INDIA BFSI

Threat Landscape Report

SOCRadar®
Your Eyes Beyond

socradar.io

Executive Summary

Top Takeaways

- The BFSI sector experienced the highest volume of dark web threats among all industries, accounting for 14.49% of the total, making it the most targeted sector.
- Within the BFSI sector, 66.02% of dark web threats were directed at the broader Finance and Insurance category, showing how threat actors continue to focus on traditional financial systems.
- 53.50% of dark web threats specifically targeted Indian entities, while the remaining 46.50% included India along with other countries, highlighting India's high exposure.
- Among dark web threat categories, 52.10% involved data being shared openly, signaling a serious risk of sensitive information being exposed without direct sale or ransom.
- Threat types showed a clear focus on data, with 77.00% of the threats involving stolen or leaked databases, making data protection a top priority.
- 96.60% of ransomware attacks were aimed directly at Indian organizations, indicating that India is a primary focus for ransomware groups.
- The ransomware group KillSec led the list of attackers targeting India, responsible for 15.83% of observed incidents.
- In phishing activity, the BFSI sector once again topped the list with 29.83% of total phishing attacks across all industries.
- Banking alone accounted for 20.87% of phishing attacks within the BFSI sector, making it the most targeted sub-industry.
- "Webmail Login" was the most commonly used phishing page title, seen in 20.22% of phishing incidents, showing that attackers often mimic email login pages to steal credentials.
- Surprisingly, 62% of phishing attacks used HTTPS, proving that secure-looking links can still lead to malicious content.

Technical Details

This report based on data collected between July 2024 and July 2025

In the following chapters, you will be reading about the various aspects of the cyber threat landscape around the Banking, financial services and insurance (BFSI) industry.

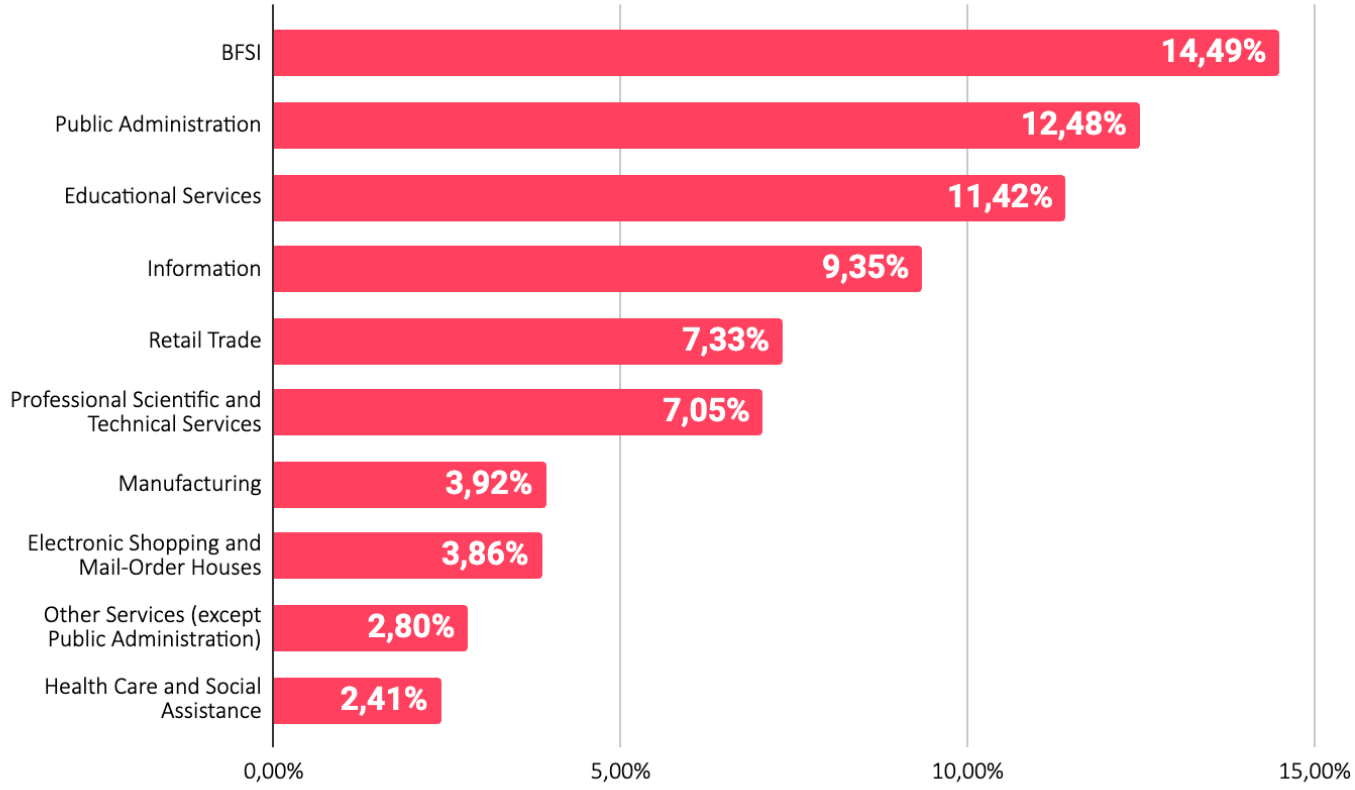
In the Dark Web Threats chapter, we will be covering the news and developments from Dark Web Forums, Telegram channels, Discord groups and so on. These are areas where threat actors with various skill sets come together, discuss, share tools and publish their alleged cyber attacks.

In the Ransomware Threats chapter you will find information and data about ransomware threats targeting the Indian BFSI industry.

The Phishing Threats chapter will show you how threat actors target various organizations with fake websites. By examining the data here, you can take the necessary steps to prevent your employees from falling into threat actors' traps.

Dark Web Threats

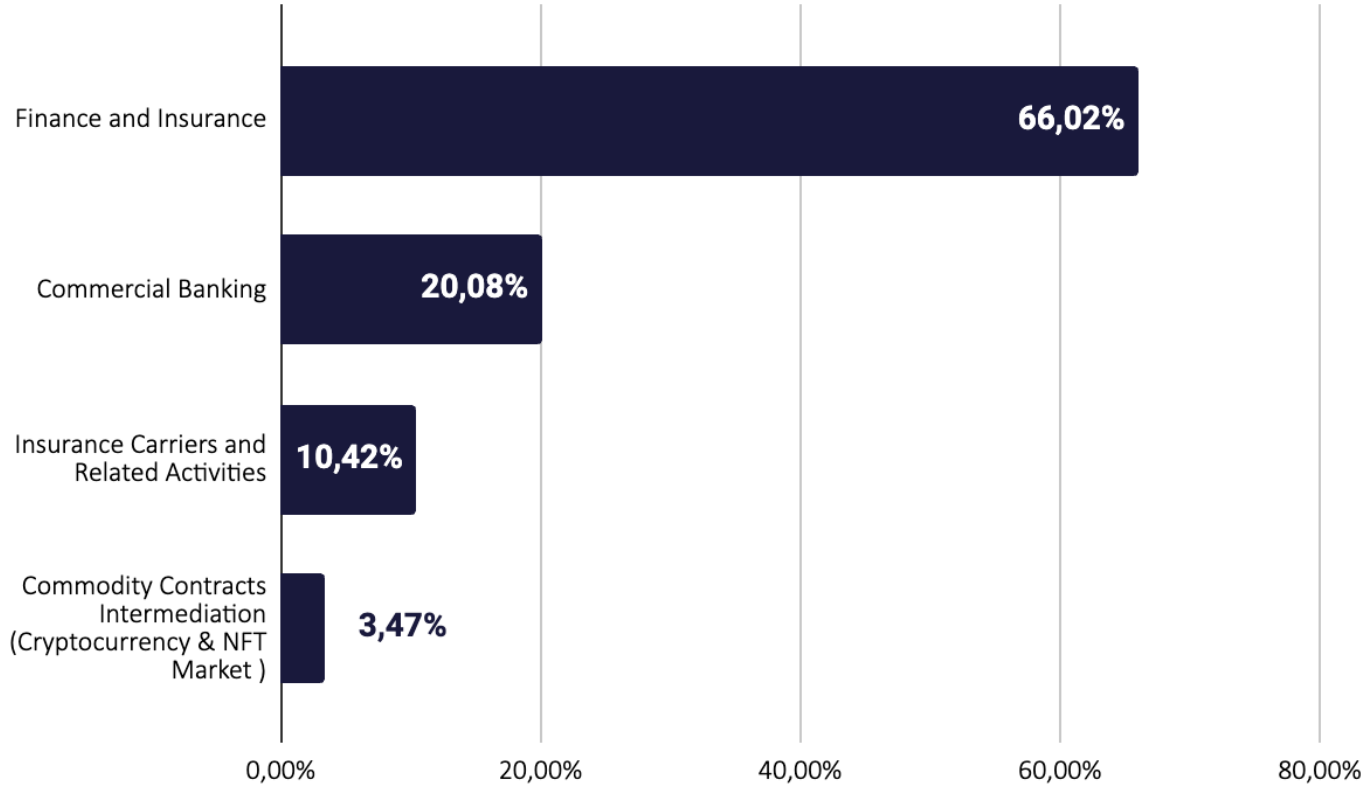
Distribution of Dark Web Threats by Industry



When combined, the BFSI sector leads with 14.49% of all observed threats, making it the top target. Public Administration follows at 12.48%, while Educational Services comes in third at 11.42%. These three sectors face the highest risk levels.

The pattern in the graph suggests threat actors focus more on industries that handle sensitive data.

Distribution of Dark Web Threats by Sub-Industry

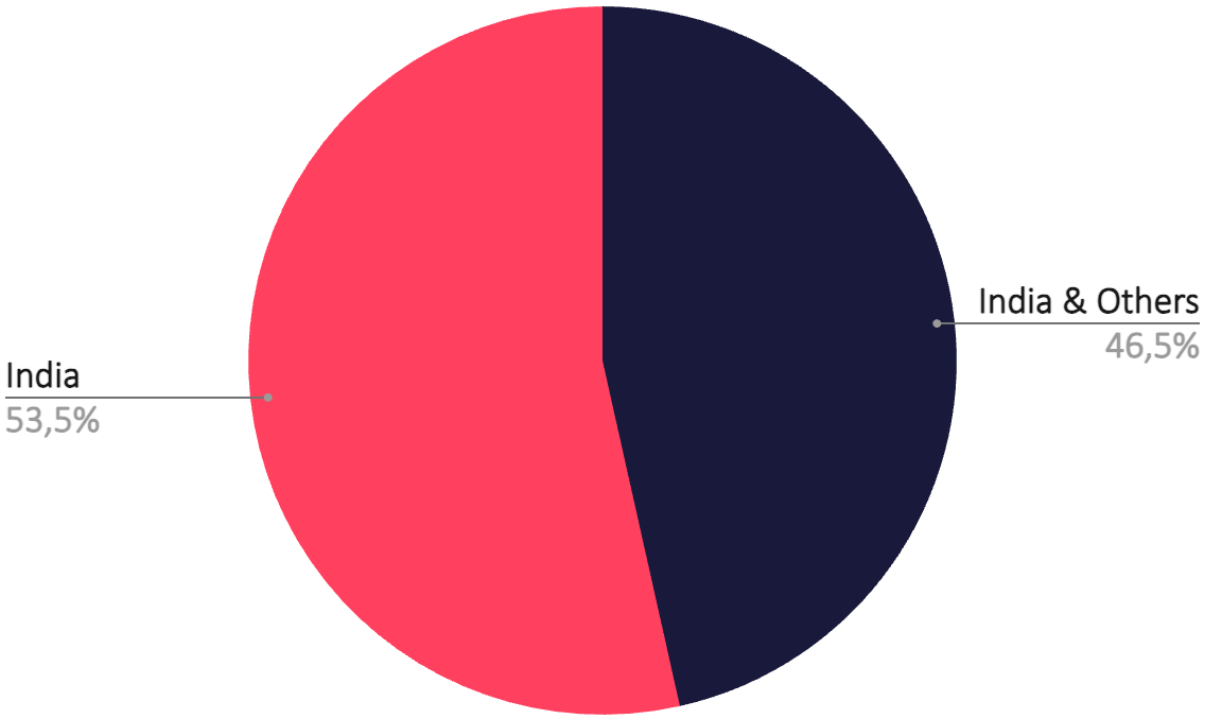


The chart shows the distribution of dark web threats within the BFSI sub-industries.

The Finance and Insurance sector makes up the majority, with 66.02% of threats. Commercial Banking follows with 20.08%, highlighting its position as a major target for cybercriminals. Insurance Carriers and Related Activities face 10.42% of threats, while the emerging area of Commodity Contracts Intermediation, which includes cryptocurrency and NFT markets, accounts for 3.47%.

This data shows that traditional financial institutions still face the most risk, but threat actors also target newer financial technologies.

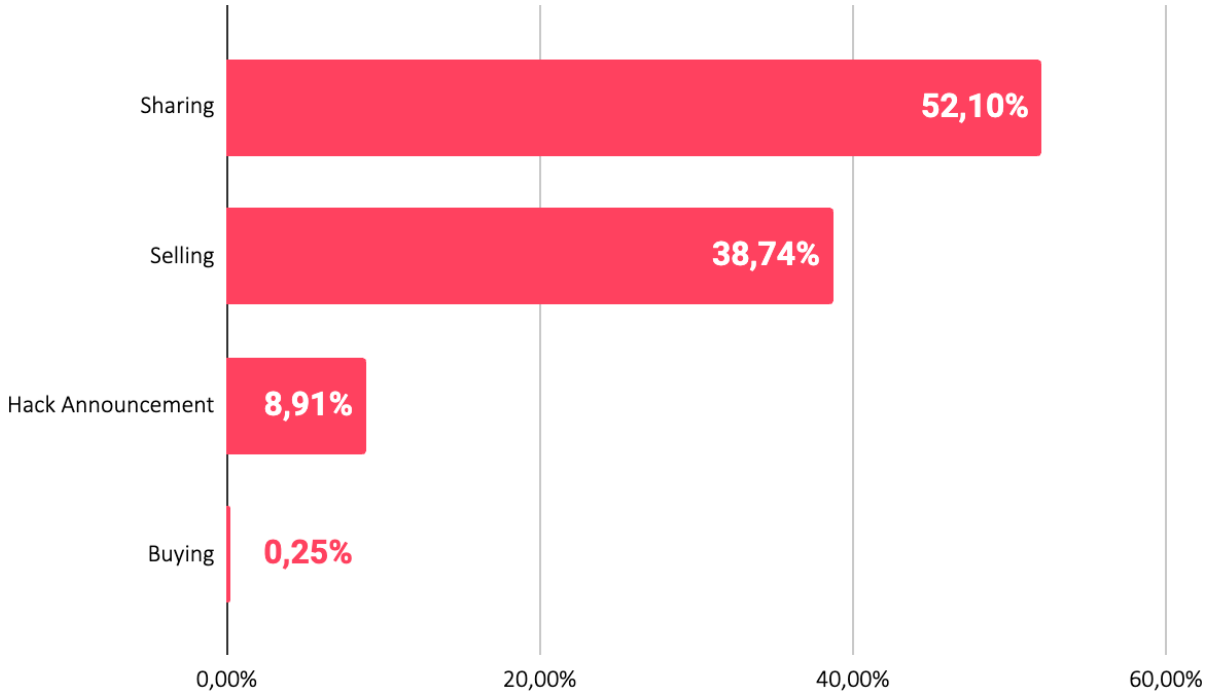
Distribution of Dark Web Threats by Country



The chart shows the split of dark web threats targeting the Indian BFSI sector by country. India alone accounts for 53.50% of all threats, while the remaining 46.50% target India along with other countries. This means more than half of the threats are specifically aimed at Indian entities, highlighting their high exposure.

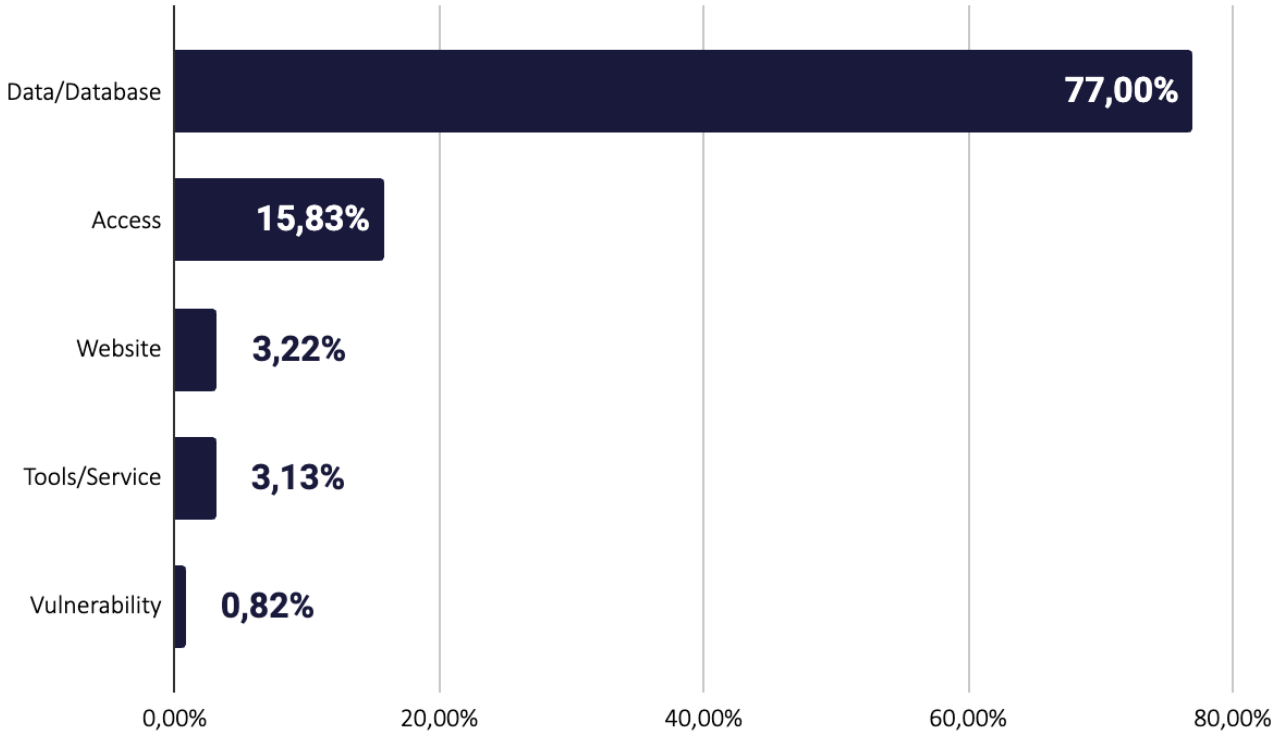
The data shows that attackers often focus on Indian organizations directly, not just as part of wider campaigns.

Distribution of Dark Web Threats by Threat Categories



Most of the threats fall under “Sharing” at 52.10%, where actors leak or expose sensitive data. “Selling” comes next with 38.74%, indicating a large market for stolen information. “Hack Announcements” make up 8.91%, where attackers claim responsibility or showcase breaches. “Buying” is the least common at only 0.25%.

Distribution of Dark Web Threats by Threat Types

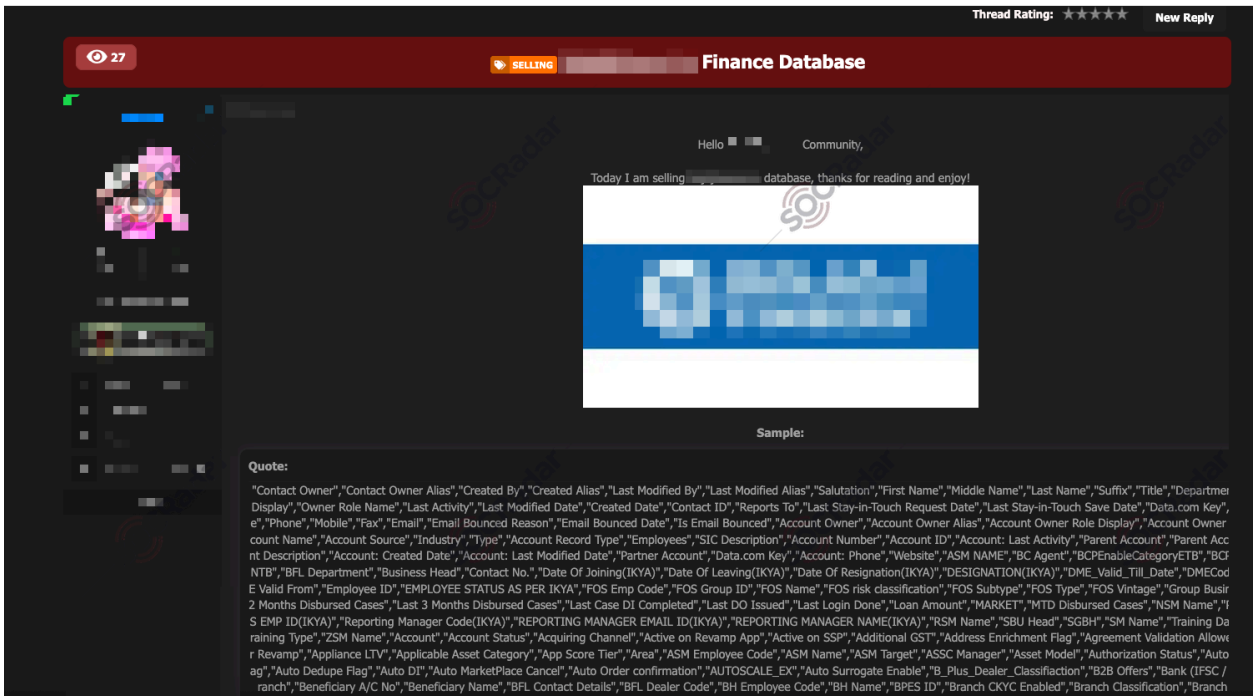


"Data/Database" threats dominate with 77.00%, showing that exposed or stolen data is the main concern. "Access" threats follow at 15.83%, where actors offer or seek unauthorized entry to systems. "Website" and "Tools/Service" threats are much lower at 3.22% and 3.13%, while "Vulnerability" listings make up just 0.82%.

This pattern shows attackers mainly target data for leaks or sales.

Recent Dark Web Activities Targeting the BFSI Industry

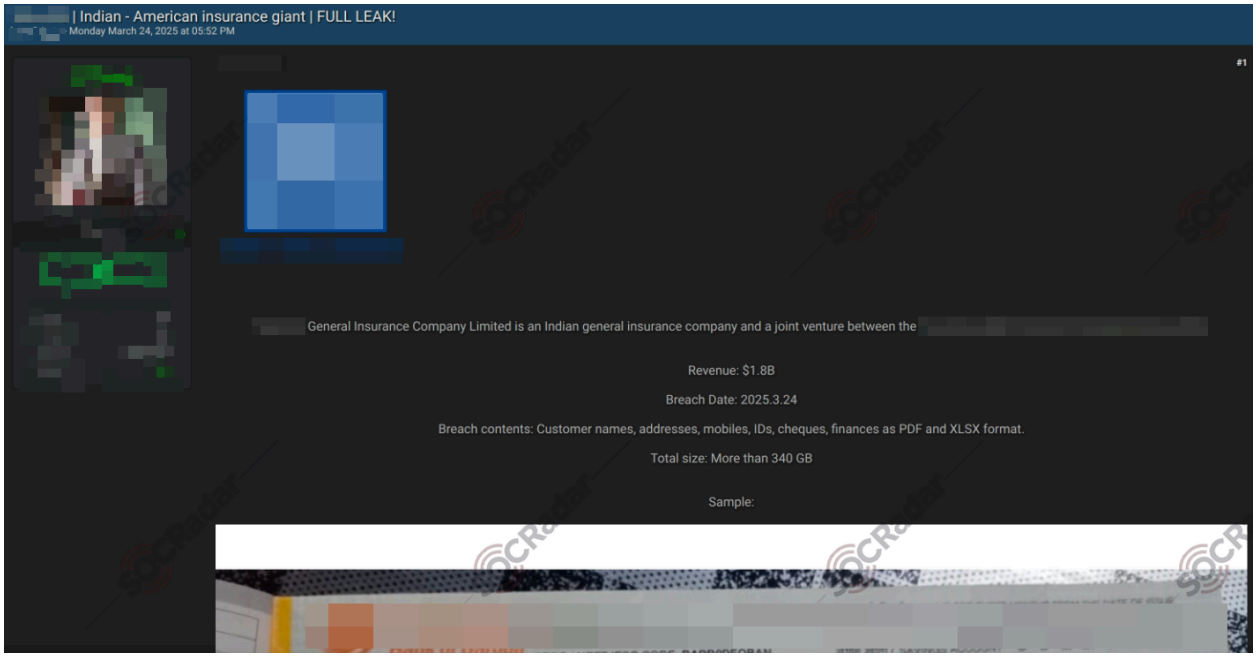
Threat Actor Claims to Sell Database of Major Indian Financial Services Firm



A threat actor has claimed to be selling a database allegedly belonging to a leading Indian financial services company on a known Dark Web forum. The firm operates in the non-banking financial sector and provides lending, insurance, and investment products across India.

The post, shared by the threat actor on the forum, includes a sample dataset with extensive fields related to employee records, account information, contact details, business operations, and even internal identifiers. Sensitive data such as email addresses, phone numbers, business roles, training details, and financial transaction records are part of the leaked structure.

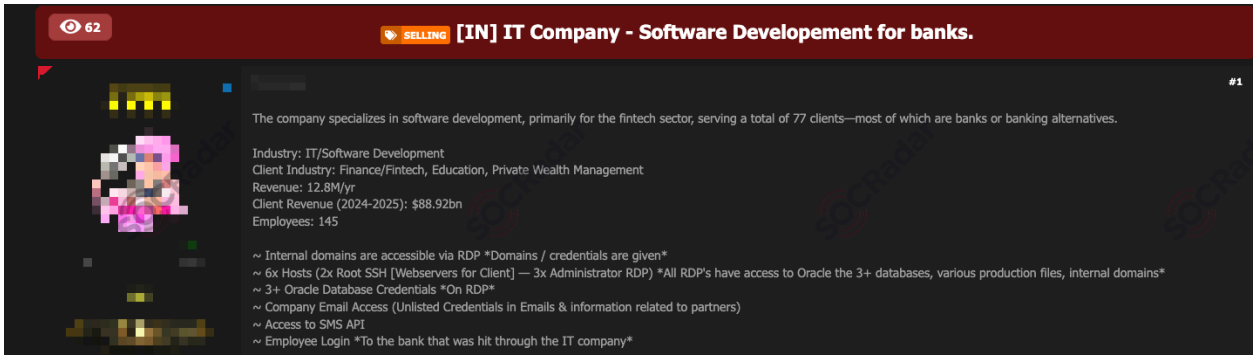
Massive Data Breach Allegedly Hits Leading Indian Insurance Firm



A threat actor on a known Dark Web forum has claimed to be selling a large dataset allegedly stolen from a major Indian general insurance company. The firm, part of a joint venture with a global insurance group, is a key player in India's insurance sector with reported revenues of $1.8 billion.

The breach involves over 340 GB of data. According to the post, the leak includes highly sensitive customer information such as names, addresses, mobile numbers, identity documents, cheque details, and financial records. A sample shared by the actor features 10,000 PDF files, suggesting a wide-scale compromise of customer records.

Threat Actor Offers Network Access to Indian Fintech Software Vendor on Dark Web

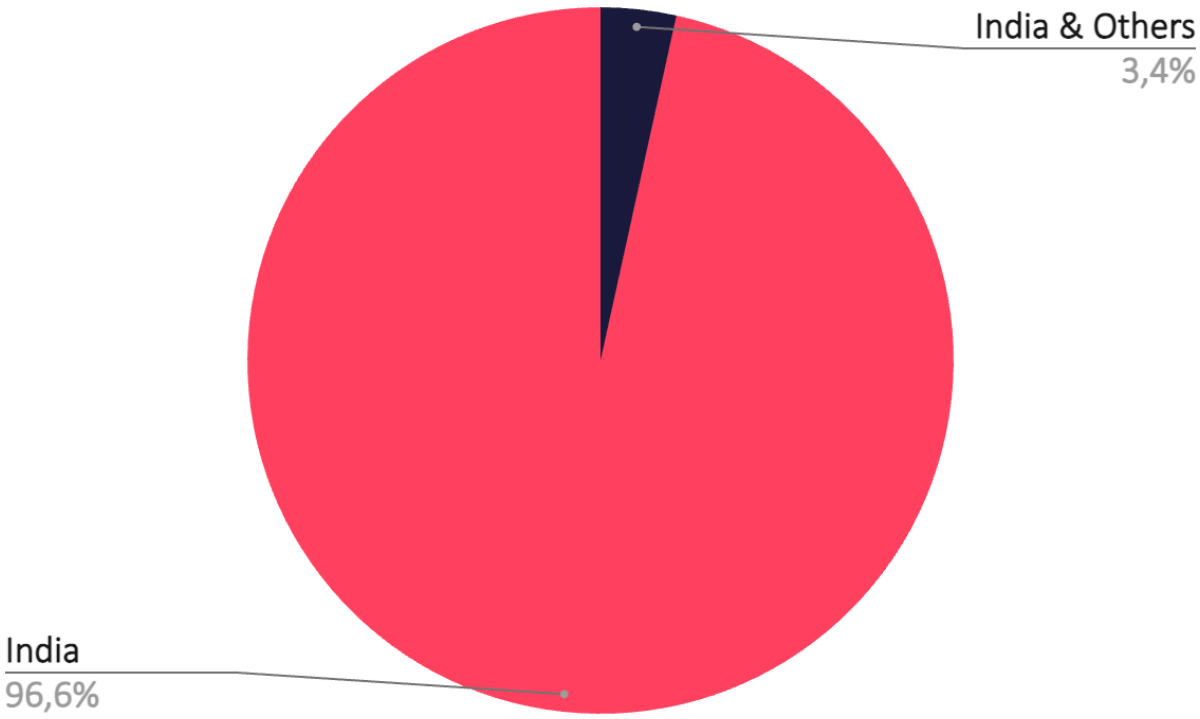


A listing on a Dark Web forum monitored by SOCRadar advertises unauthorized network access allegedly belonging to an Indian software development company. The firm operates in the IT and software services industry and focuses on building solutions for the fintech sector. It currently serves 77 clients, most of which include banks, financial institutions, and private wealth firms. The company's annual revenue stands at $12.8 million, while its client network reportedly generates nearly $88.92 billion in combined revenue.

According to the threat actor’s post, the access includes administrator-level RDP to multiple systems, root SSH access to web servers, and credentials for three or more Oracle databases. Also exposed are internal domains, company emails, and SMS API access. Notably, the listing claims to offer login access to a banking client via employee credentials, suggesting possible lateral movement within a larger financial network.

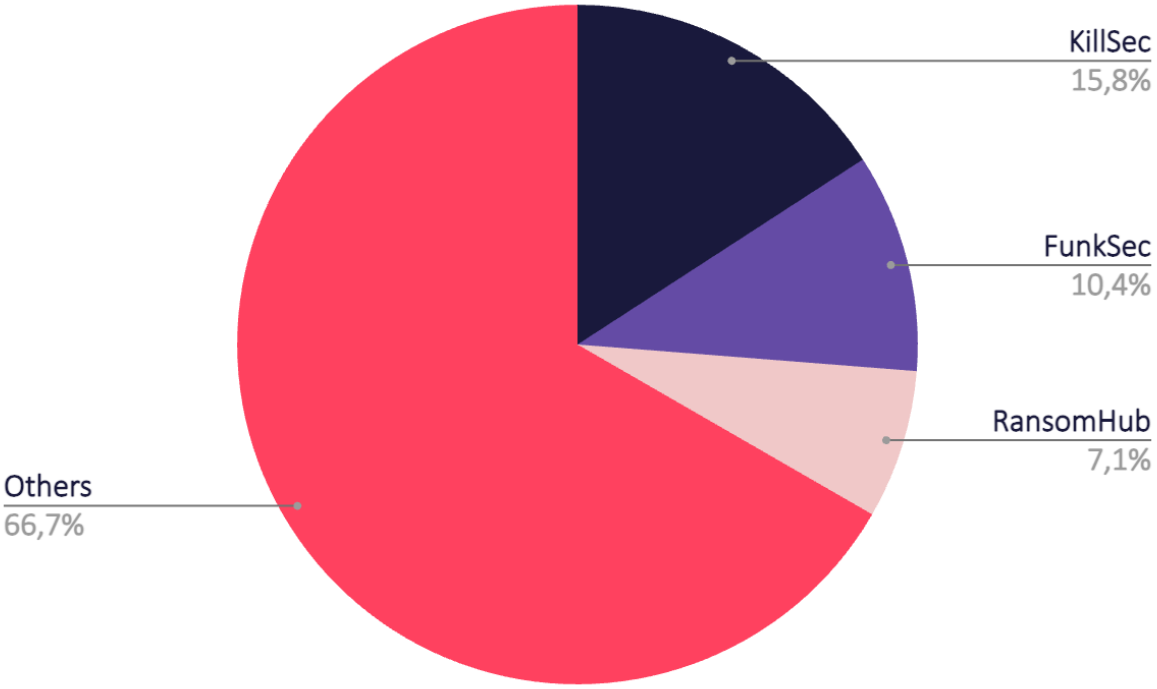
Ransomware Threats

Distribution of Ransomware Attacks by Target Country



The chart shows the split of ransomware threats targeting the Indian BFSI sector by country. A large majority of these attacks specifically target India. Only 3.40% involve India along with other countries. This highlights India as a prime focus for ransomware groups.

Top Ransomware Groups Targeting India



KillSec leads with 15.83% of known attacks, followed by FunkSec at 10.42%, and RansomHub at 7.08%.

Together, these three account for about one-third of all attacks. The remaining 66.67% come from various other groups, showing a wide range of active threat actors.

A Closer Look into The Top 3 Ransomware Groups

KillSec

KillSec is a highly active entity known for its involvement in ransomware attacks and data breaches. First identified in October 2023, this actor has steadily increased its presence by targeting organizations across sectors.

KillSec exhibits a strong focus on India, with 29.55% of its alleged attacks targeting organizations in the country. Regarding industries, KillSec has shown a distinct focus on targeting key sectors, with healthcare being its primary target, comprising 20.45% of its alleged attacks.

You can visit our ***blog post*** for more detailed information about KillSec.

FunkSec

FunkSec, a new ransomware group, emerged in December 2024 and claimed responsibility for attacks on multiple victims. By the time of writing the number of victims reached 129. The group appears to be involved in both hacktivism and ransomware, with members likely inexperienced and seeking recognition.

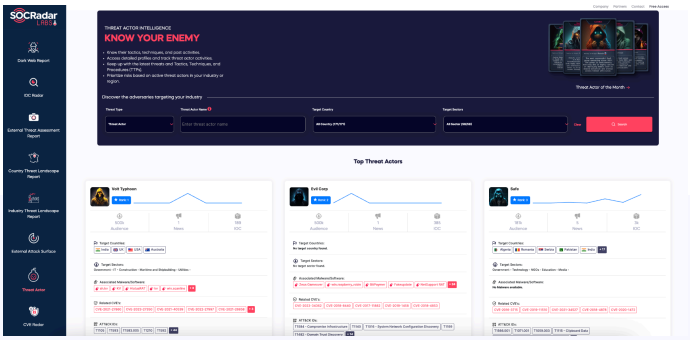
Researchers suggest that the file-encrypting malware, written in Rust, was likely developed by an inexperienced malware creator from Algeria with the assistance of AI. The developer also uploaded parts of the ransomware's source code online. Operating under the Ransomware-as-a-Service (RaaS) model, FunkSec engages in double extortion, threatening to release stolen data to coerce victims into paying the ransom.

You can visit our ***blog post*** to read the rest of the threat actor profile.

RansomHub

As stated on the group's About page, RansomHub is comprised of hackers from various locations united by a common goal of financial gain. The gang's website states that they refrain from targeting CIS, Cuba, North Korea, and China. While they suggest a global hacker community, their operations notably resemble a traditional Russian ransomware setup. In February 2024, RansomHub posted its first victim, the Brazilian company YKP.

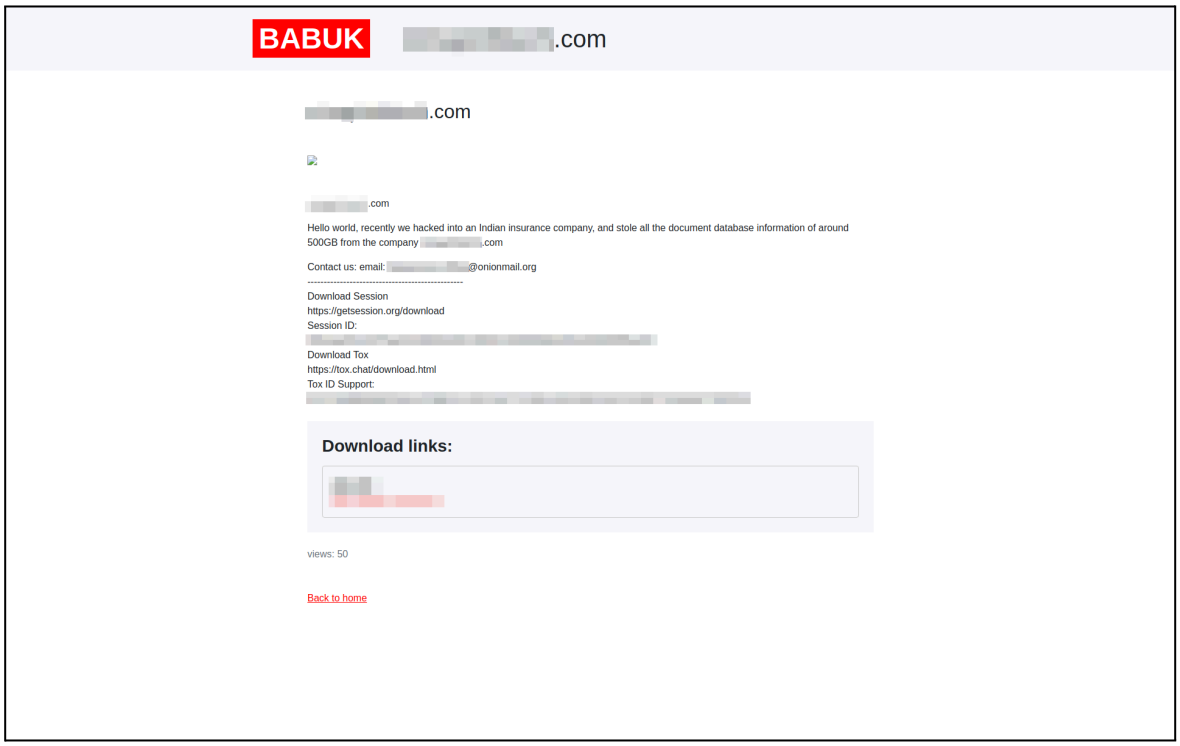
You can visit our ***blog post*** for more detailed information about RansomHub.



*Get actionable intelligence on APT groups, ransomware operators, and other threat actors targeting your industry. Turn threat data into proactive defense with SOCRadar's **Threat Actor Intelligence** module.*

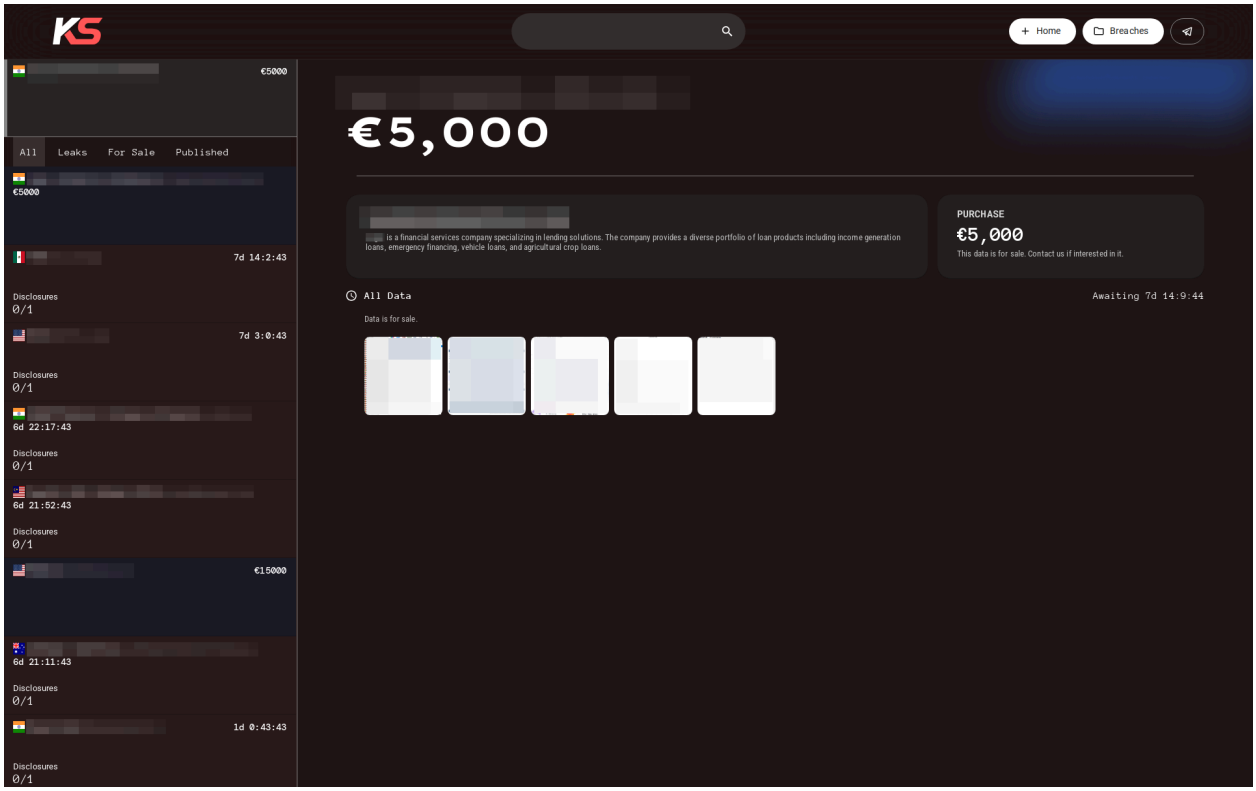
Recent Ransomware Attacks Targeting Entities in India

Babuk2 Ransomware Group Claims Indian Insurance Technology Firm as Victim



The Babuk ransomware group has listed a new alleged victim on its leak site. The company is linked to the insurance sector in India.

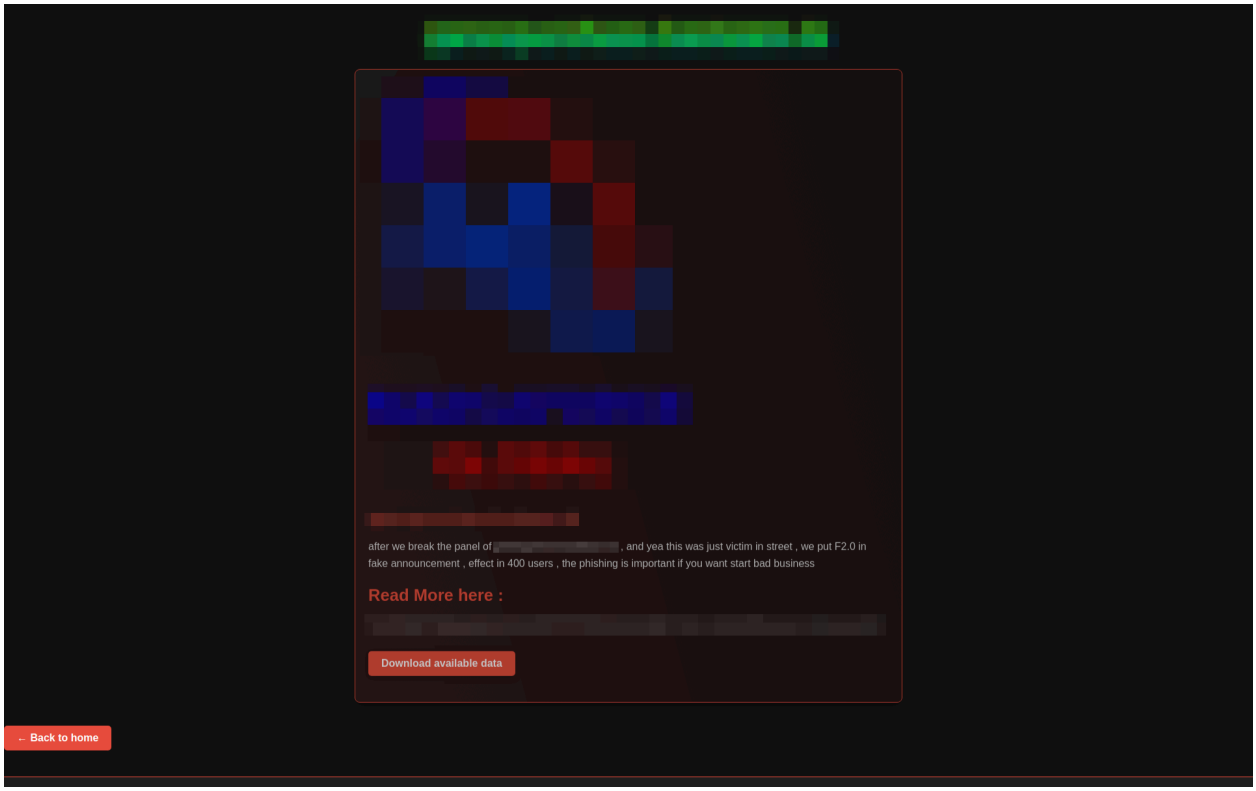
KillSec Ransomware Group Claims Financial Services Firm as a Victim



The KillSec ransomware group has listed a financial services company as its victim on its leak site.

The company is an Indian financial services firm known for offering a wide range of lending products, including income generation loans, emergency funding, vehicle financing, and agricultural crop loans. The company serves a broad customer base across both urban and rural markets.

FunkSec Ransomware Group Claims ATM Services Platform as a Victim

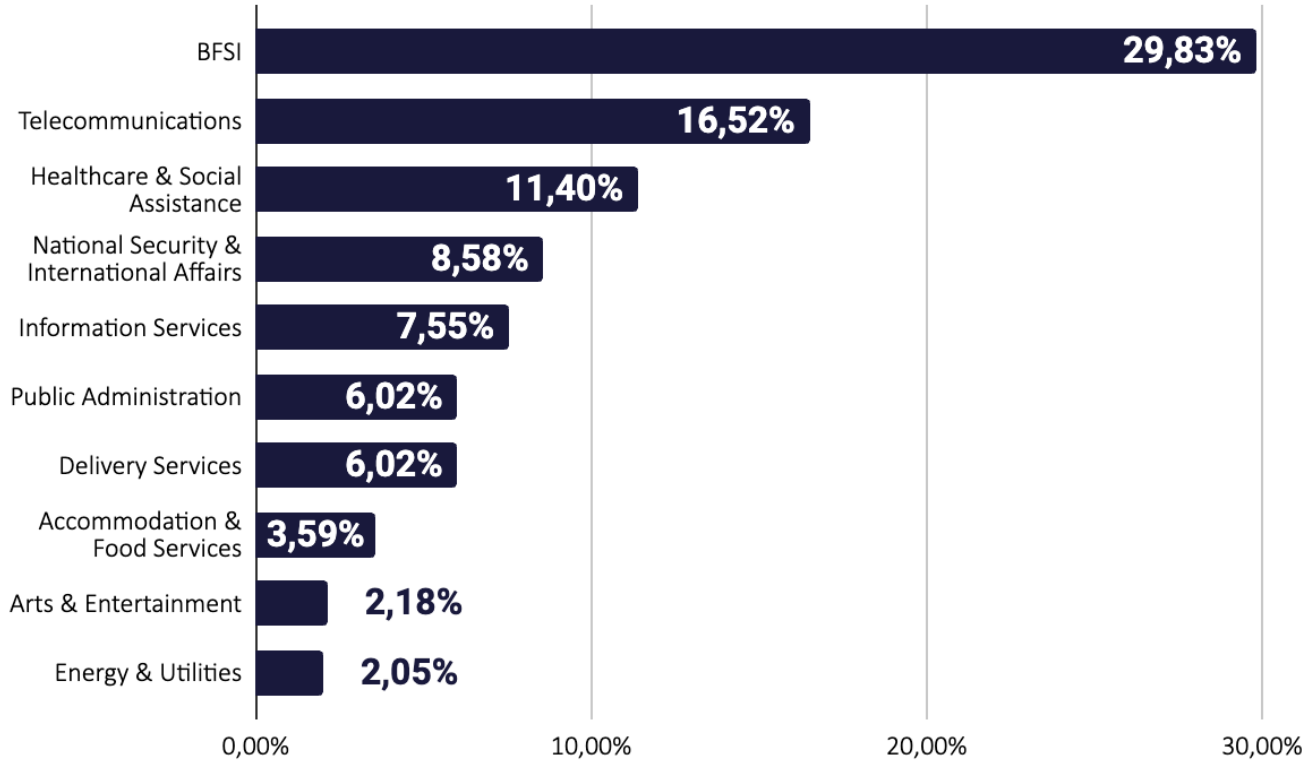


The FunkSec ransomware group has allegedly listed an ATM company as its victim.

The company operates in the banking and financial sector, providing services related to ATM procurement, management, or support for banks and financial institutions.

Phishing Threats Targeting India

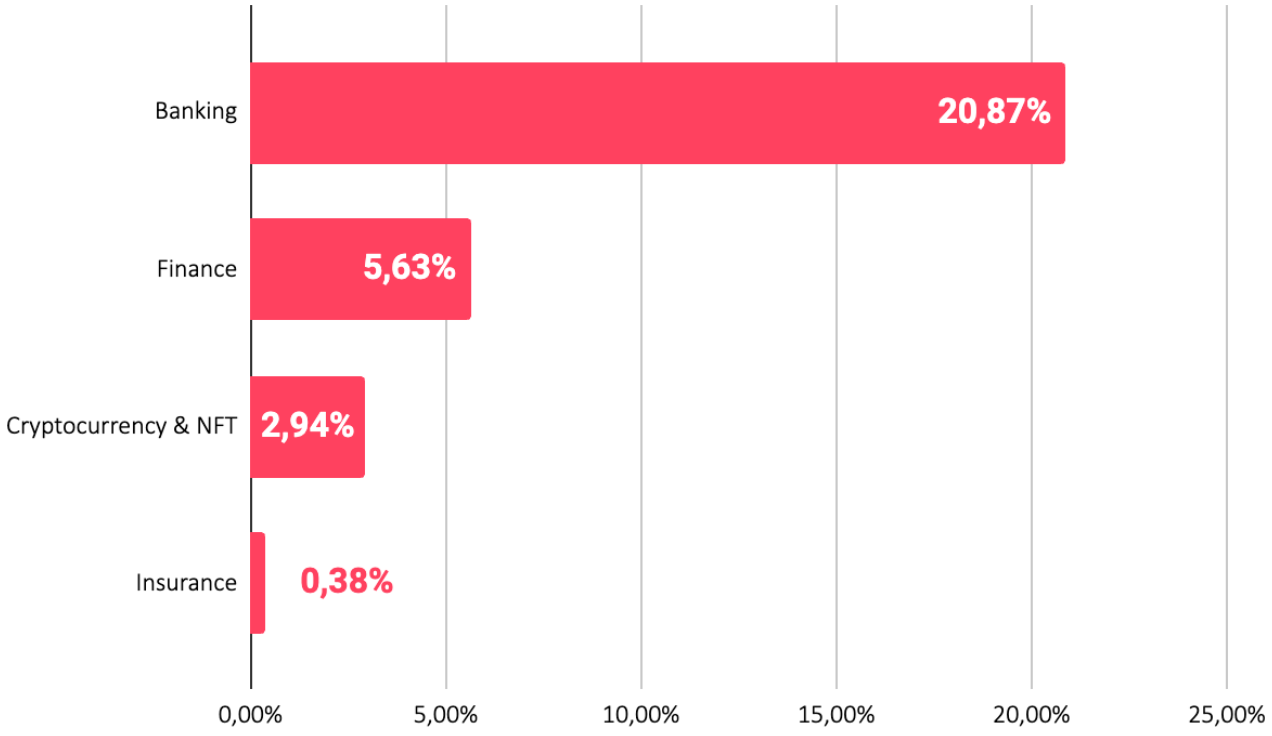
Distribution of Phishing Attacks by Industry



The BFSI sector faces the highest number, with 29.83% of all attacks. Telecommunications comes next at 16.52%, followed by Healthcare at 11.40%.

National Security, Information Services, and Public Administration also appear as key targets.

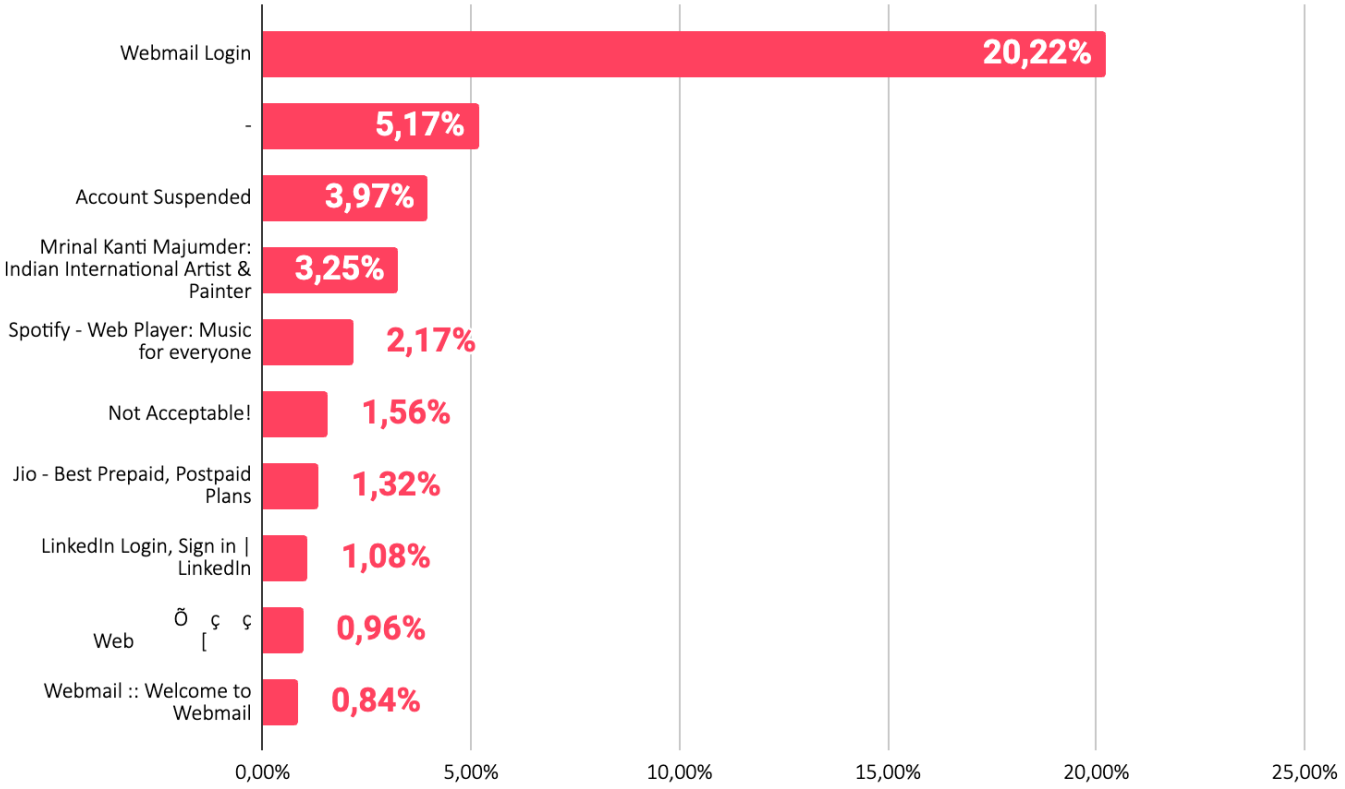
Distribution of Phishing Attacks by Sub-Industry



The chart shows phishing attacks by sub-industry within the BFSI sector. Banking is the main target, with 20.87% of attacks. Finance follows at 5.63%, while Cryptocurrency & NFT accounts for 2.94%. Insurance sees the fewest attacks at 0.38%.

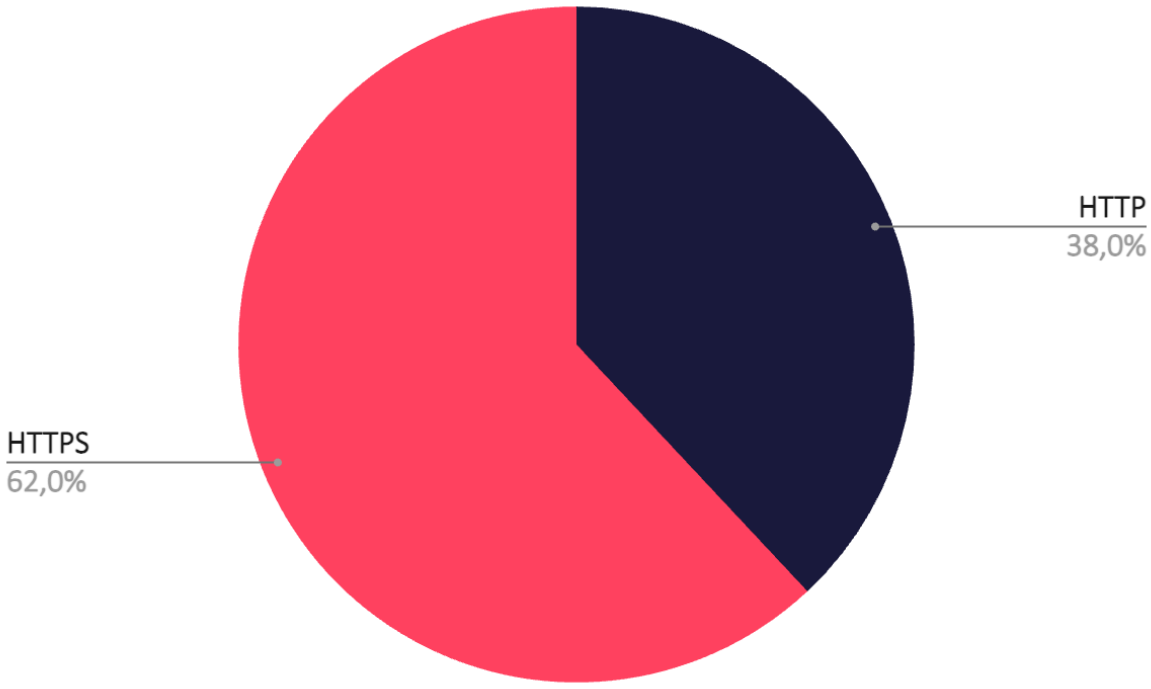
This shows that cybercriminals focus heavily on banks, likely due to direct access to funds and customer data.

Distribution of Phishing Attacks by Phishing Page Title



The chart shows phishing attacks based on fake page titles. “Webmail Login” is the most common, used in 20.22% of attacks. This suggests attackers often mimic email login pages to steal credentials. A large portion (5.17%) has no clear title, likely indicating poorly designed or hidden pages. Some attacks use known brands or personal names, such as Spotify (2.17%), LinkedIn (1.08%), and Jio (1.32%), to trick users.

Distribution of Phishing Attacks by SSL/TLS Protocol



The chart shows the use of SSL/TLS protocols in phishing attacks. Most phishing pages (62%) use HTTPS, while the rest (38%) use HTTP. This proves that a secure-looking URL does not mean the site is safe.

Attackers now use HTTPS to make fake pages appear trustworthy and avoid browser warnings. Users often assume HTTPS means a site is legitimate, which increases the risk.

Strategic Recommendations

- Enhance Endpoint Security: Implement advanced anti-malware, regular device audits, and employee training on safe browsing practices.
- Strengthen Phishing Defense: Invest in phishing detection systems, web filtering tools, and employee training on recognizing phishing attempts.
- Enforce Multi-Factor Authentication (MFA): Apply MFA across critical systems to protect against stolen credentials.
- Fortify Ransomware Defenses: Regularly back up data, segment networks, and develop incident response plans for ransomware attacks.
- Monitor Dark Web Activity: Use dark web monitoring to detect exposed company data early and respond quickly to breaches.
- Collaborate on Cyber Threat Intelligence: Share insights with industry peers and stay informed about emerging threats and new attack vectors.
- Secure Communications and Data: Ensure encryption for sensitive communications and transactions, and train employees on secure data handling.
- Proactive Vulnerability Management: Regularly apply patches and conduct penetration testing to address potential system vulnerabilities.
- Build a Cybersecurity Culture: Foster ongoing employee training, phishing simulations, and establish clear security policies to ensure a security-first mindset across the organization.

Who is SOCRadar?

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Trusted by
21.000+ companies
in 150+ countries

Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS FOR FREE

START YOUR FREE TRIAL

Discover SOCRadar's powerful tools and easy-to-use interface to enhance cyber threat intelligence efforts. Schedule a demo with our experts to see it in action, and we'll show you what SOCRadar can do.