SV // CW-U #02

Ep. 02: Prepositioning
The Threat to Our Telecom Infrastructure

Cyber Warfare: Unattributed

TOPIC SALT TYPHOON / VOLT TYPHOON / INDIA TELECOM / RECENT BREACHES

// EPISODE SUMMARY

- In December 2024, the FBI told American citizens to stop using standard phone calls and SMS and switch to end-to-end encrypted applications like WhatsApp or Signal. The reason: **Salt Typhoon**, a Chinese state-linked APT group, had breached major US telecoms and was inside the infrastructure used for lawful wiretapping.
- **At least 200 companies across 80+ countries were compromised.** Salt Typhoon accessed the intercept list: the specific phone numbers under active US law enforcement surveillance. Call detail records, SMS metadata, and in some cases live audio of senior government officials were exfiltrated.
- **Volt Typhoon**, attributed to the Chinese military, is a separate group with a different mission: prepositioning dormant implants inside US power grids, water systems, ports, and pipelines. In a classified meeting in December 2024, Chinese officials reportedly acknowledged Volt Typhoon's activity to their US counterparts and framed it as a signal over Taiwan.
- **India is on the same target list.** Trend Micro confirmed Salt Typhoon activity inside Indian organizations. Recorded Future placed India among the top three geographic concentrations of targeted Cisco devices. Not a single Indian carrier has publicly acknowledged a compromise.
- CERT-In has issued zero advisories on Salt Typhoon or Volt Typhoon. The Five Eyes nations issued joint public advisories naming both groups and directed operators to patch. India: complete institutional silence.
- India's average breach detection and containment time is **263 days**, per IBM's Cost of a Data Breach India Report 2025.

// 01 — SALT TYPHOON: INSIDE THE WIRETAP INFRASTRUCTURE

Salt Typhoon breached major US broadband providers including **Verizon, AT&T, and Lumen Technologies**, compromising the systems built specifically for law enforcement wiretapping. The group was not interested in ordinary call records. They were inside the infrastructure that governments use to surveil their own suspects.

Salt Typhoon	Also known as **RedMike, Ghost Emperor, Earth Estries, Famous Sparrow, Operator Panda**. Attributed to China's Ministry of State Security (MSS).

Attribution	MSS. China's civilian foreign intelligence service. Responsible for external intelligence collection and foreign operations.
Scale	FBI confirmed **at least 200 companies compromised across 80+ countries**.
What Was Accessed	The **CALEA intercept infrastructure.** The group accessed the active intercept list, which shows exactly which phone numbers are under ongoing law enforcement surveillance at any given moment.
Data Exfiltrated	Call detail records, SMS metadata, and in some cases **live audio intercepts of senior government officials.**
Initial Access Vector	Unpatched Cisco network devices. The vulnerabilities were discovered and patched by Cisco in **2023.** The telecom companies never applied the patches.
Persistence	The group remained active through early 2026 despite US Treasury sanctions against **Sichuan Juxinhe Network Technology Co. Ltd.**, identified as a front company. In December 2025, Salt Typhoon was found inside a US House of Representatives committee network. In January 2026, the group attempted to compromise an additional 1,000 Cisco devices globally.

CALEA: WHY THIS MATTERS

- **CALEA** is the Communications Assistance for Law Enforcement Act. Every US telecom operator must build into their network the ability for law enforcement, acting on a court order, to flip a switch and monitor the communications of a specific individual.
- Salt Typhoon did not just steal call records. They compromised the mechanism through which the US government monitors its own suspects. The intercept list tells you which phone numbers are under active investigation across the entire country.
- The operational value of this access is significant. China could check every phone number being surveilled by US law enforcement, identifying subjects of ongoing criminal and national security investigations.

// SALT TYPHOON: KEY EVENTS

2023

Cisco vulnerability discovered and patched. US telecom companies fail to apply the patches.

LATE 2024

Salt Typhoon breach of US carriers confirmed. Verizon, AT&T, and Lumen Technologies among those compromised. CALEA wiretap infrastructure accessed.

DEC 2024

FBI public advisory issued. Citizens advised to stop using standard calls and SMS and switch to end-to-end encrypted applications.

DEC 2025

Salt Typhoon found inside a US House of Representatives committee network.

JAN 2026

Group observed attempting to compromise 1,000+ additional Cisco devices globally.

2025–2026

Trend Micro confirms Salt Typhoon activity inside Indian organizations. Target cluster also includes Afghanistan, Taiwan, Philippines, and Brazil. Trend Micro

---

// 02 — VOLT TYPHOON: PREPOSITIONING FOR DISRUPTION

Volt Typhoon is a different group with a different mission. Where Salt Typhoon is about intelligence collection, **Volt Typhoon is about prepositioning.** Placing dormant implants inside critical infrastructure that can be activated when needed.

Volt Typhoon	Attributed to the **People's Liberation Army (PLA),** the Chinese military. A military operation, not a civilian intelligence one.
Mission	Not espionage. **Prepositioning for disruption and degradation of services.** Known targets include US power grids, water treatment systems, ports, and pipelines.
Dwell Time	Volt Typhoon was found lurking inside US power grid infrastructure for **approximately 300 days** before detection.
The Geneva Acknowledgement	Per The Wall Street Journal: in a classified meeting in Geneva in December 2024, Chinese officials acknowledged Volt Typhoon's prepositioning to their US counterparts. The reported message: *"Yes, that is us. Consider it a signal about Taiwan."* The first known instance of Chinese officials publicly acknowledging one of their own APT groups.
Strategic Context	Gray zone deterrence. China has positioned itself so that in any military escalation over Taiwan, it can degrade US critical infrastructure remotely. Dormant implants in power grids, water systems, and ports function as leverage held in reserve.

// 03 — INDIA: ON THE TARGET LIST, OFF THE RECORD

India is not on the periphery of this campaign. The evidence is documented. The institutional response is silence.

200+	80+	263	0
COMPANIES COMPROMISED GLOBALLY FBI confirmed	COUNTRIES AFFECTED FBI confirmed	AVG. DAYS TO DETECT & CONTAIN A BREACH IN INDIA IBM Cost of a Data Breach India 2025	CERT-IN ADVISORIES ON SALT OR VOLT TYPHOON As of episode recording

INDIA AS A TARGET: THE EVIDENCE

- Trend Micro confirmed Salt Typhoon activity inside Indian organizations across multiple sectors. The same target cluster includes Afghanistan, Taiwan, Philippines, and Brazil. Trend Micro, 2025–2026
- Recorded Future found that more than half of all targeted Cisco network devices were concentrated in the US, South America, and India. India is one of the three primary geographic concentration zones. Recorded Future
- Documented compromises exist across India's immediate neighborhood: Myanmar, Bangladesh, Indonesia, Malaysia, and Thailand have all had confirmed intrusions in their telecom companies from the same groups.
- Not a single Indian carrier has publicly confirmed a compromise. No company has issued any statement. No research firm has publicly named any Indian victim organization. The silence is not evidence that nothing has happened.

INDIA'S TELECOM VULNERABILITY SURFACE

- The vulnerability surface is identical to the one Salt Typhoon has already demonstrated it can exploit across 80+ countries. The same unpatched Cisco devices. The same lawful intercept architecture.
- **SIM swap fraud** remains rampant. Ministry of Home Affairs data: approximately Rs 22,495 crore lost to cyber fraud in 2025. A significant portion comes from SIM swap fraud, enabled by process loopholes or insider access within telecom companies.
- Customer service agents at Indian telecoms can see full subscriber profiles on their CRM screens: full name, billing address, Aadhaar number, last cell tower ping, and complete call detail records. Insider access logging and anomaly detection on these systems is minimal.
- The **2019 Airtel vulnerability** led to a major data breach. Truecaller has put approximately 300 million Indian phone numbers, names, locations, and email addresses in the public domain. Combined with KYC database leaks, a detailed profile of most Indian citizens can be assembled through OSINT and dark web searches alone.
- Indian telecom companies have no published independent security audits.
- The average Indian organization takes **263 days** to detect and contain a breach. That is enough dwell time for an attacker to establish layered persistence even after an apparent eviction. IBM, 2025

INDIA'S MILITARY COMMUNICATIONS: A SEPARATE ARCHITECTURE

- Indian armed forces do not use commercial telecom networks. Their communications infrastructure is physically independent.
- **ASCON** (Army Static Switched Communication Network) and the **AFN** (Armed Forces Network), a tri-services dedicated network. Over Rs 24,600 crore allocated in 2018; L&T and ITI Limited as vendors.
- BSNL laid 60,000 km of optical fiber cable connecting 414 army, air force, and navy bases exclusively for defense use.
- Remote forward bases along the Line of Actual Control and Line of Control are connected by dedicated satellite and microwave radio links.
- A **100 km exclusive spectrum band** runs along the entirety of India's international border. No civilian carrier can operate within it.
- **Network for Spectrum:** a dedicated telecom network built by BSNL for the army in exchange for the army vacating commercial radio spectrum bands for civilian use.

THE REGULATORY PICTURE

- The Department of Telecommunications issued **Telecom Cybersecurity Rules 2024,** mandating four things: appointment of a Chief Telecom Security Officer (CTSO), a 24/7 SOC, a six-hour breach reporting window to the government, and periodic security audits by empaneled auditors.
- The **2025 amendment** expanded scope to cover any platform using a phone number as the primary identifier, classified as Telecommunication Identifier User Entities (TIUE). WhatsApp, food delivery apps, and cab booking applications now fall under this framework.
- A **Mobile Number Verification (MNV)** system was introduced to verify numbers at point of device resale.
- The Five Eyes nations issued joint official advisories publicly naming Salt Typhoon, attributing the intrusions, and directing telecom operators to patch their systems. India issued nothing equivalent.
- CERT-In has issued **zero advisories** on Salt Typhoon or Volt Typhoon.

// 04 — RECENT BREACH NEWS

UNVERIFIED CLAIM

Ashok Leyland Alleged Breach

- A threat actor is claiming a breach of **Ashok Leyland,** India's major commercial vehicle manufacturer. Asking price: approximately USD 8,000 for a claimed 3 TB database.
- Alleged contents: vehicle telematics source code in Python and R, employee PII, customer data, and described as including live truck location data. The listing carries India Military tags, relevant given Ashok Leyland's army vehicle contracts including Stallion trucks, Super Stallion mine-protected vehicles, and army logistics chassis.
- The USD 8,000 asking price is unusually low for a 3 TB claim. If the data were genuine and critical, it would command significantly more. Suggests either a desperate seller or a low-quality dataset of recycled or fabricated material.
- Claims are unverified. Vehicle telematics for military-contracted vehicles would be a legitimate threat if real: live logistics patterns reveal operationally sensitive information. Worth tracking.

PAKISTAN-ALIGNED HACKTIVIST CLAIM

Evil Markers: Alleged Electoral Data

- A Pakistan-aligned hacktivist group called **Evil Markers** has been circulating alleged election data spanning 1948 to 2026.
- The data appears to be compiled public electoral rolls combined with recycled KYC data. The group has no established reputation. The 1948 to 2026 date range and the Telegram sale channel are both inconsistent with a genuine large-scale breach.
- Assessment: more likely information warfare and a psyop timed to the Bengal election cycle than an actual data breach.

EXTORTION

McDonald's India: Everest Group Claim

- The **Everest extortion group** claimed 861 GB of data exfiltrated from McDonald's India in January 2026. Alleged contents: customer PII and internal operations records.
- Everest is a Russian-speaking extortion group. Their methodology is data theft and ransom demand without deploying encryption. Pure extortion, not a ransomware operation.
- Neither **Westlife Development** (west and south India franchise operator) nor **Connaught Plaza Restaurants** (north and east) have issued any public confirmation.

MAJOR PLATFORM BREACH

Vercel: Third-Party AI Tool as the Entry Point

- Vercel, the cloud hosting platform that built Next.js and hosts a large portion of modern web infrastructure, disclosed a breach on April 19. April 2026
- Initial access vector: **Context.ai,** a third-party AI tool. A Vercel employee's Google Workspace account was compromised through Context.ai's OAuth access. The attacker then enumerated environment variables that were not encrypted at rest.
- Someone claiming to be **ShinyHunters** is offering data on a criminal forum for USD 2 million. Claimed contents: access keys, source code, databases, internal deployment credentials, API keys, and a list of 580 Vercel employees.
- The cryptocurrency industry has been scrambling to respond. Orca, the Solana-based exchange, publicly rotated all deployment credentials. A large number of Web3 front-end dashboards are hosted on Vercel.
- Hudson Rock research suggests the root cause may have been a **Lumma stealer** infection on a Context.ai employee's machine.
- Every third-party AI vendor with OAuth access to a primary work environment is now a potential breach vector of equivalent scale. The attack surface expands with every integration added to a workspace.

RESEARCH

Commercial Surveillance Vendors Abusing Telecom Signaling Protocols

- Research published approximately April 23 documented commercial surveillance vendors exploiting flaws in the global telecom signaling system to track target locations without the target network or device being aware. Recorded Future News, Apr 2026
- The technique abuses the carrier-to-carrier signaling protocols that enable international roaming. Surveillance firms are spoofing legitimate signaling messages to extract subscriber location at country, city, and in some cases cell tower level.
- This appears to be a commercial market serving governments, private investigators, and surveillance technology companies rather than direct nation-state APT activity.

// INDIA CYBERCRIME STATISTICS: 2025

₹22,495 Cr	28.15L	+24%	>75%
LOST TO CYBER FRAUD	CYBERCRIME CASES RECORDED	YEAR-ON-YEAR CASE VOLUME INCREASE	LOSSES FROM INVESTMENT FRAUD
Ministry of Home Affairs, 2025	Ministry of Home Affairs, 2025	MHA, 2025	Fake trading platforms, crypto scams, sham IPOs

CHINESE CRIMINAL NETWORKS IN INDIAN BANKING

- Chinese-run criminal networks are laundering over **Rs 5,000 crore per year** through mule account chains targeting Indian banks.
- These networks have been recruiting employees inside Indian banks to facilitate their operations. Gujarat Police has seized significant hardware and made arrests in ongoing investigations into this activity.

// 05 — END OF TRANSMISSION

EPISODE RECAP

- **Salt Typhoon** breached US telecom carriers and gained access to the CALEA wiretap infrastructure. The initial vector was unpatched Cisco devices from 2023. The group has not been evicted and continues to operate as of early 2026.
- **Volt Typhoon,** attributed to the PLA, is placing dormant implants inside US critical infrastructure. Chinese officials have acknowledged this on record and framed it as deterrence over Taiwan.
- **India is a documented target.** Trend Micro and Recorded Future have both confirmed it. India's telecom vulnerability surface is identical to what Salt Typhoon has already exploited elsewhere. The average dwell time before a breach is detected in India is 263 days.
- **CERT-In has issued zero advisories** on either group. India has not joined any Five Eyes attribution statement. No Indian carrier has confirmed a compromise. The silence is not evidence that nothing has happened.
- The Vercel breach is a signal: third-party AI tools with OAuth access to primary work environments are the new supply chain attack surface.

NEXT EP. *The series continues.* **End of transmission.**

// GLOSSARY: ACRONYMS AND FULL FORMS

APT	Advanced Persistent Threat. Industry classification for nation-state-backed hacker groups.
Salt Typhoon	Chinese MSS-attributed APT group. Also known as RedMike, Ghost Emperor, Earth Estries, Famous Sparrow, Operator Panda.
Volt Typhoon	Chinese PLA-attributed APT group focused on prepositioning inside critical infrastructure for disruption.
MSS	Ministry of State Security. China's civilian foreign intelligence service.

PLA	People's Liberation Army. The military of the People's Republic of China.
CALEA	Communications Assistance for Law Enforcement Act. US law requiring telecom carriers to build lawful interception capability into their networks.
CERT-In	Computer Emergency Response Team India. National cybersecurity incident response body.
Five Eyes	Intelligence alliance comprising the US, UK, Canada, Australia, and New Zealand.
ASCON	Army Static Switched Communication Network. India's dedicated military communications network.
AFN	Armed Forces Network. India's tri-services dedicated telecommunications network.
BSNL	Bharat Sanchar Nigam Limited. India's state-owned telecom operator; built the dedicated defense fiber network.
CTSO	Chief Telecom Security Officer. Mandated appointment under India's Telecom Cybersecurity Rules 2024.
TIUE	Telecommunication Identifier User Entity. Classification under the 2025 amendment covering platforms that use phone numbers as primary identifiers.
MNV	Mobile Number Verification. System introduced to verify numbers at point of device resale.
SOC	Security Operations Center. 24/7 team monitoring for cybersecurity incidents.
OSINT	Open Source Intelligence. Intelligence gathered from publicly available information.
LAC	Line of Actual Control. The de facto border between India and China.
LOC	Line of Control. The de facto border between India and Pakistan in Kashmir.
OAuth	Open Authorization. A protocol that allows third-party applications to access a user's account without sharing credentials.
C2 / C&C	Command and Control. Infrastructure attackers use to communicate with compromised systems.
KYC	Know Your Customer. Identity verification process required by Indian financial and telecom regulations.
CRM	Customer Relationship Management. Software used by telecom customer service agents to view subscriber account details.

// SOURCES AND FURTHER READING

FBI Public Advisory	December 2024 advisory on Salt Typhoon; recommendation to switch to encrypted communications.
Trend Micro	Salt Typhoon (Earth Estries) targeting of Indian organizations and target cluster analysis. trendmicro.com/research
Recorded Future	Geographic concentration of targeted Cisco devices; India among top three. recordedfuture.com/research
Peaka Security	Salt Typhoon breach summary covering US broadband providers including Verizon, AT&T, and Lumen.
The Wall Street Journal	Report on the December 2024 Geneva meeting and Chinese acknowledgment of Volt Typhoon activity.
IBM Cost of a Data Breach India Report 2025	263-day average breach detection and containment time for Indian organizations.
Ministry of Home Affairs, India	Rs 22,495 crore cyber fraud losses; 28.15 lakh cybercrime cases; 24% year-on-year increase. 2025 data.
Hudson Rock	Root cause analysis of Vercel breach: Lumma stealer infection on a Context.ai employee machine.
Recorded Future News	Research on commercial surveillance vendors abusing telecom signaling protocols. Published approx. April 23, 2026.
Department of Telecommunications, India	Telecom Cybersecurity Rules 2024 and 2025 amendment (TIUE framework). dot.gov.in

// LISTEN AND FOLLOW

Website | Spotify | Apple Podcasts | YouTube

HOSTED BY KRUTIK PRODUCED BY SPYVEIL