



# HAZY TIGER

## THREAT ACTOR PROFILE

AUG 12TH, 2025

**TLP:GREEN** Free Version

Stay updated: subscribe to our intelligence feeds for real-time updates on APT activity and emerging cyber threats. Reach out to our team at [commercial@malwarepatrol.net](mailto:commercial@malwarepatrol.net) or visit our website: <https://malwarepatrol.net/>

## STATUS

Active

## ATTRIBUTION AND ASSOCIATIONS

- Classified as an India-nexus actor; no explicit attribution to a state or criminal syndicate has been confirmed.
- No known formal associations with other threat groups.

## OPERATIONAL MODEL

- Direct, in-house operations; no evidence of Ransomware-as-a-Service model.
- No confirmed affiliates or collaborations with other threat actors.



- Hazy Tiger is an India-nexus targeted intrusion adversary, primarily engaged in espionage and information theft [ID:0].
- The actor has been active since at least 2015.
- Known aliases: TA397 (also referred to as Bitter), T-APT-17.
- Motivations: espionage, information theft, and financial gain [ID:1]; the group targets government, diplomatic, defense, and financial sectors.
- Current status: active, with ongoing campaigns reported up to May 2025.



## HISTORICAL CONTEXT

- **First known appearance:** 2015, when Hazy Tiger first conducted espionage operations against South and East Asian targets.
- **2015–2019:** Conducted credential phishing and distributed Windows/Android malware.
- **2021–2022:** Employed Microsoft Excel payloads leveraging the Equation Editor exploit to create scheduled tasks that download secondary payloads via cURL. [ID:6]
- **2025-05-06:** Identified an eight-year espionage campaign against European and Asian government, diplomatic, and defense organizations, referenced as “TA397” or “Bitter” (ID 2, 3).
- **Most recent activity:** May 6 2025, with updated malware using CHM files to execute persistence and download further stages [ID:6].



## TECHNICAL PROFILE

### Malware and Tools

- **Excel payloads (Equation Editor exploit)** - create two scheduled tasks; first task downloads an executable to %AppData%, second task executes the downloaded file (T1053.001, T1105).
- **CHM files** - compress executable payloads, use msixec to execute remote MSI files, and create scheduled tasks for persistence (T1053.001, T1106).
- **C2 communications** - use cURL to request payloads from <https://qwavemediaservicenet/hkcu/qtphp/?dt=%computername%-QT-2&ct=QT> (T1071.001).
- **Obfuscated/encoded files** - encrypted or base64-encoded executables, stored as “dwmcorexe” (T1027).

### Infrastructure

- **Command & Control:** HTTP/HTTPS servers hosted on domains such as qwavemediaservicenet and possibly dynamic C2s.
- **Distribution:** Spearphishing attachments in Microsoft Office documents (Word/Excel) and CHM files, often sent via free email providers and signed with legitimate embassy contact details (T1193).
- **Persistence:** Scheduled tasks created under names such as Windows\DWM\DWMCORE and AdobeUpdater (T1053.001).



## TARGETING AND VICTIMS

- **Primary sectors:** Government, diplomatic, defense, and financial institutions.
- **Geographical spread:** South Asia (India, Pakistan, Bangladesh), East Asia (China, South Korea), Europe (various EU nations), and Kyrgyzstan (via embassy contact).
- **Shift over time:** Early focus on regional South/East Asian targets; expanded to European government entities by 2025 (ID 2, 3).

## RECENT DEVELOPMENTS

- May 6 2025 – Active campaign against European and Asian defense entities using updated CHM payloads (ID 2, 3).
- 2021–2022 – Discovery of Excel payloads creating scheduled tasks that download secondary executables via cURL [ID:6].
- 2025 – Continued use of spearphishing attachments with legitimate embassy contact details to entice victims [ID:6].

## INTELLIGENCE GAPS

- Precise attribution to a state or specific organization.
- Detailed mapping of all compromised C2 infrastructure and command structure.
- Comprehensive list of all victim organizations and specific data exfiltrated.
- Information on potential future evolution of malware payloads beyond current Excel/CHM methods.
- Confirmation of any collaboration or shared infrastructure with other threat actors.



## DEFENSE AND MITIGATION GUIDANCE

Defensive Measure	MITRE ATT&CK Mapping
Block outbound HTTPS traffic to known C2 domains (qwavemediaservicen.net).	T1071.001
Monitor and restrict creation of scheduled tasks with suspicious names.	T1053.001
Deploy email filtering to detect spearphishing attachments, especially Office documents.	T1193
Enable execution protection for CHM files and block execution from untrusted sources.	T1204
Regularly review registry and process lists for anomalies.	T1012, T1057
Apply patching for known Office and Windows vulnerabilities.	T1195 (Supply Chain)



## DETECTION GUIDANCE

Detection Action	MITRE ATT&CK Mapping
Log and alert on schtasks.exe activity with new task names.	T1053.001
Monitor for outbound HTTP(S) requests to unknown domains.	T1071.001
Watch for execution of Office files with embedded macros.	T1204, T1193
Inspect execution of msixexec from unexpected locations.	T1106
Analyze registry changes for suspicious keys.	T1012
Correlate user account enumeration events with anomalous activity.	T1033

## IOCS - INDICATORS OF COMPROMISE

FULL LIST OF IOCS AVAILABLE TO  
MALWARE PATROL CUSTOMERS ONLY











## IOCS - INDICATORS OF COMPROMISE

FULL LIST OF IOCS AVAILABLE TO  
MALWARE PATROL CUSTOMERS ONLY



 [MALWAREPATROL.NET](https://malwarepatrol.net)

 +1 813 321 0987