Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

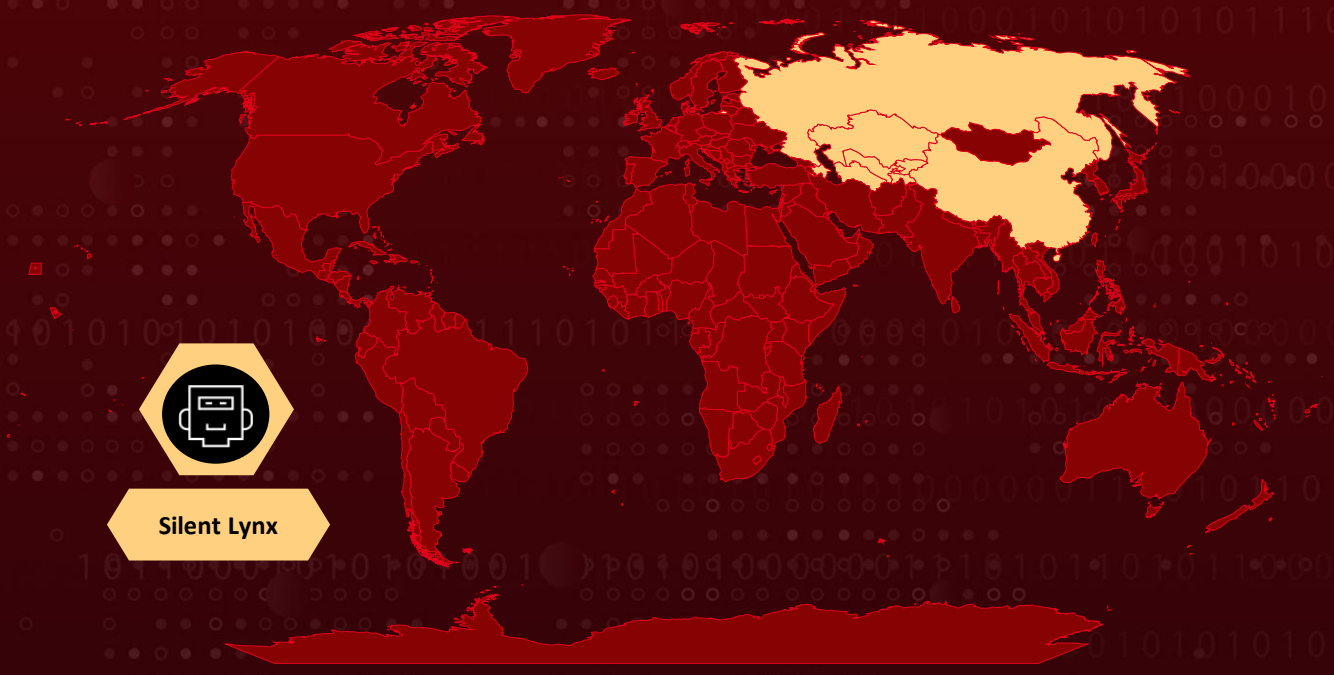
Silent Lynx APT: Espionage Operations Targeting Central Asia's Critical Infrastructure

Date of Publication	Admiralty Code	TA Number
November 6, 2025	A1	TA2025337

Summary

First Seen: Late 2024
Targeted Regions: Central Asia (Tajikistan, Kazakhstan, Kyrgyzstan, Turkmenistan, Uzbekistan), Russia, Azerbaijan, China
Targeted Platforms: Windows
Targeted Industries: Government, Diplomats, Think-tanks, Finance, Mining, Transport & Communications
Threat Actor: Silent Lynx (aka YoroTrooper, Sturgeon Phisher, Cavalry Werewolf, ShadowSilk)
Malware: Silent Loader, LAPLAS, SilentSweeper
Campaign: Operation Peek-a-Baku
Attack: Silent Lynx is an APT group conducting espionage across Central Asia since late 2024, targeting government, diplomatic, and infrastructure entities through phishing campaigns themed around regional summits. Their operation “Peek-A-Baku” uses malicious RAR or ZIP attachments that deploy PowerShell-based loaders and custom implants like Silent Loader and LAPLAS. The group leverages GitHub, Ligolo-ng, and Telegram for command-and-control, blending legitimate services with malicious traffic. Ongoing activity indicates sustained intelligence-gathering focused on Central Asian geopolitical and economic affairs.

Attack Regions



Attack Details

#1

Silent Lynx is an Advanced Persistent Threat (APT) group active since late 2024, conducting cyber-espionage campaigns primarily across Central Asia, with a focus on governmental, diplomatic, financial, and strategic infrastructure sectors. The campaign, tracked as Operation "Peek-A-Baku", seeks to collect sensitive political and economic intelligence, especially information related to regional initiatives under the UN Special Programme for the Economies of Central Asia (SPECA). Attribution analysis suggests the actor may operate out of Kazakhstan, with notable overlaps in tooling and objectives with the espionage group YoroTrooper, indicating potential shared resources or collaboration.

#2

The group's targeting is highly selective and aligned with key geopolitical events. Lures often reference diplomatic summits and strategic cooperation meetings in Dushanbe, Astana, and Baku, using email attachments themed around policy or infrastructure topics such as mining and transport corridors, including the China-Tajikistan Highway. These spear-phishing campaigns use RAR or ZIP archives containing malicious LNK or ISO files, which deliver PowerShell stagers disguised behind decoy documents. While the social-engineering content is contextually relevant, language inconsistencies in filenames suggest automation or non-native Russian proficiency.

#3

Technically, Silent Lynx uses a multi-stage infection chain that combines custom malware with open-source utilities. The attack sequence typically begins with an LNK shortcut that launches a Base64-encoded PowerShell script, hosted on GitHub, to download and execute implants. Key tools include Silent Loader (C++ loader with PowerShell payloads), LAPLAS (C++ reverse shell using TCP/TLS), and SilentSweeper (.NET implant). To maintain access and conceal activity, the group employs Ligolo-ng, an open-source tunneling tool, allowing encrypted command and data traffic to flow through compromised hosts.

#4

Silent Lynx's infrastructure spans multiple countries, with command-and-control (C2) servers identified in Russia and the Netherlands. Some variants also use Telegram bots with hardcoded tokens for issuing commands and exfiltrating data, a tactic that enhances stealth but has also exposed operational details during analysis. The actor demonstrates moderate technical capability, relying on persistent reuse of infrastructure, open-source tooling, and encoding techniques that balance simplicity with effectiveness against traditional defenses.

Recommendations

Restrict PowerShell usage: Enforce Constrained Language Mode for non-admin users. Enable PowerShell Script Block Logging and Module Logging (Event IDs 4103, 4104) to capture encoded commands.

Block risky file types: Configure email gateways to quarantine RAR, ISO, and LNK attachments, which Silent Lynx uses in phishing campaigns. Use sandbox detonation for compressed or password-protected archives before delivery.

Monitor encoded command patterns: Hunt for powershell.exe instances using -EncodedCommand, -nop, or -w hidden arguments. Alert on any PowerShell execution chained from explorer.exe, winword.exe, or Outlook processes.

Network filtering: Block known C2 IPs and domains. Detect outbound traffic to GitHub raw URLs used as payload hosts. Monitor for Ligolo-ng tunneling behavior unusual, persistent TLS or TCP connections to unfamiliar IPs on nonstandard ports.

Application allowlisting: Use Windows AppLocker or WDAC to prevent execution of unauthorized binaries and scripts in user directories.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0010 Exfiltration
TA0005 Defense Evasion	TA0004 Privilege Escalation	TA0011 Command and Control	T1053 Scheduled Task/Job
TA0011 Command and Control	T1566.001 Spearphishing Attachment	T1566 Phishing	T1204 User Execution

T1027 Obfuscated Files or Information	T1059 Command and Scripting Interpreter	T1027.013 Encrypted/Encoded File	T1204.002 Malicious File
T1204.001 Malicious Link	T1106 Native API	T1053.005 Scheduled Task	T1053 Scheduled Task/Job
T1059.001 PowerShell	T1036 Masquerading	T1095 Non-Application Layer Protocol	T1090 Proxy
T1041 Exfiltration Over C2 Channel	T1059.005 Visual Basic	T1547.009 Shortcut Modification	T1547 Boot or Logon Autostart Execution
T1071.001 Web Protocols	T1071 Application Layer Protocol	T1572 Protocol Tunneling	T1567 Exfiltration Over Web Service

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	62[.]113[.]66[.]137, 206[.]189[.]11[.]142, 62[.]113[.]66[.]7, 37[.]18[.]27[.]27, 62[.][.]113[.]66[.]7
Host Names	updates-check-microsoft[.]ddns[.]net, catalog-update-update-microsoft[.]serveftp[.]com
URL	hxxp[:]//206[.]189[.]11[.]142/

TYPE	VALUE
SHA256	ef627bad812c25a665e886044217371f9e817770b892f65cff5877b02458374e, 5b58133de33e818e082a5661d151326bce5eeddea0ef4d860024c1dbb9f94639, 5bae9c364ee4f89af83e1c7d3d6ee93e7f2ea7bd72f9da47d78a88ab5cfbd5d4, 72a36e1da800b5acec485ba8fa603cd2713de4ecc78498fcb5d306fc3e448c7b, 5e3533df6aa40e86063dd0c9d1cd235f4523d8a67d864aa958403d7b3273eaaf, b58f672e7fe22b3a41b507211480c660003823f814d58c04334ca9b7cdd01f92, ae51aef21ea4b422ef0c7eb025356e45d1ce405d66afbb3f6479d10d0600bcfd, 0bce0e213690120afc94b53390d93a8874562de5ddcc5511c7b9b9d95cf8a15d, 821f1ee371482bfa9b5ff1aff33705ed16e0147a9375d7a9969974c43b9e16e8, 262f9c63c46a0c20d1feecbd0cad75dcb8f731aa5982fef47d2a87217ecda45b, 123901fa1f91f68dacd9ec972e2137be7e1586f69e419fc12d82ab362ace0ba9, 6cb54ec004ff8b311e73ef8a8f69b8dd043b7b84c5499f4c6d79d462cea941d8, 97969978799100c7be211b9bf8a152bbd826ba6cb55377284537b381a4814216, 9de8bbc961ff450332f40935b739d6d546f4b2abf45aec713e86b37b0799526d, b5a4f459bdff7947f27474840062cfce14ee2b1a0ef84da100679bc4aa2fcf77, ffda4f894ca784ce34386c52b18d61c399eb2fc8c9af721933a5de1a8fff9e1b, 2c8efe6eb9f02bf003d489e846111ef3c6cab32168e6f02af7396e93938118dd, 1531f13142fc0ebfb7b406d99a02ec6441fc9e40725fe2d2ac11119780995cd3, 67cf0e32ad30a594442be87a99882fa4ac86494994eee23bdd21337adb804d3f, 036a60aa2c62c8a9be89a2060e4300476aef1af2fd4d3dd8cac1bb286c520959, 32035c9d3b81ad72913f8db42038fcf6d95b51d4d84208067fe22cf6323f133c,

TYPE	VALUE
SHA256	a639a9043334dcd95e7cd239f8816851517ebb3850c6066a4f64ac39281242a3, a83a8eb3b522c4517b8512f7f4e9335485fd5684b8653cde7f3b9b65c432fa81, 26aca51d555a0ea6d80715d8c6a9f49fea158dee11631735e16ea75c443a5802, 303f03ae338fddfe77c6afab496ea5c3593d7831571ce697e2253d4b6ca8a69a, 40d4d7b0bc47b1d30167dd7fc9bd6bd34d99b8e0ae2c4537f94716e58e7a5aeb, b0ac155b99bc5cf17ecfd8d3c26037456bc59643344a3a30a92e2c71c4c6ce8d, b87712a6eea5310319043414eabe69462e12738d4f460e66a59c3acb5f30e32e

References

https://www.seqrite.com/blog/operation-peek-a-baku-silent-lynx-apt-dushanbe-espionage/

https://hivepro.com/threat-advisory/silent-lynx-campaigns-targeting-central-asian-governments/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.

REPORT GENERATED ON

November 6, 2025 • 7:30 AM

More at www.hivepro.com