Head Mare: adventures of a unicorn in Russia and Belarus

By Kaspersky

Published: 2024-09-02 · Archived: 2026-04-02 11:16:36 UTC

Head Mare is a hacktivist group that first made itself known in 2023 on the social network X (formerly Twitter)[1]. In their public posts, the attackers reveal information about some of their victims, including organization names, internal documents stolen during attacks, and screenshots of desktops and administrative consoles.

By analyzing incidents in Russian companies, we identified how Head Mare conducts its attacks, the tools it uses, and established the group's connection with the PhantomDL malware (article in Russian).

Key findings

- Head Mare exclusively targets companies in Russia and Belarus.
- For initial access, the group conducts various phishing campaigns distributing RAR archives that exploit the CVE-2023-38831 vulnerability in WinRAR.
- Some of the discovered tools overlap with previously investigated groups attacking Russian organizations.
- The group encrypts victims' devices using two ransomware families: LockBit for Windows and Babuk for Linux (ESXi).

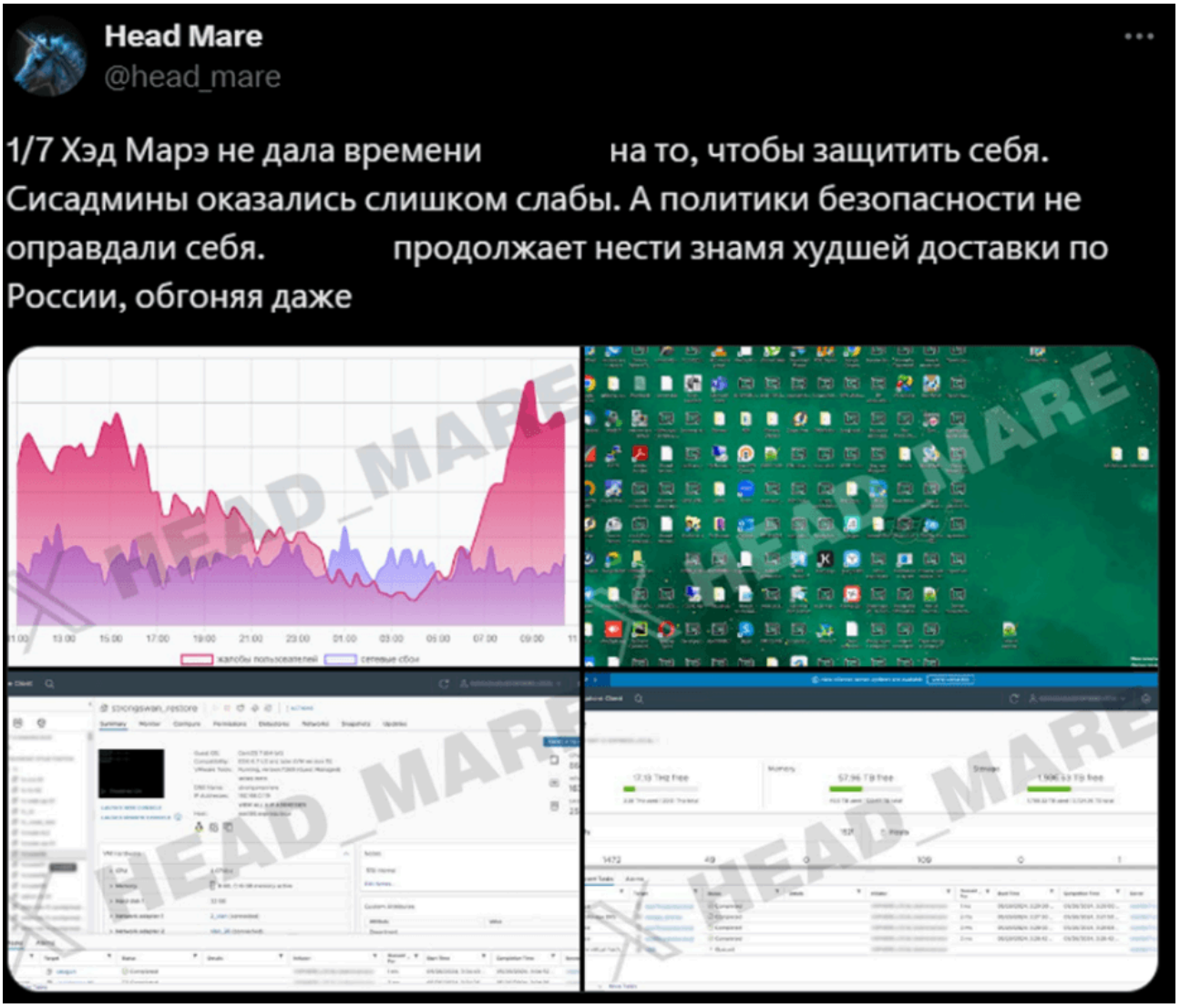
Technical details

Historical context

Since the beginning of the Russo-Ukrainian conflict, we've seen the emergence of numerous hacktivist groups whose main goal is often not financial gain but causing as much damage as possible to companies on the opposing side of the conflict. Head Mare is one such group, exclusively targeting organizations located in Russia and Belarus. This is confirmed by open-source information and telemetry from the Kaspersky Security Network – a system for collecting anonymized threat data voluntarily provided by users of our solutions.

Hacktivist groups attacking Russian organizations in the context of the Russo-Ukrainian conflict use similar techniques and tools and, when analyzed using the Unified Kill Chain method, generally resemble one another. However, unlike other similar groups, Head Mare uses more up-to-date methods for obtaining initial access. For instance, the attackers took advantage of the relatively recent CVE-2023-38831 vulnerability in WinRAR, which allows the attacker to execute arbitrary code on the system via a specially prepared archive. This approach allows the group to deliver and disguise the malicious payload more effectively.

Like most hacktivist groups, Head Mare maintains a public account on the social network X, where they post information about some of their victims. Below is an example of one of their posts:



Head Mare post on X

At the time of carrying out the study, the group has claimed nine victims from various industries:

- Government institutions;
- Transportation;
- Energy;
- Manufacturing;
- Entertainment.

The ultimate goal of the attackers is likely to cause maximum damage to companies in Russia and Belarus. However, unlike some other hacktivist groups, Head Mare also demands a ransom for data decryption.

Head Mare's toolkit

In their attacks, Head Mare mainly uses publicly available software, which is typical of most hacktivist groups targeting Russian companies in the context of the Russo-Ukrainian conflict. However, while some hacktivists

have no proprietary developments in their toolkit at all, Head Mare uses their custom malware PhantomDL and PhantomCore in phishing emails for initial access and exploitation.

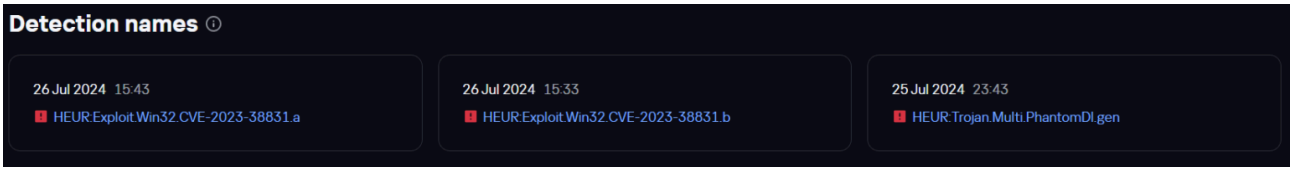
Below is a list of software discovered in Head Mare attacks:

- LockBit ransomware;
- Babuk ransomware;
- PhantomDL;
- PhantomCore;
- Sliver;
- ngrok;
- rsockstun;
- XenAllPasswordPro;
- Mimikatz.

Most of these tools are available on the internet, be it LockBit samples generated using the publicly available builder leaked in 2022, or the Mimikatz utility, whose code is available on GitHub.

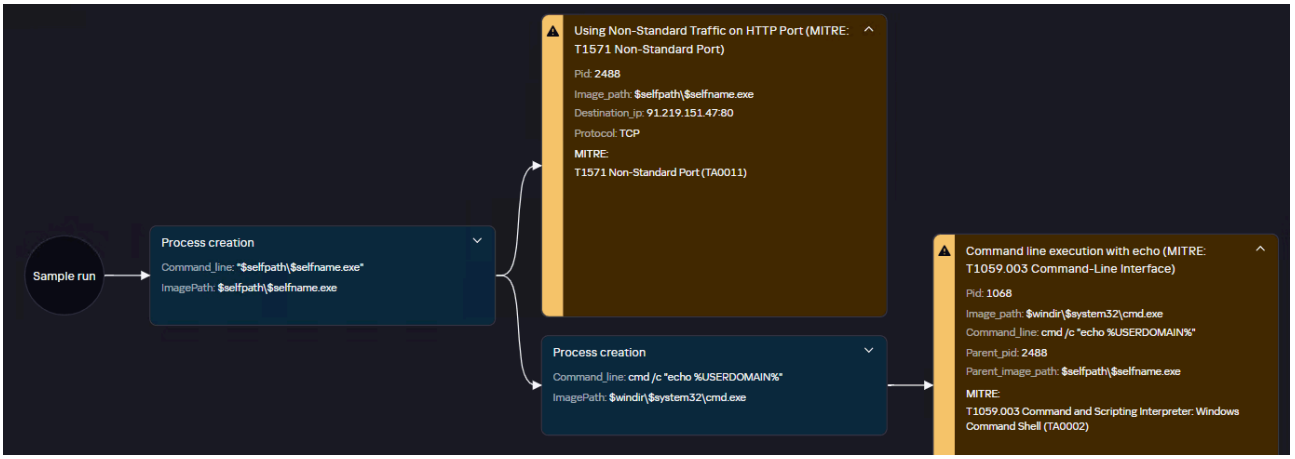
Initial access

During our investigation of Head Mare's activities, we discovered that this group is associated with targeted attacks on Russian organizations using malicious PhantomDL and PhantomCore samples. The detected samples were distributed in various phishing campaigns in archives with decoy documents of the same name. The malicious archives exploit the CVE-2023-38831 vulnerability in WinRAR. If the user attempts to open the legitimate-seeming document, they trigger the execution of the malicious file. The same sample could be distributed in different archives with decoy documents on various topics.



Verdicts with which our products detect PhantomDL samples: the malware is recognized, among other things, as an exploit for CVE-2023-38831

After execution, PhantomDL and PhantomCore establish communication with one of the attackers' command servers and attempt to identify the domain to which the infected host belongs. Below are the results of dynamic analysis of several samples in Kaspersky Sandbox (detonation graphs), reflecting the malware's behavior immediately after launch.

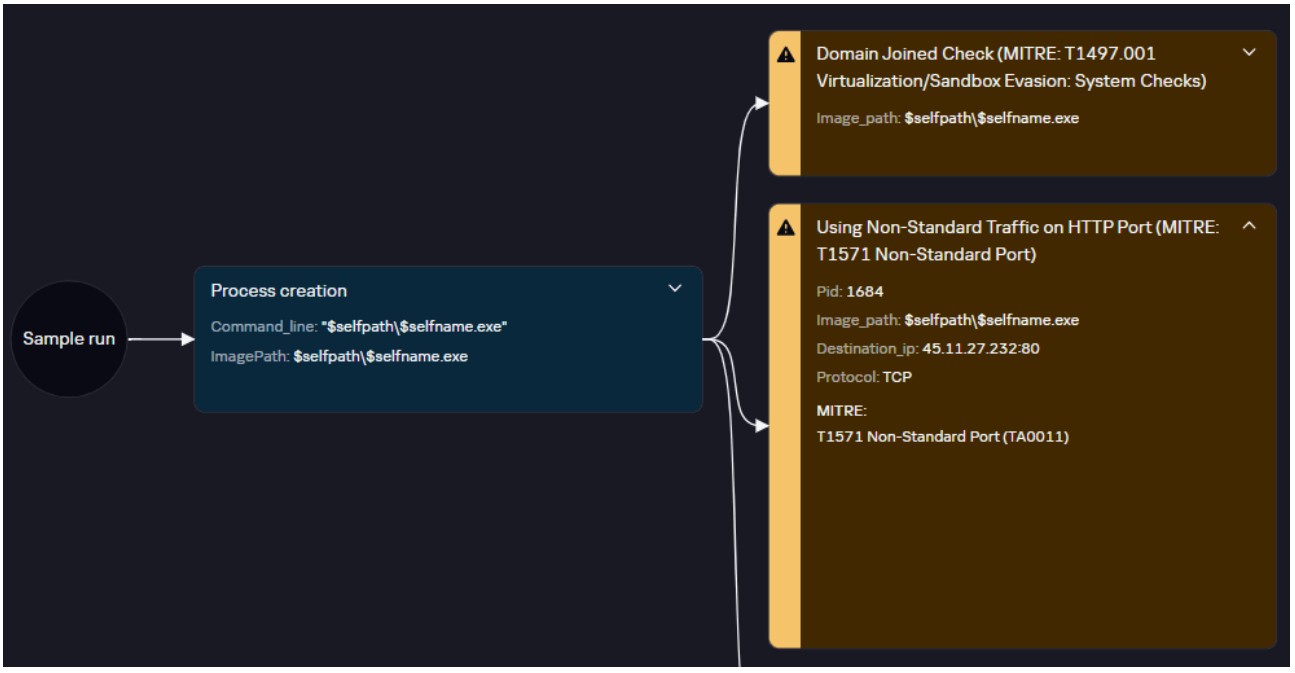


Detonation graph of a PhantomDL sample reflecting its behavior in Kaspersky Sandbox

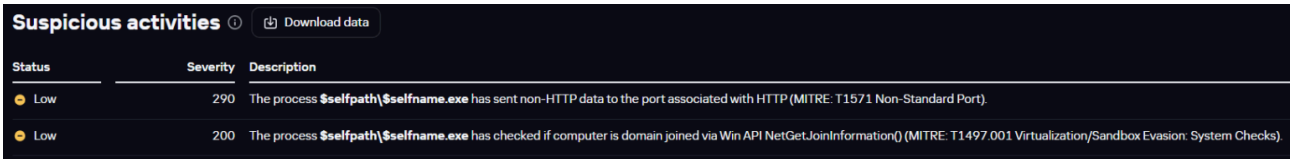
In the image above, the PhantomDL sample connects to the C2 server 91.219.151[.]47 through port 80 and performs domain identification using the command cmd.exe /c "echo %USERDOMAIN%".

PhantomDL communication with C2

The PhantomCore sample establishes a connection with another C2 (45.11.27[.]232) and checks the host's domain using the WinAPI function NetGetJoinInformation.

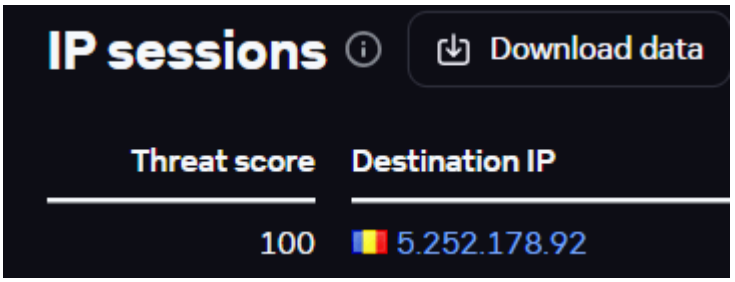


PhantomCore sample detonation in Kaspersky Sandbox



Suspicious activity of the PhantomCore sample

Another PhantomCore sample, after execution, establishes a connection with C2 5.252.178[.]92:



PhantomCore C2 connection

During our research, we also found several PhantomDL and PhantomCore samples, which we cannot attribute with complete certainty to the same cluster of activity as the samples found in Head Mare's attacks. Information about these samples can be found in the section "Samples similar to Head Mare's toolkit".

Persistence in the system

The attackers used several methods to persist in the system. For example, in one incident, they added a PhantomCore sample to the Run registry key. After execution, the sample automatically established a connection with the attackers' C2 5.252.176[.]47:

PhantomCore C2 connection

We observed the following commands adding a value to the Run registry key:

Command	Description

cmd /c “cd /d $selfpath\ && reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v \”MicrosoftUpdateCoree\” /t REG_SZ /d \”$selfpath\$selfname.exe\ /f”	Adding a value to the Run registry key named MicrosoftUpdateCoree with content $appdata\Microsoft\Windows\srvhostt.exe (PhantomCore) with the /f parameter (no confirmation prompt)
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v \”MicrosoftUpdateCoree\” /t REG_SZ /d \”$appdata\Microsoft\Windows\srvhostt.exe\” /f	
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v \”MicrosoftUpdateCore\” /t REG_SZ /d \”$appdata\Microsoft\Windows\srvhost.exe\” /f	A similar method of adding to the registry key, but the value is named MicrosoftUpdateCore

In some other cases, the attackers created scheduled tasks to persist in the victim’s system. The following tasks were used to launch a PhantomCore sample:

Command	**Description**
schtasks /create /tn \”MicrosoftUpdateCore\” /tr \”$appdata\Microsoft\Windows\srvhost.exe\” /sc ONLOGON	Creates a scheduled task named MicrosoftUpdateCore that launches $appdata\Microsoft\Windows\srvhost.exe (PhantomCore) each time the user logs in
schtasks /create /tn “MicrosoftUpdateCore” /tr “$appdata\Microsoft\Windows\srvhost.exe” /sc ONLOGON /ru “SYSTEM”	A similar method of creating a scheduled task, but in this case, the task runs with SYSTEM privileges

Detection evasion

As mentioned in the previous section, the attackers create scheduled tasks and registry values named MicrosoftUpdateCore and MicrosoftUpdateCoree to disguise their activity as tasks related to Microsoft software.

We also found that some LockBit samples used by the group had the following names:

- OneDrive.exe;
- VLC.exe.

These samples were located in the C:\ProgramData directory, disguising themselves as legitimate OneDrive and VLC applications.

In general, many of the tools used by Head Mare had names typical of legitimate programs and were located in standard paths or lookalikes:

Software	Path
Sliver	C:\Windows\system32\SrvLog.exe
rsockstun	c:\Users\<user>\AppData\Local\microsoft\windows\srvhosts.exe
	c:\Users\<user>\AppData\Roaming\microsoft\windows\srvhostt.exe
Phantom	c:\windows\srvhost.exe
	c:\Users\<user>\appdata\roaming\microsoft\windows\srvhost.exe
LockBit	c:\ProgramData\OneDrive.exe

As can be seen in the table, the attackers primarily attempted to disguise their samples as legitimate svchost.exe files in the C:\Windows\System32 directory.

The attackers also used disguise tactics in their phishing campaigns – samples of PhantomDL and PhantomCore were named to resemble business documents and had double extensions. Here are some examples we encountered:

- Счет-Фактура.pdf .exe
- договор_ №367кх_от_29.04.2024_и_доп_соглашение_ртсс 022_контракт.pdf .exe
- решение №201-5_10вэ_001-24 к пив экран-сои-2.pdf .exe
- тз на разработку.pdf .exe
- исходящее письмо от 29.04.2024 n 10677-020-2024.pdf .exe
- возврат средств реквизиты.pdf .exe

Additionally, all the samples of PhantomDL and PhantomCore we found were obfuscated, possibly using a popular obfuscator for Go called Garble.

Management and infrastructure

During our research, we discovered that the main C2 framework used by the attackers is Sliver, an open-source C2 framework designed for simulating cyberattacks and pentesting. Such frameworks are used to manage compromised systems after initial access, allowing attackers (or pentesters) to execute commands, gather data, and manage connections.

Sliver’s architecture includes an agent (implant) installed on compromised devices to execute commands from the server, a server for managing agents and coordinating their actions, and a client in the form of a command-line interface (CLI) for operator-server interaction. Sliver’s core functionality includes managing agents, executing commands via a command shell, creating tunnels to bypass network restrictions, and automating routine tasks with built-in scripts.

The Sliver implant samples we found had default configurations and were created using the following command:

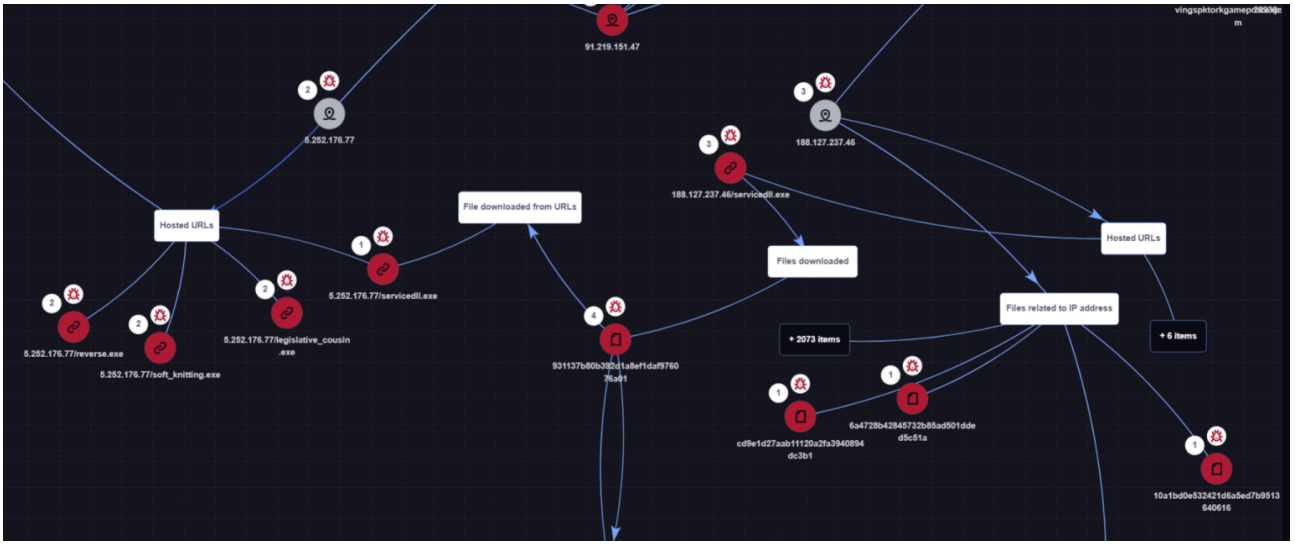
	generate --http [IP] --os windows --arch amd64 --format exe

To disguise the implants, the attackers used the popular Garble tool, which is available on GitHub.

The attackers also frequently used VPS/VDS servers as C2 servers. Below is a list of servers we observed in attacks:

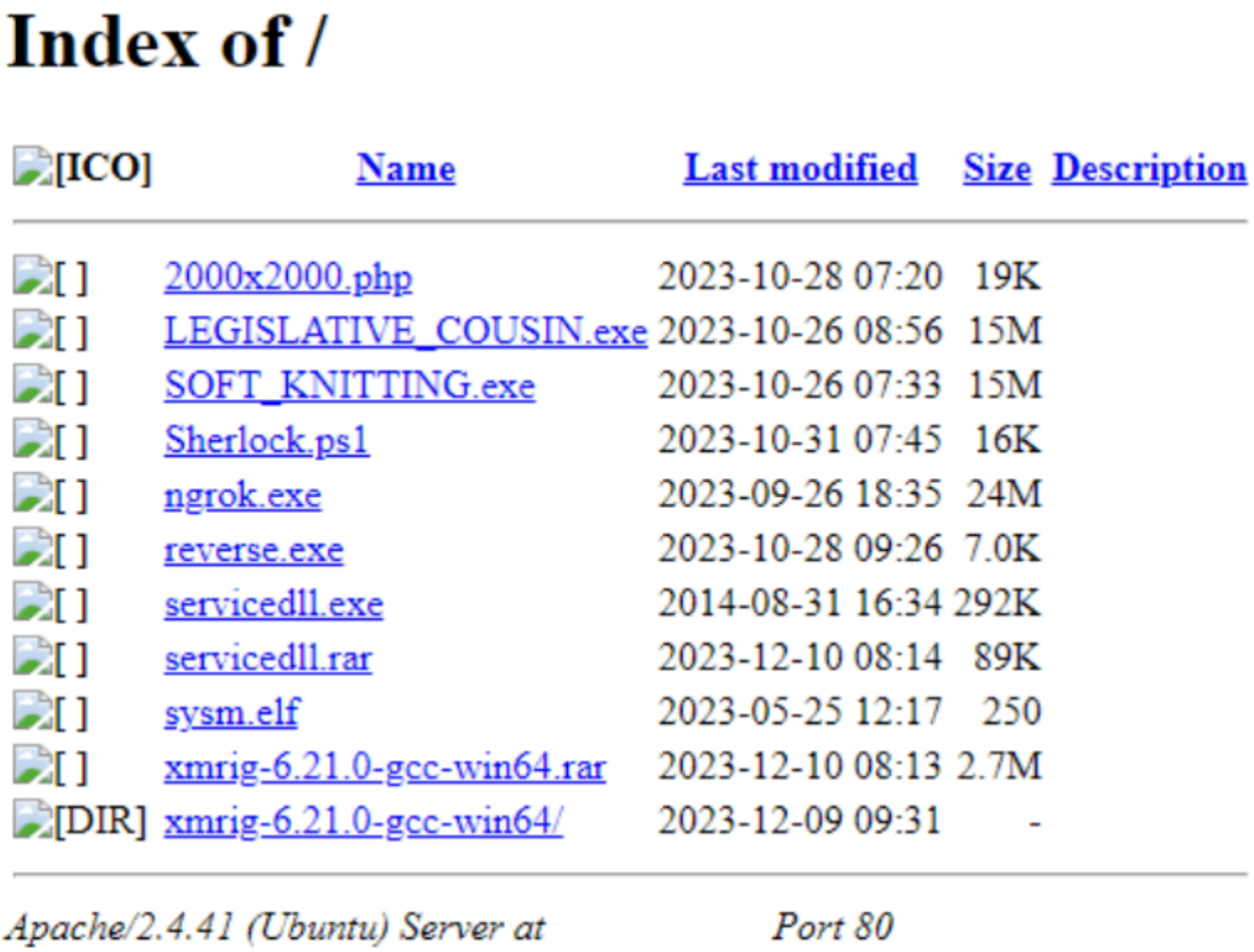
IP	First detection	ASN
188.127.237[.]46	March 31, 2022	56694
45.87.246[.]169	June 26, 2024	212165
45.87.245[.]30	–	57494
185.80.91[.]107	July 10, 2024	212165
91.219.151[.]47	May 02, 2024	56694
5.252.176[.]47	–	39798
5.252.176[.]77	October 29, 2023	39798

Various utilities used at different stages of the attacks were found on the attackers' C2 servers. The same utilities often appeared on different servers with identical file names.



Analysis of Head Mare's C2 infrastructure

Below is a list of tools found on one of the attackers' command servers:



Contents of one of the C2 server directories

Utility name	Description
2000×2000.php	PHP shell for executing commands on the server. This shell is called p0wny@shell:~# and is available on GitHub at hxxps://github[.]com/flozz/p0wny-shell.
LEGISLATIVE_COUSIN.exe	Sliver implant. Connects to 5.252.176[.]77:8888.
SOFT_KNITTING.exe	
sherlock.ps1	PowerShell script for quickly finding vulnerabilities for local privilege escalation, available on GitHub at hxxps://github[.]com/rasta-mouse/Sherlock/tree/master.
ngrok.exe	ngrok utility.
reverse.exe	Meterpreter. Connects to 5.252.176[.]77:45098.
servicedll.exe	nssm utility for managing services.

sysm.elf	Unix reverse shell using the sys_connect function to connect to the attacker's C2. If the connection attempt fails, the program enters sleep mode for 5 seconds using the sys_nanosleep function before trying again. Connects to 5.252.176[.]77:45098.
Xmrig*	XMRig miner. Not used in any attacks known to us.

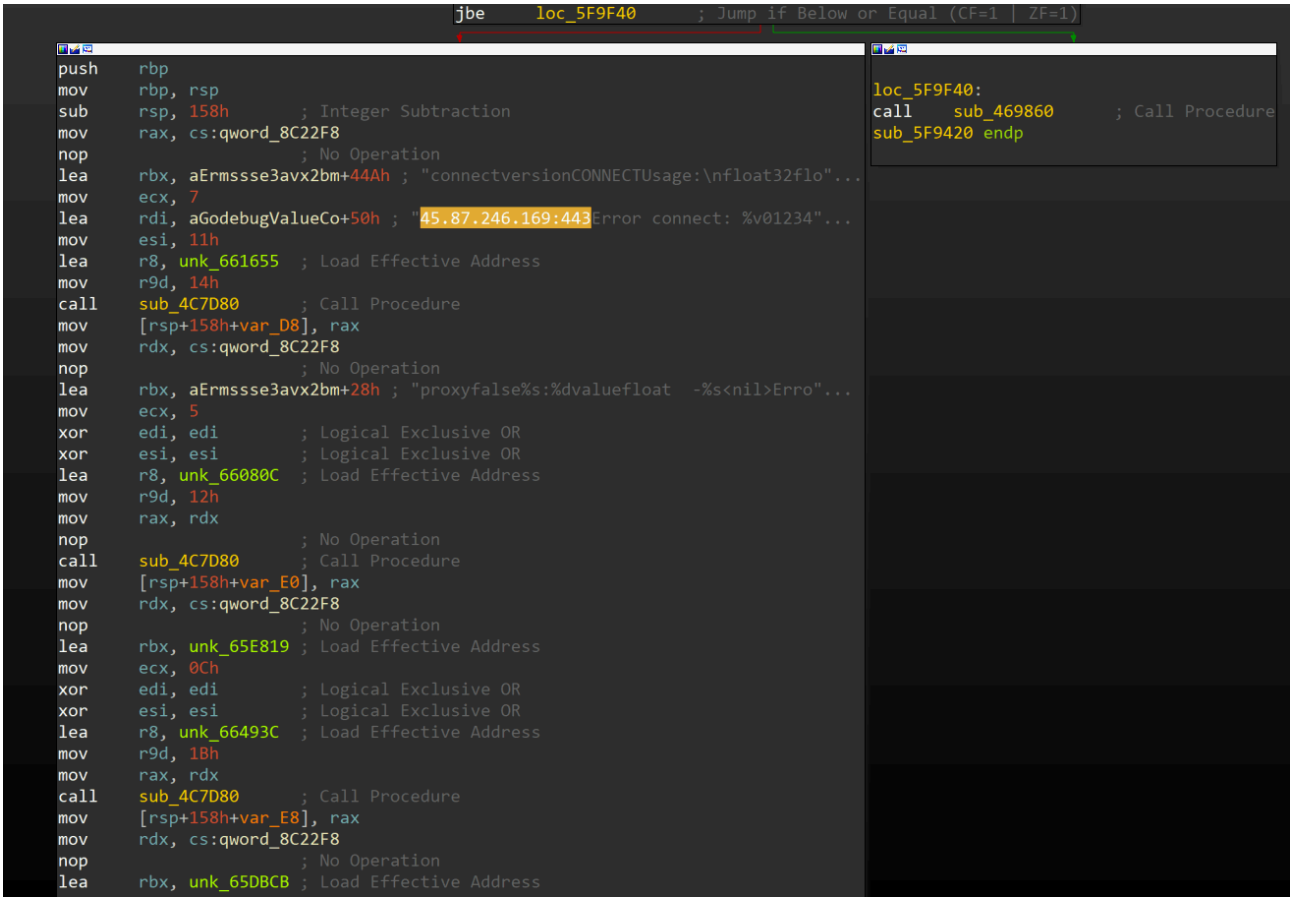
Pivoting

Pivoting is a set of methods that allow an attacker to gain access to private network segments using compromised machines as intermediate nodes. For this purpose, the attackers use the ngrok and rsockstun utilities.

The rsockstun utility creates a reverse SOCKS5 tunnel with SSL and proxy server support. It allows a client behind a NAT or firewall to connect to a server via a secure connection and use SOCKS5 to forward traffic.

We analyzed the utility's code and identified its key functions:

Client	**Server**
ConnectViaProxy function: • Establishes a connection with the server through a proxy. • Supports NTLM authentication for proxy servers. • Creates and sends requests to the proxy server and processes responses. **ConnectForSocks function:** • Establishes a connection with the server via SOCKS5. • Establishes an SSL connection to the server. • Authenticates using a password. • Creates a Yamux session for multiplexing connections.	**listenForSocks function:** • Waits for client connections via SSL. • Verifies the existence and correctness of the connection password. • Creates a Yamux client session. **listenForClients function:** • Waits for local client connections. • Opens a Yamux stream and forwards traffic between the local client and the remote server.



Fragment of rsockstun code containing one of the Head Mare C2 addresses

Ngrok is a cross-platform utility designed to create secure tunnels to local web servers over the internet. It allows quick and easy access to local services and applications by providing public URLs that can be used to access the server externally.

Network exploration

After successfully gaining a foothold on the initial node, attackers execute a series of commands to further explore the node, domain, and network environment:

Command	Description
cmd /c “echo %USERDOMAIN%”	Retrieve the victim’s domain name
arp -a	Retrieve the ARP cache for all network interfaces on the compromised system
“cmd /c “cd /d $selfpath && whoami	Gather information about the current user’s name and domain
cmd /c “cd /d $appdata && powershell Get-ScheduledTask -TaskName “WindowsCore”	Search for a scheduled task named WindowsCore

Credential harvesting

To collect credentials, attackers use the mimikatz utility.

In addition, to obtain additional credentials from the system, attackers use the console version of the XenArmor All-In-One Password Recovery Pro3 utility (XenAllPasswordPro), which can extract user credentials from registry hives.

```
"c:\ProgramData\update\XenAllPasswordPro.exe" -a

"c:\ProgramData\update\report.html"
```

End goal: file encryption

While studying Head Mare attacks, we discovered the use of two ransomware families:

- LockBit for Windows;
- Babuk for ESXi.

Babuk

The Babuk variant we discovered is a 64-bit build for ESXi, created using a publicly available configurator. The Trojan uses standard encryption algorithms for Babuk builds for ESXi – X25519 + SHA256 + Sosemanuk, as well as the standard extension for encrypted files, *.babyk.

MD5	Top similar	Type
11f513086de8fc80dcaddfef5b312c29	Babuk_Locker (86%) 4+	Original file
0a8783aec1c0572698575df1e5c421b9	Babuk_Locker (86%) 4+	Memory dump
0a8783aec1c0572698575df1e5c421b9	Babuk_Locker (86%) 4+	Memory dump

Kaspersky Threat Attribution Engine results for the found Babuk samples

The distinctive features of the discovered Trojan are:

- Ability to log its activities in /tmp/locker.log.
- Ability to destroy running virtual machines, the list of which is taken from the vm-list.txt file. This file is populated when the esxcli vm process listd command is called.

The Babuk sample we found encrypts files with the following extensions:

.vmdk	.vmem	.vswp
.vmsn	.bak	.vhdx

After encryption is complete, it leaves a ransom note. Below is an example of the note, which contains a unique identifier for the Session messenger and the message “Message us for decryption ^_^.”

Babuk sample ransom note

LockBit

The LockBit builds we found in Head Mare attacks are identical to samples generated by the publicly available LockBit builder, which was leaked online in 2022. The attackers distributed LockBit under the following names:

- lb3.exe
- lock.exe
- OneDrive.exe
- lockbithard.exe
- lockbitlite.exe
- phdays.exe
- l.exe
- VLC.exe

The ransomware was located in the following paths:

- c:\Users\User\Desktop;
- c:\ProgramData\.

The attackers used two of these ransomware versions sequentially – lockbitlite.exe and then lockbithard.exe. First, they encrypted files using LockbitLite, and then additionally encrypted the output with the LockbitHard variant.

The configuration of these variants differed slightly.

LockbitLite	**LockbitHard**
“encrypt_filename”: false,	“encrypt_filename”: true,
“wipe_freespace”: false,	“wipe_freespace”: true,

“white_folders”: “$recycle.bin;config.msi;$windows.~bt;$windows.~ws;windows;boot”,	“white_folders”: “”,

Examples of the notes from both samples, which are generated when the Trojan is created in the configurator, are presented below.

```
            ~~~ LockBit 3.0 the world's fastest ransomware since 2019~~~

>>>> Your data are stolen and encrypted

        The data will be published on TOR website if you do not pay the ransom

        Links for Tor Browser:
        http://lockbit[redacted]gy6pyd.onion
        http://lockbit[redacted]d7qd.onion
        http://lockbitapt[redacted].onion
        http://lockbitapta[redacted].onion
        http://lockbitapte[redacted]d.onion
        http://lockbitaptj[redacted]yd.onion
        http://lockbitapte[redacted].onion
        http://lockbitaptq[redacted]qd.onion
        http://lockbitapto[redacted]yd.onion

        Links for the normal browser
        http://lockb[redacted]
        http://lockbitapt[redacted].onion.ly
        http://lockbitapte[redacted].onion.ly
        http://lockbitapte[redacted]ip4ykyd.onion.ly
        http://lockbitapta[redacted]bdguqd.onion.ly
        http://lockbite[redacted]gtzjqd.onion.ly
        http://lockbit[redacted].onion.ly
        http://lockbita[redacted]cllqdxad.onion.ly
        http://lockbitap[redacted].onion.ly
        http://lockbita[redacted].onion.ly


>>>> What guarantees that we will not deceive you?

        We are not a politically motivated group and we do not need anything other than your money.

        If you pay, we will provide you the programs for decryption and we will delete your data.
        Life is too short to be sad. Be not sad, money, it is only paper.

        If we do not give you decrypters, or we do not delete your data after payment, then nobody will pay us in the future.
        Therefore to us our reputation is very important. We attack the companies worldwide and there is no dissatisfied victim after payment.

        You can obtain information about us on twitter https://twitter.com/hashtag/lockbit?f=live
```

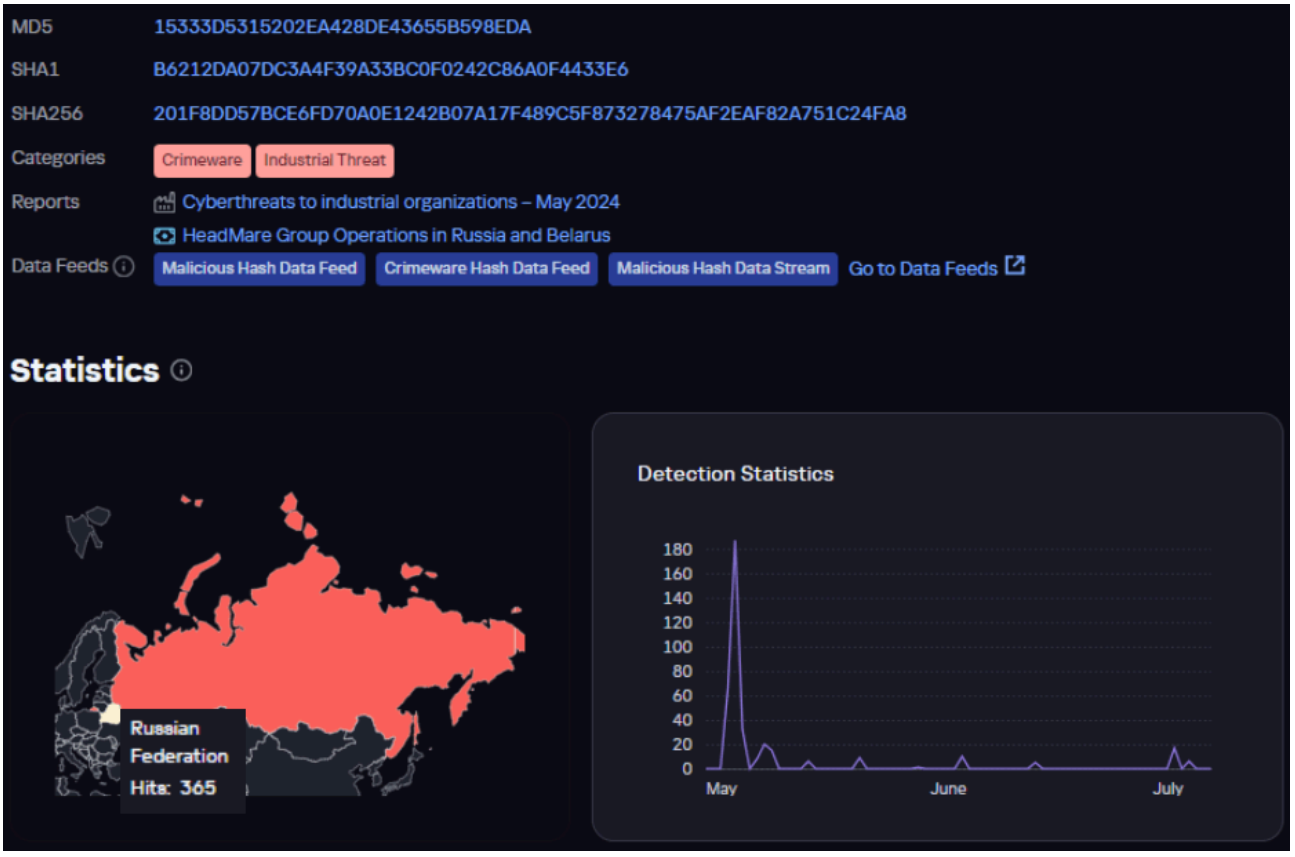
Ransom note from LockBit sample

```
————————CAUTION, PLEASE————————
sss All your files have been stolen and encrypted sss
You have to pay ransom otherwise all the data will be leaked on the Internet
as well as stay encrypted on your PC and the whole domain.

——> WHAT WE DO RECOMMEND:

DO NOT RECOVER any FILES on your own, IT CAN LEAD to irreversible consequences!

Your personal DECRYPTION ID: XXXXXXXXXXXXXXX

——> WHAT WE GUARANTEE YOU:

3 files free decryption as a tool validation.
We provide you with a decryption tool.
We delete all your data and send proofs.
We save your reputation, NO data leaks.
We share our vulnerability report with you.

——> WHAT THE REASON:
NO other reason except your MONEY!
Right now your have a chance to save your business.
Feel free to contact us.

https://getsession.org/

05983[redacted]
```

Ransom note from another LockBit sample

Victimology

According to Kaspersky Threat Intelligence, all samples related to Head Mare were detected only in Russia and Belarus. The screenshot below shows the analysis of the PhantomDL sample on the Threat Intelligence Portal.



Information about the PhantomDL sample from TIP

To get a more complete picture, we analyzed samples seen in Head Mare attacks using the Similarity technology, which helps us find similar malware samples. While we can't say for certain that the discovered files were also used by Head Mare, their similarity may help in attributing cyberattacks and further analyzing the group's activities.

PhantomDL

PhantomCore

LockBit

Conclusions

The tactics, methods, procedures, and tools used by the Head Mare group are generally similar to those of other groups associated with clusters targeting organizations in Russia and Belarus within the context of the Russo-Ukrainian conflict. However, the group distinguishes itself by using custom-made malware such as PhantomDL and PhantomCore, as well as exploiting a relatively new vulnerability, CVE-2023-38831, to infiltrate the infrastructure of their victims in phishing campaigns. This is an important aspect that Russian and Belarusian organizations should pay attention to: attackers are evolving and improving their TTPs.

Indicators of compromise

Please note: The network addresses provided in this section are valid at the time of publication but may become outdated in the future.

Hashes:

201F8DD57BCE6FD70A0E1242B07A17F489C5F873278475AF2EAF82A751C24FA8
9F5B780C3BD739920716397547A8C0E152F51976229836E7442CF7F83ACFDC69
08DC76D561BA2F707DA534C455495A13B52F65427636C771D445DE9B10293470
6A889F52AF3D94E3F340AFE63615AF4176AB9B0B248490274B10F96BA4EDB263
33786D781D9C492E17C56DC5FAE5350B94E9722830D697C3CBD74098EA891E5A
5D924A9AB2774120C4D45A386272287997FD7E6708BE47FB93A4CAD271F32A03
9B005340E716C6812A12396BCD4624B8CFB06835F88479FA6CFDE6861015C9E0
5A3C5C165D0070304FE2D2A5371F5F6FDD1B5C964EA4F9D41A672382991499C9
DC3E4A549E3B95614DEE580F73A63D75272D0FBA8CA1AD6E93D99E44B9F95CAA
053BA35452EE2EA5DCA9DF9E337A3F307374462077A731E53E6CC62EB82517BD
2F9B3C29ABD674ED8C3411268C35E96B4F5A30FABE1AE2E8765A82291DB8F921
015A6855E016E07EE1525BFB6510050443AD5482039143F4986C0E2AB8638343
9D056138CFB8FF80B0AA53F187D5A576705BD7954D36066EBBBF34A44326C546
22898920DF011F48F81E27546FECE06A4D84BCE9CDE9F8099AA6A067513191F3
2F1EE997A75F17303ACC1D5A796C26F939EB63871271F0AD9761CDBD592E7569
AF5A650BF2B3A211C39DCDCAB5F6A5E0F3AF72E25252E6C0A66595F4B4377F0F
9E9FABBA5790D4843D2E5B027BA7AF148B9F6E7FCDE3FB6BDDC661DBA9CCB836
B8447EF3F429DAE0AC69C38C18E8BDBFD82170E396200579B6B0EFF4C8B9A984
92804FAAAB2175DC501D73E814663058C78C0A042675A8937266357BCFB96C50
664B68F2D9F553CC1ACFB370BCFA2CCF5DE78A11697365CF8646704646E89A38
311EDF744C2E90D7BFC550C893478F43D1D7977694D5DCECF219795F3EB99B86
4C218953296131D0A8E67D70AEEA8FA5AE04FD52F43F8F917145F2EE19F30271
2D3DB0FF10EDD28EE75B7CF39FCF42E9DD51A6867EB5962E8DC1A51D6A5BAC50
DC47D49D63737D12D92FBC74907CD3277739C6C4F00AAA7C7EB561E7342ED65E
EDA18761F3F6822C13CD7BEAE5AF2ED77A9B4F1DC7A71DF6AB715E7949B8C78B

File paths:

$appdata\Microsoft\Windows\srvhostt.exe
$appdata\Microsoft\Windows\srvhost.exe
C:\Windows\system32\SrvLog.exe
c:\Users\User\AppData\Local\microsoft\windows\srvhosts.exe
c:\windows\srvhost.exe
c:\ProgramData\OneDrive.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

IP addresses

188.127.237[.]46
45.87.246[.]169
45.87.245[.]30
185.80.91[.]107
188.127.227[.]201
5.252.176[.]47
45.11.27[.]232

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
5.252.176[.]77/soft_knitting.exe
5.252.176[.]77/legislative_cousin.exe
5.252.176[.]77/2000×2000.php

---

[1] https://x.com/head_mare is the account supposedly associated with the hacktivist group. Use this source with caution.
