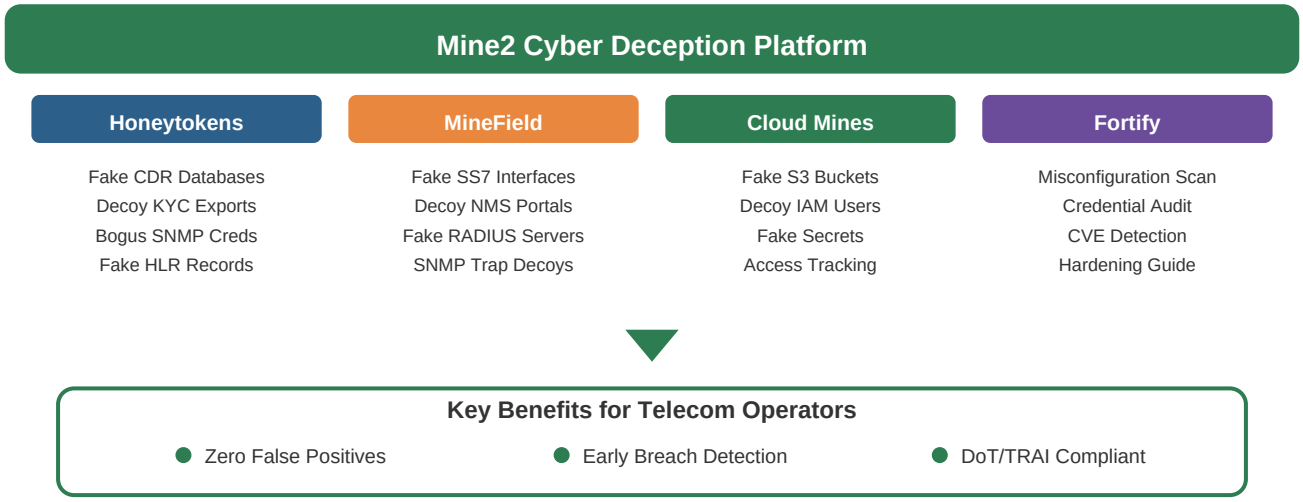
SECURING INDIAN TELECOM

Cyber Deception Strategies for Telecom Operators and ISPs

A Mine2 Industry Whitepaper



Telecom Cyber Security Rules 2024 | DPDP Act 2023 | CERT-In Ready | DoT/TRAI Compliant

www.mine2.io | info@mine2.io

Telecom Is a Tier-1 National Security Target

Indian telecom infrastructure is no longer just a business asset -- it is classified critical infrastructure that underpins every sector of the economy. With 1.2 billion+ mobile subscribers, India's telecom networks carry the nation's financial transactions, government communications, and citizen data. The threats targeting this infrastructure are not theoretical -- they are active, state-sponsored, and devastating.

What Has Already Happened in India

BSNL -- Breached Twice in 6 Months (2023-2024): In December 2023, threat actor 'Perell' leaked 2.9 million broadband subscriber records from an unpatched internal server. Then in May 2024, threat actor 'kiberphant0m' exfiltrated 278 GB of critical data including IMSI numbers, SIM card details, Home Location Register (HLR) data, SOLARIS server snapshots, and call log samples with timestamps and billing details. The data was offered for sale at $5,000 on BreachForums. The breach was confirmed in Parliament by the Minister of State for Communications.

Airtel -- 375 Million Records Alleged (July 2024): A hacker using alias 'xenZen' claimed to be selling data of 375 million Bharti Airtel users on the dark web for $50,000. The alleged data included Aadhaar numbers, addresses, SIM activation dates, and photo ID proof. While Airtel denied a breach, the incident highlighted the value of telecom subscriber data as a target.

Hathway ISP -- 41.5 Million Customers (March 2024): A critical CMS vulnerability was exploited to leak 200 GB of customer data including names, emails, billing details, and account credentials.

1.77 Crore Fraudulent SIM Connections: In 2024, DoT detected and deactivated 1.77 crore mobile connections obtained through fake or forged KYC documents -- each a potential vector for financial fraud, digital arrest scams, and SIM swap attacks.

278 GB	Rs 22,800 Cr	72M+
stolen from BSNL including IMSI, SIM, HLR data	cyber fraud losses in India in 2024	China-origin attack attempts on telecom decoys (Salt Typhoon)

The Global Wake-Up Call: Salt Typhoon

Salt Typhoon, a Chinese state-sponsored APT group linked to China's Ministry of State Security, executed the most significant telecom espionage campaign in history during 2024. The group compromised at least 9 major US telecom companies (including AT&T, Verizon, T-Mobile) using custom 'GhostSpider' backdoor malware, gaining real-time access to call records, SMS metadata, and even audio recordings of calls by senior government officials.

The Global Cyber Alliance recorded 72 million+ China-origin attack attempts against telecom decoy systems between 2023-2025. Recorded Future confirmed that over half of the 1,000+ targeted Cisco devices were in the US, South America, and India. Salt Typhoon targeted 80+ nations, with 600+ organizations notified.

> *India is explicitly in Salt Typhoon's crosshairs. Recorded Future confirmed Indian Cisco devices were among those targeted. The BSNL breaches demonstrated that Indian telecom networks have the same vulnerabilities Salt Typhoon exploited in the US -- legacy equipment, unpatched systems, and insufficient internal detection.*

Why Traditional Telecom Security Falls Short

Telecom operators invest heavily in perimeter security: firewalls, IDS/IPS, DDoS mitigation, and NOC monitoring. Yet BSNL was breached twice. Here's the fundamental disconnect:

Perimeter-Blind to Insiders: BSNL's breach came from an internal FTP server. Firewalls protect the edge, but once an attacker is inside -- via phished credentials, compromised vendor access, or a rogue employee -- perimeter tools are irrelevant. Salt Typhoon spent 1-2 years inside US telecom networks undetected.

Signature-Blind to Novel Threats: Salt Typhoon used custom GhostSpider malware that no signature database could match. State-sponsored actors develop bespoke tools specifically to evade detection. Signature-based IDS misses what matters most.

NOC Alert Fatigue: Large telecom NOCs process thousands of alerts daily across massive infrastructure. In BSNL's case, the breach went undetected until a third-party threat intelligence firm (Athenian Tech) discovered the data being sold on BreachForums. Internal monitoring failed entirely.

200+ Day Dwell Time: Industry average dwell time exceeds 200 days. Salt Typhoon was inside US networks for 1-2 years. In telecom, every undetected day means more subscriber data exfiltrated, more call records intercepted, more infrastructure mapped for future attacks.

What Is Cyber Deception -- and Why Telecom Needs It

Cyber deception takes a fundamentally different approach: instead of trying to identify attackers by their behavior (noisy) or their tools (bypassable), it places realistic fake assets throughout your network. Fake subscriber databases. Fake SNMP management consoles. Fake HLR records. Fake SSH credentials for network elements.

These decoys serve no legitimate purpose. No real engineer, no real system, no real process should ever touch them. When something does, it is a confirmed threat -- not a probabilistic guess.

> *This is exactly how Salt Typhoon was studied. The Global Cyber Alliance used honeypot decoy systems emulating telecom networks to record 72 million+ attack attempts and map Salt Typhoon's tactics. The same technology that researchers use to study nation-state attackers is what Mine2 deploys to protect your production network.*

Mine2 Cyber Deception Platform

Honeytokens

Digital tripwires planted across your environment: fake database credentials, SSH/RDP keys for network elements, decoy documents (Subscriber_KYC_Export.xlsx, CDR_Backup_May2024.sql), and fake Active Directory accounts. Any access triggers immediate alerts.

MineField

Decoy network services: fake MySQL/MongoDB instances mimicking subscriber databases, SNMP management interfaces, RADIUS/TACACS servers, FTP/SMTP services, and web-based NMS portals. Any connection to these decoys is a confirmed intrusion.

Cloud Mines

AWS deception: automated discovery, intelligent suggestions, and deployment of fake S3 buckets, IAM roles, and secrets -- critical as telecom operators migrate BSS/OSS workloads to cloud.

Fortify

Proactive hardening: scans for misconfigurations, default SNMP community strings, unpatched Cisco IOS vulnerabilities (the exact entry point Salt Typhoon exploited), and insecure credentials.

Telecom-Specific Use Cases

1. Subscriber Data Protection (HLR/HSS, CRM)

The Risk: Subscriber databases contain Aadhaar-linked KYC for 1.2B+ connections, IMSI numbers, call detail records, location data, and billing information. BSNL proved these are accessible and sellable. A single subscriber database breach affects crores of citizens.
Mine2 Approach: DB honeytokens planted near subscriber databases mimic real KYC records. Decoy exports (Subscriber_Aadhaar_KYC.xlsx, CDR_Dump_2024.csv) on internal servers act as early warning tripwires. MineField creates fake HLR/HSS interfaces that catch attackers probing for subscriber identity data.

2. Network Element Security (Routers, Switches, Core)

The Risk: Salt Typhoon specifically targeted Cisco routers and switches in telecom networks, exploiting CVE-2023-20198 and CVE-2023-20273. Compromised network elements enable traffic interception, route manipulation, and persistent backdoor access. India was among the top-targeted geographies.
Mine2 Approach: MineField decoys emulate SNMP management interfaces, SSH consoles, and NMS portals for network equipment. Fortify scans for default community strings, unpatched firmware, and the exact CVEs Salt Typhoon exploited. Any probe of decoy network elements = confirmed threat.

3. BSS/OSS & Billing Systems

The Risk: Business and operations support systems contain customer billing data, provisioning workflows, revenue assurance records, and interconnect details. Compromise enables fraud at scale.
Mine2 Approach: Honeytokens in CRM and billing databases, decoy provisioning interfaces, fake admin accounts for OSS platforms. Cloud Mines protect BSS workloads migrating to AWS/Azure.

4. SIM Swap & Telecom Fraud Detection

The Risk: With 1.77 Crore fraudulent SIM connections detected in 2024 alone, insider-assisted SIM swap fraud is a major vector for financial crime. Rogue agents or compromised dealer systems enable unauthorized SIM replacements targeting high-value accounts.
Mine2 Approach: Honeytoken subscriber accounts designed as attractive targets for SIM swap attempts. Any unauthorized SIM change request on these accounts triggers immediate alerts, identifying the dealer, agent, and system used.

5. 5G & Virtualized Infrastructure

The Risk: 5G introduces virtualized RAN, edge computing nodes, network slicing, and API gateways. Each virtualized function is a software-defined attack surface. Container orchestration platforms (Kubernetes) managing 5G core functions create new lateral movement paths.
Mine2 Approach: Cloud Mines for fake container registries and Kubernetes secrets. Honeytoken API keys for 5G core APIs. Decoy network slice configurations that detect unauthorized probing. Fortify scanning for container and orchestration misconfigurations.

6. Vendor & Supply Chain Access

The Risk: Equipment vendors (Cisco, Ericsson, Nokia), managed service providers, and tower companies have deep logical and physical access. Salt Typhoon infiltrated supply chains, embedding malicious payloads in firmware updates. A compromised vendor = compromised network.
Mine2 Approach: Deception assets in vendor-accessible network segments. Honeytoken credentials in vendor jump boxes. Fake firmware repositories and configuration files. Any vendor-side anomaly triggers alerts before it reaches production infrastructure.

Regulatory Compliance

Indian telecom operates under an evolving regulatory framework that now explicitly mandates cyber security controls. Mine2 directly supports compliance:

Telecom Cyber Security Rules, 2024

Notified by DoT on 21 November 2024 under the Telecommunications Act 2023, these rules mandate every telecom entity to implement measures ensuring telecom cyber security, prevent misuse of telecom identifiers, and protect critical telecom infrastructure. DoT has established a Telecom Security Operations Centre (TSOC) for threat detection and stakeholder alerting.
How Mine2 Helps: Provides active, demonstrable detection capabilities that satisfy the Rules' requirement for 'measures to protect and ensure telecom cyber security.' Mine2 alerts integrate with TSOC reporting workflows. Fortify identifies infrastructure vulnerabilities mandated for remediation under the Critical Telecommunication Infrastructure Rules.

DPDP Act 2023 (Subscriber Data Protection)

Telecom operators are Data Fiduciaries processing Aadhaar-linked KYC, call records, and location data for 1.2 billion+ subscribers. The Act mandates 'reasonable security safeguards' and breach notification. With BSNL's breach confirmed in Parliament, the regulatory spotlight is firmly on telecom data protection.
How Mine2 Helps: Forensic telemetry provides timestamped evidence of breach detection. Audit trails demonstrate proactive data protection. Honeytokens specifically guarding subscriber KYC databases ensure breaches are detected before they become Parliamentary questions.

CERT-In Incident Reporting (6-Hour Mandate)

CERT-In mandates 6-hour incident reporting for critical infrastructure entities. BSNL's breach was first reported not by BSNL but by an external threat intelligence firm. This is the exact scenario regulators want to prevent -- operators discovering breaches from the press, not from their own security systems.
How Mine2 Helps: Immediate alerts with complete forensic context -- source IP, user identity, accessed asset, timestamp -- enable detection and reporting without waiting for a third party to find your data on BreachForums.

DoT License Conditions & TRAI Regulations

Unified License conditions require operators to protect subscriber data and network integrity. TRAI's subscriber privacy mandates require active controls against unauthorized access. The inter-ministerial committee formed after the BSNL breach is conducting comprehensive telecom network audits -- operators need to demonstrate active security, not just policies.
How Mine2 Helps: Provides demonstrable, working detection mechanisms with low operational overhead. Audit-ready forensic trails satisfy regulatory inspections and inter-ministerial committee requirements.

How Mine2 Would Have Changed the Outcome

These scenarios are modeled on real Indian telecom incidents. We show how deception technology would have altered the timeline:

Scenario 1: The BSNL-Style Internal Server Breach

Without Mine2: An attacker gains access to an internal FTP server through compromised or default credentials. Over days, they exfiltrate 278 GB of subscriber IMSI data, SIM details, HLR records, and server snapshots. The breach is discovered months later when a threat intelligence firm spots the data being sold on BreachForums for $5,000. Parliament demands answers.

With Mine2: Same initial access. But the FTP server directory also contains a Mine2 honeytoken file: 'HLR_Full_Backup_Jan2024.tar.gz'. When the attacker downloads it, Mine2 alerts fire within seconds with source IP, credentials used, and timestamp. Security team isolates the server and resets credentials the same day. Zero subscriber data reaches the dark web.

Scenario 2: Salt Typhoon-Style Network Element Compromise

Without Mine2: A state-sponsored actor exploits an unpatched Cisco vulnerability on an internet-facing router. They establish persistent access using custom backdoor malware, then spend months mapping the core network, intercepting CDRs, and accessing lawful intercept systems. Discovery comes 18 months later from a foreign intelligence advisory.

With Mine2: Same router compromise. But during lateral movement, the attacker probes a MineField decoy SNMP management interface that looks like a core switch. Mine2 detects the connection attempt immediately. The SOC correlates the alert with the compromised router and initiates incident response within hours -- not months.

Scenario 3: Insider-Assisted SIM Swap Fraud

Without Mine2: A rogue dealer agent processes unauthorized SIM swaps for high-value customers, enabling financial fraud. The fraud is only discovered when affected customers report unauthorized bank transactions -- often after lakhs have been stolen.

With Mine2: Honeytoken subscriber accounts are seeded in the system -- accounts designed to look like high-value targets. When the rogue agent attempts a SIM swap on a honeytoken account, Mine2 alerts immediately with agent ID, dealer code, terminal, and timestamp. Evidence is captured for investigation before any real customer is defrauded.

Getting Started

1. Assess Map critical assets: subscriber databases, core network elements, BSS/OSS systems, cloud infrastructure, and vendor access points.

2. Plan Strategic placement along likely attack paths -- based on how BSNL was breached and how Salt Typhoon operates, not random scattering.

3. Deploy Days, not months. Zero impact on network operations, subscriber services, or SLA commitments.

4. Integrate Connect alerts to your NOC/SOC, SIEM, and TSOC reporting workflows. Train operations team on response procedures.

5. Evolve As 5G rollout expands, cloud migration progresses, and new vendors are onboarded -- Mine2 coverage evolves with your network.

Business Value Beyond Security

For telecom leadership evaluating cybersecurity investments, Mine2 delivers measurable value across dimensions that matter to the board:

Subscriber Trust at Scale

With 1.2 billion+ connections, a single breach like BSNL's triggers Parliamentary questions, TRAI investigations, and media firestorms. Early detection prevents subscriber data from reaching BreachForums -- protecting trust for crores of customers.

Regulatory Penalty Avoidance

DPDP Act penalties can reach Rs 250 Crore. The Telecom Cyber Security Rules add enforcement mechanisms. The inter-ministerial committee formed post-BSNL is actively auditing telecom networks. Mine2's forensic trails demonstrate proactive compliance.

Nation-State Defense

Salt Typhoon proved that telecom networks are strategic espionage targets. Deception is the technology researchers used to study Salt Typhoon's TTPs -- and it is the same technology that can detect state-sponsored lateral movement in your production network.

SOC/NOC Cost Optimization

Near-zero false positives mean your NOC team investigates confirmed threats, not noise. For operators processing thousands of alerts daily across massive infrastructure, this is a force multiplier for existing security investment.

5G Revenue Protection

As operators invest lakhs of crores in 5G infrastructure, protecting that investment from compromise is essential. Mine2 extends deception to virtualized RAN, edge computing, and 5G core without disrupting rollout timelines.

Minimal Operational Impact

No agents on network elements. No production traffic inspection. No performance impact on subscriber services. No additional latency on voice or data paths. Deployed in days alongside existing NOC/SOC tools.

Why Mine2 for Telecom:

- Near-zero false positives: every alert is a confirmed intrusion
- Catches attackers during recon -- before data exfiltration
- Complements existing NOC/SOC, IDS/IPS, and SIEM investments
- Non-bypassable: deception assets cannot be fingerprinted or evaded
- Detects both nation-state actors AND insider threats equally

Conclusion

Indian telecom is the nation's digital backbone -- and its most targeted infrastructure. BSNL proved that internal threats go undetected. Salt Typhoon proved that nation-states are inside telecom networks worldwide. The Telecom Cyber Security Rules 2024 prove that regulators expect active detection, not just perimeter defense.

The question is not whether your network will be probed by Salt Typhoon or its successors -- Recorded Future has already confirmed India is being targeted. The question is whether you will detect them before subscriber data is exfiltrated, before call records are intercepted, before your network becomes someone else's intelligence asset. Mine2 ensures you will.

Contact Mine2 Today

www.mine2.io | info@mine2.io