SV // CW-U #01

Ep. 01: Initial Access
Pakistan's Lies, Leaks, and Losses during Operation Sindoor

Cyber Warfare: Unattributed

RELEASED APRIL 2026 RUNTIME ~45 MIN TOPIC APT36 / OPERATION SINDOOR / INFORMATION WARFARE

// EPISODE SUMMARY

- One day before the Pahalgam terror attack, **APT36's Crimson RAT malware was compiled inside Pakistan**. The cyber operation was planned alongside the kinetic attack, not reactive to it.
  Seqrite Labs, May 2025
- **APT36 / Transparent Tribe** has been trying to hack India for over a decade. The track record remains mostly unsuccessful, because the skills and the initial access methods are not there.
- **Operation Sindoor (May 7, 2025)** triggered the most intensive India-Pakistan cyber conflict ever recorded. India repelled **1.5 million attack attempts**. Only 150 landed. A **0.01 percent success rate** for the adversary.
- Pakistan's hacktivist claims were overwhelmingly fabricated. The “70 percent power grid paralysis” was a complete hoax. The “government breaches” were recycled 2023 data repackaged as new.
- India nearly lost the narrative war. Army Chief General Upendra Dwivedi confirmed on record that **15 percent of operational effort during Sindoor** went into managing disinformation.
- Post-Sindoor, India has stood up a dedicated information warfare organisation and a **Psychological Defence Division (PDD)**, with battalion-level disinformation cells embedded across formations.

// THE PRE-COMPILATION: MALWARE WAS READY BEFORE THE BULLETS

On April 21, 2025, somewhere in Pakistan, someone compiled a piece of malware called **Crimson RAT**. A Remote Access Trojan. Software that, once it lands on a machine, hands the attacker full remote control. Files, keystrokes, camera, microphone. Everything.

Twenty-four hours later, twenty-six civilians were murdered in Pahalgam, Kashmir, in broad daylight. Within days, Indian defence personnel and serving officers in the Jammu and Kashmir region started receiving a phishing PDF titled “Pahalgam Terror Attack” with that same Crimson RAT embedded inside.

THE TIMESTAMP

- Forensic investigation by **Seqrite Labs**, a private Indian cybersecurity firm, pulled the compilation timestamp from the Portable Executable (PE) header. That is the metadata baked into every Windows executable file. Seqrite Labs, May 2025
- Timestamp: **April 21, 2025**. One day before the Pahalgam attack.
- This is clear evidence that Pakistani hacktivist groups are operating in conjunction with terror attack modules funded by the Pakistani leadership. The malware was compiled before the attack. The cyber operation was planned alongside the kinetic one.

// TIMELINE OF EVENTS

APR 21, 2025

Crimson RAT compiled in Pakistan. PE header timestamp recovered by Seqrite Labs.

APR 22, 2025

Pahalgam terror attack. 26 civilians murdered in Kashmir.

APR 22–24

Phishing wave begins. “Pahalgam Terror Attack.pdf” delivered to Indian defence personnel, police officers, and government staff.

MAY 7, 2025

Operation Sindoor launched. Indian precision strikes on terror infrastructure across the border.

MAY 7–10

Cyber retaliation surge. Pakistani hacktivist groups launch coordinated DDoS, defacements, and fake breach claims.

MAY 13, 2025

1.5 million attack attempts confirmed by Maharashtra Cyber. Only 150 landed.

APR 9, 2026

Gen. Dwivedi at Ran Samwad 2026 confirms 15% of operational effort during Sindoor went into countering disinformation.

// 01 — APT36: A DECADE OF FAILING TO HACK INDIA

Before looking at what happened during Operation Sindoor, it is worth understanding who Pakistan is actually fielding in cyberspace. The answer is both more sophisticated than most people credit, and yet far less capable than they claim to be.

THE BUDGET CONSTRAINT

- Pakistan's total annual cyber budget is estimated at approximately **USD 36 million**.
  `Stimson Center, 2025`
- That kind of budget does not buy a serious zero-day research program, a grey-market exploit budget, or an equivalent to commercial spyware.
- Most of the available budget goes into defence. Very little remains for offensive operations. So the default method becomes the cheapest one available: **phishing**.

APT36	Also known as **Transparent Tribe**. Pakistan's primary cyber espionage unit. Active since at least **2013**. Over a decade of targeting India with a mostly unsuccessful track record.
Primary Method	Phishing, and at times spearphishing. Spearphishing is the advanced version: not mass spamming of emails, but carefully crafted, customised payloads sent to specific Indian government officials, defence personnel, and diplomats. The emails look like the files you would receive at work. The attachments look legitimate. Open one, and the malware is planted.
Primary Weapon	**Crimson RAT.** A .NET-based Remote Access Trojan. Once planted, it grants the attacker full remote control. File exfiltration, keylogging, webcam access, command execution. The victim sees nothing.
Objective	This is not about money. APT36 targets defence and government personnel for **intelligence**. Classified documents, operational plans, internal communications. State-sponsored espionage.

SIDECOPY: THE SECOND PAKISTAN-LINKED GROUP

- **SideCopy** is a separate Pakistan-linked threat group, distinct from APT36 but operating in the same space.
- Deployed tools include **AllaKore RAT** and **Action RAT**. Same concept as Crimson RAT, different malware families. Targets have been employees at the Ministry of Defence and at times the Ministry of External Affairs. `Fortinet / QiAnXin, 2025`
- Post-Pahalgam, SideCopy's operational pattern shifted. A new RAT was introduced: **DeskRAT**, specifically designed to target **BOSS Linux**. `Sekoia.io, Nov 2025`
- BOSS stands for **Bharat Operating System Solutions**, the Indian government's endorsed Linux distribution, developed by C-DAC under the Ministry of Electronics and Information Technology (MeitY). It is deployed across government offices, defence installations, and sensitive infrastructure as the alternative to Windows on Indian government systems.
- **This is not opportunistic targeting.** Pakistan has been studying BOSS Linux, reverse engineering its structure, and hunting for vulnerabilities. It is one of the few examples of a Pakistan-linked group doing actual reverse engineering and vulnerability research, instead of going full script-kiddie mode.

GOPHER STRIKE AND SHEET ATTACK (2025 / 2026)

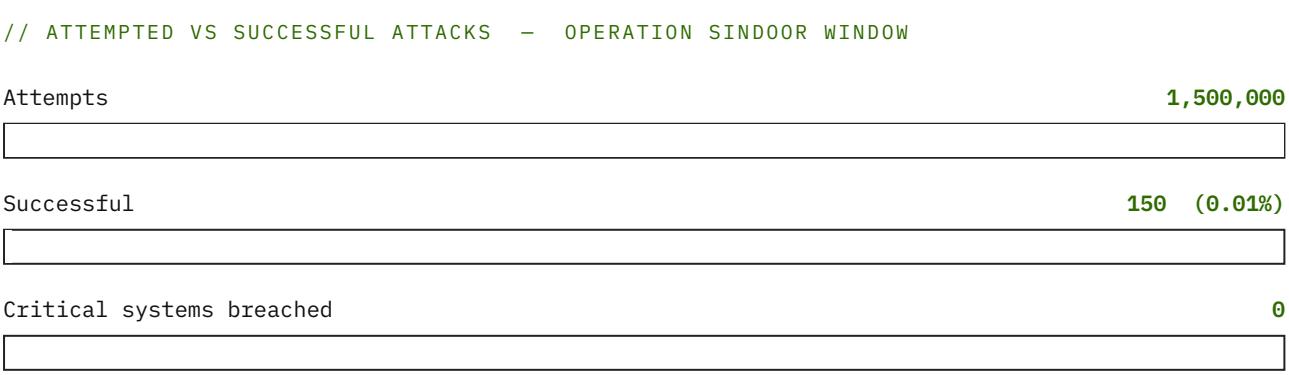
- Neither campaign is attributed directly to APT36 or SideCopy. Per **Zscaler ThreatLabz**, both are attributed to a subgroup of APT36 or a closely aligned actor. Zscaler ThreatLabz, Feb 2026
- **Sheet Attack:** Command-and-control infrastructure is set up on legitimate cloud services like **Google Sheets, Firebase, and Microsoft Graph API**. When a security tool sees traffic going to Google Sheets, it assumes someone in the organisation is working on a spreadsheet, not that data is being exfiltrated by a hacker.
- **Gopher Strike:** Much more classic. A blurred PDF lands in the inbox with a "Enable content to view" prompt. One click, payload executes on the system.
- Analysts have found **emojis inside the malware's error handling code**. That is unusual, and it is clear evidence of **AI-assisted malware development**. AI coding has lowered the barrier to entry for malware development. Pakistan has started using AI to write malware faster.
- This is worth watching. With a jailbroken AI, pretty much anyone can now get help writing malware. Fancier delivery, cloud-based C2, possibly AI-written code, and the entry point is still a phishing email. The methods are being updated. The initial access vector is not.

// 02 — OPERATION SINDOOR AND PAKISTAN'S CLAIM FACTORY

Between April 22 and May 10, 2025, Pakistani hacktivist groups launched a coordinated campaign against Indian infrastructure. Over **480 confirmed cyber incidents** in under three weeks. CybelAngel, Sep 2025

1.5M+	150	0.01%	<5 min
ATTACK ATTEMPTS ON INDIA	ACTUALLY SUCCESSFUL	ADVERSARY SUCCESS RATE	AVG DDOS DOWNTIME
PTI / Maharashtra Cyber	PTI, May 13 2025	Calculated	CloudSEK, May 2025

0
CRITICAL SYSTEMS BREACHED
CERT-In / MoP India



Source: PTI / Maharashtra Cyber / CloudSEK (May 2025)

WHAT IS A DDOS ATTACK?

- **DDoS** stands for **Distributed Denial of Service**. Picture a million people trying to walk through one doorway at the same time. Nobody gets through. That is DDoS. Flooding a server with enough fake traffic that real users cannot access it.
- It is the easiest, cheapest, lowest-skill cyber attack available. It does not steal data. It does not compromise systems. It just makes something temporarily unavailable.
- Most of the 1.5 million attack attempts on India during Sindoor were DDoS. Average downtime per incident: **under 5 minutes**. CloudSEK, May 2025

CLAIM DEBUNKED: PAKISTAN "TOOK DOWN" INDIA'S POWER GRID

PAKISTAN CLAIMED

- Pakistani cyber wing paralysed approximately **70 percent of India's power grid**.
- 4,600+ power feeders offline in Maharashtra, 3,600+ in Uttar Pradesh, 600+ in Jammu and Kashmir.
- AI-powered servers at Punjab load dispatch centre disabled.
- 235+ solar and wind stations in Karnataka knocked offline.

Telegram channels / Pakistan-aligned media, May 2025

REALITY

- India's Ministry of Power and **PGCIL (Power Grid Corporation of India Limited)**, the central transmission utility, confirmed **zero disruption** to grid operations at any point.

PGCIL / Ministry of Power

- Not a single OSINT channel or media house reported any blackouts across India during this period. Not a single India-based social media account mentioned any blackouts.
- Not a single anomaly was recorded by third-party monitors like NetBlocks, Cloudflare Radar, or ESET.
- BSE and NSE, India's two major stock exchanges, restricted overseas web access as a **proactive DDoS defence measure**. Without overseas internet access, there was no vector to perform DDoS attacks against them. Economic Times, May 7 2025

VERDICT

- **Complete fabrication.** A psyop designed for Pakistani domestic consumption, possibly for local politicians to score brownie points, and to muddy international perception of the conflict.

CLAIM DEBUNKED: “100+ SUCCESSFUL HACKS ON INDIAN GOVERNMENT”

PAKISTAN CLAIMED

- 100+ successful attacks on Indian government sites including PMO, President's Office, CERT-In, National Testing Agency (NTA), and Election Commission.
- 1 million citizen records exfiltrated from Andhra Pradesh High Court.
- Election Commission of India database compromised.

Various Pakistan-aligned hacktivist Telegram channels, May 2025

REALITY

- CloudSEK forensic analysis confirmed most DDoS attacks caused **under 5 minutes of disruption**. PMO and ministry sites stayed operational throughout. CloudSEK, May 2025
- The Andhra Pradesh High Court “leak” was **data originally breached in 2023**, repackaged with a fresh date and a sensational headline.
- The Election Commission “breach” was also **2023 data repackaged**. Claim surfaced by **Team Ezrael**, a group with a documented history of recycling old leaks. This was the second time Pakistan-based hacker groups used Team Ezrael's old dump during Operation Sindoor.
- CERT-In and NTA websites both confirmed operational with zero outage during the claimed attack windows.
- Of 1.5 million attempts, **150 landed. That is 0.01 percent.** PTI, May 13 2025

VERDICT

- India's cyber defences held completely. The information war was the actual operation. Manufacture the perception of damage regardless of whether damage occurred.

THE FABRICATION PLAYBOOK

- **Step 1:** Take data from a previous breach, often several years old.
- **Step 2:** Repackage with a new name and date. Slap a sensational, clickbaity title on it.
- **Step 3:** Post on Telegram with screenshots that look dramatic.
- **Step 4:** International media picks it up without any verification. “Hackers claim they did this, they did that.”
- **Step 5:** By the time anyone debunks it, the narrative has already spread.
- This is not cyber warfare. It has nothing to do with cyber warfare. This is **information warfare** using the aesthetic of cyber warfare. Going on the dark web or Telegram, downloading old data, organising it, putting it together, and changing the title to 2025. That is all they have been doing.

ATTRIBUTION FOG: THE FALSE-FLAG ROUTING

- Maharashtra Cyber confirmed attack traffic was routed through **Indonesian, Moroccan, and Bangladeshi IP addresses**. Stimson Center, Nov 2025
- This false-flag routing is nothing new. It is the same technique used by many hacktivist groups. Find proxy servers in other regions, mask traffic through them, avoid attribution.
- TTPs (Tactics, Techniques, and Procedures) are the behavioural fingerprint of a threat actor. Combined with malware signatures and the command-and-control infrastructure, they are what lead to attribution. Not IP addresses.
- **IP addresses are not attribution. TTPs are.**

// 03 — INDIA'S CYBER RESPONSE

// THE RECEIPTS EXIST

- As for what India's civilian cyber community actually did in response, the full picture is not being detailed here on the public record.
- If you want to see the receipts, check the highlights on Twitter. It is all documented in real time.
- **One side produced evidence. The other side produced propaganda.**
- The asymmetry tells you everything you need to know about the actual state of the play.

// 04 — THE INFORMATION WARFARE GAP

THE SPEED PROBLEM

- During Operation Sindoor, **official Indian handles were slow**. Pakistan's Telegram channels were pushing narratives within minutes of events. Real-time, high volume, very coordinated.
- By contrast, India's myth debunks and attribution of fake news were very slow. The institutional response lagged way behind.
- The gap was filled by **civilian OSINT accounts**. Veterans, civilians, independent analysts, Twitter anons. Across Twitter, Telegram, and defence forums. They tracked events in real time, debunked claims with forensic evidence, and provided analysis faster than any official channel could.
- This was the only reason India had a fighting chance in the information war. Civilians filled a critical gap that institutions are simply not yet ready to fill at that speed.

GEN. DWIVEDI AT RAN SAMWAD 2026 (APR 9, BENGALURU)

- Chief of Army Staff **General Upendra Dwivedi** at the Ran Samwad 2026 tri-service defence dialogue confirmed on record: **15 percent of operational effort during Operation Sindoor was dedicated to managing disinformation**. One in every seven units of effort was spent not on fighting or logistics, but on managing lies. Daily Pioneer / Organiser, Apr 2026
- Post-Sindoor, the Indian Army has created a **dedicated information warfare division**: the **Psychological Defence Division (PDD)**, currently operating at the corps and command levels. Republic World, Apr 2026
- **Battalion-level disinformation cells** have been embedded across formations. During Sindoor, the Army enforced a "single source of truth". All unofficial handles were shut down, with only the ADG (Strategic Communication) authorised to speak.

GEN. DWIVEDI AT IIT MADRAS (AUG 4, 2025)

- At the inauguration of the Indian Army Research Cell at IIT Madras, General Dwivedi made an observation about Pakistan's narrative management that deserves to be heard directly:
- *"Victory is in the mind. It's always in the mind. If you ask a Pakistani whether you lost or won, he'd say, my chief has become a Field Marshal, we must have won only."* Swarajya Mag / The Wire, Aug 2025
- Dwivedi also noted that India's first strategic message of Operation Sindoor, **"Justice Done"**, recorded strong global engagement. The capability still exists. Speed remains the main problem.

WHAT'S NEW VS WHAT ALREADY EXISTED

- The **Defence Information Warfare Agency (DIWA)**, under the Defence Intelligence Agency (DIA), has existed since approximately 2019 or 2020. Information warfare is not a new concept for the Indian military.
- What **is new** post-Sindoor is the PDD and an expanded structure designed as a **permanent institutional capability**. A structural upgrade, not a temporary response.
- Also new: embedded **battalion-level disinformation cells** operating at corps and command levels.

// 05 — STRATEGIC TAKEAWAYS

WHAT THE EVIDENCE COMPELS

- **Cyber and kinetic operations must now be planned together. Always.** Pakistan's Inter-Services Intelligence (ISI) and its cyber apparatus are coordinating at the planning stage. Cyber is integrated into the operation from the start, before the terror attacks. India must treat these as one unified domain, not separate compartmentalised silos.
- **A 0.01 percent adversary success rate is strong, but it is not a reason to stop investing in cyber.** India repelled the highest-intensity cyber attack in the country's history. The adversary will iterate. The next wave will study what worked, what did not, and will improve accordingly.
- **BOSS Linux being specifically on the adversary's radar is a serious signal.** They are no longer just sending random phishing emails. They are hunting for systemic vulnerabilities inside the operating system itself. India needs to watch for any serious vulnerability research program Pakistan invests into, whether through China or any other state. Dedicated security auditing and red-teaming of all military and nuclear installations is now required, coordinated centrally, emulating current and future adversaries. This is just Pakistan. China's capability is 100 times better.
- **The narrative warfare gap has been partially closed, but speed remains the main vulnerability.** Battalion-level disinformation cells may be the right institutional response right now, but institutions are almost always going to be slower than Telegram channels. The answer is countering narratives *before* the claims land in the public domain. India has to be proactive with narrative warfare.
- **Civilian OSINT is a strategic asset, not a curiosity.** Not just some anon sitting in a basement typing on Twitter. It is more than that. General Dwivedi acknowledged it publicly. India needs a framework for working with this asset instead of suppressing it. OSINT accounts have been bothered by law enforcement and other agencies. There has to be an understanding, at a granular level, between these agencies and how information warfare actually works. Plus a framework for how the military leverages civilian intelligence inputs without compromising operational security and while verifying them in real time. That framework does not exist yet, at least not publicly. It should.
- **The fabrication playbook is repeatable. It has been used before and it will be used again.** Pakistan will recycle old data, repackage it, amplify on Telegram, and hope nobody checks in real time. India needs a permanent rapid-response debunking capability. The media needs to understand how information warfare works and stop falling for fake claims, especially technical ones.

// 06 — THE SCORECARD

EPISODE RECAP

- **Pakistan's APT36** has been trying to hack India for over a decade. Still using phishing. Still getting caught. The Crimson RAT pre-compilation before Pahalgam is the most alarming detail. It is clear evidence of coordinated planning between cyber and kinetic operations.
- **Pakistan's hacktivists** launched 1.5 million attack attempts during Sindoor. 150 succeeded. A 0.01 percent success rate. Zero critical systems compromised. The “70 percent power grid paralysis” was a complete fabrication. The “government breaches” were recycled 2023 data.
- **India's cyber defences held.** Under the highest-intensity cyber attack the country has ever faced, the infrastructure stood.
- **India nearly lost the narrative war**, but civilians stepped in where institutions were too slow. The Army has since created a Psychological Defence Division and battalion-level disinformation cells. The institutional response is real.
- **One side produced evidence. The other produced propaganda.** That asymmetry is the story of this episode.

NEXT EP. *The series continues with a deeper look at the tools and the tradecraft. The malware families, the command-and-control infrastructure, the operational techniques both sides actually used, and how these groups run their operations once they are inside.* **End of transmission.**

// GLOSSARY: ACRONYMS AND FULL FORMS

APT	Advanced Persistent Threat. Industry classification for nation-state-backed hacker groups.
APT36 / Transparent Tribe	Pakistan-linked espionage group, active since 2013.
Crimson RAT	APT36's primary .NET-based Remote Access Trojan. Compiled April 21, 2025 per Seqrite Labs.
RAT	Remote Access Trojan. Malware that gives attackers remote control of an infected machine.
SideCopy	Pakistan-linked threat group. Deployed AllaKore RAT, Action RAT, and DeskRAT against Indian targets.
DeskRAT	Malware deployed by SideCopy specifically targeting BOSS Linux systems.
BOSS Linux	Bharat Operating System Solutions. India's government-endorsed Linux OS developed by C-DAC under MeitY.
C-DAC	Centre for Development of Advanced Computing. Indian government R&D organisation that develops BOSS Linux.
MeitY	Ministry of Electronics and Information Technology, Government of India.

CERT-In	Computer Emergency Response Team India. National cybersecurity incident response body.
NTA	National Testing Agency. India's government body that conducts entrance exams (JEE, NEET, etc.).
PGCIL	Power Grid Corporation of India Limited. India's central power transmission utility.
DDoS	Distributed Denial of Service. Attack that floods a server with traffic to make it temporarily unavailable.
C2 / C&C	Command and Control. Infrastructure attackers use to communicate with compromised systems.
TTP	Tactics, Techniques, and Procedures. The behavioural fingerprint of a threat actor, used for attribution.
PE Header	Portable Executable header. Metadata inside a Windows executable, includes compile timestamp.
Spearphishing	Targeted phishing. Emails crafted for specific individuals, not mass spam.
OSINT	Open Source Intelligence. Intelligence gathered from publicly available information.
Operation Sindoor	India's military strike against terror infrastructure, launched May 7, 2025.
PDD	Psychological Defence Division. New Indian Army unit created post-Sindoor for countering disinformation.
DIWA	Defence Information Warfare Agency. Existing agency under DIA handling information warfare.
DIA	Defence Intelligence Agency. India's tri-service military intelligence body, established 2002.
ADG (Strat Comm)	Additional Directorate General (Strategic Communication). Designated single source of truth during Sindoor.
BSE / NSE	Bombay Stock Exchange / National Stock Exchange. India's two major stock exchanges.
PIB	Press Information Bureau. Government of India's official communication wing.
Ran Samwad 2026	Annual tri-service defence dialogue, held April 9-10, 2026 in Bengaluru.
ISI	Inter-Services Intelligence. Pakistan's primary intelligence agency.

// SOURCES AND FURTHER READING

Seqrite Labs	PE header timestamp analysis on Crimson RAT. seqrite.com/blog

CloudSEK	Forensic debunking of Pakistani hacktivist claims during Sindoor. cloudsek.com/threatintelligence
Zscaler ThreatLabz	Gopher Strike and Sheet Attack campaign analysis. zscaler.com/blogs/security-research
PTI / Maharashtra Cyber	1.5M attack attempts figure. Official Indian government source, May 2025.
CybelAngel	480+ total cyber incidents during the India-Pakistan conflict window, Sep 2025.
Stimson Center	Pakistan cyber budget estimate and false-flag routing analysis. stimson.org
Fortinet / QiAnXin	SideCopy campaigns against India's Ministry of Defence, 2025.
Sekoia.io	DeskRAT targeting BOSS Linux, Nov 2025. blog.sekoia.io
Ministry of Power, India / PGCIL	Confirmation of zero grid disruption during Sindoor.
Economic Times	BSE/NSE proactive DDoS defence measures, May 7 2025. economictimes.indiatimes.com
Daily Pioneer / Organiser	Gen. Dwivedi at Ran Samwad 2026: 15% effort on disinformation, PDD creation, Apr 2026.
Republic World	Battalion-level disinformation cells, single-source-of-truth enforcement, Apr 2026. republicworld.com
Swarajya Magazine / The Wire	Gen. Dwivedi at IIT Madras: “Victory is in the mind” quote, Aug 2025.
CERT-In	Advisory CIAD-2025-0019 and related threat guidance. cert-in.org.in
MITRE ATT&CK	APT36 / Transparent Tribe technique documentation. attack.mitre.org/groups/G0134

// LISTEN AND FOLLOW

Spotify | Apple Podcasts | YouTube

HOSTED BY KRUTIK PRODUCED BY SPYVEIL