MITRE ATT&CK

CYBER SECURITY

MITRE ATT&CK-BASED THREAT LANDSPACE ANALYSIS OF SIDEWINDER APT TARGETING THE INDIAN DEFENCE SECTOR

PROJECT-03

NAME-ADARSH KUAMR SINGH
SUBJECT-CYBER SECURITY
ERP-6606714
COLLEGE-RCET
COURSE-B.TECH(CSE)

MITRE ATT&CK

INTRODUCTION

Understanding the Basics

Project Overview

- The Threat Actor: This project analyses SideWinder (APT-C-17), an advanced persistent threat group with a history of espionage against Indian critical infrastructure.
- Primary Targets: Indian Army, Navy, DRDO, and strategic research institutions.
- The Methodology: We utilise the MITRE ATT&CK Enterprise Framework to deconstruct real-world intelligence reports and map SideWinder's specific behaviors.
- The Goal: To move beyond traditional signature-based detection and provide a behavior-based threat model, visualising detection gaps in defense networks using the MITRE ATT&CK Navigator.

MITRE ATT&CK

WHY THIS ANLYSIS IS CRITICAL FOR NATIONAL SECURITY

Problem statement & motivation

- **Persistent Espionage:** SideWinder challenges Indian defence sectors not with destructive malware, but with long-term, stealthy intelligence gathering.
- **Failure of Traditional Defence:** Conventional antivirus tools often miss these attacks because SideWinder "lives off the land," abusing legitimate Windows tools (like PowerShell) rather than just using custom malware.
- **The Engineering Need:** There is an urgent need to shift Defence Security Operations Centers (SOCs) from reacting to tools (hashes/IPs that change daily) to detecting behaviors (Tactics, Techniques, and Procedures - TTPs that change rarely).

TARGET PROFILE: THE INDIAN DEFENCE SECTOR]

High-Value Targets for SideWinder

Defence Personnel: Targeted via spear-phishing to gain initial entry into secure networks.

Research & Development (DRDO): Targeted to steal intellectual property related to defence technology and strategic projects.

Military Operations: Targeted to gather intelligence on deployment, procurement, and strategic planning.

THE FRAME WORK :MITRE ATT&CK

ADVERSARIAL TACTICS, TECHNIQUES, AND COMMON KNOWLEDGE (ATT&CK)T

- ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.
- It serves as the "common language" for defenders to discuss adversarial behavior.

Framework Hierarchy used in this project:

Tactics (The Goal): e.g., "Get into the network" (Initial Access).

Techniques (The How): e.g., "Send a malicious email attachment" (T1566.001).

Procedures (The Specifics): e.g., "SideWinder sending a lure document named 'Salary_Hike_Gov.docx' containing a malicious macro."

MITRE ATT&CK

SideWinder Attack Lifecycle (The Kill Chain)]

- [Phase 1: Infiltration] Spearphishing Email sent to Defence Official -> Lure Document Opened
- [Phase 2: Execution & Evasion] Malicious Scripts execute (PowerShell) -> Obfuscated code bypasses AV
- [Phase 3: Persistence] Registry Keys modified for reboot survival
- [Phase 4: Command & Control] Establish encrypted HTTPS connection to attacker server -> Data Exfiltration

MITRE ATT&CK

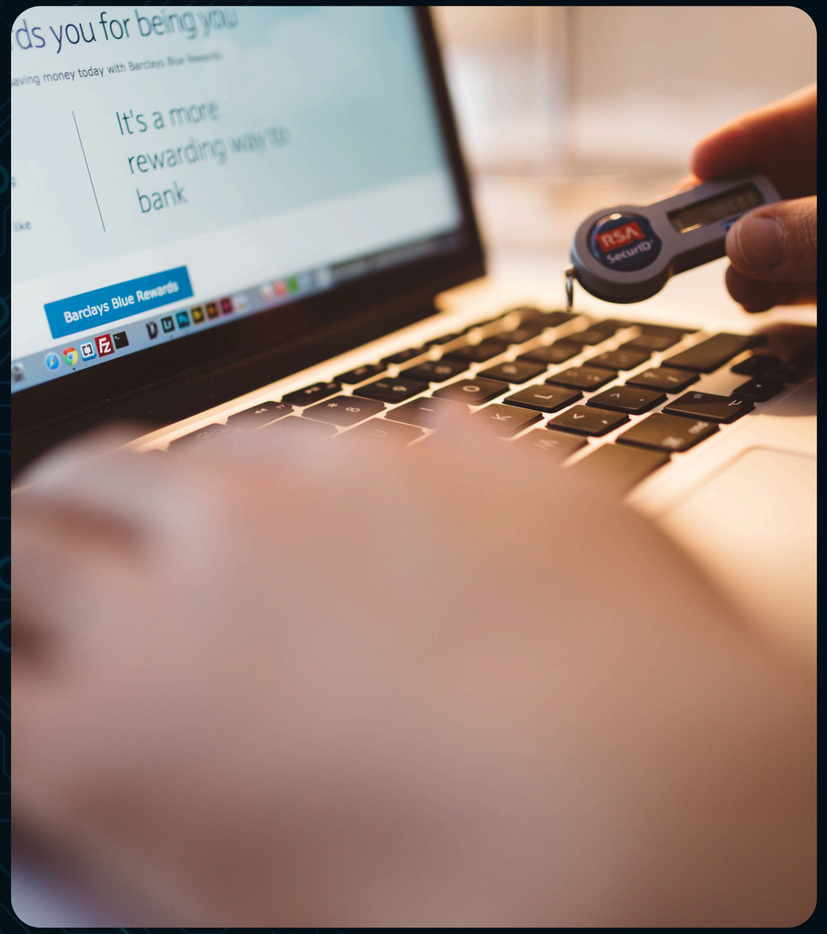
Deep Dive: Initial Access & Execution

Tactic: Initial Access

- Technique: T1566.001 - Spearphishing Attachment
- Analysis: SideWinder craft highly contextual emails disguised as official communications from other Indian government bodies (e.g., "Cabinet Secretariat circulars"). The attached documents (often .rtf or .docx) contain weaponized exploits.

Tactic: Execution

- Technique: T1059.001 - PowerShell
- Analysis: Once the document is opened, it triggers the execution of PowerShell. PowerShell is a native Windows administration tool; its use is referred to as "living off the land," making it very difficult for security software to distinguish between administrative tasks and malicious activity.



MITRE ATT&CK

Deep Dive: Persistence & Defense Evasion

Tactic: Persistence

- Technique: T1547.001 - Registry Run Keys / Startup Folder
- Analysis: To ensure they remain in the network after a system reboot, SideWinder modifies the Windows Registry (e.g., HKCU\Software\Microsoft\Windows\CurrentVersion\Run). This forces the malware implant to restart automatically every time the victim logs in.

Tactic: Defense Evasion

- Technique: T1027 - Obfuscated Files or Information
- Analysis: The PowerShell scripts and payloads used are rarely plain text. They utilize encoding (like Base64) and complex string manipulation to hide commands from signature-based scanners, rendering basic antivirus useless.

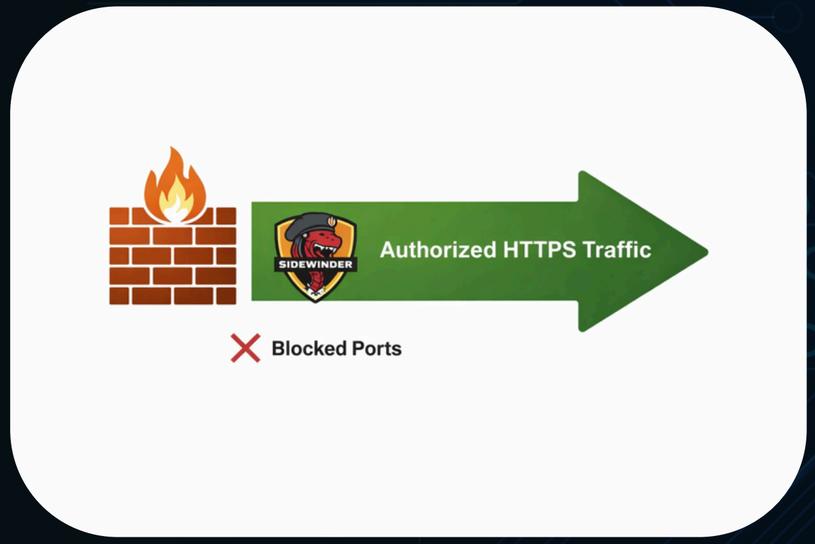
MITRE ATT&CK

DEEP DIVE: COMMAND & CONTROL (C2)

Tittle: Command & Control

- Technique: T1071.001 - Application Layer Protocol: Web Protocols (HTTPS)

- Analysis: SideWinder communicates with its handlers using standard HTTPS (Port 443) traffic.



- The Challenge: Defence networks generate massive amounts of legitimate HTTPS traffic daily. Hiding C2 communications within this stream makes it incredibly difficult to detect without deep packet inspection or behavioral analysis of beaconing patterns.

MITRE ATT&CK

INDIAN DEFENCE – CYBER ATTACKS
(Mapped to MITRE ATT&CK – Public Reports Only)

1. APT36 (Transparent Tribe)

- Targets: Indian Army, Air Force, DRDO, defence recruits
- Active Period: 2016 – Present
- Objective: Cyber espionage

Tools / Malware

- CrimsonRAT
- PeppyRAT
- Android spyware (fake defence apps)

MITRE ATT&CK Techniques

- T1566.001 – Spearphishing Attachment
- T1204 – User Execution
- T1059.001 – PowerShell
- T1547.001 – Registry Run Keys
- T1071.001 – HTTPS Command & Control

Vulnerability Type

- Phishing emails
- Malicious documents
- Human error (user execution)

2. SideWinder (Rattlesnake)

- Targets: Indian Navy, Air Force, missile & defence programs
- Active Period: 2018 – Present
- Objective: Long-term surveillance

Tools / Malware

- Custom loaders
- Weaponized Office documents

MITRE ATT&CK Techniques

- T1566.001 – Spearphishing

Attachment

- T1221 – Template Injection
- T1053 – Scheduled Task
- T1027 – Obfuscated Files

Vulnerability Type

- Trust in email attachments
- Legacy systems
- Poor document security controls

3. Confucius Group

- Targets: Indian Army officers, defence journalists
- Active Period: 2017 – 2023
- Objective: Intelligence collection

Tools / Malware

- NjRAT variants
- Spyware loaders

MITRE ATT&CK Techniques

- T1566 – Phishing
- T1082 – System Information Discovery
- T1005 – Data from Local System

Vulnerability Type

- Weak endpoint security
- Unpatched systems
- Credential exposure

MITRE ATT&CK

🇮🇳 INDIAN DEFENCE – CYBER ATTACKS
(Mapped to MITRE ATT&CK – Public Reports Only)

4. APT41 (Winnti Group)

- Targets: Indian government & defence-linked infrastructure
- Active Period: 2020 – 2023
- Objective: Strategic cyber espionage

Tools / Malware

- ShadowPad
- PlugX
- Cobalt Strike (abused)

MITRE ATT&CK Techniques

- T1190 – Exploit Public-Facing Application
- T1055 – Process Injection
- T1105 – Ingress Tool Transfer
- T1027 – Obfuscation

Vulnerability Type

- Misconfigured servers
- Web application weaknesses
- Poor network segmentation

5. Mustang Panda (APT10 / RedDelta)

- Targets: Defence think tanks, policy & research organizations
- Active Period: 2019 – 2023
- Objective: Policy & defence research espionage

Tools / Malware

- PlugX
- Custom backdoors

MITRE ATT&CK Techniques

- T1566.001 – Spearphishing Attachment
- T1027 – Obfuscated Files
- T1071.001 – HTTPS C2

Vulnerability Type

- Email-based delivery
- Lack of advanced email filtering

6. Rancor Group

- Targets: Indian military & regional security bodies
- Active Period: 2018 – 2022
- Objective: Regional cyber espionage

Tools / Malware

- Custom RATs

MITRE ATT&CK Techniques

- T1059 – Command & Scripting Interpreter
- T1105 – Tool Transfer
- T1071 – C2 Communication

Vulnerability Type

- Weak endpoint hardening
- Insufficient monitoring

MITRE ATT&CK

🇮🇳 INDIAN DEFENCE – CYBER ATTACKS
(Mapped to MITRE ATT&CK – Public Reports Only)

7. Patchwork (Dropping Elephant / APT-C-09)

- Targets: Indian Army, diplomats, government officials
- Active Period: 2016 – 2021
- Objective: Intelligence theft

Tools / Malware

- BADNEWS malware
- Data stealers

MITRE ATT&CK Techniques

- T1566.001 – Spearphishing Attachment
- T1203 – Exploitation for Client Execution
- T1027 – Obfuscation

Vulnerability Type

- Outdated software
- Poor attachment handling

8. Dark Basin

- Targets: Defence lawyers, policy advisors
- Active Period: 2019 – 2020
- Objective: Targeted surveillance

Tools

- Commercial-grade phishing kits

MITRE ATT&CK Techniques

- T1566 – Phishing
- T1114 – Email Collection

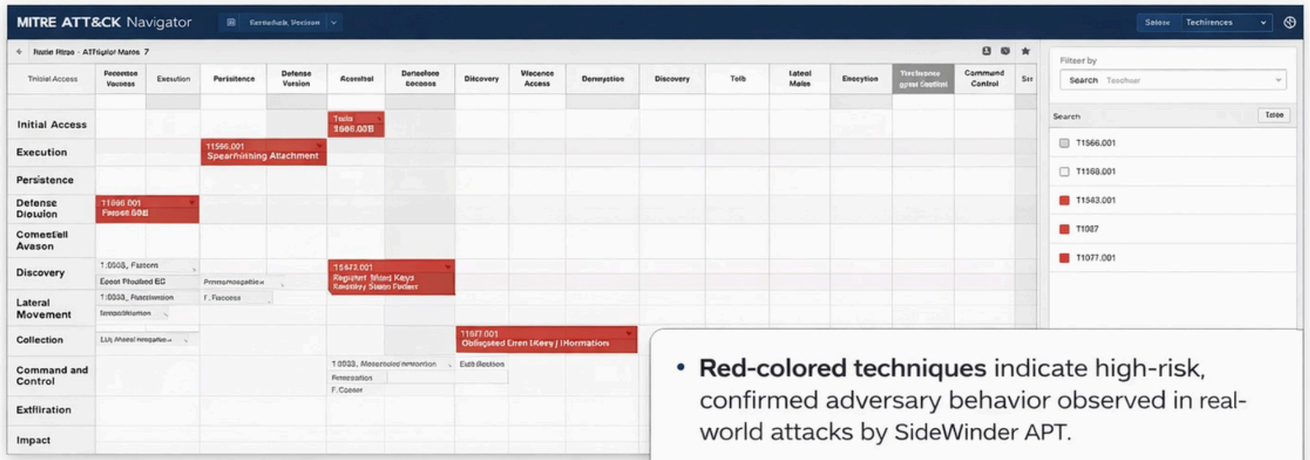
Vulnerability Type

- Credential reuse
- Lack of MFA

MITRE ATT&CK

Project Visualization: ATT&CK Navigator Heatmap

MITRE ATT&CK Navigator – SideWinder APT Technique Mapping



- **Red-colored techniques** indicate high-risk, confirmed adversary behavior observed in real-world attacks by SideWinder APT.
- Techniques mapped using the Enterprise ATT&CK matrix.
- Full attack lifecycle visualized:
  - **Initial Access** → Execution → **Persistence** → C2 (Command & Control)

- Mapping SideWinder's TTPs
- This heatmap visualises the "DNA" of a typical SideWinder campaign targeting Indian interests.
- The highlighted cells represent the specific techniques analysed in this project, indicating where defensive controls must be prioritized.

MITRE ATT&CK

KEY FINDINGS & DEFENSIVE RECOMMENDATIONS

SHIFT FROM INDICATORS OF COMPROMISE (IOCS) TO INDICATORS OF ATTACK (IOAS)

Observation	Legacy Recommendation (Ineffective)	Behavioral Recommendation (Effective)
PowerShell Abuse	Block PowerShell.exe (Breaks IT Admin work)	Monitor for MS Word spawning PowerShell as a child process.
Registry Persistence	Registry Persistence	Registry Persistence
HTTPS C2 Traffic	HTTPS C2 Traffic	HTTPS C2 Traffic

MITRE ATT&CK

CONCLUSION & FUTURE SCOPE

Conclusion

- This project successfully mapped major TTPs of the SideWinder APT against the MITRE framework, demonstrating that their success relies heavily on abusing legitimate tools and social engineering Indian defense personnel, rather than using zero-day exploits.

Future Scope

- Automated Detection: Developing SIGMA rules based on these MITRE techniques to automate detection in SIEM (Security Information and Event Management) systems.
- Adversary Emulation: Using tools like Caldera to simulate these specific SideWinder attacks in a controlled lab environment to test defence readiness.

REFERENCE

- MITRE ATT&CK® Enterprise Framework. (attack.mitre.org)
- "SideWinder APT and their targeting of Indian Defence." [Insert reputable OSINT report names here if you have them, e.g., TrendMicro, Kaspersky reports on SideWinder].
- T.S. Sobti, "Cyber threats to India’s national security," Journal of Defence Studies.

MITRE ATT&CK

THANK YOU

PRASANT SIR