

Cryptocurrency & NFT

Threat Landscape Report
2024





Table of Contents

Executive Summary	3
Key Findings	5
Data-driven Overview	7
Getting to Know the Top Threat Actor: Chucky	12
Notable Cyber Security Incidents in The Industry	14
How Can SOCRadar Help?	25

EXECUTIVE SUMMARY

Within the Cryptocurrency and NFT industry, SOCRadar has diligently monitored around 1,700 unique Dark Web threats directed at systems and users from 2021 to the present.

Examining these threats on an annual basis reveals a notable trajectory. From 2021 to 2022, we observed an increase of approximately 37.2%, while transitioning from 2022 to 2023, a decrease of around 56.5% is notable. As of the first month of 2024, for now, 19 threats have been observed.

Analyzing the content of Dark Web data reported by SOCRadar; we observe that user data acquired by threat actors typically consists of critical information such as personal details, complete contact information, account, and wallet details, either in the form of cleartext lists or directly extracted databases. This compromised data is then either offered for sale or shared for free on Dark Web forums.

Simultaneously, we also note that some other reported Dark Web posts consist of Partnership/Cooperation offers initiated by threat actors

Further analysis of the exposed/sold data reveals that half of the compromised information is global user data. Regionally, the breakdown emphasizes the predominant regions, with 17.9% allocated to America, 15.7% to Europe, and 10.3% to Asia, highlighting the top three regions with the highest percentage distribution.



Focusing specifically on country-specific data, the majority of the exposed information encompasses global user profiles, incorporating diverse details from various countries. Upon closer examination, the top three countries with the highest percentage of compromised user information are the United States of America (18%), the United Kingdom (5%), and the Russian Federation (3%).

In summary, the **Cryptocurrency & NFT Threat Landscape Report 2024** provides a comprehensive analysis spanning from 2021 to the present, delving into the intricate dynamics of threats within the industry. The insights derived from this report aim to empower decision-making processes for organizations operating in the Cryptocurrency and NFT sectors. By shedding light on the potential risks and threats, this report equips both stakeholders and individual users with the knowledge necessary to fortify their security posture and effectively navigate the challenges posed by cybersecurity threats within the dynamic landscape of digital assets and transactions.

KEY FINDINGS



Comparing the threats reported by SOCRadar in the Cryptocurrency & NFT industry on an annual basis, there were 567 incidents in 2021 and 776 in 2022. However, in 2023, the number of threats targeting this industry on the Dark Web decreased to 338. As of the first month of 2024, only 19 threats have been reported.



The most prevalent threat in the Cryptocurrency & NFT industry is the compromise and subsequent sale of personal information of industry users on Dark Web forums.



The analyses conducted by SOCRadar's research team reveal that the majority of the approximately 1,700 unique Dark Web threats detected from 2021 to the present involve the sale of compromised user data on a global scale. Hence, threat actors targeting the Cryptocurrency & NFT industry pose a global threat to all users.



While the overall impact of Dark Web posts affects users globally, a regional breakdown indicates that predominantly United States of America (18%), United Kingdom (5%), and Russian Federation (3%) users are affected.

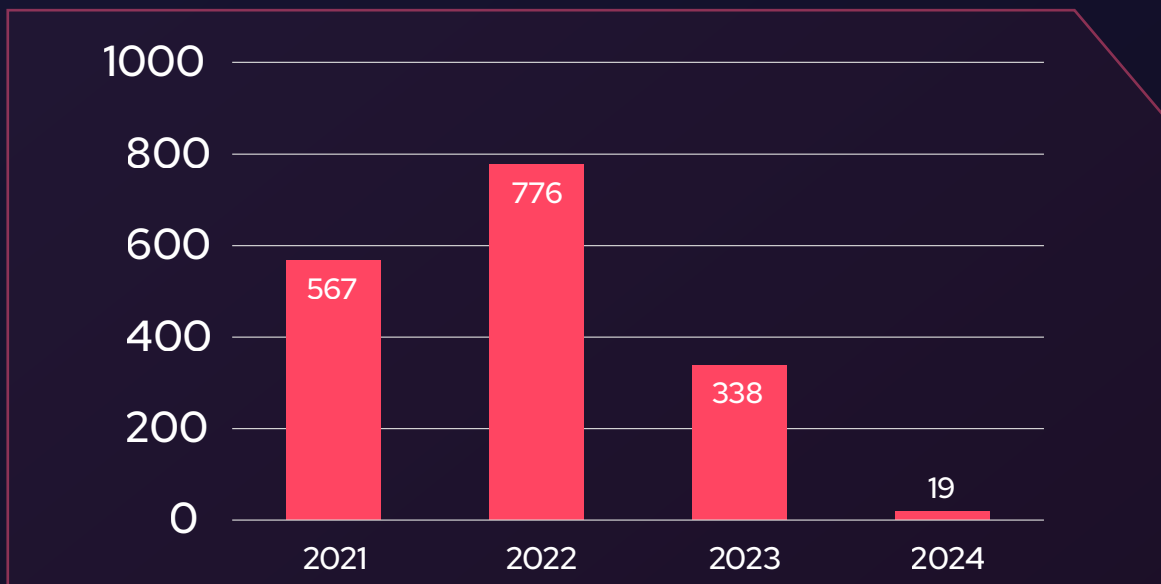


Despite a 56.5% decrease in the number of Dark Web threats reported by SOCRadar in 2023 compared to 2022, current statistics project that the total revenue in the Cryptocurrency & NFT market is expected to reach 51.5 billion US dollars by the end of 2024. This anticipation signifies a 26.5% increase compared to 2023. Therefore, it can be inferred that the industry will face intensified attacks by threat actors in 2024.

DATA-DRIVEN OVERVIEW

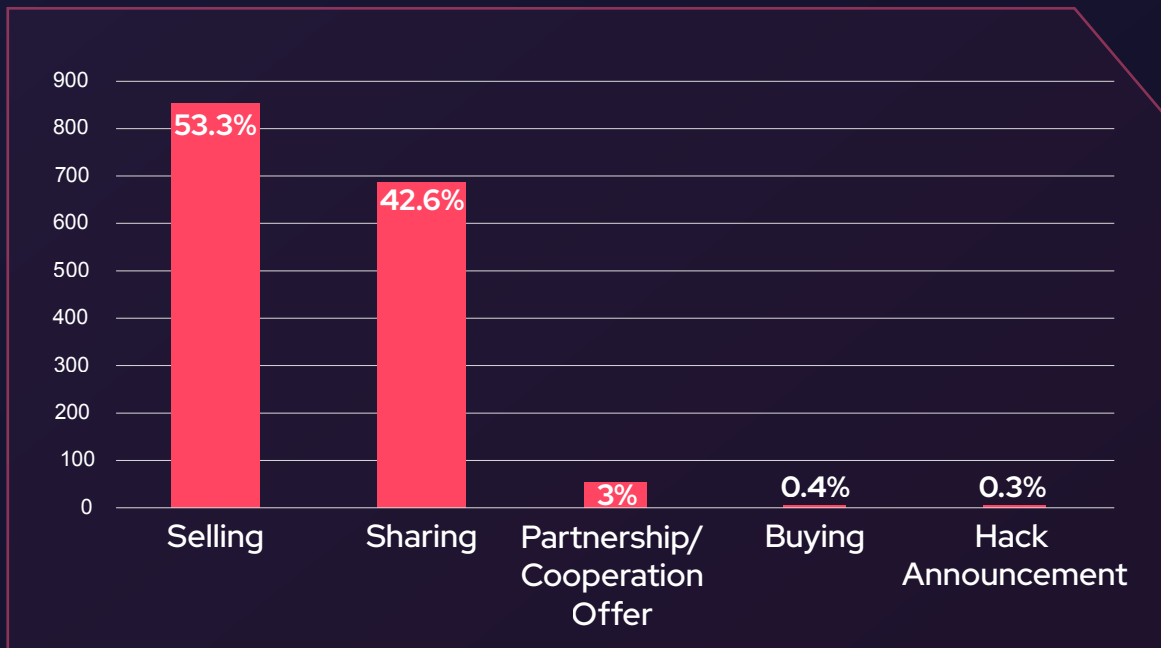
Cryptocurrency & NFT Threat Landscape unfolds vividly through graphical insights in this data-driven overview. These visual representations offer a concise yet detailed perspective on key statistics, illuminating the threat trends and patterns.

► Number of Reported Threats Over the Years



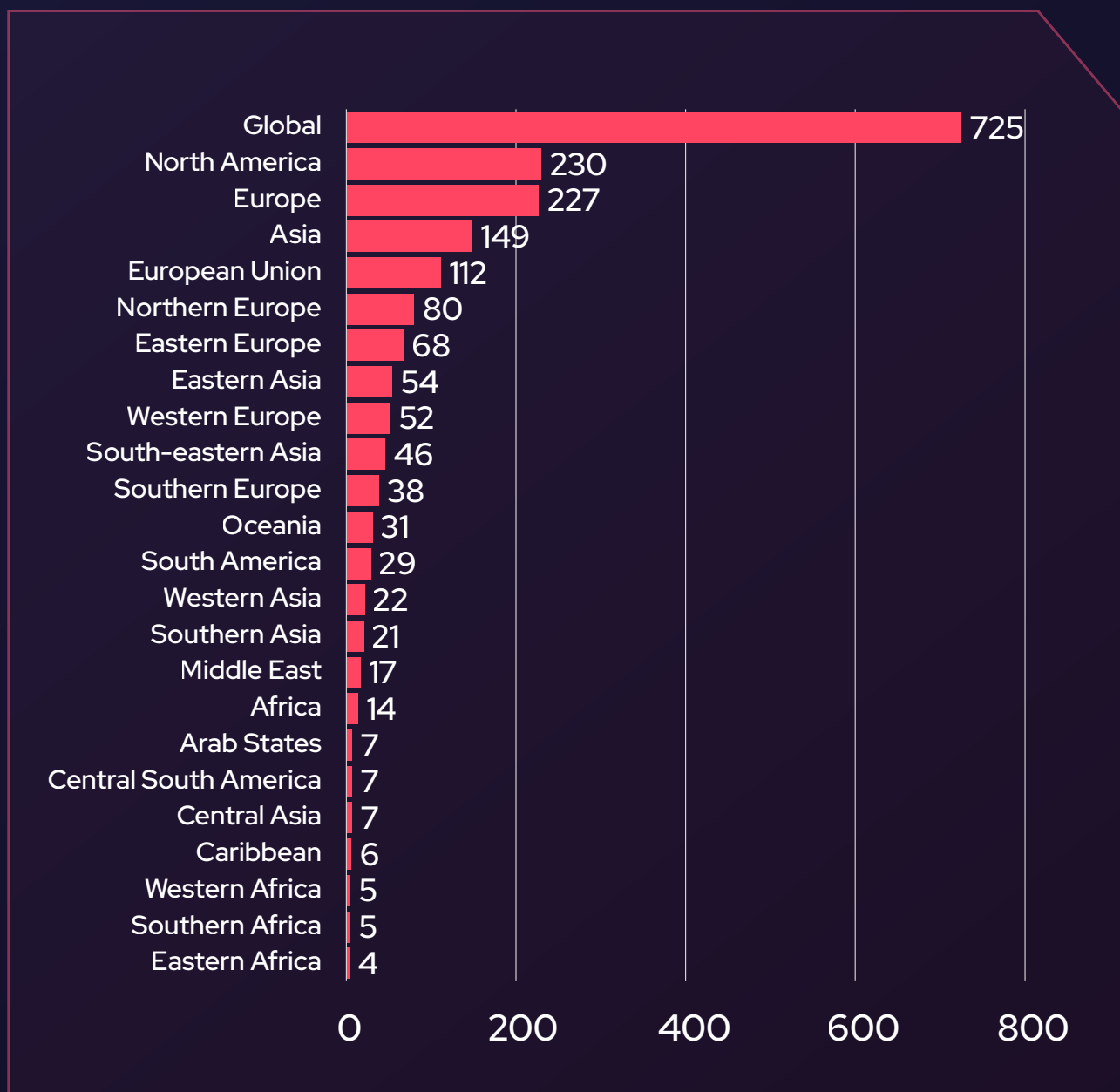
From 2021 to 2022, we observed an increase of approximately 37.2%, while transitioning from 2022 to 2023, a decrease of around 56.5% is notable. As of the first month of 2024, for now, 19 threats have been documented.

► Distribution by Threat Categories



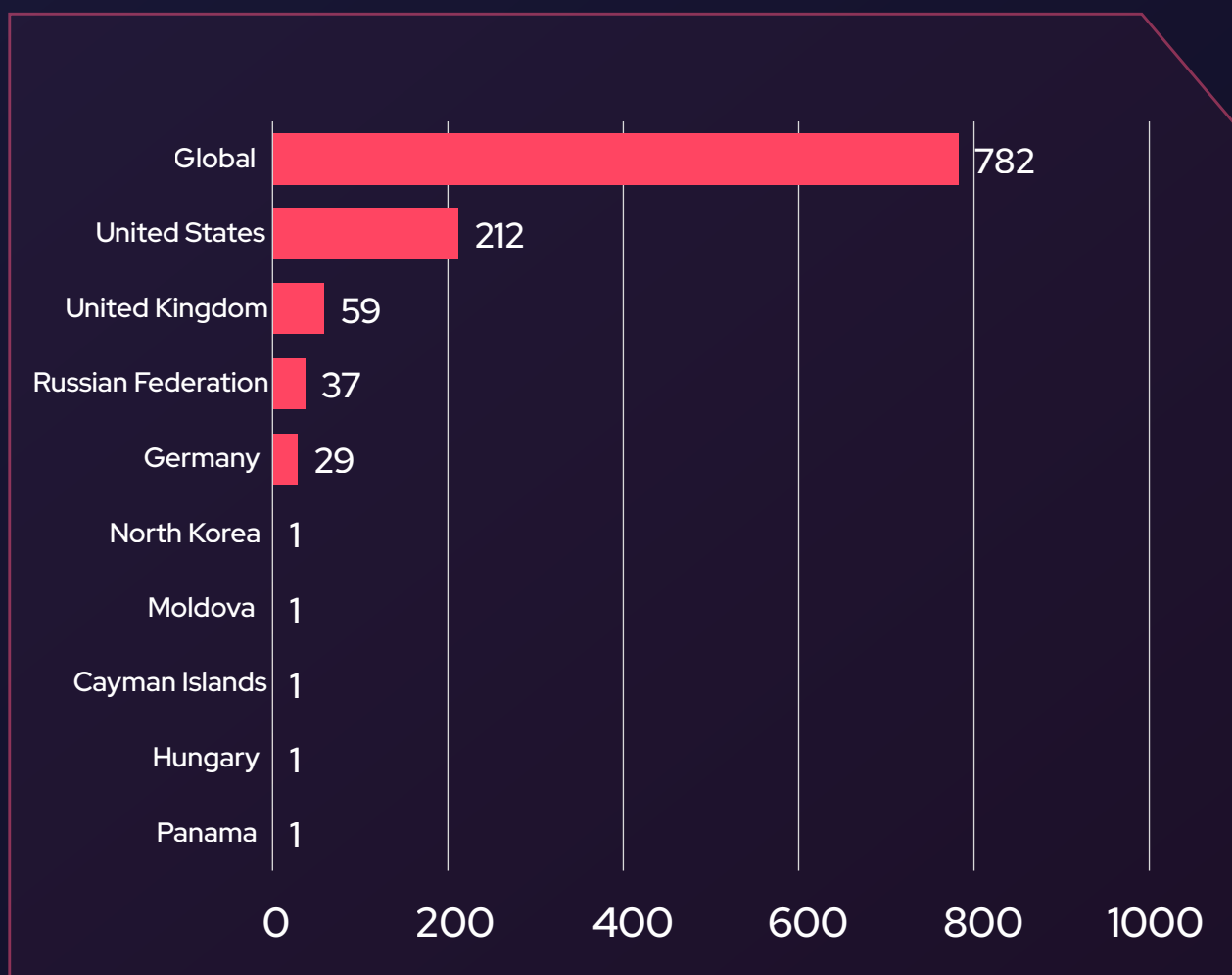
Upon closer inspection of reported Dark Web threats, it is evident that 53.3% of the data involves the sale of user information (Selling), with 42.6% being publicly exposed (Sharing). Additionally, 0.4% of the threats consist of data purchase announcements (Buying), while 0.3% falls under Hacking Announcements.

► Distribution of Threats by Region



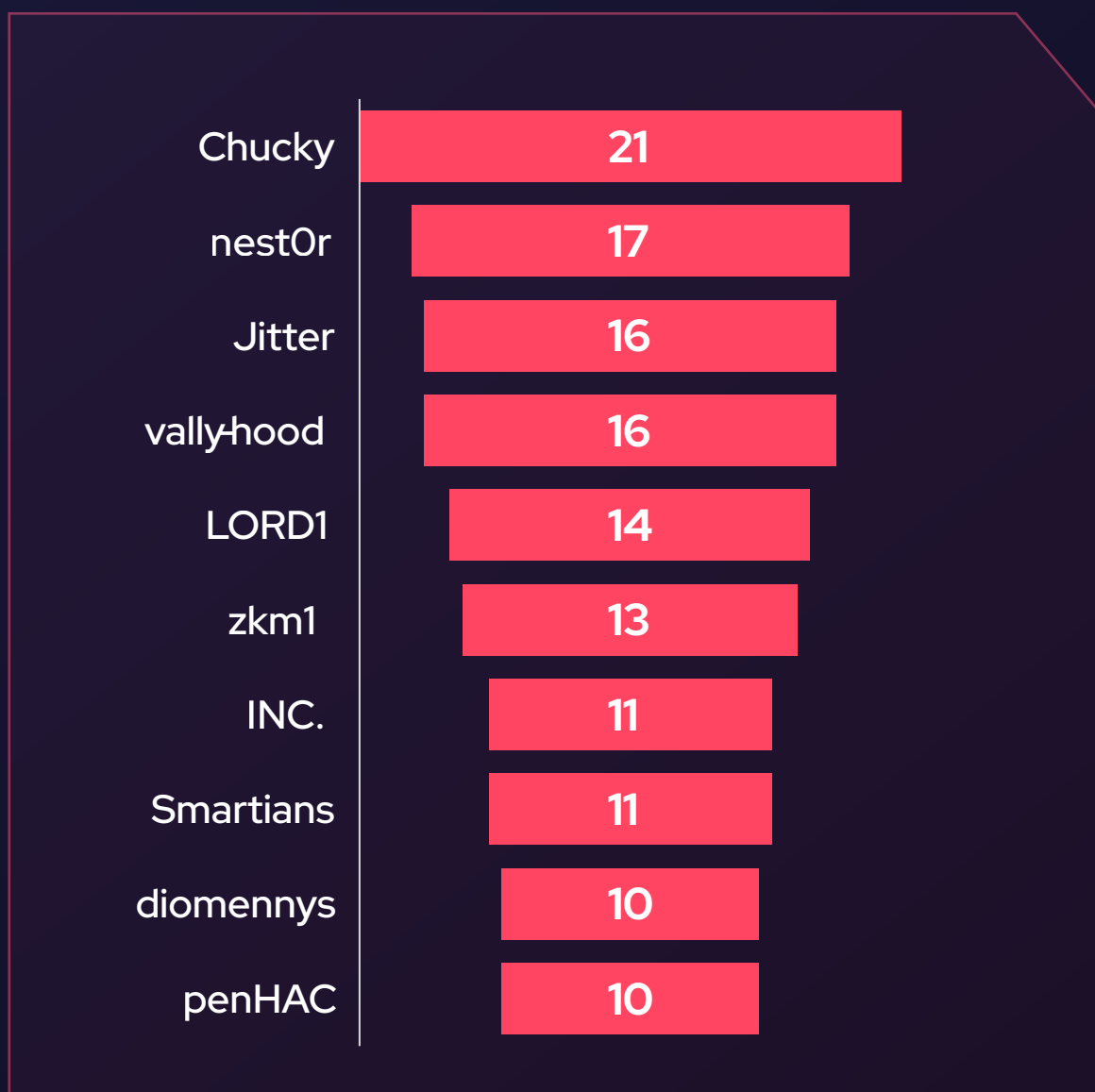
The global perspective comprises 725 incidents, with North America and Europe closely following at 230 and 227, respectively. Asia represents 149 incidents, while the European Union accounts for 112. These figures emphasize the concentration of threats in the top five regions, with North America, Europe, Asia, the European Union, and Northern Europe standing out as the most affected areas.

► Distribution of Threats by Country



The graph reveals that the majority of the exposed information is of global nature, with 782 incidents. Delving into the top three countries with the highest percentage of compromised user information, the United States leads with 212 incidents, followed by the United Kingdom at 59, and the Russian Federation at 37. Germany and North Korea also demonstrate notable instances, with 29 and 1 incidents, respectively.

► Top 10 Threat Actors



The graph above illustrates the Top 10 Threat Actors in the Dark Web landscape associated with the Cryptocurrency & NFT industry. Each segment represents the contribution of a specific threat actor to the total incidents reported. This visual representation allows for a quick and informative overview of the key actors involved in potential cyber threats within the analyzed period.

GETTING TO KNOW THE TOP THREAT ACTOR:

CHUCKY


Chucky, also known by aliases such as LeakBase, Sqlrip, and Chuckies, is a significant threat actor active across various underground forums. Operating under multiple monikers, especially LeakBase, Chucky shares vast collections of databases, often containing sensitive information from global entities.

LeakBase, one of Chucky's identities, was previously known for providing data breaches and had reportedly faced shutdown in 2017. However, recent activities indicate a resurgence, with the actor regularly sharing new collections of databases, including those obtained via unauthorized means.

One of the most notable attacks attributed to this threat actor is the breach of the Swachh Bharat Mission's swachh.city platform, which is run by the Ministry of Housing and Urban Affairs, threatening exposure of critical information of 16 million Indian users. Then, LeakBase posted a 6GB data dump on BreachForums in September 2022. This incident underscores the significant impact of Chucky's activities on both individuals and organizations alike.



Members



Chucky

Staff member Moderator

Expert SQL

Joined: 972 day ago

Last seen: Today at 7:46 AM

User ID	Messages	Solutions	Link directory items	Reaction score	#CR
1	4,130	1	40	21,745	43

Follow Start conversation Find

Profile posts Latest activity **Postings** Link directory items About

6K_Files_Passwords.txt [Logs](#) [Chucky](#) [Premium](#)

*** Hidden text: You do not have sufficient rights to view the hidden text. Visit the forum thread! ***

Chucky Thread · Today at 4:18 AM · Replies: 0 · Forum: Private Logs & Passwords

19K_Files_Passwords.txt [Logs](#) [Chucky](#) [Premium](#)

*** Hidden text: You do not have sufficient rights to view the hidden text. Visit the forum thread! ***

Chucky Thread · Today at 4:17 AM · Replies: 0 · Forum: Private Logs & Passwords

X150 Good Ftp Serv + Full Log [FTP](#) [Chucky](#)

*** Hidden text: You do not have sufficient rights to view the hidden text. Visit the forum thread! ***

Chucky Thread · Yesterday at 8:35 PM · Replies: 4 · Forum: FTP & Hosting Acces

450Gb Fatelogs Packs [64Files Packed] [Logs](#) [Premium](#)

*** Hidden text: You do not have sufficient rights to view the hidden text. Visit the forum thread! ***

*** Hidden text: You do not have sufficient rights to view the hidden text. Visit the forum thread! ***

Chucky Thread · Yesterday at 6:02 PM · Replies: 0 · Forum: Private Logs & Passwords

Posts made by Chucky on leakbase.io

The screenshot showcases the activities of the threat actor known as Chucky (also referred to as Leakbase) on Leakbase.io, where there are numerous significant posts in the platform.

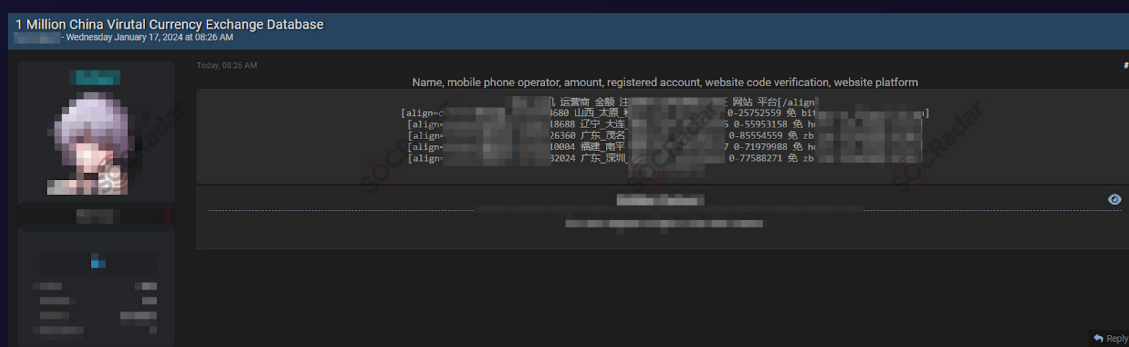
NOTABLE CYBER SECURITY INCIDENTS IN THE INDUSTRY

In this section, we delve into recent occurrences, meticulously identified by SOCRadar on the Dark Web within the Cryptocurrency & NFT industries. This segment provides an in-depth exploration of specific incidents, shedding light on noteworthy threats and malicious activities. Our analysis is grounded in real-time insights derived from the SOCRadar platform, offering a comprehensive view of the evolving cyber threat landscape.

Database of a Chinese Virtual Currency Exchange is Leaked

17 Jan
2024

In a hacker forum monitored by SOCRadar, a new alleged database leak is detected for a Chinese virtual currency exchange. The leaked database contains sensitive information of users, including names, mobile phone numbers, amounts, registered accounts, website code verification, and website platforms.

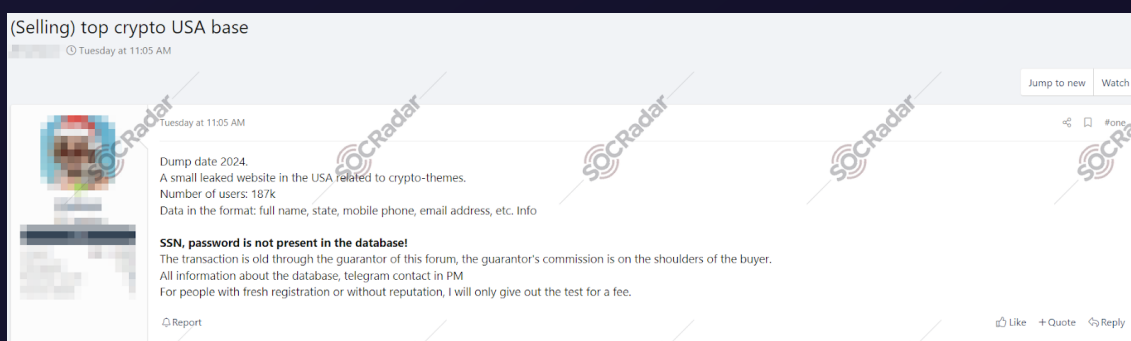


Database breach aftermath: Stolen data being sold on a hacker forum

Data of an American Crypto Website are on Sale



In a hacker forum monitored by SOCRadar, a new alleged data sale is detected for an American crypto website. The data of an American crypto website is being sold on a hacker forum, potentially exposing the personal information of 187,000 users. The data includes full name, state, mobile phone, and email address, but does not include SSN or password.



Stolen data being sold on a hacker forum

CoinCollector V4 Tool is Shared

15 Jan
2024

The CoinCollector V4 tool is being shared in a hacker forum, indicating that it may be used for malicious purposes. The tool is designed to collect cryptocurrency from multiple faucets, which could potentially lead to financial losses for users. The tool is capable of automatically creating accounts and checking earnings, making it easier for attackers to exploit unsuspecting users. As the tool is being shared with download links, this could potentially lead to malware infections or other security breaches.

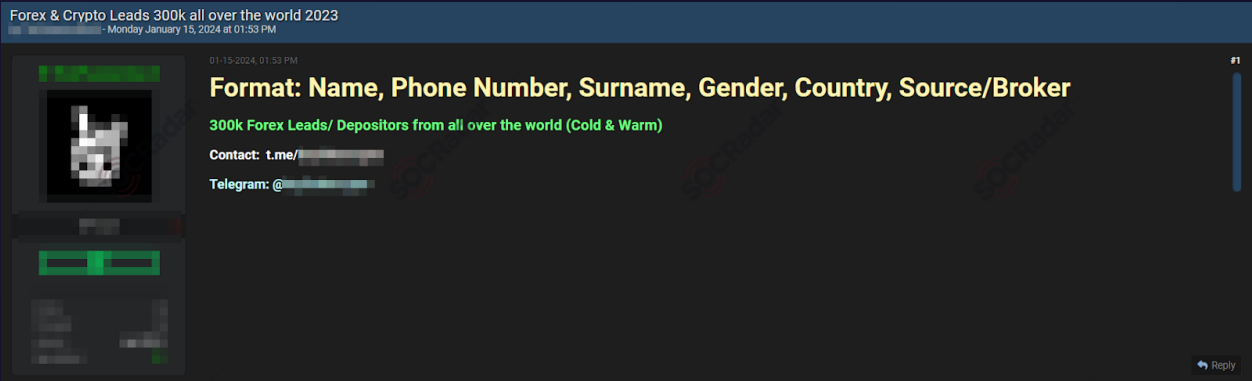
[illegible]

CoinCollector V4 tool shared in hacker forum, posing potential risks

Forex and Crypto Leads Data of Worldwide are on Sale



In a hacker forum monitored by SOCRadar, a new alleged forex and crypto leads data sale is detected for Worldwide. The data includes personal information such as names, phone numbers, surnames, gender, country, and the source or broker. The sale of forex and crypto leads data indicates a data breach or compromise of a database containing this information. This breach could have occurred due to vulnerabilities in the systems of the forex or crypto platforms, or through phishing attacks or malware infections.

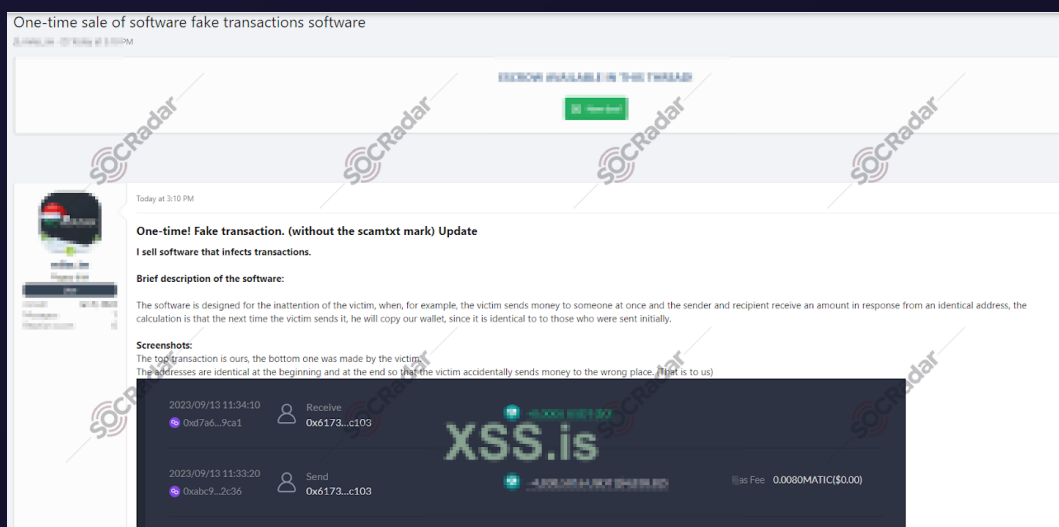


Forex and crypto leads data sale detected

New Fake Transaction Tool is on Sale

14 Jan
2024

The dark web is being used to sell a new fake transaction tool that can be used to trick victims into sending money to the wrong address. The tool works by creating a fake wallet address that is similar to the victim's intended recipient address. The victim is then tricked into sending money to the fake address, believing that they are sending it to the intended recipient.



Fake transaction tool shared on a hacker forum

Customer Database of Bitkub is on Sale

11 Jan
2024

A hacker forum monitored by SOCRadar has detected the sale of an alleged customer database belonging to Bitkub, Thailand's largest cryptocurrency exchange. The database reportedly contains sensitive information of approximately 1 million Bitkub customers, including names, email addresses, and phone numbers. This data could be exploited for various malicious activities such as phishing attacks, identity theft, and targeted scams.

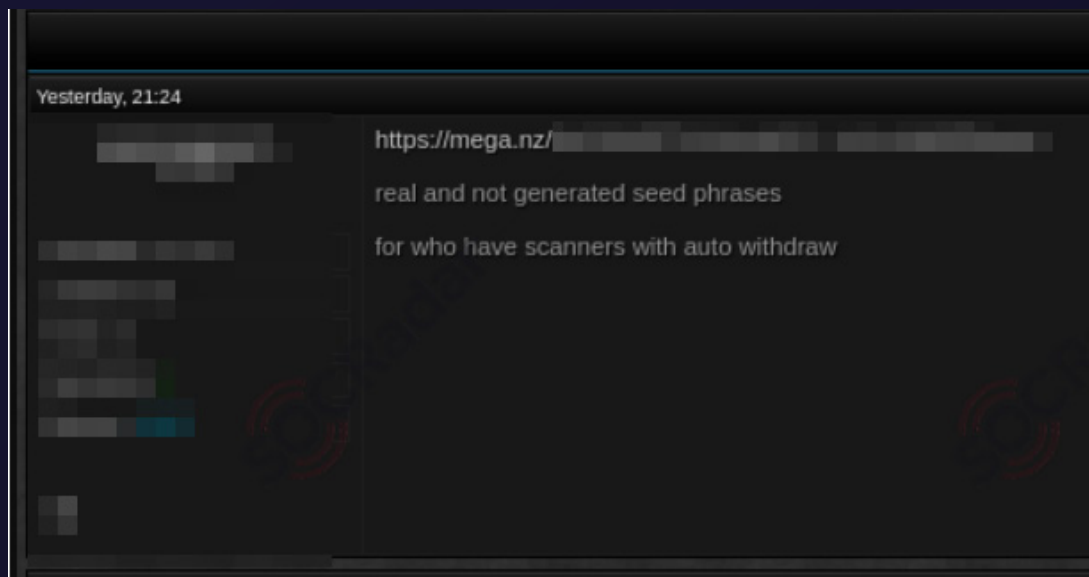


Database breach aftermath: Stolen data being sold on a hacker forum

A New Seed Phrase Scanner Tool is Shared

9 Jan
2024

The dark web news pertains to the sharing of an alleged seed phrase scanner tool in a hacker forum monitored by SOCRadar. The tool is claimed to scan for real and non-generated seed phrases, potentially enabling attackers to withdraw cryptocurrency funds from victims' wallets. The reported auto-withdrawal feature of the tool further exacerbates the risk, as it automates the process of transferring funds from victims' wallets, making it easier for attackers to steal cryptocurrency without manual intervention.

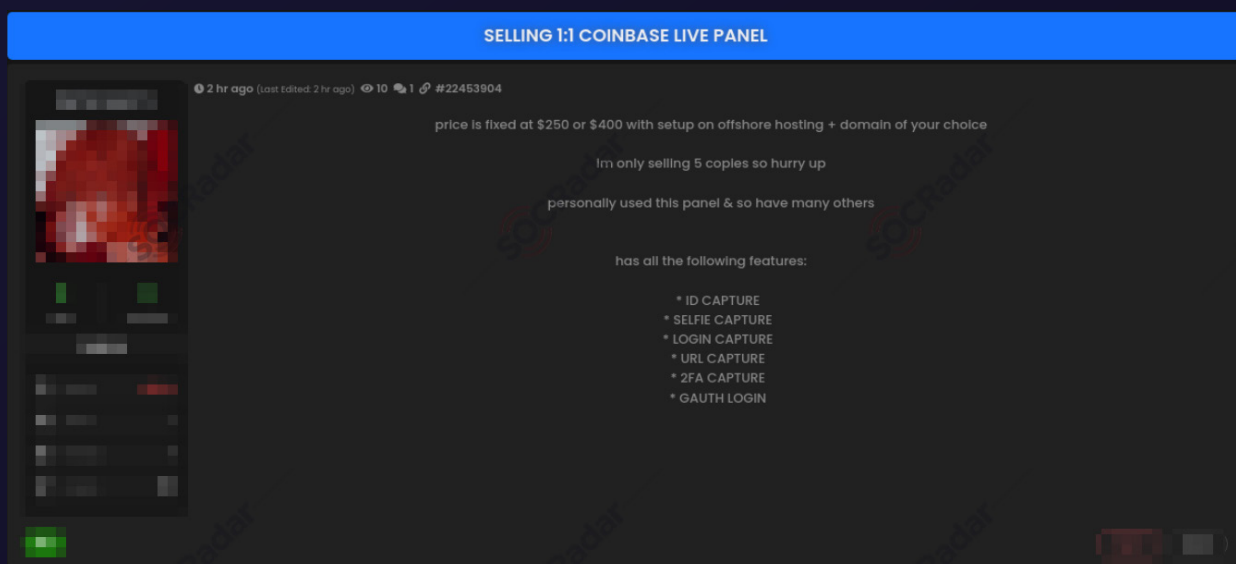


Seed Phrase Scanner tool being shared on a hacker forum

Live Panel of Coinbase is on Sale

8 Jan
2024

The dark web news pertains to the sale of a live panel for Coinbase, a cryptocurrency exchange platform. The panel is being offered for \$250 or \$400 and includes features such as ID capture, selfie capture, login capture, URL capture, 2FA capture, and GAUTH login. The seller claims to have personally used the panel and that many others have as well. Allegedly, the panel's features, such as ID capture and selfie capture, could be used to bypass Coinbase's security measures and gain unauthorized access to user accounts.

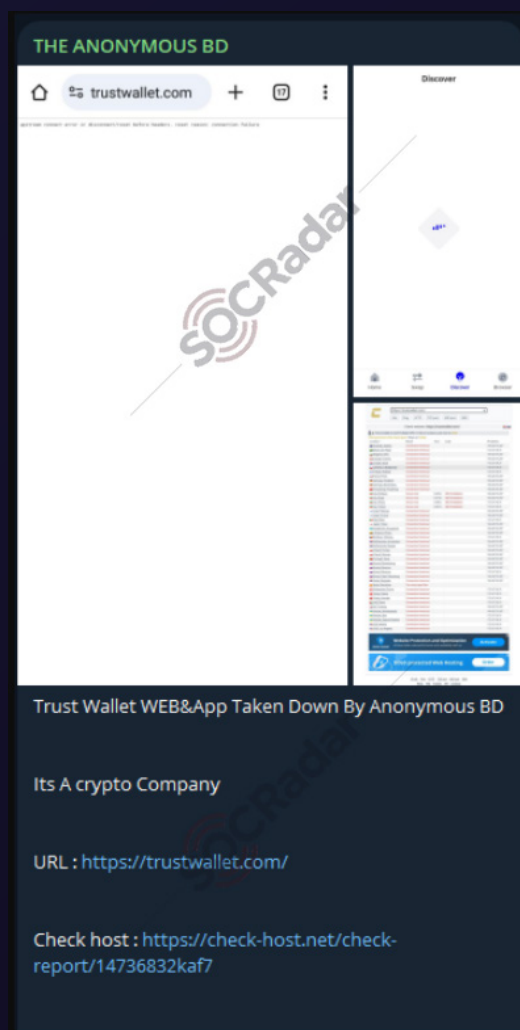


Live Panel of Coinbase being sold on a hacker forum

The Anonymous BD Conducted DDoS Attack on Trust Wallet

7 Jan
2024

The hacking group, Anonymous BD, initiated a DDoS attack against Trust Wallet, a crypto wallet company. The main goal of a Distributed Denial of Service (DDoS) attack is to disrupt the normal functioning of a target system, network, or website by overwhelming it with a flood of traffic from multiple sources, which expectedly resulted in the takedown of the TrustWallet website and mobile app and caused disruptions in accessing the services. The news was detected by SOCRadar's monitoring of The Anonymous BD's Telegram channel.



Anonymous BD hacking group's Telegram message regarding DDoS attack

The Anonymous BD Conducted DDoS Attack on BTC.com

25 Dec
2023

BTC.com, a prominent cryptocurrency website, experienced disruption and unavailability due to a DDoS attack carried out by the Anonymous BD group. The announcement of the DDoS attack was detected on the Anonymous BD's Telegram channel, indicating the use of encrypted messaging platforms by cybercriminal groups to communicate and coordinate their activities.

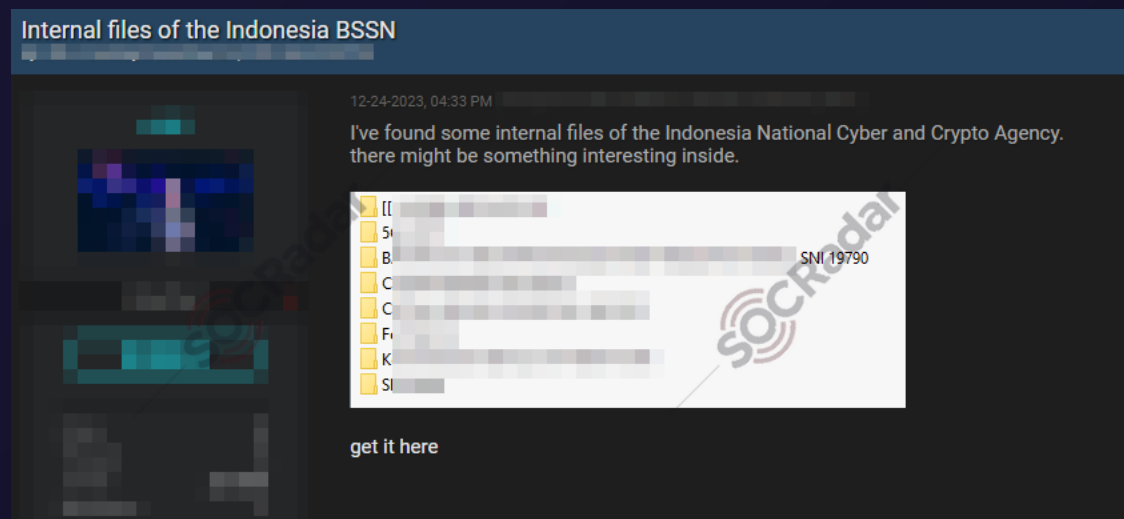


Anonymous BD hacking group's Telegram message regarding DDoS attack

Sensitive Files of Indonesia National Cyber and Crypto Agency are Leaked

24 Dec
2023

The dark web news pertains to a purported leak of sensitive files belonging to the Indonesia National Cyber and Crypto Agency. These files were discovered on a hacker forum monitored by SOCRadar. The leaked files may contain sensitive information that could be exploited by malicious actors for various purposes, such as targeted attacks, fraud, or espionage.



Sensitive Files of Indonesia National Cyber and Crypto Agency being sold on a Dark Web forum

HOW CAN SOCRADAR HELP?

Cyber threat actors frequently gain unauthorized access to systems by acquiring credentials or intelligence through dark and deep web forums and communication channels. **SOCRadar** actively monitors these channels, generating alerts and incidents for any information associated with your company.

Social engineering and phishing serve as initial vectors for numerous cyber attacks. In tandem with your company's training on refraining from clicking on untrusted links and email attachments without proper verification, **SOCRadar** can identify impersonating and typosquatting domains that may be utilized in phishing campaigns targeting your employees and users.

The screenshot displays the SOCRadar Labs website. On the left is a dark blue sidebar with the SOCRadar Labs logo and five navigation items: Dark Web Report, IOC Radar, CVE Radar (marked with a 'beta' badge), and Country Threat Landscape Report (also marked with a 'beta' badge). The main content area has a white background. At the top right, there are links for 'Company', 'Partners', 'Contact', and 'Free Access'. Below these are six service icons: IP Reputation, Phishing Radar, DoS Resilience, VPN Security, Email Analyzer, and Email Grader. A section titled 'Full Featured Tools SOC Tools' features a search bar with the placeholder text 'Search on the Phishing Radar. Enter domain...' and a red 'Search' button. Below the search bar, a paragraph states: 'SOC Tools are the next generation tools to investigate the everyday incidents like phishing, malware, account breach, etc. These tools are built on SOCRadar bigdata platform and includes machine learning and advanced behavioral analytics.' At the bottom, there are three white cards. The first card is titled 'Check For IP Reputation' and describes the service as allowing users to search for their IP or IP block in any blacklist. The second card is titled 'Check For Phishing Radar' and describes it as generating possible words from a domain name to search in all domain name databases to detect domain spoofing and phishing. The third card is titled 'Check For DoS Resilience' and describes it as allowing users to check their domain's or subnet's resilience against DoS attacks such as slowloris attack etc.

The Phishing Radar service detects domain spoofing and phishing.

DEFENSE IN WEALTH

SECURE YOUR DIGITAL ASSETS

Use Two-Factor Authentication

Enable Two-Factor Authentication (2FA) on your cryptocurrency and NFT accounts to add an extra layer of security. This additional step ensures that even if your password is compromised, unauthorized access remains significantly challenging.

Encrypt Your Wallet

Prioritize wallet encryption to safeguard your digital assets. Encryption adds a protective shield, making it arduous for malicious entities to access and misuse your wallet information.

Use Trustworthy Wallets:

Opt for well-established and reputable cryptocurrency wallets. Choosing wallets with a proven track record minimizes the risk of vulnerabilities and enhances the overall security of your holdings.

Maintain Multiple Wallets:

Diversify your cryptocurrency holdings across multiple wallets. In the event of a security breach on one platform, this strategy helps mitigate potential losses by separating your assets.

Store Your Cryptocurrency Safely:

Securely store your cryptocurrency assets offline in hardware wallets or cold storage solutions. This precautionary measure safeguards your holdings from online threats, reducing the likelihood of unauthorized access.

Use Strong Passwords:

Create robust and unique passwords for your cryptocurrency and NFT accounts. Utilize a combination of uppercase and lowercase letters, numbers, and symbols to fortify your password against brute-force attacks.

Avoid Phishing Attacks:

Exercise caution and vigilance against phishing attempts. Be skeptical of unsolicited emails, messages, or links and verify the authenticity of communications to prevent falling victim to phishing attacks targeting your sensitive information.

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.

21.000+
Free Users

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.

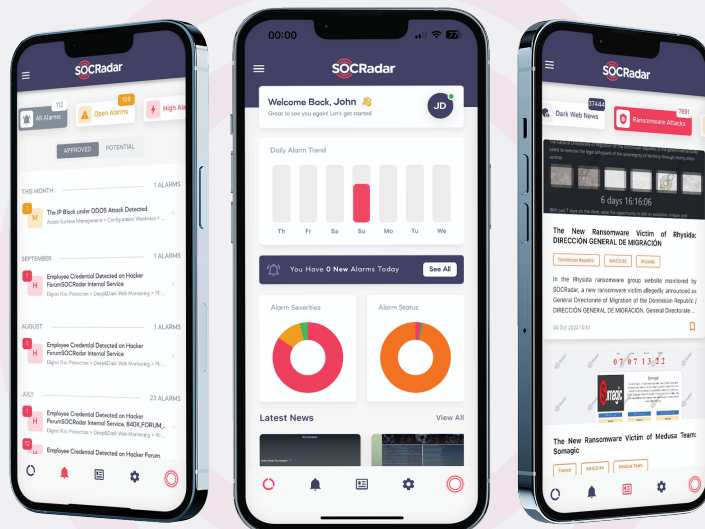
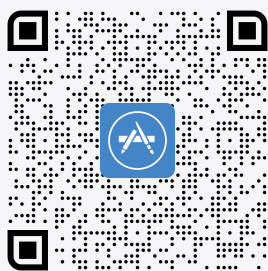
360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS FOR FREE

MEET THE NEW MOBILE APP

Access threat intelligence, act on-the-go, and be instantly notified of new threats. View alerts, breaking Dark Web news, and new ransomware attacks

Download on the
App Store



GET IT ON
Google Play



Gartner
Peer Insights™

4.9/5
★★★★★

**SOCRadar HQ**

HQ Office: 254 Chapman Rd, Ste
208 Newark, Delaware 19702 USA

Call

+1 (571) 249-4598

Email

info@socradar.io

socradar.io

Virtual Addresses**London, UK**

167 City Road Old Street,
London EC1V 1AW

Dubai, UAE

8W building 5th Floor,
DAFZA, Dubai

São Paulo, Brasil

7th & 8th Floors Torre
Joao Salem, Av. Paulista
1079 São Paulo

Bangalore, India

The Estate, 8th Floor
Dickenson Road 560042
Bangalore Karnataka

