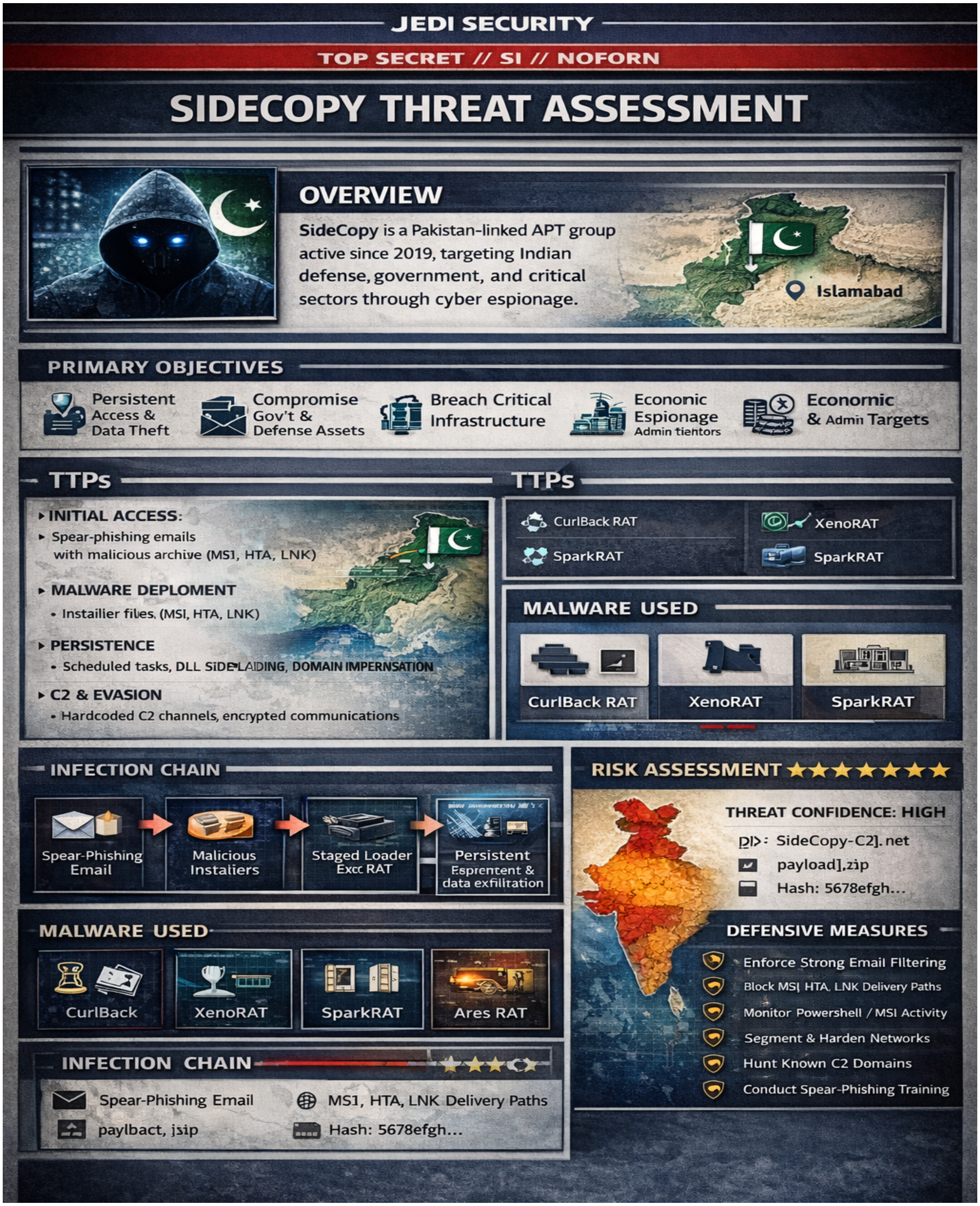
JEDI SECURITY

THREAT INTELLIGENCE DIVISION



JEDI SECURITY

TOP SECRET // SI // NOFORN

SIDECOPY THREAT ASSESSMENT

OVERVIEW

SideCopy is a Pakistan-linked APT group active since 2019, targeting Indian defense, government, and critical sectors through cyber espionage.

PRIMARY OBJECTIVES

- Persistent Access & Data Theft
- Compromise Gov't & Defense Assets
- Breach Critical Infrastructure
- Econonic Espionage Admin tientors
- Econornic & Admin Targets

TTPs

- **INITIAL ACCESS:**
  - Spear-phishing emails with malicious archive (MS1, HTA, LNK)
- **MALWARE DEPLOMENT**
  - Instailier files, (MSI, HTA, LNK)
- **PERSISTENCE**
  - Scheduled tasks, DLL SIDELAIDING, DOMAIN IMPERNSATION
- **C2 & EVASION**
  - Hardcoded C2 channels, encrypted communications

TTPs

- CurlBack RAT
- XenoRAT
- SparkRAT
- SparkRAT

MALWARE USED

- CurlBack RAT
- XenoRAT
- SparkRAT

INFECTION CHAIN

Spear-Phishing Email → Malicious Instaiiers → Staged Loader Excc RAT → Persistent Esprentent & data exfilltation

RISK ASSESSMENT ★★★★★★★

THREAT CONFIDENCE: HIGH

- DI> : SideCopy-C2].net
- payload],zip
- Hash: 5678efgh...

MALWARE USED

- CurlBack
- XenoRAT
- SparkRAT
- Ares RAT

DEFENSIVE MEASURES

- Enforce Strong Email Filtering
- Block MS| HTA, LNK Delivery Paths
- Monitor Powershell / MSI Activity
- Segment & Harden Networks
- Hunt Known C2 Domains
- Conduct Spear-Phishing Training

INFECTION CHAIN

- Spear-Phishing Email
- MS1, HTA, LNK Delivery Paths
- paylbact, jsip
- Hash: 5678efgh...

Executive Summary

SideCopy is a Pakistan-linked Advanced Persistent Threat (APT) group active since 2019, conducting targeted cyber espionage campaigns primarily against Indian government, defense, and critical infrastructure sectors. The group leverages spear-phishing, staged payload delivery, and remote access trojans to maintain persistent access and exfiltrate sensitive data.

Tactics, Techniques, and Procedures (TTPs)

- Spear-phishing emails with malicious MSI, HTA, and LNK attachments
- Use of open-source and customized RATs (XenoRAT, SparkRAT, CurlBack RAT)
- DLL side-loading and staged payload execution
- Scheduled task persistence mechanisms
- Encrypted command-and-control communications

Risk Assessment

- High risk to government and defense entities
- High risk to critical infrastructure sectors
- Moderate-to-high risk to academic and research institutions
- Moderate risk to private sector organizations with regional exposure

Prepared by Jedi Security Threat Intelligence Division