Threat Intelligence Report on Bank of Baroda Data Breach

July 2026

Table of Contents

1. Executive Summary

The emergence of a large-scale alleged data exposure involving Bank of Baroda has raised significant concerns regarding the potential compromise of customer information and internal banking records. Between 25 and 27 July 2026, a threat actor operating under the name "TripleX" published a listing on its Tor-hosted leak portal claiming possession of approximately 1 terabyte (TB) of data purportedly belonging to the bank. The listing advertises unrestricted public access to the alleged dataset and is accompanied by multiple sample documents, apparently intended to demonstrate the authenticity of the claimed breach.

Unlike conventional ransomware operations that typically encrypt systems and negotiate financial demands with victims, the observed activity appears to follow a **data extortion and public disclosure model**. The threat actor has not publicly issued a ransom demand against Bank of Baroda. Instead, the claimed dataset has been advertised as freely downloadable through the actor's leak portal, a tactic designed to maximise reputational damage, increase media attention, and facilitate widespread redistribution of the exposed information. This approach significantly increases the risk of downstream criminal abuse, including identity theft, financial fraud, phishing campaigns, and other forms of social engineering.

As part of this assessment, Athenian Tech reviewed the limited set of sample documents published by the threat actor to evaluate the credibility of the claim. The reviewed samples appear consistent with authentic Bank of Baroda operational records and include customer onboarding (KYC) documentation, government-issued identity documents such as Aadhaar and PAN cards, customer photographs, signatures, account-related forms, loan documentation, and internal branch records. The diversity and structure of the published material provide a **high level of confidence** that the threat actor possesses genuine Bank of Baroda documentation. However, Athenian Tech has **not independently verified** the complete archive or confirmed the threat actor's claims regarding the total dataset size or the estimated number of affected customer records.

Public statements issued by Bank of Baroda indicate that the incident is under active investigation. According to the bank, the unauthorised access originated from a **compromised employee email account**, which was subsequently used to access certain internal information. The bank has further stated that its **core banking infrastructure, customer transaction systems, and financial operations remain unaffected**, and that forensic investigations are being conducted in coordination with the appropriate authorities and cybersecurity experts. At the time of this assessment, the precise scope of the exposure and the total number of affected individuals have not been officially confirmed.

Open-source intelligence further indicates that **TripleX** has previously been associated with a similar incident involving **PT Bank Negara Indonesia (BNI)** in May 2026, where the actor claimed to have exfiltrated approximately **2 TB** of banking data before publishing sample documents on a Tor-based leak platform. The similarities between the two incidents—including the targeting of large state-owned financial institutions, publication of customer identity documents and internal banking records, and the use of public leak sites instead of traditional ransom negotiations—suggest a repeatable operational methodology focused on large-scale document exfiltration and public data exposure. While attribution remains based primarily on the actor's own branding and publicly observable tactics, the consistency of these activities provides **moderate confidence** that both incidents are linked to the same threat actor or closely associated operators.

Based on the available evidence, Athenian Tech assesses that this incident represents a **significant data exposure event** with potentially serious implications for both Bank of Baroda and its customers. If the leaked documents are authentic and widely redistributed, affected individuals may face increased risks of identity theft, account impersonation, fraudulent financial applications, targeted phishing and vishing campaigns, SIM-swap attacks, and other forms of financial crime. The apparent inclusion of internal banking documents may also provide adversaries with valuable operational knowledge that could be leveraged to enhance future social engineering campaigns or support follow-on attacks against the organisation.

At the time of this report, the threat actor's claimed dataset remains publicly advertised through a Tor-hosted leak portal, and the long-term impact of the incident will depend on the extent of the compromised information, the speed of containment measures, and the effectiveness of customer notification and remediation efforts. Athenian Tech recommends continued monitoring of underground forums and dark web marketplaces for evidence of secondary distribution, commercial sale, or further publication of the leaked material, while supporting ongoing forensic investigation and incident response activities.

Key Findings

- A threat actor operating under the name "TripleX" has published a listing on a Tor (.onion) leak portal claiming possession of an alleged ~1 TB dataset associated with Bank of Baroda. The listing was first identified through dark web monitoring on 25 July 2026 and advertises unrestricted public access to the purported dataset.

- Based on the publicly released sample files, the exposed information appears to include customer KYC and account-opening forms, Aadhaar and PAN card copies, customer photographs, loan and gold-loan documentation, insurance-related records, and internal branch documents. While these samples enhance the credibility of the claim, the complete dataset has not been independently verified.

- TripleX has previously been linked to the alleged compromise of PT Bank Negara Indonesia (BNI) in May 2026, where the actor claimed to have exfiltrated approximately 2 TB of sensitive banking data. The similarities in victim profile, exposed data types, and publication methodology suggest a repeatable operational pattern targeting major financial institutions across South and Southeast Asia.

- The threat actor appears to employ a public data extortion strategy rather than a conventional ransomware model. In both observed incidents, the alleged stolen data was advertised for free public download instead of being used solely as leverage during ransom negotiations, indicating an emphasis on maximising reputational damage, media attention, and opportunities for downstream fraud.

- Bank of Baroda has publicly stated that the incident originated from the compromise of an employee email account and has indicated that its core banking systems and customer transaction infrastructure remain unaffected. At the time of this report, these statements have not been independently validated through forensic evidence available to Athenian Tech.

2. Incident Overview

Attribute	Detail
Victim organisation	Bank of Baroda (state-owned Indian bank)
Date first observed	25 Jul 2026
Claimed data volume	~1 TB
Claimed record count	~100,000–300,000 customer application forms
Leak site	Tor-hosted blog, “Triple X WebBlog”

The listing frames the disclosure in the voice of a concerned data subject (“Imagine I'm going to the bank to open an account... my personal data should be leaked”), a rhetorical device the actor also uses to pre-empt questions of legal liability. This framing, combined with the free-download model, suggests the operator is optimising for maximum public exposure and reputational pressure on the bank rather than for a quiet, negotiated ransom.

2.1 Categories of Data Referenced in the Leak Listing

- **Personal banking** — Savings and current account details
- NetBanking credentials/records (“bob World” corporate and retail users)
- **Loan records** — Personal, home, vehicle, and education loans; gold-ornament pledge documentation
- NRI and corporate banking service records
- Customer support and branch/ATM locator data
- **Internal documents** — Branch audits, loan appraisal files, internal communications, vigilance investigation material

Athenian Tech reviewed a limited number of sample documents published by the threat actor to assess the credibility of the alleged data exposure. The sample documents reproduced in Section 6 are taken from the threat actor's publicly accessible leak page and are included solely for evidentiary and analytical purposes. These samples provide insight into the nature, structure, and sensitivity of the allegedly exposed information and assist in validating the threat actor's claims. The reproduced material is intended exclusively for the designated recipients of this confidential report and should not be further distributed, reproduced, or disclosed without appropriate authorisation.

3. Threat Actor Profile: TripleX

Attribute	Detail
Actor name	TripleX (“Triple X”)
Type	Data-extortion / leak-focused threat actor (not a confirmed encryption-ransomware crew — no encryption payload has been publicly reported for either known incident)
First tracked activity	May 2026 (BNI, Indonesia)
Known forum presence	Exploit.in underground forum, handle reported as “apt8172”
Infrastructure	Tor-hosted leak/blog sites; sample files distributed via direct .onion links, occasionally password-protected archives
Known victims (public, as of this report)	PT Bank Negara Indonesia (May 2026); Bank of Baroda, India (July 2026)
Sector focus (observed)	State-owned / large retail banking institutions
Geographic focus (observed)	South and Southeast Asia
Extortion style	Public free-leak model; leverages media attention and regulator pressure rather than direct ransom negotiation with the victim

3.1 Case History

May 2026: TripleX was first observed claiming responsibility for a large-scale data breach targeting a major banking institution in Southeast Asia. The threat actor alleged the exfiltration of approximately 2 TB of sensitive customer and internal banking data and published sample documents through a Tor-hosted leak portal, indicating a strategy focused on public disclosure of stolen information.

July 2026: Approximately two months later, TripleX claimed another large-scale data exposure targeting Bank of Baroda, alleging the compromise of approximately 1 TB of customer and internal banking records. The incident followed a similar pattern, with the publication of sample documents and public distribution of the alleged dataset through the actor's leak portal.

The similarities in the targeted sector, exposed data categories, and publication methodology suggest a consistent operational pattern focused on large-scale document exfiltration and public disclosure. However, as of the date of this report, the complete scope of both incidents and the threat actor's claims have not been independently verified through publicly available forensic evidence.

3.2 Assessed TTPs (MITRE ATT&CK-aligned, moderate confidence)

Tactic	Technique (assessed)
Initial Access	Compromised email account / credential-based access (per Bank of Baroda's own preliminary statement); phishing or credential theft is the leading hypothesis pending confirmation
Collection	Bulk collection of scanned customer onboarding documents and internal branch reporting files
Exfiltration	Large-volume exfiltration (multi-hundred-GB to multi-TB) consistent with mass document-repository access rather than single-database extraction
Impact	Public data leak via Tor-hosted site in lieu of, or in addition to, ransom demand — reputational and downstream-fraud impact rather than operational disruption
Command & Control / Hosting	Tor (.onion) infrastructure for both the leak blog and file hosting

4. Impact Assessment

The exposed document categories — Aadhaar and PAN copies, signatures, photographs, account and loan details — are sufficient to support identity theft, SIM-swap fraud, synthetic identity creation, and highly credible phishing/vishing campaigns against named customers. The presence of internal audit and branch-operations material additionally creates a secondary risk: attackers or fraudsters could use internal terminology, branch codes, and process details to craft more convincing social-engineering attacks against both customers and bank staff.

Risk Area	Assessment
Customer identity theft / fraud	High — government ID numbers, photos, and signatures are present in sampled documents
Account takeover / financial fraud	Medium–High — account numbers, branch details, and NetBanking references are included
Targeted phishing/vishing	High — combination of real names, ID numbers, and bank-specific document language enables convincing pretexting
Regulatory / compliance exposure	High — likely reportable personal-data breach under Indian data-protection and RBI cyber-security reporting obligations
Reputational impact	High — free public release maximises press coverage and customer-facing visibility
Core banking system integrity	Reported unaffected by the bank; unverified by Athenian Tech at time of writing

5. Indicators of Compromise (IOCs)

The following indicators were identified during this engagement and are provided for the bank's internal blocking, monitoring, and takedown-request purposes. Distribution beyond the bank's designated security/legal team is not recommended.

Indicator	Type	Notes
ojcmpbdncjo5dhaxxll44bq6to3kwqtoeraevgsjquhdtt4uv5l4igid.onion	Tor hidden-service domain	site (“Triple X WebBlog”) hosting the claim and sample files
“Triple X WebBlog” / “TripleX”	Actor	Self-identified name used on leak posts across both known incidents
6qqz6m3b6htudohg2mlf5gdcalonxy3sh5g4dix4mpyirjcgelqqufad.onion	Tor hidden-service domain	Leak site used in the prior BNI (Indonesia) incident, May 2026 — same actor brand

Athenian Tech recommends the bank's security and legal teams pursue Tor-hosting-provider abuse reporting, coordinate with CERT-In and RBI on takedown and customer-notification obligations, and preserve the above indicators for law-enforcement referral rather than accessing the leak site directly outside of a controlled forensic environment.

6. Evidence

As part of this assessment, Athenian Tech reviewed the sample documents published by the threat actor to validate the credibility of the alleged breach. The following figures present representative samples from the leak page, illustrating the nature and sensitivity of the information allegedly exposed. These samples are included solely to support the findings of this report and for evidentiary purposes.

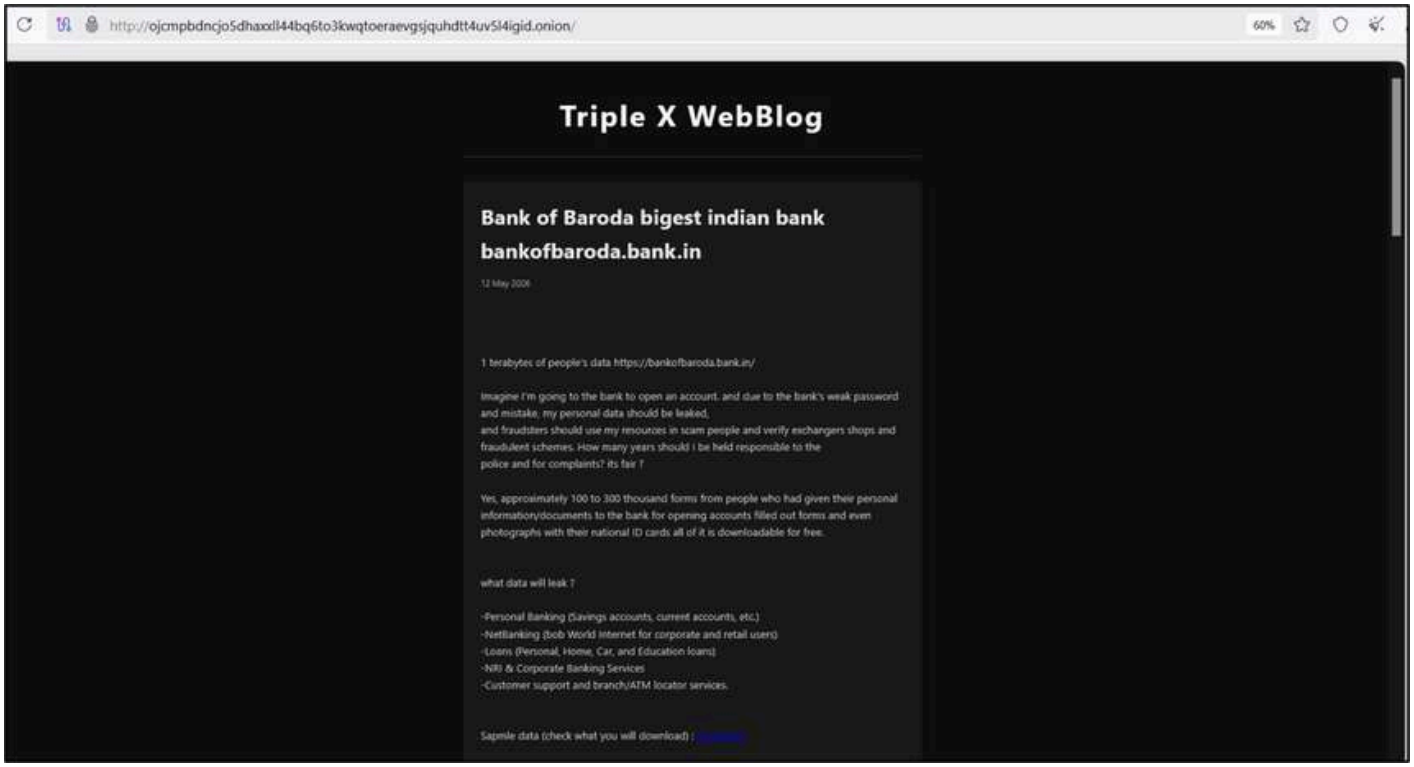

Figure 1: TripleX leak page claiming the compromise of Bank of Baroda and advertising the alleged dataset along with representative sample files.


बैंक ऑफ़ बड़ौदा Bank of Baroda

Certificate No. 35

CERTIFICATE ON MEMORANDUM OF CHANGES (MOCs) NOT ACCEPTED BY THE BANK

Zone : PUNE Region : PANAJI Branch : GOGOL

We have completed the audit of Hinganghat Branch for the year ended 31.03.2026 and issued the audit report dated N.A.. We confirm that there are no Memorandum of Changes (MOCs) which have been recommended by us but have not been accepted by the Branch management except as under **(to be mentioned as nil in case of no such case)**:

1. MOC 14 Not accepted by Bank $ NIL
2. MOC 14D Not accepted by Bank. $ NIL
3. MOC 14R Not accepted by Bank. $ NIL

The impact of such MOCs have not been included in the details stated in para ..... of our Audit report.

Income increased/ decreased* by :
Expenses increased/ decreased* by :
Assets increased/ decreased* by :
Liabilities increased/ decreased* by :

Figure 2: Sample internal Bank of Baroda audit document published by the threat actor, indicating the alleged exposure of internal operational records.

Figure 3: Sample customer KYC/mobile number update application form published by the threat actor, illustrating the alleged exposure of customer onboarding records containing personally identifiable information (PII).

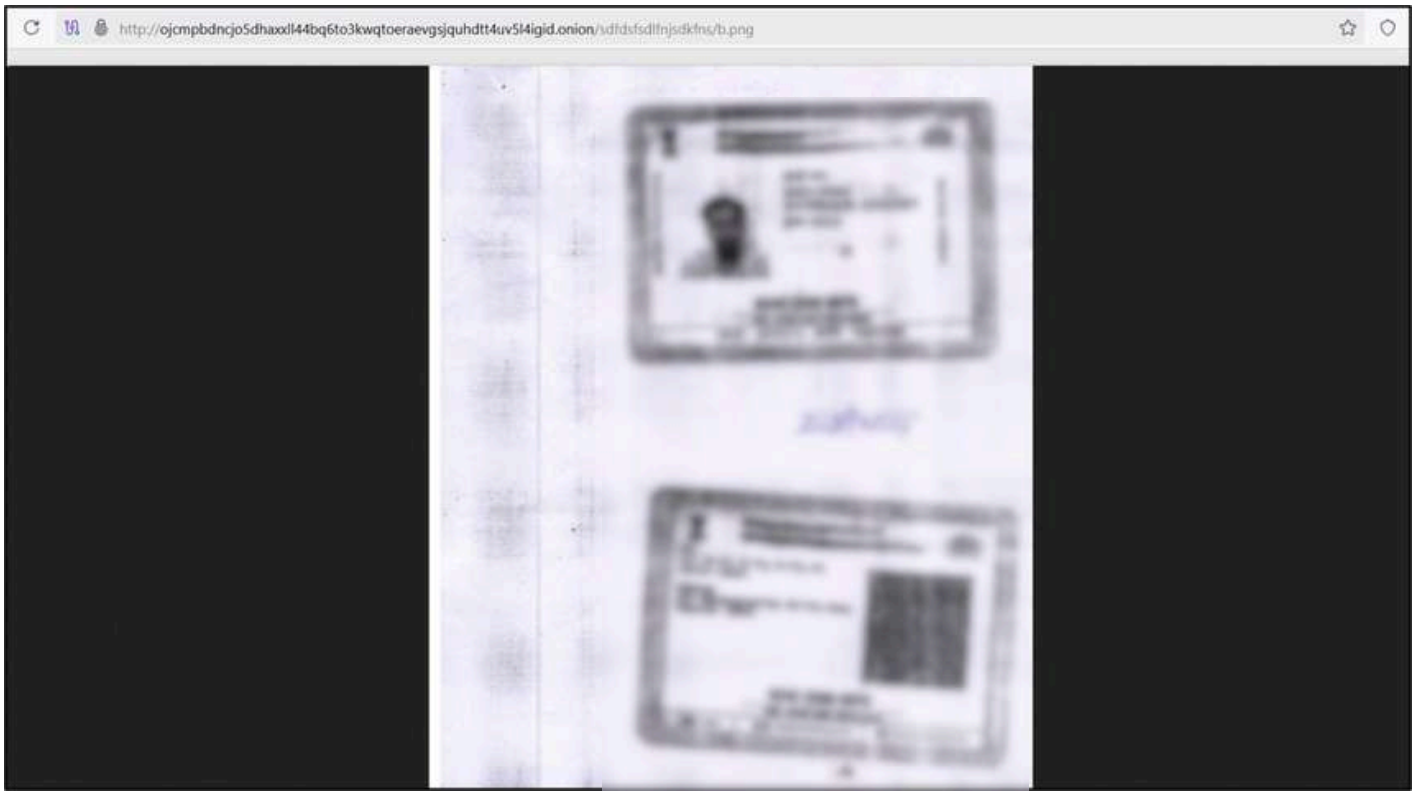

Figure 4: Representative Aadhaar card included within the published sample set, indicating the alleged exposure of government-issued identity documents associated with customer KYC records.

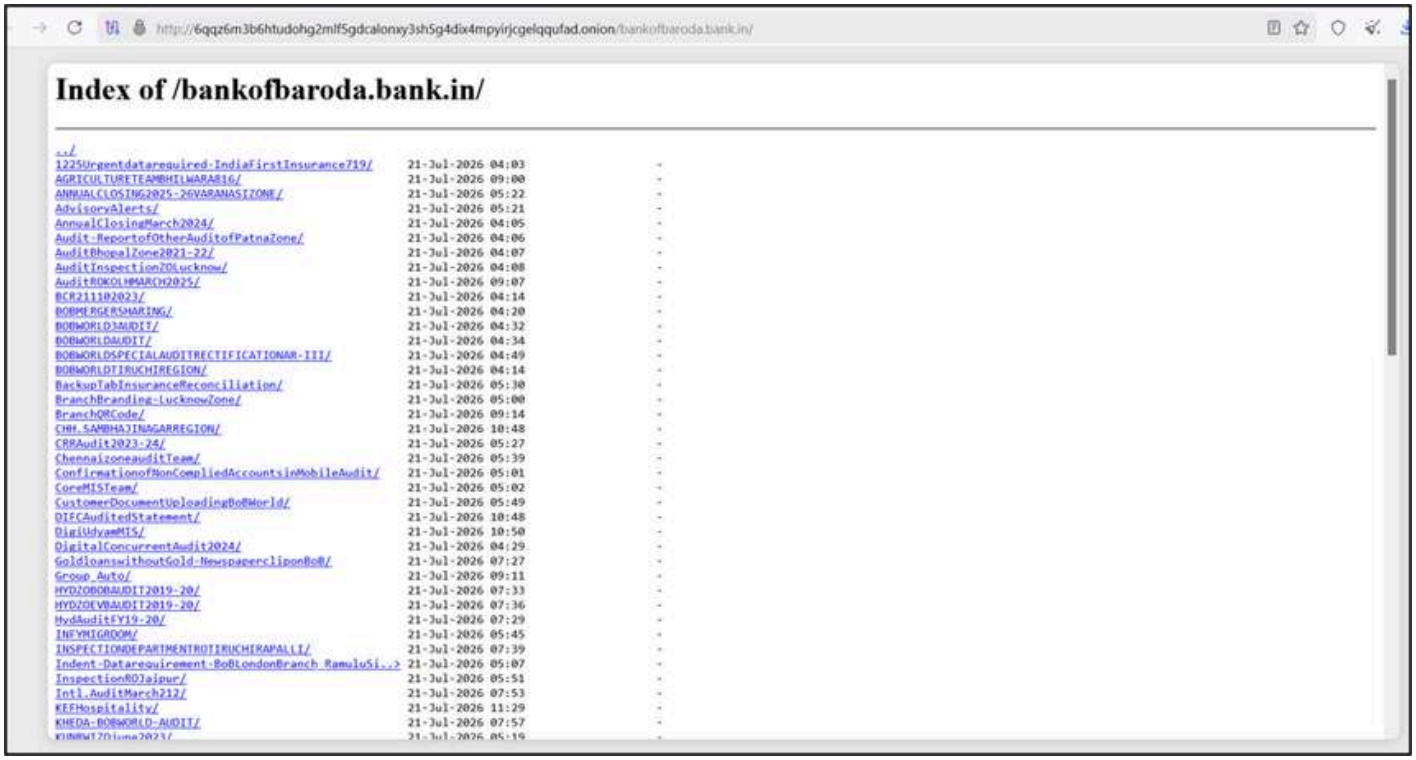

Figure 5: Directory listing published on the threat actor's leak portal, displaying the alleged Bank of Baroda dataset organised into multiple folders corresponding to branch operations, audit records, customer documentation, and internal business functions.

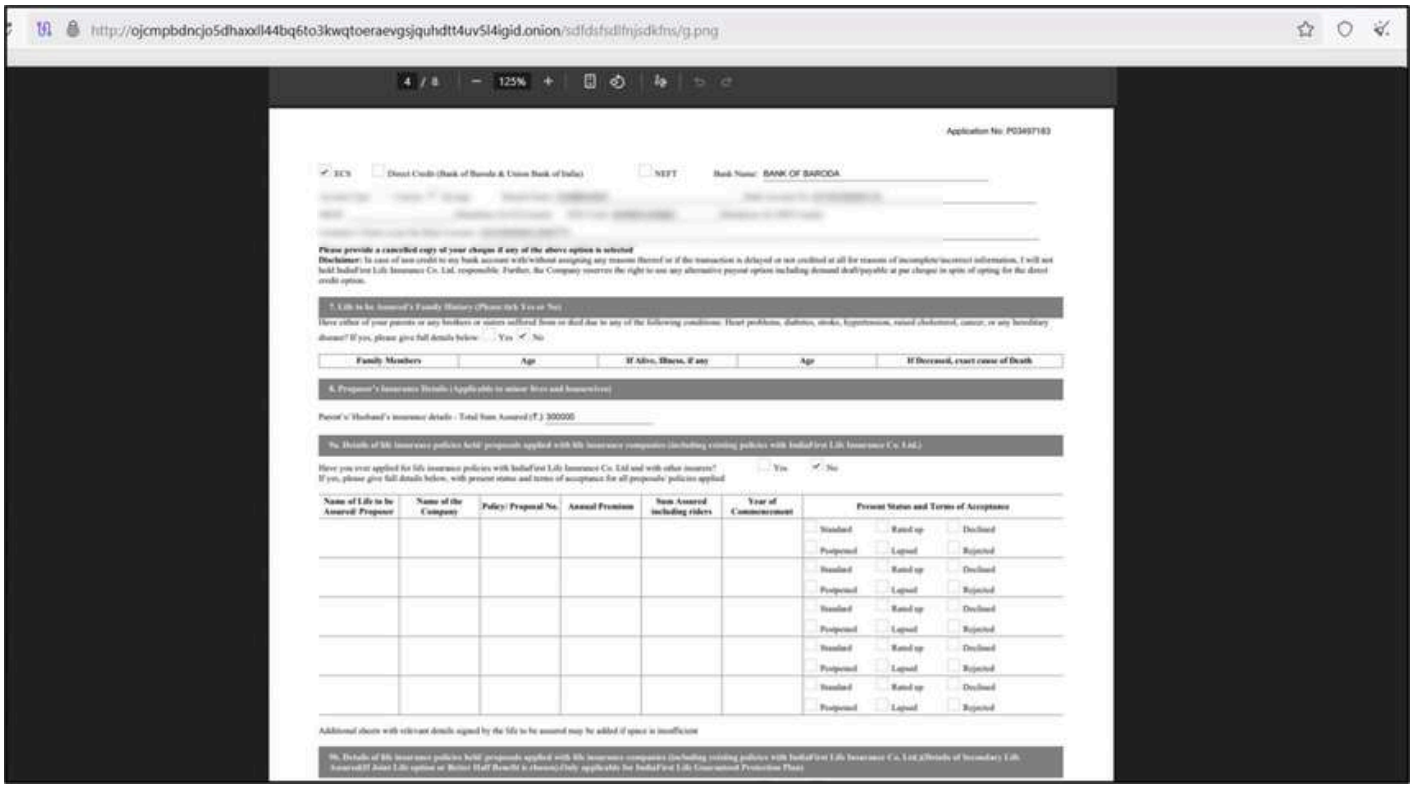

Figure 6: Sample insurance proposal document published by the threat actor, illustrating the alleged exposure of customer insurance records linked to Bank of Baroda accounts.

7. Recommendations

Immediate Actions (0–48 Hours)

- Initiate a comprehensive investigation to determine the scope of the compromise, with particular focus on the affected employee account(s), associated credentials, mailbox rules, OAuth authorisations, and any unauthorised persistence mechanisms.
- Activate the incident response process and coordinate with relevant regulatory authorities, including CERT-In and the Reserve Bank of India (RBI), in accordance with applicable breach notification and reporting requirements.
- Preserve all available forensic evidence and coordinate with law enforcement agencies while pursuing takedown requests for the identified leak infrastructure and associated malicious resources.
- Increase monitoring for indicators of fraudulent activity, including suspicious NetBanking access, SIM-swap attempts, unauthorised account modifications, fraudulent loan applications, and other identity-based financial abuse targeting potentially affected customers.
- Assess the potential exposure of customer and internal data repositories to determine the scale of the incident and identify individuals requiring notification.

Short-Term Actions (1–4 Weeks)

- Conduct a comprehensive forensic investigation of email systems, document repositories, file-sharing platforms, and KYC processing environments to identify the initial intrusion vector, attacker activities, data exfiltration path, and any remaining unauthorized access.
- Review and strengthen access controls for repositories containing customer KYC documents, loan records, audit reports, and other sensitive information by implementing least-privilege access, periodic access reviews, and enhanced monitoring of bulk data exports.
- Expand continuous monitoring of dark web forums, leak portals, underground marketplaces, and other external sources to detect additional releases, redistribution, or commercial sale of the exposed data.
- Review third-party vendor and branch-level access to sensitive customer information and verify compliance with the organisation’s security policies and contractual obligations.

Medium-Term Actions (1–3 Months)

- Enforce Multi-Factor Authentication (MFA) and Conditional Access policies across all enterprise email accounts, document management platforms, remote access services, and other business-critical systems.
- Strengthen Data Loss Prevention (DLP) controls, user activity monitoring, and alerting mechanisms to identify unauthorized bulk access, abnormal downloads, and large-scale data exfiltration attempts.
- Review data retention policies for customer onboarding documents, KYC records, and supporting identity documentation to minimize long-term exposure of highly sensitive personal information.
- Conduct an enterprise-wide security assessment covering identity management, email security, privileged access, and document management systems to identify and remediate similar attack vectors.
- Perform regular incident response exercises and tabletop simulations based on this attack scenario to evaluate organizational preparedness, improve cross-functional coordination, and strengthen the institution's ability to respond effectively to future data breach incidents.

ATHENIAN TECH

Contact Us

www.atheniantech.com