Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

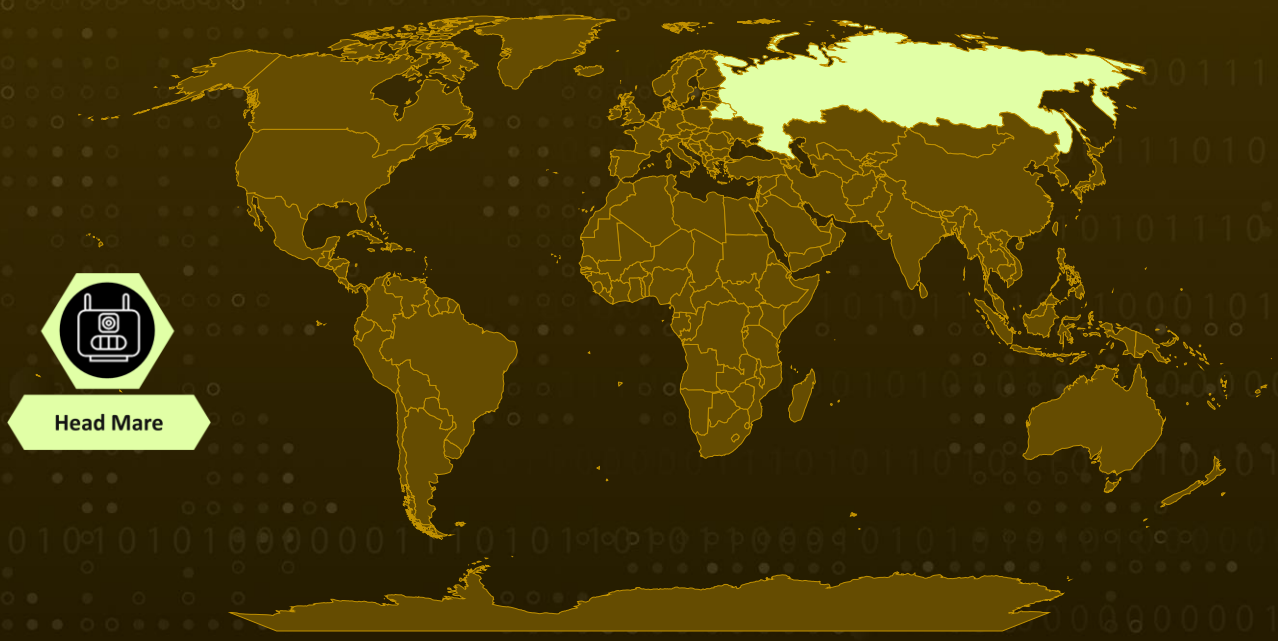
Hacktivism in Action the Case of Head Mare Campaigns

Date of Publication	Admiralty Code	TA Number
September 19, 2024	A1	TA2024361

Summary

First Seen: 2023
Threat Actor: Head Mare
Malware: PhantomDL, PhantomCore, LockBit ransomware, Babuk ransomware
Targeted Countries: Russia and Belarus
Targeted Industries: Government, Transportation, Energy, Manufacturing, Entertainment
Attack: Head Mare, a hacktivist group that emerged in 2023, gained notoriety through its public account on the social media platform X. Known for exposing sensitive information from victims, the group specifically targets companies in Russia and Belarus, employing timely attack techniques such as phishing and ransomware.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-38831	RARLAB WinRAR Code Execution Vulnerability	WinRAR version 6.22 and older versions	✓	✓	✓

Attack Details

#1 Head Mare, a hacktivist group that surfaced in 2023, gained recognition through its public account on the social network X. The group has exposed sensitive information about its victims, including organization names, stolen internal documents, and screenshots of compromised desktops and administrative consoles.

#2 Head Mare focuses on targeting organizations in Russia and Belarus, using contemporary techniques to gain initial access. Notably, they carry out sophisticated phishing campaigns that distribute RAR archives exploiting the CVE-2023-38831 vulnerability in WinRAR.

#3 Their malware toolkit includes PhantomDL, a Go-based backdoor used for delivering additional payloads and exfiltrating files to a command-and-control (C2) server. Another tool in their arsenal, PhantomCore (also known as PhantomRAT), serves as the predecessor to PhantomDL.

#4 In addition, the group deploys ransomware to encrypt victim devices, utilizing LockBit for Windows systems and Babuk for Linux ESXi environments. They demand ransom payments in exchange for decryption keys. Head Mare's activities appear to be part of a larger strategy to destabilize the political and economic landscape of Russia and Belarus through cyberattacks, further escalating existing geopolitical tensions.

Recommendations

Targeted Vulnerability Scanning and Patching: Regularly scan for vulnerabilities that could be exploited by hacktivist groups like Head Mare, particularly focusing on CVE-2023-38831 and similar vulnerabilities. Prioritize the timely application of patches to minimize exposure to exploitation tactics used by Head Mare.

Utilize Application Control: Implement application whitelisting to ensure that only approved applications can run on your systems, preventing unauthorized or malicious executables, such as backdoors, from executing. Additionally, deploy application control solutions that analyze application behavior to detect and block unusual or unauthorized activities.

Network Traffic Analysis: Use deep packet inspection (DPI) to examine the contents of network traffic and detect hidden or encrypted data channels that malware might use for command-and-control communication. Additionally, implement anomaly-based detection systems to identify unusual network traffic patterns that could indicate backdoor activity.

Enhanced Backup Strategies Against Ransomware: Maintain encrypted backups in isolated locations to defend against ransomware attacks that Head Mare may deploy. Ensure backups are tested frequently for restoration efficacy, especially against attacks targeting critical data.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0010** Exfiltration	**TA0011** Command and Control
TA0040 Impact	**T1012** Query Registry	**T1105** Ingress Tool Transfer	**T1497.001** System Checks
T1566 Phishing	**T1203** Exploitation for Client Execution	**T1071** Application Layer Protocol	**T1219** Remote Access Software
T1486 Data Encrypted for Impact	**T1003** OS Credential Dumping	**T1562** Impair Defenses	**T1543** Create or Modify System Process
T1571 Non-Standard Port	**T1059.003** Windows Command Shell	**T1059** Command and Scripting Interpreter	**T1497** Virtualization/Sandbox Evasion
T1041 Exfiltration Over C2 Channel			

Indicators of Compromise (IOCs)

TYPE	VALUE
File Path	C:\Windows\system32\SrvLog.exe, C:\Users\<user>\AppData\Local\microsoft\windows\srvhosts.exe, C:\Users\<user>\AppData\Roaming\microsoft\windows\srvhostt.exe, C:\windows\srvhost.exe, C:\Users\<user>\appdata\roaming\microsoft\windows\srvhost.exe, C:\ProgramData\OneDrive.exe, $appdata\Microsoft\Windows\srvhostt.exe, $appdata\Microsoft\Windows\srvhost.exe, C:\Users\User\AppData\Local\microsoft\windows\srvhosts.exe, C:\ProgramData\update\XenAllPasswordPro.exe, C:\ProgramData\update\report.html, $user\desktop\rsockstun.exe, C:\ProgramData\resolver.exe, $user\desktop\lockbitlite.exe, $user\desktop\lb3.exe, C:\ProgramData\lock.exe, $user\desktop\x64\mimikatz.exe, C:\Users\User\Documents\srvhost.exe, C:\microsoft\windows\srchost.exe
IPv4	188[.]127[.]237[.]46, 45[.]87[.]246[.]169, 45[.]87[.]245[.]30, 185[.]80[.]91[.]107, 91[.]219[.]151[.]47, 5[.]252[.]176[.]47, 5[.]252[.]176[.]77, 45[.]11[.]27[.]232, 5[.]252[.]178[.]92, 188[.]127[.]227[.]201
URLs	188[.]127[.]237[.]46/winlog[.]exe, 188[.]127[.]237[.]46/servicedll[.]exe, 194[.]87[.]210[.]134/gringo/splhost[.]exe, 194[.]87[.]210[.]134/gringo/srvhost[.]exe, 94[.]131[.]113[.]79/splhost[.]exe, 94[.]131[.]113[.]79/resolver[.]exe, 45[.]156[.]21[.]178/dlldriver[.]exe, 5[.]252[.]176[.]77/ngrok[.]exe, 5[.]252[.]176[.]77/sherlock[.]ps1, 5[.]252[.]176[.]77/sysm[.]elf, 5[.]252[.]176[.]77/servicedll[.]rar, 5[.]252[.]176[.]77/reverse[.]exe,

TYPE	VALUE
URLs	5[.]252[.]176[.]77/soft_knitting[.]exe, 5[.]252[.]176[.]77/legislative_cousin[.]exe, 5[.]252[.]176[.]77/2000×2000[.]php, hxxps[:]//x[.]com/head_mare
MD5	15333d5315202ea428de43655b598eda, a2bd0b9b64fbdb13537a4a4a1f3051c0, 16f97ec7e116fe3272709927ab07844e, 855b1cba23fb51da5a8f34f11c149538, 55239cc43ba49947bb1e1178fb0e9748, 0e14852853f54023807c999b4ff55f64, 99b0f80e9ae2f1fb15bfe5f068440ab8, 1d2d6e2d30933743b941f63e767957fb, 76b23dd72a883d8b1302bb4a514b7967, 6ddc56e77f57a069539dcc7f97064983, 7acc6093d1bc18866cdd3feccb6da26a, 59242b7291a77ce3e59d715906046148, 6568ab1c62e61237baf4a4b09c16bb86, f7abdaae63bf59ca468124c48257f752, 79d871ff25d9d8a1f50b998b28ff752d, 78cc508882aba99425e4d5a470371cb1
SHA1	b6212da07dc3a4f39a33bc0f0242c86a0f4433e6, 69383141c5270ca8876674026c0a228011bb5d7d, 9ab4d91d3db34431f451106ede4f0ed5b163ce94, 0695028a13d35aa60732b6f5069b9907d6987576, 17f6119755f80fb0308bb9aaa77b6706e5649edc, 508b88a1cdc936be6da3d58a7ea6c82b491956ee, a27c67cec10295f27c660e25ee00648d77300a01, f3e489cf30036bce1e07a6c5bca23df6c7f469d6, 338e19e8a3615c29d8a825ebba66cf55fa0caa2c, 8fee139dc37447f2f221b0858734a88ff8eafc05, 41e19260552d038009f0835e7a19ddecaca8ae34, 3af0cb27b6a509c34bb4485fd64a0e777e9aace2, 3a8120cfd574e6eecc15aec2fa3fa1e50e98e1a7, b9ca6711d007d1b6f0ef8bd262987fad96595968, 7bcb6cb60fc08c8cf446e7b631e524a00f924fc3, 1da019570a4af615eba5d6ca85fa5ed392503450
SHA256	201f8dd57bce6fd70a0e1242b07a17f489c5f873278475af2eaf82a751c24fa8, 582c4674ba4880f0e5dec38917e970f906ac18205499de67b076d8fb17c0dd22, 5d924a9ab2774120c4d45a386272287997fd7e6708be47fb93a4cad271f32a03, 0060c80acddb1801830b50ec87c1f66e3d00fbc9e83ea732b83ffb871217406f,

TYPE	VALUE
SHA256	5a3c5c165d0070304fe2d2a5371f5f6fdd1b5c964ea4f9d41a672382991499c9, 5192a92730e5eee19dea67ba65ec4ed8eaab4314b389faa44ea051290a4b4a66, 22eb1e647e4c5f7f0d0dcc45af02d5ac44e270ed067ca1eed504692f80014bc6, 1fe97e87d00f0141449bfb3e50e2749d5c2519923bd50b9c586d7e95089698f6, 311edf744c2e90d7bfc550c893478f43d1d7977694d5dcecf219795f3eb99b86, da2191203b39fda0823520a85a9ca0bb8c42c4ef5b341a929d69dfd99e971d7d, d10996d627adec7ae4cfd25a23b034387db98de569da9f7795520c0c49944698, 9c62569f840151c89e776f57669f74ccbcaa29fa7f644653084117aee76b1d53, 2d3db0ff10edd28ee75b7cf39fcf42e9dd51a6867eb5962e8dc1a51d6a5bac50, 072be899f5a9892c39250aae8a6fd89c480c02135ed0a85e0d7a181577e67454, 0edd5b8945061d801ecb60a852dcecdd507e839c23f7c93036c244c754b93459, 5fb9263c435c494b7e5b25da3d772ce62945e0efbd4d2bb64529c75b9dd1e47c, 9f5b780c3bd739920716397547a8c0e152f51976229836e7442cf7f83acfdc69, 08dc76d561ba2f707da534c455495a13b52f65427636c771d445de9b10293470, 6a889f52af3d94e3f340afe63615af4176ab9b0b248490274b10f96ba4edb263, 33786d781d9c492e17c56dc5fae5350b94e9722830d697c3cbd74098ea891e5a, 9b005340e716c6812a12396bcd4624b8cfb06835f88479fa6cfde6861015c9e0, dc3e4a549e3b95614dee580f73a63d75272d0fba8ca1ad6e93d99e44b9f95caa, 053ba35452ee2ea5dca9df9e337a3f307374462077a731e53e6cc62eb82517bd, 2f9b3c29abd674ed8c3411268c35e96b4f5a30fabe1ae2e8765a82291db8f921, 015a6855e016e07ee1525bfb6510050443ad5482039143f4986c0e2ab8638343, 9d056138cfb8ff80b0aa53f187d5a576705bd7954d36066ebbbf34a44326c546, 22898920df011f48f81e27546fece06a4d84bce9cde9f8099aa6a067513191f3,

TYPE	VALUE
SHA256	2f1ee997a75f17303acc1d5a796c26f939eb63871271f0ad9761cdbd592e7569, af5a650bf2b3a211c39dcdcab5f6a5e0f3af72e25252e6c0a66595f4b4377f0f, 9e9fabba5790d4843d2e5b027ba7af148b9f6e7fcde3fb6bddc661dba9ccb836, b8447ef3f429dae0ac69c38c18e8bdbfd82170e396200579b6b0eff4c8b9a984, 92804faaab2175dc501d73e814663058c78c0a042675a8937266357bcfb96c50, 664b68f2d9f553cc1acfb370bcfa2ccf5de78a11697365cf8646704646e89a38, 4c218953296131d0a8e67d70aeea8fa5ae04fd52f43f8f917145f2ee19f30271, dc47d49d63737d12d92fbc74907cd3277739c6c4f00aaa7c7eb561e7342ed65e, eda18761f3f6822c13cd7beae5af2ed77a9b4f1dc7a71df6ab715e7949b8c78b

Patch Details

Upgrading to WinRAR version 6.23 or later is highly recommended.

References

https://securelist.com/head-mare-hacktivists/113555/

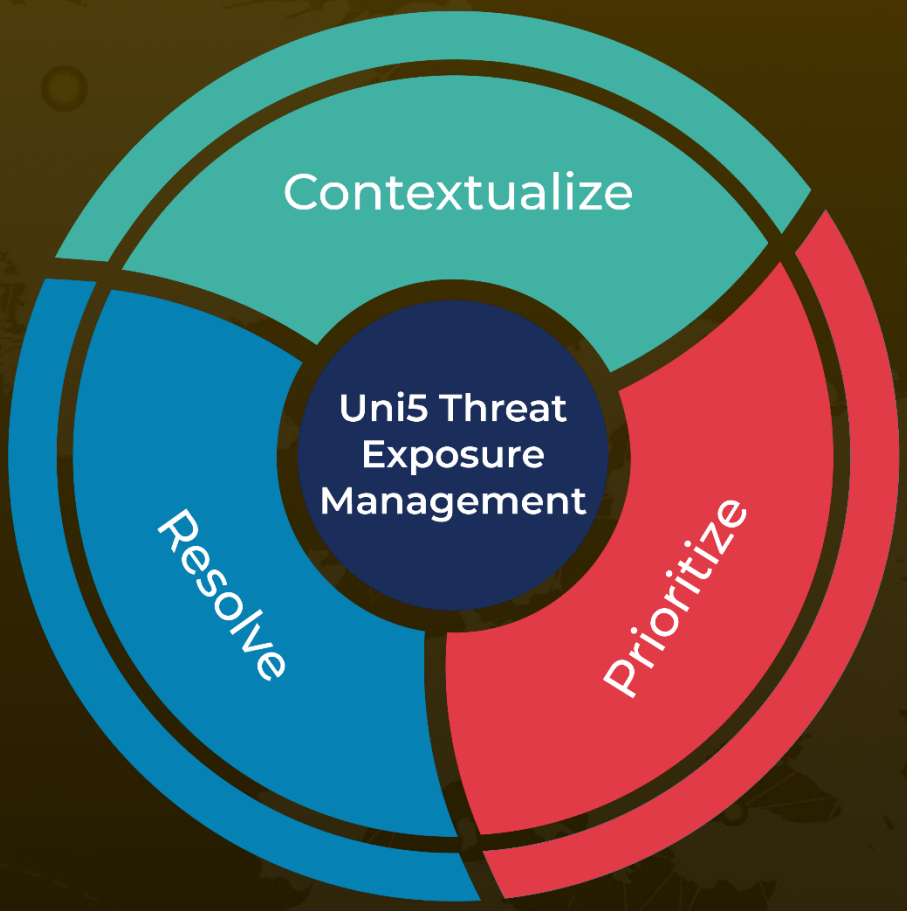
https://cyble.com/blog/the-rise-of-head-mare-a-geopolitical-and-cybersecurity-analysis/

https://hivepro.com/threat-advisory/winrar-zero-day-exploit-targeting-traders-since-april/

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

September 19, 2024 • 3:00 AM

More at www.hivepro.com