JEDI SECURITY

Threat Assessment Report: APT36 (Transparent Tribe)

Executive Summary

APT36, also known as Transparent Tribe, is a Pakistan-linked Advanced Persistent Threat (APT) group primarily targeting Indian government, defense, diplomatic, and strategic organizations. The group conducts long-term cyber espionage operations using spear-phishing campaigns and remote access trojans (RATs) to infiltrate and maintain persistent access within targeted networks.

Attribution & Background

APT36 has been active since at least 2013. Multiple cybersecurity firms have attributed the group to Pakistan-aligned interests based on infrastructure patterns, targeting focus, and operational behaviors. The group primarily conducts intelligence gathering operations aligned with geopolitical tensions in South Asia.

Tactics, Techniques, and Procedures (TTPs)

- Spear-phishing emails using malicious attachments (LNK files, Office documents, PowerPoint add-ins).
- Deployment of Remote Access Trojans (RATs) such as Crimson RAT, Geta RAT, Ares RAT, and custom payloads.
- Use of staged payload delivery via command-and-control (C2) infrastructure.
- Cross-platform targeting (Windows and Linux environments).
- Persistence mechanisms including registry modifications and scheduled tasks.
- Credential harvesting and sensitive document exfiltration.

Primary Target Profile

APT36 primarily targets: Indian defense personnel, government ministries, diplomatic staff, military contractors, research institutions, and individuals associated with strategic infrastructure. Campaign lures often impersonate official communications or defense-related documentation.

Risk Assessment

- High espionage risk for government and defense sectors.
- Moderate-to-high risk for contractors and supply chain entities.
- Low risk for general public unless directly tied to strategic sectors.

Defensive Recommendations

- Implement advanced email filtering and attachment sandboxing.
- Enable multi-factor authentication (MFA) across all strategic systems.
- Deploy endpoint detection and response (EDR) solutions.
- Monitor outbound traffic for anomalous C2 communication patterns.
- Conduct regular phishing awareness training for staff.

Prepared by Jedi Security Threat Intelligence Division