UNG0002: Regional Threat Operations Tracked Across Multiple Asian Jurisdictions

By Subhajeet Singha

Published: 2025-07-16 · Archived: 2026-04-05 15:31:32 UTC

Overview

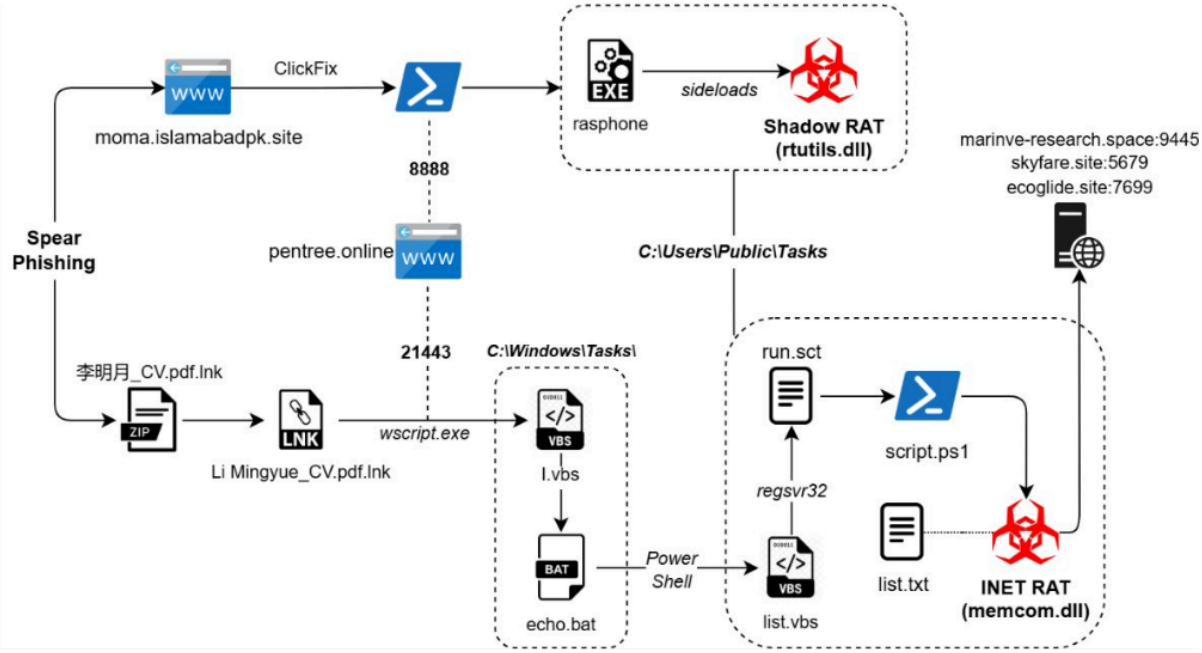
Seqrite Labs APT-Team has identified and tracked UNG0002 also known as Unknown Group 0002, a bunch of espionage-oriented operations which has been grouped under the same cluster conducting campaigns across multiple Asian jurisdictions including China, Hong Kong, and Pakistan. This threat entity demonstrates a strong preference for using shortcut files (LNK), VBScript, and post-exploitation tools such as Cobalt Strike and Metasploit, while consistently deploying CV-themed decoy documents to lure victims.

The cluster's operations span two major campaigns: **Operation Cobalt Whisper (May 2024 – September 2024)** and **Operation AmberMist (January 2025 – May 2025)**. During Operation Cobalt Whisper, 20 infection chains were observed targeting defense, electrotechnical engineering, and civil aviation sectors. The more recent Operation AmberMist campaign has evolved to target gaming, software development, and academic institutions with improved lightweight implants including Shadow RAT, Blister DLL Implant, and INET RAT.

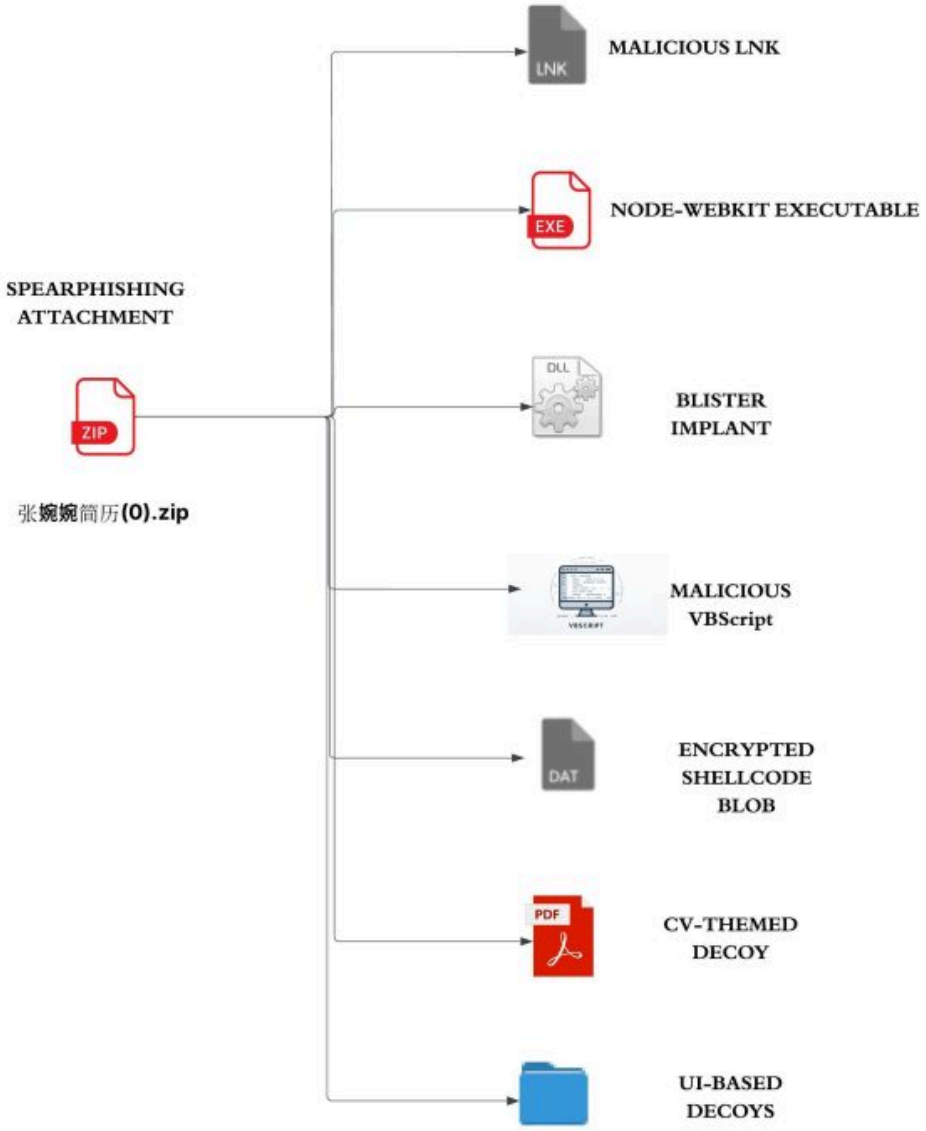
In the recent operation AmberMist, the threat entity has also abused the ClickFix Technique – a social engineering method that tricks victims into executing malicious PowerShell scripts through fake CAPTCHA verification pages. Additionally, UNG0002 leverages DLL sideloading techniques, particularly abusing legitimate Windows applications like Rasphone and Node-Webkit binaries to execute malicious payloads.

Key Findings

- **Multi-Stage Attacks**: UNG0002 employs sophisticated infection chains using malicious LNK files, VBScript, batch scripts, and PowerShell to deploy custom RAT implants including Shadow RAT, INET RAT, and Blister DLL.
- **ClickFix Social Engineering**: The group utilizes fake CAPTCHA verification pages to trick victims into executing malicious PowerShell scripts, notably spoofing Pakistan's Ministry of Maritime Affairs website.



- **Abusing DLL Sideloading**: In the recent campaign, consistent abuse of legitimate Windows applications (Rasphone, Node-Webkit) for DLL sideloading to execute malicious payloads while evading detection.
- **CV-Themed Decoy Documents**: Use of realistic resume documents targeting specific industries, including fake profiles of game UI designers and computer science students from prestigious institutions.
- **Persistent Infrastructure**: Maintained command and control infrastructure with consistent naming patterns and operational security across multiple campaigns spanning over a year.



OPERATION AMBERMIST - EARLY-MAY [2025]

- **Targeted Industry Focus**: Systematic targeting of defense, electrotechnical engineering, energy, civil aviation, academia, medical institutions, cybersecurity researchers, gaming, and software development sectors.
- **Attribution Challenges**: UNG0002 represents an evolving threat cluster that demonstrates high adaptability by mimicking techniques from other threat actor playbooks to complicate attribution efforts, with Seqrite Labs assessing with high confidence that the group originates from South-East Asia and focuses on espionage activities. As more intelligence becomes available, associated campaigns may be expanded or refined in the future.

Summary

UNG0002 represents a sophisticated and persistent threat entity from South Asia that has maintained consistent operations targeting multiple Asian jurisdictions since at least May 2024. The group demonstrates high adaptability and technical proficiency, continuously evolving their toolset while maintaining consistent tactics, techniques, and procedures.


Timeline of UNG0002
Cobalt Whisper
2024
May
[Enterprise Decryption]
Early-July
[Targets CN-Universities]
Mid-July
[Parking-Fee Campaign].
Late-July
[Targets Pakistan].
Early-August
[Research on Pre-Fueling].
Late-August
[Study on Fusion Power].
September
[Technology-Awards]

> CREATED BY
>
> APT-Team, SEQRITE LABS

The threat actor’s focus on specific geographic regions (China, Hong Kong, Pakistan) and targeted industries suggests a strategic approach to intelligence gathering AKA classic espionage related activities. Their use of legitimate-looking decoy documents, social engineering techniques, and pseudo-advanced evasion methods indicates a well-resourced and experienced operation.


Timeline of UNG0002
AmberMist
2025
January
[Targets MOFA & MOMA
of Pakistan]
Early- May
[Targets Gaming Industry]
Late-May
[Targets AI/Tech Industry]

CREATED BY

APT-Team, SEQRITE LABS

UNG0002 demonstrates consistent operational patterns across both Operation Cobalt Whisper and Operation AmberMist, maintaining similar infrastructure naming conventions, payload delivery mechanisms, and target selection criteria. The group's evolution from using primarily Cobalt Strike and Metasploit frameworks to developing custom implants like Shadow RAT, INET RAT, and Blister DLL indicates their persistent nature.

Notable technical artifacts include PDB paths revealing development environments such as C:\Users\The Freelancer\source\repos\JAN25\mustang\x64\Release\mustang.pdb for Shadow RAT and C:\Users\Shockwave\source\repos\memcom\x64\Release\memcom.pdb for INET RAT, indicating potential code names "Mustang" and "ShockWave" which indicate the mimicry of already-existing threat groups. An in-depth technical analysis of the complete infection chains and detailed campaign specifics can be found in our comprehensive whitepaper.

Conclusion

Attributing threat activity to a specific group is always a complex task. It requires detailed analysis across several areas, including targeting patterns, tactics and techniques (TTPs), geographic focus, and any possible slip-ups in operational security. UNG0002 is an evolving cluster that Seqrite Labs is actively monitoring. **As more intelligence becomes available, we may expand or refine the associated campaigns**. Based on our current findings, we assess with high confidence that this group originates from South-East Asia and demonstrates a high level of adaptability — often mimicking techniques seen in other threat actor playbooks to complicate attribution focusing on espionage. We also, appreciate other researchers in the community, like malwarehunterteam for hunting these campaigns.

IOCs

- Non-PE [Script-Based Files, Shortcut, C2-Config, Encrypted Shellcode blobs]

File Type	Hash (SHA-256)
LNK (Shortcut)	4ca4f673e4389a352854f5feb0793dac43519ade8049b5dd9356d0cbe0f06148
	55dc772d1b59c387b5f33428d5167437dc2d6e2423765f4080ee3b6a04947ae9
	4b410c47465359ef40d470c9286fb980e656698c4ee4d969c86c84fbd012af0d
SCT (Scriptlet)	c49e9b556d271a853449ec915e4a929f5fa7ae04da4dc714c220ed0d703a36f7
VBS (VBScript)	ad97b1c79735b1b97c4c4432cacac2fce6316889eafb41a0d97f2b0e565ee850
	c722651d72c47e224007c2111e0489a028521ccdf5331c92e6cd9cfe07076918
	2140adec9cde046b35634e93b83da4cc9a8aa0a71c21e32ba1dce2742314e8dc

Batch Script (.bat)	a31d742d7e36fefed01971d8cba827c71e69d59167e080d2f551210c85fddaa5
PowerShell (.ps1)	a31d742d7e36fefed01971d8cba827c71e69d59167e080d2f551210c85fddaa5
TXT – C2 Config	2df309018ab935c47306b06ebf5700dcf790fff7cebabfb99274fe867042ecf0 b7f1d82fb80e02b9ebe955e8f061f31dc60f7513d1f9ad0a831407c1ba0df87e
Shellcode (.dat)	2c700126b22ea8b22b8b05c2da05de79df4ab7db9f88267316530fa662b4db2c

- PE – Implants

Hash (SHA-256)	**Malware Type**	**Notes**
c3ccfe415c3d3b89bde029669f42b7f04df72ad2da4bd15d82495b58ebde46d6	Blister DLL Implant	Used in Operation AmberMist, DLL sideloaded via Node-Webkit
4c79934beb1ea19f17e39fd1946158d3dd7d075aa29d8cd259834f8cd7e04ef8	Blister DLL Implant	Same family as above, possible variant
2bdd086a5fce1f32ea41be86febfb4be7782c997cfcb028d2f58fee5dd4b0f8a	INET RAT	Shadow RAT rewrite with anti-analysis and C2 flexibility
90c9e0ee1d74b596a0acf1e04b41c2c5f15d16b2acd39d3dc8f90b071888ac99	Shadow RAT	Deployed via Rasphone with decoy and config loader

MITRE ATT&CK

Tactic	**Technique**	**Technique ID**	**Observed Behavior / Example**
Reconnaissance	Spearphishing for Information	T1598.002	Use of job-themed resumes (e.g., Zhang Wanwan & Li Mingyue CVs) to target specific sectors.

Resource Development	Develop Capabilities	T1587	Custom implants: INET RAT (rewrite of Shadow RAT), use of Blister DLL loader.
	Acquire Infrastructure	T1583.001, T1583.006	Use of spoofed domains (e.g., moma[.]islamabadpk[.]site); ASN usage.
Initial Access	Spear Phishing Attachment	T1566.001	Use of malicious ZIPs with LNKs and VBS (e.g., 张婉婉简历.zip, 李明月_CV.pdf.lnk).
	Drive-by Compromise (ClickFix technique)	T1189	Malicious site tricks user into pasting PowerShell copied to clipboard.
Execution	Command and Scripting Interpreter (PowerShell, VBScript, Batch)	T1059	Multi-stage execution via VBS → BAT → PowerShell.
	Signed Binary Proxy Execution (wscript, rasphone, regsvr32)	T1218	Use of LOLBINs like wscript.exe, regsvr32.exe, rasphone.exe for execution and sideloading.
	Scripting (Scriptlets – .sct files)	T1059.005	Use of run.sct via regsvr32 for further payload execution.
Persistence	Scheduled Task/Job	T1053.005	Tasks like SysUpdater, UtilityUpdater scheduled for recurring execution.
Privilege Escalation	DLL Search Order Hijacking	T1574.001	DLL sideloading via rasphone.exe, node-webkit for Shadow RAT, Blister loader.
Defense Evasion	Obfuscated Files or Information	T1027	Scripts with obfuscation, hex-encoded C2 configs, junk code in SCTs.
	Deobfuscate/Decode Files or Information	T1140	INET RAT decrypting C2 configuration from list.txt.
	Software Packing (Shellcode loader)	T1027.002	Blister decrypts and injects shellcode from update.dat using AES.
	Indirect Command Execution	T1202	Executing SCT through regsvr32, using P/Invoke to load DLLs.
Credential Access	Input Capture (potential within Shadow/INET RAT)	T1056	RAT capabilities imply possible credential theft.

Discovery	System Information Discovery	T1082	INET RAT collects computer/user names upon execution.
Command & Control	Application Layer Protocol: Web Protocols	T1071.001	Shadow/INET RATs communicate over HTTP(S).
	Ingress Tool Transfer	T1105	Payloads and decoys downloaded from external servers.
Collection	Data from Local System	T1005	Likely via RATs for file collection or clipboard access.
Exfiltration	Exfiltration Over C2 Channel	T1041	Shadow/INET RAT reverse shell features suggest data tunneling over same HTTP channel.

Authors

Sathwik Ram Prakki

Subhajeet Singha
