INFY (Prince of Persia) — Threat Intelligence Profile

Classification: Nation-State Cyber Espionage (Iran-linked)

Executive Summary

INFY, also known as Prince of Persia, is a long-running Iranian cyber-espionage actor assessed to be state-sponsored. The group conducts low-noise, highly targeted operations focused on intelligence collection against individuals and organizations aligned with Iranian strategic interests. Recent activity confirms adaptive command-and-control (C2) infrastructure, multi-channel exfiltration, and disciplined operational timing correlated with domestic Iranian internet controls.

Attribution & Confidence

High confidence Iran-linked attribution based on operational timing during January 2026 national internet shutdowns, tradecraft continuity, infrastructure behavior, and tooling lineage observed by SafeBreach.

Observed Tooling

Family	Purpose	Notes
Foudre	Backdoor / Access	Used for data theft and staging
Tonnerre / Tornado v50–51	Primary implant	HTTP + Telegram C2 support
ZZ Stealer	Credential harvesting	Stage-one reconnaissance

Tactics, Techniques & Procedures (TTPs)

- Initial access via weaponized WinRAR archives (1-day exploitation)
- Self-extracting archives deploying DLL-based payloads
- Scheduled task creation for persistence
- Dual-channel C2 using HTTP and Telegram Bot API
- Dynamic domain generation (DGA + blockchain-derived naming)

Defensive Detection Priorities

- Monitor WinRAR execution chains spawning child processes
- Alert on new scheduled tasks from user-writable paths
- Flag Telegram API traffic from non-approved applications
- Watch for low-reputation domain beacons with rotating patterns

Risk Assessment

Impact: High (espionage, data exfiltration)
Likelihood: Medium–High for journalists, researchers, NGOs, policy, defense-adjacent targets
Sophistication: High operational discipline; moderate exploit development reliance

Bottom Line

INFY prioritizes stealth, persistence, and intelligence value over volume. Organizations should treat this actor as a patient, adaptive espionage threat capable of maintaining long-term access if basic hygiene and egress controls are not enforced.

```
Prepared for: Jedi Security — Threat Intelligence Use
Date: February 2026
```