

Мертвые души в инфраструктуре — атака Shedding Zmiy на госсектор

 rt-solar.ru/solar-4rays/blog/6523

January 1, 2000



Атакующие более 6 месяцев имели доступ к инфраструктуре организации из госсектора через VPN и занимались шпионажем. Подключение к инфраструктуре выполнялось с помощью учетных записей уволенных сотрудников, которые не были своевременно выведены из эксплуатации и оказались скомпрометированными. В процессе расследования были обнаружены новые версии инструментов группы Shedding Zmiy, позволяющие экспортировать данные из баз данных и делать скриншоты экрана.

Обзор инцидента

В ноябре 2025 года к нам обратились представители госорганизации с просьбой помочь в расследовании вероятной компрометации инфраструктуры. Причиной обращения стало детектирование подключений к IP-адресам GSocket на пограничном устройстве в сети.

При предварительном анализе нескольких систем мы выяснили, что в инфраструктуре было скомпрометировано несколько десятков Unix-систем, атакующие имеют доступ к системам не менее 6 месяцев, а вся цепочка компрометации сводится к VPN-серверу организации.

После получения доступа к VPN в апреле 2025 года атакующие скомпрометировали сервер PostgreSQL, в журналах которого мы обнаружили следы удаленного выполнения команд в системе с использованием легитимной функциональности самой БД. Доступ к выполнению команд был получен в результате компрометации стандартной УЗ в PostgreSQL, у которой был установлен ненадежный пароль. Для закрепления в системе атакующие разместили утилиту gs-netcat, закрепив ее в файлах «.profile» и «cron» УЗ в PostgreSQL.

Уже через несколько дней у атакующих появилось множество учетных данных (в том числе root), с помощью которых началось активное боковое перемещение и заражение инфраструктуры. Стоит отметить, что атакующие с новыми учетными данными продолжали подключаться напрямую через VPN и длительное время не использовали размещенные в системах бэкдоры.

При исследовании систем мы обнаружили множество файлов вредоносного ПО:

- **gs-netcat**. Атакующие использовали и оригинальный исполняемый файл, и дополнительные упаковщики, такие как Bincryptor и UPX (некоторые файлы были упакованы сразу в оба упаковщика). Также нами были обнаружены образцы, собранные из исходников gs-netcat с измененным сервером управления.
- **Bulldog Backdoor**. Характерный инструмент группы Shedding Zmiy.
- **Megatsune Rootkit** (семейство Kitsune Rootkit). Также является характерным инструментом Shedding Zmiy, с помощью которого, вероятно, и были получены учетные данные для бокового перемещения, так как данный Rootkit обладает функцией сбора паролей и ключей ssh.
- **Revsocks Proxy**. Open-source-прокси с GitHub.
- **Nmap**. Атакующие несколько раз за 6 месяцев выполняли сканирование инфраструктуры с разных систем.
- Различные утилиты для повышения привилегий, разведки и удаления логов.

Достаточно частый вопрос, который задают нашей команде форензики: «Почему атакующих не замечали так долго?» В данном инциденте их все же заметили, и, вероятно, не один раз. В процессе исследования мы столкнулись с тем, что администраторы и служба ИБ заказчика уже проводили реагирование ранее — данный факт был установлен при ретроспективном анализе некоторых систем, где имеются следы удаления вредоносного ПО с последующим повторным заражением. А некоторые системы вообще были удалены по причине их участия в «иных» инцидентах ИБ летом 2025 года. На деле, вероятно, это были следы более крупного инцидента.

При самостоятельном реагировании были совершены достаточно распространенные ошибки:

1. Пропуск уникальных файлов вредоносного ПО, которое не может быть обнаружено антивирусами из-за отсутствия сигнатуры.
2. Не был обнаружен источник компрометации, в данном случае VPN-сервер.

Подробнее об ошибках реагирования на инциденты и их последствиях рассказали [в блоге Solar JSOC](#).

Анализ VPN-сервера стал для нас непростой задачей, так как уровень его логирования не позволял провести ретроспективный анализ за 6 месяцев — глубина журналов составляла лишь несколько дней, но совместно с заказчиком нам удалось определить несколько

скомпрометированных IP-адресов из сети VPN (каждый IP-адрес был закреплен за конкретным сотрудником). Это удалось сделать с помощью журналов различных сервисов, к которым можно было подключиться из сети VPN — так мы обнаружили косвенные следы сетевого сканирования с помощью Nmap в периоды активности атакующих.

Однако на этом наше расследование столкнулось с проблемой: большая часть обнаруженных подозрительных IP-адресов из VPN-пула принадлежала сотрудникам, которые были уволены до или в период инцидента, а их системы уже были недоступны для анализа. При этом учетные записи уволенных сотрудников не были своевременно выведены из эксплуатации, чем и воспользовались атакующие. Определить причину компрометации личных систем сотрудников на момент нашего расследования не представлялось возможным. Вероятно, это мог быть фишинг.

В результате анализа одной из систем мы обнаружили утилиту cloudflared проху, которую группа Shedding Zmiy периодически использует при атаках на Windows-инфраструктуру. Система была скомпрометирована в мае 2025, т. е. уже после начала атаки, и не являлась точкой входа.

Техническое описание

Утилита IC

Представляет собой средство чистки логов.

Большинство параметров имеют дефолтный режим работы (где, например, логи очищаются для настоящего пользователя) и режим работы с regex, где можно установить различные параметры, которые при совпадении будут удалены из логов.

Параметр	Описание
-p	Очистка логов (utmp wtmp btmp lastlog secure messages auth.log auditd.log)
-l b	Очистка bashhistory
-l d	Очистка логов apache, найденных через открытые дескрипторы родительского процесса
-u<user>	Очистка по паттерну username
-z	Удалить утилиту

-y<tty>	Очистка по tty-паттерну
-a<host>	Очистка по паттерну хоста
-t<date>	До даты
-s<text>	Удаление из логов по паттерну строки
-f<date>	От даты
-e	Extended regex
-i	Ignorecase

Утилита в цикле вызывает функции очистки разных типов логов с указанными флагами, которые проверяются в функциях.

```

uv
dq offset aVarRunUtmp ; "/var/run/utmp"
dq offset sub_40094C
dq offset aVarLogWtmp ; "/var/log/wtmp"
dq offset sub_40094C
dq offset aVarLogBtmp ; "/var/log/btmp"
dq offset sub_40094C
dq offset aVarLogLastlog ; "/var/log/lastlog"
dq offset sub_40071D
dq offset aVarLogSecure ; "/var/log/secure"
dq offset sub_400AC5
dq offset aVarLogMessages ; "/var/log/messages"
dq offset sub_400AC5
dq offset aVarLogAuthLog ; "/var/log/auth.log"
dq offset sub_400AC5
dq offset aVarLogAuditAud ; "/var/log/audit/audit.log"
dq offset sub_400AC5
dq offset aVarLogXferlog ; "/var/log/xferlog"
dq offset sub_400AC5
db 0

```

Функция очистки и логи, которые она чистит

GSM-exploit nas

Представляет собой скомпилированный эксплойт CVE-2023-6546 с [GitHub](#) для ядер 5.4.4.15 4.18. Эксплойт ориентирован на подсистему GSM в ядре Linux. В нем используется уязвимость в модуле p_gsm, которая приводит к race condition и use-after-free при работе с

GSM-модемами, что, в свою очередь, позволяет получить доступ на выполнение произвольного кода в ядре с повышенными привилегиями (root).

Эксплойт способен обходить KASLR, SMAP/SMEP.

Bulldog Backdoor 1.7.6

Новая версия старого инструмента Shedding Zmiy. Мы смогли провести сравнение версий 1.3.0, 1.7.6 и 1.9.5 с [ранее описанными](#) версиями. Несмотря на разницу в одну мажорную и несколько минорных версий большая часть информации остается актуальной и для самых новых версий.

В данном разделе мы опишем причастную к этому инциденту версию 1.7.6. В коде бэкдора были сильно переработаны структуры модулей:

go.red/bb – связанное с командами и работой бэкдора
go.red/core – связанное с работой с системой и сетью
go.red/bart-backend-client – отправка коллекций от collector
go.red/teleport – транспортная конфигурация
go.red/gecko – теперь имеет модуль birdwatch
go.red/revproxy – теперь отдельный от bb модуль
go.red/revshell – теперь отдельный от bb модуль
go.red/collector – добавились новые модули

Интересно также использование более новых версий Garble на более старых версиях бэкдора и наоборот. Видимо, бэкдор используется разными операторами с иногда не самыми актуальными версиями инструментов.

Некоторые команды поменяли имя:

- bb-update -> self-update
- creds-watcher-> credentials-watcher

Также были обнаружены новые команды:

Команда	Подкоманды/флаги и описание
bb-df	Аналог df в Linux. Позволяет узнать использование файловой системы

bb-du	Аналог du в Linux. Отображает размер файлов. Флаги: • depth — глубина поддиректорий • specified — аналог -d 0 • print-errors — отображать ошибки
bb-resolve	Получение IP-адреса по домену. Флаги: • reverse — получить домен по ip • v6 — отображать ipv6
bb-wol	Отправляет wake-on-lan-пакет, получает mac в качестве аргумента. Флаги: • broadcast-address — адрес бродкаста • port — порт
download-and-run	Скачивает и запускает файл, получает путь как аргумент Флаг: target — позволяет загрузить с бакета
running-commands	Позволяет просматривать запущенные команды. Подкоманды: • list — вывести • stop — остановить
shollect	Использует grpc-команды shollector, упоминаемого в панели «Бульдога»
destroy	Самоуничтожение
take-screenshot	Сделать скриншот
sql-export	Позволяет запускать запросы и экспортировать результаты. config — путь до локального или внешнего конфига

http-proxy	HTTP прокси.
	Флаги:
	• port — обслуживаемый порт • verbose — больше логов

В переменных окружения заметна интеграция бэкдора с новыми инструментами Shedding Zmiy. В рассматриваемых версиях есть новые переменные окружения:

- Переменная окружения BB_MYCELIUM_ADDR для подключения к Mycelium — бэкдору на Rust, работающему в связке с библиотекой Leech и более подробно описанному в нашей [статье](#).
- Переменные окружения для форвардинга трафика BB_RP_LISTEN (получение трафика), BB_RP_DEST (отправка трафика).

Также была обновлена команда стилера collect.

Флаги	Описание
local-archive	Локальное хранение архива
skip-trees	Пропуск сбора информации о деревьях файловой системы
skip-files	Пропуск сбора информации конкретных путей
std-out	Вывод результатов в std-out
exec-timeout	Таймаут сбора
skip-browser-creds	Пропуск сбора браузерных учеток
win-creds	Сбор учетной информации Windows
target-id	Идентификатор цели для перезаписи идентификатора в конфигурации (если указан)
login	Логин, используемый для доступа к машине

password	Пароль, используемый для доступа к машине
----------	---

gather-protected-passwords	Попытка собрать пароли, защищенные KeyChain. По умолчанию значение равно false для macOS и true для Linux и Windows
----------------------------	---

Модуль стилера Collector обзавелся функциональностью сбора информации о контейнерах, браузерных паролях из Firefox и Chromium. (А версия 1.3.0 имеет функционал сбора информации о Active Directory).

```
v38[0] = x_go_red_collect_process_wrap;
v38[1] = v4;
v39[0] = v38;
v37[0] = x_go_red_collect_envvars_wrap;
v37[1] = v4;
v39[1] = v37;
v36[0] = x_go_red_collect_host_wrap;
v36[1] = v4;
v39[2] = v36;
v35[0] = x_go_red_collect_interfaces_wrap;
v35[1] = v4;
v39[3] = v35;
v34[0] = x_go_red_collect_netstats_wrap;
v34[1] = v4;
v39[4] = v34;
v33[0] = x_go_red_collect_commands_wrap;
v33[1] = v4;
v39[5] = v33;
v32[0] = x_go_red_collect_hardware_wrap;
v32[1] = v4;
v39[6] = v32;
v30 = x_go_red_collect_containers_wrap;
v31 = v4;
v39[7] = &v30;
v29[0] = x_go_red_collect_creds_n_configs_wrap;
v29[1] = v4;
v39[8] = v29;
v28[0] = x_go_red_collect_trees_wrap;
v28[1] = v4;
v39[9] = v28;
v27[0] = x_not_impl_wrap;
v27[1] = v4;
v39[10] = v27;
v26[0] = x_go_red_collect_browsers_wrap;
```

v26[1] = v4;

Функция Collect из метода go_red_collector__ptr_Collector_Gather

Украденные учетные данные сохраняются в структуре **model_Credentials**.

```
struct model_Credential
{
    string MachineID;
    string Service;
    string Target;
    uuid_UUID TargetID;
    string Login;
    string Password;
    string PasswordHash;
    string Key;
    string Comment;
    string Source;
    _ptr_time_Time LastUsed;
    string Cmd;
    _ptr_time_Time ExpiredAt;
};
```

И отправляются в составе запроса на C2 на */b/v1/collection-result*.

```
struct v2_StoreCollectionResultRequest
{
    v2_UpsertTargetHostBase UpsertTargetHostBase;
    string CollectorVersion;
    _slice_model_Credential Credentials;
    _slice_uint8 Archive;
};
```

gs-necat под Bincrypter

Инструмент с открытым кодом, [давно](#) используемый Shedding Zmiy и позволяющий создавать туннели и обходить ограничения файрвола. Предназначен для передачи данных, установления соединений и удаленного взаимодействия между машинами. Вместо прямого TCP-соединения между хостами используется промежуточная relay-сеть, называемая Global Socket Relay Network (GSRN). При этом прямая сетевая доступность не требуется, а сама relay-инфраструктура не имеет доступа к содержимому передаваемых данных.

В случае ff003528ae7775cd482fa43a6b96f6121feff7d40a75bb6f3cb66dd4370bde67 gs-netcat был накрыт [bincrypter](#). Данный криптер позволяет сжимать и шифровать программы, а также имеет опцию задания пароля для расшифровки. В качестве пароля могут выступать технические характеристики атакуемой системы.

Заключение

Shedding Zmiy прервали затишье, которое продолжалось почти год, и совершили новые атаки. За год группировка обновила свои инструменты на нескольких минорных версиях. Новейший на данный момент Bulldog Backdoor обзавелся новыми командами и структурно обновился. Видно, что SZ также нацеливаются и на пользовательские машины. Для этого они добавили новый модуль стилера для работы с браузерами и команду для создания скриншотов. Интерес также вызывает упоминание macOS в описании одной из команд: это говорит, что SZ, возможно, могут атаковать устройства из «яблочной» экосистемы.

По итогам данного расследования хотим еще раз напомнить:

1. Регулярно проводите инвентаризацию пользователей, как в доменах, так и в различных сервисах. Не копите «мертвые души» в своих сервисах — учетные записи уволенных сотрудников должны быть выведены из эксплуатации, как и прочие неиспользуемые УЗ.
2. Автоматизируйте управление учетными записями сотрудников и своевременно выводите их из эксплуатации (например, с помощью [IdM-решения](#)).
3. Подключение к VPN должно осуществляться с использованием второго фактора.
4. Настройте логирование VPN с сохранением журналов в SIEM. Компрометация VPN является достаточно частым вектором атаки, но при расследованиях VPN нередко становится черной дырой, из которой вылезают злоумышленники.

IOC

Files

MD5

2ab8ac9ec5f3f91a76b237dd83c5469c
f0e80499bcae7a4c83f5c3154ea7ae14
5d5490f1b2267828c805b64c749de112
893119b113d6952a11478efce099016c
5feb756bf7ab578722c560195bf7d411
840b15a948408a9fa1ee79b4516b7165

SHA1

ffb950627de389a9e6193e7178a369ee578f7054
053dbf9a056de6a1cc5ef8b9881c0784c08646c7
d4556652349c6fab16059da161a955d1a7dd5ad0
2ec0d066ad47d13caa78e758859f405970ad4718
a7476d92a215dc680d211ee4428acfd427aa86d3
095463a681936cbba36aa9419ab8ad8c37f3cb47

SHA256

cd89d661c1a3f2d7b199993732d814e5c5780e4bd4ac31f75e68430d46804999
b5393f6e9519590d1b3e69401f4cf7482ecd058c6d6c7d660f6ebdd8042a947a
9483d721e395c512715f41a8d4ea46dd3489b0784cc7a27bf0de2e2735235262
d7747a46f61867688b86eb7f04668cb8c4131f47471122a4c8ef6ea3d507b974
ff003528ae7775cd482fa43a6b96f6121feff7d40a75bb6f3cb66dd4370bde67
dd7acc09dcf30d50311623459a2d543fddb789e7e5cc829caff411cc2b1532fe

Domain

xy7ozq[.]info
leo[.]jruby33[.]xyz
ocelot[.]jruby33[.]xyz
tiger[.]jruby33[.]xyz
sm4l1pp[.]online
hexa10[.]biz

IP

103[.]71[.]23[.]102

-
- Денис Чернов



- Pandora Hive Mind

Денис Чернов, Pandora Hive Mind

Содержание статьи

Получать новости

Аналитический отчет по целевым кибератакам за 2025 год

[Читать](#)

Подпишитесь на полезные рассылки Solar 4RAYS

Email

Я даю [согласие на обработку персональных данных](#) , на условия [Политики по обработке персональных данных](#) , а также на получение информационных материалов и рассылок

А еще новости можно получать в ТГ и на RSS