Global Banking & Finance threats facing customers

Authors: Hansika Saxena and Benila Susan Jacob
Co-Author: Anshuman Das
Threat Research and Information Analytics Division (TRIAD)

White papers and reports can be downloaded from CloudSEK website by visiting https://cloudsek.com/whitepapers_reports or by mailing to info@cloudsek.com.

Table of Contents

Overview:

BFSI the Most Targeted Sector in FY 2021—2022

The Banking Finance Services and Insurances (BFSI) industry is critical to a country's economic growth because it contributes significantly to capital formation, industrial development, job creation, and financial strength. The banking industry is in much better shape since the financial crisis of 2008. However, the recent Russia-Ukraine war has dealt a serious blow to this industry. Studies suggest that the war could **cost the global economy 1% of its GDP growth in 2022 and 0.2% in 2023**. And global inflation is expected to be 2-3% higher than predicted before the war.

Despite the ups and downs in the sector, it continues to be the most lucrative sector for threat actors. XVigil data shows that ~10% of the recorded cyber incidents in the financial year 2021–22 (April 2021 to March 2022) were aimed at the BFSI sector, making it the most targeted industry. Two major paradigm shifts are responsible for accelerating this threat:

- The expansion of the ever-evolving threat landscape assisted by the growing digital transformation witnessed in the COVID era.
- The emergence of specialized threat actors, such as state-sponsored cyber criminals, as well as individual actors.

In this report, we have corroborated the data from Xvigil and other sources to provide an in-depth overview on:

- Common Attack Vectors used to target the BFSI sector
- Improvised TTPs evolved over the years
- Major Threat Actors targeting the industry
- Regions and Countries with the maximum recorded incidents
- Long term impacts and mitigation measures for the same

Schedule a CloudSEK demo

At CloudSEK, we predict cyber threats.

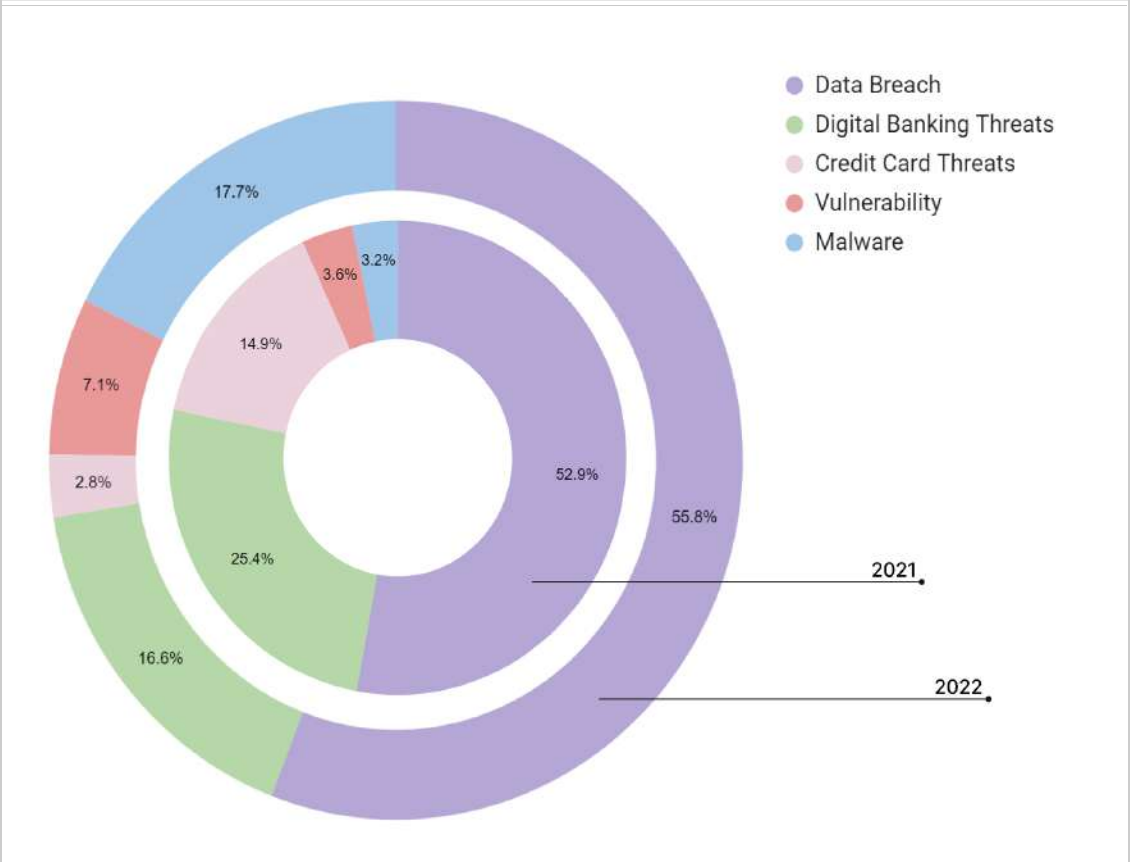
Our solutions have relevant use cases for several industries including BFSI. At CloudSEK, we combine the power of Cyber Intelligence, Brand Monitoring, Attack Surface monitoring, Infrastructure Monitoring and Supply chain to give visibility and context to our customer's Initial Attack Vectors.

Interested to know more? Let our CloudSEK experts give you a detailed walkthrough of our platform's capabilities.

Request A Demo

Major Threats to the BFSI Sector

Data breaches and digital banking threats were the two major types of attacks targeting this sector, with more than 50% of the reported cases, in both the years (2021 and 2022), involving the leak or sale of databases, i.e data breach. About 20% of reported events concerned threats to digital banking, which mostly comprised selling, buying, compromising, and bypassing access to various digital payment systems, banking accounts, and digital wallets (crypto or otherwise).



Graph depicting the major threats to the BFSI sector as seen in 2021 and 2022

Data Breach

Data breach is the biggest arrow in the quiver employed by threat actors attacking BFSI entities. Threat actors employ various strategies ranging from simple scrapping, web injection commands, exploiting exposed endpoints to sophisticated malware attacks, exploiting CVEs, etc., to steal information from various organizations. The collected data equip these actors to perform further malicious activities including:

- Social engineering attacks
- Phishing/Smishing/Scam campaigns
- Identity thefts

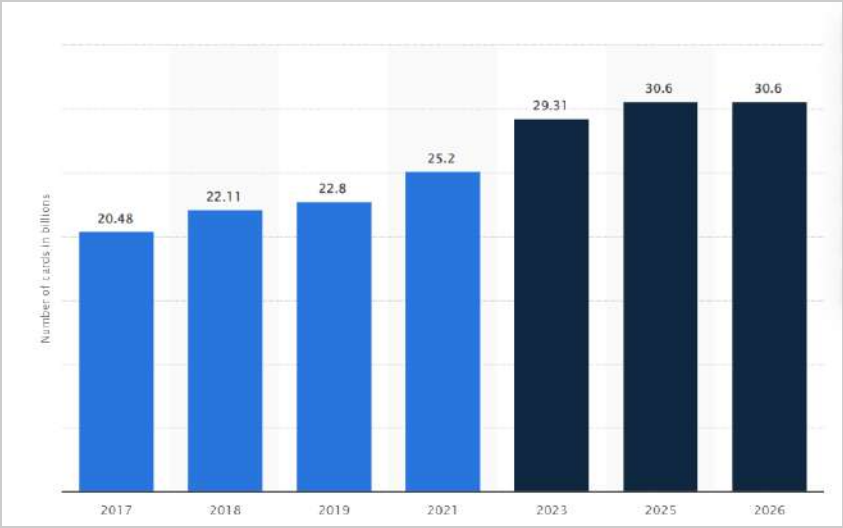
Data breaches in the banking sector can lead to exposure of sensitive information such as banking credentials, credit card details, source codes, etc., which can be exploited to carry out unauthorized transactions and financial fraud.

Digital Banking Threats

Statista has projected that by 2024, 2.4 billion individuals worldwide will be actively utilizing internet banking. Given the simplicity and convenience provided by chatbots, neobanks, and other digital financial systems, this should come as no surprise. Neobanks are direct banks which operate exclusively online without any physical branch networks. Ever since their emergence in 2016, neobanks have been posing a real challenge to the traditional banking systems and are expected to expand at a compound annual growth rate (CAGR) of 53.4% through 2030. The increased digital penetration provides cybercriminals with greater opportunities to capitalize on the growing digitalization to gain access into the company's infrastructure. This can also be followed up with data exfiltration or more sophisticated threats.

Credit Card Threats

According to Statista, the number of credit, debit, and other payment cards in circulation worldwide increased by more than two billion between 2019 and 2021 and is expected to rise further. In 2021, approximately 15% of BFSI instances recorded by XVigil involved credit card-based threats, indicating threat actors' growing interest in using financial resources as a mode of operation to handicap targets. Payment cards can be misused by criminals not only in online but also offline modes by employing various techniques including but not limited to carding, ATM hijacking, card-not-present fraud, card-present fraud, counterfeit card fraud, card ID theft, point-of-sale (POS) fraud, etc.



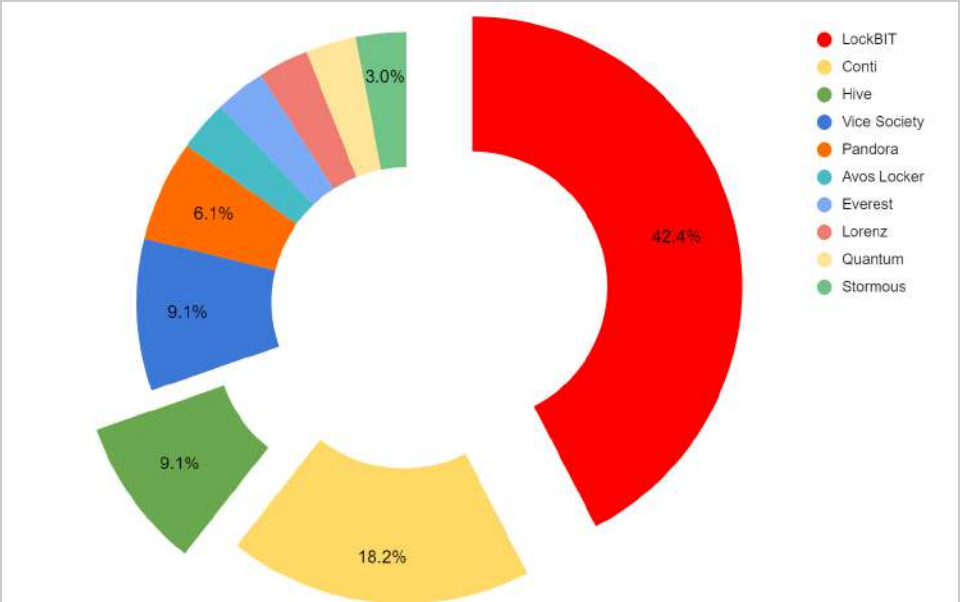
Statista's prediction of the number of credit, debit and prepaid cards worldwide

Vulnerabilities

Many threat actor groups launch attacks on target organizations by leveraging publicly known software or web vulnerabilities. The year 2022 saw an uptick in the use of vulnerabilities as an exploitation tactic in the BFSI sector, with 7% of reported incidents involving the exploitation of a vulnerability. In 2022, some highly critical vulnerabilities were discovered, such as Spring4Shell, out-of-bounds read vulnerability in Apple, multiple vulnerabilities in Microsoft, etc., which were actively being exploited across the globe to compromise organizations in all sectors. According to Akamai's annual security report, successful exploitation of vulnerabilities such as SQL Injections (SQLi), Cross-Site Scripting (XSS), Local File Inclusion (LFI), and OGNL Java Injection facilitated 94% of observed cyberattacks in this sector.

Malware

Malware-based cyber incidents accounted for ~18% of the total attacks recorded against the BFSI sector in 2022. Trojans, Ransomware, Botnet, and Info Stealers have been the most popular attack vectors used by cybercriminals to target this industry. Inspired by the ease of implementation of the Business as a Service (BaaS) model, cybercriminals have developed their variant known as Malware-as-a-Service (MaaS). Majority of the MaaS groups in the first half of the year 2022 were specialized groups that tinkered with the Ransomware tactic. Some of these groups also unleashed a barrage of attacks in succession. According to XVigil data, the most common ransomware variant used in BFSI sector attacks in 2022 is LockBIT, closely followed by Conti and Hive.



Percentage of ransomware attacks recorded by XVigil against the BFSI sector in 2022

Most Exploited Tactics, Techniques, and Procedures (TTPs)

Threat actors have been constantly improvising on their TTPs with regard to the Banking and Finance domain. It is an ever-evolving sphere and actors are moving away from tried and tested strategies to more sophisticated techniques. Below is a list of TTPs most commonly used to target this sector.

The most popular campaign launched against the industry has been one of the **fake domains or cloned websites** being used to target customers to enter their banking credentials.

Lately, there has been a shift in the TTPs employed as **phishing sites** have emerged to collect victims' banking credentials and PII, post which an Android SMS forwarding malware is downloaded to the devices of Android users.

Attackers are also using fake APKs to target victims by deploying **malicious Android applications**, hosted at Firebase via socially engineered pages, that require customers to input card details and account credentials.

Shortened URLs are being used to conduct Reverse Tunnel attacks against the BFSI sector. Multiple reverse tunnel services that enable applications to expose local server ports to the internet and serve malicious content have been identified in 2022. **Reverse tunnel and URL shortening services** were preferred by malicious threat actors to host malicious content. These URLs direct users to fake (phishing) login pages to avoid detection and create panic among the banking community.

Threat actors were also seen using **SMS forwarding malware** to steal OTP and evade antivirus detection by creating malicious phishing websites without mentioning any banking name or logo.

2022 saw a significant increase in the emergence of **fake online complaint portals** targeting the customers of the banking industry.

Improvised Phishing Campaigns

In 2022, phishing incidents accounted for 10% of all data breach incidents recorded in the BFSI sector. Phishing has long been a favorite tactic of threat actors. Several actors were seen purchasing and selling

phishing kits and related services. CloudSEK's Threat Research & Information Analytics Division (TRIAD) discovered these three distinct phishing methods used by attackers to target the Indian banking industry.

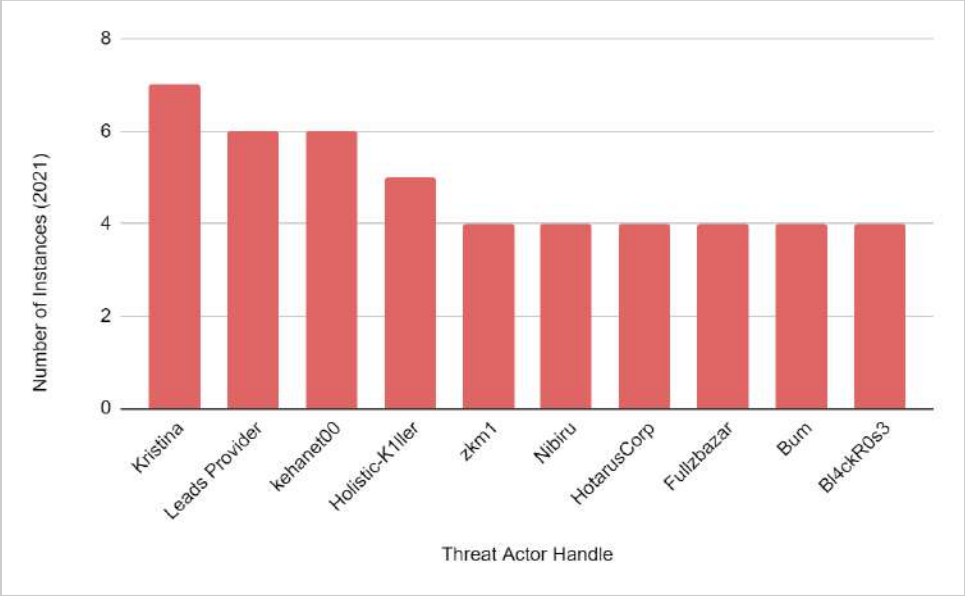
- **Using Hostinger's preview domains to host phishing sites and evade early detection -** Threat actors are using the domain preview feature, provided by Hostinger, which allows them to distribute phishing URLs during the DNS Zone Propagation time (time taken for a newly registered domain to start working globally).
- **JAMStack platform, Cloudflare Pages, misused to launch phishing campaigns -** Threat actors are cloning the target entity's internet banking login and KYC verification pages, which have a subdomain of the pages.dev domain, in order to steal PII and internet banking credentials from the customers.
- **Zoho Forms catapulted to gain sensitive PII information from banking customers -** Threat actors create fake Twitter accounts impersonating banking entities. When a customer tags the bank's official Twitter handle, the actors use the fake accounts to redirect them by providing a fake customer care number and an external shortened link that leads to a Zoho Form service. The gullible customer inputs the required PII information and banking credentials, which are then forwarded to the threat actors.

Major Threat Actors Targeting the BFSI Sector

As discussed above, threat actors have significantly shifted in their pattern of exploitation from 2021 to 2022. A possible reason for this could be the emergence of new actors in the year 2022 that were not active prior to this year. Below is a year-wise listing of the most active threat actors in this industry.

10 Most Active Threat Actors in 2021

The top ten threat actors were categorized on the basis of the number of instances carried out by them during the period. A threat actor by the name 'Kristina' popularly known as 'KelvinSecurity' led the onslaught with the maximum number of attacks (7 recorded incidents) followed by 'Leads provider' and 'kehanet00' who followed with modest numbers (6 incidents each). 'Holistic-K1ller' was next on the list followed by zkm1, Nibiru, HotarusCorp, Fullzbazar, Bum, and Bl4ckR0s3 who contributed equally during the period (4 incidents each).

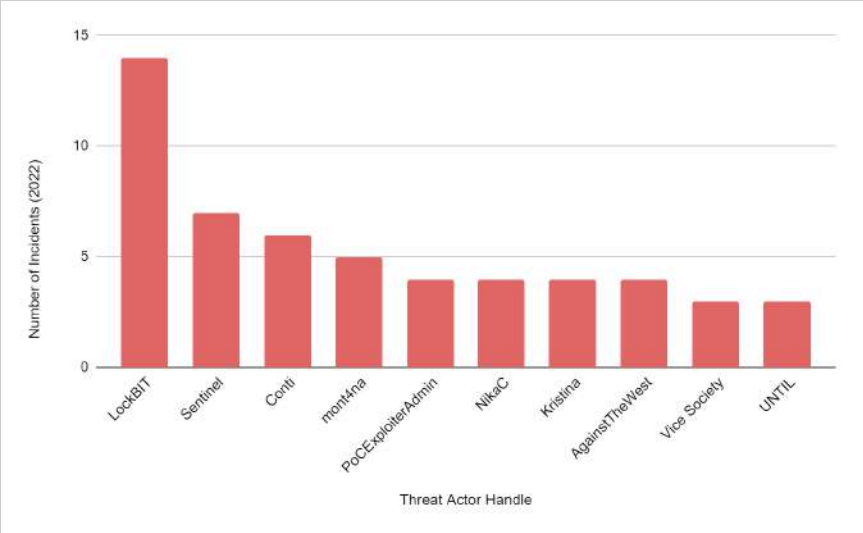


Most active Threat Actor Handles in the BFSI sector in 2021

10 Most Active Threat Actors in 2022

The LockBIT ransomware group, collectively with all its variations and 14 recorded incidents, emerged as the frontrunner in campaigns targeting the BFSI sector, followed by Sentinel with 7 recorded incidents and the Conti ransomware group with a total of 6 recorded incidents against this sector. mont4na was next on the list with 5 reported incidents, followed by PoCExploiterAdmin, NikaC, Kristina, and AgainstTheWest, each having 4 recorded incidents. Several smaller players also cashed in on this fad by attacking the

sector with their tried and tested methods and these included the Vice Society ransomware group and UNTIL (each having 3 recorded incidents).



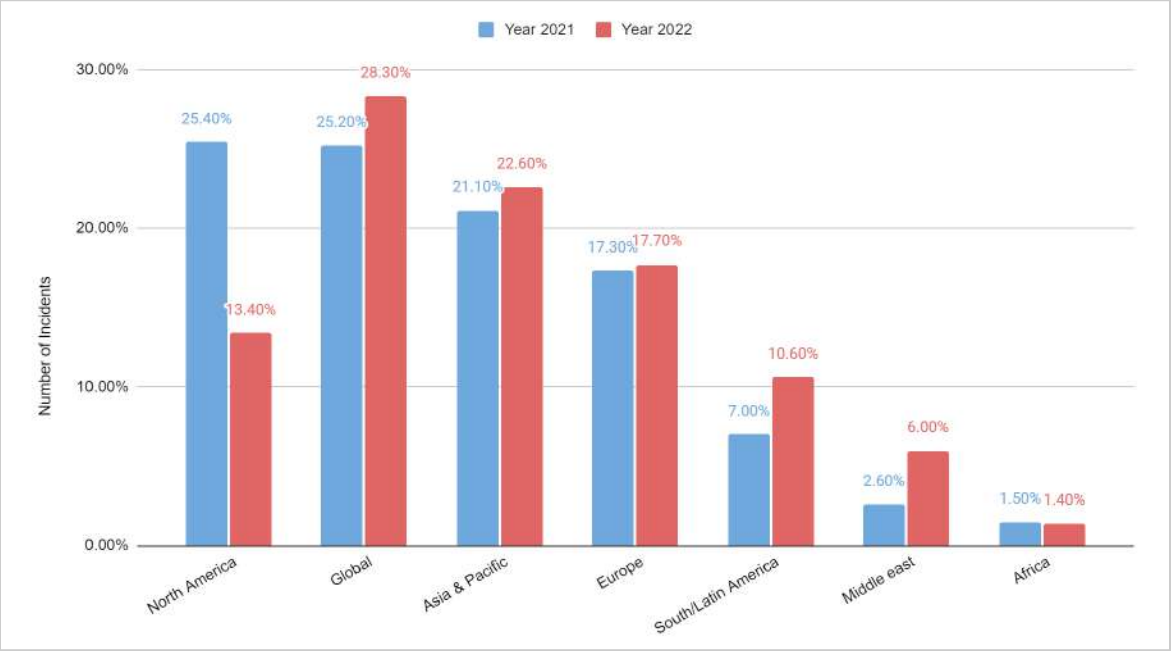
Most active Threat Actor Handles in the BFSI sector in 2022

Threat Actor - Kristina

- The threat actor with the handle 'Kristina' was the only attacker to appear in the top ten actors in both the years 2021 and 2022.
- This handle is used by a threat group that was previously known as the **Kelvin Security team**.
- The group uses targeted fuzzing and exploits common vulnerabilities to target victims. Being highly skilled in the use of tools and having a wide knowledge of various exploits, they share their list of tools and payloads for free.
- They typically target victims with common underlying technologies or infrastructure at any given time.
- The group doesn't shy away from attention and publicly shared information such as new exploits, targets, and databases on cybercrime forums and communication channels such as Telegram.
- Recently, they started their data leak websites where other threat actors can come and share databases.

Most Targeted Regions*

Focus regions have also shifted from the year 2021 to 2022. What was once considered a priority (in the year 2021) has seen a massive shift.



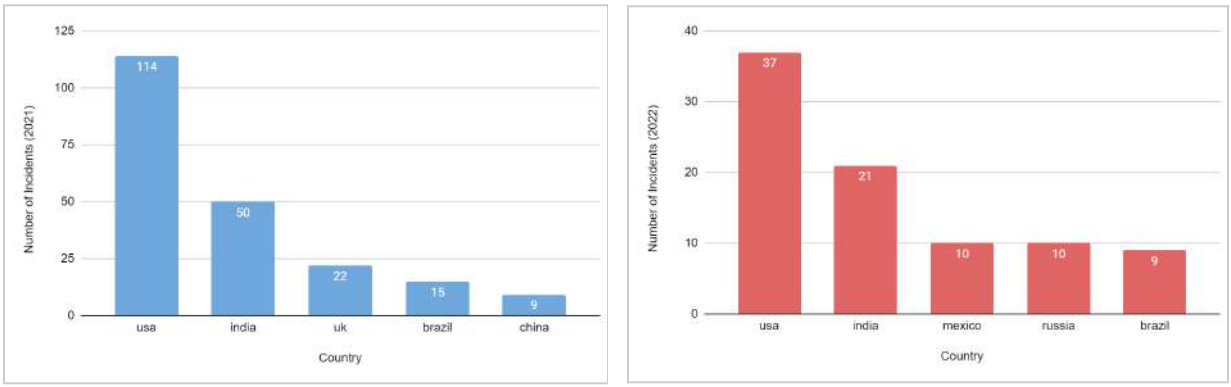
Graph depicting the most targeted regions in the BFSI sector as seen in 2021 and 2022

North America was the most targeted region in 2021 with 25.4% of the total recorded instances in the BFSI sector while 25.2% of the total recorded instances were globally spread without much reference to any specific region or country. Asia & Pacific had 21% of the recorded instances with Europe close on heels having 17% of the recorded instances. South/Latin America and the Middle East ranked lowest in the total number of recorded incidents in the BFSI sector in 2021.

However, these statistics took a major turn in the year 2022. A significant shift of operations was witnessed with a whopping 28.3% of recorded instances having a global impact. Attacks on BFSI in North America were almost reduced by half in 2022 (with 13.4% of the total recorded instances), while attacks on the Middle East BFSI sector surged by more than twice the amount seen in 2021 (with 6% of the total recorded instances). An overall increase was observed in the number of incidents recorded in Asia & Pacific (22.6%), Europe (17.7%), and South/Latin America (10.6%).

Africa recorded the least number of cyber incidents against the BFSI sector in both the years (2021 and 2022). It is interesting to notice such a paradigm shift in just the first 6 months of 2022.

USA, India & Brazil Emerge as Prime Targets



Graphs depicting the most targeted countries in the BFSI sector as seen in 2021 and 2022

While the number of attacks on specific nations fluctuated, India, Brazil, and the United States maintained their positions as the top five countries in the BFSI industry (in 2021 and 2022).The USA recorded twice the number of cyber incidents in the BFSI sector than any other country in both 2021 and 2022. Given that banking assets are estimated to be 56% of the U.S. economy, it is home to some of the largest banks in the world including JPMorgan Chase, Bank of America, Wells Fargo, Citigroup, and Goldman Sachs. Given the BFSI industry's growth, expenditure, and digitalization in the USA, it is easy to see why it is the most targeted country when it comes to cyberattacks on this sector.

***Note: The insights and distribution of threats by region are contingent on the presence of our clients in those regions.**

Long-Term Impact & Mitigation Measures

A country's economy is fundamentally supported by its banking and finance industry, hence any threat to this sector puts the entire nation at risk. Threats to this sector can result in significant loss of consumer information and financial resources, not to mention reputational harm to the compromised firm as the public's awareness of their vulnerabilities acts as a deterrent to attracting new clients. In some cases, it can also result in data corruption and operations disruption. According to IBM research, **the average cost of data breaches in the financial sector is USD 5.72 million**, with a 10% year-over-year increase in average total cost (2019 - 2020).

Due to the increased sophistication of the strategies and malware used to target this industry, it has become imperative to develop stronger and more responsive preventive measures to protect this sector from any further attacks. The following is a list of challenges and mitigation strategies to assist with the same.

Challenges

- Severe talent crunch is an obstacle that can handicap this industry's security perimeter.
- Weak credentials employed by both employees and third-party contractors severely affect the security framework of a firm.
- Allocating an appropriate budget for security measures is a handicap for most entities.
- Uninformed employees who tinker with the system, and pose a threat to the infrastructure
- Third-party users who need to be educated and third-party services that are not secure.
- Staggered Infrastructure and fragmented stakeholders add to the industry woes.

Mitigation Measures

- Financial institutions and related government entities:
    - Conduct continuous security awareness programs (regarding cyber-attacks, online scams, and phishing) at the employee, customer, and third-party user levels
    - Enact strong password policies and enable multi-factor authentication (MFA)
    - Update and patch software, systems, and networks on a regular basis
    - Maintain multiple backups, both online and offline, in separate and secure locations
    - Monitor logs for unusual traffic and activity to websites and other applications
    - Block illegitimate IP addresses and deactivate port forwarding using network firewalls

    - Perform real-time monitoring of the internet to identify and mitigate low-hanging threats, such as misconfigured apps, exposed data, and leaked accesses, that are leveraged by cybercriminals to carry out large-scale attacks.
- Banking customers should enact the following:
    - Keep up-to-date with ongoing financial scams in the news
    - Avoid disclosing banking information unless absolutely necessary
    - Do not share OTP and ATM pins with any individual or organization
    - Avoid clicking on suspicious emails, messages, and links
    - Not download or install unverified apps
    - Use strong passwords and enable multi-factor authentication (MFA) across accounts

References

- The 6 Biggest Cyber Threats for Financial Services in 2022 | UpGuard
- The Global Cyber Threat to Financial Systems – IMF F&D
- The 5 Biggest Threats to a Bank's Cyber Security
- Cyber Threats In The Banking Industry
- Timeline of Cyber Incidents Involving Financial Institutions - Carnegie Endowment for International Peace
- Cyber Security in Banking Sector - Top Threats & Importance
- How Is The Banking Industry Affecting GDP Growth -Rakesh Tulsiani - BW Businessworld
- 18 Online Banking Statistics You Need to Know in 2022
- • Global Banking & Finance – Industry Insights & Data Analysis | Statista
- The digital trends disrupting the banking industry in 2022
- • Neobanks global market size 2021 | Statista
- • Global number of users at selected digital banks 2020 | Statista
- • Payment cards in circulation worldwide 2026 | Statista
- The Unabated Reign of ATM Hacking: The 2021 Rajasthan ATM Attack and the Proliferation of Novel ATM Hacking Tools and Techniques - CloudSEK
- Akamai Threat Research: Phishing and Credential Stuffing Attacks Remain Top Threat to Financial Services Organizations and Customers
- Popular Trends in Digital Banking for 2022
- Banking in the United States - Wikipedia

- 2022 Global Outlook for Banking and Financial Markets | IBM
- Cloudflare Pages Misused in a Phishing Campaign Against Indian Banking Customers
- Zoho Form Service Leveraged to Exfiltrate Sensitive PII from Banking Customers
- Hostinger's Preview Domain Feature Abused to Launch Phishing Campaigns and Evade Detection
- Cybercriminals Exploit Reverse Tunnel Services and URL Shorteners to Launch Large-Scale Phishing Campaigns
- Improvised Modus Operandi for Targeting Indian Banking Customers via SMS Forwarding Malware
- Unpatched Java Spring Core Zero-Day Vulnerability: "Spring4Shell" - CloudSEK
- The Surge of Cybersecurity Challenges in Neobanking - BeVigil Blog

About CloudSEK

CloudSEK is a contextual AI company that predicts Cyber Threats even before they occur. We combine the power of Cyber Crime monitoring, Brand Monitoring, Attack Surface monitoring, and Supply chain intelligence to provide context to our customer's digital risks. Our unified dashboard allows customers to triage and visualize all digital threats in one place. We also offer workflows and integrations to manage and remediate the identified threats.

To learn more about CloudSEK, visit cloudsek.com.

To schedule a demo, click the link below and our expert will guide you through CloudSEK capabilities.

Request A Demo