infomineo
BRAINSHORING SERVICES

Cyber threats and trends landscape

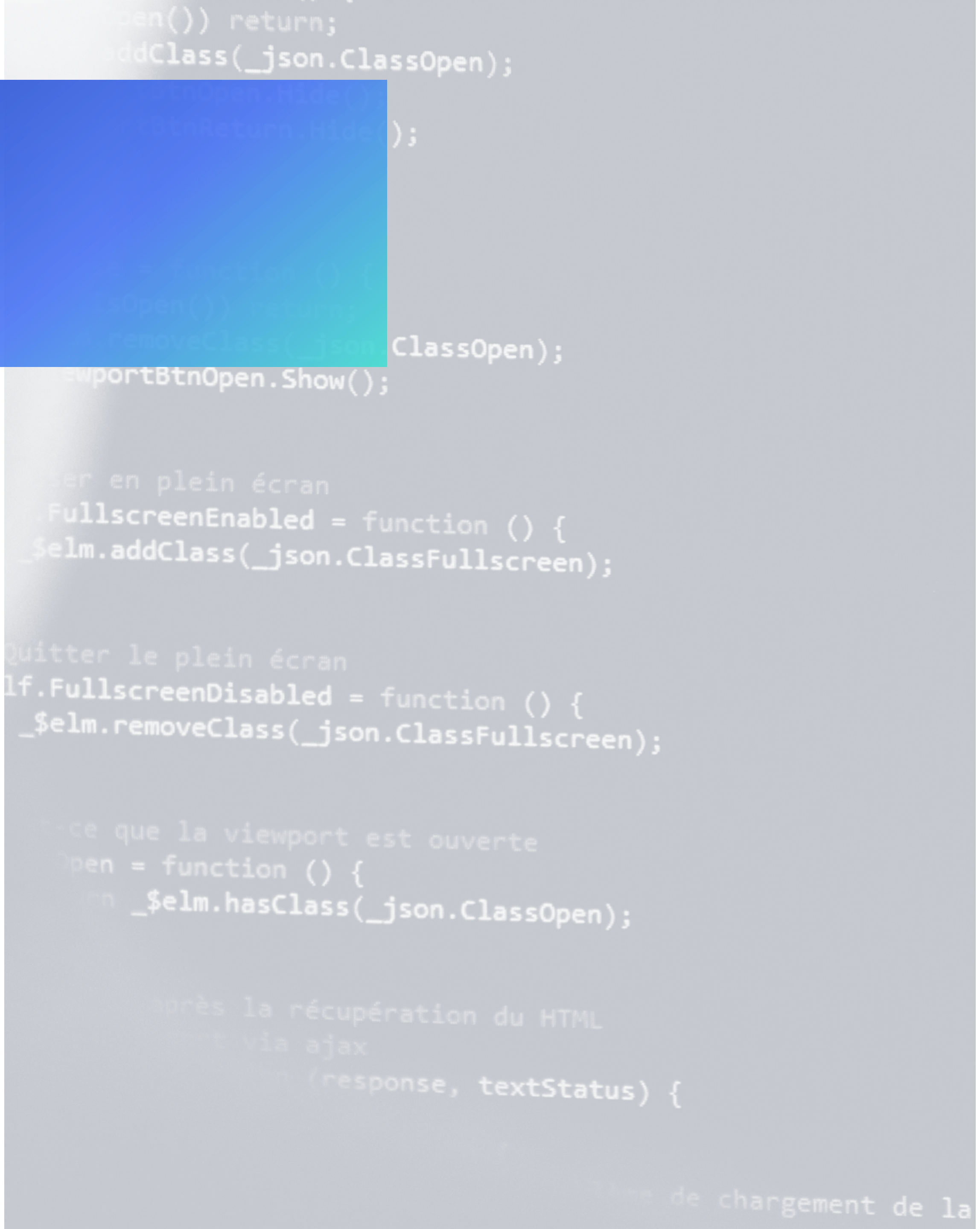
Focus on the GCC

Table of contents

1. **Global Cyber Overview:** highlighting the global cyber threats landscape and trends, and the initiatives to mitigate them

2. **Cyber Threats in GCC:** analyzing cyber threats facing the region and discussing current and potential threat trends

3. **GCC Cybersecurity Efforts:** discussing the initiatives conducted by GCC countries to enhance their cyber resilience



Introduction

In today's interconnected digital landscape, the global community faces **an ever-evolving and complex array of cyber threats, such as ransomware and phishing**. As technology continues to advance, so do the tactics and methods employed by malicious actors seeking **to exploit vulnerabilities for financial gain, political motives, and other nefarious purposes**. From individual users to nations, the omnipresence of cyber threats **demands initiatives in place to counteract them.**

The Gulf Cooperation Council (GCC) is no exception to this trend. As leading oil and gas exporters, GCC countries have cultivated competitive and digitized economies. However, the **pandemic-induced digitalization brought unexpected cyber threats**. Particularly, Saudi Arabia and the UAE witnessed a **surge in cyber attacks**, prompting the countries to take **commendable steps** in establishing regulations, conducting training, and promoting innovative solutions to enhance cybersecurity in the region. However, disparities in cybersecurity readiness remain amidst the rapid digitalization sweeping the region.

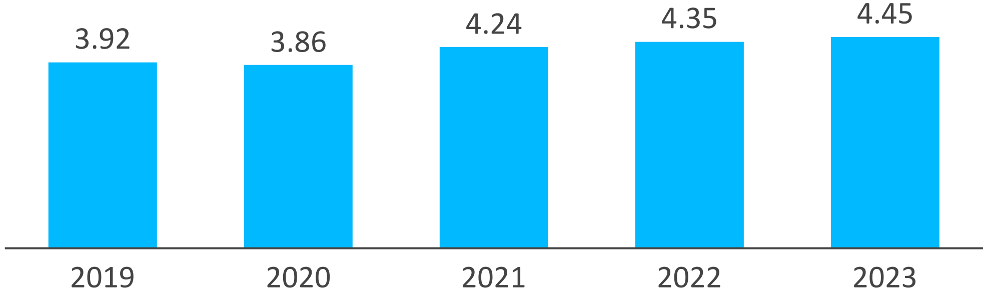
This report starts with a macro-level analysis of global cybersecurity trends, including evolving threat dynamics and examples of global initiatives to enhance cybersecurity. It then focuses on the GCC countries, the cyber threat landscape in the region, projected threat trends, and initiatives to enhance cybersecurity readiness.

Global Cyber Overview

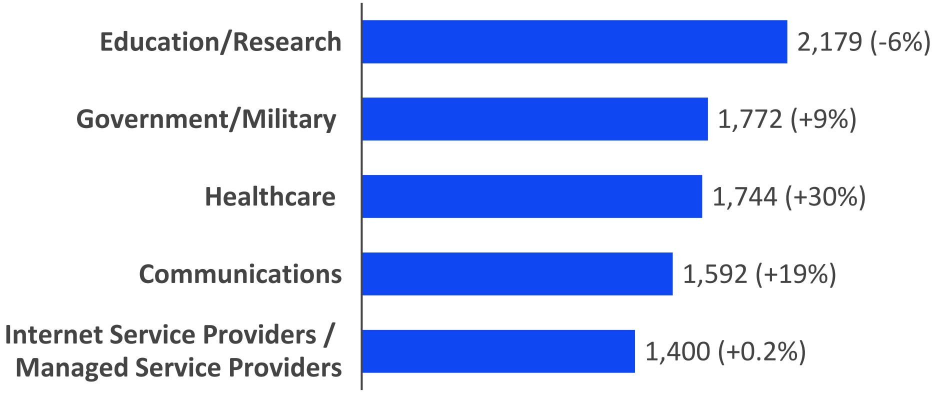
Global cybercrime costs surged to 7.08 trillion USD in 2023, with the average data breach cost reaching USD 4.45 million

- The **global cybercrime costs** reached **USD 7.08T in 2022**, projected to reach USD 13.82T by 2028. **Financial loss, operational disruption, and brand damage** were significant concerns for affected organizations
- Global weekly cyberattacks have spiked in recent years, reaching 1,258 attacks per week per firm
- In Q2 2023, attacks surged across industries, while **the educational and research sector** saw a **6% decrease in attacks** compared to Q2 2022, facing around 2,179 weekly attacks per organization**.** In terms of impact**, Healthcare organizations**' **average breach cost** peaked at **USD 10.93M in 2023**, marking a 53.3% increase in three years since the onset of COVID-19

Average cost of a data breach in Million USD



Global average weekly attacks per organization by industry Q2 2023 (and YoY growth)



Sources: Checkpoint Research "2023 Cyber Security Report" (2023) and "Average Weekly Global Cyberattacks" (2023, Deloitte Insights "Cybersecurity threats and incidents differ by region" (2023), IBM Security "Cost of a Data Breach Report" (2023), Statista, Press search

Cyber threats are increasingly becoming more frequent and sophisticated, posing heightened risks to organizations of all sizes

Expanding Threat Landscape

- **Cyberattacks** are becoming **more sophisticated and frequent, making every company**, regardless of size, **vulnerable** to cyber threats
- The expanding digital ecosystem exposes **brand reputation, revenue pipelines, and critical operations to potential breaches**

The Impact of AI and ML on Cybersecurity

- While **AI** enhances cyber defense, **it's also a tool for hackers,** as shown by the rise of AI-driven deep fakes and bots
- Adversarial nations and cybercriminals are **employing AI and ML to exploit vulnerabilities in threat detection models**

Cyber security trends

Rise of Ransomware and Phishing Attacks

- **Ransomware attacks are on the rise**, causing significant disruptions and financial losses to organizations
- **Phishing remains a prevalent method**, with attackers using social engineering and automation tools for successful attacks

Critical Infrastructure Vulnerabilities

- **Geopolitical events**, like the Russia-Ukraine conflict, **highlight vulnerabilities in cyber infrastructure and cause DDoS attacks on websites**
- Critical infrastructure sectors, such as finance and utilities, are at **risk due to outdated systems**

Sources: Forbes, Press Search

Global training efforts to raise cyber security awareness are targeting employees and SMEs

Examples of academies and programs for employees:

UK

The UK's DSIT and SANS Institute launched the second **Upskill in Cyber program, offering free 14-week training to transition professionals into cybersecurity careers**. Over 3,600 applied in 2023, with nearly half being women

Southeast Asia

Launched in February 2022, the **ASEAN Cybersecurity Skilling Programme (ACSP)** is a joint effort by ASEAN Foundation and Microsoft. Through 14 workshops across seven ASEAN nations and in collaboration with 11 local partners, ACSP provides free Introduction to Cybersecurity courses to **30,000 educators, professionals, and youth** via an online module

Training and Raising awareness

Examples of training and coaching for SMEs:

EU

The **'Safe at the office' Online Cybersecurity Course is offered to SMEs during the European Cyber Security Month 2021** by SI-CERT. It covers 4 modules tailored to job roles, providing essential knowledge to protect against cyber attacks

Singapore

In 2021, the CSA introduced a **cybersecurity toolkit** for SME owners. It includes areas such as **cybersecurity leadership, staff education, safeguarding assets** (hardware, software, data), **access security, and enhancing cyber resilience.** The Toolkit offers practical advice and insightful questions to enhance SME owners' cybersecurity practices

Sources: Cyber Security Agency of Singapore (CSA), Association of Southeast Asian Nations (ASEAN), SI-CERT, Press Search

Governments are creating funding opportunities to enhance cybersecurity infrastructure and encourage innovative solutions

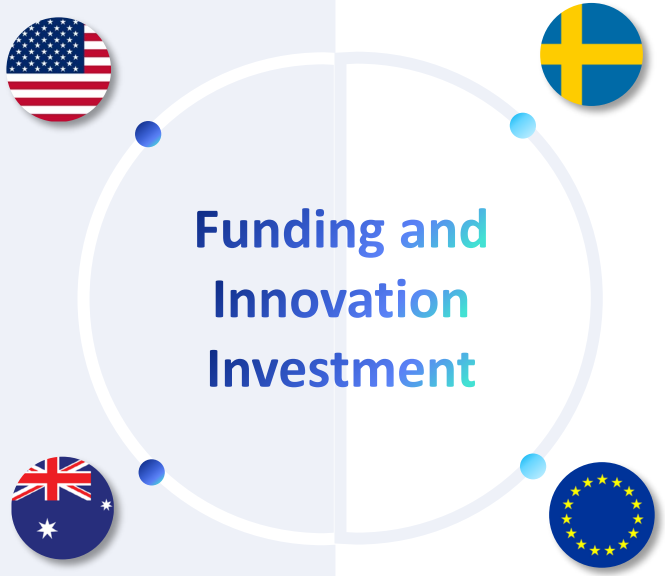
Examples of funds for tools and infrastructure enhancement:

USA

The White House Infrastructure Investment and Jobs Act (IIJA) allocated **around USD 1.2T to nearly 400 programs** in 2021**, supporting U.S. infrastructure**. For cybersecurity reinforcement, the IIJA offers support through direct funding and eligible cybersecurity-related expenditures.

Australia

The Australian Signals Directorate launched **the REDSPICE initiative** in 2022, committing **a record AUD 9.9B over a decade to enhance cyber and intelligence capabilities**. It aims to add 1,900 cyber jobs over the decade to triple its offensive cyber defense, improve cyber infrastructure's resilience, and scale up on cloud-based AI and ML intelligence for improved foundational technologies



Examples of private sector engagement through grants:

Sweden

The **"Cybersecurity for Industrial Advanced Digitalization 2023"** initiative seeks proposals for novel industry cybersecurity solutions, addressing challenges linked to advanced digitalization. **Selected projects can secure funding of SEK 2-10M per project**, covering 50-100% of eligible costs based on organization type. The initiative begins with an **initial budget of SEK 40M**

EU

Supported by Horizon Europe, the NLnet Foundation opened **a call for proposals from ICT professionals for an open, reliable internet.** The foundation is looking for **contributions from troubleshooters to enhance core internet aspects and address security, privacy, and scalability concerns**. Projects can receive a grant of up to EUR 50K

Sources: Australian Signals Directorate, Swedish Innovation Agency Vinnova, Press Search

Cyber Threats in GCC

Info stealing and leakage in dark web posts is one of the most prominent cyber threats targeting the GCC

Dark web threats

Impact

From March 2022 to February 2023, **15,258 dark web posts were detected globally*.** Out of these, **766 were linked to organizations in the Middle East***

By industry

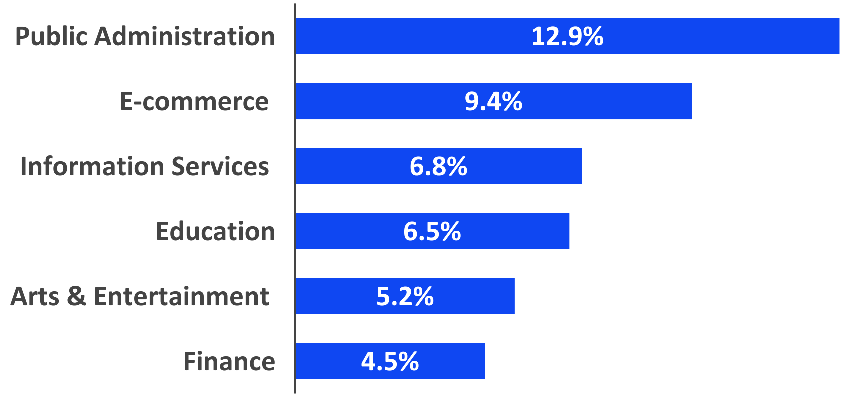
The **Public Administration sector** experienced the highest number of attacks in the GCC region. Interestingly, the **oil and gas industry did not rank among the top** six industries in the dark web data.

By country

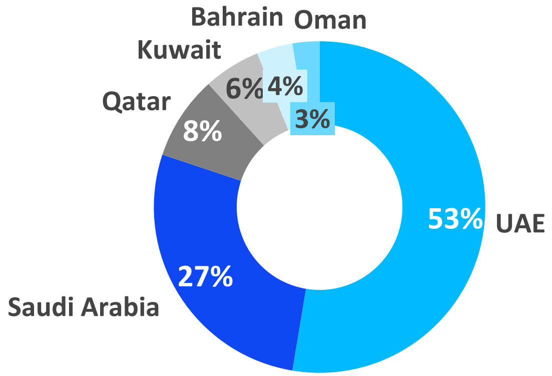
Most **dark web posts** in the GCC region were **related to the UAE**. A new study found that the **most common item in the dark web markets was payment card data,** with the UAE's payment card information cost being the **fifth most expensive globally**, costing twice as much as the world's average.

Reported on October 31st, 2022, a dark web vendor made an offer to **sell stolen databases from the Ministry of Internal Affairs and the Ministry of Education of the UAE**. The databases supposedly contained sensitive data **of 9.5 million foreign residents and 80 million tourists' information.**

Top industries with the highest dark web threats 2022/23



Dark web threats by country 2022/23



* Identified by Socradar

Sources: Socradar "GULF COOPERATION COUNCIL (GCC) COUNTRIES" (2023), NordVPN, Press Search

The GCC has been significantly targeted by ransomware attacks, with organizations in Saudi Arabia and the UAE being most affected

Ransomware threats

Impact

Between March 2022 and February 2023, 2,677 ransomware incidents were identified globally*. Out of these incidents, **47 targeted organizations within the GCC region***

By industry

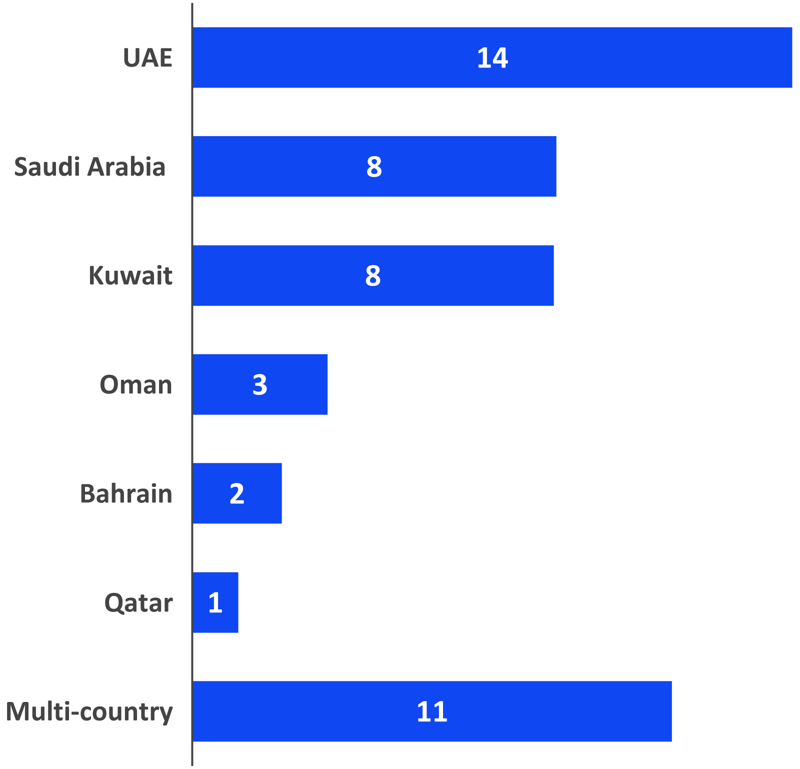
Manufacturing companies were the most targeted by ransomware attacks in 2022/23 in the GCC region (14.9%). Compared to global averages**, the Retail (6.4%) and Accommodation & Food Service (8.5%) industries experienced higher** attack rates in the region, which could be linked to major events like **World Cup 22 and pilgrimage season.**

By country

Most **ransomware in the GCC region was related to organizations in the UAE**. In 2021, UAE firms were found to have paid **USD 1.4 million in ransomware over 2 years,** with 42% halting operations post-attack.

On March 16th, 2023, the FBI, CISA, and MS-ISAC jointly released a **Cyber Security Advisory called "#StopRansomware: LockBit 3.0“,** warning about the Ransomware-as-a-Service model of LockBit 3.0.

Ransomware threats by country 2022/23



* Identified by Socradar

Sources: Socradar “GULF COOPERATION COUNCIL (GCC) COUNTRIES” (2023), Press Search

Phishing attacks are on the rise in the GCC, with the financial industry being heavily targeted

Phishing threats

Impact

From March 2022 to February 2023, close to 600K potential phishing domains were detected*, out of which **only 755 targeted enterprises in the GCC region***

By industry

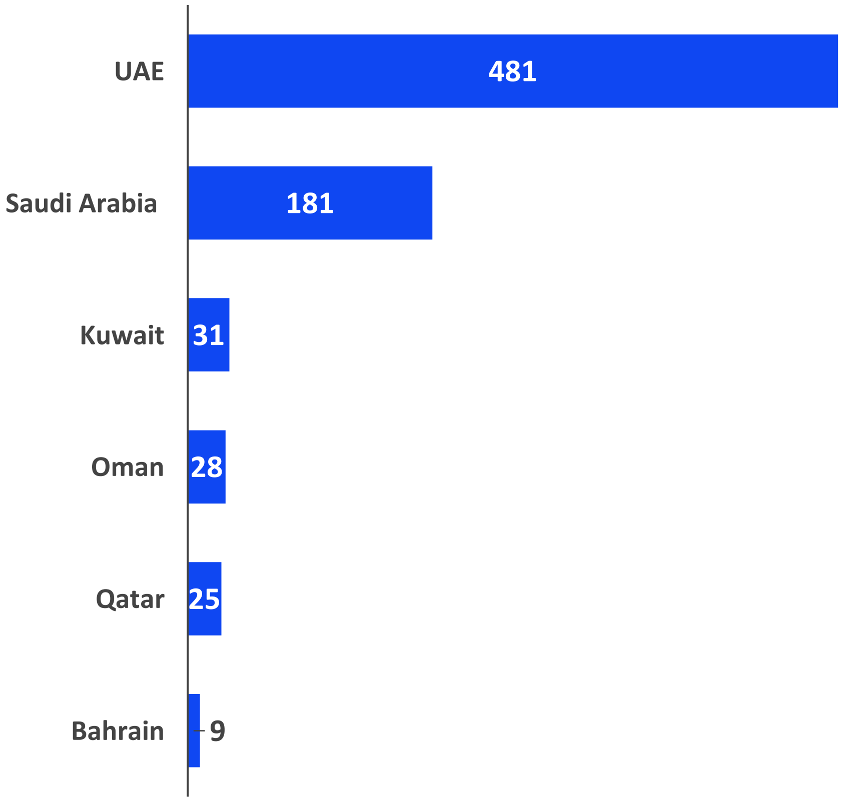
Limited information was available regarding the targeted industries. Nonetheless, **the finance industry was the most heavily targeted**, comprising 35.2% of the available data

By country

Most phishing attacks were directed at the UAE (64%) and Saudi Arabia (24%). Of the UAE's targeted organizations, **86% faced successful email phishing, and 44% incurred financial losses**

Email-based phishing attacks in the Middle East have doubled in October ahead of the World Cup in Qatar, with cybercriminals impersonating FIFA help desks and ticketing offices and using credential harvesting and data exfiltration

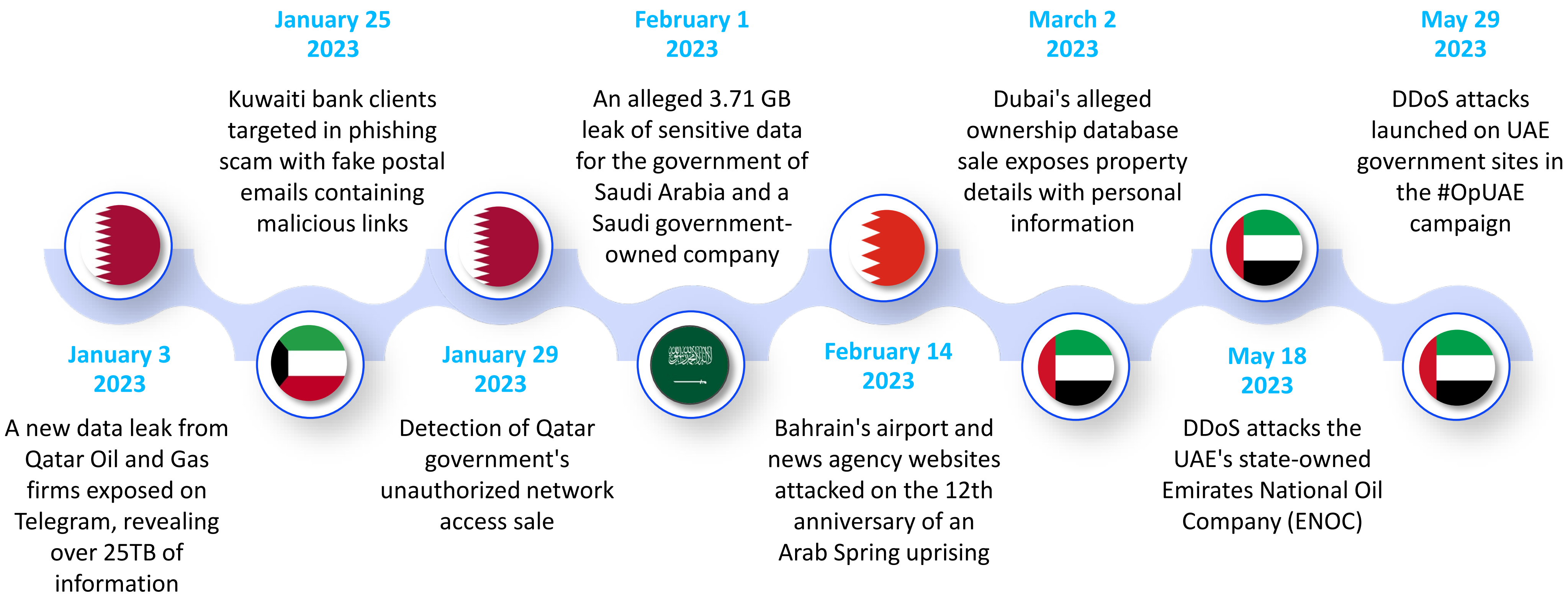
Phishing threats by country 2022/23



* Identified by Socradar

Sources: Socradar "GULF COOPERATION COUNCIL (GCC) COUNTRIES" (2023), Press Search

Notable GCC cyberattacks in the first half of 2023 aimed at stealing information from government and influential companies



January 3 2023

A new data leak from Qatar Oil and Gas firms exposed on Telegram, revealing over 25TB of information

January 25 2023

Kuwaiti bank clients targeted in phishing scam with fake postal emails containing malicious links

January 29 2023

Detection of Qatar government's unauthorized network access sale

February 1 2023

An alleged 3.71 GB leak of sensitive data for the government of Saudi Arabia and a Saudi government-owned company

February 14 2023

Bahrain's airport and news agency websites attacked on the 12th anniversary of an Arab Spring uprising

March 2 2023

Dubai's alleged ownership database sale exposes property details with personal information

May 18 2023

DDoS attacks the UAE's state-owned Emirates National Oil Company (ENOC)

May 29 2023

DDoS attacks launched on UAE government sites in the #OpUAE campaign

Sources: Socradar, Press Search

Trojan banking, APT, and crypto crime threats are rising in the GCC, while mobile malware threats are declining

Cyber Threat Trends in GCC

Crypto Crime

- The crypto market in the GCC is facing an increase in scams and illicit fund transfers
- Since November 2021, Binance, a major exchange platform, has been aiding law enforcement agencies in tracking illicit funds

Trojan Banking

- **A global rise in Trojan banking attacks** was observed in Q1 2023
- **Trojan banking attacks have also increased in the GCC**, with Kuwait experiencing the highest YoY growth (218%)

Advanced persistent threat (APT)

- **GCC's rapid digitization attracts APT groups** like MuddyWater, CHRYSENE, and Turla
- **Government institutions, diplomatic agencies, and key industries** face persistent cyber threats that require strong defenses and intelligence sharing

Mobile malware

- Mobile malware attacks in most GCC countries **notably dropped in 2021,** with Qatar seeing the largest decrease. However, **Saudi Arabia saw a 19% increase**
- This aligns with a global trend where cybercriminals prioritize complex threats that conventional security solutions may struggle to counter effectively

Sources: Kaspersky, Binance, Press Search

Meanwhile, the increasing use of Gen AI, IOT, super apps, and cloud technologies could lead to the emergence of new cyber threats

Increasing Utilization of Generative AI in the Public Sector

- The public sector is actively **embracing generative AI to empower smart government in the GCC** region, as highlighted by the recent investments in AI
- Existing chatbots like Dubai's "**Rashid" are already in use by regional governments**

Embracing Super Apps as Essential Government Tools

- **Super apps** are increasing in the **GCC's public sector,** with significant success observed
- **The Dubai Now government app** has processed **20 million transactions** worth USD 2.7 billion since its launch
- **Global prediction:** Over 50% daily users of multiple super apps by 2027

Harnessing IoT to Revolutionize the Mega-Events Industry

- **IoT is revolutionizing GCC mega-event management** through wireless sensors, drones, and AI. These technologies enable dynamic crowd response and attendee safety
- **In the FIFA World Cup in Qatar,** "digital twins" and 40,000 IoT devices were used to efficiently manage large stadium crowds

GCC's Intensified Focus on Cloud Infrastructure

- **National digital transformations** and **increased security efforts** propel swift **advances in cloud maturity**
- **Saudi Arabia's cloud market** is projected to exceed **USD 6 billion by 2025**, reflecting substantial dedication

Emerging technology trends in GCC

Sources: Press Search

GCC Cybersecurity Efforts

GCC countries are focusing on providing training to employees and students to raise cyber risk awareness

Examples of student coaching and awareness raising initiatives:

Saudi Arabia

The **CyberIC Fresh Graduates Program,** developed in 2022, seeks to **train and qualify cybersecurity experts in Saudi Arabia**. It focuses on **recent graduates** from local universities with cybersecurity or related degrees, aiming to **enhance the nation's cyber preparedness across government entities**

Qatar

In 2023, the National Cyber Security Agency (NCSA) launched **an awareness campaign for 30 schools, benefiting 3,000 students, teachers, and parents**. This joint initiative **aims to foster cyber excellence and improve digital security education within the school community**

Examples of employee training and education initiatives:

UAE

'Jahiz' is a **digital platform, launched in 2022,** that **boosts UAE government employees with crucial future skills, like cybersecurity, through interactive training.** It prepares the government for the future by enhancing talents with 20 vital skills, helping them stay updated and efficient in a changing world

Saudi Arabia

In 2022, the **"National Program for Cyber Drills"** was introduced with the goal of **training more than 5,000 participants in the initial phase of the program**. This initiative will enhance **the capabilities of various national entities**, making them more resilient against cyber threats and better prepared to respond to such incidents

Sources: Press Search

GCC countries are addressing their cyber vulnerabilities by investing in threat prevention drills and supporting SMEs

Examples of support for cybersecurity SMEs and Startups:

Bahrain

Bahrain's **National Cyber Security Centre** is planning to collaborate with telecom companies in 2023 to **provide cost-effective cybersecurity services** for small businesses, as they are perceived as easy targets by hackers

Saudi Arabia

The National Cybersecurity Authority (NCA) created an accelerator as part of the "CyberIC" program in 2022. It connects **startups with investors** and plans **to support about 40 startups in three years**, **offering over SAR 6.5 million** in funding and 500+ hours of guidance

Funding and other initiatives

Examples of cyber–attack prevention measures:

Kuwait

In 2023, the Kuwaiti National Center for Cybersecurity launched **a platform for data exchange** to **enhance cyber security** among government agencies and to take precautionary measures before any cyber attack occurs

Saudi Arabia

In 2023, the NCA conducted a **"Cybersecurity Drill" during the 2022 Hajj season to enhance the cyber readiness of national authorities. Over 350 officials from 100 organizations** participated across various sectors. The drill **simulated cyber threats in a virtual environment** using the 'Cyber Drill Platform’

Sources: Press Search

International partnerships aimed at bolstering cybersecurity resilience in GCC nations are emerging

Saudi Arabia and the United States of America

- In 2022, **Saudi Arabia's National Cybersecurity Authority** entered a **bilateral accord** with **the US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA)**
- The partnership involves **exchanging intelligence on cybersecurity threats and malicious actors, bolstering collective defense efforts**, and **collaborating on cybersecurity training**, tools, technologies, and effective practices

Qatar and Singapore

- **In 2023, Singapore and Qatar signed multiple MOUs** for business collaboration across sectors, **including cybersecurity**
- Their cybersecurity agencies have **agreed to enhance cooperation by sharing information among computer emergency response teams**
- They'll also exchange insights on securing industrial control systems and operating technology, critical for information infrastructure

United Arab Emirates and Albania

- Following **cyberattacks in 2022 that disrupted its digital infrastructure**, the **UAE joined hands with Albania to sign a cybersecurity agreement**
- This collaboration **secures crucial information networks that oversee entry points, such as ports,** using an exchange of expertise and knowledge
- The necessary analysis for future strategies has been completed, and **all challenges have been presented to partners and specialized agencies**

Kuwait and the United States of America

- In 2023, the U.S. Embassy in Kuwait is working to **bolster cybersecurity cooperation with Kuwait's National Center for Cybersecurity**
- The goal is to **connect American and Kuwaiti cybersecurity experts to strengthen defense against cyber threats** to critical infrastructure, military facilities, and communication networks
- This effort aligns with the U.S. National Cybersecurity Strategy, emphasizing global partnerships and responsible behavior in cyberspace

Sources: Saudi Arabia National Cybersecurity Authority, Press Search

Conclusion

- As cyberthreats continue to rise around the world, **ransomware attacks, phishing attempts, and dark web information thefts** have been increasingly targeting GCC countries, highlighting the importance of cybersecurity. While initiatives have been taken **to establish regulations, conduct training, promote innovative solutions, and collaborate internationally,** the region faces challenges that they must overcome:
  - **Address Awareness Gap**: Cybersecurity training and campaigns targeting employees need to be prioritized to raise awareness and share best practices
  - **Build cybersecurity Frameworks:** While some nations have made notable strides in establishing legal and regulatory frameworks, others still need to reinforce and harmonize their regulations for a unified and strong defense against cyber threats
  - **Develop Information exchange and cooperation:** Effective cybersecurity hinges on robust collaboration and the exchange of information among GCC countries. Notably, in October 2022, the GCC Ministerial Committee for Cybersecurity held a meeting to foster joint cyber efforts
  - **Invest in limiting tech vulnerabilities:** The swift integration of emerging technologies, such as the Internet of Things (IoT), artificial intelligence (AI), and cloud computing, introduces both prospects and security vulnerabilities. It prompts GCC nations to invest in research and innovation to develop proactive security measures
- As the GCC confronts these challenges, the path to a secure cyber environment demands **collaborative efforts, continuous education, adaptable frameworks, and investments in advanced technology**

infomineo

BRAINSHORING SERVICES

www.infomineo.com