SOCRadar®

Threat Landscape Report

UNITED ARAB EMIRATES

March 2022

TABLE OF CONTENTS

EXECUTIVE SUMMARY

As the United Arab Emirates companies became technologically more advanced, threat actors, including notorious APT groups and financially-motivated ransomware gangs, have turned their eye on them.

SOCRadar Threat Landscape Report provides organizations with an understanding of evolving cyber threats relevant to their geographical operating locations to enable security leaders to make better decisions.

The intelligence provided in this report can help plan enterprise-wide security programs, make investment decisions, and define cybersecurity requirements.

The SOCRadar CTIA team leverages SOCRadar's extensive data monitoring, collection, classification, and analysis capabilities while characterizing the threat landscape based on recently observed threat actor activity, malware campaigns, new critical vulnerabilities, and exploits and data gathered from open threat sharing platforms.

SOCRadar CTIA Team performs deep/dark web threat research, HUMINT observations, OSINT research and analyzes information gathered on social media trends, thanks to its unique perspective on cyber incidents to bring you the threat landscape report.

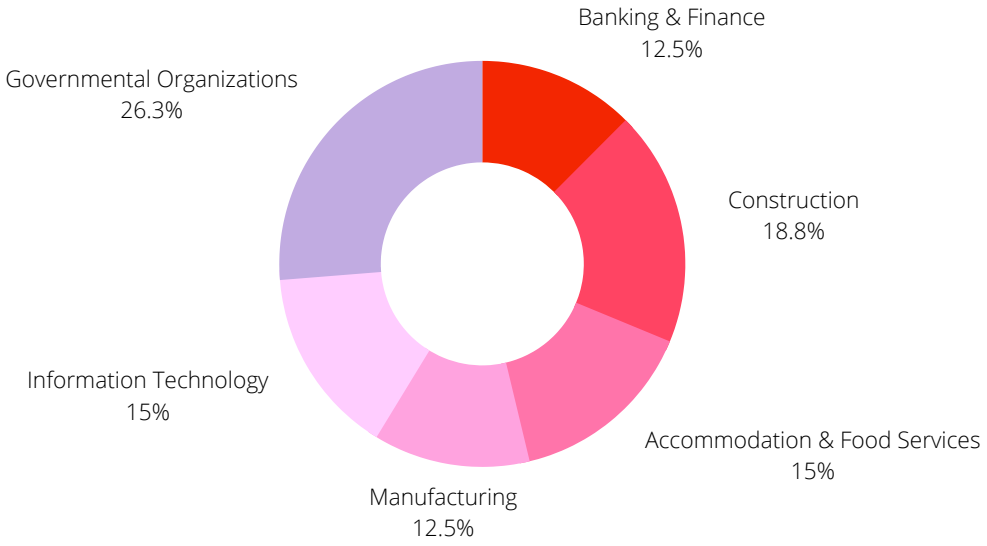
KEY FINDINDS

- **SOCRadar CTIA Team has detected around 200 posts of 57 different threat actors targeting UAE enterprises.**
- **Top ransomware gangs targeting the UAE are "LockBit, Conti, and Snatch".**
- **APT groups from China and Iran have recently targeted leading organizations in the government, information technology, and finance sectors.**
- **SOCRadar has detected 299 phishing attacks targeting the UAE since the beginning of 2021.**
- **In 2021, the most commonly exploited vulnerabilities in the UAE were Microsoft Server Exchange Vulnerabilities.**
- **There are 430K bots for sale for the UAE.**
- **DDoS attacks in 2021 impacted critical emergency services.**

Dark Web Threats

The dark web is the underground central hub where hackers and threat actors frequently communicate. We have analyzed the Dark Web to find trends about target countries and industries, and when it came to the target countries on the Dark Web, the UAE was the runner-up for the top 10 targeted countries.

Over the last 12 months, the SOCRadar CTIA Team has detected around 200 posts of 57 different threat actors targeting UAE enterprises. Most of these posts were customer database sales and unauthorized network access sales of UAE organizations. Thanks to the dataset SOCRadar provides, we also found that government organizations and construction companies were the top two most targeted sectors, followed by accommodation and food services.



The most targeted sectors in the UAE based on DarkMirror Intelligence data

57

Dark web threat actors / aliases

Government

The most targeted vertical

Leaked database

The most common threat category

199

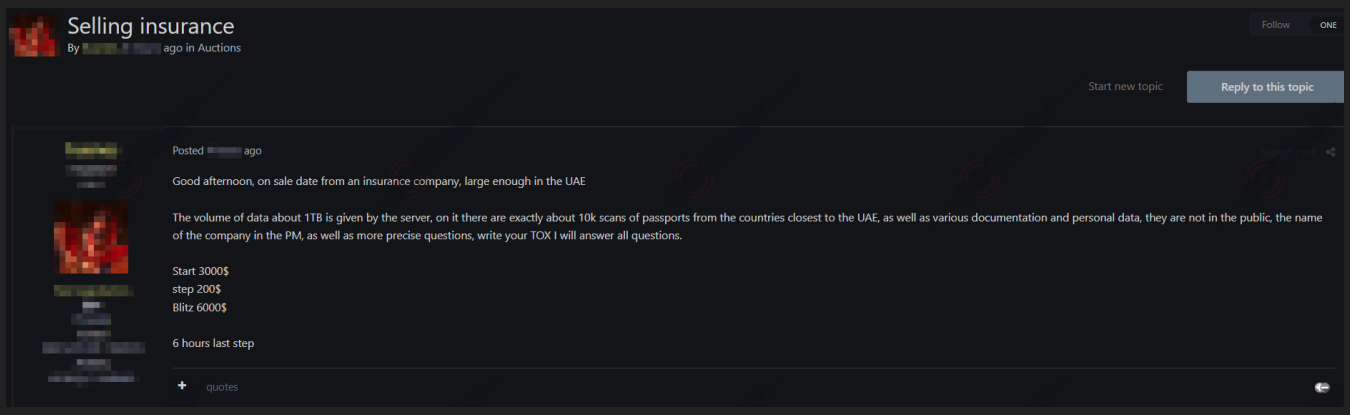
Threat posts over the last year

Major Dark Web Incidents of 2021

Sensitive Data of Ministries of United Arab Emirates are on Sale

On October 31, on a dark web forum tracked by SOCRadar, a vendor attempted to sell stolen databases of the Ministry of Internal Affairs and the Ministry of Education of the United Arab Emirates, allegedly containing sensitive data. The vendor claimed the leaks included sensitive information about 9.5 million foreign residents and 80 million tourists. The vendor did not specify a price for the database.

Database of an Insurance Company Operating in the UAE is on Sale

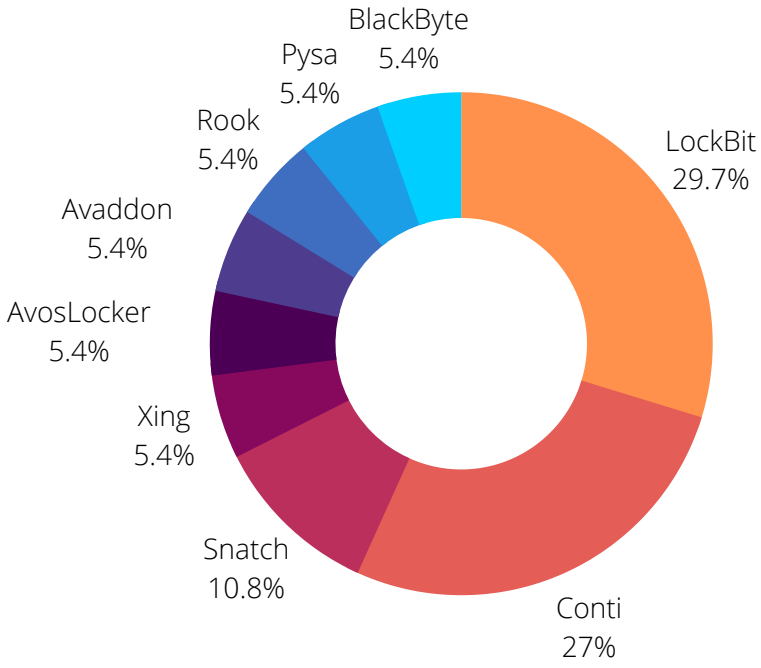


A vendor in a Dark Web underground marketplace monitored by SOCRadar attempted to sell the database of an insurance company operating in the United Arab Emirates on December 13, 2021. The vendor stated that the database contains 1 TB of data, including passport scans and personal data of UAE citizens. The start price for the database was 3000$.

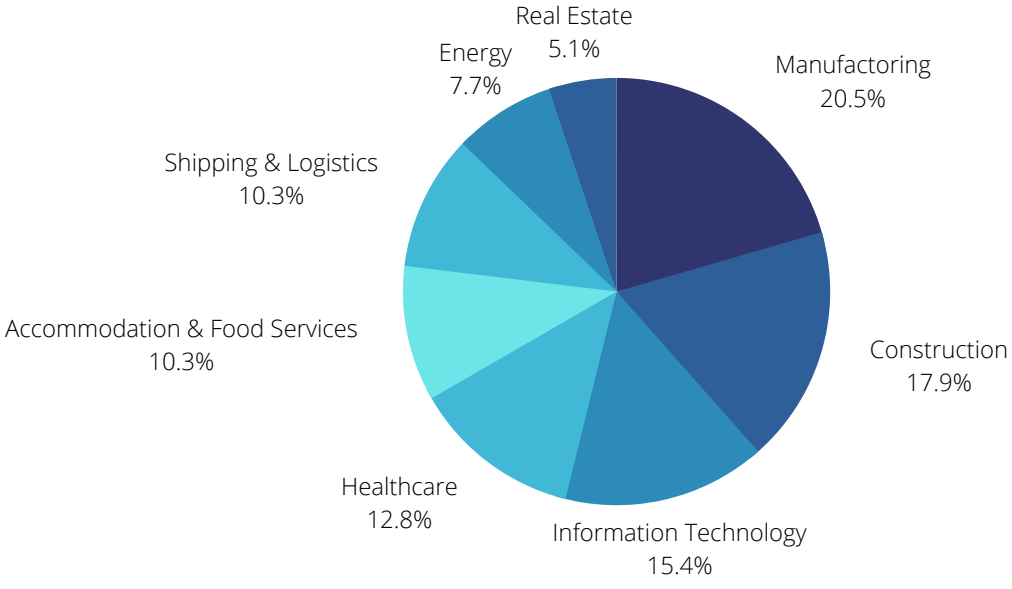
Ransomware Threats

Ransomware attacks have dominated the headlines in 2021. The top 10 ransomware gangs believed to be behind criminal activity had moved about $5.2bn worth of bitcoin over the past three years. As for the United Arab Emirates ransomware, LockBit and Conti were the most active gangs targeting UAE organizations, responsible for more than half of the attacks.

During the last three months of 2021, the rate of increase in ransomware attacks skyrocketed. Some organizations in the UAE have had their share of the rise in ransomware, with major manufacturing and construction companies being hit by ransomware attacks. SOCRadar has also detected data leaks after ransomware attacks in the UAE.



Distribution of ransomware gang activities targeting the UAE organizations in 2021



Most targeted sectors in the UAE by ransomware groups in 2021

Top Ransomware Gangs Targeting United Arab Emirates

LockBit

- Ransomware-as-a-service (RaaS) operator.
- It's one of the best-designed lockers regarding encryption speed and overall functionality.
- Lately, the long list of victims has included Jay Kal General Trading LLC, a company selling hardware materials imported from China, India, and Taiwan.

Conti

- Ransomware-as-a-service (RaaS) operator, operating out of Russia.
- The group has added multiple UAE organizations to their victims' list and allegedly leaked some of their victims' data.
- The source code and inner chat logs of Conti were leaked by a Conti member in February 2022.

Snatch

- First disclosed in December 2019.
- Snatch was an active ransomware group targeting UAE organizations.
- Known for rebooting PCs into safe mode to bypass protection and brute-forcing RDP ports to gain initial access.

State-Sponsored APT Activities

Organizations in the United Arab Emirates continue to be targets of advanced threats with diverse motivations. Specific APT groups from China and Iran have recently targeted leading organizations in the government, information technology, and finance sectors. Reaching the state goals through the collection of strategic intelligence is believed to be the primary motivation of the state-sponsored actors.

Financial gain through the direct theft of funds is another common motivation. Over the last few months, the SOCRadar CTIA team has observed multiple activities reflecting these motivations by continuously collecting data across the surface, deep and dark web sources while tracking 16 APT groups that have targeted the UAE government, military, and private sectors in the past.

Significant APT Groups

APT1
Last activity:
November 13, 2021

APT41
Last activity:
December 27, 2021

MuddyWater
Last activity:
November 25, 2021

APT39
Last activity:
October 12, 2021

Iran-linked MuddyWater APT Group Targets UAE and Kuwait Companies

The APT group MuddyWater has launched a new cyber espionage campaign against two critical countries in the META region: UAE and Kuwait. The specific targets of the campaign were government agencies and ministries. Cybersecurity experts have found that the MuddyWater APT was using two ZIP files, one a report about Arab countries and Israel and the other one about scholarships, as bait to lure users into downloading a file.

The file would force the victim's computer to start the ScreenConnect process, which would let the threat actor gain control. In the campaign, the malicious files were distributed through phishing emails.

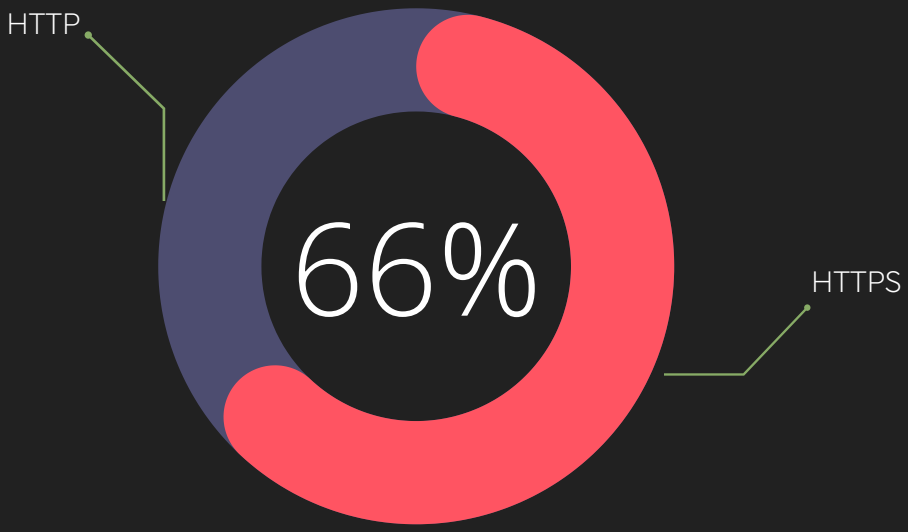
SOCRadar collects Advanced Persistent Threat (APT) IOC Feeds from several public and private sources and sensors. These feeds are free and refreshed daily.

DOWNLOAD

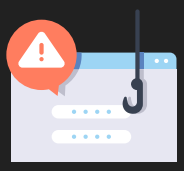
Phishing Threats

Email phishing remains the top attack vector in ransomware attacks targeting UAE. The typical tactic is to deliver malicious macro-enabled Office documents attached to the email or lure users into entering their credentials to a phishing site. The effects can increase dramatically with business email compromise (BEC) scams and social engineering methods.

Attackers are increasingly using https to lure their victims into clicking malicious links



SOCRadar has detected 299 phishing attacks targeting the United Arab Emirates companies since 2021. SOCRadar CTIA team is seeing a phishing-enabled fraud trend targeting critical fast-growing industries, including telecommunication, e-commerce, and healthcare.



299

Total phishing attacks detected over the last 1 year

Microsoft

Top SaaS phishing scheme for credential harvesting

Telecommunication
E-Commerce
Healthcare

Top targeted sectors in the UAE

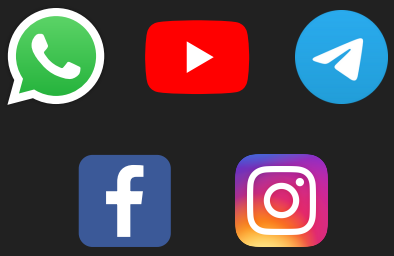
Search On Phishing Radar

Enter your domain

The Digital Industries Commonly Targeted by Phishing Attacks

Common Platforms

Social Media /IM



Cloud / Webmail

Attackers Objective

To distribute malware and steal the social media login credentials of individuals.

To steal the corporate email credentials to gain an initial foothold to the victim's communication channels.

Other Critical Findings

18
Exim Server v4.92

5,180
Open RDP 3389

141
CVE-2014-0160
#Heartbleed

80
CVE-2019-0708
#BlueKeep

Source: SHODAN

Critical Asset Exposures & Vulnerabilities

When SOC analysts, vulnerability management teams, and security leaders have limited time and budget, prioritizing vulnerabilities to reduce the public attack surface becomes paramount. Following is a high-level statistical view of the critical ports and vulnerabilities in the internet-facing infrastructure and technologies.

Ransomware gangs heavily exploit these as they are exposed, but we can still observe them unpatched or exposed to any remote actors. It is highly recommended to check the technologies listed so far for unpatched, critical, exploited vulnerabilities.

Vulnerable Hosts | CVE ID | CVSSv3

The most commonly exploited vulnerabilities in the UAE.

65	Microsoft Exchange Server Unauthenticated Remote Code Execution Vulnerability	CVE-2021-26857 #ProxyLogon	CVSS: 7.8
180	Microsoft Exchange Server Remote Code Execution Vulnerability	CVE-2021-34473 #ProxyShell	CVSS: 9.8
180	Microsoft Exchange Server Elevation of Privilege Vulnerability	CVE-2021-34523	CVSS: 9.8
180	Microsoft Exchange Server Microsoft Exchange Server Security Feature Bypass Vulnerability	CVE-2021-31207	CVSS: 7.2

Credentials Intelligence

Using stolen credentials is one of the most common initial access techniques leveraged by your adversaries. C-level certificates are significantly more helpful for BEC attackers. Last year, SOCRadar detected more than 1 billion exposed credentials by analyzing the breach datasets shared on the deep and dark web forums, which are tied to plain-text passwords.

Password reuse is continuing to be a concern for security professionals. It becomes a bigger problem when it merges with the lack of MFA mechanisms. Ransomware and APT actors continuously seek access to sensitive information, intellectual property, confidential business data through stolen identities.

Stolen Data Intelligence

Along with compromised credentials, stolen data such as keylogger logs, infostealer logs, or database dumps could help adversaries gain the upper hand against innocent companies trying to defend themselves against critical cyberattacks.

The stolen data could include sensitive information such as credit card data, credentials, or even personal information which could be leveraged to carry out social engineering attacks. SOCRadar CTIA team has performed dark web research to assess the current risk situation in the United Arab Emirates. Following are the statistics about the current risk situation of the UAE.

CHECK FOR ACCOUNT BREACH

Enter your domain/email

544
Compromised Credentials for sale | UAE

164
Bots for sale | UAE

430K
Total bots for sale

14586
Stealer Logs for sale | UAE

16945
Data Dumps for sale | UAE

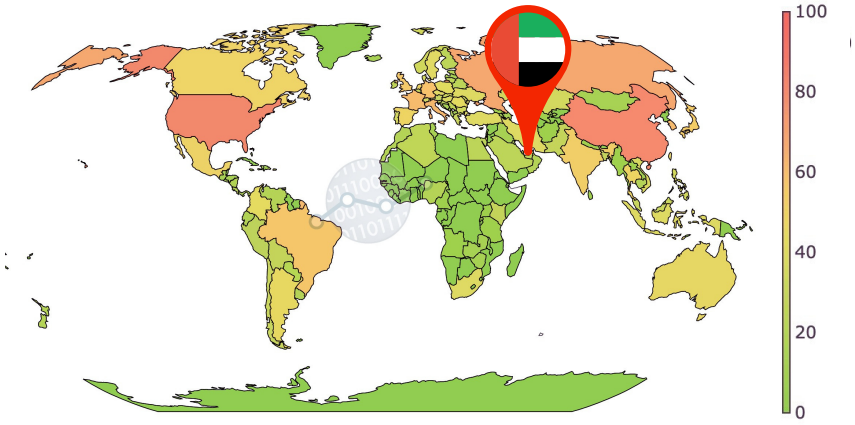
Source: Genesis marketplace

The Genesis Marketplace is a dark web underground avenue for threat actors to buy compromised credentials and stealer malware logs.

DDoS | Risk-to-others

The global internet ecosystem is currently vulnerable and carrying high malicious traffic. Sophisticated threat actors, including ransomware gangs, exploit these potential vectors to amplify disruptive DDoS attacks against organizations, resulting in financial losses and numerous critical service outages worldwide.

Based on the global risk condition dataset provided by Cyber Green Initiative, United Arab Emirates can generate ~8TBit/sec DDoS traffic, which is enough to take down critical businesses for long periods.



Global heatmap view of total potential DDoS bandwidth by country

Data source: CyberGreen

CHECK FOR DoS RESILIENCE

Enter your domain/IP Block

8 TBit/Sec

United Arab Emirates | Total DDoS Potential

10,101
Open Recursive DNS

1,329
Open SNMP

10,807
Open NTP

4,117
Open CHARGEN

1,027
Open SSDP

ABOUT SOCRadar®

SOCRadar platform is an all-in-one solution that provides Extended Threat Intelligence, Digital Risk Protection, and External Attack Surface Management. Its false-positive free platform helps companies proactively defend themselves against cyber incidents. SOCRadar is empowered with robust AI algorithms and a highly talented analyst team; together, they eliminate false positives.

FOLLOW US!

DISCOVER SOCRADAR® FREE EDITION

With SOCRadar® Free Edition, you'll be able to:

- **Discover your unknown hacker-exposed assets**
- **Check if your IP addresses tagged as malicious**
- **Monitor your domain name on hacked websites and phishing databases**
- **Get notified when a critical zero-day vulnerability is disclosed**

TRY FOR FREE

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