Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

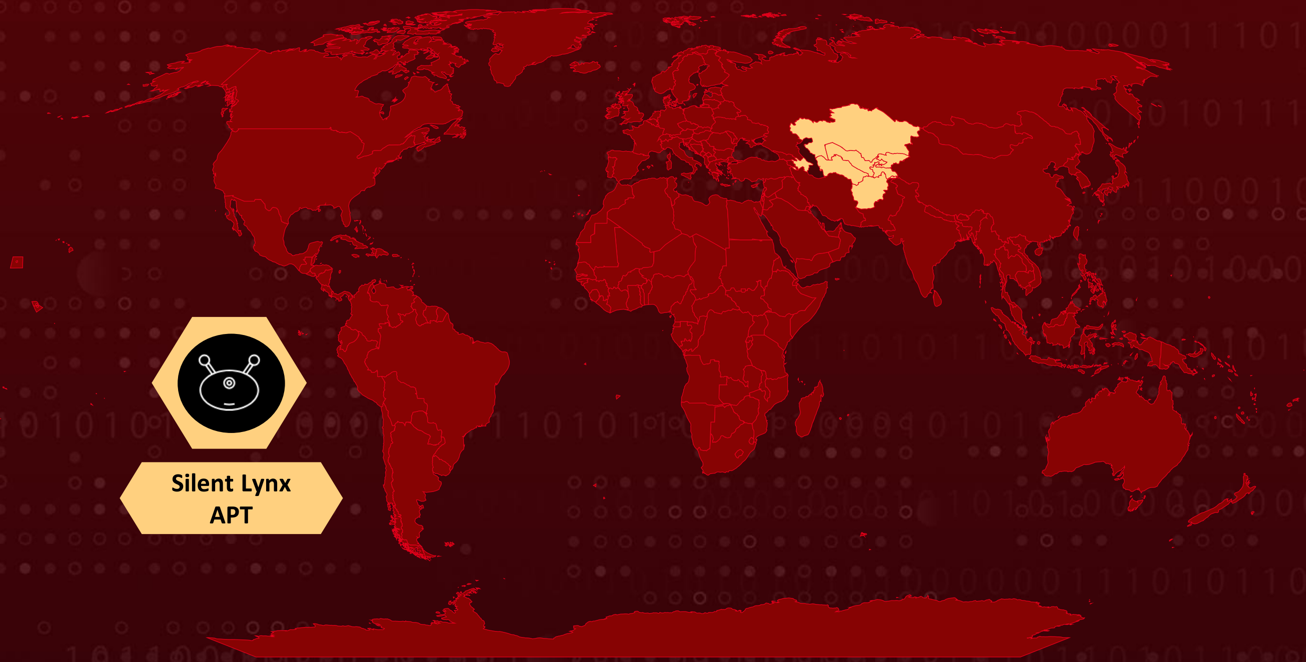
Silent Lynx Campaigns Targeting Central Asian Governments

Date of Publication	Admiralty code	TA Number
January 22, 2024	A1	TA2025016

Summary

First Seen: December 27, 2024
Malware: Resocks Toolkit
Threat Actor: Silent Lynx APT
Targeted Regions: Central Asia and Special Programme for the Economies of Central Asia (SPECA) based nations
Affected Platform: Windows
Targeted Industries: Government banks, think tanks, embassies, legal entities

Actor Map



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Actor Details

#1 Two sophisticated campaigns attributed to a new APT group named Silent Lynx, targeting key government institutions in Kyrgyzstan. These campaigns align with the group's focus on espionage, particularly within nations participating in the Special Programme for the Economies of Central Asia (SPECA). Leveraging phishing emails, malicious attachments, and decoy documents, the campaigns infiltrated entities like the National Bank of Kyrgyz Republic and the Ministry of Finance of Kyrgyzstan, exposing sensitive data and disrupting operations.

#2 The first campaign began with a phishing email containing an RAR attachment that housed a malicious ISO file. This ISO file included a decoy document and a C++ executable embedding encoded PowerShell scripts. The scripts enabled the attackers to execute commands and exfiltrate data through Telegram bots, a tactic that provides remote access while maintaining stealth. The decoy document impersonated an official SPECA-related invitation, adding credibility to the lure and reducing detection risk.

#3 The second campaign targeted the Ministry of Finance using a similar phishing email tactic, but with a password-protected RAR file containing a malicious Golang implant and a decoy document resembling an official government memo on employee bonuses. The Golang implant served as a reverse shell, connecting to a command-and-control (C2) server to execute commands and gather intelligence. This campaign highlighted the group's adaptability in deploying multiple payload types to achieve their espionage objectives.

#4 Technical analysis of Silent Lynx's operations revealed their reliance on multi-stage infection chains, including phishing, malicious payloads, and persistent infrastructure. They used Telegram bots for C2 communication and hosted malicious payloads on domains like pweobmxdlboi[.]com. Evidence suggests that Silent Lynx shares tooling and tactics with YoroTrooper, a Kazakhstan-based threat group, reinforcing the attribution to a shared regional nexus.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Silent Lynx	-	Central Asia and SPECA based nations	Government banks, think tanks, embassies, and legal entities
	MOTIVE		
	Espionage and Information theft		

Recommendations

Strengthen Email Security: Implement email security solutions capable of detecting and blocking phishing emails, malicious attachments, and suspicious links. Use sandboxing technologies to analyze email attachments (e.g., RAR, ISO files) for malicious behavior before delivery. Educate staff on recognizing phishing attempts, especially those containing themes like government or financial communications.

Endpoint Security Enhancements: Deploy EDR tools to monitor and respond to suspicious activities, such as PowerShell execution or unauthorized downloads. Restrict the execution of untrusted scripts and binaries, particularly from removable media or downloaded files. Ensure all operating systems, applications, and third-party tools (e.g., email clients, browsers) are up-to-date with security patches.

Network Defense Strategies: Use intrusion detection and prevention systems (IDS/IPS) to flag unusual connections, such as those to Telegram or uncommon domains. Restrict access to public file-sharing services (e.g., Google Drive, Pastebin) and ensure legitimate use of these platforms is monitored. Implement DNS filtering to block access to known malicious domains, such as those identified in the campaigns (e.g., pweobmxdlboi.com).

Network Segmentation and Access Control: Proper network segmentation limits the damage that can be done if an attacker gains access to one part of the system. By segmenting critical infrastructure from less sensitive data, organizations can better contain breaches and make lateral movement more difficult for attackers. Tightening access control policies can also limit the attacker’s ability to move across the network.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0003 Persistence	TA0001 Initial Access	TA0002 Execution
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration
T1589.002 Email Addresses	T1589 Gather Victim Identity Information	T1204.002 Malicious File	T1204 User Execution
T1078.002 Domain Accounts	T1078 Valid Accounts	T1059.001 PowerShell	T1059 Command and Scripting Interpreter
T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution	T1056.001 Keylogging	T1056 Input Capture
T1552.001 Credentials In Files	T1552 Unsecured Credentials	T1087 Account Discovery	T1083 File and Directory Discovery
T1046 Network Service Discovery	T1012 Query Registry	T1018 Remote System Discovery	T1016 System Network Configuration Discovery
T1007 System Service Discovery	T1560.001 Archive via Utility	T1560 Archive Collected Data	T1567 Exfiltration Over Web Service
T1567.002 Exfiltration to Cloud Storage			

Indicator of Compromise (IOCs)

TYPE	VALUE
SAH256	efb700681713cd50a2addd1fea6b7ee80c084467d3e87668688b9f06642062ba, e6f76a73180b4f2947764f4de57b52d037b482ece1a88dab9d3290e76be8c098, 3560660162f2268d52b69382c78192667a7eee5796d77418a8609b2f1709f834, 297d1afa309cdf0c84f04994ffd59ee1e1175377c1a0a561eb25869909812c9c, c045344b23fc245f35a0ff4a6d6fa744d580cde45c8cd0849153dee7dce1d80c, 1b76931775aa4de29df27a9de764b22f17ca117d6e5ae184f4ef617c970fc007, 66294c9925ad454d5640f4fe753da9e7d6742f60b093ed97be88fcdd47b04445, 99c6017c8658faf678f1b171c8eb5d5fa7e7d08e0a0901b984a8e3e1fab565cd
URLs	hxxps[://]pweobmxdlboi[.]com, hxxps[://]document[.]hometowncity[.]cloud, hxxps[://]mailboxdownload[.]com, hxxps[://]api[.]telegram[.]org/bot8171872935[:]AAHLoudjpHz1bxA26bV5wPuOEL3LOHEl6Qk, hxxps[://]api[.]telegram[.]org/bot7898508392[:]AAF5FPbJ1jlPQfqCIGnx-zNdw2R5tF_Xxt0
File names	147.exe, Xerox_Scan17510875802718752175.exe, 14789.exe, resocks.exe, 20241228_140656.iso, Application No. 14-214-14-12-5-15docx, sokcs.exe, udadd.exe

References

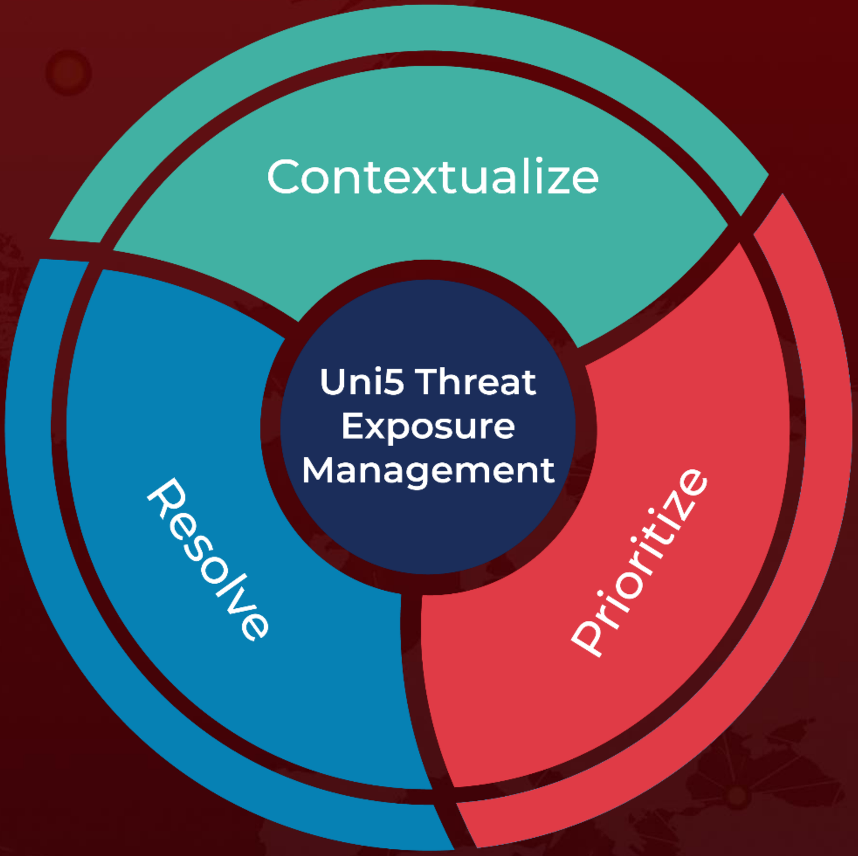
https://www.seqrite.com/blog/silent-lynx-apt-targeting-central-asian-entities/

https://www.hivepro.com/yorotrooper-covert-cyber-espionage-masters-of-kazakhstan/

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

January 22, 2025 • 10:30 PM

More at www.hivepro.com