CRYPTOCURRENCY & NFT
Industry Threat Landscape Report

SOCRadar®
Your Eyes Beyond

socradar.io

Table of Contents

Executive Summary

Top Takeaways

- **U.S. Dominance in Threat Mentions:** The United States is the most discussed target in dark web forums (19.47%), indicating its central role in global crypto and NFT activity.
- **Cybercrime Driven by Monetization:** Selling accounts for nearly 70% of threat activity, reflecting a dark web economy focused on monetizing stolen data and services.
- **Credentials Are the Primary Target:** Over 622,000 email/password pairs were exposed, far outpacing other compromised data types like credit cards or IP addresses.
- **Emerging Markets Hit Hardest:** Brazil, Pakistan, and Egypt lead in compromised user data, suggesting heightened risk in regions with rapidly growing crypto adoption but weaker defenses.
- **Crypto Exchanges Are Prime Targets:** Binance (38.73%) and Coinbase (32.59%) dominate in domain-related breaches, showing attackers prioritize platforms with direct access to funds.
- **Phishing Attacks Are Sophisticated:** 75% of phishing sites use HTTPS, and most impersonate trusted brands like Coinbase and Kraken, indicating efforts to boost credibility.
- **Data Sharing and Tools Proliferate:** Beyond selling, threat actors actively share data (23%) and offer tools/services (32%), supporting a robust cybercrime ecosystem.

Technical Details

This report based on data collected between May 2024 and April 2025

In the following chapters, you will be reading about the various aspects of the cyber threat landscape around the Crypto and NFT industry.

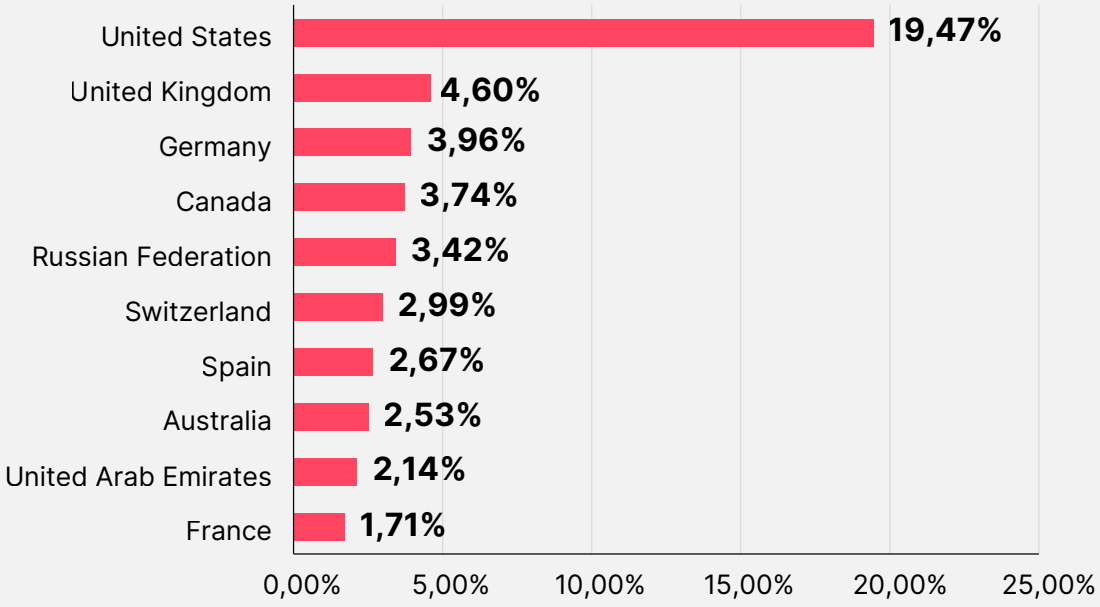
In the Dark Web Threats chapter, we will be covering the news and developments from Dark Web Forums, Telegram channels, Discord groups and so on. These are areas where threat actors with various skill sets come together, discuss, share tools and publish their alleged cyber attacks.

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.

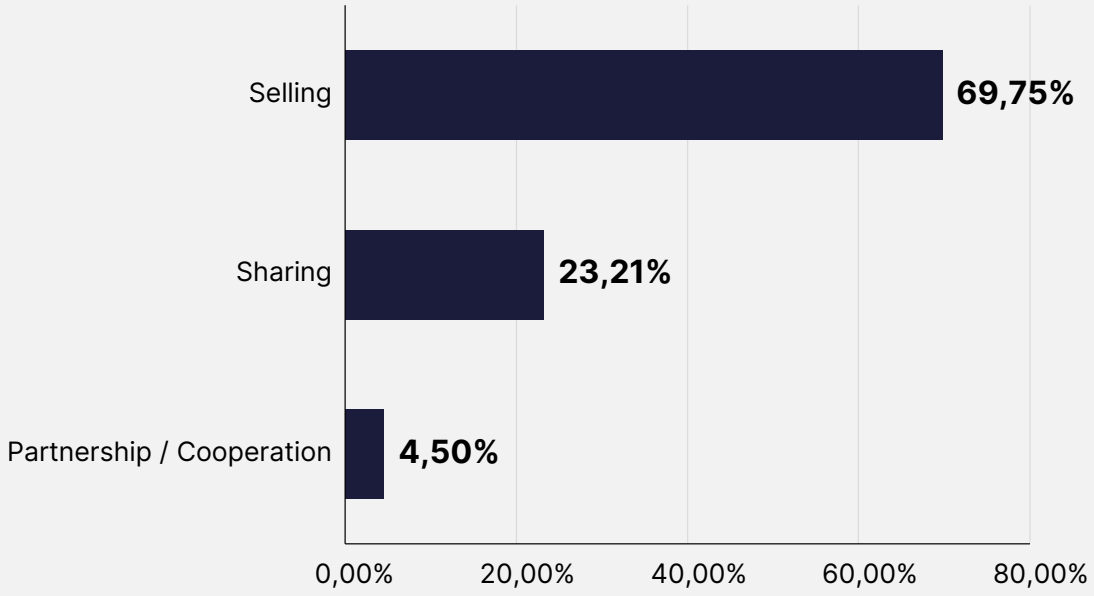
Dark Web Threats

Distribution of Dark Web Threats by Country



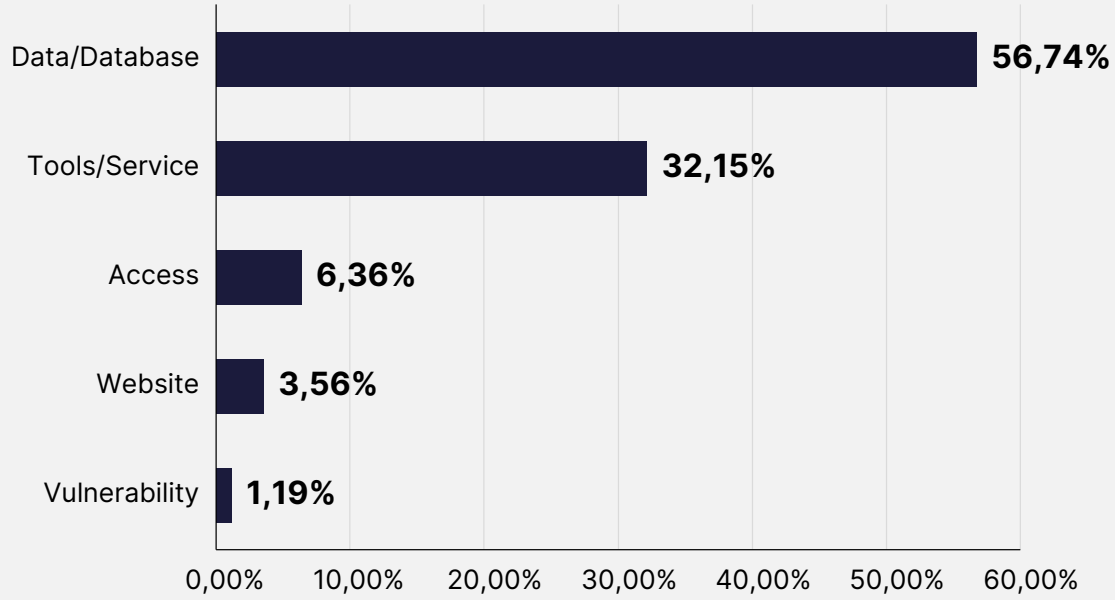
The United States is the primary target in dark web discussions and threat reports, accounting for nearly 20% of mentions which is over four times higher than the United Kingdom, the next most affected country. This suggests a disproportionate focus on U.S. based crypto and NFT activity, likely due to its large market presence. Other Western countries like the UK, Germany, and Canada also show notable activity. The spread indicates a global interest, with both economic hubs and crypto-adopting nations being key targets.

Distribution of Dark Web Threats by Threat Categories



The majority of dark web activity related to crypto and NFTs involves selling (nearly 70%), indicating a strong underground market for stolen assets, tools, or data. Sharing accounts for over 23%, suggesting active distribution of knowledge, tools, or leaks within the community. Partnerships and hack announcements are relatively low, highlighting limited collaboration or public disclosure of attacks. Buying and targeted attacks are minimal, reinforcing that the dark web is primarily used as a platform to monetize cybercrime, rather than coordinate complex operations.

Distribution of Dark Web Threats by Threat Types



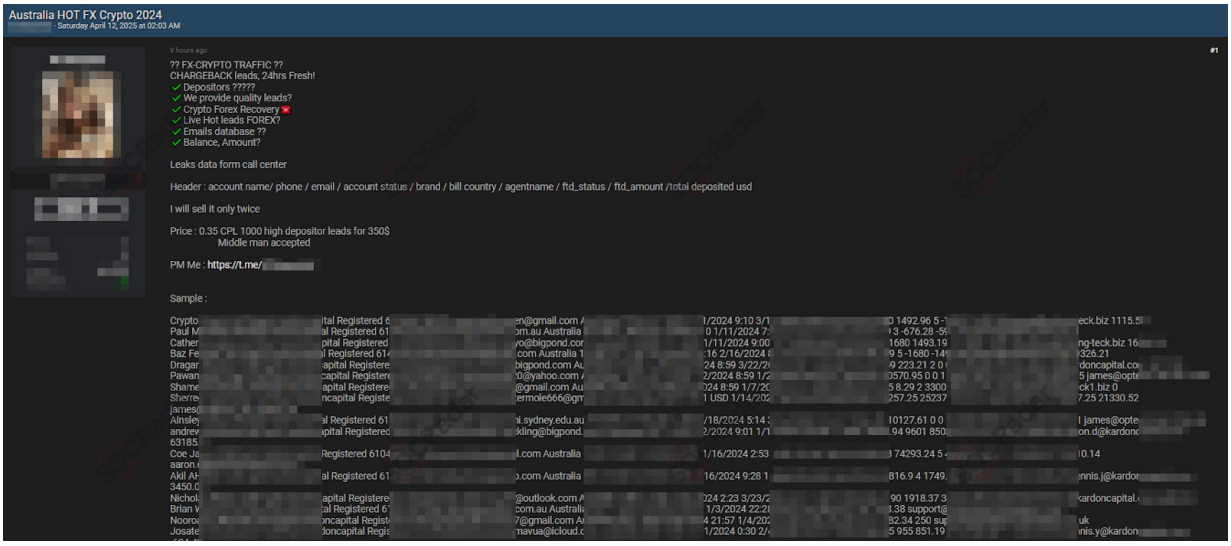
Threats related to data and databases dominate (56.74%), indicating a strong focus on leaking or trading stolen information, such as user credentials or transaction records. Tools and services (32.15%) are also prominent, suggesting active development and sale of malware, phishing kits, or laundering services. Access (6.36%) and website-related threats (3.56%) reflect attempts to breach platforms or exploit web infrastructure. Vulnerabilities are rarely discussed (1.19%), implying threat actors prefer exploiting known weaknesses or using ready-made tools over discovering new flaws.

Recent Dark Web Activities Targeting the Cryptocurrency & NFT Industry

Bybit Exchange Hack

Dubai-based crypto exchange Bybit lost $1.5 billion after hackers exploited a vulnerability during a routine wallet transfer. The attackers gained access to a developer's computer and inserted malicious code into the interface used for Bybit transactions. This tricked Bybit into signing off on a fake transaction, allowing the theft of 401,000 ETH. The stolen funds were then moved through multiple wallets to hide their trail, converted into other cryptocurrencies like BTC and DAI, and laundered using decentralized exchanges and no-KYC services. A portion of the funds remains idle, likely to avoid detection.

The Alleged Crypto Data of Australia are on Sale

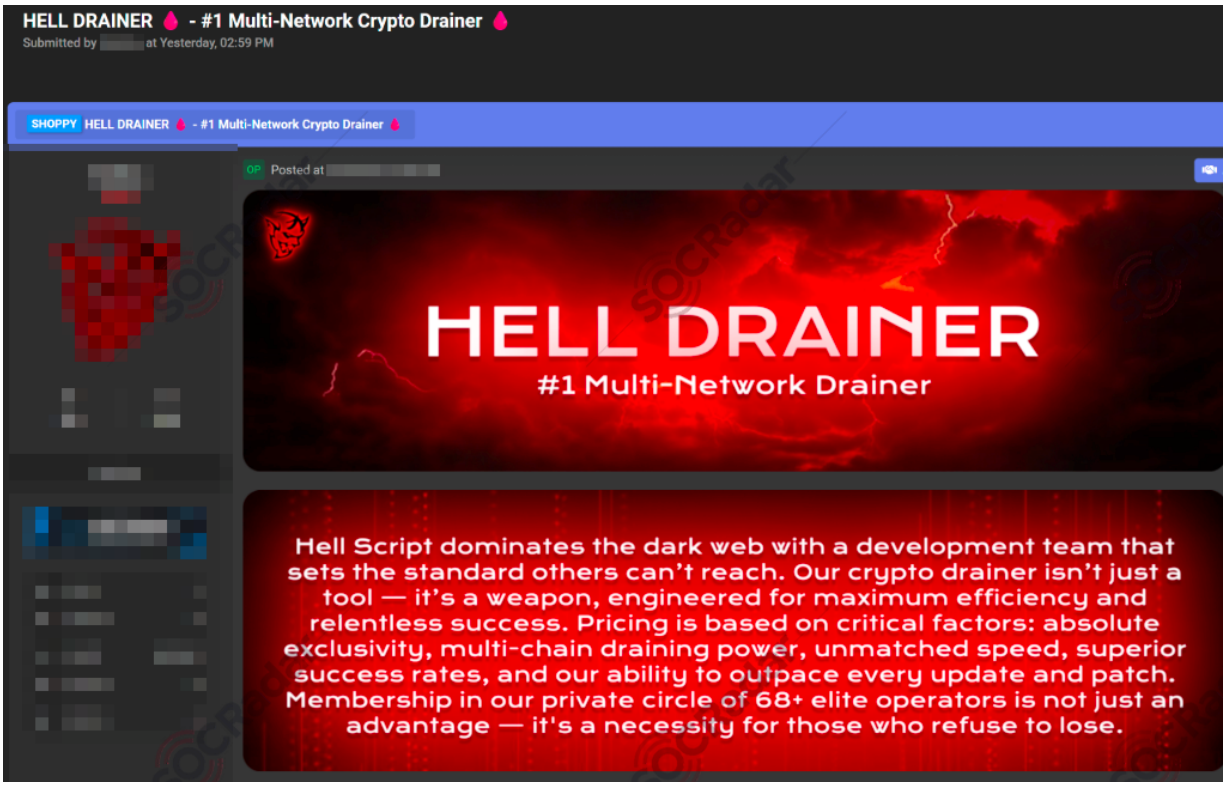


SOCRadar has identified a new data leak on a hacker forum, where an individual is advertising the sale of alleged crypto and forex-related user data linked to Australia. The post offers what the seller claims are fresh, "chargeback leads" and "high depositor leads" from a call center database.

The leaked dataset reportedly includes sensitive information such as account names, phone numbers, emails, account status, brand affiliation, billing country, agent names, first-time deposit (FTD) status and amount, and total deposited funds in USD.

The seller is offering 1,000 leads for $350, stating the data will be sold to only two buyers and is open to using a middleman to facilitate the transaction. A sample of the data was also provided in the post. Communication is being directed through a Telegram contact.

A New Alleged Hell Drainer Tool is on Sale



A threat actor on a dark web forum published a post promoting a wallet drainer known as "Hell Script". The post is selling an advanced crypto-draining tool marketed as a cutting-edge weapon for digital theft. The tool, described as more than just malware, promises high efficiency, multi-chain capabilities, and speed that outpaces security patches.

Hell Script claims its software is available only to a select group of over 68 members, positioning membership as essential for those seeking dominance in illicit crypto operations.

Stealer Log Statistics

What is a Stealer?

A stealer is a specialized form of malware engineered to exfiltrate sensitive information from infected devices. Stealers operate covertly, maintaining persistence while methodically collecting valuable data. Modern stealers can harvest credentials from browsers, extract cryptocurrency wallet information, capture authentication cookies and collect system information.

What are Stealer Logs?

Stealer logs are the compiled datasets of stolen information from infected devices. These logs typically contain:

- Browser-saved credentials (usernames and passwords)
- Session cookies and authentication tokens
- Cryptocurrency wallet information and private keys
- Personal information including names, addresses, phone numbers
- Financial data such as credit card information
- System information including hardware specifications, installed software, and IP addresses
- Corporate access credentials including VPN, email, and cloud service logins

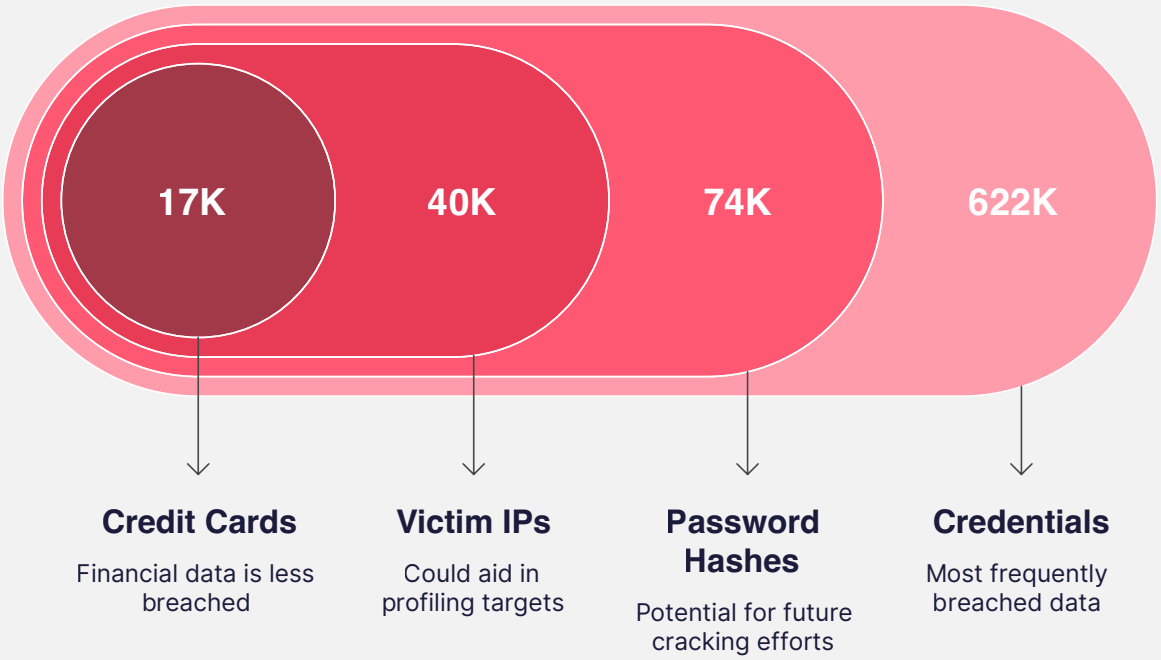
Once collected, these logs are either transmitted to command-and-control servers controlled by the threat actors or stored locally for retrieval. Threat actors then either use these logs themselves or sell them on underground marketplaces.

Stealer Log Statistics: Top Domains in the Cryptocurrency & NFT Industry

Top Domains

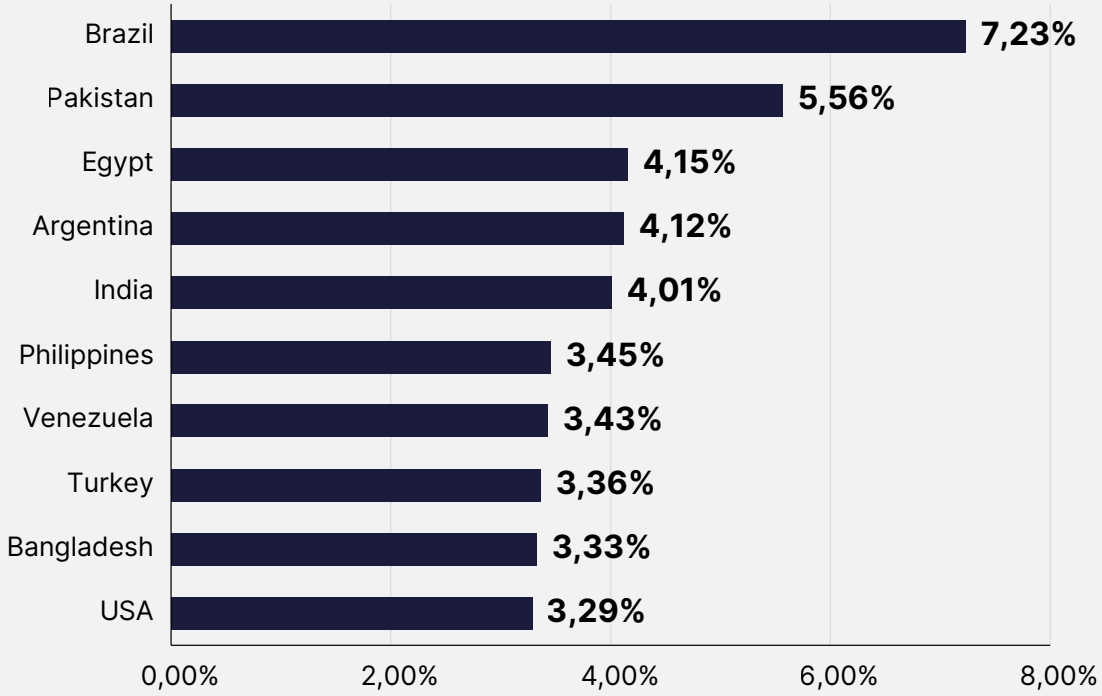
opensea.io
blur.io
magiceden.io
binance.com
coinbase.com
kraken.com
uniswap.org
metamask.io
rarible.com
foundation.app

Stealer Logs - Distribution of the Compromised Data

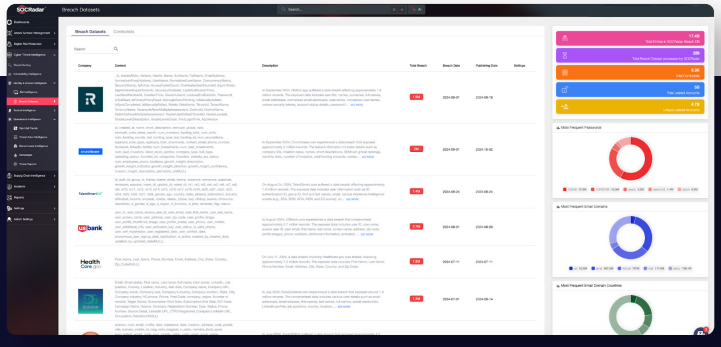


The vast majority of compromised data consists of email/password credentials (over 622K), highlighting a significant risk of account takeovers across crypto and NFT platforms. Password hashes (74K) suggest potential for future cracking efforts, while victim IPs (40K) could aid in profiling or further targeting. The exposure of 17K credit cards is notable but relatively smaller, indicating financial data is less frequently breached compared to login credentials. Overall, credentials are the primary commodity in this threat landscape.

Stealer Logs - Distribution of the Compromised Data by Victim Country



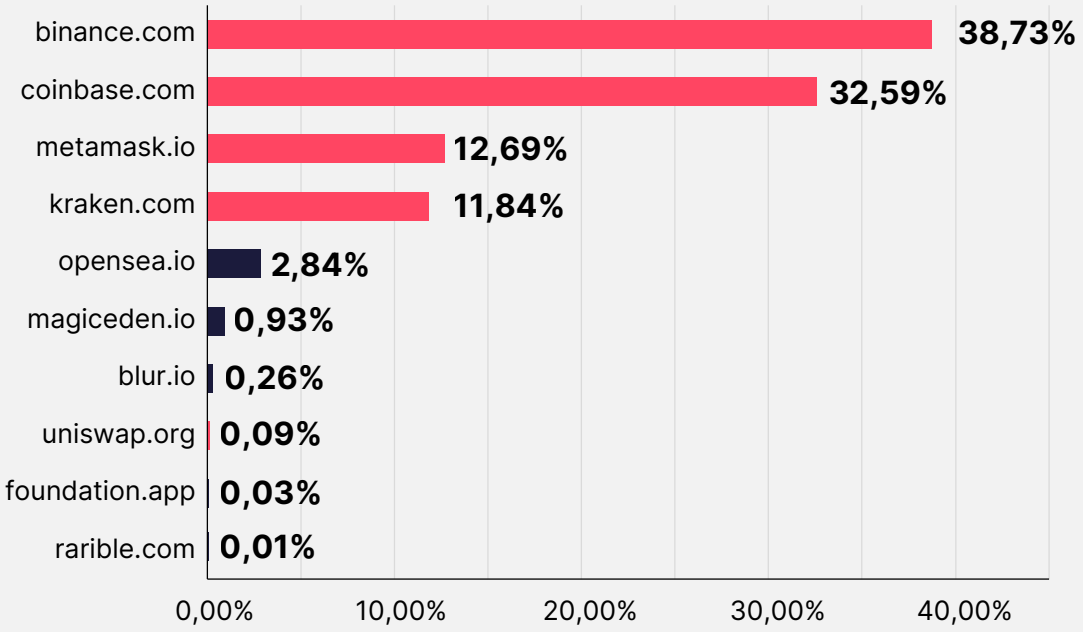
Brazil tops the list of countries with compromised data at 7.23%, followed by Pakistan and Egypt. Notably, emerging markets dominate the top ten, suggesting that users in these regions may be more vulnerable due to weaker cybersecurity practices or increased engagement with high-risk platforms. The USA ranks lower (3.29%) despite being a primary target on dark web forums, indicating that while the U.S. is frequently discussed, actual data breaches are more prevalent in developing countries.



SOCRadar's Identity & Access Intelligence Module

SOCRadar's Identity & Access Intelligence Module can detect stealers on your devices and identify their location, facilitating a secure working environment. Changing passwords without eliminating stealers is insufficient to secure your organization, as it will only provide new passwords to threat actors.

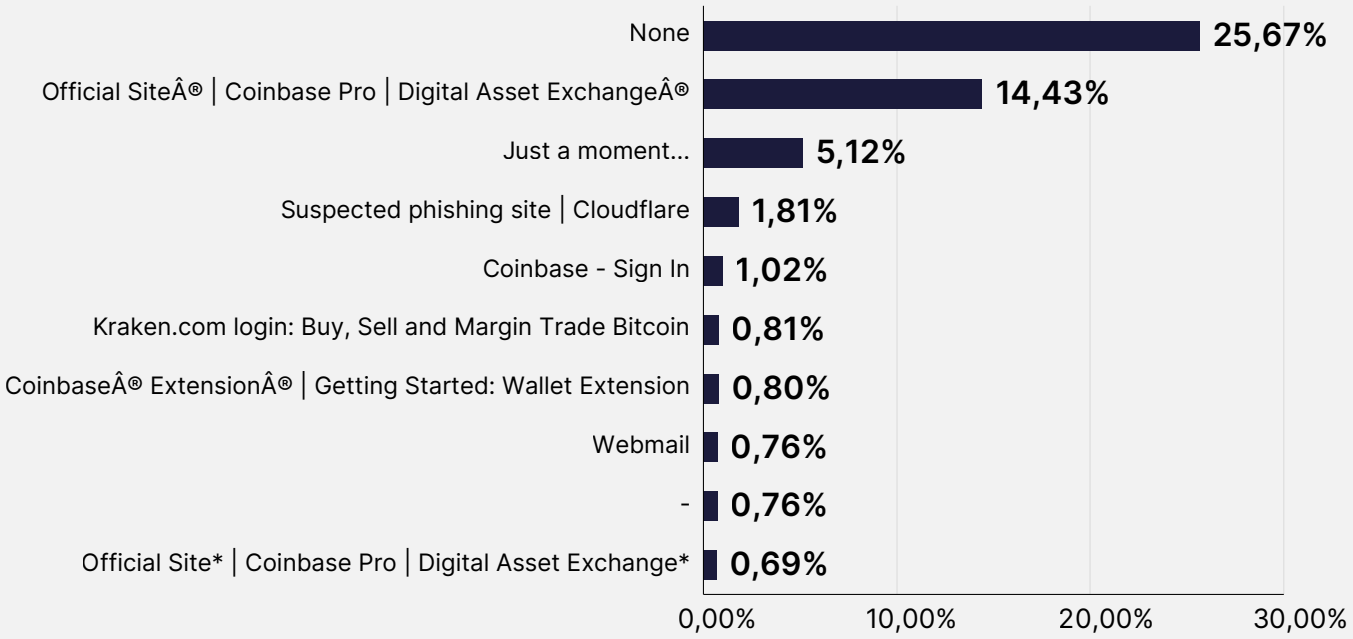
Stealer Logs - Distribution of the Compromised Data by Domains



The vast majority of compromised data is tied to cryptocurrency exchanges and wallets, with Binance (38.73%) and Coinbase (32.59%) alone accounting for over 70%. MetaMask and Kraken also show significant exposure. In contrast, NFT marketplaces represent a small fraction, with OpenSea leading at just 2.84%. This suggests attackers are primarily targeting platforms where funds and assets are stored or transacted, rather than marketplaces focused on digital collectibles.

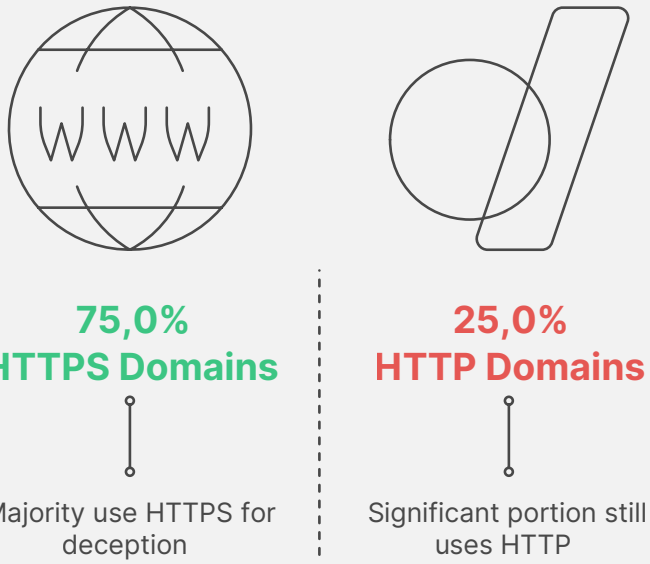
Phishing Threats

Phishing Attacks - Distribution by Phishing Page Title



Phishing attacks heavily mimic Coinbase-related services, with multiple variations of its login and wallet extension pages collectively accounting for a significant share. Titles like “Official Site | Coinbase Pro” and “Coinbase - Sign In” suggest attackers aim to deceive users with convincing replicas. Notably, 25.67% of phishing pages lack clear titles (“None”), likely to evade detection or indexing. Other common titles such as “Just a moment...” or security warnings may indicate pages impersonating security checks or exploiting trust in browser infrastructure.

Phishing Attacks - Distribution by SSL/TLS Protocol



A majority of phishing sites (75.04%) use HTTPS, indicating attackers increasingly adopt SSL/TLS to create a false sense of security and legitimacy. Despite the presence of encryption, these sites remain malicious. HTTP is still used in about 25% of cases, likely for quick deployments or targeting less tech-savvy users. This highlights that SSL is no longer a reliable indicator of trust, reinforcing the need for deeper threat detection methods beyond protocol checks.

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®?

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.