GLOBAL Ransomware - New Tactics Revealed

By Written byJayden Palacios

Archived: 2026-04-05 20:04:16 UTC

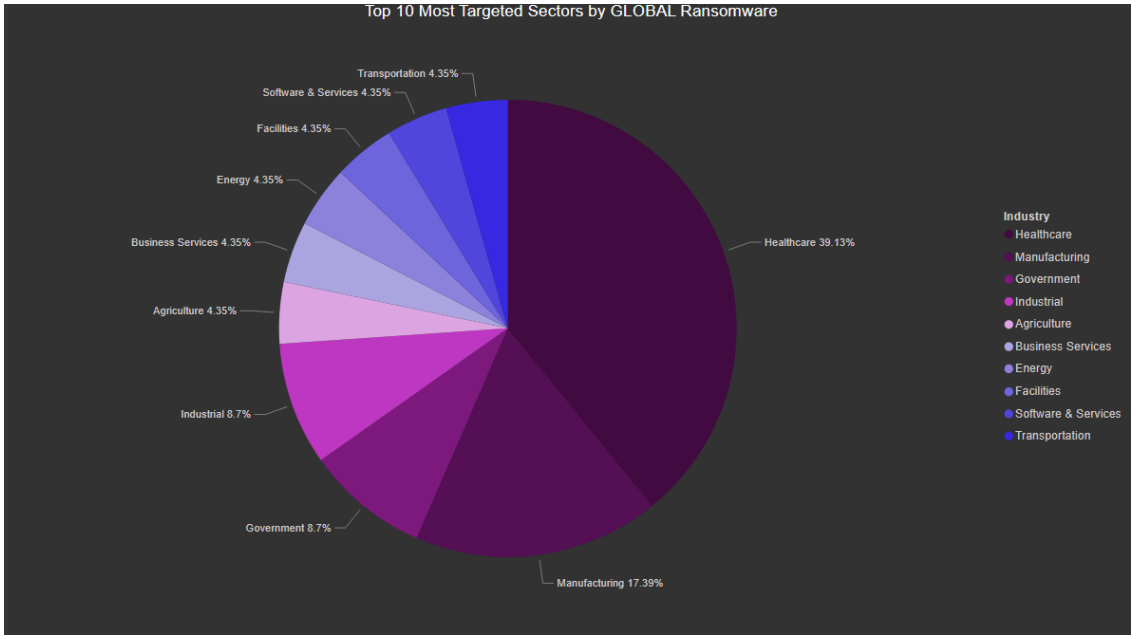
Summary

GLOBAL ransomware is a recently established Ransomware-as-a-Service (RaaS) group that surfaced in mid-2025 but is linked through OPSEC mistakes to earlier families such as Mamona and BlackLock. The operation is financially motivated and wants to attract as many affiliates as possible, offering high revenue shares, no entry fees, and an admin panel with AI-driven negotiation tools. Victimology shows a clear focus on healthcare and manufacturing sectors where downtime creates maximum pressure to pay. GLOBAL offers cross-platform lockers written in C++, C, and Golang with enterprise-oriented features such as LDAP propagation, token impersonation, and configurable execution modes designed for speed and scalability. GLOBAL affiliates leverage Initial Access Brokers to streamline intrusions, which expands participation and attack volume. The group uses aggressive negotiation tactics, ransom notes delivered across multiple vectors, and a Tor-hosted AI chatbot portal to manage communications.

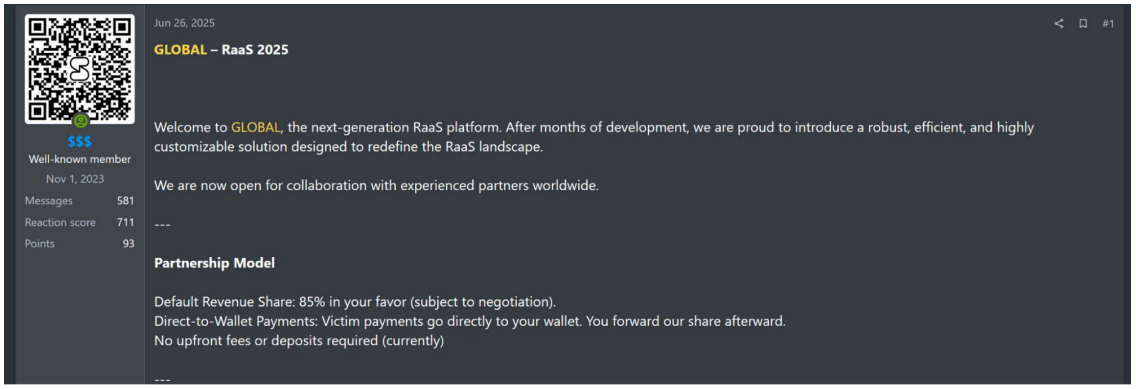
Analysis

Overview

GLOBAL Ransomware, also known as the GLOBAL GROUP, is a Ransomware-as-a-Service (RaaS) group that first emerged in June 2025. Since then, it has claimed 32 victims on its tor data leak site (DLS). Over half of GLOBAL’s victims operate in the healthcare or manufacturing sectors, following a larger trend where cyber extortionists target industries that are heavily reliant on digital systems for business operations. In healthcare, this can disrupt patient care and overall well-being, creating additional pressure on victims during ransom negotiations. This also reveals the financial motivations of the group, targeting high value sectors that are more likely to pay a ransom to resume normal operations.



Mistakes in operational security (OPSEC) revealed that the group is a continuation of the Mamona and Blacklock ransomware families. When first deploying its Tor DLS, GLOBAL used an insecure REST API on the frontend that exposed an SSH connection field containing the true IP address of its backend infrastructure, 193.19.119[.]4. This server is hosted by Russian VPS provider IPServer, the same hosting provider previously used by Mamona ransomware. The clearest evidence, however, is the use of an identical mutex string, `Global\Fxo16jmdgujs437`, found in samples of both ransomware families. In addition, the same alias, `$$$`, was used to advertise GLOBAL, Mamona, and Blacklock ransomware lockers on the RAMP forum.



Forum posts advertising the RaaS use three languages; English, Russian, and Chinese. This indicates their desire to attract as many affiliates as possible as most RaaS advertisements only cater to English and Russian-speaking threat actors. This is reflective of a shift in the cybercrime ecosystem where China-based threat actors are beginning to contribute to the ransomware ecosystem. Furthermore, this may suggest GLOBAL intends to target Chinese based organizations.

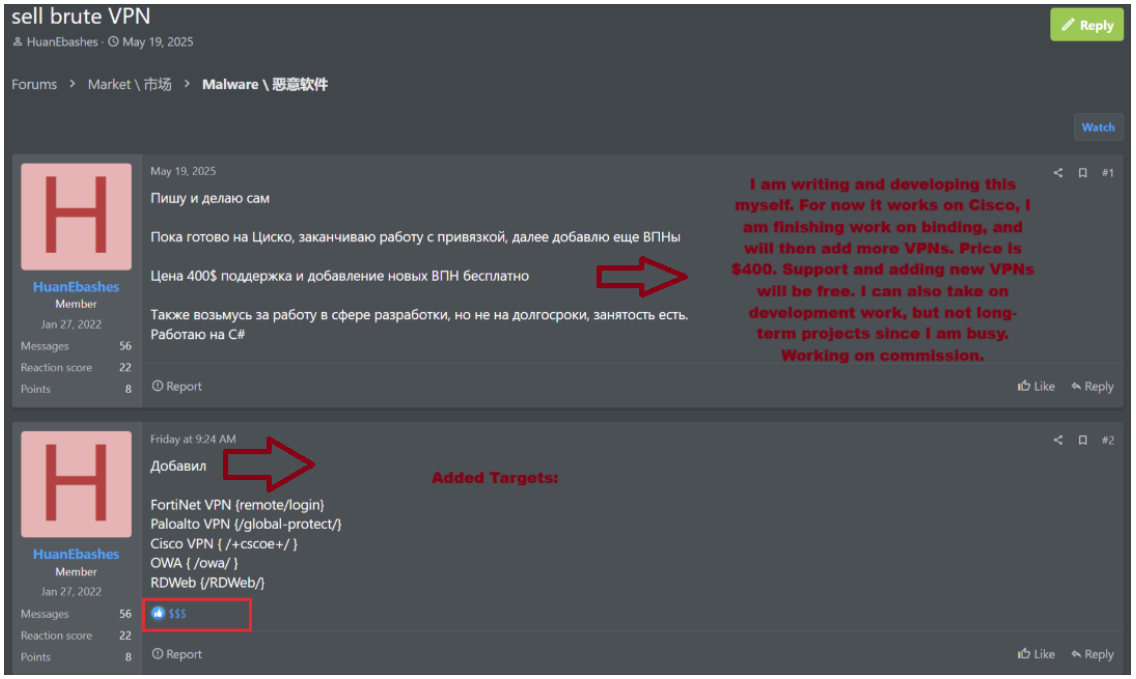
GLOBAL operates in the same fashion as most RaaS groups. Affiliates are attracted using a high revenue share of 85% for every ransom they extract from a victim. Currently, there is no fee to join GLOBAL'S affiliate program, giving security researchers an opportunity to infiltrate the operation. GLOBAL offers an admin panel, enabling affiliates to conduct AI-assisted ransom negotiation chats, manage builds, and download decryptors.

Our investigation into this threat group uncovered a Windows locker sample written in C++. The file was located by searching open malware exchange platforms for GLOBAL's DLS onion site, which is hardcoded into their lockers. Sandbox analysis of the sample revealed the full ransom note with instructions to access a negotiation chat room. We repeated this process for additional GLOBAL ransomware samples, providing insight into both their negotiation tactics and attack chain.

The malware itself targets Windows, ESXi environments, network-attached storage (NAS) devices, and BSD-based operating systems (FreeBSD, OpenBSD, NetBSD, etc.). The lockers are written in C++, C, and Golang, respectively. Its authors employ anti-analysis techniques to prevent reverse engineering including debugger checks to prevent dynamic analysis and dead code to confuse disassemblers.

Kill Chain

GLOBAL affiliates rely on Initial Access Brokers (IABs) to obtain footholds in victim networks, reflecting a lack of in-house expertise to perform the more technical intrusion work themselves. Rather than developing their own initial access methods, they outsource access or purchase tools that simplify the process. Forum activity shows GLOBAL's operator "$$$" interacting with the actor "HuanEbashes," who was selling a $400 "Brute VPN" tool capable of password-spraying Fortinet VPN, Palo Alto GlobalProtect, Cisco VPN, Outlook Web Access (OWA), and RDWeb. This behavior demonstrates how GLOBAL compensates for limited intrusion skills by turning to IABs or malicious tools sold by other threat actors to secure valid credentials and initial entry.



After gaining initial access, the locker payload is deployed. The locker code includes extensive configuration and execution controls. Strings from a GLOBAL locker sample built for Windows show support for multiple runtime arguments such as `-force`, `-detached`, `-threads`, `-delay`, and `-skip-net`, allowing affiliates to customize encryption behavior for speed, stealth, or delayed execution times (payload activates encryption at specified time). The malware can also toggle spreading modes with `-ldap` for Active Directory domain propagation and

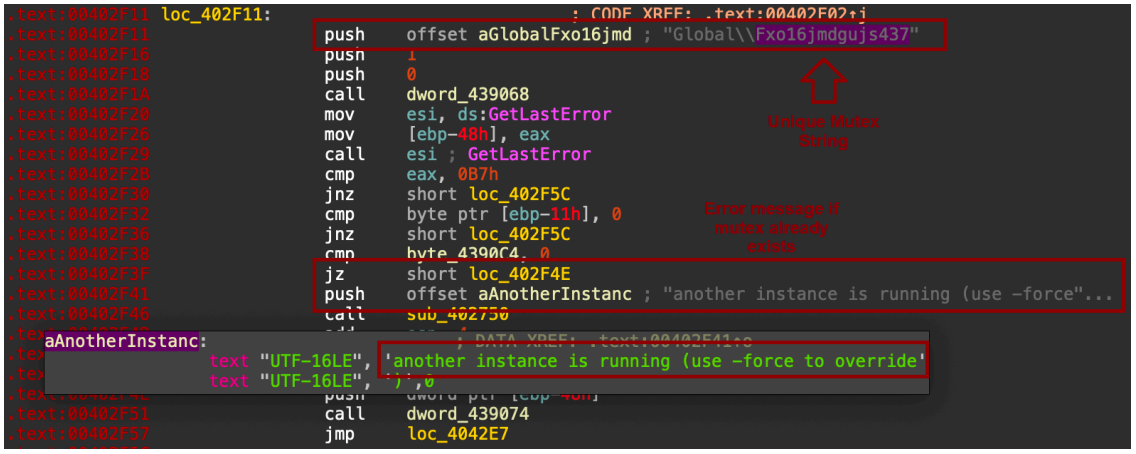
impersonation, indicating enterprise-focused design. Execution logs reference modes like `Local + Network` and `Panic Mode`, indicating the ability to rapidly encrypt all reachable storage in high-pressure scenarios.

When GLOBAL engages in lateral movement primarily over LDAP, enabling domain-wide propagation in enterprise environments. The malware can operate with two distinct approaches: affiliates may supply direct domain credentials to authenticate and spread across the network, or if credentials are not available, the malware attempts to impersonate the current user to continue propagation. It does this by invoking Windows API calls such as `OpenProcessToken`, `DuplicateToken`, and `SetThreadToken` to clone and apply a valid security token, granting it the ability to act under the user's context. This redundancy ensures execution, allowing GLOBAL to spread effectively whether or not valid credentials are on hand.

GLOBAL affiliates engage in data theft prior to the encryption stage. Exfiltrated files are sent to a server under the threat actor's control, ensuring they still have leverage even if encryption fails. To obfuscate their entry point and data servers, the attackers route this traffic through proxy servers and VPNs.

Before the locker payload is deployed, GLOBAL affiliates employ several defense evasion techniques to maximize impact and reduce detection. The malware executes commands such as `cmd.exe /c vssadmin delete shadows /all /quiet` to remove Volume Shadow Copies and prevent easy recovery. It also attempts to terminate antivirus and endpoint detection and response (EDR) processes, then clears Windows Event Logs to hinder forensic analysis and incident response.

For encryption, the ransomware uses the ChaCha20-Poly1305 algorithm and prioritizes speed. Files less than 5MB are fully encrypted and files greater than 5MB only have 20% of their file encrypted. Affiliates are able to use custom file extensions for encrypted files with some affiliates using seemingly random strings. The malware also uses multiple threads to encrypt multiple drives, directories, and files concurrently. As mentioned before, operators can configure their execution using command lines arguments that dictate what is encrypted, granting greater control over potential encryption time. GLOBAL ransomware uses a unique mutex to determine if the machine its executing on has already been encrypted. If the mutex exists on the machine, ransomware was already executed so the malware exits to avoid wasting time encrypting the data again. However, this can be overridden using the -force flag.

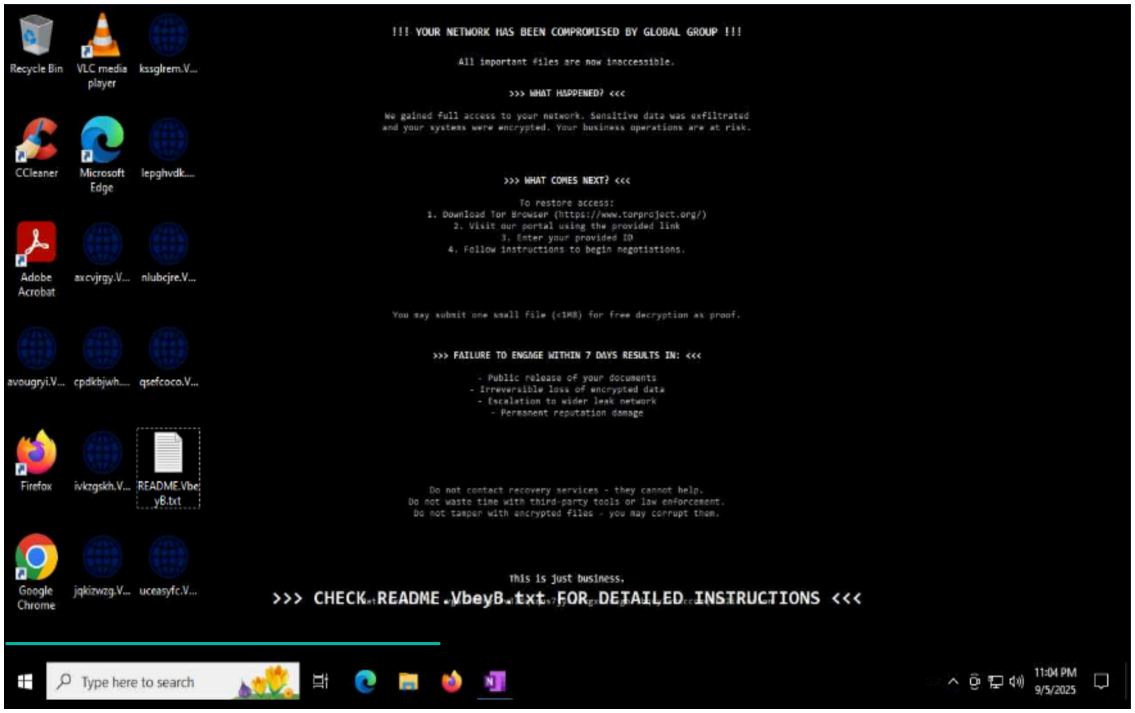


Finally, text files containing two different ransom notes are created. A short "stub" note is dropped across many directories, stating that files were encrypted and tells the user to visit the site and use the ID, but it does not

include the URL or the ID. This stub is hardcoded as plain text in the binary. The full ransom note, which includes the Tor onion chat link and the unique victim ID, is written to the user's Desktop and Documents folders.

```
.rdata:0042A2E0                 text "UTF-16LE", 'All important files are now inaccessible.',0
.rdata:0042A334 aWhatHappened:                          ; DATA XREF: .text:004064CA↑o
.rdata:0042A334                 text "UTF-16LE", '>>> WHAT HAPPENED? <<<',0
.rdata:0042A362                 align 8
.rdata:0042A368 aWeGainedFullAc:                        ; DATA XREF: .text:00406526↑o
.rdata:0042A368                 text "UTF-16LE", 'We gained full access to your network. Sensitive da'
.rdata:0042A3CE                 text "UTF-16LE", 'ta was exfiltrated',0Ah
.rdata:0042A3F4                 text "UTF-16LE", 'and your systems were encrypted. Your business oper'
.rdata:0042A45A                 text "UTF-16LE", 'ations are at risk.',0
.rdata:0042A482                 align 4
.rdata:0042A484 aWhatComesNext:                         ; DATA XREF: .text:0040657A↑o
.rdata:0042A484                 text "UTF-16LE", '>>> WHAT COMES NEXT? <<<',0
.rdata:0042A4B6                 align 4
.rdata:0042A4B8 aToRestoreAcces:                        ; DATA XREF: .text:004065D0↑o
.rdata:0042A4B8                 text "UTF-16LE", 'To restore access:',0Ah
.rdata:0042A4DE                 text "UTF-16LE", '1. Download Tor Browser (https://www.torproject.org'
.rdata:0042A544                 text "UTF-16LE", '/)',0Ah
.rdata:0042A54A                 text "UTF-16LE", '2. Visit our portal using the provided link',0Ah
.rdata:0042A5A2                 text "UTF-16LE", '3. Enter your provided ID',0Ah
.rdata:0042A5D6                 text "UTF-16LE", '4. Follow instructions to begin negotiations.',0
.rdata:0042A632                 align 8
.rdata:0042A638 aYouMaySubmitOn:                        ; DATA XREF: .text:00406627↑o
.rdata:0042A638                 text "UTF-16LE", 'You may submit one small file (<1MB) for free decry'
.rdata:0042A69E                 text "UTF-16LE", 'ption as proof.',0
.rdata:0042A6BE                 align 10h
.rdata:0042A6C0 aFailureToEngag:                        ; DATA XREF: .text:0040668A↑o
.rdata:0042A6C0                 text "UTF-16LE", '>>> FAILURE TO ENGAGE WITHIN 7 DAYS RESULTS IN: <<<'
.rdata:0042A726                 text "UTF-16LE", 0
.rdata:0042A728 aPublicReleaseO:                        ; DATA XREF: .text:004066E4↑o
.rdata:0042A728                 text "UTF-16LE", '- Public release of your documents',0Ah
.rdata:0042A76E                 text "UTF-16LE", '- Irreversible loss of encrypted data',0Ah
.rdata:0042A7BA                 text "UTF-16LE", '- Escalation to wider leak network',0Ah
.rdata:0042A800                 text "UTF-16LE", '- Permanent reputation damage',0
.rdata:0042A83C                 align 10h
.rdata:0042A840 aDoNotContactRe:                        ; DATA XREF: .text:0040672B↑o
.rdata:0042A840                 text "UTF-16LE", 'Do not contact recovery services - they cannot help'
.rdata:0042A8A6                 text "UTF-16LE", '.',0Ah
.rdata:0042A8AA                 text "UTF-16LE", 'Do not waste time with third-party tools or law enf'
.rdata:0042A910                 text "UTF-16LE", 'orcement.',0Ah
.rdata:0042A924                 text "UTF-16LE", 'Do not tamper with encrypted files - you may corrup'
.rdata:0042A98A                 text "UTF-16LE", 't them.',0
```

The ransomware also attempts to print ransom notes on any available printers and replaces all desktop wallpapers with a redacted version of the note. Morado identified a new version of the GLOBAL ransomware note. Both versions will be included alongside IOCs.



In one negotiation, affiliates shared a high-level summary of their kill chain. Initial access was achieved through phishing that delivered a Remote Access Trojan (RAT), which created a remote connection to the infected host. Persistence was maintained by installing additional software configured to execute at startup and evade detection. The actors conducted reconnaissance of the internal environment, enumerating servers, user accounts, and permissions. Privilege escalation was obtained by exploiting a system vulnerability to gain administrator rights, followed by lateral movement to compromise additional machines. Finally, data was exfiltrated to attacker-controlled servers, with proxy servers and VPNs used to obfuscate the exit points and external infrastructure.

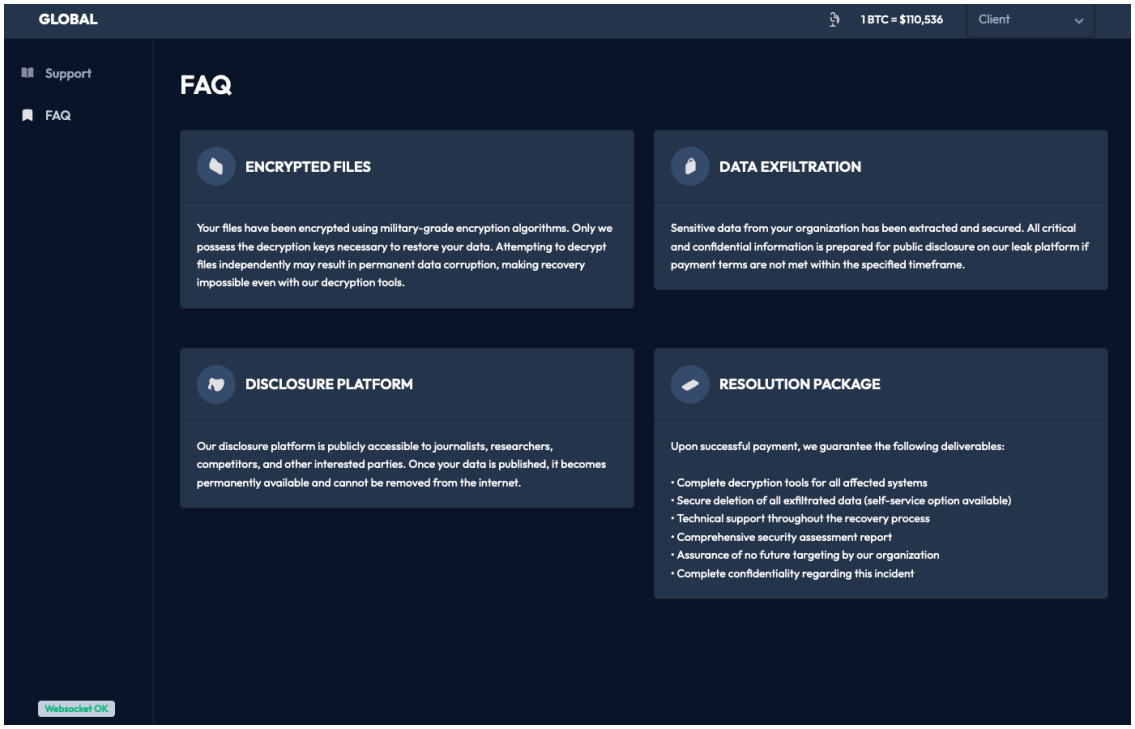
This account directly supports the earlier analysis. The use of a RAT aligns with the type of access commonly sold by IABs, lateral movement matches observed LDAP-based propagation techniques, and the reliance on VPNs and proxies reinforces how affiliates conceal the location of their exfiltration servers.

Negotiation Tactics

Once data is exfiltrated and encrypted, ransom negotiations are started. Victims are typically given three days to respond before threatening to leak stolen data, but this slight varies by incident. Once negotiations begin, this grace period is extended until a payment is made or no agreement is reached. GLOBAL affiliates have been seen demanding ransom payments of over one million USD. In some chats, affiliates require victims to pay 50% of the ransom demand upfront in order to continue negotiations. Payments are made via bitcoin. Affiliates work to induce a sense of urgency using direct language alongside threats of data leakage leading reputational impact.

They use OSINT and compromised data to evoke a feeling of deep surveillance and knowledge of the victim’s business operations, further pressuring a payment. Affiliates also state plainly that they only care about money, showing clear financial motivations. Their negotiation strategy is aggressive, starting with extremely high demands but conceding to most counter offers. In one case, a ransom was lowered by nearly 75% from the original price with no resistance from the affiliate, indicating flexibility designed to secure quick payments.

The FAQ within the portal expresses that GLOBAL provides decryption tools after successful payments, deletion of all data, technical support, and a security assessment. GLOBAL clearly wants to be viewed as trustworthy to convince victims that paying a ransom is the best option. However, there is no way to confirm these claims and should be assumed to be false like the claims of any cybercriminal.



Conclusion

GLOBAL ransomware represents the continued evolution of mid-tier RaaS operations into enterprise-focused threats. The group has clear lineage to Mamona and BlackLock but distinguishes itself through multilingual recruiting, AI-assisted negotiation tooling, and two-stage ransom note delivery. Its reliance on Initial Access Brokers and purchased attack tools lowers the barrier to entry, broadening affiliate participation and increasing attack volume.

The operation’s emphasis on rapid, configurable encryption and pre-encryption data theft creates significant pressure on victims in healthcare and manufacturing, sectors already vulnerable to downtime. Combined with aggressive negotiation tactics and flexible ransom demands, GLOBAL poses a significant threat to organizations operating in critical sectors.

Given its growth trajectory and focus on sectors with low tolerance for disruption, GLOBAL should be treated as an active and expanding threat. Defenders should expect campaigns leveraging IAB access, brute-force tooling, and opportunistic targeting of exposed enterprise services.

Recommendations

- Limit and monitor LDAP services to reduce risk of domain-wide propagation.
- Isolate critical systems (e.g., healthcare or manufacturing control systems) from user endpoints to contain potential lateral movement. and reduce operational impact
- Enforce strict access controls, disable unused accounts, and use Just-in-Time (JIT) privileges to limit token abuse.
- Continuously assess exposure from Initial Access Brokers (IABs) by monitoring compromised credentials and stealer log markets within the Threatnote platform.

- Watch for creation of the unique mutex string `Global\\Fxo16jmdgujs437` or variants, which indicate execution attempts.
- Ensure a backup strategy is in place, clearly outlined, and has been tested to verify its efficacy.

Ransom Notes

Our investigation revealed a new, slightly modified, version of the previously known GLOBAL ransom note. Both are provided below.

New GLOBAL Ransom Note

```
 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
   Your network has been compromised by GLOBAL Group
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

 All important files are now inaccessible. They have been locked using
military-grade encryption. Only GLOBAL holds the decryption keys.

 >>> What happened? <<<
=======================
We gained full access to your network. Sensitive data was exfiltrated
and your systems were encrypted. Your business operations and customer
data are at risk.

>>> What comes next? <<<
========================
To restore access:
1. Download Tor Browser (https://www.torproject.org/)
2. Visit our portal: gdbkvfe6g3whrzkdlbytksygk45zwgmnzh5i2xmqyo3mrpipysjagqyd.onion/chat/{redacted
slug}
3. Enter your ID: >>> {redacted chat room password}<<<
4. Follow instructions to begin negotiations.

 You may submit one small file (<1MB) for free decryption as proof.
We will send you a file-listing proving we have stolen your data.

>>> FAILURE TO ENGAGE WITHIN 7 DAYS RESULTS IN: <<<
=================================================
- Public release of your documents
- Irreversible loss of encrypted data
- Escalation to wider leak network
- Permanent reputation damage
```

```
Do not contact recovery services - they cannot help.
Do not waste time with third-party tools or law enforcement.
Do not tamper with encrypted files - you may corrupt them.

This is just business.

Data Leak Site: http://vg6xwkmfyirv3l6qtqus7jykcuvgx6imegb73hqny2avxccnmqt5m2id.onion/

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
              **GLOBAL operates globally.**
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Old GLOBAL Ransom Note

```
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/{redeacted slug}
3. Enter your unique ID: {redacted chat room password}
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://vg6xwkmfyirv3l6qtqus7jykcuvgx6imegb73hqny2avxccnmqt5m2id.onion/`

`**GLOBAL operates globally.**`

`IOCs`

Type	Value	Note
FileHash-SHA256	23b43226d53e2c8cd9519d785ba75b833fbd11939cd1d70999f84c1365b2da5d	Ransomware executable
FileHash-SHA256	1d5bd6014a9c37e06b0c02b29eaed53725c9abf8be57bed0151c5599af3e3f4d	Old Ransom Note
FileHash-SHA256	791ecebd558390e04c96fc86e995bfb0240d601ca2d4d183fa5e0d16a6358e39	New Ransom Note
Onion URL	http://gdbkvfe6g3whrzkdlbytksygk45zwgmnzh5i2xmqyo3mrpipysjagqyd.onion	Victim Portal
Onion URL	http://vg6xwkmfyirv3l6qtqus7jykcuvgx6imegb73hqny2avxccnmqt5m2id.onion/	DLS
String	"Global\Fxo16jmdgujs437"	Unique Mutex Used
FileHash-SHA256	b5e811d7c104ce8dd2509f809a80932540a21ada0ee9e22ac61d080dc0bd237d	Ransomware Sample
FileHash-SHA256	232f86e26ced211630957baffcd36dd3bcd6a786f3d307127e1ea9a8b31c199f	Ransomware Sample
FileHash-SHA256	28f3de066878cb710fe5d44f7e11f65f25328beff953e00587ffeb5ac4b2faa8	Ransomware Sample
FileHash-SHA256	1f6640102f6472523830d69630def669dc3433bbb1c0e6183458bd792d420f8e	Ransomware Sample
FileHash-SHA256	232f86e26ced211630957baffcd36dd3bcd6a786f3d307127e1ea9a8b31c199f	Ransomware Sample

Type	Value	Note
FileHash-SHA256	a8c28bd6f0f1fe6a9b880400853fc86e46d87b69565ef15d8ab757979cd2cc73	Ransomware Sample

`TTPs`

Tactic	Technique	Subtechnique
TA0001: Initial Access	T1190: Exploit Public-Facing Application	
	T1133: External Remote Services	
	T1078: Valid Accounts	T1078.001: Default Accounts
	T1078: Valid Accounts	T1078.002: Domain Accounts
TA0002: Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
	T1203: Exploitation for Client Execution	
	T1053: Scheduled Task/Job	
	T1569: System Services	T1569.002: Service Execution
	T1047: Windows Management Instrumentation	
	T1106: Native API	
TA0003: Persistence	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1133: External Remote Services	
	T1053: Scheduled Task/Job	
	T1078: Valid Accounts	T1078.001: Default Accounts
	T1078: Valid Accounts	T1078.002: Domain Accounts
TA0004: Privilege Escalation	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1068: Exploitation for Privilege Escalation	

Tactic	Technique	Subtechnique
	T1053: Scheduled Task/Job	
	T1078: Valid Accounts	T1078.001: Default Accounts
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
TA0005: Defense Evasion	T1480: Execution Guardrails	T1480.002: Mutual Exclusion
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1656: Impersonation	
	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
	T1036: Masquerading	
	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
	T1078: Valid Accounts	T1078.001: Default Accounts
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
	T1622: Debugger Evasion	
	T1497: Virtualization/Sandbox Evasion	T1497.003: Time Based Evasion
TA0006: Credential Access	T1110: Brute Force	
TA0007: Discovery	T1083: File and Directory Discovery	
	T1046: Network Service Discovery	
	T1135: Network Share Discovery	
	T1057: Process Discovery	

Tactic	Technique	Subtechnique
	T1016: System Network Configuration Discovery	
TA0008: Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
	T1021: Remote Services	T1021.002: SMB/Windows Admin Shares
TA0011: Command and Control	T1105: Ingress Tool Transfer	
TA0010: Exfiltration	T1020: Automated Exfiltration	
	T1041: Exfiltration Over C2 Channel	
	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
TA0040: Impact	T1486: Data Encrypted for Impact	
	T1657: Financial Theft	
	T1490: Inhibit System Recovery	
	T1489: Service Stop	
