GLOBAL GROUP: Emerging Ransomware-as-a-Service, supporting AI driven negotiation and mobile control panel for their affiliates

Archived: 2026-04-05 19:25:40 UTC

Executive summary

On June 2, 2025, EclecticIQ analysts observed the emergence of GLOBAL GROUP, a new Ransomware-as-a-Service (RaaS) brand promoted on the Ramp4u forum by the threat actor known as “$$$”. The same actor controls the Black Lock RaaS [1] and previously managed Mamona [2] ransomware operations. GLOBAL GROUP targets a wide range of sectors across the United States and Europe.

EclecticIQ assesses with medium confidence that GLOBAL GROUP was likely established as a rebranding of the BlackLock RaaS operation. This rebranding aims to rebuild trust and expand the affiliate network by giving 80% of extorted ransom money to affiliates.

GLOBAL GROUP operates a dedicated leak site (DLS) on the Tor network. EclecticIQ analysts traced the real IP address of the DLS to a Russia-based Virtual Private Server (VPS) provider service called IpServer. Same VPS provider was previously used by Mamona RaaS gang. The site already lists confirmed victims, including healthcare providers in the United States and Australia, and an automotive services firm in the United Kingdom.

GLOBAL GROUP heavily relies on Initial Access Brokers (IABs) to acquire access to vulnerable edge appliances. These include Fortinet, Palo Alto, and Cisco devices. The group also uses brute-force tools for Microsoft Outlook and RDWeb portals. These enable high-privilege initial access and rapid ransomware deployment, often bypassing traditional EDR solutions.

Analysts also observed that GLOBAL GROUP’s ransom negotiation panel features an automated system powered by AI-driven chatbots. This enables non-English-speaking affiliates to engage victims more effectively. The AI-driven negotiation functionality increases psychological pressure during negotiations and facilitates seven-figure ransom demands for decryption keys.

GLOBAL GROUP ransomware emerges with nine victims in five days

On June 2, 2025, EclecticIQ analysts observed the emergence of a new ransomware group called GLOBAL GROUP. The group made its first public appearance in a chatroom of the Ramp4u forum. A Russian-speaking threat actor using the alias "$$$" sent a chat message that contained an onion link to GLOBAL GROUP’s dedicated leak site. The actor accidentally named the group "GLOBALY", a misspelling that indicate threat actor is not a native English speaker.

In the same message, actor “$$$” clarified that GLOBAL GROUP is not yet a fully operational Ransomware-as-a-Service (RaaS). Despite the disclaimer, on June 26, 2025, EclecticIQ analysts observed GLOBAL GROUP announcing that 'GLOBAL RaaS officially released,' indicating the launch of a ransomware-as-a-service (RaaS) offering.

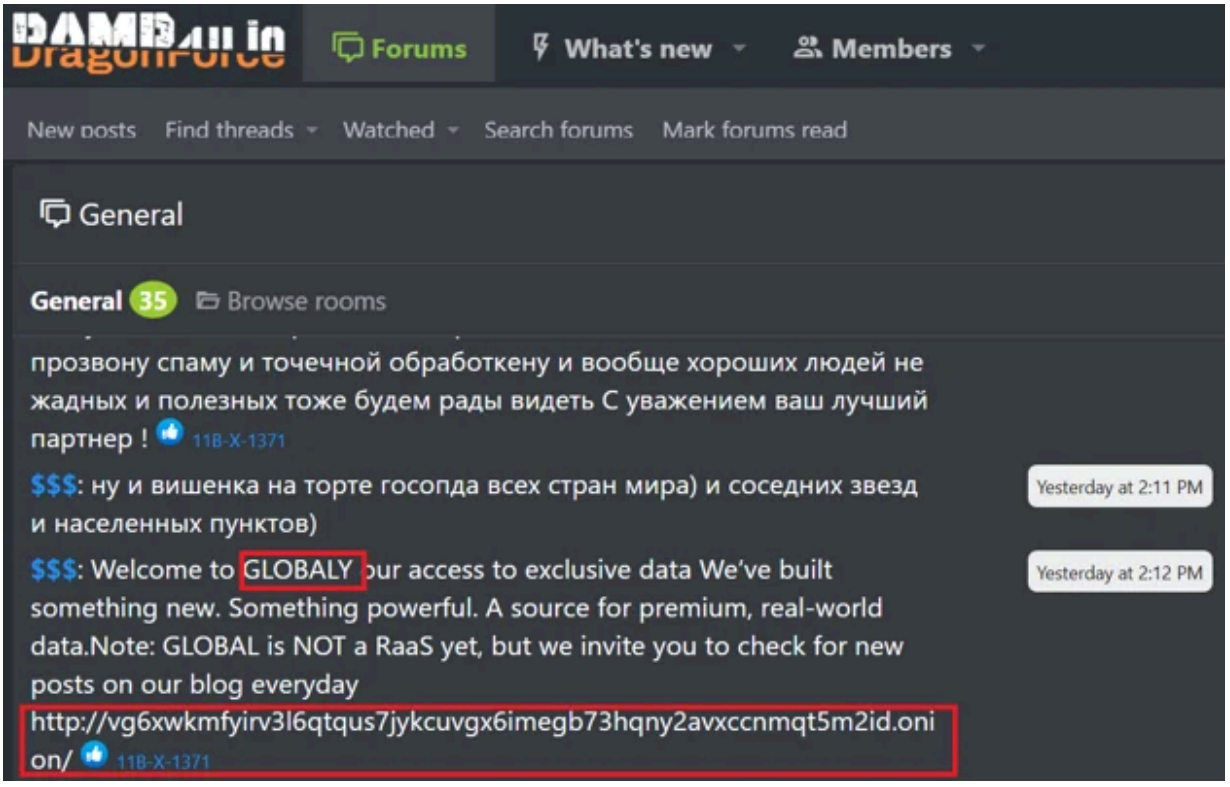

Figure 1 - On Ramp4u forum, threat actor "$$$" shared the DLS in an announcement of GLOBAL GROUP.

GLOBAL GROUP ransomware initially emerged with nine victims in five days. As of July 14, 2025, the group has claimed responsibility for 17 victims across multiple countries and industries. The majority belong to the healthcare sector and are located across regions including:

- Healthcare providers in Australia and the United States
- Oil-and-gas equipment fabrication in Texas, United States
- Industrial machinery and precision engineering in the United Kingdom
- Automotive repair and accident-recovery services in the United Kingdom
- Large-scale business-process outsourcing and facilities-management services in Brazil

All nine organizations were posted between June 2–7, 2025. This demonstrates a broad geographic reach and a diverse range of industry targets across the United States, United Kingdom, Australia, and Brazil.

The DLS is accessible via the below Onion address:

- vg6xwkmfyirv3l6qtqus7jykcuvgx6imegb73hqny2avxccnmqt5m2id[.]onion

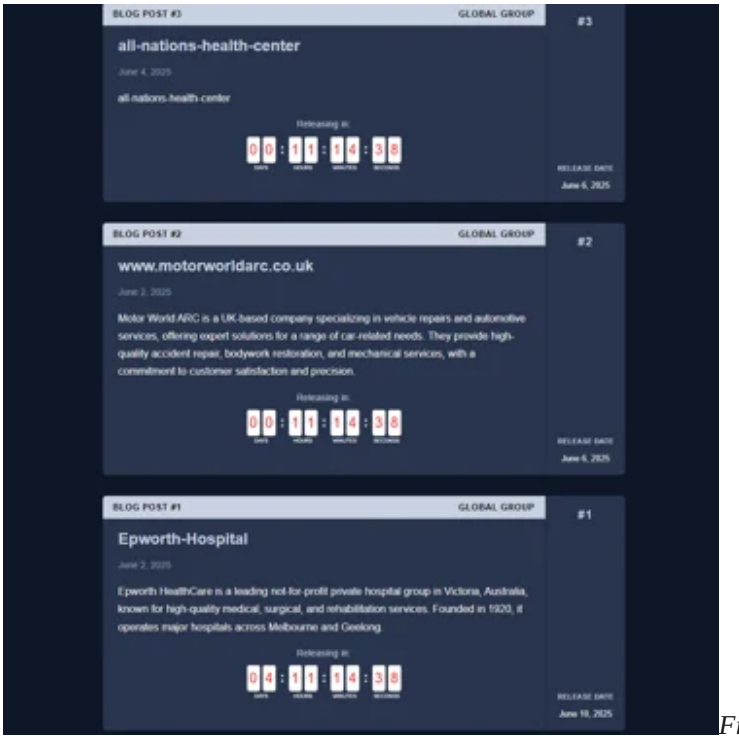

Figure 2 - GLOBAL GROUP DLS hosted on the Tor network.

OPSEC failure and shared malware mutex links GLOBAL GROUP to previous mamona operations

Analysts assess with high confidence that the same actor operating under the persona '$$$' behind GLOBAL GROUP was also responsible for the now-defunct Mamona RIP ransomware operation.

Multiple pieces of technical evidence confirm this connection between the two ransomware operations.

Shared infrastructure evidence

EclecticIQ analysts observed that both operations use the same Russian VPS provider called IpServer. [3] The provider was previously used by threat actor "$$$" to manage Mamona RIP Ransomware at IP address 185.158.113[.]114.

GLOBAL GROUP's current infrastructure uses the same provider at IP address 193.19.119[.]4 under port 3304. This connection was revealed through an operational security (OPSEC) mistake in GLOBAL GROUP's infrastructure. The group attempted to hide their leak site behind a Tor hidden service. However, an exposed API endpoint /posts returned JSON metadata that revealed the real-world hosting environment. Inside the returned JSON field, the sshConnectionName section for each victim entry included IP address 193.19.119[.]4 and a SSH username as dataleak. This leak confirmed that victim data was stored on a misconfigured system, reachable over the internet.

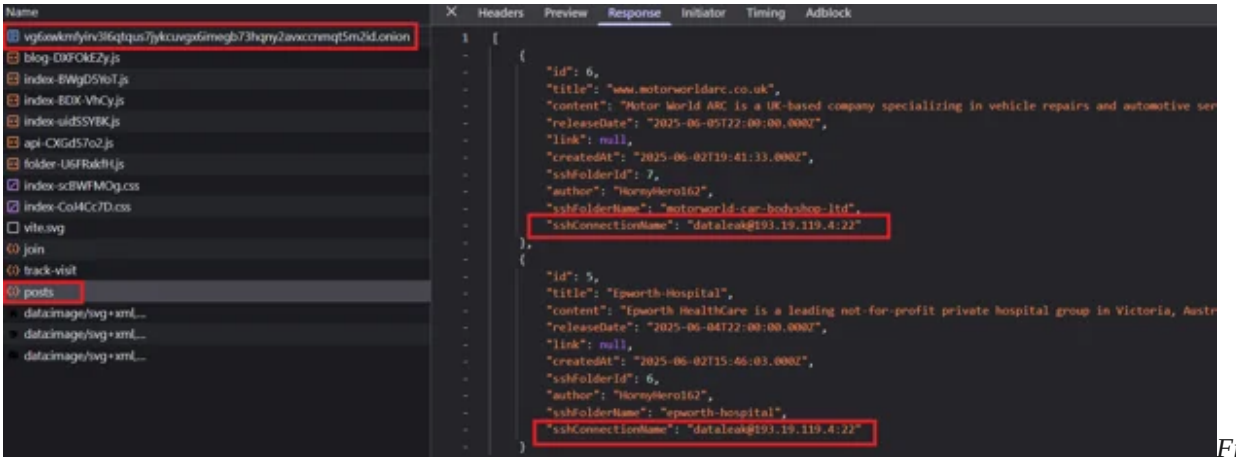

Figure 3 - API leaking the real IP address of the data leak site.

Malware code similarities

Analysis of the GLOBAL ransomware sample confirms the group uses a customized variant of Mamona ransomware. Both malware strains use the identical mutex key Global\Fxo16jmdgujs437. Unlike Mamona Ransomware, GLOBAL includes added functionality for automated domain-wide ransomware installation. It uses SMB connections and malicious Windows service creation for more scalable deployment.

On June 7, 2025, a VirusTotal user uploaded a Golang-compiled variant of the GLOBAL ransomware. The sample is built in the Go programming language and uses the modern encryption routine ChaCha20-Poly1305. The payload leverages Go's ability to run many parallel threads automatically. This allows it to encrypt huge volumes of data in minutes on Windows, Linux, or macOS from one self-contained binary.

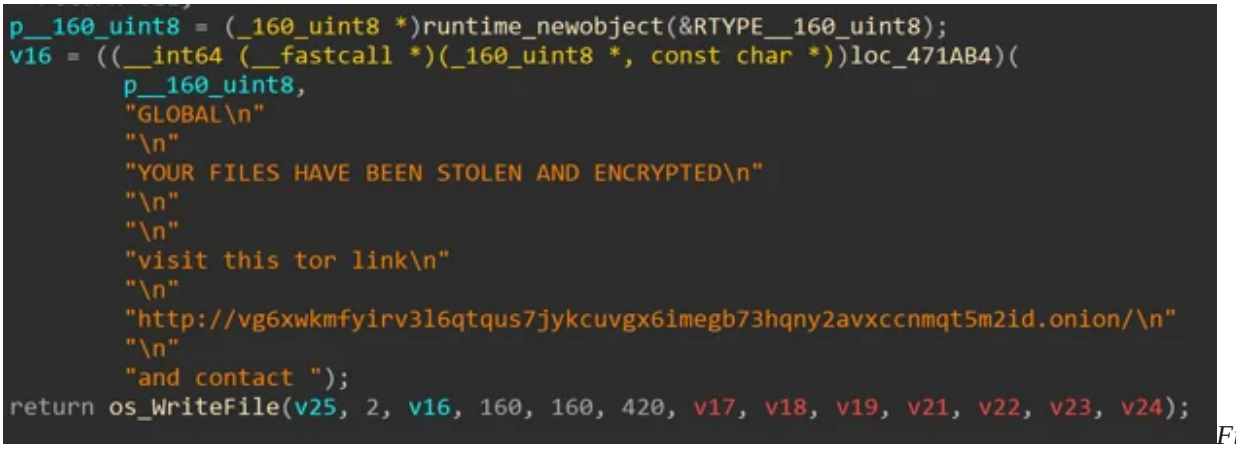

Figure 4 - README message inside the GO Based GLOBAL ransomware sample.

Possible rebranding for Black Lock RaaS

EclecticIQ analysts assess with medium confidence that the threat actor "$$$" is rebranding the Black Lock ransomware (previously known as El Dorado) [5] operation as "GLOBAL GROUP".

EclecticIQ analysts observed that threat actor “$$$” has a scannable QR code in their Ramp4u profile that shows a qTOX [7] ID for encrypted communication. This is linked to the Black Lock Ransomware profile. Ransomware operators commonly use qTOX, an open-source encrypted messaging application, for affiliate management,

cybercriminal communication, and ransom negotiation with victims. The application's decentralized architecture and strong encryption provide operational security advantages.

The qTOX ID of the threat actor “$$$”:

- 667798F921A68529C74094664C1B890D4E1156C4588906071398FA4F76C 2095C2B3AC79FF086

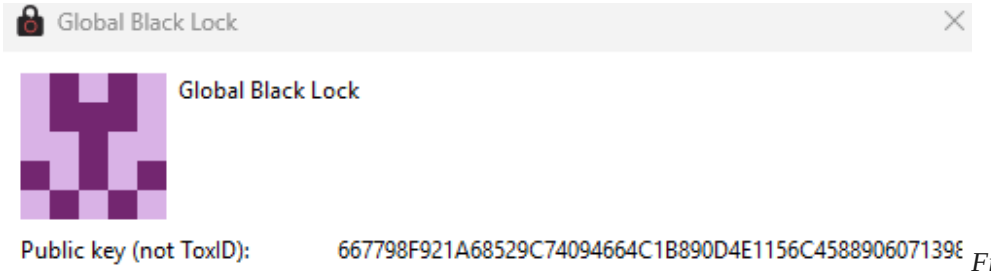

Figure 5 - Black Lock admin changed qTOX account to “Global Black Lock”.

Analysts observed that, on June 6, 2025, “$$$” changed the qTOX display name from "Black Lock" to "Global Black Lock," indicating a shift toward new brand identity as GLOBAL. Black Lock was another RaaS operation that first emerged in January 2025.

Black Lock's reputation suffered significant damage. Researchers from Resecurity exposed the Black Lock dedicated leak site [6] and other cybercriminals posted vulnerability details in the same advertisement thread, that leads to damaging Black Lock's reputation within underground communities.

Black Lock DLS site remains active without corresponding brand changes, suggesting the rebranding effort may be incomplete or actor “$$$” decided to manage two separate RaaS groups at the same time.

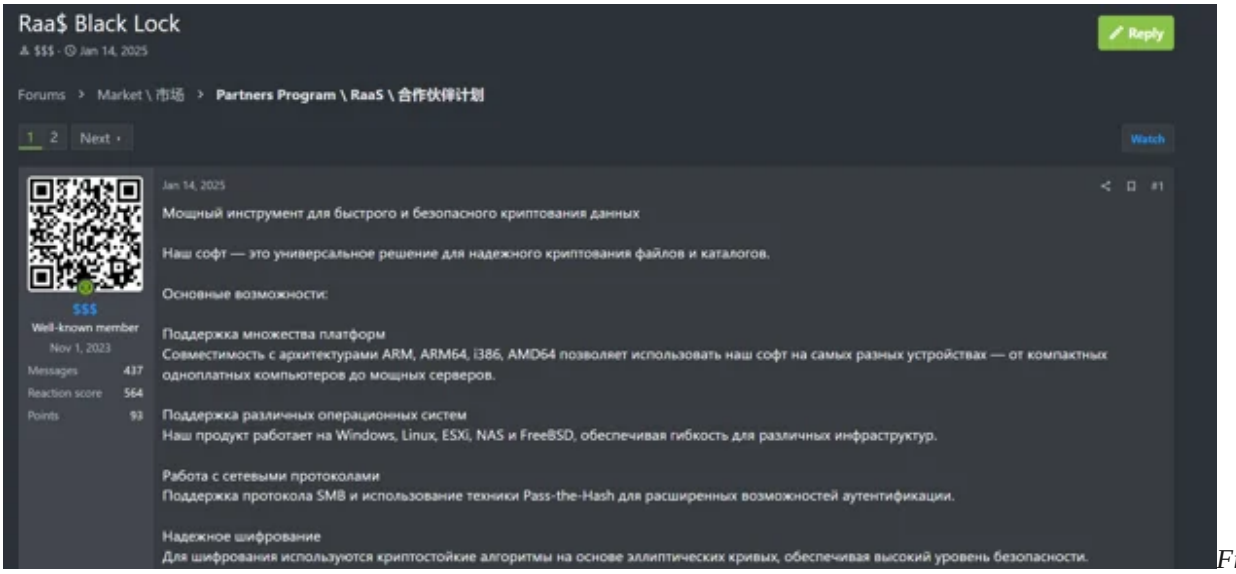

Figure 6 - Threat actor $$$ advertising Black Lock RaaS on Ramp4u.

GLOBAL GROUP markets RaaS platform with 85% revenue share

GLOBAL GROUP hosts a promotional video on their DLS. The video shows a fully featured Ransomware-as-a-Service (RaaS) platform with a negotiation portal and an affiliation panel. Analysts assess with high confidence that

this video is aimed at attracting new affiliates.

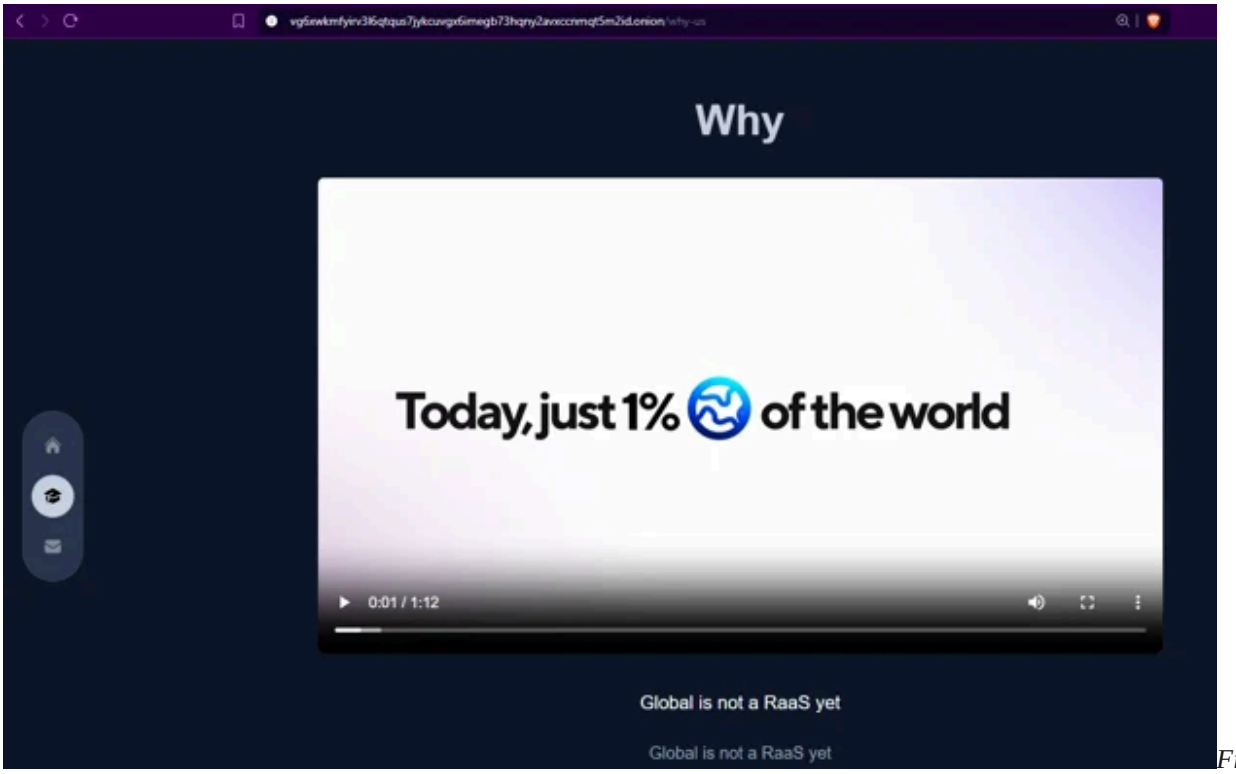

Figure 7 - Video advertisement on the data leak site.

The promotional video showcases an interactive affiliate panel that allows cybercriminals to manage victims, build ransomware payloads, and monitor operations. The interface enables custom configurations such as encryption percentage, file extension naming to replace each encrypted file with a specific extension, and operational flags (e.g., self-delete, log deletion, service termination).

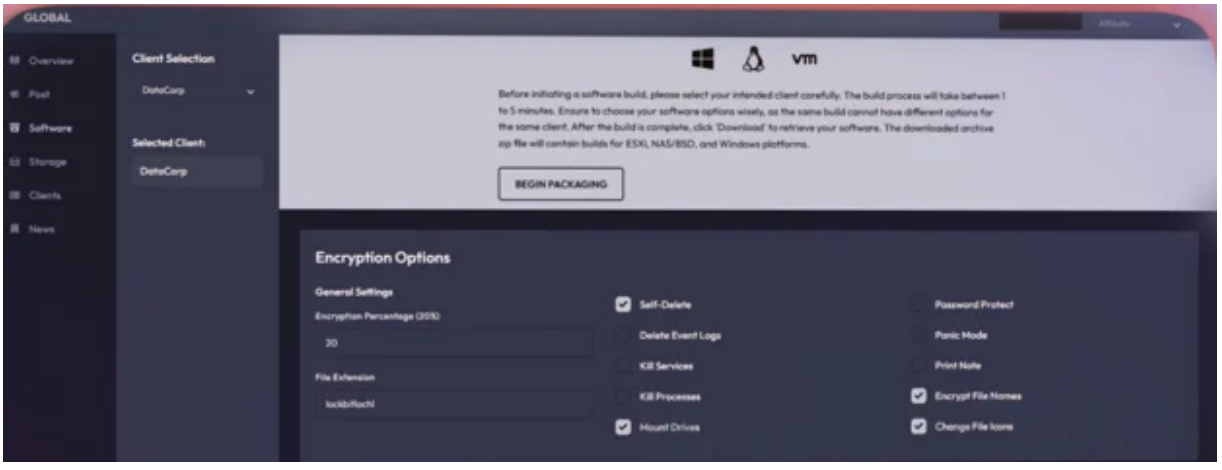

Figure 8 - Affiliate panel from the advertisement video.

The platform claims to support cross-platform ransomware builds such as: ESXi, NAS, BSD, and Windows OS. The affiliate panel is also supporting mobile devices where RaaS members can negotiate ransom payment over their mobile phones. The RaaS brands itself as 'undetectable by EDR' and promotes AI-powered ransom negotiation to improve affiliate workflows.

Figure 9 - Examples of the affiliate panel on mobile devices.

GLOBAL GROUP promises a revenue-sharing model of 85%, positioning itself as a competitor to other RaaS operators. The advertisement video and marketing tone suggest GLOBAL GROUP is trying to attract more affiliates, highlighting their intent to scale ransomware operations.

Figure 10 - 85% revenue share percentage in GLOBAL Raas.

The ransom note from recent intrusions directs victims to initiate negotiations via a dedicated Tor-based portal located at:

- gdbkvfe6g3whrzkdlbytksygk45zwgmnzh5i2xmqyo3mrpipysjagqyd[.]onion

```
GLOBAL

Your network has been encrypted.

All of your important files — documents, databases, backups, and configurations are now inaccessible.
They have been locked using military-grade encryption. Only GLOBAL holds the decryption keys.

What happened?
-------------------------
We have gained full access to your internal network. During this time,
sensitive data was exfiltrated and your systems were encrypted.

Your business operations, internal communications, and customer data are at risk.

What comes next?
-------------------------
To restore access:
1. Download the Tor Browser (https://www.torproject.org/)
2. Visit our secure portal: gdbkvfe6g3whrzkdlbytksygk45zwgmnzh5i2xmqyo3mrpipysjagqyd.onion/chat/cqe81lbjg5wdgrni4ujexu7zr37oypn5
3. Enter your unique ID: K65U9Ar9^%
4. Follow the instructions to begin negotiations.

You may submit one small file (<1MB, non-sensitive) for free decryption as proof we hold the keys.
We will also send you a file-listing to prove to you that we have stolen your data.

Failure to engage within 3 days will result in:
- Public release of your internal documents
- Irreversible loss of your encrypted data
- Escalation of your case to a wider leak network

There is no other way. Do not waste time with third-party tools or law enforcement. You will only make things worse.

This is not personal. Just business.

Data Leak Site - http://vq6xwkmfyirv3l6qtqus7jykcuvqx6imeqb73hqny2avxccnmqt5m2id.onion/

**GLOBAL operates globally.**
```

Figure 11 - GLOBAL ransomware readme file dropped after the encryption.

Victims are instructed to verify the breach by uploading an encrypted file for free decryption. They are warned of public data leaks if negotiations are not initiated within three days. This showcases a mature extortion ecosystem with automated victim onboarding via a custom chat interface on the Tor network.

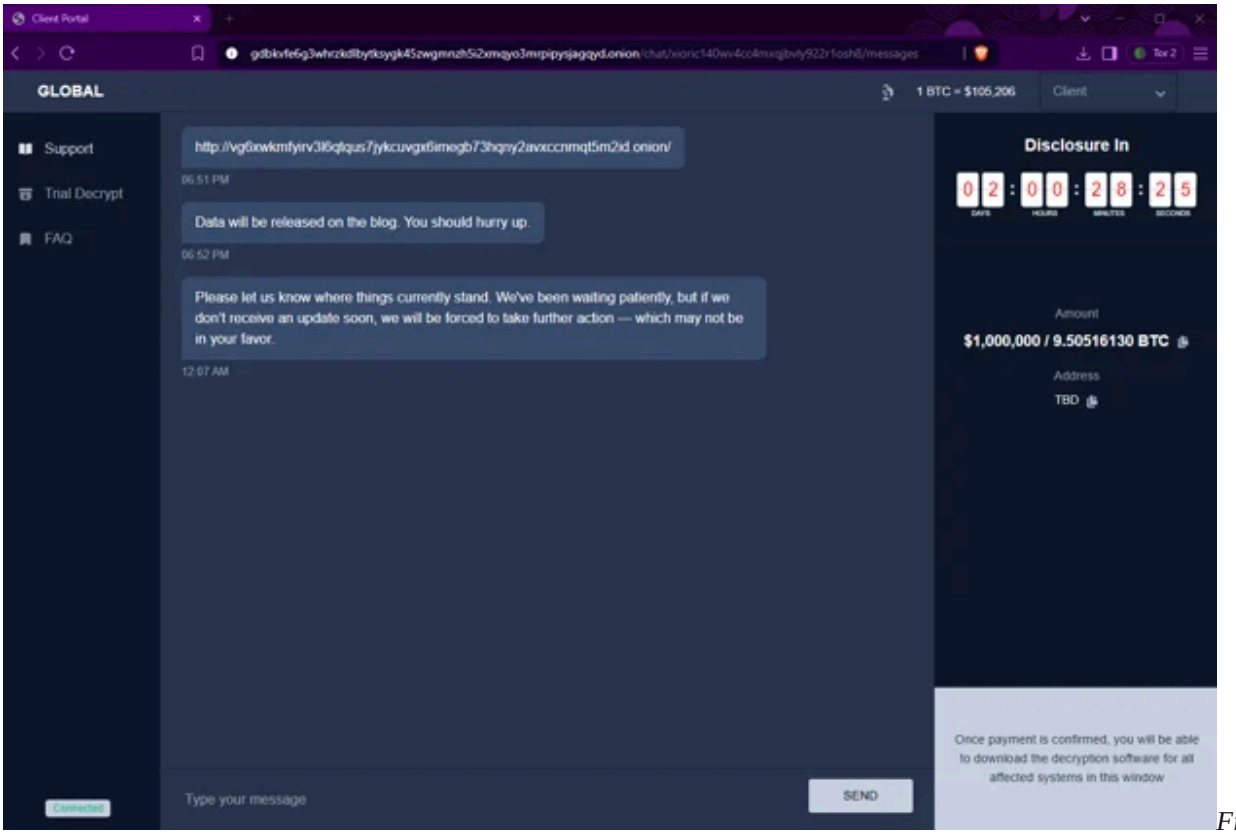

Figure 12 - Negotiation panel; the threat actor demands 1 million US dollars for the decryption key.

Figure 12 shows a GLOBAL GROUP negotiation panel. An affiliate demanded $1 million (approximately 9.5 BTC at the time) from a victim within 48 hours. This illustrates the group's strategy of targeting high-value ransoms, frequently seeking seven-figure payments through data extortion.

Buying remote access from initial access brokers

GLOBAL GROUP RaaS manager (aka $$$) routinely looks for remote access to corporate networks through Initial Access Brokers (IABs). These purchases typically involve several methods:

- **RDP/Webshell access to high-value targets**: The threat actor has acquired RDP-level access to a U.S. law-firm environment protected by standard AV.
- **Domain user & local admin privileges via webshells**: The actor has purchased webshell access on Linux-based systems such as SAP NetWeaver granting direct footholds in target networks.
- **VPN credentials and edge-device exploits**: The actor shows clear interest in brute-forcing or exploiting enterprise VPN appliances (Fortinet, Palo Alto, Cisco), aiming to gain initial entry at the network perimeter.

“$$$” combine these access vectors for rapid deployment, and quickly deploy post-exploitation tooling for lateral movement. The actor then exfiltrates large amount of sensitive data for extortion. This lifecycle usually ends with ransomware execution across compromised networks.

Acquisition for remote desktop protocol (RDP) access on U.S. based law-firm

On February 17, 2025, a Russian-speaking Initial Access Broker (IAB) using the alias “HuanEbashes” posted an advertisement on the Ramp4u forum. The post offered RDP access to a U.S.-based law firm. The broker noted the presence of legal personnel, a domain-connected system, and confirmation of access to financial and income-related data. These characteristics made the target attractive to ransomware operators. The broker highlighted that they had not verified antivirus protections on the victim’s system and set the initial asking price at $1,000, with room for negotiation.

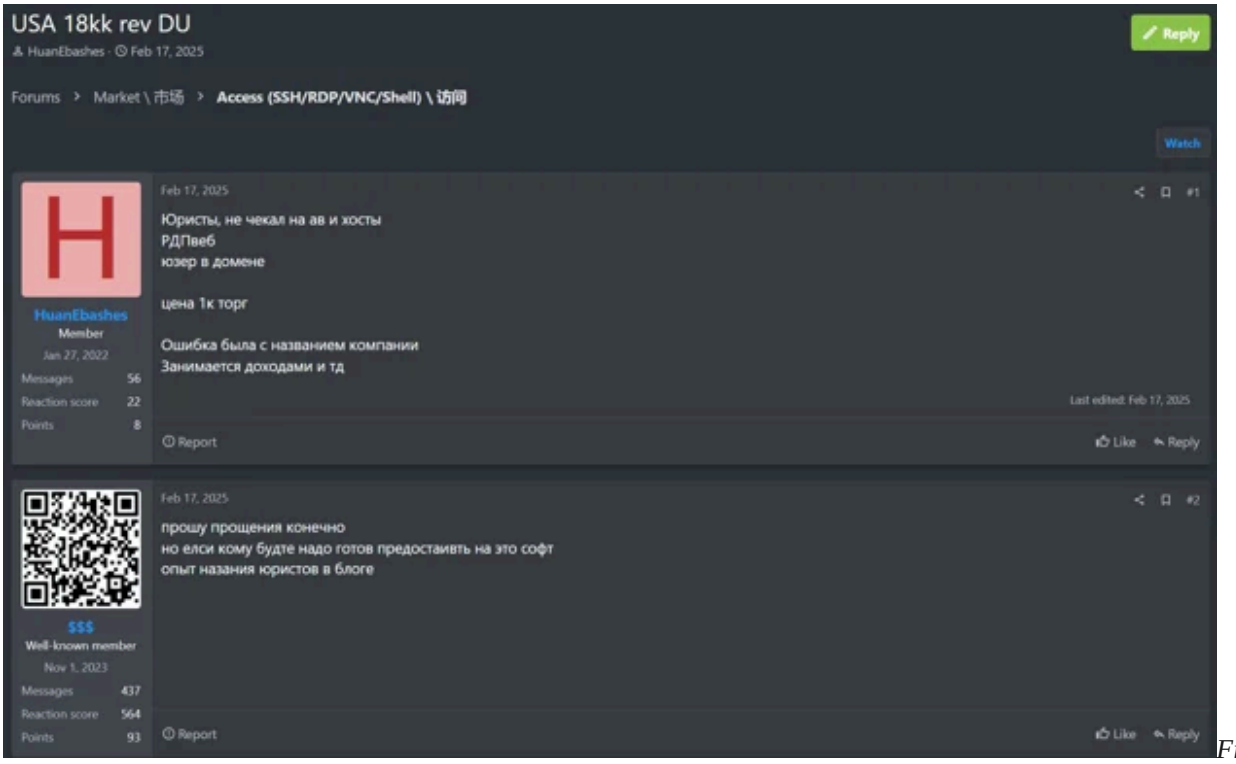

Figure 13 - Threat actor “$$$” engaging with initial access broker “HuanEbashes” on Ramp4u.

Figure 14 shows a response from threat actor “$$$” who expressed interest and clarified his willingness to either purchase the access outright or enter into a profit-sharing agreement. The latter would involve using his own ransomware service against that U.S.-based victim.

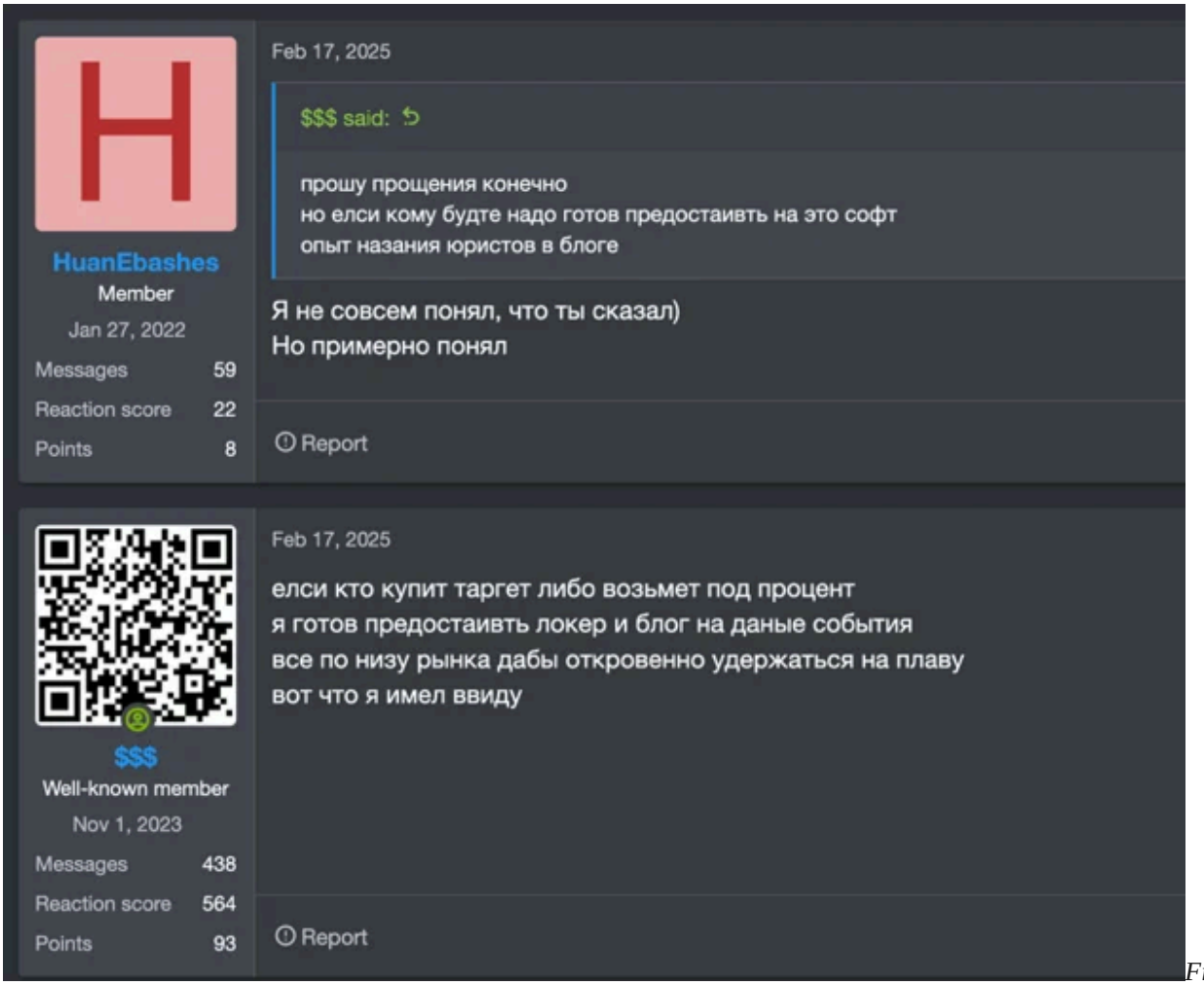

Figure 14 - Communication between “HuanEbashes” and “$$$” about profit-sharing agreement.

This exchange indicates active collaboration between access brokers and ransomware actors with a focus on targeting high-value institutions for potential high returns. The law firm's internal access, paired with financial and legal-sensitive data, makes it an attractive target for data extortion. The initial access broker's willingness to negotiate and the affiliate’s operational readiness demonstrate a service-oriented criminal ecosystem that works like a real enterprise who are open for any kind of collaboration for profit.

HuanEbashes selling VPN Brute-force tools and possible interest from GLOBAL GROUP

On May 19, “HuanEbashes” posted another advertisement for a newly developed “Brute VPN” tool. The actor explained that this tool was specifically designed to automate password-spraying attacks against a variety of VPN and web-access portals used by corporate networks. The post highlighted a base price of $400.

According to the post, the tool targets products including Fortinet VPN, Palo Alto GlobalProtect, and Cisco VPN.

Besides the VPN solution, threat actor “HuanEbashes” also mentioned two internet-facing applications used in the Microsoft ecosystem. These are also within the scope of this brute forcing tool: Outlook Web Access (OWA/Outlook Web Access) and RDWeb (Remote Desktop Web Access).

EclecticIQ analysts observed multiple interactions between threat actor “$$$” and IAB persona called **“**HuanEbashes**”** suggesting the two are likely establishing a business arrangement to scale the ransomware

operations.

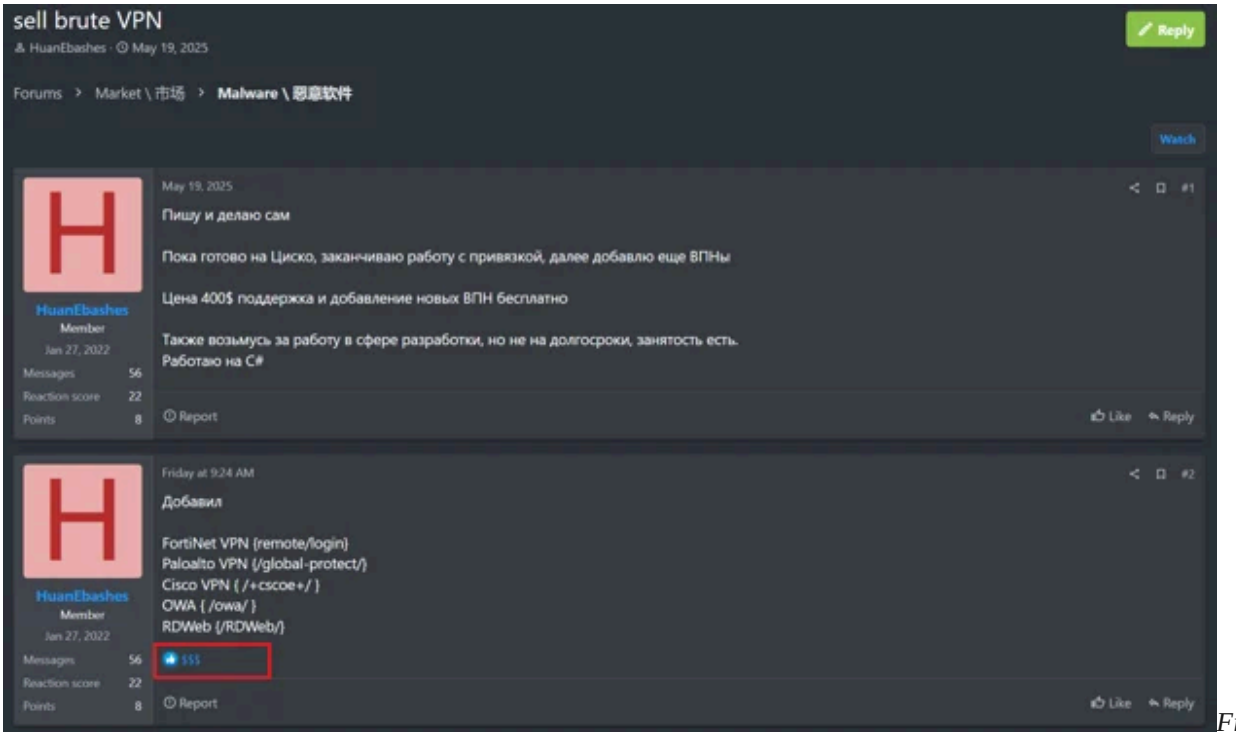

Figure 15 - Threat actor "$$$" liked a thread by "HuanEbashes" advertising brute-force VPN access tools.

Interactions between "$$$" and "HuanEbashes" reveal several calculated motivations for GLOBAL GROUP:

1. **Broaden initial access options.**
   GLOBAL GROUP does not want to rely solely on initial access brokers (IABs). A brute-force tool lets attackers harvest valid VPN credentials or session tokens directly. Successfully compromising a VPN gateway grants stealthy entry, often without any host-level antivirus or endpoint-detection alert.

1. **Increase the speed of ransomware operations.**
   Attackers can move laterally into the network once they obtain valid VPN. They can then deploy ready-to-run ransomware kits to increase the impact.

Targeting high-privilege, externally exposed access points such as VPN gateways gives adversaries an ability to evade endpoint defenses and host-based monitoring, handing them legitimate credentials or session tokens that appear benign to most security controls; once inside, the attackers inherit the trust and permissions of real users that often come with a default broad network reach, allowing them to move laterally, disable safeguards, and detonate ransomware payloads with minimal friction and maximum speed, turning what is normally a multistage intrusion into a repeatable business process.

Leveraging Initial Access Brokers (IAB) to gain foothold in edge network devices and accelerate ransomware operations

The creation of GLOBAL GROUP by Black Lock's administrator is a deliberate strategy to modernize operations, expand revenue streams, and stay competitive in the ransomware market. This new brand integrates AI-powered negotiation, mobile-friendly panels, and customizable payload builders, appealing to a broader pool of affiliates.

GLOBAL GROUP further accelerates ransomware deployment by leveraging Initial Access Brokers (IABs), who supply pre-compromised entry points into enterprise networks. This outsourcing of infiltration reduces time-to-compromise and enables affiliates to focus on payload delivery and extortion rather than network penetration.

GLOBAL GROUP supports payloads tailored for VMware ESXi environments, allowing affiliates to directly encrypt virtualized infrastructure. By compromising hypervisors, attackers can lock down dozens—or even hundreds—of virtual machines at once, multiplying the impact of a single intrusion and drastically increasing pressure on victims to pay.

Security teams must continuously monitor for IAB-linked access sales, harden internet-facing infrastructure—particularly edge network appliances—and implement strict access segmentation and hypervisor hardening for ESXi hosts by disabling SSH, enabling lockdown mode, enforcing signed-only script execution via UEFI Secure Boot and TPM, and isolating management interfaces behind PAM-controlled jump servers with no direct internet exposure [8].

Integrating real-time threat intelligence that detects both ransomware tooling and access brokerage is critical. As ransomware-as-a-service models increasingly mimic the scalability and efficiency of SaaS platforms, defenders must treat these actors not as isolated criminals but as organized, operationally mature adversaries.

MITRE ATT&CK Matrix

Figure 16 - MITRE ATT&CK TTP Linked to Global Group.

IOCs

IP address of the GLOBAL GROUP DLS:

- 193.19.119[.]4

GLOBAL ransomware samples:

- b5e811d7c104ce8dd2509f809a80932540a21ada0ee9e22ac61d080dc0bd237d
- 232f86e26ced211630957baffcd36dd3bcd6a786f3d307127e1ea9a8b31c199f
- 28f3de066878cb710fe5d44f7e11f65f25328beff953e00587ffeb5ac4b2faa8

- 1f6640102f6472523830d69630def669dc3433bbb1c0e6183458bd792d420f8e
- 232f86e26ced211630957baffcd36dd3bcd6a786f3d307127e1ea9a8b31c199f

Go based GLOBAL ransomware sample:

- a8c28bd6f0f1fe6a9b880400853fc86e46d87b69565ef15d8ab757979cd2cc73

Onion sites:

- vg6xwkmfyirv3l6qtqus7jykcuvgx6imegb73hqny2avxccnmqt5m2id[.]onion
- gdbkvfe6g3whrzkdlbytksygk45zwgmnzh5i2xmqyo3mrpipysjagqyd[.]onion

Social media account:

- x[.]com/GlobalTeamLock

YARA rule

https://gist.github.com/whichbuffer/e9c298008395e5dc18fbc4f8180dec58

References

[1] “Eldorado Ransomware: The New Golden Empire of Cybercrime? | Group-IB Blog,” Group-IB. Accessed: Jun. 10, 2025. [Online]. Available: https://www.group-ib.com/blog/eldorado-ransomware/

[2] “Mamona Ransomware.” Accessed: Jun. 10, 2025. [Online]. Available: https://www.broadcom.com/support/security-center/protection-bulletin/mamona-ransomware

[3] “Blog - Global,” archive.ph. Accessed: Jun. 04, 2025. [Online]. Available: https://archive.ph/YQ5WK

[4] “VirusTotal - File - a8c28bd6f0f1fe6a9b880400853fc86e46d87b69565ef15d8ab757979cd2cc73.” Accessed: Jun. 10, 2025. [Online]. Available: https://www.virustotal.com/gui/file/a8c28bd6f0f1fe6a9b880400853fc86e46d87b69565ef15d8ab757979cd2cc73/detection

[5] “BlackLock Ransomware: What You Need To Know | Tripwire.” Accessed: Jun. 10, 2025. [Online]. Available: https://www.tripwire.com/state-of-security/blacklock-ransomware-what-you-need-know

[6] T. H. News, “BlackLock Ransomware Exposed After Researchers Exploit Leak Site Vulnerability,” The Hacker News. Accessed: Jun. 10, 2025. [Online]. Available: https://thehackernews.com/2025/03/blacklock-ransomware-exposed-after.html

[7] “qTox: A New Kind of Instant Messaging.” Accessed: Jun. 11, 2025. [Online]. Available: https://qtox.github.io/

[8] Sygnia, “Understanding ESXi Ransomware: SSH Tunneling and Defense Strategies,” Sygnia. Accessed: Jun. 05, 2025. [Online]. Available: https://www.sygnia.co/blog/esxi-ransomware-ssh-tunneling-defense-strategies/
