SOCRadar®

"17.5 Million Credit Card Information Sold on Black Markets"

FINANCIAL INDUSTRY THREAT LANDSCAPE REPORT

OCTOBER 2022

"17.5 MILLION CREDIT CARD INFORMATION SOLD ON BLACK MARKETS"

Finance is one of the most attractive targets for threat actors because of the high reward possibility after a successful attack. The number of cyber threats against financial institutions that appeared on the dark web constantly increased throughout 2021. The trend is still holding in 2022, even though it has lost momentum. Finance is still the most targeted industry in this report's scope, the first eight months of 2022.

The finance industry in this report consisted of institutions like banks, cyber currency exchange platforms, micro, and macro loan firms, fintech firms, and financial advisory firms.

SOCRadar discovered over 10,000 impersonating domains and analyzed around 11,000 dark web posts, some from ransomware channels. We also investigated banking trojans in the wild, DDoS threats, vulnerabilities, and supply-chain threats for financial institutions.

Regarding the number of posts on dark web forums and hacker channels, finance is the most.

- On average, 16% of the dark web posts will be related to the Finance Industry in 2022.
- 90% of posts related to the finance industry belong to threat actors who want to sell or share sensitive data of financial institutions.
- The SOCRadar CTIA team discovered posts from around 80 ransomware gangs that mentioned financial institutions. The LockBit 3.0 ransomware group is responsible for about a third of attacks.
- 17.4 million credit card information has been sold on the black market over the last eight months.
- 5,520,908 mobile malware, adware, and riskware attacks were blocked only in the second quarter of 2022.
- In the first eight months of 2022, threat actors registered more than 10,000 phishing domains, all impersonating financial institutions. Around 75% of those phishing domains have a valid SSL certificate.

ABOUT SOCRadar®

Who is SOCRadar?

As an Extended Threat Intelligence (XTI) platform and inventor of the concept, SOCRadar's approach effectively integrates Threat Intelligence, Digital Risk Protection, and External Attack Surface Management (EASM). Adapting proactive security with a hacker mindset, our aim is to help security teams to detect blindspots before attackers.

To provide the "right blend" to the security teams, SOCRadar focuses on relative and actionable intelligence with minimized false positives. To generate the contextualized intelligence, SOCRadar's EASM service first maps out an organization's internet-facing digital assets with a hacker mindset and strengthens the organization's visibility on what to defend. The second integral part of the XTI is the DRP services with which SOCRadar provides monitoring capabilities across all environments. Besides monitoring, SOCRadar includes site takedown and automated remediation to its DRP services. The third leg of XTI is threat intelligence. Gathering intelligence from not only open sources and social media but also dark web forums along with other secret communication platforms attackers use, SOCRadar becomes the organization's eye on the dark side of the Internet.

Why Industry Reports?

The shortage of cybersecurity experts is a growing problem worldwide. Financial institutions must use resources efficiently to provide adequate cyber security with their limited resources. Automated security solutions offer precisely the opportunity that corporations are looking for. With its AI-powered automation technology, SOCRadar has become an extension of financial institutions' SOC teams.

This report highlights the threats financial institutions face and how SOCRadar can help companies with financial institutions.

ABOUT SOCRadar®

SOCRadar provides extended cyber threat intelligence (XTI) that combines,

- Cyber Threat Intelligence,
- Digital Risk Protection,
- External Attack Surface Management Services

SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Darknet and Deep Web Monitoring

SOCRadar's fusion of its unique dark web Recon technology with the human analyst eye achieves further provides in-depth insights into financially-targeted APT groups and the threat landscape.

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.

Protecting Customers’ PII

Scan millions of data points on the surface web, deep web, and darknet to accurately identify the leakage of your customers' personally identifiable information (PII) in compliance with regulations.

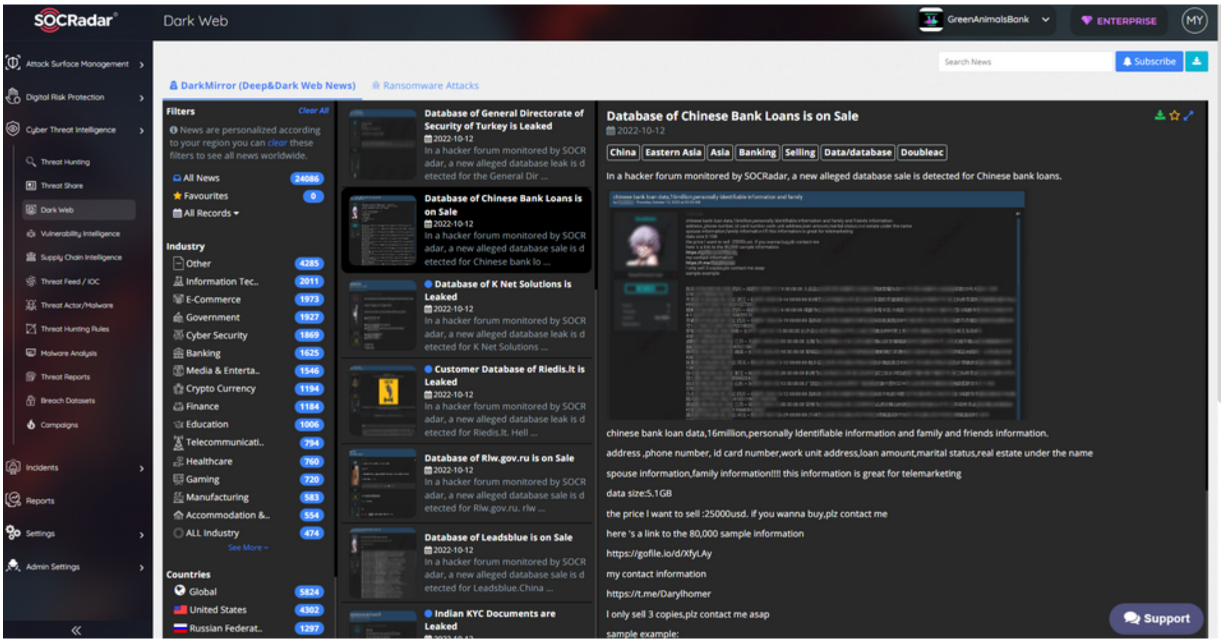
360-Degree Visibility

Achieve digital resiliency by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

Financial Industry Threat Landscape: "Threats to Financial Institutions Are Still High"

SOCRadar Research Team analyzed indicators such as posts in dark web forums and chatter on hacker channels discovered by SOCRadar DarkMirror to explore threats during the first eight months of 2022.

The SOCRadar DarkMirror is a tool where all the activities on the dark web are collected via following the dark market forums, leak sites, and hacker chatters.



Filters — Clear All

News are personalized according to your region you can clear these filters to see all news worldwide.

All News	24086
Favourites	0
All Records	

Industry

Other	4285
Information Tec..	2011
E-Commerce	1973
Government	1927
Cyber Security	1869
Banking	1625
Media & Enterta..	1546
Crypto Currency	1194
Finance	1184
Education	1006
Telecommunicati..	794
Healthcare	760
Gaming	720
Manufacturing	583
Accommodation &..	554
ALL Industry	474

See More

Countries

Global	5824
United States	4302
Russian Federat..	1297

Database of General Directorate of Security of Turkey is Leaked
2022-10-12
In a hacker forum monitored by SOCRadar, a new alleged database leak is detected for the General Dir ...

Database of Chinese Bank Loans is on Sale
2022-10-12
In a hacker forum monitored by SOCRadar, a new alleged database sale is detected for Chinese bank lo ...

Database of K Net Solutions is Leaked
2022-10-12
In a hacker forum monitored by SOCRadar, a new alleged database leak is detected for K Net Solutions ...

Customer Database of Riedis.lt is Leaked
2022-10-12
In a hacker forum monitored by SOCRadar, a new alleged database leak is detected for Riedis.lt. Hell ...

Database of Rlw.gov.ru is on Sale
2022-10-12
In a hacker forum monitored by SOCRadar, a new alleged database sale is detected for Rlw.gov.ru. rlw ...

Database of Leadsblue is on Sale
2022-10-12
In a hacker forum monitored by SOCRadar, a new alleged database sale is detected for Leadsblue.China ...

Indian KYC Documents are Leaked

Database of Chinese Bank Loans is on Sale
2022-10-12

China | Eastern Asia | Asia | Banking | Selling | Data/database | Doubleac

In a hacker forum monitored by SOCRadar, a new alleged database sale is detected for Chinese bank loans.

chinese bank loan data,16million,personally Identifiable information and family and friends information.

address ,phone number, id card number,work unit address,loan amount,marital status,real estate under the name

spouse information,family information!!!! this information is great for telemarketing

data size:5.1GB

the price I want to sell :25000usd. if you wanna buy,plz contact me

here 's a link to the 80,000 sample information

https://gofile.io/d/XfyLAy

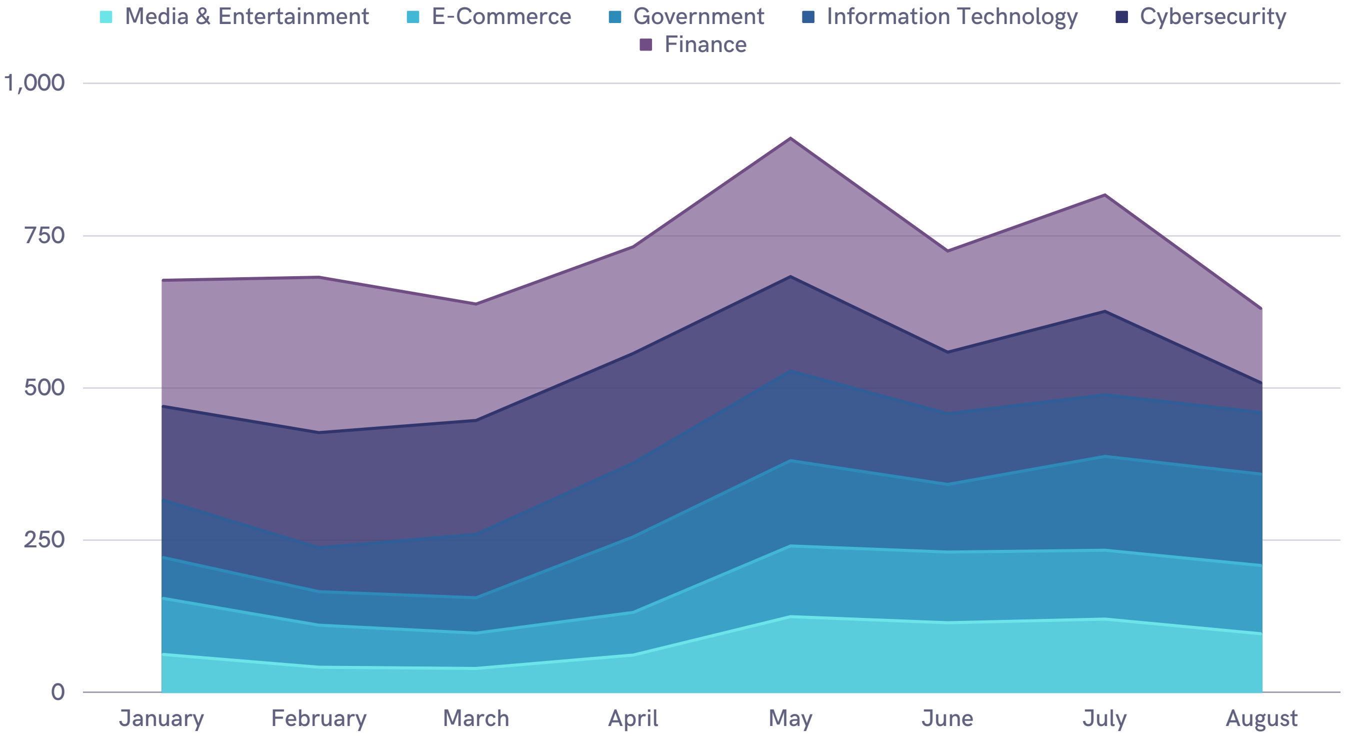
my contact information

https://t.me/Darylhomer

I only sell 3 copies,plz contact me asap

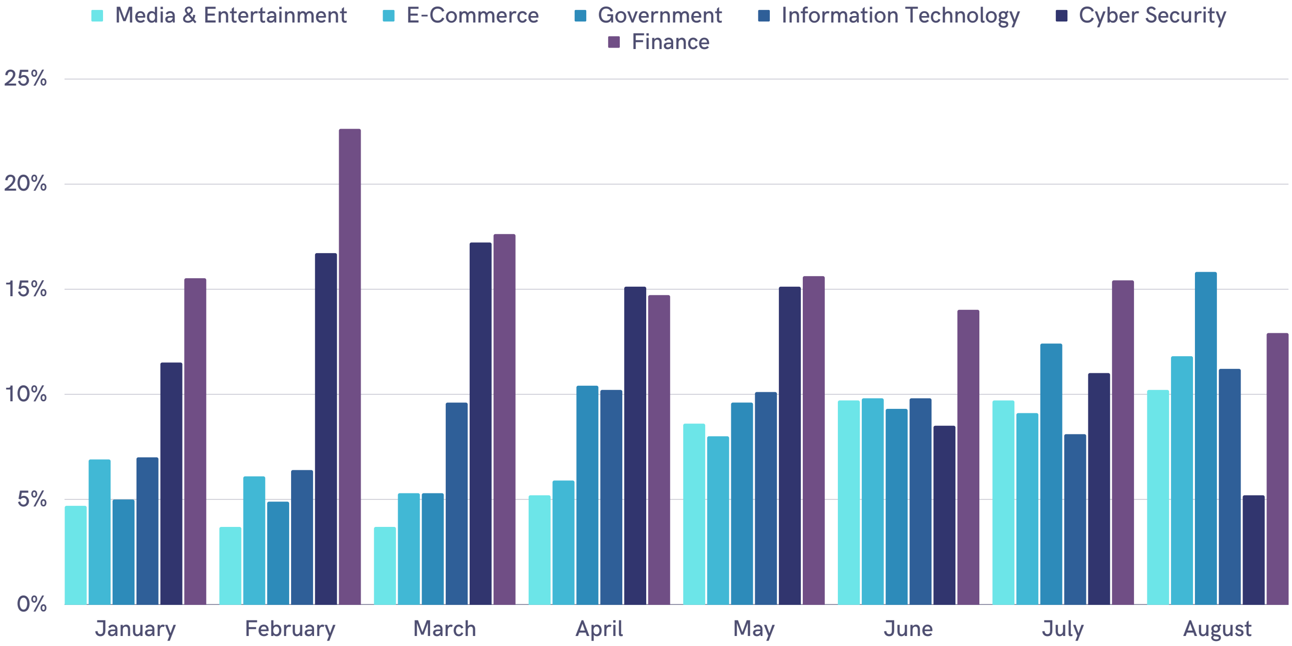
sample example:

SOCRadar CTIA Team utilizes more than 9,500 entries in the DarkMirror to clarify the finance industry's threat landscape.

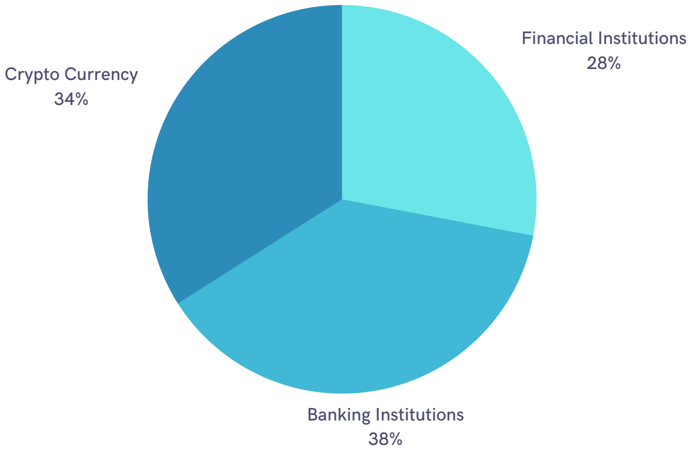


Almost every month, the number of dark web forum posts about finance was more than the other five industries.

SOCRadar analyzed the percentage share of the top six sectors identified in dark web posts by threat actors in 2022 and the percentage change in dark web posts mentioning financial institutions.



You can follow the change in the sub-categories of the posts targeting the Finance Sector from the chart below. (Banks and Cryptocurrency institutions and financial institutions: such as micro and macro loan firms, fintech, and financial investment firms)



Banking had the most posts with 38%, cryptocurrency came next with 34%, and other financial institutions had a 28% share.

The mentions of banking and cryptocurrency institutions were at the highest in February, which coincides with the prewar conflict between Ukraine and Russia.

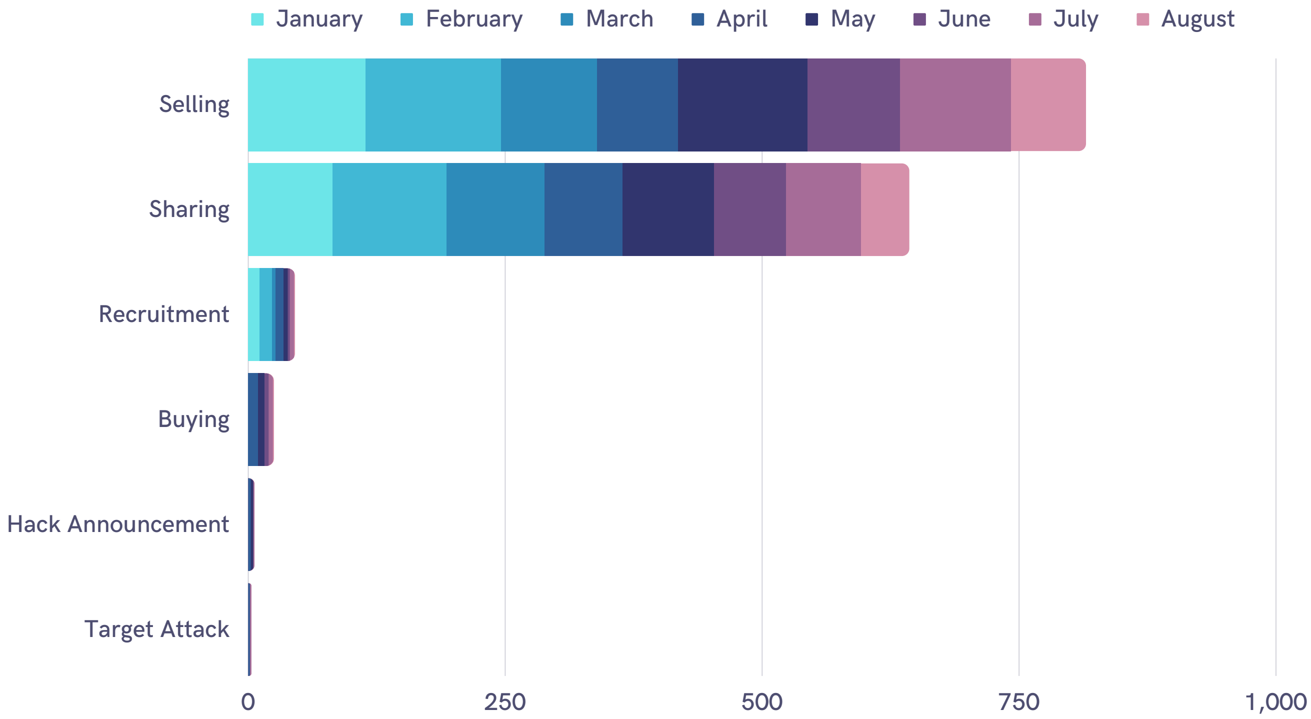
As you might remember, Russia allegedly cyber-attacked Ukraine's government and financial institutions. The peak in February was closely related Russian prewar effort. After Russia's cyber attacks, groups such as Against The West also launched counterattacks.

In addition, 16% of the dark web posts on average in the SOCRadar platform are related to the finance industry in 2022.

Dark Web Radar for Financial Institutions

Most data obtained from dark web posts related to financial institutions are sensitive data sold or shared by threat actors. When threat actors curate a collection of sensitive data, there are a couple of ways they spread the data at a predetermined price or an auction. The other way is to share data for free.

However, when the data is accessible, the threat actor might have a hidden agenda, such as hiding their tracks after they have already used data to attack. **The exposed data on sale generally includes credit card information, employee PII data, and customer databases.**

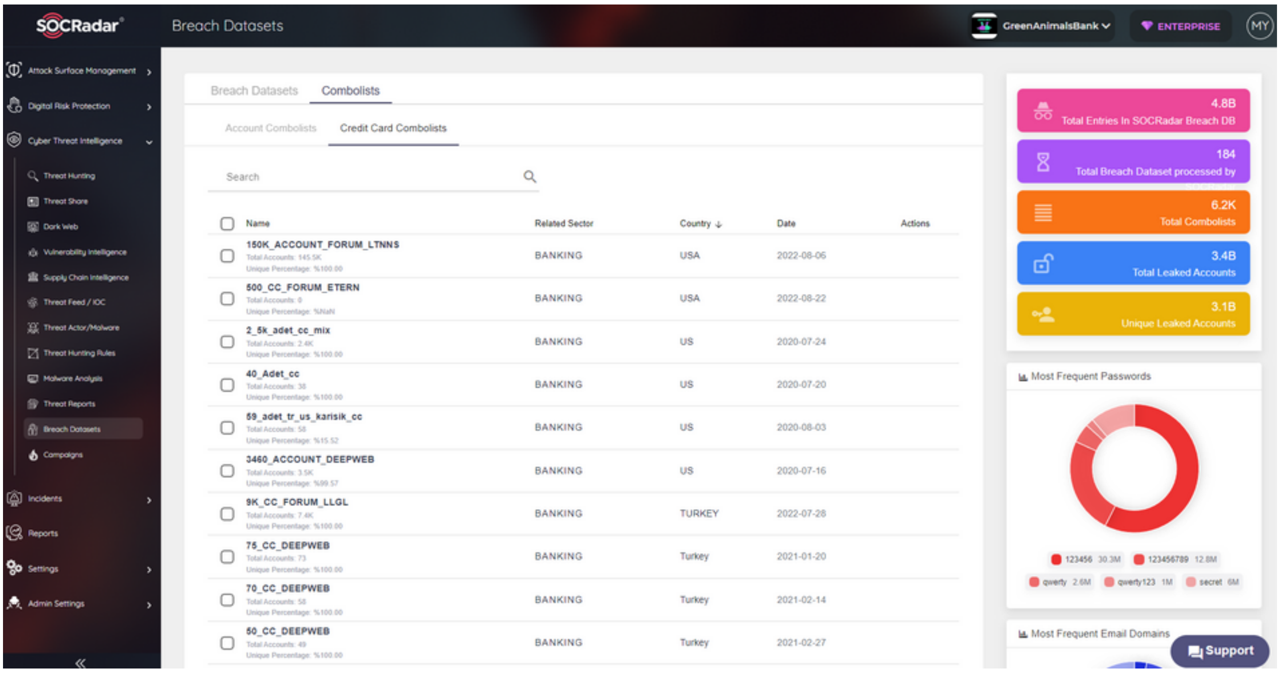


In 2022, data selling (49.9%) and sharing (39.4%) are almost 90% of all dark web posts targeting financial institutions on average. The posts that aim to sell sensitive data about financial institutions reached almost 60% of all dark web posts, according to SOCRadar DarkMirror at the end of August 2022. Concerning the dark web post and hacker channel shares targeting financial institutions, the most targeted countries in 2022 are China, Brazil, Estonia, Egypt, Germany, U.A.E., and Malaysia.

"17.5 million Credit Card Information Sold on Black Markets"

The total number of credit card information sold on Black Markets and dark web hacker forums during the first eight months of 2022. Even though the validity ratio for these shares is relatively low (at most 10%), 17.5 million is still a significant number affecting the finance industry and its customers.

SOCRadar XTI Platform monitors the black market, where bulk credit card information is sold. When shared, SOCRadar classifies the CCI to identify the country and the bank and send alarms accordingly.



□	Name	Related Sector	Country ↓	Date	Actions
□	150K_ACCOUNT_FORUM_LTNNS Total Accounts: 145.5K Unique Percentage: %100.00	BANKING	USA	2022-08-06	
□	500_CC_FORUM_ETERN Total Accounts: 0 Unique Percentage: %NaN	BANKING	USA	2022-08-22	
□	2_5k_adet_cc_mix Total Accounts: 2.4K Unique Percentage: %100.00	BANKING	US	2020-07-24	
□	40_Adet_cc Total Accounts: 38 Unique Percentage: %100.00	BANKING	US	2020-07-20	
□	59_adet_tr_us_karisik_cc Total Accounts: 58 Unique Percentage: %15.52	BANKING	US	2020-08-03	
□	3460_ACCOUNT_DEEPWEB Total Accounts: 3.5K Unique Percentage: %99.57	BANKING	US	2020-07-16	
□	9K_CC_FORUM_LLGL Total Accounts: 7.4K Unique Percentage: %100.00	BANKING	TURKEY	2022-07-28	
□	75_CC_DEEPWEB Total Accounts: 73 Unique Percentage: %100.00	BANKING	Turkey	2021-01-20	
□	70_CC_DEEPWEB Total Accounts: 58 Unique Percentage: %100.00	BANKING	Turkey	2021-02-14	
□	50_CC_DEEPWEB Total Accounts: 49 Unique Percentage: %100.00	BANKING	Turkey	2021-02-27	

4.8B Total Entries In SOCRadar Breach DB

184 Total Breach Dataset processed by

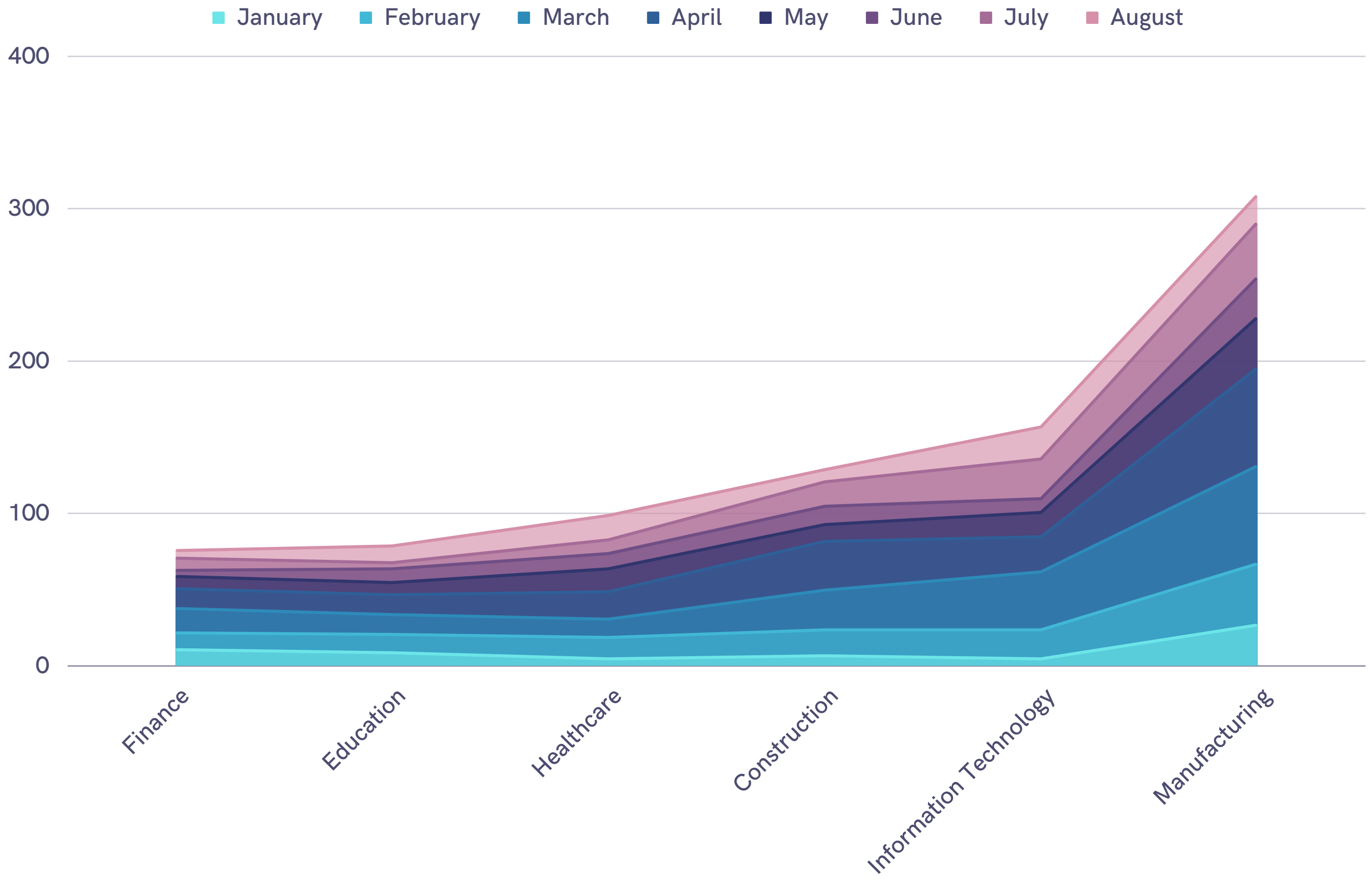
6.2K Total Combolists

3.4B Total Leaked Accounts

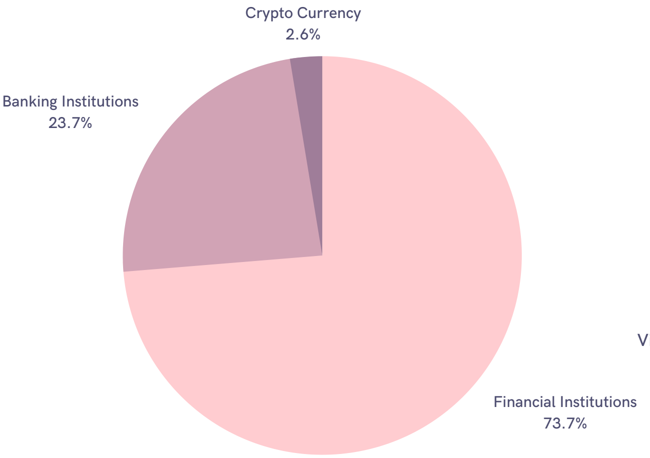
3.1B Unique Leaked Accounts

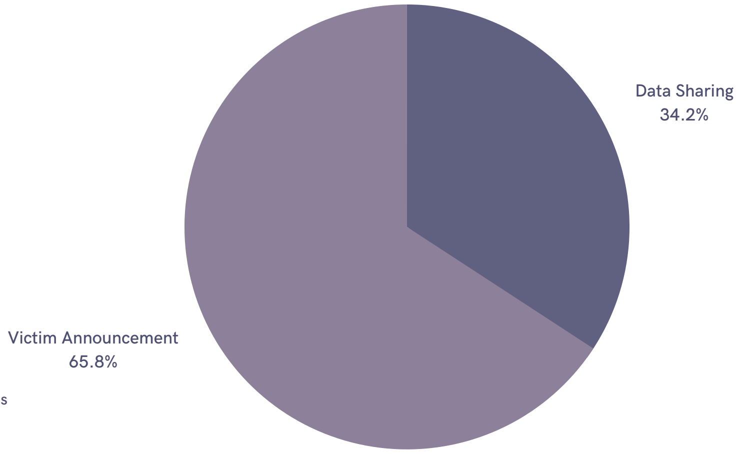
Ransomware Threats

SOCRadar CTIA Team analyzed 1,700 ransomware threats shared on dark web forums and hacker channels published during the first eight months of 2022.

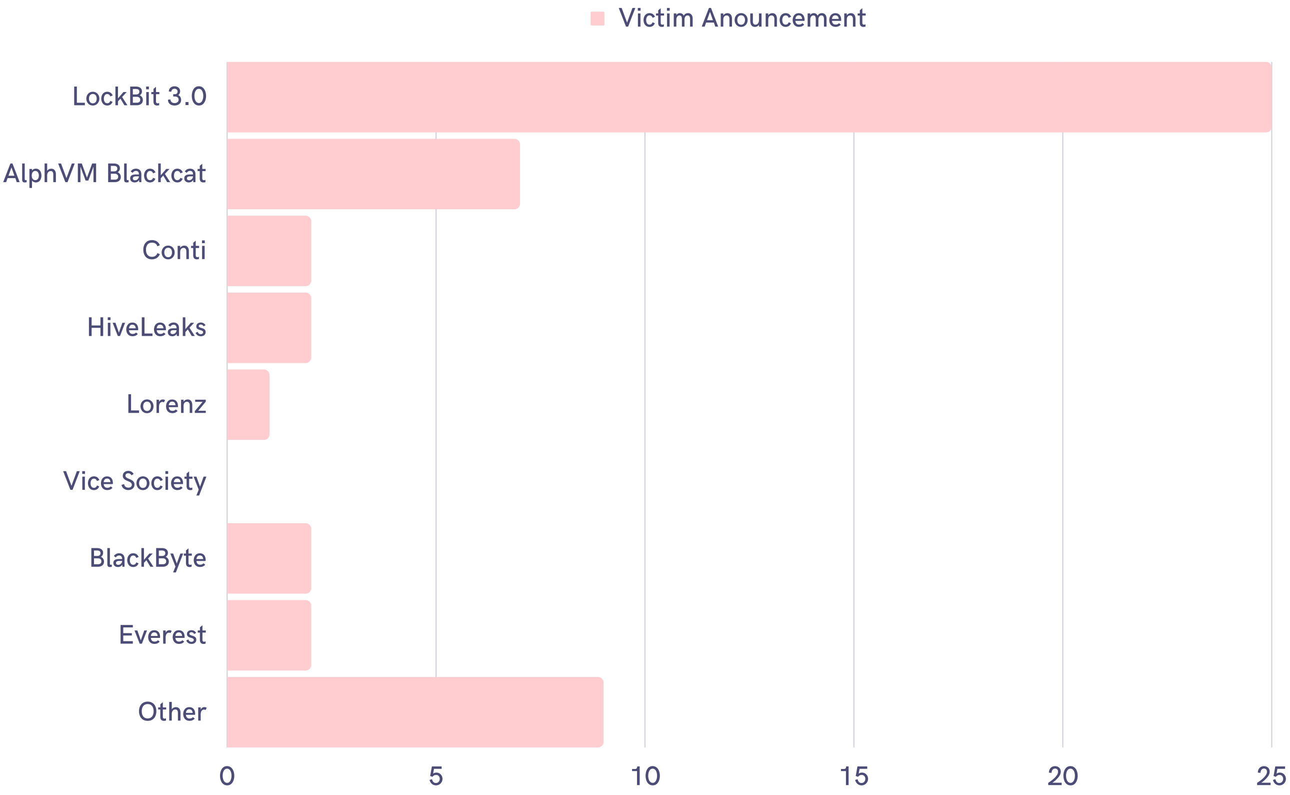


4.5 % of the ransomware posts that SOCRadar tracks are about the Finance Industry so far in 2022 on average. Subcategories of the ransomware posts targeting Finance: Three-quarters of the posts were aimed directly at financial institutions, One quarter were aimed at Banks, and only 2% were related cryptocurrency industry. Two-thirds were data-sharing posts. Probably, the sensitive data was shared after the ransom payment was rejected.





Various ransomware groups targeted financial institutions in the last eight months LockBit 3.0, Conti, HiveLeaks, AlphVM Blackcat, AvosLocker, and Lorenz are some of them. SOCRadar analysts discovered 76 attacks on the dark web in the first months of 2022, and twenty-five of these attacks belonged to LockBit 3.0.



Malware Targeting Banks and Their Customers

With the pandemic, contactless digital payments and the use of mobile banking reached new heights. This increased digitalization also created an opportunity for threat actors and cybercriminals. Banking trojans in smartphones could secretly take actions that affect personal or confidential information stored on the device and take control of the device.

Around 100 thousand new mobile banking Trojans were discovered in 2021. More than 17,000 new mobile ransomware Trojans and approximately 3.5 million malicious installation packages were specified. The most targeted by mobile banking Trojans countries were Japan, Spain, Turkey, France, Australia, Germany, Norway, Italy, Croatia, and Austria. More than 5,5 million mobile malware, adware, and riskware attacks were blocked in the second quarter of 2022. More than 400,000 installation packages were detected. More than 55,000 packages were related to mobile banking Trojans, and about 4,000 were mobile ransomware Trojans.

TOP 5 BANKING TROJANS AND THEIR FUNCTIONS

Banker.AndroidOS.Agent.eq	Steals usernames and passwords for banking apps
Banker.AndroidOS.Anubis.t	Steals banking information
Banker.AndroidOS.Svpeng.t	Gets administrator rights on the phone
Banker.AndroidOS.Svpeng.q	Steals banking information
Banker.AndroidOS.Asacub.ce	Steals payment information

A Returning Threat: Trickbot

Trickbot malware targeted the customers of 60 significant institutions,including major financial institutions, primarily located in the U.S., using phishing attacks through web injections. Those 60 firms include big technology corporations such as Amazon, Microsoft, and Google, financial institutions like Paypal, American Express, such as like Bank of America and Wells Fargo & Co., and cryptocurrency exchange markets such as blockchain.com and robinhood.com. Check Point Research (CPR) estimates more than 140,000 have been infected since November 2020.

Trickbot started as a regular Banking Trojan alongside Zeus, Agent Tesla, Dridex, and DanaBot. However, it has been continuously evolving since 2016. Since the malware is now modular, the Trickbot gang may modify and customize the program to carry out a variety of attacks. TrickBot uses phishing e-mails for the initial payload delivery. Therefore, phishing awareness and training is a defense mechanism against Trickbot.

Phishing Domains Impersonating Financial Institutions

SOCRadar detected over 10,000 phishing domains impersonating financial institutions registered in the first eight months of 2022. Threat actors use phishing domains to lure customers and employees into stealing their credentials and accessing the company systems.

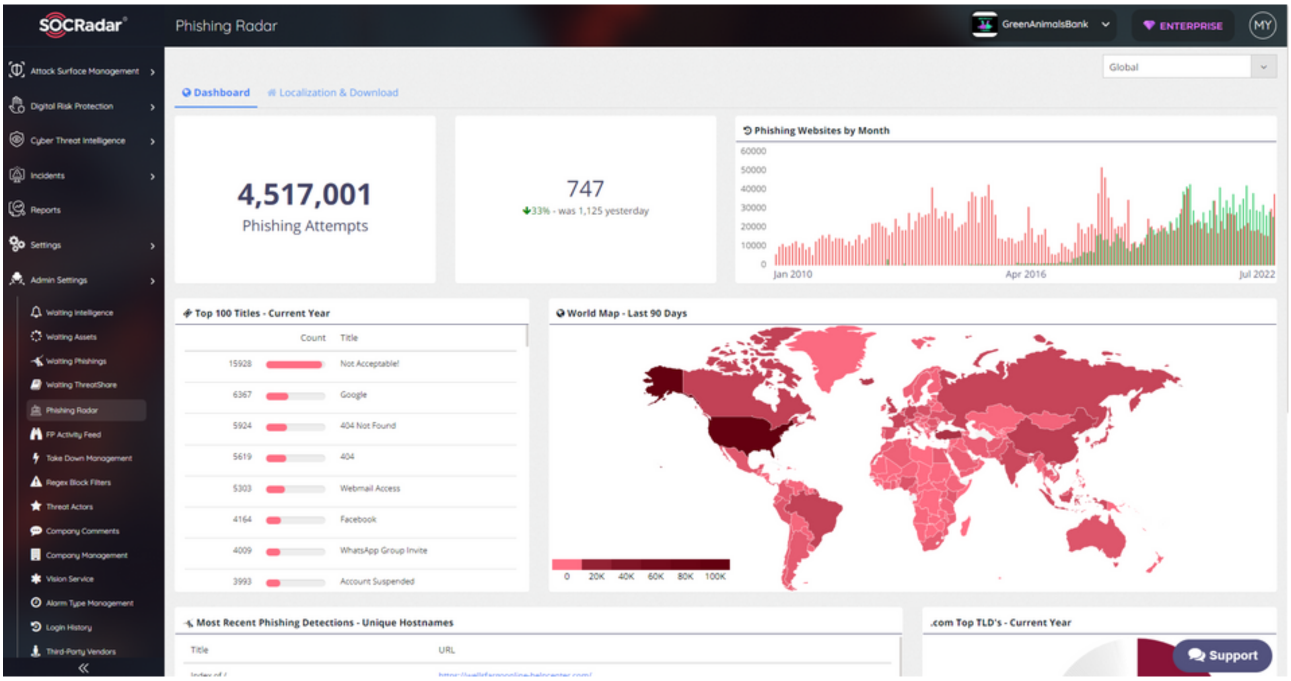
While threat actors prefer free registrars to register these phishing domains, they also might get an SSL/TLS certificate to convince the victims about the website's legitimacy. Seeing the HTTPS at the beginning of the URL with a padlock sign beside it gives the users a false sense of security.

SOCRadar discovered that almost three-quarters of the phishing domains impersonating financial institutions have valid SSL certificates. A high ratio is not observed in phishing domains impersonating companies in other industries.

Most often, threat actors design impersonating websites and keep them vulnerable to exploits with SSH. OpenSSH vulnerabilities CVE-2017-15906 and CVE-2018-15919 were detected in almost 3.5 % of the impersonating phishing domains by SOCRadar scanners.

The phishing domain takedown is as important as the detection of them. Unified extended threat intelligence solutions, such as SOCRadar, should offer takedown services on behalf of the customers as a part of risk protection services.

The countries most targeted by phishing sites were the United States, Russia, the United Kingdom, China, and Brazil, respectively.



4,517,001
Phishing Attempts

747
33% - was 1,125 yesterday

Top 100 Titles - Current Year

Count	Title
15928	Not Acceptable!
6367	Google
5924	404 Not Found
5619	404
5303	Webmail Access
4164	Facebook
4009	WhatsApp Group Invite
3993	Account Suspended

Most Recent Phishing Detections - Unique Hostnames

Title	URL
Index of /	https://wellsfargoonline-helpcenter.com/

Impact of the Russia-Ukraine War on the Finance Industry

Before the globe recovered from the financial repercussions of the COVID-19 epidemic, the war influenced the whole financial sector and the global economy. In an unprecedented development, financial institutions and fintech firms responded by imposing sanctions and boycotts against Russia. Some international companies supported the sanctions to remove the Russian government and businesses from their client list or stopped or limited their trade with them.

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) initially suspended seven Russian central banks from performing transactions permanently. The Russian government created SPFS (System for Transfer of Financial Messages), a SWIFT substitute that only functions in Russia and a few banks in Switzerland, Kazakhstan, Azerbaijan, Cuba, and Belarus. Russia also uses China's Cross-border Interbank Payment System (CIPS) for international transactions.

Many businesses decided to exit the Russian market of their own volition without being forced to do so by legislation or penalties. Money transfer firms like Western Union and Wise, as well as financial institutions including VISA, Mastercard, Amex, Paypal, Payoneer, and Revolut, either discontinued operating in Russia or imposed restrictions on their activities there. The crypto community upholds partial neutrality despite the big financial companies' ambivalence in their denunciation and boycott (full or partial) of Russia.

Even though the Russian physical invasion of Ukraine started in February 2022, the attacks in cyberspace can be traced back as early as 2014. On many occasions, Ukraine was exposed to destructive cyberattacks, including NotPetya, to its public and communication institutions, banks, and infrastructure, such as power plants.

Most of the time, the Ukrainian officials held either Russia or pro-Russian hacktivists responsible. We could say that the recent cyberattacks on Ukraine are limited compared to the past. Some researchers attribute this to the increased cyber resilience of Ukraine. In contrast, others think Russia is more hesitant because a full-capacity cyberattack would most probably spill over the US and Europe Union, taking more offensive and defensive precautions in cyberspace.

The cyberattacks on Ukraine around this conflict included but were not limited to attacks on the KA-SAT satellite network, DDoS attacks on state-owned banks and government institutions, and data-wiper attacks on government and finance, making the data unusable.

Also, a fake surrender message from Ukrainian President Volodymyr Zelenskyy created using deep-fake technology was spread in social media and placed on a Ukrainian news website by pro-Russian hackers. There were phishing and spear-phishing campaigns, trojans and malware to steal sensitive information, credentials for government and military officials, and banking and payment data of citizens.

DDoS Attacks

Threat actors execute DDoS attacks against financial institutions, especially banks, with various objectives. DDoS attacks could interrupt business operations and cost millions of dollars to the financial institution. Or they can be used sometimes to increase pressure on Ransomware victims.

Another reason for DDoS attacks is to create a distraction. While executing a DDoS attack using a botnet and keeping the security team busy, threat actors can infiltrate the company's systems by other means.

Recent DDoS Attacks on Financial Institutions

Recent DDoS attacks were observed in the Russia- Ukraine Conflict in mid-February 2021. Several websites of government organizations and state-owned banks, including The Ministry of Defence of Ukraine, The Armed Forces of Ukraine, The Ukrainian Public Radio, Privatbank, and Oschadbank, experienced a massive disruptive distributed denial-of-service (DDoS) attack. In September, a substantial DDoS campaign against New Zealand companies resulted in service outages for businesses, including ANZ New Zealand and Kiwibank. The internet banking app and website were offline for several hours.

Third-Party/Supplier Risks

Most enterprises could have resilient security systems against cyber risks, but these defense systems will not protect the enterprise from third-party service risks. The risks faced by financial institutions involving third parties are significant since financial institutions' digital ecosystem includes far more many vendors in different industries, such as SWIFT Companies, First-party Collection Vendors, Credit Reporting & Specialty Agencies, Financial Software Vendors, Identity & Technology Firms, Interbank Network Providers, Know Your Customer/Anti-Money Laundry (KYC/AML) Vendors, and Payment Providers.

Threat actors usually aim for the weakest link in the vendor ecosystem to gain access to or obtain sensitive data of multiple financial institutions with one hack. The notorious SolarWinds breach was a supply chain attack. That is a reminder that relying on third-party suppliers and service providers in the finance industry poses a risk that financial institutions cannot fully control.

Recent Major Cyber Attacks Targeting Financial Institutions

The data leak at the POS server provider in Malaysia: In June 2022, a research team at Safety Detectives revealed a significant data leak on an unsecured database belonging to the point of sale (POS) and management software provider StoreHub. The data was stored on an Elasticsearch server in Singapore without encryption or password protection. So far, there is no sign that malicious actors exfiltrated data. However, the server had 1.7 billion records and over one terabyte of data, including the personal information of approximately 1 million customers.

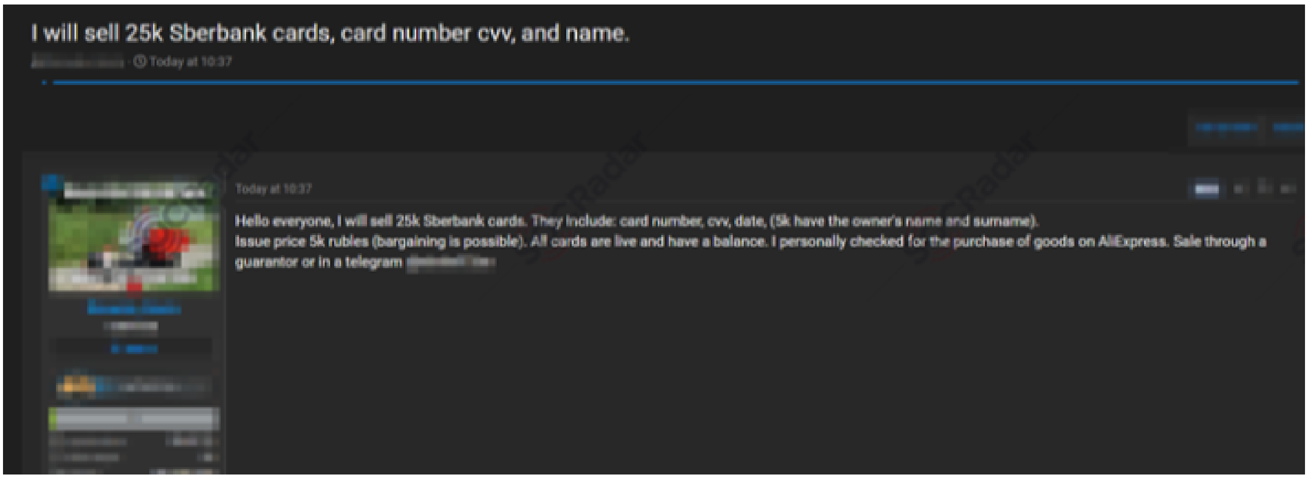
The central bank of Zambia was Attacked by the Hive ransomware gang: The Bank of Zambia informed the public that it experienced a partial disruption to some of its Information Technology (I.T.) applications on Monday, May 9th, 2022, in a press release. The extortionate hack group Hive claimed responsibility for the attack. The Bank of Zambia stated that it rejected to pay the ransom and was fully operational as of May 13th.

Beanstalk Farms cryptocurrency theft: On April 17th, 2022, $182 million was stolen from stablecoin provider and decentralized finance platform Beanstalk Farms in a 'flash loan' hacking attack. The attackers borrowed enough coins to obtain enough voting rights to modify the organization's governance and relocate all of Beanstalk's reserves.

$625M Theft from blockchain gaming platform Ronin: Ronin's Axie Infinity game enables players to earn digital currency and NFTs. After the firm pushed back security standards and protocols to handle the growing audience, the hack was made using an exploit in the bridge, which let funds transfer between the Ethereum and Ronin blockchains in late March 2022. The attackers stole around $625 million in cryptocurrencies.

TransUnion South Africa data breach: A cyber-attack on the credit bureau TransUnion S.A. resulted in the theft of the personal information of about three million customers.

Anonymous Hacks Russia's Largest Bank, Sberbank: The Moscow Stock Exchange and Sberbank were both subject to DDoS attacks on February 28th, 2022, which rendered both websites inaccessible. On May 17th, Anonymous claimed to hack Sberbank and leaked e-mails, phone numbers, and addresses in Excel files. In a hacker forum monitored by SOCRadar, a new credit card sale is detected allegedly belonging to Sberbank.



I will sell 25k Sberbank cards, card number cvv, and name.

[redacted] · Today at 10:37

Today at 10:37

Hello everyone, I will sell 25k Sberbank cards. They include: card number, cvv, date, (5k have the owner's name and surname).
Issue price 5k rubles (bargaining is possible). All cards are live and have a balance. I personally checked for the purchase of goods on AliExpress. Sale through a guarantor or in a telegram [redacted]

Ukrainian government and banking sector under DDoS attack: One of the worst DDoS attacks ever unleashed on a nation occurred on February 15th, 2022, and they brought down the webpage of the Ukrainian Defence Ministry as well as the banking and terminal services of many state and private organizations.

How Can SOCRadar Help? Recommendations

Cyber attacks are not a matter of "if "but "when" for financial firms.

1. Keeping Track of the Vulnerabilities of Digital Assets

There are specific vulnerabilities and zero days that threat actors love to exploit. SOCRadar discovers almost all your digital assets and their vulnerabilities. SOCRadar's External Attack Surface Mapper tracks and updates your assets and vulnerabilities.

2. Identifying and Monitoring Threat Actors

Many organized threat actors like APTs have signature Tactics, Techniques, and Procedures (TTPs). Some of them are only actives and specific regions and sectors. Monitoring the threat landscape and threat actors will make your defenses stronger. SOCRadar's threat intelligence threat feeds, IOCs and IOAs will give you the proactive readiness you need.

3. Phishing Control

Social engineering and phishing are the starting vectors for many cyber attacks. In addition to your company's training for not untrusted links and e-mail attachments without verifying their authenticity, SOCRadar can discover impersonating and typo-squatting domains that could be used for phishing campaigns against your customers and employees.

4. Dark Web Awareness

Threat actors often find their way into systems by purchasing credentials or intelligence from dark web forums and chatter channels. SOCRadar monitors these channels and creates alarms and incidents for anything related to your company.

In addition to these steps, there are more things to protect yourself, such as:

- Using multiple-factor authentication (MFA) and one-time-password (OTP) technologies, you could create strict identity and access management policies.
- You could protect your endpoints using trusted security software as much as possible.
- You must have backup policies and practices. In addition, you should have multiple recent copies (preferably at least one offline) of your critical data and settings and configurations of your security devices.