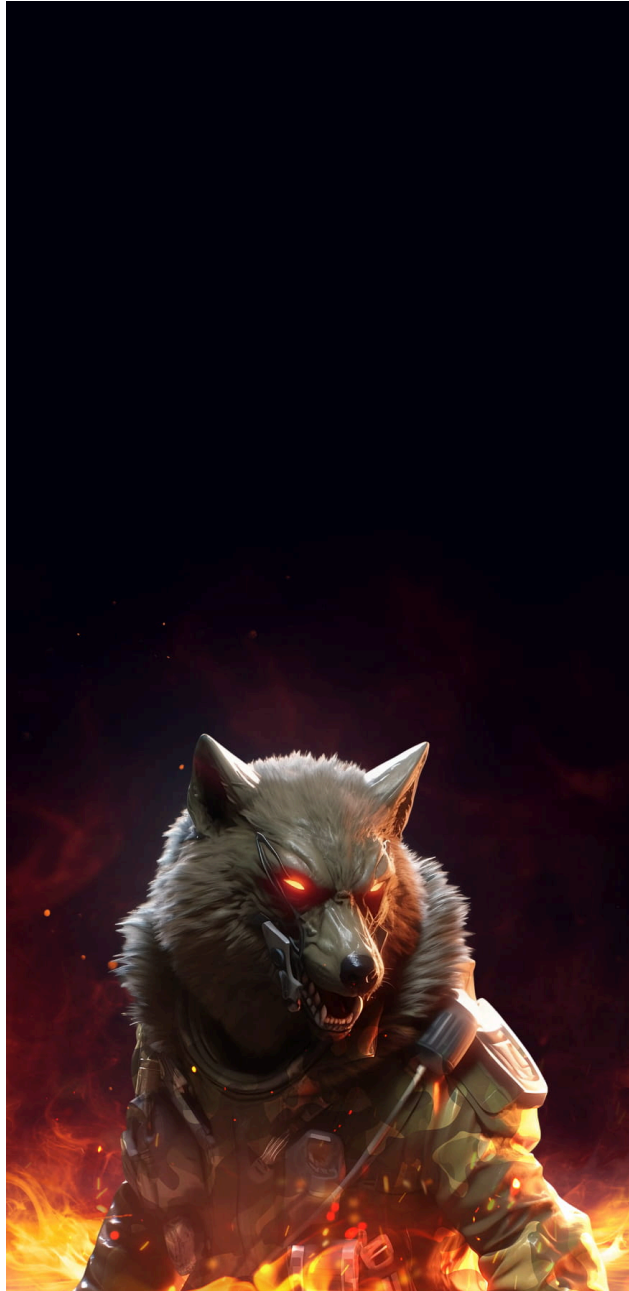


Arsenal revamped: Core Werewolf hits Russian organizations with CoreRAT

bi.zone/en/expertise/blog/core-werewolf-menyaet-klyki-troyan-corerat-v-atakakh-na-rossiyskie-organizatsii

BI.ZONE

July 30, 2026



The threat actor uses custom malware instead of UltraVNC

Overview

From June to July 2026, we recorded Core Werewolf and detected a previously undocumented CoreRAT. The malicious payload was distributed via the 7zSFX and Rust droppers. The threat actor penetrated infrastructures through phishing messages on Telegram. We assumed the attackers targeted Russia's public

sector and defense industry. Our retrospective analysis identified that CoreRAT had been used since at least March 2026.

Key findings

- Fueled by the ongoing geopolitical tensions, Core Werewolf continued to attack Russia's public sector and defense industry.
- The cluster employed its own CoreRAT instead of the legitimate UltraVNC remote access software. This helped the attackers stay under the radar longer and demonstrated their growing technical capabilities. Core Werewolf had already used custom minibackdoors, but CoreRAT was its first fully operational RAT.
- To make phishing messages more convincing, the threat actor used specially crafted decoy PDFs disguised as official military and government documents.

Campaigns

7zSFX dropper

Core Werewolf distributed 7zSFX under these names:

- Scan_437_ТЛГ_на_переподготовку.exe (*refresher training message*)
- исх1051_от_20.04.2026_сл_паспорт.exe (*passport*)

The dropper contained a decoy PDF and CoreRAT, and ran:

```
cmd.exe /c copy /y \"%CD%\*.*\" \"%CD%\\..\\F0hf6\" \"%HOMEPATH%\Desktop\CyzG.pdf\" <- copying decoy to  
%HOMEPATH%\Desktop  
cmd.exe /c copy \"%CD%\\..\\yNtns.GqV\" \"%HOMEPATH%\Links\Firepoin.exe\" <- copying CoreRAT to  
%HOMEPATH%\Links  
cmd.exe /c cd \"%HOMEPATH%\Links\" & start \"%\" \"%Firepoin.exe\" <- launching CoreRAT  
cmd.exe /c cd \"%HOMEPATH%\Desktop\" & start \"%\" \"%CyzG.pdf\" <- launching decoy
```

The analyzed 7zSFX samples copied the decoy to one of the paths:

- %USERPROFILE%\Desktop\CyzG.pdf
- %USERPROFILE%\Downloads\Vppq.pdf
- %USERPROFILE%\Documents\EY5Tm.pdf
- %USERPROFILE%\Downloads\r0po.pdf
- %USERPROFILE%\Downloads\H5nY.pdf

The CoreRAT executable was copied to one of these paths:

- %USERPROFILE%\Links\Firepoin.exe
- %USERPROFILE%\Links\Baresl.exe
- %USERPROFILE%\Links\brhost.exe
- %USERPROFILE%\Links\Biostars.exe
- %USERPROFILE%\Links\LiteEdit.exe

Rust dropper

Core Werewolf distributed the malware under these names:

- Указания - [redacted]_9f36b79847.exe(*instructions*)
- Указания по [redacted]_498 от 15.06.2026_47.exe(*instructions*)

The dropper contained a ZIP with a decoy and CoreRAT executable, and saved the archive contents to %TEMP%.

Example target paths on the victim host:

- %TEMP%\integrated.exe
- %TEMP%\Указания по [redacted]_498 от 15.06.2026_47.pdf
- %TEMP%\atrocitiy.exe
- %TEMP%\Указания - [redacted]_9f36b79847.pdf

After saving the files, the Rust dropper launched the decoy followed by the CoreRAT executable via:

```
cmd /c "ping.exe -n 38 127.0.0.1" & %TEMP%\integrated.exe
```

The analysis of other samples revealed the same file-saving logic.

The only difference was in the CoreRAT launch command:

```
cmd /c "ping.exe -n 65 127.0.0.1" & %TEMP%\atrocitiy.exe
```

Decoy PDFs

Our analysis of the decoy PDFs revealed a number of signs of fabrication, including wording and phrasing atypical of official government communications, as well as artifacts of document editing and signature forgery.

For official use only

Ex. No. 1

APPROVED

Commanding Officer
of the Grouping of Troops



PLAN

Work of the Working Group

No. Item	Name of Activity	Time	Location	Responsible Official
July 13, 2026 (Monday)				
1.	Meeting of the working group	12:00	()	Responsible for the meeting and escort, Deputy Commanding Officer of the Grouping of Troops
2.	Escort of the working group until	12:00–13:20		Responsible for the meeting and escort, Deputy Commanding Officer of the Grouping of Troops

For Official Use

Copy No. ____

To the Commander of the Troops

Dear [redacted]

Based on the results of visits in May 2026 to the troops [redacted] as part of the working group of the Ministry of Defense of the Russian Federation for coordinating the activities of military command bodies on issues of stabilizing law and order and military discipline in the troops (forces), factors and deficiencies affecting the state of law and order and the effectiveness of task performance at permanent and temporary troop deployment locations have been summarized (a consolidated report is attached).

I request that additional measures be taken to neutralize the identified factors, and that the results of the work carried out be reported by 1 August 2026.

“15” June 2026

Outgoing No. [redacted]

For official use only

Return to: DEPARTMENT

TELEGRAM
(URGENT)

From: _____

To: In accordance with the transmission calculation

For: In accordance with the transmission calculation

In addition to the instruction dated March 26, 2026, No. _____

I ORDER:

1. Commanders of formations and military units shall organize the assignment of military personnel under contract, who do not have the corresponding training at the Military Training Center (MTC), of the proposed MTC (retraining to other types of the Armed Forces) in training military units deployed on the territory of the military district, as follows:

- a) to the military unit _____ from January 5 to December 10, 2026, for:
junior sergeant _____ – military
personnel of the military unit _____
- b) to the military unit _____ from January 29 to
February 8, 2025, for:
lieutenant _____ – military personnel
- c) to the military culinary school _____ from October 28 to
December 10:
for _____
private _____ – military personnel
private _____ – military personnel
private _____ – military personnel
private _____ – military personnel
- d) to the military unit _____ from November 22 to
December 19, 2024, for:
private _____ – military personnel
private _____ – military personnel
private _____ – military personnel
private _____ – military personnel
for _____
junior sergeant _____ – military personnel

Decoy avth.gGAT.pdf

We also found that avth.gGAT.pdf was similar to Scan_125992145_TLG_na_perepodgotovku_dsp.pdf (SHA-256: c907b15b60fe77e42d3c37932f545e5d094370d5b709966a2fb572c5a6799660), which had been used in attacks by [Vortex Werewolf](#). This similarity could indicate that the clusters shared tools, decoys, and expertise. An alternative hypothesis was that Core Werewolf and Vortex Werewolf were part of the same group and used a common development infrastructure. However, the available data was insufficient to confirm this theory and required further investigation.

For official use only

Return to: DEPARTMENT

TELEGRAM
(URGENT)

From: _____

To: In accordance with the transmission calculation

For: In accordance with the transmission calculation

In addition to the instruction dated July 22, 2024, No. _____

I ORDER:

1. Commanders of formations and military units shall organize the assignment of military personnel under contract, who do not have the corresponding training at the Military Training Center (MTC), of the proposed MTC (retraining to other types of the Armed Forces) in training military units deployed on the territory of the military district, as follows:

a) to the military unit _____, from December 22 to December 30, 2025, for:
junior sergeant _____ – military personnel of the military unit _____

b) to the military unit _____ from December 22 to December 30, 2025, for:

lieutenant _____ – military personnel _____

c) to the military culinary school _____ from December 22 to December 30, 2025:

for _____

private _____ – military personnel _____

private _____ – military personnel _____

private _____ – military personnel _____

private _____ – military personnel _____

d) to the military unit _____ from December 22 to December 30, 2025, for:

private _____ – military personnel _____

private _____ – military personnel _____

private _____ – military personnel _____

private _____ – military personnel _____

private _____ – military personnel _____

for _____

junior sergeant _____ – military personnel of the military unit _____

;

Decoy Scan_125992145_TLG_na_perepodgotovku_dsp.pdf

CoreRAT

The malware is written in C++. String constants inside CoreRAT are AES-encrypted in CBC (AES-CBC) mode.

At startup, CoreRAT creates mutex 301525677, then runs anti-virtualization checks in a separate thread:

1. Uses the CPUID instruction to analyze a hypervisor for VMwareVMware, VBoxVBoxVBox, XenVMMXenVMM, and KVMKVMKVM strings.
2. Analyzes the BIOSVersion and BIOSVendor parameter values in the register key HKLM\HARDWARE\DESCRIPTION\System\BIOS for VMW and Vmware substrings.
3. Checks the number of LNK files in %APPDATA%\Microsoft\Windows\Recent\AutomaticDestinations. If the directory contains less than 15 LNK files, the malware identifies the environment as virtual.

If the checks fail, the malware terminates. If no signs of a virtualized environment are detected, CoreRAT decrypts C2 addresses:

```
dezinsekciya-top[.]ru:443|94.232.248[.]34:443|ahmetgurses[.]net:443|194.190.153[.]182:443
```

The C2 addresses are separated by |. CoreRAT attempts to connect to each of them until it succeeds.

After establishing the connection, the malware gathers basic information and generates a JSON object that contains:

- computer name obtained via GetComputerNameW()
- BIOSVersion register parameter value from HKLM\HARDWARE\DESCRIPTION\System\BIOS; if the value cannot be retrieved, the string Unknown is used instead
- number of valid LNK files in %APPDATA%\Microsoft\Windows\Recent\AutomaticDestinations whose target file objects exist on disk
- total number of LNK files in %APPDATA%\Microsoft\Windows\Recent
- list of running processes in the following format:

Image Name	PID

[PROCESS_NAME]	[PID]

- list of files and directories on the user's desktop in the following format:

```
Desktop path is %HOMEPATH%\Desktop
MM/DD/YYYY HH:MM [TYPE] [FILENAME]
```

where MM/DD/YYYY HH:MM is the object's last modification time

- information on network adapters in the following format:

Adapter Name	IP Address	MAC Address

Name:	[NAME]	
Description:	[DESCRIPTION]	
MAC:	[MAC_ADDR]	
IPv4:	[IPV4_ADDR]	
Subnet:	[SUBNET]	
DHCP:	[Enabled/Disabled]	

Once data is gathered, CoreRAT generates a JSON object containing all the obtained information.

```
{
  "1d22922b": "1640185028",
  "245c736a": [PROCESSES_LIST]
  "2ca93a25": [%APPDATA%\Microsoft\Windows\Recent LNK_COUNT],
  "2fe3b8c4": [DESKTOP_LS]
  "8feff34e": [ADAPTERS_INFO]
  "92481bcc": [%APPDATA%\Microsoft\Windows\Recent\AutomaticDestinations RESOLVED_LNKS_COUNT],
  "fb638856": [BIOSVersion],
  "host_name": [HOSTNAME]
}
```

The generated JSON is Base58-encoded and transmitted to the C2 via an HTTPS POST request:

```
hxxps://[c2]:[port]/5743e279
```

For network communications, the malware uses modified code from this [repository](#).

The server returns the parameter `session_token=<value>` which is transmitted in the Cookie header in subsequent requests.

Upon successful registration, CoreRAT generates an HTTPS GET request to retrieve the command:

```
hxxps://[c2]:[port]/0a445b0e
```

Commands from C2 are also Base58-encoded.

Supported commands:

Command	Description
6055bc66 [dir]	Enumerates the specified directory contents and sends the output to the C2 in the following format: Desktop path is [DIR] MM/DD/YYYY HH:MM [TYPE] [FILENAME]
8cb382b9	Generates a list of running processes and transmits it to the C2 in the following format: Image Name PID ----- [PROCESS_NAME] [PID]
2990a8e1	Gathers data on network adapters and sends it to the C2 in the following format: Adapter Name: [Adapter_Name] IP Address: [IPv4] DNS Suffix: [DNS_name]
4e86fd31	Generates an ARP table and transmits it to the C2 in the following format: Interface: [Interface] Internet Address Physical Address Type [ipv4] [MAC] [dynamic/static]
434cf996	Generates a list of active TCP connections and related processes and transmits it to the C2 in the following format: Proto Local Address Foreign Address State PID TCP [local_ip] [remote_ip] [state] [processID]

Command	Description
a004af05	Initiates the CoreRAT self-deletion: the malware renames its executable to [corerat_filename].exe.1, creates %TEMP%\tmp[random].bat, runs the batch script, and terminates. After a short delay, the script removes the malware executable and self-deletes. The contents of tmp[random].bat: <pre>@echo off timeout /t 3 >nul del /Q "[corerat_filename].exe.1" start "" /b cmd /c "ping 127.0.0.1 -n 3 >nul && del %~f0"</pre>
e81ff8fd [command / process]	Runs the specified command or process via WinAPI CreateProcessW(). The format e81ff8fd [url] [output] is also supported. In this case, CoreRAT downloads a file from the specified URL, saves it to [output] without running, and decrypts it using AES-CBC (key: 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff, IV: 0102030405060708090a0b0c0d0e0f10)
1188b874 [output]	Downloads a file from hxxps://[c2]:[port]/97e8be66, saves it to [output], decrypts it using AES-CBC (the key and IV are the same as in the e81ff8fd command), and runs it via CreateProcessW(). The format 1188b874 [url] [output] is also supported, allowing the file to be downloaded from an arbitrary URL instead of a standard C2 path

Upon execution, the command result is encoded using Base58 and sent to the C2 via an HTTPS POST request.

hxxps://[c2]:[port]/ba4b6dc1

CoreRAT samples

Our analysis revealed other CoreRAT samples that differ by checks for signs of virtualized environment.

Possible check options:

1. After decryption, one of the samples generated the following list of MD5 hashes:

```
1c69c262000994ac06ec153469eab55b|dc8dc902852fff973c9c51cef62bb4ba|a29ba2ff5388d667cc353730075fba4b  
|f34f4b89e95084d3a9b00b9c878fdcfca|b8d7886ca654a5e6feb3f9a56fa40b75|7228b3f08edb7754dec4d4e555fe853  
9
```

Then, it searched %USERPROFILE%\Desktop for .pdf files. The sample calculated the MD5 hash for each file and matched it against the list of decrypted values. If at least one match was found, CoreRAT continued execution. We confirmed that the specified MD5 hashes corresponded to the decoy PDFs distributed with CoreRAT as part of 7zSFX droppers. Thus, the malware checked for the expected decoy, verifying that it was launched upon the dropper execution.

2. The sample distributed via the Rust dropper implemented a different check. CoreRAT enumerated all the files in %TEMP% and compared their creation date (year, month, and day) with its process creation date obtained via GetProcessTimes(). If the dates matched, it calculated the MD5 hash of the file contents and then compared it with the list of known hashes:

```
09f192018e1a42f577d0f136b59e2888|b90f78b83282a7c7ccf8b6f61ab4af4d|6dbb3abbd19859c6f2771d7e32029818  
|7c3754bb07904de3708f1fae02bb9d0c|ad5f31bb0f53662c5ad659a3de2df2d0|d4af404ee8b55fc40b3ef620d90396a  
a|af7ad3dbf7666a88e19d076efe858f49|9b4f048ec84b13d5138d937109f2cddb6|73a8ef0d8fb7960ce6a29c38190aec  
6d|f4a647575c4fd3cb3c29b2a69c3aa6fe|907988b8337495e5245f3a01fd6fd121|808157c74ecd47961c7d2d6f934d7  
06f|3cbb25f5f3a9ac6908d93cc58909536d|729598a8473203c1938b69995d816c31|1406fb20fce3c82bd55616e7949e  
7aca|6813c4f5170125d134a38ea2af45da97|b6a7dc31b3e1059b227e032f35727ebd|09c659fa24c98ba0f65c7a03696  
49903|a5be3e5a8bd37feee8bcff7b5d4a4dba|9e372e0f2356edd059af47e70044830a|b3eef6b2ecb165e50d057e1e21  
0d6558|c2af530aff5108ab953eec30ec2399e7|0aaeb5c679e8f42e160248d5ef9e1d83|bd128b66eb000fd08ada754ed  
9ceba2e|3da4b2eaa2359e55bc33cca7468792ad|65a9da2d23cf0baae86bd0be8d97ed03|eee77075b5077c5abf03a9e0  
9567ca08|2304e7a62565f45db890a341fb7a7d70|305b6e15b0209a0684fc6d8352b49839|65d112c2e2673d5fa5b22de  
b1b4a430e|5bef05f58d53791fc49ee8d66f2cb652|a2ef7d18d943af3c9dc6e9960f26ccbd|bb7eae1628af407ed9fc02  
40e92eccfe|b1410e77bfee794f52adc29e0ef9aed6|d98ed128086144ef699ef7584f858aa1|bc0608ca923518bb05bc0  
0b608f377eb|04028f5fd20a6fa60694962ae72bb96f|4ced3337ca412a638a504e697caa954f|3454030cd9b40280f1a0  
e7e585c0f639|761f92ed3f949daa790b2cc96d2efbd5|0d003702bec166aec8f3869d53ccf89f|9705d2d1c30b0ae4c4a  
50c6acb3a9dc8|3215f75e96dad896f961e13a23c5d17f|3efbb378747d3e7d96d077ec6afefbc7|63ae279bcfc0babcab  
0539f44b97c76a|800076766e58c0f4cfd8a929865a6c9e|92d4dabf7348b0dad11c1295b030611d|bf17c89f315e0b11a  
812a87783417c0f|4b0c15b864b643c3a4ab38360c7c027a|fa3948732fef4f81dbc13102db6f641f|a59c46d04b6274de  
33093e6d9f62f334|8d4900aed87db884e183145d2a56ea92|720e4c35995f95413d9d3d7ebe57d88f|7c3835a54017325  
3460763b19a4565fa
```

This mechanism enabled the detection of files created by the Rust dropper immediately before CoreRAT was launched and allowed them to be used as an additional indicator of execution within the expected compromise chain.

3. One of the early samples ran anti-virtualization checks by analyzing network adapter MAC addresses. It checked each network adapter MAC address for one of the following prefixes:

```
000C29
001C14
080027
000F4F
```

The sample also searched MAC addresses for the following substrings:

```
0003BA
00015D
001851
506B8D
9600
```

Matches against these values were considered indicators of a virtualized environment, as the corresponding prefixes are used by popular hypervisors such as VMware, VirtualBox, and Microsoft Hyper-V.

The analysis of CoreRAT samples revealed that each of them used unique C2 endpoints and varying JSON fields to gather and transmit compromised system information.

Below is an example of the data structure from another sample:

```
{
  "diff-stats-582": "[DESKTOP_LS]",
  "host_name": "[PC_NAME]",
  "projection-deliver-594": "[PROCESSES_LIST]",
  "seller_issue_95": -1,
  "shipment-views-323": -1,
  "slow-privilege-847": "[ADAPTERS_INFO]",
  "version_acl": "2539284801" [BUILD_ID]
}
```

Command names also vary across CoreRAT samples. During the analysis, we restored their original names:

Original name	Obfuscated name
!dir	6055bc66 , parse-299
!tasklist	8cb382b9, topics_attachment_891
!ipconfig	2990a8e1, identity-projection
!arp	4e86fd31, middleware-883
!netstat	434cf996, monitor_279
!terminate	a004af05, secret_892
!download	1188b874, formats-daemon-380
!payload	e81ff8fd, warm-762

Indicators of compromise

Checksums

- 604ffe14ab558bf79f00adbf050760ba5d0156ad7326586013c5d3fb3d7ef2f7
- 4661735db0f33dd567d29b2a056a967bb3762f831eb3678b27c4ffb06dbb8ec1
- 465913946d4985ab60899ed2b7bc779ea83d08683c041d0e33b496358b684106
- b40b8978430ebbcbe8101ec51409fef86798d88e24287a1173fde2a106fd0d76
- d34eb87981cd144c0916b1e720b94dc22b52924b3358c32350a235925e7dfa7e
- 6ccfd6b2964f564ab1b308b1c6b4d78f994ec1e975f4e848620ebb302d3e70ac
- 085db99b37298266b48dba20749c1567f99895b5ae3f60d3ea08047d3903542d
- 07956ee6bbd628bcaafe36c4b01f3fe146b87df16bbbb6d884c5e5ab1608858
- 7a489dc1e1dc13ec35fb94b4faedcb294879c7fe3597888aec7ad3f516c1cc20
- 02933405aac6676fd892ff311418877185bbaadc7151807f54a3bc3d6b75241d
- 1402053d6edb096b59b8df3b81d56d5a30e6577f9022ef9b5dae910f328d0401
- 909dfb4388334d66877debcb46d36c7d0a5a75c231241aa4c989ff0cafacc8f9
- 722e7b896d5c6026af26ac368de2aed93ff341128478a6cd57849549abf773d2
- ea9600c3d62d807c07055f0951d08db03725417b9342a76e62410e2694050033
- 6f04ceb8d83ceb8b160314ac1829fba7054464006990e47a1493faf1185c2dab
- a4f21177027e07280edf929adfd1403e0f4e7eb1892ca38069d45a9cd06e2929
- fe2cc8991ec22325283cd246856f7869caae0ff8b4d90cbbb734593b5b3d99ed
- 31ef487ed72e96d3d8ce50459e2d63786f51925b6e7fc4ede372e26ea7709a1c
- d447e296f7da71a05d38077ae27295519151d56b6cd44ca272e731d702f7fe63
- 8925168fa34fb8e823f7329fb775b6c2cc3b41767524fc639452e93ec5c360e1
- 9a1491258e5d0131b0bb237c7221016c737af79961427c1f2fed9f80d75787b3
- 7c5dd94fbda84bd1dc9122dc7f6b2df1469f9e757f7ca577ba82d3ab4bc13d08
- 1641001dd82ed4e7ad59dfc4e5f4d9c6cd9937d47a6e59931d382926c0632de3
- be8a351d80e15c6ae88dd566939600162375441c538ee61be36bb81c93da182f

Network indicators

- teambusiness-mail[.]ru:443
- xakklinkprik[.]ru:443
- dezinsekiya-top[.]ru:443
- ahmetgurses[.]net:443
- msgntfsys[.]link:443
- arendelle[.]ru:443
- sgpsib[.]ru:443
- 185.102.139[.]30:443
- 130.49.181[.]212:443
- 138.124.76[.]77:443
- 95.81.125[.]145:443
- 178.253.39[.]45:443

- 104.128.129[.]184:443
- 95.215.108[.]140:443
- 45.128.150[.]49:443
- 195.47.250[.]173:443
- 91.212.150[.]141:443
- 5.101.88[.]7:443
- 194.190.153[.]182:443
- 94.232.248[.]34:443

MITRE ATT&CK

Tactic	Technique	Procedure
Execution	Command and Scripting Interpreter: Windows Command Shell	Core Werewolf employs a 7zSFX dropper to copy and launch the CoreRAT payload via <code>cmd.exe</code>. <pre>cmd.exe /c copy /y "%CD%*.*" "%CD%\..\\" cmd.exe /c copy "%CD%\..\F0hf6" "%HOMEPATH%\Desktop\CyzG.pdf" cmd.exe /c copy "%CD%\..\yNtns.GqV" "%HOMEPATH%\Links\Firepoin.exe" cmd.exe /c cd "%HOMEPATH%\Links" & start "" "Firepoin.exe" cmd.exe /c cd "%HOMEPATH%\Desktop" & start "" "CyzG.pdf"</pre> Uses the Rust dropper to delay the CoreRAT startup and execution via <code>cmd.exe</code> and <code>ping.exe</code>: <pre>"cmd" /c "ping.exe -n 38 127.0.0.1" & %TEMP%\integrated.exe "cmd" /c "ping.exe -n 65 127.0.0.1" & %TEMP%\atrocitiy.exe</pre>
	Native API	Leverages CoreRAT to run commands and processes via <code>e81ff8fd (!payload)</code> using the <code>CreateProcessW()</code> WinAPI function
Stealth	Deobfuscate/Decode Files or Information	Employs CoreRAT to decrypt strings and C2 addresses using AES-CBC, and to decrypt the downloaded files with the key <code>00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff</code> and the IV <code>0102030405060708090a0b0c0d0e0f10</code>
	Indicator Removal: File Deletion	Initiates the CoreRAT self-deletion via <code>a004af05 (!terminate)</code>. The malware renames itself to <code>[corerat_filename].exe.1</code> and creates a <code>.bat</code> file in <code>%TEMP%</code>, which removes the executable and self-deletes: <pre>@echo off timeout /t 3 >nul del /Q "[corerat_filename].exe.1" start "" /b cmd /c "ping 127.0.0.1 -n 3 >nul && del %~f0"</pre>

Tactic	Technique	Procedure
	Obfuscated Files or Information:	Leverages a 7zSFX dropper to unpack and launch CoreRAT and a decoy.
	Embedded Payloads	Uses a Rust dropper to unpack an embedded ZIP archive containing CoreRAT and a decoy into %TEMP%
	Virtualization/Sandbox Evasion: System Checks	Employs CoreRAT to run anti-virtualization checks: analyze hypervisors for VMwareVMware, VBoxVBoxVBox, XenVMMXenVMM, and KVMKVMKVM strings using the CPUID instruction; check the BIOSVersion and BIOSVendor registry parameters for VMW and VMware substrings; count the number of valid LNK files in %APPDATA%\Microsoft\Windows\Recent\AutomaticDestinations; calculate MD5 hashes of files in %USERPROFILE%\Desktop and %TEMP% and compare them against a predefined list of decoy hashes; and analyze network adapter MAC addresses against known prefix values
Discovery	File and Directory Discovery	Employs CoreRAT to enumerate files in the specified directory via 6055bc66 (!dir)
	Process Discovery	Leverages CoreRAT to generate a list of running processes via 8cb382b9 (!tasklist)
	Query Registry	Uses CoreRAT to read the BIOSVersion and BIOSVendor values from the HKLM\HARDWARE\DESCRIPTION\System\BIOS registry hive to detect a virtualized environment and gather system information
	System Information Discovery	Leverages CoreRAT to gather system information, including the computer name (GetComputerNameW), BIOS version, list of processes, list of desktop files and directories, and network adapter data. The collected information is exfiltrated as a Base58-encoded JSON object
	System Network Configuration Discovery	Uses CoreRAT to gather network adapter data via 2990a8e1 (!ipconfig) and ARP table data via 4e86fd31 (!arp)
	System Network Connections Discovery	Employs CoreRAT to generate a list of active TCP connections and related processes via 434cf996 (!netstat)
Command and Control	Application Layer Protocol: Web Protocols	Leverages CoreRAT to communicate with the C2 via HTTPS

Tactic	Technique	Procedure
	Data Encoding: Non-Standard Encoding	Uses CoreRAT to Base58-encode transferred data and commands
	Ingress Tool Transfer	Employs CoreRAT to download files from the C2 via 1188b874 (!download) and e81ff8fd (!payload) and subsequently decrypt them using AES-CBC

How to protect your company against Core Werewolf

Building an effective cybersecurity strategy against Core Werewolf and similar clusters requires knowledge of the current threat landscape and an understanding of the tools and techniques used by threat actors. The portal provides organizations with timely insights on indicators of compromise and adversary toolkits. This information facilitates incident response and helps build corporate defenses against relevant threats.

However, effective protection demands timely detection and containment of attempted intrusions. EDR solutions such as enable early detection of attacks and immediate incident response—either automated or manual.

How useful was this material?

You might find interesting
