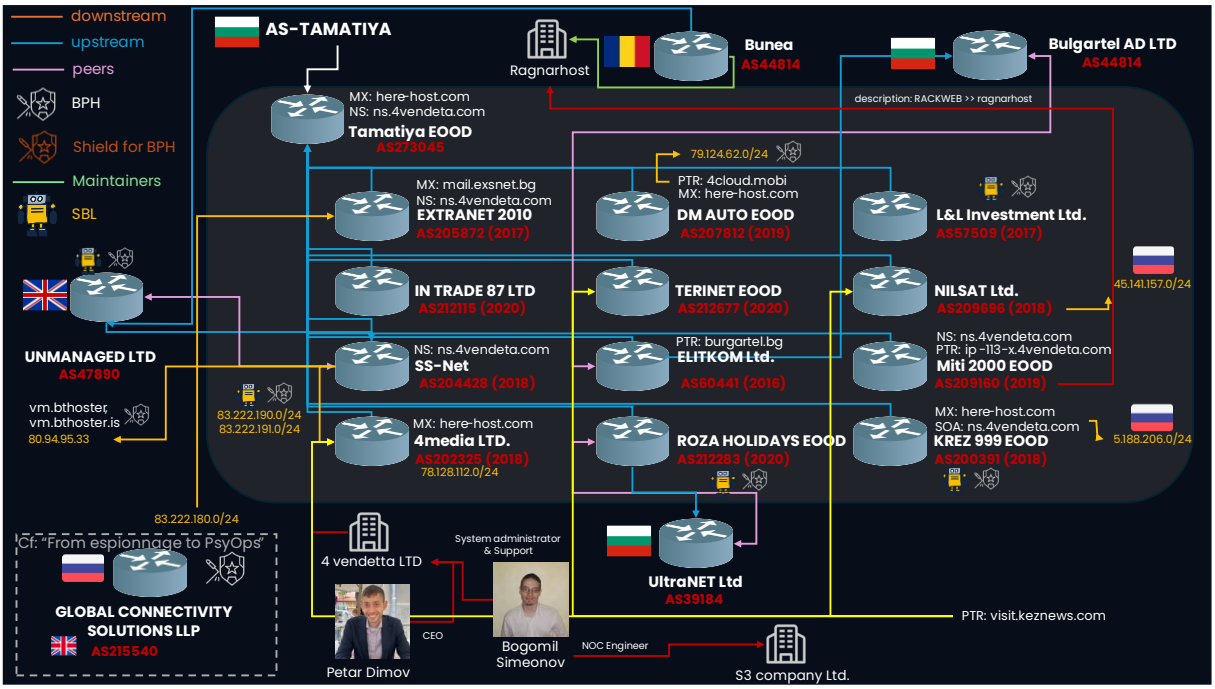


Figure 20 The diagram uses red lines for downstream connections, blue for upstream, and purple for peer relationships. Bulletproof hosting (BPH) providers are marked with shield icons, while shield providers for BPHs are shown with a flaming shield. Green lines indicate maintainers. Yellow robot icons labelled SPL represent listings on the Spamhaus Policy Blocklist. Country flags indicate the jurisdiction of each entity. IP blocks, PTR, MX, and NS records show infrastructure associations, while individuals are linked to companies by their roles in ownership, management, or technical support.

This figure maps a dense network of hosting providers and ASNs linked to AS-Tamatiya, a Bulgarian cluster of 22 autonomous systems. IP blocks, MX/NS/PTR records, and domain infrastructure (like here-host.com and 4vendeta.com) trace how hosting and DNS services are layered across various entities. Key individuals such as **Petar Dimov** and **Bogomil Simeonov** are identified with their roles in the front company 4vendetta LTD.

Overall, we assess that most of the underlying ASNs of AS-TAMATIYA share traits of bulletproof hosters operated from Russian.

We provide further insights in **Appendix** for every Autonomous System Numbers (ASN), which **enabled us to conjecture that ShadowSyndicate solely leverages a network of imbricated Russian BPHs**.

4. Conclusion

In this report we have uncovered a new heuristic that enables continued tracking of the group ShadowSyndicate, known for collaborating with a wide range of top-tier Ransomware-as-a-Service (RaaS) programs. The group has been observed using the same SSH fingerprint across 138 servers, echoing a TTP previously reported by Group-IB in September 2023.

We assess with moderate confidence that the group has access to a network of bulletproof hosters (BPHs) in Europe, which may function as Intelligence Agencies Hosting (IAH), but this assumption remains speculative. These BPHs, resilient to takedowns, operate through complex structures in

offshore jurisdictions but are believed to be managed from Russia, with some showing ties to Kremlin interests. They disguise their operations under the guise of legitimate services such as VDS, VPS, VPN, residential proxies, and DDoS protection layers.

We assess with good confidence that ShadowSyndicate leveraged SSH access to such a league of private BPHs (or even likely IAH) enabling APT and APT-like Russian, North Korea and even perhaps China intrusion sets to conduct both cyberattacks involving infostealers/ransomware.

Additional analysis revealed links between ShadowSyndicate infrastructure and other malicious operations, including Cl0p/Truebot, Citrix Bleed exploitations linked to Lockbit ransomware, as well as infrastructure associated Amos/Koi/Rustdoor Stealers and ToneShell backdoor.

To rationalize the sophistication level assessed as innovator (based on 0-day discovery/development of new attack) and an attack resource level assessed as organization possibly state-sponsored (leveraging a league of private BPHs), we suggest that ShadowSyndicate functions as an Initial Access Broker (IAB) fuelling not only Russian APTs and APT-like ransomware (high confidence) but also North Korean (moderate confidence) and Chinese (low confidence) APTs. It remains unclear whether ShadowSyndicate has a structured business model with formal clients or partners in cybercrime, or whether it represents a more fluid, hybrid threat actor.

Such a wide range of involved intrusion sets leveraging Shadow Syndicate's infrastructure in cyberspace, likely because it's an IAB, echoes recent developments observed on the battlefield, reports of North Korean soldiers joining the war in Ukraine, and, to a lesser extent, signs of Chinese alignment.

As us, the reader might have notice that "Exotic lily" could be a good candidate based on the TTP we could gather on this group and the findings we collected upon this investigation as well as the timeline.

> **initial access broker (IAB)** tracked as **Exotic Lily** by Google TAG **is also known as** DEV-0413 (**Microsoft)** or **Projector Libra** (Unit42) or TA580 (proofpoint) or Prophet Spider (CrowdStrike) or UNC961 (Mandiant) or gold melody (Secureworks).
> Working in close collaboration with **Exotic Lily,** RiskIQ tied with high confidence the cobalt strike BEACON payloads (**DEV-0413**) to **Wizard Spider** (based on the use of **unique Malleable C2 Profiles used by cobalt strike implants**). Exotic lily is known for distributing the Bumblebee loader that conducts reconnaissance and fetches Cobalt strike payloads.
> Exotic lily**acts, at least sometimes, as an Initial Access Broker for other intrusion sets**. We found **another IAB in the literature having strong TTP, infrastructure, victimology and sophistication level overlap with Exotic lily** that is tracked as **Zebra2104** by Blackberry since 2021**.**
> Summarising the literature about the intrusion set Exotic Lily, one can state it has conducted **low-volume, opportunistic web server compromises since at least 2016 focusing on organizations in North America** leveraging a wide range of n-days vulnerabilities and even 0-days. Exotic lily

However, we have seen ShadowSyndicate using Bumblebee loader only for one IP address (45.227.252[.]252), which hinders a direct attribution. It's interesting to note that this IP address was seen to resolve the domain devsecurityservices[.]com in March 2023 for a couple of months; that domain was cited in a Microsoft's legal action against Cobalt Strike as a service infrastructure to *infine* deploy a broad range of ransomware. The presence of this domain in a formal complaint aimed at actors such as DEV-0193 (Trickbot) and affiliates like Conti, LockBit or DEV-0237 Pistachio Tempest (FIN12) or DEV-0504 umbrella (six RaaS payloads since 2020 such as Blackcat) but also DEV-0206 (raspberry robin also cited as an IAB) known to be related to DEV-0243 (evilcorp). This overlap

suggests that ShadowSyndicate may be more deeply embedded in the ransomware-as-a-service ecosystem than previously understood.

5. Actionable content

Overall, blocking bulletproof networks is essential to prevent initial access attempts by ransomware operators or initial access brokers (IABs), who often use these networks for phishing, brute-forcing, or scanning exposed assets.

5.1. Indicators of compromise

Value	Type	Description
47890	ASN	UNMANAGED LTD
215540	ASN	GLOBAL CONNECTIVITY SOLUTIONS LLP
209272	ASN	Alviva Holding Limited
209132	ASN	Alviva Holding Limited
59580	ASN	Batterflyai Media ltd.
273045	ASN	DataHome S.A.
57043	ASN	HOSTKEY B.V.
50867	ASN	HOSTKEY B.V.
49453	ASN	Global layer B.V.
43350	ASN	NForce Entertainment B.V.
AS-TAMATIYA	AS-SET	22 ASNs (old, created in 2014)
AS-4VENDETA	AS-SET	22 ASNs (new AS-SET cloned from AS-TAMATIYA created in early 2021)
88.214.25.246	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
147.78.46.104	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
193.142.30.96	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
200.107.207.13	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
91.199.163.54	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
193.142.30.6	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
179.60.144.12	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
185.164.34.197	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
5.188.86.178	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
193.142.30.101	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
179.60.145.215	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)

179.60.145.211	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
45.227.255.111	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
5.188.86.172	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
88.214.25.249	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
88.214.25.250	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
88.214.27.52	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
88.214.25.196	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
88.214.25.197	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
5.188.87.27	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
5.188.86.216	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
179.60.149.207	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
193.142.30.116	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
5.188.86.190	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
147.78.46.158	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
5.188.86.179	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
147.78.46.137	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
37.156.246.170	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
92.51.2.73	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
5.188.86.174	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
193.29.13.158	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (extracted from FOFA the 2nd May 2025)
193.142.30.133	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
88.214.25.251	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
88.214.25.201	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
179.60.147.168	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)

141.98.82.219	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
194.34.239.43	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
179.60.149.250	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
78.128.112.209	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
45.156.248.208	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
45.156.248.207	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
193.142.30.76	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
193.142.30.186	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
45.182.189.92	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
45.182.189.115	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
185.232.67.14	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
194.34.239.37	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
147.78.46.162	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
45.145.20.216	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
45.145.20.218	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
147.78.46.156	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
147.78.46.93	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
88.214.26.33	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
46.161.27.157	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
141.98.82.241	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
45.227.252.219	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
45.227.252.252	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
45.227.252.220	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
45.227.252.244	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)

5.188.87.36	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
45.145.20.215	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
194.34.239.41	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
193.142.30.61	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
5.188.86.171	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
91.191.209.8	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
193.142.30.176	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
147.78.47.245	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
147.78.47.239	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
147.78.47.175	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
88.214.25.248	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
81.19.135.228	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
5.188.86.170	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
193.142.30.60	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
147.78.46.118	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
88.214.27.40	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
194.165.16.62	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
88.214.26.34	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
147.78.47.222	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
88.214.27.37	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
147.78.46.177	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
78.128.112.219	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
5.188.87.29	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
193.142.30.28	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)

185.99.3.97	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
193.142.30.32	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
193.142.30.43	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
193.29.13.167	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
193.142.30.224	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
45.182.189.113	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
5.188.86.230	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
46.161.27.159	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
5.188.86.74	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
46.161.27.156	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
45.227.253.21	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
5.188.86.214	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
179.60.149.241	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
179.60.149.206	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
193.142.30.202	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
193.142.30.67	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
193.142.30.135	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
31.41.33.239	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
193.142.30.29	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
5.188.87.35	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
5.188.206.94	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
193.142.30.196	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
193.142.30.114	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
5.188.86.211	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)

45.227.252.232	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
193.142.30.198	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
193.142.30.235	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
193.142.30.119	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
194.34.239.38	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
88.214.25.230	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
45.227.255.216	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
147.78.46.192	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
179.60.147.182	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
78.128.112.206	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
78.128.112.132	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
179.60.147.170	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
5.188.206.213	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
78.128.112.131	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
45.227.255.28	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
45.227.255.189	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
193.142.30.141	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
179.60.147.79	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
179.60.149.247	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
193.142.30.239	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
147.78.47.172	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
5.188.87.59	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
193.142.30.31	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
194.34.239.33	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)

5.188.86.232	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
5.188.87.46	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
5.188.87.62	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
45.182.189.103	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
193.142.30.87	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified from December 20, 2024, to May 2, 2025)
141.98.82.243	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
147.78.47.115	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
147.78.47.177	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
179.60.149.242	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
179.60.149.254	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
193.142.30.103	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
194.34.239.34	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
37.156.246.166	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
179.60.149.212	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
179.60.149.219	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
179.60.149.220	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
179.60.149.231	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
193.142.30.109	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
193.142.30.132	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
193.142.30.14	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
193.142.30.222	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
31.41.33.240	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
45.227.255.31	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
46.161.27.160	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)

5.188.86.168	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
5.188.86.169	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
5.188.86.19	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
5.188.86.203	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
5.188.86.24	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
88.214.25.240	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
88.214.25.253	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
88.214.25.254	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
88.214.26.22	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
91.238.181.225	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
91.238.181.239	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)
91.238.181.250	IPv4-Addr	Secure Shell (SSH) fingerprint of ShadowSyndicate (verified on December 20, 2024; SSH key not found after verification on May 2, 2205)

5.2. Recommendations

- Monitor all traffic from/to any IP address belonging to above-mentioned autonomous systems and organizations
- Incorporate the IOCs from this report into your Threat Intelligence platform and/or communicate them to your SOC to anticipate and detect these threats
- 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 distrusted sources in your company
- Raise awareness on the risk of external emails with attachments in your company
- To preempt double extortion scheme, craft fake documents (financial, cyber insurance, employee data falling under GDPR) that will alert blue teams once opened, using services such as, for example, Canarytokens

6. Sources

- https://www.group-ib.com/blog/shadowsyndicate-raas/
- https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/

7. Appendix

*Batterflyai Media ltd. (**AS59580**)*

Upon a black Hat conference on 2016 Batterflyai Media ltd was **related to Iran** and assessed as **Bullet Proof Hoster**. The name "**AbdAllah"** (aka-Mykhailo Rytikov,- Webhost,-Whost) is also mentioned. It was shown that the IP address 193.142.30[.]30 **resolved Maza and Joker's stash domains** and their **jabber servers**, two old **elite cybercrime Russian-speaking forums respectively** massively hacked and shut down by the **FBI/Interpol** in late 2020.

The **Ukrainian police** with the help from the US/UK arrested **Mykhailo Rytikov in Odessa (as he is a Ukrainian national),** in 2019 that is related to older indictments of **four other Russian citizens**. This old wolf was already accused by the US of **having enabled vit its BPH services to steal 160 million "credit card numbers"** in 2013.

Cyber Scoop reported that **Mykhailo Rytikov** allegedly **bribed Ukrainian officials**, including members of the SBU (Security Service of Ukraine), to avoid prosecution, get tipped to empty places before raids and secure his release after arrests. These bribes reportedly helped him **maintain operations despite law enforcement interest** and facilitated his protection for years while supporting cybercriminals with hosting services.

Moreover, one of the **Mykhailo Rytikov**' notorious clients is known as **Evgeniy Bogachev** (aka Slavik), on which we recall previous intel from the report **ThreeAM / 3AM** ransomware 6c12d810-5f61-467c-8d6b-61196cbd5125.

> ANSSI reported that Yakubets was the leader of the infamous "Business Club" based in Moscow. This club collaborated with M. Bogatchev (alias Slavik, lucky12345), who created the malware-as-a-service Zeus (alias Zbot) to produce new variants with uncovered features. In September 2011 GameOverZeus (botnet GoZ) was now able to deploy Cryptolocker Ransomware. Such a botnet will be used by the **FSB** to conduct *"cyberespionage operations or DDoS attacks by 'patriotic hackers during military conflicts"* according to Recorded Future.
> **Yakubets** (together with Igor Turashev) worked directly for the **Russian FSB** in 2017. It would seem Yakubets attempted to obtain a security clearance in 2018 in to work with Russian classified information. It is even more important to underline that **Yakubets** was tasked by the FSB to acquire "confidential documents through cyber-enabled means and conducting cyber-enabled operations on its behalf", most of the targets being in the USA, and UK.

More recently another trusted source IPfire vetted **Batterflyai Media Ltd**. as a:

*"**bulletproof ISP** and **IP hijacker**, **claims to be located in CH, but traces to NL** [.] ISP located in **RU**, but some RIR data for **announced prefixes contain garbage**".*

Regarding **RIPE database entry** associated with this ASN, one can find sine qua non ingredients of BPHs. The physical address **registered is in Panama** (an offshore jurisdiction), while maintainers (mnt-ref/mnt-by) fields point at two other organizations **on which ShadowSyndicate relied via SSH access**, namely **DataHome S.A**. and **HOSTKEY**.

Moreover, on the IP subnet **147.78.46.0/24** that belongs to **Batterflyai Media ltd.**, we found that the IP address 147.78.46[.]40 was used as a C2 in an attack campaign against Ukraine (conducted by UAC-0099 according to Deepinstinct); UAC-0099 overlaps with infamous Gamaredon group (see G0047).

DataHome S.A.

A single Autonomous System Number (ASN) **AS273045** was registered to **DATAHOME S.A.**, a network services provider based in **Panama**. Established on July 26, 2023, and registered with LACNIC (Latin America and Caribbean Network Information Centre), this ASN is associated with the domain cloud-home.biz.

The responsible according to Domaintools of the domain cloud-home[.]biz (created on 2019-08-14) is **Ricardo Emilio Vasquez located in Panama** (address: Global Bank Tower 18th Floor 50th Avenue 1801, 83218)**, an offshore jurisdiction.**

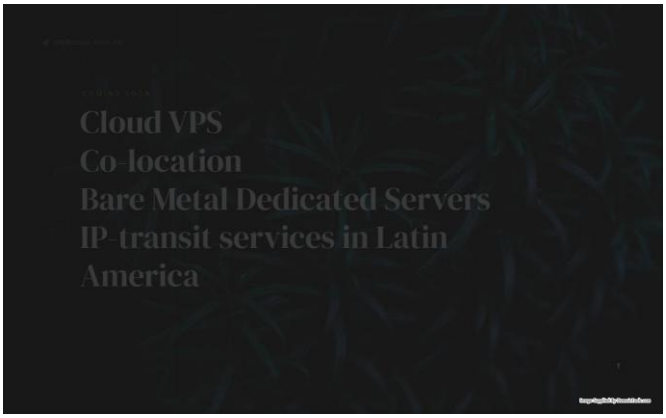


Figure 21 Screenshot taken from Domaintools on 2022-09-10 of the Abuse contact info (cloud-home[.]biz) of Datahome S.A. organization.

Ns2.cloud-home.biz was seen to be resolved by 190.123.44.119 (Panamaserver.com, AS52284) since 2024-02-07 according to Domaintools. All other resolutions point to 142.202.136.224 (Panamaserver.com, AS52284) from 2021-01-30. The website offshore[.]cat, that reviews so-called "offshore services", has listed PanamaServer as being a "verified" offshore hoster that accepts Crypto, paypal, Visa & Mastercard, only requires email request confirmation to open an account, making them an attractive hoster for cybercriminals.

The ISP IP information from Domaintools unveils **EXA Solutions (abuse@corpexa.com)** from which 72 domains (most of which hold a high-risk score) are related. Amongst those malicious domains one targeted the French banking sector throughout the **bank Société Générale** "soxiete-generale[.]fr" (first seen 2022-06-22).

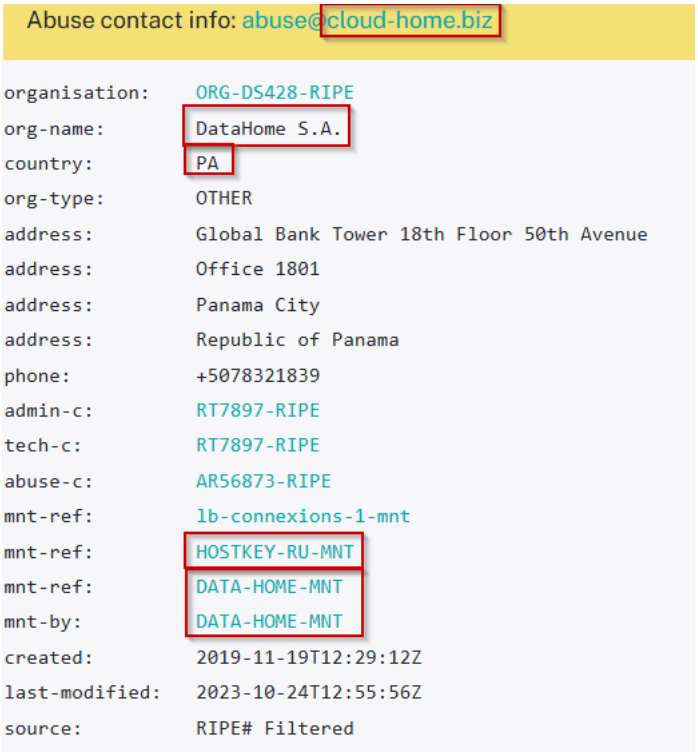


Figure 22 DataHome S.A. was registered in Panama (an offshore jurisdiction). The latter is also maintained by a Russian organization called Hostkey (that was also leveraged by ShadowSyndicate). DATA-HOME-MNT is also registered as 'mnt-by'. Screenshot taken from RIPE.

The abuse email goes by cloud-home.]biz.

The domain cloud-domain.]biz was first seen to resolve to the following IP address 179.60.147[.]10 according to VT in 2019-06-23 associated to the **ASN Flyservers S.A**. AS209588).

From a trusted source, we found that the same organization DataHome S.A. was assessed to be related to a VPN provider named "Perfect Privacy LTD" that was in Brazil in 2021 associated to the AS207688.

Looking at most recent screenshots taken from Urlscan one can observe that it mostly hosted generic porn scam and dating apps. More recently on the last known ASN of DataHome S.A. (AS273045) we found via most recent screenshots from Urlscan that some IPs are linked to boolka injecter

DataHome S.A. is also maintained by a **Russian** organization called **Hostkey**. It's important to note that **ShadowSyndicate also used several servers related to the Hostkey infrastructure** (see next paragraph dedicated to that suspicious infrastructure).

Global Layer B.V.

Global layer B.V. originally belongs to **24x7 Holding B.V.**, a **Netherlands-based conglomerate**, specializing in internet infrastructure services.

Global Layer B.V. is a **Netherlands-based provider specializing in large-scale IP and capacity services** (website http://www.global-layer.com). Their offerings include IP transit, managed colocation, and transport services, leveraging a carrier-grade platform with 100G and 400G backbone connectivity. The company maintains a presence in over **10 data centers across Europe and South Africa**, aiming to deliver high-performance, scalable, and redundant network solutions.

Global layer B.V. abuse email contact is **channelnet.org** according to **RIPE** database. While pivoting on this domain we found via the hosting history of Domaintools that it resolved to the given IP address 5.188.86[.]28 on 2020-01-17 but also (channel.ie) on 2019-10-22. Domaintools provided in addition another domain (scsvcreg[.]com, first seen 2024-04-12) that was associated with **Blacksuit** (ex trickbot/Conti group) cobalt strike infrastructure (watermark **1580103824**, see maintext).

Pivoting again on the abuse email contact, we found that it is shared with two prefixes related to another organization on which ShadowSyndicate rely, which is NForce Entertainment B.V. Indeed, The domain **channelnet.org** resolves to the IP address **141.98.80.154**, which is part of the **141.98.80.0/24** subnet announced by **AS43350**, operated by **NForce Entertainment B.V..** This IP address is also utilized for the domain's MX (mail exchange) records, indicating that NForce provides both web and email hosting services for this domain.

More precisely for the prefixes on which Shadow Syndicate has access at least for some servers (5.188.86.0 - 5.188.87.255, description**: pool for VPS and Cloud hosting**) we found that the abuse contact info points to Russia (abuse@pindc.ru, responsible organization: Petersburg Internet Network ltd.)

This domain appears in a recent report published by Unit42 reporting on Clop ransomware group distributing victim data using torrents. One original seeding server was identified as *95.215.0[.]76= **AS34665** Petersburg Internet, St. Petersburg Russia (hosting company offerings at pindc[.]ru).*

The ***AS34665*** was involved in prefix hijacking from other ASNs as reported on 2022 according to researchers, which resonate with a TTP that we mentioned several times for hosters on which ShadowSyndicate rely. The same year IPFire reported that some RIR data of this ASN for announced prefixes "contains garbage" and traces back to Germany (instead of Russia).

In addition, we found via the name server history provided by Domaintools that Internet-spb[.]ru located in Moscow precedented Pinspb.ru.

HostKey

The Autonomous System Number (ASN) **AS57043** is the primary ASN for HOSTKEY B.V., allocated on July 7, **2011**, supporting a significant number of IPv4 and IPv6 addresses, and hosting nearly 10,000 domains.

HOSTKEY has indeed expanded its operations **beyond Russia**, establishing a presence in the **Netherlands** (**AS50867** allocated in late 2020) and the **USA** (AS395839 allocated around 2017), and offers services such as colocation, equipment leasing, and cloud solutions.

Mir Telematiki Ltd and HOSTKEY are essentially **the same entity** operating under different names. Mir Telematiki Ltd, a Russian telecommunications company based in **Moscow**, has been providing hosting and rental services since 2007 under the trademark **HOSTKEY**.

Mir Teklematiki Ltd was cited as under **the surveillance of the NSA** by **Der Spiegel in 2014** and hosting **Wikileaks's infrastructure** in early 2014 by the Newyorker. We verified such a latter statement and it's indeed the case as **WikiLeaks** publicly confirmed that at least the IP address 141.105.65[.]113 is one of theirs (see figure below).

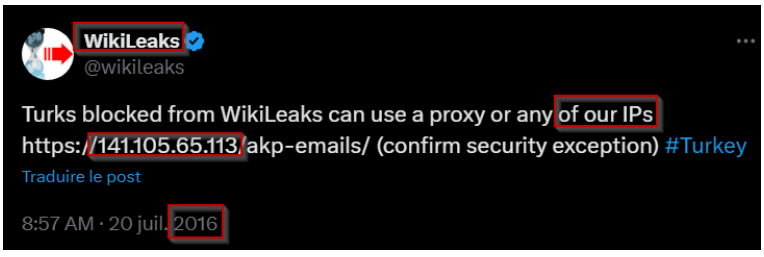


Figure 23 Tweet from official twitter account of Wikileaks stating that the IP address 141.105.65[.]113 is one of its ips that can be used as a proxy to bypass censorship. This IP address belongs to Hostkey B.v aka Mir Telematiki Ltd.

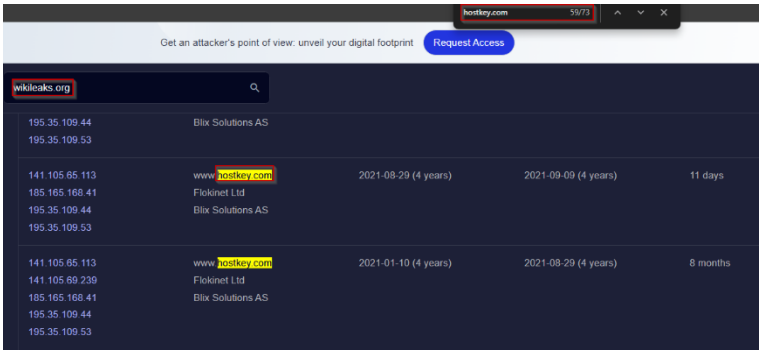


Figure 24 Screenshot taken from Securitytrails history data of the domain wikileaks.org. It shows that wikileaks.org is frequently resolved by an IP address that belongs to the Russian Hostkey infrastructure from 2014 till 2021.

Moreover, we found multiple consistent resolutions thanks to **Securitytrails historical data** between 2014 and 2021 (see Figures below).

The abuse email of Hostkey infrastructure is abuse@hostkey.ru or abuse@hostkey.nl. **The BPH covered in this analysis Flyservers S.A. (AS209588)** is listed as a peer in the BGP routing database or system used by **Hostkey B.V.**.

Via Domaintools while pivoting on support@hostkey.com, we found tens of related domains with a permutation in TLDs (*e.g.*, hostkey.tr, hostkey.io, hostkey.uk etc). We also found hpcsol.ru and hcpsol.com (registered in 2016) that points to High-Performance Computing as a Service (HPCaaS) offers located in **Moscow** (Barabannyy per., 4, bld.4).

From the prefixes found in BGPtool we found that LLC ***"Server v arendy"*** is also located at the same address **in Moscow**. In contrast with **Hostkey B.v.**, we found multiple mentions of LLC ***"Server v arendy"*** in the report of GroupIB covering **ShadowSyndicate infrastructure** in 2023.

This ASN was ranked in the **top 10 most common second stage ones already in December 2021**. @Bushidotken tagged the **AS57043** that belongs to **Hostkey B.v**. as a **BPH** in February 2023.

While pivoting on IP 185.130.225[.]69 (HostKey B.B. AS57043 **ServerKing B.V.Netherlands**) resolving the hostname ns2.hostkey.com we found a link with **Temok IT services DMCC in Dubai**. The registered address seems however to be a very common registered address for many companies.

The **registrant Name is "OLEG CALUGHER"**, which is consistent with a **Romanian citizen** who has registered two IT companies in the UK, including **TEMOK IT SERVICES LTD**. A Pakistani **MALIK, Hisham is also cited as a director** and **TEMOK IT SERVICES LTD** was dissolved in 2017 in UK. The other company **APPRAN IT SERVICES LTD** still runs and was registered with another **Romanian** citizen **COTRUTA, Victor** (but located in Moldova)**.**

Albanian Hosting SH.P.K.

Though ShadowSyndicate has a few SSH access to servers that belong to Albanian Hosting we found no malicious activities to those IP addresses.

Albanian Hosting SH.P.K. (**AS48014**), operating under the brand name **AlbHost**, is a leading web hosting and IT services provider based in Gjakovë, **Kosovo**. Established in 2008, the company has built a strong reputation in Albania and Kosovo for delivering reliable and affordable hosting solutions, including shared hosting, VPS/VDS, dedicated servers, and domain registration services.

Albanian Hosting SH.P.K. (AS48014) has a direct network relationship with **Alviva Holding Limited** (AS209272). Specifically, Alviva is listed as both a **Peer** and a **Downstream** of Albanian Hosting,

indicating a mutual interconnection (peering) and a downstream transit relationship, respectively. This means that **Albanian Hosting provides internet connectivity or transit services to Alviva**, while also exchanging internet traffic directly with Alviva through a peering arrangement. This connection suggests a collaborative or service-based relationship between the two entities, with Albanian Hosting playing a role in supporting Alviva's network infrastructure.

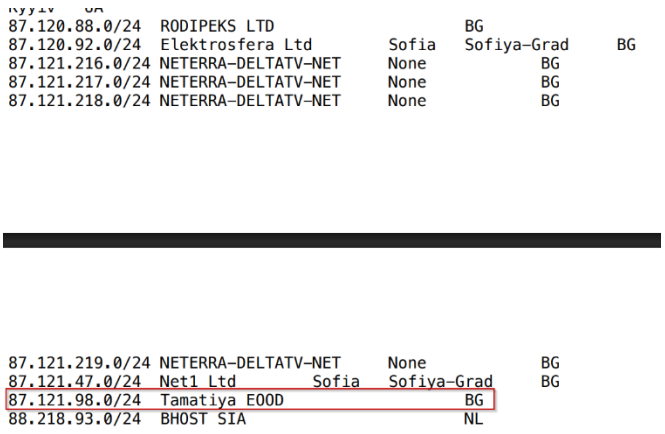
Besides, the **RIPE entry** for "Albanian Hosting SH.P.K." (ORG-AHS27-RIPE using the domain **albahost.net**) shows the **use of "Dummy address** for ORG-AHS27-RIPE" and the non-functional email unread@ripe.net. The **MNT-NETERRA**, which suggests an upstream or partner relationship with **Neterra**, a well-known carrier and service provider in the region.

4media Ltd.

AS202325 is an Autonomous System Number (ASN) assigned to **4Media Ltd**., a hosting and internet infrastructure provider based in **Bulgaria** (35, Ivan Vazov str, Sopot, Bulgaria according to RIPE). The company operates under the domain **4media.bg** (abuse@4media.bg) and has maintained its ASN since June 1, 2018.

AS202325 appears to be a small AS that relies entirely on **AS50360** (**Tamatiya EOOD, website:** 4vendeta.com) for both transit and potentially some level of peering. This single-homed *ASN* ***has* no known downstreams**, which aligns with low-scale or personal ASN usage *but is* ***also a trait for bullet proof hosters***.

*Figure 25 Screenshot taken from Brian Krebs blog post entitled "**Stark Industries Solutions: An Iron Hammer in the Cloud**".*



As shown in the figure (at the left) **Tamatiya EOOD** owns a dedicated IP space (87.121.98.0/24) announced by the **infamous Stark industries** (successor of IP Oleinichenko Denis, which was at 99% of RDP attacks against France) as shared by Brian Krebs in a snapshot of May 2024. Besides we also found eighteen IP spaces for Nettera in Bulgaria.

The subnet 87.121.98.0/24 was announced by **AS215590 (DpkgSoft International Limited)**. It appears to be using a consistent reverse DNS naming scheme, pointing to 4vendeta.com (autogenerated reverse DNS entries). The IP WHOIS holder points to **Neterra** Ltd. (ORG-NL38-RIPE) with the following abuse contact abuse@neterra.net.

We found that **DpkgSoft International Limited** is being routed **solely through AS49418**, known as **Netshield Ltd**. This organization is a **controversial DDoS protection provider** registered under the name of **Pavlo Misiura, a Ukrainian citizen** using a virtual office in London (together with two Russians **DIABIN, Aleksei** and **MUSKAFIDI, Konstantin**). Despite having non-functional websites (netshield[.]ltd and netshield[.]pro), Netshield quickly established peering agreements with carriers in Russia and Germany starting in 2023, according to Quirium.

We found that **Pavlo Misiura** registered another suspicious organization called "CLOUD HOSTING SOLUTIONS LIMITED" (together with another Russian citizen, **SHARAPOV, Nikita**), which also points to a single peer and upstream provider: Netshield.

We started to observe malicious content hosted by AS199785 since February of this year (see ThreatFox ASN report). A close scheme was found for **INTERNATIONAL HOSTING COMPANY LIMITED** registered by **MUSKAFIDI, Konstantin** (see previous mention of this Russian citizen) associated to the **AS216127** (malicious content started to emerge around mid-2024 according to threatfox database).

Netshield is part of a growing network of **DDoS protection ASNs, which are known to serve bulletproof hosting operations and infrastructure involved in the hosting of front proxies for disinformation** like **Dpkgsoft International Limited, according to** Quirium.

So, this IP space is owned by **Neterra** but announced by **DpkgSoft International Limited**. This is a **common tactic** where suspicious actors lease IP space from reputable LIRs like **Neterra** to avoid scrutiny but then repurpose the address block for suspicious or malicious use. Here they added another layer of protection via **routing the traffic via the front proxy Netshield.**

Now focusing on 4media we found the following domain names (4vendeta.com) thanks to pivot on the email address registrant (found via Domaintools with 4media.bg):

- 4media.bg
  - MX :mail.here-host.com
- exstranet.bg (A record: 195.230.25.66 => 195.230.25.0/24 => AS50360 Tamatiya EOOD)
- dm-auto.eu, not active (A record: 195.230.24.19 => 195.230.24.0/24 => AS50360 Tamatiya EOOD)
  - MX :mail.here-host.com
  - NS : ns1.fibernet.bg ; ns.4vendeta.com
  - Bad packets by Okta recommended on Dec 2022 to drop all traffic from **AS207812**.
- fibernet.bg (A record: 195.230.25.250 => 195.230.25.0/24 => AS50360 Tamatiya EOOD)
- 4vendeta.com (A record: 79.124.60.2 => 79.124.60.0/24 => AS50360 Tamatiya EOOD)
  - MX :mail.here-host.com
- krez999.com, not active (A record: 195.230.24.19 => 195.230.25.0/24 => AS50360 Tamatiya EOOD)
  - MX :mail.here-host.com
  - NS : ns1.fibernet.bg ; ns.4vendeta.com
  - SOA: ns.4vendeta.com

The email address registrant thus links directly **4media Ltd** (4media.bg) to **Tamatiya EOOD** (4vendeta.com). We also see a direct link **krez999.com** associated with the ASN 200391 (**KREZ 999 EOOD**) from which ShadowSyndicate also owns servers (via its common SSH key aforementioned).

As far as **4Media Ltd**. Is concerned we found a tweet of.@banthisguy9349 *relaying on* X *(ex-twitter) an assessment of* Spamhaus *vetting* **4Media Ltd**. (212.70.149.0/24) *as* ***a bullet proof hoster*** *already in late* ***2023.*** .@banthisguy9349 also highlighted traffic connectivity between AS 204428 (**SS-Net**), and upstreams AS50360 - Tamatiya EOOD, AS47890 - UNMANAGED LTD.

We also provided in a precedent analysis **a link between SS-Net and another bulletproof provider** named "**BtHoster**" (*cf. BtHoster networks: Identifying noisy ISPs emitting high levels of malicious traffic, 84b4ab89-5a7d-4a8a-819e-cc7bac5a2865*).

BtHoster LTD – AS 198465 is a known bulletproof provider named "**BtHoster**", that used to operate an autonomous system of the same name: *BtHoster LTD* – **AS198465**, also registered in the United Kingdom.
BtHoster advertises the bulletproof nature of his business stating that activities such as "*scan / brute / cracking*" are allowed to be operated on its servers. Additionally, pre-configured masscan servers can be rented with routing capacities maxing 1300kpps.

We found **vm.bthoster.is and vm.bthoster**.com to be present in **the latest FDNS data** of **80.94.95.0/24 prefixes of SS-Net** AS204428, which likely host the new domain of this BPH services while their new Telegram channel from 4th of march 2025 is t[.]me/bthostercomis.

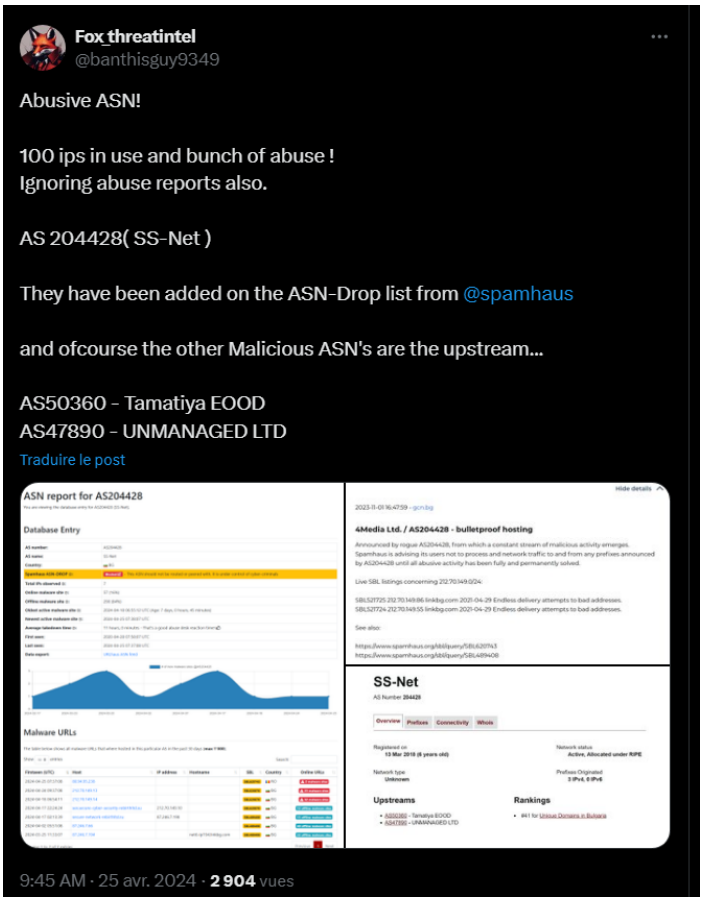


Figure 26 Overview of AS204428 ("SS-Net") abuse activity. The graph displays the volume of malicious URLs and abuse incidents linked to AS204428 over time. SS-Net has been added to the Spamhaus ASN-Drop list due to persistent malicious activity and non-responsiveness to abuse reports. Upstream providers AS50360 (Tamatiya EOOD) and AS47890 (UNMANAGED LTD) are also associated with this activity Screenshot taken from X (ex-twitter).

Seeking to get the big picture, we thus investigated on **AS50360 (Tamatiya EOOD)**, which, is a **Bulgarian** hosting provider with a diverse set of **upstream connections** and a clientele comprising **various downstream** networks. **Tamatiya EOOD** offers substantial network infrastructure and ***open-peering* policies**. According to riskrecon it accounted in 2023 for 1/3 of the top IP addresses engaging **in malicious activity** and was **in the top 10 of attacking AS organizations** according to Baffinbay (Mastercard).

*A*ssociation with **spam activities** and *hosting* anonymizing services *(we found 7 proxies including Tor via* Spur*)* have raised concerns within the cybersecurity community. @banthisguy9349 *even assessed* **AS50360** *on* X *(ex-twitter) as* ***a bullet proof hoster*** *already in late* ***2023 because of*** **the persistence of the botnet TBOTNET** *(aka hailbotnet, hailbot)* despite previous abuse reports.

We found later in the RIPE database that precedent ASNs are part of the **RIPE AS-SET AS-TAMATIYA**. Such a **cluster or collection of 22 Autonomous Systems** (ASNs) is grouped under a common policy, usually for routing, peering, or administrative reasons, which resonates with our previous findings.

We then found another cluster named AS-4VENDETA that once compared to the previous umbrella looked very similar to as shown in the figure below.

AS-4Vendeta				
Countries	Member	ASN Count/Whois Name	v4 Count	v6 Count
	AS50360	Tamatiya EOOD	25	1
	AS205872	EXTRANET 2010	2	0
	AS60441	ELITKOM Ltd.	9	0
	AS199173	TechnoLux Ltd.	23	0
	AS57509	L&L Investment Ltd.	1	0
	AS204428	SS-Net	4	0
	AS34368	ZONATA - INVEST sLLC	45	1
	AS202325	4Media Ltd.	4	1
	AS200391	KREZ 999 EOOD	1	0
	AS58271	Tyatkova Oksana Valerievna	0	0
	AS209696	NILSAT Ltd.	1	0
	AS209272	Alviva Holding Limited	4	0
	AS209272	Alviva Holding Limited	4	0
	AS206370	Next Generation Technologies Ltd	0	0
	AS209160	Miti 2000 EOOD	1	0
	AS209282	we.systems AG	3	4
	AS209128	Evresis SA	1	0
	AS208410	ARTKOM.NET LLC	2	0
	AS212283	ROZA HOLIDAYS EOOD	4	0
	AS212115	IN TRADE 87 LTD	4	0
	AS212677	Terinet EOOD	2	0
?	AS205092	AS205092	0	0
?	AS41466	AS41466	1	1

AS-TAMATIYA				
Countries	Member	ASN Count/Whois Name	v4 Count	v6 Count
	AS50360	Tamatiya EOOD	25	1
	AS205872	EXTRANET 2010	2	0
	AS60441	ELITKOM Ltd.	9	0
	AS199173	TechnoLux Ltd.	23	0
	AS57509	L&L Investment Ltd.	1	0
	AS204428	SS-Net	4	0
	AS34368	ZONATA - INVEST sLLC	45	1
	AS202325	4Media Ltd.	4	1
	AS200391	KREZ 999 EOOD	1	0
	AS58271	Tyatkova Oksana Valerievna	0	0
	AS209696	NILSAT Ltd.	1	0
	AS209272	Alviva Holding Limited	4	0
	AS209272	Alviva Holding Limited	4	0
	AS206370	Next Generation Technologies Ltd	0	0
	AS209160	Miti 2000 EOOD	1	0
	AS209282	we.systems AG	3	4
	AS209128	Evresis SA	1	0
	AS212283	ROZA HOLIDAYS EOOD	4	0
	AS212115	IN TRADE 87 LTD	4	0
	AS212677	Terinet EOOD	2	0
	AS207812	DM AUTO EOOD	1	1
?	AS205092	AS205092	0	0
?	AS41466	AS41466	1	1

Figure 27 Comparison of (left) AS-VENDETA and (right) AS-TAMATIYA clusters of ASNs. A strong overall overlap is shown via an almost perfect match of ASNs except for DM AUTO EOOD that is not present anymore in AS-4VENDETA that was "replaced" by ARTKOM .NET LLC.

The two ASN clusters list 22 ASNs, while the principal difference is the presence of **AS207812 - DM AUTO EOOD** in **AS-TAMATIYA**, which does not appear in **AS-4VENDETA** (whereas ARTKOM.NET LLC, AS208410 was added). In terms of IP prefix count, AS-**4VENDETA** has slightly more IPv4 prefixes (131 vs. 129), while **AS-TAMATIYA** has one more IPv6 prefix (9 vs. 8).

A migration from **AS-TAMATIYA** to **AS-4VENDETA** could thus have served to hide **AS207812 - DM AUTO EOOD**, which is a lead that we have investigated.

As shown in the figure below **CLOUDVPS-NET** is indeed related to 5.181.86.0/24 and 77.83.36.0/24 prefixes according to RIPE database (we used Full Text Search).

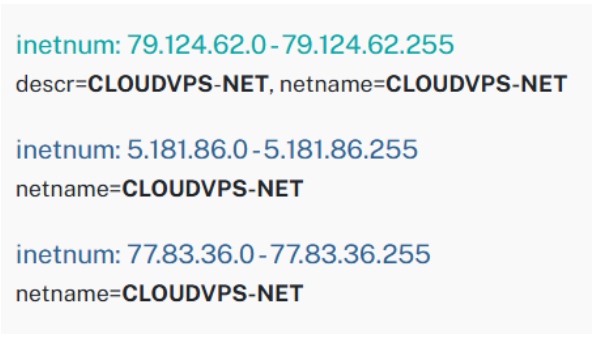


Figure 28 The image highlights how the "netname" CLOUDVPS-NET network is linked to three specific prefixes according to the RIPE database.

As shown in the figure below both prefixes 5.181.86.0/24 and 77.83.36.0/24 do exhibit commonalities such as mnt-by "**PITLINE".** The latter is a **Ukrainian** ISP provider upstreaming via RETN located at Northern Kharkiv front of the Russo-Ukrainian War. Another commonality is the "Responsible organization" that is **Internet Solutions & Innovations LTD** with the associated abuse contact info abuse@**4cloud.mobi** (4cloud naming could recall 4vendeta, low confidence).

Internet Solutions & Innovations LTD. is located at National Cultural Centre 865 P.O. Box 1494, Victoria Mahe, **Seychelles** (according to RIPE database)**,** thus an **offshore jurisdiction**.

We could retrieve this shell company in the Pandora papers (data from **Alpha Consulting**), which was tied from 20-MAR-2019 to a **Russian person named Sergey Orekhov** (located at 181 PERVOMAJSKAYA STR., APT. 77, JOSHKAR-OLA, MARIJ EHL, RUSSIA). The mention of **Alpha Consulting** suggests that this shell company was screened via the same scheme as demonstrated in the paragraph on **Flyservers S.A**. (see main text for details).

Responsible organisation: Internet Solutions & Innovations LTD. Abuse contact info: abuse@4cloud.mobi	
inetnum:	5.181.86.0 - 5.181.86.255
netname:	CLOUDVPS-NET
country:	EU
admin-c:	NOC299-RIPE
tech-c:	NOC299-RIPE
abuse-c:	NOC299-RIPE
status:	ASSIGNED PA
mnt-routes:	ISI1
mnt-domains:	ISI1
org:	ORG-ISI14-RIPE
mnt-by:	PITLINE-MNT
created:	2021-07-30T12:45:41Z

Responsible organisation: Internet Solutions & Innovations LTD. Abuse contact info: abuse@4cloud.mobi	
inetnum:	77.83.36.0 - 77.83.36.255
org:	ORG-ISI14-RIPE
netname:	CLOUDVPS-NET
country:	EU
admin-c:	NOC299-RIPE
tech-c:	NOC299-RIPE
abuse-c:	NOC299-RIPE
status:	ASSIGNED PA
mnt-routes:	ISI1
mnt-domains:	ISI1
mnt-by:	PITLINE-MNT
created:	2021-02-02T11:12:58Z

Further probing suggests that **Sergey Orekhov**, alongside **Vladyslav Nechyporenko**, cofounded **Nadezda** Invest D.o.o. in **Montenegro**, a firm involved in the trade of **titanium tetrachloride**. This company falls in the range of strategic companies for the Kremlin in the context of the **war with Ukraine as Titanium** is manufactured to be used for war airplanes and missile production.

Overall, our findings suggest AS-**Tamatiya/4vendeta acts as a core or umbrella organization** for numerous smaller or shell hosting firms, often **Bulgarian**-registered to malicious activities. Moreover, we suspect that it's operated from Russia as we found several links such as

- 5.188.206.0/24 subnet managed by **KREZ 999 EOOD** (AS200391) was registered under RIPE to an entity named ru.pin (aka **Petersburg Internet Network** Ltd based in Russia). The latter owns the block but are leasing it to KREZ 999 EOOD, or transferred operational use to KREZ 999 without updating WHOIS.
- 45.141.156.0/22 subnet managed by **NILSAT Ltd**. (AS209696) was acquired in 2020 by **Mayak Smart Services Ltd**.(under the ASN AS44345 and has upstream connections with major Russian ISPs.), from **Neterra** Ltd.
- We linked a prefix of the ASN (DM Auto EOOD) missing from the new cluster of ASNs named AS-4vendera to **Sergey Orekhov,** a Russian person. We suspect that the owner of such company could also be the owner of **Nadezda Invest D.o.o**, a key asset in the Russian defense industry.

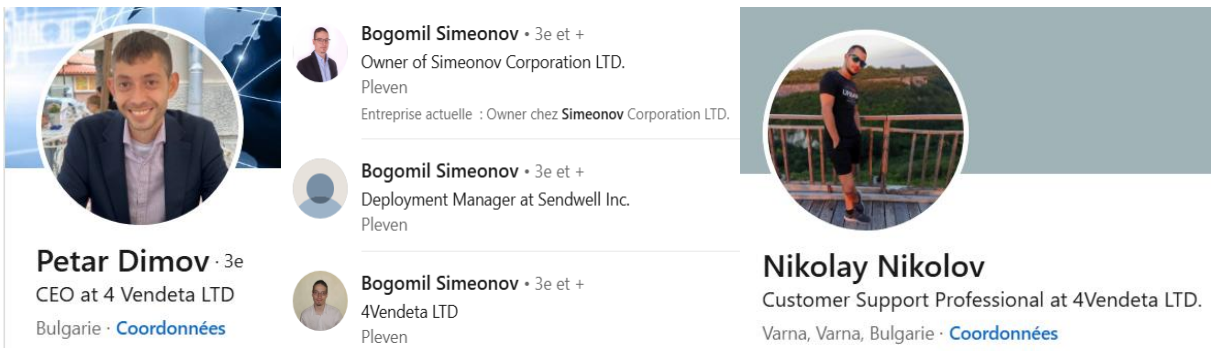


Figure 29 Left: The CEO at 4Vendeta LTD is Petar Dimov as mentioned on LinkedIn and information we could cross check from domaintools while pivoting around the registrant email address hostmaster@fibernet.bg. Center: Bogomil Simeonov has been the System administrator & Support since 2014 as mentioned in one of his LinkedIn' profile, of HereHost LTD between 2014 -

2017 and at S3 company since 2023. Right: Nikolay Nikolov is the Customer Support at 4vendeta LTD. as mentioned on his LinkedIn' profile.

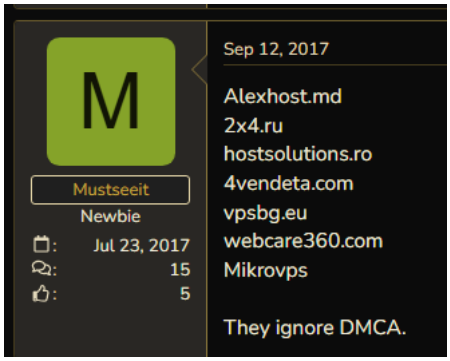
The CEO **at 4Vendeta LTD is Petar Dimov** as mentioned on LinkedIn (see Figure below) and information we could cross check from domaintools while pivoting around the registrant email address hostmaster@fibernet.bg. We also found n.nikolov@4vendeta.com and b.simeonov@4vendeta.com email addresses to be related respectively to **Nikolay Nikolov** (Customer Support Professional at 4Vendeta LTD.) and **Bogomil Simeonov** (**System Administrator & Support**).

Bogomil Simeonov has three LinkedIn profiles, and a High School Diploma focused in **Russian and English languages** from Foreign Language High School – Pleven (Bulgaria). We then got an interesting lead from antiabuse mail archives of RIPE where anti-spam researcher **Ronald F. Guilmette** tied **Bogomil Simeonov to an organization named MEGA-SPRED LTD (AS201640**, abuse:*grimhosting.com*) created in late September 2014 in **Bulgaria** (we could confirm this link via domaintools whois history database on 2014-06-17; the domain was likely overtaken by the FBI according to the new postal address registered on 2015-07-18)**.** Grim hosting as shown below was selling Minecraft Hosting and dedicated hosting with DDOs protection.

*Figure 30Screenshot taken from Domaintools (2016-12-19) of grimhosting.com, known as the abuse domain of a registered company within RIPE database known as **MEGA-SPRED LTD (AS201640)**.*

MEGA-SPRED LTD hijacked unallocated or wrongly sourced IPv4 address space that are then leased out to other actors. for spam and likely other malicious activities. Brian Krebs explained that *"If nothing or nobody objects to the change, the Internet address ranges fall into the hands of the hijacker"*.

This is how, as reported in the B.Krebs blog in 2014, according to an analysis of both hosting providers **Mega-Spred** and **Visnet** (Romania) used highjacked IP address spaces to conduct malicious activities. Later in 2016 was shown that an American citizen **Michael A. Persaud,** known as the top-10 worst spammer at that time by Spamhaus, **was raided by the FBI.** Persaud managed to send millions of junk emails while avoiding spam filters and blacklists thanks to the use of the "snowshoe" technique (*i.e.*, *"being relayed through broad swaths of Internet address space that had been hijacked from hosting firms and other companies"* such as Mega-Spred).



We also found another related organization named "ROZA HOLIDAYS EOOD" (A record: 195.230.24.20, 195.230.24.0/24, AS50360 - Tamatiya EOOD) with p.dimov@4vendeta.com as a registration email; its abuse email is abuse@rosa-holidays.com. No website was deployed while 4vendeta.com is cited already in 2017 as a known infrastructure ignoring DMCA.

*Figure 31 A testimony where 4vendeta.com is cited already in 2017 as a known infrastructure ignoring DMCA (Digital Millennium Copyright Act). DMCA refers to **a hosting provider or registrar that does not comply with DMCA takedown requests. Screenshot taken from Blackhatworld.com.***

As far as AS-Tamatiya is concerned in the literature, here are the key findings we could relate to in terms of cyberattacks.

Forescout reported in 2022 that *"the adversary used a Bulgarian IP address of 78.128.113.]10 and hostname of "ip-113- 10.4vendeta.]com" to download and install SonicWall's Virtual Assist module"*. Forescout linked the IP address to *"shared hosting pool belonging to RACKWEB-NET which leads us to believe this is a burner IP address"*. The adversary was an affiliate of the **Blackcat/AlphV RaaS program**, which targeted VMware ESXi systems.

In a report of CERT-UA in May 2023, it's been shown that the **intrusion set UAC-0063** (overlapping with medium confidence with the **GRU-operated APT28** has used an IP address that belongs to **Tamatiya EOOD** (4vendeta[.]com) but also **Hostkey** (see dedicated part in main text).

APT28 (aka IRON TWILIGHT, SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127, Forest Blizzard, FROZENLAKE, TAG-110) **conducted cyber espionage campaigns to collect strategic intelligence in Central Asia** according to **Recorded Future.** Our fellows at Sekoia substantiated that **Zebrocy** could be at play, a subgroup of **APT28** (but also the name of a backdoor).

*Alviva Holding Limited (AS Number **209132**)*

To be noted is that **Alviva Holding Limited** was already related to multiple malicious IP addresses in the analysis of GroupIB of ShadowSyndicate in 2023. It's also been seen as the initial SysAid cluster in 2023 by @josh_penny researcher and related to multiple clusters related known attacks from Clop infamous group leveraging 0days.

Let's first have a look to the **AS209132** (**Alviva Holding Limited**) by querying the **RIPE** database. One can already observe red flags in the returned information as highlighted in the figure below.

Figure 27 Screenshot taken from RIPE. Registered in Seychelles (an offshore jurisdiction), by a Russian organization called Permtelecom

The **mnt-ref** (provide a set of authorization tokens used for creating references to this **mntner** object) points to **ru-permtelecom-2-mnt** that was registered by **o.pishulev@59telecom.ru**. This email

points directly to a **Russian organization** called Permtelecom (**AS39735**). In addition we found that the domain 59telecom.ru (with the Russian registrar RU-CENTER-RU) is mentioned as the site URL of the organization named Agronet LLC (AS50949) that is located in the **war zone of Crimea** (Симферополь or Simferopol) since 2010 that got multiple unresolved abuse complaints in the past.

As shown in the figure above, there are also as **mnt-ref DIGI**, which stands for DIGICLOUD-NET (digi-cloud.net), which is the abuse contact info of Aviva Holding Limited. And also mnt-ru-am-1 (upd-to amamaew@mail.ru) related to **Anton Mamaev**, (located at Belinskogo str 86 – 36, 620026, Ekaterinburg, Russia). This person likely owns an ASN on his name (**AS207967**, Russia, Moscow, Tverskaya-7) that was **involved recently in IP space highjacking** as reported by **Spamhaus**. From RIPE database of this ASN we found the e-mail and abuse-mailbox to be ipocean[.]ru, which points to a website owned and operated by **MAMAEV ANTON EVGENIEVICH**, who offers "Ipv4 block leasing" (/22 or /21) or "buying" (/22) as well as "Registration of LIR"

As shown in the figure below, the ASN **name Alviva Holding Limited** is registered in the pandora papers. The beneficial owner is **Denis NECHAEV** (from 30-JAN2019). A physical address is related to **Denis NECHAEV** located in Russia at *"9 KOMMUNISTICHESKAIA STR., APT. 7, SVETLYI CITY, KALININGRADSKAIA **OBLAST, RUSSIAN FEDERATION**"*; we found no other companies linked to that identity.

Entity (1)

	Role	From	To	Incorporation	Jurisdiction	Status	Data From
ALVIVA HOLDING LIMITED	Beneficial owner	30-JAN-2019	-			-	Pandora Papers

Address (1)

	Data From
9 KOMMUNISTICHESKAIA STR., APT. 7, SVETLYI CITY, KALININGRADSKAIA OBLAST, RUSSIAN FEDERATION	Pandora Papers

Figure 32 Screenshot taken from offshoreleaks unveiling the main beneficial owner of Alviva holding limited (Denis NECHAEV from 30-JAN-2019).

Oblast (**Kaliningrad)** is a small province known to be the westernmost part of Russia (separated from the Russian territory) considered as a thorn in NATO's side.

Information unveiled above are amongst key figures to set up a Russian operated bulletproof hoster. Moreover, we found that a trusted source (IPFire) vetted this ASN as **a bulletproof ISP operating from a war zone in eastern Ukraine**.

While analysing Alviva via **BGP tools**, we found that **around December** its network policy was upstreaming and peering traffic **with Verdina and RETN** (see left inside the figure below).

Verdina Ltd' ASN was registered in Belize, an offshore jurisdiction, which was allocated ten years ago. Verdina[.]net was already categorized as a **rogue infrastructure a year after** its creation **in 2016** as covered in an analysis of B.Krebs. BackConnect, a **legitimate DDoS mitigation company**, admitted to have performed defensive BGP's hijacking of Verdina in 2016 to identify the server of vDOS (DDoS-for-hire or "booter" service) attacking the firm as a DDoS mitigation by "hacking back".

Reverse DNS entries of the IP range 85.217.223.0/24 (**Verdina Ltd.,** see BGPtools here) revealed **another known rogue infrastructure called *histate*** (hastate.net) providing anonymous hosting and that was part of a sophisticated scheme as described in the presentation "THE CURIOUS CASE OF FAKE BRITISH LIRS" given as the 78th RIPE conference on May 2019.

As far as **RETN** is concerned, we provided a recent analysis on this **Russian massive hybrid infrastructure**. The recent switch we observed in March through **Aurologic** is also interesting, as we know, it **often facilitates upstreaming malicious traffic from bulletproof hosting providers**.

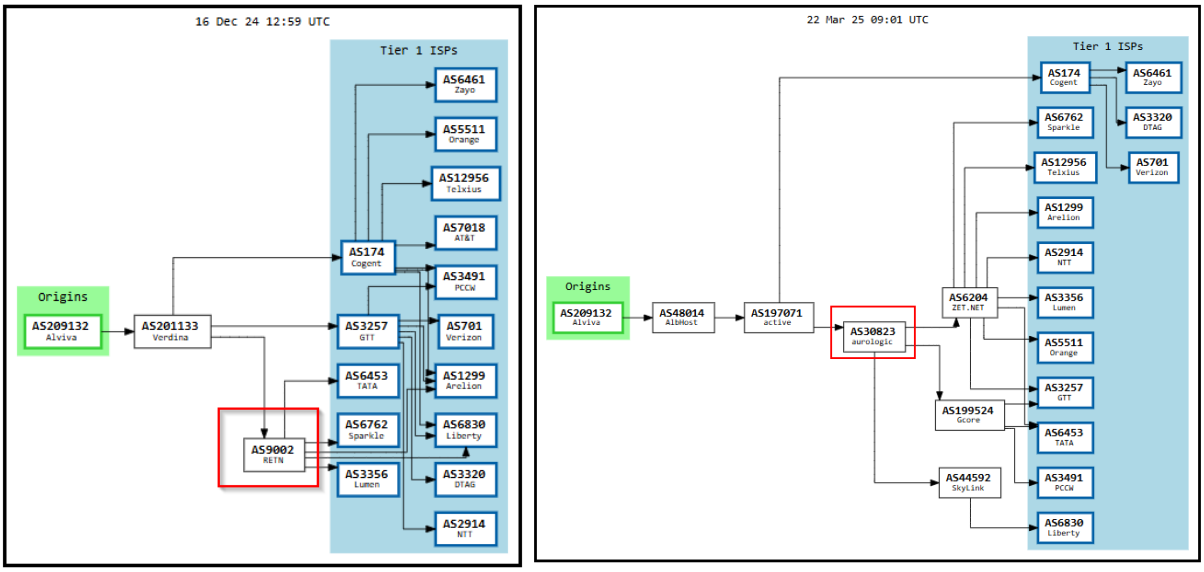


Figure 33 Screenshot taken from BGP tools exhibiting Alviva's connectivity throughout Verdina and RETN (16th of December 2024) that evolved recently throughout AlbHost, active and Aurologic (22 March 2025).

The abuse contact of **Alviva Holding Limited** (AS209132) is streaming-host[.]net. Pivoting on this domain via BGP.tools, we found **its presence in the MX records** of the IP address 185.55.243.102 but also in the abuse contact, which belongs to **LAYER7-NETWORKS** (AS35042) through its prefix 185.55.240.0/22. The domain streaming-host[.]net resolved that IP address since around 2022-04-04 according to VT whereas before that date we found a **resembling domain** stream-host[.]net.

LAYER7-NETWORKS AS35042 also hosted payloads from Clop group as well as cobalt strike beacons and loaders (from our Opencti database) around Nov 2023.

As expected the ASN **AS209132** peers with its other ASN from Alviva Holding Limited (AS209272) but also with **Albanian Hosting SH.P.K.** (that we observed to be used by **ShadowSyndicate**) and **Belcloud** LTD (AS44901). ASN **AS209132 also** downstreams network traffic for **Alviva Holding Limited** (AS209272).

Flyservers S.A.

Upon our investigations we encountered two IP ranges:

- 45.227.252.0/24 AS267784 (responsible David Menotti, RU, see offshoreleaks)
- 81.19.135.228 AS209588

As shown in the figure below Flyservers S.A. was created 2019-01-14T08:42:10Z. The RIR transfer history shows that it was registered before as **ADM Service Ltd** (transfer date at 2021-12-15). Flyservers S.A became valid from 2022-04-28 10:02:01 (according to RIPEstat). This ASN entered already in the top10 of most common second stage ASNs in July 2022 according to @cobaltstrikebot.

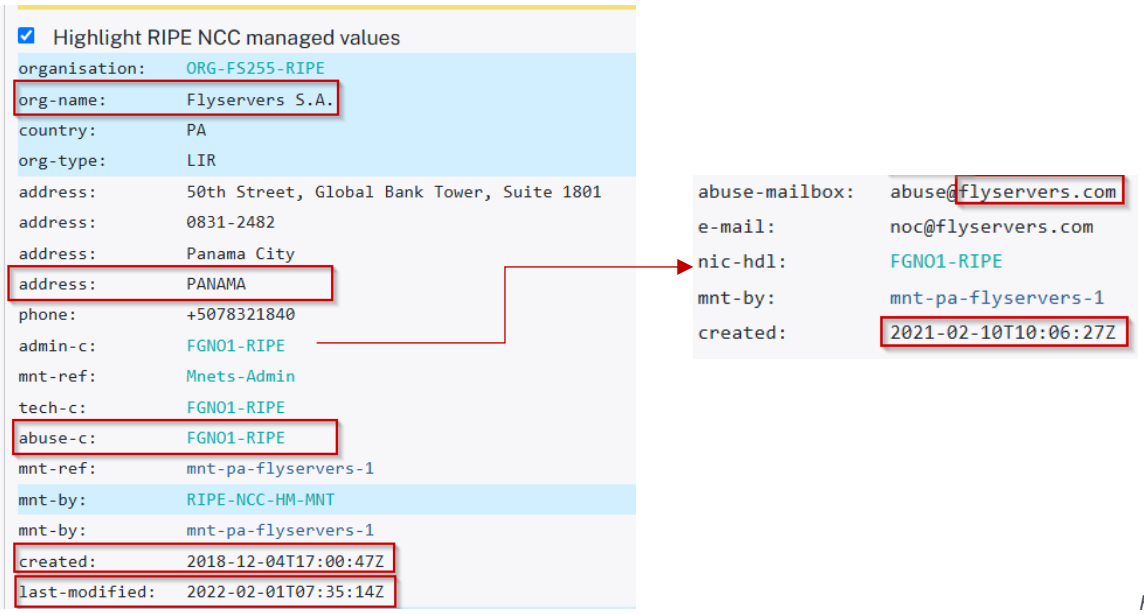


Figure 34 Screenshot taken from RIPE. Registered in Panama (offshore jurisdiction), by an organization called pa-Flyservers.

According to Domaintools the admin email contact and the abuse contact are registered as admin@flyservers.com and abuse@flyservers.com, respectively.

The website flyservers.com's domain has a A record with the IP address 45.227.255[.]30 (AS43350, Panama, offshore jurisdiction) that belongs to NForce Entertainment B.V. The first resolution dates to 2014-09-19 (AS33785, CITYNET, Egypt).

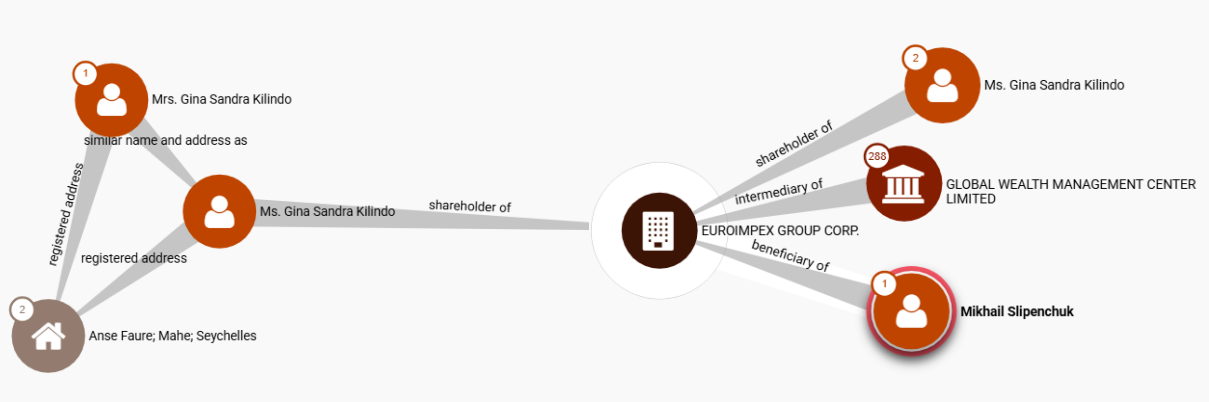


Figure 35 Screenshot taken from offshoreleaks unveiling the relationship between the registrant of FlyNetworks LTD (flyservers.com) namely Mrs Gina Sandra Kilindo and a Russian enterprise named Euroimpex group CORP located in Moscow (its beneficiary is a Russian named Mikhail Slipenchuk, with the known address 6; Pionernaya street; Ozerny village; Yeravninsky district; the Republic of Buratiya; the Russian Federation). Euroimpex group CORP. is an intermediary of Global Wealth management center limited, itself connected to 289 intermediaries all registered in fiscal paradises.

From Domaintools we obtained the contact information of this website's registrant as ***"Gina Sandra Kilindo"***, **Fly Networks LTD** located at Suite 1, Sound &Vision House Francis Rachel Street Victoria, Mahe **SC** (**Seychelles,** an offshore jurisdiction).

We found in the **Panama papers** a good match with **Mrs. Gina Sandra Kilindo** that was located in **Seychelles** and related to a **Russian enterprise named Euroimpex group CORP located in Moscow**. Euroimpex group CORP. is an intermediary of **Global Wealth management center limited**, itself connected to **289 intermediaries all registered in tax havens**.

Figure 36 Image of Михаил Викторович Слипенчук from wikidata.

The main **beneficiary of Euroimpex group CORP** is a **Russian oligarch named Mikhail Slipenchuk**, with the known address 6; Pionernaya street; Ozerny village; Yeravninsky district; the Republic of Buratiya; the Russian Federation. Slipenchuk has been the Vice Chairman of the Parliamentary Committee for **Natural Resources and Ecology at the Russian Parliament**, **elected by President Putin's "United Russia" party, from 2011 to 2016**. Mikhail Slipenchuk is seen as the Russia's richest politician. **He is currently** under sanctions of the **National Security and Defense Council of Ukraine** since 2018 that blocked its assets in Ukraine.

We found that Gina Sandra Kilindo could be Gina Esparon but also Gina kilindo based on LinkedIn accounts having Alpha Consulting Ltd and Seychelles in common (see figure below).

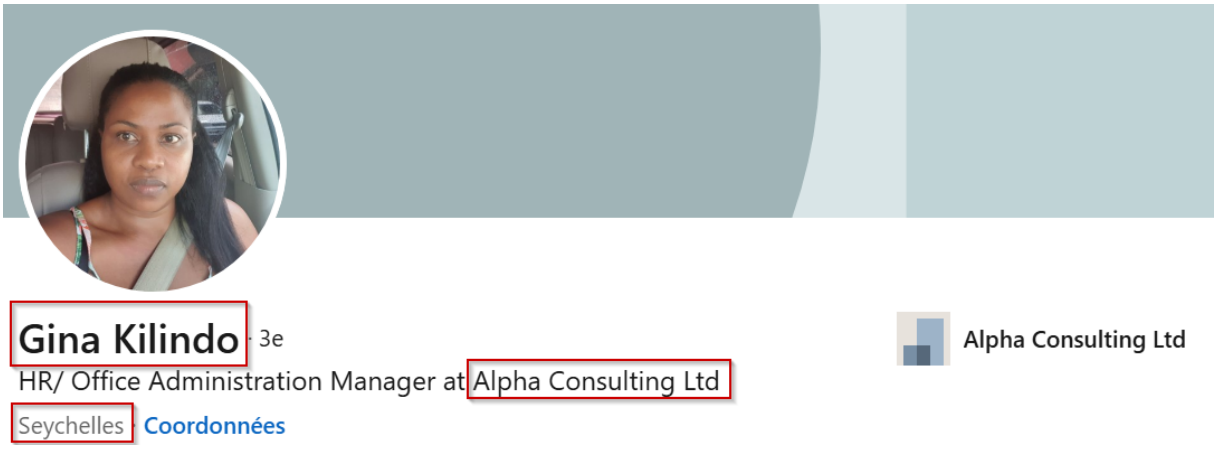


Figure 37 Linkedin profile of Gina kilindo working for Alpha Consulting Ltd as HR/Office administration manager.

Gina Esparon, a Seychelles's citizen, appears in multiple sources such as PeakD reporting in 2018 that she was the **legal officer of 63 UK registered companies** (up to 137). Peak analysts also found **variations in her name with multiple identities** used to sign legal documents. She was the director of **Alpha consulting group limited registered in UK** until it was dissolved in 2018, which is an interesting case we already encountered in several investigations (e.g., Suspicious Seychellois Network Management for Russian Businesses, a3d4c76c-404e-44ee-bffe-b517f6f2cec2).

> Seychellois consulting firm **Alpha Consulting Group**, founded by the **Russian** businesswoman **Victoria Valkovskaya in 2008**, whose documents and hard drives were seized in 2023. They revealed that *"the firm had exploited a U.K. secrecy loophole[…]hundreds of **Alpha Consulting** documents contained in the Pandora Papers cache to uncover **more than 900 U.K.**-registered firms set up by nominee directors linked to the Seychelles provider."*
> For context, **Alpha Consulting Group** specializes in international tax planning and in assisting with registering companies in low-tax jurisdictions, opening foreign bank accounts and establishing trusts and funds. According to the investigation by the International Consortium of Investigative Journalists (ICIJ), 75% of the Seychelles implanted consulting firm's customers are **Russian**. As a reminder, registering a company in the **United Kingdom costs as little as 12 pounds**, and Companies House does not verify names and addresses supplied by applicants, making it a privileged location for cybercriminals looking to quickly establish a legal infrastructure.

Alpha Consulting already helped in summer 2017 to blur the funding of the **ex-trump lobbyist Nick Muzin** via a shell company named **Biniatta Trade based in Edinburgh**. The shell company is present in the leaked Alpha documents and hired **Nick** to enhance the standing and operations of an **Albanian right-wing political party** by arranging a series of events **in the US to profit from Trump notoriety**. The origin of the funding could be traced from **Russia**, which **used the US political system to fuel political discord in the Balkans** as reported MotherJones in 2018.

The BBC in 2023 unveiled a much broader strategy of massively leveraging such shell companies intermediated by **Alpha consulting** to be *"**used by members of Vladimir Putin's inner circle**"*, which includes *"**the late mercenary boss Yevgeny Prigozhin's yacht**"*.

Now analyzing on VT the passive DNS replication of IP address 45.227.255[.]30 (seen to resolve flyservers.com), we found 29 domains resolving the IP address from 2021-03-04 to 2024-05-22 **almost**

based on the same patterns evoking adult contents as shown in the figure below before it **resolved more recently to flyservers.com**.

Considered all intelligence we gathered on **Flyservers** S.A, but also the fact that Recorded Future mentioned it as an example of a bulletproof hoster in 2022 (proofs were not shared) **we assess with good confidence that Flyservers S.A. should be blocked on all perimeters**.

Speaking of **Ransomware brand SpaceBears**, we found **another related server** (again with the SSH fingerprint of ShadowSyndicate) but **on another ASN** (**Layer7 Networks GmbH**). Indeed, we found that **mail.spacebears[.]top** resolved the IP address 88.214.25[.]246 on July 8th, 2024 (ASN35042).

Moreover, this IP address **exhibits lots of open ports** (39) which includes **a Metasploit server** on port 3790. We also found multiple ports with **traits of SOCKS5 proxy** such as on port 7691. At least two **payloads of SystemBC** (dd1bff3bb1654d213a144c9f0adcb98016ff5c940e49963be9acf143516fdd9b ; ef691a7d4c160dcb00c491b6e58188d62974dcc9357c4bc067af03920b89ac7e) communicated with that IP around 2023-10-27 and were linked **to Blackcat** according to crowdsources on VT but also @TLP_R3D. Again, we found that this IP address **resolved o*.*.claudfront[.]net** on 2024-03-15 (see section in the main text dedicated to **DecoyDog: DNS tunnelling as C2**).

While investigating that IP on Domaintools we found a pivot on the ISP ***"Thinktech Technology Industrial Co. Limited"***, which exhibited 62 domains with high score risks. As amongst the tens of malicious domains we found already encountered ones such as visualstudiomacupdate[.]com (linked to OSX Rustdoor). This is where we realized that the same organization name ***"Thinktech Technology Industrial Co. Limited"*** described as **VDS&VPN services** spans several of previously encountered bulletproof hosters.

VDS&VPN services (Thinktech Technology Industrial Co. Limited)

According to RIPE database, the abuse contact of the organization ThinkTech Technology Industrial CO. Limited is abuse@one-host.net (2018-11-22T21:37:06Z). This domain appears six times in the blackbasta chat log leaks. This organization is **geolocated in an offshore jurisdiction, namely Hong Kong** (International Business Center, Suite 811 Tsimshatsui Centre, East Wing, 66 Mody Road, Tsimshatsui East, Kowloon, see RIPE) and a peers of the Russian RETN network service provider specializing in high-speed data transmission and IP transit across **Europe, Asia, and North America**.

Moreover, one-host.net hosts a fake website mimicking legitimate data center offers. The last IP that resolved one-host[.]net belongs to the **ASN NForce Entertainment B.V.** (46.161.27[.]211, 2019-12-12). A pivot on its ISP ***"Vps And Shared Hosting Pool"*** on Domaintools unveiled **208 malicious domains** that we link (**with high levels of confidence for 98 of them) to Magentocore, a campaign likely linked to MageCart group**.

Another pivot on the IP address 141.98.80[.]151 unveiled the domain innovaservers[.]net (first seen in 2020-04-13) associated to the org "Ovlyagulyyev Dovlet" located in the offshore jurisdiction **Seychelles**.

We also found that ***"Vps And Shared Hosting Pool"*** is actually the top 3 most servers used by the owner in the list A provided by GroupIB while tracking **ShadowSyndicate previous infrastructure in 2023**.

As far as the **AS organization Aixit GmbH is concerned**, we only encountered upon our analysis the IP ranges 88.214.25.0/24 that we could link to the organization **ThinkTech Technology Industrial CO. Limited**. Indeed, this IP range is related to the AS Name: **Layer7 Networks GmbH** (**AS35042**), which upstreams only towards Aixit GmbH and holds "ThinkTech Technology Industrial CO. Limited" as an org name.

safe-vpn.mobi

We also found several occurrences of "**safe-vpn.mobi"** upon the analysis of ShadowSyndicate **infrastructure** (*c.g.*, for the IP address 179.60.149[.]241 HOSTKEY-USA).

According to Shodan the usage of this hostname has increased substantially since mid-2024. It historically transitioned from organizations named ISP4P IT Services, GHOSTnet GmbH and Safe VPN S.A..

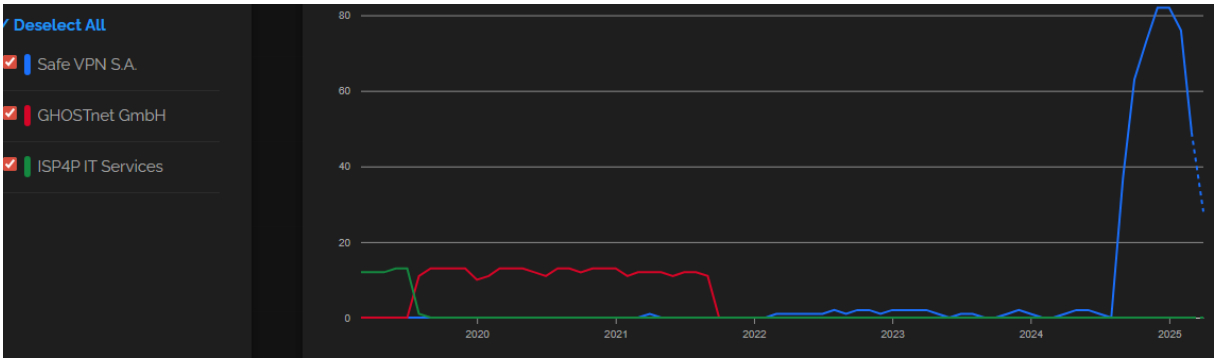


*Figure 38 Shodan trend database exhibiting an increase in the usage of the hostname safe-vpn.mobi. Safe VPN S.A. is linked to AS262287 (**Latitude.sh LTDA**) while **GHOSTnet GmbH** corresponds to **AS12586** and **Safe VPN S.A.** corresponds to AS395839 (**Hostkey USA, Inc**).*

As far as threats relying on **Safe VPN S.A.** is concerned, we found that the domain safe-vpn[.]mobi was seen to be resolved the most according to shodan lately by 179.60.149[.]4. This IP address was related to malicious activities in line with Sliver, ligolo-ng C2 infrastructure reported around Nov 204 by hunt.io and as seen in exfiltration upon **8Base** ransomware operation by Almond. We found a recent ELF payload of **Sliver** (first submitted on Feb 2025 on VT) with C2 traffic on port 3333 pointing to this IP address, named **ivanti**.listener.

We found also found the domain **safe-vpn[.]mobi** in a report of the CISA that was published on September 2023. We observed a **perfect match of meta information** reported by the CISA, which linked an intrusion set to this service, allegedly used by **nation-state actors exploiting CVE-2022-47966** (Zoho ManageEngine) and **CVE-2022-42475 (FortiOS SSL-VPN) vulnerabilities**.

Once a footstep was established on vulnerable devices, a malicious Windows executable (likely a Metasploit/Meterpreter shellcode) connected to a remote IP of the same subnet (179.60.147[.]4) on port 58731 as such that another payload is injection into memory.

The last vulnerability exploitation of vulnerable **FortiOS devices** was documented by Mandiant (google) conjecturing that **Chinese Threat Actors were involved leveraging a malware called BOLDMOVE for cyber espionage operations** (low confidence).

Threatfox provides two occurrences of **Safe VPN S.A.** and linked them to **Darkgate** (Meh, MehCrypter), a commodity loader seen as the continuation of Qbot (after its takedown) together with Pikabot to fuel ransomware ecosystems.

In the figure below is the actual website while browsing safe-vpn[.]mobi, which allegedly offers three types of offers namely to bypass the **China Firewall, L2TP \IPsec or OpenVPN**. Payments in **bitcoins** or via **Skrill** are possible.

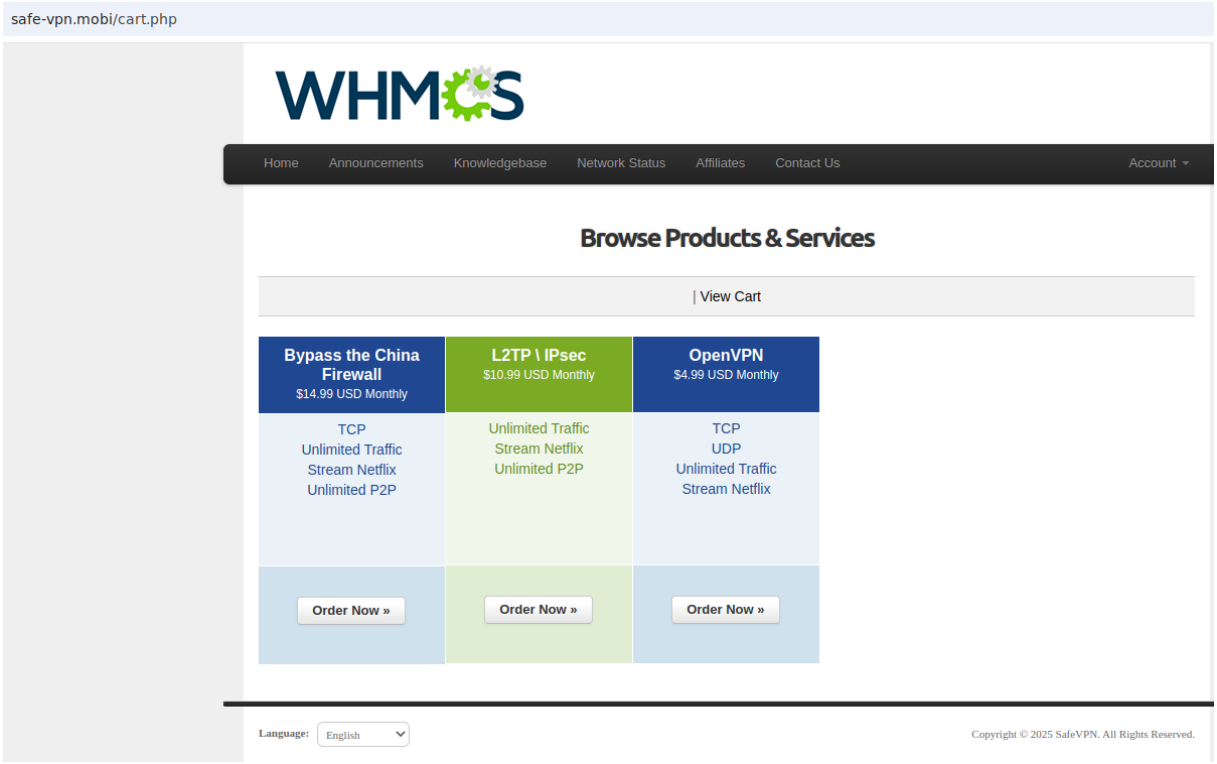


Figure 39 Order form of safe-vpn.]mobi offering services to bypass the China Firewall, L2TP \IPsec or OpenVPN. Payments in bitcoins or via Skrill are possible.

Since February 2025 we found in RIPE database that safe-vpn[.]mobi is the contact email and abuse mailbox of **SAFE GATE LTD organization** registered in **Seychelles** (an offshore jurisdiction).

WHOIS information was provided by URLscan (see figure below) created the 2022-03-01.

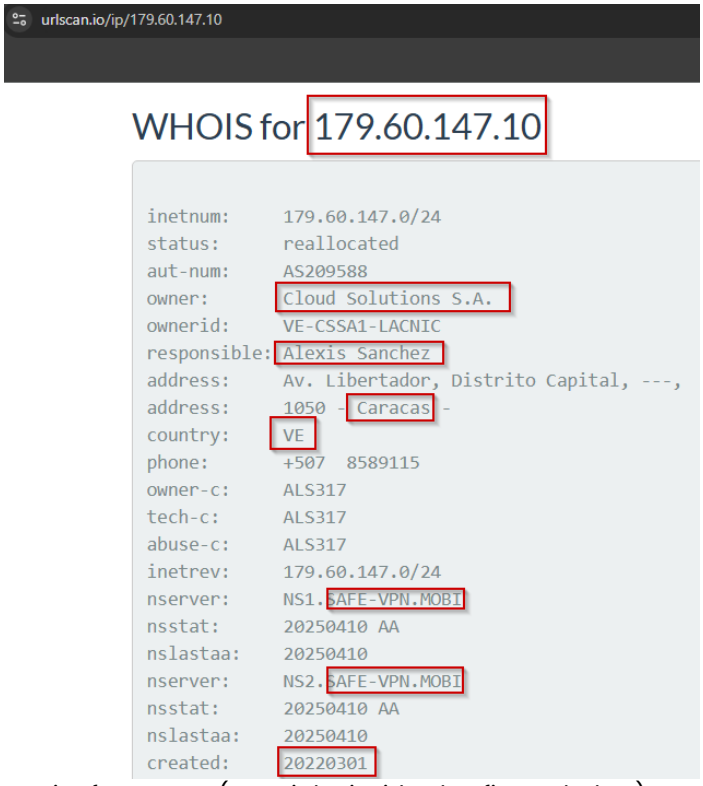


Figure 40 Screenshot taken from URLscan. WHOIS information regarding the IP prefixes 179.60.147.0/24. The owner and the responsible are "Cloud Solutions S.A." and Alexis Sanchez, respectively. Its location is in Caracas, Venezuela.Safe-vpn.mobi domain appears in authoritative name servers of this IP block created in 2022.

Below we present screenshots from **RIPE** exhibiting information we obtained after full text research of safe-vpn[.]mobi. An organization named **Usi Tech Limited was registered in United Arabic Emirates on May 14, 2018** (offshore jurisdiction), which states **HOSTKEY** as the **maintainer** (mnt-ref) The **email information contact** and **abuse contact info** are respectively **info@safe-vpn.]mobi and abuse@safe-vpn.]mobi**.

Again, from RIPE (see right inside the figure below) we found an email address sending update notifications or error messages related to this maintainer (mntner; usitech) object to be fastvpncontact@lenta.]ru, which points to the well-known **news portal in Russia and the CIS**.

Figure 41 Screenshot taken from RIPE after full text research of safe-vpn[.]mobi. Left: An organization named Usi Tech Limited was registered in United Arabic Emirates on May 14, 2018, which states HOSTKEY as the maintainer (mnt-ref) The email information contact and abuse contact info are respectively info@safe-vpn.]mobi and abuse@safe-vpn.]mobi. Right: Email address to send update notifications or error messages related to this maintainer (mntner; usitech) object is fastvpncontact@lenta.]ru, which points to the well-known news portal in Russia and the CIS.

Although known to usually spread the Kremlin narrative since 2014 when occurred the first onset of the war between Russia and Ukraine but also fueling portal Kombat "Pravda" websites, lena.ru remains a legitimate news portal located in Moscow. Its

Web content is managed **behind the CDN Rambler** and, as mentioned by Ptsecurity, Rambler enables **anyone to create email addresses with a lenta[.]ru domain**. As far as Usi tech limited is concerned, we found that it was a Dubai-based crypto (but we saw that registered location is Ras al Khaimah) and forex platform trading platform suspected of having set up a Ponzi scheme scamming millions of dollars.

The suspicious website safe-vpn[.]mobi is hosted on a dedicated server, which resolves to 185.55.243[.]104 (Layer7 Networks GmbH, AS35042) since at least 2018 according to Domaintools. The abuse information goes by:

- abuse@ordertld.com
- +86.5922179566
- Washington
- Killgore Chung

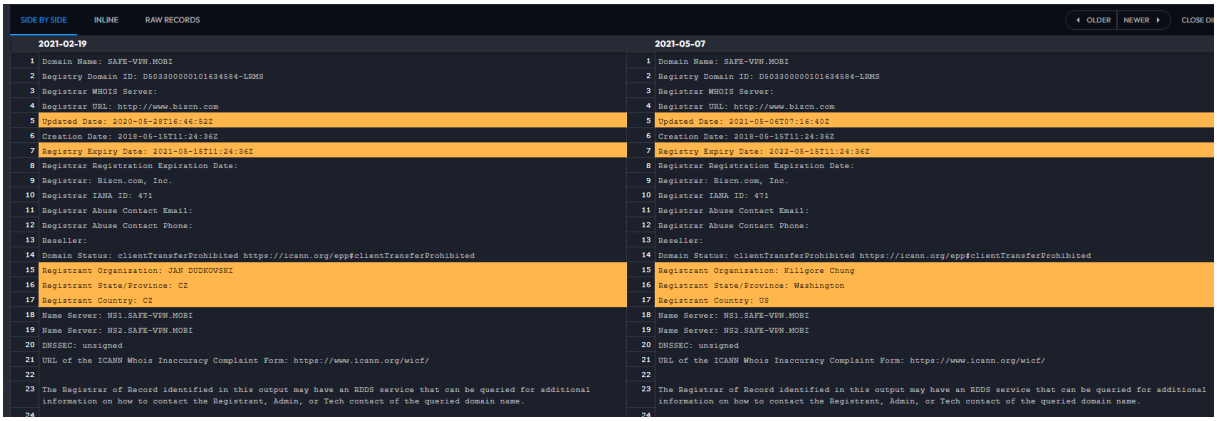


Figure 42 Whois history according to Domaintools database.

From domaintools we found 5 domains linked to the organization "Fillgore Chung":

- j-network[.]biz (risk score 100) => jabber/xmpp server
- safe-vpn.mobi (risk score 70)
- buhariki.biz (risk score 65)
- friendscorporation.biz (risk score 65)
- gangsteri.biz (risk score 65)

*NForce Entertainment B.V. (AS Number **43350**)*

Operating **since 2003**, **NForce** (website nforce.com) is a **Netherlands-based** hosting provider offering services not only such as dedicated servers, cloud hosting, colocation, and IP transit but also maintain any current RIPE account (administrative part of IP space and AS numbers).

```
organisation:    ORG-NE3-RIPE
org-name:        NForce Entertainment B.V.
country:         NL
org-type:        LIR
address:         Postbus 1142
address:         4700BC
address:         Roosendaal
address:         NETHERLANDS
phone:           +31206919299
admin-c:         NFAR
tech-c:          NFTR
abuse-c:         NFAB
mnt-ref:         RIPE-NCC-HM-MNT
mnt-ref:         MNT-NFORCE
mnt-by:          RIPE-NCC-HM-MNT
mnt-by:          MNT-NFORCE
created:         2007-06-19T08:39:06Z
last-modified:   2023-08-07T08:14:17Z
```

```
role:            NFOrce Internet Services -
address:         Postbus 1142
address:         4700BC Roosendaal
address:         The Netherlands
phone:           +31 (0)206919299
e-mail:          abuse@nforce.com
abuse-mailbox:   abuse@nforce.com
remarks:         Please use automated abuse
nic-hdl:         NFAB
mnt-by:          MNT-NFORCE
created:         2013-05-15T07:54:52Z
```

Figure 43 Screenshot taken from RIP. Left: An organization named Nforce Entertainment B.V. was registered in the Netherlands on June 19, 2007. Right: The abuse contact info is abuse@nforce.]com.

Over the years, **NForce** has expanded its **cryptocurrency payment options**. In March 2018, they added Bitcoin Cash (BCH) as a payment method via BitPay. More recently, in February 2025, NForce announced the introduction of USD Coin (USDC) support, offering customers additional stablecoin options for transactions.

In contrast with other studied ASNs upon this investigation, the latter holds lots of peers and downstream some network traffic while by querying Spur.us database we found **various VPN and proxy services** (23 and 29 respectively; mainly proxystore and protonvpn). This finding resonates with a tweet of a trusted source mentioning in 2022 that **this ASN is associated to a "notorious VPN service"** and advised to block it.

Figure 44 @sansecio advising publicly in 2022 on X (ex-twitter) to block Nforce Entertainment.

NForce Entertainment B.V. was already recorded in the abuse of RIPE in2016 as facilitating a *"broad range of criminal activities"* by upstreaming malicious traffic from the bulletproof hoster AS60117 (Host Sailor, Ltd.).

While **following** previous **links between Nforce Entertainment B.V**. and the **BPH Flyservers** via mail.flyservers.com, our attention was drawn towards the **PTR** entry srv.cl-**leaks**[.]com. This domain name used is linked to the **infamous Clop Ransomware group** that we encountered several times upon this investigation (see figure below).

Address	PTR
45.227.255.1	cisco-core.web4net.org.
45.227.255.30	mail.flyservers.com.
45.227.255.195	srv.cl-leaks.com.

*Figure 45 Screenshot taken from BGPTools while investigating on **AS43350** (NForce Entertainment B. V.). It shows a suspicious domain with 'leaks' that we could link to the infamous Clop ransomware group.*

Indeed, as shown in a **ransom note** (see figure below) that we could find on VT, this domain appears in a ransom note of a Clop payload. The latter is contained in a contact for ransom negotiations. We found that the server at that IP address is running a **Roundcube** server hosted by **Nforce** entertainment using the address unlock@cl-leaks[.]com.

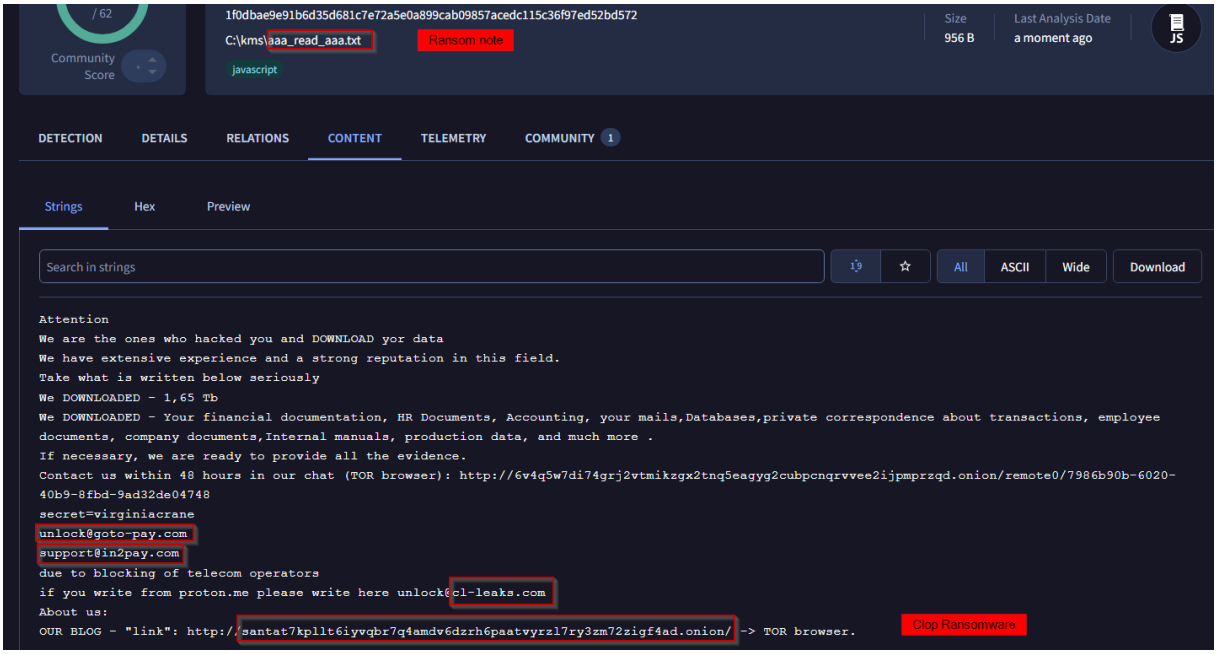


Figure 46 Screenshot taken from VT of a ransom note generated by Clop ransomware. The email support address shared for negotiations if a victim writes from protonmail is unlock@cl-leaks[.]com

We then found a tweet of @TLP_R3D that substantiates previous findings and relates that ransomware attack to the exploitation of SysAid vulnerability (0day on November 8, 2023, and tracked as CVE-2023-47246). Besides, one can note that the other IP address 45.227.253[.]147 related to previous famous massive exploitation of MOVEit 0day CVE-2023-34362 mentioned in the tweet belongs to the BHP **Alviva Holding Limited**.

To the least we assess with **high confidence** that the **following IP range of Nforce Entertainment B.V. shall be blocked**: **45.227.255.0/24** (AS43350, Okpay Investment Company).

We also found this range (**45.227.255.0/24**) involved in **multiple incident cases in the past years**. For instance, It was **leveraged by LockBit** **RaaS as an exfiltration** infrastructure, and it appears twice in the List A reported by **GroupIB** as servers deployed by **ShadowSyndicate** (fueling a wide range of top tier ransomware brands).

From RIPE we found more **links between the previous IP range and the two other ASNs** analyzed in this report (see figure below). Inetnum *45.227.255/24* is owned by ***"Okpay Investment Company"***

having as a responsible person "Diego Garcia" located in **Panama** (offshore jurisdiction). A **traceroute** of this IP range, however, **streams to the Netherlands**.

```
inetnum:      45.227.255/24
status:       reallocated
owner:        Okpay Investment Company
ownerid:      PA-OICO-LACNIC
responsible:  Diego Garcia
address:      Av la Paz, El ingenio, 1292
address:      0000 - Panama - --
country:      PA
phone:        +507 661 72618 []
owner-c:      OIC5
tech-c:       OIC5
abuse-c:      OIC5
inetrev:      45.227.255/24
nserver:      NS1.WEB4NET.ORG
nsstat:       20190816 AA
nslastaa:     20190816
nserver:      NS2.WEB4NET.ORG
nsstat:       20190816 AA
nslastaa:     20190816
created:      20180507
changed:      20180507
inetnum-up:   45.227.252/22
```

.

Figure 47 Screenshot taken from RIPE. Inetnum 45.227.255/24 is owned by "Okpay Investment Company » having as a responsible person "Diego Garcia" located in Panama (offshore jurisdiction). The following domain WEB4NET.ORG (used as a Nserver) resolved to an IP address that belongs to Hostkey B.v. on August 1st, 2018 (and Layer7 Networks GmbH since 2021).

The following domain *WEB4NET.ORG* (used as a Nserver) resolved to an IP address (85.93.31[.]124) that belongs to **Hostkey B.v.** on August 1st, 2018 (and **Layer7 Networks GmbH** since 2021). *WEB4NET.ORG* was related by bediger4000 to a *"hosting company, offering email hosting, virtual private servers, dedicated servers, and VPNs"*; we could not confirm that information. A traceroute carried out on this IP range draws not to **Panama** but **the Netherlands (185.107.116.0/23 and then 45.227.255.0/24)**.

By identifying okpayinvest[.]net via VT relations of domains that resolved to the given IP 85.93.31[.]124 (Hostkey B.v.) on 2019-04-11, we found via a pivot on Domaintools of 291 suspicious domains. We found that **150 domains** follow the {firstname}dns.com convention; 6 domains are targeting Transport/Logistics sector in the USA (-us, -usa; -united, road, -cargo, logistics).

Lots of which are related to **Carbanak** (*e.g.,* applepay-invoice.com) and webskimmers used by Magentocore (*e.g,* jqueryfact[.]com).

Carbanak (aka ITG14, Carbon Spider, ELBRUS, Sangria Tempest, FIN7, GOLD NIAGARA, GOLD WATERFALL, Sangria Tampest) is a **notorious Russian nexus conducting both espionage and financially-motivated attacks** blamed for **stealing more than a billion dollars** from banks**.** Carbanak group born from late 2013 and origins from Russia, Eastern Ukraine and Europe, which is highly skilled in pursuing payment card data, attacks against **SWIFT** network. After arrests of Russian members around 2013 before it switched to **conduct ransomware attacks and eventually became a RaaS operator**
Carbanak (aka Anunak, Sekur RAT) is also used for a remote backdoor (initially based on Carberp) that was used by Carbanak group until 2016 and then transitioned to **Cobalt malware**.
Carbanak group preceded **FIN7, which** the U.S. Department of Justice described as *"a criminal enterprise with more than 70 people organized into distinct business units and teams"*. FIN7 is known to have used several fake cybersec companies as fronts for its operations to shield ransomware attacks and rented dedicated IP spaces from BPHs like Stark industries lately.
Fin7 was found to also benefit from the **ShadowSyndicate infrastructure**. **Fin7,** at the origin of the Colonia pipeline attack that had substantiate geopolitical involvements **via Darkside ransomware** then became **Blackmatter and** suspected to have rebranded to **AlphaV/Blackcat** RaaS.

Beyond FIN7 and Carbanak, not only links between **Magecart Group 4-5** and **Carbanak** have been explored since 2019 **but also with Dridex** phishing campaigns. Dridex is known to be developed and distributed by **EvilCorp** (aka Ta505).

The first registrant of okpayinvest[.]com domain (2018-05-04) was **Viktor Andriyan**, a **Moldovan** citizen with the email address viktorandriyan@yandex.ru that is related to the **registrant organization** "Tir-Telecom LTD". Three days after the domain was transferred from Tir-Telecom LTD to Wuxi Yilian LLC. We found that both organizations share a pattern of domain abuse in which WPO ruled in favour of the complainants (see examples respectively for Tir-Telecom LTD to Wuxi Yilian LLC).

This suggests either a conscious hand-off of domain portfolios (possibly due to investigation pressure) or **Tir-Telecom and Wuxi Yilian operating as aliases or front companies** under a broader cybersquatting or domain-squatting operation.

*Bunea TELECOM SRL (AS Number **35478**)*

Bunea TELECOM SRL is in **Romania** and having its website at https://bunea.eu/, suport@bunea.eu +40752481282. The homepage mentions that numerous cryptocurrencies are accepted to rent servers.

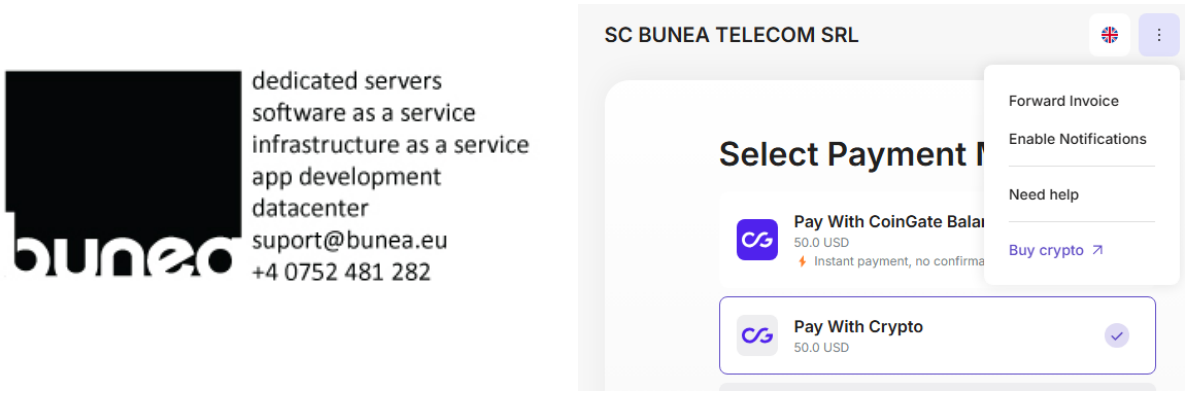


Figure 48 Homepage (right) of bunea.eu allowing users to rent servers where cryptocurrencies are available via coingate[.]com

BGP tools indicates that only one peer, named **UNMANAGED LTD**, is upstreaming and peering Bunea TELECOM SRL' IP ranges. We found an enterprise in the UK database matching **UNMANAGED LTD** that we assess is likely to be the same enterprise based on our knowledge of UK being a prime country for registering shell companies and the identity of the director **Petru-Octavian** BUNEA (date of birth April 1988). Both the name and its Romanian nationality match the name of the downstream **Bunea TELECOM SRL** behind **UNMANAGED LTD**, which again upstreams towards **RETN** and is connected to another studied **bulletproof hoster ASN Flyservers S.A** (AS209588) as peers and downstream.

We found an X account (ex-twitter) that **we linked with good confidence** to **Petru-Octavian** BUNEA by analyzing its followees. We likely found its LinkedIn account based on the same avatar's picture and names (this account has no past activity and mentions **Harrow in the UK** which matches the country of residence mentioned in the gov.uk database of registered companies).

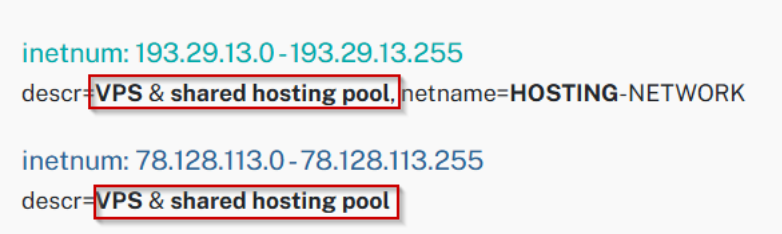
As far as **Bunea TELECOM SRL** is concerned, it is important to note that Joshua penny showed in Nov 2023 that this organization (amongst the others also covered in our analysis) was used upon the **GoAnywhere MFT** secure file transfer protocol **campaign of Cl0p** that breached 130 orgs in Feb 2023.

Huntress mentioned at that time the observation of an **overlap with Truebot** and **Ta505** that could have been behind such attack campaign.

Through a **combination of RIPE database pivots, DNS resolution history, and visual inspection of web** interfaces, we identified a **shared infrastructure framework** operating under two brands: **RAGNARHOST** (ragnarnet.com) and **RACKWEB** (rack-web.com). These appear to be functionally identical services offered via **distinct ASNs in Romania and Bulgaria**—namely **AS42397 (Bunea TELECOM SRL)** and **AS50360 (Tamatiya EOOD)**, respectively.

A full-text search in RIPE for the term "VPS & shared hosting pool" uncovered two key netblocks (see figure below):

- 193.29.13.0/24, listed under Bunea TELECOM with the abuse contact abuse@ragnarnet.com (see example of two states sponsored APTs using that range in the main text)
- 78.128.113.0/24, registered to Miti 2000 EOOD with abuse routed via abuse@rack-web.com



Both IP ranges are assigned the same descr and use ambiguous country codes ("EU"), suggesting

Figure 49 Full Text Search to query RIPE Database. Screenshot taken from RIPE.

intent to obscure geographic origin. Maintainer fields such as TAMATYA-MNT (for the Bulgarian block) and the presence of RACKWEB across multiple entities reinforce the operational and administrative links.

Domain history further confirms the connection while historical A records show :

- ragnarnet.com resolved to 193.29.13.150 (AS42397)
- rack-web.com to 193.29.13.152 (same /24)

Both IPs lie within the Romanian infrastructure subnet, and **VirusTotal data** from 2019–2020 shows low detection activity. Archived and live access to the domains reveals **nearly identical WHMCS login pages**, indicating a shared backend. The pages include:

- Identical site structure and layout
- Matching URL paths (/whmcs/clientarea.php and /billing/clientarea.php)
- The same language toggle, cart system, and styling — likely rebranded instances of a single WHMCS deployment template

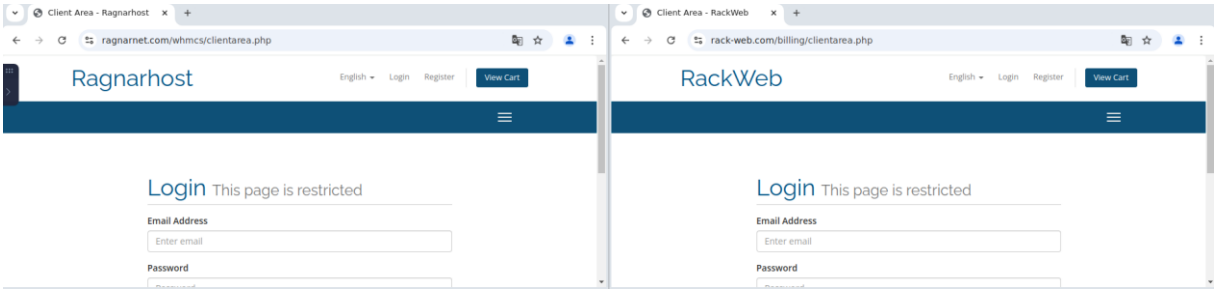


*Figure 50 Side-by-side comparison of RAGNARHOST and RACKWEB client portals. This image displays the login pages for two domains—**ragnarnet.com** (left) and **rack-web.com** (right)—highlighting their visual and structural similarities. Both pages are powered by WHMCS and feature identical layouts*

This visual and structural congruence demonstrates that RAGNARHOST and RACKWEB are not merely similar but **likely operated by the same entity or under a shared platform**.

This infrastructure provides services typical of **low-regulation, abuse-tolerant VPS providers**, and should be flagged for continued monitoring, particularly given the tendency of such networks **to facilitate spam, malware distribution, and bulletproof hosting**.

Further attribution efforts link while pivoting on abuse contact domain **ragnarnet.com** to a privacy-shielded registrant using the pseudonym **Gustaf Finnbjornsson**, whose contact address is ragnar.host@gmx.com. Besides, we found a role named **Tackweb NOC** to be located in an **offshore jurisdiction** (National Cultural Centre 861 P.O. Box 1492, Victoria Mahe, **Seychelles**) according to RIPE database.

The oddity of visit.keznews[.]com

On three ASNs related to **AS-Tamatiya umbrella**, we found an odd commonality. Indeed, we observed the same PTR (visit.keznews[.]com) on all IPs of each of the three following prefixes, according to BGPtools:

- **4media LTD** for the prefixes 78.128.112.0/24
- **NILSAT Ltd.** for the prefixes 45.141.157.0/24
- **Terinet EOOD** for the prefixes 79.124.54.0/24

This contrasts with usually encountered PTRs that are incremented or customized by users/providers to match services or branding. Moreover, as we found an intriguing tweet related to visit.keznews[.]com and a huge underlying infrastructure posted by @UK_Daniel_Card on mid-2022, we decided to investigate this oddity further and found interesting findings as such that it will likely be developed in a separate analysis.

- https://www.bitdefender.com/en-us/blog/labs/new-macos-backdoor-written-in-rust-shows-possible-link-with-windows-ransomware-group
- https://www.bridewell.com/insights/blogs/detail/shadowsyndicate?source=post_page-----799a4ff1ca59----------------------------
- https://medium.com/s2wblog/rustdoor-and-gatedoor-a-new-pair-of-weapons-disguised-as-legitimate-software-by-suspected-34c94e558b40