Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

GLOBAL GROUP RaaS Gains Momentum with AI-Powered Negotiation Tools

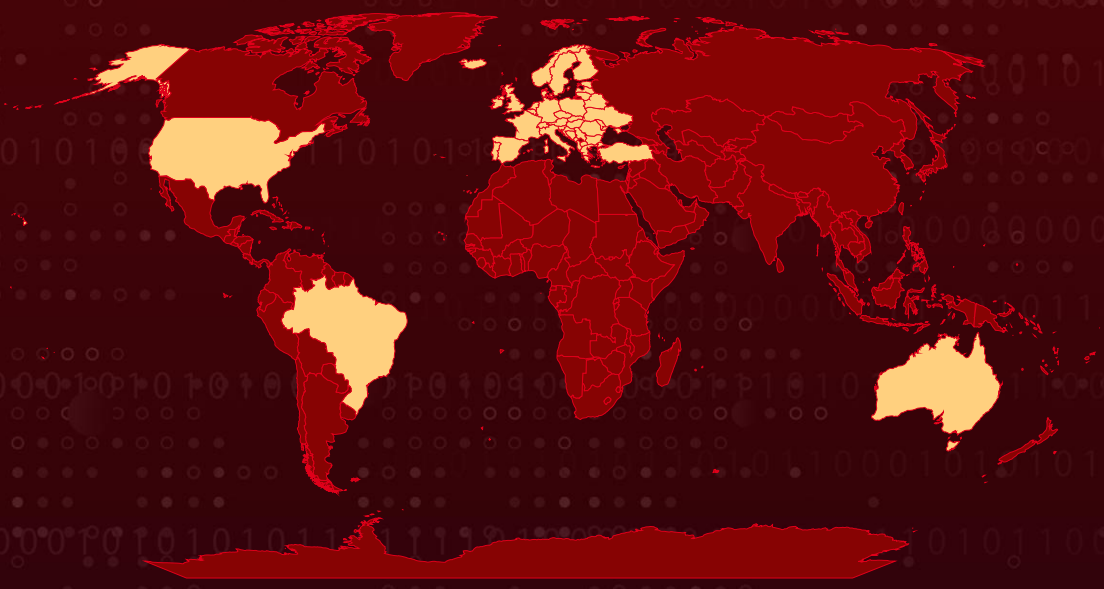
Date of Publication	Admiralty Code	TA Number
July 17, 2025	A1	TA2025223

Summary

First Seen: June 2025
Malware: GLOBAL Ransomware
Ransom Demand by Affiliate: $1 million
Targeted Countries: United States, Australia, United Kingdom, Brazil, Sweden, Belgium, Turkey, Germany, France, Italy, Spain, Ukraine, Poland, Romania, Netherlands, Czech Republic, Portugal, Greece, Hungary, Austria, Belarus, Switzerland, Bulgaria, Serbia, Denmark, Finland, Norway, Slovakia, Ireland, Croatia, Bosnia and Herzegovina, Moldova, Lithuania, Albania, Slovenia, Latvia, North Macedonia, Estonia, Luxembourg, Montenegro, Malta, Iceland, Andorra, Liechtenstein, Monaco, San Marino, Holy See
Targeted Industries: Agriculture, Automotive, Business Process Outsourcing, Business Services & Consulting, Energy, Engineering, Financial Services, Healthcare, Industrial, Manufacturing, Oil and Gas, Retail, Technology, Transportation

Attack: GLOBAL GROUP, a Ransomware-as-a-Service (RaaS) operation active since June 2025, is gaining traction on Russian-speaking cybercrime forums by offering high affiliate payouts and flexible tooling. The group relies on Initial Access Brokers for network entry. It offers affiliates AI-powered negotiation systems, mobile-accessible dashboards, and customizable ransomware builders, making the platform more attractive to a wider range of cybercriminal partners.

Attack Regions



Attack Details

#1 GLOBAL GROUP is a relatively new Ransomware-as-a-Service (RaaS) operation that emerged in June 2025. It is actively promoted on the Ramp4u forum by a Russian-speaking threat actor known as '$$$', who previously operated the Mamona ransomware and now manages BlackLock, a rebrand of an earlier RaaS scheme known as **Eldorado**.

#2 GLOBAL GROUP sets itself apart by offering an unusually high revenue-sharing model, granting affiliates up to 80% of ransom proceeds. This indicates an aggressive strategy to scale operations. The group relies heavily on Initial Access Brokers (IABs) and brute-force techniques to compromise enterprise networks.

#3 The GLOBAL ransomware payload, compiled in the Go programming language, uses the ChaCha20-Poly1305 encryption algorithm to ensure cross-platform compatibility. Once inside a network, the ransomware is deployed rapidly and often evades conventional endpoint defenses.

#4 The operation features a data leak site to publicly pressure victims and employs AI-driven negotiation functionality to enhance communication and increase psychological leverage during ransom discussions. The affiliate platform also supports mobile access, allowing actors to manage and negotiate remotely, further highlighting its operational maturity.

#5 GLOBAL ransomware samples show the use of a customized version of the Mamona ransomware. However, GLOBAL includes upgrades for automated domain-wide deployment, leveraging SMB connections and malicious Windows services to scale attacks more efficiently. Within a short span, GLOBAL GROUP has already claimed responsibility for 18 victims across various countries and industries as of July 2025, signaling a rapid and concerning expansion.

Recommendations

Network and System Hardening: Restrict SMB (Server Message Block) traffic where possible, especially lateral movement via open shares. Disable unnecessary SMB services on endpoints and servers. Limit administrative privileges to essential personnel and apply the principle of least privilege across all systems. Enforce strong network segmentation to isolate critical systems and limit lateral propagation opportunities.

Implement the 3-2-1 Backup Rule: Maintain three total copies of your data, with two backups stored on different devices and one backup kept offsite or in the cloud. This ensures redundancy and protects against data loss from ransomware attacks.

Backup & Recovery Preparedness: Maintain offline, immutable, and regularly tested backups. Ensure recovery time objectives (RTOs) and recovery point objectives (RPOs) meet business continuity requirements in the event of ransomware deployment.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery	**TA0008** Lateral Movement
TA0010 Exfiltration	**TA0040** Impact	**TA0042** Resource Development	**T1650** Acquire Access
T1190 Exploit Public-Facing Application	**T1203** Exploitation for Client Execution	**T1053** Scheduled Task/Job	**T1053.005** Scheduled Task
T1068 Exploitation for Privilege Escalation	**T1027** Obfuscated Files or Information	**T1027.013** Encrypted/Encoded File	**T1110** Brute Force
T1046 Network Service Discovery	**T1135** Network Share Discovery	**T1021** Remote Services	**T1021.002** SMB/Windows Admin Shares
T1020 Automated Exfiltration	**T1041** Exfiltration Over C2 Channel	**T1567** Exfiltration Over Web Service	**T1567.002** Exfiltration to Cloud Storage
T1486 Data Encrypted for Impact	**T1078** Valid Accounts	**T1133** External Remote Services	**T1543.003** Windows Service

T1543 Create or Modify System Process	**T1505** Server Software Component	**T1505.003** Web Shell	**T1562.001** Disable or Modify Tools
T1562 Impair Defenses	**T1036** Masquerading	**T1083** File and Directory Discovery	**T1016** System Network Configuration Discovery
T1491 Defacement	**T1491.002** External Defacement		

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4:Port	193[.]19[.]119[.]4[:]3304
SHA256	b5e811d7c104ce8dd2509f809a80932540a21ada0ee9e22ac61d080dc0bd237d, 28f3de066878cb710fe5d44f7e11f65f25328beff953e00587ffeb5ac4b2faa8, 1f6640102f6472523830d69630def669dc3433bbb1c0e6183458bd792d420f8e, 232f86e26ced211630957baffcd36dd3bcd6a786f3d307127e1ea9a8b31c199f, a8c28bd6f0f1fe6a9b880400853fc86e46d87b69565ef15d8ab757979cd2cc73
TOR Address	vg6xwkmfyirv3l6qtqus7jykcuvgx6imegb73hqny2avxccnmqt5m2id[.]onion, gdbkvfe6g3whrzkdlbytksygk45zwgmnzh5i2xmqyo3mrpipysjagqyd[.]onion
qTox ID	667798F921A68529C74094664C1B890D4E1156C4588906071398FA4F76C2095C2B3AC79FF086
Email	globalteam[@]cyberfear[.]com

Recent Breaches

http://loraincountyauditor.gov/
http://emphail.com/
https://entab.se/
https://www.skylinesalt.com/
http://letrychina.com/
https://fenol.com.tr/en
https://wellwaycentral.co.uk/
http://capitoltax.com/
http://rosewfarm.com/
https://deakinmedical.com.au/
https://www.personalservice.com.br/
https://ad-engineering.co.uk/
https://www.avhg.com.au/
https://www.tcwilson.com/
https://lsproline.com/
https://allnations.health/
http://www.motorworldarc.co.uk/
https://www.epworth.org.au/

References

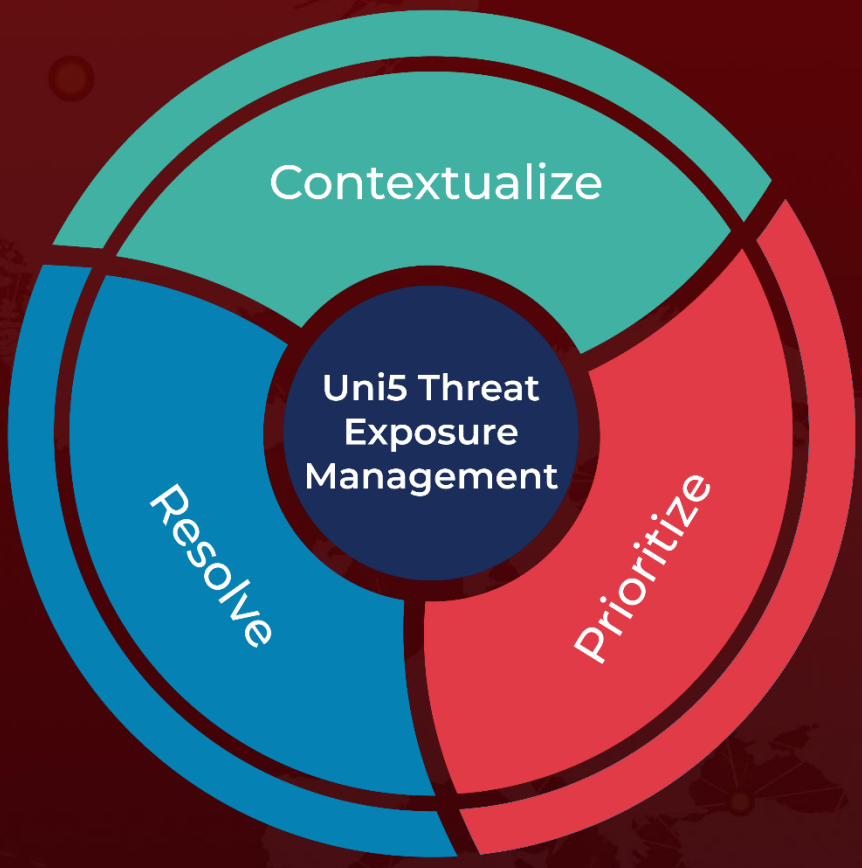
https://blog.eclecticiq.com/global-group-emerging-ransomware-as-a-service

https://hivepro.com/threat-advisory/eldorado-a-new-ransomware-threat-targeting-windows-and-vmware/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

July 17, 2025 • 10:00 PM

More at www.hivepro.com