Advanced Persistent Threat Report: APT36 (Transparent Tribe)

Cyber-Espionage Group Targeting Indian Defense and Diplomatic Assets

Executive Summary

APT36, also known as **Transparent Tribe**, **Mythic Leopard**, **ProjectM**, or **Operation C-Major**, is a Pakistan-linked APT group active since **2013**. The group primarily targets Indian **military personnel**, **diplomatic missions**, and **research institutions**. It leverages **honeytrap tactics**, **macro-enabled maldocs**, and **fake domains** to deploy spyware and **Remote Access Trojans (RATs)**—notably **Crimson RAT**, **ObliqueRAT**, and **njRAT**—for cyber espionage.

Targeting Profile

Targeted Sectors

- **Military & Defense Personnel**
- **Diplomatic Entities**
- **Research Organizations**
- **Defense Contractors**
- **Conference Attendees**

Targeted Countries

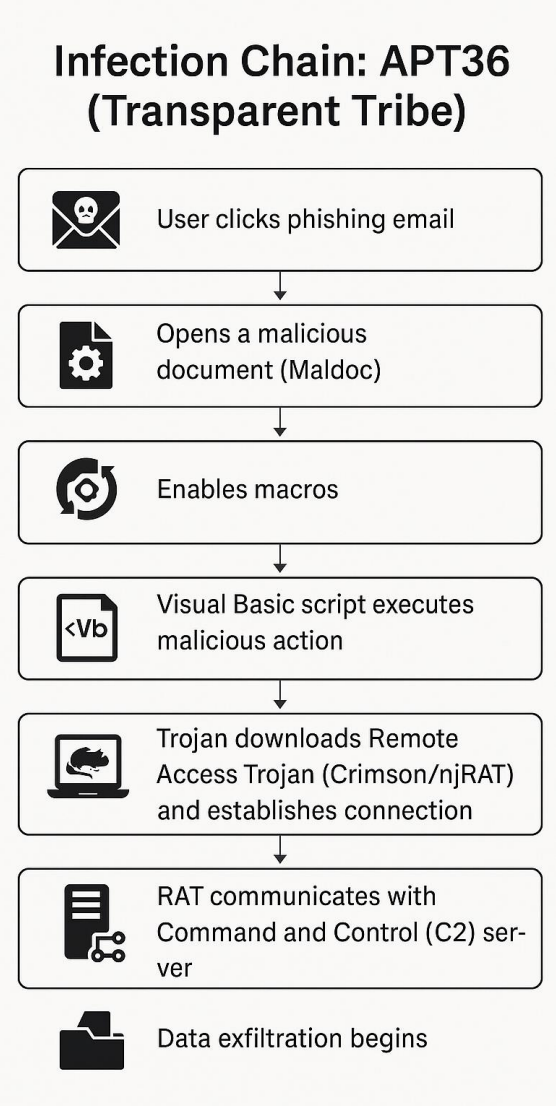
Primarily India, but also Afghanistan, Australia, Austria, Belgium, Canada, China, Germany, Iran, Japan, Kenya, Malaysia, Mongolia, Netherlands, Saudi Arabia, UK, USA, and more.

Attack Vectors & Infection Chain

Honeytrap and Spear Phishing Techniques

- Fake **CVs**, **conference invitations**, and **health advisories** were sent via spear-phishing emails.
- Emails often impersonated **Indian government** agencies.

Infection Chain Diagram:



Example Lure Themes:

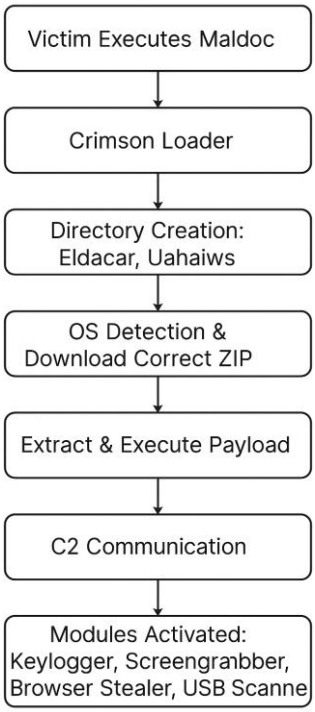
- Defense logistics reports
- 7th Pay Commission updates
- COVID-19 advisories
- Fake dating profiles (honeytraps)

Technical Analysis

RATs and Toolset

RAT/Tool	Description
Crimson RAT	Keylogging, webcam spying, credential theft, data exfiltration
ObliqueRAT	Delivered via malicious images/links from spoofed Indian sites
SmeshApp	Android-based spyware targeting military
njRAT, Bozok, PeppyRAT	Alternative payloads for different victim profiles
DarkComet, Luminosity, USBWorm	Additional espionage tools in the arsenal

Crimson RAT Architecture



Key Modules in Crimson RAT

- **Keylogger:** Stores logs at %APPDATA%\NVIDIA\
- **Credential Stealer:** Extracts Chrome/Firefox passwords
- **USB Module:** Scans/removes USB-based data
- **Peppy Module:** Uses HTTP POST for file uploads
- **Downloader Module:** Uses scheduled logic to fetch further payloads

Indicators of Compromise (IOCs)

Malicious Domains (Sample)

- clawsindia[.]com
- millitarytocorp[.]com
- drivestransfer[.]com
- mediabox[.]live
- cloudsbox[.]net
- larsentobro[.]com
- 7thcpcupdates[.]info
- india[.]gov[.]in

Malicious URLs

- hxxp://drivestransfer[.]com/files/Officers-Posting-2021.doc
- hxxp://mediafiles[.]live/files/khushi%20pics%20all.zip

IP Addresses

- 107.175.64.209
- 173.212.228.121
- 185.174.102.105

Hashes

File MD5 hash	Filename
123b180ed44531bfbac27c6eb0bbe01d	Update Portal.vhdx
3817590cf8bec4a768bb84405590272f	Student online update.exe
0ed6451ffe34217e44355706f4900ecc	NvidiaUpdate (2).scr
94daa776792429d1cb65edc1d525e2fc	Student detail.vhdx
c195d6bb06c93b94d39e5c1a2dfc6792	Confirmation_ID.vhdx
889c5c98e88c4889220617f57f5480f7	details.exe
ac3f2c8563846134bb42cb050813eac8	Confirmation_ID.exe

Malicious Email IDs

- maymis-mhupa[at]pmayindia[.]com
- vikaskumar[.]patel[at]larsentobro[.]com
- larsento[at]larsentobro[.]com

Mobile Espionage: SmeshApp

An Android spyware attributed to APT36, **SmeshApp**, was disguised as a dating/social media app and used to:

- Track military personnel movement
- Intercept SMS/calls
- Extract photos/files from infected devices

Defensive Recommendations

Measure	Description
Block IOCs	Implement in firewalls and SIEM
Awareness Training	Educate personnel against spear-phishing
Endpoint Monitoring	Deploy EDR/XDR tools
Patch Management	Fix CVEs like **CVE-2017-0199**, **CVE-2012-0158**
Incident Response	Disconnect infected systems immediately, re-image, and rotate credentials

References

- Cisco Talos: Transparent Tribe Analysis
- FireEye: APT36 Blog
- Malwarebytes: APT36 & COVID-19
- TA459, Group G0062 | MITRE ATT&CK®