SOCRadar®
Your Eyes Beyond

2023 Q1 TÜRKİYE THREAT INTELLIGENCE REPORT:

Executive Summary

Türkiye, one of the economically developing countries and a member of G20 has geo-strategic advantage, population over 80 million. According to recent data from the World Bank, the proportion of its population with access to the Internet has exceeded 80% (more than 71 million Internet users). In addition, Türkiye Digital Quality of Life Index indicates that E-infrastructure, E-government, and E-security were the highest-scoring segments. Moreover, the country maintains its top ranking in digital development among OECD countries. Due to the above-mentioned characteristics, Türkiye has become increasingly a target for cyber threat actors.

Cyber security risks can cause substantial financial and reputational losses and minimizing security risks can not only be achieved through compliance processes and defensive security technologies. Organizations must acknowledge the importance of cyber threat intelligence (CTI) in obtaining actionable information about threat actors and how they weaponize their internet-facing assets and change their TTPs.

SOCRadar's Türkiye Threat Intelligence Report, presented the intelligence obtained by continuously scanning underground forums and channels and comprehensive insights on industry basis. The report provides insights that help security professionals to make informed decisions in mitigating cyber risks, and how to enhance your security posture.

It is necessary to take proactive and predictive measures by being aware of the dynamically expanding attack surfaces to gain broader visibility and awareness of the cyber gangs as strong as the weakest link of the chain. SOCRadar also performs dark web threat research, analysis, OSINT & HUMINT & SOCMINT observations, cybersecurity vendor blogs, and aggregating & normalizing & prioritizing information gathered from a range of open sources such as social media, internet, professional and academic publications, and commercial data.

SOCRadar characterizes and maps the threat landscape based on recently observed cyber threat actors' (especially, Ransomware groups, APTs) activities, phishing campaigns, malware attacks, top new critical and known exploited vulnerabilities (KEV), exploit kits, and stealers data gathered from dark web platforms and leveraging the comprehensive data monitoring, collection, classification, and analysis capabilities.

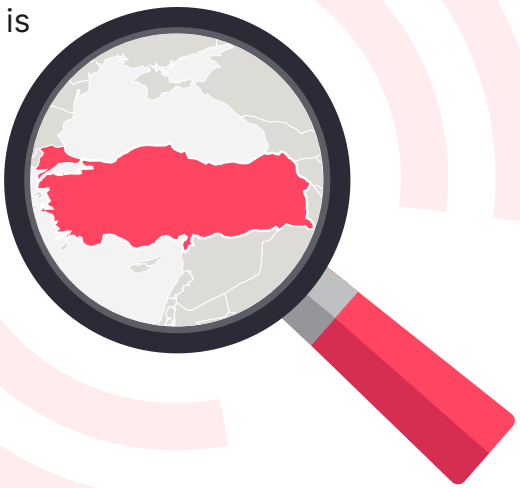
Key Findings

• In Q1 of 2023, SOCRadar DarkMirror Intelligence Module detected more than 170 dark web posts related to data breaches that targeted Türkiye. SOCRadar Research Analysts identified and analyzed the findings by enriching them with both OSINT and dark web intelligence and created a report with an emphasis on prioritizing the risks that pose threat to Türkiye on a sectoral basis.

• As a result of this analysis, the top five impacted industries, except for "other services" are; Public Administration (29%),

• Information Services/Telecommunication (15%), Arts & Entertainment (9%), Educational Services (8%) and Finance (8%).

• In the Other Services category, with a 12% proportion, there are 8 sectors and subsectors, and the top ones are Professional, Scientific, and Technical Services (28%), Religious, Grantmaking, Civic, Professional, and Similar Organizations (16%), Transportation and Warehousing (12%), Retail Trade (12%) and Construction sector (12%) respectively. This shows that the cyber-attack surface is expanding on a sectoral basis.



• More than half of the cyber incidents involving Public Administrators are related to Turkish citizens and consist of personal (PI, PII) and sensitive data (SPI, PHI)
In the Information Services sector category, prominently targeted sub-sectors are Telecommunication (42%), Internet Publishing and Broadcasting, and Web Search Portals (31%).
More than half of the cyber incidents involving the Arts & Entertainment sector are related to Gambling & Betting industry.

• Comparative analysis shows that the Educational Services, Finance, Health Care and Social Assistance, and E-commerce sectors are constantly among the most threatened sectors targeted by cyber threat actors and retain their significance compared to 2022 Q4 data.

• A large part of the data detected in dark web consists of 80% sharing and 20% selling. The Sharing data category consists primarily of Citizen/Customer/Employee data, personal and sensitive data, and the others are Access data (VPN, RDP and etc.) and Tools & Services.

Key Findings

- SOCRadar analysts have identified 187 malicious domains related to earthquake relief alone. In 2023 Q1, SOCRadar Phishing Radar detected 22,673 malicious websites related to Turkish entities.

- Most Common Malware Attacks are used in the malware family, such as Android banking trojan Nexus, Xenomorph Android malware, Emotet, BlackLotus, S1deload Stealer malware, and Hook Android malware.

- As a parallel study on info-stealer malware also shows that Türkiye ranked 6th among 200 countries exposed to this specific cyber threat, and the top malware strains targeting Türkiye included RedLine, Stealc, Meta, and Aurora info-stealers, respectively.

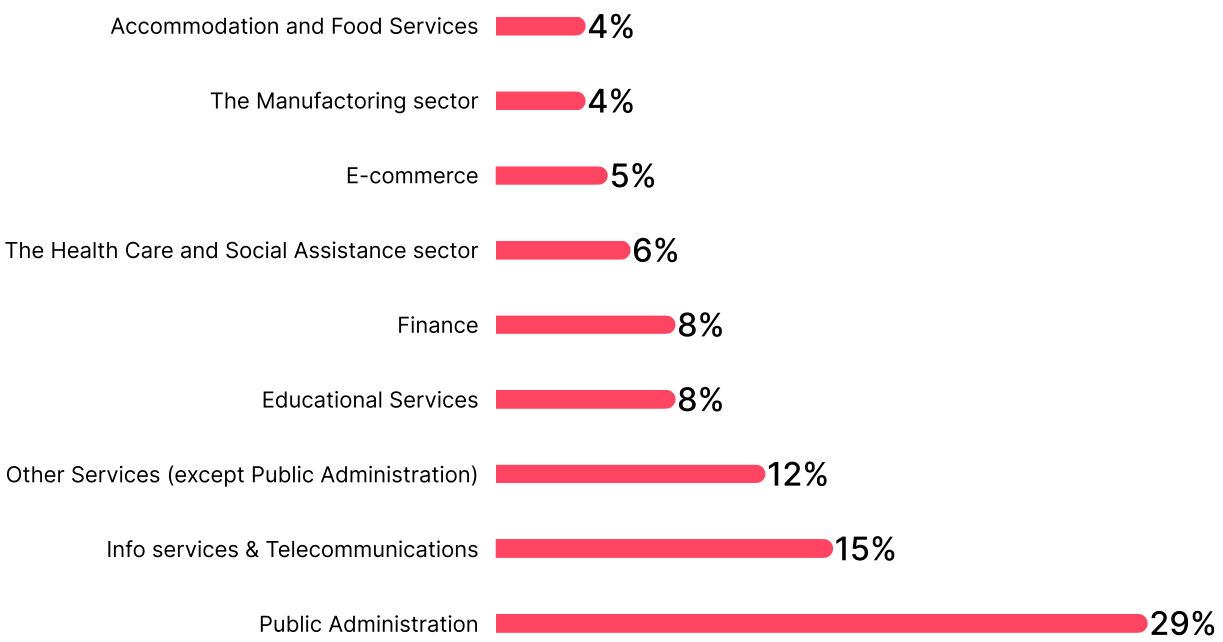
- SOCRadar's tracking on infrastructures associated with significant threat actors such as the APT groups that actively targeted Türkiye in the first quarter of 2023 concluded that the following groups are highly active in conducting cyber operations against Turkish assets:YoroTrooper, APT38 (Lazarus/Hidden Cobra), APT 34 (TA452, OilRig), and TA482.

- As long as attackers are able to profit significantly from successful attacks, ransomware will continue to develop. SOCRadar analysts identified that five (5) ransomware groups, including CL0p, Dark power, Lockbit 3.0, AlpHV /Blackcat, and Mallox, actively conducted assaults targeting across diverse industries in Türkiye, including Manufacturing, Information Technologies, Energy & Utilities, and Transportation & Warehousing respectively.

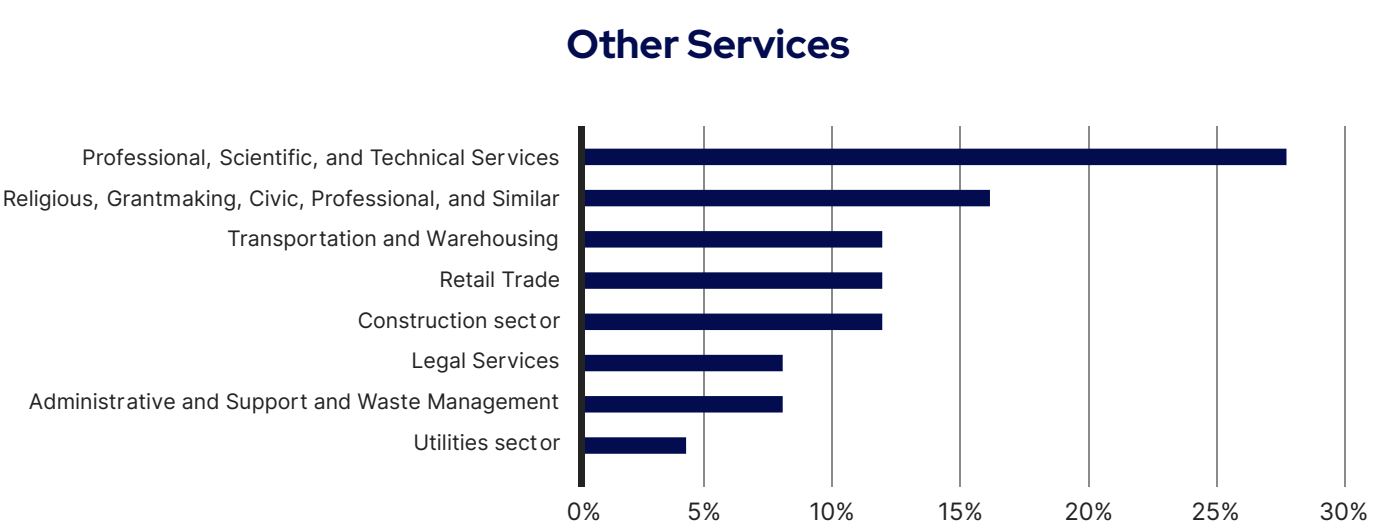
- In 2023, a number of newly discovered vulnerabilities associated with larger vendors, also affect Türkiye including CVE-2023-23397 (MS Outlook), CVE-2022-39952 (Fortinet FortiNAC), CVE-2021-21974 (Vmware ESXi) CVE-2023-21716) (MS Office), CVE-2023-20078(Cisco IP Phones)

1. Spotlight on: Dark Web Threats Targeting Türkiye

The distribution of cyber incidents targeting Türkiye by sector is given below. It is apparent that there are more and more sectors and more and more victims.



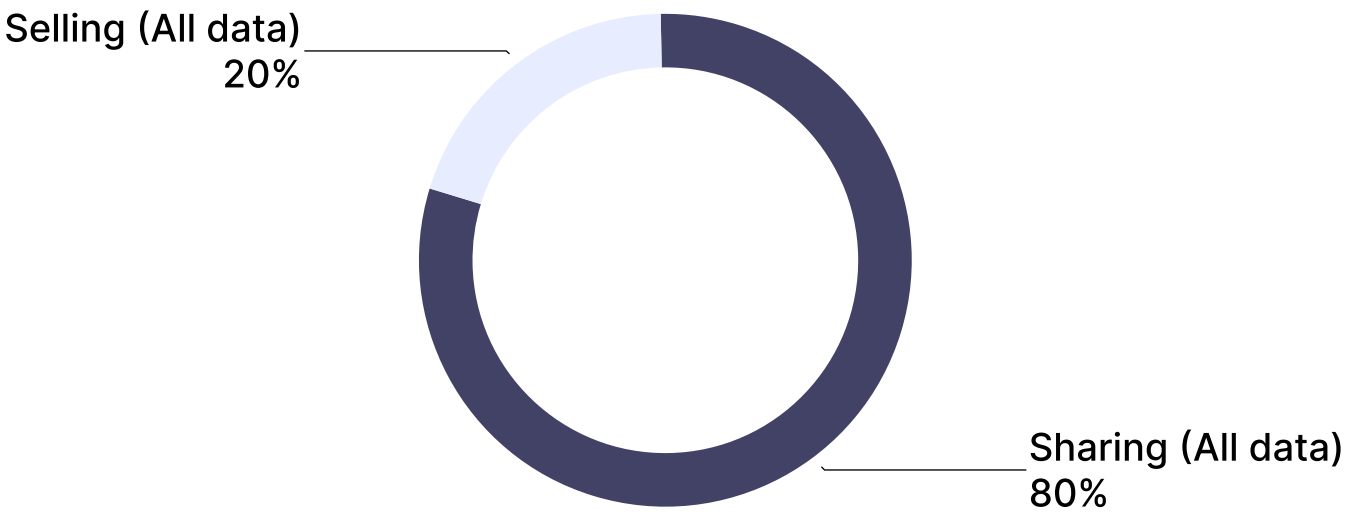
The breakdown of the sectors and sub-sectors in the “Other services" category is shown below. It can be a lesson learned that the attack surface is expanding with the rise of digitalization process and that security professionals should be ready for cyber-attacks at any time.



Although dark web posts are mostly shared for free on underground forums (80%), a small percentage (20%) of them are offered for sale as technical tools, such as valuable data, login credentials, or vulnerability exploits like zero-days.

There are some reasons why threat actors tend to share stolen data instead of monetizing at first sight. One of them is to ensure popularity and credibility in forums and Telegram channels, and also, even if purchased once, the data can be reused and distributed repeatedly. Moreover, as observed in ransomware groups, the effect of blackmailing, namely double extortion, may be used to carry out the naming and shaming process by publishing the data publicly if the ransom is not paid.

Dark Web Post Type



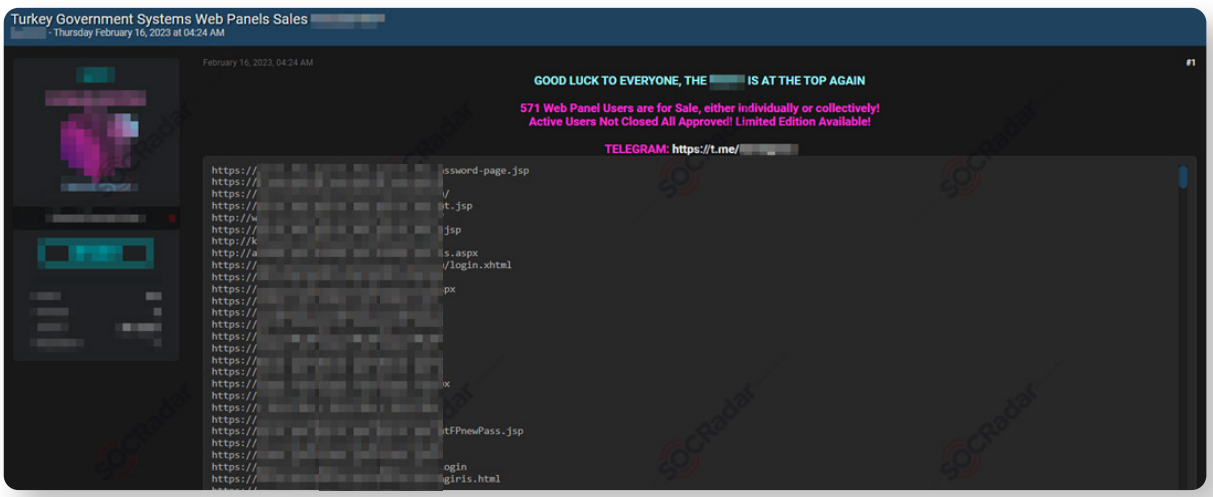
2. Recent Dark Web Activities Targeting Turkish Entities

a. Dark Web Post Type

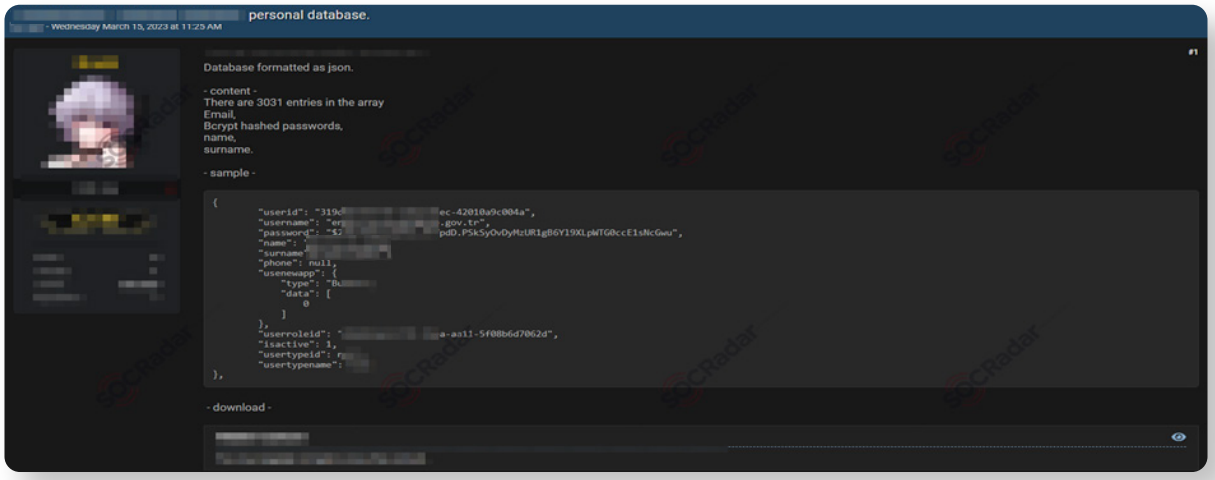
Public Administration related intelligence data usually come into sight as the sharing of databases on Turkish citizens periodically appears on dark web forums. This type of data is often not fresh, but a combination of databases previously obtained from different governmental institutions and also intercepted data individually using info-stealer malware. SOCRadar dark web analysts check whether this information is up-to-date and inform relevant organizations in time. One of the last recent shares is seen below.

On March 3rd, in a hacker forum monitored by SOCRadar, a new alleged number database leak was detected for the number and identity information of Türkiye citizens.

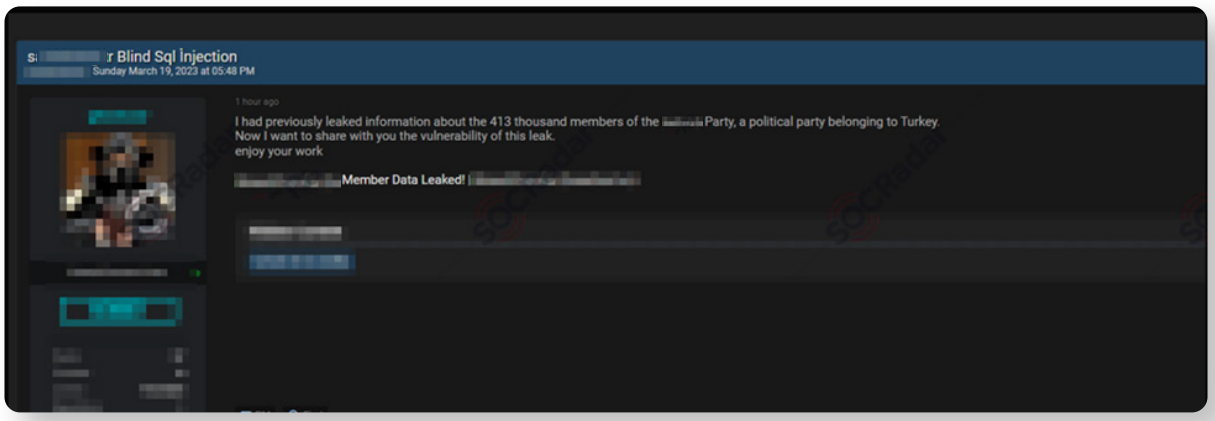
Moreover, shared data is not limited to citizen information; it is shown that 571 governmental web panel users' information is for sale below.



Threat actors can target state institutions, municipalities, and political parties. On March 15th, it was seen that the database of 3.031 personnel of Türkiye's largest megacity was shared in a way that includes email, bcrypt hashed passwords, name, and surname information.



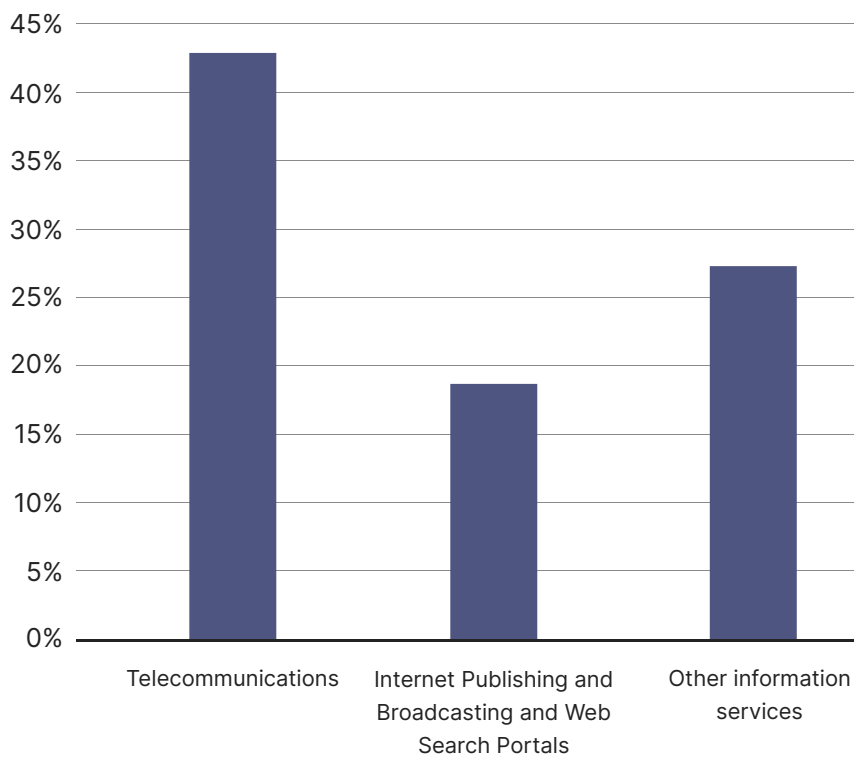
In countries like Türkiye, where political opposition is intense, motivations can go beyond the economy. In Q1 of 2023, SOCRadar dark web analysts detected and reported 5 data leaks belonging to the ruling and some opposition parties. In addition, a hacker forum monitored by SOCRadar was found to have leaked an alleged SQL injection vulnerability on an opposition party's website.



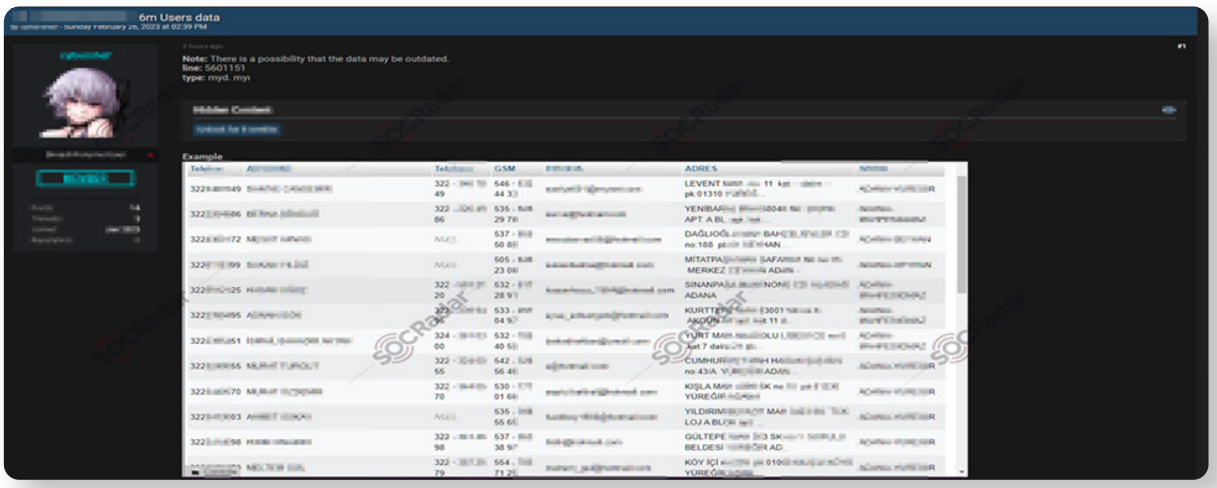
b. Information Services & Telecommunication

The information Services sector comprises establishments primarily engaged in producing and distributing information such as telecommunication, data processing, hosting, and related services, as also other information services like Internet Publishing and Broadcasting and Web Search Portals.

The breakdown of sub-sectors in the information service category is given below. Although the telecommunications sector (42%) is targeted at a high rate, Internet Publishing and Broadcasting and Web Search Portals (31%), which represent Internet media, especially online news channels, are under serious threat.



On March 26th, A hacker forum monitored by SOCRadar leaked telecommunications data allegedly belonging to Türkiye. Among information systems, attacks targeting the telecommunications sector (42%) remain important. Below is a post claiming the data of Türkiye's largest telecommunications company. Although it is determined by SOCRadar dark web analysts that it is outdated, the information such as phone-mail-address, etc. are not always updated in actual practice, so it emphasizes that personal and sensitive data could be in the hands of malicious actors.



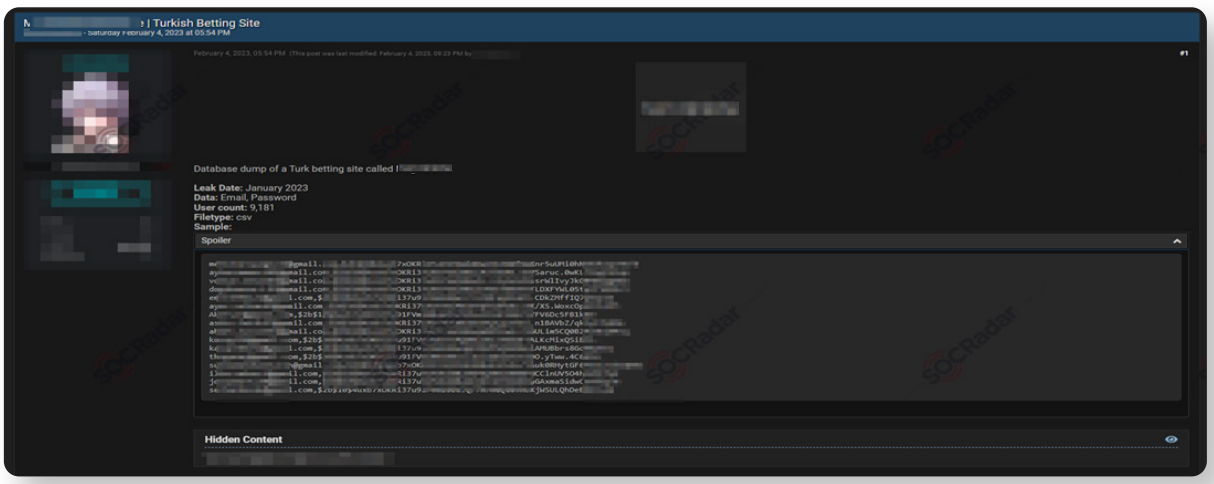
Services can be offered to different sectors, such as media, by providing an intermediate layer in the field of IVR and mobile by using the infrastructure of GSM companies operating in the field of information systems.

On January 4th, in a hacker forum monitored by SOCRadar, a new alleged data sale was detected for a company that is a leading mobile messaging provider, offering advanced mobile messaging, location-based solutions, and other services to mobile network providers, mobile virtual network providers, enterprise customers, government entities. Leaked data included in package 17.3-million-line phone: first name: last name combo list.

c. Arts & Entertainment Sector

As the Arts & Entertainment sector continues to grow around the world, gambling plays an important role in this growth. According to the Gambling Commission report, 44% of adults have participated in gambling in the last four (4) weeks. Furthermore, according to Statista analysis, it is observed that the demand for gambling/betting websites, both online and mobile, in Türkiye is intensifying and is included in future predictions.

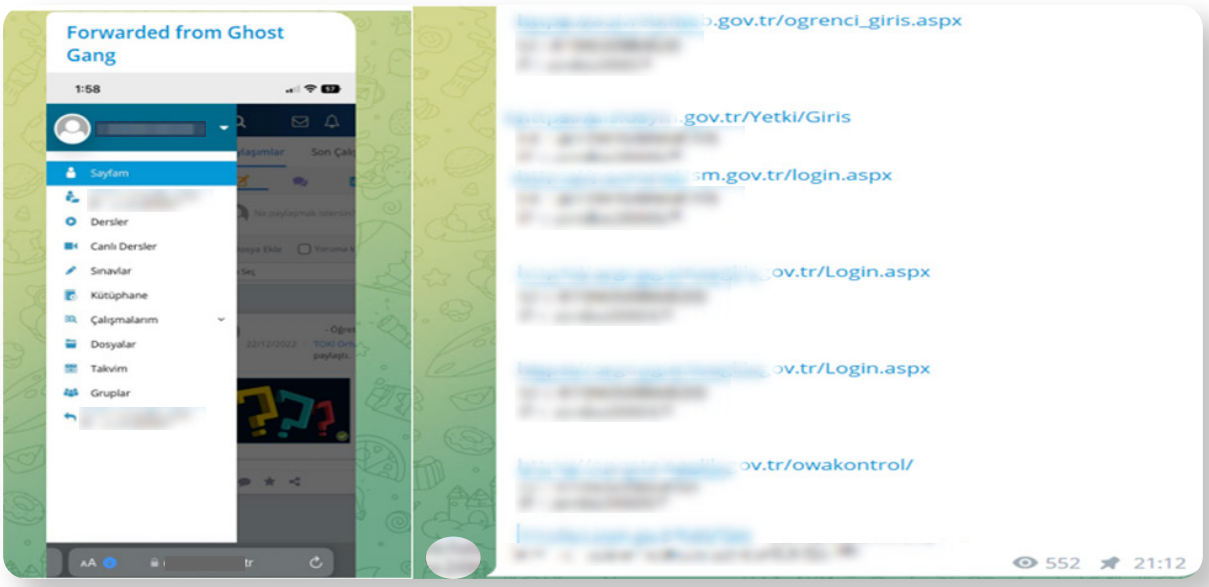
On February 4th, In a hacker forum monitored by SOCRadar, a new alleged database leak was detected for a notorious betting site. The data of 9.081 people were shared in CSV format and included email and hashed password information.



d. Education Sector

Educational services cover all formal and non-formal education institutions, starting from primary school up to and including universities. According to SOCRadar Education Threat Landscape Report, the number of education industry-related postings shared on underground forums increased by 61% in 2022 compared to 2021. While the education sector globally is becoming more targeted by cyber threat actors year by year, correspondingly, the cyber incidents related to the Turkish education sector continue to maintain their importance, considering both 2022 Q4 and 2023 Q1 findings.

On January 7th, the images below, taken from the Telegram channels of threat actors, show the leaked user login information of the university selection center, the education login network of national education institutions, vocational and open educational high school entities.



On February 4th, on a hacker forum monitored by SOCRadar, unauthorized network access allegedly belonging to a Turkish university was put up for sale.

e. Finance Sector & E-commerce

The Finance sector has always been of intense interest to cyber attackers due to its economic motivations. Türkiye's transaction potential in e-commerce has reached $14 billion, and it is estimated and projected to exceed $25 billion by 2025. According to SOCRadar Financial Industry Threat Landscape Report 2022 has shown that 17.4 million credit card information was sold on the black market in the first eight months of 2022.

Although increasing cybercrime incidents on e-commerce platforms due to storing customers' bank accounts and credit card details, and mailing addresses are expected to decrease market growth, some payment gateway services can keep their customers' bank card confidential information out of threats via data encryption and the offer automatically accepts, declines, or verifies card processing via secured internet links to authorize payment for traditional businesses, retailers and other online businesses.

On February 22nd, In a hacker forum monitored by SOCRadar, an unauthorized database access sale was detected, allegedly belonging to a Turkish payment gateway. Selling access to another Türkiye Payment gateway with around 700.000 credit cards in the DB currently + full info included. Also, there is the list of shops connected with POS details (private keys and so on), around 50/100+ new CC a day. The data auction starts out with bids of 2.000$.

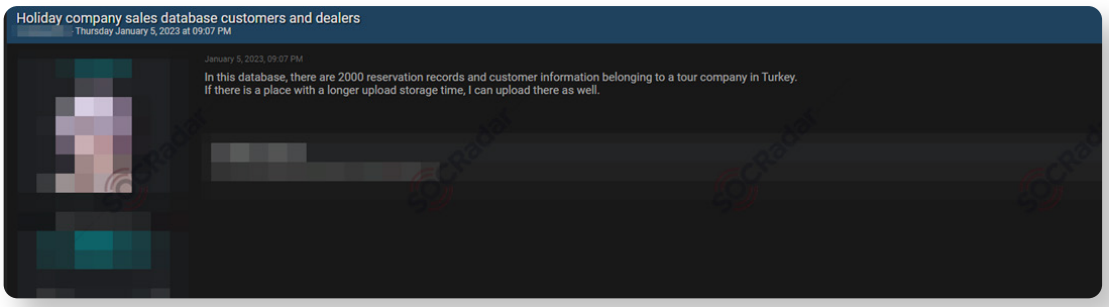
f. The Health Care and Social Assistance Sector

According to 2022 Healthcare Data Breach Report posted by HIPAA Journal, In addition to cyber-attacks targeting the healthcare sector being on the rise globally, these attacks, such as data breaches and ransomware, could cause huge financial losses for healthcare organizations. The 2022 IBM cost of a data breach report has shown that the average cost of a healthcare data breach reached an all-time high of $10.1 million in 2023. SOCRadar Research analysts found out that the cyber incidents related to the Turkish healthcare sector continue to maintain their importance, considering both 2022 Q4 and 2023 Q1 findings. As a result, sensitive data exposure could cause harm to Turkish citizens as well.

On March 1st, in a hacker forum monitored by SOCRadar, a new alleged patient data sale was detected in many countries such as the UK- US - Spain - Bulgaria - Kuwait - Dubai - Türkiye – Germany.

The alleged data of people who had aesthetic surgery was shared in Excel format and in a way to include name - family - surgery - country - mobile - email information.

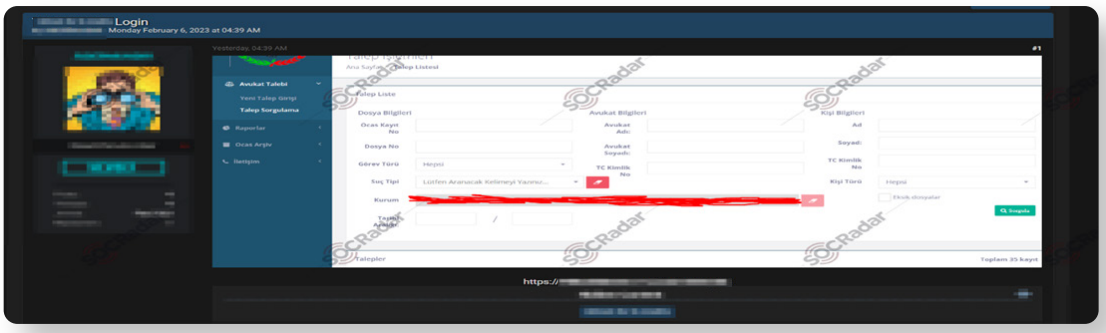
According to ISAPS data, Türkiye is among the leading countries in terms of foreign-patient ratios in aesthetic surgery operations, which are observed to increase significantly as to global statistics and forecasts.



g. The Other Prominent Cyber Incidents

Although the Legal Services, Manufacturing, and Construction sectors are not among the top targeted ones according to observed data, they could be subject to critical cyber incidents. Especially in legal services, the protection of personal and private information of citizens is essential in terms of their fundamental constitutional rights.

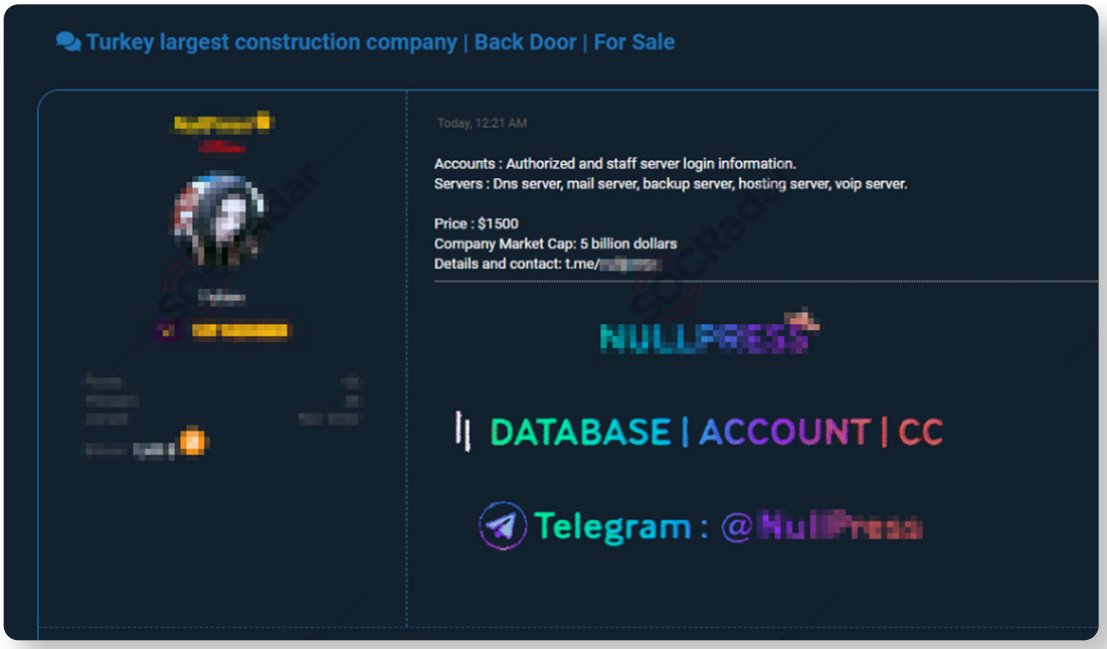
On February 6th, In a hacker forum monitored by SOCRadar, a user login information leak was detected allegedly belonging to an automation system developed to fulfill the authority and obligation of law society associations to appoint defense counsel and attorneys have been compromised.



In a notorious ransomware group website monitored by SOCRadar, new data leaks detected allegedly belong to a major pulses producer operating in the Manufacturing sector with annual revenues of $5m.

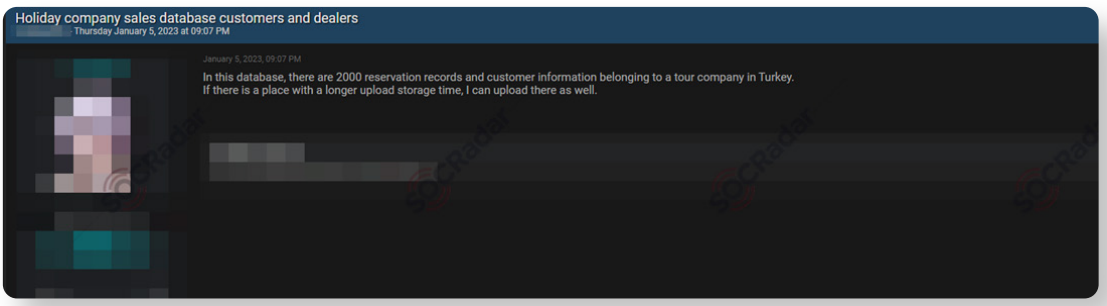
As it is known, the Construction sector has been a pioneer sector in terms of economic investments in Türkiye for 20 years.

On January 10th, in a hacker forum monitored by SOCRadar, an unauthorized access sale was detected, allegedly belonging to Türkiye's largest construction company whose market gap is 5b$. Leaked databases comprise not only authorized and staff server login information of accounts but also DNS server, mail server, backup server, hosting server, and VoIP server information.



The Accommodation Services sector is used by millions of Türkiye citizens and tourists where summer and winter tourism are common. Inadequate data security measures may cause unauthorized leakage of personal and sensitive data.

On January 5th, in a hacker forum monitored by SOCRadar, a new alleged database leak was detected for a holiday company. In this database, there are 2.000 reservation records and customer information belonging to a tour company in Türkiye.



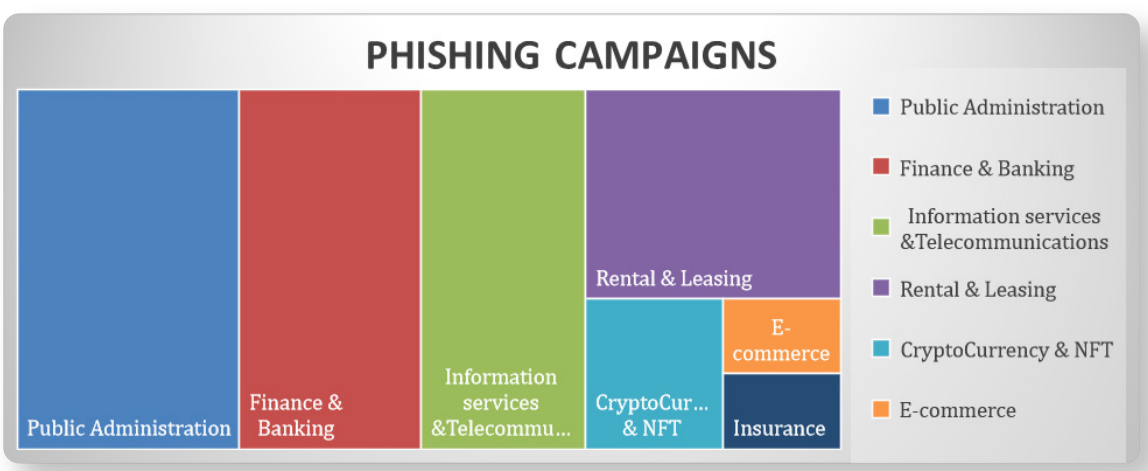
3. 2023 Türkiye–Syria Earthquake and Phishing Campaigns Targeting Türkiye

On Monday, February 6, 2023, Türkiye woke up to the morning of a major natural disaster. With two devastating earthquakes of 7.7 and 7.6 magnitudes in Eastern Anatolia, Southeastern Anatolia, and Mediterranean regions, people in 10 different cities were deeply affected. While emergency teams continue to fight against time in the disaster zone with all their means, aid, and support continue to be collected both nationally and internationally through many platforms and organizations, especially the internet and social media.

Unfortunately, even in the face of this disaster, according to SOCRadar observations, threat actors who want to exploit the goodwill of people have been coveting aid for the disaster area.

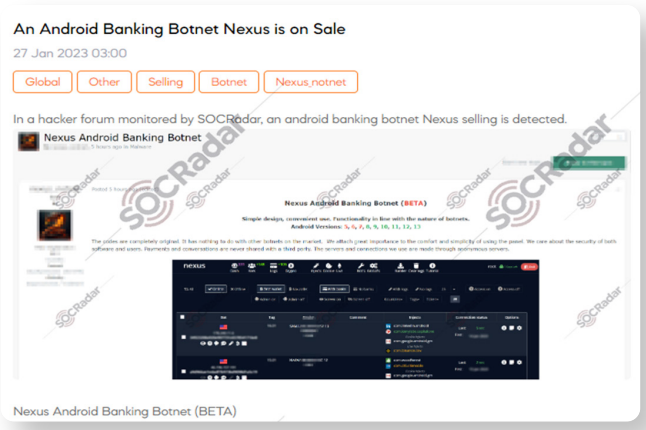
SOCRadar has been monitoring threat actors who carry out fraud and phishing attacks, imitating official and voluntary aid organizations such as AFAD and Ahbap; that may lead to disinformation since the disaster that deeply wounded Türkiye and taking necessary actions to prevent abuse. You can access SOCRadar's GitHub page created to track the detected fraud domains and IP addresses from this link.

To date, SOCRadar analysts have identified 187 malicious domains related to earthquake relief alone. In 2023 Q1, SOCRadar Phishing Radar detected 22,673 malicious websites related to Turkish entities. The following graph shows the distribution of the top sectors targeted by phishing attacks.

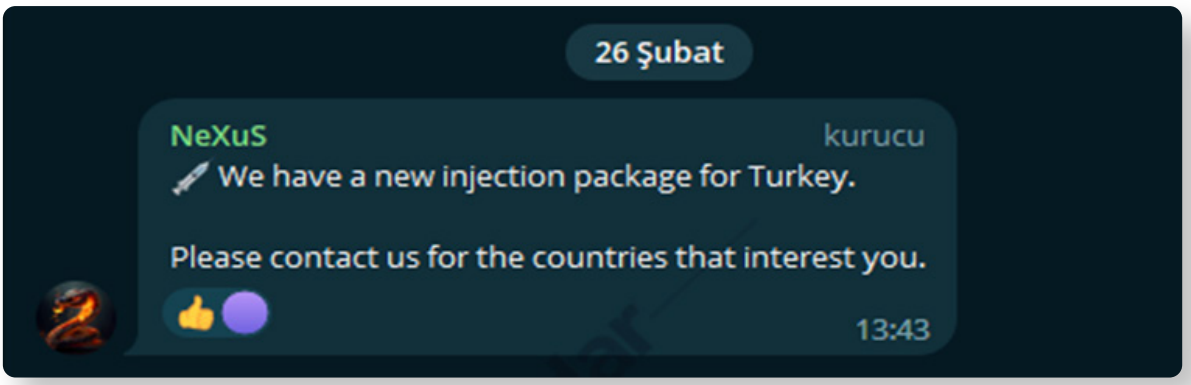


4.Most Common Malware Attacks Targeting Türkiye

A malware is produced by threat actors and can be easily distributed through botnets. In underground forums, exploit codes such as zero-day exploits can be sold and shared at times. In addition, a malware that can be distributed by millions of computers over the internet network can pose a huge threat because threat actors can get and use them easily for malicious activities to target organizations.



One example, Nexus Banking trojan continues to pose a threat to more than 450 bank and crypto exchange applications worldwide. Nexus stands out among other malware because it has many features that allow attackers to hijack accounts and potential funds.



On February 26, the developers of Nexus announced a new Türkiye-specific injection package. Following this announcement, the malware was found to have spread rapidly in Türkiye.

Security researcher Rohit Bansal and the malware's developers, operating through a Telegram channel, confirmed that the majority of infections were found in Türkiye. A total of 583 devices were affected, 547 of which were located in Türkiye.

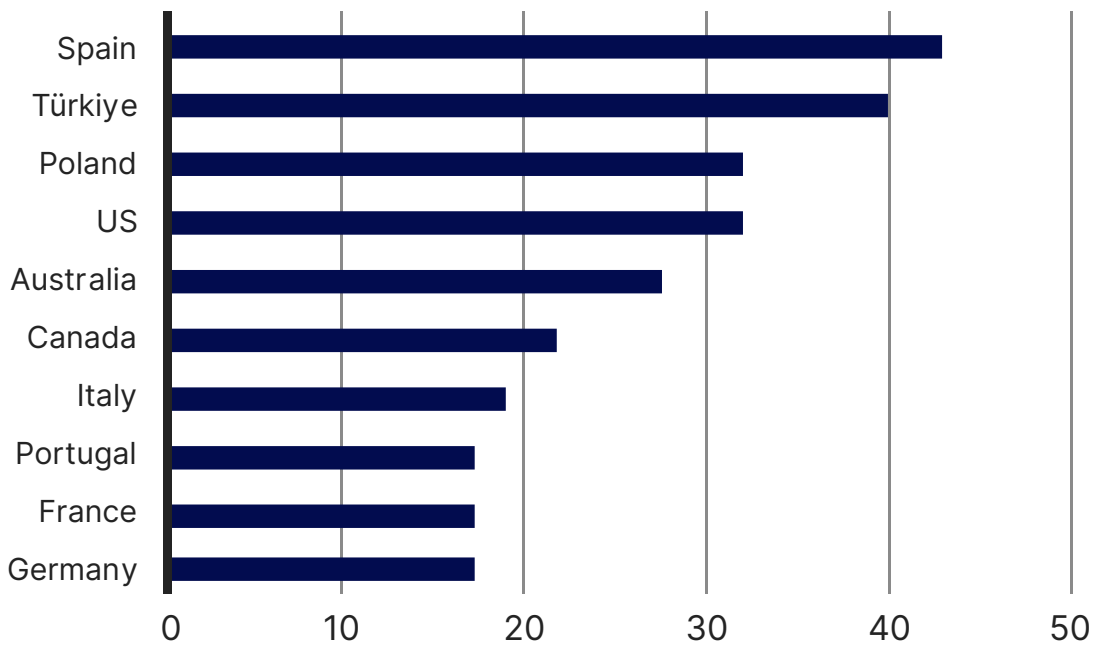
Moreover, the other malware botnets targeting Türkiye are listed below.

The Prometei is a highly modular botnet with worm-like capabilities that has continuously improved and updated since it was first seen in 2016, posing a persistent threat to organizations. It is known that Prometei is one of the malware types that has been taking advantage of the ProxyLogon vulnerability. ProxyLogon is a Microsoft Exchange Server vulnerability covered by CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065 which was firstly discovered as zero-day in December 2020 and has allowed several threat actors to carry out attacks such as bypass authentication and impersonate administrators against unpatched systems.

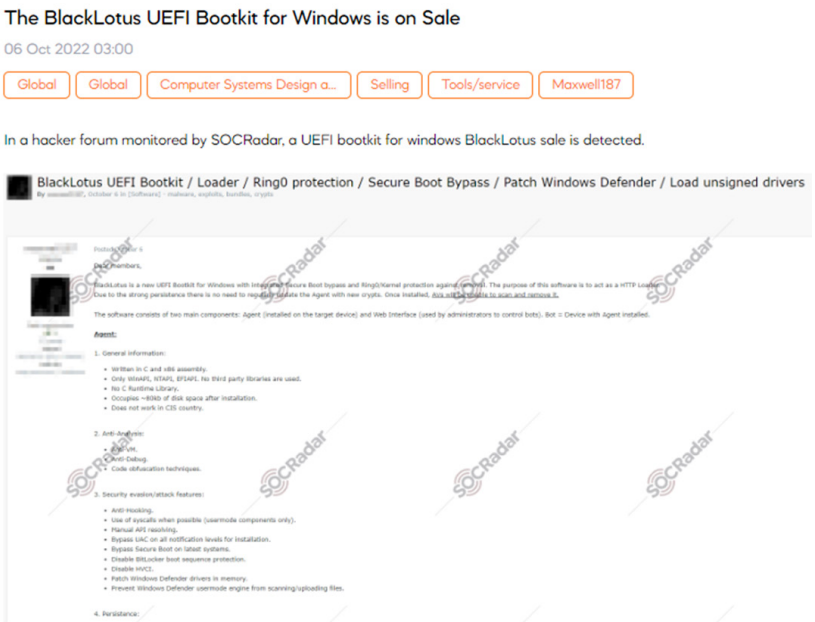
Türkiye, Brazil, and Indonesia are among the countries most infected by the Prometei botnet. The Prometei botnet has also notable for its tendency to avoid targeting Russia and other CIS countries.

The Xenomorph Android malware was first detected by researchers in February 2022. Since then, it has evolved into a more dangerous and sophisticated malware that poses a significant threat to Android users worldwide. The latest version, Xenomorph v3, is one of the most advanced and dangerous Android malwares.

The latest version of Xenomorph targets 400 financial institutions in Spain, Türkiye, Poland, the United States, Australia, Canada, Italy, Portugal, France, Germany, the United Arab Emirates, and India.



Emotet is blamed for some of the most devastating cyberattacks leading to data theft and full-blown ransomware attacks on breached networks. Emotet is one of the most widespread and dangerous malwares and is often distributed via emails containing malicious MS Word and Excel document attachments. Once the macros are enabled, Emotet's DLL file is downloaded and loaded into memory, waiting for instructions from a remote command and control server.


The BlackLotus UEFI Bootkit for Windows is on Sale

06 Oct 2022 03:00

Global | Global | Computer Systems Design a... | Selling | Tools/service | Maxwell187

In a hacker forum monitored by SOCRadar, a UEFI bootkit for windows BlackLotus sale is detected.

BlackLotus UEFI Bootkit / Loader / Ring0 protection / Secure Boot Bypass / Patch Windows Defender / Load unsigned drivers

A malware called BlackLotus is the first known malware that can bypass the UEFI Secure Boot feature and run even on updated Windows 11 systems.

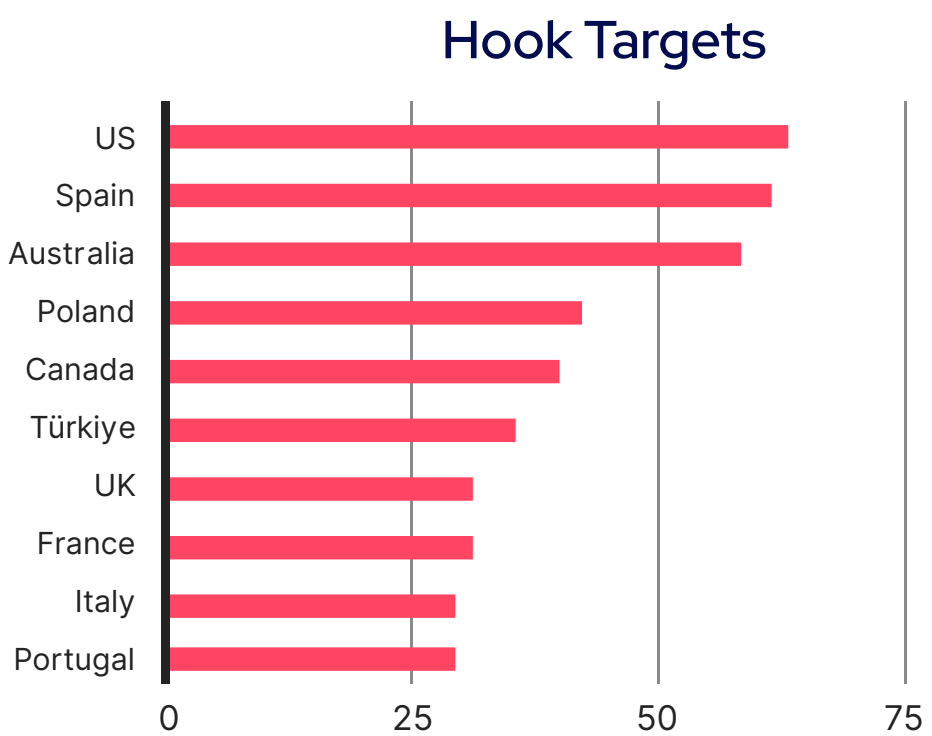
BlackLotus was first spotted on October 6, 2022 on a hacker forum monitored by the SOCRadar dark web team and was seen being sold by the threat actor for $5,000.

The S1deload Stealer malware is used to steal users' credentials, increase engagement with videos and other content, mine cryptocurrency, and spread malicious links to users' followers. Attackers take control of users' Facebook and YouTube accounts and increase views and like for videos and posts shared on the platforms.

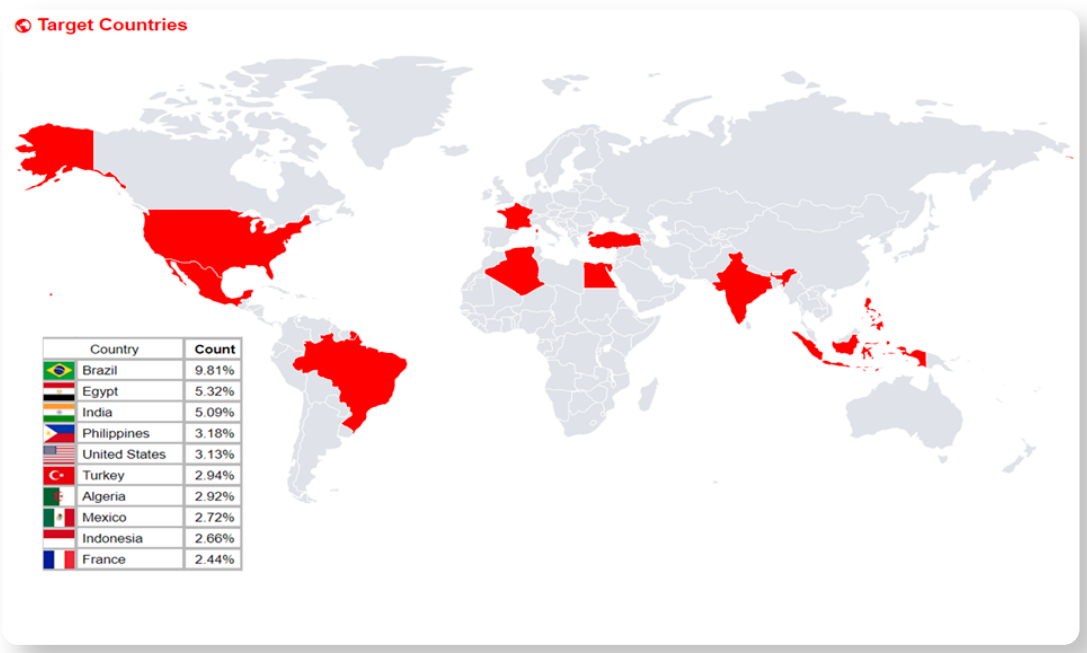
Researchers estimate that more than 600 individual users were affected by the campaign between July and December 2022, with infections mostly found in Türkiye, Romania, France, Bangladesh, Mexico, Peru, and Canada.

On 24 January, A new "Hook" Android malware with RAT features was recently announced by the developer of the Ermac and BlackRock malware.

Hook typically targets financial and banking applications. Many of the financial applications targeted by the malware are located in the US, Spain, Australia, Poland, Canada, Türkiye, the UK, France, Italy, and Portugal.



Furthermore, according to the recent research performed by SOCRadar Threat Research Team, which examined over 100 thousand stealer log records; approximately 200 countries are affected by info-stealers, and Türkiye ranked 6th among these countries. The main info-stealer malwares targeting Türkiye are RedLine, Stealc, Meta, Aurora respectively. The image below shows the distribution of countries.



5. Top Ransomware Groups Targeting Turkish Entities

In the first quarter of 2023, SOCRadar dark web analysts identified that five(5) ransomware groups actively targeted different sectors in Türkiye and achieved success.

1- CL0p Ransomware

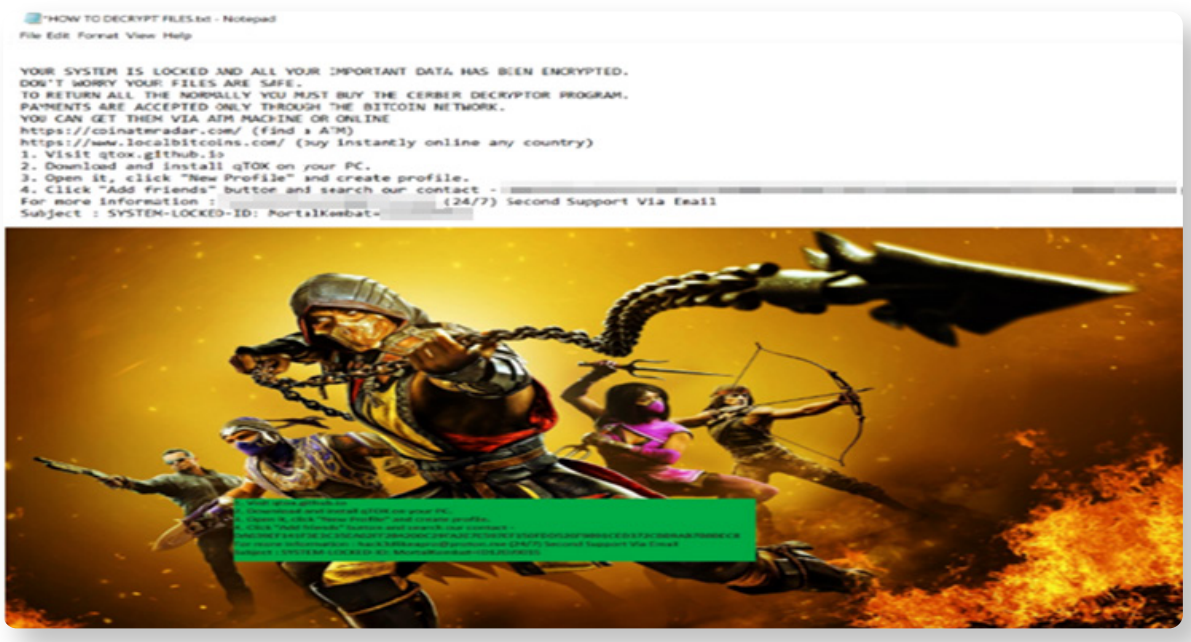
2- Dark Power Ransomware

3- Lockbit 3.0 Ransomware

4- AlpHV / Blackcat Ransomware

5- Mallox Ransomware

Moreover, a new ransomware group that is named MortalKombat which emerged in January 2023, has been identified as targeting businesses in Türkiye is being closely monitored by the SOCRadar dark web team.



In Q1 of 2023, the main sectors targeted by ransomware groups are listed below.

1- Manufacturing

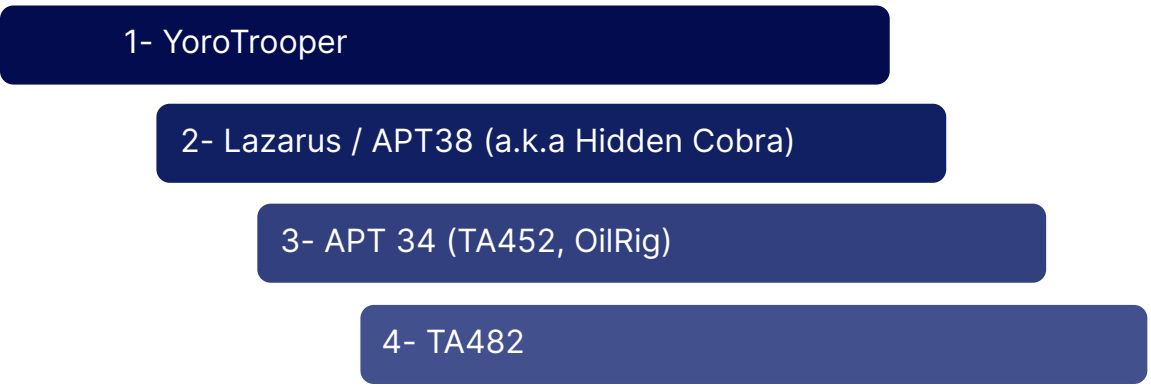
2- Information Technologies

3- Energy & Utilities

4- Transportation & Warehousing

6. Top Cyber Threat Actors Targeting Türkiye

The cyber gangs targeting Türkiye are not limited to ransomware groups. Many threat actors, especially APT groups known for targeted and sophisticated attacks, continue to threaten organizations in Türkiye. According to intelligence data obtained by SOCRadar dark web analysts, the threat actors that actively targeted Türkiye in the first quarter of 2023 are listed below.



A new threat actor named YoroTrooper, believed to consist of Russian-speaking individuals that has been running several successful espionage campaigns, targeting other organizations across Europe and Turkish government agencies since June 2022. They can use many open-source info-stealers malware like Stink-Stealer to steal information such as credentials from multiple applications, browser histories & cookies, system information and screenshots, and also deployed malware, such as AveMaria/Warzone RAT, LodaRAT, and also Meterpreter as known legit pentest tool and used as payload by threat actors.

7. Top Exploited Vulnerabilities

Exploitable vulnerabilities of software used in organizations and open to the internet that are actively scanned by the SOCRadar vulnerability intelligence module, and customers are notified instantly, considering their attack surfaces. As in the global market, vulnerabilities that have not been patched even though an update has been released by the vendors in Türkiye pose a great risk. The top vulnerabilities exploited by threat actors of widely used products with a large user base affecting Türkiye are listed below.

1. CVE-2023-23397 (Microsoft Outlook Elevation of Privilege Vulnerability) 9.8 CVSS3, 99/100 SVRS
2. CVE-2022-39952 (FortiNAC - External Control of Filename or Path in keyUpload scriptlet) 9.8 CVSS3, 89/100 SVRS
3. CVE-2021-21974 (Vmware ESXi OpenSLP heap-overflow vulnerability) 8.8 CVSS3, 80/100 SVRS
4. CVE-2023-21716 (Microsoft Word Remote Code Execution Vulnerability) 9.8 CVSS3, 89/100 SVRS
5. CVE-2023-20078, CVSS 9.8 (Cisco IP Phone 6800, 7800, and 8800 Series Command Injection Vulnerability) 9.8 CVSS3, 84/100 SVRS

CONCLUSIONS AND RECOMMENDATIONS

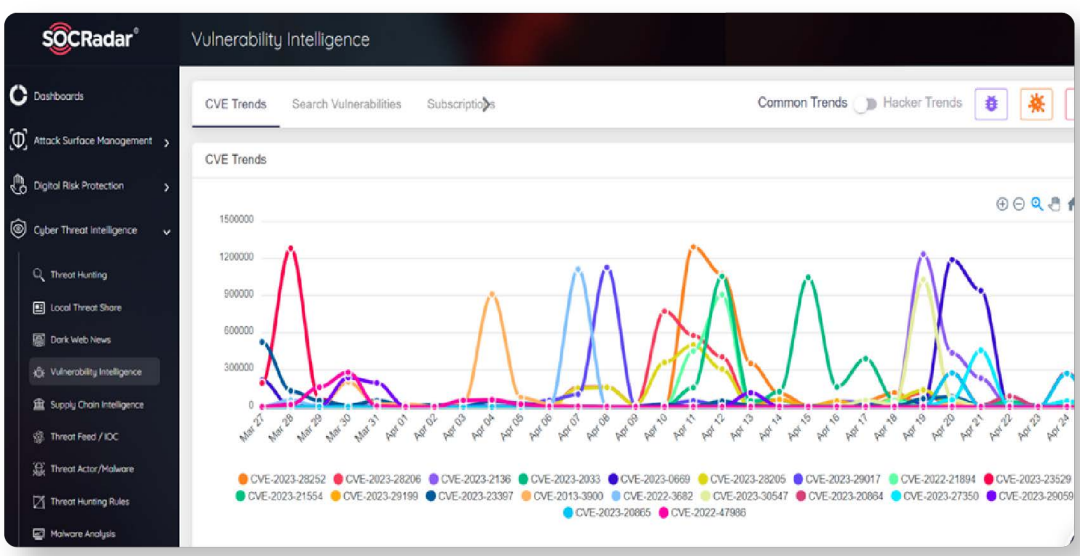
This report has tried to present a big picture by analyzing the whole sector in Türkiye without delving into technical details in terms of cyber threat intelligence. Firstly, we can conclude that a wide range of sectors are targeted by numerous threat actors. In general, considering that the main motivation in cyber-attacks such as ransomware is money, it should not be ignored that while customers/citizens benefit from each online service provided in the digital environment, cybercriminals can often try to exploit these online services' and web applications' vulnerabilities.

As long as international tensions due to global instability, such as the Russia-Ukraine war, result in division and confrontation among threat actors; Türkiye needs to strengthen its cyber resilience in order not to become an easy target. The most basic forecast for the Q2 of 2023 is that manipulations and misinformation may be conducted by threat actors to take advantage of May 14 elections by using personal information in their hands and especially phishing domains. In addition, it can be predicted that reliable media and news channels may be impersonated, and social media accounts with large followers can be hacked and used for these types of manipulations.

Some key lessons learned in Q1 of 2023, and recommendations are listed below for industry stakeholders.

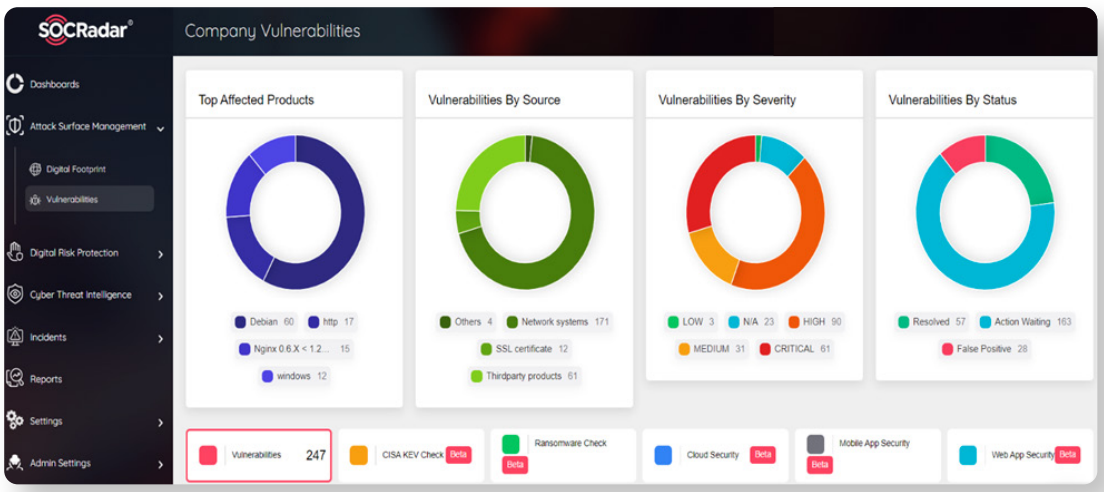
a. Based on the findings that threat actors, especially ransomware groups, are exploiting an increasing number of security vulnerabilities, prioritizing patch management, and deploying patches in a timely manner are vital. Moreover, since known exploited vulnerabilities tend to increase, databases such as CISA's KEV catalog should be constantly monitored to take action as soon as possible.

The Vulnerability Intelligence module gives security teams real-time insights into threat actor behavior, allowing them to understand better why and how some vulnerabilities are targeted while others are ignored.



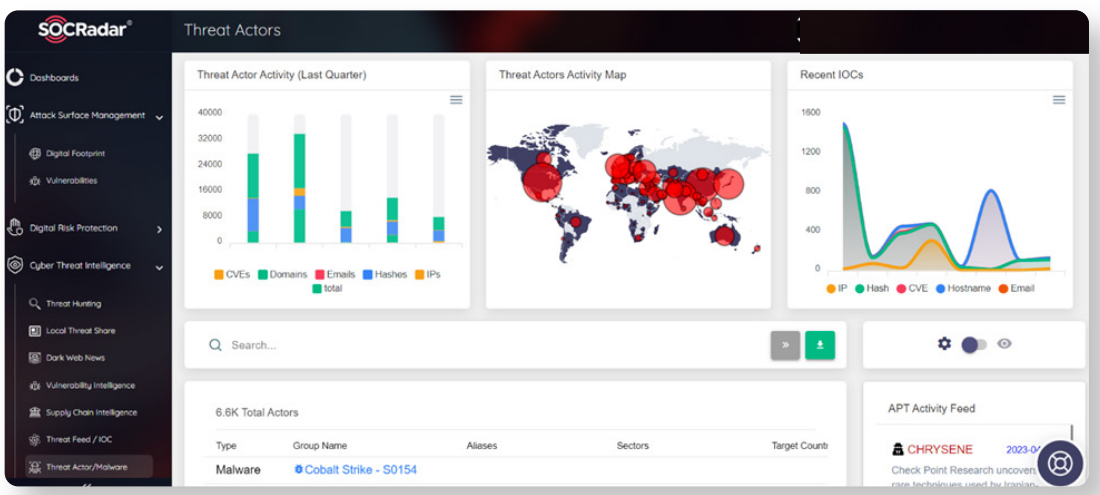
b. Digital attack surfaces should be well-defined and managed via ASM (Attack Surface Management) services that discover your digital assets, assess your cyber security risk, and mitigate them. These services are critical due to providing a unified view of your cyber assets to get full visibility of your expanding attack surface.

The External Attack Surface Management module (EASM) monitors all your systems around the clock for newly discovered security vulnerabilities.



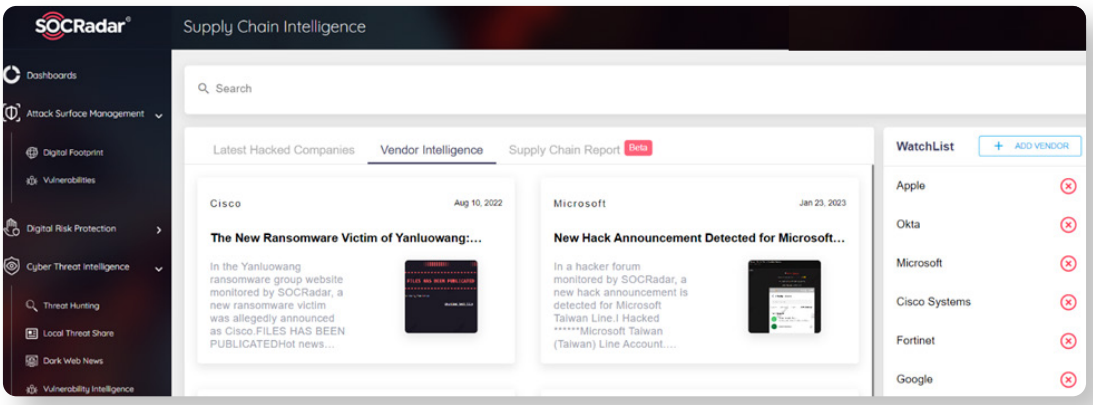
c. Given the inference that threat actors specifically select their victims, and could be sectorally concentrated, it is necessary to obtain contextual information extracted from dark web intelligence about the changing TTP and malware campaigns of cyber attackers for proactive measures.

The Threat Actors/Malware module keeps you alerted on threat actors' activities, helping you define use cases for more effective modeling and also detect and prevent malicious activities



d. Supply chain attacks are emerging threats that target organizations by infecting legitimate apps to distribute malware, usually linked to vendors' vulnerabilities with poor security postures. Therefore, in order not to add the service providers as a weak and insecure link to the digital supply chain, trust, and accredited or certified suppliers should be selected, and security policies should be followed, not ignored.

The Supply Chain Intelligence module provides the capability to improve business security posture by utilizing analytical assessments about prominent vendors and products.



e. As is known, companies often learn about cyber incidents like a data breach long after being hacked. Consequently, organizations should get service from a strengthened SOC infrastructure with CTI feeds, which is the ultimate combination of cyber threat detection and response that provides actionable information for SOC analysts from dark web intelligence.

The Threat Feed & IoC Management module can customize the enriched data feeds and help to stay up-to-date with recent threats via searching for indicators-of-compromise (IoCs)