# JEDI SECURITY

## THREAT INTELLIGENCE DIVISION

# APT36 (Transparent Tribe)

## Comprehensive Threat Assessment & Intelligence Dossier

Classification: Internal Distribution

# Executive Summary

APT36, also known as Transparent Tribe, is a Pakistan-linked Advanced Persistent Threat group conducting long-term espionage campaigns primarily targeting Indian government, defense, and strategic infrastructure entities. Operations focus on credential harvesting, persistent access, intelligence exfiltration, and reconnaissance aligned with geopolitical objectives.

## MITRE ATT&CK; Mapping

| Tactic | Technique | ID |
|---|---|---|
| Initial Access | Spearphishing Attachment | T1566.001 |
| Execution | User Execution | T1204 |
| Persistence | Registry Run Keys / Scheduled Tasks | T1547 |
| Credential Access | Credential Dumping | T1003 |
| Command & Control | Web-based C2 | T1071.001 |
| Exfiltration | Exfiltration Over C2 Channel | T1041 |

## Known Malware Families

- Crimson RAT
- Geta RAT
- Ares RAT
- DeskRAT
- Custom PowerShell Loaders

## Infrastructure Patterns

• Use of spoofed domains impersonating government portals • Rapid domain rotation for C2 resilience • Use of compromised hosting providers • Staged payload delivery architecture

## Operational Timeline Overview

| Year | Activity |
|---|---|
| 2013-2016 | Initial spear-phishing and Crimson RAT campaigns |
| 2017-2020 | Expansion into defense and diplomatic targeting |
| 2021-2024 | Enhanced persistence mechanisms and modular RATs |
| 2025-2026 | Cross-platform (Windows/Linux) campaigns with SideCopy collaboration |

## Indicators of Compromise (IOC Template Section)

Domain Patterns: *.gov-support[.]com, *.defense-update[.]net IP Patterns: Frequently rotating VPS infrastructure File Hashes: (To be updated per campaign intelligence feed) Email Lures: Defense briefings, policy updates, recruitment documents

## Risk & Confidence Assessment

| Sector | Threat Level |
|---|---|
| Government / Defense | HIGH |
| Military Contractors | HIGH |
| Academic / Research | MODERATE-HIGH |
| General Public | LOW |

Analytical Confidence Level: High (Multi-source corroboration)

## Strategic Defensive Recommendations

- Deploy advanced EDR with behavioral analytics
- Implement strict email attachment sandboxing
- Enforce MFA across all privileged accounts
- Network segmentation for defense-related systems
- Continuous threat hunting for C2 beacon patterns
- Supply chain security audits

---

Prepared by Jedi Security Threat Intelligence Division