SOCRadar®
Your Eyes Beyond

END OF YEAR REPORT 2022

www.socradar.io

SOCRadar®
Your Eyes Beyond

Table of Contents

Executive Summary 2

2023 Cybersecurity Predictions 4

SOCRadar with Numbers 5

Phishing Statistics in 2022 6

Top 10 Targeted Industries and Countries in 2022 10

Top 10 Countries Targeted by Threat Actors 12

Most Active Ransomware Groups 14

Top 10 Cyber Incidents in 2022 16

Top 10 Data Leaks/Breaches in 2022 19

Top 5 Vulnerabilities Routinely Exploited by Threat Actors in 2022 24

Executive Summary

2022 has been a challenging year for cybersecurity worldwide. Russian invasion of Ukraine accompanied by waves of cyberattacks marked the start of the year. Perhaps too often, the CISOs of large corporations did not sleep well due to the constant new cyberattacks and significant data breaches that emerged throughout the year. In those same sleepless nights, we at SOCRadar were called to new challenges, fighting deep inside the trenches to prevent the following significant cyber incident proactively.

Throughout the year, we have seen simple endpoint attacks become complex, multi-stage operations, and ransomware attacks hit small businesses and large corporations. That's why the need for integrated cyber threat intelligence platforms like SOCRadar, which appeals to companies of all sizes from all sectors throughout the year, has often found its place in Gartner reports.

Crypto mining attacks gave cybercriminals easy access to company networks. For this reason, the importance of dark web monitoring has increased this year.

And it was a year when cybercriminals significantly improved their threat game. While fighting against cyber attacks, the need for products such as SOCRadar to reach more segments in the sector has also increased. Therefore, contextualized threat intelligence looks set to change the game's rules in 2023. With contextualized threat intelligence, SOC analysts ensure that they have clear guidelines for effective threat hunting.

From the detection of cyber security breaches to the use of artificial intelligence and MDR-supported XDR that allows timely intervention, to the detection of day 0 vulnerabilities that can be exploited with attack surface management, and the detection of threat actors trying to infiltrate your institution with a stolen VPN account that has been sold on the Darkweb. The need and investments for "actionable threat intelligence" solutions will continue to increase in 2023.

Here are the largest cyber attacks, threats, and data breaches that will shake the world in 2022:

•.com is the leading choice of **threat actors by 33%**.

•Scammers were targeting Government and IT industries the most.*

•**55% of the Impersonating domains** use an SSL certificate to give users a false sense of security.

•The threat actors were targeting the US by far.

•Government and finance were at the forefront industries that threat actors discussed the most over dark web channels.

•Manufacturing and Information Technologies were the top two sectors most targeted by ransomware groups.

•According to the data taken from SOCRadar platform, **163 ransomware attacks** against the healthcare industry were reported in 2022, with LockBit ransomware being the most active ransomware group.

•Besides China and Brazil, 8 of the top 10 countries affected by cyber-attacks were from North America, Europe, and the Commonwealth of Nations.

LockBit was the most active ransomware group in 2022 followed by BlackCat and Conti.

Diplomatic conflicts as well as armed aggression created manoeuvre zones for cyber threat actors.

•On September 24, 2022, SOCRadar's integrated Cloud Security Module discovered that **65.000 entities'** sensitive data became public due to a server configuration error at Microsoft's Azure Blob Storage. Six significant public buckets of the many found contained data on more than **150.000 companies** across **123 nations**. With sensitive data contained in a single bucket and affecting more than **65.000 entities across 111 countries,** it can be considered one of the biggest B2B leaks.

•The top 5 vulnerabilities in 2022 curated from the SOCRadar Vulnerability Intelligence module were: "CVE-2021-26084(Atlassian Confluence Server and Data Center RCE), CVE-2020-1472(Zerologon), CVE-2021-22205(Gitlab), CVE-2022-40684 (Fortinet FortiProxy), CVE-2021-44228 (Log4Shell)"

2023 Cybersecurity Predictions

Cloud Security Vulnerabilities

The importance of timely detection and removal of public buckets and files will increase this year. As seen in the BlueBleed data leak case revealed by SOCRadar, the work and concerns of CISOs on cloud security will likely increase this year.

Ransomware-as-a-Service (RaaS) and Containers-as-a-Service (CaaS)

The increase in RaaS and CaaS services are likely to facilitate the process of conducting the attacks which will cause more number of related cyber cases.

DDoS, yes, again

Looking at the past year's examples, there will be another break of new records in DDoS attacks.

Rise of Supply Chain Attacks

Organizations that are difficult to hack and infiltrate will continue to be infiltrated through Supply Chain-3rd party vendors.

Talent Shortage

Extended threat intelligence solutions integrated with AI systems that solve the cybersecurity industry's talent shortage will be discussed more frequently.

Ransomware, again

2023 will be a year in which attention should be paid to ransomware (again) by looking at the financial losses caused by the cases in the last five years based on countries or continents and the increases every year. With the increase in ransomware attacks, companies can do more projects to implement Zero Trust Architecture.

DRPS

The value of information in underground forums is getting more and more critical every day. Considering this year's Medibank case, the information sold on Telegram for the first entry is precious. Dark web monitoring is mentioned frequently in 2023.

MFA Bypass

MFA Bypass methods will be used more as the use of MFA increases. The importance and usefulness of Yubikey-style FIDO2 passwordless authentication will increase.

Business E-mail Compromise (BEC) Attacks

It can be stated that BEC attacks, which are the second after phishing attacks in causing the most financial damage to institutions, will again come to the fore in 2023; perhaps they can surpass phishing attacks and pose a severe threat to organizations.

SOCRadar With Numbers*

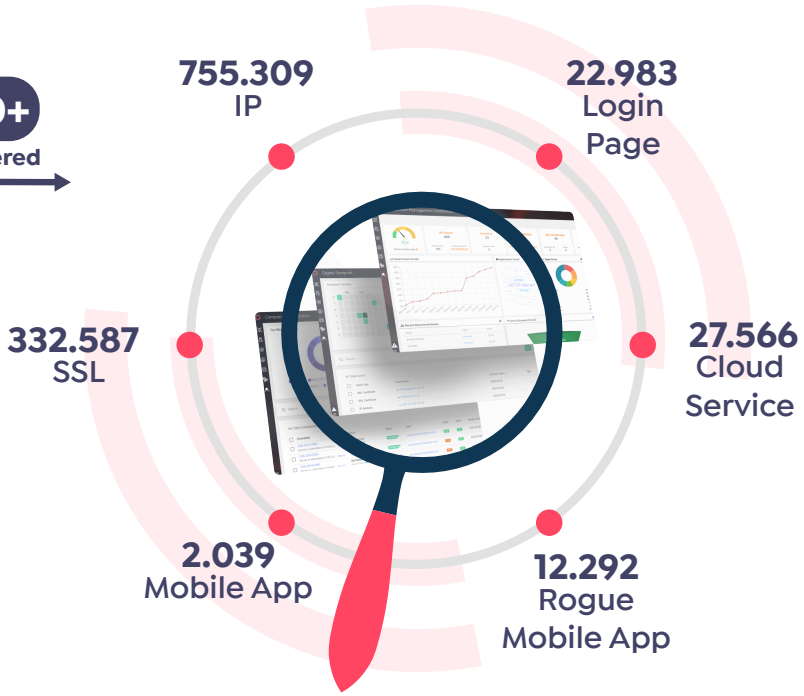
*Scope: January 1- December 31 2022,

6.500+ Users

100+ Million IP Search

27.5+ Billion PORT Search

1.580.000+ Domain Discovered



We Shared

15.126
Dark Web News

2.549
Ransomware News

1.012
Regional News

Notifications to Our Users

1M+ Contextualized Phishing Alarms

+200k Dark Web News Notification*

4.488.326
Generated Alarms

78.437
Detected Impersonating Accounts

75.828
Detected Credit Card Information of Our Users on the Dark Web

7+ Million
Discovered PII Exposures

1.011 Malware Analyzed

10M Unique IOC

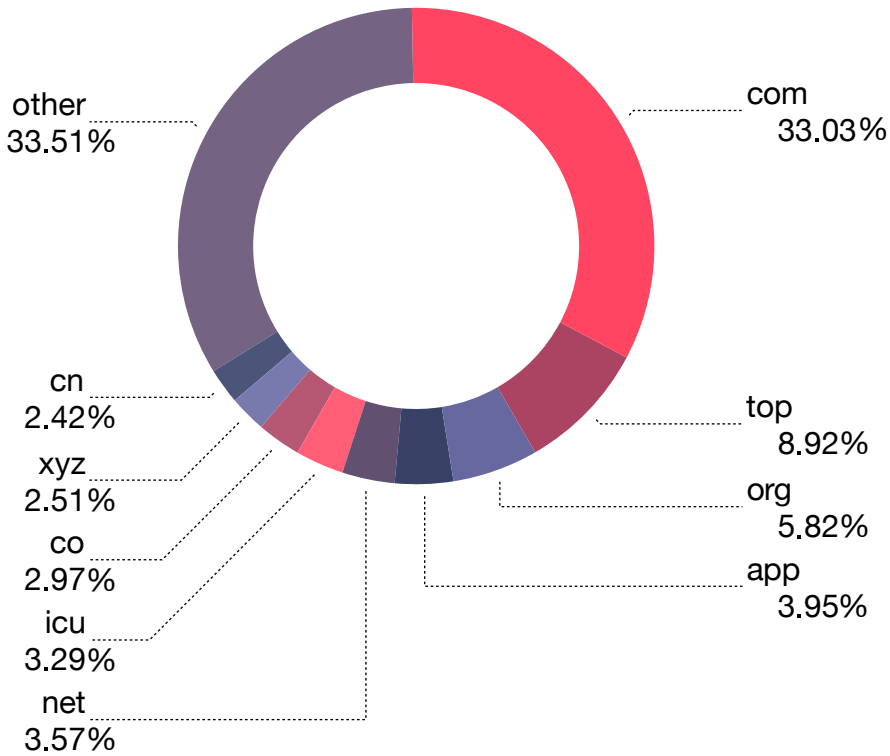
14k Yara and Sigma Rules

(*62538 Threatshare, 9013 Vulnerability Subscription, 4552 Report Subscription e-mails)

Phishing in 2022

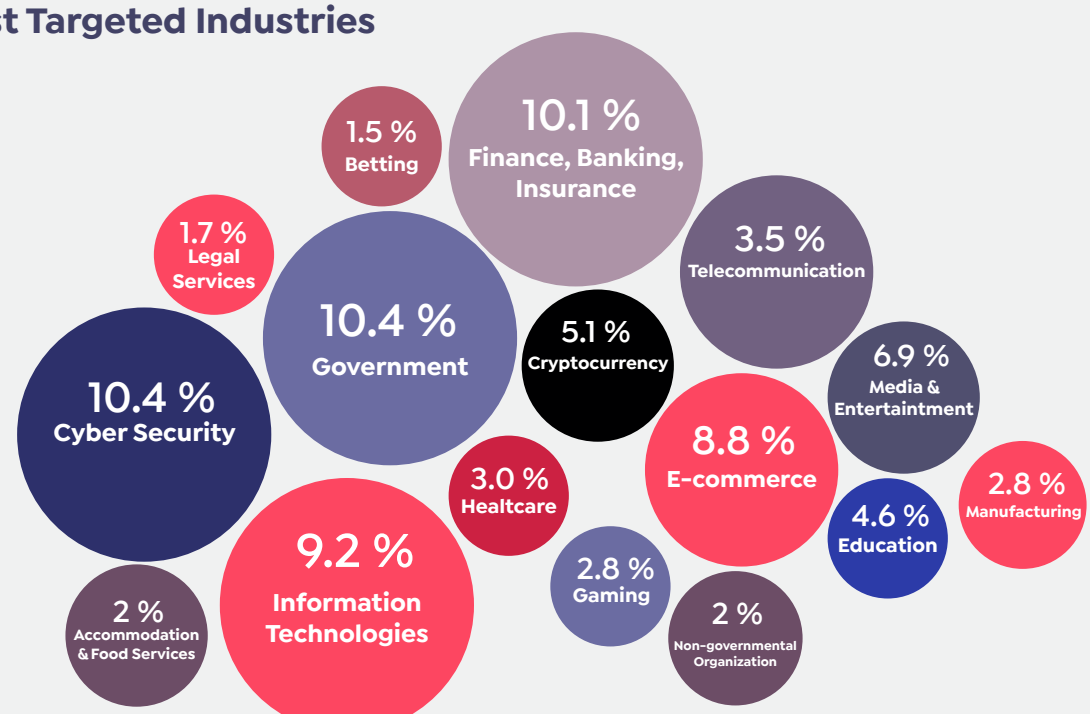
One of the services SOCRadar provides is discovering and taking action against impersonating domains trying to harvest credentials and personally identifiable information from your employees and customers. Remember that phishing and social engineering are still the starting points of many cyber attacks.

A. Most used Top Level Domains



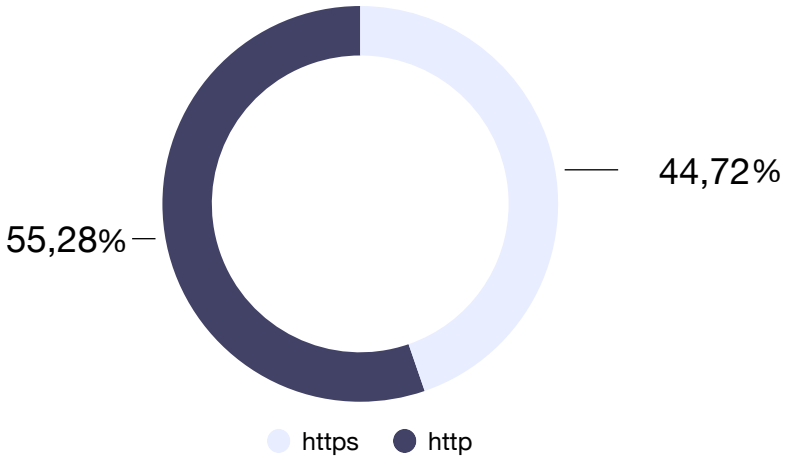
.com is the leading choice of threat actors by 33%.

B. Most Targeted Industries



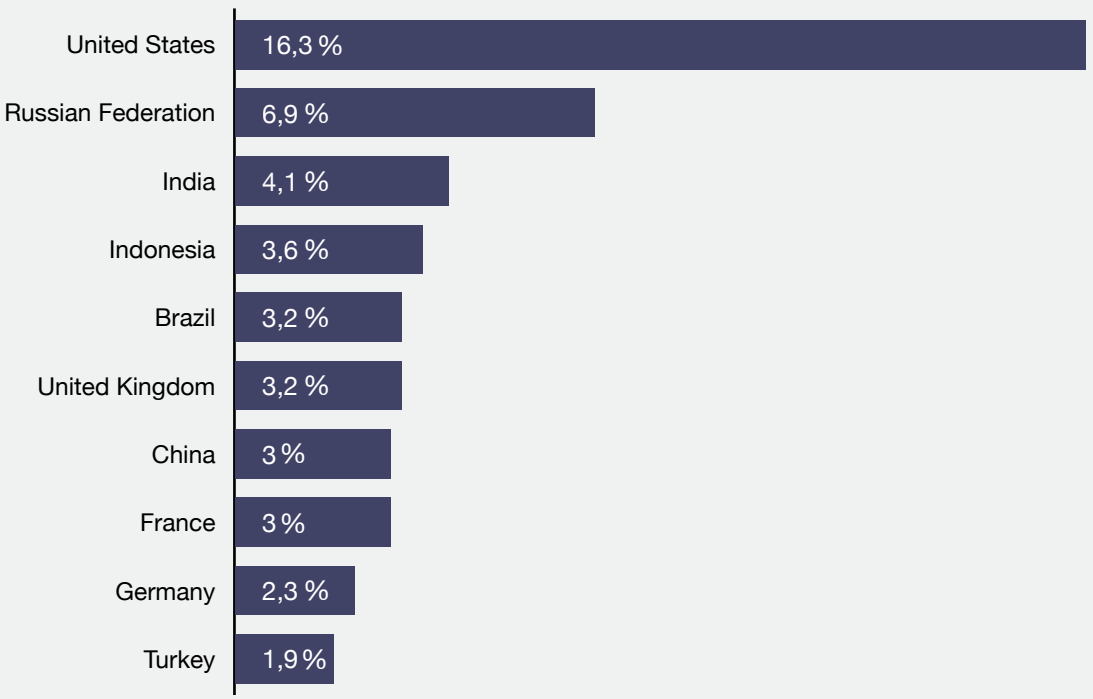
Phishing in 2022

C. SSL Certificate Preference



55% of the Impersonating domains use SSL certificates to give users a false sense of security.

D. Most affected Countries



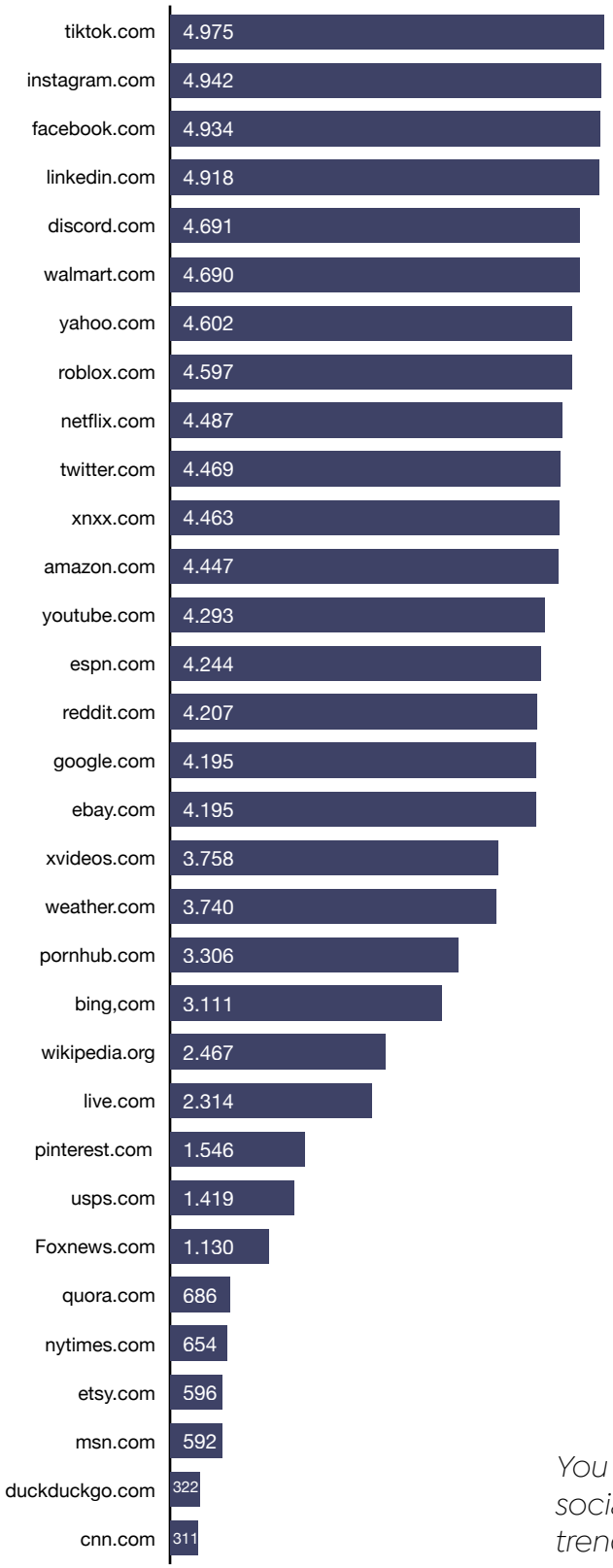
The threat actors targeted the US by far

Phishing in 2022

E. Most Affected Websites

We analyzed some of the most visited sites of the US for potential impersonating domains using one of the SOCRadar`s free SOC Tools, Phishing Radar.

Here are the results:

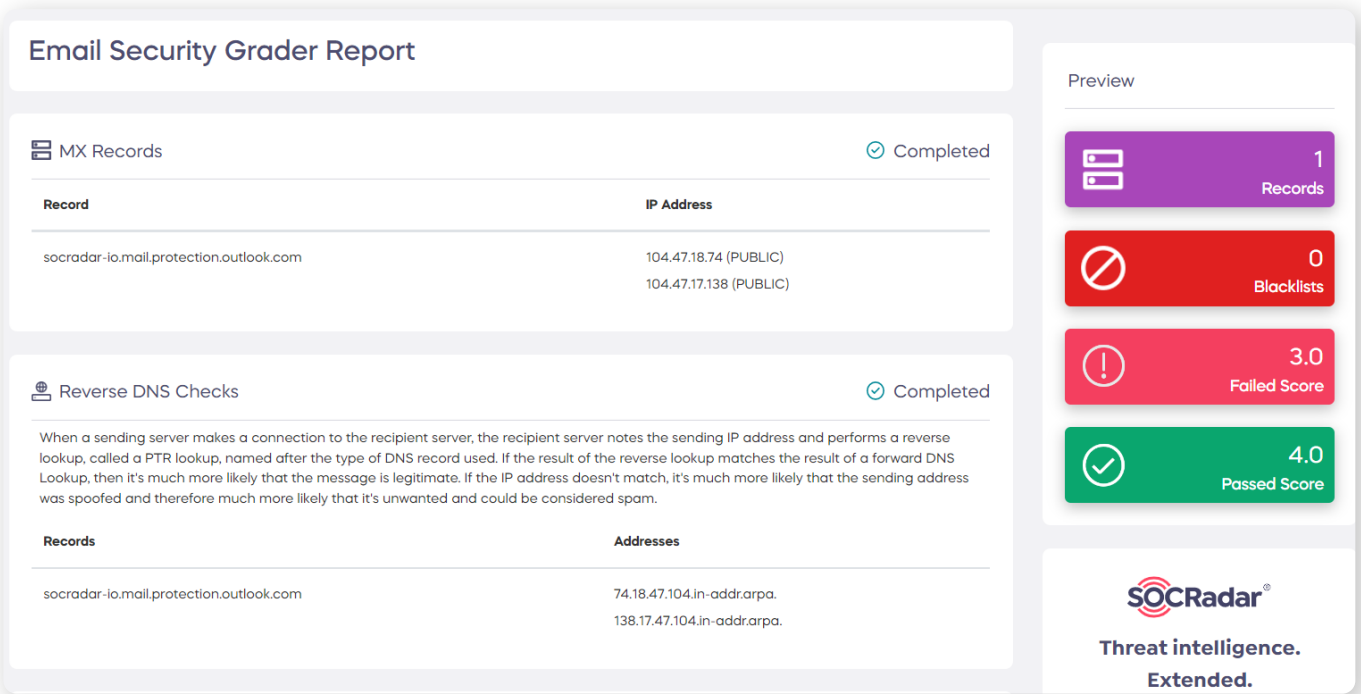


You will notice at first glance that the top 5 sites are all social media networks. This result corroborates the trend that threat actors are targeting mobile devices.

Phishing in 2022

F. Email Security Grader and Analyzer

One of the measures against phishing is keeping your e-mail services secure. Another free tool from the free SOC Tools of SOCRadar, "Email Security Grader Report," allows you to determine that.Then, Email Security Grader performs passive and active checks using cyberattack techniques. Afterward, it completes its work by making checks on threat intelligence.



Also, if you have a suspicious email, save it as a .eml file and upload it to the E-mail Threat Analyzer. It will help you figure out if the email is a scam.

3. Top 10 Targeted Industries and Countries in 2022

On the Darkweb

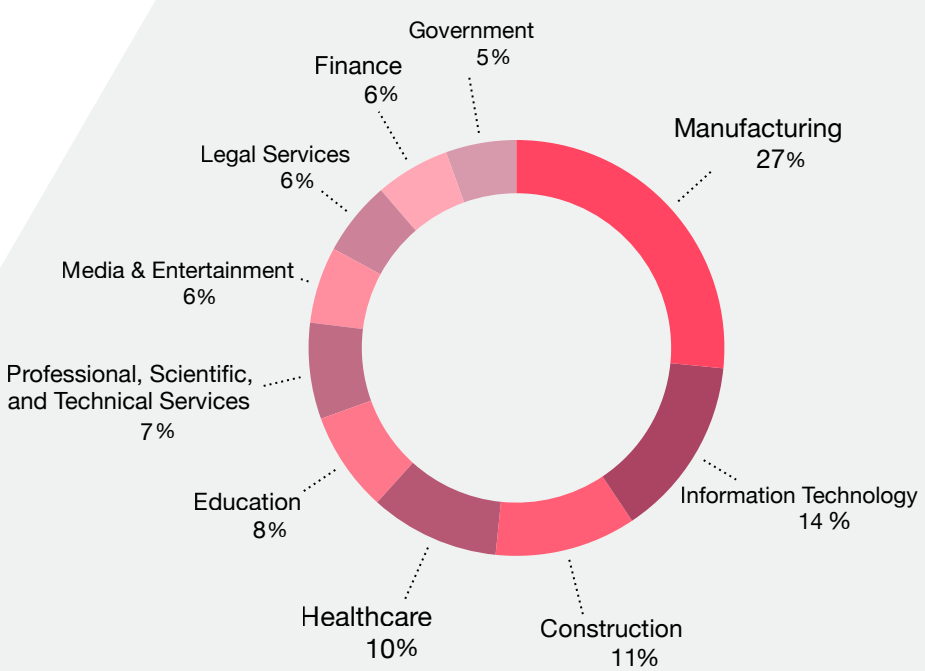
Now, let us discuss some of our findings from the Dark web.
Cyberattacks monitored by SOCRadar between January 1st and December 15th, 2022, can cause various problems regardless of the business, from minor inconveniences to significant losses and, worse yet, lawsuits against your company.

Threat actors could choose a company in any field as their target to compromise the victim's digital assets. However, being attacked reduces significantly a company's productivity and damages its reputation.

Here are the top 10 industries that the threat actors discussed the most over the dark web channels:

- Government
- Finance
- Cybersecurity
- IT
- E-commerce
- Media & Entertainment
- Cryptocurrency
- Education
- Telecommunication
- Healthcare

Industries Mentioned Most on the Darkweb



(Source: SOCRadar)

The top industries targeted by ransomware threat actors differ from those mentioned in dark web posts. The graph shows that ransomware actors choose industries in which business continuity has utmost importance.

Based on the information above, dark web forums and ransomware groups in 2022 targeted the health industry. As SOCRadar monitored, 163 ransomware attacks against the healthcare industry were reported in 2022, with LockBit ransomware being the most active ransomware group. More information about the functional ransomware groups and notable cyberattacks on the healthcare industry in 2022 can be found in SOCRadar's research.

Top 10 Targeted Industries and Countries in 2022

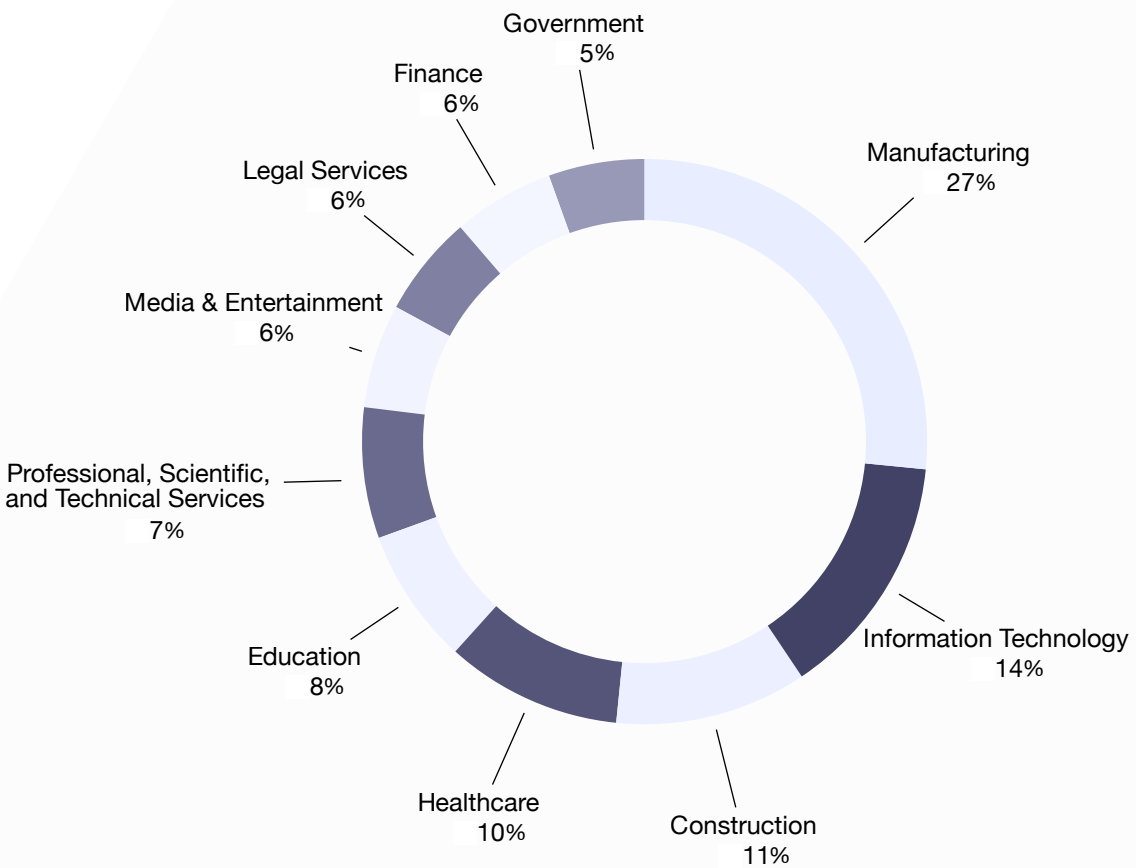
By the Ransomware Groups

Since the ransomware and extortion gangs do not follow the same patterns as the rest of the cybercrime world and are very picky about going after certain types of targets, the intelligence about these gangs needs to be differentiated from other **dark web intelligence.**

Analysts at SOCRadar keep an eye on these gangs through the standard methods in addition to the affiliated blogs and forums. Here are the top 10 industries where ransomware and extortion gangs are most discussed on their blogs and forums.

- **Manufacturing**
- **Information Technology**
- **Construction**
- **Healthcare**
- **Education**
- **Professional, Scientific, and Technical Services**
- **Media & Entertainment**
- **Legal Services**
- **Finance**
- **Government**

Industries Targeted Most by Ransomware Gangs

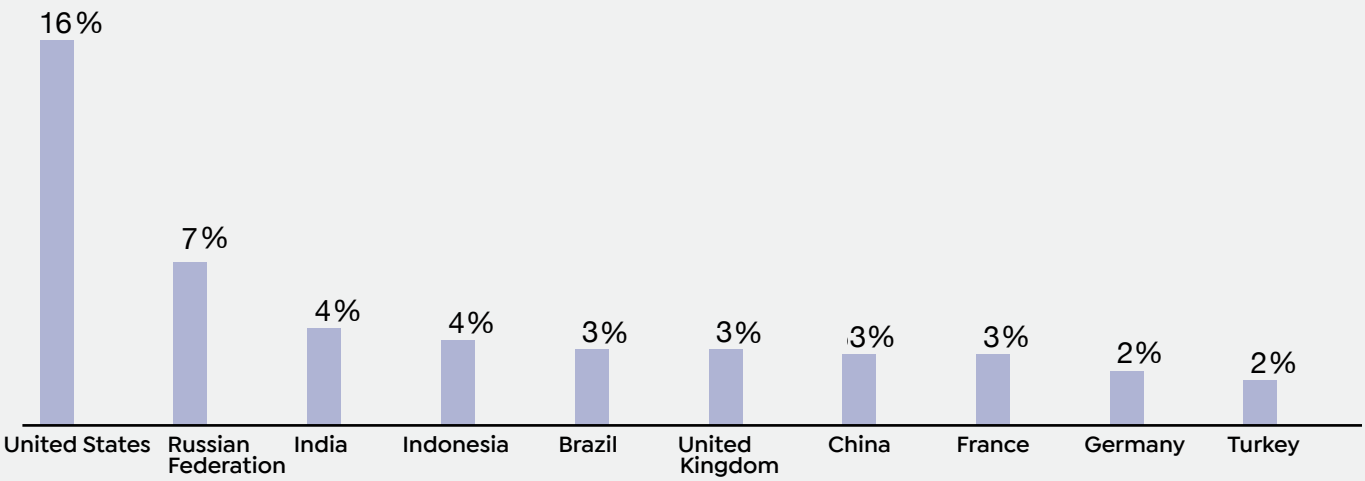


(Source: SOCRadar)

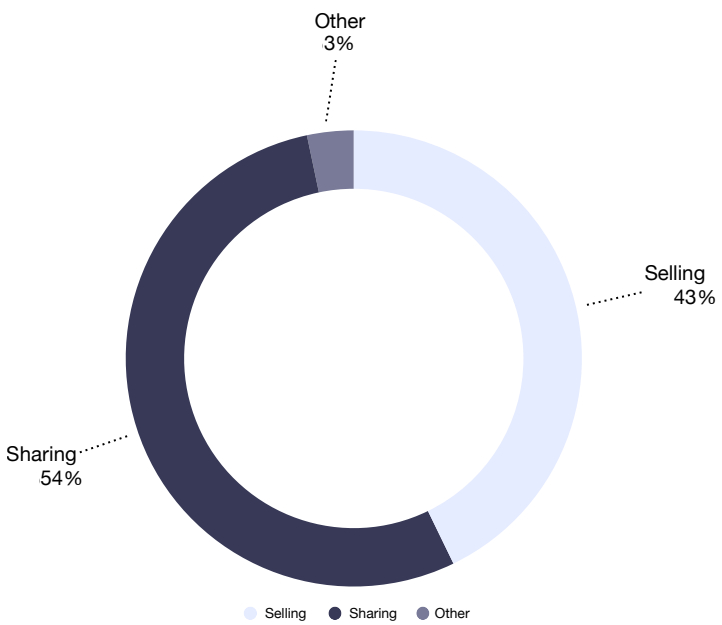
4. Top 10 Countries Targeted by Threat Actors in 2022

On the Darkweb

No single answer is why one nation is targeted more than another. Still, a larger country equates to more devices, which indicates a larger attack surface for attackers to exploit. Other significant factors include the level of cybersecurity awareness across the country and the existence of more important targets like infrastructure or companies.



The list of the most mentioned countries in these channels (Source: SOCRadar)

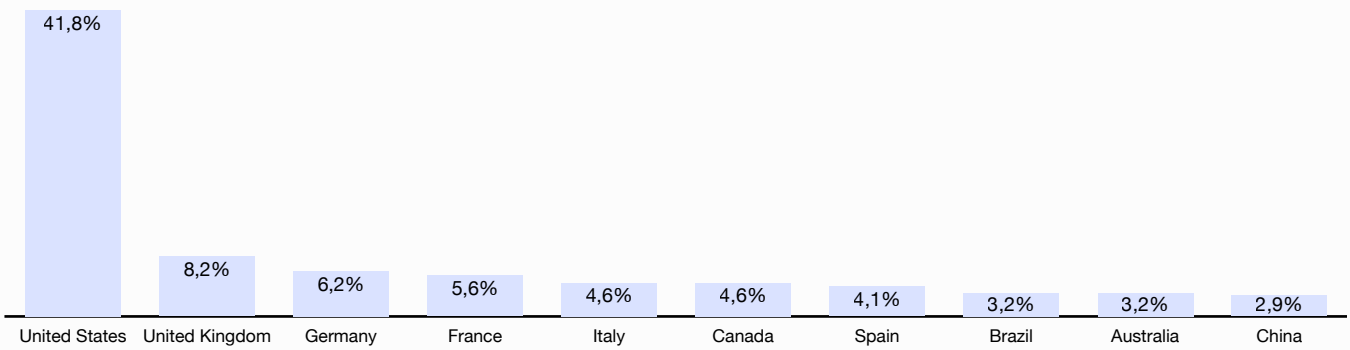


(Source: SOCRadar)

In addition, most of these posts is about trading and exchanging data.

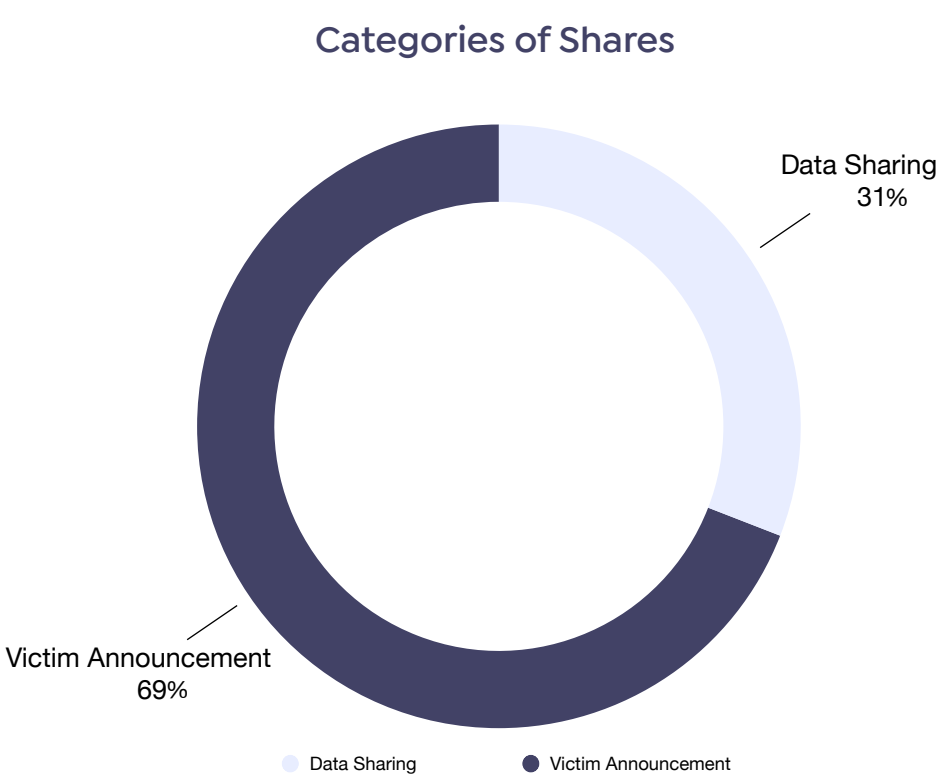
The other 3.3% is about buying data, hacking and target announcements, and partnership/cooperation offers. Again, the top 10 are ranked differently for ransomware actors. In our CTI solution of SOCRadar Platform, you can find intelligence about ransomware and extortion gangs in different categories. SOCRadar analysts follow these threat actors in communication channels, forums and blogs.

Top 10 Countries Targeted by Threat Actors in 2022



Distribution of posts linked to countries (Source: SOCRadar)

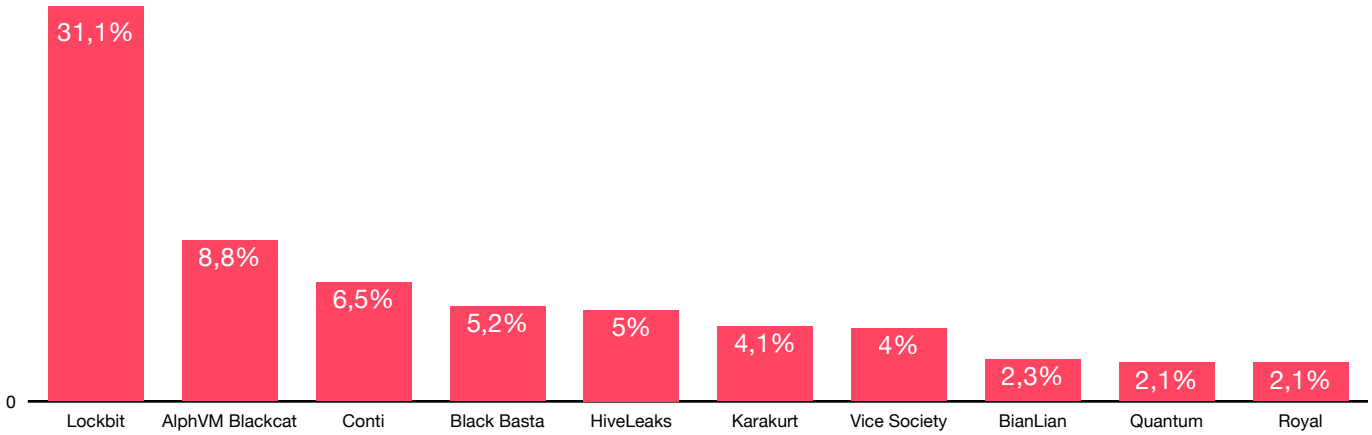
Except for Brazil and China, 8 of the top 10 targets are located in North America, Europe and Commonwealth Countries. What has been shared in these channels are the announcements of victims and exposed data of uncooperative victims. As shown in the circle graph below, most posts were victim announcements, either because the victim paid the demanded ransom or because the statement was a fake story. Even if the ransomware attack is unsuccessful, it will still harm an organization's reputation.



Percentage of post categories (Source: SOCRadar)

5. Ransomware Attacks in 2022

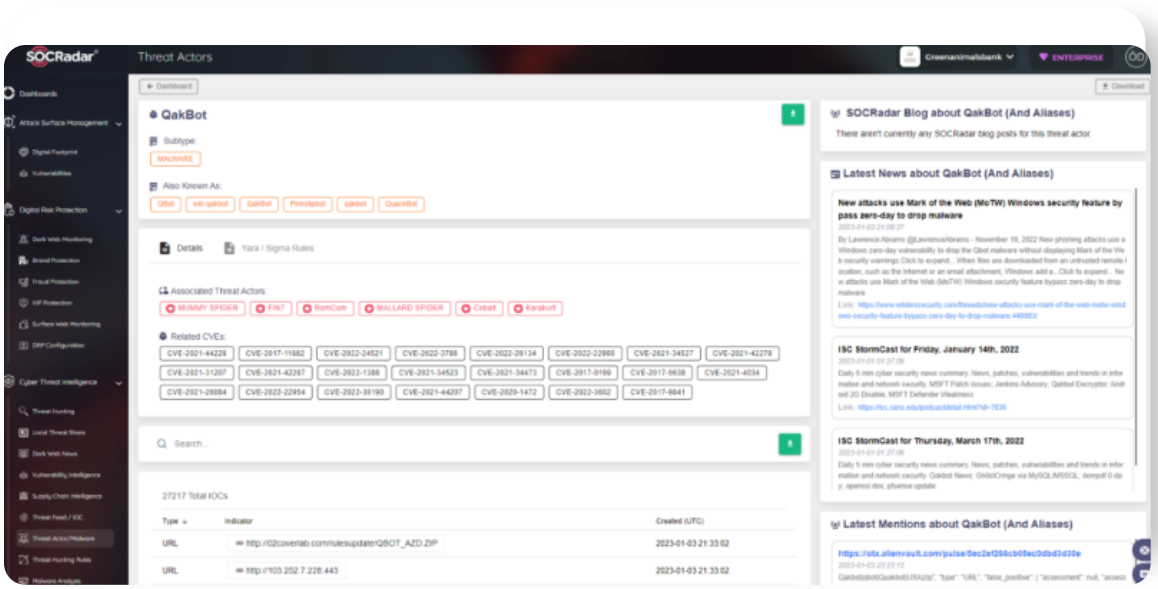
LockBit was the most active ransomware group with the most mentions on dark web forums in 2022 followed by BlackCat and Conti.



Most active ransomware groups. (Source: SOCRadar)

What Have We Learned from Ransomware Attacks in 2022?

Lesson 1: Although many researchers thought ransomware attacks would decrease when Conti ceased operations, it did not turn out that way. In 2022, when many ransomware groups surfaced, their TTP showed unique features as well as similarities. One of the unique tactics used by a ransomware group, Royal Ransomware, is "callback phishing". It is one of the recently emerged phishing techniques. Callback phishing is a type of phishing attack that impersonates a business. The attack starts off as a phishing email, typically claiming that the victim needs to renew a subscription or pay a bill for a service that they did not purchase. The email contains a "customer service" phone number with direction to call if the victim has questions and concerns.



The SOCRadar Threat Actors/Malware tab can track and index hacker groups, ransomware organizations, and the malware they use, giving you access to relevant IoCs.

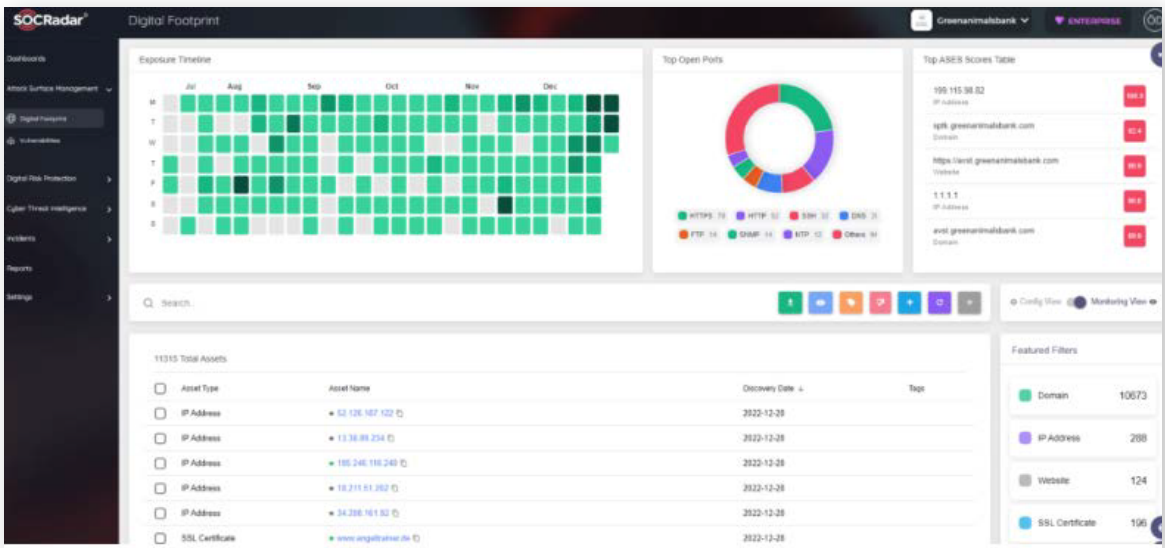
Lesson 2: It is clear that ransomware groups are only sometimes motivated by financial gains. We saw that in 2022, nonprofit and governmental organizations could also suffer tremendous damage from such groups. For this reason, these kinds of organizations should also take precautions against these threats.

Lesson 3: The emergence of new and updated variants will complicate signature-based detection. As a solution to this situation, SOC analysts should be able to follow up-to-date IoCs, and organizations should support their cybersecurity technologies with cyber threat intelligence to adopt a more proactive defensive approach.

Lesson 4: Although industries where uptime and data sensitivity is critical make relatively less money, they may seem more prone to paying the ransom because they have less tolerance for such attacks. One of the most common security vulnerabilities in industries such as healthcare and education is that the systems are outdated. It may be necessary to regularly update and replace the devices that reached the end of life.

Digital assets also should be tracked by using External Attack Surface Management products. In this way, organizations gain visibility on all known and unknown assets.

Lesson 5: Small and medium-sized enterprises spend less money on cybersecurity measures. As a result, it can cause them to spend much more money in the event of a ransomware attack. It is essential for every organization to meet specific standards in cybersecurity and to detect where attacks may come from to take precautions.



SOCRadar, Attack Surface Management tab can help identify and reduce the number of potential entry points for ransomware, further reducing the risk of a successful attack.

6. Top Cybersecurity Incidents in 2022

Everyone worked to overcome the negative effects of COVID-19 in 2022, while threat actors merely sought to get more money from these efforts. International crises like the diplomatic conflict about Taiwan and Russian invasion of Ukraine have also inspired threat actors. Let us take a look back at the top cyber incidents of 2022.

February

Russian Invasion of Ukraine

As a beginning, several Ukrainian companies were infected with malware in January 2022. DDoS attacks began soon after, targeting government agencies in Ukraine, such as the Ministry of Foreign Affairs and the Security and Defense Council. The second wave of DDoS attacks hit the government and two of the state's largest banks. Some known hacker groups also participated in the conflict. Anonymous, the world's largest hacktivist organization, has declared cyber war on Russia; and the ransomware gang Conti sided with Russia.

March

Ronin Bridge Hacked: $625M Has Been Stolen

In one of the most significant crypto attacks, hackers stole about $600 million from a blockchain network linked to the well-known online game Axie Infinity. Players can earn virtual money, and non-fungible tokens (NFTs), a type of financial security made up of digital data stored in a blockchain, by playing Ronin's Axie Infinity game.

August

China-Taiwan Conflict

Nancy Pelosi was the first US representative to visit Taiwan in the last 25 years, and her visit in August 2022 sparked some diplomatic events and cyberattacks. China did not want the visit to happen and started to pressure Taiwan in response to its recent political recognition. Before Pelosi arrived, attackers hacked billboards in shops and train stations. The hacked billboards showed Chinese messages that were urging Pelosi to leave Taiwan. Threat actors launched strong DDoS attacks against Taiwan's presidential office and other official government agencies' websites, including the Ministries of Foreign Affairs and National Defense; as a result, the websites went offline. Around the time of the visit, many threat actors began selling and leaking company and citizen data related to Taiwan and China on underground forums.

Top Cyber Incidents in 2022

August

Twilio, Cloudflare, and MailChimp Attackers Targeted Over 130 Organizations

The hackers responsible for some hacks, including those on Twilio, MailChimp, and Cloudflare, have been linked to a more extensive phishing campaign that targeted 136 organizations and resulted in the theft of 9,931 account login credentials. This login information was gathered using the phishing tool known as 0ktapus. Most of the victim organizations are based in the US (114), India (4), Canada (3), France (2), Sweden (2), and Australia (1). There have reportedly been at least 169 phishing domains for this purpose.

September

Cisco Confirms Hacking by the Yanluowang Ransomware Gang

Cisco has confirmed that the Yanluowang ransomware group has compromised their local network and that the actor attempted to extort them by threatening to publish stolen data online. Investigation results showed a Cisco employee's credentials were compromised after a hacker took over a personal Google account where the victim's browser was synchronizing credentials.

September

Nearly the Entire Uber IT System Was Breached

The internal systems of Uber were compromised on September 15. The hacker was able to access the company's Slack account, HackerOne account, and full admin access to their AWS Web Services and GCP accounts. The entry attack used a social engineering campaign to target Uber's employees. An Uber employee received a text message from the hacker, which appeared to be from the company's IT department.

September

Hackers Released 10 Terabytes of Military Emails and Files

Approximately ten terabytes of emails and other documents from military and police organizations in Chile, Mexico, El Salvador, Colombia, and Peru were released by the hacking group Guacamaya, which has mainly aimed at Central American targets.

Top Cyber Incidents in 2022

October

$529M is Stolen from Indian Citizens by Chinese-linked Hackers

According to the cybercrime unit in the state of Uttar Pradesh, Chinese scammers have allegedly stolen $529 million from Indian citizens using instant lending apps, part-time job lures, and fake cryptocurrency trading schemes.

October

$570M Stolen from Binance Blockchain

Due to a cyberattack that happened on October 4, 2022, led to the theft of about two million BNB (Binance Coin) tokens, which could have been exchanged for more than $570 million in fiat currency.

October

The Largest DDoS Attack by Mirai Botnet on Wynncraft Minecraft Server

Cloudflare, a web infrastructure and security provider, announced that a Mirai botnet had successfully stopped a 2.5 Tbps distributed denial-of-service (DDoS) attack. Researcher Omer Yoachimik described the attack as a multi-vector attack consisting of UDP and TCP floods. It was targeted at the Wynncraft Minecraft server.

6.Top 10 Data Breaches in 2022

BlueBleed Data Leak

On September 24, 2022, SOCRadar's integrated Cloud Security Module discovered that 65.000 entities' sensitive data became public due to a server configuration error at Microsoft's Azure Blob Storage. PII (Personally Identifiable Information) data, documents that may contain intellectual property, Proof-of-Execution (PoE) and Statement of Work (SoW) documents, user information, product orders and offers, project information, and other information are all part of the leak. Six significant public buckets of the many found contained data on more than 150.000 companies across 123 nations. With sensitive data contained in a single bucket and affecting more than 65.000 entities across 111 countries, it can be considered one of the biggest B2B leaks.

Threat actors need sensitive information to carry out most of their malicious activity. They typically obtain the information by conducting various cyberattacks or simply gathering it from unprotected platforms, accounts, or databases. Data leaks typically have a long-lasting effect because the information is always reusable in different attack techniques.

NVIDIA | 71,000 Employee Credentials

71.000

In February, Nvidia experienced a breach that led to the theft of 71.335 employees' credentials. The threat actors later leaked the information of compromised accounts. The Lapsus$ gang later claimed responsibility for the hack and disclosed that they had stolen 1TB of data from Nvidia's network. After a futile ransom demand, 20GB of the data was leaked on threat actors' Telegram channel.

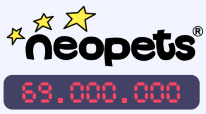
ChatVPN, GeckoVPN, and SuperVPN | 21 Million Accounts

21.000.000

A threat actor exposed 10GB of data on a Telegram channel. The data contained 21 million records from users of various VPN services. In 2021, threat actors listed 21 million data records belonging to ChatVPN, GeckoVPN, and SuperVPN users for sale on the dark web. Later, in May 2022, the data dump was leaked to the public via a Telegram hacker channel.

Top 10 Data Breaches in 2022

Neopets | 69 Million Accounts



The virtual pet platform Neopets, which introduced its own NFTs, had its source code and database publicized. A data breach of the Neopets platform led to over 69 million users' personal information theft. A threat actor under the alias "TarTarX" sold the data on a breach forum. Researchers found that the attackers had access to Neopets' systems since January 3, 2021.

Rockstar Games | Source Code, Assets, Test Clips

Slack and Confluence servers owned by Rockstar Games were compromised due to a network breach. Data from video games called "GTA 5" and the upcoming "GTA 6" were stolen. "Teapotuberhacker," also responsible for Uber's intrusion, leaked the data on GTAForums. The threat actor sold some of the data for more than $10.000. GTA 5 and GTA 6 source code and assets, as well as GTA 6 testing videos, were allegedly stolen.

MyDeal | 2.2 Million Customer Information

An Australian retail marketplace operated by Woolworths, called MyDeal, reported a data breach that affected 2.2 million customers. According to the company, a hacker gained access to the CRM system using stolen credentials and obtained the sensitive customer information. The hacker then offered the stolen information for sale on a dark web forum.

Optus | 9.8 Million Customer Information

A threat actor gained unauthorized access to Optus' network and stole 9.8 customer information records. It is unclear when the actual breach happened, but it was detected on September 22. The telecom company had an API allowing customer data access without authorization or authentication. The vulnerable API could be the entry point of the attack. The hacker "optusdata" uploaded a sample of 10.200 customers' stolen data and demanded a $1 million ransom.

Top 10 Data Breaches in 2022

Twitter | 7 Million Accounts

7.000.000

Twitter, had a significant data leak incident in July. The leak resulted in a much larger leak afterward. A threat actor acquired over 5.4 million Twitter user records with private information and leaked it on a hacker forum. Attackers obtained the information in December 2021 by using an API vulnerability that had been made public in a HackerOne bounty program and was fixed in January 2022. In July 2022, the threat actor sold personal information for $30.000. In November, security researchers found nearly 7 million Twitter profiles with private information on the dark web. In addition to the 1.4 million suspended user profiles collected using a different API, the database also contained the 5.4 million user profiles from the earlier leak. Leaks included public information like verified status, account names, Twitter IDs, bios, screen names, and personal phone numbers.

WhatsApp | 487 Million Phone Numbers

487.000.000

In November, a threat actor advertised the phone numbers of 487 million WhatsApp users for sale on a breach forum. According to reports, the database was recent. Although it was most likely scrapped, it is unclear how the threat actor got access to these records. The threat actor divided the records into datasets and priced them differently. Later, the post was taken down, but new dark web posts started to spread similar information. Using the exposed phone numbers, attackers could trick users via SMS or phone calls. The leaked data included phone numbers from users in 84 countries, most of whom were from Egypt, Italy, and the US.

Medibank | 9.7 Million Customer Data

medibank
For Better Health

9.700.000

Medibank's customer data was compromised due to the company's refusal to pay its attackers following a ransomware incident. The data was stolen but not encrypted because Medibank stopped the attack following reports from Australian authorities. During the breach, attackers gained access to 9.7 million customers' data. They published sample data and demanded a $10 million ransom from Medibank, threatening to leak the stolen data on the dark web if they refused. Medibank refused to pay the ransom, so the attackers leaked the documents on the dark web on November 9.

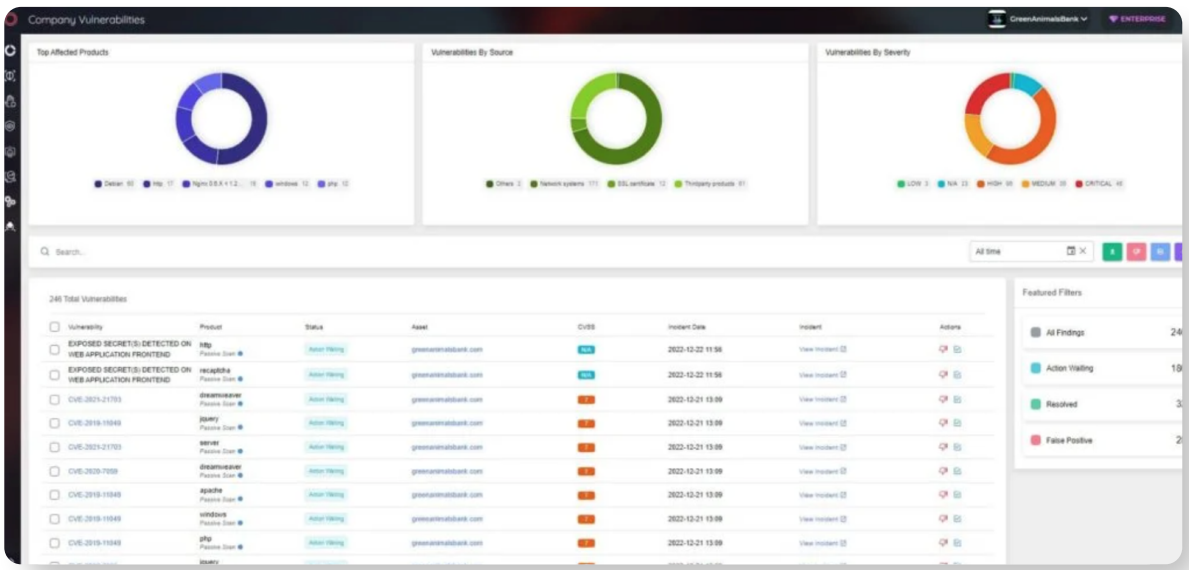
BidenCash | 1.22 Million Credit Cards

1.220.000

BidenCash carding marketplace leaked an advertisement dump that contained information of 1.221.551 credit cards. The data was made publicly available. The marketplace obtains the information in leaks via stealer malware and skimmers. BidenCash had leaked a promotional dump before the carding website was first launched on June 16. The initial database dumped then contained about 8 million lines of data, including email addresses, with about 6.700 credit cards.

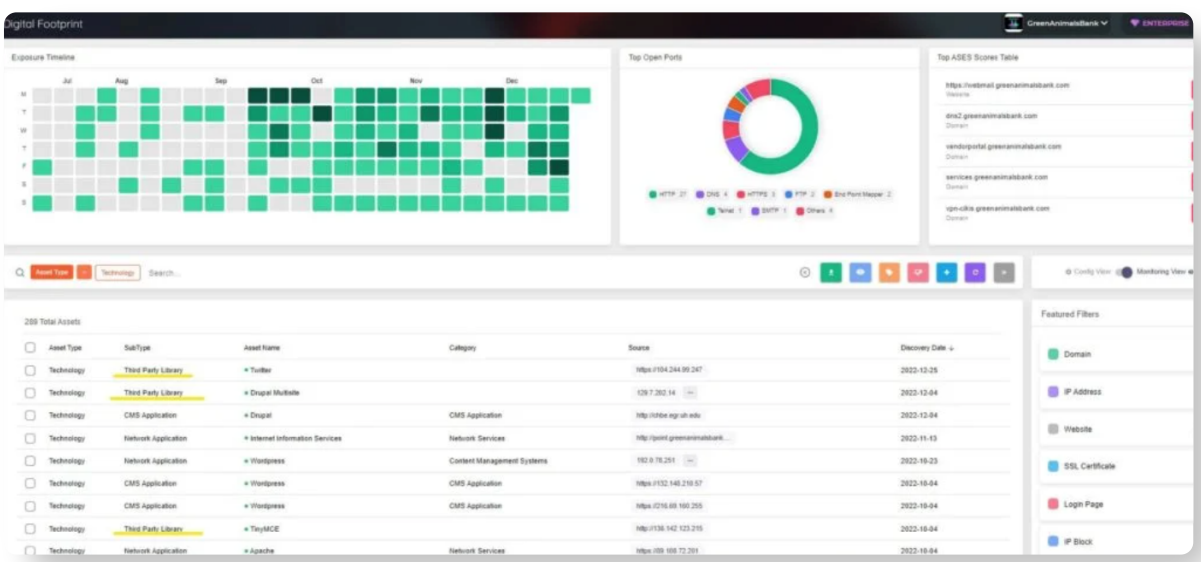
What Have We Learned from Data Breaches in 2022?

Lesson 1: Regular posture review reviews help to identify potential exposures promptly and efficiently. In this context, reviewing and updating security measures should be one of the priorities to avoid vulnerabilities.



SOCRadar XTI, Attack Mapper, Company Vulnerabilities

Lesson 2: Companies that share data with a third-party organization must ensure they have at least the same cybersecurity awareness. Third-party vendors and service providers should be closely monitored, conduct due diligence, and provide necessary security protocols to prevent abuse of data exchanges between them by threat actors.



SOCRadar XTI, Attack Mapper, Digital Footprint

What Have We Learned from Data Breaches in 2022?

Lesson 3: Organizations need to educate employees about identifying and avoiding cyber threats. Also, it is crucial to deploy multi-factor authentication for employee access.

Lesson 4: Companies must ensure that access to critical data corresponds to an employee's specific role in the company. Also, authorities should review all critical users' access levels. When an employee leaves, the company must revoke access to systems immediately. Additionally, implementing a zero-trust framework will improve organizational security.

Lesson 5: Organizations should use Extended Threat Intelligence solutions that provide to identify and mitigate threats across the surface and dark web.

7. Top 5 Critical Vulnerabilities Routinely Exploited by Threat Actors in 2022

For threat actors, **vulnerabilities** are essential tools in their arsenal. Vulnerabilities are software security flaws that may be unknown to the developer or the vendor and are one of the most vital security concerns. However, even if the vendor provides security patches for a vulnerability, the threat actors do not cease their efforts in abusing the unpatched systems.

Here are the **top 5 vulnerabilities in 2022** curated from the SOCRadar Vulnerability Intelligence module:

Atlassian Confluence Server and Data Center RCE Vulnerability | CVE-2021-26084

It is a remote code execution (RCE) vulnerability, precisely, an OGNL injection vulnerability. A threat actor can execute an arbitrary code on a Confluence Server or Data Center without needing authentication. With nearly 250.000 customers, Atlassian is in every corner of the world. As a result, any vulnerability it has can be an attractive target for threat actors. According to CISA's multiple alerts, the CVE-2021-26084 has been one of the top vulnerabilities exploited by the threat actors since it was reported. Atlassian provides short-term workaround and patches.

Zerologon | CVE-2020-1472

It is an elevation of privilege vulnerability. It occurs when a threat actor, using the Netlogon Remote Protocol, establishes a vulnerable Netlogon secure channel connection to a domain controller. As a result, a threat actor could run a specially crafted application on a device on the network. Since Windows 3.11, every release of Windows has NetLogon. Combined with the presence of Windows machines worldwide, ZeroLogon should not be ignored. Microsoft recommends patching immediately.

Top 5 Critical Vulnerabilities Routinely Exploited by Threat Actors in 2022

Gitlab | CVE-2021-22205

An issue in GitLab CE/EE affecting all versions starting from 11.9. GitLab was not properly validating image files that were passed to a file parser, which resulted in a remote command execution. Anyone able to upload an image that goes through the GitLab Workhorse could achieve RCE via a specially crafted file.

Fortinet FortiProxy | CVE-2022-40684

It is an authentication bypass using an alternate path or channel found in Fortinet FortiOS, FortiProxy, and FortiSwitchManager. It allows an unauthenticated attacker to perform operations on the administrative interface via specifically crafted HTTP or HTTPS requests. According to Fortinet, more than 615000 customers are using Fortinet appliances. With this number of customers, threat actors could feel tempted to try and abuse a Critical vulnerability such as CVE-2022-40684 constantly.

Log4Shell | CVE-2021-44228

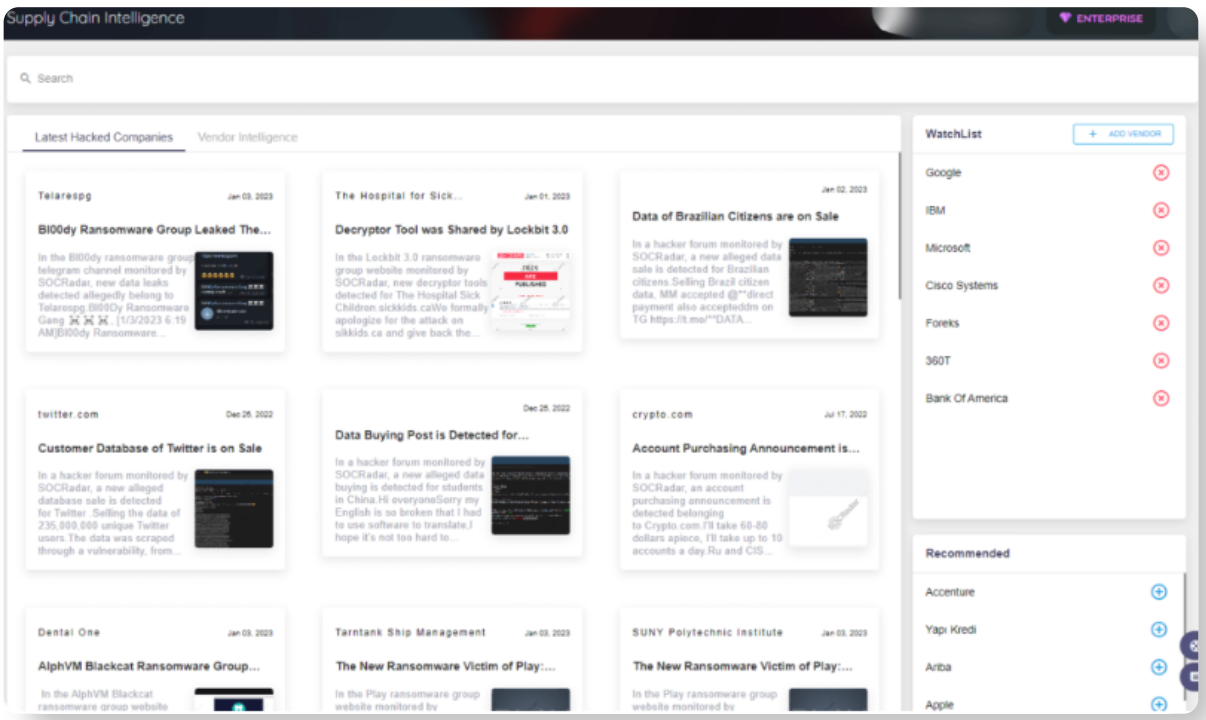
It is a remote code execution (RCE) flaw found on Apache Log4j 2 Java logging library. One of the most dangerous vulnerability types because it allows remote attackers to control servers over the Internet entirely. At the time of the discovery, all the versions of Log4j 2 were open to vulnerability. The first 72 hours of the vulnerability saw nearly a million attempts at exploitation. It is still present and widely used by threat actors. Also, the CISA's report on China State-Sponsored Threat Actors states that it is still one of the top vulnerabilities leveraged by China-linked threat actors. For a detailed explanation. Apache has released a patch for the vulnerability. In addition to patches, some mitigation techniques are also shared by Apache.

What Have We Learned from Log4Shell in 2022?

Lesson 1: Apache Log4j is an open-source library, meaning that programmers can copy, modify, and use it in their projects. Log4j is seen as a dependency in almost 7.000 other open-source projects. Because of its freedom and usefulness, some software, such as the Log4j logging library, became prevalent. This prevalence might lead the developers to think that if there were any problems, they would be disclosed by now.

To get ahead of problematic situations such as this, developers can leverage from Software Bill of Materials (SBOM). SBOM enables organizations to identify and track all third-party components, particularly open-source components, and comply with licensing requirements. It also helps ensure that the organization does not run vulnerable open-source components and keeps track of critical updates and patches.

Lesson 2: Despite the widespread awareness of the Log4Shell vulnerability within the cybersecurity community, vulnerable versions of Log4j remain hard to detect in some instances. Some applications might use the open-source logging library as a direct dependency in their applications. SOCRadar provides Supply Chain Intelligence. With its help, you can proactively configure security measures using the intelligence provided by SOCRadar.



SOCRadar XTI, Attack Mapper, Digital Footprint

SOCRadar provides Supply Chain Intelligence. With its help, you can proactively configure security measures using the intelligence provided by SOCRadar.

What Have We Learned from Log4Shell in 2022?

Lesson 3: Visibility equates to speed in time of a potential crisis. Complete visibility into your environment when vulnerabilities such as Log4j are discovered is paramount when time is of the essence. Being able to immediately access your network and know exactly where to look for certain tools, technologies, attributes, and software can be the difference between a breach and a successful defense.

With the help of SOCRadar's External Attack Surface Management, organizations can have broader visibility into their system. In a case such as Log4j, organizations could have had a high level of visibility into their environment and would be able to understand how to handle a Log4j attack.

Lesson 4: A strong patching strategy should not be optional. As vulnerabilities become known in software, organizations must provide the necessary resources to their cybersecurity teams to remediate the vulnerabilities before threat actors can exploit them. In reflection of Log4j, patches for the applications with the logging library were released even before the vulnerability disclosure. However, the swiftness of the patches means nothing if the organization cannot allocate the time or resources to apply the patch.

Who is SOCRadar®?

Your Eyes Beyond

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, we aim to help security teams to detect blindspots before attackers.

The shortage of cybersecurity experts is a growing problem worldwide. All companies around the world companies 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. **With providing protection against threats for more than 4.000 companies from 150 countries, SOCRadar has become an extension of SOC teams from every industry**

SOCRadar provides extended cyber threat intelligence (XTI) that combines: **"Cyber Threat Intelligence, Digital Risk Protection, and External Attack Surface Management Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

5.600
Freemium Companies

Darknet and Deep 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 web, deep web, and darknet 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 resiliency by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS 12 MONTHS FOR FREE

Gartner peerinsights™ 5.0

Contact Us info@socradar.io +1 (571) 249-4598 651 N Broad St, Suite 205, Middletown, DE 19709