IMPORTANT: HEAD MARE AND TWELVE JOIN FORCES TO TARGET RUSSIAN ENTITIES

Vairav Security News Report

Date: March 21, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Recent findings from Kaspersky indicate a collaboration between two threat clusters, **Head Mare** and **Twelve**, in cyberattacks against Russian organizations. The connection is evidenced by Head Mare's use of Twelve's command-and-control (C2) servers and tools previously associated with the group. The attackers' leverage exploited vulnerabilities, phishing emails, and contractor compromises to gain initial access, culminating in ransomware deployment and infrastructure destruction.

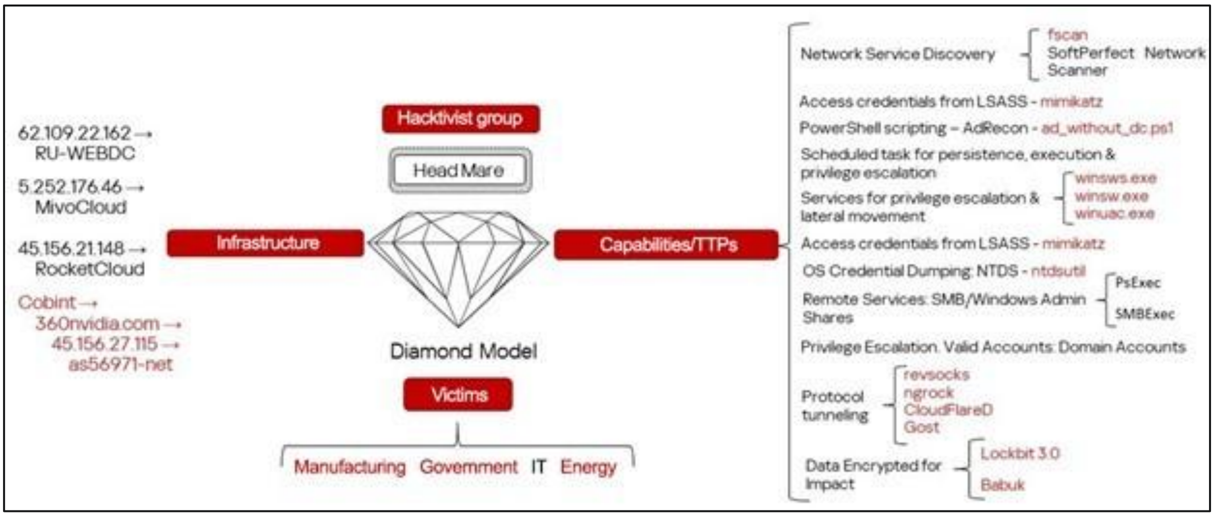
62.109.22.162 →
RU-WEBDC
5.252.176.46 →
MivoCloud
45.156.21.148 →
RocketCloud
Cobint →
360nvidia.com →
45.156.27.115 →
as56971-net
Infrastructure
Hacktivist group
Head Mare
Diamond Model
Victims
Manufacturing
Government
IT
Energy
Capabilities/TTPs
Network Service Discovery
fscan
SoftPerfect Network Scanner
Access credentials from LSASS - mimikatz
PowerShell scripting – AdRecon - ad_without_dc.ps1
Scheduled task for persistence, execution & privilege escalation
Services for privilege escalation & lateral movement
winsws.exe
winsw.exe
winuac.exe
Access credentials from LSASS - mimikatz
OS Credential Dumping: NTDS - ntdsutil
Remote Services: SMB/Windows Admin Shares
PsExec
SMBExec
Privilege Escalation. Valid Accounts: Domain Accounts
Protocol tunneling
revsocks
ngrock
CloudFlareD
Gost
Data Encrypted for Impact
Lockbit 3.0
Babuk

Figure 1: Analysis of the Head Mare techniques and tools

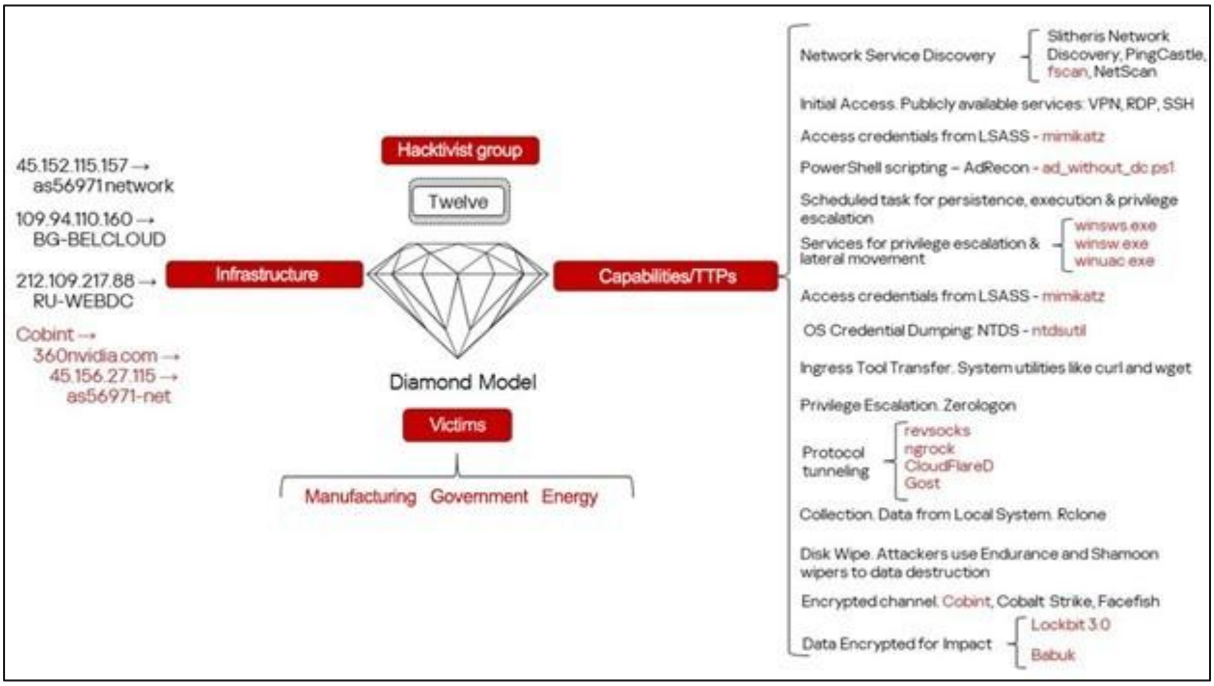
45.152.115.157 →
as56971network
109.94.110.160 →
BG-BELCLOUD
212.109.217.88 →
RU-WEBDC
Cobint →
360nvidia.com →
45.156.27.115 →
as56971-net
Infrastructure
Hacktivist group
Twelve
Diamond Model
Victims
Manufacturing
Government
Energy
Capabilities/TTPs
Network Service Discovery
Slitheris Network Discovery, PingCastle, fscan, NetScan
Initial Access. Publicly available services: VPN, RDP, SSH
Access credentials from LSASS - mimikatz
PowerShell scripting – AdRecon - ad_without_dc.ps1
Scheduled task for persistence, execution & privilege escalation
Services for privilege escalation & lateral movement
winsws.exe
winsw.exe
winuac.exe
Access credentials from LSASS - mimikatz
OS Credential Dumping: NTDS - ntdsutil
Ingress Tool Transfer. System utilities like curl and wget
Privilege Escalation. Zerologon
Protocol tunneling
revsocks
ngrock
CloudFlareD
Gost
Collection. Data from Local System. Rclone
Disk Wipe. Attackers use Endurance and Shamoon wipers to data destruction
Encrypted channel. Cobint, Cobalt Strike, Facefish
Data Encrypted for Impact
Lockbit 3.0
Babuk

Figure 2: Analysis of the Twelve techniques and tools

DETAILED EXPLANATION

Head Mare and Twelve have been active since at least September 2024, targeting state-owned and private entities in Russia. While Head Mare previously relied on a WinRAR vulnerability *(CVE-2023-38831)* to distribute malware and ransomware **(LockBit for Windows** and **Babuk for Linux/ESXi**), Twelve specializes in destructive attacks using wipers and encryption to make recovery impossible.

The latest attacks reveal Head Mare deploying two new tools:

- **CobInt** – A backdoor linked to ExCobalt and Crypt Ghouls, previously used against Russian firms.
- **PhantomJitter** – A custom implant enabling remote command execution on compromised servers.

These tools indicate tactical overlaps with Twelve and Crypt Ghouls, suggesting coordination among multiple groups targeting Russian infrastructure.

ATTACK TECHNIQUES & TOOLS

Initial Access & Persistence:

- Exploited Microsoft Exchange vulnerabilities, including ProxyLogon *(CVE-2021-26855),* to install CobInt.
- Phishing emails with malicious attachments.
- Trusted relationship attacks, infiltrating victims via compromised contractors.

Stealth & Defense Evasion:

- Created privileged local users instead of relying on scheduled tasks.
- Used fake OS file names (e.g., *calc.exe, winuac.exe*).
- Cleared event logs and used tunneling tools (*Gost, Cloudflared*) to evade detection.

Reconnaissance & Lateral Movement:

- quser.exe, tasklist.exe, netstat.exe for system discovery.
- fscan, SoftPerfect Network Scanner, and ADRecon for network reconnaissance.
- Mimikatz, secretsdump, and ProcDump for credential theft.
- RDP, PsExec, and smbexec for lateral movement.

Data Theft & Ransomware Deployment:

- Rclone for data exfiltration.
- LockBit 3.0 & Babuk ransomware deployed on compromised systems.
- Victims are instructed to contact attackers via Telegram for decryption.

The Head Mare-Twelve collaboration signals a strategic escalation in cyberattacks against Russian entities, blending espionage, financial extortion, and infrastructure destruction. With ransomware, credential theft, and destructive wipers, these groups pose a severe risk. Organizations must proactively monitor TTPs, strengthen defenses, and implement advanced threat detection to mitigate these emerging threats.

INDICATORS OF COMPROMISE (IOCs)

File name	Hashes
ADRecon.ps1	6008E6C3DEAA08FB420D5EFD469590C6
calc.exe, c.exe	09BCFE1CCF2E199A92281AADE0F01CAF
locker.exe	70C964B9AEAC25BC97055030A1CFB58A
mcdrive.vbs	87EECDCF34466A5945B475342ED6BCF2
mimikatz.exe	E930B05EFE23891D19BC354A4209BE3E
proxy.ps1	C21C5DD2C7FF2E4BADBED32D35C891E6
secretsdump.exe, secretsdump (1).exe	96EC8798BBA011D5BE952E0E6398795D
update.exe	D6B07E541563354DF9E57FC78014A1DC
IP Addresses	
45.87.246[.]34	45.156.27[.]115
185.229.9[.]27	45.156.21[.]148
185.158.248[.]107	64.7.198[.]109
Domains	
360nvidia[.]com	web-telegram[.]uk

RECOMMENDATIONS

Organizations should implement the following security measures:

- Apply updates for WinRAR, Microsoft Exchange, and other exploited software to close attack entry points.
- Block phishing attempts with advanced filtering and endpoint protection.
- Investigate the creation of privileged local users on critical servers.
- Prevent unauthorized lateral movement and restrict access to sensitive systems.
- Enable detailed event logging, monitor for tools like Rclone, PsExec, and Mimikatz, and review unexpected C2 communications.

ADDITIONAL RESOURCES

https://thehackernews.com/2025/03/kaspersky-links-head-mare-to-twelve.html

https://securelist.com/head-mare-twelve-collaboration/115887/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com