Обновленные инструменты группировки BO Team

Kaspersky ⋮ ⋮ 9/25/2025

Авторы

- Expert Kaspersky

Введение

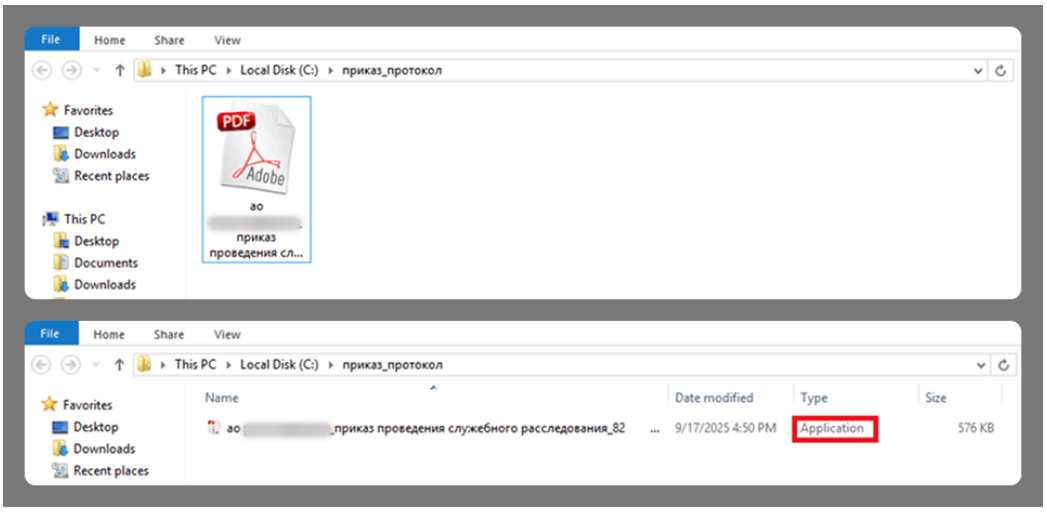
В начале сентября мы обнаружили новую вредоносную рассылку группы BO Team с использованием запароленных RAR-архивов. В фишинговых письмах говорилось о проведении служебного расследования, связанного со злоупотреблением использования полисов ДМС. В ходе анализа мы обнаружили, что BO Team обновила свой инструментарий: теперь атакующие рассылают новую версию бэкдора BrockenDoor, переписанную на C#, а также используют его для установки обновленной версии бэкдора ZeronetKit.

BO Team — это одна из активных на текущий момент группировок хактивистов, существующих как минимум с начала 2024 года. Она нацелена на российские компании. Ранее мы рассказывали об инструментах и методиках, используемых этой группой на протяжении последних двух лет.

Новая кампания

В новой кампании, зафиксированной в сентябре 2025 года, группировка BO Team продолжает использовать фишинговые письма для заражения пользователей. Так, например, один из вредоносных образцов мы обнаружили во вложении письма, в котором получателю угрожали служебным расследованием, якобы связанным с обращениями по полису ДМС. Вложенный RAR-архив с именем `Приказ_протокол.rar` был защищен паролем для предотвращения автоматического сканирования антивирусом, при этом пароль предположительно указан в теле письма.

Внутри архива содержится исполняемый файл с иконкой PDF-файла и расширением `.exe`, отделенным от имени файла большим количеством пробелов — таким образом, в проводнике содержимое архива выглядит как вполне легитимный документ.



Пример содержимого архива

Запустив вредоносный файл, пользователь видит документ-приманку. Этот документ представляет собой фальшивый протокол проведения служебного расследования, связанного с использованием услуг ДМС.

В отличие от образцов из предыдущих кампаний, новая версия вредоносного файла не запустится, если в системе не установлена русская раскладка клавиатуры.

ПРОТОКОЛ

проведения служебного расследования по фактам, выявленным в ходе контрольных мероприятий в сфере ДМС

«25» августа 2025 г. № 41-ДМС

Москва

В соответствии с приказом Генерального директора от 11.07.2025 № 82 «О проведении служебного расследования», комиссия в составе:

Председатель комиссии:

— Первый заместитель начальника дирекции,

Члены комиссии

— Ведущий эксперт заместитель директора

— Заместитель начальника дирекции по безопасности,

— Начальник управления медицинской деятельности,

провела служебное расследование по выявленным в первом полугодии 2025 года фактам, установленным в ходе медико-экономической экспертизы (МЭЭ) и экспертизы качества медицинской помощи (ЭКМП), проведённых в рамках плановых контрольных мероприятий по программам добровольного медицинского страхования (ДМС).

Установлено:

1. В ходе анализа страховых случаев были выявлены обращения за медицинской помощью, вызывающие обоснованные сомнения в их достоверности.

Документ-приманка

Новая версия BrockenDoor

Исполняемый файл — это модифицированная версия бэкдора BrockenDoor. Его функциональность не претерпела значительных изменений, однако основной вредоносный код был полностью переписан на языке C#. Список команд бэкдора практически идентичен тому, что мы описывали ранее, хотя в этой версии вместо

полных названий команд используются сокращения до двух-трех символов. Так, например, команда `set_poll_interval` стала называться `spi`, а `run_program` — `rp`.

Команда	Описание
spi	Ранее называлась **set_poll_interval**. Изменить интервал опроса командных центров (по умолчанию равен 5 секундам)
rp	Ранее **run_program**. Создать на диске файл, переданный с командного центра, и запустить его. Команда предусматривает следующие подкоманды: **sy** (ранее **system**) и **we** (ранее **win_exec**): использовать Process.Start() для запуска **se** (ранее **shell_exec**) и **cp** (ранее **create_process**): использовать Process.Start() для запуска, но с дополнительными параметрами в структуре ProcessStartInfo: CreateNoWindow = true, UseShellExecute = false и WindowStyle = ProcessWindowStyle.Hidden
sd	Ранее **self_destruct**. Удалить себя через команду: powershell.exe Start-Sleep 5; Remove-Item «$selfname» -Force
ec	Ранее **exec_command**. Выполнить команду, используя интерпретатор командной строки. Допускает следующие подкоманды: **cm** (ранее **cmd**): выполнить команду cmd.exe /C $command **ps** (ранее **powershell**): выполнить команду powershell.exe -noprofile -command «$command»
rl	На момент написания статьи не была реализована

Бэкдор ZeronetKit

В одном из случаев в качестве полезной нагрузки BrockenDoor загружал и выполнял ZeronetKit. Это бэкдор, написанный на Go, который используется в атаках группы BO Team. Он получил свое название за строку `ZeroNet by Vegas`, присутствующую в ранних версиях. ZeronetKit был впервые обнаружен в конце 2024 года, и его функциональность сводилась к четырем командам.

Номер команды	Описание
0x01	Запуск скрытой удаленной консоли (cmd.exe) с перенаправлением ввода/вывода
0x08	Отправка файлов с зараженной системы на C2
0x09	Получение файлов с C2 и сохранение их в зараженной системе
0x10	Создание туннеля TCP/IPv4

Взаимодействие с C2 обеспечивается по протоколам HTTPS и WebSocket, а для разделения потоков данных внутри соединения используется библиотека Yamux (Yet another Multiplexer).

В июне 2025 года появилась обновленная версия ZeronetKit (6fe8943f364f6308c2e46910bffefeaf), в которую были добавлены команды с номерами 0x18 и 0x22.

Номер команды	Описание
0x18	Скачивание с C2 шелл-кода, его настройка в памяти и запуск в отдельном потоке
0x22	Обновление интервала взаимодействия с C2

В сентябре 2025 года мы зафиксировали попытку BrockenDoor скачать новую версию бэкдора ZeronetKit (12772caa05f2c28ebe8c99abb35ac39c). Для этого BrockenDoor вызывал PowerShell с командной строкой, полученной от C2. Как и в предыдущей версии, базовые настройки взаимодействия с C2 и список доменов, использующихся в качестве C2, хранятся в исходном исполняемом файле. Однако теперь при запуске бэкдор проверяет наличие ключей реестра beh и в HKCU\Software\Windows\Applets\Config и, если они существуют, данные из них используются в качестве списка C2 и интервала взаимодействия. Эти данные обновляются при помощи соответствующих команд (0x22 и 0x24). Если ключи реестра не обнаружены, используются базовые настройки. Команда под номером 0x18 по-прежнему присутствует, однако теперь представляет собой заглушку. Кроме того, были добавлены две новые команды (0x26 и 0x29), тем не менее они также не реализуют вредоносных действий.

Номер команды	Описание
0x01	Запуск скрытой удаленной консоли (cmd.exe) с перенаправлением ввода/вывода
0x08	Отправка файлов с зараженной системы на C2

0x09	Получение файлов с C2 и сохранение их в зараженной системе
0x10	Создание туннеля TCP/IPv4 (IPv6)
0x18	Объявлена, реализована в виде заглушки
0x22	Обновление интервала взаимодействия с C2 (при наличии записи в реестре HKCU\Software\Windows\Applets\Config:beh)
0x24	Обновление списка C2 (при наличии записи в реестре HKCU\Software\Windows\Applets\Config:ad)
0x26	Объявлена, реализована в виде заглушки
0x29	Объявлена, реализована в виде заглушки

ZeronetKit не способен самостоятельно закрепляться в зараженной системе, поэтому злоумышленники при помощи BrockenDoor копируют скачанный бэкдор в автозагрузку.

```
1 "cmd.exe" /C copy "$appdata\Microsoft\msfch.exe" "%APPDATA%\Microsoft\Windows\Start Menu\Programs\startup"
```

Заключение

Мы продолжаем отслеживать активность группы BO Team. В своей последней кампании злоумышленники обновили инструментарий: уже знакомый нам бэкдор BrockenDoor был переписан на C#, а в зловред ZeronetKit, также известный с 2024 года, были добавлены новые команды для сетевой коммуникации.

Жертвами этих атак стали российские компании в различных сферах. Злоумышленники представлялись поставщиками услуг страхования и банковскими организациями. При этом стоит отметить, что фишинговые письма, ставшие вектором проникновения в инфраструктуру пострадавших компаний, а также документы-приманки, скорее всего, создавались под конкретные цели: атакующие не использовали типовые шаблоны, а адаптировали вложения в каждой атаке под юридические документы, призывая жертву срочно ознакомиться с их содержанием.

Для защиты от этой угрозы мы рекомендуем применять комплексные защитные решения, которые позволят выстроить гибкую и эффективную систему безопасности, включающую в себя надежную защиту рабочих мест, сбор и анализ данных о событиях безопасности со всех источников в инфраструктуре, выявление и остановку атак любой сложности на ранних стадиях и обучение сотрудников базовым навыкам цифровой грамотности. Комбинации таких решений под потребности компании любого масштаба содержатся в уровнях новой линейки продуктов для защиты бизнеса Kaspersky Symphony.

Индикаторы компрометации

Хэши файлов

BrockenDoor .NET

070a2ffca59750da411dec500343e416	Кредитный Договор_[redacted]
0d6cac44a709deae78dceb7e776c3d04	ao [redacted]_протокол проведения служебного расследования_41-дмс
6a9b2384a93ff47a7006771dc32b837e	ao [redacted]_приказ проведения служебного расследования_82
9034c24a153d3ac199652acd305ce212	удостоверение адвоката_[redacted]
db605d3f3fcfa2c3c19f0cabfb9764db	мировое соглашение
e0e91afe88da0fedfc748bb0ab5a7ad8	договор об оказании правовой помощи
e51554d5e11f27bf981c8e63b8a091d1	Договор поручительства_13.03.24
f24deac452e684e216f43055fc26258a	справка-расчет_[redacted]

ZeronetKit

4793753ef5800f2adc088e359d61b793	Декабрь 2024
8351fa0448a85ffe8bcd1fbef20ed801	Январь 2025
9f1eca64a49c2accf8770e9fd932402a	Февраль 2025
c99e34cac21fefe10eaf3303ff447131	Март 2025
373b22dca89f57c138c83cb99a6c6120	

9b7695bfbff339d78a58eb528e13c784 5c8887f6bbfd92134523e8e49c701112	
6c3deaa478e0e19c8757e1ba5ba1dd5a	Апрель 2025
5ac1fec6ac88fad7779e914b2b48fad3 6fe8943f364f6308c2e46910bffefeaf 71612ebcc591b2475d3488e5580db56a	Июль 2025
9f136dfe7c89d7581341055d49832835	Август 2025
e500b01182c00f05a448842270723e23 5bfcb7f54e2804a86630823e7a567396 12772caa05f2c28ebe8c99abb35ac39c 732fe189bedda7cf4bb944e954b49685 7430e63b949c45f99381116ad85127e3 7dd08b7116a9007a776483ec9234e11d ceed053bdab80f7ff6dd9925bf8fc1de 3fde2928159c5c5ab54e51e91f4553b1	Сентябрь 2025

Сетевые индикаторы

BrockenDoor C&C

213.165.60[.]118

ZeronetKit C&C

invuln[.]xyz
lizzardsnails[.]online
railradman[.]site
easybussy[.]space
urbantvpn[.]online
icecoldwind[.]online
wholewell[.]online

URL-адреса

hxxps://mgutu-vf[.]ru/js/scripts/msfch.zip
hxxps://mgutu-vf[.]ru/js/scripts/msfch.exe
hxxps://mgutu-vf[.]ru/js/scripts/msfch5.exe
hxxps://mgutu-vf[.]ru/js/scripts/msfch3.exe
hxxps://mgutu-vf[.]ru/js/scripts/msfch15.exe

Обновленные инструменты группировки BO Team