# APT UNG0002 Expands Cyber Espionage Campaigns Across Asia - Active IOCs - Rewterz

Published: 2025-07-23 · Archived: 2026-04-02 12:33:25 UTC

**Severity**

## High

## Analysis Summary

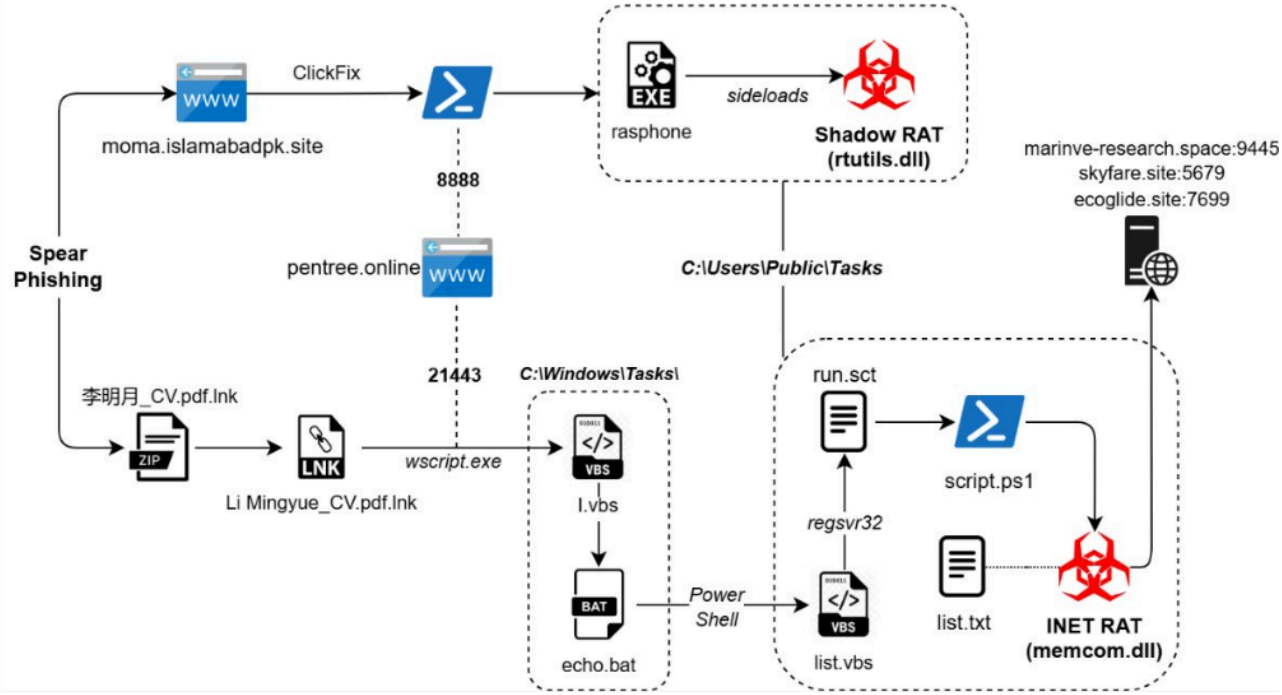
Cyber espionage in Asia is intensifying as researchers from a security firm have revealed new details on UNG0002, also known as Unknown Group 0002. This technically adept yet obscure group is conducting large-scale campaigns targeting strategic sectors across China, Hong Kong, and Pakistan. Its focus spans defense, electrical engineering, energy infrastructure, civil aviation, healthcare, universities, IT enterprises, and even the video game sector.

According to the latest report by the security firm, UNG0002 prefers using LNK shortcuts, VBScript files, and post-exploitation tools like Cobalt Strike and Metasploit. The group lures victims with deceptive documents disguised as résumés, lending authenticity to their phishing attacks. The analysis, conducted by a researcher, highlights the group’s methodical approach and adaptability.

UNG0002 has orchestrated two major campaigns: Cobalt Whisper (May–September 2024) and AmberMist (January–May 2025). Both relied heavily on phishing emails delivering malicious ZIP archives and LNK files to initiate complex malware deployment chains.

The Cobalt Whisper campaign, first identified in October 2024, used ZIP attachments containing LNK and VBScript files. Once executed, these deployed modules of Cobalt Strike, enabling attackers to maintain command and control within compromised systems.

In the AmberMist campaign, attackers distributed fake résumés as LNK files initiating a multi-stage infection process, culminating in the deployment of INET RAT and Blister DLL trojans. INET RAT is believed to be a customized variant of Shadow RAT spyware, while Blister DLL acts as a shellcode loader to establish remote access.




A notable attack variant observed in January 2025 redirected victims to a spoofed Pakistan Ministry of Maritime Affairs website. Masquerading as a CAPTCHA verification page, it executed PowerShell commands via ClickFix to activate Shadow RAT, establishing covert communication channels with command-and-control servers.

The malware used, such as Shadow RAT, employs DLL Sideloading and supports remote command execution, making it stealthy and difficult to detect. Despite exposure of its tools, UNG0002 continues refining its toolkit and expanding infrastructure.

Though direct attribution remains unconfirmed, circumstantial evidence suggests UNG0002 may originate from South or Southeast Asia. Analysts describe the group as resilient and inventive, highlighting the persistent effectiveness of phishing, spoofed sites, and DLL Sideloading in strategic cyber espionage campaigns likely to intensify further.

## Impact

- Command Execution
- Unauthorized Access
- Cyber Espionage

## Indicators of Compromise

### MD5

- 76c6694bb3446752f305376f212aca32
- f5a9c3ec6b00cea79eae2f9b9a808f5f
- 35fe5143d83829bb574e8021d47187ab
- a8a7e7494b9ded05685d6b91b1b7ffa6

- ab5aeb2f25745580b80d7326bcecc620
- bba575d4a89f285cf8c0650be09cc12e
- 7a2b0d8860a7188a936275907785d421
- a1fdb6d4220598e0f394e0a850343fe9
- 309f84937dc4e489517f5cbe1193538a
- 3992f53bb3d217900a56eec7f656b909
- 35bf8a85d61ec695fcaec19b6e25e1ca
- 2d2dc4dbefa47b9ac563a0f9fd65929f

**SHA-256**

- 4ca4f673e4389a352854f5feb0793dac43519ade8049b5dd9356d0cbe0f06148
- 55dc772d1b59c387b5f33428d5167437dc2d6e2423765f4080ee3b6a04947ae9
- 4b410c47465359ef40d470c9286fb980e656698c4ee4d969c86c84fbd012af0d
- c49e9b556d271a853449ec915e4a929f5fa7ae04da4dc714c220ed0d703a36f7
- ad97b1c79735b1b97c4c4432cacac2fce6316889eafb41a0d97f2b0e565ee850
- c722651d72c47e224007c2111e0489a028521ccdf5331c92e6cd9cfe07076918
- 2140adec9cde046b35634e93b83da4cc9a8aa0a71c21e32ba1dce2742314e8dc
- 2c700126b22ea8b22b8b05c2da05de79df4ab7db9f88267316530fa662b4db2c
- c3ccfe415c3d3b89bde029669f42b7f04df72ad2da4bd15d82495b58ebde46d6
- 4c79934beb1ea19f17e39fd1946158d3dd7d075aa29d8cd259834f8cd7e04ef8
- 2bdd086a5fce1f32ea41be86febfb4be7782c997cfcb028d2f58fee5dd4b0f8a
- 90c9e0ee1d74b596a0acf1e04b41c2c5f15d16b2acd39d3dc8f90b071888ac99

**SHA1**

- ab774153c0fe0e968f57df3bdc209612056b0ad4
- 302bebfa44e4c04baab423ac798997fb87b8d1a2
- bf5b9e0c4f2497a0e501dba361c94a5e401ad135
- e28ff664767b55373f43c909cab287b471b5a9dd
- bf76ae47197bd947c2d7e582aa2a565ad6beaed2
- a42dfab48fb50fed3a560f0e272d5aa49a09d2b2
- fee6bab9751d24a3f0171c6c72c67010d262adf3
- 98ea070e684ce6e8fea1ee60a1dc9a7115187826
- 87df9a5dcf7d18816eadff78aff242f0cc7a04cc
- a9ad4f730cc37aeef7c0368638e7e732f13bfa31
- 98008af4ab20fbc6234af6bf9b27d698accca4d4
- 23382a69715a8e597d7ff605b9e41ef0f64b9897

## Remediation

- Update and patch systems regularly to close vulnerabilities exploited by tools like Cobalt Strike and Metasploit

- Implement strong email security gateways to detect and block phishing emails with malicious ZIP or LNK attachments
- Train employees to identify deceptive résumés and suspicious email attachments to reduce phishing success
- Restrict execution of LNK, VBScript, and PowerShell files through endpoint protection policies
- Monitor network traffic for connections to known C2 infrastructures and unusual beaconing behaviour
- Deploy endpoint detection and response (EDR) solutions to detect post-exploitation tools and RAT activity
- Use application whitelisting to prevent unauthorized scripts and shellcode loaders from executing
- Regularly review and harden web infrastructure to prevent spoofing or redirection attacks
- Enable multi-factor authentication to reduce the impact of compromised credentials
- Conduct threat hunting focused on DLL Sideloading and living-off-the-land techniques used by UNG0002

---