SILENT LYNX

[/ ˈsaɪ.lənt lɪŋks /]

Silent Lynx is a likely Kazakhstan-based APT active since late 2024, focused on espionage against governments and banks in Central Asia. Assessed as high risk, it uses multi-stage loaders, PowerShell, and Golang implants with Telegram bots for C2, seen in recent Kyrgyzstan and Turkmenistan campaigns, with expansion into Eastern Europe.

IDENTITY

Attribution	: Likely Central Asian threat actor, suspected origins in **Kazakhstan**.
Active Since	: At least **late 2024**, with active campaigns into 2025.
Aliases	: Silent Lynx (no widely accepted alternative names yet).
Motivation	: Espionage-focused — intelligence collection against governments, banks, and policy-making institutions in Central Asia.

TTPs

Initial Access	• **Spear-phishing emails** with RAR/ISO attachments, leveraging compromised accounts (e.g., Kyrgyz government bank employee). • **Thematic lures:** UN economic meeting invitations, Ministry of Finance bonus distribution orders.
Execution	• **C++ loader executables** embedded in ISO files. • **PowerShell** scripts decoded from within the C++ binaries, used for RAT functionality and persistence. • **Golang implants** establishing reverse shells.
Persistence	• **Multi-stage loaders** (ISO -> C++ loader -> PowerShell RAT). • **Telegram bots** for persistent C2 channel.
Privilege Escalation / Defense Evasion	• **Decoy documents** (UNESCAP invitations, government forms) to distract targets. • **Encoded PowerShell commands** (Base64) to evade detection. • **Use of legitimate cloud services** (Google Drive, Pastebin) for payload hosting.
Command & Control (C2)	• **Telegram Bots:** (@south_korea145_bot, @south_afr_angl_bot) for command execution & exfiltration. • **Custom domains:** pweobmxdlboi[.]com, others for payload hosting. • **Golang reverse shell** connecting to 185.122.171[.]22:8082.
Discovery / Lateral Movement / Collection	• Focused primarily on **exfiltration of sensitive financial/government documents.** • Limited observed lateral movement — operations appear **surgical and targeted.**
Exfiltration	• **Telegram-based exfiltration** of harvested data. • **Google Drive & Pastebin** leveraged as staging/exfiltration infrastructure.
Malware & Tools	• **C++ Loaders** (embedded with decoy docs + PowerShell payloads). • **PowerShell RATs** (multi-stage, Telegram-controlled). • **Golang reverse-shell implants** (custom, lightweight).

TARGET PROFILE

Target Sectors	• **Government ministries** (Finance, economics, digitalization). • **National banks & government-backed financial institutions.** • **Embassies and legal advisors.** • **Regional think tanks** focused on economic policy.
Geographies Targeted	• **Primary:** Kyrgyzstan, Turkmenistan. • **Secondary:** Broader Central Asia (SPECA nations, e.g., Uzbekistan, Tajikistan).

THREAT ASSESSMENT

Risk Level	: **High** — targeted espionage with sophisticated multi-stage infection chains.
Most Recent Activity	• **Dec 2024:** Campaign using UN-themed lure, ISO loader, PowerShell RAT via Telegram bots, targeting National Bank of Kyrgyz Republic. • **Jan 2025:** Campaign using Ministry of Finance lure, RAR with Golang implant, reverse shell to C2 server.
Evolution	: Rapid transition from C++ loaders + PowerShell payloads to **hybrid PowerShell/Golang toolset**.
Overlap	: Tactical similarities with **YoroTrooper (SturgeonPhisher)** campaigns in CIS.

NOTABLE OPERATIONS

- **Dec 2024:** UNESCAP-themed ISO file delivering **C++ loader + PowerShell RAT;** targeting **National Bank of Kyrgyz Republic.**
- **Jan 25: Ministry of Finance lure**; malicious RAR archive with **Golang reverse shell implant**, C2 to 185.122.171[.]22:8082.
- **Ongoing 2025:** Expanded espionage activity against Kyrgyzstan & Turkmenistan ministries, banks, and think tanks.

ANALYST NOTES (Defensive Takeaways)

- Harden defenses against RAR/ISO phishing lures with attachment filtering.
- Monitor for Telegram-based C2 traffic in government/banking networks.
- Track for outbound connections to suspicious infrastructure (pweobmxdlboi[.]com, 185.122.171[.]22).
- Detect Base64-encoded PowerShell executions and investigate anomalies.
- Apply regional threat intelligence — Silent Lynx is highly focused on Central Asia and finance/government targets.