Break the silence: Kazakhstan-nexus UAT-6275 targets CIS government organizations

By Ashley Shen

Published: 2026-10-14 · Archived: 2026-10-30 02:00:51 UTC

Wednesday, October 14, 2026 10:00

This research was conducted jointly with Julian-Ferdinand Vögele of Recorded Future's Insikt Group. Details of the joint research and presentation are available here.

- Cisco Talos identified UAT-6275 (TAG-193 by Recorded Future) activity targeting government organizations across the Commonwealth of Independent States (CIS). Recovered artifacts show additional interest in water resources and energy. This focus is consistent with intelligence collection and may reflect the regional effects of the Russia–Ukraine war.
- In activity observed from June 2025 through August 2026, Talos identified four infection-chain types that use macro-enabled documents, PS2EXE downloaders, GitHub-hosted PowerShell, and a crafted WinRAR archive exploiting CVE-2025-8088. The recovered payloads include several custom reverse shells that provide interactive remote access.
- Three publicly accessible staging directories and GitHub repository history exposed payload builds, tool inventories, and changes to command-and-control (C2) infrastructure. These operational security lapses gave us direct visibility into the group's recent activity.
- The files recovered from the exposed infrastructure suggest preparation for post-compromise operations and potential activity against Linux hosts and internet-facing appliances.
- Talos assesses with medium confidence that UAT-6275 has a Kazakhstan nexus, based on infrastructure access, language artifacts, sample submissions, working hours analysis, and regional targeting interests.

Background

Cisco Talos and Recorded Future Insikt Group jointly investigated UAT-6275 activity targeting government organizations across the Commonwealth of Independent States (CIS). The investigation uncovered three publicly accessible staging directories and a previously unreported GitHub repository used to host malicious scripts and payloads. These exposed assets provided visibility into the threat actor's malware development, infrastructure changes and preparations for additional intrusion activity.

Talos tracks this activity as UAT-6275, while Recorded Future tracks it as TAG-193. It overlaps with Silent Lynx (first reported by Seqrite) and sits within a broader set of campaigns connected to YoroTrooper, which we first reported in 2023. Subsequent research on Tomiris (Kaspersky), ShadowSilk (Group-IB), Cavalry Werewolf (BI.ZONE), and Hydra Saiga (VMRay) identified overlapping indicators across these reported clusters. We assess that UAT-6275 and YoroTrooper likely belong to the same broader activity cluster. However, we continue to track them separately because we have not observed direct indicator or toolset overlap between the two.

This post summarizes our joint Virus Bulletin 2026 white paper, "Break the silence: tracking Silent Lynx through exposed infrastructure" which contains the full technical analysis and indicators of compromise (IOCs).

Victimology

UAT-6275's targeting is concentrated in Central Asia and the wider CIS region. Across the reviewed campaigns, observed victims and lure themes span nine countries: Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan, Armenia, Azerbaijan, Russia, and Belarus.

Figure 1. Regional targeting.

Government and diplomatic affairs

UAT-6275 targets government institutions responsible for diplomacy, economic development, agriculture, and environmental management. These organizations hold information that can inform bilateral negotiations, economic planning, and regional security decisions.

Our network flow analysis identified activity involving a Tajik government entity shortly after treaty discussions with Kazakhstan in March 2026 and a Belarusian government entity ahead of a bilateral meeting in April. This timing may indicate an interest in regional diplomatic developments.

The decoy documents we recovered also suggest an interest in diplomatic relations, international trade, and aviation. Examples include a diplomatic letter addressed to Armenia's Ministry of Foreign Affairs.

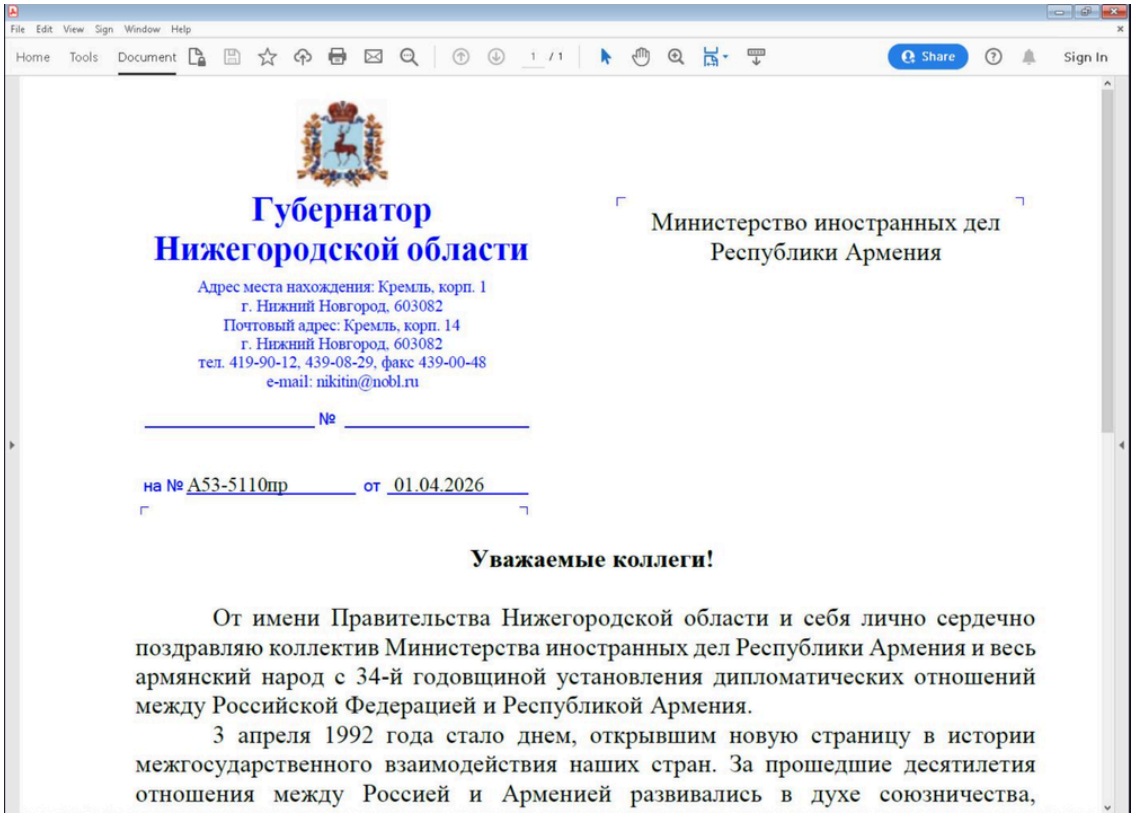

Figure 2. Lure document masquerading as a Russian diplomatic congratulatory letter to the Armenian Ministry of Foreign Affairs.

Water security and resource management

The group's interest in regional resources spans environmental management and energy. Talos observed activity involving an Armenian government entity responsible for environmental matters and Uzbekistan's Smart Forestry initiative, consistent with earlier reporting on Silent Lynx targeting water resource organizations across Central Asia.

Energy-themed decoys included a cooperation proposal between Turkmenistan's state oil company, Turkmennebit, and Russia's Orsk Oil Refinery, used in an August 2025 sample. The refinery supplies petroleum products to Kazakhstan and later shut down after a Ukrainian drone strike in August 2026, with repairs expected to take up to six months. These ties suggest a possible intelligence interest in regional fuel supplies and the war's implications for Kazakhstan's energy security.

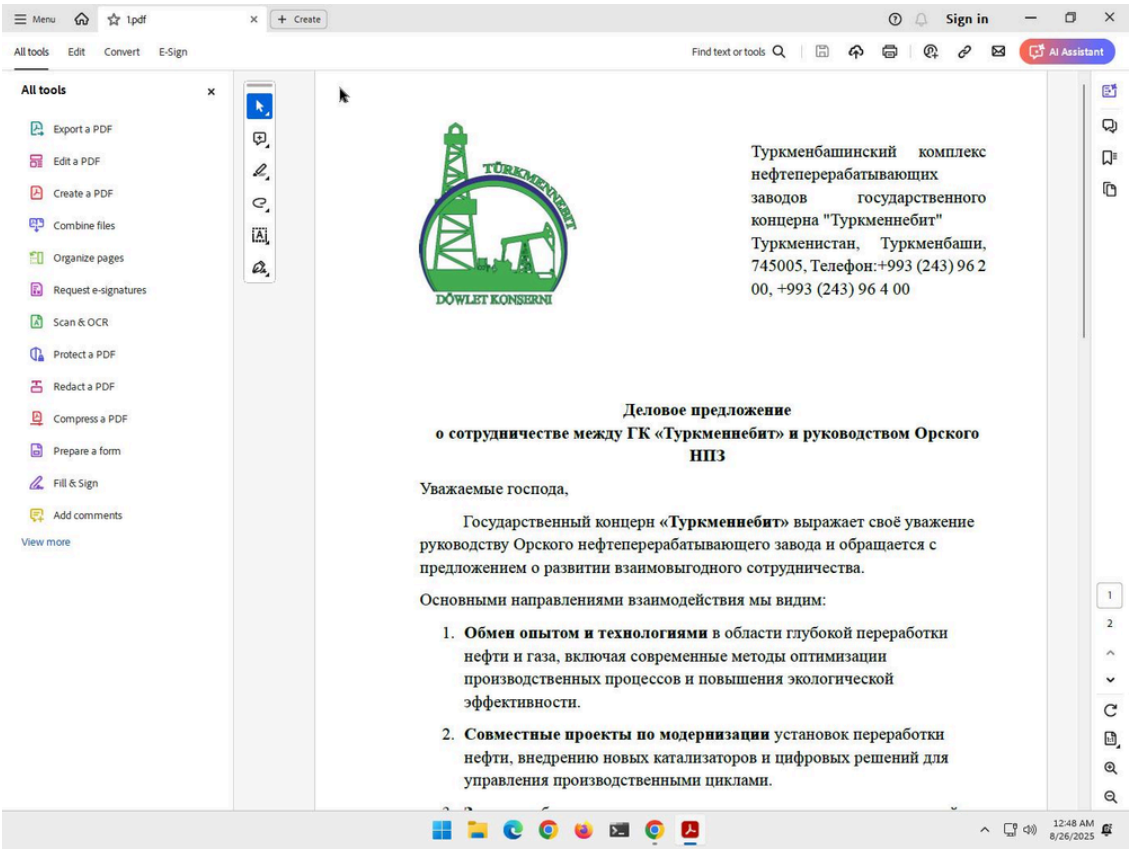

Figure 3. Decoy impersonating Turkmennebit and proposing cooperation with Orsk Oil Refinery management.

Campaign timeline

Since Seqrite first reported Silent Lynx in January 2025, we have identified at least eight campaigns across the region through May 2026. These include malware delivery targeting Russia, Turkmenistan, and Uzbekistan; a credential-harvesting site impersonating Azerbaijan's State Agency for Public Service; and lures referencing the China–Central Asia Summit and Russian energy infrastructure. In 2026, we also observed activity involving government entities in Tajikistan, Armenia, and Belarus, as well as Uzbekistan's Smart Forestry initiative in May.

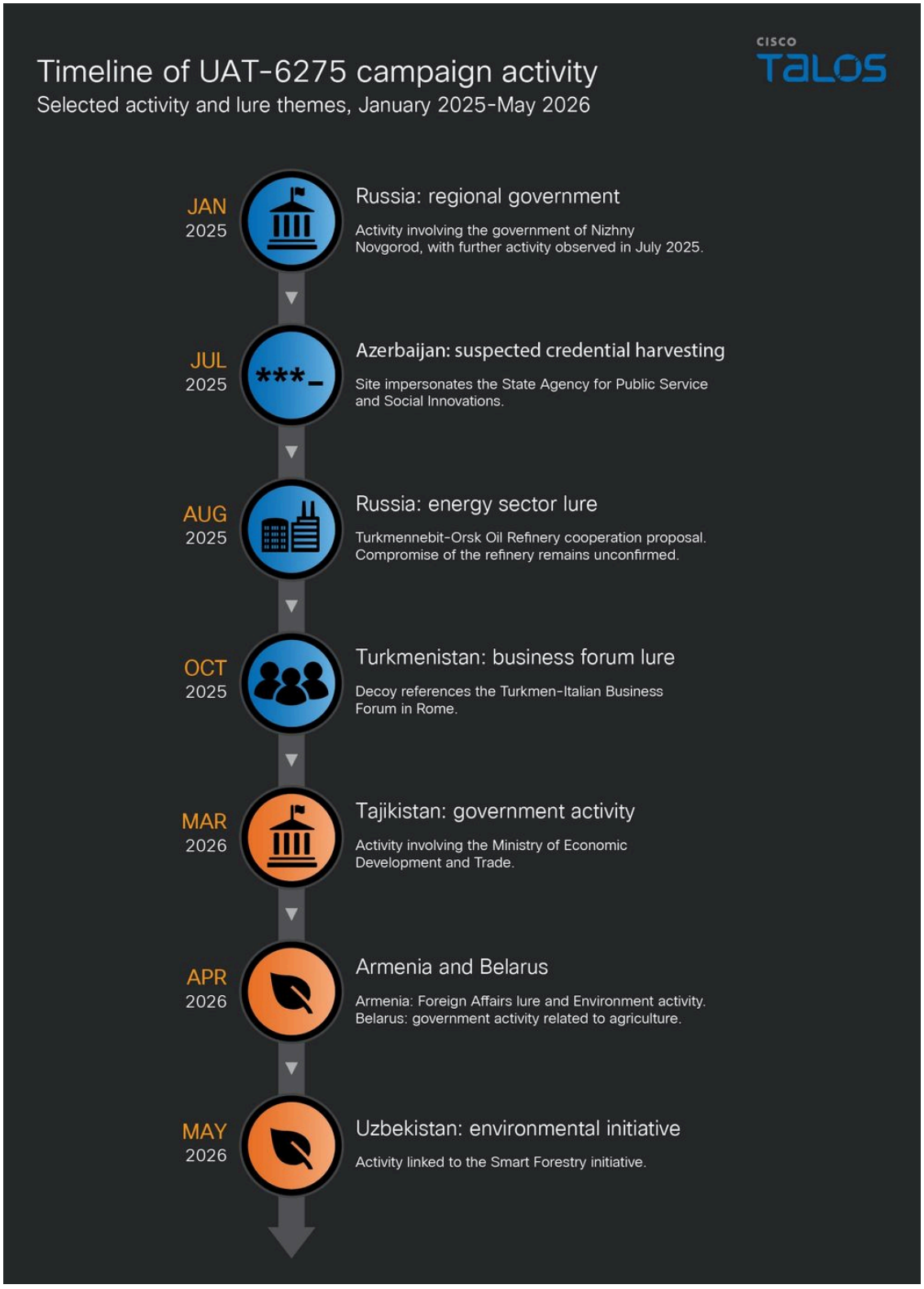

Figure 4. Campaign timeline.

Infrastructure and malware delivery

Talos identified three publicly accessible staging directories containing malware and tools of UAT-6275. One sample led to the previously unreported GitHub repository, where the group hosted PowerShell scripts and payloads. Its commit history allowed us to track infrastructure changes and malware development.

The group relies on lightweight reverse shells, including Chvost, Laplas, and PickleShell, to issue commands on compromised systems.

We also recovered Linux-compatible tooling and a publicly available proof-of-concept exploit for FortiWeb CVE-2025-25257 from UAT-6275 infrastructure. These findings suggest interest in expanding the group's operational capabilities.

Four infection chains

UAT-6275 used malicious documents, executable downloaders, and shortcuts to deliver malware, and later incorporated a WinRAR exploit. Talos categorized the recovered samples into four infection chains, A – D, based on how they retrieve and execute their payloads.

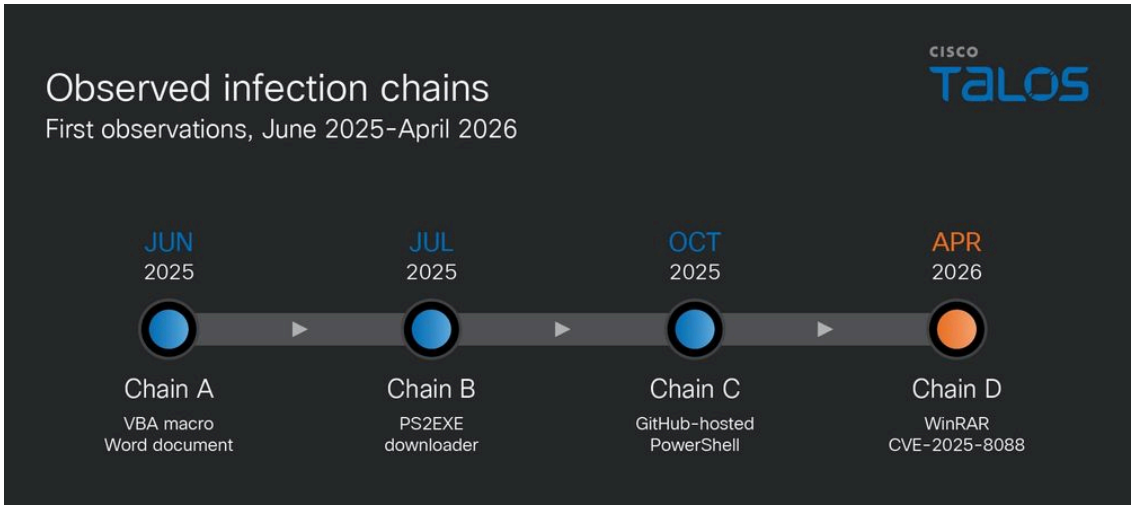

Figure 5. First observations of four UAT-6275 infection chains, June 2025 – April 2026.

The first Chain A samples, observed in June 2025, used macro-enabled Word documents to download and execute a second-stage binary. In July 2025, we observed Chain B downloaders built with PS2EXE, a tool that packages PowerShell scripts as standalone Windows executables. These downloaders retrieved reverse-shell payloads and created scheduled tasks for persistence.

We first observed Chain C in October 2025. A malicious shortcut launches PowerShell to retrieve and execute a GitHub-hosted script that provides remote shell access. Later samples also downloaded PickleShell and placed it in the Windows Startup folder for persistence.

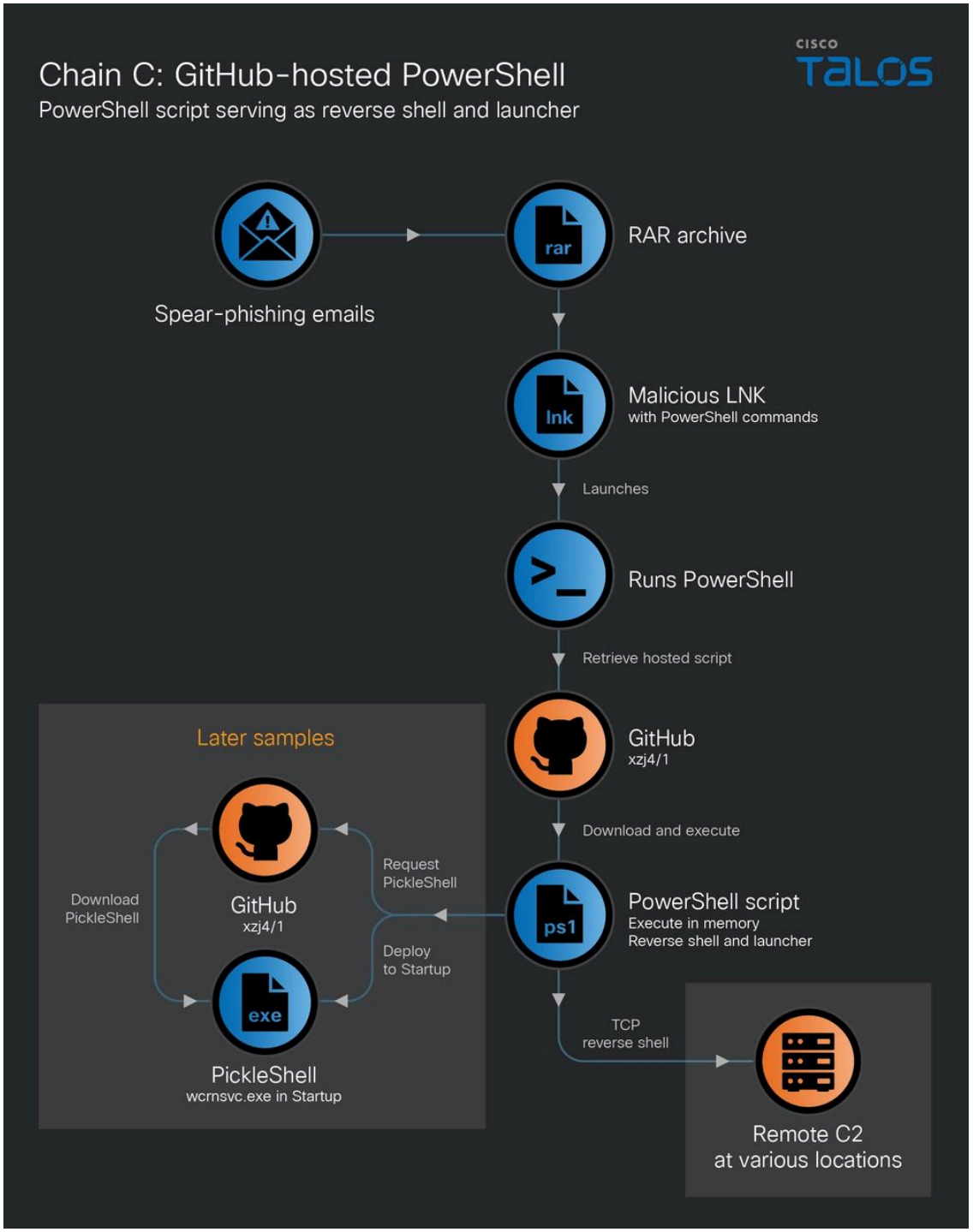

Figure 6. Chain C retrieves a GitHub-hosted PowerShell script; later samples also deploy PickleShell to the Startup folder.

In April 2026, we identified a RAR archive that exploited CVE-2025-8088 in WinRAR to place PickleShell in the Windows Startup folder (Chain D). The payload runs at the next user sign-in. This was the first vulnerability exploit we observed in UAT-6275's malware delivery.

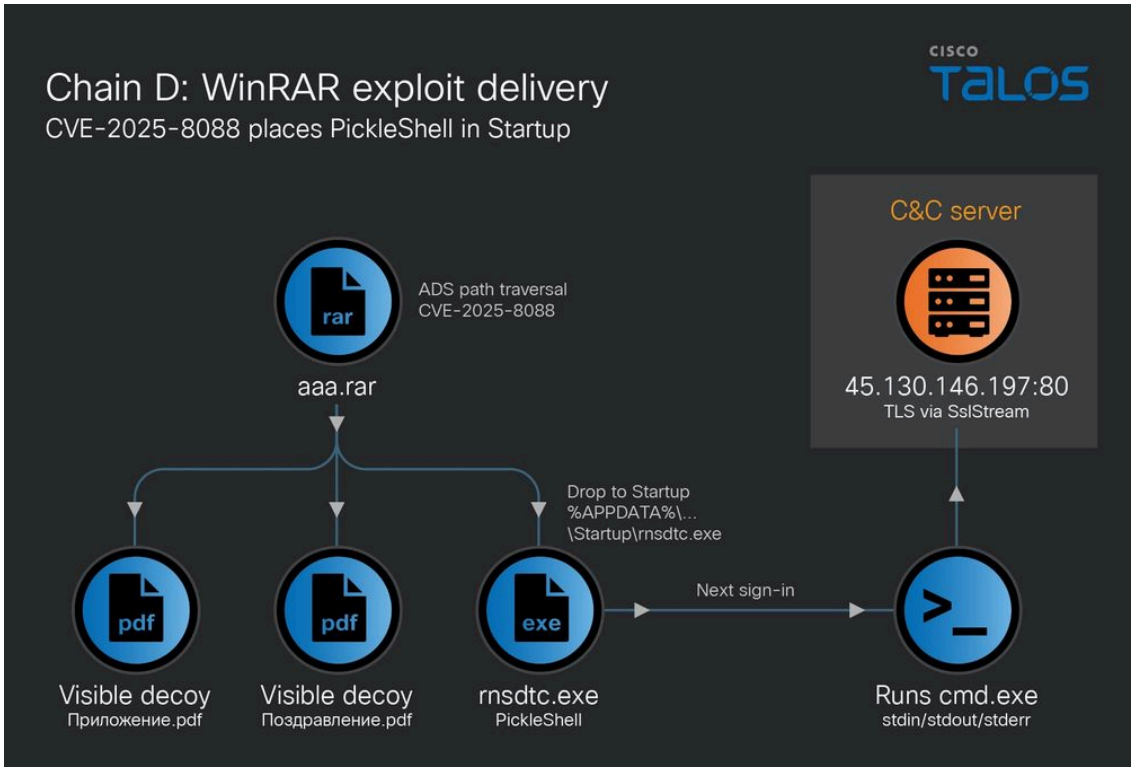

Figure 7. Chain D exploits CVE-2025-8088 to place PickleShell in the Windows Startup folder for execution at the next sign-in.

Kazakhstan nexus assessment

Talos assesses with medium confidence that UAT-6275 has a Kazakhstan nexus. Supporting evidence includes Russian-language artifacts, apparent malware-testing submissions from Kazakhstan shortly after compilation, and operator activity consistent with UTC+5 working hours.

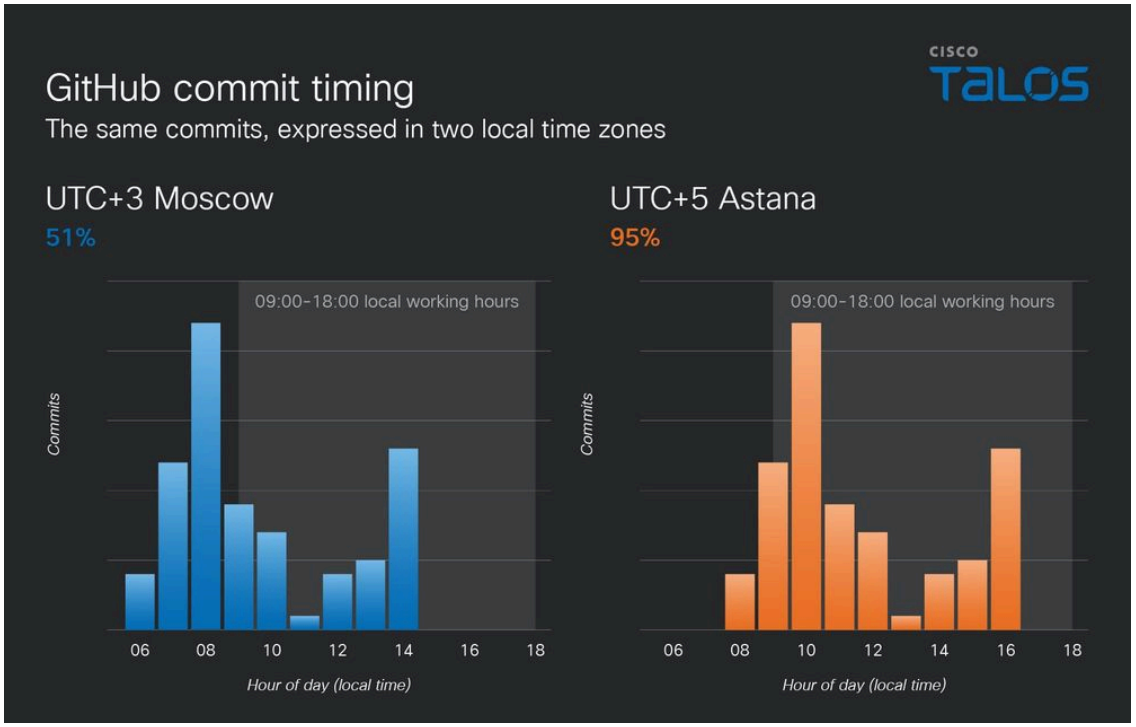

Figure 8. Timing of 77 GitHub commits in UTC+3 and UTC+5, with 09:00–18:00 local working hours shaded.

Looking ahead

UAT-6275's sustained activity and adoption of new delivery techniques suggest the group will continue pursuing access to government organizations across Central Asia and the CIS. Its interest in environmental agencies, economic ministries, and energy infrastructure reflects the intelligence value of regional diplomacy and resource management.

Defenders in these sectors should monitor unexpected PowerShell activity and payload downloads from public services such as GitHub, alongside scheduled tasks and Startup-folder changes. Keeping archive utilities patched can help reduce exposure to the exploit-assisted delivery observed in this campaign.

For further details on this research and our accompanying presentation, see "Break the Silence: Tracking Silent Lynx Through Exposed Infrastructure" on Virus Bulletin's website, as well as Recorded Future's related blog post.

Coverage

The following ClamAV signatures detect and block this threat:

- Win.Backdoor.PickleShell-10060602-0
- Win.Backdoor.Chvost-10060603-0
- Win.Malware.Generic-10060604-0
- Win.Malware.LAPLAS-10060605-0
- Win.Malware.LAPLAS-10060606-0
- Win.Proxy.Generic-10060628-0

The following Snort rules cover this threat:

- Snort 2: 1:11192, 1:15306, 1:46983, 1:47398
- Snort 3: 1:46983, 4:16

IOCs

IOCs for this research can be found at our GitHub repository here.

Source: https://blog.talosintelligence.com/break-the-silence-kazakhstan-nexus-uat-6275-targets-cis-government-organizations/