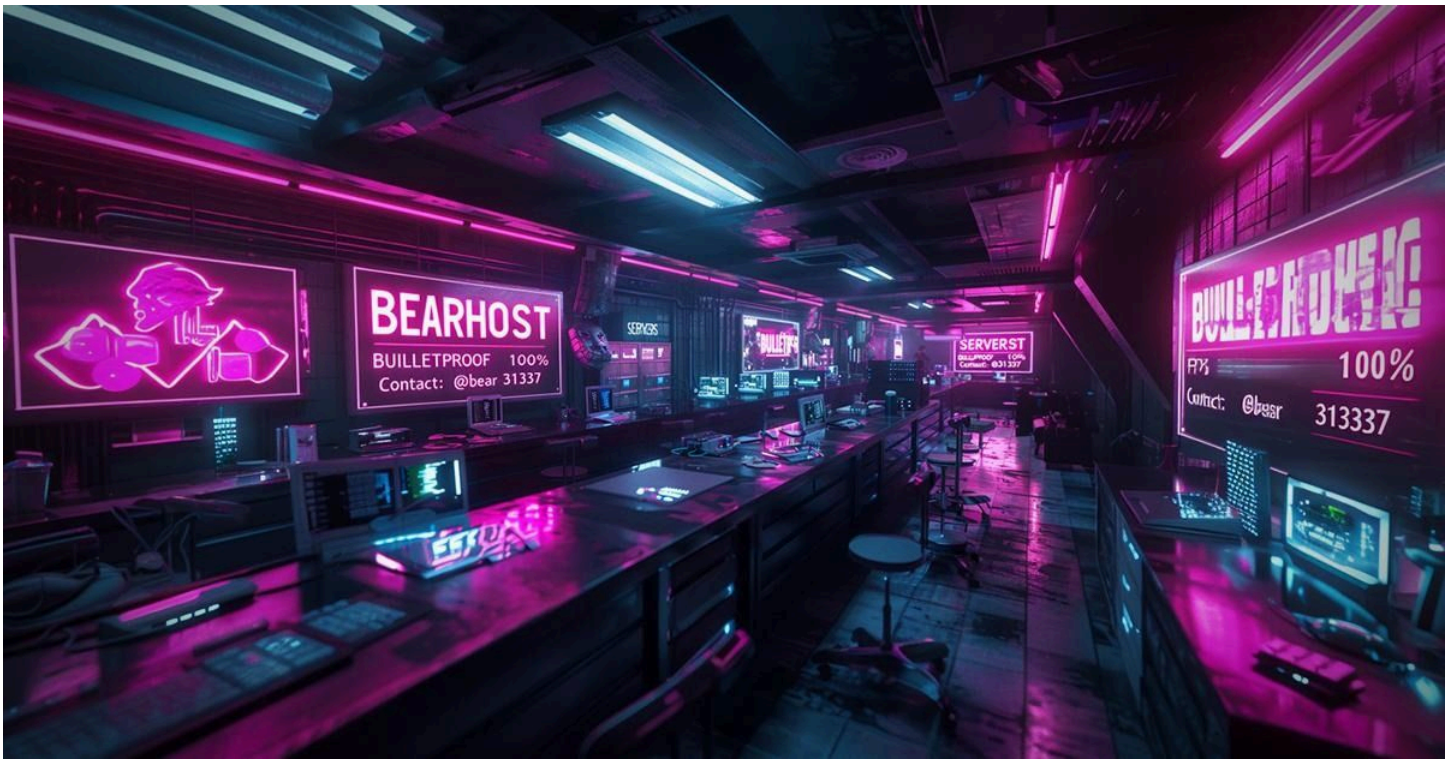
Qilin Ransomware and the Ghost Bulletproof Hosting Conglomerate

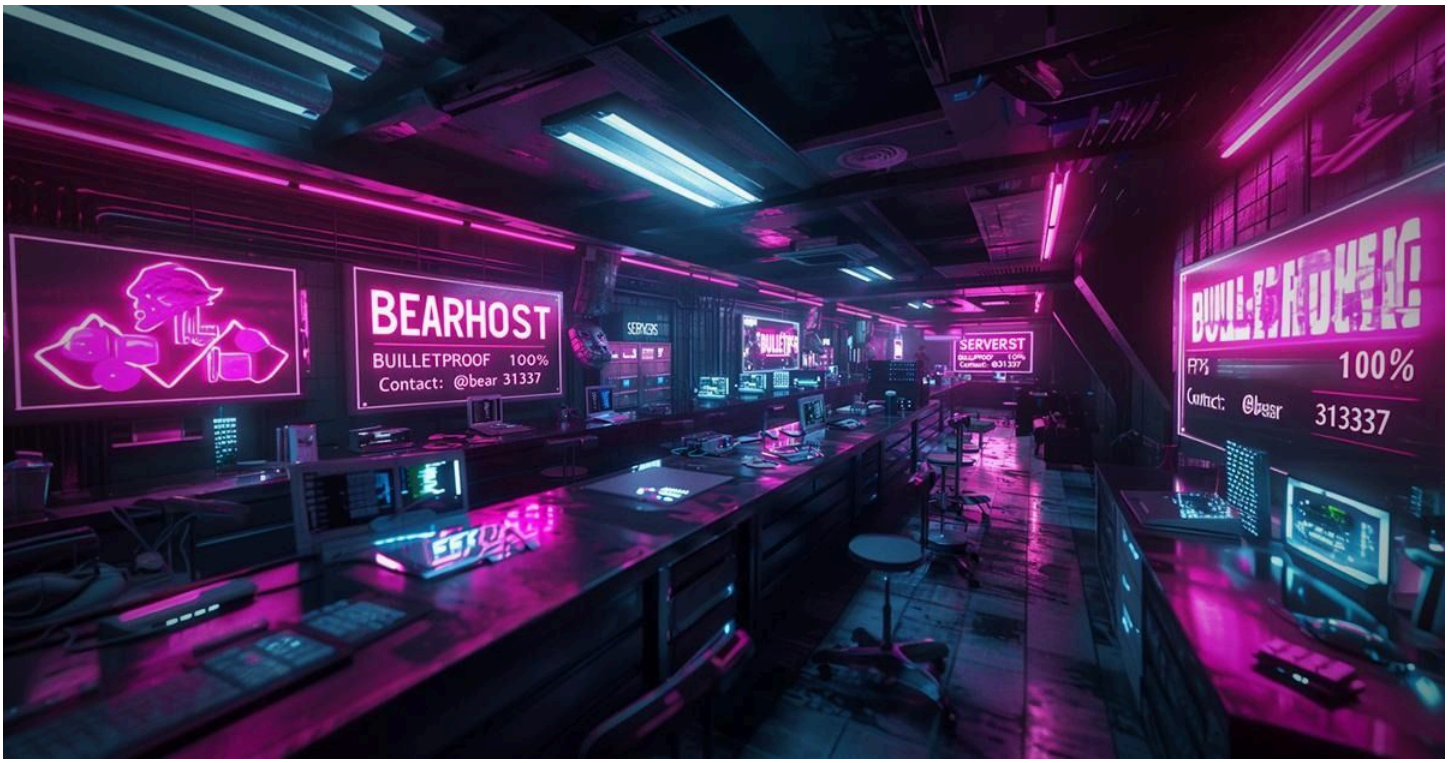
Back

Cyber Threat Intelligence

15 Oct 2025

dark web, cybercrime, cybercriminals, ransomware, ISP, telco





Intro

The following Resecurity report will explore the **Qilin** ransomware-as-a-service (RaaS) operation's reliance on bullet-proof-hosting (BPH) infrastructures, with an emphasis on a network of rogue providers based in different parts of the world. **Qilin** is one of the most prolific and formidable threat groups extorting organizations today. Most notably, they recently claimed responsibility for the September ransomware attack that crippled operations and manufacturing functions at Japanese brewing conglomerate, **Asahi Group Holdings**, for nearly two weeks.

Qilin's use of prominent BPH providers, highlights the latter's role as critical infrastructure for cybercriminal operators. Rogue BPH services enable their clients to host content with minimal or no oversight. Frequently incorporated in pro-secrecy jurisdictions and structured across complex webs of anonymous and geographically distributed shell companies, BPH services are designed to be resilient to abuse complaints and even law enforcement intervention.

Their business model thrives on zero KYC (Know Your Customer) and a total absence of due-diligence checks, effectively creating safe havens for cyber-offenders who wish to remain anonymous. These malign infrastructures, and the pro-corporate secrecy regimes that shield them, enable destructive ransomware campaigns and other malicious cybercriminal operations to persist undisturbed for prolonged durations.

What is Qilin Ransomware?

Qilin is a highly sophisticated Ransomware-as-a-Service (RaaS) operation that first emerged in mid-2022, initially using the name "**Agenda**." The group rebranded to "**Qilin**" later that year. According to the Health Sector Cybersecurity Coordination Center (HC3), **Qilin** ransomware has "variants written in Golang and

Rust, and is known to gain initial access through spear phishing, as well as leverage Remote Monitoring and Management (RMM) and other common tools in its attacks."

Qilin is also "known to practice double extortion, demanding ransom payments from victims to prevent data from being leaked," according to HC3. The gang's moniker, **Qilin**, refers to a mythical creature from Chinese folklore that combines features of a dragon and a horned beast, often compared to a unicorn. However, the operation is believed to have roots in Russian-speaking cybercriminal forums and is structured around a RaaS model, where core developers provide the ransomware infrastructure and tools to a network of affiliates.

These affiliates, who are recruited via underground forums, carry out the actual attacks and share ransom payments with the operators - typically keeping 80-85%, while the operators take 15-20%. The gang has gained widespread notoriety for their malicious ransom campaigns targeting healthcare organizations, government entities, critical infrastructure operators, and asset management firms. Most notably, however, is the gang's crippling breach of the Japanese brewer Asahi Group Holdings in late September 2025.

Qilin's RaaS platform allows affiliates to configure attacks, manage victims, and negotiate ransoms via a user-friendly panel. The group maintains a **Data Leak Site (DLS)** on Tor for publishing stolen data and pressuring victims. **Qilin** has targeted a wide range of organizations across multiple sectors and geographies, with a focus on high-value targets where disruption is costly, and data is sensitive.

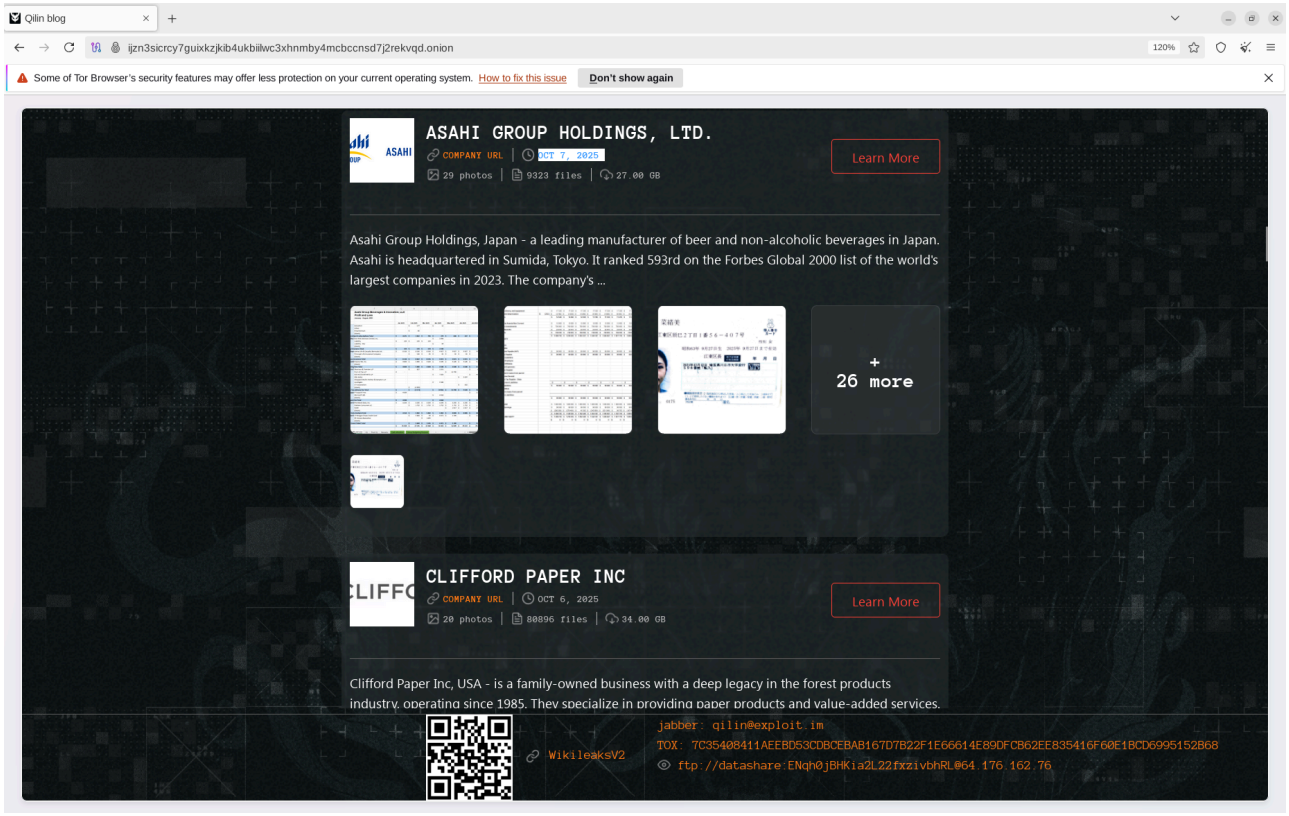
The group is also responsible for a significant number of hack-and-leak incidents and active recruitment of access brokers and affiliates. Microsoft reported actors from **North Korea** joined the group some time ago, and may include other foreign actors. In fact, one of the most interesting and less widely detailed sides of Qilin is its strong connection to an underground bulletproof hosting conglomerate with origins in Russian-speaking underground and Hong Kong (China). Resecurity is sharing collected intelligence to increase awareness within the cybersecurity community given the gang's heightened activity.

Cyberattack on Japan

Qilin ransomware group claimed responsibility for the September cyberattack on Japan's Asahi Group Holdings, the country's largest beverage manufacturer commanding nearly 40% of the national beer market, according to Morningstar. The attack disrupted operations across the conglomerate's brewing facilities, temporarily halting production and shipping at most of its 30 factories, according to *BBC* reporting.

Qilin publicly claimed responsibility for the attack and alleged the theft of a substantial amount of data from Asahi's system. As of October 10, all of Asahi Japanese facilities have partially reopened but its computer systems are still down.

Asahi confirmed that the disruption was caused by a ransomware attack and acknowledged evidence of data exfiltration. The incident led to interruptions in order processing, shipping, and customer services.**Qilin** later published internal documents and claimed to have stolen 27 GB of data from Asahi.

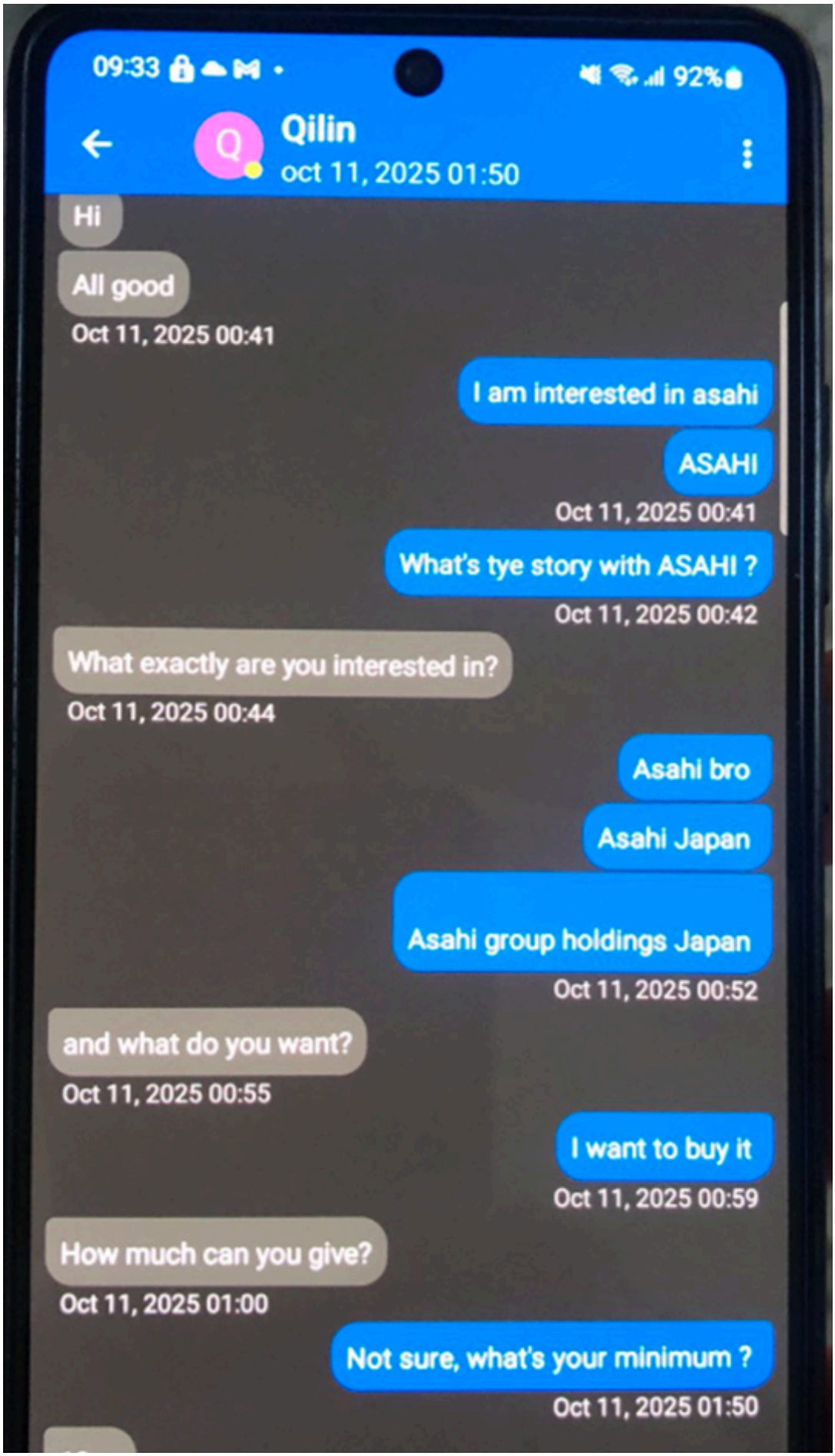


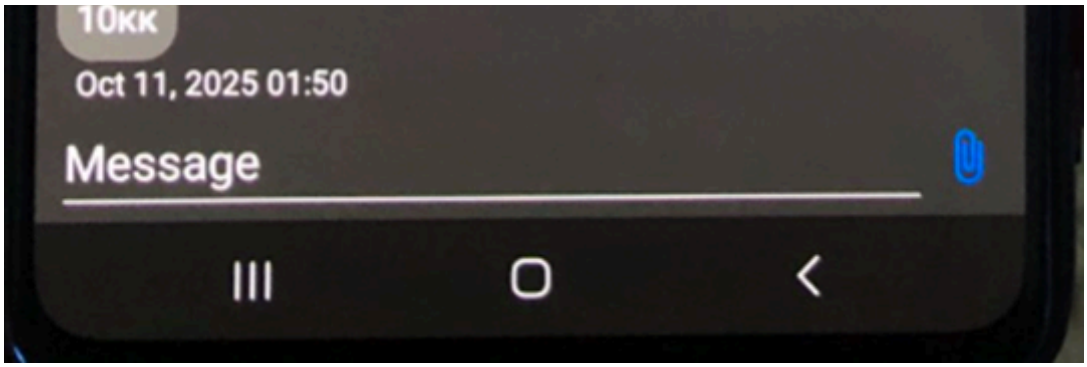
The **Qilin** ransomware attack, presumably conducted on September 29, 2025, paralyzed Asahi's digital order placement, shipment, and customer service systems, forcing the company to halt production at most of its 30 factories nationwide. Asahi had to revert to manual processes (phone, fax, hand-written orders) to maintain supply—an inefficient measure that fell far short of meeting demand during the digital outage.

The attack led to nationwide shortages of Asahi products, with major retailers and restaurants reporting out-of-stock items. The company also postponed the launch of 12 new products due to the ongoing system outage. The digital logistics and order management systems were paralyzed, causing significant supply chain bottleneck.

In terms of impact, the incident bears striking similarities to the **Trinity of Chaos**' recent ransomware attack on JLR (Jaguar Land Rover), which halted production at all its major plants globally, including facilities in the UK, Slovakia, Brazil, and India. Manufacturing and IT systems were shut down, leading to a complete stoppage of vehicle assembly lines. Both companies suffered substantial financial losses due to halted production, supply chain disruptions, and lost sales. While JLR's lost sales were estimated to approach £72 million ($97 million) per day, Asahi faced the prospect of an 83% drop in domestic operating profit in the event of a prolonged outage.

Notably, Resecurity HUNTER (HUMINT) investigators engaged in private conversations with Qilin operators and learned the threat actors are attempting to sell the stolen Asahi data **for $10 million USD**.


09:33
92%
Qilin
oct 11, 2025 01:50
Hi
All good
Oct 11, 2025 00:41
I am interested in asahi
ASAHI
Oct 11, 2025 00:41
What's tye story with ASAHI ?
Oct 11, 2025 00:42
What exactly are you interested in?
Oct 11, 2025 00:44
Asahi bro
Asahi Japan
Asahi group holdings Japan
Oct 11, 2025 00:52
and what do you want?
Oct 11, 2025 00:55
I want to buy it
Oct 11, 2025 00:59
How much can you give?
Oct 11, 2025 01:00
Not sure, what's your minimum ?
Oct 11, 2025 01:50



These demands were received on October 11, following the Asahi operations disruption, what is likely one of Qilin's tactics to exclude middlemen and accelerate pressure on the victim.

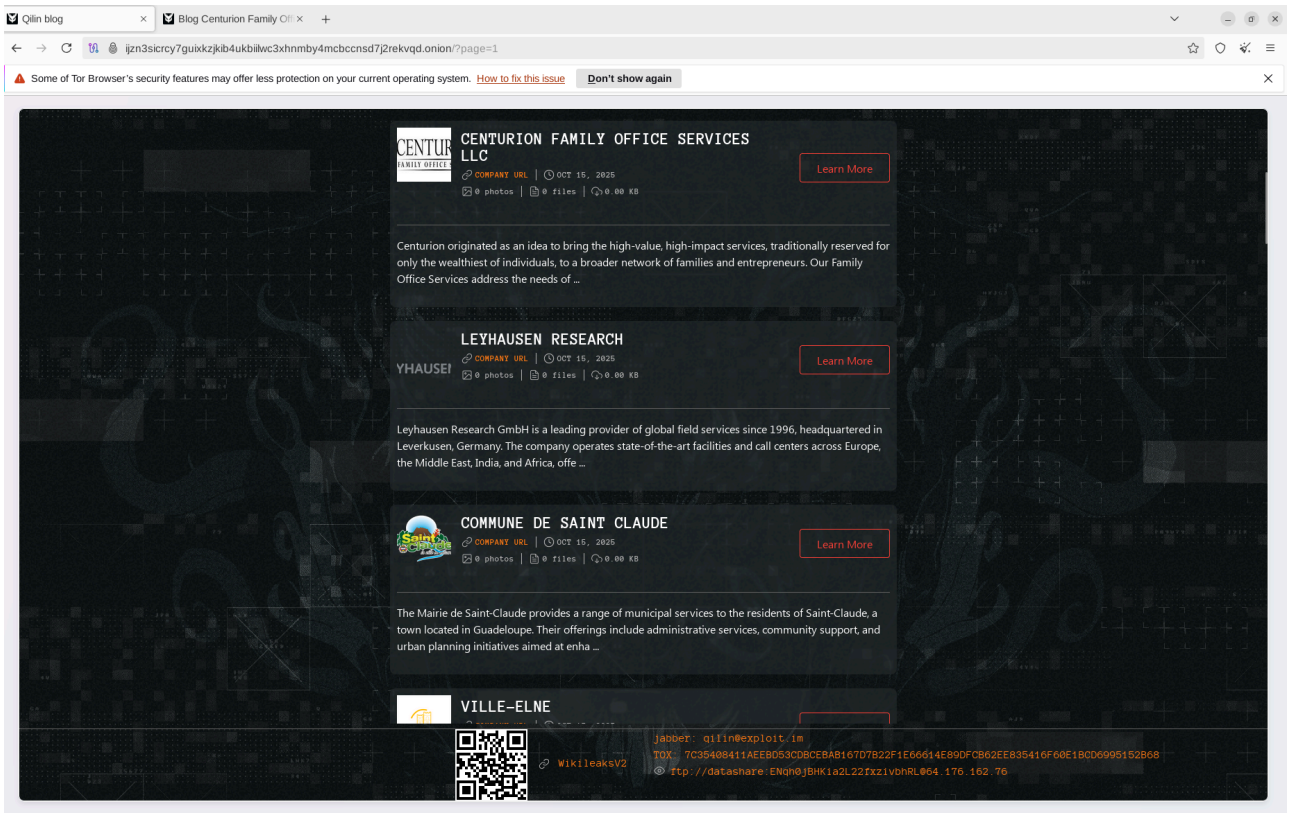
New Victims Announced

New targets and confirmed victims have been announced by Qilin today (**October 15**), including but not limited to:

- The Spanish Tax Administration Agency (Agencia Tributaria), the revenue service of the Kingdom of Spain
- Centurion Family Office Services LLC, USA
- Rasi Laboratories, a manufacturer and developer of nutraceuticals, specializing in dietary supplements like capsules, tablets, probiotics, and functional foods, USA
- Victory Christian Center, a community-focused church located in Tulsa, OK, USA
- Richmond Behavioral Health Authority (RBHA), a statewide organization dedicated to providing comprehensive mental health, mental retardation, substance abuse and prevention services to the residents of the City of Richmond
- Turnkey Africa, a leading provider of technology solutions for the insurance industry across Africa
- Charles River Properties, USA, a real estate brokerage based in Waltham, Massachusetts
- New Jersey Property-Liability Insurance Guaranty Association, USA
- Commune De Saint Claude, a municipal services body
- Ville-Elne, a commune in the Pyrénées-Orientales department in southern France.

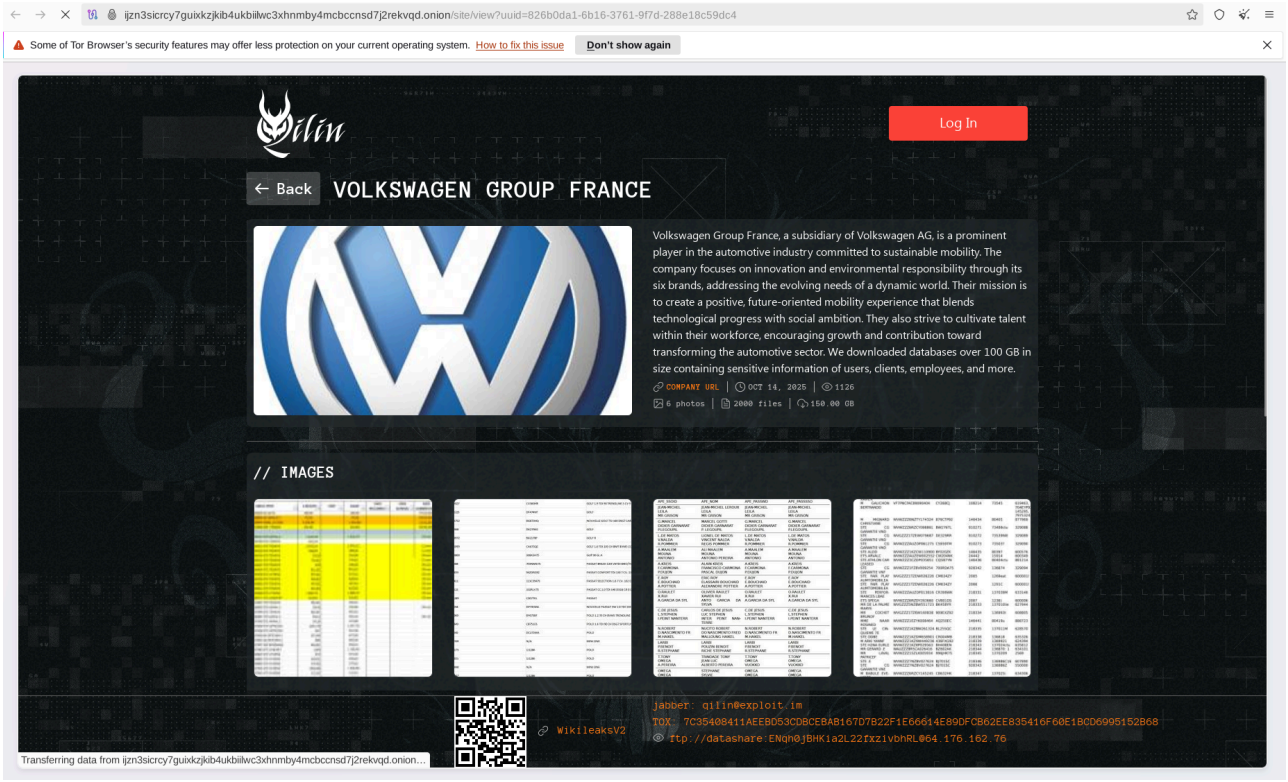
The Spanish Tax Administration Agency is especially notable among the new victims. This agency employs more than 26,000 staff and operates with a budget of $1.5 billion, processing vast amounts of data from both private and public sectors.

Prior to that, on **October 14**, Qilin announced Volkswagen Group France, a subsidiary of Volkswagen AG; Texas' San Bernard Electric Cooperative; and Karnes Electric Cooperative as compromised.

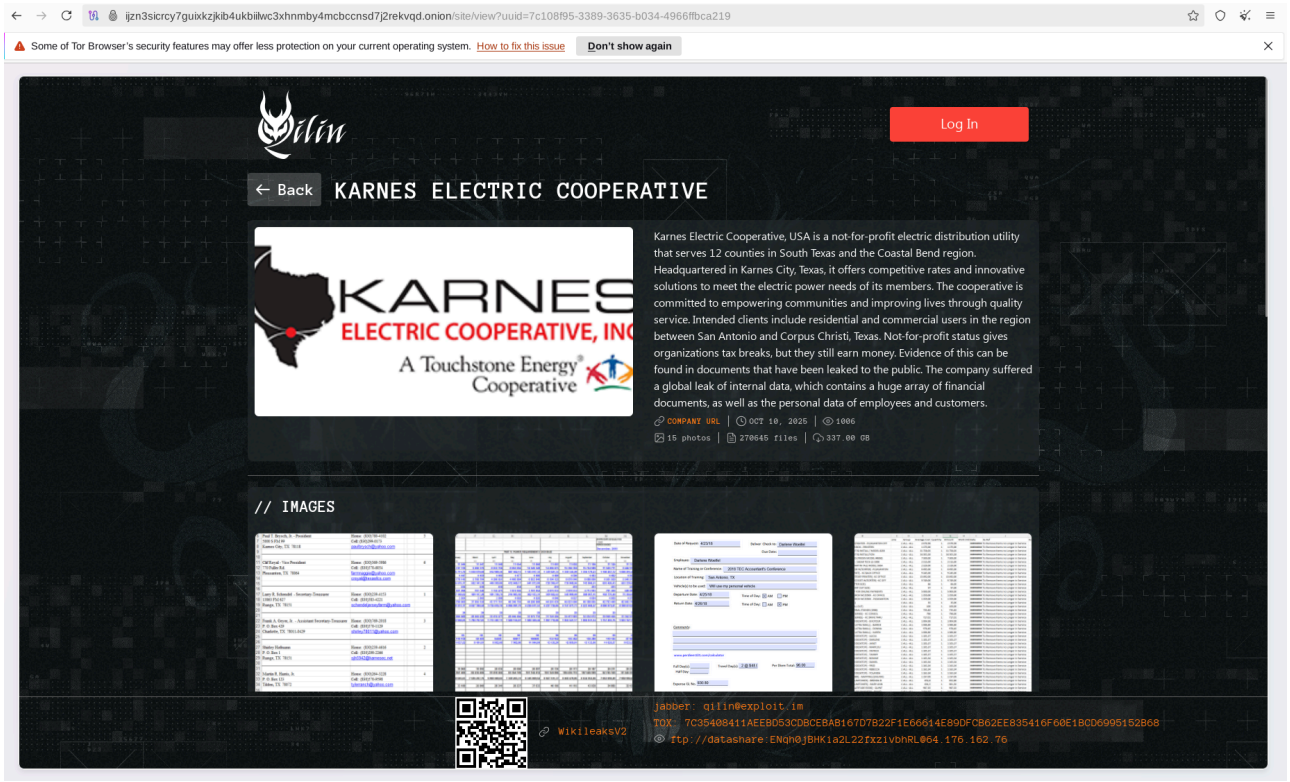


Targeting the automotive industry is particularly interesting, especially in the context of the past incident with JLR and the disruptive consequences of ransomware activity. It is possible that Qilin was inspired by the

successful outcomes of the data breach or that they collaborated with **initial access brokers (IAB)** offering compromised access to such organizations for sale on the Dark Web.



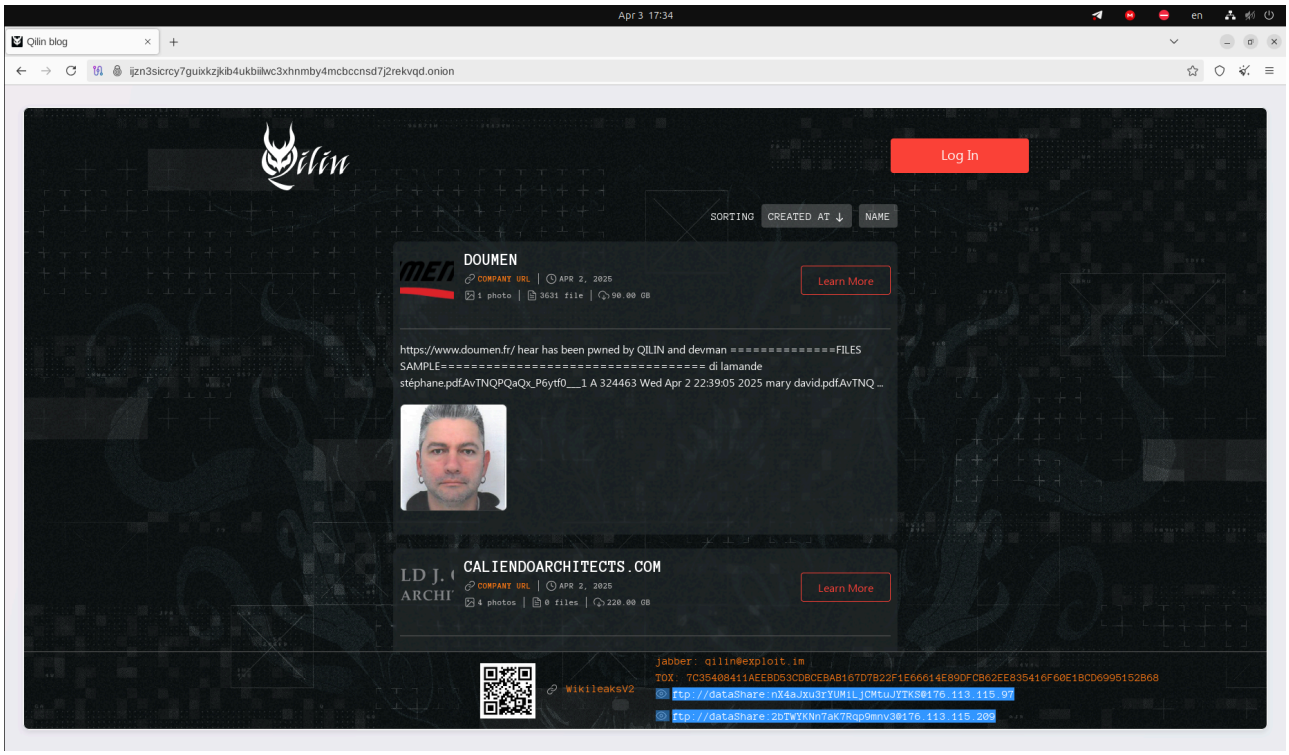
Resecurity also reviewed and validated the leaked data from the affected electric service and distribution organizations. According to our assessment, the root cause of the compromise could be **insecure remote access** and **business email compromise (BEC)** involving staff, based on historical indicators of malicious infections.



The month of October could be considered one of the most "fruitful" for Qilin, given the number of victims published and new organizations targeted. It is also evident that the group is increasing its focus on the US, attacking local municipalities such as the City of Riviera Beach, Florida, and Cobb County earlier. The group has published over 50 new victims from various market verticals and geographies, including Croatia, Grenada, France, Germany, Hungary, Italy, South Korea, Spain, Pakistan, and Qatar.

Underground Connection

A noteworthy aspect of the Qilin ransomware group is its close affiliation with underground BPH operators, who enable cybercriminals to discreetly host illicit content and infrastructure beyond the reach of law enforcement. For instance, since its emergence, the group has routinely cited multiple file-sharing hosts to retrieve victim data stored in complex legal jurisdictions. A close look at those hosts may confirm that resources are clearly managed by BPH providers. Their IP addresses are also changing from time to time.



Resecurity has been monitoring the network infrastructure associated with **Qilin** ransomware and BPH providers involved since 2024. For example, in April 2024, their DLS mentioned 176[.]113[.]115[.]97 and 176[.]113[.]115[.]209, associated with Hong Kong-based hosting provider **Cat Technologies Co. Limited.**

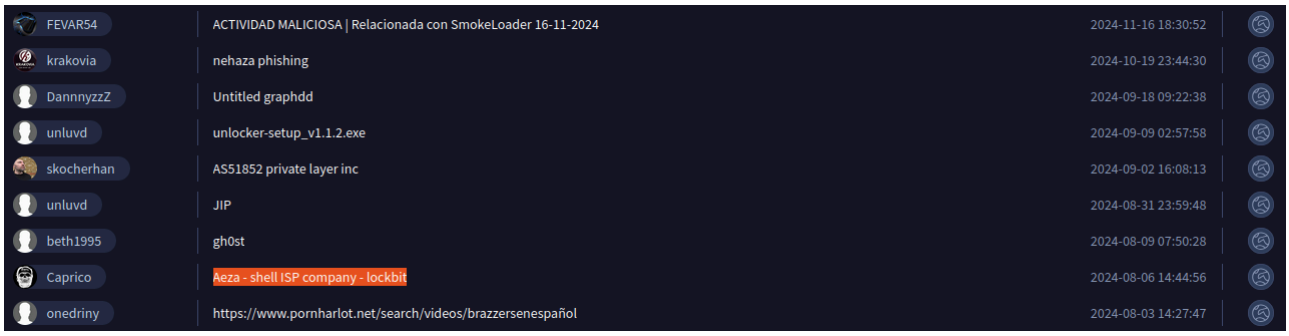
IP Address	176.113.115.97
Country	Russian Federation [RU]
Region	Moskva
City	Moscow
Coordinates of City	55.752260, 37.615470 (55°45'8"N 37°36'56"E)
ISP	Cat Technologies Co. Limited
Local Time	04 Apr, 2025 03:56 AM (UTC +03:00)
Domain	catcompany.info
Net Speed	(T1) Data Center/Transit
IDD & Area Code	(7) 0495
ZIP Code	101990
Weather Station	Moscow (RSXX0063)

The domain name associated with this entity, "**catcompany[.]info**," has been registered by an anonymous individual "Alexander," who defined "Seoul" (South Korea) as a possible location of the administrator and

Russia-based DNS servers.

```
Domain Name: catcompany.info
Registry Domain ID: a11c4fa9584a4027a03895eb24df40ea-DONUTS
Registrar WHOIS Server: <a href="http://whois.eranet.com"
rel="nofollow">http://whois.eranet.com</a>
Registrar URL: <a href="http://www.eranet.com"
rel="nofollow">http://www.eranet.com</a>
Updated Date: 2025-03-05T09:44:17Z
Creation Date: 2022-04-05T15:34:56Z
Registry Expiry Date: 2025-04-05T15:34:56Z
Registrar: Eranet International Limited
Registrar IANA ID: 1868
Registrar Abuse Contact Email: abuse@eranet.com
Registrar Abuse Contact Phone: +882.39995473
Registrant Organization: Alexander
Registrant State/Province: Seoul
Registrant Country: KR
Name Server: ns1.reg.ru
Name Server: ns2.reg.ru
```

This domain is tied to IP 194[.]58[.]112[.]174 having an extensive history of malicious activity. Notably, the entity has been linked to a shell company connected to the sanctioned **Aeza Group,** which has been implicated in a wide array of cyber-enabled criminal conspiracies.



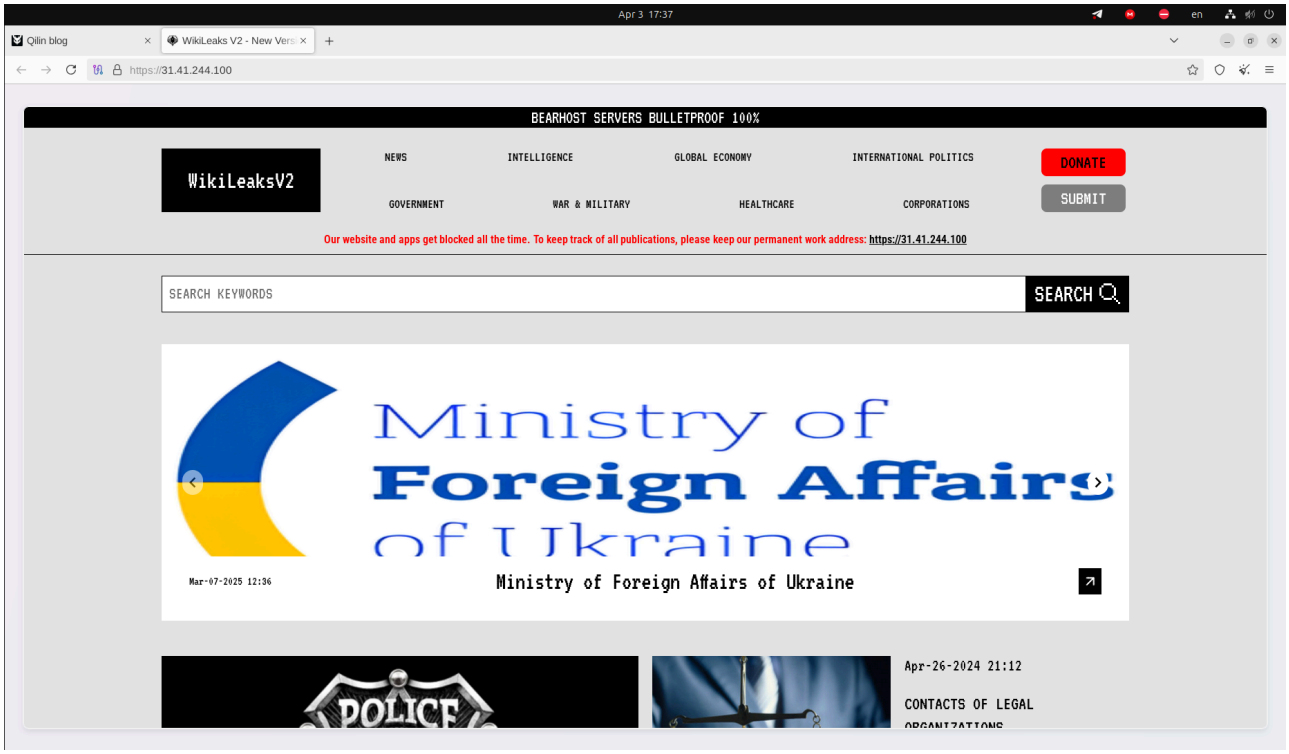
In July 2025, the U.S. Treasury Department sanctioned this entity for providing BPH services to cybercriminals. The company is accused of aiding ransomware groups like **BianLian** and hosting illicit drug markets such as BlackSprut. The sanctions also targeted Aeza International Ltd. in the UK, which was used to lease IP addresses to cybercriminals.

Previously, Aeza Group was named as the core ISP underpinning the infrastructure of a massive disinformation network dubbed **Doppelgänger** that gained infamy for spreading fake articles on websites that resemble the design of real media outlets such as *Der Spiegel* and *The Guardian.*

According to the Russian business newspaper *Kommersant*, in April 2025, the Federal Security Service (FSB) of Russia and the St. Petersburg Police Department raided an office of Aeza Group located in the former business center of the Wagner Group, a private military contractor that has been prolific throughout the Ukrainian war. According to the publication, Aeza Group was suspected of carrying out illegal banking activities and creating an organized criminal group.

Bearhost Servers - A Bulletproof Host with History

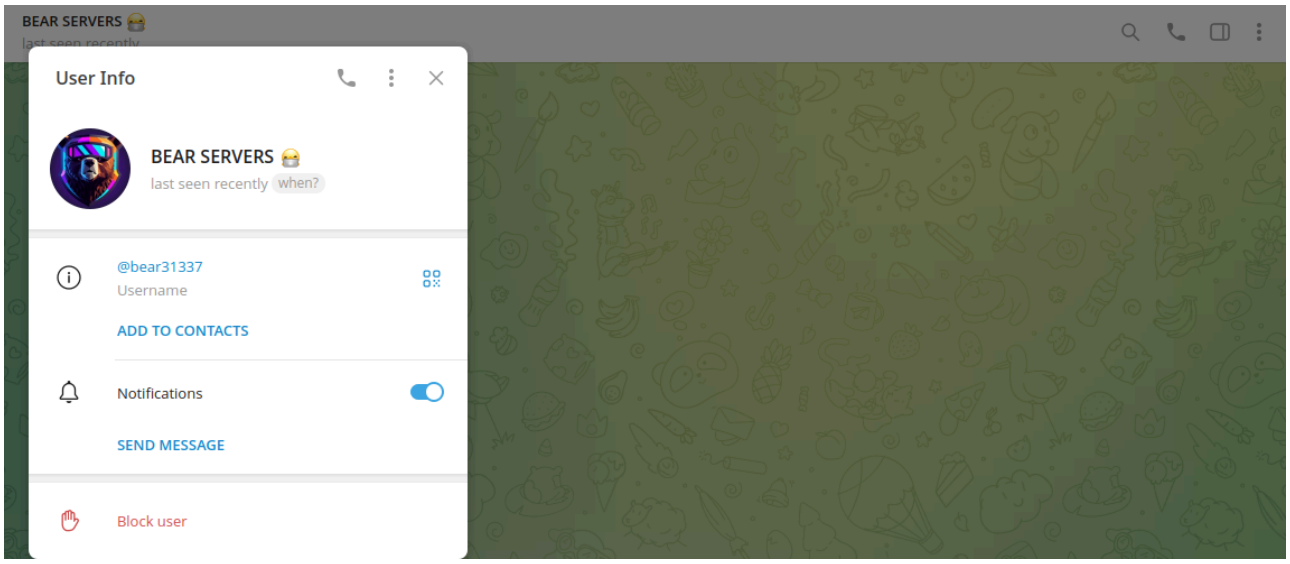
Qilin Ransomware has also launched so called "**WikiLeaksV2**" where they publish content about their activities. The header contains ads for **BEARHOST Servers**, one of the largest BPH providers, also known as **Underground** and **Voodoo Servers**.



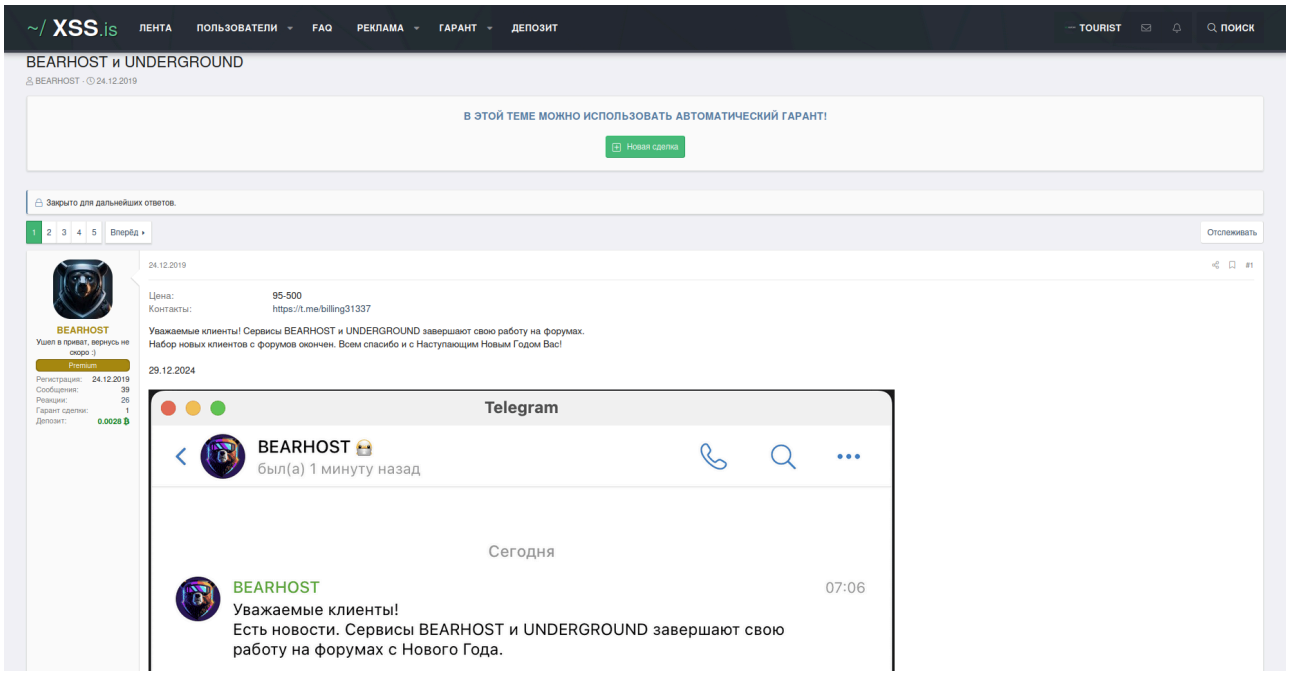
Based on historical Passive DNS records, the project was hosted at IP 31[.]41[.]244[.]100 associated with **Red Bytes LLC** (Saint Petersburg, Russia) and the domain name networkmaze[.]hk:

IP Address	31.41.244.100
Country	Russian Federation [RU]
Region	Sankt-Peterburg
City	Saint Petersburg
Coordinates of City	59.894440, 30.264200 (59°53'40"N 30°15'51"E)
ISP	Red Bytes LLC
Local Time	04 Apr, 2025 03:57 AM (UTC +03:00)
Domain	networkmaze.hk
Net Speed	(T1) Data Center/Transit
IDD & Area Code	(7) 0812
ZIP Code	190990
Weather Station	Saint Petersburg (RSXX0091)

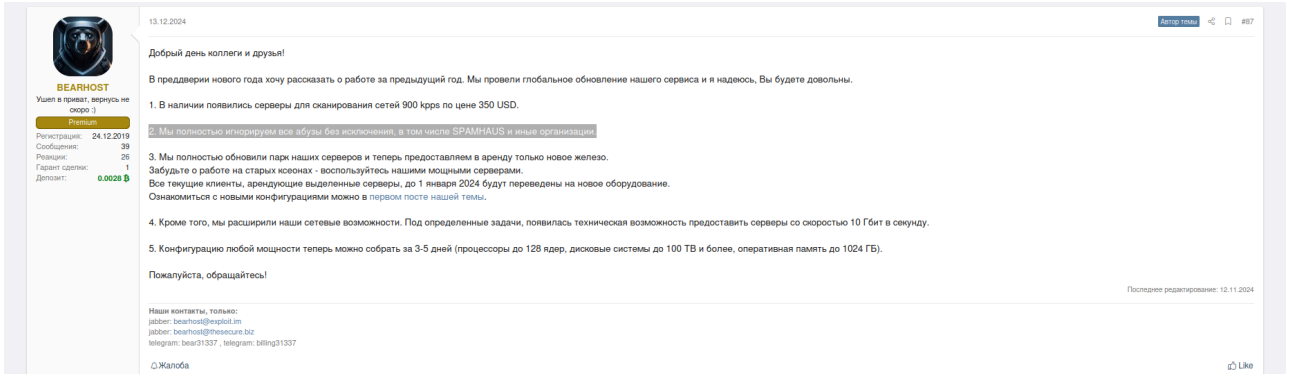
EARHOST Servers has a Telegram contact where cybercriminals can order BPH services for various needs.



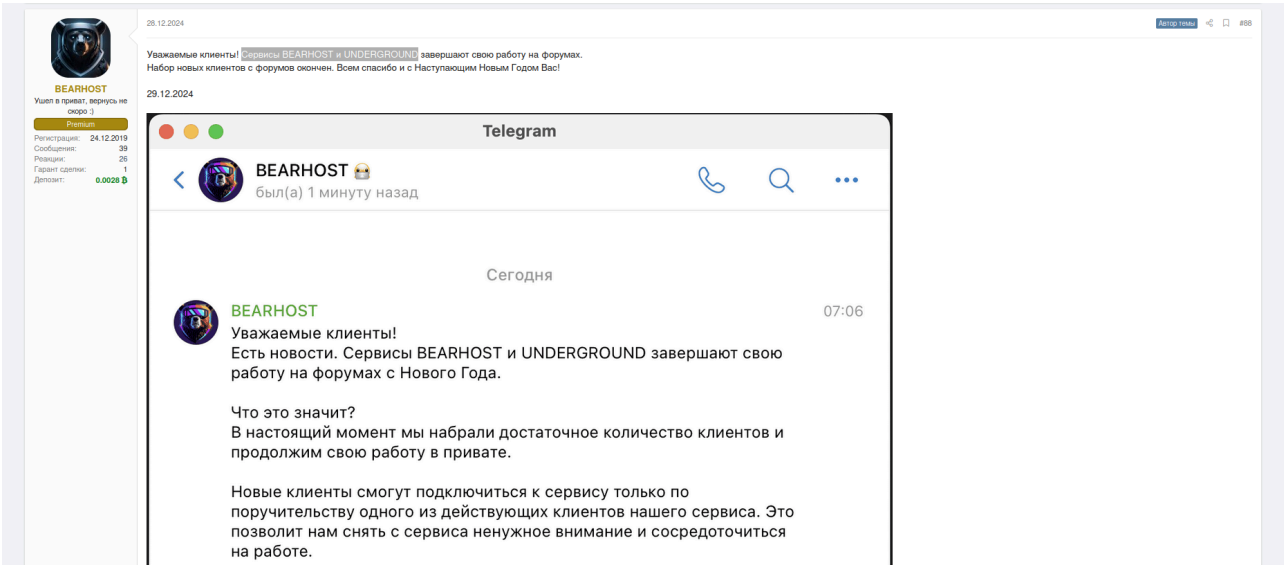
The service has been operating since at least 2019 and has registered accounts on multiple underground forums including XSS and Exploit. The pricing for their services varies from $95 to $500 and more depending on the configuration of the server.



Around December 13, 2024, BEARHOST announced the availability of servers for mass scanning. Typically, cybercriminals purchase such servers to scan for vulnerable hosts and applications and exploit them at scale. The operators behind BEARHOST highlighted their ability to provide servers with network bandwidth of up to 10 Gbps, which should facilitate network scanning. They also mentioned that they will move all existing clients to new equipment.



A few days before the start of 2025, the main operator behind BEARHOST suddenly announced that their service had stopped working.



In reality, their announcement is not so straightforward. The operators behind the BPH service mentioned that new customers will only be accepted based on vetting and through invitations from existing customers due to increased scrutiny. The BPH has not terminated any service, but has gone into private mode, servicing trusted and vetted underground actors. This concept is not new and is typical for underground vendors with credible reputations who have already built a significant customer base and are no longer interested in servicing random visitors who could be law enforcement or cybersecurity researchers trying to get more details about their subnets.

Chronological References to Bulletproof Hosting

Cat Technologies Co. Limited registered in Hong Kong (7/F, MW Tower, 111 Bonham Strand Sheung Wan Hong Kong) is sharing this address with two other legal entities related to the same bulletproof hosting conglomerate:

- Starcrecium Limited (Cyprus)
- Chang Way Technologies Co. Limited (Hong Kong)

According to RIPE Database, the contact information defined in the networks, also has reference to Starcrecium:

```
organisation:    ORG-CAT7-RIPE
org-name:        Cat Technologies Co. Limited
country:         HK
address:         7/F, MW Tower, 111 Bonham Strand
address:         Sheung Wan
address:         Hong Kong
e-mail:          info@starcrecium.com
abuse-c:         CAT77-RIPE
```

```
mnt-ref:          IP-RIPE
mnt-by:           IP-RIPE
org-type:         OTHER
created:          2023-02-20T16:35:59Z
last-modified:    2023-07-10T07:02:40Z
source:           RIPE
```

Cached copy of Starcrecium:

STARCRECIUM LIMITED
a company incorporated and registered in Cyprus
under registration No. HE 410784

1060, Nicosia, Cyprus, BOUBOULINA BUILDING,
3rd floor, Flat/Office 31
info@starcrecium.com

Starcrecium Limited (Cyprus) and Chang Way Technologies Co. Limited (Hong Kong) were named as "the official representatives" of the Russia-based hosting provider "Hostway.ru" (operating under legal entity OOO "Information Technologies"). This statement was published on their official website and Twitter accounts at far back as 2021:

Хостинг и серверы Hostway
2 May 2021 ·

Офисы и представительства Hostway 🏢

Приоритет Hostway - постоянное развитие и оказание качественных услуг. Мы открыты к диалогу и сотрудничеству с вами, поэтому сегодня расскажем о наших офисах и представительствах.

📌 Кипр
Наш основной офис располагается на Кипре. Компания Hostway (Starcrecium Limited) зарегистрирована на Кипре и имеет государственный номер No. HE 410784
Адрес: Boumpoulinas 1, Bouboulina building, Office 31, 3rd floor, Flat/Office 31, 1060, Nicosia, Cyprus

📌 Россия
Деятельность компании на территории РФ осуществляется через официального представителя компании STARCRECIUM LIMITED: ООО «Информационные Технологии», ОГРН 1177847370788
Адрес: 196066, город Санкт-Петербург, Алтайская улица, дом 7 литер б, помещение 1-н офис 24

📌 Китай
На территории Китайской Народной Республики, а также в странах Восточной Азии, деятельность компании осуществляется через официального представителя компании STARCRECIUM LIMITED: CHANG WAY TECHNOLOGIES CO. LIMITED Компания зарегистрирована в КНР, Гонг Конг и имеет регистрационный номер 2979817
Адрес: 7/F, MW Tower, 111 Bonham Strand, Sheung Wan, Hong Kong

Red Bytes LLC (Saint Petersburg, Russia) was also later added as an additional representative. Around December 2024, this information was deleted from their official website, but it is still available in a cached copy, which can be verified through the Internet Archive's Wayback Machine.

The connection between Chang Way Technologies Co. Limited and Starcrecium Limited was detailed in an August 2022 article titled “Analyzing Attack Data and Trends Targeting Ukrainian Domains”. The report highlighted IP address 152.89.196.102, previously geolocated in Russia and part of an ASN registered to Chang Way but assigned to Starcrecium. According to the article, this IP was blocked 78,438 times on .ua domains and was responsible for a total of 3,803,734 blocked attack attempts globally.

What do all these entities have in common? According to the acquired corporate records, Mr. Lenar Davletshin has been identified as a director of these entities, including but not limited to:

- Chang Way Technologies Co. Limited (Hong Kong)
- Starcrecium Limited (Cyprus)
- OOO "Red Byte" (Russia)
- OOO "Information Technologies" (Russia)
- OOO "Hostway" (Russia)
- OOO "Hostway Rus" (Russia)
- OOO "Triostars" (Russia)
- OOO "F1" (Russia)

Contact information of this individual has been also identified in subnets related to these entities:

```
person: Lenar Davletshin
address: Information Technologies LLC
address: ul. Lakhtinskaya, 18A, pom. 1-H, of. 4k
address: 197136 Saint-Petersburg
address: Russia
phone: +7 981 8068891
nic-hdl: LD5832-RIPE
mnt-by: IP-RIPE
created: 2019-04-08T18:49:08Z
last-modified: 2019-10-14T15:16:14Z
```

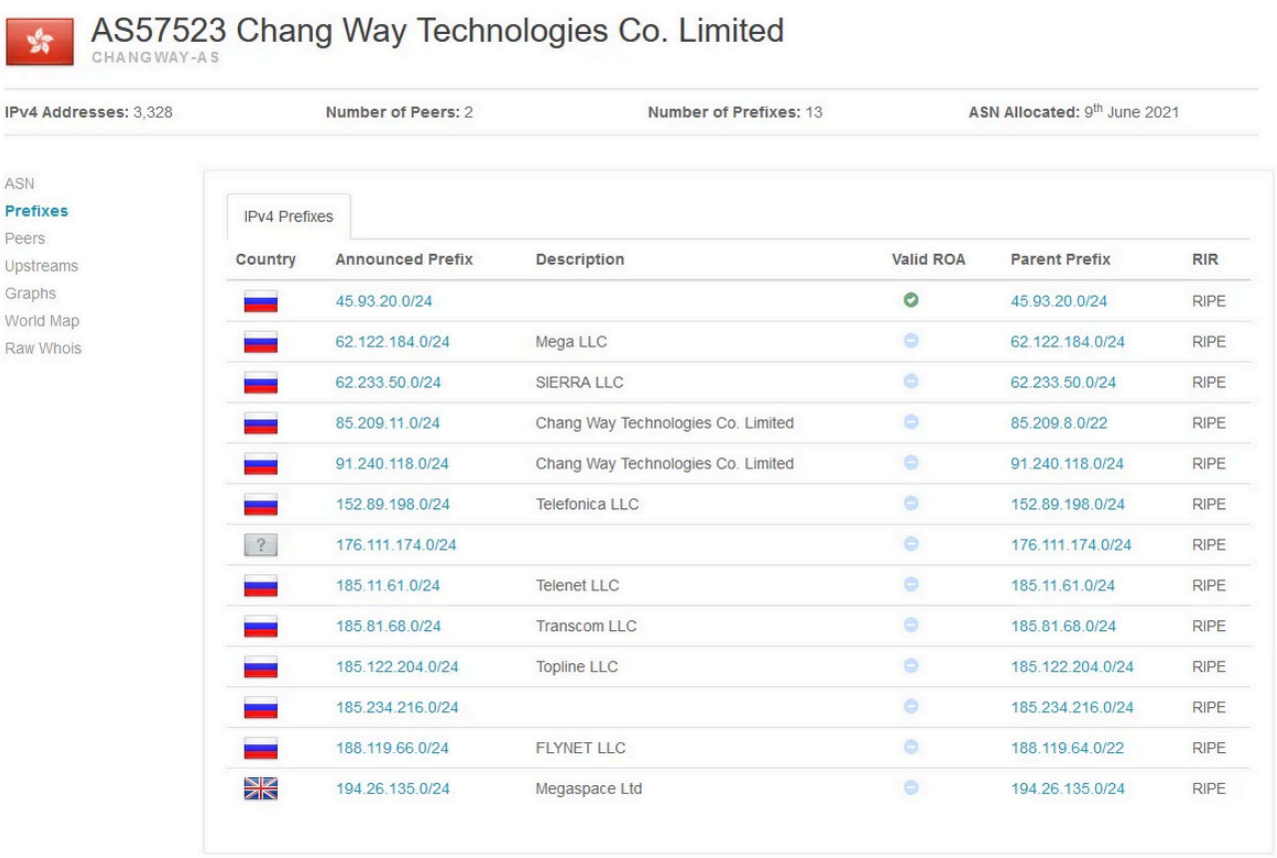
Qilin also specified a host having reference to Kyrgyzstan, according to GEO2IP providers and a UAE-based company.

ftp://dataShare:nX4aJxu3rYUMiLjCMtuJYTKS[@]85.209.11.49

IP Address	85.209.11.49
Country	Kyrgyzstan [KG]
Region	-
City	-
Coordinates of City	42.870000, 74.590000 (42°52'12"N 74°35'24"E)
ISP	FreeNet L.L.C-FZ
Local Time	04 Apr, 2025 07:04 AM (UTC +06:00)
Domain	freenetworks.net
Net Speed	(T1) Data Center/Transit
IDD & Area Code	(996) -
ZIP Code	-
Weather Station	Bishkek (KGXX0001)

Notably, a new legal entity which appeared at the same address in Hong Kong as Chang Way Technologies (Room 1405, 135 Bonham Strand Trade Centre, 135 Bonham Strand, Sheung Wan, Hong Kong), is Next Limited. According to independent reporting, the company was managed by Fedor Berg (a Kyrgyzstani national). This entity was linked to malicious activity tied to Proton66 operator detailed by other cybersecurity experts.

In fact, some time ago exactly the same IP address was tied to Chang Way Technologies Co. Limited, and likely the operator behind this address has changed the description or purchased an autonomous network (AS) from a previous owner. It is common for BPH operators to use confusing network descriptions to complicate further investigation of the exact organization or individual managing those networks.



IPX-FZCO is another operator likely misused by bulletproofhosting tied to**Qilin** Ransomware. This organization is known for leasing their networks to other companies, this is why some of their hosts have been previous has previously been the subject of significant abuse linked to suspected threat actors focused on brute-force attack campaigns and mass-scanning, according to 2024 research published by Heimdal Security.

ftp://dataShare:2bTWYKNn7aK7Rqp9mnv3@188.119.66.189

IP Address	188.119.66.189
Country	Russian Federation [RU]
Region	Moskva
City	Moscow
Coordinates of City	55.752260, 37.615470 (55°45'8"N 37°36'56"E)
ISP	IPX - FZCO
Local Time	04 Apr, 2025 04:08 AM (UTC +03:00)
Domain	iplir.com
Net Speed	(T1) Data Center/Transit
IDD & Area Code	(7) 0495
ZIP Code	101990
Weather Station	Moscow (RSXX0063)

Resecurity was able to confirm the interconnection between IPX-FZCO and Chang Way based on historical records of autonomous networks, for e.g. AS57523:

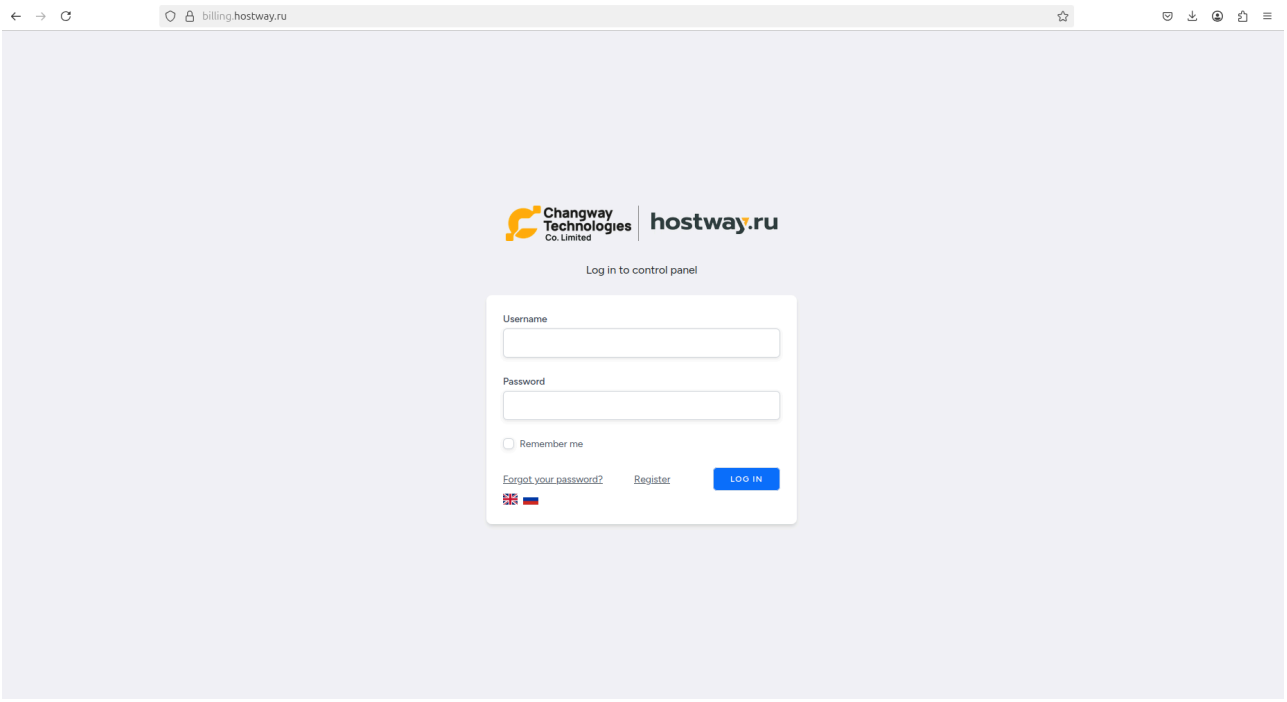
```
netname: HK-CHANGWAY-20220125
country: RU
org: ORG-CWTC1-RIPE
admin-c: LD6315-RIPE
tech-c: LD6315-RIPE
status: ALLOCATED PA
mnt-by: lir-hk-changway-1-MNT
mnt-by: RIPE-NCC-HM-MNT
created: 2024-10-03T14:58:24Z
last-modified: 2024-10-03T14:58:24Z
source: RIPE
role: CHANG WAY
address: HONG KONG
address: HK
address: 7/F, MW Tower, 111 Bonham Strand
phone: +357 2 2008059
e-mail: admin@changway.hk
nic-hdl: LD6315-RIPE
mnt-by: lir-hk-changway-1-MNT
```

Interestingly, several companies linked to U.S. sanctions bypass have been registered at exactly the same address as Chang Way's in Hong Kong, including Piraclinos Limited, which has was flagged in a 2024 report published by the Committee for Freedom in Hong Kong Foundation for exporting dual-use semiconductor technology to a blacklisted Russian company.

Piraclinos claimed to be a fertilizer and charcoal seller, while shipping millions of dollars' worth of electronic integrated circuits to the sanctioned Russian company VMK, masking its true beneficial owners through frequent changes in directors and owners from corporate services firms in Cyprus and Central Asia.

According to The Guardian, Hong Kong has become a global trade hub for "the world's most brutal regimes," citing the foundation's report examining the territory's role in facilitating the flow of goods to countries under sanctions by the West, including Russia, Iran, and North Korea.

According to AbuseIPDB, the IP address 85.209.11.79 has been reported over 11,346 times as malicious and having multiple indicators of attacks including exploit probing and network scanning. Interestingly, the billing login page of Russia-based hosting operator Hostway.ru has a reference to the logo of the same Hong Kong-based company (Changway):



Resecurity also identified a dedicated billing page tied to the domain of **Chang Way Technologies Co. Limited** offering virtual servers and dedicated servers. It remains unclear whether this entity operated as a shell company to acquire servers from Hostway.ru, or if it was simply an affiliate misusing the provider's services. It remains uncertain whether the company is aware of this activity, or if it simply lacks effective abuse management protocols, given the extent of malicious actions observed.

The WHOIS records of the domain name of this suspicious Hong Kong company state "Victor Zaycev" (fake identity) as the owner with email "bernard.webmal@gmail.com":

```
Domain Name:  CHANGWAY.HK
Domain Status: Active
DNSSEC:  unsigned
Contract Version:   Refer to registrar
Active variants
Inactive variants
Registrar Name: NICENIC INTERNATIONAL GROUP CO., LTD
Registrar Contact Information: Email Address: abuse@nicenic.net   Phone No.:
(852) 6858 1006
Reseller:
Registrant Contact Information:
Holder English Name (It should be the same as your legal name on your HKID card
or other relevant documents):  ZAYCEV VICTOR
Holder Chinese Name:
Email:  bernard.webmail@gmail.com
Domain Name Commencement Date: 07-05-2021
Country: Russian Federation (RU)
Expiry Date:  07-05-2027
Re-registration Status:  Complete
Account Name:  HK9567240T
Technical Contact Information:
Given Name:  ZAYCEV
Family name:  VICTOR
Company Name:  ZAYCEV VICTOR
Name Servers Information:
NS1.ENTRYDNS.NET
NS2.ENTRYDNS.NET
```

```
NS3.ENTRYDNS.NET
NS4.ENTRYDNS.NET
```

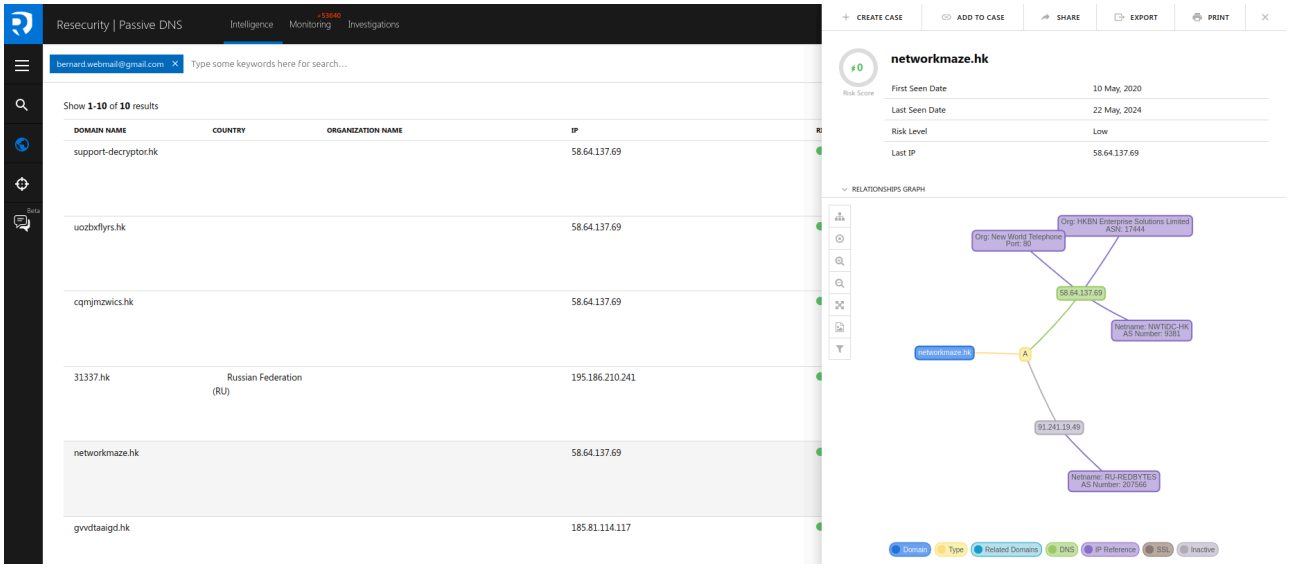
The email "bernard.webmail@gmail.com" was used for several domain registrations, including "networkmaze.hk". The name of the domain is likely derived from **Maze** ransomware, a group active from 2019 to 2020, and which gained notoriety for their attack on technology services giant Cognizant.

The **Maze** ransomware gang was the first major threat group to widely employ double extortion, where threat actors both encrypt and steal victim data. In 2020, Maze formed a temporary alliance with other ransomware groups like **LockBit**, a collaboration that further popularized double extortion tactics. The **Maze** "cartel" is the historical precedent for the new 2025 alliance that includes **DragonForce**, **Qilin,** and **LockBit**. While **Maze** shut down in 2020, its methods and collaboration model continue to influence the modern ransomware ecosystem.

```
Domain Name: NETWORKMAZE.HK
Domain Status: Active
Dnssec: unsigned
Contract Version: Refer to registrar
Registrar Name: NICENIC INTERNATIONAL GROUP CO., LTD
Registrar Contact Information: Email Address: support@nicenic.net Phone No.:
(852) 6858 1005
Registrant Contact Information Company English Name (it Should Be The Same As
The Registered/corporation Name On Your Business Register Certificate Or
Relevant Documents): HOSTWAY LLC
Registrant Contact Information Address: MAIN STREET 10 140000
Registrant Contact Information Country: Russian Federation (RU)
Registrant Contact Information Email: bernard.webmail@gmail.com
Domain Name Commencement Date: 08-02-2020
Expiration Date: 08-02-2021
Re-registration Status: Complete
Administrative Contact Information Given Name: ZAYCEV
Administrative Contact Information Family Name: VICTOR
Administrative Contact Information Company Name: HOSTWAY LLC
Administrative Contact Information Address: MAIN STREET 10 140000
Administrative Contact Information Country: Russian Federation (RU)
Administrative Contact Information Phone: +7-9818060012
Administrative Contact Information Fax: +7-9818060012
Administrative Contact Information Email: bernard.webmail@gmail.com
Administrative Contact Information Account Name: HK9282475T
Technical Contact Information Given Name: ZAYCEV
Technical Contact Information Family Name: VICTOR
Technical Contact Information Company Name: HOSTWAY LLC
```

```
Technical Contact Information Address: MAIN STREET 10 140000
Technical Contact Information Country: Russian Federation (RU)
Technical Contact Information Phone: +7-9818060012
Technical Contact Information Fax: +7-9818060012
Technical Contact Information Email: bernard.webmail@gmail.com
Name Servers Information: OWEN.NS.CLOUDFLARE.COM
Name Servers Information: RUTH.NS.CLOUDFLARE.COM
```

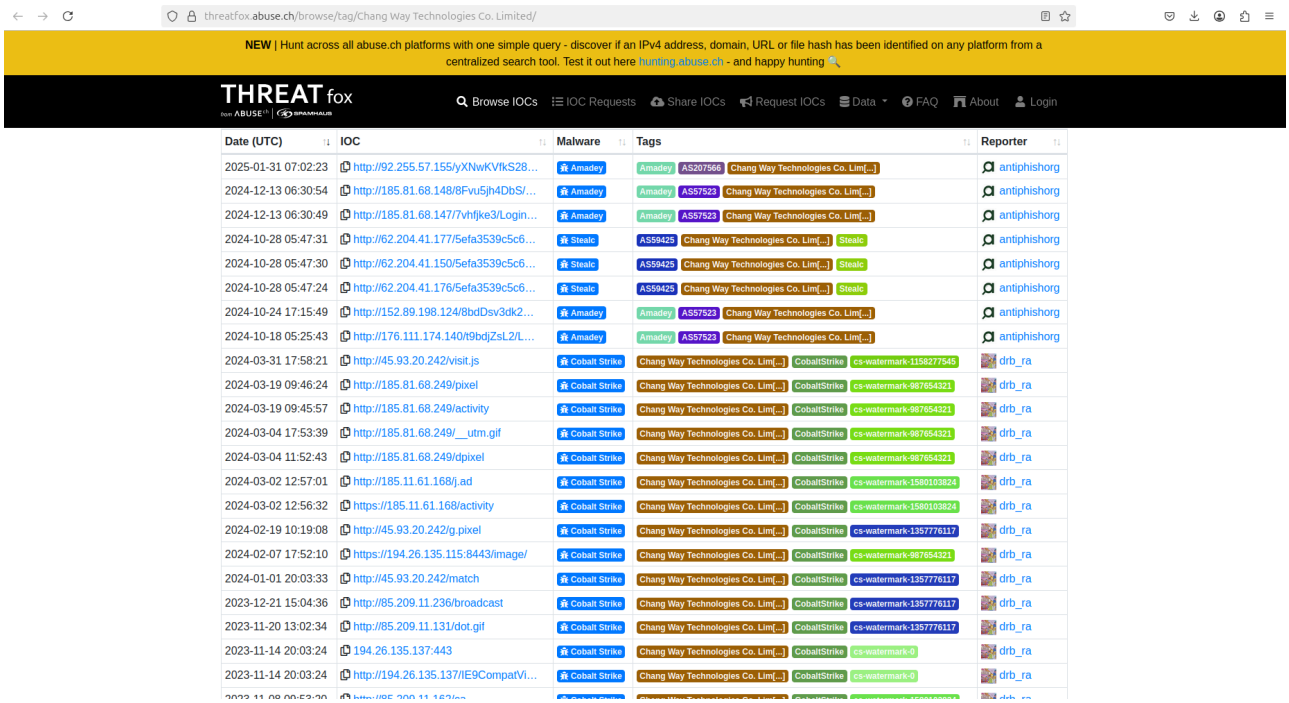
The email is tied to 10 domain names, including "support-decryptor.hk":



The identified domains later updated the email to **88db011bbcb06078s@gmail[.]com** and were using it for renewals.

C2C Heaven - Hosting Malware for Fun and Profit

Chang Way Technologies Co. Limited is associated with extensive malware activity, hosting command-and-control (C2C) servers of **Amadey**, **StealC**, **CobalStrike**, and other tools used by cybercriminals.

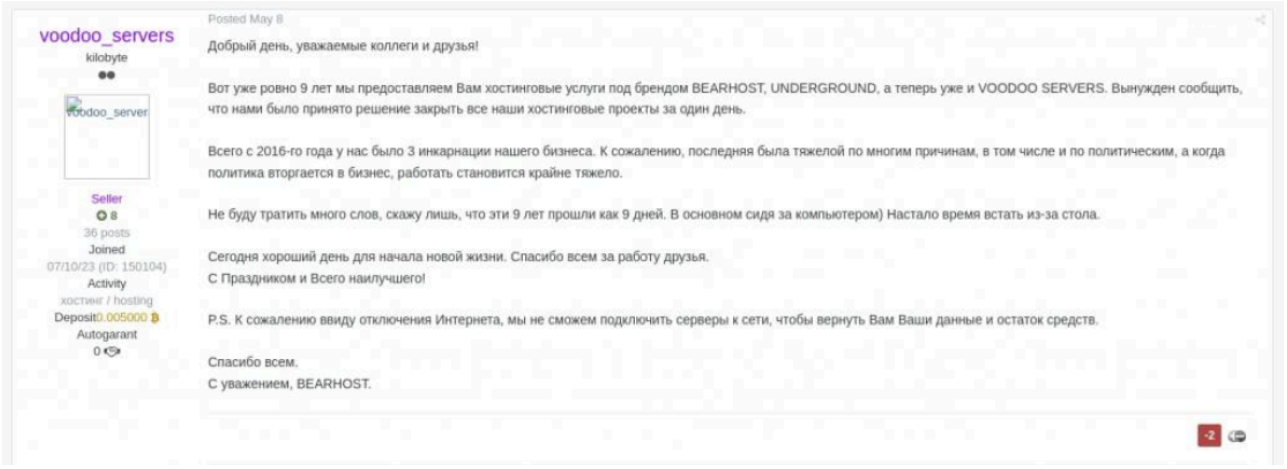


Date (UTC)	IOC	Malware	Tags	Reporter
2025-01-31 07:02:23	http://92.255.57.155/yXNwKVfkS28...	Amadey	Amadey AS207566 Chang Way Technologies Co. Lim[...]	antiphishorg
2024-12-13 06:30:54	http://185.81.68.148/8Fvu5jh4DbS/...	Amadey	Amadey AS57523 Chang Way Technologies Co. Lim[...]	antiphishorg
2024-12-13 06:30:49	http://185.81.68.147/7vhfjke3/Login...	Amadey	Amadey AS57523 Chang Way Technologies Co. Lim[...]	antiphishorg
2024-10-28 05:47:31	http://62.204.41.177/5efa3539c5c6...	Stealc	AS59425 Chang Way Technologies Co. Lim[...] Stealc	antiphishorg
2024-10-28 05:47:30	http://62.204.41.150/5efa3539c5c6...	Stealc	AS59425 Chang Way Technologies Co. Lim[...] Stealc	antiphishorg
2024-10-28 05:47:24	http://62.204.41.176/5efa3539c5c6...	Stealc	AS59425 Chang Way Technologies Co. Lim[...] Stealc	antiphishorg
2024-10-24 17:15:49	http://152.89.198.124/8bdDsv3dk2...	Amadey	Amadey AS57523 Chang Way Technologies Co. Lim[...]	antiphishorg
2024-10-18 05:25:43	http://176.111.174.140/t9bdjZsL2/L...	Amadey	Amadey AS57523 Chang Way Technologies Co. Lim[...]	antiphishorg
2024-03-31 17:58:21	http://45.93.20.242/visit.js	Cobalt Strike	Chang Way Technologies Co. Lim[...] CobaltStrike cs-watermark-1158277545	drb_ra
2024-03-19 09:46:24	http://185.81.68.249/pixel	Cobalt Strike	Chang Way Technologies Co. Lim[...] CobaltStrike cs-watermark-987654321	drb_ra
2024-03-19 09:45:57	http://185.81.68.249/activity	Cobalt Strike	Chang Way Technologies Co. Lim[...] CobaltStrike cs-watermark-987654321	drb_ra
2024-03-04 17:53:39	http://185.81.68.249/__utm.gif	Cobalt Strike	Chang Way Technologies Co. Lim[...] CobaltStrike cs-watermark-987654321	drb_ra
2024-03-04 11:52:43	http://185.81.68.249/dpixel	Cobalt Strike	Chang Way Technologies Co. Lim[...] CobaltStrike cs-watermark-987654321	drb_ra
2024-03-02 12:57:01	http://185.11.61.168/j.ad	Cobalt Strike	Chang Way Technologies Co. Lim[...] CobaltStrike cs-watermark-1580103824	drb_ra
2024-03-02 12:56:32	https://185.11.61.168/activity	Cobalt Strike	Chang Way Technologies Co. Lim[...] CobaltStrike cs-watermark-1580103824	drb_ra
2024-02-19 10:19:08	http://45.93.20.242/g.pixel	Cobalt Strike	Chang Way Technologies Co. Lim[...] CobaltStrike cs-watermark-1357776117	drb_ra
2024-02-07 17:52:10	https://194.26.135.115:8443/image/	Cobalt Strike	Chang Way Technologies Co. Lim[...] CobaltStrike cs-watermark-987654321	drb_ra
2024-01-01 20:03:33	http://45.93.20.242/match	Cobalt Strike	Chang Way Technologies Co. Lim[...] CobaltStrike cs-watermark-1357776117	drb_ra
2023-12-21 15:04:36	http://85.209.11.236/broadcast	Cobalt Strike	Chang Way Technologies Co. Lim[...] CobaltStrike cs-watermark-1357776117	drb_ra
2023-11-20 13:02:34	http://85.209.11.131/dot.gif	Cobalt Strike	Chang Way Technologies Co. Lim[...] CobaltStrike cs-watermark-1357776117	drb_ra
2023-11-14 20:03:24	194.26.135.137:443	Cobalt Strike	Chang Way Technologies Co. Lim[...] CobaltStrike cs-watermark-0	drb_ra
2023-11-14 20:03:24	http://194.26.135.137/IE9CompatVi...	Cobalt Strike	Chang Way Technologies Co. Lim[...] CobaltStrike cs-watermark-0	drb_ra

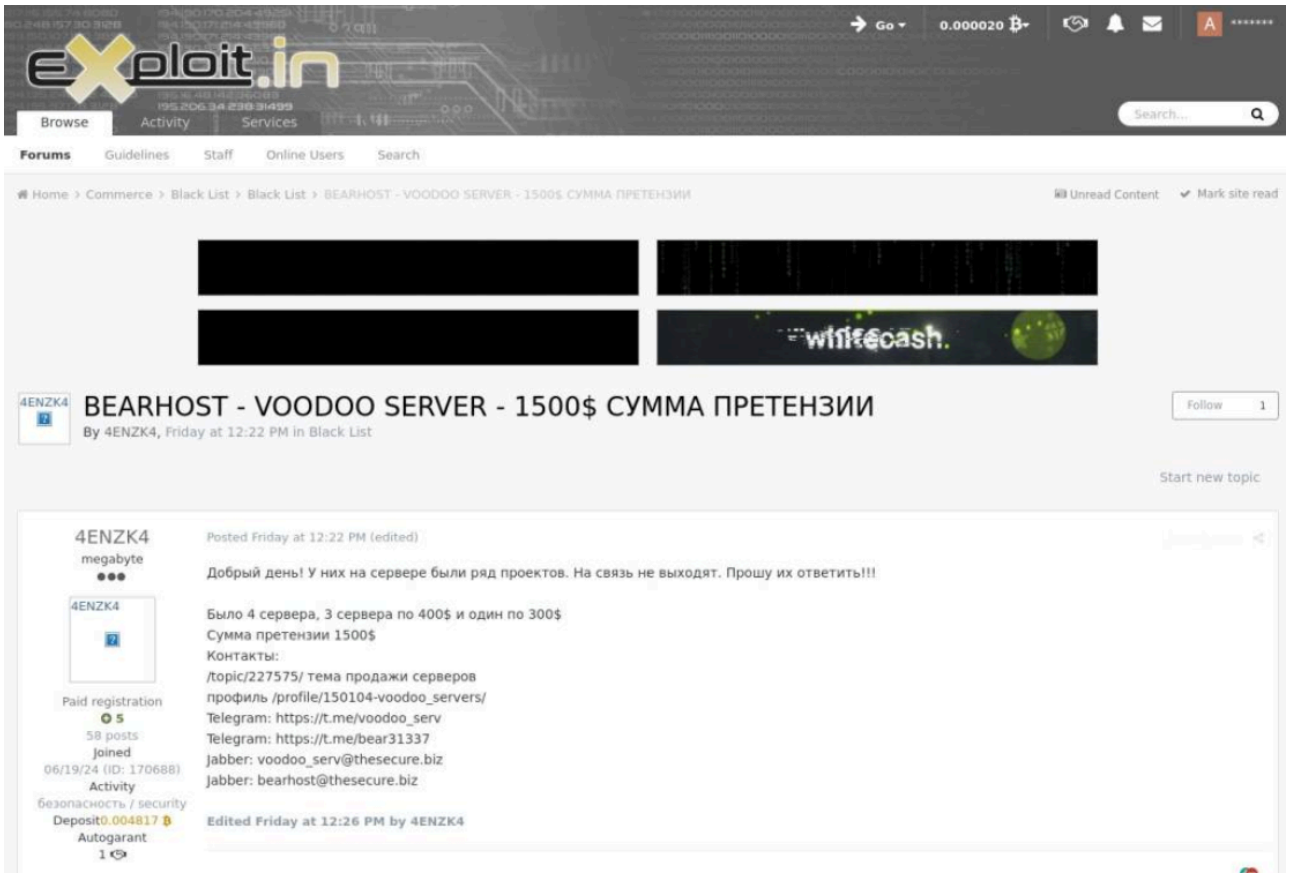
It is unlikely that the individuals behind this hosting "conglomerate" are unaware of this activity, given the numerous abuse reports submitted by other telecom operators, cybersecurity companies, and victims.

Cutting Loose Ends

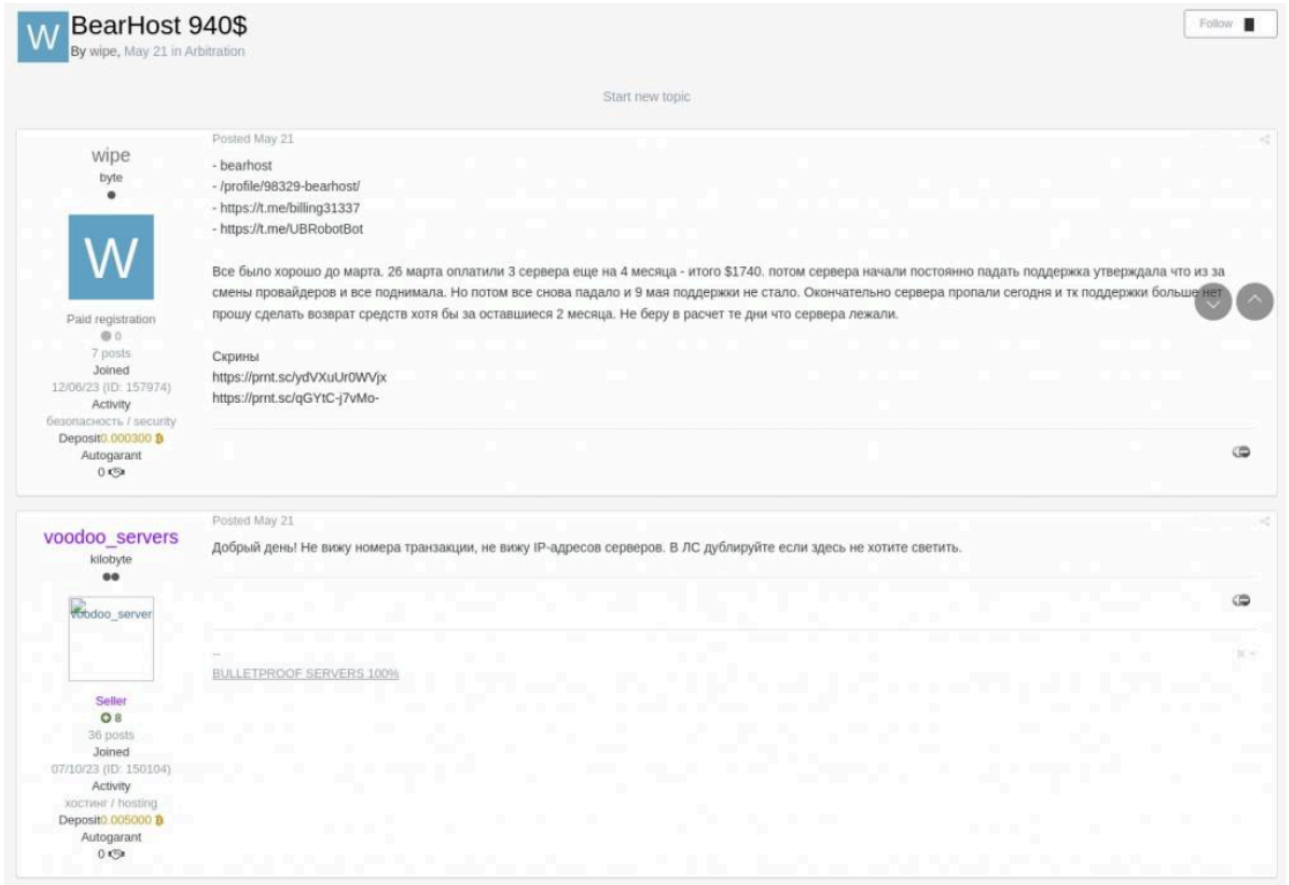
In May 2025 BearHost rebranded as "**voodoo_servers**" following some complaints on their service published on Exploit[.]in.



Complaint 1:


Exploit.in
Browse
Activity
Services
Forums
Guidelines
Staff
Online Users
Search
Home > Commerce > Black List > Black List > BEARHOST - VOODOO SERVER - 1500$ СУММА ПРЕТЕНЗИИ
Unread Content
Mark site read
4ENZK4
BEARHOST - VOODOO SERVER - 1500$ СУММА ПРЕТЕНЗИИ
By 4ENZK4, Friday at 12:22 PM in Black List
Follow 1
Start new topic
4ENZK4
megabyte
Posted Friday at 12:22 PM (edited)
Добрый день! У них на сервере были ряд проектов. На связь не выходят. Прошу их ответить!!!
Было 4 сервера, 3 сервера по 400$ и один по 300$
Сумма претензии 1500$
Контакты:
/topic/227575/ тема продажи серверов
профиль /profile/150104-voodoo_servers/
Telegram: https://t.me/voodoo_serv
Telegram: https://t.me/bear31337
Jabber: voodoo_serv@thesecure.biz
Jabber: bearhost@thesecure.biz
Edited Friday at 12:26 PM by 4ENZK4
Paid registration
5
58 posts
Joined
06/19/24 (ID: 170688)
Activity
безопасность / security
Deposit0.004817 ₿
Autogarant
1

Complaint 2:


BearHost 940$
By wipe, May 21 in Arbitration
Follow
Start new topic
wipe
byte
Posted May 21
- bearhost
- /profile/98329-bearhost/
- https://t.me/billing31337
- https://t.me/UBRobotBot
Все было хорошо до марта. 26 марта оплатили 3 сервера еще на 4 месяца - итого $1740. потом сервера начали постоянно падать поддержка утверждала что из за смены провайдеров и все поднимала. Но потом все снова падало и 9 мая поддержки не стало. Окончательно сервера пропали сегодня и тк поддержки больше нет прошу сделать возврат средств хотя бы за оставшиеся 2 месяца. Не беру в расчет те дни что сервера лежали.
Скрины
https://prnt.sc/ydVXuUr0WVjx
https://prnt.sc/qGYtC-j7vMo-
Paid registration
0
7 posts
Joined
12/06/23 (ID: 157974)
Activity
безопасность / security
Deposit0.000300 ₿
Autogarant
0
voodoo_servers
kilobyte
Posted May 21
Добрый день! Не вижу номера транзакции, не вижу IP-адресов серверов. В ЛС дублируйте если здесь не хотите светить.
BULLETPROOF SERVERS 100%
Seller
8
36 posts
Joined
07/10/23 (ID: 150104)
Activity
хостинг / hosting
Deposit0.005000 ₿
Autogarant
0

The actors announced the termination of their bulletproof hosting services under the brands Bearhost, Underground, and Voodoo_Servers due to unnamed reasons. According to their statement published on the Dark Web, the service has been operating since 2016 and was "reborn" three times, but they have to close it due to "political reasons." Interestingly, they mentioned that "when politics gets into business - it becomes difficult to work." They also added that they will not have the opportunity to re-enable servers or return funds to their customers. The actors decided to disappear through an "exit scam" scenario, keeping the underground audience completely clueless. Notably, the legal entities behind the service continue their operations.

How soon will we hear their new brand on the Dark Web? Only time will tell. These events occurred in very close proximity to major incidents like Asahi in Japan, when Qilin was at the peak of their activities. Likely, the actors are regrouping and improving their OPSEC - moving towards much bigger targets.

Following Bearhost's exit scam, it is highly probable that the malicious activities previously conducted within their networks will shift towards Prospero (AS200593) and Proton66 (AS198953) operators, as well as the Hong Kong-based entities, **Next Limited** and/or **Address Limited** using the same address in Hong Kong.

Significance

BPH services are a significant concern in the cybersecurity industry due to their role in the enablement of professional cybercrime and, specifically, the way they shield the real-world identities of threat actors from discovery. BPH providers allow their clients to host content with minimal or no oversight in addition to non-existent identity verification. These providers turn a blind eye to the nature of the hosted content, even if it is illegal or harmful.

Furthermore, BPH providers are designed to be resilient to complaints and law enforcement interventions. They often operate through a network of unresponsive and geographically dispersed shell companies, making it difficult for law enforcement to trace or shut them down. The resilience enabled by global regulatory arbitrage, which threat actors exploit through the formation of myriad and interconnected legal entities scattered across pro-secrecy jurisdictions, allows cybercriminals to keep their operations running for prolonged periods of time.

BPH services are frequently used to host content and infrastructure for illegal activities, including:

- Phishing sites: These are used to steal sensitive information like login credentials and financial data.
- Malware distribution: Cybercriminals use BPH to host and distribute malware, which can infect systems and steal data.
- Botnet command-and-control servers: These servers are critical for managing botnets, which are networks of compromised devices used for cyberattacks like DDoS.
- Spam and misinformation: BPH providers often host spam distribution sites and platforms for spreading misinformation.
- Child Sexual Abuse Material (CSAM): See Freedom Hosting

The covert nature of BPH services makes it challenging for cybersecurity researchers and law enforcement agencies to identify their operators and dismantle their infrastructure. This complicates efforts to combat cybercrime and protect users from online threats

Conclusion

BPH services pose a significant threat because they provide anonymous and unregulated platforms for cybercriminals and other bad actors. Their resilience to legal actions and their role in facilitating a wide range of illegal activities make them a critical challenge for global cybersecurity efforts. Addressing this issue requires coordinated action from governments, law enforcement, the banking industry, and cybersecurity professionals.

The interconnection with ransomware groups like Qilin confirms the organized nature of this activity, which is characteristic of modern cybercrime groups that operate for profit and exploit jurisdictional challenges to conceal their activities.

Notably, all of the above-mentioned legal entities associated with the activity described in this publication **continue their operations** as of today (October 15, 2025).

Reference

This research would not be possible without the contributions and insights shared by other independent cybersecurity researchers and organizations. The intelligence shared by them has significantly increased visibility into Qilin operations and the associated bulletproof hosting providers:

Qilin, aka Agenda Ransomware - Threat Profile (TLP:CLEAR)
https://www.hhs.gov/sites/default/files/qilin-threat-profile-tlpclear.pdf

HostingHunter Series: CHANG WAY TECHNOLOGIES CO. LIMITED (by Joshua Penny)
https://medium.com/@joshuapenny88/hostinghunter-series-chang-way-technologies-co-limited-a9ba4fce0f6...

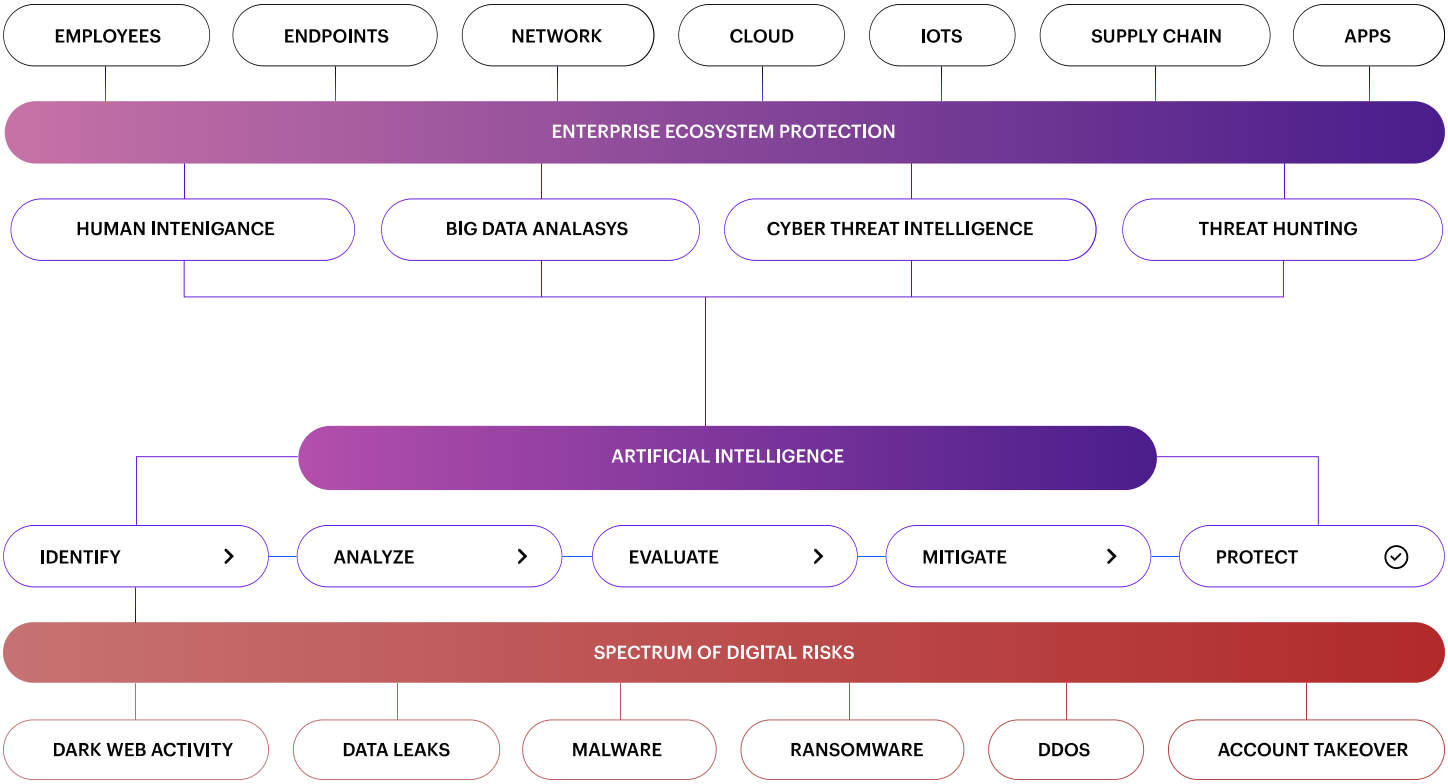
Bearhost Bolts — But the Investigation Is Just Beginning
https://decodecybercrime.com/bearhost-bolts-but-the-investigation-is-just-beginning/

Proton66: Mass Scanning and Exploit Campaigns
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/proton66-part-1-mass-scanning-and-ex...

Ces mystérieuses entreprises qui se font attribuer des blocs IPv4
https://www.lemagit.fr/actualites/252496421/Ces-mysterieuses-entreprises-qui-se-font-attribuer-des-b...

By subscribing, I understand and agree that my personal data will be collected and processed according to the Privacy and Cookies Policy

Cloud Architecture



Resecurity

contact@resecurity.com

(+1) 888 273 82 76

445 S. Figueroa Street
Los Angeles, CA 90071
↳ Google Maps

Contact us by filling out the form

Try Resecurity products today with a free trial

Hi there! I'm here to answer your questions and assist you.
Before we begin, could you please provide your name and email?