KELA DATASHEET

CYBERCRIME THREATS TO THE FINANCIAL SECTOR

In 2023, the financial sector is one of the prime targets for cyber threats. As financial institutions remain integral to the global economy, cybercriminals employ advanced techniques to compromise sensitive data and disrupt crucial financial operations. KELA delves into cybercrime threats to the financial sector, including insider threats and data theft, ransomware attacks, network access sales, and DDoS.

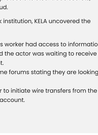
INSIDER THREATS

In the world of bank fraud, KELA's observations have shown some clear patterns: many of these individuals use similar methods, share common characteristics and often have an insider within a specific bank who assists them in their activities.

These insiders exploit their knowledge of internal systems and protocols to steal trade secrets, intellectual property, customer data, or engage in financial fraud.

When investigating one of the insider threats to a specific bank institution, KELA uncovered the following malicious scheme:

1. The actor knew someone who worked at a bank branch. This worker had access to information about potential targets who are clients of the institution, and the actor was waiting to receive this target information from the employee based on request.
2. The actor posted an announcement on one of the cybercrime forums stating they are looking for a hacking group able to steal funds.
3. The plan then would be to do SIM swaps, and use the insider to initiate wire transfers from the accounts. Funds would be wired out of the bank to another account.



Banking fraud tutorials found on Telegram

BANKING DATA ON SALE

Common bank fraud tactics include phishing and social engineering targeting bank customers, credit card skimming, card cracking, money muling, and more. Banking fraud tutorials proliferate on Telegram, enabling beginner cybercriminals to conduct attacks. As a result, various stolen information is being traded in cybercrime communities. The underground credit card markets, such as Omerta, Brian's Club, and Yale Lodge, offer compromised cards with CVV/CVV2 information. Additionally, fraudulent checks and stolen valid checks are circulated on Telegram channels, often as part of scam schemes.

DATABASE DUMPS

Cybercriminals target financial institutions not only for stealing funds and financial data, but also for customer records that can be later used in other attacks.

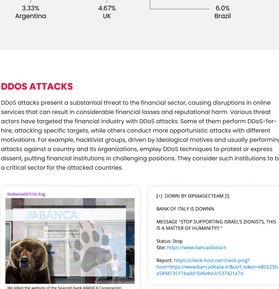
For example, in November 2023, a data breach occurred at an India-based bank, The Kurla Nagrik Sahakari Bank; a threat actor leaked a database containing sensitive information of 76,890 users on a cybercrime forum. The leaked database included details such as age, birth date, caste, academic and professional history, email addresses, and more. This extensive dataset could be exploited by cybercriminals in various ways, such as orchestrating phishing campaigns using the victims' personal details to craft convincing messages.

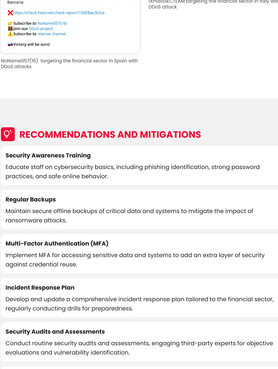
Additionally, the exposed information could facilitate identity theft and financial fraud, with threat actors potentially using the stolen data to impersonate individuals for illicit financial transactions or other malicious activities.

An actor shared a database of an Indian bank

RANSOMWARE ATTACKS

In 2023, the financial sector is in the top 10 sectors targeted the most by ransomware & extortion actors, with more than 250 attacks. The **most targeted country is the US**, accounting for almost 50% of the ransomware & extortion attacks in this sector. Other top targeted countries are **the UK, India, Italy, and Canada.** The most prolific ransomware groups targeting the financial sector were **Clop, LockBit, Alphv, 8Base, and Black Basta.**





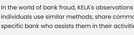
NETWORK ACCESS OFFERS

Network access is an important part in the ransomware-as-a-service supply chain, with Initial Access Brokers (IABs) serving as key players. In 2023 alone, KELA has observed more than 80 network access listings related to financial institutions being offered for sale.

The US was the most targeted country by IABs, accounting for 31% of the victims, followed by **Brazil, Argentina, and the UK.**

DDOS ATTACKS

DDoS attacks present a substantial threat to the financial sector, causing disruptions in online services that can result in considerable financial losses and reputational harm. Various threat actors have targeted the financial industry with DDoS attacks. Some of them perform DDoS-for-hire, attacking specific targets, while others conduct more opportunistic attacks with different motivations. For example, hacktivist groups, driven by ideological motives and usually performing attacks against a country and its organizations, employ DDoS techniques to protest or express dissent, putting financial institutions in challenging positions. They consider such institutions to be a critical sector for the attacked countries.



NoNameh057(16) targeting the financial sector in Spain with DDoS attacks

ISP666SECTEAM targeting the financial sector in Italy with DDoS attack

RECOMMENDATIONS AND MITIGATIONS

Security Awareness Training

Educate staff on cybersecurity basics, including phishing identification, strong password practices, and safe online behavior.

Regular Backups

Maintain secure offline backups of critical data and systems to mitigate the impact of ransomware attacks.

Multi-Factor Authentication (MFA)

Implement MFA for accessing sensitive data and systems to add an extra layer of security against credential reuse.

Incident Response Plan

Develop and update a comprehensive incident response plan tailored to the financial sector, regularly conducting drills for preparedness.

Security Audits and Assessments

Conduct routine security audits and assessments, engaging third-party experts for objective evaluations and vulnerability identification.

Collaboration and Information Sharing

Foster collaboration with other financial institutions, sharing threat intelligence and participating in industry-specific forums.

Endpoint Protection

Implement advanced endpoint protection solutions, including antivirus, endpoint detection and response (EDR), and behavior-based analysis to defend against malware.

Monitor Cybercrime Platforms

Stay vigilant by monitoring cybercrime sources for chatter on database dumps, compromised accounts, cyber trends, and ransomware attacks. Get started with KELA for free today.