Finance Industry

Threat Landscape Report

SOCRadar®
Your Eyes Beyond

socradar.io

SOCRadar®
Your Eyes Beyond

Table of Contents

Executive Summary

Top Takeaways

The United States financial sector faces the most severe cyber threat exposure, being the primary target for both ransomware attacks (60.47%) and stealer malware campaigns (18.81%), while also experiencing the highest overall malicious cyber activities (19.10%).

Threat actors overwhelmingly focus on data acquisition and monetization, with 67.94% of underground market listings involving data/databases, accompanied by a high volume of exposed credentials (2.89M) and credit cards (90.428) from stealer malware operations.

The ransomware landscape shows significant concentration with LockBit 3.0 leading at 23.81% of attacks, while the broader threat landscape demonstrates sophisticated commercialization with 61% of activities focused on selling and 30.09% on sharing malicious assets.

Emerging markets, particularly in South Asia and Latin America, are experiencing increased targeting by stealer malware, suggesting threat actors are exploiting regions with growing digital banking adoption and potentially weaker security controls.

Access trading has emerged as a critical threat vector, representing 12.65% of underground market listings, indicating a mature cybercrime ecosystem where specialized actors focus on different stages of the attack lifecycle.

The financial sector faces a complex threat landscape where 63.10% of ransomware attacks come from diverse groups outside the top three actors, suggesting a highly fragmented attack surface requiring comprehensive intelligence strategies.

Technical Details

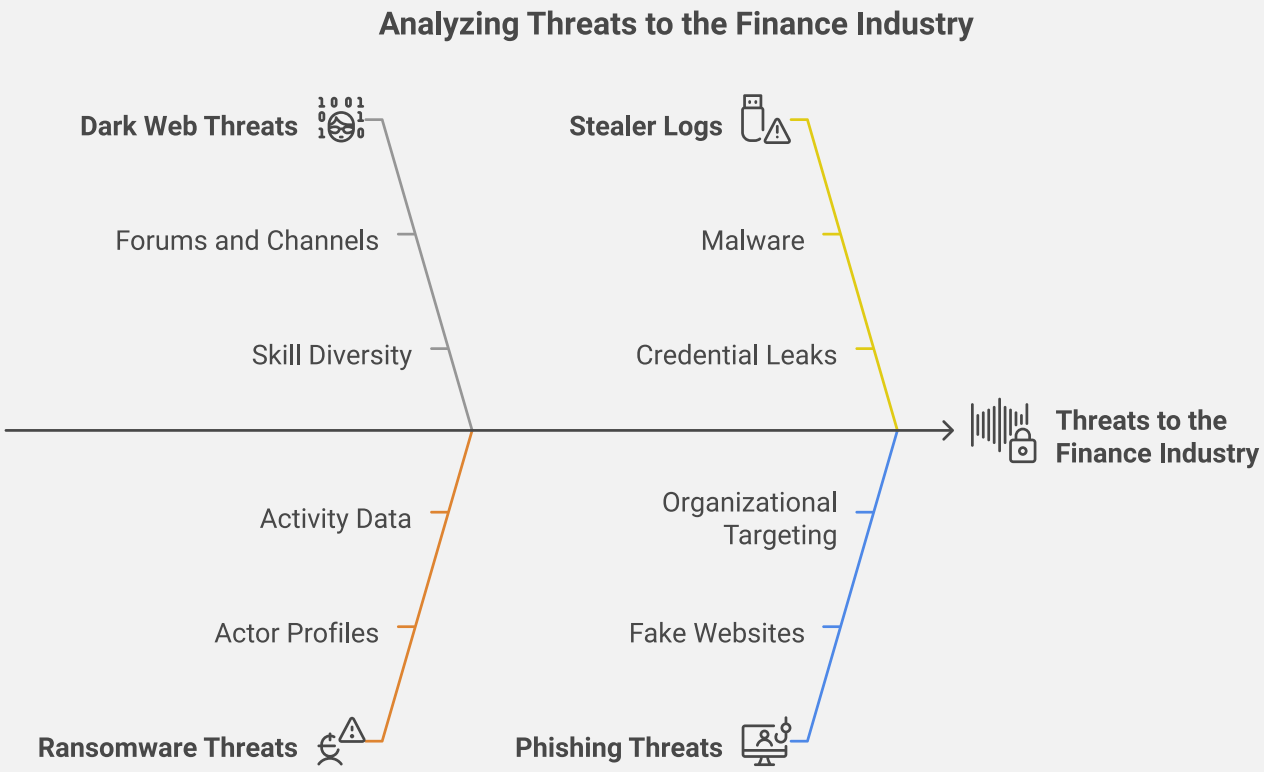
In the following chapters, you will read about the threats targeting the finance industry.

In the Dark Web Threats chapter, we will be covering the data, 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 detailed information about ransomware actors targeting the finance industry, their detailed profiles and the necessary data that summarizes the ransomware activities.

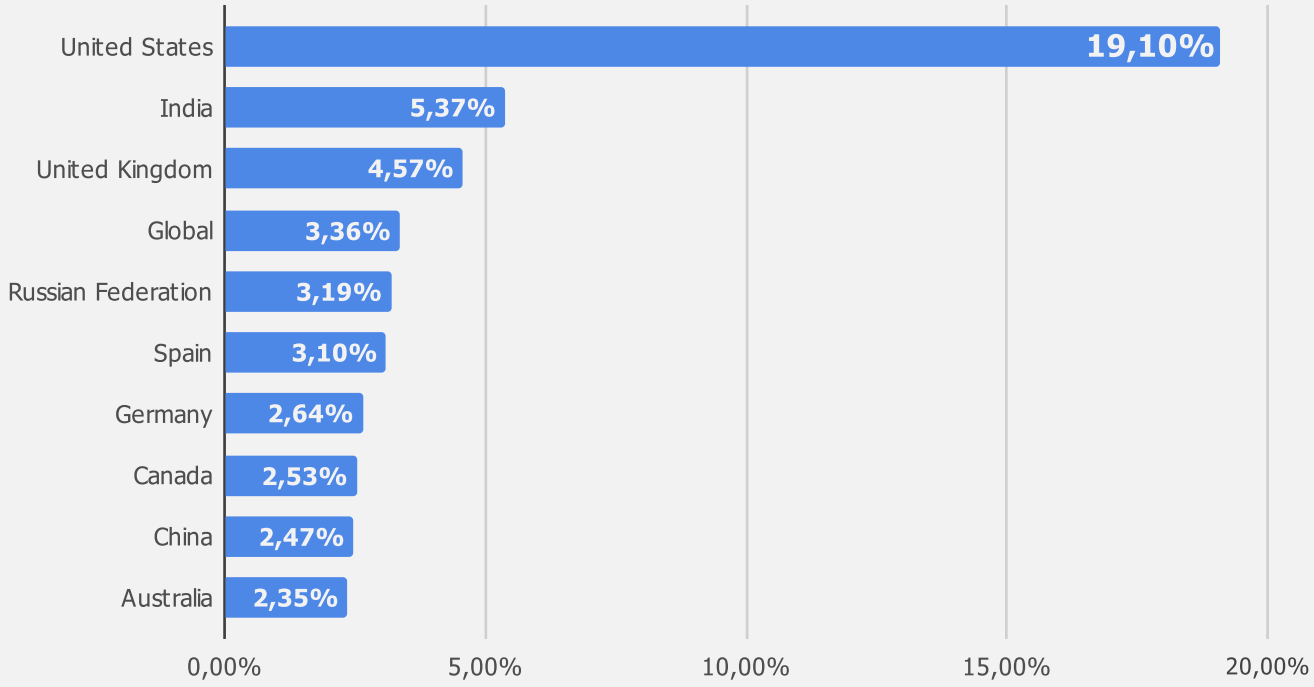
Stealer Logs Statistics chapter is all about stealer malware and the data around leaked credentials. These days, hackers don't hack, they log in. It is important to make sure that employee credentials are not compromised.

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 Country



Western concentration and North American dominance in targeting:

- Five of the top 10 targets are Western nations (US, UK, Spain, Germany, Canada), indicating a clear preference for developed economies with mature financial markets.
- The US and Canada combined represent over 21% of all activities, suggesting threat actors are heavily focused on the region's financial sector, likely due to its economic significance.

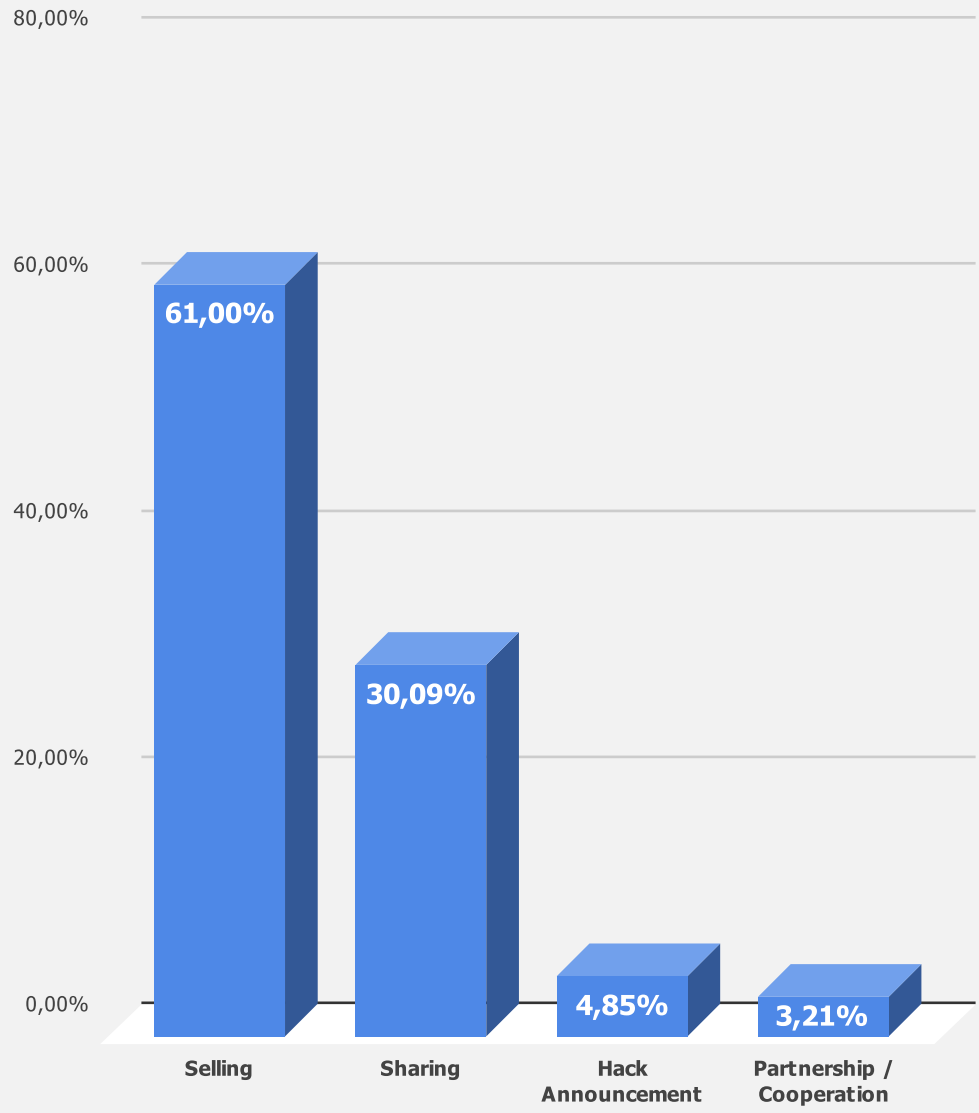
APAC emerging threat landscape:

- The presence of India (5.37%), China (2.47%), and Australia (2.35%) shows a significant but secondary focus on Asia-Pacific financial institutions, possibly targeting their growing digital banking initiatives.

Low Chinese percentage:

- China's relatively low percentage (2.47%) might indicate either strong defensive capabilities, under-reporting, or threat actors focusing on other sectors within the country.

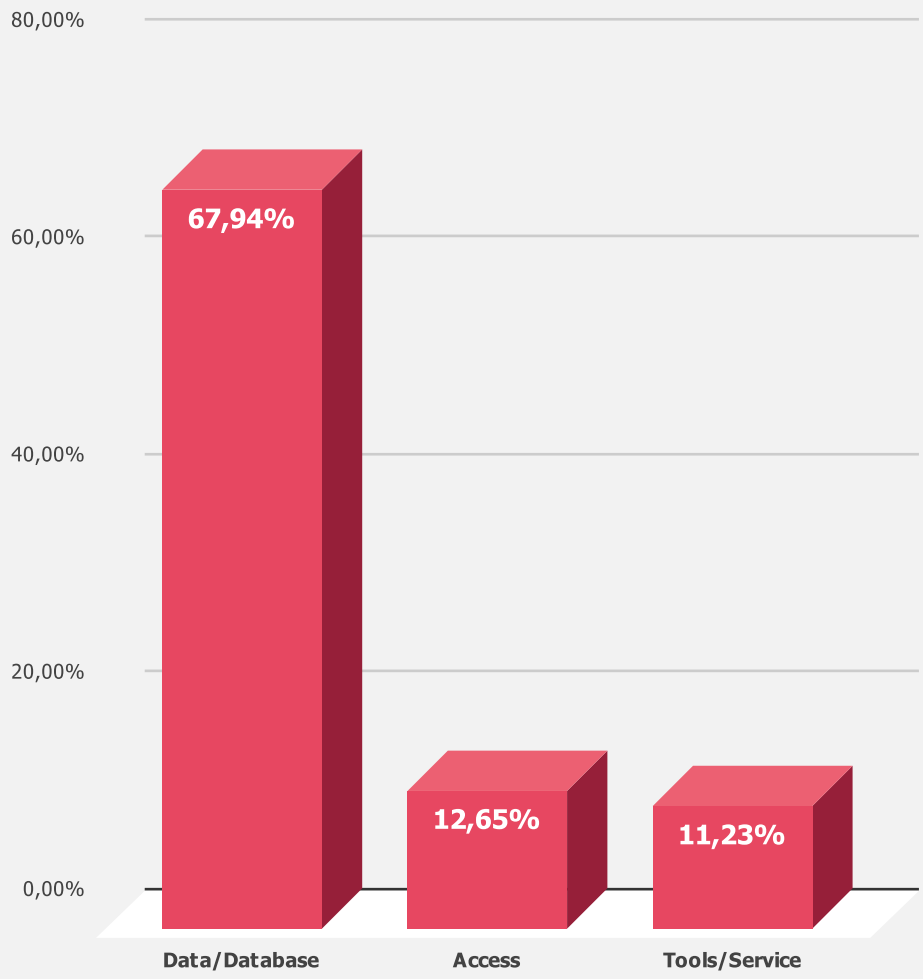
Distribution of Dark Web Threats by Industry



Monetization dominance:

- The overwhelming focus on selling (61%) and sharing (30%) activities indicates a highly commercialized threat landscape where financial data and tools are treated as commodities.

Distribution of Dark Web Threats by Threat Categories



Data-centric threats:

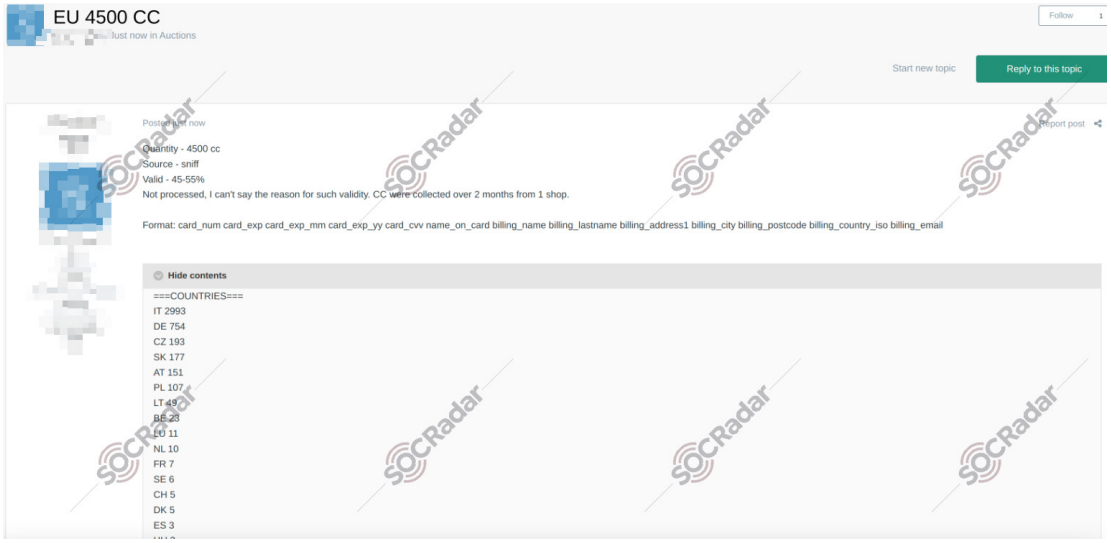
- The overwhelming dominance of data/database offerings (67.94%) aligns with the financial sector's primary concern - the protection of sensitive financial and customer data. This suggests threat actors are primarily focused on data exfiltration and trading.

Access market maturity:

- The significant percentage of access offerings (12.65%) indicates a thriving market for initial access brokering, where threat actors sell network access to financial institutions, potentially enabling ransomware groups and other sophisticated attackers.

Recent Dark Web Activities Targeting the Finance Industry

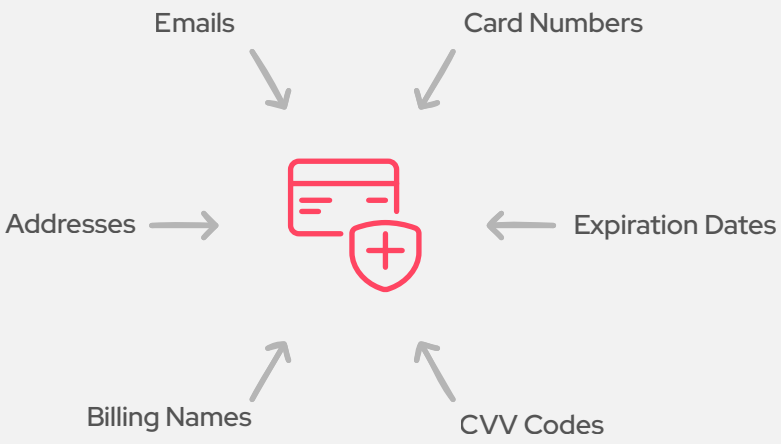
Alleged 4500 Credit Cards Belonging to Many Countries are on Sale



SOCRadar analysts have flagged a recent post on a dark web marketplace where a threat actor alleges the sale of 4,500 credit card records from multiple countries.

According to the forum post, the data was acquired through “sniffing” over a two-month period from a single shop.

Components of Compromised Credit Card Information



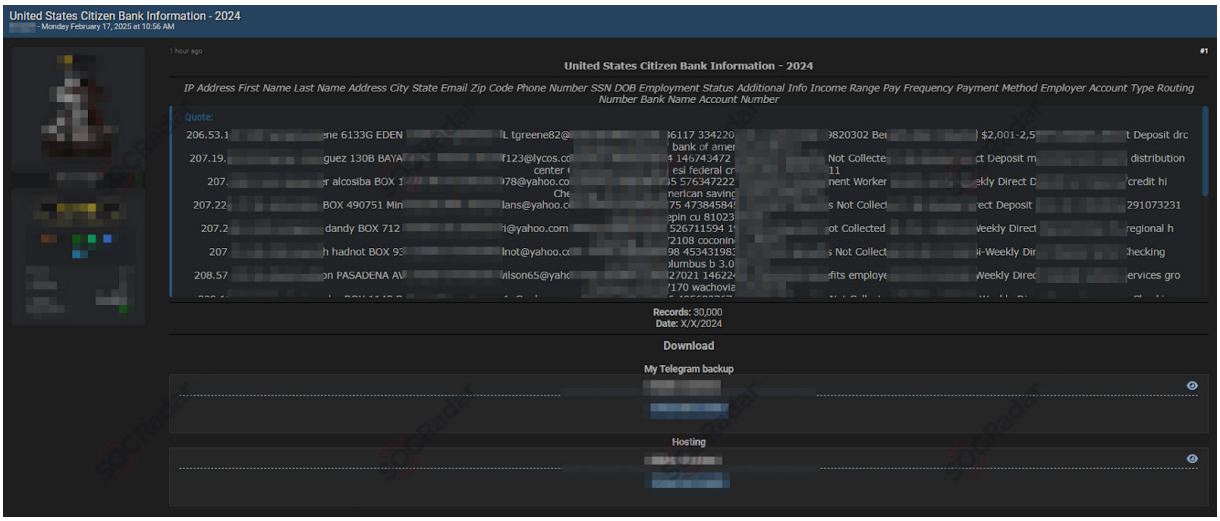
It is important to emphasize that the presence of such posts does not confirm a successful data breach. This may be an attempt to resell older stolen data or mislead potential buyers.

Alleged Login Credentials of Various Banks are on Sale

SOCRadar analysts have detected an alarming post on a dark web forum, where a threat actor is allegedly offering login credentials for various bank accounts for sale.

The alleged price for these credentials ranges from $500 to $1,000. The seller also provided a contact link directing potential buyers to a Telegram account.

Alleged Banking Data of American Citizens are Leaked



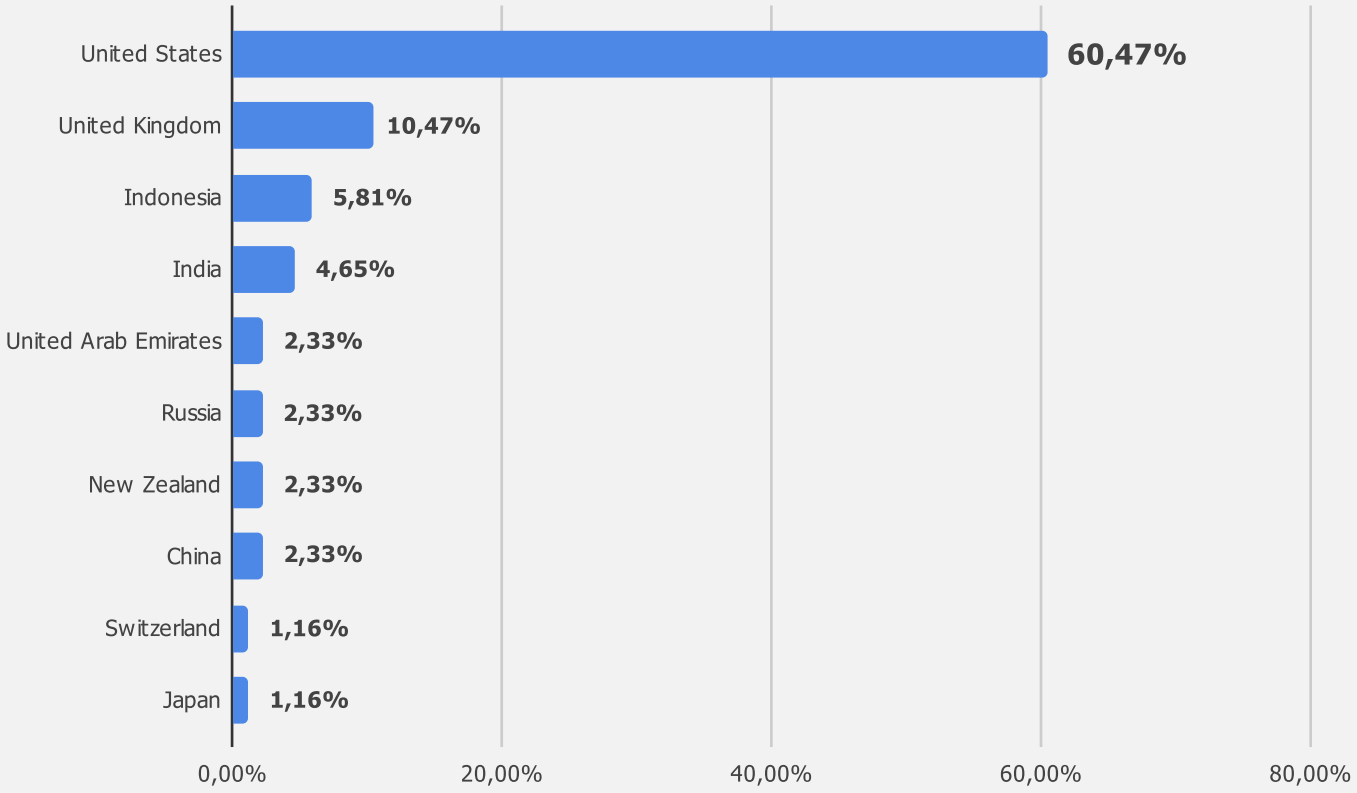
A post on a dark web forum, recently monitored by SOCRadar, claims to offer a database containing sensitive financial and personal information of approximately 30,000 American citizens.

According to the forum post, the dataset allegedly includes a wide range of personal and financial details such as Social Security numbers (SSNs), addresses, bank account numbers, routing numbers, income ranges, and employment statuses.

The forum post provides links for downloading the alleged database and references a Telegram backup, allowing interested parties to access the data outside of the forum. While the post does not specify how the information was obtained, past incidents suggest that such leaks could stem from phishing attacks, data breaches, or insider threats within financial institutions.

Ransomware Threats

Distribution of Ransomware Attacks by Country



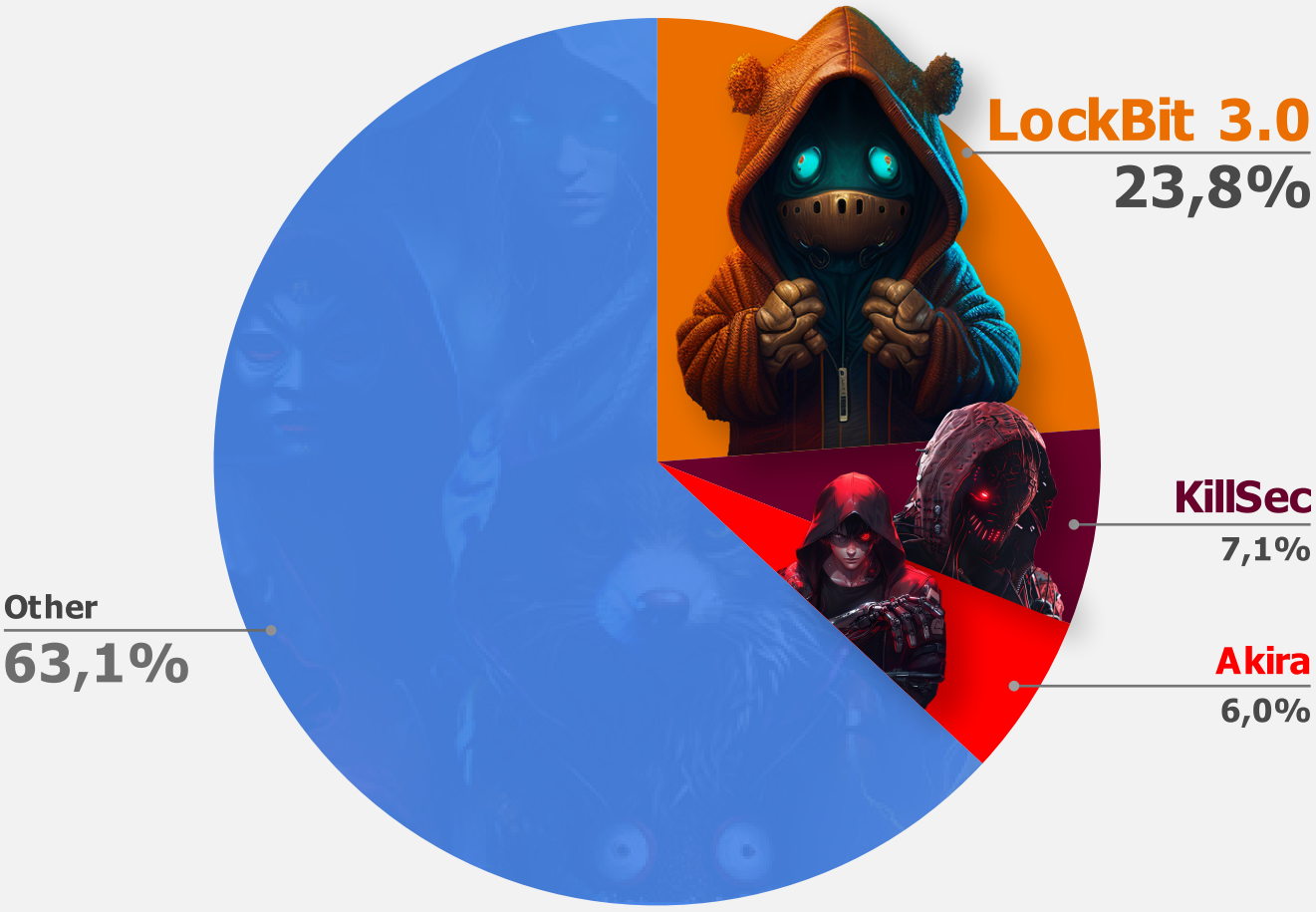
Anglo-American focus:

- Combined targeting of US and UK financial sectors (70.94%) suggests ransomware groups are predominantly focused on English-speaking countries with developed financial markets.

APAC diversity:

- The spread across Indonesia (5.81%), India (4.65%), China (2.33%), and Japan (1.16%) shows a strategic targeting of diverse APAC economies, but at significantly lower rates than Western targets.

Top Ransomware Groups Targeting the Finance Industry



LockBit dominance:
LockBit 3.0's significant market share (23.81%) demonstrates their continued dominance in financial sector targeting, likely due to their sophisticated operations and proven ability to monetize attacks.

Market fragmentation:
The large "Other" category (63.10%) indicates a highly fragmented ransomware landscape.

Emerging players:
The presence of KillSec (7.14%) suggests new groups are successfully establishing themselves.

Concentration risk:
The top 3 groups account for roughly 37% of attacks, indicating that while the landscape is fragmented, a small number of sophisticated actors are responsible for a significant portion of high-impact attacks.

A Closer Look into The Top 3 Ransomware Groups

LockBit

Threat Actor Card of Lockbit 3.0 Ransomware Group

LockBit 3.0, succeeding LockBit and LockBit 2.0, functions as a Ransomware-as-a-Service (RaaS) entity.

Since January 2020, LockBit has transitioned to an affiliate-based model, employing diverse methodologies to target businesses and critical infrastructure entities. Noteworthy tactics include double extortion and the utilization of initial access broker affiliates, alongside recruitment efforts involving insiders and hacker recruitment competitions.

With over 1,500 victim disclosures on the SOCRadar platform, LockBit emerged as the most active ransomware group in 2022 following Conti's cessation. As of the first quarter of 2023, they retain their position as the most prolific group, with over 300 disclosed victims.

You can visit our *blog post* for more detailed Lockbit 3.0 Ransomware Group information.

KillSec

Threat Actor Card of 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.

Akira

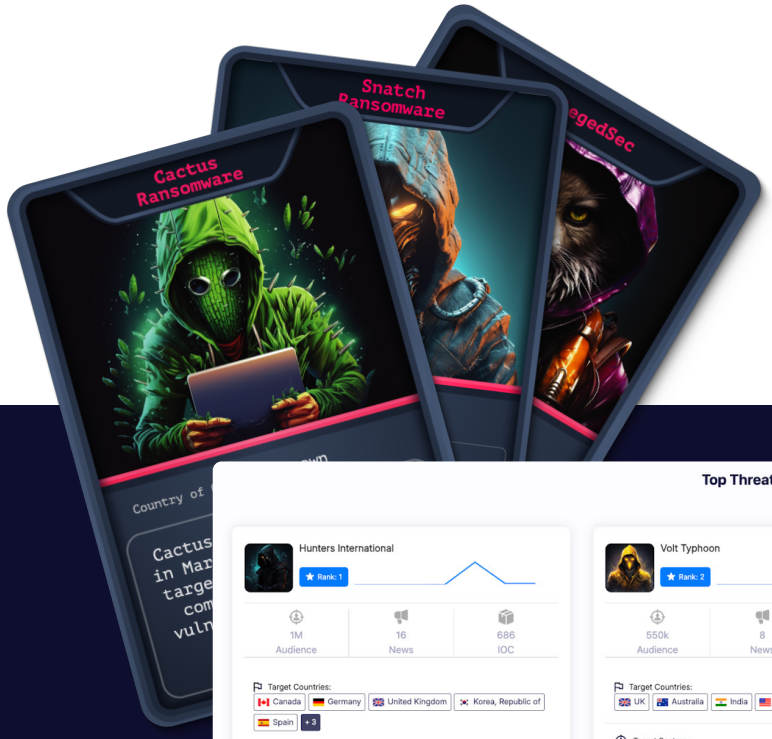
Threat Actor Card of Akira

Since its discovery in early 2023, Akira ransomware has evolved from a seemingly ordinary addition to the ransomware landscape to a significant threat affecting many businesses and critical infrastructure entities. This evolution and the unique aesthetic of its leak site and communications have drawn attention to its operations.

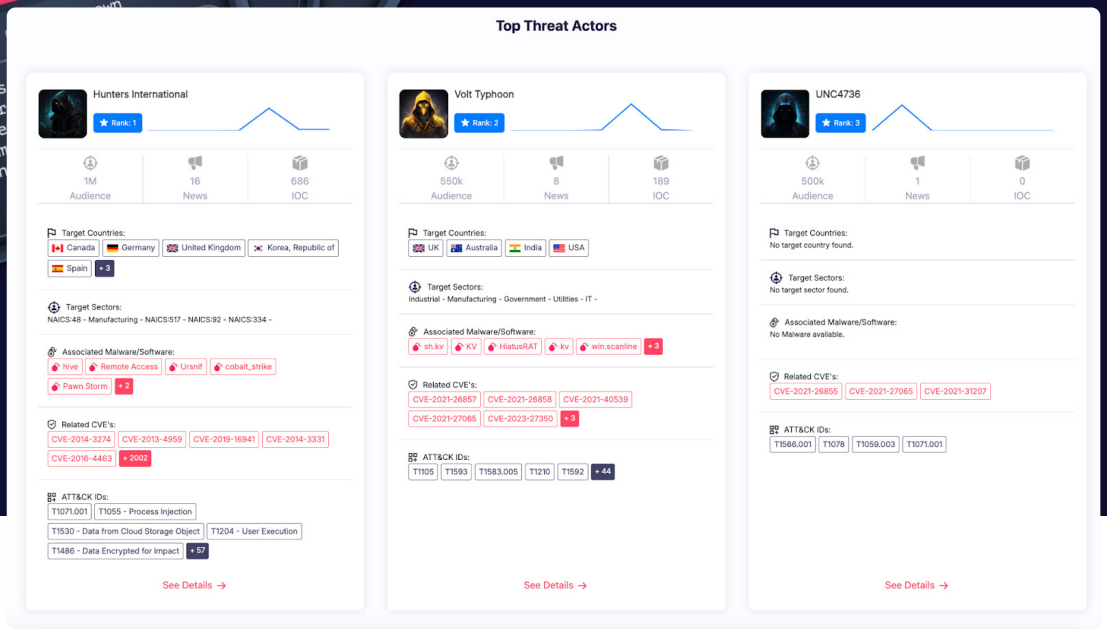
The ransom group employs a double extortion strategy, first exfiltrating data and then encrypting devices within the targeted network. Payment is then demanded not only for decrypting files but also for preventing the exposure of leaked data.

The Akira ransomware group frequently demands hefty ransoms, primarily targeting large enterprises across North America, Europe, and Australia. The malware typically spreads through targeted threat campaigns using phishing emails or exploiting software vulnerabilities, focusing on industries such as education, finance, manufacturing, and healthcare.

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



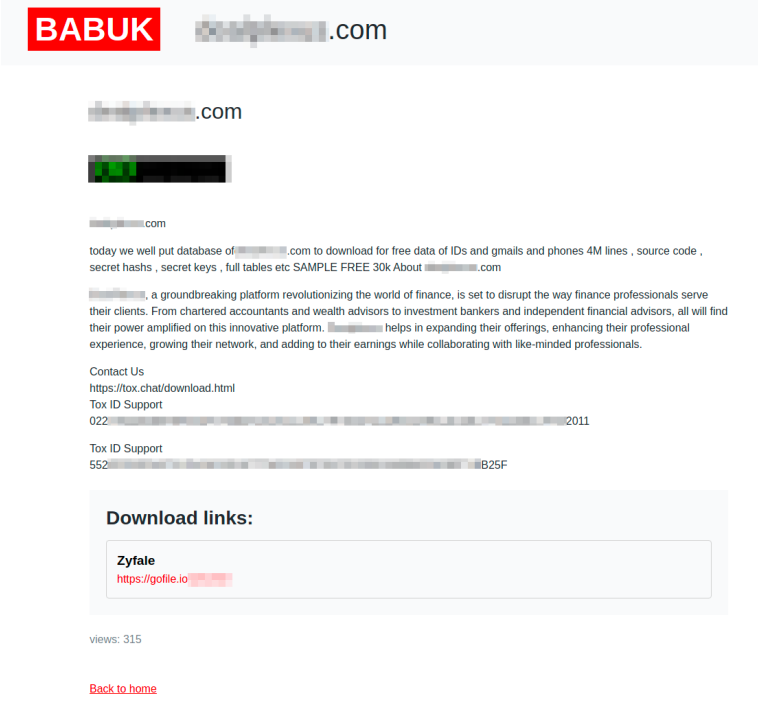
SOCRadar enhances cybersecurity measures with its *Threat Actor Intelligence Module*, which features advanced Threat Actor Tracking capabilities for organizations that want to stay ahead of cyber threats in real time.



SOCRadar Labs - Threat Actor Page

Recent Ransomware Attacks Targeted the Finance Industry

Babuk targeted a FinTech Platform



A recent post on a dark web forum, reportedly associated with the Babuk ransomware group, alleges that a financial networking platform has fallen victim to a data breach. The post, which was identified through continuous monitoring by SOCRadar, claims that a vast amount of sensitive information from the company has been leaked.

Potential Implications

If the claims are accurate, this could represent a significant security incident, potentially exposing sensitive financial data and personal details of professionals using the platform.

Stolen Data Components

Personal Information

This includes IDs, Gmail addresses, and phone numbers.

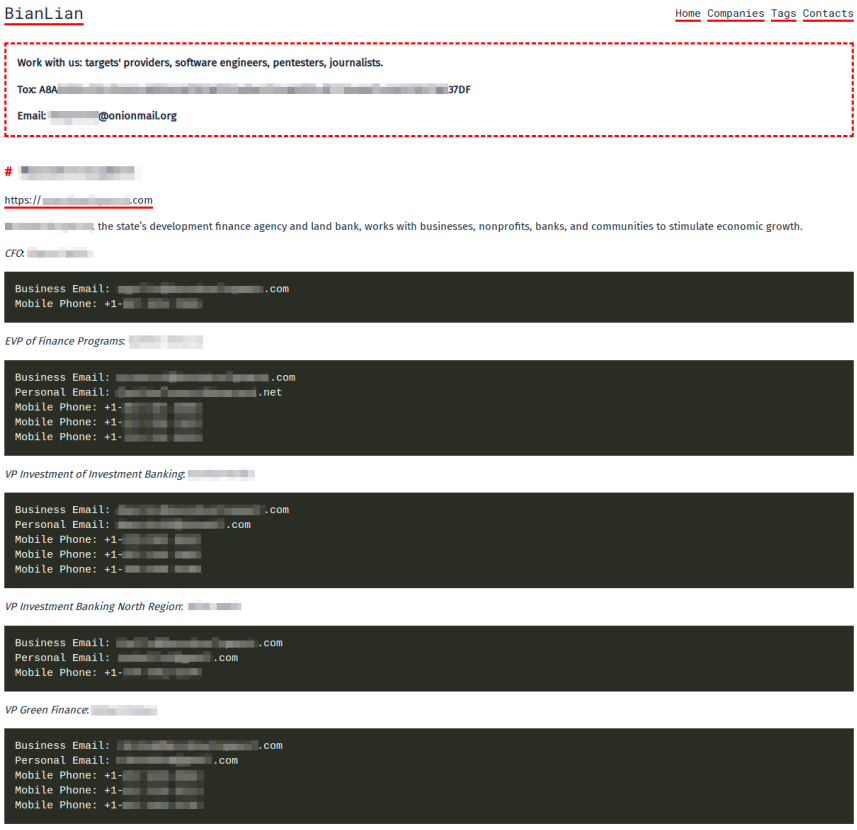
Internal Assets

This encompasses source code, secret hashes, secret keys, and database tables.

Sample Records

A sample of 30,000 records has been provided.

BianLian Targeted a State's Development Finance Agency



BianLian

Home Companies Tags Contacts

Work with us: targets' providers, software engineers, pentesters, journalists.

Tox: A8A[redacted]37DF

Email: [redacted]@onionmail.org

#

https://[redacted].com

[redacted] the state's development finance agency and land bank, works with businesses, nonprofits, banks, and communities to stimulate economic growth.

CFO:

Business Email: [redacted].com
Mobile Phone: +1-[redacted]

EVP of Finance Programs:

Business Email: [redacted].com
Personal Email: [redacted].net
Mobile Phone: +1-[redacted]
Mobile Phone: +1-[redacted]
Mobile Phone: +1-[redacted]

VP Investment of Investment Banking:

Business Email: [redacted].com
Personal Email: [redacted].com
Mobile Phone: +1-[redacted]
Mobile Phone: +1-[redacted]
Mobile Phone: +1-[redacted]

VP Investment Banking North Region:

Business Email: [redacted].com
Personal Email: [redacted].com
Mobile Phone: +1-[redacted]

VP Green Finance:

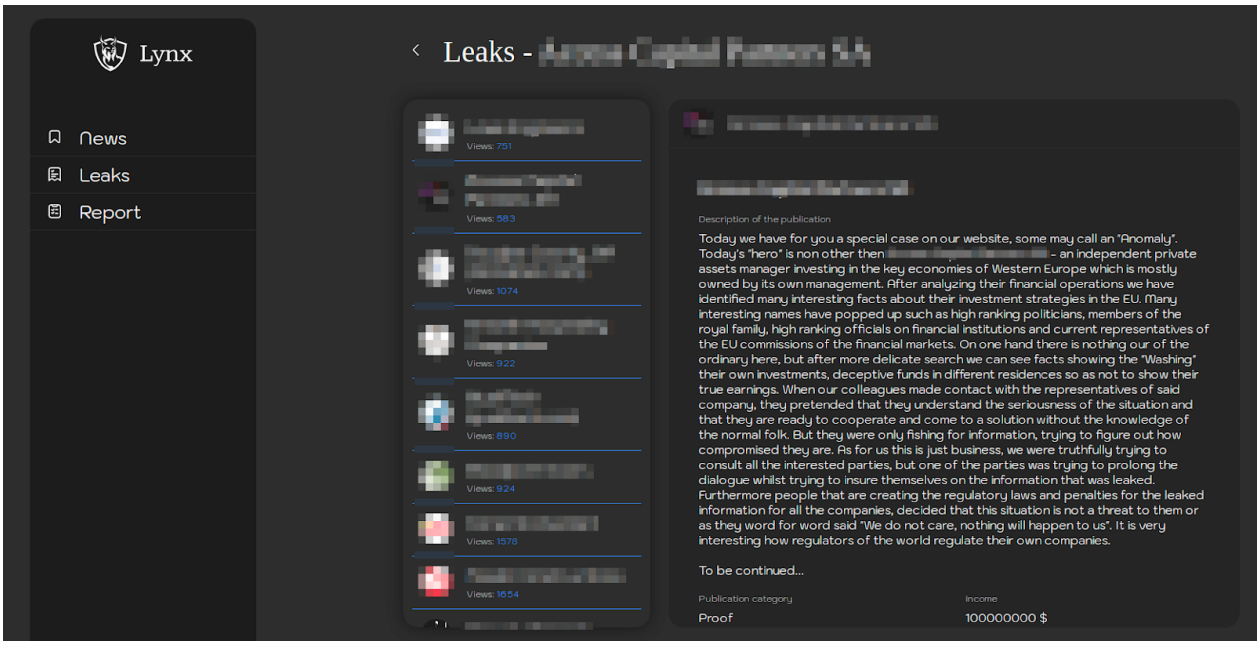
Business Email: [redacted].com
Personal Email: [redacted].com
Mobile Phone: +1-[redacted]
Mobile Phone: +1-[redacted]
Mobile Phone: +1-[redacted]

A recent post on a dark web forum associated with the BianLian ransomware group has allegedly listed a state agency as a victim of a ransomware attack. The claim was observed on the ransomware group's leak site, which is monitored by SOCRadar.

The Massachusetts-based development finance agency, plays a key role in fostering economic growth by supporting businesses, nonprofits, banks, and communities.

Threat Actor Card of BianLian *Ransomware Group*

Lynx Targeted a Private Asset Management Firm



A post, published on the Lynx ransomware group's website, has allegedly named a private asset management firm as their victim. The claims, which were monitored by SOCRadar, suggest that the firm, which primarily operates within Western Europe, has engaged in questionable financial activities. However, it is essential to emphasize that these remain unverified allegations originating from a threat actor.

The Lynx ransomware group, known for its cyber extortion tactics, asserted in its statement that their analysis of the company's financial operations revealed connections to high-ranking politicians, royal family members, financial institution officials, and EU commission representatives overseeing financial markets.

According to the post, while such associations are not necessarily unusual, the group claims to have uncovered practices that suggest investment fund manipulation and deceptive financial structuring across different jurisdictions.

Stealer Log Statistics

Stealer Log Statistics: Top Domains in the Finance Industry

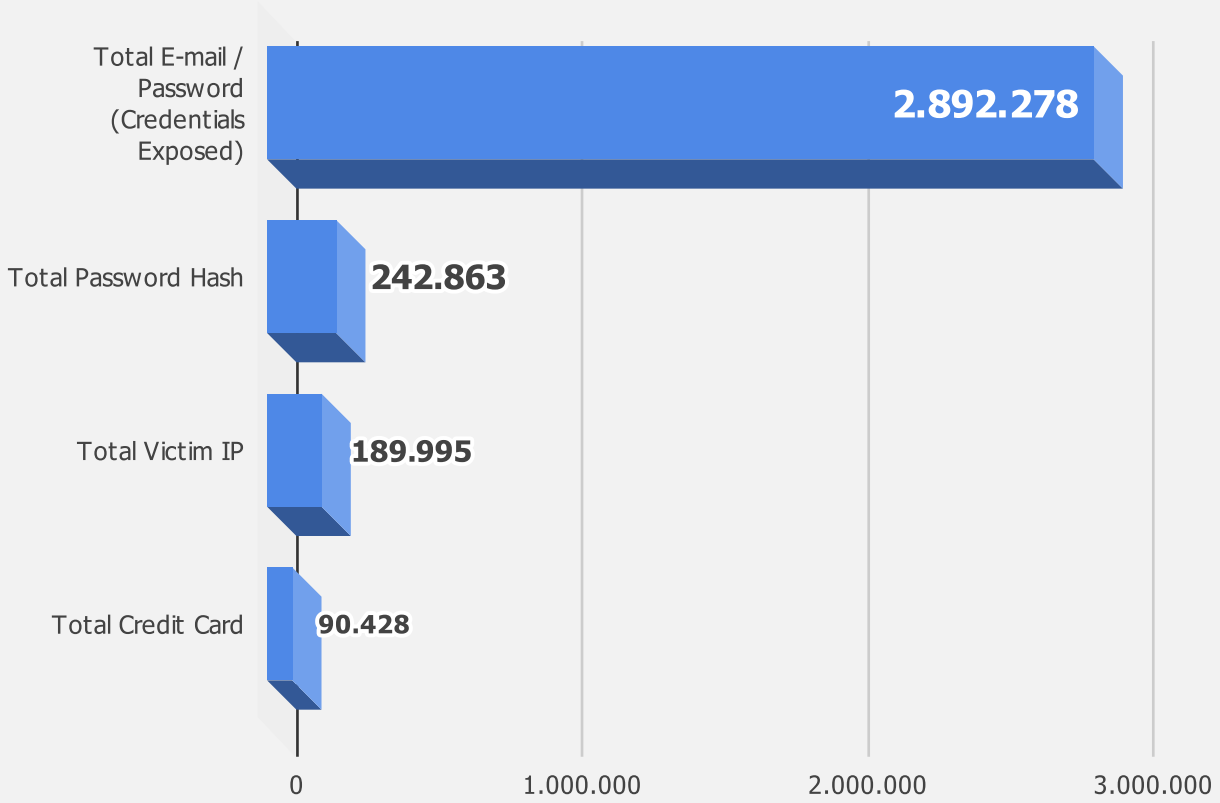
Stealers are a type of tool that collects sensitive data from victims' systems, primarily targeting login credentials, session tokens, and personal information. These logs, often produced by malicious software such as info stealers or keyloggers, can contain detailed information about the websites users visit, their login activities, and the credentials they input. Attackers use stealer logs to harvest credentials, gain unauthorized access to accounts, and orchestrate further attacks, including fraud, identity theft, or lateral movement within a network.

Monitoring and analyzing stealer logs is critical for identifying active threats and understanding attacker behavior, as these logs reveal which platforms are being targeted and how attackers are exploiting victims' data. By tracking these logs, organizations can gain valuable insight into high-risk domains, detect compromised accounts early, and implement targeted defensive measures to mitigate damage.

In order to detect these logs, it is useful to check the most visited domains in a specific country or industry. We analyzed the logs from the following domains in order to identify the leaked credentials that can be used to attack organizations in the financial sector.

Online Payment Systems	Banking and Financial Institutions	Cryptocurrency Platforms	Financial Services and Investment Platforms
paypal.com	chase.com	binance.com	robinhood.com
venmo.com	wellsfargo.com	kraken.com	fidelity.com
cash.app	hsbc.com	bitfinex.com	vanguard.com
zellepay.com	natwest.com	metamask.io	etrade.com
skrill.com	bankofamerica.com	coinbase.com	-

Stealer Logs - Distribution of the Compromised Data



The massive volume of exposed email/password combinations (2.89M) suggests:

- Large-scale credential harvesting operations
- High likelihood of credential stuffing attacks against financial services

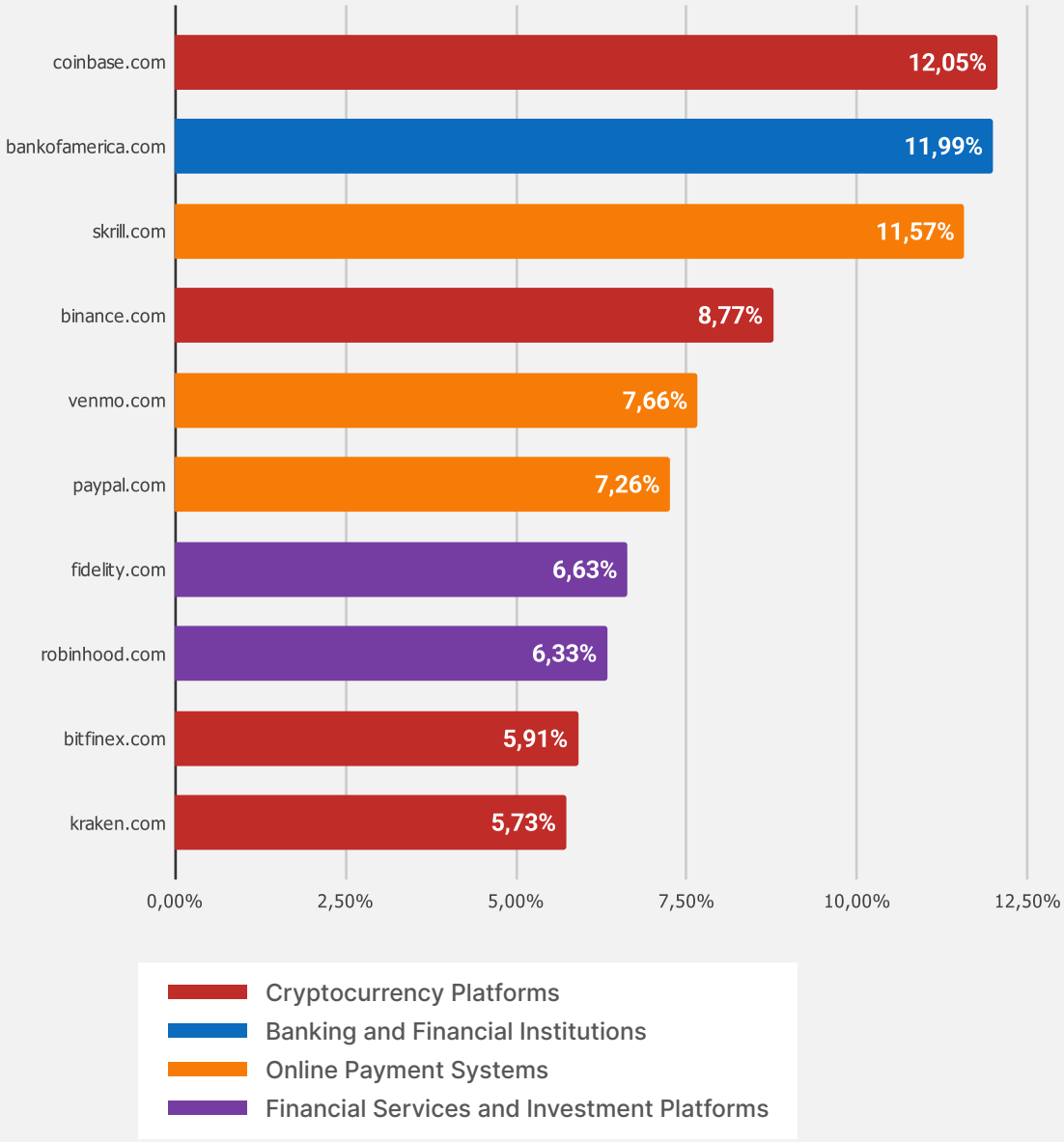
90,428 exposed credit cards represents a serious financial impact risk:

- Direct monetary theft potential
- Significant fraud risk for financial institutions

The reason behind the ratio of credentials to credit cards:

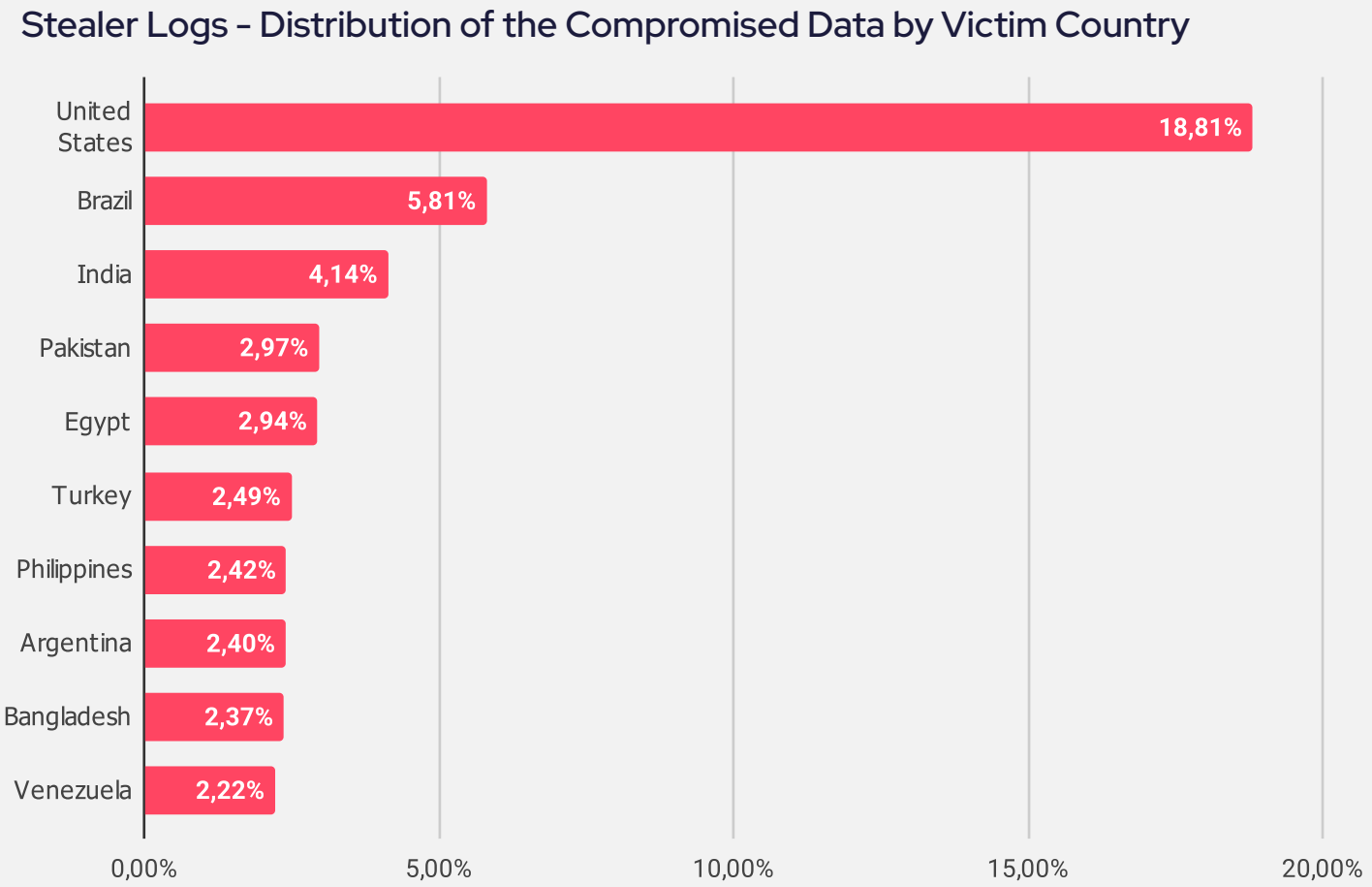
- Users generally have more accounts on other platforms than their bank accounts. A typical user might have 50 different accounts on social media platforms, educational platforms, email providers etc. combined. But an average human will have approximately 5-10 bank accounts in total.
- In addition to the previous point, people generally use mobile devices for financial applications in their daily lives. Generally, the stealer malware don't target mobile phones.

Stealer Logs - Distribution of the Compromised Data by Domains and Sub-Sectors



Diverse Financial Targets

- This diversity indicates that attackers are not focusing on a single type of user but are broadly targeting where stolen credentials could yield monetary benefits.
- Crypto platforms take the lead among financial institutions. Majority of victims have accounts on various crypto platforms.
- Payment services like Skrill (11.57%), Venmo (7.66%), and PayPal (7.26%) are attractive due to their role in fast, often less-regulated money transfers.
- Investment platforms such as Fidelity (6.63%) and Robinhood (6.33%) further round out the list, suggesting that attackers are keen to exploit any financial account that could facilitate quick financial gain.



Emerging market focus: Strong presence of developing economies (Brazil, India, Pakistan, etc.) indicates:

- Targeting of regions with growing digital banking adoption
- Focus on countries with potentially less mature security awareness
- Exploitation of regions with high cryptocurrency adoption rates

In addition to that, presence of countries with economic challenges (Venezuela, Turkey) implies:

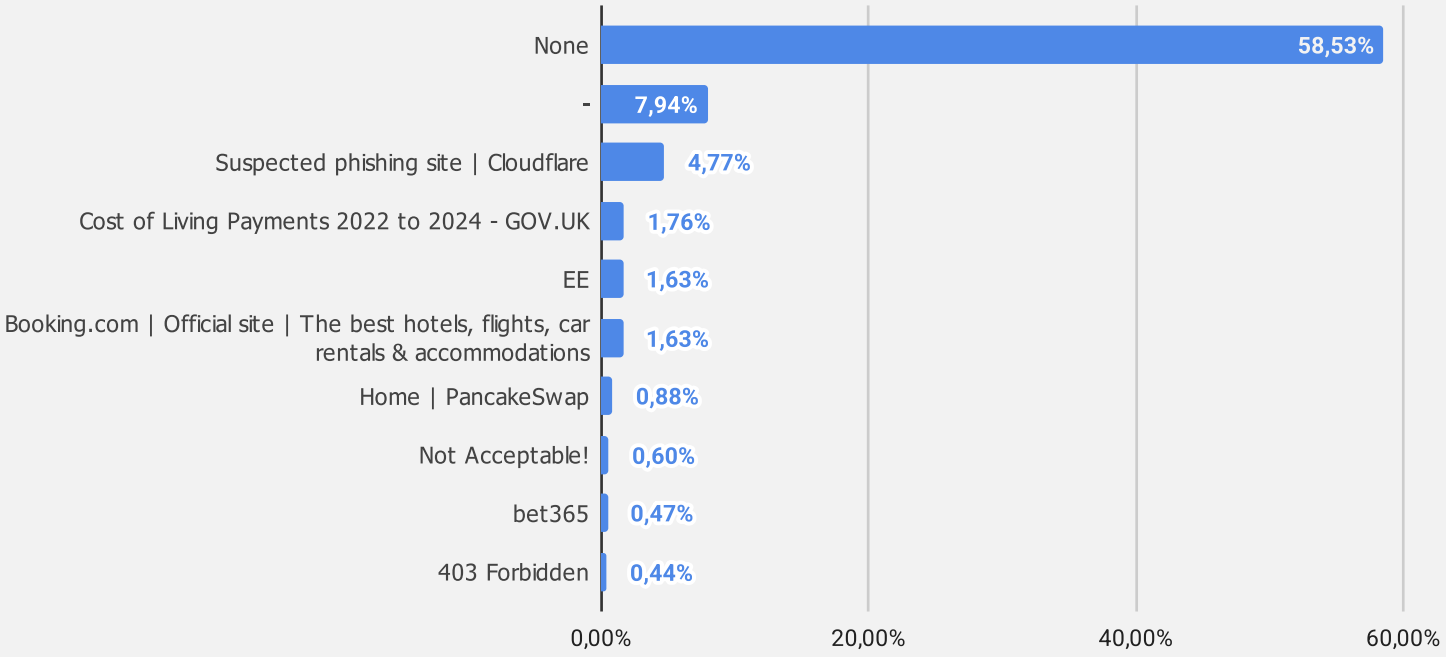
- Targeting of populations seeking alternative financial services
- Exploitation of regions with high cryptocurrency adoption
- Focus on areas with less regulated financial sectors

Economic pattern shift:

- Unlike ransomware data, Western European countries are notably absent, suggesting better endpoint protection in European markets, more careful users or users that are less prone to use suspicious websites.

Phishing Threats

Phishing Attacks - Distribution by Phishing Page Title



High Prevalence of Unbranded Phishing Pages:

66.47% of phishing pages lack a clear title ("None" and "-"). Threat actors may be using generic or dynamically generated titles to evade detection.

Government & Financial Themes (1.76%):

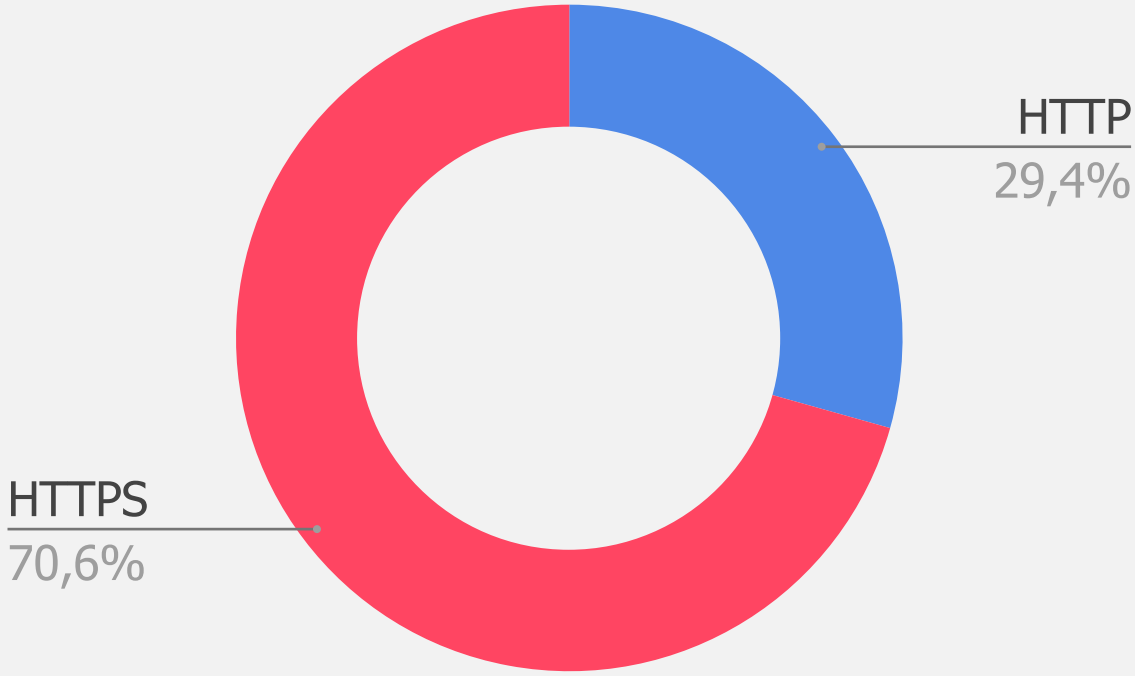
"Cost of Living Payments 2022 to 2024 - GOV.UK" suggests attackers are exploiting financial relief programs to target victims, likely attempting to steal banking credentials or payment details.

Brand Impersonation of Financial and E-commerce Services:

bet365 (0.47%) and Booking.com (1.63%) indicate attackers are targeting online payment users, possibly to steal credit card or account details.

PancakeSwap (0.88%) signals a risk for crypto investors, highlighting phishing threats in decentralized finance (DeFi).

Phishing Attacks - Distribution by SSL/TLS Protocol



Attackers overwhelmingly favor HTTPS over HTTP, suggesting a strong inclination toward encrypted channels for evading detection.

Malicious HTTPS Use Cases:

Threat actors leverage HTTPS for phishing, command-and-control (C2) communications, and data exfiltration while bypassing security controls that focus on unencrypted traffic.

Unencrypted HTTP Still Relevant:

Despite the lower count, HTTP instances indicate continued use in legacy exploits, credential harvesting, and man-in-the-middle (MitM) attacks.

Strategic Recommendations:

- Financial institutions should prioritize cryptocurrency-related security measures, given the clear shift in threat actor focus toward crypto platforms. This includes implementing enhanced authentication protocols and developing specific threat detection rules for crypto-asset operations.

- Organizations must strengthen their credential protection mechanisms in response to the widespread credential theft campaigns. This involves deploying robust endpoint detection and response (EDR) solutions to detect stealer malware, implementing Identity&Access solutions to detect stealer logs and compromised credentials, and regularly conducting credential compromise assessments with the help of CTI firms.

- Given the sophisticated commercialization of cyber threats, institutions should increase their focus on threat intelligence. The high percentage of selling and sharing activities in underground markets necessitates proactive monitoring of access brokers and data markets for early warning signs of potential compromises.

- Regional offices in emerging markets, particularly in South Asia and Latin America, require enhanced security controls and awareness programs. The increased targeting of these regions demands localized security strategies that account for regional threat patterns and user behavior.

- To counter the ransomware threat, particularly from dominant actors like LockBit 3.0, organizations should implement comprehensive backup strategies, network segmentation, and ransomware-specific incident response plans. The high concentration of attacks in North America and the UK requires organizations in these regions to maintain heightened security postures.

- Financial institutions should also establish dedicated security programs for their digital payment platforms, given the significant targeting of payment services. This includes implementing advanced fraud detection systems and enhancing transaction monitoring capabilities.

This proactive approach doesn't just make your organization more secure, it makes it more resilient. And since you've made it this far, why not take it a step further? Claim your *Free Dark Web Report* now and get actionable insights tailored to your needs.

Who is SOCRadar®?

Your Eyes Beyond

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.