Freemindtronic

Reference Document: APT36 (Transparent Tribe / Mythic Leopard) Cyberespionage Group
Last Updated: May 16, 2025
Version: 1.1
Main Source of Initial Information: Freemindtronic Andorra (Post-Incident Analysis of 16/05/2025)

Introduction

The Advanced Persistent Threat (APT) group known as APT36, Transparent Tribe, and Mythic Leopard has been an active cyber espionage actor for several years. Primarily targeted at India, APT36 is notorious for its persistent campaigns to collect sensitive intelligence from a variety of organizations, including government, military, and potentially the research and education sectors. Their operations are often characterized by the use of sophisticated spearphishing techniques and bespoke malware, such as Poseidon, Crimson RAT, ElizaRAT, and CapraRAT. The purpose of this reference document is to compile and analyze the available information about APT36, its tactics, techniques, and procedures (TTPs), infrastructure, and recommended mitigation measures.

History and Evolution

Although the initial analysis provided by Freemindtronic Andorra focuses on recent IOCs (2023-2025), APT36's activity dates back several years. Previous reports from other security organizations have documented campaigns using similar tools and targeting Indian entities as early as 2016. The evolution of their TTPs suggests a continuous adaptation to security measures and the development of new tools to maintain their access to the targeted systems. For example, the appearance of Android versions of their RATs (such as CapraRAT) indicates an expansion of their scope to mobile devices. The use of platforms like Telegram for C2 (ElizaRAT) also shows an attempt to exploit potentially less monitored communication channels.

The precise attribution of APT36 remains a topic of discussion within the cybersecurity community. Although the main targets are in India, there is some evidence of a potential link to Pakistani state interests, given the themes of the decoys and the targeted sectors. However, a formal attribution requires more conclusive evidence and is often complex in the cybersecurity field.

Techniques, Tactics and Procedures (TTPs)

- **Recognition:** APT36 likely conducts careful reconnaissance of its targets, collecting publicly available information (OSINT) on employees, organizational structures, and sensitive projects. Social media profiles and official websites are potential sources of information. Social engineering can also be used to obtain information from employees.
- **Initial point of entry:**
    - **Spearphishing:** This is APT36's preferred attack vector. Emails are meticulously designed to mimic legitimate communications (e.g., government notifications, invitations to academic events, security app updates). Malicious attachments (Word documents, PDFs, executables, RTF files, screensavers) or links to compromised websites are used to distribute the initial payloads. Identified filenames (e.g., Briefing_MoD_April25.docx, Alert_Kavach_Update.exe) illustrate this tactic by targeting topical themes or topics relevant to potential victims.

    - **Exploiting Vulnerabilities:** Although not explicitly mentioned in the initial IOCs, it is possible that APT36 could exploit known software vulnerabilities in commonly used applications (e.g., Microsoft Office) to gain initial access. RTF files are often used in such attempts.
    - **Website Compromise:** It is possible, although not directly proven by IOCs, that APT36 could compromise legitimate websites to host payloads or to redirect victims to phishing pages.

- **Persistence:** Once a system is compromised, APT36 puts mechanisms in place to maintain access even after a reboot. IOCs reveal the use of specific Windows registry keys (HKEY_CURRENT_USER\Software\CrimsonRAT, HKEY_LOCAL_MACHINE\SYSTEM\ElizaRAT\Persistence, HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\CapraStart) to ensure the automatic execution of malware. On Android, persistence is often achieved by masquerading as legitimate app updates (com.kavach.update.apk).
- **Lateral Movement:** After obtaining an initial foothold, APT36 attempts to move laterally within the victim's network to reach more sensitive systems. This can involve exploiting network shares, using stolen credentials (potentially obtained via keylogging), and executing remote commands via deployed RATs.
- **Command and Control (C2):** The malware used by APT36 communicates with attacker-controlled C2 servers to receive instructions and exfiltrate data. The identified IP addresses (45.153.241.15, 91.215.85.21, etc.) potentially represent this C2 infrastructure. ElizaRAT's use of TelegramBot suggests leveraging popular messaging platforms for C2, which can make detection more difficult. HTTP and HTTPS are likely used for C2 traffic, potentially hidden within legitimate web traffic.
- **Data exfiltration:** Since APT36's primary focus is espionage, data exfiltration is a crucial step. The types of data targeted likely include sensitive documents (military, government, research), credentials (usernames, passwords), and other strategic information. Data can be exfiltrated through established C2 channels, potentially compressed, or encrypted to avoid detection.
- **Tools and Malware:**
    - **Poseidon malware:** A sophisticated RAT with extensive espionage and data theft capabilities. Its hash (3c2cfe5b94214b7fdd832e00e2451a9c3f2aaf58f6e4097f58e8e5a2a7e6fa34) allows it to be identified on compromised systems.
    - **Crimson RAT:** Another RAT commonly associated with APT36, offering keylogging, screen capture, and remote command execution features. Its mutex (Global\CrimsonRAT_Active) and registry key (HKEY_CURRENT_USER\Software\CrimsonRAT) are important indicators.
    - **ElizaRAT:** This RAT appears to be using Telegram for C2 communication, which is a potential evasion tactic. Its loader (9f3a5c7b5d3f83384e2ef98347a6fcd8cde6f7e19054f640a6b52e61672dbd8f) and its mutex (Local\ElizaRATSession) are key IOCs.

    - **CapraRAT (Android):** Indicates APT36's ability to target mobile devices. Its features can include stealing SMS, contacts, audio recording, and location tracking. Its package name (com.kavach.update.apk) and mutex (\Sessions\BaseNamedObjects\CapraMobileMutex) are specific flags.

- **Obfuscation and Evasion:** APT36 uses a variety of techniques to make its malware and communications more difficult to detect and analyze. Examples of these tactics include Base64 encoding of sensitive information (bXlQYXNzd29yZDEyMw==, JAB1c2VyID0gIkFkbWluIg==) and obfuscation of JavaScript code (eval(decodeURIComponent('%75%70%64%61%74%65'))) are examples of these tactics.

Infrastructure

APT36's infrastructure includes the command and control (C2) servers used to direct malware deployed on victims' systems. The identified IP addresses (45.153.241.15, 91.215.85.21, 185.140.53.206, 192.241.207.45, 103.145.13.187) are focal points for blocking and monitoring. Analysis of these IP addresses can reveal information about the hosting providers used and potentially other related activities.

Malicious domains (kavach-app[.]com, indiapost-gov[.]org, gov-inportal[.]org, indian-ministry[.]com, securekavach[.]in) are used in phishing campaigns to host fake login pages or to distribute malware. These domains often imitate legitimate websites to trick victims. Analyzing the registration information of these domains can sometimes provide clues about the actors behind these activities.

It is also possible that APT36 is using compromised servers as relays to hide the origin of its attacks and make tracing more difficult.

Motivations and Targets

The main motivation for APT36 appears to be cyber espionage, with a particular interest in gathering strategic intelligence related to India. Typical targets include:

- Indian government entities (ministries, agencies).
- Military and defense organizations.
- Research institutes and universities.
- Telecommunications companies.
- Potentially other sectors considered strategically important.

The themes of phishing lures (defense, foreign affairs, security updates of government applications) reinforce this assessment of targets and motivations.

Detailed Indicators of Compromise (IOCs)

- **IP addresses of C2 Servers (2023–2025):**
    - 45.153.241.15: Observed in C2 communications related to APT36 malware samples.
    - 91.215.85.21: Frequently associated with command and control activities for Crimson and Eliza RATs.
    - 185.140.53.206: Used as a point of contact for data exfiltration.
    - 192.241.207.45: Server potentially hosting malicious web infrastructure components (phishing pages).
    - 103.145.13.187: IP address involved in the distribution of malicious payloads.

- **File Hashes (SHA-256):**
    - 3c2cfe5b94214b7fdd832e00e2451a9c3f2aaf58f6e4097f58e8e5a2a7e6fa34 (Poseidon malware): Identifies a specific strain of the Poseidon RAT.
    - bd5602fa41e4e7ad8430fc0c6a4c5d11252c61eac768835fd9d9f4a45726c748 (Crimson RAT) : Signature unique d'une variante de Crimson RAT.
    - 9f3a5c7b5d3f83384e2ef98347a6fcd8cde6f7e19054f640a6b52e61672dbd8f (ElizaRAT loader): Allows you to detect the initial ElizaRAT deployment program.
    - 2d06c1488d3b8f768b9e36a1a5897cc6f87a2f37b8ea8e8d0e3e5aebf9d7c987 (CapraRAT APK) : Hash de l'application Android malveillante CapraRAT.
- **Malicious domains:**
    - kavach-app[.]com: Imitation of the security application "Kavach", probably used to distribute CapraRAT.
    - indiapost-gov[.]org: Impersonates the Indian Postal Service site, used for phishing or distributing malicious attachments.
    - gov-inportal[.]org: Attempt to imitate an Indian government portal to target civil servants.
    - Indian-Ministry[.]com: Generic but credible domain name to target Indian ministries.
    - securekavach[.]in: Another attempt to imitate "Kavach", aimed at appearing legitimate to Indian users.
- **Suspicious URLs:**
    - http://kavach-app.com/update: Fake update URL for the "Kavach" app, potential distribution point for CapraRAT.
    - http://gov-inportal.org/download/defense-docs.exe: Link to a malicious executable disguised as a defense document.
    - http://securekavach.in/assets/login.php: Potential phishing page to steal credentials.
    - https://indiapost-gov.org/track/status.aspx: A sophisticated phishing page that mimics package tracking to trick sensitive information into entering or downloading malware.
- **Phishing File Names:**
    - Briefing_MoD_April25.docx: Decoy potentially targeting the Ministry of Defense.
    - Alert_Kavach_Update.exe: False update alert for "Kavach" probably distributing a RAT.
    - IndiaDefense2025_strategy.pdf: Decoy containing strategic information on Indian defense.
    - MoEA_internal_memo_23.rtf: Fake internal memo from the Ministry of Foreign Affairs.
    - academic-research-invite.scr: Malicious screensaver masquerading as an academic invite.
- **Fake Android Application Package Names:**
    - com.kavach.update.apk: Malicious package masquerading as an update of "Kavach".

    - com.defensebriefing.alert.apk: Malicious Android app related to defense.
    - com.india.education.portal.apk: Fake app linked to an Indian educational portal.

- **Mutexes:**
    - Global\CrimsonRAT_Active: Indicates the active presence of the Crimson RAT on a Windows system.
    - Local\ElizaRATSession: Indicates an active Eliza RAT session.
    - \Sessions\BaseNamedObjects\CapraMobileMutex: A Mutex specific to the Android version of CapraRAT.

- **Registry Keys (Windows):**
    - HKEY_CURRENT_USER\Software\CrimsonRAT: Key used by Crimson RAT to store its configuration.
    - HKEY_LOCAL_MACHINE\SYSTEM\ElizaRAT\Persistence: A key indicating a persistence mechanism for ElizaRAT.
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\CapraStart: Automatic startup key for CapraRAT.

- **Known User-Agents:**
    - Mozilla/5.0 (Windows NT 10.0; Win64; x64) APT36Client/1.0: User-agent potentially used by a communication tool or an APT36-specific implant.
    - TelegramBot-ElizaRAT/2.5: Indicates the use of the Telegram API by the Eliza RAT for C2 communication.
    - CapraAndroidAgent/1.4: User-agent identifying the Capra malicious agent on Android devices.

- **Encoded/Obfuscated Strings Used in Payloads:**
    - bXlQYXNzd29yZDEyMw==: A Base64-encoded string, decoding as "myPassword123", potentially hard-coded identifiers or configuration strings.
    - JAB1c2VyID0gIkFkbWluIg==: Another Base64 string, decoding to $user="Admin", suggesting the use of PowerShell for malicious operations.
    - eval(decodeURIComponent('%75%70%64%61%74%65')): Obfuscated JavaScript code that, when de-encoded and evaluated, executes the "update" function, potentially indicating a malicious update or dynamic code execution feature.

Mitigation and Detection Measures

- **General recommendations:**
    - **Awareness of the threat of spearphishing:** Train employees to identify suspicious emails, verify the authenticity of senders, and not click on links or open attachments from unknown or unsolicited sources.
    - **Implement multi-factor authentication (MFA):** Strengthen account security by requiring a second form of authentication in addition to the password.
    - **Keeping systems and software up to date:** Regularly apply security patches for operating systems, applications, and web browsers to reduce the risk of vulnerability exploitation.
    - **Network segmentation:** Limit the spread of threats by segmenting the network and enforcing strict access control policies.

    - **Network traffic and log monitoring:** Implement monitoring systems to detect suspicious network activity, communications to known IP addresses and C2 domains, and unusual access attempts. Regularly analyze system and application logs.
    - **Use robust security solutions:** Deploy and maintain anti-virus solutions, endpoint detection and response (EDR) systems, and intrusion prevention and detection (IDS/IPS) systems.

- **Specific measures based on IOCs:**
    - **IOC Blocking:** Integrate identified IP addresses, domains, and file hashes into firewalls, DNS servers, antivirus solutions, and web filtering systems to block communications and malware associated with APT36.
    - **Rule-Based Detection:** Implement Yara and Sigma rules (if available) to identify patterns and characteristics of malware and APT36 activities on systems and in logs.
    - **Traffic Inspection:** Configure security systems to inspect network traffic for suspicious user agents (APT36Client/1.0, TelegramBot-ElizaRAT/2.5, CapraAndroidAgent/1.4).
    - **Registry and Mutex Monitoring:** Use endpoint monitoring tools to detect the creation of registry keys and mutexes associated with RATs used by APT36.
    - **Email Scanning:** Implement spam filters and email scanning solutions to identify and block messages containing known file names and phishing URLs.
    - **Mobile device security:** Deploy mobile security solutions and educate users about the risks of installing apps from unknown sources. Monitor Android devices for the presence of malicious package names.

- **Incident response strategies:**
    - **Response Plan:** Develop and maintain a cybersecurity incident response plan specific to APT threats, including steps to follow in the event of detection of APT36-related activity.
    - **Isolation:** In the event of a suspected compromise, immediately isolate the affected systems from the network to prevent the spread of the attack.
    - **Forensic Analysis:** Perform in-depth forensic analysis to determine the scope of the breach, identify compromised data, and understand the tactics used by attackers.
    - **Eradication:** Completely remove malware, persistence mechanisms, and tools used by attackers from compromised systems.
    - **Restore:** Restore systems and data from clean, verified backups.
    - **Lessons learned:** After an incident, analyze causes and processes to improve security measures and response procedures.

References

- https://www.zscaler.com/blogs/security-research/transparent-tribe-apt-targeting-india
- https://research.checkpoint.com/2023/transparent-tribe-evolution-of-a-cyber-espionage-threat/
- https://threatresearch.ext.hp.com/transparent-tribe-apt-group/
- This technical reference document is based on the original analysis published by Freemindtronic Andorra, available at: https://freemindtronic.com/apt36-spearphishing-india/

Strengthening Security Posture: The Freemindtronic HSM Ecosystem

The table below summarizes how each threat vector used by APT36 is mitigated by Freemindtronic's sovereign tools — whether mobile or desktop, fixed or remote, civilian or military-grade. It compares threat by threat how DataShielder and PassCypher mitigate attacks — whether on mobile, desktop, or air-gapped infrastructure.

APT36 Tactic / Malware	**DataShielder NFC HSM (Lite/Auth/M-Auth)**	**DataShielder HSM PGP (Win/macOS)**	**PassCypher NFC HSM (Android)**	**PassCypher HSM PGP (Win/macOS)**
Spearphishing (India Post, Kavach)	✓ QR-code encryption + sandbox	✓ Signature check + offline PGP	✓ URL sandbox + no injection	✓ Sandboxed PGP container
Crimson RAT	✓ NFC avoids infected OS	✓ No system-stored keys	✓ Secrets off-device	✓ No memory exposure
ElizaRAT	✓ No cloud or RAM access	✓ PGP keys isolated in HSM	No RAM usage / no clipboard	✓ OTP only if URL matches
ApolloStealer	✓ Credentials never exposed	✓ Key never loaded in system	✓ Immune to clipboard steal	✓ Phishing-proof login
Poseidon (Fake Kavach on Linux)	✓ NFC-only: bypasses compromised OS	✗ Not Linux-compatible	✗ Not on Android	✓ No OS dependency
CapraRAT (Android)	✗ (Not on Android)	✗	✓ Secrets never stored in app	✓ Desktop-paired use only
ClickFix (command injection)	✓ No shell interaction possible	✓ PGP validation	✓ No typing / no pasting	✓ No terminal interaction
Telegram / Cloud C2 Abuse	✓ No cloud usage at all	✓ Fully offline	✓ 100% offline	✓ 100% offline
CEO Fraud / BEC	✓ Auth/M-Auth modules encrypt orders	✓ Digital signature protection	✓ No spoofing possible	✓ Prevents impersonation

The benchmarking highlights the significant potential of Freemindtronic's HSM ecosystem, including DataShielder and PassCypher, to strengthen organizations' security posture against APT36's sophisticated threats. By integrating hardware-based encryption, isolation of keys and secrets outside of the potentially compromised operating system environment, and robust anti-phishing

verification mechanisms, these solutions provide a proactive defense barrier against many of the digital espionage and privileged information theft tactics employed by advanced players like APT36. The adoption of such HSM technologies represents a crucial step towards increased resilience against persistent threats.

For more details on the PassCypher and DataShielder HSM NFC modules:
https://freemindtronic.com/shop/

Outlook and Next Steps

APT36 (Transparent Tribe / Mythic Leopard) embodies a persistent and structured threat, primarily targeting strategic Indian entities for cyberespionage purposes. Its campaigns rely on sophisticated decoys, custom RATs, and an agile C2 infrastructure.

A thorough understanding of their tactics, techniques, and procedures (TTPs), as well as the currently known Indicators of Compromise (IOCs), provides a solid foundation to guide detection, defense, and response policies. Faced with the constant evolution of the techniques used by this group, a posture of continuous vigilance is essential.

This document is produced in an evolving manner. We believe it is essential to keep it up to date with new threats and tools observed in order to maintain a proactive security posture aligned with the latest available APT36 intelligence.