SOCRadar®
Your Eyes Beyond

MEA
Regional Threat Landscape Report

SOCRadar®
Your Eyes Beyond

Table of Contents

Executive Summary

Top Takeaways

- **Public administration** is the most targeted industry in MEA, accounting for **14,91%** of all posts on Dark Web forums monitored by SOCRadar. The **retail trade** industry takes second place with **8,92%** of the posts, while the **information** sector ranks third with **8,09%** of all Dark Web forum posts.

- **Israel** was the most targeted country in MEA, accounting for **35.43%** of all Dark Web posts. The **United Arab Emirates** was second, with **13.55%** of the posts targeting it. **Pakistan** came in third, with **10.11%** of the posts targeting Spanish organizations.

- Threat actors targeting MEA mostly shared the product of their illicit activities. The **"Sharing"** category is in first place, comprising **44,75%** of all posts from Dark Web forums. The **"Hack Announcement"** category follows with **30,40%** of the posts. In third place is **"Selling,"** which accounts for **24,39%** of the posts.

- Ransomware groups most targeted the **information** industry in MEA, accounting for **14.49%** of all attacks. The **manufacturing** industry took the second spot with **13.04%** of the attacks, while **Professional, Scientific, and Technical Services** ranked third with **8.7%.**

- The **United Arab Emirates** was the most targeted country in MEA by ransomware groups, with **21,57%** of the attacks targeting organizations there. **Israel** was in second place, suffering from **13,73%** ransomware attacks. **Iran** ranked third, targeted by **9,80%** of the ransomware attacks.

- Our analysis shows that LockBit 3.0 was the most active ransomware group targeting MEA, responsible for **31.7%** of all attacks. Hunters International was the second most active group, accounting for **5.2%** of the attacks. In third place, **GhostSec** appeared, responsible for **5%** of all ransomware attacks on regional organizations.

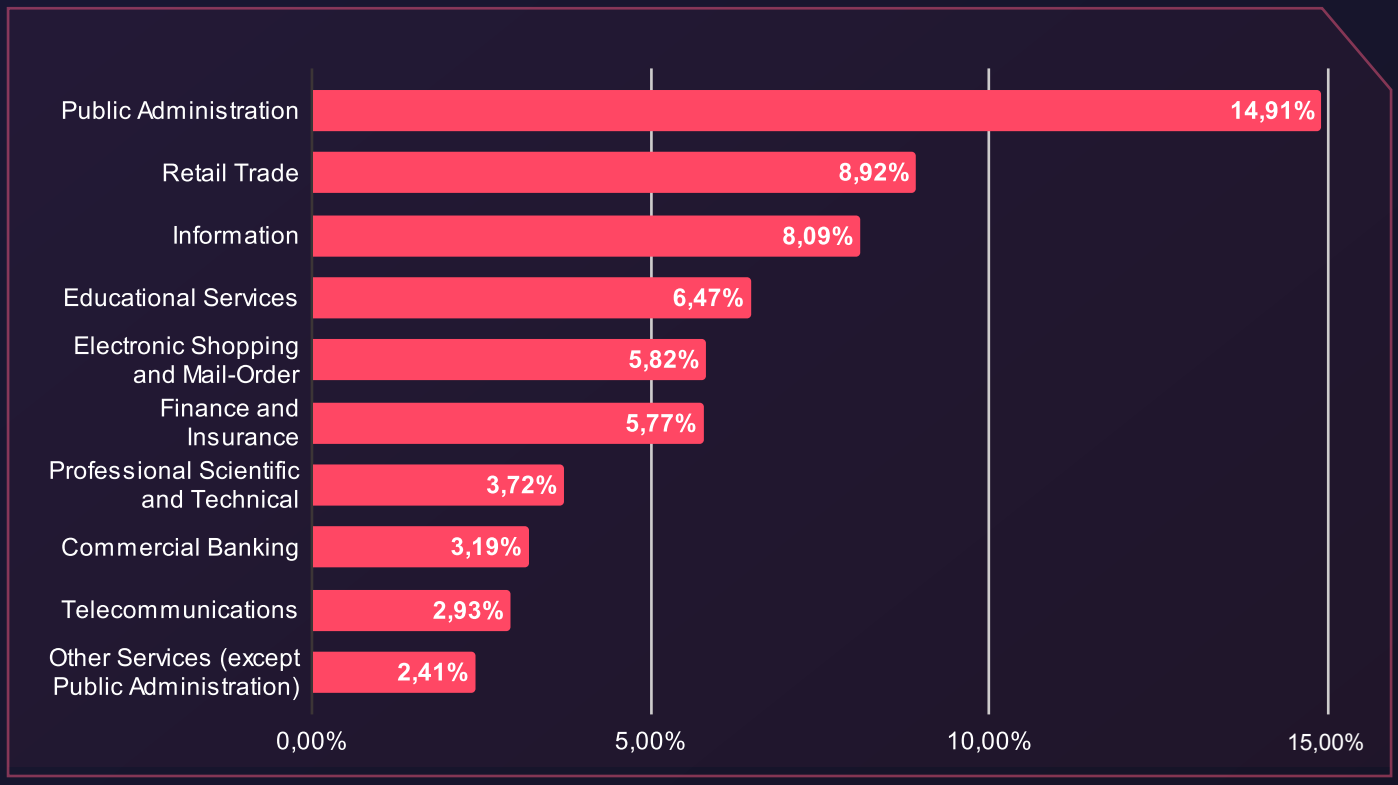
- The **Information Services** industry in the MEA region faced the most phishing attacks, with **17,02%** of the total attempts. **The retail** industry was second with **15,6%** of the attacks, and **Telecommunications** was targeted with **14,89%.**

- **Tunisia** had the highest presence of stealer logs in the MEA region, with **24.71%** of logs linked to individuals from there. **Iran** followed, with **10.29%** of stealer logs associated with users from the country, while **Kuwait** ranked third, with **7.59%** of logs originating from there.

Dark Web Threats Targeting the MEA Region

Industry Distribution of Dark Web Threats

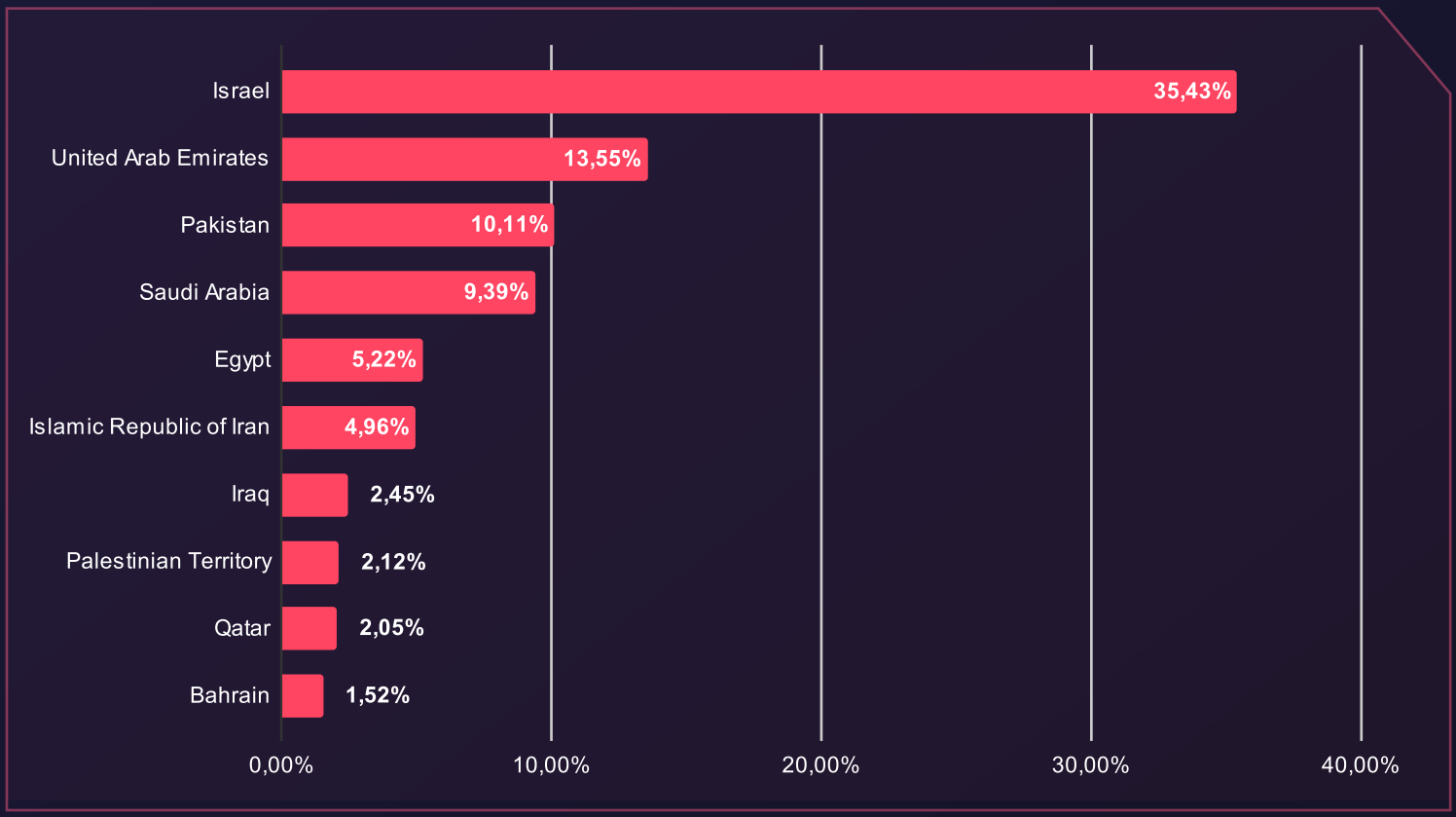
Dark Web Threats - Distribution by Industries



Public administration is the most targeted industry in MEA, accounting for **14,91%** of all posts on Dark Web forums monitored by SOCRadar. The **retail trade** industry takes second place with **8,92%** of the posts, while the **information** sector ranks third with **8,09%** of all Dark Web forum posts.

Distribution of Dark Web Threats by Primary Target Country

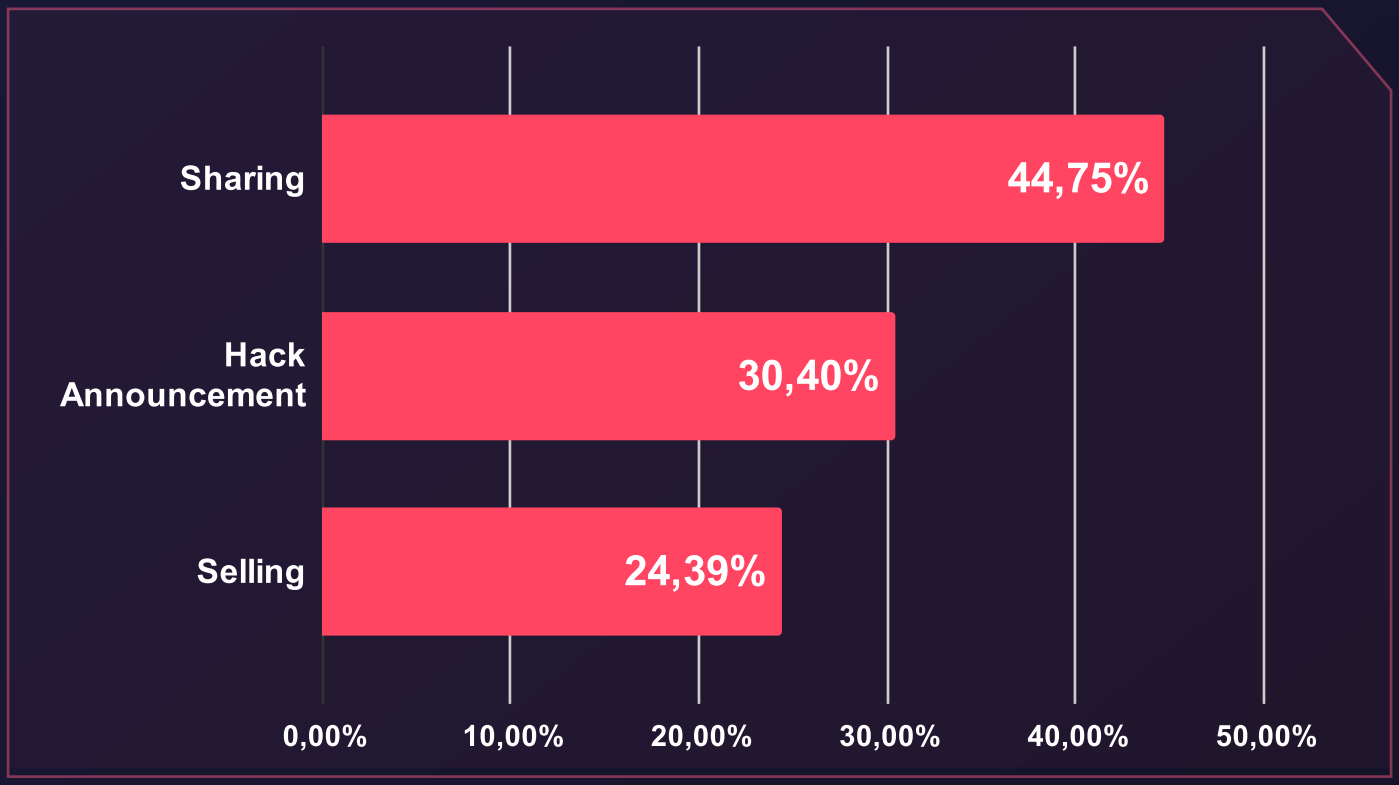
Dark Web Threats - Distribution by Target Country



Israel was the most targeted country in MEA, accounting for **35,43%** of all Dark Web posts. **The United Arab Emirates** was second, with **13,55%** of the posts targeting it. **Pakistan** came in third, with **10,11%** of the posts targeting Spanish organizations.

Distribution of Dark Web Threats by Threat Categories

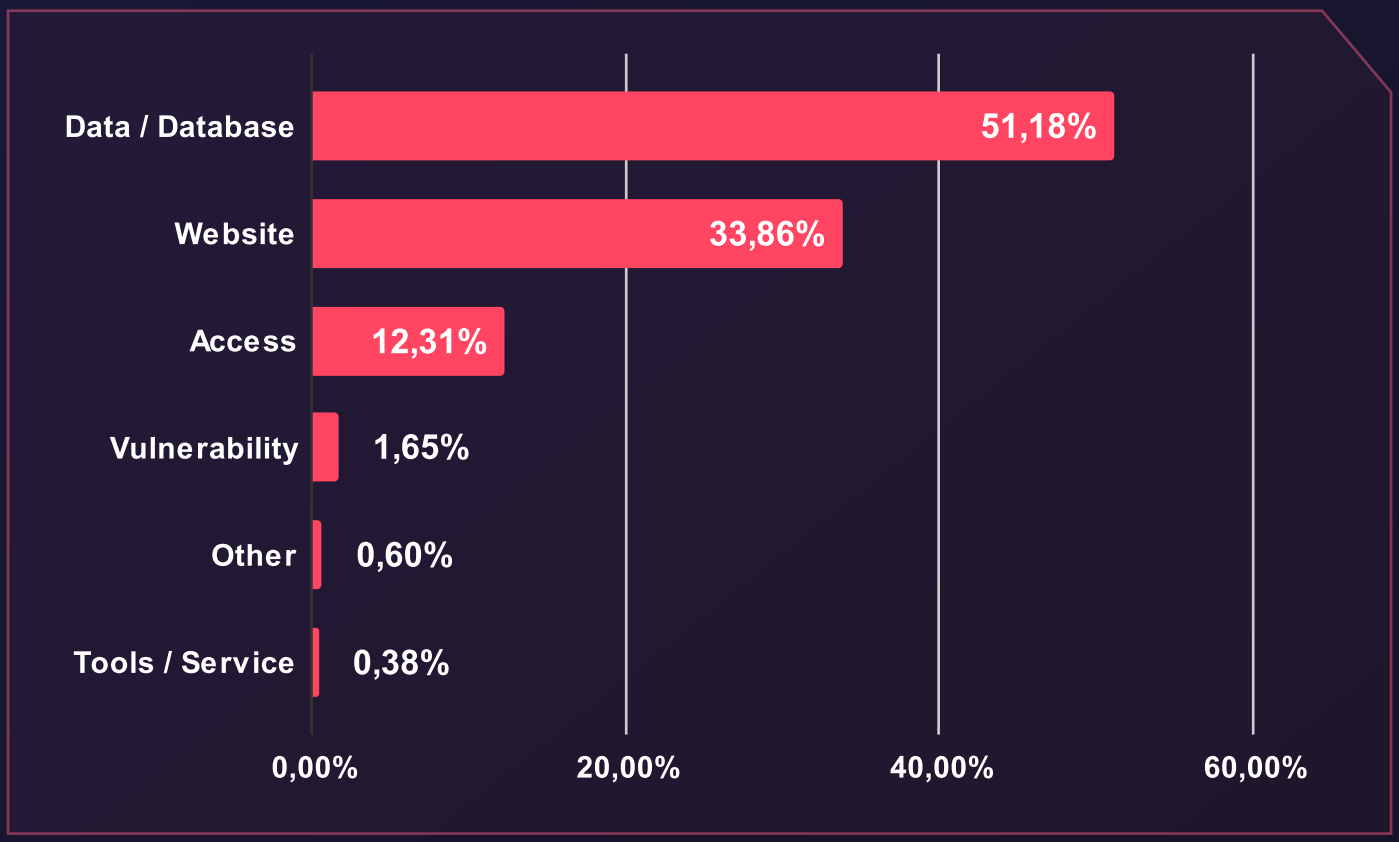
Dark Web Threats - Distribution by Threat Categories



Threat actors targeting MEA mostly shared the product of their illicit activities. The **"Sharing"** category is in first place, comprising **44,75%** of all posts from Dark Web forums. The **"Hack Announcement"** category follows with **30,40%** of the posts. In third place, there is **"Selling,"** which accounts for **24,39%** of the posts.

Distribution of Dark Web Threats by Threat Type

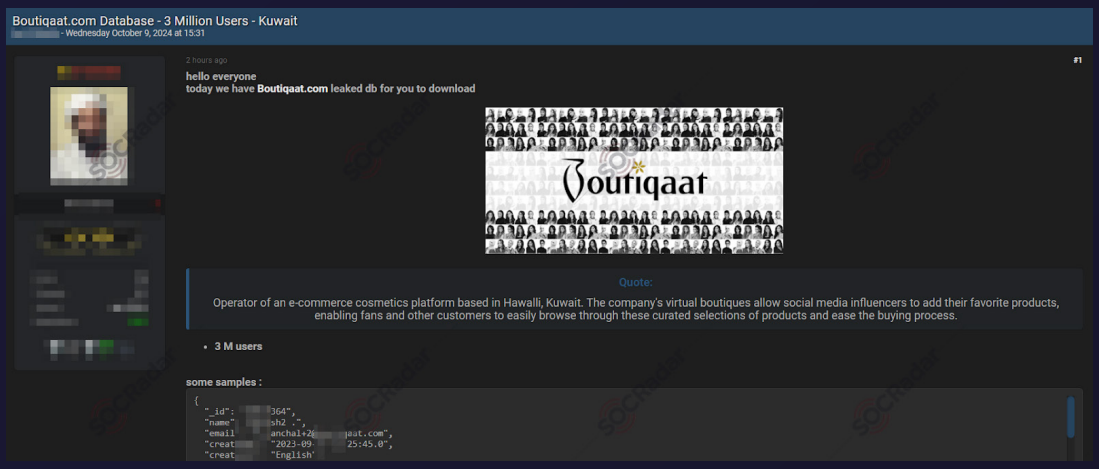
Dark Web Threats - Distribution by Threat Type



When examining the type of information published on Dark Web forums, **databases** take the top spot, accounting for **51,18%** of all posts. The second most popular type of information that threat actors share is related to **website** information (defacements, DDoS attacks, etc.), comprising **33,86%** of the posts. Lastly, posts related to **access** information (sales, shares, etc.) make up **12,31%.**

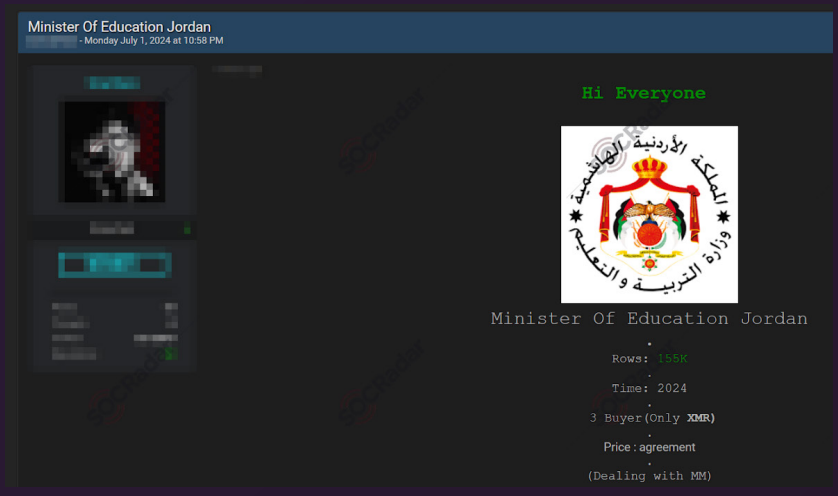
Recent Dark Web Activities Targeting Entities in the MEA Region

The Alleged User Database of Boutiqaat is Leaked



In a post published on a Dark Web forum, a threat actor claimed to possess and leak the user database of Boutiqaat, a prominent e-commerce platform headquartered in Kuwait. The forum post, which SOCRadar detected, alleges that the compromised data includes personal information of approximately 3 million users.

Alleged Database of the Minister of Education of Jordan is on Sale

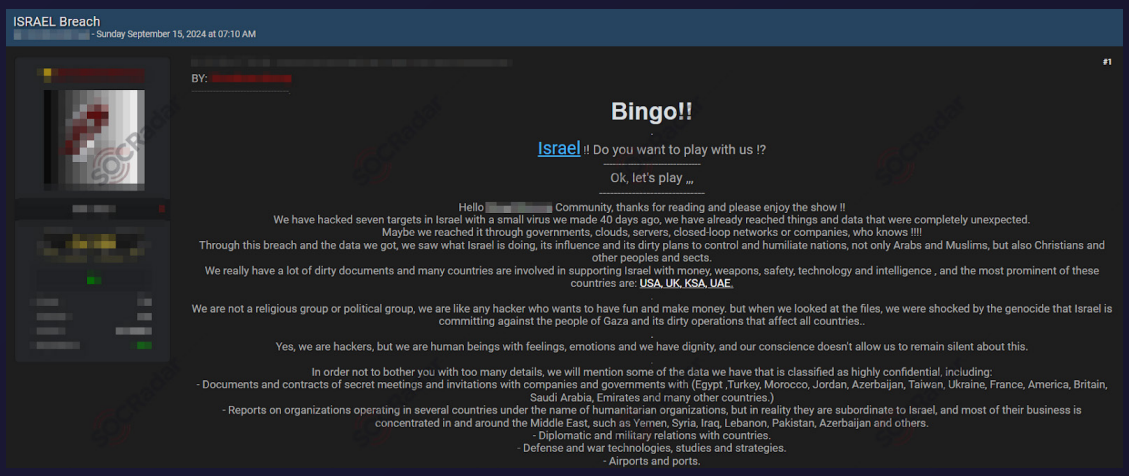


In a recent post on a Dark Web forum, a threat actor claims to have obtained and is selling a database allegedly linked to the Ministry of Education in Jordan. The post, detected by SOCRadar, details that the dataset contains sensitive information about individuals and has 155,000 rows of data from 2024.

The threat actor has put the data up for sale exclusively in Monero (XMR), a privacy-focused cryptocurrency, and has stated that they will only deal with three buyers. The price is not fixed but will be negotiated, with the actor offering to use an intermediary to facilitate the transaction.

The database is claimed to include several CSV files containing a wide range of personal details, such as national IDs, birthdays, gender, names, and even educational institution information. The threat actor shared sample data structures from the files to demonstrate the types of information allegedly contained in the dataset.

The Alleged Hack Announcement is Detected for Israeli Systems

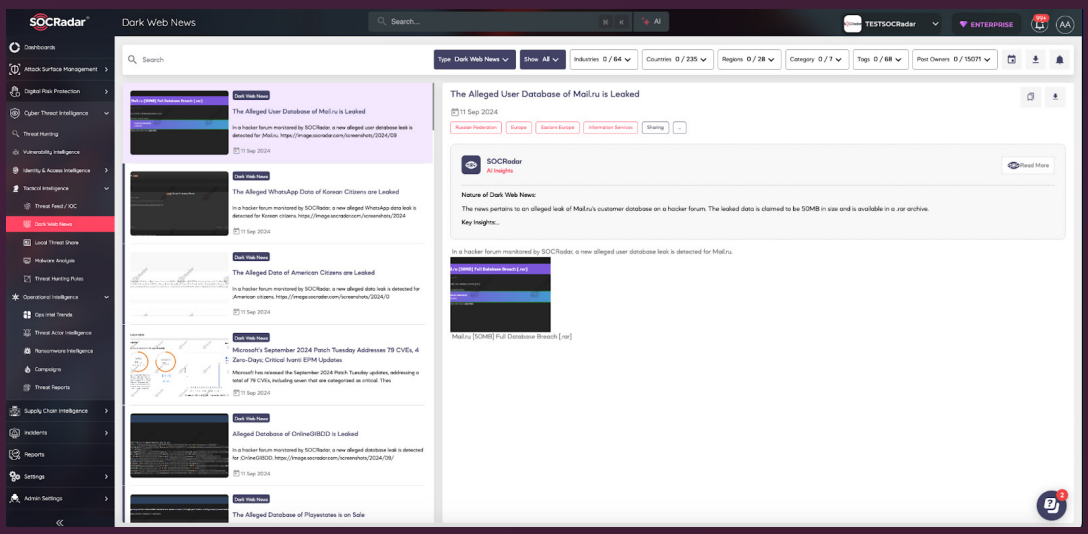


In a recent post on a Dark Web forum monitored by SOCRadar, a threat actor claims to have carried out a significant cyberattack targeting multiple Israeli systems.

The threat actor claims to have access to confidential documents from 1980 to the present. According to their post, the compromised data includes reports on secret meetings, defense systems like Israel's Iron Dome, diplomatic relations, and even highly detailed military intelligence regarding Israel's borders and weapons stockpiles.

The threat actor has offered to sell the data to specific adversaries of Israel, including Hamas, Hezbollah, and Iran, among others, for a substantial sum, demanding payment in Monero (XMR) cryptocurrency.

While these are serious allegations, it is essential to highlight that the threat actor's claims remain unproven.

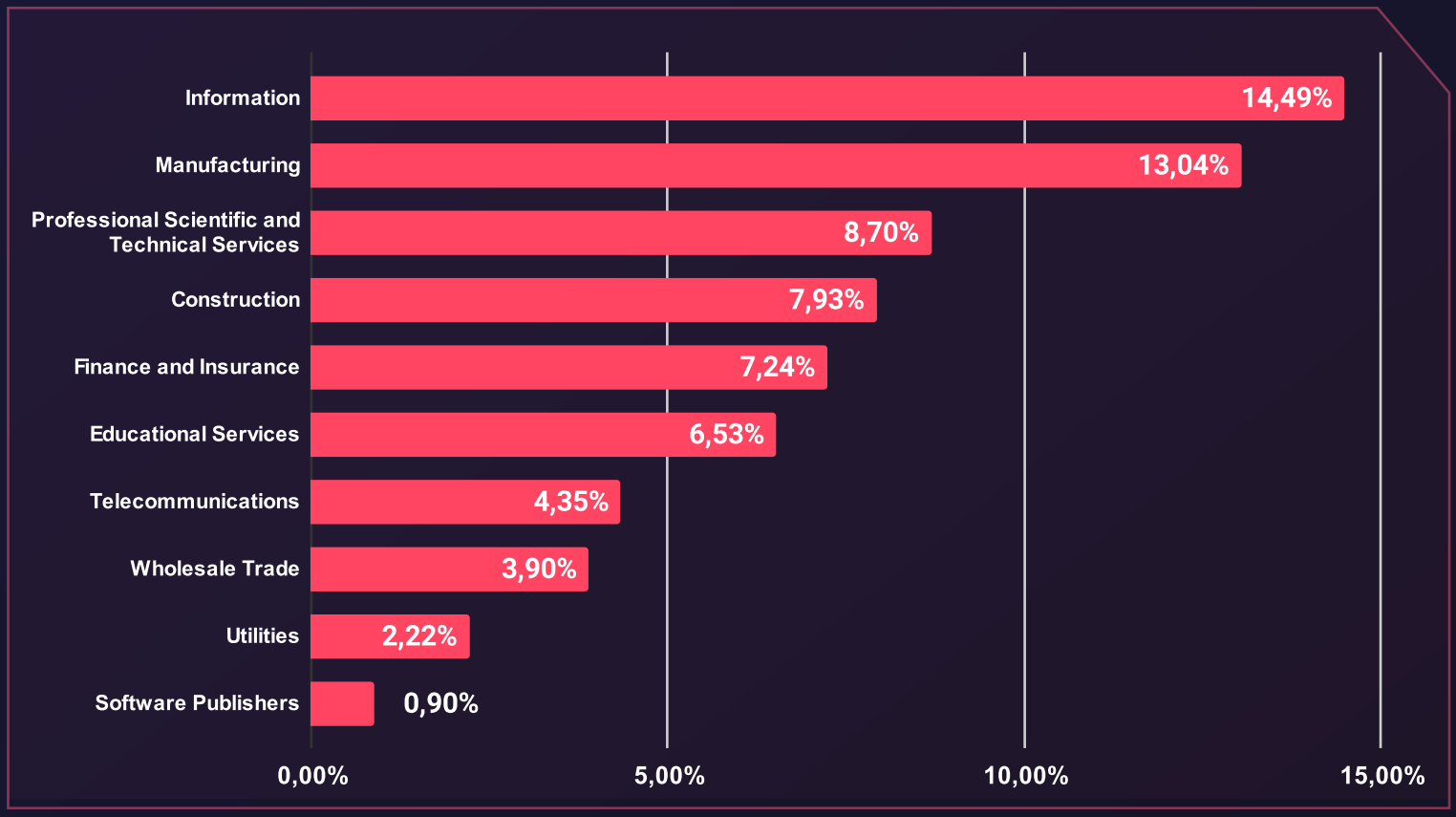


You can learn about the latest Dark Web developments with ***SOCRadar's Dark Web News module.*** SOCRadar's Dark Web News page revolutionizes how you stay informed. It's not just an information aggregator; it's a sophisticated filter, meticulously separating the signal from the noise.

Ransomware Threats Targeting the MEA Region

Distribution of Ransomware Attacks by Industry

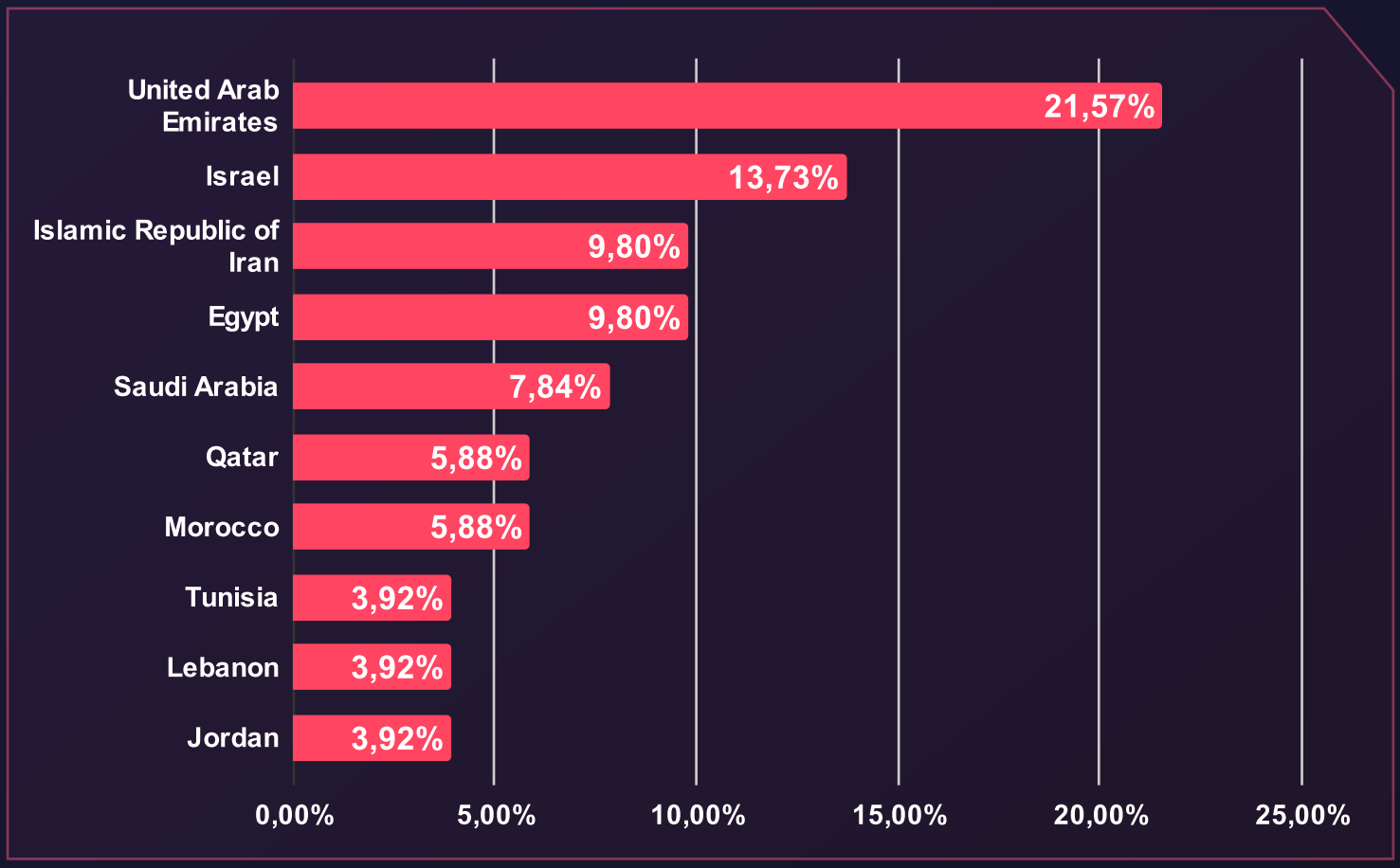
Ransomware Attacks - Distribution by Industry



Ransomware groups most targeted the **information** industry in MEA, accounting for **14,49%** of all attacks. The **manufacturing** industry took the second spot with **13,04%** of the attacks, while **Professional, Scientific, and Technical Services** ranked third with **8.7%.**

Distribution of Ransomware Attacks by Primary Target Country

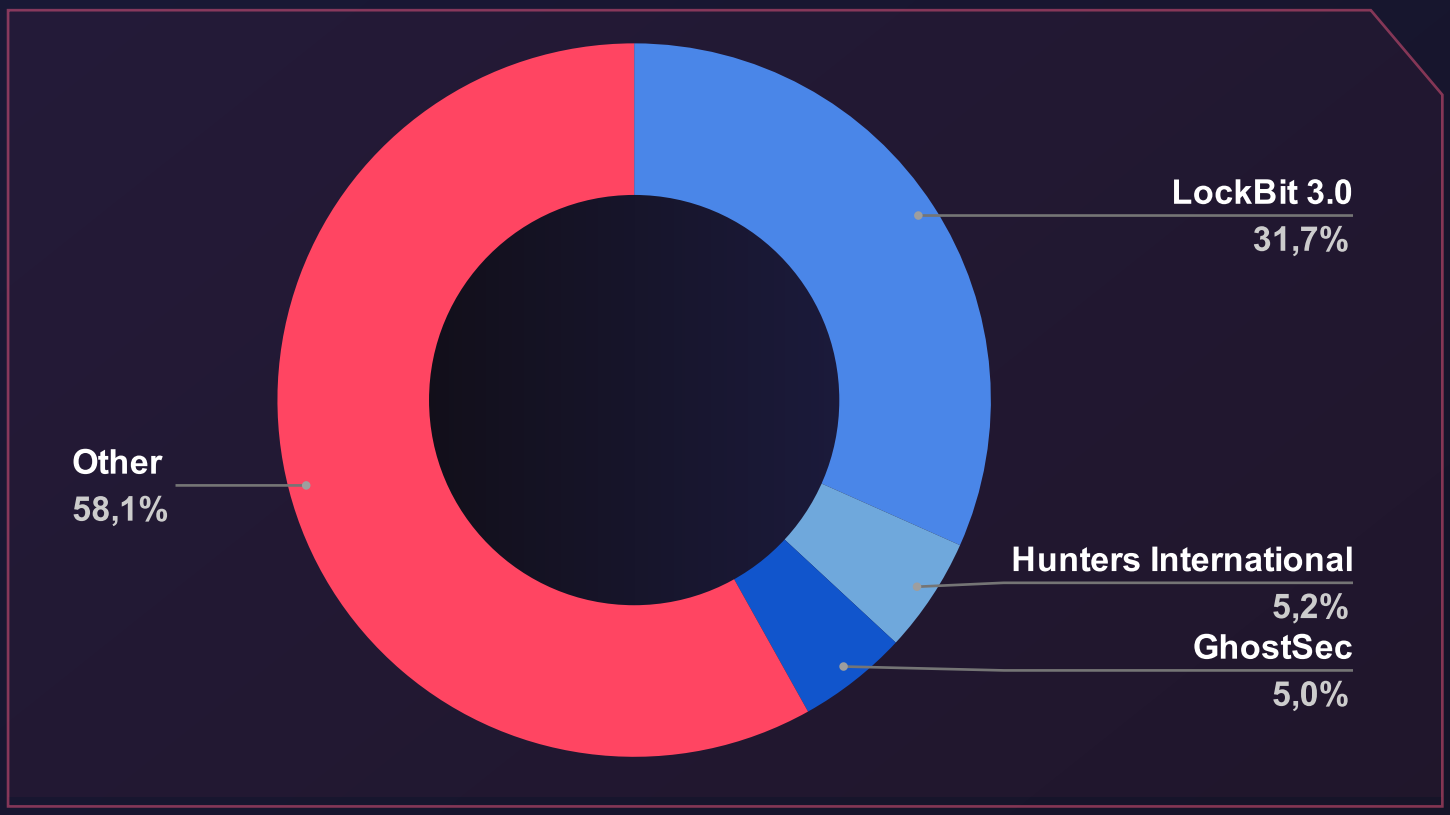
Ransomware Attacks - Distribution by Target Country



The United Arab Emirates was the most targeted country in MEA by ransomware groups, with **21,57%** of the attacks targeting organizations there. **Israel** was in second place, suffering from **13,73%** ransomware attacks. Iran ranked third, targeted by **9,80%** of the ransomware attacks.

Top Ransomware Groups Targeting MEA Region

Top 3 Ransomware Groups



Our analysis shows that LockBit 3.0 was the most active ransomware group targeting MEA, responsible for **31,7%** of all attacks. Hunters International was the second most active group, accounting for **5,2%** of the attacks. In third place, **GhostSec** appeared, responsible for **5%** of all ransomware attacks on regional organizations.

A Closer Look into The Top 3 Ransomware Groups

LockBit 3.0

Threat Actor Card of Lockbit 3.0 Ransomware Group

LockBit 3.0, succeeding LockBit and LockBit 2.0, functions as a Ransomware-as-a-Service (RaaS) entity.

Since January 2020, LockBit has transitioned to an affiliate-based model, employing diverse methodologies to target businesses and critical infrastructure entities. Noteworthy tactics include double extortion and the utilization of initial access broker affiliates, alongside recruitment efforts involving insiders and hacker recruitment competitions.

With over 1,500 victim disclosures on the SOCRadar platform, LockBit emerged as the most active ransomware group in 2022 following Conti's cessation. As of the first quarter of 2023, they retain their position as the most prolific group, with over 300 disclosed victims.

You can visit our **blog post** for more detailed information about the Lockbit 3.0 Ransomware Group.

Hunters International

Hunters International emerged in the cyber landscape around the time law enforcement agencies disrupted the Hive ransomware group. This new group, detected in Q3 of 2023, exhibited significant technical overlap with Hive, suggesting an evolution or offshoot of the dismantled operation.

Hunters International has targeted diverse industries worldwide, demonstrating a global reach with a strategic focus on maximizing impact and ransom potential. Their victims span healthcare, automotive, manufacturing, logistics, financial, educational, and food sectors, indicating a non-discriminatory approach to exploiting any vulnerable entity.

You can visit our **blog post** for more detailed information about Hunters International.

GhostSec

-Hacker Collective-

Motivation:	Financial
Target Countries:	US, Europe, China, Turkiye, Egypt, Brazil
Target Sectors:	Information Technology, Education, Manufacturing
Attack Type:	Double-Extortion, Encryption, Twin Ransomware

-TTPs-

Startup Items:	T1037.005
Masquerading:	T1036
Data Encrypted for Impact:	T1486

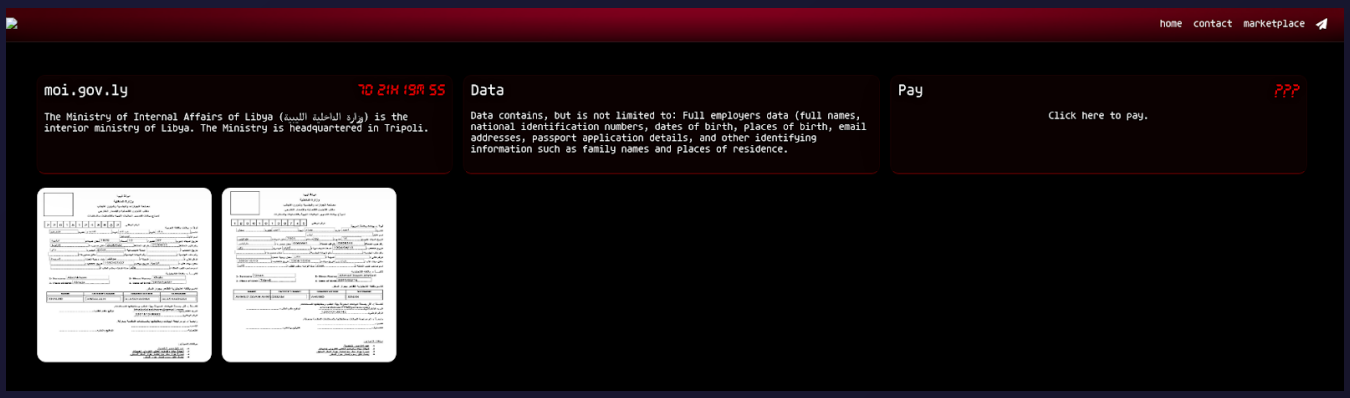
GhostSec, a significant member of The Five Families, has garnered substantial attention with the latest research following their recent twin ransomware attack with Stormous, another Five Families–-affiliated threat group. Researchers and the group itself allege that this group, supposedly initially linked with Anonymous and often identified as vigilante hackers, had taken on the responsibility of combating extremist content and activities on the internet, explicitly targeting ISIS when they first emerged.

As in their sayings, GhostSec's initial mission revolved around the somewhat vague aim of disrupting the online presence and communication of terrorist organizations like ISIS (Islamic State of Iraq and Syria) and Al-Qaeda. However, while the group initially appeared neutral in the **Israel-Hamas conflict,** they later declared their support for Palestine against what they perceived as Israel's war crimes.

You can visit our **blog post** for more detailed information about GhostSec.

Recent Ransomware Attacks Targeting Entities in MEA Region

The Ransomware Victim of KillSec: moi.gov.ly

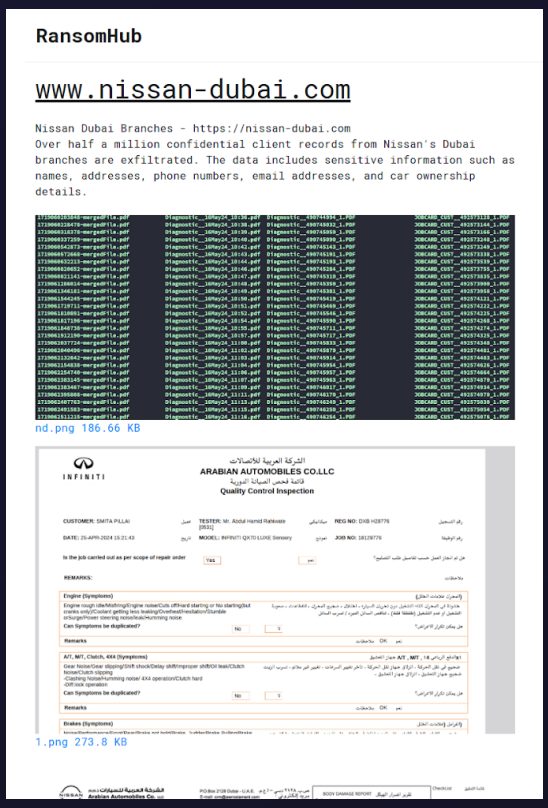


In the killsec ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as moi.gov.ly

The Ministry of Internal Affairs of Libya (وزارة الداخلية الليبية) is headquartered in Tripoli.

While these claims have not been verified, it is crucial to emphasize that these are allegations made by the ransomware group.

The Ransomware Victim of RansomHub: www.nissan-dubai.com

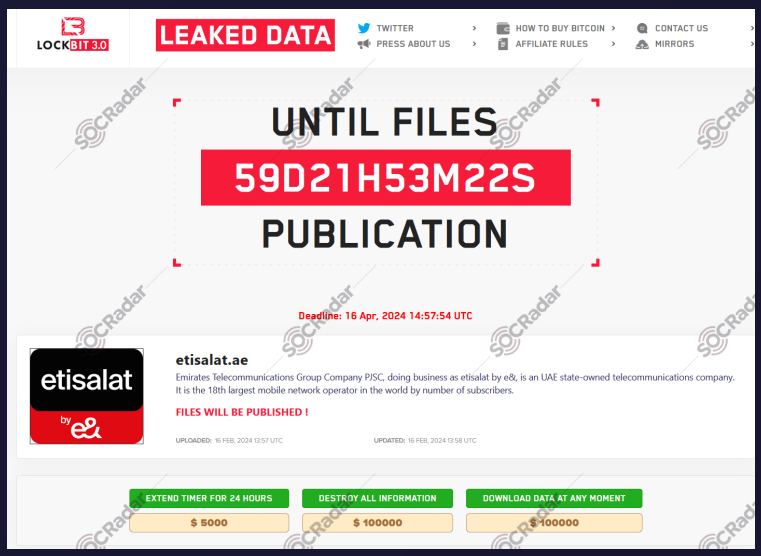


In the RansomHub ransomware group website monitored by SOCRadar, Nissan Dubai was announced as a ransomware victim.

Nissan Dubai is a leading automotive company that specializes in selling and servicing Nissan vehicles in Dubai.

While these claims have not been verified, it is crucial to emphasize that these are allegations made by the ransomware group.

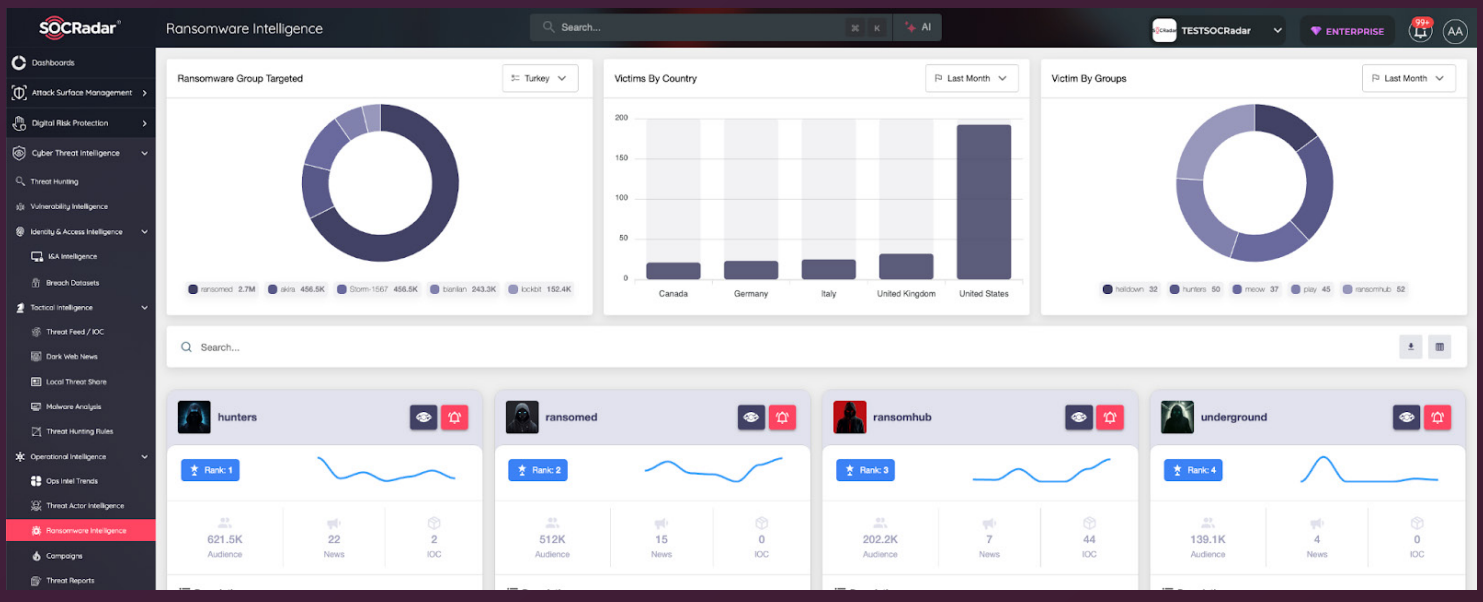
The Ransomware Victim of LockBit 3.0: Emirates Telecommunications Group



LockBit 3.0 ransomware group allegedly announced Emirates Telecommunications Group as a victim. The group claimed responsibility for a ransomware attack on the UAE-based state-owned telecommunications company, one of the world's largest mobile network operators, with millions of subscribers.

While these claims have not been verified, the allegations raise serious concerns about potential data exposure for a major telecommunications company. It is crucial to emphasize that these are allegations made by the ransomware group.

Explore our newly renovated ***Ransomware Intelligence module*** and gain comprehensive insights with detailed group profiles, MITRE Visualizer, and actionable IOCs. These insights will empower you to stay ahead of evolving threats and enhance your cybersecurity strategy.



Stealer Log Statistics

Stealer Log Statistics: Top Domains in the MEA Region

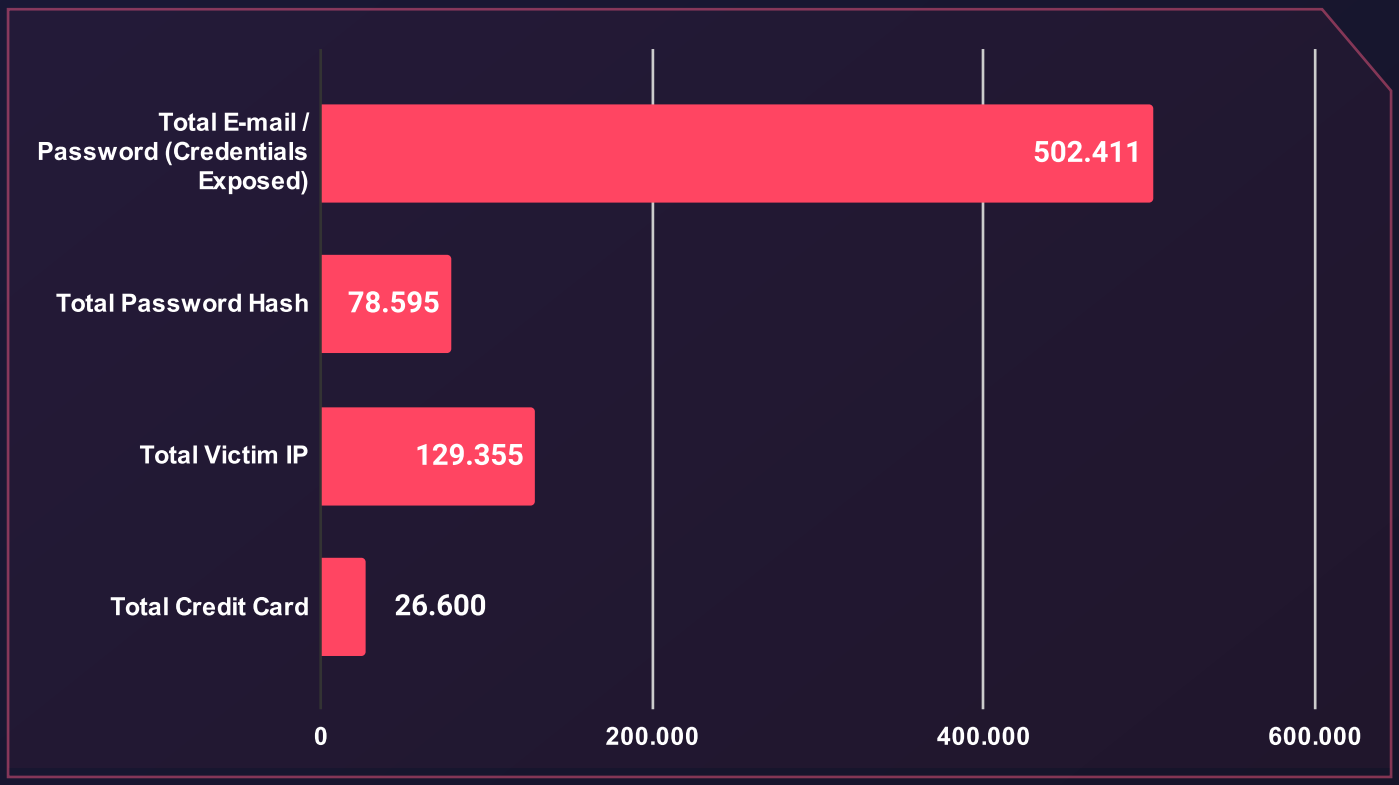
Thousands of users' IDs, email addresses, passwords, credit card data, password hashes, and victim IP addresses were compromised via Stealers from some of the most popular domains in the MEA region.

The table below lists the domains in MEA with the highest traffic in various parts of the region.

lequipe.fr	e.gov.kw	talabat.com	cricbuzz.com
education.tn	moi.gov.qa	moe.gov.om	beytoote.com
matchendirect.fr	allocine.fr	sanjaesh.org	donoghte.com
dahaboo.com	mytek.tn	shobiddak.com	bahrain.bh
kora-lives.com	tunisianet.com.tn	roozaneh.net	footmercato.net
clubic.com	islamweb.net	justgiving.com	digikala.com
savefrom.net	moi.gov.kw	365scores.com	alazhar.edu.ps
opensooq.com	paci.gov.kw	cafebazaar.ir	maannews.net
webteb.com	alaqsa.edu.ps	lingvanex.com	lmra.gov.bh
tayara.tn	alaneesqatar.qa	edunet.bh	uob.edu.bh

Stealer Logs - Distribution of the Compromised Data

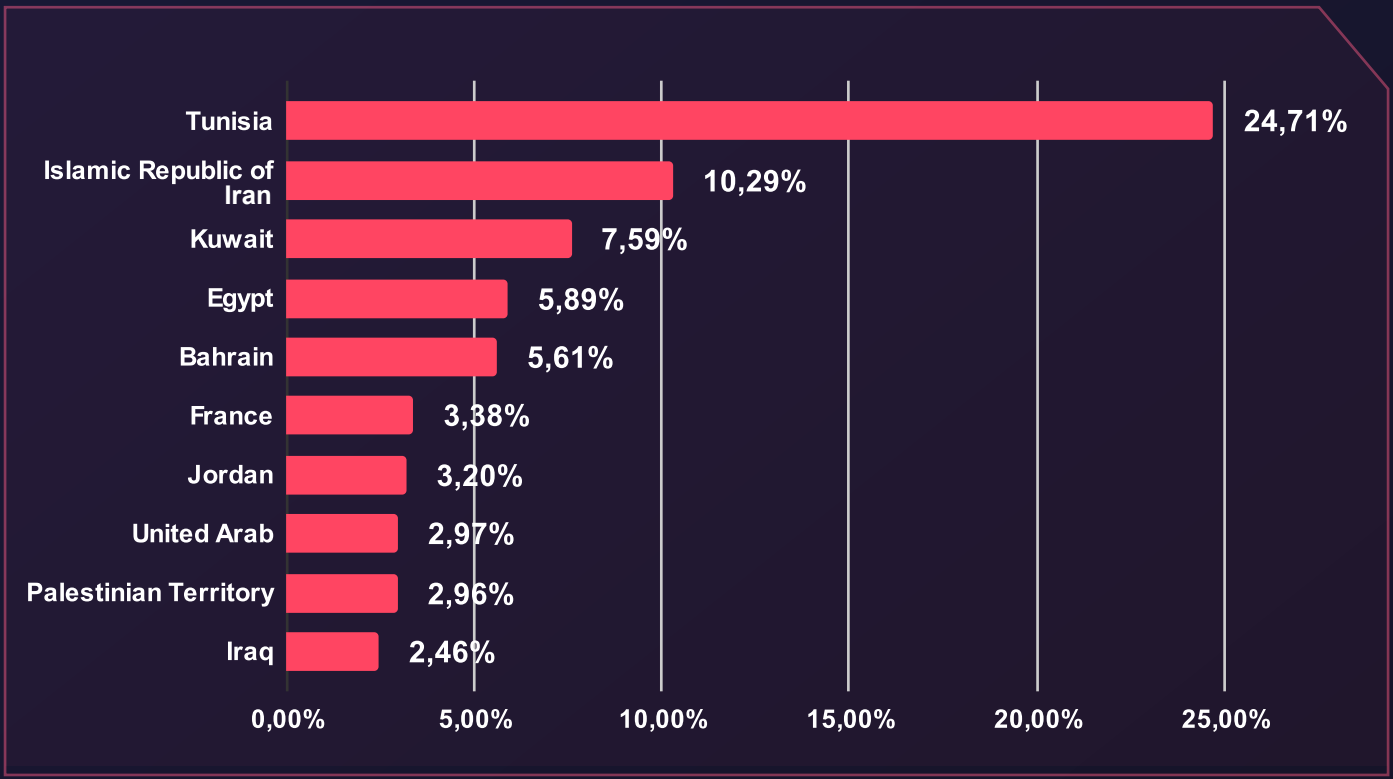
Stealer Logs - Compromised Data



Stealer logs reveal victims' information in plain text, indicating a significant risk for organizations in MEA. The information in these logs, including employees' data, can be used to target their workplaces.

Stealer Logs - Distribution of the Victim Countries

Stealer Logs - Distribution of Victims' Countries



Stealers are malware that track and save your activity, including credentials. They infiltrate your system and compromise sensitive information, which threat actors can later sell.

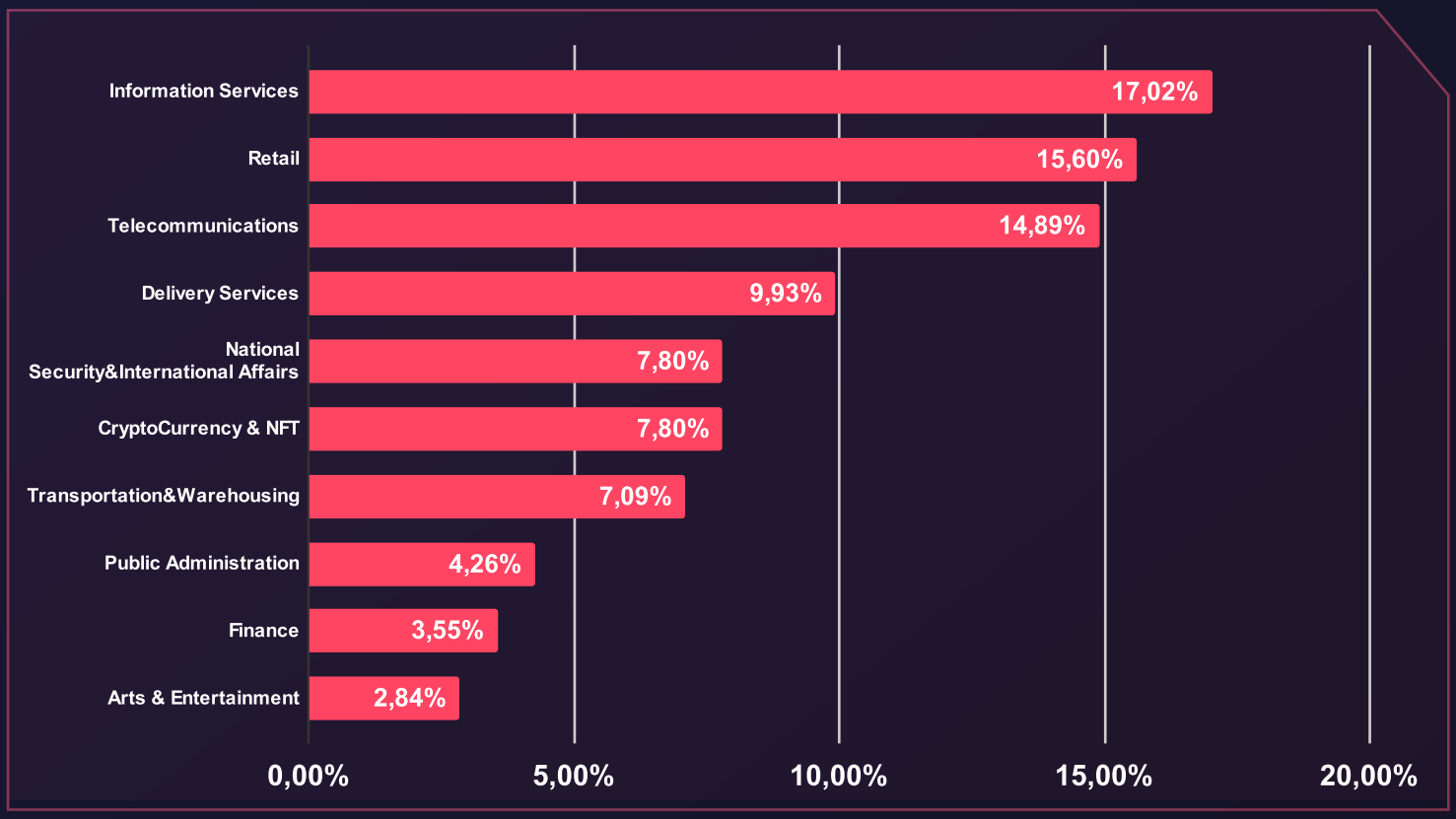
Regardless of your organization's size or location, it is crucial to prioritize robust password management and maintain a secure, organized work environment. Maintaining strong, unique passwords and securing your digital work environment from malicious software can significantly reduce the risk of unauthorized access and data breaches.

Tunisia had the highest presence of stealer logs in the MEA region, with **24,71%** of logs linked to individuals from there. **Iran** followed, with **10,29%** of stealer logs associated with users from the country, while **Kuwait** ranked third, with **7,59%** of logs originating from there.

Phishing Threats Targeting the MEA Region

Phishing Threats Targeting the MEA Region

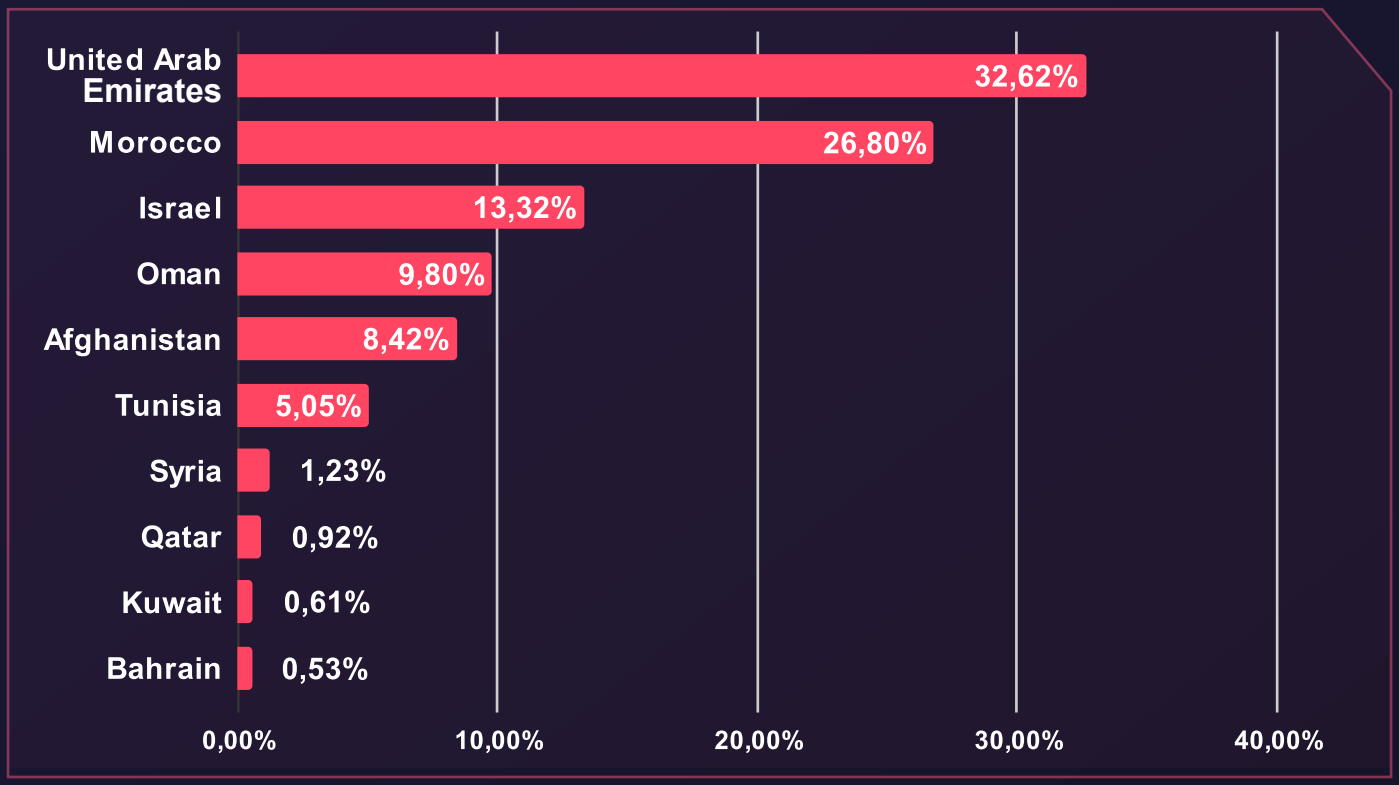
Phishing Attacks - Distribution by Industry



The **Information Services** industry in the MEA region faced the most phishing attacks, with **17,02%** of the total attempts. **The retail industry was second** with **15,6%** of the attacks, and **Telecommunications** was targeted with **14,89%.**

Phishing Attacks - Distribution by Target Country

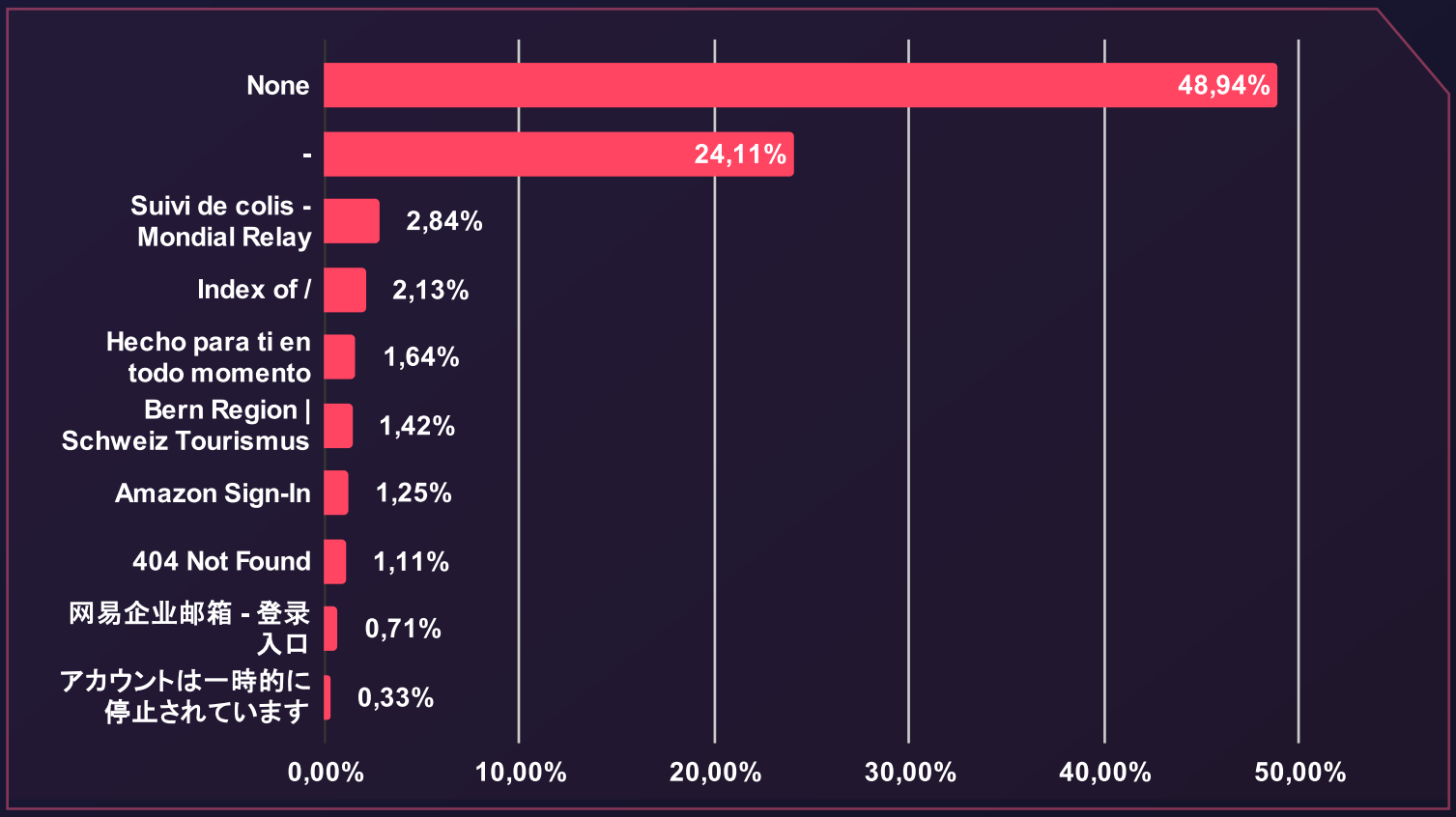
Phishing Attacks - Distribution by Target Country



The United Arab Emirates was targeted the most by phishing attacks, with **32,62%** of the attacks compared to other countries in the MEA region. **Morocco** was in the second spot, being the victim of **26,8%** of phishing attacks. In the third spot, **Israel** suffered **13,32%** of the phishing attacks.

Phishing Attacks - Distribution by Phishing Page Title

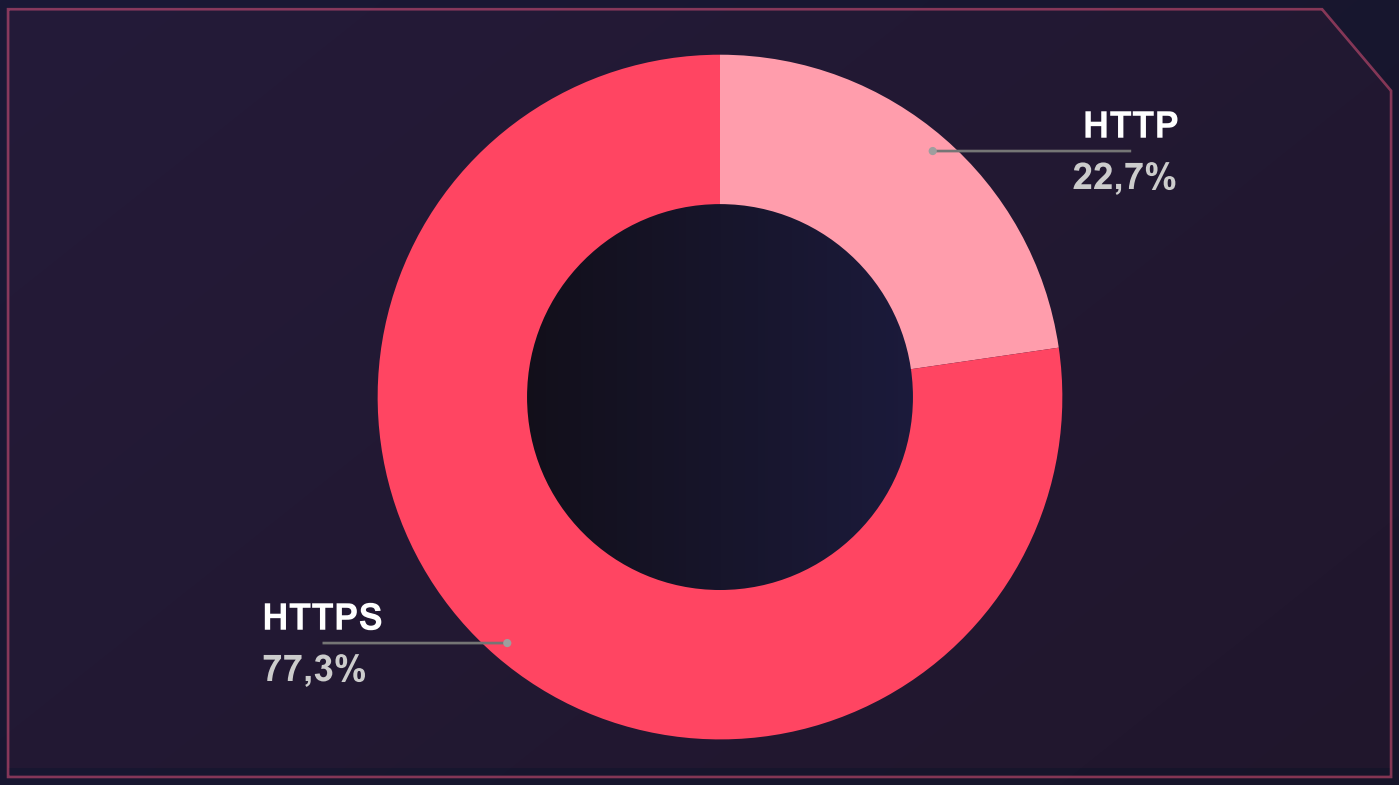
Phishing Attacks - Distribution by Phishing Page Title



Our analysis shows the most used pages in phishing attacks. The data reveals a predominant usage of the “None” page.

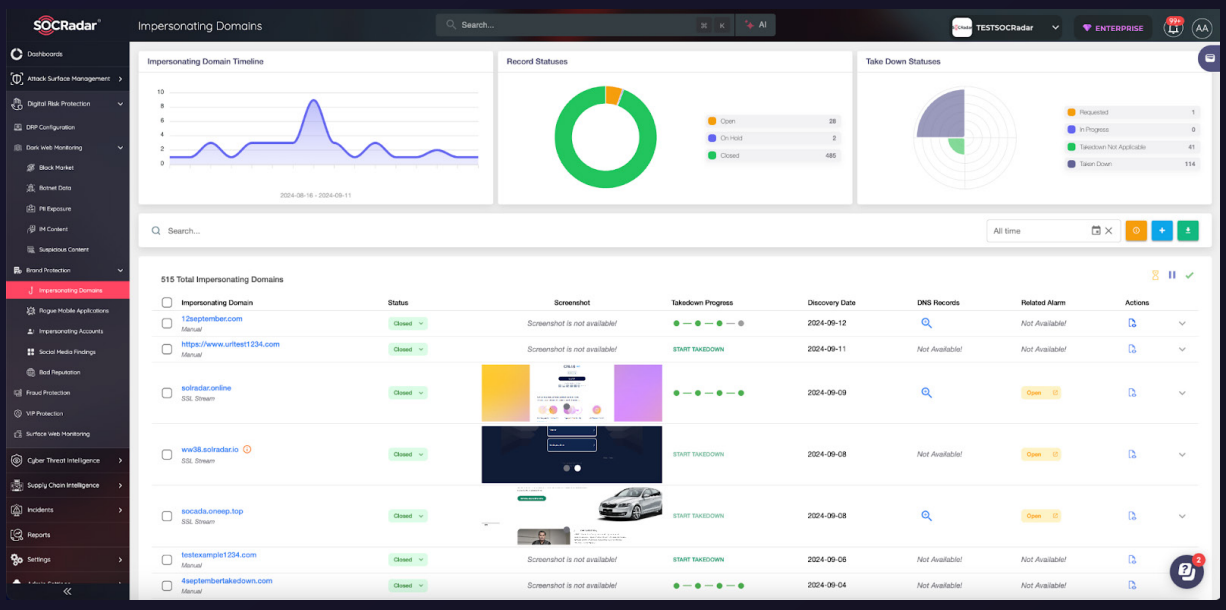
Phishing Attacks - Distribution by SSL/TLS Protocol

Phishing Attacks - Distribution by SSL/TLS Protocol



When we analyze the protocols used by phishing websites, we see a predominant use of HTTPS protocols. This is generally done to improve the websites' genuineness.

SOCRadar Labs provides free services such as Phishing Radar, which helps identify phishing attacks swiftly. Our AI-powered Digital Risk Protection platform scans millions of domain registrations to detect malicious domains and alerts on suspicious activity.



SOCRadar Brand Protection Module

DDoS Attack Statistics

The threat landscape was pretty active for the MEA region.

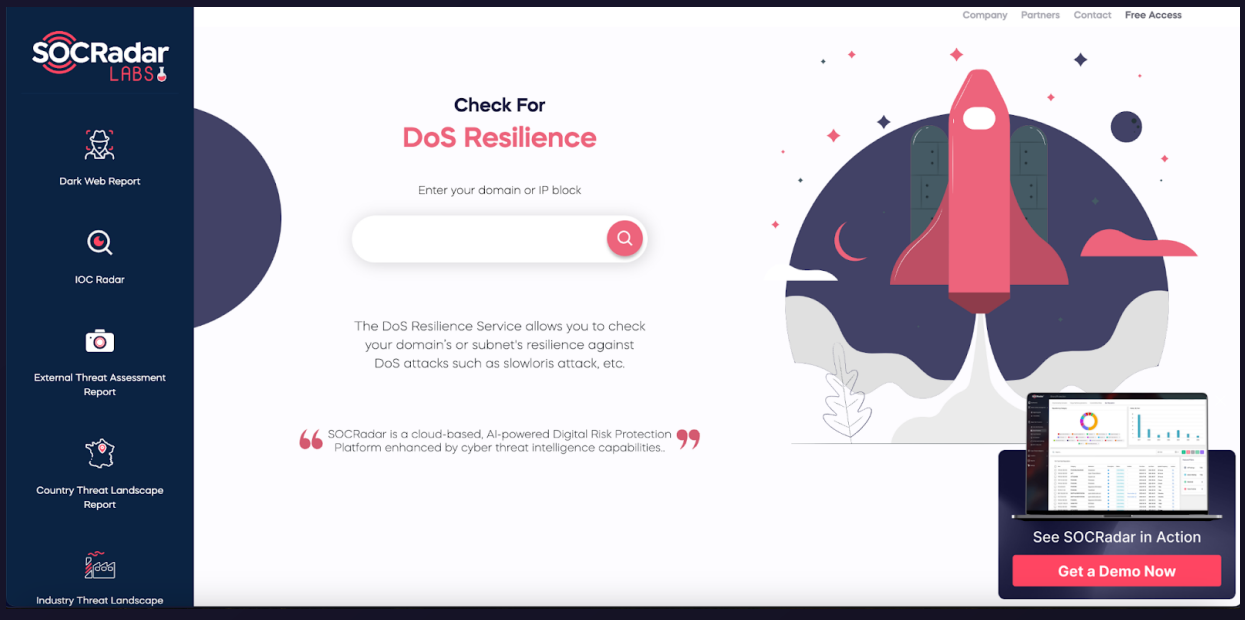
- The **peak bandwidth** witnessed during a DDoS attack reached 3847,58 Gbps, highlighting a significant capacity from the cyber threats.
- **The highest recorded throughput** during these incidents was 728,40 Mpps.
- Most DDoS attacks lasted **36 minutes** on average.
- **787,347 DDoS attacks** were recorded, highlighting the high frequency of cyberattacks and illustrating the general threat landscape for MEA targets.

The numbers above show that the MEA region faces a serious DDoS risk. The attacks don't take too long, but the amount of attacks and their size are considerable threats to organizations.

Top DDoS Attack Vectors

Attack Vector	Number of Attacks (1H 2024)
TCP ACK	251,412
TCP SYN	8,149
TCK RST	42,639
DNS Amplification	234,626
ICMP	59,874

Enhance your DDoS defense with SOCRadar's DoS Resilience Free Tool. Our Free DoS Resilience Service allows you to check your domain's or subnet's resilience against DoS attacks, such as slow loris attacks.



Lessons Learned: Key Insights and Strategic Recommendations

Upon reflection of the cyber threat landscape impacting organizations in MEA, several pivotal lessons and recommendations emerge. These insights, coupled with the capabilities of SOCRadar, offer a roadmap for enhancing cyber resilience and preserving operational integrity. The following are the top 5 takeaways from our analysis:

Maintain vigilance regarding the evolving cyber threat landscape:
The cyber threat landscape is dynamically evolving, as evidenced by the surge in Dark Web activity related to MEA and the proliferation of ransomware incidents. Organizations must stay abreast of these developments and adapt their security strategies accordingly. Leveraging *SOCRadar's Cyber Threat Intelligence* provides businesses with real-time insights into emerging threats, enabling them to stay ahead of cyber adversaries.

Emphasize multi-layered security measures:
The diverse range of industries targeted by cyber threats underscores the necessity for multi-layered security measures. As demonstrated, threat actors do not discriminate based on industry, necessitating a comprehensive security approach across all industries, from Information Technology to Public Administration. SOCRadar can support this effort through *proactive threat intelligence* and monitoring services.

Maintain vigilance against ransomware:
Ransomware remains a significant threat, highlighting the importance of robust defenses and response plans. *SOCRadar's threat intelligence* capabilities enable businesses to identify potential ransomware threats and develop effective response strategies.

Educate and train employees:
Continuous employee education and training are essential, given the persistent threat of phishing attacks. Familiarity with phishing tactics and detection methods is critical. SOCRadar's solutions can assist by identifying potential phishing domains and raising awareness of the latest phishing techniques.

Ensure defense against Stealers:
Organizations must enhance their defenses against these malicious software. *SOCRadar's advanced threat intelligence* aids in detecting and mitigating Stealer Threats, bolstering the organization's overall security posture. Adopting a proactive, informed, and comprehensive approach to cybersecurity is paramount. By partnering with solutions such as SOCRadar, organizations in MEA can fortify their defenses and effectively navigate the evolving cyber threat landscape.

Who is SOCRadar®?

Your Eyes Beyond

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Trusted by 21.000+ companies in 150+ countries

Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

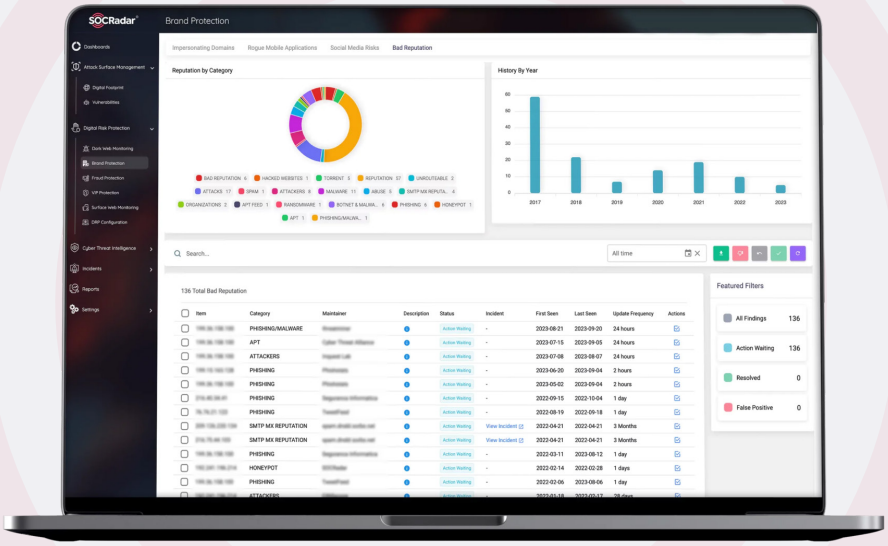
Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

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

GET ACCESS FOR FREE

START YOUR PERSONALIZED DEMO

Discover SOCRadar's powerful tools and easy-to-use interface to enhance cyber threat intelligence efforts. Schedule a demo with our experts to see it in action, and we'll show you what SOCRadar can do.



Start Your Demo

SOCRadar®
Your Eyes Beyond

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

Call
+1 (571) 249-4598

Email
info@socradar.io

socradar.io

Virtual Addresses

London, UK
167 City Road Old Street, London EC1V 1AW

Dubai, UAE
8W building 5th Floor, DAFZA, Dubai

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

Bangalore, India
The Estate, 8th Floor Dickenson Road 560042 Bangalore Karnataka