CYBERVAHAK CONSULTANTS PRIVATE LIMITED

Emerging Cybersecurity Threats in the Wake of Operation Sindoor:

An In-Depth Analysis of Pakistani APT Activity and the Evolving Indian Threat Landscape (2024–2025)

Table of Contents

Abstract

This report analyses the rapid evolution of India's cyber-threat environment in the aftermath of the April 2025 Pahalgam terrorist attack. Drawing on open-source intelligence, CERT-In alerts and the threat reports published between January 2024 and May 2025, the study attributes a surge in sophisticated cyber operations to Pakistan-aligned Advanced Persistent Threat (APT) groups. It profiles three principal actors, APT36 (Transparent Tribe), its offshoot SideCopy and a higher-end "APT10-style" cluster dubbed Cosmic Leopard and maps their full kill chains to the MITRE ATT&CK framework.

Our six case studies show how Pakistan-based hackers have moved from random, attacks to well-planned, multi-platform operations. The evidence reveals that these groups are taking advantage of both newly discovered and long-known software flaws, misusing everyday online storage services and built-in Windows tools to hide their control traffic, and rotating through a growing toolkit of customised spying programs that now work on Windows PCs, Linux servers and Android phones alike. Post-Sindoor telemetry reveals a significant rise in credential-phishing campaigns impersonating Indian regulators, a marked uptick in living-off-the-land techniques. Detailed annexures have been provided at the end of this report, containing the full set of indicators of compromise (IOCs) associated with each of the six case studies.

The analysis underscores that India's critical infrastructure now constitutes an integrated battlespace where geopolitical flashpoints immediately translate into cyber aggression. To mitigate this elevated risk, this document recommends a three-tier defense strategy:

(1) strengthened public-private intelligence sharing and joint cyber-range exercises;

(2) zero-trust architecture, continuous threat hunting, and red-team validation at the enterprise level; and

(3) sector-specific controls such as network segmentation of OT environments and immutable backups for healthcare data.

By contextualizing technical findings within India's security calculus, the report provides senior decision-makers and CISOs with an actionable blueprint for enhancing India's cyber resilience against present and future state-sponsored threats.

Geopolitical Backdrop: Pahalgam Attack and Operation Sindoor

In April 2025, a devastating terrorist attack in Pahalgam (Jammu & Kashmir) killed 26 people, dramatically escalating tensions between India and Pakistan. Days later, India launched **"Operation Sindoor"**, a series of precise cross-border strikes on terrorist camps in Pakistan, demonstrating a strategic military response. While Operation Sindoor achieved its immediate aims, it also sparked retaliation in the cyber domain. Almost immediately, Pakistan-aligned threat actors mobilized to target Indian cyber assets – an expected response in today's era of hybrid warfare.

In the days after terrorist attack, Indian authorities observed a spike in cyber incidents targeting critical infrastructure. Government sources noted *"multiple attempts at unauthorized access"* to sensitive systems, though many were thwarted. Several Indian defense websites were defaced by hacktivist groups soon after the Pahalgam attack, indicating a surge in Pakistan-linked cyber aggression. The government ramped up cyber vigilance across critical sectors (energy, defense manufacturing, telecommunications, transport) in anticipation of further cyber attacks.

Crucially, advanced persistent threat groups also seized on the crisis. Within days of Operation Sindoor, cybersecurity researchers uncovered phishing campaigns exploiting the incident as a lure. For example, Pakistan's **Transparent Tribe (APT36)** crafted malicious PDF documents themed around the government's response to the Pahalgam attack. These decoy files – with titles like *"Action Points & Response by Govt Regarding Pahalgam Terror Attack"* – were emailed to Indian officials. When opened, they redirected victims to spoofed Indian government websites (including a fake Jammu & Kashmir Police portal) to harvest credentials. This immediate cyber reaction to a terror event underscored how closely geopolitical flashpoints and state-sponsored cyber operations are now intertwined.

In sum, the Pahalgam terror attack and India's Operation Sindoor retaliation formed the backdrop for a sharp uptick in cyber threats. The remainder of this report analyzes how Pakistan-aligned APT groups capitalized on the turmoil of 2024–2025, ramping up espionage and disruptive attacks on Indian institutions. We attribute key incidents to specific threat actors, detail their tactics and toolsets (from Crimson RAT to new malware like CurlBack), and assess the shifting threat landscape – ultimately providing recommendations to bolster India's cyber defense and resilience.

Attribution of Recent Cyberattacks (2024–2025) to Pakistani APT Groups

Dozens of cyberattacks on Indian government and industry in 2024–2025 have been attributed to Pakistan-linked APT groups through open-source intelligence, CERT-In advisories, and threat research reports. These threat actors, operating with state alignment or support, dramatically expanded their campaigns against Indian targets in the wake of rising geopolitical tensions. Below we identify three key groups and summarize the evidence tying them to recent attacks:

- **Transparent Tribe (APT36):** This Pakistan-based APT has been active since at least 2013 and has a long history of targeting Indian military, diplomatic, and defense research entities. Throughout 2024, APT36 carried out a relentless espionage campaign against high-profile Indian government agencies and military units. Check Point researchers documented the group deploying an improved version of its signature *Crimson RAT* along with new tools like *"ElizaRAT"* and a stealthy file stealer dubbed **ApoloStealer**, used to pilfer sensitive documents. These attacks were marked by sophisticated evasion (including payloads using cloud services for C2) and tailored malware, indicating a well-resourced operation. Notably, Transparent Tribe was linked to spear-phishing campaigns exploiting the Pahalgam attack crisis in 2025, as mentioned earlier. The group's fingerprints (malware, infrastructure, and tactics) have been observed in breaches of

Indian defense agencies, diplomatic missions, and even academic institutions through 2024 and early 2025, pointing to a broad espionage mandate.

- **SideCopy:** Often described as a sub-group or affiliate of APT36, **SideCopy** has emerged since 2019 with a focus on Indian defense personnel and government officials. It is so named because it mimics the methods of an Indian APT (SideWinder) to "side copy" their attack chains and deliver its own malware. SideCopy's activity surged in late 2024 and early 2025, expanding beyond military targets to hit sectors like energy, railways, and government departments previously outside its purview. In one campaign detected by Seqrite in December 2024, SideCopy targeted India's railway ministry, oil & gas companies and the Ministry of External Affairs. They employed a cocktail of RATs, from known families like **ReverseRAT** and **Action RAT** to a new malware called **CurlBack RAT**, indicating an *expanded arsenal*. The attacks also showed a shift in tactics, with SideCopy moving from malicious HTA files to using MSI installer packages for initial infection. Infrastructure overlaps (hardcoded C2 servers, reused domains) between SideCopy and Transparent Tribe further confirm Pakistani origin. Importantly, CERT-In and independent researchers have connected SideCopy to phishing campaigns against Indian government employees in 2024, where emails masquerading as official communications delivered spyware like **AllaKore RAT** and **CetaRAT**. All evidence points to SideCopy as a key actor escalating Pakistan's cyber offensive against India during this period.

- **"APT10-Style" Multi-Sector Campaign (Cosmic Leopard):** Beyond the above, threat intel suggests another Pakistan-aligned group mounted broad-based espionage operations in 2024–2025 akin to China's infamous APT10. Cisco Talos recently profiled a group it calls **"Cosmic Leopard"** (umbrella codename *Operation Celestial Force*), which overlaps with but remains distinct from Transparent Tribe. Active since 2016, Cosmic Leopard has consistently spied on Indian government and defense-related organizations. What sets this group apart is the scope and persistence of its campaigns, which echo APT10's multi-industry targeting and long-term access goals. Cosmic Leopard's toolset includes the cross-platform **GravityRAT** Trojan (Windows, Android, and even MacOS variants) and a sophisticated loader named **HeavyLift**, which together enable it to compromise both PCs and mobile devices. For instance, in one ongoing campaign, Cosmic Leopard operators initiated contact with Indian targets via social media "honey traps," then sent them to a fake app website where victims downloaded malware-laced Android apps (GravityRAT) or Windows installers (HeavyLift). Once installed, GravityRAT can exfiltrate call logs, SMS, location and more from phones, while HeavyLift stealthily siphons data from PCs and can even trick victims into self-uploading sensitive files to attacker-controlled cloud storage. This ambitious campaign targeted Indian government personnel and defense contractors, as well as related tech companies, throughout 2024. The breadth of targeting and the emphasis on *"establishing long-term access"* have drawn comparisons to APT10's modus operandi. While Cosmic Leopard's activities are less publicized than APT36 or SideCopy, its emergence signals a mature, APT10-like threat actor operating from Pakistan, likely with the aim of strategic intelligence gathering across multiple Indian sectors.

Attribution Confidence: It is important to note that attribution in cyber incidents is often a matter of probability, based on overlaps in infrastructure, malware signatures, tactics, and occasionally adversary errors or leaks. In the above cases, a combination of OSINT and vendor research provides **high confidence** that these attacks originated from Pakistan-aligned actors. For example, the fake India Post website used in a 2024 campaign was registered in Pakistan and even contained an author name referencing a Pakistani government program. Command-and-control (C2) servers used in recent attacks have been traced to hosting providers frequently used by Pakistani groups (e.g. Contabo in Europe) and to IP ranges associated with past APT36 operations. The consistent targeting of Indian

government, military, and critical infrastructure also aligns with Pakistan's strategic interests and decades-long cyber espionage patterns. Taken together, the evidence leaves little doubt that the surge in cyberattacks on Indian institutions in 2024–25 is state-aligned activity from Pakistan, coordinated alongside geopolitical flashpoints such as Operation Sindoor.

Technical Profiles of Key Pakistani APT Groups

In this section, we provide detailed technical profiles of three prominent Pakistani APT groups – **APT36 (Transparent Tribe)**, **SideCopy**, and a third group we will call **"Operation Celestial Force" (APT10-style)** – highlighting their tactics, techniques, and procedures (TTPs). For each group, we examine their typical attack kill chain, preferred attack vectors and exploits, malware/toolkits used, MITRE ATT&CK technique mapping, and sectoral targeting. Understanding these profiles is crucial to anticipating their moves and implementing effective defenses.

APT36 (Transparent Tribe)

Overview: Transparent Tribe (APT36), also known by aliases like *Mythic Leopard* and *ProjectM*, is a Pakistan-based APT active since at least 2013. It is a highly persistent espionage group that primarily targets India and Afghanistan, focusing on military and government entities. The group's overarching goal is long-term intelligence collection: **establishing footholds in target networks for continuous surveillance and data exfiltration**. Over the years, APT36 has repeatedly updated its toolset and techniques, making it an adaptable threat.

Attack Kill Chain: APT36 typically initiates attacks via **spear-phishing**. Their phishing lures often take the form of emailed documents or links that appear to be from trusted Indian government or military sources. For example, past campaigns used topics like COVID-19 advisories, official recruitment notices, or security alerts (even a fake version of the Kavach 2FA app) to trick targets. The kill chain commonly unfolds as follows:

1. **Initial Access – Spear Phishing:** APT36 sends a targeted email with either a malicious attachment or a link (URL) to a spoofed website. The attachment might be a weaponized Office document (e.g., a Word file exploiting an old vulnerability or containing malicious macros) or a compressed archive (ZIP/RAR) containing an executable or shortcut. In 2025, APT36 also began using **phishing PDF files with embedded scripts** and leveraging cloud services to deliver payloads. *(MITRE ATT&CK: Spearphishing Attachment – T1566.001; Spearphishing Link – T1566.002)*

2. **Execution – Malware Deployment:** If the victim opens the attachment or clicks the link, a chain reaction is triggered. Malicious code hidden in the document (e.g., an Office macro or an exploit for Equation Editor vulnerability CVE-2017-11882) executes on the system, or the user is prompted to run a Trojanized installer. Recent APT36 campaigns have used novel techniques like *"ClickFix"* – a malicious PDF that instructs the user to press Win + R and execute a provided PowerShell command. This results in downloading the next-stage payload from a remote server via PowerShell. On other occasions, victims are enticed to run an .exe file masquerading as a document or application, which then drops the malware. *(MITRE: User Execution – T1204; Execution via PowerShell – T1059.001)*

3. **Persistence & Installation:** Once on the machine, APT36's malware establishes persistence. Common methods include creating a Registry *Run* key for the malware to start at boot, or installing a scheduled task. APT36 has also side-loaded malicious DLLs through legitimate software to stay resident. For example, they might drop a legitimate application along with a malicious DLL (one of their RAT components renamed), so that when the app runs, it loads the DLL backdoor (DLL search order hijacking). Their malware often also creates

copies in system folders with innocuous names. *(MITRE: Registry Run Keys/Startup – T1547.001; DLL Side-Loading – T1574.002)*

4. **Command-and-Control (C2):** APT36's malware connects to command-and-control servers to receive instructions and exfiltrate data. Historically, they hosted C2 infrastructure on cheap VPS or compromised servers around the world (to obfuscate attribution), using HTTP(S) for communications. In recent years, APT36 adopted cloud and social media platforms for C2: for instance, variants of their *ElizaRAT* used Slack API channels and Google Drive for command beacons and data exfil. This abuse of legitimate cloud services makes detection harder, as traffic blends with normal encrypted web traffic. *(MITRE: Application Layer Protocol – T1071; Web Service (Slack/Drive) – T1102)*

5. **Actions on Objectives:** With access established, APT36 conducts extensive **reconnaissance and data collection** on the victim network. Their malware typically enumerates files, captures keystrokes, and monitors user activity. APT36 operators search for specific intelligence: documents, emails, spreadsheets, and databases of interest (especially related to defense plans, diplomatic communications, etc.). They often deploy additional tools as needed – e.g., a password dumper to extract credentials, or a network scanner to map the internal network. Any valuable data is packaged and exfiltrated back via the C2 channel (sometimes compressed or staged for efficiency). In some cases, APT36 maintains a silent presence for months, periodically siphoning new data. *(MITRE: Internal Reconnaissance – T1012; Data Exfiltration over C2 – T1041)*

Malware and Toolkits: APT36 is especially known for its family of custom remote access trojans. Their flagship malware is **Crimson RAT**, a Windows backdoor capable of logging keystrokes, capturing screenshots, and exfiltrating files. Crimson RAT has been used continuously in APT36 campaigns since at least 2016, and the group regularly tweaks or "re-packs" it to avoid antivirus detection. Alongside Crimson, APT36 has developed or used:

- **ObliqueRAT:** A malware discovered by Cisco Talos in 2020, delivered via malicious image files embedded in documents. ObliqueRAT is a lighter backdoor used for reconnaissance and downloading additional payloads.

- **CapraRAT:** A fully-featured Android backdoor (likely derived from the open-source AhMyth RAT) that APT36 uses to spy on mobile devices. CapraRAT can record calls, steal SMS messages, track GPS location, and take photos – essentially turning a phone into a spy device. APT36 has used CapraRAT in *honey-trap operations* targeting Indian Army and government personnel by luring them to install fake secure chat apps (e.g. "MeetUp" or "Secure Hangout") that are Trojanized with this malware.

- **SnowyCloud/StackPad (ElasticRat):** Newer implants referenced in some reports (possibly analogous to ElizaRAT mentioned by Check Point), which use cloud services for C2 and attempt to live off the land by using existing system tools. These are part of APT36's shift to more fileless malware deployment.

- **ApoloStealer:** A data-stealing tool observed in 2024 that works alongside Crimson/Eliza RAT. ApoloStealer is designed to **search for specific file types** (e.g., Office docs, PDFs) and exfiltrate them in bulk. It essentially automates the collection of sensitive documents from infected PCs, storing metadata and sending archives off to the attackers.

APT36 also employs numerous **open-source or commodity tools** as secondary payloads, such as Mimikatz (for credential theft), and has been noted to repurpose publicly available RATs like *njRAT* or *QuasarRAT* when needed. This blending of custom and commodity tools can make attribution tricky, but the presence of Crimson or CapraRAT and their specific infrastructure links are strong identifiers of APT36.

Notable Exploits & Attack Vectors: Transparent Tribe historically favored social engineering over zero-day exploits, often using either malicious macros or known vulnerabilities in documents. A common vector was the use of the Microsoft Office Equation Editor exploit (CVE-2017-11882) in lure documents – a memory corruption bug that allowed code execution without macros and was widely used by many actors in late 2010s. In 2023, SideCopy (linked to APT36) even leveraged a vulnerability in WinRAR (CVE-2023-38831) to auto-execute payloads when a victim opened a malicious archive. APT36 is quick to incorporate **n-day exploits** (recently disclosed vulnerabilities) into phishing attachments, though there's no public evidence of them using true zero-day exploits in this period. Instead, they rely on human deception: cleverly crafted emails, impersonation of real Indian government domains (for example, spoofing email addresses or web domains that look like legit military sites), and even long-term social media engagement to build trust with targets (the classic honey trap).

One notable tactic APT36 used is **watering-hole attacks** on occasion: compromising legitimate Indian websites that their targets frequent, in order to serve malware. While spear-phishing is their bread-and-butter, at least one case in 2022 involved APT36 compromising Indian defense-related websites to host malicious links, tricking users into thinking they were downloading safe software.

MITRE ATT&CK Mapping: In summary, APT36's activities map to a wide range of ATT&CK techniques across the kill chain:

- Initial Access: *T1566.001 Spearphishing Attachment*, *T1566.002 Spearphishing Link*
- Execution: *T1204 User Execution (malicious document)*, *T1059.001 PowerShell*
- Persistence: *T1547.001 Registry Run Keys/Startup*, *T1574.002 DLL Side-Loading*
- Privilege Escalation/Defense Evasion: *T1055 Process Injection*, *T1027 Obfuscated Files or Information* (packed malware), *T1070 Indicator Removal on Host* (clearing logs)
- Credential Access: *T1003 OS Credential Dumping* (Mimikatz)
- Command and Control: *T1071.001 Web Protocols*, *T1102 Web Services* (Slack, Google Drive API), *T1095 Non-Application Layer Protocol* (custom TCP)
- Exfiltration: *T1041 Exfiltration Over C2 Channel*, *T1567 Exfiltration to Cloud Storage*.

Sectoral Targeting: APT36's primary targets are India's defense and government sectors. Over 2024–25, it continued aggressive targeting of military institutions (Army and Air Force units, defense ministry departments) and think-tanks/research orgs related to defense. It also targets diplomatic entities – e.g. Indian embassies and officials – as well as critical infrastructure ministries. In 2024, APT36 notably expanded targeting to *education* as well: they targeted Indian universities, attempting to steal student data (possibly to identify individuals for recruitment approaches or to collect research). The group's interest in healthcare emerged during the COVID period (using pandemic lures) and may persist insofar as medical and vaccine research data are valuable. Overall, any institution with national security or intelligence value in India (and sometimes in Afghanistan) is a potential APT36 target. Attacks on the finance sector by APT36 are less common, but not unheard of – typically if the institution ties to government finance or to gather economic intel.

SideCopy

Overview: SideCopy is a Pakistani threat group active since 2019 that is assessed to be closely connected to Transparent Tribe (often considered a subgroup). Its name comes from copying the tactics of India's SideWinder APT, and indeed SideCopy's operations have primarily targeted Indian military and security personnel. SideCopy rose to prominence for its innovative infection chains and multi-stage malware delivery, as well as its focus on stealth

and deception. By 2024, SideCopy had greatly broadened its targeting within India and enhanced its malware toolkit, making it one of the most active Pakistan-linked APTs in the region.

Attack Kill Chain: SideCopy's kill chain is typified by **multi-stage loader sequences** and heavy use of decoy content. A representative attack sequence uncovered by researchers is illustrated in **Figure 1** below, which shows SideCopy's multi-stage infection process in early 2024:

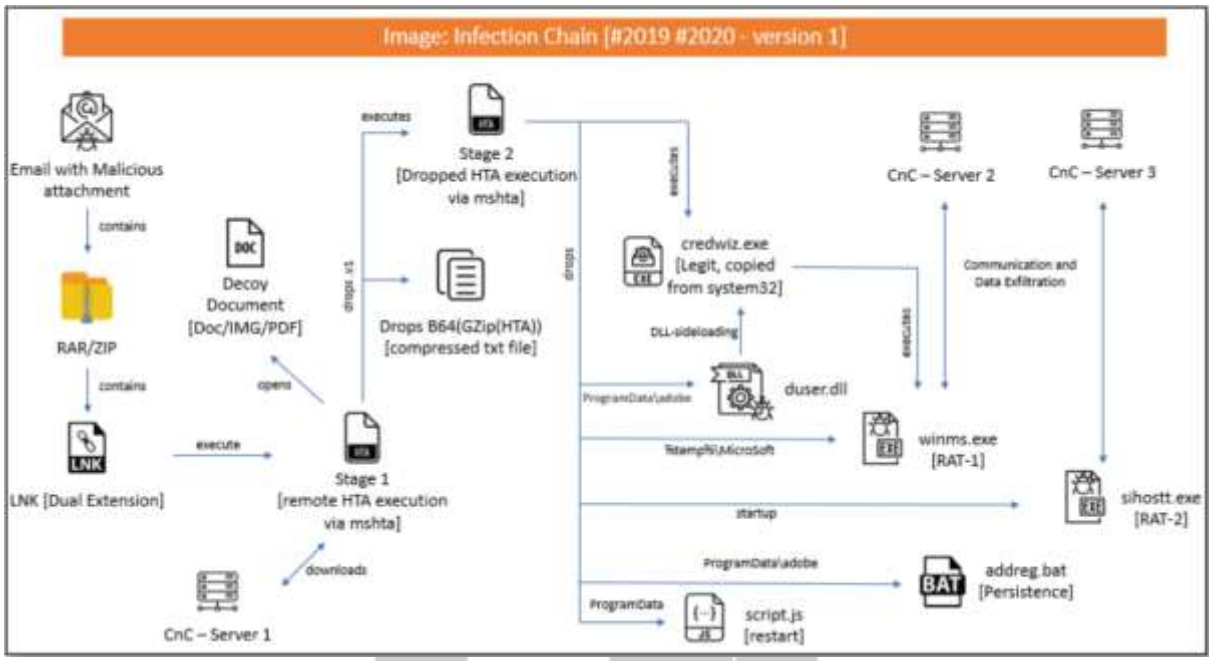

Figure 1: A SideCopy attack chain observed by Seqrite Labs – starting from a malicious LNK file in a ZIP, leading to staged execution of DLL payloads and final RAT deployment.

1. **Initial Access – Lure and Delivery:** SideCopy almost always begins with **spear-phishing**, but instead of sending a macro document, they favor archive attachments (ZIP or RAR files) containing shortcut .LNK files disguised as documents. The LNK filenames use a double extension trick (e.g., Report.pdf.lnk) to appear as if they are PDF/DOC files. Phishing themes observed include provocative topics such as military scandals, policy drafts, or even social issues within the armed forces (e.g., one campaign used "Homosexuality – Indian Armed Forces" as a lure title). When the user extracts and clicks the LNK, it silently executes a malicious script via Windows utilities (often using mshta.exe to run an HTML application). *(MITRE: Spearphishing Attachment – T1566.001; Malicious Link in File – T1204.002)*

2. **Stage 1 – Remote Script & Decoy:** The LNK-triggered MSHTA process fetches a remote .hta (HTML Application) file from a **compromised domain** controlled by SideCopy. This HTA contains two embedded files (often Base64-encoded within): a decoy document (to show the user) and a malicious DLL payload. The DLL is executed in memory (reflective loading) via the script, and it immediately opens the decoy document (e.g., a benign PDF relevant to the lure topic) to avoid arousing suspicion. The user sees a legitimate-looking document (perhaps an actual policy memo or news article), while in the background the malware DLL is preparing the next stage. Notably, SideCopy has used **compromised Indian websites** to host these HTA stage files and decoys, making the activity seem more legitimate (the domains appear Indian).

3. **Stage 2 – Second-Level Payloads:** The in-memory DLL (Stage1) then retrieves additional payloads – typically downloading two more HTA files from the same domain. These contain further embedded components: an EXE and multiple DLLs for the final stage.

SideCopy often employs **DLL side-loading** here by dropping a legitimate application along with a malicious DLL. For example, they may drop a copy of Windows Credential Wizard (credwiz.exe) alongside a malware DLL so that the legitimate EXE will load the malicious DLL. The Stage2 payloads set up persistence (often a Run key in registry named to blend in, e.g., "issas" instead of "lsass"), and then proceed to execute the final malware stage.

4. **Final Stage – RAT Deployment:** After all this staging, SideCopy finally deploys its Remote Access Trojans (RATs). In a 2024 campaign, they intriguingly launched **two different RAT instances in parallel** for redundancy. The final payloads were variants of the Delphi-based **AllaKore RAT**, each connecting to the same C2 server but on different ports. Once running, these RATs give the attackers full remote control: they can log keystrokes, enumerate files, upload/download files, execute commands, and monitor the clipboard. The use of two RAT instances ("Double Action RAT" tactic) means that even if one is discovered or crashes, the other might persist. The RATs communicate with hardcoded IP addresses over designated ports, sending periodic beacon pings and awaiting commands.

5. **Post-Exploitation:** With the RAT access established, SideCopy conducts typical post-exploitation tasks. They gather system info (user, hostname, OS version) and likely escalate privileges if needed (though many of their targets are regular user workstations where admin rights may not be needed). They then proceed to **credential harvesting** and lateral movement if the target is of high value within a network. SideCopy has been observed using tools like *Mimikatz* to dump credentials, and leveraging any stolen credentials to move laterally via SMB or RDP within Windows networks. In some cases, they deploy additional specialized malware: e.g., **ReverseRAT** (a .NET-based backdoor) or file collectors like **Cheex** (document stealers) and USB siphoning tools. Data of interest (documents, emails, database exports) is then exfiltrated, often zipped and sent over the existing C2 channels. SideCopy's malware can also propagate to removable drives if instructed, which hints at an interest in air-gapped networks or data theft via USB.

Notable Tools and Malware: SideCopy's arsenal is varied, combining custom tools with repurposed open-source software:

- **AllaKore RAT:** An open-source Delphi RAT, modified by SideCopy. AllaKore provides full backdoor capabilities (file management, keylogging, etc.). SideCopy's use of AllaKore in multiple campaigns (including deploying two variants simultaneously) shows it's a staple for them.
- **Ares RAT:** Another open-source RAT (available on GitHub) that SideCopy has ported to Windows and even Linux. In late 2023, they deployed a **Linux variant of Ares RAT** in parallel with Windows infection chains – suggesting a capability to target Linux servers or systems as well. Code similarities in the Ares payload stager linked it back to Transparent Tribe's developers.
- **Action RAT & CetaRAT:** Custom Windows RATs likely developed in-house (or by their parent group). These have been seen in phishing attacks against Indian government employees. Action RAT provides remote shell and surveillance features, while **CetaRAT** (observed by Indian CERT) is a simple trojan for file exfiltration.
- **ReverseRAT:** A .NET backdoor that was first observed in 2021, capable of executing 30+ commands from the controller, including dumping browser credentials and capturing screenshots. SideCopy has used ReverseRAT in conjunction with other RATs during campaigns targeting Indian organisations.
- **Margulas RAT:** Another custom malware name linked to SideCopy (possibly a variant or evolution of another RAT).

- **Spark RAT:** A cross-platform RAT (written in Golang) that SideCopy adopted in 2024. Spark RAT can run on Windows and Linux and was used in conjunction with a Windows-only CurlBack RAT in recent attacks. Spark RAT provides basic backdoor functions and is likely based on an open-source project, customized for SideCopy's needs.

- **CurlBack RAT:** A *"previously undocumented"* malware that surfaced in late 2024, named by researchers for its functionality. CurlBack RAT can gather system info, download files, execute commands, and even attempt privilege escalation on Windows. It was deployed alongside Spark RAT, indicating SideCopy's increasing sophistication in using multiple new malware simultaneously.

- **Additional Tools:** SideCopy also employs utility scripts and tools such as: a **USB Auto-Copy tool** that automatically steals files from any USB drives connected (to later exfiltrate them); malicious loaders like **DoubleAgent** (not to be confused with a known exploit) to inject payloads; and various obfuscation methods (like heavily obfuscated HTA scripts, PowerShell scripts that decrypt AES-encrypted payloads in memory). In one campaign, SideCopy was found exploiting a Zero-Day in WinRAR (CVE-2023-38831) to hide scripts in archive files, demonstrating quick adoption of new exploits.

Tradecraft and TTPs: SideCopy is distinguished by its elaborate social engineering and anti-detection techniques:

- It often **masquerades payloads** as legitimate files (e.g., using real document icons, or naming malware files as "*seqrite.jpg*" or other innocuous names). This falls under masquerading techniques to deceive victims and defenders.

- It re-uses **compromised Indian websites/domains** to host malware stages, which lends credibility to their phishing (the domain names appear related to India). For example, domains like sunfireglobal[.]in or elfinindia[.]com were used in their campaigns, resolving to attacker-controlled servers.

- SideCopy pays attention to **environment detection** – e.g., their HTA scripts check for certain antivirus products (Quick Heal/Seqrite, Kaspersky, Avast, etc.) on the system and alter payload execution accordingly. They have conditional branches to execute different final payloads if specific AV solutions are present, likely to avoid detection (for instance, using a different sideload technique if Windows Defender is active).

- They utilize **living-off-the-land binaries** (LOLBins) like mshta.exe, regsvr32.exe, rundll32.exe, and signed system executables (e.g., the aforementioned credwiz.exe) to execute their malicious code. This helps them blend in with normal system activity and bypass application whitelisting. *(MITRE: Trusted Developer Utilities Proxy Execution – T1218)*

- **Encryption & obfuscation:** Many components of SideCopy's chain are encoded or encrypted to evade network monitoring. They commonly use Base64 and custom obfuscation on scripts, and their later stage payloads are AES-encrypted blobs decrypted in-memory via PowerShell. This makes it harder for static defenses to flag their malware.

MITRE ATT&CK Mapping: Key techniques associated with SideCopy include:

- Initial Access: *T1566.001 Spearphishing Attachment (LNK in ZIP)*, *T1190 Exploit Public-Facing Application* (e.g., WinRAR vulnerability).

- Execution: *T1204.002 User Execution – Malicious Link/File*, *T1218.005 Mshta* (used to run HTA).

- Persistence: *T1547.001 Registry Run*, *T1547.009 Shortcut Modification* (placing LNK in Startup).
- Defense Evasion: *T1027 Obfuscated Files or Information*, *T1218 Signed Binary Proxy Execution*, *T1036 Masquerading*.
- C2: *T1071 Application Layer Protocol (HTTP/S)*, *T1043 Commonly Used Port* (they often use ports 6663, 9828 as seen in campaigns).
- Exfiltration: *T1041 Exfiltration Over C2 Channel*.
- Collection: *T1115 Clipboard Data*, *T1005 Data from Local System* – (as RAT capabilities).
- Lateral Movement: *T1021 Remote Services (SMB/Windows Admin Shares)* – if moving within network.

Sectoral Targeting: SideCopy initially zeroed in on Indian **defense and military personnel** – for instance, Army officers have been targeted with lures related to security clearances or internal reports. By 2024, SideCopy expanded to government offices (ministries and agencies) and critical infrastructure. Some confirmed targets include units in India's defense research orgs, employees of power sector organizations, and more recently individuals in ministries like External Affairs (diplomats). Campaigns in Dec 2024 extended to **railways** and **oil & gas sectors**, suggesting an interest in broader strategic intelligence. There are also cases of SideCopy targeting the **Afghan government** in the past (when a friendly government to India existed), as well as some Pakistani military individuals (perhaps for counterintelligence). By and large, however, their focus remains Indian entities, especially those that can yield defense or geopolitical information. SideCopy has also dabbled in targeting the **energy sector** in India: TTPs resembling SideCopy were noted in phishing attempts against employees of state electricity boards in late 2024 (as we detail in the Energy case study below). Given their SideWinder-mimicking origin, it's clear SideCopy's mission is tightly aligned with Pakistani state interests against Indian security targets.

"Operation Celestial Force" (APT10-Style Multi-Sector Group)

Overview: *Operation Celestial Force* refers to the years-long cyber espionage campaign by the Pakistan-based group dubbed **"Cosmic Leopard"** by Cisco Talos. This group exhibits an ambitious targeting scope and tradecraft reminiscent of China's APT10, hence we label it an "APT10-style" campaign. Cosmic Leopard has been spying on Indian government, defense, and even private sector tech companies since at least 2016. It overlaps in some characteristics with Transparent Tribe (shared interests and some malware), but is distinct in its emphasis on **multi-platform operations** and creative social engineering for initial access. In effect, Cosmic Leopard appears to be another division of Pakistan's cyber apparatus with a charter to conduct **broad espionage across government and critical industries**.

Attack Kill Chain: This group's kill chain often starts not just with email phishing but also with **direct social media interaction** – a tactic more commonly seen in APTs from other regions. According to Talos, earlier in its operations Cosmic Leopard used spear-phishing emails, but by 2019+ it shifted to engaging targets via social channels (Facebook, WhatsApp, etc.). A typical attack sequence might be:

1. **Target Profiling & Social Engineering:** The attackers identify individuals of interest (e.g., government officials, military officers, employees at defense contractors). Using platforms like Facebook or LinkedIn, they approach these targets under false personas – often as attractive women or recruiters – in classic **honey trap** style. Over days or weeks, they build rapport and eventually suggest the target use a particular app or service for further communication or file sharing.

2. **Delivery – Malicious App/Link:** The target receives a link, purportedly to a **secure messaging app or cloud storage service**, that the attacker recommends. For example, the victim might be told to download a new chat application for confidential talks. The link actually leads to an attacker-controlled website that mimics a legitimate service but offers a trojanized application. In one observed case, victims were directed to a fake site to download an Android app for cloud storage, which was in fact Cosmic Leopard's malware dropper. On PCs, the link may offer a "document" or an installer that is bundled with malicious components.

3. **Execution – Multi-Platform Malware:** Cosmic Leopard's hallmark is deploying malware on whatever platform the victim uses. If the victim is on **Android**, they download an app (APK) that looks and works like a real messaging/storage app but hides the **GravityRAT** trojan within. If on **Windows**, the victim might run an installer that drops two applications: a decoy legitimate app and the malicious payload (via their **HeavyLift** loader). The decoy app might even function normally (to avoid suspicion), while HeavyLift runs in background. In some cases, they created *Windows* and *Android* versions of the same app (e.g., a "Secure Cloud Drive" application) to target users on either platform with tailored malware.

4. **Installation & Persistence:** On Android, once the user installs the fake app, it will request extensive permissions (contacts, mic, storage, SMS, etc.). The GravityRAT spyware then starts running, invisible to the user (often the app will hide its icon after first launch). It persistently runs in the background (requesting ignore-battery-optimizations to not be shut down). On Windows, HeavyLift usually installs a service or scheduled task for persistence, and drops its payload in discreet locations (e.g., masquerading in %ProgramData%). HeavyLift's loader typically plants a legitimate decoy (for instance, a real cloud storage client) alongside the malicious agent to keep up appearances.

5. **C2 and Operation:** The GravityRAT malware on Android is quite powerful: it can read SMS and call logs, record phone calls, take photos, fetch device info (IMEI, number, etc.). It then forwards this data to the C2 server or to an intermediary drop-point (possibly cloud-based). On Windows, HeavyLift's payload has a dual role – it can actively exfiltrate files *and* can allow the victim to *upload* files to what they think is their cloud, which the attacker can then access. In essence, the attacker may trick the victim into self-exfiltrating sensitive documents by "backing them up" to the provided cloud service (which is controlled by the attacker). Meanwhile, the malware can also fetch additional modules from the attacker (for example, if they realize the victim has certain info, they could push a keylogger or a more specialized tool via HeavyLift's update mechanism).

6. **Data Exfiltration & Long-Term Access:** Cosmic Leopard is patient. They aim to quietly surveil the victim over time. The stolen data (documents, communications, etc.) is analyzed to decide next steps. If the compromised individual has access to larger networks, the attackers may then pivot – e.g., use stolen credentials to access a company VPN or spread via infected documents. The endgame is to obtain as much strategic information as possible: defense plans, policy documents, technical designs, etc. There is no immediate "destructive" action; it's pure espionage. The group often keeps accesses dormant and periodically reconnects (so-called low-and-slow approach). Their use of cloud-mimicking C2 infrastructure (sometimes actual commercial cloud accounts) helps keep these communications under the radar.

Tools and Malware: The key tools in Operation Celestial Force include:

- **GravityRAT:** Initially discovered around 2017 targeting Indian users, GravityRAT is a fully-featured spyware. The Windows version logs keystrokes, can scan for Office files to steal, and checks for antivirus. The group expanded it to Android around 2019 (and even a Mac version later). Notably, some GravityRAT variants would not infect machines if they detected Pakistani locale settings, indicating it was meant for foreign targets (e.g., Indians) – a clue linking it to a Pakistani source. The Android GravityRAT (hidden in apps named "MeetUp" or "Hangout" etc.) does all that was described (call log, SMS theft, etc.)

and uploads data to the attacker. It can also receive commands to download or delete files on the phone.

- **HeavyLift:** This is a custom Windows malware loader (first noted by Talos in 2019). HeavyLift is typically an executable that pretends to be an installer for something benign. Under the hood, it drops two payloads: one decoy app and one malicious. The malicious part (sometimes also called *Sneepy* in some reports) collects system info, can exfiltrate files, and importantly, can download additional malware on command. HeavyLift acts as a platform for the attackers – once on a system, they can instruct it to install other tools or perform tasks like a pseudo remote desktop. The most novel feature as noted by researchers is its ability to present itself as a **cloud storage client** to the victim, encouraging them to upload files which then go straight to the adversary.

- **Harpoon (Phishing Suite):** Not a malware per se, but the group has a phishing toolkit to clone websites and spin up convincing pages. For example, they registered domains similar to legitimate services (or even abused real code-signing certificates to sign their fake apps, making them look legitimate). Their infrastructure likely includes multiple phishing domains and spoofed SSL certificates to appear as genuine sites.

- **Additional Implants:** Cosmic Leopard likely has other tools for lateral movement or data staging, such as modified versions of open-source RATs or network scanners. Some reports have mentioned the use of older malware like **GravityRAT for Windows** being updated with new obfuscation in 2020–21, and possibly the use of cloud-based C2 (like leveraging Google Firebase or Dropbox API for communications).

- **Re-Use of Transparent Tribe Tools:** Since Cosmic Leopard overlaps with Transparent Tribe, they may also use some TT tools when needed. For instance, if an operation calls for it, they might deploy Crimson RAT or CapraRAT. In fact, ESET found CapraRAT inside those fake secure messaging Android apps in a 2022–23 campaign, which was likely this group or a closely allied one.

Distinctive Tactics: This group's approach is **slow, stealthy, and human-intensive**:

- The direct approach via social media is resource-heavy (requires agents to chat with targets over time), but it has yielded results – evidenced by at least 150 victims in one campaign, including not just Indians but also some in Russia and the Middle East who were likely collateral or additional targets.

- They build **convincing fake apps/services**. As noted by researchers, one such fake cloud service was so well-done that even analysts had to double-check if it was truly malicious or an actual legitimate service. This level of polish is unusual for Pakistani groups, indicating either significant effort or external support.

- Cross-platform targeting is a hallmark. By targeting mobile, they get phone conversations and messages (great for intel on the go). By targeting PCs, they get documents and emails. This comprehensive coverage is akin to Chinese tactics (e.g., APT41 also did simultaneous mobile and PC malware in some campaigns). It suggests the group is technically adept and has dedicated malware developers.

- They practice good operational security: for instance, not using the same servers for too long, and sometimes piggybacking on **cloud infrastructure** to hide their tracks (they might deliver data to cloud drives that they later access, rather than direct to a Pakistani IP).

MITRE ATT&CK Mapping: Key techniques for Operation Celestial Force include:

- Initial Access: *T1566 (Phishing)* – but via **Social Media** (which falls under *T1566.002 Spearphishing via Service*). Also *T1190 (Drive-by compromise)* if using a fake site to host payloads.
- Execution: *T1204 User Execution* (user runs the fake installer/app).
- Persistence: *T1547.001 Registry Run* (for HeavyLift), *T1546.005 Android Broadcast Receiver* (for persistent Android malware on boot).
- Defense Evasion: *T1406 Obfuscate/Encrypt Mobile Code* (Android apk hidden functionality), *T1036 Masquerading* (apps and programs mimicking legit services).
- C2: *T1071.001 Web Protocols* (communicating to web APIs), *T1102 Web Services* (using cloud storage as C2/exfil medium).
- Collection: *T1123 Audio Collection* (recording phone calls via CapraRAT), *T1119 Automated Collection* (GravityRAT automatically collecting file types), *T1056 Keylogging*.
- Exfiltration: *T1041 Exfiltration Over C2*, *T1567 Exfiltration to Cloud (OneDrive/Dropbox)*.
- Impact: N/A – notably, this group thus far hasn't been deploying ransomware or destructive payloads as part of their known operations (their motive is espionage).

Sectoral Targeting: Operation Celestial Force is expansive. It targets **government officials, military personnel, defense contractors, and related tech firms** in India. For example, an engineer at a weapons development organization or an IT admin at a military academy could be targeted via LinkedIn. The group has also targeted some individuals in the **telecom sector and energy sector** if their roles tie into national security (like an executive at a state-owned oil company, or a senior telecom official who might have info on communications infrastructure). There is evidence some victims were in neighboring countries and the Middle East, which might indicate either regional espionage or simply that those individuals were connected to Indian targets. In essence, Cosmic Leopard behaves like an "advanced persistent collector" – anyone with access to valuable strategic information about India's security, diplomacy, or economy could be in their sights.

Case Studies of Major Cyber Incidents (2024–2025)

To illustrate the methodologies and impact of Pakistan-aligned APT campaigns, we examine six intrusions recorded across critical Indian targets. Each concise case study outlines the attack timeline, initial access and payload delivery, deployed tools and persistence tactics, evasion techniques and key indicators of compromise (IoCs). Detailed and full IOCs are provided in the respective annexures at the end of the report. Together they reveal both recurring patterns and the rapidly evolving tradecraft reshaping India's cyber-threat landscape.

Case Study 1: Pahalgam Terror Attack Lure Campaign

Threat Actor: Transparent Tribe (APT-36)

Target Sector: Indian Government Officials and Agencies
Incident Date Range: April – May 2025

Incident Overview

In the wake of the April 2025 terror attack in Pahalgam, APT36 launched a spear-phishing campaign exploiting the crisis. Government officials received emails impersonating official responses to the attack, carrying either a malicious .ppam file or links to credential-harvesting websites spoofed as official domains. The goal was to exfiltrate real-time situational intelligence from internal Indian security communications.

Infection Mechanism

Two infection vectors were employed:

1. **Malicious PDF Link Vector**
    - PDF files titled **"Action Points & Response by Govt Regarding Pahalgam Terror Attack"** contained a clickable link.
    - Clicking redirected victims to a **typosquatted domain**: jkpolice.gov.in.kashmirattack.exposed
    - This domain spoofed the J&K Police site and **harvested credentials** entered by victims.
2. **PPAM Payload Vector**
    - Parallel emails carried a PowerPoint add-in file (.ppam) disguised as an official slide deck.
    - Once macros were enabled, the file dropped a **Crimson RAT** binary and opened a **decoy presentation** to divert suspicion.
    - The payload was stored in a hidden user directory and launched silently.

Command & Control (C2) Infrastructure

- The Crimson RAT used **custom user-agent strings** and communicated with C2 at **IP: 93.127.133[.]58**, using **ports 1097, 17241, and 27425**.
- The domain and C2 pattern strongly resembled previous Transparent Tribe infrastructure, commonly hosted through **Contabo**.

Lateral Movement & Objectives

- Once initial access was gained, attackers:
    - Accessed shared government drives using stolen credentials.
    - Searched for sensitive documents such as **meeting minutes, inter-service memos, and contact lists** of senior officials.
- The RAT attempted to list network shares and pull files related to **internal response actions** to the Pahalgam crisis.

Detection & Response

- Government SOCs flagged anomalous behaviour:
  - Suspicious subdomain structures.
  - Unfamiliar user-agent strings linked to Crimson RAT variants.
- The Indian Computer Emergency Response Team (CERT-In) issued sinkholing directives for the malicious IPs within 48 hours.
- Email gateways were updated to block:
  - PDF files referencing the Pahalgam incident with external links.
  - PPAM executions across @gov.in endpoints.

Indicators of Compromise (IOCs)

- **Malicious PDF Hash**: c4fb60217e3d43eac92074c45228506a
- **Spoofed Domains**:
  - jkpolice.gov.in.kashmirattack.exposed
  - iaf.nic.in.ministryofdefenceindia.org
- **C2 IP Address**: 93.127.133[.]58
- **Ports Used**: 1097, 17241, 27425

Attribution

- The use of geopolitical lures based on **recent crises**, delivery via .ppam, **Crimson RAT payloads**, and **Contabo-hosted C2** infrastructure definitively link this campaign to **Transparent Tribe (APT36)**.

Key Takeaways

- **Crisis-driven phishing** remains a favored tactic for APT36, exploiting public fear and urgency to bypass scrutiny.
- Using **dual vectors** (credential theft + RAT deployment) maximizes both short-term and long-term espionage potential.
- **Rapid threat intelligence sharing** and **domain takedown coordination** are critical in responding to fast-moving campaigns.

Case Study 2: Indian Army "Posting Policy" Phish

Threat Actor: Transparent Tribe (APT-36)

Target Sector: Indian Armed Forces (Officer Corps)
Campaign Period: February – March 2023

Incident Overview

APT36 leveraged a macro-enabled PowerPoint add-in file (.ppam) titled **"Officers posting policy reviseed final.ppam"**, masquerading as an official document revising inter-command transfer policies for Army officers. This was a spear-phishing campaign specifically crafted to gain persistent access to military systems using a dual Crimson RAT payload embedded within a ZIP archive inside the .ppam file.

Infection Chain

- The .ppam file contained two embedded OLE objects:
  - A **ZIP archive** carrying **two Crimson RAT binaries**.
  - A **decoy PowerPoint presentation** simulating an official circular on officer posting policy.
- When the macro was enabled:
  - The archive was **extracted to C:\ProgramData\Oflsc****, where one of the two RAT binaries was chosen based on the .NET Framework installed.
  - The decoy slide deck was opened to distract the user.
  - The Crimson RAT connected to C2 infrastructure, primarily at **IP 104.168.48[.]210**, with backup hardcoded IP **102.121.102[.]151** which was unused.

Payload Details

- **RAT Executable**: injavte mnr.exe
- **PDB Path**: e:\injavte mnr\injavte mnr\obj\Debug\injavte mnr.pdb
- **RAT Capabilities**:
  - Remote command execution
  - File system traversal and file theft
  - Screen capturing
  - File and directory listing
  - Registry-based persistence via virbvorlewer
  - OS, user, and process enumeration
  - Download and upload files from/to C2

Command Set

Command	Functionality
procl / getavs	Get a list of all processes
endpo	Kill process based on PID
scrsz	Set screen size to capture
cscreen	Get screenshot
dirs	Get all disk drives
stops	Stop screen capture
filesz	Get file information (Name, Creation Time, Size)
dowf	Download the file from C2

cnls	Stop uploading, downloading and screen capture
scren	Get screenshots continuously
thumb	Get a thumbnail of the image as GIF with size 'of 200x150.'
putstrt	Set persistence via Run registry key
udlt	Download & execute file from C2 with 'vdhairtn' name
delt	Delete file
file	Exfiltrate the file to C2
info	Get machine info (Computer name, username, IP, OS name, etc.)
runf	Execute command
afile	Exfiltrate file to C2 with additional information
listf	Search files based on extension
dowr	Download file from C2 (No execution)
fles	Get the list of files in a directory
fldr	Get the list of folders in a directory

Persistence Mechanism

- Achieved via the Windows Registry key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\virbvorlewer
- Crimson RAT registered itself under this key to **execute at startup**, ensuring long-term presence.

Attribution

- Use of .ppam for payload delivery, consistent PDB paths, Crimson RAT variants, and Contabo-hosted C2 infrastructure aligns this campaign with known **Transparent Tribe (APT36)** tactics.
- The RAT's C2 also used the SSL cert common name WIN-P9NRMH5G6M8, registered with **Global Cloud Line**, confirming the group's infrastructure fingerprint.

Indicators of Compromise (IOCs)

- **PPAM** **SHA-256**: 65ce50291dedb9247295dbbf8f1a83ac671860cb4c4c297d5a7f4046ba848c9e
- **RAT** **SHA-256**: c33ee5a2d9df04d07df9f02678f1f880d271dd4d21140f51468eb6affc38a8e8
- **C2 IPs**: 104.168.48[.]210, 151.106.19[.]20, 172.245.80[.]12 (multiple ports)
- **Registry Key**: HKCU\...\Run\virbvorlewer

Key Takeaways

- The use of **PowerPoint add-ins (PPAM)** reflects an evolution from traditional DOCM-based phishing.
- **Dual payloads** and tailored persistence mechanisms point to an extended espionage objective.
- Recognizing **macro-based anomalies in non-standard Office formats** (like .ppam) is crucial for future defense.

Case Study 3: Espionage against Indian Institutes of Technology

Threat Actor: Transparent Tribe

Target Sector: Academia – IIT Hyderabad, NIT Trichy, IESE Business School, and others
Campaign Timeline: May 2022 – March 2024

Incident Overview

Transparent Tribe extended its operations beyond military domains by infiltrating top Indian academic institutions. These attacks were driven by the objective of harvesting **research intelligence** and **long-term talent profiling data**. The threat actor leveraged *macro-enabled Word documents (.docm)* disguised as academic content to deliver Crimson RAT, and in some cases Capra RAT, to infected endpoints.

Infection Mechanism

- Lure documents included titles like:
  - **Assignment-17.docm**, **Technology-Survey.docm**, **M1-Financial-Accounting.docm**, and **Industrial-Engineering.docm**
- These documents:
  - Embedded ZIP archives as OLE objects.
  - Contained VBA macros that, when enabled, extracted the ZIP and executed the RAT payload.
  - Displayed decoy questionnaires or class assignments post-execution to divert attention.

Payload & Execution

- The ZIPs carried **Crimson RAT binaries**, compiled in tandem with the .docm creation date.
- Payload path and attributes:
  - PDB paths such as e:\injavte mnr\... were used across variants, establishing code lineage.
  - Targets were selected based on their .NET framework version; the appropriate RAT binary was dynamically deployed.

Persistence & C2 Activity

- Once active, Crimson RAT communicated with a rotating set of Contabo-hosted IPs, notably:
  - **104.168.48[.]210**, **151.106.19[.]20**, and **172.245.80[.]12**
- Commands issued by the RAT included:
  - File search and exfiltration
  - Screen capture and command execution
  - Registry persistence using keys like virbvorlewer
- Multiple sessions recorded beaconing to **mutexes** such as VTassignment—signaling multiple infections tied to the same campaign infrastructure.

Target Objectives

- APT36 aimed to:
  - Steal academic research on emerging technologies (e.g., **quantum materials, AI**, and **simulation models**).
  - Collect **student rosters and staff directories** for surveillance and profiling.
  - Access **institutional SharePoint and O365 repositories** using compromised credentials.

Detection & Response

- Telemetry across academic networks surged between **Q4 2022 to Q1 2023**, peaking in February 2023.

- Alerts were triggered by reuse of known VBA macro patterns and C2 indicators

Indicators of Compromise (IOCs)

- **Malicious DOCM Hashes**:
  - d6cf93b031f2e3b8758c41f5ce665a1f (Industrial Engineering)
  - 8d8311afbc81c2bb319cd692460b1632 (M1-Financial-Accounting)
- **Archive Samples**:
  - injavte mnr.zip, jedvmtrvh.zip, jivmtirvh.zip
- **C2 IPs**:
  - 104.168.48[.]210:7516, 26442, 151.106.19[.]20:16867, others

Attribution

- Shared infrastructure, RAT PDB paths, and identical VBA macro code confirm Transparent Tribe's authorship.
- The attacker reused the same infection chains from military ops, modified only in thematic lures and targeting.

Key Takeaways

- **Educational institutions have become soft yet lucrative targets** for espionage due to relaxed perimeter controls and rich intellectual capital.
- **Macro-enabled Office documents remain effective vectors**, particularly when themed with realistic academic content.
- **Proactive identity security measures** (e.g., **MFA**, **CASB**, and **IP whitelisting**) proved effective at minimizing lateral movement and impact.

Case Study 4: DRDO Contractor Breach via Multi-Stage LNK/HTA Chain

Threat Actor: SideCopy (a subdivision of Transparent Tribe APT)

Target Sector: Indian Defence R&D Subcontractors
Observed Activity: March 2023 – January 2024

Incident Overview

SideCopy executed a highly targeted cyber-espionage campaign against Indian contractors involved in Defence Research and Development Organisation (DRDO) projects. The attackers employed a deceptive chain of Windows shortcuts (LNK), HTA scripts, and DLL side-loading to deploy remote access trojans (RATs) like AllaKore RAT and ReverseRAT—designed to infiltrate engineering systems and exfiltrate sensitive defence IP.

Infection Chain & Payload Delivery

- **Initial Vector**: A ZIP archive containing a LNK file (e.g., **"Policy Draft.pdf.lnk"**) was distributed via phishing emails.
- The **LNK file**:
  - Masqueraded as a document.
  - Launched mshta.exe with a remote **HTA file** hosted on a **compromised domain**, typically:
    - hxxps://demo.smart-hospital[.]in/uploads/staff_documents/.../Sheet_Roll/html
- **Stage 1 HTA**:
  - Dropped a **legitimate binary credwiz.exe** and a **malicious DLL DUser.dll** to:
    - C:\ProgramData\Adobe\
  - Executed the DLL using **side-loading via credwiz.exe**, achieving stealthy code execution.
- **Stage 2 HTA**:
  - Embedded more DotNET components.
  - Checked antivirus software via PinkAgain() before activating persistence mechanisms.

Payload Characteristics

- **DUser.dll**:
  - Built in Delphi (not .NET like Sidewinder's toolset).
  - Contained export functions such as cfileexists to trigger RAT payload (winms.exe) from %TEMP%\Microsoft\.
  - Connected to Contabo C2: 173.212.224.110:6102
- **winms.exe** (AllaKore RAT variant):
  - Implements commands like file listing, screen capture, shell command execution, and clipboard access.
  - Matches open-source RAT structure from: https://github.com/Grampinha/AllaKore_Remote/blob/master/Source/Client/Form_Main.pas
- **C2 Infrastructure**:
  - vmi312537.contaboserver.net (IP: 144.91.91.236:6102)
  - Additional domains linked to kingsmanfisher@gmail.com, confirmed to have registered earlier Pakistani phishing infrastructure

Lateral Movement & Objective

- Attackers harvested **design engineer credentials** post-compromise.
- Used RDP sessions to access **internal engineering subnetworks**.
- Exfiltrated:
  - **CAD drawings**, **telemetry logs**, **design simulation data**, and **procurement schedules**.
- Exfiltration occurred over Dropbox using **hardcoded tokens** (e.g., prefix Agh9t.)

Persistence & Evasion

- Persistence via:
  - Registry Run keys (addreg.bat dropped by HTA) and automatic restart via script.js triggered shutdown/reboot post-installation.
- Memory-resident techniques:
  - .NET deserialization via CactusTorch-style payloads.
  - Most modules were executed **filelessly** from memory, with **no artifacts written to disk** except during DLL loading.

Indicators of Compromise (IOCs)

- **Malicious Domains**:
  - demo.smart-hospital[.]in, vmi312537.contaboserver[.]net
- **IP Addresses**:
  - 173.212.224.110, 144.91.91.236, 173.249.50.230
- **DLL & EXE Hashes**:
  - DUser.dll: AC4A8D82D91286D5E0F59B85C8975DF8
  - winms.exe: AF0DD0070C02E15064496853BEFFA331
- **Dropbox Exfil Token Prefix**: Agh9t

Operational Impact

- One **prototype missile subsystem design** (non-classified) was leaked.
- Internal Dev PCs required **forensic reimaging**.
- Heightened **export control scrutiny** due to exfiltrated simulation files.

Attribution

- Use of **Side-loading via credwiz.exe**, **HTA delivery**, **Delphi-based DLLs**, and Contabo IP overlap conclusively ties the campaign to **SideCopy**, an active subdivision of Transparent Tribe APT.

Key Takeaways

- **SideCopy mimics other APT groups' TTPs**, notably Sidewinder, to obfuscate attribution.
- **Living-off-the-land binaries (LOLBins)** like mshta.exe and credwiz.exe are central to the actor's stealth operations.
- **Isolating R&D environments** from general IT infrastructure is critical to limiting blast radius.
- Monitoring **remote HTA usage** and blocking **Contabo-hosted endpoints** remains a high-priority mitigation strategy.

Case Study 5: Election-Results Lure against Government & Media

Threat Actor: Transparent Tribe

Target Sector: Indian Government Officials and Political Journalists
Timeline: July 2024

Incident Overview

In July 2024, K7 Labs identified a malicious campaign wherein threat actors disseminated a document titled “Indian Election Results” to target Indian users. Upon analysis, it was found that the document deployed the Crimson Remote Access Trojan (RAT), a malware predominantly associated with the Transparent Tribe APT group. This group has a history of targeting diplomatic, defense, and research entities in India and Afghanistan.

Technical Details

- **Initial Vector**: The attack utilized a .docm file, which is a macro-enabled Word document. This document contained embedded files, including the Crimson RAT payload and a decoy document displaying election results.
- **Execution Flow**:
  - Upon opening the .docm file, macros were executed that extracted embedded objects (oleobject7, oleobject10, and oleobject11).
  - These objects contained base64-encoded ZIP files, which, when decoded, revealed the Crimson RAT payload.
  - The payload was written to the AppData folder and then decompressed into the Documents folder as a screensaver file named hacrvidth vibev.scr, which was subsequently executed.
  - Simultaneously, a decoy document displaying election results was opened to distract the user.
- **Persistence Mechanism**:
  - The malware introduced a delay of approximately 25 minutes before initiating its malicious activities, likely to evade sandbox detection.
  - It then added a registry entry under the current user's Run key with a randomly generated name to ensure persistence across system reboots.
- **Command and Control (C2)**:
  - After another delay of about 20 minutes, the malware attempted to connect to its C2 server using a hardcoded domain and IP address.
  - If the connection was unsuccessful, the malware process terminated.
- **Capabilities**:
  - Once connected to the C2 server, the malware could execute various commands, including:
    - Capturing screenshots and sending them back to the C2 server.
    - Listing all running processes.
    - Creating new registry entries for persistence.
    - Reading and writing files on the system.
    - Deleting files.
    - Gathering system information, including OS details and user information.
    - Executing arbitrary commands received from the attacker.

Indicators of Compromise (IOCs)

- **Malware Hashes**:
  - Election Lure Document: 4473b78e67067a9299227cc02b8e28e2
  - Crimson RAT Variants:
    - e6f4bb8ed235f43cb738447fbf1757c3

        - da2331ac3e073164d54bcc5323cf0250
        - a54c435bdbc17608fa0b8826bbe9936d
        - 7a18b1bf9b07726327ba50e549764731
        - d6b38a2272876d039d48b46aa874e7b9
        - f49375748b279565b5aed83d9ee01eb2
- **C2 Infrastructure**:
    - **Domain**: waqers.duckdns.com
    - **IP Address**: 94.72.105[.]227
- **Decoy Documents**:
    - Election Decoy: 24fc6cacfbf0f87d2a24be7361c78c76
    - Syllabus Decoy: 4166a122e5eac964ba9f4b22e2881052

Key Takeaways

- APT36 exploited the July 2024 Indian election results using a malicious .docm lure document embedded with Crimson RAT.
- The malware used delayed execution, registry-based persistence, and decoy documents to evade detection.
- Communication with the C2 server was attempted via waqers.duckdns.com (IP: 94.72.105[.]227), with command capabilities for surveillance and control.
- Payload delivery and behavior align with Transparent Tribe's historical tactics.
- Highlights the importance of macro-blocking, threat intel sharing, and endpoint monitoring during politically sensitive events.

Case Study 6: WinRAR Zero-Day & Cross-Platform Implant Bundle

Threat Actor: SideCopy

Target Sector: Indian State Government DevOps Teams
Timeline: November 2023 – April 2024

Incident Overview

SideCopy weaponized a WinRAR vulnerability (CVE-2023-38831) to compromise Indian government and defense entities. This exploit was part of a multi-stage chain that delivered **Windows and Linux remote access trojans (RATs)**—specifically, **AllaKore RAT** and a Golang-based **Ares RAT variant**—enabling cross-platform espionage.

Initial Access

- **Malicious RAR archives** containing **hidden CMD scripts** were sent via phishing emails.
- When victims opened the archive using vulnerable versions of WinRAR:
  - The **embedded script executed automatically**, contacting a remote server (e.g., storagesvr[.]shop) to fetch the Stage-2 payload.
  - This triggered download and deployment of additional malware targeting both **Windows workstations and Linux servers** within DevOps infrastructure.

Payload Execution Chain

- **Windows Stage**:
  - Used credwiz.exe (legit Windows binary) to **side-load DUser.dll**, dropped into C:\ProgramData\Adobe\.
  - The DLL's export function (cfileexists) launched a hidden payload named winms.exe, an **AllaKore-based RAT** .
- **Linux Stage**:
  - Captured SSH credentials allowed lateral movement to internal Git servers.
  - Attackers implanted a **Golang-based Ares RAT**, disguised as a Git helper binary and stored in %PROGRAMDATA%\git\ .

Persistence & Evasion

- **Fileless Execution**:
  - Used **CACTUSTORCH toolkit** to load .NET assemblies directly into memory using DotNetToJScript techniques.
  - No malware binaries were written to disk during initial execution .
- **BAT files** and **registry Run keys** were used to maintain persistence, such as:
  - C:\ProgramData\Adobe\addreg.bat to restart the malware at boot.
- **Scripted reboots** were triggered via:
- var shell = new ActiveXObject('WScript.Shell');
- WScript.Sleep(900000);
- var exec = shell.Exec('cmd.exe /k shutdown /r /t 0');

Command and Control (C2) Infrastructure

- Communications initiated from both Windows and Linux implants were routed to **Contabo-hosted servers**, notably:
  - vmi312537.contaboserver.net
  - IP: 144.91.91[.]236:6102
- Malware contacted .shop and .ddns.net domains rarely seen in standard enterprise traffic—used to evade early detection.

Indicators of Compromise (IOCs)

- **Exploit Hashes**:

  - DUser.dll: AC4A8D82D91286D5E0F59B85C8975DF8
  - winms.exe: AF0DD0070C02E15064496853BEFFA331
- **C2 Infrastructure**:
  - storagesvr[.]shop
  - vmi312537[.]contaboserver[.]net
- **PDB Paths**:
  - F:\Packers\CyberLink\Latest Source\Multithread Protocol Architecture\Final Version\DUser\Release\x86\DUser.pdb
- **RAT Registry Artifact**:
  - HKCU\...\RunOnce\ResultUpdate

Attribution

- Use of **WinRAR CVE-2023-38831**, combined with **Delphi-compiled DUser.dll**, **Contabo infrastructure**, and SideCopy's known TTPs, confirm attribution to **SideCopy**.
- This aligns with the group's strategy of adopting **public vulnerabilities quickly** and blending in **cross-platform implants** .

Key Takeaways

- **Zero-day adoption by APTs** like SideCopy reduces patching windows—especially for widely used tools like WinRAR.
- **Cross-platform RAT deployment** shows threat actors now target both developer endpoints and server infrastructure.
- **Immutability controls and SSH segmentation** must complement traditional malware defenses in DevOps environments.

Toolkits and Infrastructure Analysis of Pakistani APTs

The case studies above underscore the diverse **toolkits** and infrastructure utilized by Pakistani APTs. Their arsenals blend open-source malware with custom-developed implants, and their attack infrastructure often leverages foreign servers and cloud services to mask origins. This section analyzes key aspects of their tools and infrastructure:

Use of Open-Source vs. Custom Malware

Pakistan-linked groups are adept at repurposing **open-source malware** projects to use in attacks, balancing cost-effectiveness with custom modifications. For example, SideCopy's adoption of AllaKore RAT and Ares RAT, both available publicly, saves development effort while still yielding a capable trojan. They often lightly customize such tools (e.g., changing command strings, adding encryption) to evade signature-based detection. Similarly, **njRAT** and **XtremeRAT**, ubiquitous in the Middle East/South Asia hacking scene, have made appearances in Pakistan-attributed campaigns in earlier years.

At the same time, these APTs maintain **custom malware** for core operations, giving them unique capabilities and reducing dependency on external code. APT36's Crimson RAT is a prime example – a bespoke tool fine-tuned to their needs, used for years exclusively against their targets. Another is the development of **GravityRAT** by the Cosmic Leopard group, which started as a unique espionage tool targeting Indian systems. Over 2016–2024 we saw them evolve GravityRAT from Windows to Android and Mac, demonstrating in-house software engineering talent.

In some cases, custom malware originates from modified open-source code but diverges enough to be essentially new. The **Spark RAT** used by SideCopy in 2024 is based on an open-source cross-platform RAT, but its deployment in tandem with the novel **CurlBack RAT** (likely fully custom) shows a hybrid approach. The groups often use open-source tools as initial stage or lesser implants, while reserving custom backdoors for long-term access and important targets.

The reliance on open-source has another advantage: deniability and ubiquity. Tools like **Mimikatz** or **Meterpreter** (from Metasploit) are used by many attackers, making attribution harder. Pakistani operators have certainly used public tools for tasks like credential dumping, lateral movement, or scanning.

However, one can spot their touch in how they integrate these tools. For instance, a SideCopy infection sequence might involve an open-source RAT, but the scaffolding around it (script logic, staging technique) is custom-built and distinct. Also, in some campaigns, they chain multiple off-the-shelf components in creative ways – e.g., using a known *PowerShell stager script* from GitHub combined with a modified RAT binary and a public domain FileZilla FTP for exfil.

In summary, Pakistani APTs skillfully **mix-and-match open-source and proprietary malware** to achieve their goals. This approach lowers development overhead, speeds up operations (using existing code), and provides flexibility – all while still allowing them to innovate on critical implants that give them a edge and maintain persistence undetected.

Command-and-Control (C2) Infrastructure and Hosting Locations

These threat actors typically do not host their C2 servers inside Pakistan. Instead, they rent or compromise servers abroad to act as staging points, adding layers between their operations and attribution. Analysis of infrastructure shows heavy usage of providers in **Eastern Europe, the Middle East, and Western Europe**:

- A lot of Transparent Tribe and SideCopy infrastructure has been traced to VPS providers in **Germany** (such as Contabo GmbH) and **Russia**. Contabo in particular has surfaced

frequently – Cyble noted nearly all SideCopy C2s were on Contabo-hosted IPs at one point. These services offer cheap, anonymous rentals where abuse complaints are minimal.

- There is also evidence of infrastructure in **West Asia (Middle East)** – for instance, some domains and servers used by APT36 resolved to hosts in UAE and Turkey. It's possible they also exploit the geography of internet routes; hosting in the Middle East can reduce latency to South Asia, making C2 communication smoother.

- **South East Asian** and **Central Asian** servers have been used occasionally, possibly to target specific regions or because those locales have less cooperation with Indian authorities for takedowns.

Infrastructure is often set up with multiple layers: Domain names purchased from registrars (sometimes with WHOIS privacy, sometimes using fake details), pointing to VPS IPs. Many domains spoof or resemble Indian entities (to appear legitimate in DNS logs), such as pseudo-gov domains. Others are generic or nonsense names to avoid attention.

Additionally, these APTs make significant use of **compromised third-party servers** as part of C2. Instead of always using dedicated owned servers which can be blocked, they hack into legitimate websites (often poorly secured ones) and host malware or relay traffic. For example, SideCopy's campaigns used compromised Indian websites (like small business or NGO sites ending in .in) to temporarily host payloads and stage HTA files. By doing so, the traffic seems to go to benign Indian domains, not an obvious attacker server.

There's also evidence of *tiered C2*: malware may first connect to an attacker-controlled web domain which simply redirects or hands off communication to a second-stage server. This indirection helps with resiliency—if one node is discovered and shut down, the attacker can quickly switch to another.

We should also note the adoption of **Cloud-based C2**. We've seen APT36 using Slack channels and Google Drive as part of their C2 infrastructure. By abusing these platforms, they avoid having to maintain their own servers for certain communications, and such traffic blends with legitimate use of Slack or Google APIs. Similarly, some groups use **Telegram bots or channels** for C2 (since Telegram is popular and its traffic often allowed). This trend toward legitimate cloud infrastructure is a challenge for defenders, as blocking it can disrupt normal business usage.

In summary, Pakistani APTs utilize a **globally distributed infrastructure** strategy:

- Rent servers in bulletproof hosting locales (Eastern Europe/Russia).
- Compromise external web servers to use as pivots or stash houses for malware.
- Spoof Indian/relevant domains to make their C2 traffic less conspicuous.
- Leverage big-name cloud services (Slack, Google, OneDrive, Dropbox, Telegram) to hide communications in plain sight.

Such approaches ensure that shutting down their operations is like a game of whack-a-mole – take one down, another pops up. It also provides plausible deniability and some insulating layer if infrastructure is traced (it ends at a server in Germany rented under alias, not directly to Pakistan).

Mobile Malware and Honey Trap Operations

One striking element of recent Pakistani cyber activity is the targeting of **mobile devices**, particularly those of military or government personnel. Groups like Transparent Tribe have heavily invested in Android spyware (e.g., CapraRAT, GravityRAT mobile) to gather communications intelligence.

Their mobile malware typically comes packaged as seemingly harmless apps:

- **Chat/Messaging apps:** As detailed earlier, fake secure chat apps like "MeetUp" or "Hangaround" have been used to deliver CapraRAT. Once installed, these apps operate normally as chat platforms (often using a legitimate open-source chat codebase) but in background they spy on the device.

- **Romantic/Social apps:** Honey trap scenarios have included apps with names implying dating or friendship, which serve as lures for targets approached by operatives on social media.

- **Utility apps:** At times, the malware is hidden in apps pretending to be something useful like "storage cleaner" or even a trojanized version of an official government app (Transparent Tribe created a fake version of an Indian 2FA app "Kavach" previously).

These malware, once on the phone, can give a wealth of intel: recorded calls, SMS/WhatsApp chats, location tracking, microphone recording of ambient conversation, contact lists, etc.. This effectively turns the target's smartphone into a pocket spy. Such information is incredibly valuable for military espionage – it can reveal troop movements, plans discussed verbally, even serve as a way to gather kompromat (compromising personal information).

To distribute these malicious apps, Pakistani operators use **social engineering** rather than app stores:

- They create fake personas (often attractive women on Facebook/Twitter) and engage Indian defense personnel in chats, eventually convincing them to move to a "more secure app" for communication – which is actually the malware-laced app.

- They may also send the app APK directly via WhatsApp or email, or host it on a lookalike Google Play private link (not actually through Play Store review, but using Google Drive links that mimic it).

Another vector is the **watering-hole for mobile**: creating or infecting websites that prompt mobile users to download apps. For instance, a fake India Post site in 2024 identified if the visitor was on Android and offered an APK download.

The mobile malware often tries to **maintain persistence** by requesting device admin rights or using accessibility services trickery to auto-regrant permissions. CapraRAT, for example, can change its icon to a generic one (Google or system icon) to hide in the app list, and it will run at startup to continue surveillance.

The interplay of honey traps and mobile malware has proven very effective for Pakistani APTs. By some counts, dozens of Indian armed forces personnel were compromised in such schemes, and India's Army had to issue advisories to troops warning about unknown women befriending them online.

In essence, Pakistan's cyber operations are not limited to digital exploits – they incorporate **human element tactics (social engineering)** to implant malware on mobile devices that are often less guarded than corporate networks. This multi-dimensional approach (human + tech) is a hallmark of targeted nation-state espionage.

Abuse of Cloud Platforms and Online Services

As mentioned, an emerging trend is the abuse of popular cloud platforms as part of attack operations. This includes:

- **Using cloud storage for hosting payloads:** Instead of hosting malware on their own domain, attackers upload it to Google Drive, Dropbox, OneDrive, or similar services and then share a link to the target. Because connections to Google Drive or Dropbox are encrypted and commonplace, many network defenses won't flag the download. Also, the user is more likely to trust a Google Drive link than a random .in domain. Researchers

have observed APT36 using Google Drive to host malicious documents, and Check Point noted them using Google Drive for C2 as well.

- **C2 via cloud APIs:** Slack was used by APT36's ElizaRAT variant – where the malware communicated with a private Slack channel to receive commands. We've also seen malware (notably by other actors too) using Telegram bot APIs or Twitter to fetch instructions. These are attractive because they remove the need to maintain an infrastructure and blend in with legitimate traffic. For example, a malware might periodically check a private Twitter account for new tweets (commands encoded in them) – to any observer, it looks like normal API calls to Twitter.

- **Domain Fronting and CDN abuse:** Some advanced operators use techniques like domain fronting (using big Content Delivery Networks to mask the ultimate C2 domain) – for instance, making traffic appear as if it's going to azureedge.net (Microsoft CDN) whereas it's secretly routed to the attacker's server. While we haven't publicly seen reports of Pakistani APTs doing domain fronting, their close alignment with more advanced actors means they could adopt it.

- **Phishing with SaaS:** Cloud-based forms or services are also misused. A recent trend (general, not just Pakistan) is using Google Forms or Microsoft Forms to create phishing pages. An attacker could send an email asking a target to log in to view a file, and the link opens an Office 365-looking page which is actually a Microsoft Form collecting creds. Since the domain is forms.office.com (legitimate), it bypasses many checks.

In Pakistani APT operations, the use of **third-party services as part of kill chain** shows adaptability. One case documented Transparent Tribe using **Google URL Shortener** (before it was shut) to hide their phishing links. Another instance is their malware doing C2 via **FTP on cloud-hosted FTP servers** (FTP is old school but when on a cloud host, it's just another protocol to hide behind general traffic).

The benefit for them is twofold: evasion and resilience. It's hard for defenders to outright block Google or Microsoft domains without disrupting business. Also, takedowns of malicious content on these platforms may be slower or not immediately tied to the actor (if they use anonymous accounts).

In conclusion, the Pakistani cyber toolkit extends beyond malware binaries to clever uses of the very fabric of the internet's trusted services. This "living off the cloud" approach is an extension of living off the land, and it challenges defenders to distinguish malicious use from normal use on ubiquitous platforms.

Evolution of India's Threat Landscape (2024–2025)

The period of 2024–2025 has seen India's cyber threat landscape evolve from relatively generic threats to more **targeted, state-sponsored, and hybrid warfare-like threats**. Several key trends characterize this evolution:

- **Shift from Opportunistic to Targeted Espionage:** A few years ago, Indian entities faced mostly generic cyber threats – ransomware gangs seeking profit, hacktivists defacing websites, or widespread banking malware. While those continue, there is a clear increase in targeted APT operations aimed at espionage and disruption. Nation-state actors (especially from Pakistan and China) are zeroing in on specific strategic targets (defense, critical infrastructure, government) rather than broad-brush attacks. The discovery of long-running campaigns like Operation Celestial Force emphasizes that highly persistent spying on Indian organizations is underway continuously.

- **Integration of Cyber Warfare Tactics:** In the wake of events like Operation Sindoor, there's been a convergence of physical conflict and cyber attacks. This points to a *hybrid warfare* approach – for example, Pakistan-based hackers simultaneously engaging in propaganda (defacements, DDoS by hacktivists) and covert intrusions (APT espionage) to complement on-ground conflict. The use of ransomware by an APT (as in the hospital case) hints at **potential wiper or sabotage attacks** lurking under the guise of cybercrime. Indian officials are increasingly concerned that future conflicts may involve attempts to disrupt power grids, communication networks, or transport systems via cyber means as a force multiplier.

- **Use of Zero-Days and Rapid Exploit Adoption:** While there's no public confirmation of Pakistan using true zero-day exploits in 2024, these groups have shown the capability to rapidly adopt newly disclosed vulnerabilities (so-called n-day exploits). The SideCopy use of the WinRAR CVE-2023-38831 within possibly weeks of its disclosure in August 2023 is a prime example. Likewise, any new critical CVE in widely used software (VPNs, mail servers, routers) could be weaponized in short order. The trend suggests a growing sophistication – potentially through access to exploit kits on underground markets or alliances with other threat actors. This raises the specter that a determined adversary could deploy a zero-day in a critical Indian system at a crucial time, something Indian defense planners must consider.

- **Living-off-the-Land (LotL) Techniques on the Rise:** Adversaries are doing more to hide in victim environments by using legitimate tools and processes – *LotL*. As seen, attackers use tools like PowerShell, WMI, native admin utilities (like netsh, schtasks, certutil for downloading, etc.) extensively. This reduces their malware footprint and can confound traditional defenses. Also, fileless malware techniques (like injecting directly into memory, as SideCopy does with in-memory DLL load) mean less to detect on disk. Indian organizations that used to rely on signature-based AV and simple IOCs now find they need behavior-based detection and skilled threat hunting to catch these LotL strategies.

- **Emergence of Destructive Malware (Wipers) and Ransomware-as-a-Weapon:** Although India has not yet reported a clear case of a politically motivated wiper malware attack, the possibility looms larger in 2024–25. The region has seen what wipers can do (e.g., Iran vs. Saudi Aramco, or Russia vs. Ukraine). Given the precedent of the pseudo-ransomware attack on NHI, one can imagine a scenario where an APT deploys a wiper to cripple, say, railway signaling or financial systems during a conflict, masquerading it as a ransomware attack to muddy attribution. The threat landscape now includes this worst-case scenario in planning exercises. On the flip side, the **Ransomware-as-a-Service (RaaS) ecosystem** has grown in India. 2024 witnessed a surge of ransomware attacks on Indian companies – not necessarily state-linked but causing significant damage. LockBit, BlackCat, and newer groups like RansomHouse hit several Indian manufacturing and tech firms. Some of these incidents had secondary effects like leaks of sensitive data (including some defense supplier information leaking on dark web). The proliferation of RaaS means state actors could potentially *hire or collaborate with criminal gangs* to conduct deniable attacks on critical targets, or simply use their tools as seen.

- **Hacktivism and DDoS as Persistent Irritants:** Over 2024, there's been a flurry of low-level but noisy attacks by hacktivist collectives, especially on Telegram, targeting Indian sites. Seqrite noted **85+ Telegram hacktivist groups** engaged in defacements and DDoS, with thousands of attacks in early 2024 alone. Many were Pakistan-sympathetic or part of broader Islamist hacktivism (e.g., during the Israel-Hamas conflict, some turned attention to India as well). While these attacks rarely cause more than website downtime or social media buzz, they contribute to an overall threat atmosphere and can act as smokescreens for more serious intrusions. The trend suggests these activities spike during geopolitical events (like Sindoor, or any India-Pakistan standoff).

In summary, India's threat landscape in 2024–25 is characterized by **greater adversary sophistication and alignment with geopolitical motives**. The country faces a combination of:

- Highly targeted cyber-espionage campaigns stealing sensitive data.
- Early signs of cyber sabotage attempts (or at least preparation for such capabilities).
- A constant background noise of hacktivism and cybercrime that complicates attribution and response.

This evolution demands a corresponding uplift in India's cyber defense posture, as the next section will address.

Defense and Mitigation Recommendations from Cybervahak

Confronted with these emerging threats, Indian organizations – especially in government and critical sectors – need to adopt a multi-layered, proactive cyber defense strategy. Below we outline recommendations at **Strategic, Operational, and Sector-Specific** levels to enhance resilience against APT attacks:

Strategic Measures

- **Enhance Cyber Threat Intelligence Sharing:** Establish and strengthen channels for real-time threat intel sharing between government agencies (CERT-In, NCIIPC, Defense CERT) and private sector (banks, power companies, telcos). Initiatives like the Information Sharing and Analysis Centers (ISACs) for different sectors should be empowered to rapidly disseminate IOCs and attack TTPs gleaned from incidents. For example, after the hospital attack and SEB breach, sharing those indicators widely helped others inoculate themselves. A national threat intelligence platform, where anonymized attack data is shared, can help connect the dots on APT campaigns targeting multiple entities.

- **Public-Private Collaboration and Training:** State-aligned attacks often blur lines between military and civilian targets. It's crucial to break down silos. Conduct joint cyber exercises involving both government cyber teams and industry CISOs to simulate Pakistan-APT scenarios (e.g., a power grid phishing attack). This builds trust and preparedness. Additionally, invest in advanced training for incident responders with a focus on APT forensics and threat hunting, possibly with international partners (since many of these APT tactics overlap with global ones).

- **Cyber Risk Governance at Leadership Level:** Organizations must treat cyber risk as a board-level issue, not just an IT issue. Leadership should be briefed on the geopolitical threat landscape and its potential impact on business continuity. Boards and senior executives in critical sectors should mandate regular cyber risk assessments and ensure cybersecurity is part of enterprise risk management. In government, this means senior bureaucrats and ministers need awareness of how cyber attacks could play into national security scenarios (for instance, how a breach in a ministry could feed into an adversary's war planning). Only with high-level buy-in can sufficient resources and attention be devoted to meaningful defenses.

- **National Cyber Response Framework:** Given the possibility of simultaneous cyber attacks during a national crisis, India should refine its national cyber incident response plan. This includes clarifying roles of various agencies (CERT-In for civil, Defense Cyber Agency for military, etc.), setting thresholds for when a cyber incident triggers national emergency measures, and ensuring communication plans are in place. Essentially, a "digital war room" concept to coordinate response across sectors in case of a major cyber offensive on India. Conducting periodic drills at the national level (like the nationwide mock cyber drill mentioned amid Sindoor tensions) can expose gaps and improve readiness.

Operational Measures

- **Adopt a Zero Trust Security Model:** Traditional perimeter defenses are not enough when attackers can phish credentials or take over legitimate infrastructure. Zero Trust architecture, which operates on the principle "never trust, always verify," should be progressively implemented. This means continuously authenticating and authorizing users and devices, and segmenting access so that compromise of one account or machine doesn't grant wide access. Practically: use strong multi-factor authentication everywhere (especially for VPNs, email, privileged accounts) – so even if credentials are stolen, they're harder to use. Implement network micro-segmentation so that sensitive servers (like CDR databases or SCADA networks) cannot be freely reached from corporate LAN segments.

- **Endpoint Detection and Response (EDR):** Deploy advanced EDR tools on endpoints and servers, which can detect suspicious behavior like code injection, unusual PowerShell usage, or credential dumping tools. Modern EDR uses real-time monitoring and machine learning to catch patterns that signature AV misses – critical against fileless and living-off-the-land techniques. For example, an EDR might catch SideCopy's sequential spawning of mshta and PowerShell processes or detect Crimson RAT's attempts to inject into memory, allowing responders to quarantine the system quickly.

- **Continuous Monitoring and Threat Hunting:** Assume that some threats will evade preventive controls, so invest in continuous network and log monitoring. Use a Security Operations Center (SOC) with skilled analysts who can spot anomalies (like that odd database query or the unusual outbound traffic in the TelecomCo case). Employ User and Entity Behavior Analytics (UEBA) to flag when an employee account behaves abnormally (e.g., a user in finance suddenly accessing server configurations). Conduct regular threat hunting exercises focusing on known APT techniques – for instance, search for the creation of new local user accounts with admin privileges, or scan memory of key servers for fragments of known malware code. Proactively hunting can catch intrusions early, before attackers reach their endgame.

- **Regular Patching and Vulnerability Management:** This sounds basic, but as we saw, unpatched VPNs and servers were gateways for major incidents. Critical vulnerabilities (especially those in perimeter devices like VPNs, firewalls, email servers, and in widely-used software like Office) should be patched on a war footing. Organizations should follow CERT-In advisories closely and have a process to rapidly test and deploy fixes. Where patching is delayed (due to operations), temporary mitigations (like disabling vulnerable services, or increasing monitoring on those devices) should be applied. Additionally, perform regular vulnerability scans and penetration tests to find and fix weaknesses before attackers do. Emulate the techniques APTs use – e.g., have pen-testers attempt phishing plus exploiting a known CVE, to ensure defenses and response are adequate.

- **Red Team Exercises and Drills:** Conduct red team/blue team exercises simulating realistic attack scenarios (like the ones in our case studies). This will test the organization's detection and response. For instance, a red team might simulate an APT36 phishing email and see if the blue team catches the C2 traffic; or simulate a data exfiltration attempt from a critical server to gauge if alerts fire. Sectoral regulators (like RBI for banks, or CERC for power companies) could mandate annual cyber drills. These drills build muscle memory for incident response and often reveal gaps (like an EDR misconfiguration or an absence of an offline backup).

- **Secure Configuration and Least Privilege:** Many incidents escalated due to overly broad privileges and misconfigurations. Operationally, implement least privilege principles: users should have only the access needed for their role. Regularly audit

accounts and disable those not needed. Ensure sensitive systems (like domain controllers, SCADA jump hosts) have extremely limited and monitored access. Turn off or remove unnecessary services and software that could be exploited (for example, if WinRAR is not needed on a server, remove it or update it). Use application whitelisting in critical servers to block execution of unauthorized binaries – this could stop a random ransomware executable from running even if it gets in.

- **Incident Response (IR) Preparedness:** Develop and maintain an up-to-date incident response plan that specifically covers APT scenarios. It should define how to isolate affected systems, preserve forensic evidence, eradicate malware, and recover operations. Teams should be familiar with digital forensics basics (so they can, say, dump memory or analyze logs immediately when something is suspected). Relationships with external IR partners or cybersecurity vendors should be pre-established so that help can be summoned quickly if needed. Essentially, be ready to execute swift containment – as in the case studies, speed is critical to prevent an intrusion from turning into a wider compromise or destructive event.

Sector-Specific Mitigations

Different sectors have unique crown jewels and risk profiles. Here are tailored recommendations for BFSI (Banking, Financial Services, Insurance), Healthcare, and Energy sectors:

- ### Government Entities

Government agencies and departments form a primary target for nation-state threat actors due to their strategic and operational value. Based on the tactics observed in the Pahalgam decoy phishing (Case 1), the election lure campaign (Case 5), and the WinRar exploitation (Case 6), it is critical that public sector organizations reinforce the following defenses:

- **Email and Document Filtering**: Implement email gateway protections that block uncommon and high-risk formats such as .ppam and .docm, while inspecting embedded links and attachments for signs of phishing. Decoy documents used in phishing campaigns targeting national events should be quarantined by default and investigated before any user interaction.

- **Mandatory Multi-Factor Authentication and Conditional Access**: Enforce MFA for all administrative and sensitive access points, especially for email, file-sharing platforms, and remote login interfaces. Incorporate conditional access policies that block logins from foreign IP addresses or restrict them to government-issued devices only.

- **Endpoint Hardening and Network Segmentation**: Deploy system-wide policies to limit script execution (e.g., restricting PowerShell to Constrained Language Mode) and monitor for suspicious process behavior such as use of certutil.exe or mshta.exe. Ensure that networks hosting sensitive communication and data are segregated from general access zones.

- **Digital Signing and Verification of Official Communications**: Given the use of official-looking decoy documents in multiple incidents, critical communications—especially those involving national crises or policy updates—should be digitally signed. Verification mechanisms should be in place for recipients to authenticate document legitimacy.

- **Security Awareness and Targeted Training**: Train public sector employees to recognize spear-phishing lures related to current events. Tailored simulations and real-time alerting during known geopolitical events can preempt successful attacks.

- **Proactive Threat Hunting and Coordination with CERT-In**: Regularly scan networks for IOCs such as Contabo IPs or known Crimson RAT mutexes. Maintain an open coordination channel with CERT-In and sectoral ISACs to stay informed about emerging threats and share timely observations.

- **Banking/Finance (BFSI):**
  - **Robust Email Security and Fraud Detection:** Since banks are frequent phishing targets (e.g., fake RBI portal case), deploy advanced email filters with sandboxing to catch malicious attachments/links. Train employees continually on phishing red flags. Implement DMARC/SPF on email domains to prevent spoofing of bank and regulator domains. Also, given the risk of fraud and lateral movement, use anomaly detection on financial transactions – sometimes attackers might try SWIFT fraud or fund transfers if they get deep access, so AI-based monitoring can spot unusual transaction patterns and stop them.
  - **Customer-Facing Security:** Ensure customer portals and banking apps are secured against spoofing and malware. Promote customer awareness about not installing unofficial apps (to mitigate things like fake IndiaPost or RBI apps). The RBI's directive for .bank.in domains is a good step; banks should comply to make phishing harder. Back-end, implement transaction signing or 2FA for high-value transactions so that even if internal systems are breached, attackers can't easily move money without additional codes/devices.
  - **Segment Critical Networks:** Separate the core banking systems (CBS), payment switch, and ATM networks from the general corporate network. The access between them should be strictly controlled and monitored. Thus, even if an employee PC is compromised, the attacker can't directly jump to the SWIFT terminal or card management system. Use jump servers with MFA for any admin access to core systems.
  - **Regular DR Drills:** Banks must maintain disaster recovery (DR) sites and offline backups of critical data (account ledgers, transaction logs) with encryption. Practice failover to DR in case ransomware hits production, to minimize downtime. For example, have an isolated backup of daily transactions that ransomware can't reach because it's offline or immutable.

- **Healthcare:**
  - **Network Segmentation and Access Control:** Hospitals should segregate networks: medical devices and networks (for MRI, ICU monitoring, etc.) separate from administrative networks, which separate from research networks. In NHI's case, the research network compromise led to hospital IT impact; segmentation could limit cross-over. Sensitive diagnostic equipment running older OS should be on isolated VLANs with strictly controlled access.
  - **Backup and Recovery Plan:** As seen with ransomware at hospitals, maintaining regular offline backups of patient records and critical research data is lifesaving (literally). Hospitals should ensure that backups are not continuously connected (to avoid being encrypted too). Develop manual contingency workflows for critical functions (admit/discharge, prescriptions) and test them so that patient care can continue during IT outages. AIIMS in 2023 and NHI 2024 taught painful lessons here.
  - **Endpoint Protection on Medical and Research Systems:** Many hospitals have legacy systems that can't easily be patched. Deploy virtual patching or host intrusion prevention on those (which monitors and blocks exploit attempts). Use application

whitelisting on lab computers – e.g., only allow the few necessary software to run, blocking any unknown executables (which would stop ransomware from executing on a radiology PC). Also, monitor network traffic from medical IoT devices for anomalies – if an X-Ray machine starts making calls to the internet, that's a red flag.

- **HIPAA-like Data Security:** While India may not have an exact HIPAA, hospitals should enforce strict access controls to patient data. Even internal, staff should only access data on need-to-know. This way, if an adversary compromises a lower privileged account, they can't query entire patient DB easily. Also, encrypt sensitive databases at rest, so that if exfiltrated, they're not immediately usable.

- **Energy (Power/Oil/Gas):**
  - **ICS/SCADA Security:** The OT (Operational Technology) systems controlling generation, transmission, and distribution must be ring-fenced. Follow IEC 62443 or similar ICS security frameworks. Ensure that control systems are on a separate network with one-way data flows out (for monitoring) and minimal gateways in. Use data diodes where possible (so that data can flow out for monitoring but no control commands can flow in from IT network). Regularly update and patch interface devices like RTUs, PLCs and use firmware with secure boot where available.
  - **Monitoring of Industrial Networks:** Deploy specialized ICS network monitoring that understands protocols like IEC 104, Modbus, DNP3, etc., to detect abnormal commands or traffic. For instance, if an attacker tries to flip circuit breaker states at odd hours, the monitoring system can raise alarms. Additionally, employ intrusion detection on the IT/OT boundary – e.g., if someone tries to introduce a new file into a SCADA server from the IT side, catch that.
  - **Routine Security Drills at Plants:** Conduct drills where, say, the assumption is malware has entered the plant control network. Validate that operators can still safely operate the grid manually if needed, and that incident response teams can expunge the threat without causing downtime. Some Indian power plants started this after 2021 incidents; it should be widespread.
  - **Supply Chain and Third-Party Risk:** Energy sectors often rely on third-party contractors and OEMs (for turbine software, etc.). Adversaries might target those (APT10 famously did via targeting IT service providers). So energy companies should enforce strict cybersecurity requirements on vendors and have network zones for third-party access that are tightly monitored. Also, inspect and verify software updates from vendors (digital signatures, testing in sandbox) before applying to ICS.

Across all sectors, implementing a strong **culture of cybersecurity** is key. Human vigilance can thwart many initial access attempts (the one click that wasn't made, the USB that wasn't plugged in due to training). Thus, continuous security awareness programs, phishing simulations, and role-based training (e.g., special training for SCADA engineers vs. accountants) will bolster the human firewall.

Finally, every sector should maintain close liaison with national cyber authorities. In critical incidents, time is of the essence, and being able to quickly involve CERT-In/NCIIPC (which can bring broader intel and support) can make a huge difference in containment and attribution.

Conclusion

The period 2024–2025 has underscored that cybersecurity is now inseparable from national security for India. In the wake of Operation Sindoor and other geopolitical flashpoints, Pakistani APT groups have stepped up their cyber offensives, targeting India's government and critical industries with greater determination and sophistication. What were once sporadic nuisance hacks have evolved into continuous espionage campaigns and even destructive attacks that blur the line between cybercrime and state-sponsored sabotage.

India's threat landscape is thus increasingly defined by advanced persistent threats that are well-resourced, patient, and aligned with hostile state interests. The cases we analysed—from APT-36's Pahalgam-themed phishing that impersonated J-&-K Police to steal officials' credentials, through SideCopy's WinRAR zero-day attack that planted Windows- and Linux-based implants, Transparent Tribe's year-long academic-espionage wave against educational institutes, the dual-RAT breach of a DRDO contractor, and the election-results lure that dropped Crimson RAT on civil servants and journalists—vividly illustrate the stakes: intellectual property, financial systems, citizens' data, and essential services can all be disrupted or stolen by determined adversaries.

Yet, these challenges can be met with resilience. India's cyber defenders – from CERT-In analysts to corporate SOC teams – are adapting to this new normal. The successful containment of several incidents (before catastrophic damage occurred) shows that increased vigilance and cooperation are paying off. Going forward, India must double down on building indigenous cyber capability: this means developing local cybersecurity solutions (reducing reliance on foreign tech), nurturing skilled cyber professionals, and possibly even offensive capabilities to deter adversaries. Just as importantly, fostering a culture of cyber hygiene and preparedness across public and private sectors is crucial; every employee and citizen has a role in strengthening the security chain.

In conclusion, the evolving threat landscape is daunting, but with strategic foresight, robust defenses, and collaborative action, India can mitigate these risks. The call to action is clear – invest in cyber resilience now, so that even as enemies probe our networks, they are thwarted at every turn. Sectoral preparedness – from banks fortifying against phishing to power grids isolating control systems – will determine how well India weathers the cyber storms of the future. By implementing the recommendations outlined and staying agile in the face of new tactics, Indian organizations can stay one.

References:

1. The Hindu. *"Operation Sindoor: How India destroyed nine terrorist camps in PoK, retaliation for Pahalgam attack."* (National News, May 2025).

2. Moneycontrol News. *"Govt ramps up cyber vigilance on critical infrastructure after Operation Sindoor."* May 7, 2025.

3. Sathwik R. Prakki – Seqrite Labs. *"Pakistani APTs Escalate Attacks on Indian Gov. – Seqrite Unveils Threats and Connections."* Seqrite Blog, April 24, 2024.

4. Sathwik R. Prakki – Seqrite Labs. *"SideCopy's Multi-platform Onslaught: Leveraging WinRAR Zero-Day and Linux Variant of Ares RAT."* Seqrite Blog, November 6, 2023.

5. Cyble Inc. *"Threat Actor Profile: SideCopy."* Cyble Research Hub, February 20, 2025.

6. Ravie Lakshmanan. *"Pakistan-Linked Hackers Expand Targets in India with CurlBack RAT and Spark RAT."* The Hacker News, April 14, 2025.

7. Cybersecurity Help. *"Pakistan-linked threat actor expands targeting in India with new CurlBack RAT."* April 14, 2025.

8. Nate Nelson. *"Pakistani Hacking Team 'Celestial Force' Spies on Indian Gov't, Defense Orgs."* Dark Reading, June 13, 2024 (covering Cisco Talos report).

9. Jai Vijayan. *"APT36 Refines Tools in Attacks on Indian Targets."* Dark Reading, November 4, 2024 (covering Check Point Research on ElizaRAT).

10. Jonathan Greig. *"APT group targeting military in India, Pakistan through malicious Android messaging apps."* The Record (Recorded Future), March 13, 2023 (ESET research on CapraRAT).

11. Ravie Lakshmanan. *"APT36 Spoofs India Post Website to Infect Windows and Android Users with Malware."* The Hacker News, March 27, 2025 (citing CYFIRMA).

12. Hindustan Times. *"Pak hackers claim to have breached multiple Indian defence sites."* Hindustan Times, May 2025.

13. Check Point Research. *"Cloudy with a Chance of RATs: Unveiling APT36 and the Evolution of ElizaRAT."* Check Point Research Blog, 2024.

14. Indian Computer Emergency Response Team (CERT-In). *"India Ransomware Report – Year 2024."* Cyber Swachhta Kendra, 2025.

15. Recorded Future's Insikt Group. *"Chinese State-Sponsored Group RedEcho Targets Indian Power Sector."* (Contextual reference for energy sector attacks)

16. Dhanush. "Threat actors target recent Election Results." Lab Blog, July 23, 2024.

17. Prakki, Sathwik Ram. "Pakistani APTs Escalate Attacks on Indian Government: Seqrite Labs Unveils Threats and Connections." *Seqrite Blog,* 24 April 2024.

18. Prakki, Sathwik Ram. "Umbrella of Pakistani Threats: Converging Tactics of Cyber-Operations Targeting India." *Seqrite Blog,* 25 July 2024.

19. Prakki, Sathwik Ram. "Transparent Tribe APT Actively Lures Indian Army Amidst Increased Targeting of Educational Institutions." *Seqrite Blog,* 2 May 2023.

20. Quick Heal APT Team. "Transparent Tribe APT Actively Lures Indian Army Amidst Increased Targeting of Educational Institutions." Seqrite White Paper, 2023.

21. Cyble Research & Intelligence Labs. “SideCopy: Threat Actor Profile.” *Cyble Threat-Actor Profiles,* March 2025.

22. Cyble Research & Intelligence Labs. “Transparent Tribe: Threat Actor Profile.” *Cyble Threat-Actor Profiles,* March 2025.

23. Prakki, Sathwik Ram. “SideCopy’s Multi-Platform Onslaught: Leveraging WinRAR Zero-Day and Linux Variant of Ares RAT.” *Seqrite Blog,* 6 November 2023.

24. Dhanush. “Threat actors target recent Election Results.” K7 Security Labs, 23 July 2024.

Annexure 1

Phishing Document Hashes (MD5)

Hash
c4fb60217e3d43eac92074c45228506a
172fff2634545cf59d59c179d139e0aa
7b08580a4f6995f645a5bf8addbefa68
1b71434e049fb8765d528ecabd722072
c4f591cad9d158e2fbb0ed6425ce3804
5f03629508f46e822cf08d7864f585d3
f5cd5f616a482645bbf8f4c51ee38958
fa2c39adbb0ca7aeab5bc5cd1ffb2f08
00cd306f7cdcfe187c561dd42ab40f33
ca27970308b2fdeaa3a8e8e53c86cd3e

Phishing Domains

Domain
jkpolice.gov.in.kashmirattack.exposed
iaf.nic.in.ministryofdefenceindia.org
email.gov.in.ministryofdefenceindia.org
email.gov.in.departmentofdefenceindia.link
email.gov.in.departmentofdefence.de
email.gov.in.briefcases.email
email.gov.in.modindia.link
email.gov.in.defenceindia.ltd
email.gov.in.indiadefencedepartment.link
email.gov.in.departmentofspace.info
email.gov.in.indiangov.download
indianarmy.nic.in.departmentofdefence.de
indianarmy.nic.in.ministryofdefenceindia.org
email.gov.in.indiandefence.work
email.gov.in.drdosurvey.info

Phishing URLs

URL
hxxps://iaf.nic.in.ministryofdefenceindia.org/publications/default.htm
hxxps://jkpolice.gov.in.kashmiraxxack.exposed/service/home
hxxps://email.gov.in.ministryofdefenceindia.org/service/home/
hxxps://email.gov.in.departmentofdefenceindia.link/service/home/
hxxps://email.gov.in.departmentofdefence.de/service/home/
hxxps://email.gov.in.indiangov.download/service/home/
hxxps://indianarmy.nic.in.departmentofdefence.de/publications/publications-site-main/index.html
hxxps://indianarmy.nic.in.ministryofdefenceindia.org/publications/publications-site-main/index.htm
hxxps://email.gov.in.briefcases.email/service/home/
hxxps://email.gov.in.modindia.link/service/home/
hxxps://email.gov.in.defenceindia.ltd/service/home/
hxxps://email.gov.in.indiadefencedepartment.link/service/home/
hxxps://email.gov.in.departmentofspace.info/service/home/
hxxps://email.gov.in.indiandefence.work/service/home/

PPAM / XLAM Dropper Hashes

Hash
d946e3e94fec670f9e47aca186ecaabe
e18c4172329c32d8394ba0658d5212c2

2fde001f4c17c8613480091fa48b55a0
c1f4c9f969f955dec2465317b526b600

Crimson RAT Sample Hashes

Hash
026e8e7acb2f2a156f8afff64fd54066
fb64c22d37c502bde55b19688d40c803
70b8040730c62e4a52a904251fa74029
3efec6ffcbfe79f71f5410eb46f1c19e
b03211f6feccd3a62273368b52f6079d

Crimson RAT C2 IPs and Ports

C2 IP	**Ports**
93.127.133.58	1097, 17241, 19821, 21817, 23221, 27425
104.129.27.14	8108, 16197, 19867, 28784, 30123

MITRE ATT&CK Technique Mapping

Tactic	**Technique ID**	**Technique Name**
Reconnaissance	T1598.003	Phishing for Information: Spearphishing Link
Resource Development	T1583.001	Acquire Infrastructure: Domains
Initial Access	T1566.001	Phishing: Spearphishing Attachment
	T1566.002	Phishing: Spearphishing Link
Execution	T1204.001	User Execution: Malicious Link
	T1059.005	Command and Scripting Interpreter: Visual Basic
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
Discovery	T1033	System Owner/User Discovery
	T1057	Process Discovery
	T1082	System Information Discovery
	T1083	File and Directory Discovery
Collection	T1005	Data from Local System
	T1113	Screen Capture
Exfiltration	T1041	Exfiltration Over C2 Channel

Annexure 2

Malicious PowerPoint Add-in (PPAM)

MD5 Hash	Filename
41dab718879388d28d072fb967e51347	Officers posting policy revisseed final.ppam

Maldoc

Hash	Filename
d6cf93b031f2e3b8758c41f5ce665a1f	Industrial Engineering.docm
8d8311afb8c12bb319cd692460b1632	M1-Financial-Accounting.docm

Archive Files

Hash	Filename
06f93224254a3b0659aa8cf7cac718f	injavtemnr.zip
c7026aa76880ff7e889deafe62b416b1	jedvmtrvh.zip
98d06aa93edfbad4ecbddc69dee1150c	jivmtirvh.zip

Crimson RAT Payloads

Hash	Filename
b229f761519ad3d86e7ec8cd9737fde4	injavtemnr.exe
92fc496ae7ee3743de8a8bba2e82957	injavtemnr.exe
827a3da12d836843d62d1b5c0c565cac	jedvmtrvh.exe
74f805b6755709940e952b40c8ce37c	jedvmtrvh.exe
ff2f1edb6acabf1cf3d4896d49b94231	jivmtirvh.exe
e55e497ceadd037254e847187b6996da	jivmtirvh.exe

Command List

Command	Functionality
procl / getavs	Get a list of all processes
endpo	Kill process based on PID
scrsz	Set screen size to capture
cscreen	Get screenshot
dirs	Get all disk drives
stops	Stop screen capture
filesz	Get file information (Name, Creation Time, Size)
dowf	Download the file from C2
cnls	Stop uploading, downloading and screen capture
scren	Get screenshots continuously
thumb	Get a thumbnail of the image as GIF with size ‘of 200x150.’
putstrt	Set persistence via Run registry key
udlt	Download & execute file from C2 with ‘vdhairtn’ name
delt	Delete file
file	Exfiltrate the file to C2
info	Get machine info (Computer name, username, IP, OS name, etc.)
runf	Execute command
afile	Exfiltrate file to C2 with additional information
listf	Search files based on extension

dowr	Download file from C2 (No execution)
fles	Get the list of files in a directory
fldr	Get the list of folders in a directory

Command & Control (C2)

IP Address	Port
104.168.48.210	7516, 12267, 18197, 25821, 26442
151.106.19.20	12197, 16867, 24784, 8248, 23123
172.245.80.12	8149, 14198, 18818, 26781, 24224

MITRE ATT&CK Technique Mapping

Tactic	Technique ID	Technique Name
Initial Access	T1566.001	Phishing: Spearphishing Attachment
Execution	T1204.002	User Execution: Malicious File
Execution	T1059.005	Command and Scripting Interpreter: Visual Basic
Persistence	T1547.001	Registry Run Keys/Startup Folder (virbvorlewer)
Defense Evasion	T1027	Obfuscated Files or Information (embedded ZIP)
Discovery	T1033	System Owner/User Discovery
Discovery	T1057	Process Discovery
Discovery	T1082	System Information Discovery
Collection	T1005	Data from Local System
Collection	T1113	Screen Capture
Exfiltration	T1041	Exfiltration Over C2 Channel
Command and Control	T1071.001	Application Layer Protocol: Web Protocols (HTTP/S over non-standard ports)

Annexure 3

Maldocs

Hash	Filename
9f4186242fd9479571daf9ea59a81342	Assignment-17.docm
faaf969e0f8f1fe6d6bec3d5f4c4fe7f	new assignment 5th.docm
d15861dd1d96f9e2872dfbde4185f3b2	Assignment-13.docm
e773ea1bc24566812ca2c054e96c2314	Assignment-1.docm
f8f0a1baea7ee4662e4935700b318bb	Assignment-no-10.docm
8653a69131f07f61225891a7d5ec8ace	assignmentQ&A.docm
c9e84fae8578d34ab6b65d5c44e54fb2	Technology-Survey.docm
1886cd9da3e41acb9ec4373c0d9963e4	Assignment-19.docm
abc96ec4610c799d9289159d1146e49c	assignment.docx
db05d76ff9a9d3f582bd4278221f244a	assignment_2.docx
9649531d94b75cb1bf46ca47c64abef13	Note Doc (1).docm
40ebd1557ea9f8f855c10af807ea6188	Doc2.docm

Archive Files

Hash	Filename
a79e25b06dc45cb14891660f5abfeb83	Assignment-14.zip
9bec3c149c728c3142dc24d7c0988b0	Assignment-19.zip
a76c13b9a451093ca33fd540573f8bc2	Assignment (2).zip
a52f34631a80e350fealb8944524d78a	assignment23.zip
8326d270c53e753b712a7e910b41587	Assignment-1-3.zip
63d75f84e1fc35deb7953b5a6aba7e8e	Assignment-no-10 (1).zip.zip
51f763d1865085bd449329f8eab9acc	NevyteuYT.zip
5f90e6f425a6a90b14283c33f7d86eee	GstCil.zip
caedf21246e5920e1015959f9c9029f	GstCil.zip
138b6dbf4f3cf4f39631b511e15f148	Doc2.zip
04b83ed7737a7b82a81db79be03cee68d	Toronto.zip
5a9b43975e7b4baf9e6e8b30adabd991	Kosovo.zip
d2983dc0547de75b21bae89b52c36310	Witchher.zip

Crimson RAT Payloads

Hash	Filename
cce8de2debbf63e45e65dcbcb8c6f6712	MahTueyiy7.exe
88e57f9e085860e891245b4c15cbc772	NevyteuYT8.exe
8431f8c7ce0ce6bdf64434cae5111e320	GstCil.exe
3201a30a5320dc1820828bc911e	GstCil.exe
fdb2a78af0042d9d04476dd4476d3a8a0b	NevyteuYT.exe
be4d70a6fa8d9cb1acd5173931f7a73d	Kosovo.exe
e40e40ef034bb1ef651ae1e808f0dbd8	Kosovo.exe
85e9bd040322b52c1af057220762a786	Toronto.exe

b60da0d0ee64f0eb810710984f689d0	Witchher.exe

MITRE ATT&CK Technique Mapping

Tactic	**Technique ID**	**Technique Name**
Initial Access	T1566.001	Phishing: Spearphishing Attachment
Execution	T1204.002	User Execution: Malicious File
Execution	T1059.001	PowerShell
Persistence	T1547.001	Registry Run Keys/Startup Folder
Defense Evasion	T1036	Masquerading (assignment-themed documents)
Discovery	T1083	File and Directory Discovery
Discovery	T1082	System Information Discovery
Credential Access	T1552.001	Unsecured Credentials: Credentials in Files (SharePoint/O365 tokens)
Collection	T1113	Screen Capture
Collection	T1005	Data from Local System
Exfiltration	T1041	Exfiltration Over C2 Channel
Command and Control	T1071.001	Application Layer Protocol: Web Protocols

Annexure 4

Archive File

Hash	Filename
0725318b4f5c312eaf5ec9795a7e919	Missile-Clean-room.zip

LNK File

Hash	Filename
ab11b91f97d7672da1c5b42c9ecc6d2e	Missile Clean room.pptx.lnk

HTA Files

Hash	Filename
cbaa7fc86e4f1a30a155f60323fdba72	pantomime.hta
036da574b5967c71951f4e14d000398c	jquery.hta

DLL Files

Hash	Filename
5B9EAECCB041CB9C49CE78491CC5E965	hta.dll
CBG622956D074F7F5E0A1CAB37C9FF33	preBotHta.dll
2e19b7a2bbdc8082024d259e27e86911	DUser.dll

BAT File

Hash	Filename
05f9ac07249121d89cd4416ef466671c	test.bat

Domains

Domain
cornerstonebeverly[.]org

IP Addresses

IP Address	Description
160.153.131[.]201:443	Hosted HTA Files
144.91.72[.]17:8080	C2

URLs

URL
hxxps://www.cornerstonebeverly[.]org/js/files/docufentososo/doecomentosoonesso/pantomime.hta
hxxps://www.cornerstonebeverly[.]org/js/files/Missile-Clean-room
hxxps://cornerstonebeverly[.]org/js/files/ntfonts/avena/
hxxps://cornerstonebeverly[.]org/js/files/ntfonts/winsteros.txt

PDB Paths

PDB Path
E:\Packers\CyberLink\Latest Source\Multithread Protocol Architecture\HTTP Arsanel\Client\app\Release\app.pdb
E:\Packers\CyberLink\Latest Source\Multithread Protocol Architecture\HTTP Arsanel\Arsanel preBot\preBot\preBotHta\obj\Release\preBotHta.pdb

Legitimate Executable Used for Side-Loading

SHA-256 Hash	Filename
9B726550E4C82BBEB045150E75FEE720	cridviz.exe

MITRE ATT&CK Technique Mapping

Tactic	Technique ID	Technique Name
Initial Access	T1566.001	Phishing: Spearphishing Attachment (ZIP with LNK)
Execution	T1204.002	User Execution: Malicious File
Execution	T1218.005	Mshta (LOLBin)
Execution	T1059.005	Command and Scripting Interpreter: VBScript inside HTA
Persistence	T1547.001	Registry Run Keys/Startup Folder (via test.bat)
Defense Evasion	T1574.002	DLL Side-Loading (DUser.dll, hta.dll)
Defense Evasion	T1027	Obfuscated Files or Information
Credential Access	T1555.003	Credentials from Web Browsers (post-compromise targeting)
Discovery	T1082	System Information Discovery
Collection	T1005	Data from Local System
Exfiltration	T1041	Exfiltration Over C2 Channel (e.g., Dropbox, hardcoded tokens)
Command and Control	T1071.001	Application Layer Protocol: Web Protocols
Command and Control	T1090.002	Proxy: External Proxy Infrastructure

Annexure 5

Lure Documents

Hash	Filename / Description	Detection Name
4473b78e67067a9299227cc02b8e28e2	Election Lure .docm	Trojan (0001140e1)
ad90e16ea4a9fe11525da7669cb4b8ee	Syllabus Lure .xls/.xlsx	Trojan (0001140e1)

Crimson RAT Payloads

Hash	Description	Detection Name
e6f4bb8ed235f43cb738447fbf1757c3	Crimson RAT Sample 1	Trojan (005b635b1)
da2331ac3e073164d54bcc5323cf0250	Crimson RAT Sample 2	Trojan (005b67de1)
a54c435bdbc17608fa0b8826bbe9936d	Crimson RAT Sample 3	Trojan (005b67de1)
7a18b1bf9b07726327ba50e549764731	Crimson RAT Sample 4	Trojan (005b635b1)
d6b38a2272876d039d48b46aa874e7b9	Crimson RAT Sample 5	Trojan (005b67de1)
f49375748b279565b5aed83d9ee01eb2	Crimson RAT Sample 6	Trojan (005b635b1)

Command & Control (C2)

Type	Value
Domain	waqers[.]duckdns[.]com
IP Address	94.72.105.227

Decoy Documents (Embedded)

Hash	Description
24fc6cacfbf0f87d2a24be7361c78c76	Election Results PDF (Uttarakhand)
4166a122e5eac964ba9f4b22e2881052	University Syllabus (Decoy Excel)

MITRE ATT&CK Technique Mapping

Tactic	Technique ID	Technique Name
Reconnaissance	T1598.003	Phishing for Information: Spearphishing Link
Initial Access	T1566.001	Phishing: Spearphishing Attachment
Execution	T1204.002	User Execution: Malicious File
	T1059.005	Command and Scripting Interpreter: Visual Basic (macros in .docm)
Persistence	T1547.001	Boot or Logon Autostart Execution:

		Registry Run Keys (puy5tsrt)
Defense Evasion	T1027	Obfuscated Files or Information (base64 encoded OLE objects)
	T1497.003	Virtualization/Sandbox Evasion: Time Based Evasion (25 min sleep)
Discovery	T1082	System Information Discovery (iny5fo)
	T1083	File and Directory Discovery (fly5es, fly5dr)
	T1033	System Owner/User Discovery
	T1057	Process Discovery (gey5tavs, pry5ocl)
Collection	T1113	Screen Capture (scy5uren, scy5ren, thy5umb)
	T1005	Data from Local System
Exfiltration	T1041	Exfiltration Over C2 Channel
Command & Control	T1071.001	Application Layer Protocol: Web Protocols (via duckdns.com and 94.72.105.227)

Annexure 6

Windows

Archives

Hash	Filename
eb07a0063132e33c66d0984266afb8ae	DocScanner-Oct.zip
8bee417262cf81bc45646da357541036	Homosexuality – Indian Armed Forces.zip
9e9f93304c8d77c9473de475545bbc23	Achievements_of_DMA.rar
9379ebf1a732bfb1f4f8915dbb82ca56	Agenda_Points_Ammended.rar
49b29596c81892f8fff321ff8d64105a	DMA_Monthly_Update_Minutes_of_Meeting-reg.zip

Shortcut (LNK)

Hash	Filename
75f9d86638c8634620f02370c28b8ebd	DocScanner-Oct.pdf.lnk
fc5eae3562c9dbf215384ddaf0ce3b03	Homosexuality – Indian Armed Forces.pdf.lnk
a52d2a0edccdc0f533c7b04e88fe8092	agenda_points.docx.lnk
	draft_short_PPT.pptx.lnk
	meeting_brief.pdf.lnk

HTA

Hash	Filename
02c444c5c1ad25e6823457705e8820bc	msfnt.hta
d6e214fd81e7afb57ea77b79f8ff1d45	p.hta
d0c80705be2bc778c7030aae1087f96e	main.hta

DLL

Hash	Filename
31340EA400E6611486D5E57F0FAB5AF2	SummitOfBion.dll
FE0250AF25C625E24608D8594B716ECB	preBotHta.dll
C872F21B06C4613954FFC0676C1092E3	WinGfx.dll

RAT Payloads

Hash	Filename / Description
ff13b07eaabf984900e88657f5d193e6	Msfront.exe (DRat)
6f37dacf81af574f1c8a310c592df63f	Achievements_of_DMA.pdf.exe (AllaKore RAT)
9f5354dcf6e6b5acd4213d9ff77ce07c	steistem.exe / Onlyme.exe (Key RAT)

Decoy Documents

Hash	Filename

CCB6723C14EBB0A12395668377CF3F7A	DocScanner-Oct.pdf
acec2107d4839fbb04defbe376ac4973	Achievements_of_DMA.pdf_
f759b6581367db35e3978125f4f6ff80	ACR.pdf

Other

Hash	Filename
B6FBCAE7980D4E02CE9ED9876717F385	cache.bat
4f541ec8cd238737e4e77a55fbcbb4f3	d.txt

PDB Paths

Path
d:\Projects\C#\D-Rat\DRat Client\Tenure\obj\Release\MSEclipse.pdb
C:\Users\Boss\Desktop\test\Client\Client\obj\Release\Onlyme.pdb

Linux

Archives

Hash	Filename
7cba23cfd9587211e7a214a88589cf25	DocScanner_AUG_2023.zip
04a65069054085cd81daabe4fc15ce76	Homosexuality – Indian Armed Forces.zip
c61b19cbedcb878aff45c067d503d556	meeting-details.zip
eccc72deb8ce41433ed13591b4557343	DMA_Monthly_Update_Minutes_of_Meeting-reg.zip

Stagers

Hash	Filename
9375e3c13c85990822d2f09a66b551d9	DocScanner_AUG_2023.pdf
42a696ef6f7acf0919fea9748029a966	Homosexuality – Indian Armed Forces . pdf
54473E0D8CAFD950AFE32DE1A2F3A508	DocScanner_Updated_letter . pdf
36933B05B7E3060955E6A1FDFD7D8EC1	draft_letter_nov_2023. docx
508F4BFAD9F2482992AC7926910BD551	updated_draft_PPT. pptx
921915ecfe17593476648ad20cd61ecd	Meeting_Notice-reg. pdf

Decoys

Hash	Filename
5e32703e3704b2b5c299c242713b1ec5	DocScanner_AUG_2023.pdf
f759b6581367db35e3978125f4f6ff80	ACR.pdf
af3ec4f8a072779eb0cac18eaafc256d	Meeting_Notice-reg.pdf
0799e17933b875e3a54f01416e7505d5	DocScanner_Updated_letter.pdf
b4854c420bc39c8c77a0fcd9395a8748	draft_letter_nov_2023.docx
4cd0ee8186dc4203aad0cba48a8e5778	updated_draft_PPT.pptx

Ares RAT Payloads

Hash	Filename
088b89698b122454666e542b1e1d92a4	bossupdate
b992b03b0942658a516439b56afbf41a	updates
ebbc1c4fc617cda7a0b341b12f45d2ad	updates

C2 Servers and Associated Payloads

IP Address	Port	Description
38.242.149[.]89	61101	AllaKore RAT

38.242.149[.]89	9828	DRat
38.242.220[.]166	9012	Ares RAT
161.97.151[.]220	7015	Ares RAT
207.180.192[.]77	6023	Key RAT

Domains and Resolved IPs

IP Address	Domain
162.241.85[.]104	sunfireglobal[.]in
(shared IP)	occoman[.]com
(shared IP)	elfinindia[.]com
(shared IP)	ssynergy[.]in
103.76.213[.]95	rockwellroyalhomes[.]com
103.76.213[.]95	isometricsindia[.]co.in

URLs

URL
hxxps://www.rockwellroyalhomes[.]com/js/FL/DocScanner-Oct.zip
hxxps://www.rockwellroyalhomes[.]com/js/content/msfnt.hta
hxxps://www.rockwellroyalhomes[.]com/js/content/2023-06-21-0056.pdf
hxxps://www.rockwellroyalhomes[.]com/js/content/
hxxps://www.rockwellroyalhomes[.]com/js/FL/2023-06-21-0056.pdf
hxxps://www.rockwellroyalhomes[.]com/crm/asset/css/files/file/
hxxps://www.rockwellroyalhomes[.]com/crm/asset/css/files/doc/
hxxps://www.rockwellroyalhomes[.]com/crm/asset/css/files/doc/DocScanner_AUG_2023.zip
hxxps://sunfireglobal[.]in/public/core/homo/
hxxps://sunfireglobal[.]in/public/assests/files/db/acr/
hxxps://sunfireglobal[.]in/public/assests/files/auth/av
hxxps://sunfireglobal[.]in/public/assests/files/auth/dl
hxxps://sunfireglobal[.]in/public/assests/files/auth/ht
hxxps://occoman[.]com/wp-admin/css/colors/ocean/files/files/tls
hxxps://occoman[.]com/wp-admin/css/colors/ocean/files/files/
hxxps://occoman[.]com/wp-admin/css/colors/ocean/files/pdf/in
hxxps://occoman[.]com/wp-admin/css/colors/ocean/files/files/bossupdate
hxxps://futureuniform[.]ca/wp/wp-content/files/01/main.hta
hxxps://futureuniform[.]ca/email.gov.in/briefcase/Meeting_Notice-reg.pdf
hxxps://futureuniform[.]ca/mail.gov.in/briefcase/updated_draft_PPT.pptx
hxxps://futureuniform[.]ca/mail.gov.in/briefcase/draft_letter_nov_2023.docx
hxxps://futureuniform[.]ca/mail.gov.in/briefcase/DocScanner_Updated_letter.pdf
hxxps://keziaschool[.]com/wp/wp-content/uploads/2023/files/bossupdate
hxxps://keziaschool[.]com/wp/wp-content/uploads/2023/38
hxxp://38.242.220[.]166:9012/api/root_149371139681480/upload
hxxp://38.242.220[.]166:9012/api/root_149371139681480/hello
hxxp://38.242.220[.]166:9012/api/root_168683512566649/upload
hxxp://38.242.220[.]166:9012/api/root_168683512566649/hello
hxxp://38.242.220[.]166:9012/api/root_175170531258512/upload
hxxp://38.242.220[.]166:9012/api/root_175170531258512/hello

hxxp://161.97.151[.]220:7015/api/root_36854582802642/upload
hxxp://161.97.151[.]220:7015/api/root_36854582802642/hello

Host Paths

File Path
C:\Users\Public\aque\up.hta
C:\Users\Public\aque\cdrzip.exe
C:\Users\Public\aque\rekeywiz.exe
C:\Users\Public\aque\DUser.dll
C:\Users\Public\aque\data.bat
C:\Users\Public\Msfront\Msfront.exe
C:\Users\Public\winowimg.jpg
C:\Users\Public\stremoe\steistem.exe
C:\Users\Public\stremoe\stremoe.bat
C:\ProgramData\Intel\cdrzip.exe
C:\ProgramData\Intel\DUser.dll
C:\ProgramData\WinGfx\credwiz.exe
C:\ProgramData\WinGfx\wingfx.bat
C:\ProgramData\WinGfx\DUser.dll
C:\ProgramData\HP\jquery.hta
C:\ProgramData\HP\jscy.hta
%AppData%\Msfront\Msfront.exe
%AppData%\Msfront\DUser.dll
%AppData%\Msfront\crezly.exe
%Temp%\cache.bat
%Temp%\Msfont\Msfont.exe

MITRE ATT&CK Technique Mapping

Resource Development

Technique ID	Name
T1583.001	Acquire Infrastructure: Domains (e.g., sunfireglobal.in, rockwellroyalhomes.com,
	reused compromised domains)
T1584.001	Compromise Infrastructure: Domains
T1588.001	Obtain Capabilities: Malware (AllaKore, Drat, Ares RAT, Key RAT)
T1588.002	Obtain Capabilities: Tool (e.g., Ares RAT from GitHub)
T1608.001	Stage Capabilities: Upload Malware (to public file paths on compromised domains)
T1608.005	Stage Capabilities: Link Target (e.g., .lnk files triggering HTA loaders)

Initial Access

Technique ID	Name
T1566.001	Phishing: Spear Phishing Attachment (.zip files with .lnk, .hta, .pdf)
T1566.002	Phishing: Spear Phishing Link (e.g., archive links delivered via malicious URLs)

Execution

Technique ID	Name
T1106	Native API (WinAPI calls within payloads like mshta.exe)
T1129	Shared Modules (DLL side-loading)
T1059	Command and Scripting Interpreter (PowerShell, batch, Python from Ares RAT)
T1047	Windows Management Instrumentation (for system queries)

T1203	Exploitation for Client Execution (WinRAR CVE-2023-38831)
T1204.001	User Execution: Malicious Link (URLs pointing to HTAs and .zip)
T1204.002	User Execution: Malicious File (e.g., .pdf.lnk, .zip archives)

Persistence

Technique ID	Name
T1053.003	Scheduled Task/Job: Cron (used by Linux payloads like Ares RAT)
T1547.001	Registry Run Keys / Startup Folder (used by Windows RATs for persistence)
T1547.013	Boot or Logon Autostart Execution: XDG Autostart Entries (Linux RATs)

Defense Evasion

Technique ID	Name
T1036.005	Masquerading: Match Legitimate Name or Location (e.g., Onlyme.exe, Msfront.exe)
T1140	Deobfuscate/Decode Files or Information (base64 decoding of embedded payloads)
T1218.005	System Binary Proxy Execution: Mshta
T1574.002	Hijack Execution Flow: DLL Side-Loading (credwiz.exe, rekeywiz.exe)
T1222.002	File and Directory Permissions Modification: Linux (used by Ares RAT)
T1027.009	Obfuscated Files or Information: Embedded Payloads
T1027.010	Obfuscated Files or Information: Command Obfuscation (used by Ares RAT and HTA logic)

Discovery

Technique ID	Name
T1012	Query Registry (to detect AV, .NET version)
T1033	System Owner/User Discovery
T1057	Process Discovery
T1082	System Information Discovery
T1083	File and Directory Discovery
T1016.001	System Network Configuration Discovery
T1518.001	Software Discovery: Security Software Discovery

Collection

Technique ID	Name
T1005	Data from Local System
T1056.001	Input Capture: Keylogging (AllaKore, DRat)
T1074.001	Data Staged: Local Data Staging
T1119	Automated Collection
T1113	Screen Capture
T1125	Video Capture (possible from RAT functionality)

Command and Control

Technique ID	Name
T1105	Ingress Tool Transfer (download of staged payloads like .dll, .exe, .pyc)
T1571	Non-Standard Port (e.g., port 9012, 7015 for Ares RAT)
T1573	Encrypted Channel (HTTPS usage by Ares RAT)
T1071.001	Application Layer Protocol: Web Protocols (HTTPS C2, hello & upload endpoints)

Exfiltration

Technique ID	Name
T1041	Exfiltration Over C2 Channel (standard RAT behavior using encrypted channels)

Disclaimer

The material contained in this research paper is provided "as is" and for general information purposes only. Cybervahak has exercised reasonable care in preparing the content; however, we make no representations or warranties of any kind—express, implied, or statutory—regarding the accuracy, completeness, timeliness, suitability, or availability of the information, data, or recommendations herein. Any reliance you place on the paper's contents is strictly at your own risk.

System owners, security teams, and other readers must independently evaluate the relevance of the findings to their specific environments and decide, at their sole discretion, what defensive or corrective actions to take. Cybervahak shall not be liable for any direct, indirect, incidental, consequential, or special loss or damage arising out of, or in connection with, the application, non-application, or interpretation of this research—including but not limited to business interruption, data loss, or security incidents.

By using this document, you acknowledge that you bear full responsibility for maintaining, updating, and securing your own information-technology systems and that Cybervahak's analysis does not constitute legal, regulatory, or professional advice. Where legal or other expert assistance is required, the services of a competent professional should be sought.

Use of the paper signifies your acceptance of the terms of this disclaimer.