DRONA
CYBER SOLUTIONS

CONFIDENTIAL

THREAT ADVISORY

ALLEGED DATA BREACH TARGETING

BANK OF BARODA

THREAT ACTOR
TRIPLEX

Alleged large-scale data exposure involving customer information and internal banking records published on a dark web leak portal.

PUBLICATION DATE
JULY 2026

SEVERITY
HIGH

INDUSTRY
BANKING & FINANCIAL SERVICES

REPORT TYPE
THREAT INTELLIGENCE REPORT

CLASSIFICATION
CONFIDENTIAL
TLP: AMBER

DARK WEB MONITORING | THREAT INTELLIGENCE | RISK MITIGATION

1. EXECUTIVE SUMMARY

Key Threat Intelligence Findings

On 25 July 2026, threat actor group **TripleX** published a listing on their Tor-hosted Data Leak Site (.onion) alleging the acquisition and free distribution of 1 Terabyte (1 TB) of sensitive customer and internal operational records belonging to Bank of Baroda. The actor operates a pure data extortion model—releasing datasets directly to maximize public exposure, brand disruption, and regulatory consequences rather than demanding system decryption ransoms.

Core System Status: Based on technical analysis of the leaked directory structure and sample files, there is no evidence indicating compromise of core transaction processing, account ledger systems, or live banking databases. The breach stems from a perimeter compromise of an enterprise email/document storage tenant, through which attachments, onboarding scans, and internal branch reports were systematically harvested.

2. INCIDENT TIMELINE & KEY OBSERVABLES

DATE / TIMELINE	OBSERVED ACTIVITY & THREAT EVENT
May 2026	**Regional Precursor Incident (PT Bank Negara Indonesia):** TripleX compromises PT Bank Negara Indonesia (BNI), exfiltrating and leaking 2 TB of corporate data. Establishes a distinct operational focus on large South/Southeast Asian financial institutions.
June 2026	**Credential Exposure & Security RFPs:** Security researchers highlight historical credential exposures linked to the RBI bank.in domain registry. Bank of Baroda publishes RFPs for an Enterprise Data Privacy Governance Platform and Behavioral Biometrics/MFA solutions.
Early July 2026	**Initial Compromise Vector:** TripleX gains access to a Bank of Baroda corporate email environment using compromised or weak employee credentials, establishing a quiet foothold without triggering core banking alerts.
Mid July 2026	**Internal Harvesting & Exfiltration:** Threat actor systematically scrapes email attachments, regional branch shared folders, and audit repositories, compiling an estimated 700 GB to 1 TB dataset.
25 July 2026	**Tor DLS Publication:** TripleX lists Bank of Baroda on their Tor leak portal, providing sample archives containing KYC documents, Aadhaar/PAN cards, loan files, and internal audit reports.
27–28 July 2026	**Containment & Forensics:** Bank of Baroda isolates the compromised enterprise email segment, engages external digital forensics teams, notifies regulatory authorities, and files loss assessment with National Insurance Company.

3. ANALYSIS OF EXPOSED DATA ASSETS

The exfiltrated repository comprises both highly sensitive customer Personally Identifiable Information (PII) and internal administrative files. Below is a detailed categorization of the affected data streams:

CATEGORY	EXPOSED DOCUMENT TYPES & FEATURES	PRIMARY THREAT VECTORS
Customer KYC & PII	Aadhaar cards, PAN cards, customer passport photos, physical signatures, and account opening application forms.	Identity Theft, SIM Swap, Synthetic ID Creation
Loan & Asset Documents	Personal, home, vehicle, education, and gold-loan pledge memos (including IIFL joint scheme paperwork and appraisal memos).	Targeted Extortion, Vishing Scams
Net Banking Records	Corporate and retail bob World Net Banking user applications, service logs, and registration references.	Credential Stuffing, Social Engineering
Internal Governance	Branch audit reports (Patna, Lucknow, Varanasi, Bhopal zones), bob World special audit files, and vigilance reports.	Workflow Exploitation, Infrastructure Reconnaissance
Third-Party Data	Reconciliation files from insurance partners (IndiaFirst Life Insurance) and external empanelment records.	Supply Chain Compromise

4. THREAT ACTOR PROFILE & OPERATIONAL TACTICS

Threat Group: TripleX (also identified as Triple X). Active on Russian-language underground cybercrime forum Exploit under the username `apt8172`.
Model: Pure Data Extortion / Extortion-via-Leak. The group bypasses traditional ransomware encryption in favor of rapid data exfiltration followed by public disclosure to maximize reputational pressure.

MITRE ATT&CK Framework Mapping:

TACTIC	TECHNIQUE NAME & ID	OBSERVED MECHANISM
Initial Access	Valid Accounts (T1078) / Phishing (T1566)	Compromise of employee enterprise email account via stolen/weak credentials.
Credential Access	Unsecured Credentials (T1552)	Harvesting credentials exposed in sector domain registries and historical dumps.
Collection	Email Collection (T1114) / Local Data (T1005)	Bulk scraping of email attachments, onboarding scans, and shared drive files.
Exfiltration	Exfiltration Over Web Service (T1567)	Staged exfiltration of multi-hundred gigabyte archives over encrypted web channels.
Impact	Data Destruction / Public Leak (T1485)	Unrestricted hosting on Tor hidden services to trigger public and regulatory fallout.

5. TECHNICAL INDICATORS OF COMPROMISE (IOCS)

```
# Tor Hidden Service TripleX Data Leak Site (Bank of Baroda)
ojcmpbdncjo5dhaxx1144bq6to3kwqtoeraevgsjquhdtt4uv514igid.onion

# Associated Tor Infrastructure (PT Bank Negara Indonesia Incident)
6qqz6m3b6htudohg2mlf5gdcalonxy3sh5g4dix4mpyirjcgelqqufad.onion

# Threat Actor Forum Aliases & Handles
TripleX | Triple X | apt8172 (Exploit Forum)
```

6. STRATEGIC RECOMMENDATIONS & RISK MITIGATION FRAMEWORK

Drona Cyber Solutions Pvt Ltd advises implementing a multi-layered response framework divided into immediate containment and strategic posture enhancement:

Phase 1: Immediate Containment Actions (Weeks 1–4)

- **Enterprise Credential & Session Reset:** Execute global session revocation and password resets across all corporate email tenants, remote access portals, and cloud document repositories.
- **Forensic Scope Verification:** Perform deep host and tenant forensics to verify the precise boundaries of exfiltrated data and confirm total attacker removal.
- **Brand & Dark Web Monitoring:** Continuous automated tracking across dark web forums, paste sites, and Telegram channels for secondary distribution of the dataset.
- **Targeted Customer Fraud Alerts:** Issue advisory notices to high-risk customer segments regarding potential vishing, phishing, and SIM-swap attempts using their exposed details.

Phase 2: Strategic Posture Enhancement (Months 1–3)

- **Accelerate Phishing-Resistant MFA:** Deploy hardware keys or FIDO2-compliant biometrics across all employee and contractor access points.
- **Data Loss Prevention (DLP) & UEBA Integration:** Configure strict DLP rules preventing bulk downloading or unencrypted attachment transfers, paired with User & Entity Behavior Analytics to detect unusual data harvesting.
- **KYC Data Lifecycle Overhaul:** Implement automated data purging policies so that customer KYC scans and temporary onboarding files are erased after processing rather than persisting in mail stores.

DRONA CYBER SOLUTIONS PVT LTD

Cyber Threat Intelligence & Incident Response Division

Email: info@dronacybersolutions.com • Web: www.dronacybersolutions.com