SOCRadar®
Your Eyes Beyond

GULF COOPERATION COUNCIL (GCC) COUNTRIES

REPORT:

“Public Administration is the most targeted industry in GCC region”

SOCRadar®
Your Eyes Beyond

Table of Contents

Executive Summary 2

Timeline of Recent Cyber Attacks 4

Dark Web Threats 9

Ransomware Threats 12

Top Ransomware Group in the GCC Region: LockBit3.0 14

State Sponsored APT Activities 15

Phishing Threats 15

An Inherent Weakness: Critical Infrastructures in GCC 17

Cyber Resilience in the Countries of Gulf Cooperation Council (GCC) 18

SAMA CTI & SOCRadar Compatibility 19

www.socradar.io

Executive Summary

“Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates constitute the Cooperation Council for the Arab States of the Gulf, generally known as the Gulf Cooperation Council (GCC), a regional, intergovernmental, political, and economic association. The council's secretariat is in Riyadh, the Saudi Arabian capital. On May 25, 1981, the Charter of the GCC was signed, thereby founding the organization.”

GCC consists of the wealthiest countries in the Arab region and its total economy is one of the biggest in the world. As the world’s largest oil and gas exporter, GCC countries have established competitive and digitalized economies.

Despite the challenges caused by regional and global developments, especially the COVID-19 pandemic, infrastructure projects have continued in GCC countries. The GCC countries have experienced improvements in the transport and logistics, healthcare, retail, real estate, education, tourism, and finance sectors, and governments have invested in these fields.

The relative stability they experienced made the public benefit from the riches of the oil and gas as well as the governments to invest in other fields like transport and logistics, healthcare, retail, real estate, education, tourism, finance, etc..
In addition to local industries, the unexpected global digitalization came with Covid-19 pandemic created opportunities for cyber crime actors. Especially the GCC countries Saudi Arabia, UAE, and Kuwait became a target of millions of cyber attacks each month.

This report investigated various types of cyber incidents that SOCRadar dark web team relates to GCC, in the time interval of March 2022 and February 2023. We hope to provide insight to what was happening in the Cyber Threat Landscape of GCC countries and their cyber preparedness.

Key Findings

• In March 2022, **SAMA announced the Cyber Threat Intelligence Principles** as part of the Cybersecurity Framework. CTI principles has become a requirement for Saudi financial institutions to achieve SAMA Cybersecurity Framework Compliance. We are providing a SOCRadar & SAMA CTI principles compliance chart at the end of this report which shows how SOCRadar assists SAMA member organizations to achieve in implementing SAMA CTI principles.

• SOCRadar DarkMirror detected 309 dark web posts related to GCC countries between the time scope of March 1, 2022 to February 28, 2023. **98% of the post aims to either sell or share data without any compensation.**

• SOCRadar DarkMirror data shows that the highest number of posts were at **December 2022.**

• The SOCRadar dark web team has analyzed the dark web shares by post types. The analysis shows us that **data exposure** was the most common dark web post type.

• 47 ransomware incidents were observed against GCC countries by SOCRadar.The **top ransomware group in the region is LockBit3.0.** AlphVM/Blackcat and Mallox groups were also very active in the region.

• The countries were targeted most by the threat actors were **UAE, Saudi Arabia, and Kuwait** between the time scope of March 1, 2022 to February 28, 2023.

• SOCRadar DarkMirror data shows that, **"Public Administration"** was the most targeted industry in GCC region, followed by E-commerce and Information Services industries.

• **Total of 755 phishing attacks** against GCC were recorded according to SOCRadar dark web team.

• Almost **60% of the phishing websites** were hosted on HTTPS domains using a valid SSL certificate.

• During the Qatar World Cup, researchers found at least five websites posing as employment application forms and about **40 fraudulent apps** in the Google Play Store promising access to tickets.

• Significant APT groups targeting GCC organizations are **MuddyWater, CHRYSENE, Turla Group, Leviathan, Naikon, HAZY TIGER , El Machete, MAGNALLIUM, RAZOR TIGER, Infy.**

• Threat actors pose a major risk to the ONG industry of the GCC region. The region contains attractive facilities for threat actors, like: **Ghawar, Safaniyah, Abqaiq, Ras Tanura.**

Timeline of Recent Cyber Attacks

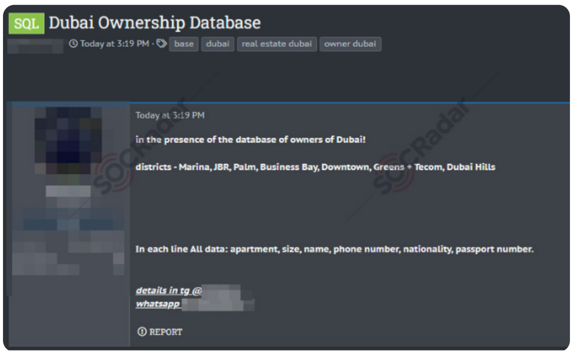
March 4
2023

According to local sources, the Kuwaiti Ministry of Commerce and Industry stopped a hacking attempt and has already implemented several security measures. The Ransomware Lockbit 3.0 virus infiltrated the network through two personal computers. However, the malware was detected early, and the computers disconnected.

March 2
2023

Database of Dubai Residents is on Sale

In a hacker forum monitored by SOCRadar, a new alleged ownership database sale is detected for Dubai. The alleged database has information about the property ownership in the following districts: Marina, JBR, Palm, Business Bay, Downtown, Greens, Tecom, and Dubai Hills. Threat actors claim the following information on the database: Apartment, Size, Name, Phone number, Nationality, Passport number.



SQL Dubai Ownership Database

[redacted] Today at 3:19 PM · base dubai real estate dubai owner dubai

Today at 3:19 PM

in the presence of the database of owners of Dubai!

districts - Marina, JBR, Palm, Business Bay, Downtown, Greens + Tecom, Dubai Hills

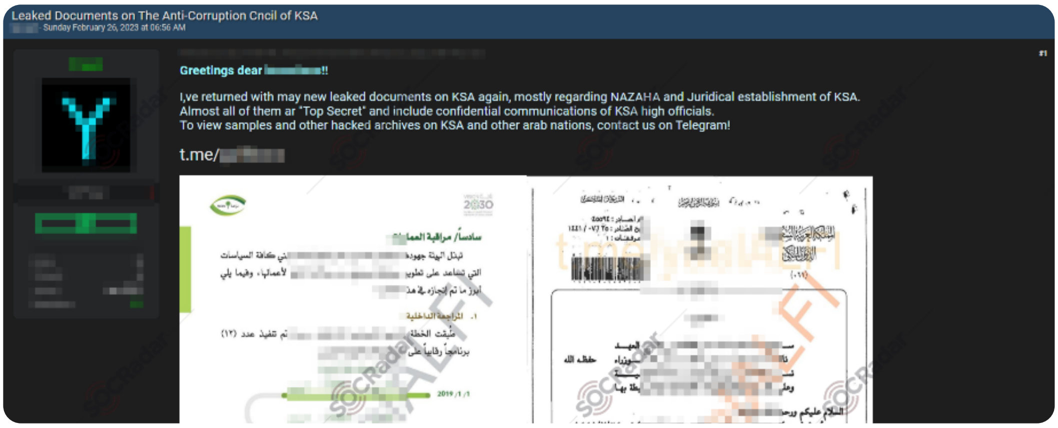
In each line All data: apartment, size, name, phone number, nationality, passport number.

details in tg @[redacted]
whatsapp [redacted]

February 25
2023

Sensitive Documents of Saudi Arabia's National Anti-Corruption Commission are Leaked

In a hacker forum monitored by SOCRadar, a new alleged sensitive documents leak is detected for the Kingdom of Saudi Arabia's (KSA) National Anti-Corruption Commission. The actor claimed that almost all of the leaked documents were highly classified and were including confidential communications of KSA high officials.



Leaked Documents on The Anti-Corruption Cncil of KSA
[redacted] - Sunday February 26, 2023 at 06:56 AM

Greetings dear [redacted]!!

I,ve returned with may new leaked documents on KSA again, mostly regarding NAZAHA and Juridical establishment of KSA.
Almost all of them ar "Top Secret" and include confidential communications of KSA high officials.
To view samples and other hacked archives on KSA and other arab nations, contact us on Telegram!

t.me/[redacted]

Timeline of Recent Cyber Attacks

February 14
2023

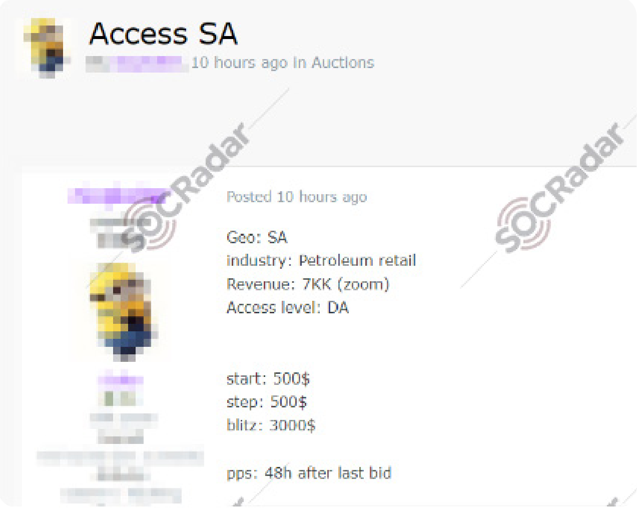
Hackers Target Bahrain Airport, News Sites to Mark Uprising

A group calling itself Al-Toufan claimed that they took down the websites of Bahrain's international airport and state news agency to mark the 12-year anniversary of an Arab Spring uprising in Bahrain in an online statement.

February 6
2023

Unauthorized Access Sale is Detected for a Saudi Arabian Petroleum Company

In a hacker forum monitored by SOCRadar, an unauthorized access sale is detected allegedly belongs to a petroleum company that operates in Saudi Arabia.



Access SA

[redacted] 10 hours ago in Auctions

Posted 10 hours ago

Geo: SA
industry: Petroleum retail
Revenue: 7KK (zoom)
Access level: DA

start: 500$
step: 500$
blitz: 3000$

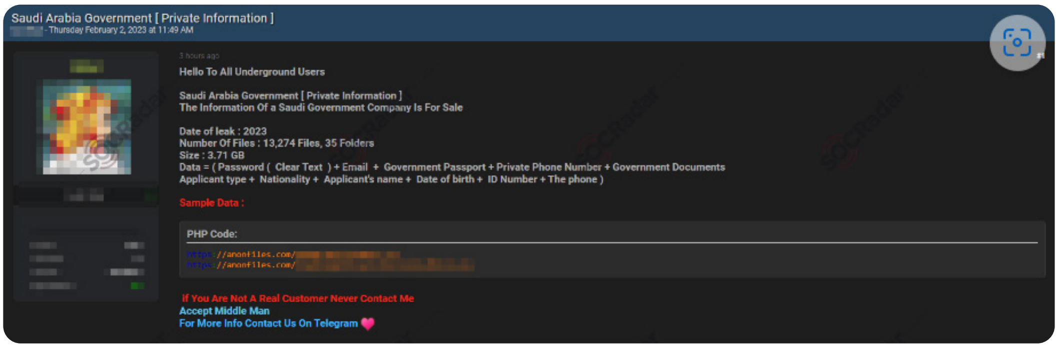
pps: 48h after last bid

February 1
2023

Sensitive Data of Saudi Arabia Government is on Sale

In a hacker forum monitored by SOCRadar, an alleged sensitive data leak was detected for Saudi Arabia Government and a Saudi Government Company.

Threat actors claimed that the data belonged to 2023 and the following information was on the database: Password in clear text format, Email, Government Passport, Private Phone Number, Government Documents, Applicant type, Nationality, Applicant's name, Date of birth , ID Number, Phone Number. They also claimed that data consisted 35 folders and 13,274 files in the size of 3.71 GB.



Saudi Arabia Government [Private Information]
[redacted] - Thursday February 2, 2023 at 11:49 AM

3 hours ago

Hello To All Underground Users

Saudi Arabia Government [Private Information]
The Information Of a Saudi Government Company Is For Sale

Date of leak : 2023
Number Of Files : 13,274 Files, 35 Folders
Size : 3.71 GB
Data = (Password (Clear Text) + Email + Government Passport + Private Phone Number + Government Documents
Applicant type + Nationality + Applicant's name + Date of birth + ID Number + The phone)

Sample Data :

PHP Code:

```
https://anonfiles.com/[redacted]
https://anonfiles.com/[redacted]
```

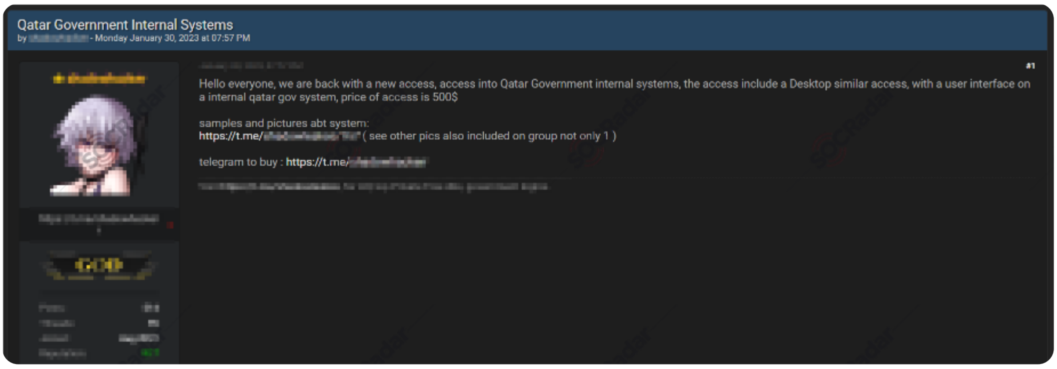
If You Are Not A Real Customer Never Contact Me
Accept Middle Man
For More Info Contact Us On Telegram 💗

Timeline of Recent Cyber Attacks

January 29
2023

Unauthorized Network Access Sale is Detected for Qatar Government's Internal Services

In a hacker forum monitored by SOCRadar, an unauthorized network access sale is detected that allegedly belongs to the Qatar government's internal service.



Qatar Government Internal Systems
by [redacted] - Monday January 30, 2023 at 07:57 PM

#1

Hello everyone, we are back with a new access, access into Qatar Government internal systems, the access include a Desktop similar access, with a user interface on a internal qatar gov system, price of access is 500$

samples and pictures abt system:
https://t.me/[redacted] (see other pics also included on group not only 1)

telegram to buy : https://t.me/[redacted]

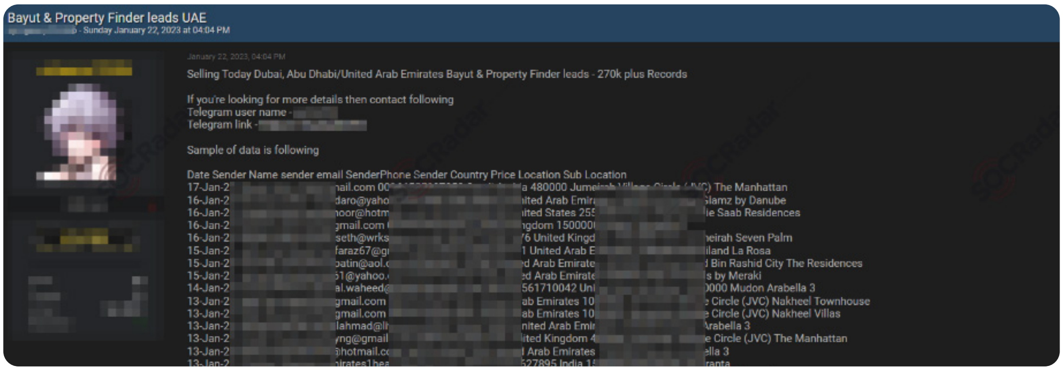
January 25
2023

Around mid-January, many clients of Kuwaiti banks became victims of a phishing campaign via email. Victims received emails looked like coming from the postal department of Kuwaiti Ministry of Communications or from courier companies such as DHL and Aramex with a malicious link. When the link clicked, it stole banking information from smart devices. It can be said that there is a CSRF-like vulnerability in the payment system, since the attack is realized by clicking the link.

January 21
2023

Data of Emirati Citizens are on Sale

In the hacker forums monitored by SOCRadar, three alleged data sets sale were detected for Emirati citizens: Bayut (UAE real estate portal) and property finder leads database, Luxury Products Buyers Database and Data of Forex Leads.



Bayut & Property Finder leads UAE
[redacted] - Sunday January 22, 2023 at 04:04 PM

January 22, 2023, 04:04 PM

Selling Today Dubai, Abu Dhabi/United Arab Emirates Bayut & Property Finder leads - 270k plus Records

If you're looking for more details then contact following
Telegram user name - [redacted]
Telegram link - [redacted]

Sample of data is following

```
Date Sender Name sender email SenderPhone Sender Country Price Location Sub Location
17-Jan-2[redacted]nail.com 00[redacted]a 480000 Jume[redacted]C) The Manhattan
16-Jan-2[redacted]daro@yaho[redacted]ited Arab Emir[redacted]Glamz by Danube
16-Jan-2[redacted]noor@hotm[redacted]ited States 255[redacted]ie Saab Residences
16-Jan-2[redacted]gmail.com [redacted]gdom 150000[redacted]
16-Jan-2[redacted]seth@wrks[redacted]76 United Kingd[redacted]eirah Seven Palm
15-Jan-2[redacted]faraz67@g[redacted]1 United Arab E[redacted]iland La Rosa
15-Jan-2[redacted]patin@aol.[redacted]d Arab Emirate[redacted]d Bin Rashid City The Residences
15-Jan-2[redacted]51@yahoo.[redacted]ed Arab Emirate[redacted]s by Meraki
14-Jan-2[redacted]al.waheed@[redacted]561710042 Uni[redacted]0000 Mudon Arabella 3
13-Jan-2[redacted]gmail.com [redacted]ab Emirates 10[redacted]e Circle (JVC) Nakheel Townhouse
13-Jan-2[redacted]gmail.com [redacted]ab Emirates 10[redacted]e Circle (JVC) Nakheel Villas
13-Jan-2[redacted]lahmad@l[redacted]nited Arab Emi[redacted]Arabella 3
13-Jan-2[redacted]yng@gmail[redacted]ited Kingdom 4[redacted]e Circle (JVC) The Manhattan
13-Jan-2[redacted]@hotmail.c[redacted]l Arab Emirates [redacted]ella 3
13-Jan-2[redacted]nirates1hea[redacted]527895 India 1[redacted]ranta
```

Timeline of Recent Cyber Attacks

Cyber Crime During the FIFA WORLD CUP Qatar2022

Scammers have set up many ways to collect personal information and defraud individuals of their money during the World Cup. The Hayya Card system, which is required for World Cup visitors to enter Qatar and to access tickets and other services like transportation, was found to have numerous potentially compromised accounts.

The researchers saw the attackers utilizing data-stealing malware like Redline and Erbium to carry out their World Cup scams. The researchers also discovered fake websites selling false goods and tickets used to steal money from customers or their banking information. Also, they found at least five websites posing as employment application forms and about 40 fraudulent apps in the Google Play Store promising access to tickets.

To learn more about Qatar World Cup and cyber crime you can visit SOCRadar's detailed blog post. You can also search for major events like the World Cup on the "Campaign" page on the SOCRadar platform.

November 22
2022

Qatar World Cup employees targeted by phishing cyberattacks

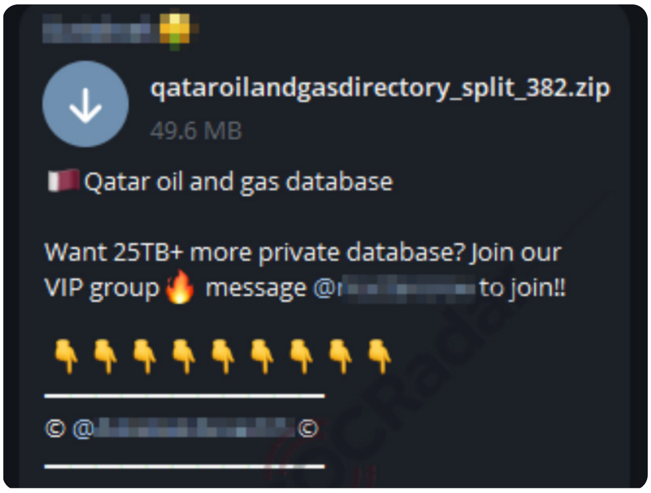
Employees of the World Cup organizers had to avoid a sharp rise in cyberattack efforts, mostly from five infamous cybercriminal gangs at the forefront of the current wave of cybercrime: Qakbot, Emotet, Formbook, Remcos, and QuadAgent.

Timeline of Recent Cyber Attacks

January 3
2023

Data of Qatar Oil and Gas Companies are Leaked

In a hacker Telegram channel monitored by SOCRadar, a new alleged data leak is detected allegedly belonging to Qatar Oil and Gas companies. Threat actors claimed to have more than 25TB of data.



[redacted]

qataroilandgasdirectory_split_382.zip
49.6 MB

🇶🇦 Qatar oil and gas database

Want 25TB+ more private database? Join our VIP group 🔥 message @[redacted] to join!!

👇👇👇👇👇👇👇👇👇

© @[redacted] ©

25 August
2022

Researchers spotted a new RAT (Remote Administration Tool) advertised in Dark Web and Telegram called Escanor. Resecurity researchers discovered a new remote access trojan (RAT), dubbed Escanor, being advertised on the dark web and Telegram. The RAT is offered as Android and Windows versions, alongside an HVNC module and exploits builder to weaponize Microsoft Office and Adobe PDF documents. The mobile version is currently used to target online banking customers by intercepting one-time password codes and stealing credentials. Most victims are based in the United States, Canada, UAE, Saudi Arabia, Kuwait, Bahrain, Egypt, Israel, Mexico, and Singapore.

July 4
2022

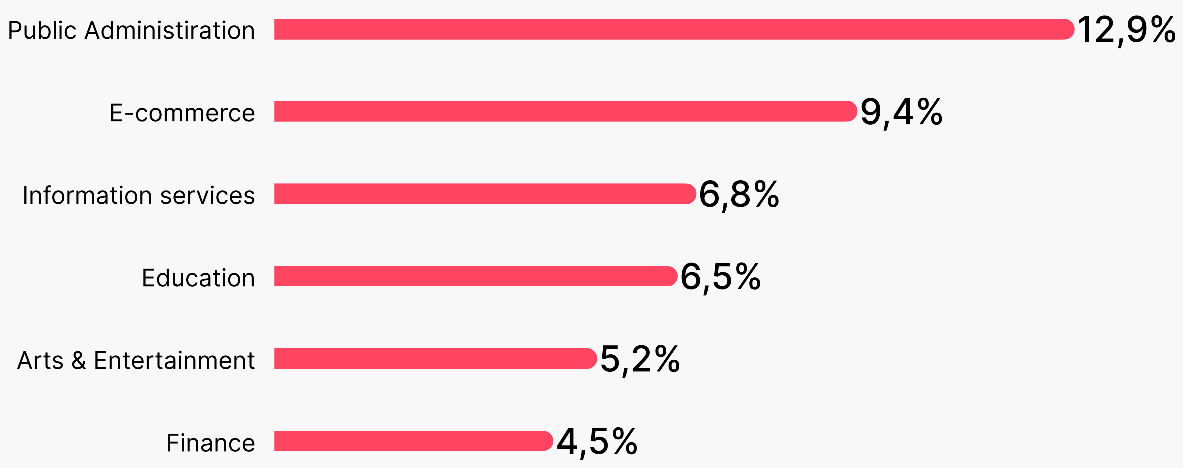
Over 2 million cyber attacks recorded in a month during Hajj season

Dark Web Threats

SOCRadar's dark web team has conducted comprehensive research, with the help of SOCRadar DarkMirror data, on dark web threats targeting GCC organizations to bring you insight into GCC cyber threat landscape. These dark web posts were provided by SOCRadar DarkMirror, which crawls through the dark web to detect malicious posts

Globally, within our time scope, March 2022 – February 2023, SOCRadar DarkMirror has detected 15.258 dark web posts. 3906 of these posts belonged to organizations in Asia, whereas only 766 of these posts were related to organizations in Middle East. During this research, the SOCRadar dark web team analyzed 309 dark web posts related to GCC countries from March 2022 to end of February 2023.

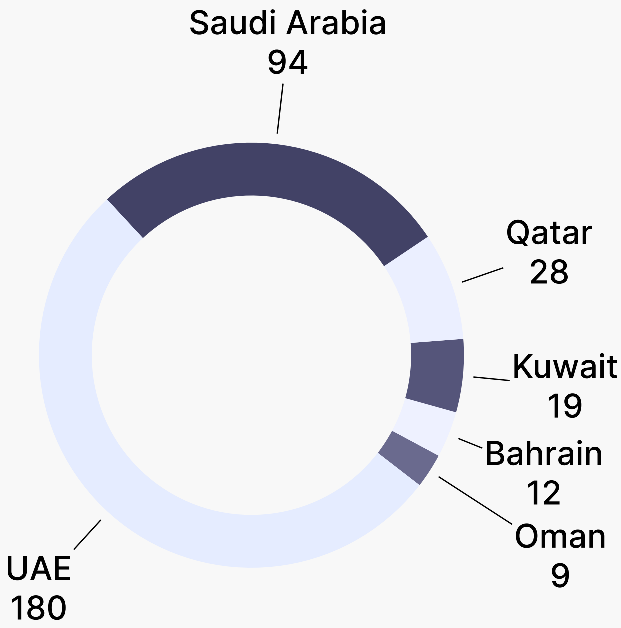
SOCRadar DarkMirror data shows that, for the period mentioned above, Public Administration was the most targeted industry in GCC region, followed by E-commerce and Information Services industry. However it is surprising that we did not see Gas and Oil or energy industry in top 6 industries mentioned in the dark web.



Dark Web Threats - Top 6 Industries

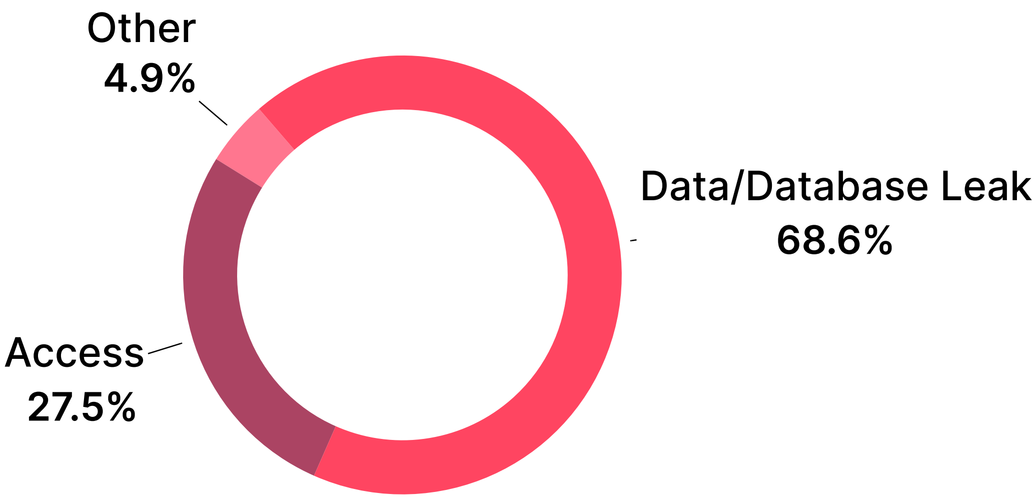
Dark Web Threats

When we look at the Dark web posts in the period, the mentions of organizations in UAE and Saudi Arabia were the more than 3 quarters of all mentions concerning GCC region.



Mentions by Countries

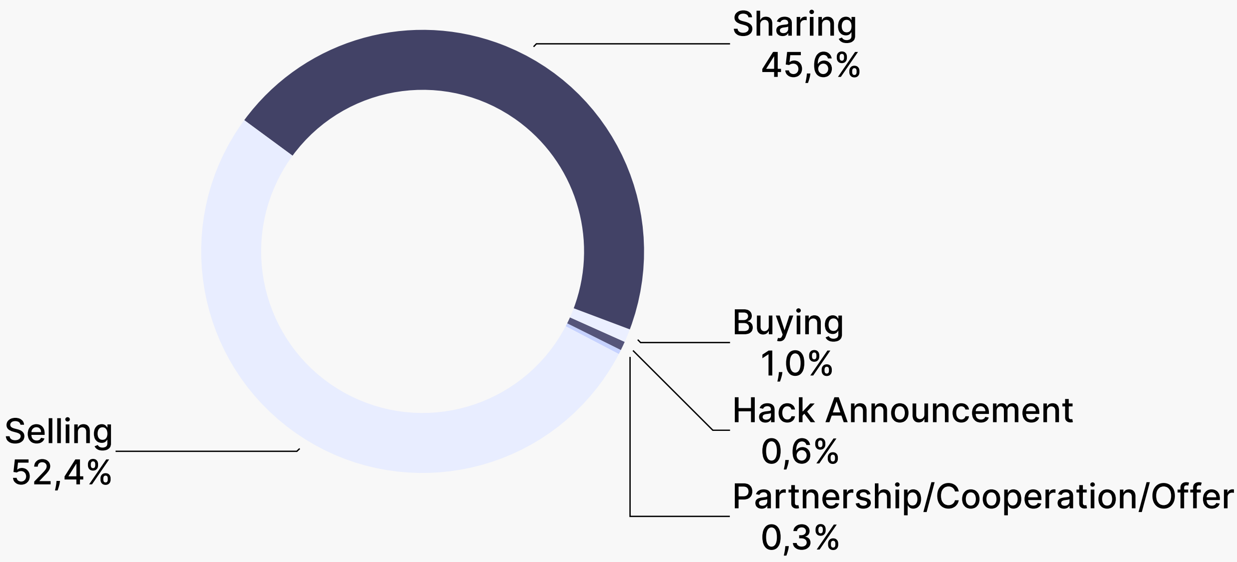
The SOCRadar dark web team has analyzed the dark web shares by post types. The analysis shows us that data exposure was the most common dark web post type. The exposed data include confidential data of private companies and governmental organizations, employee, and customer PIIs, and much more. Following sensitive data leak, posts about selling access to organizations' networks and admin panels was the second most common post type. The exposed data include credentials to company networks, admin panels, and/or credentials VPN and RDP connections.



Dark Web Threats – Dark Web Post Types

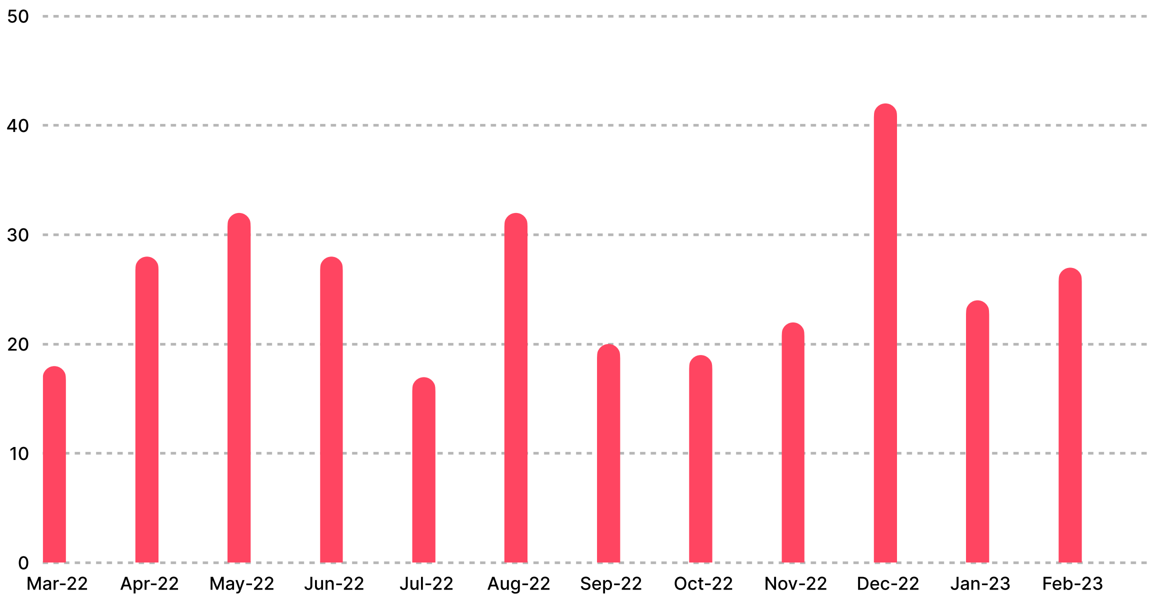
Dark Web Threats

Another way to look at these posts is to understand what kind of actions the threat actors want to take. 98% of the post aims to either sell or share data without any compensation. Only 1% of the posts are looking for some data or access to buy and 0.3% offers some kind of a partnership. It will not be a stretch to say that the threat actors could easily find whatever they need to attack GCC countries.



Dark Web Threats – Top 5 Dark Web Post Types

Lastly, SOCRadar DarkMirror data shows that the highest number of posts were at December 2022. Cyber attacks generally peak around the holiday season, especially In December. It seems that GCC region is not exception.

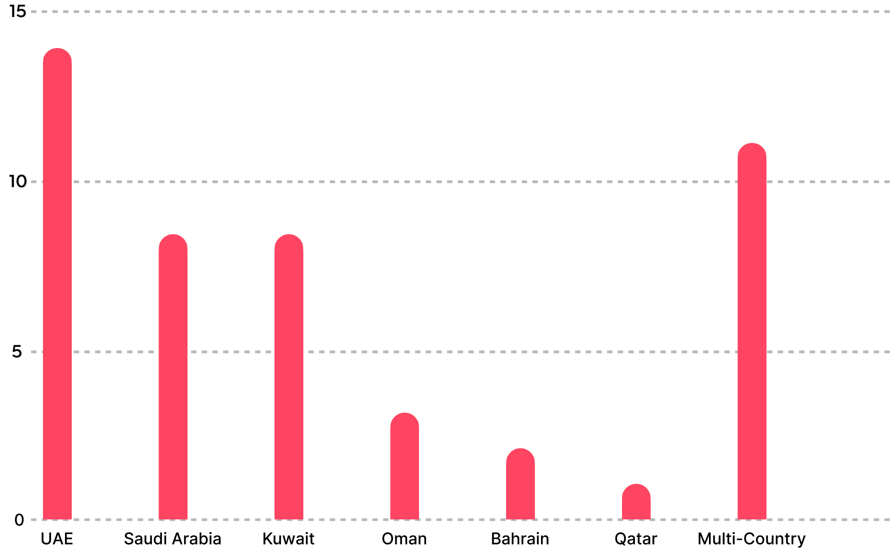


Dark Web Threats – Top 5 Dark Web Post Types

Ransomware Threats

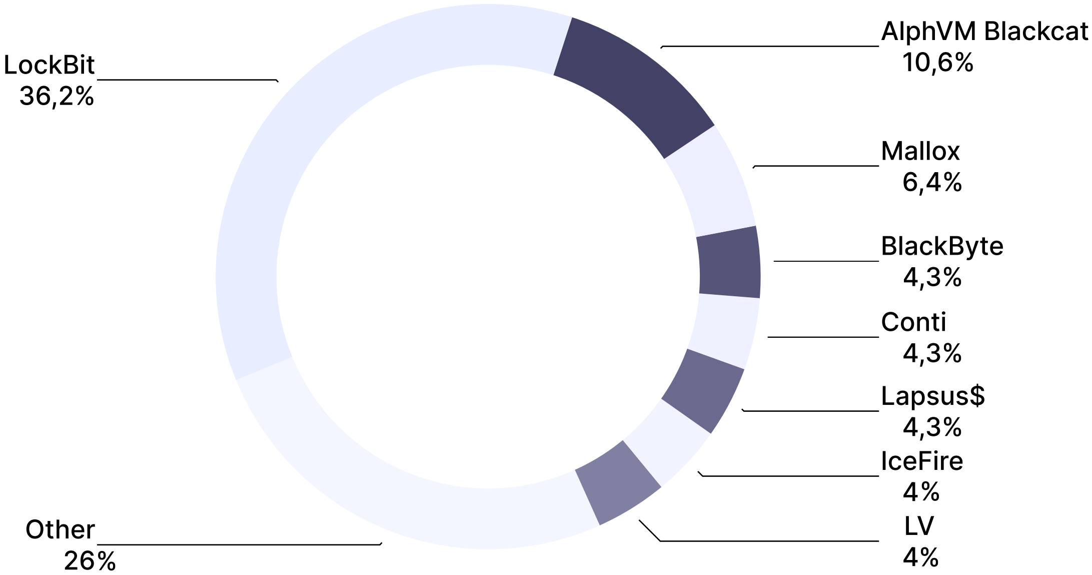
From March 2022 – February 2023, SOCRadar has detected exactly 2677 ransomware incidents globally belonging to 51 unique ransomware groups. 47 of these incidents belonged to organizations in GCC region.

Graph shows that the countries were targeted most by the threat actors were UAE, Saudi Arabia, and Kuwait.



Ransomware Threats – Ransomware attacks to each GCC Country (Total: 47)

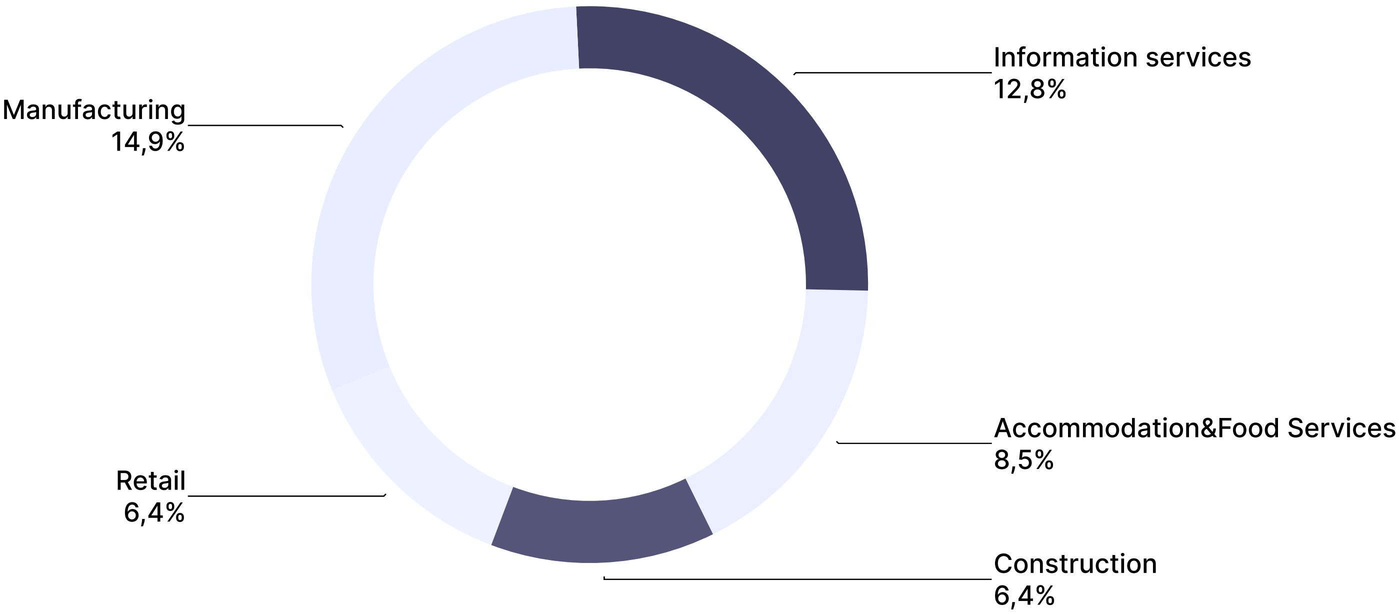
Twenty different ransomware groups were active in the region. When we consider Lockbit 2.0 and 3.0 together, Lockbit was responsible more than one-third of the ransomware attacks. AlphVM/Blackcat and Mallox groups were also very active in the region.



Ransomware Threats – Ransomware attacks to each GCC Country (Total: 47)

Ransomware Threats

SOCRadar data shows that, within our time scope, manufacturing was the most targeted Industry in GCC countries, followed by Information services. Compared to the SOCRadar's global averages (not given here) in the same period, Retail and Accomodation&Food Service Industries were more attacked in the region. This could be attributed to tourism efforts in the region and the global events in the region like World Cup 22 and Hajj (pilgrimage for muslims).



Ransomware Threats – Top 5 Targeted Industries by Ransomware Groups

Top Ransomware Group in the GCC Region: LockBit3.0

In March 16th of 2023, three organizations of US, The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing & Analysis Center (MS-ISAC), were released an Cyber Security Advisory called, #StopRansomware: LockBit 3.0.

In the advisory, Lockbit operations described as “The LockBit 3.0 ransomware operations function as a Ransomware-as-a-Service (RaaS) model and is a continuation of previous versions of the ransomware, LockBit 2.0, and LockBit. Since January 2020, LockBit has functioned as an affiliate-based ransomware variant; affiliates deploying the LockBit RaaS use many varying TTPs and attack a wide range of businesses and critical infrastructure organizations, which can make effective computer network defense and mitigation challenging”.

As described above, Lockbit tries many different kind of tricks to gain unauthorized access to the victims’ networks. You could find all the TTPs and more in this advisory

Initial Access		
Technique Title	**ID**	**Use**
Valid Accounts	T1078	LockBit 3.0 actors obtain and abuse credentials of existing accounts as a means of gaining inital access.
Exploit External Remote Services	T1133	LockBit 3.0 actors exploit RDP to gain access to victim networks.
Drive-by Compromise	T1189	LockBit 3.0 actors gain access to a system through a user visiting a website over the normal course of browsing.
Exploit Public-Facing Application	T1190	LockBit 3.0 actors exploit vulnerabilities in internet-facing systems to gain access to victims’ systems.
Phishing	T1566	LockBit 3.0 actors use phishing and spearphishing to gain access to victims’ networks.

Figure from #StopRansomware: LockBit 3.0 Cyber Security advisory.

In addition if you would like to learn about the history and evolution of ransomware you could click here.

State Sponsored APT Activities

APT (Advanced Persistent Threat) groups are groups of threat actors aiming to carry out a specific nation's malicious intentions.APT groups are generally not financially motivated, their main targets mostly include governmental organizations and critical infrastructures.

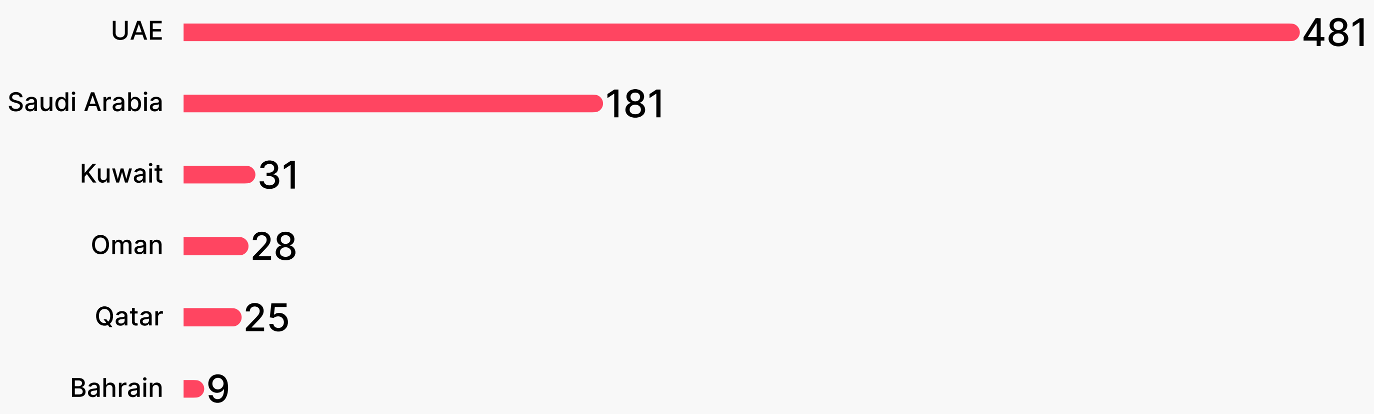
Significant APT groups targeting GCC organizations

- MuddyWater
- CHRYSENE
- Turla Group
- Leviathan
- Naikon
- HAZY TIGER
- El Machete
- MAGNALLIUM
- RAZOR TIGER
- Infy

Phishing Threats

Within our time scope, SOCRadar's Phishing Radar detected almost 600.000 potential phishing domains, but only 755 of them were targeting the enterprises in GCC region.

As seen in the graph below, most domains were aiming the United Arab Emirates and the Kingdom of Saudi Arabia.

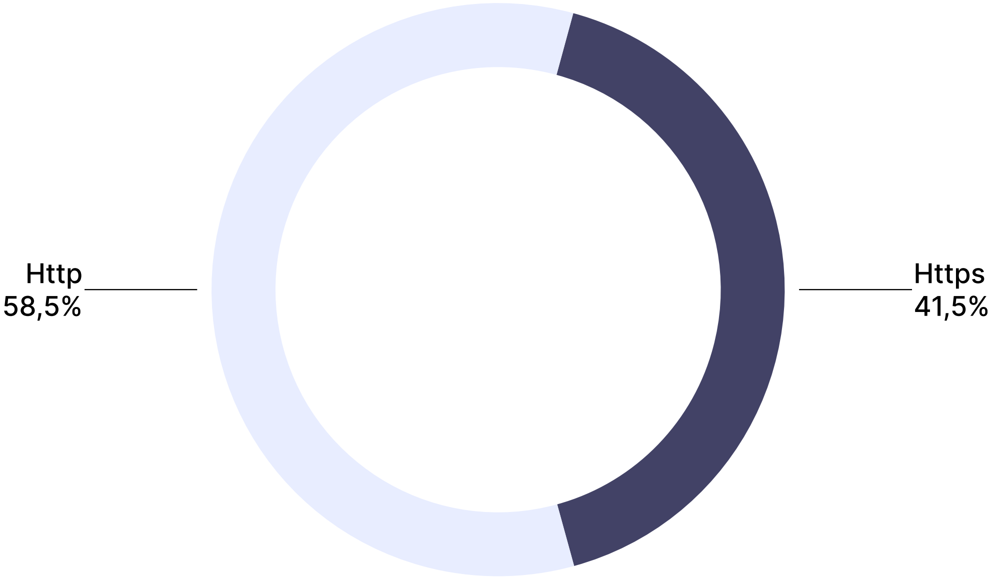


Phishing Threats – Number of Attacks to Each GCC Country

Phishing Threats

When we look at the ASN (Autonomous System Number), 75% of them could not be determined but we see that almost 11% of the sites were geolocated in US and 5.4% in Cyprus and 2.3% in Great Britain. Similarly, we only have a limited information (14.3% of the total) about the industry of the impersonating domains target. However, the finance industry with %35.2 was the most targeted industry of the remaining domains which we could discern the industry.

The graph below shows us that even if a website communicates with HTTPS protocol, the chances of it being a phishing scam do not evaporate. People should always be careful about potential phishing attacks. The fact that almost 60% of the phishing websites were hosted on HTTPS domains using a valid SSL certificate shows us that the threat actors are increasingly using HTTPS to trick users into falling into their phishing traps.



Phishing Threats – Categorized by SSL/TLS Protocol

An Inherent Weakness: Critical Infrastructures in GCC

One of the most devastating cyberattacks on critical infrastructure was the Colonial Pipeline attack in the United States in May 2021. This attack caused chaos nationwide and was considered a national security threat affecting consumers, airlines, and public transportation. The Colonial Pipeline attack has once again demonstrated how cyberattacks against the energy industry and the oil and gas industry (ONG) could affect social order or cause widespread damage.

The oil and gas industry plays an essential role in the prosperity and growth of Gulf Cooperation Council (GCC) countries due to their oil-based economies. Therefore, it is both an important target for cyber attacks against GCC countries, and it makes GCC countries a prime target for cyber attacks against the oil and gas industry.

The “Nigth Dragon” campaign and “Troja.Laziyak” malware attacks against the energy industry globally have also seriously affected the GCC countries. On the other hand, significant cyber attacks have also occurred, directly targeting the Gulf countries' ONG industry and critical infrastructures. Saudi Aramco, one of the world's largest energy companies, was hit by a disk-wiping malware, Shamoon, in 2012.

The Shamoon resulted in the complete or partial destruction of more than 30,000 computers, significantly affecting the company's supply chain, transportation, and contracts. The attack not only demonstrated the potential for cyberattacks to cause significant damage to critical infrastructure and industrial control systems, but it also had an impact on global energy markets by causing a temporary drop in oil supply and raising concerns about the potential for cyber attacks to disrupt global supply chains and trade. In 2012, the RasGas liquefied natural gas (LNG) producing company in Qatar was the target of a wiper malware attack. In August 2017, Triton (a.k.a Trisis) malware was detected in the industrial control systems of Petro Rabigh, a Saudi petrochemical company.

No significant attacks on critical infrastructures in GCC countries were detected within the time scope of this report. However, threat actors pose a major risk to the ONG industry of the GCC region. The region contains attractive facilities for threat actors, like:

- **Ghawar, one of the largest onshore oil fields globally**
- **Safaniyah, the world's largest offshore oil field**
- **Abqaiq, the world's largest oil processing plant and crude oil stabilization facility with a daily capacity of more than 7 million barrels (bpd)**
- **Ras Tanura, the world's largest offshore oil export port**

A possible cyber-attack with devastating consequences on the region could adversely affect the global oil market considering the potential of decreased supply because of the Russia- Ukraine War.

On the other hand, renewable natural water resources are scarce in the region, and water desalination is vital to obtain drinking water. Gulf countries host approximately 40% of the world's total desalination plants. The world's largest desalination plant, Ras al-Khair, is also in the region. Cyber attacks pose a risk for also Water and Wastewater Systems (WWS) as a critical infrastructure. In addition, WWS is dependent on the ONG sector as an energy source, and the ONG interruption to be experienced will adversely affect the functioning of the water system.

Cyber Resilience in the Countries of Gulf Cooperation Council (GCC)

The GCC countries have made significant strides in developing their cybersecurity capabilities in recent years. The region has seen a rise in cyber threats and attacks, leading to increased investments in cybersecurity infrastructure and capacity building. GCC countries have established cybersecurity agencies and have implemented cybersecurity regulations and standards to protect critical infrastructure and sensitive data. For example, the UAE has implemented the Dubai Cyber Security Strategy, which aims to enhance cybersecurity and establish Dubai as a global leader in cybersecurity. Saudi Arabia has also implemented its Cybersecurity Strategy, which aims to strengthen cybersecurity across all sectors, including government, industry, and critical infrastructure.

In addition to government efforts, many GCC countries have also invested in developing local cybersecurity talent and fostering partnerships with international organizations to enhance their cybersecurity capabilities. However, cyber threats are constantly evolving, and it is essential for GCC countries to continue to invest in their cybersecurity infrastructure and capacity building efforts to maintain cyber resilience.

A good example of the regulations in the region is that the Saudi Arabian Monetary Authority (SAMA) has developed a Cybersecurity Framework (CSF) for Banks and Financial Institutions based on international best practices and standards. In March 2022, SAMA announced the Cyber Threat Intelligence (CTI) Principles as part of the CSF. This framework provides resilience to cyberattacks and raises awareness of the need for cyber threat intelligence. As a result of this development, implementing CTI principles has become a requirement for Saudi financial institutions to achieve SAMA Cybersecurity Framework Compliance. SAMA member organizations can benefit from extended threat intelligence solutions like SOCRadar to successfully execute the SAMA CTI principles, allowing them to improve their security perceptions. We are providing a SOCRadar & SAMA CTI principles compliance chart at the end of this report which shows how SOCRadar assists SAMA member organizations to achieve in implementing SAMA CTI principles.

Here, you can see the SAMA principles and how SOCRadar satisfies them:

SAMA CTI & SOCRadar Compatibility

Core Cyber Threat Intelligence Principles		SOCRadar Compatibility	
Principle 1: Define roles and responsibilities	Member Organizations should define roles and responsibilities within the organization to produce threat intelligence with their own CTI capability. This includes a dedicated CTI team. CTI team should be supported by skilled resources with **purpose-specific advanced tools.**	SOCRadar provides a thorough CTI solution that enables organizations to identify and mitigate threats across the surface, deep, and dark web. SOCRadar delivers the actionable and timely intelligence context organizations need to support financial services with its external attack surface management, digital risk protection, and threat intelligence capabilities modules. Thanks to SOCRadar's automated and unique Web Recon technology with a dedicated analyst team, SOCRadar enables SOC teams to take control of the outer world beyond their perimeters and aims to understand the threat landscape better.	**SOCRadar fully supports the organization as a technology partner.**
Principle 2: Define threat intelligence planning and collection requirements	Principle 2 requires organizations to define their intelligence objectives. Member organizations should consider different areas of analysis relevant to their business priorities (e.g., technology, threat actors, etc.).	SOCRadar generates intelligence at different CTI levels and ensures the best use of information by categorizing under different areas such as industry, threat actors, and technology compatible with Annex B. Areas of Analysis of SAMA CTI Principles. SOCRadar can be utilized to receive purpose-specific intelligence from infrastructure visibility to dark web events.	**SOCRadar fully supports the Organization as a technology partner.**
Principle 3: Select and validate relevant sources	Member Organizations should select sources that provide information that is relevant to their business and in line with the threat intelligence requirements defined.	SOCRadar brings its users the most relevant threat intelligence and cybersecurity news and provides searchable data. The ThreatShare module enables users to subscribe to security bulletins, vendor sites, blogs, credible RSS, Twitter, and Telegram channels. The Threat Reports module features the latest cyber security reports as classified and sorted.	**SOCRadar fully supports the Organization as a technology partner.**

Core Cyber Threat Intelligence Principles		SOCRadar Compatibility	
Principle 4: Collect data through intelligence sources	Member Organizations should **collect data via various intelligence sources** (e.g. OSINT, TECHINT, SOCMINT, HUMINT and deep web and dark web intelligence).	SOCRadar automatically scraps black markets and dark web forums that are not visible to regular users. Intelligence from hacker chatters, deep web forums, social media, communication channels such as Telegram, ICQ, IRC, etc., and ransomware groups' websites are gathered in ThreatShare, including screenshots and texts. SOCRadar takes the burden off SOC team for manual intelligence/OSINT scanning by performing the scans automatically.	**SOCRadar fully supports the Organization as a technology partner.**
Principle 5: Define specific standard operating procedures (SOPs)	Member Organizations should **define specific standard operating procedures (SOPs) when conducting specific types of intelligence .**	SOCRadar helps CTI teams by performing deep and dark web intelligence on their behalf defined by Intelligence Standard Operating Procedures. A large team of analysts examines the data and converts information into intelligence. This provides no-huss no-fuss searchable data for its users and keeps them up-to-date about trending threats.	**SOCRadar fully supports the Organization as a technology partner.**
Principle 6: Process and classify information	Member Organizations should **process and classify collected intelligence** - either manually, automatically, or a combination of the two - from the selected sources and store it securely.	The collected intelligence is automatically labeled on the SOCRadar platform. Its smart tagging feature allows users to filter the results based on the country, industry, attack type, and content.	**SOCRadar fully supports the Organization as a technology partner.**
Principle 7: Analyze information	Member Organizations should apply a variety of quantitative and qualitative **analytical techniques to analyze the importance and implications of the processed information,** and, in turn, produce actionable intelligence.	SOCRadar automatically processes and correlates intelligence for its customers. It combines automation with human power as well. Before the intelligence is presented to the customer, it is checked by analysts to eliminate false positives. Human analysts turn the findings into actionable intelligence that customers can act upon.	**SOCRadar fully supports the Organization as a technology partner.**

Core Cyber Threat Intelligence Principles		SOCRadar Compatibility	
Principle 8: Share intelligence	The Member Organization's threat intelligence team should **share relevant intelligence with other relevant departments** such as the Security Operations Center (SOC), IT, etc.	SOCRadar users can share curated intelligence in various ways. CTI Teams can share critical intelligence with other departments over the SOCRadar platform manually. The platform can be customized to share specific threat intelligence automatically with different teams by e-mail. Curated intelligence can be shared over security incident and event management (SIEM) tools, team management apps, and ticketing system.	**SOCRadar fully supports the Organization as a technology partner.**
Principle 9: Deliver actionable threat intelligence	Member Organizations should **take relevant mitigation actions or measures to improve defense infrastructure based on threat intelligence produced** and their knowledge of relevant threats.	SOCRadar delivers actionable intelligence for current threats in real time. Using its unparalleled reconnaissance capacities and actionable and timely intelligence context, SOCRadar users can take relevant measures to secure their organization proactively.	**SOCRadar fully supports the Organization as a technology partner.**
Principle 10: Continuously improve methods of intelligence	This principle requires member organizations to consider the services of a dedicated threat intelligence provider, who can offer relevant insights to complement the organization's existing understanding of threats.	Recognized by Gartner as a Threat Intelligence Representative Vendor, SOCRadar is a unique Extended Cyber Threat Intelligence solution combining external attack surface and digital risk protection with cyber threat intelligence. Prioritized, up-to-date, and relevant cyber threat intelligence empowers its customers to take actions starting from the reconnaissance stage of the cyberattack life cycle.	**SOCRadar fully supports the Organization as a technology partner.**
Principle 11: Integrate CTI	This principle requires Member Organizations to integrate CTI in situational awareness and red teaming assessments to validate the organisation's security posture.	With intelligence from dark web forums and hacker channels, IoCs, digital asset discovery, SOCRadar supports the establishment of a solid security posture for the known techniques, tactics, and procedures (TTPs) of threat actors. SOC teams, threat intelligence analysts, and incident response teams can integrate SOCRadar intelligence with SIEM and SOAR platforms to improve their organization's security posture.	**SOCRadar fully supports the Organization as a technology partner.**

Core Cyber Threat Intelligence Principles		SOCRadar Compatibility	
Strategic Cyber Threat Intelligence			
Principle 12: Identify a cyber threat landscape	This principle requires Member Organizations to **identify the cyber threat landscape relevant to their organization** and operations, with information on **identified vulnerable assets,** threats, risks, threat actors, and observed trends.	SOCRadar alerts the company when a vulnerability related to the Organization is published. Based on the products and technologies auto-discovered in the Organization's external-facing digital assets, aggregated intelligence together with the information on vulnerable assets and estimated risk score is presented automatically.	**SOCRadar fully supports the Organization as a technology partner.**
Principle 13: Identify strategic cyber-attack scenarios	This principle requires Member Organizations to **identify the strategic cyber attack scenarios** and perform an assessment of the identified scenarios to prioritize the most likely and impactful scenarios.	SOCRadar enables security decision-makers (CISOs) to understand the risks posed to their organizations through attack-surface-centric and industry-specific reports. With tactical intelligence from known techniques, tactics, and procedures (TTPs) of threat actors and technical intelligence from dark web forums, hacker channels, and IoCs, SOCRadar assists CISOs in creating realistic attack scenarios.	**SOCRadar fully supports the Organization as a technology partner.**
Principle 14: Elaborate Requests for Information (RFIs) and Tailored Threat Assessments	This principle requires Member Organizations to **provide, upon request, detailed information (e.g. cyber threats, trends, events, and malware or tools) related to possible cyber attacks that could target them.** The principle holds the CISO of the Member Organization responsible for validating the quality and relevance of this information.	SOCRadar supports CISOs in improving their investigation through IOC enrichments. CISOs can benefit from SOCRadar's curated intelligence on real-time dark web monitoring, past leaks, phishing domains, and SSL/TLS grades related to their organizations. Armed with this information, CISOs always remain vigilant in understanding the risks posed to their organizations and elaborating information when requested.	**SOCRadar fully supports the Organization as a technology partner.**

Core Cyber Threat Intelligence Principles		SOCRadar Compatibility	
Operational Cyber Threat Intelligence			
Principle 15: Define the attack chain	This principle requires Member Organizations to define the **various phases of an attack performed by the threat actors based on industrial standards or frameworks such as MITRE.**	SOC teams can use SOCRadar for high visibility into the MITRE ATT&CK tactics, techniques, and procedures of the most skilled adversaries for accurate threat detection. SOCRadar covers MITRE ATT&CK's Reconnaissance tactics to prevent any unwanted situation that might occur in the future with its unique scanning system.	**SOCRadar fully supports the Organization as a technology partner.**
Principle 16: Identify TTP	Member Organizations should **analyze the information collected related to relevant threat actors, tools, or malware to identify relevant Techniques, Tactics, and Procedures (TTPs).** Member Organizations should also rely on Indicators of Compromise (IoCs) for the identification of these TTPs.	SOCRadar keeps track of cybersecurity incidents and informs organizations about attackers through industry-specific reports. SOCRadar supports SOC teams in getting trends about threat actors' TTPs that can be used with the MITRE ATT&CK framework. Cybersecurity professionals can customize the feeds and stay up-to-date with recent threats, search for indicators-of-compromise (IoCs), and integrate with the company systems with TAXII protocol.	**SOCRadar fully supports the Organization as a technology partner.**
Principle 17: Identify malware and tools	Member Organizations should **identify malware and tools during an attack.** Member Organizations can obtain information regarding the different types of malware and tools used by the threat actors using different sources, such as Indicators of Compromises (IoCs), dark web, deep web, OSINT, code repositories, information sharing platforms, etc.	SOCRadar continuously monitors the common forums, source code repositories, and information sharing platforms and provides information about botnets, malware, data dumps, exploits, and hacking as-a-service. Malware's IOCs such as their hash signatures or command and control IPs can be searched through the platform to aggregate the intelligence.	**SOCRadar fully supports the Organization as a technology partner.**

Core Cyber Threat Intelligence Principles		SOCRadar Compatibility	
Operational Cyber Threat Intelligence			
Principle 18: Collect IoCs	Member Organizations should **identify, collect, and aggregate IoCs** and implement them in their defence infrastructure.	Threat Feed & IoC Management module provides daily threat trends and indicators of the latest malicious incidents. All feeds can be filtered by source or country. In addition to SOCRadar's honey pots, the platform provides 115+ open source & commercial IoC feeds (e.g. vulnerability scanners, DDoS attackers, Botnet C&Cs, APT groups, Log4j scanning IPs). SOCRadar's recommended lists provide a daily supply of around 100,000 up-to-date IoCs. IoC lists are passed through over 43+ million whitelists policies and validation processes to prevent possible false positives.	**SOCRadar fully supports the Organization as a technology partner.**
Principle 19: Monitor and report vulnerabilities	Member Organizations should **constantly monitor announcements of new vulnerabilities discovered,** as well as zero-day vulnerabilities exploited by threat actors. Member Organizations should adopt **a risk-based approach that correlates asset value, the severity of vulnerabilities, and threat actor activity via the use of threat intelligence and analytics to calculate a realistic risk rating.** This rating should be used to prioritize remediation activities.	SOCRadar Vulnerability Intelligence module is a real-time tool for monitoring vulnerabilities and their remediation. It automatically collects data from the NVD database, GitHub repositories, and social media about current vulnerabilities and shows them on a graphical interface by highlighting the latest and critical vulnerabilities. SOCRadar has developed a Vulnerability Risk Score (SVRS) score to assess the real risk associated with the vulnerabilities. SVRS is a combination of many vulnerability Intelligence elements such as Social Media, News, Code Repositories, Dark/Deep Web, attribution with Threat actors, and malware as opposed to quantitative elements in CVSS calculation. SOC teams can make research about vulnerabilities by filtering based on exploitable vulnerabilities, CVSS score, and SOCRadar SVRS score.	**SOCRadar fully supports the Organization as a technology partner.**

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