INTRINSEC

Innovative by design

PROSPERO & Proton66 : Uncovering the links between bulletproof networks

Cyber Threat Intelligence

November 2024

@Intrinsec @Intrinsec Blog Website

Table of contents

1. Key findings

- The Russian autonomous system ***PROSPERO* (AS200593)** could be linked with a high level of confidence to ***Proton66* (AS198953)**, another Russian AS, that we believe to be connected to the **bulletproof services** named '**SecureHost**' and '**BEARHOST**'. We notably observed that both network's configurations are almost identical in terms of peering agreements and their respective share of loads throughout time.

- Amongst the activities shared by the two networks, we noticed that both **GootLoader** and **SpyNote** malwares recently changed their infrastructure of **command-and-control servers** and **phishing pages** from *PROSPERO* to *Proton66*. Additionally, the domains hosting the phishing pages deploying SpyNote were hosted on either one of the two AS and had already been used in previous campaigns delivering **revoked AnyDesk** and **LiveChat versions** for both **Windows** and **Mac**.

- Regarding the other malicious activities found on *PROSPERO*'s IPs, we found that throughout September, multiple **SMS spam campaigns** targeting citizens from various countries were leading to phishing domains hosted on *PROSPERO* and *Proton66*. While most phishing templates were **usurping bank login pages** to steal credit card details, we also noticed that some of them were used to deploy **android spywares** such as **Coper** (a.k.a. **Octo**).

- **SocGholish**, another **initial access broker (IAB)** that we found to be hosting a major part of its infrastructure on *Proton66*, continues to leverage this autonomous system to host **fingerprinting scripts** contained on the websites it infects. Along SocGholish, we found out that **FakeBat**, another loader that infects systems through compromised websites, was using the **same IPs** to host both screening and redirection scripts.

2. Introduction

In the continuity of our constant monitoring of bulletproof networks, we discovered **an autonomous system named *PROSPERO OOO* (AS200593)** based in **Russia**. We believe that it could be linked to ***Proton66 OOO* (AS198953)**, another Russian and anonymous autonomous system that we previously found to be connected to a bigger infrastructure composed of multiple AS and offshore companies all operated by a common Russian national. This individual notably promotes its bulletproof hosting businesses named '**UNDERGROUND**' and '**BEARHOST**' on various Russian-speaking underground marketplaces stating that the service is "*100% bulletproof […] we completely ignore all abuses and complaints, including Spamhaus*". He notably used to work with another bulletproof provider named '**SecureHost**', advertised on the same underground platforms that we believe with a high level of confidence to be the present operator of both *PROSPERO OOO* and *Proton66 OOO*.

Bulletproof hosting
A bulletproof hosting service is a type of web hosting service known for offering **high levels of privacy**, security, and **leniency** regarding the content and activities allowed on their servers. These services typically provide robust protection against **takedown requests**, **legal actions**, and **law enforcement investigations**, often by locating their servers in jurisdictions with **minimal regulations** or weak enforcement of international laws. Bulletproof hosting is often associated with **hosting illicit content** or activities, such as **malware distribution**, **spam operations**, or **copyright-infringing materials**, due to its permissive stance and commitment to client confidentiality. However, it's important to note that not all uses of such services are illegal, as some users may seek such hosting for **legitimate privacy concerns**.

The connection between *PROSPERO* and *Proton66* could be made through similarities in the way both networks are operated, notably in their respective peering agreements shared with other Russian networks. Additionally, we noticed that botnets operated by **GootLoader**, an initial access broker, and **SpyNote**, an android RAT, had moved their infrastructure from *PROSPERO* to *Proton66*, or would sometimes host their command-and-control servers on both AS. We previously noticed the same occurrence in the **Matanbuchus** campaigns that we reported in May 2024 (see blog post), where the C2s were hosted on both *Chang Way Technologies* and *Proton66*. This could potentially mean that *Proton66* was operated by BEARHOST, as we unveiled his administration role of *Chang Way Technologies Co. Limited* (AS207566). Along those finds, this report aims to provide an overview of all the malicious activities that are hosted on *PROSPERO OOO*.

Legal format of Russian companies
As a reminder, the Russian format "**OOO**" stands for "**Obschestvo s Ogranichennoy Otvetstvennostyu**" which corresponds to the Anglo-Saxon format "**LLC**" or "**limited liability company**".

3. Linking Hostway and Chang Way to Proton66

3.1. Hostway and Chang Way

During a previous private investigation on BEARHOST's network, we described how multiple companies and websites were used as legal fronts for his bulletproof hosting business advertised on underground forums.

This started with the company ***Hostway LLC***, registered in **Russia** in 2019, from which he was appointed the role of director[1]. The billing page of the company's website (billing.hostway[.]ru) displays a clear relation with ***Chang Way Technologies Co. Limited***, a **Hong Kongese** company operating its own autonomous system **AS207566**.

[1] *https://www.rusprofile.ru/id/11936277*

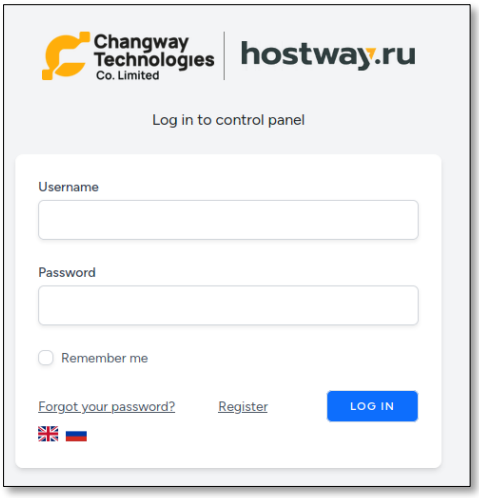

Figure 1. Login page hosted on billing.hostway[.]ru.

The website is also hosted on AS207566, which is part of an as-set named '**AS-SET-HOSTWAY**'.[2] Finally, to strengthen the bond that these two companies share, AS207566's description previously was "**HOSTWAY-AS**", before changing to '**CHANGWAY007-AS**' in May 2022.[3] Based on those elements, we can assess with *a high level of confidence* that this Russian national could also be the director of *Chang Way Technologies Co. Limited*.

However, the website currently displays the name of an offshore **Cypriot** company "*Starcrecium Limited*" and not its original company *Hostway LLC*. This is probably with the intention of hiding the past mistake that he made of registering a company with his own name in Russia and taking advantage of Cyprus' favourable tax regime and overall corporate confidentiality.

3.2. IT Resheniya LLC and Proton66 LLC

In addition to AS207566, *Hostway LLC* can be linked to another Russian autonomous system named "***IT Resheniya LLC***" or ООО "АйТи Решения" (AS49943). Despite redirecting to an offline website "rentaserv[.]ru", this autonomous system used to display *Hostway*'s website 'hostway[.]ru' in its Whois details.

Indeed, the following Whois information from May 2023 of one of AS49943's IPv4 range '**5.42.199**[.]**0/24**' used to display *Hostway*'s website:

```
organisation: ORG-ITR1-RIPE
org-name: IT Resheniya LLC

IT REShENIYa LLC | LLC AyTi Resheniya | ООО "АйТи Решения"
ul. Novoselov, d. 8A, of. 692
RU-193079 Saint Petersburg, Russie
Tel: +7 903 271 28 22
Emails: itresh7811764289@yandex.ru | abuse@hostway.ru
Websites: http://itreshenia.ru | http://www.hostway.ru
```

[2] *https://bgp.he.net/irr/as-set/AS-SET-HOSTWAY*
[3] *https://bgpranking.circl.lu/*

Overall, *IT Resheniya LLC* announced three IPv4 ranges, all owned by the same company "*Proton66 LLC*".

IPv4 range	Company name
194.32.236[.]0/24	Proton66 LLC
213.226.123[.]0/24	Proton66 LLC
5.42.199[.]0/24	Proton66 LLC

Proton66 LLC or ООО "Протон66", happen to possess its own autonomous system; **AS198953**, which was notably used to host a project that was created before Hostway named 'cyberpol[.]net' that shared the same email address 'dl@hostway[.]ru' as 'hostway[.]ru'. Before being turned off, the website displayed the same addresses as *Starcrecium Limited* in Cyprus and *Chang Way Technologies Co. Limited* in Hong Kong on the contact form.

Furthermore, one can notice the similarities in the websites design in the figure below (*figure 2*). While these elements may not constitute an undeniable proof that *Proton66 OOO* could be operated by the same person as *Hostway LLC*, it already constitutes a strong lead towards this hypothesis.

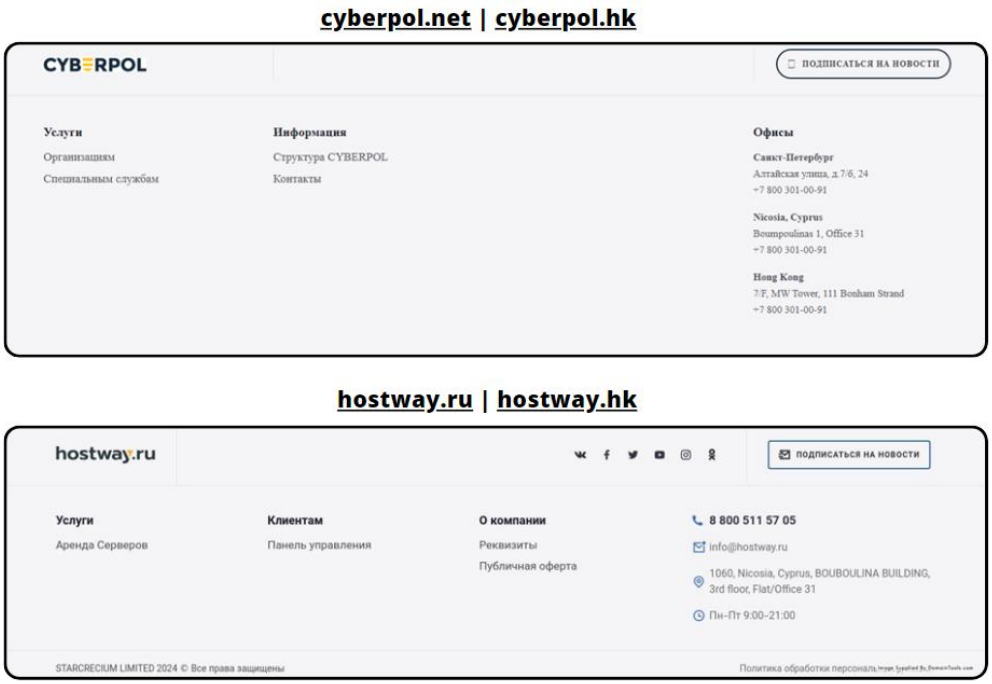

Figure 2. Snippet of the websites cyberpol[.]net and hostway[.]ru.

3.3. Intel from clashes between bulletproof providers

In July 2023, a client of the bulletproof service "**SecureHost"** filed a complaint on an underground forum against the owner of the service. In the complaint, the client states that SecureHost had scammed him "*under a false name*". Indeed, the client tried to contact **BEARHOST** (the bulletproof provider that we previously mentioned) through Telegram with an old contact of his but was instead answered by SecureHost.

Unintentionally, this complaint unveiled the relationship between the two bulletproof providers, as BEARHOST immediately answered to the complaint by explaining in a long paragraph how his previous Telegram "@bearhost" had been hacked and was now under the control of SecureHost.

In his complaint, the user happened to provide a proof of their exchange with screenshots even displaying the two IPs that were given to him: '**45.140.17**[.]**3**' and '**45.134.26**[.]**63**', both part of AS198953 – *Proton66 OOO*. Clearly implicating that SecureHost is operating *Proton66 OOO*.

SecureHost
SecureHost is a bulletproof hosting provider advertised since 2022 on underground Russian-speaking forums. It notably declares **ignoring DMCA** and **Spamhaus requests**. The servers are located in Russia, with a direct access to an Internet Exchange Point (IX).

The following layout (*figure 3*) aims to summarize the links that we could find between the previously mentioned entities and highlight the key elements strongly suggesting that they could be part of a common network.

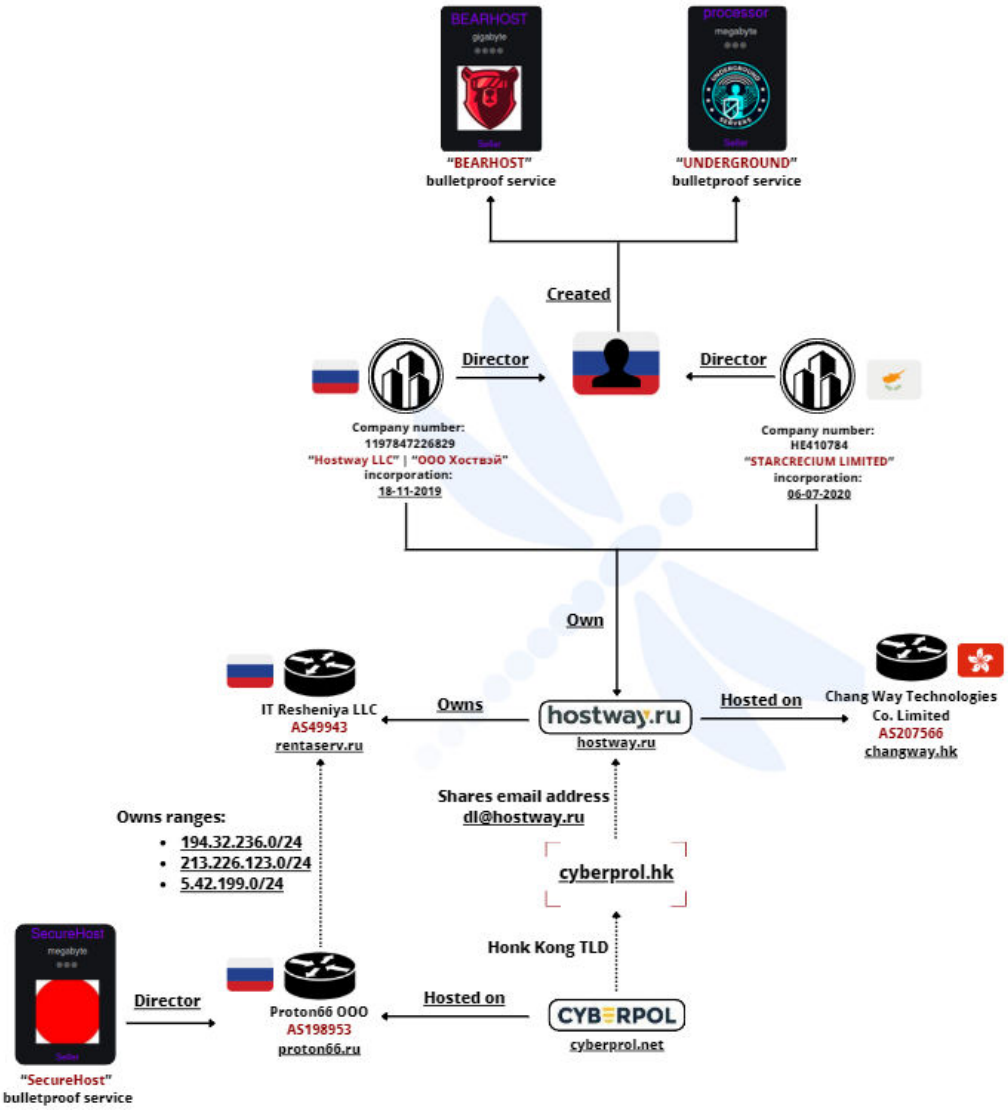

Figure 3. Layout of the links that the above-mentioned entities share with one another.

4. Linking Proton66 to PROSPERO

4.1. Network infrastructure similarities

We noticed that, in October 2024, *Proton66 OOO* (AS198953) shared almost the **same percentage** of peering agreements[4] with larger Russian ISPs as another anonymous Russian autonomous system named *PROSPERO OOO* (AS200593). Indeed, Both AS get their upstream from the **same ISPs** with almost the same percentage of load and are both connected in the datacentre **PITER-IX** located in **St. Petersburg**.[5]This corroborates with SecureHost' statements, that mentioned how his network is directly connected to an internet exchange point in Russia.

	AS3216	AS9002	AS35000
PROSPERO OOO AS200593	**51**%	**35**%	**11**%
Proton66 OOO AS198953	**44.6**%	**29.7**%	**22.8**%

Source: Hurricane Electric.

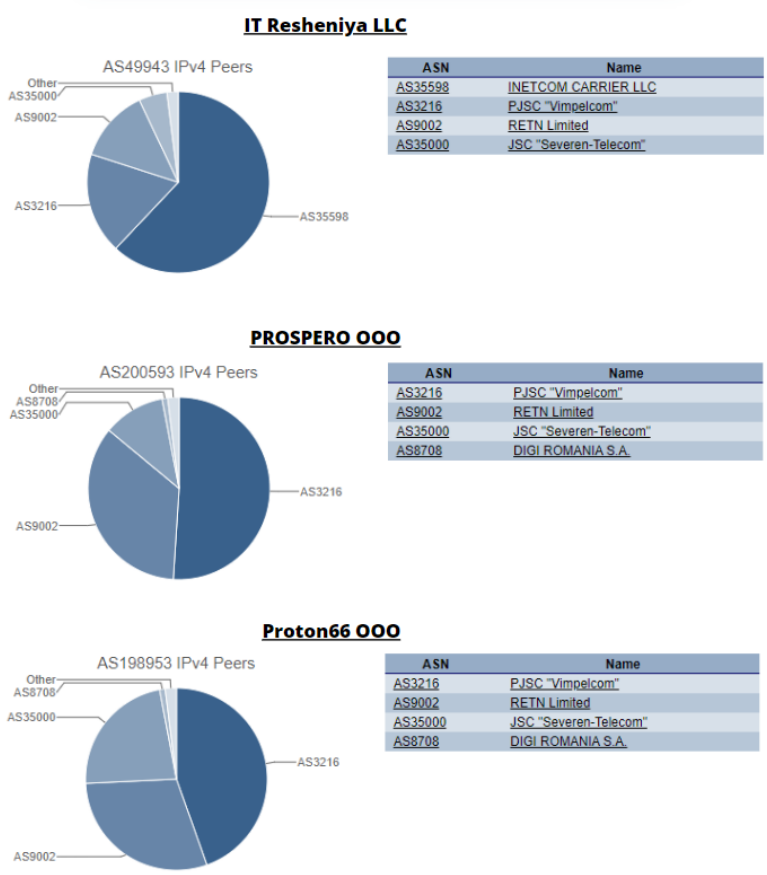

Figure 4. Pie charts of the percentage of load shared with the above-mentioned autonomous systems. Source: Hurricane Electric.

[4] *https://bgp.he.net/*

[5] *https://bgp.he.net/exchange/PITER-IX%20St.%20Petersburg*

In November, both *PROSPERO* and *Proton66* changed their peering agreements at the same time with the same ISPs: **AS35000** and **AS3216**—thus sharing respectively about the same amount of load. Shortly after, they both "*re-peered*" with *RETN Limited* – AS9002, at the same time with the same previous percentage of load (~30%).

	AS35000	AS3216
PROSPERO OOO AS200593	**21**%	**79**%
Proton66 OOO AS198953	**33**%	**67**%

Source: Hurricane Electric.

These similarities, again, do not constitute an indisputable proof that *Proton66 OOO* and *PROSPERO* OOO may be operated by the same administrator, but remain a strong element that reinforce this hypothesis.

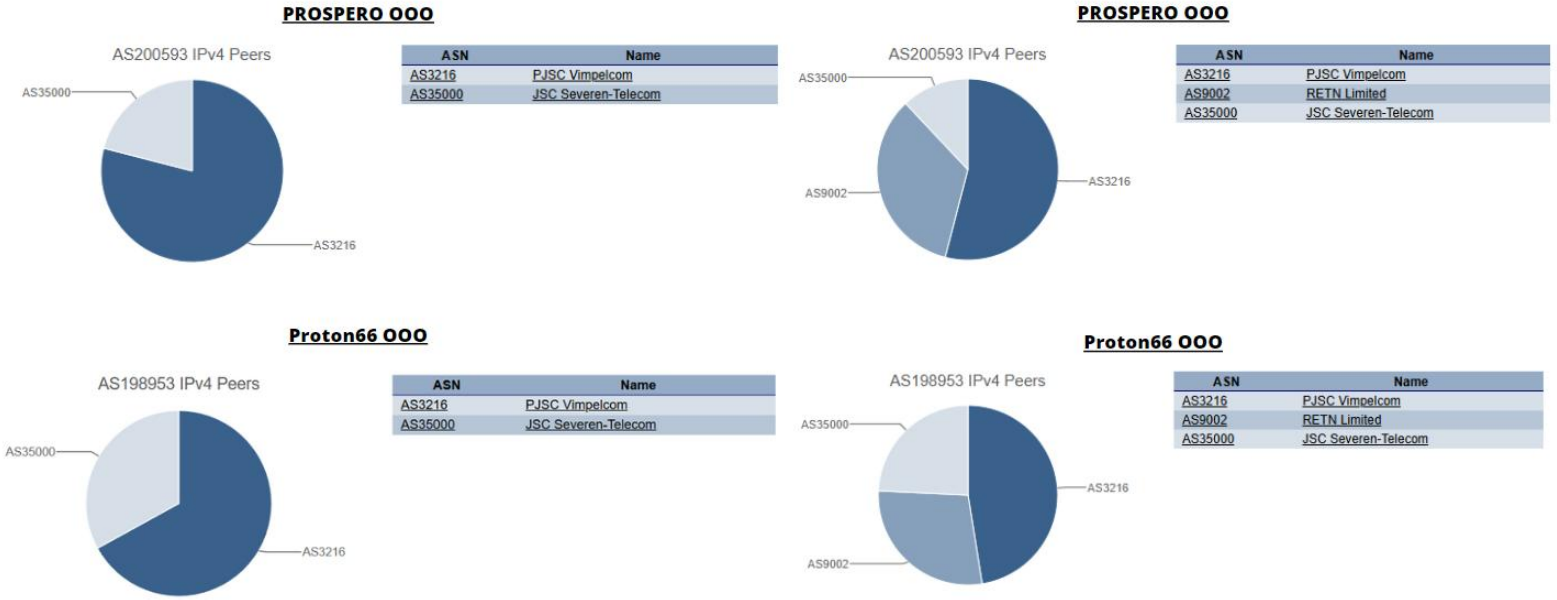

Figure 5. Pie charts of the percentage of load shared with the above-mentioned autonomous systems. Source: Hurricane Electric.

5. The network's links with Access Brokers

5.1. GootLoader's command-and-control servers

GootLoader is an **initial access broker** known for leveraging SEO techniques and compromised WordPress websites to make them host **fake forum discussions** related to trending or common topics that users may search on search engines; the most common subjects being related to **legal** or **financial** issues. Deepwatch notably discovered[6] that a compromised WordPress website could host up to **200 blog posts** covering all kinds of subjects.

Regarding GootLoader affiliation with PROSPERO, as mentioned on a blog post[7] operated by an anonymous security researcher "*dedicated to pissing off the GootLoader threat actor*" (as he indicates), GootLoader recently changed its command-and-control server in early **September 2024**. It moved from '**temporary**[.]**fail**' hosted on '**91.215.85**[.]**21**' along '**91.215.85**[.]**111**', both owned by *PROSPERO OOO*, to '**setting**[.]**cc**' hosted on '**45.135.232**[.]**53**' and owned by *Proton66 OOO*.

The operators of GootLoader seem to be long-time clients of *PROSPERO*: in **February 2023** the DFIR Report reported[8] on an intrusion that started with a GootLoader infection in which the threat actor deployed a **Cobalt Strike beacon** with watermark **206546002**. The payload then communicated with a C2 hosted on another IP owned by *PROSPERO*: '**91.215.85**[.]**143**'.

Leveraged by ransomware affiliates
According to a tweet[9] by Microsoft posted in September, GootLoader was notably observed being used as an initial access vector for **ransomware attacks** operated by the **INC ransomware** group to target US healthcare providers.
Additionally, CrowdStrike revealed that **Vice Spider**, a cybercrime threat actor that used to deploy the **Rhysida ransomware**, has been leveraging GootLoader for initial access purposes since at least June 2024. More recently in October 2024, Vice Spider used it to access two U.S-based entities.[10]
In August 2024, CISA notably warned in its #StopRansomware report[11] that **BlackSuit** actors used SystemBC and GootLoader to "*load additional tools and maintain persistence*".

5.2. SpyNote infrastructure

SpyNote is a malware targeting **Android** users usually via fake applications. Once installed on the victim's machine, SpyNote exfiltrates sensitive information such as the **device's location**, **the contacts list**, **SMS**, and can **record audios** or **phone calls**.

We recently discovered an infrastructure of domains hosted on *PROSPERO* distributing SpyNote payloads through **fake Chrome updates**. Once one is visiting those domains, the download of a SpyNote APK would launch automatically. When executed, some payloads would communicate with

[6] *https://5556002.fs1.hubspotusercontent-na1.net/hubfs/5556002/2022%20PDF%20Download%20Assets/ADA%20Compliant%20pdfs/Reports/PUBLIC_Gootloader%20-%20Foreign%20Intelligence%20Service.pdf*
[7] *https://gootloader.wordpress.com/2024/09/05/gootloader-c2-sails-to-new-hoster-and-new-url/*
[8] *https://thedfirreport.com/2024/02/26/seo-poisoning-to-domain-control-the-gootloader-saga-continues/*
[9] *https://x.com/MsftSecIntel/status/1836456417315656076*
[10] *CrowdStrike CSA-241150*
[11] *https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a*

C2 '**45.94.31**[.]**96**' on port **7544**, and others with '**45.141.58**[.]**120**' on port **5353**. Both IPs are announced by *1337 Services GmbH* – **AS210558**, another network that we believe with *a high level of confidence* to be linked to the bulletproof hosting provider '**StarkRDP**', often advertised on underground forums.

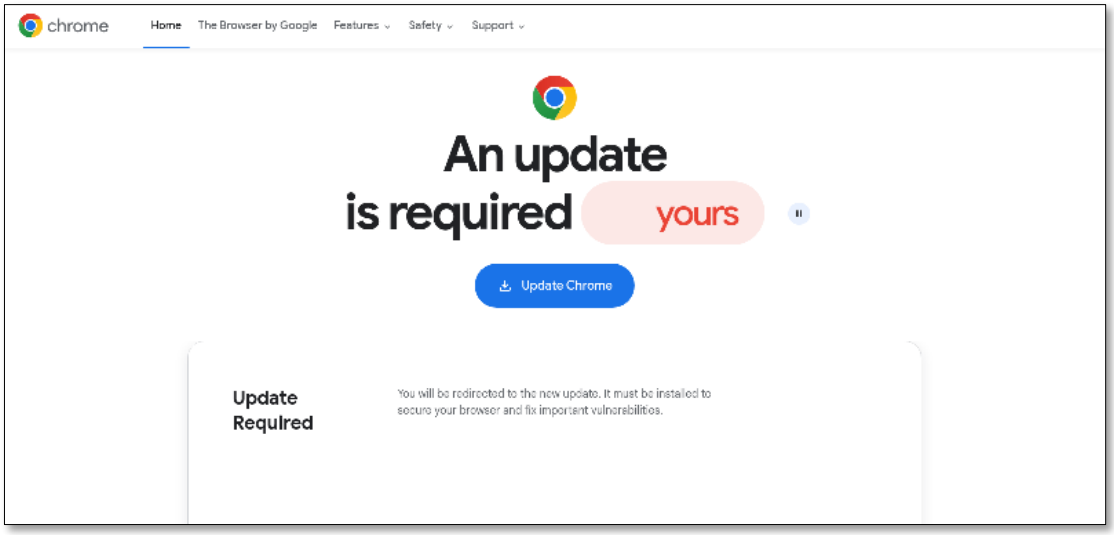

Figure 6. Phishing page hosted on: 'crome-update-gr[.]com/ready.apk' downloading a SpyNote APK.

The chrome phishing domains were hosted on either *PROSPERO OOO* – AS200593 or *Proton66 OOO* - AS198953, once again, strengthening the potential link between the two. The following table lists the domains that were deploying the same SpyNote payloads at around the same period of time.

Domain name	IP	AS name
avastpx[.]com	193.143.1[.]14	Proton66 OOO
avastpy[.]com	193.143.1[.]14	Proton66 OOO
avastuo[.]com	193.143.1[.]14	Proton66 OOO
avastxo[.]com	193.143.1[.]14	Proton66 OOO
avastop[.]com	193.143.1[.]14	Proton66 OOO
avastme[.]com	193.143.1[.]99	Proton66 OOO
avastsf[.]com	91.215.85[.]79	PROSPERO OOO
avastcsw[.]com	91.215.85[.]79	PROSPERO OOO
avastxp[.]com	91.215.85[.]79	PROSPERO OOO
updatemyacc[.]com	91.215.85[.]16	PROSPERO OOO
avastpm[.]com	193.143.1[.]86	Proton66 OOO
avastpn[.]com	193.143.1[.]86	Proton66 OOO
avastax[.]com	193.143.1[.]86	Proton66 OOO
avastcsm[.]com	193.143.1[.]86	Proton66 OOO
avastga[.]com	193.143.1[.]86	Proton66 OOO
avastcv[.]com	193.143.1[.]14	Proton66 OOO
avastsgp[.]com	193.143.1[.]14	Proton66 OOO
avastpst[.]com	91.215.85[.]79	PROSPERO OOO
avastnw[.]com	91.215.85[.]79	PROSPERO OOO
avastsp[.]com	91.215.85[.]79	PROSPERO OOO
avastvx[.]com	91.215.85[.]79	PROSPERO OOO

This is the second time that *Proton66 OOO* is used along another AS to host C2 panels or phishing pages for a specific campaign. As a reminder, when a **Matanbuchus** campaign was launched in May, the C2s were hosted on both *Chang Way Technologies Co. Limited* – AS207566 and *Proton66 OOO* - AS198953. Since the Russian individual managing the bulletproof service '**UNDEGROUND**' (a.k.ka **BEARHOST**) controls *Chang Way Technologies Co.*, we could be led to believe that he also controls *Proton66 OOO*, and thus *PROPSPERO OOO*, or that the Matanbuchus operator contacted both UNDERGROUND and SecureHost.

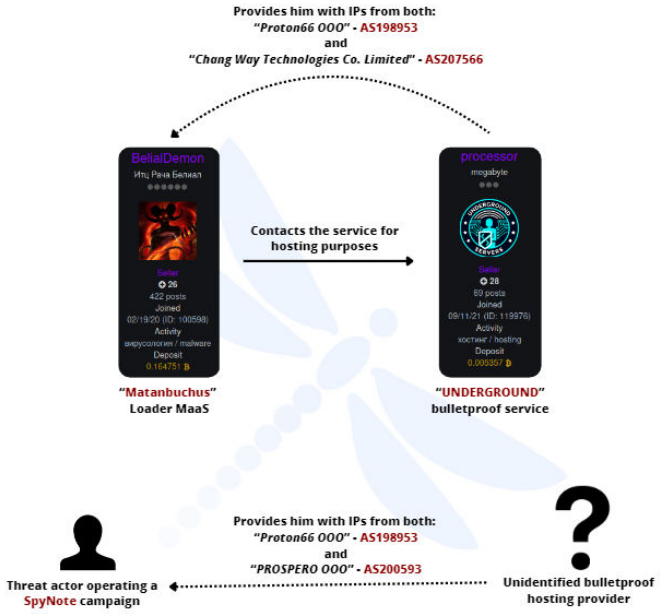

Figure 7. Layout summarizing the hypothesis that both the threat actor that operated the SpyNote campaigns and the threat actor behind the Matanbuchus campaigns contacted the same bulletproof provider 'UNDERGROUND'.

5.2.1. Simultaneously distributing revoked AnyDesk versions

Before deploying SpyNote, some of these domains were used to distribute **revoked AnyDesk versions** for both **Windows** and **Mac**. For example, the domain "**avastcsw**[.]**com**" hosted on *PROSPERO* IP **91.215.85**[.]**79**, continues to host both AnyDesk on URL '*avastcsw*[.]*com/anydesk.dmg*', and SpyNote on URL '*avastcsw*[.]*com/Avastavv.apk*'.

AnyDesk leaked data
In January 2024, the French Cybersecurity Agency ANSSI released a security bulletin[12] regarding the data leak suffered *by AnyDesk Software GmbH*, resulting in private keys and certificates disclosure and thus forcing the company to revoke some versions of the software. Those campaigns prove that this **leak continues to be abused** by threat actors in campaigns distributing revoked versions.

[12] *https://www.cert.ssi.gouv.fr/alerte/CERTFR-2024-ALE-003/*

Figure 8. Phishing page used to distribute revoked AnyDesk versions.

5.3. SocGholish fingerprinting scripts

Placed on the 11th position of most seen malwares C2 in Spamhaus' threat update of January to June 2024[13], **SocGholish** is a loader used as an initial access vector for **ransomware** attacks. It was notably used by ransomware groups such as **Evil Corp** and **LockBit**.[14]

We mentioned in a previous analysis[15] how SocGholish was hosting its fingerprinting script on domain '*marvin-occentus*[.]*net/statistic/js/stat.js*' resolving the IP **91.212.166**[.]**21** owned by *Proton66 OOO* – AS198953. We recently discovered that SocGholish was still using that IP to host a new domain for its fingerprinting script: '*www-wpx*[.]*net/assets/core.js*'.

This new URL and script can already be found in many infected websites (see "Indicators of compromise" section of this report) and redirects to the same domain that we previously found: '**pluralism.themancav**[.]**com**'.

[13] *https://info.spamhaus.com/hubfs/Botnet%20Reports/Jan-Jun%202024%20Botnet%20Threat%20Update.pdf*
[14] *https://cloud.google.com/blog/topics/threat-intelligence/unc2165-shifts-to-evade-sanctions?hl=en*
[15] *https://www.intrinsec.com/wp-content/uploads/2024/04/TLP-CLEAR-Matanbuchus-Co-Code-Emulation-and-Cybercrime-Infrastructure-Discovery-1.pdf*

5.3.1. FakeBat scripts

On the same IP '**91.212.166**[.]**21**', a domain hosting a different script could also be found: '*letmespellmoons*[.]*com/bg/js/stat.js/*', this time operated by another loader named "**FakeBat**", a malware regularly mistaken with SocGholish. This specific script was used to display a fake Chrome update template depending on the system language of the victim visiting the website infected with FakeBat's script.

```
function replaceTextByLanguage(lang) {
          var translations = {
              'en': {
                  't1': 'You are using an older version of ',
                  't2': 'Update now to keep your',
                  't3': 'browser running smoothly and securely.',
                  't4': 'Your download will begin automatically. If not, click here:',
                  't5': 'Update'
              },
              'fr': {
                  't1': 'Vous utilisez une version plus ancienne de ',
                  't2': 'Mettez a jour maintenant pour maintenir votre',
                  't3': 'navigateur fonctionne en douceur et en toute securite.',
                  't4': 'Votre telechargement debutera automatiquement. Sinon, cliquez ici :',
                  't5': 'Mettre a jour'
              },
              'de': {
                  't1': 'Sie verwenden eine altere Version von ',
                  't2': 'Aktualisieren Sie jetzt, um Ihre',
                  't3': 'Browser reibungslos und sicher zu halten.',
                  't4': 'Ihr Download beginnt automatisch. Wenn nicht, klicken Sie hier:',
                  't5': 'Aktualisierung'
              },
              'es': {
                  't1': 'Estas usando una version anterior de ',
                  't2': 'Actualice ahora para mantener su',
                  't3': 'navegador funcionando sin problemas y de forma segura.',
                  't4': 'Su descarga comenzara automaticamente. Si no es asl, haga clic aqul:',
                  't5': 'Actualizar'
              }
          };
```

Figure 9. Content of the script found on websites infected by FakeBat.

Once the victim tries to download this fake update, the payload is downloaded from a different domain also hosted on the same IPs:

- doggygangers[.]com/YfMv2QsjpCQl845BWSYNfNOQitweyze_Z6lIlrRr43MRjX_HrM/get_download_file_name.php

This domain was previously found in an investigation[16] led by eSentire in April 2024, regarding a FakeBat campaign. Nonetheless, they didn't mention at that time the other domain "letmespellmoons[.]com" that we found to be hosting FakeBat's fingerprinting script.

[16] *https://www.esentire.com/blog/fakebat-malware-distributing-via-fake-browser-updates*

6. Leveraging PROSPERO for ransomware activities

Among the other malwares that briefly used PROSPERO for their infrastructure, we can mention the ransomware group "**Buthi**" in 2023, in an incident reported by Symantec,[17] and the ransomware group "**Mallox**" in September 2024, mentioned in a blog post written by Securelist.[18]

The botnet **Gozi** used IPs managed by *PROSPERO* for its command-and-control servers in campaigns targeting Italian companies in 2023. [19] This Russian-speaking group notably changed activities from banking account theft to initial access for its own ransomware group.[20]

PikaBot, the successor of **QakBot**, known for deploying the **BlackBasta** ransomware, also used multiple IPs from *PROSPERO* to host its command-and-control servers as reported by Sekoia[21] in June 2024.

In February 2023, The DFIR Report responded to an incident[22] that started with an **IcedID** infection, another initial access broker, and ended with the encryption of the victim's network by the **Nokoyawa** ransomware group. In this attack the threat actor used a *PROSPERO* IP for its **Cobalt Strike** C2.

7. Deploying Coper (Octo) spyware in Greece

Along SpyNote, we found another spyware targeting android devices named "**Coper**", being hosted on domains spoofing the Greek bank *Alpha Bank*. For example, the URL "*allphaa-gr*[.]*com/assets/myAlpha.apk*", hosted on *PROSPERO* IP '**91.215.85**[.]**79**', would launch the download of a Coper infected APK when visited. These malicious domains were spread to Greek citizens through SMS spam campaigns.

When executed, the Coper APK would communicate with two C2 servers hosted on a different *PROSPERO* IP '**91.202.233**[.]**138**':

- *mine-495834*[.]*xyz*
- *mine-495834*[.]*net*

This specific range, '**91.202.233**[.]**0/24**', was notably added to the Spamhaus blocklist (**SBL631395**)[23] in December 2023.

[17] *https://symantec-enterprise-blogs.security.com/threat-intelligence/buhti-ransomware*
[18] *https://securelist.com/mallox-ransomware/113529/*
[19] *https://x.com/JAMESWT_MHT/status/1641002609765916672*
[20] *https://www.bleepingcomputer.com/news/security/ursnif-malware-switches-from-bank-account-theft-to-initial-access/*
[21] *https://blog.sekoia.io/pikabot-a-guide-to-its-deep-secrets-and-operations/*
[22] *https://thedfirreport.com/2024/04/01/from-onenote-to-ransomnote-an-ice-cold-intrusion/*
[23] *https://check.spamhaus.org/results/?query=SBL631395*

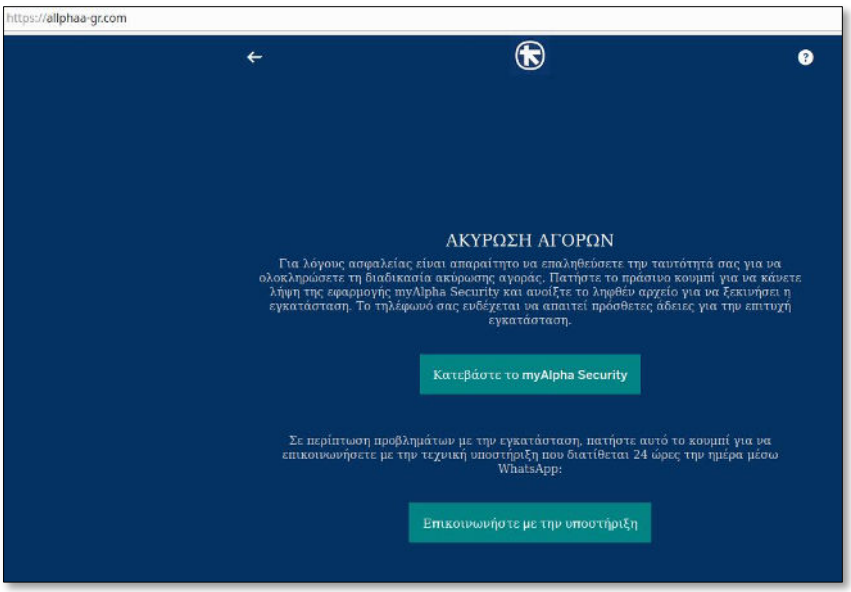

Figure 10. Phishing page usurping the Greek bank Alpha Bank.

8. Cryptocurrency themed phishing

Many phishing pages usurping **cryptocurrency airdrops** or **wallet solutions** could also be found on *PROSPERO*'s IPs. Their main purpose consists of luring the user visiting the website into **entering the passphrase** used to recover their crypto accounts.

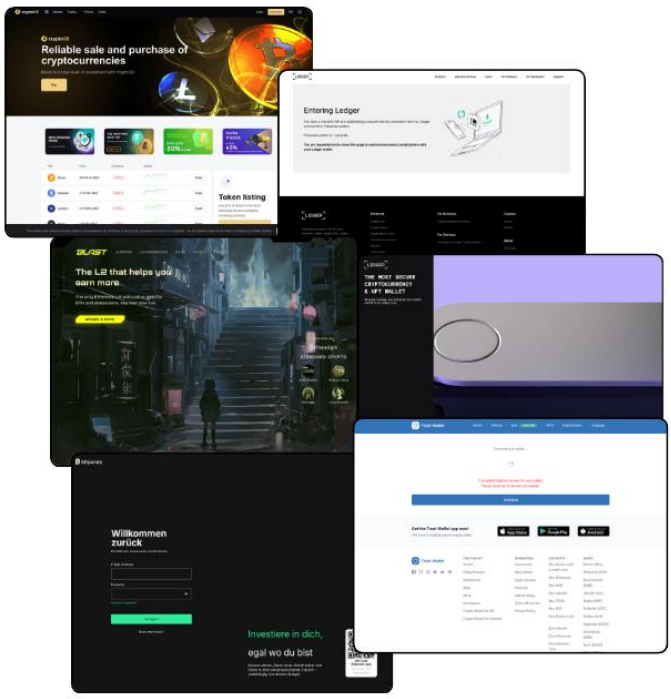

Figure 11. Snippet of the phishing pages related to cryptocurrency fraud schemes that we could find on PROSPERO IPs.

The table below lists the variety of pages related to cryptocurrency frauds that we were able to find on *PROSPERO*'s autonomous system:

Domain name	Descripition
crypto-qs[.]com	Fake platform to sale and purchase cryptocurrencies
ledger-hardware-services[.]com	Phishing for Ledger wallet recovery phrase
ledger-service-hardware[.]com	Phishing for Ledger wallet recovery phrase
ledger-portal[.]com	Phishing for Ledger wallet recovery phrase
app-blastl2[.]com	Usurp real cryptocurrency airdrop named "Blast"
873911-coinbase[.]com	Fake Coinbase login page
29395341-coinbase[.]com	Fake Coinbase login page
path-coinbase[.]com	Fake Coinbase login page
trust-wallet-service[.]com	Phishing for Trust Wallet recovery phrase
trstwalsecu[.]com	Phishing for Trust Wallet recovery phrase
account.bitpanda-bestaetigungsverfahren[.]com	Fake Bitpanda login page

9. SMS spam campaigns for banking fraud

Some of the various phishing pages hosted on *PROSPERO* were sent to various countries through **SMS spamming campaigns**. In **Australia** for example, the Energy Bill Relief Fund, a direct energy bill rebate provided by the Australian Government[24], was used to lure citizens of Australia receiving these fakes governmental SMS into entering their MyGov[25] credentials.

Domain name	IP address
mygovau-service[.]com	91.215.85[.]79
notice-ausreport[.]com	91.215.85[.]79
notice-reportaus[.]com	91.215.85[.]79
mygovau-service[.]com	91.215.85[.]79
energy-smtp-services-encrypted-redir[.]com	91.215.85[.]16
ausenergyrebate[.]com	91.215.85[.]16
energy-relief-fund[.]com	91.215.85[.]16

Along the phishing pages, the IP '91.215.85[.]79' also resolved two domains: `ayrebzignar[.]com` and `sms-mougin[.]com`, which were hosting SMS gateways probably used to operate the spamming campaigns.

[24] *https://www.energy.vic.gov.au/households/help-paying-your-energy-bills/energy-bill-relief-fund*

[25] MyGov is a governmental website ran by Services Australia that gives access to a range of online government services in one place.

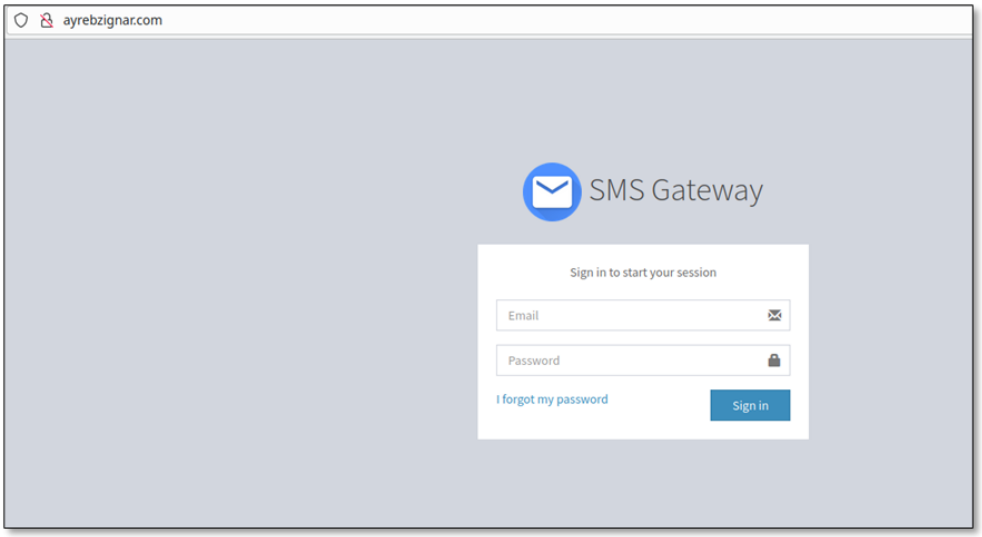

Figure 12. Login page for a SMS gateway service hosted on ayrebzignar[.]com and sms-mougin[.]com.

The same kind of domain nomenclature targeting the Australian platform could also be found on *Proton66*. The following table only highlights a few of those:

Domain name	IP address
notice-servicesaus[.]com	193.143.1[.]14
mygovaus-inbox[.]com	193.143.1[.]14
mygov-inboxaus[.]com	193.143.1[.]14
mygov-security[.]com	193.143.1[.]14

In addition to Australia, **Poland** was also targeted in September 2024 by the same kind of spamming campaigns, this time with phishing pages spoofing the financial service *Revolut*.[26]

During the same month, **France** also received its fair share of spamming and phishing pages related to various services of **transportation** and **banking**, along other countries such as **Sweden**, **Scotland** and the **United States**.

Domain name	Targeted country
notif-bnp[.]com	France
8-bnpparibas[.]com	France
api-confirmer-bnp[.]com	France
confirmer-bnp[.]com	France
clien-bnp[.]com	France
macledigital-bnp[.]com	France
alerte-bnp[.]com	France
cledigitales-bnp[.]com	France
api.alerte-bnp[.]com	France
validation-bnp[.]com	France
louvrebanqueprivee-moncompte[.]com	France

[26] *https://cert.orange.pl/ostrzezenia/oszusci-udaja-revolut/*

louvrebanqueprivee-monespace[.]com	France
Swed banks:	Sweden
swedbank-help[.]com	Sweden
Scottish bank:	Scotland
scotiabank-auth[.]com	Scotland
scotiaonline-loginscotia[.]com	Scotland
snb-olbanking[.]com	United States

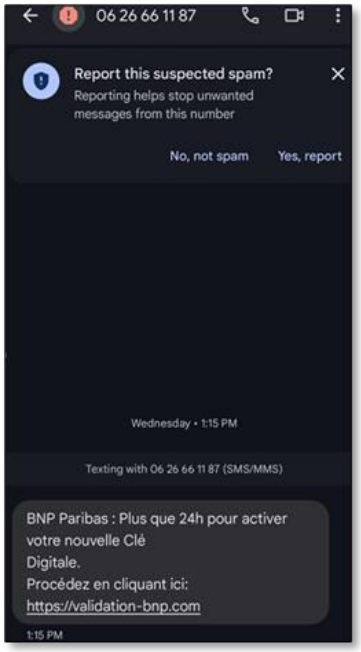

Figure 13. SMS spam received from a French number that contained a phishing domain hosted on a PROSPERO announced IP.

Once again, those type of campaigns could also be observed on IPs owned by *Proton66*. This time the campaigns also targeted **Portugal**, **Spain** and **Mexico**, along the countries that we previously observed on *PROSPERO* (see table below).

Domain name	Targeted country
ativar-conta[.]com	Portugal
portal-dasfinancas[.]com	Portugal
santanderhelppage[.]com	Spain
web-manage-help-secure-support[.]com	Spain
hsbcsecure-mexico[.]com	Mexico
cba-support-team[.]com	Australia
device-authorisation[.]com	United Kingdom
borgerindberetning[.]com	Denmark

Interestingly, some of those IPs used for phishing were **recycled** for multiple uses and campaigns throughout time. '**91.215.85**[.]**183**' for example, which hosted most of the phishing pages targeting France, was also used for both the **Nokoyawa** and **Buhti** ransomware operations from 2023 that we previously mentioned in this report.

10. Conclusion

Investigating those networks unveiled additional malware infrastructures and reinforced our beliefs on these autonomous systems' malicious nature. Finding the links between them expanded our capacities to map the entire infrastructure of this bulletproof provider. This enabled us to block more efficiently the threats hosted on them, from **loaders** operated by **initial access brokers** providing an entry into corporate networks for **ransomware groups**, to **fraud schemes** and **phishing pages** in general.

International cooperation is often required to tackle cybercrime, and political tensions can complicate or delay this process. Russia in this case, may not always cooperate with international takedown requests, particularly if it perceive it as intrusive or politically motivated. Such actors like bulletproof services based in Russia, could be considered as "Privateer" groups, a concept first introduced by Talos[27], defining them as groups that "*are not sponsored directly by a state and are financially motivated but do benefit from direct or indirect protection from that state […] The protecting state [Russia] doesn't receive direct benefit from these groups,* ***but it is shielded from their activities****, which frequently target the geopolitical adversaries of the protecting state*". Both services analysed in this report indeed mentioned how the malicious activities operated by their clients couldn't be operated against countries of the CIS region.

Therefore, as long as bigger ISPs do not "*de-peer*" with those networks and provide them with connectivity to the internet, the activities hosted on their servers will **continue to prosper**.

[27] https://blog.talosintelligence.com/privateer-groups/

11. Actionable content

11.1. Indicators of compromise

Value	Type	Description
c0c90848a962514b8f3e40b18721fb868f615422cedc1b7472b5301fc5ac74c7	SHA-256	SpyNote – "ready.apk"
94a3b1fc830323234f5ac6e69cf0840507c23e15bee5c8c3aa86fddaf61ef8b1	SHA-256	SpyNote – "Avastavv.apk"
b020cedfec9f721dddfcdeededfc4d7f18f495c7862a84151df4b5eab01eb1b7	SHA-256	Coper - "MyAlpha.apk"
ec33d8ee9c3881b8fcea18f9f862d5926d994553aec1b65081d925afd3e8b028	SHA-256	Revoked AnyDesk version for Windows
9960c49e9e2b4d98c0b3ae2da97f17daf7bf5dd19b974f5d2bdfbece8e888b3b	SHA-256	Revoked AnyDesk version for Mac
200593	ASN	"PROSPERO OOO"
198953	ASN	"Proton66 OOO"
49943	ASN	"IT Resheniya LLC"
207566	ASN	"Chang Way Technologies Co. Limited"
91.202.233[.]0/24	IPv4 range	AS200593
91.215.85[.]0/24	IPv4 range	AS200593
193.143.1[.]0/24	IPv4 range	AS198953
45.134.26[.]0/24	IPv4 range	AS198953
45.135.232[.]0/24	IPv4 range	AS198953
45.140.17[.]0/24	IPv4 range	AS198953
91.212.166[.]0/24	IPv4 range	AS198953
194.32.236[.]0/24	IPv4 range	AS49943
213.226.123[.]0/24	IPv4 range	AS49943
5.42.199[.]0/24	IPv4 range	AS49943
185.7.214[.]0/24	IPv4 range	AS207566
92.255.57[.]0/24	IPv4 range	AS207566
92.255.85[.]0/24	IPv4 range	AS207566
45.94.31[.]96	IPv4	SpyNote C2
45.141.58[.]120	IPv4	SpyNote C2
91.212.166[.]21	IPv4	Hosting SocGholish's screening script
www-wpx[.]net	Domain	Hosting SocGholish's screening script
letmespellmoons[.]com	Domain	Hosting SocGholish's screening script
cleanenergycommercial[.]com	Domain	Infected with SocGholish
islanderalumni[.]org	Domain	Infected with SocGholish
newwesttruck[.]ca	Domain	Infected with SocGholish
khirallahboston[.]com	Domain	Infected with SocGholish
acist[.]com	Domain	Infected with SocGholish
russolresolution. [.]om	Domain	Infected with SocGholish
medm[.]ca	Domain	Infected with SocGholish
coveragecollege[.]com	Domain	Infected with SocGholish
subrogationstrategist[.]com	Domain	Infected with SocGholish
hirevalueinc[.]com	Domain	Infected with SocGholish

ivgea[.]org	Domain	Infected by FakeBat
saratogacasino[.]com	Domain	Infected by FakeBat
mdlgroup[.]com	Domain	Infected by FakeBat
doggygangers[.]com	Domain	FakeBat operated
setting[.]cc	Domain	GootLoader C2
temporary[.]fail	Domain	GootLoader C2
avastcsw[.]com	Domain	Deploying revoked AnyDesk and SpyNote
avastsf[.]com	Domain	Deploying revoked AnyDesk version
avast-antivirus[.]com	Domain	Deploying revoked AnyDesk version
tsb-live-chat[.]com	Domain	Deploying revoked LiveChat version
crome-update-gr[.]com	Domain	Deploying SpyNote
allphaa-gr[.]com	Domain	Deploying Coper
mine-495834[.]xyz	Domain	Coper C2
mine-495834[.]net	Domain	Coper C2
avastpx[.]com	Domain	Deploying SpyNote
avastpy[.]com	Domain	Deploying SpyNote
avastuo[.]com	Domain	Deploying SpyNote
avastxo[.]com	Domain	Deploying SpyNote
avastop[.]com	Domain	Deploying SpyNote
avastme[.]com	Domain	Deploying SpyNote
avastxp[.]com	Domain	Deploying SpyNote
updatemyacc[.]com	Domain	Deploying SpyNote
avastpm[.]com	Domain	Deploying SpyNote
avastpn[.]com	Domain	Deploying SpyNote
avastax[.]com	Domain	Deploying SpyNote
avastcsm[.]com	Domain	Deploying SpyNote
avastga[.]com	Domain	Deploying SpyNote
avastcv[.]com	Domain	Deploying SpyNote
avastsgp[.]com	Domain	Deploying SpyNote
avastpst[.]com	Domain	Deploying SpyNote
avastnw[.]com	Domain	Deploying SpyNote
avastsp[.]com	Domain	Deploying SpyNote
avastvx[.]com	Domain	Deploying SpyNote
crypto-qs[.]com	Domain	Cryptocurrency themed phishing
ledger-hardware-services[.]com	Domain	Cryptocurrency themed phishing
ledger-service-hardware[.]com	Domain	Cryptocurrency themed phishing
ledger-portal[.]com	Domain	Cryptocurrency themed phishing
app-blastl2[.]com	Domain	Cryptocurrency themed phishing
873911-coinbase[.]com	Domain	Cryptocurrency themed phishing
29395341-coinbase[.]com	Domain	Cryptocurrency themed phishing
path-coinbase[.]com	Domain	Cryptocurrency themed phishing
trust-wallet-service[.]com	Domain	Cryptocurrency themed phishing
trstwalsecu[.]com	Domain	Cryptocurrency themed phishing
account.bitpanda-bestaetigungsverfahren[.]com	Domain	Cryptocurrency themed phishing

11.2. Recommendations

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

12. Sources

- https://web.archive.org/web/20231018093233/https://oliverhough.io/prospernot-PROSPERO-as-the-little-as-that-could-part-1/
- https://www.hyas.com/blog/hyas-insight-uncovers-and-mitigates-a-russian-based-cyberattack
- https://cert.orange.pl/ostrzezenia/oszusci-udaja-revolut/
- https://symantec-enterprise-blogs.security.com/threat-intelligence/buhti-ransomware
- https://thedfirreport.com/2024/04/01/from-onenote-to-ransomnote-an-ice-cold-intrusion/
- https://www.lemagit.fr/actualites/252496421/Ces-mysterieuses-entreprises-qui-se-font-attribuer-des-blocs-IPv4
- https://www.silentpush.com/blog/anydesk/
- https://medium.com/@Appsec_pt/diving-into-a-phishing-campaign-the-mistery-of-plesk-servers-and-proton66-ooo-7f2eb25a96bd
- https://www.esentire.com/blog/fakebat-malware-distributing-via-fake-browser-updates
- https://info.spamhaus.com/hubfs/Botnet%20Reports/Jan-Jun%202024%20Botnet%20Threat%20Update.pdf
- https://www.csoonline.com/article/3531730/microsoft-warns-of-ransomware-attacks-on-us-healthcare.html
- https://www.cert.ssi.gouv.fr/alerte/CERTFR-2024-ALE-003/
- https://bgp.he.net/irr/as-set/AS-SET-HOSTWAY
- https://bgp.he.net/exchange/PITER-IX%20St.%20Petersburg
- https://bgpranking.circl.lu/
- https://www.intrinsec.com/wp-content/uploads/2024/04/TLP-CLEAR-Matanbuchus-Co-Code-Emulation-and-Cybercrime-Infrastructure-Discovery-1.pdf
- https://check.spamhaus.org/results/?query=SBL631395
- https://blog.talosintelligence.com/privateer-groups/

INTRINSEC

Innovative by design

Cyber Threat Intelligence

@Intrinsec @Intrinsec Blog Website

If you have any inquiries regarding this report, please contact cti-rens-invest@intrinsec.com