Cyber Resilience Report

UAE THREAT LANDSCAPE 2021

Level 15, Aldar HQ
PO BOX 111787

Abu Dhabi,
United Arab Emirates

TABLE OF CONTENTS

EXECUTIVE SUMMARY

01.

The year 2020 has been one of the most challenging in recent memory.

The COVID-19 pandemic altered our lives in many different ways, whether by forcing countries into lockdowns, confining people within their homes or forcing employees to work remotely – even as organisations of all sizes were required to maintain a laser-sharp focus on business continuity. The pandemic accelerated digital transformation trends that were already in motion, highlighting existing flaws and surfacing new digital threats.

Indeed, the pandemic worked as a **force multiplier for existing cyber threats, while giving birth to a new set of threats.** Irrespective of industry sector or location, remote working scenarios engendered new cyber threats, as employees shifted to their personal devices, used inadequate security protections and often did not follow established best practices. In tandem, **threat actors also altered their tactics to target remote workers**, whether by taking advantage of fears and uncertainties occurring as a result of the pandemic or exploiting the new remote working environment. Organisations across the UAE found themselves dealing with these new and varied attacks more frequently than ever before.

Over the course of 2020, Digital14 helped multiple clients to defend their organisations against targeted attacks. For this report, Digital14 evaluated and analysed multiple digital assets within the UAE, enabling analysts to chart an accurate and in-depth understanding of the country's current threat landscape.

The Digital14 analysis revealed the following realities about UAE organisations:

- There are **old vulnerabilities**, published as early as 2000, that have yet to be remediated within organisations' networks. These can easily provide threat actors with an entry point for launching devastating cyberattacks.
- Over 100 vulnerabilities affecting UAE entities have **public exploits** that can be abused by even the most unsophisticated threat actors in order to breach IT and OT environments with minimal effort.
- The most common weaknesses coupled with sensitive environments facilitate **remote code execution**, which provides threat actors with the ability to execute malicious code of their choice within victims' networks.
- **Password reuse** is among the most common weaknesses in UAE organisations.
- The most common incident types are associated with **unauthorised access** and **malicious code**.

The Head of Cybersecurity for the UAE Government, Dr. Mohamed Hamad Al Kuwaiti, stated that 'there is a cyber pandemic, not only a biological pandemic.' [1]

This statement is supported by the findings that in 2020, the UAE witnessed a 250% increase in cyberattacks, specifically an exponential surge in phishing and ransomware.[2]

Digital14's analysis shows that **phishing** remains among the observed top threat vectors in 2020.[3] Following the changes to standard work practices brought about by the pandemic, employees are at a greater risk of exploitation through social engineering, and global threat actors have capitalised on this shift proportionately. **Vulnerability exploitation, the use of previously stolen valid accounts**, and **supply chain attacks** were also identified as the most prominent threat vectors this year.

In summary, Digital14's findings indicate that the **UAE continues to be a constant and attractive target for threat actors**, with **cyberespionage** being the most prominent motive. In particular, **government and critical infrastructure** were among the major sectors attacked over 2020.

Digital14's first UAE Threat Landscape report for 2021 details the **immediate and pressing need for UAE organisations to improve their cyber resilience** by addressing vulnerabilities that could provide threat actors with a welcome avenue for cyberattacks. Organisations in the UAE must also remain cognisant that poor security posture permits even unsophisticated threat actors to easily penetrate their networks using publicly released exploits. As cybersecurity threats evolve to take more innovative forms, traditional approaches will no longer suffice. It isn't enough for organisations to adopt defensive postures, rather, they must look to augmenting their security policies with always-on protection. Traditional perimeter-based network defence, for example, is obsolete. Not only does the perimeter no longer exist in our newly connected environments, but organisations must also recognise that their networks have most likely already been breached.

With the ongoing development and adoption of new technology, organisations in the UAE must adopt a zero-trust architecture and embrace cyber transformation if they are to avoid prohibitive financial and reputational costs over the course of the pandemic and beyond.

02 THREAT TRENDS

In 2018, an industry report found that the UAE is the **second most targeted nation globally for cybercrime,** sustaining **USD1.4bn in annual losses**.[4] Wealthy nation states such as the UAE typically suffer higher cybercrime losses compared to other countries, because threat actors consider such nations as lucrative targets for ransom and other financially driven activities. In addition, the UAE was also a target of hacktivism in 2020 – even though hacktivist activity has been falling since 2016 and hacktivist groups have lost media traction.[5]

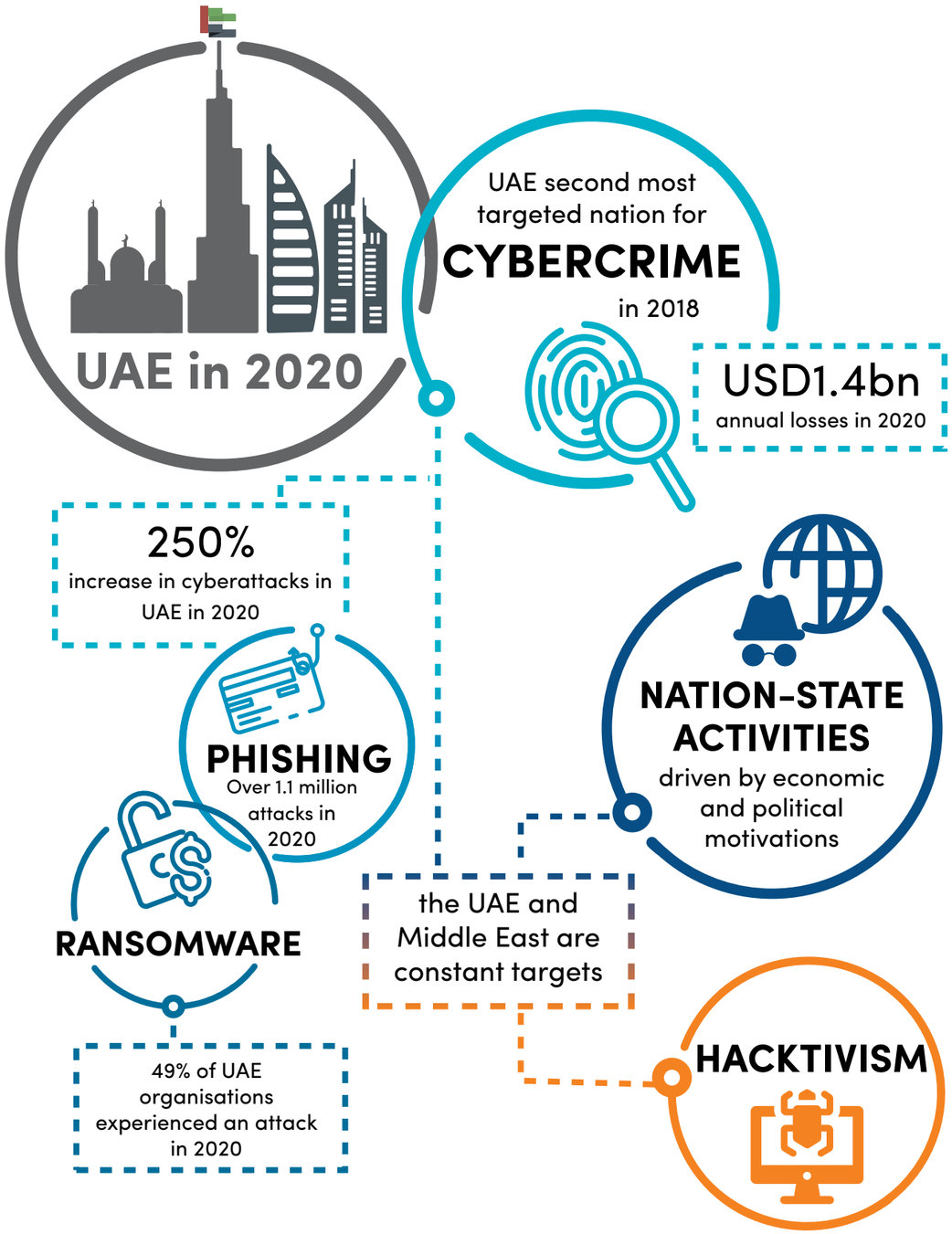
Digital14's threat research also shows that nation-state cyber-threat actors have become more active between 2017 and 2020, with significant time and resources being devoted to advancing their interests.[6] These actors are not only growing in number, but they are also becoming more sophisticated and are increasingly harder to identify. In particular, **the UAE and the wider Middle East are constant targets of nation-state activities driven by economic and political motivations**.[7 8]

Industry estimates put the **cost of a data breach in the Middle East as the second-highest in the world at USD6.52 million on average in 2020**, just after the United States. This figure is 69% higher than the 2020 global average of USD3.86 million,[9] and a 9% increase over the 2019 figure of USD5.97 million for the region.[10]

In 2020, the Head of Cybersecurity for the UAE Government, Dr. Mohamed Hamad Al Kuwaiti, noted a **250% increase in cyberattacks in the UAE,** with phishing and ransomware incidents surging.[11] The UAE faced **over 1.1 million phishing attacks in 2020**.[12] These attacks peaked at moments when UAE residents were restricted to their homes and needed to rely on internet platforms for their daily needs and work.

Ransomware also increased significantly in 2020, with an industry study showing an increase of over 33% in the number of new ransomware families compared with 2019.[13]

A similar growth was observed in the number of malware operators using double extortion tactics, where data is encrypted and stolen, and victims are then pressured into paying ransoms in order to avoid this stolen data being leaked or any backups being rendered useless.[14] Nearly 40% of ransomware attacks discovered in 2020 used this tactic.



The threat actors behind the Maze ransomware reportedly pioneered double extortion: by the end of 2020, 15 different ransomware operators had used this approach.[15] In a 2020 survey of 300 UAE IT managers, **49% of UAE organisations reported having experienced a ransomware attack**.[16]

THREAT GROUPS 03.

In the following section, Digital14 Threat Intelligence Center describes some of the major threat groups that targeted the UAE in 2020. These groups vary considerably in terms of capability and sophistication and rely on a wide range of resources and training to support their activities.

Nation state

Nation-state threat actors are frequently the most sophisticated, with dedicated resources and personnel, and extensive planning and coordination.[17] Digital14 presents some of the major nation-state actors targeting the UAE and the wider Middle East in 2020.

INTENT: Espionage

APT28

Believed to be operating under Russia's foreign military intelligence agency since 2004, APT28 is a threat actor that launched a phishing campaign using compromised email accounts of UAE entities.[18]

TARGET

ATTACK VECTOR

- OPEN-SOURCE HACKING TOOLS
- CUSTOM MALWARE
- MALICIOUS OFFICE DOCUMENTS[19]

APT41

First seen in 2012, APT41 is a highly sophisticated Chinese-linked threat group known for its supply chain compromises against multiple industries worldwide.[20]

TARGET

ATTACK VECTOR

- CUSTOM MALWARE
- WEB SHELLS
- OPEN-SOURCE HACKING TOOLS[21]

The key for target and attack vector icons can be found on Page 34

OILRIG[22]

Iran-linked threat group OilRig, first seen in 2014, has targeted multiple victims globally but has largely focused on the Middle East.[23]

TARGET

ATTACK VECTOR

- OPEN-SOURCE HACKING TOOLS
- CUSTOM MALWARE
- LEGITIMATE TOOLS[24]
- WEB SHELLS

CHAFER

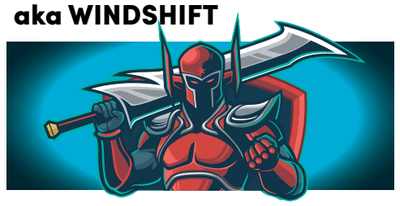
First seen in 2014, the Iran-linked threat group Chafer is known for targeting critical infrastructure sectors in the Middle East for espionage purposes.[25]

TARGET

ATTACK VECTOR

- OPEN-SOURCE HACKING TOOLS[26]
- CUSTOM MALWARE
- MALICIOUS OFFICE DOCUMENTS

BAHAMUT aka WINDSHIFT



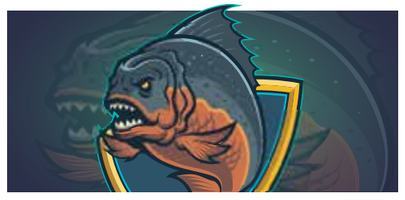
First seen in 2016,[27] Bahamut is an evasive threat group believed to be operating as a hack-for-hire group launching targeted attacks in the Middle East and South Asia.[28]

TARGET

ATTACK VECTOR

- OPEN-SOURCE HACKING TOOLS[29]
- CUSTOM MALWARE
- MALICIOUS OFFICE DOCUMENTS

MUDDYWATER



Active since 2017, Iran-linked threat group MuddyWater targets organisations across multiple verticals primarily in the Middle East.[30]

TARGET

ATTACK VECTOR

- OPEN-SOURCE HACKING TOOLS
- CUSTOM MALWARE
- MALICIOUS OFFICE DOCUMENTS
- LEGITIMATE TOOLS[31]

The key for target and attack vector icons can be found on Page 34

MOLERATS

Molerats is an Arabic-speaking, politically motivated APT group operating in the Middle East since 2012. [32]

TARGET

ATTACK VECTOR

- OPEN-SOURCE HACKING TOOLS [33]
- CUSTOM MALWARE
- MALICIOUS OFFICE DOCUMENTS

CHARMING KITTEN

Active since 2014, Iran-linked threat group Charming Kitten is focused on targeting individuals in the academic, human rights and media sectors in Iran, Israel and the UK. [34 35]

TARGET

ATTACK VECTOR

- OPEN-SOURCE HACKING TOOLS [36]
- CUSTOM MALWARE
- MALICIOUS OFFICE DOCUMENTS

Hacktivists

Digital14 has identified the key hacktivist group operating in the UAE in 2020. Hacktivists are usually motivated by ideological themes and typically employ a broad repertoire of tools to target a diverse range of organisations.

INTENT: Ideology

ANONYMOUS

OpArabia, a campaign linked to the Anonymous group first emerged in 2012. The operation was launched in support of the Arab Spring Revolution. This hacktivist group operates across a vast, geographically dispersed network. The UAE has been a constant target of this group. [34 35]

TARGET

ATTACK VECTOR

- DDoS – degradation of service –

The key for target and attack vector icons can be found on Page 34

DRUMRLU aka 3lv4n

First observed in May 2020, drumrlu is an independent hacker known for breaching and selling network access and databases. The UAE was identified as a target when drumrlu advertised full network access to servers and data owned by a UAE government entity on a hacker forum. [37]

TARGET

ATTACK VECTOR

- UNKNOWN

Cybercriminals

Cybercriminals targeting the UAE and the wider Middle East range from lone agents to known malware operators. Digital 14 takes a closer look at these cybercriminals by target industry, attack vector, intent and malicious tools.

INTENT: Financial

EGREGOR

First seen in September 2020, Egregor directs ransomware at large organisations worldwide. Various reports indicate that operators of the recently shut down 'Maze' ransomware have shifted to Egregor. [38]

TARGET

ATTACK VECTOR

- OPEN-SOURCE HACKING TOOLS
- CUSTOM MALWARE

MAZE

First identified in May 2019, Maze has been linked with TA2101. Operators using Maze have been highly active, targeting a range of sectors in North America and Europe. [39 40]

TARGET

ATTACK VECTOR

- OPEN-SOURCE HACKING TOOLS
- CUSTOM MALWARE
- MALICIOUS OFFICE DOCUMENTS

Nov 2020 – MAZE announced a shutdown of their operation. [40]

TA505

Active since 2014, TA505 is a financially motivated threat group that demonstrated a propensity to operate with a wide range of malware variants such as Dridex and Trickbot. [41]

TARGET

ATTACK VECTOR

- OPEN-SOURCE HACKING TOOLS
- CUSTOM MALWARE

TA542

A cybercrime actor linked to the Emotet malware, which was first seen in June 2014. It is a sophisticated banking trojan that is also used as a dropper for additional malware like Trickbot and Qakbot. [42]

TARGET

ATTACK VECTOR

- OPEN-SOURCE HACKING TOOLS
- CUSTOM MALWARE
- MALICIOUS OFFICE DOCUMENTS

UAE INTERNET FOOTPRINT REVIEWED 04.

In partnership with Oryx Labs,[44] a UAE-based cybersecurity research and development company, Digital14 analysed passive data related to the UAE's Internet footprint. In order to provide UAE organisations with a holistic understanding of the threats tied to the UAE's current threat landscape, Digital14 reviewed the following elements: known vulnerabilities, vulnerabilities by year of discovery, vulnerabilities with public exploit, common weaknesses, exposed ports and foreign hosting.

Known vulnerabilities

- In 2020, a total of **249,955 vulnerabilities** were found in **800,315 unique instances**.[45]
- On average, there were 3.7 vulnerabilities found per instance hosting a website.

Vulnerabilities by year of discovery

- UAE organisations today still face challenges in **vulnerability management and timely patching**.
- Digital14 observed that in some UAE organisations, vulnerabilities that were discovered five years ago, and as far as 20 years ago, still **remain unpatched**.

Vulnerabilities by technology

- Digital14 observed **22,809 vulnerable instances** against **143 known vulnerabilities** (Figure 1) with a public exploit. In other words, any threat actor – regardless of sophistication levels – can exploit these flaws.
- Nearly half of the 143 vulnerabilities (69) were classified as **high** or **critical** (Figure 1).

One of the most notable vulnerabilities with public exploits in 2020 was **CVE-2020-0688**.[46] It has been ranked among the year's most serious weaknesses on the CVSS rating scale. The flaw is found in the Exchange Control Panel (ECP) component, which is a web-based management interface used by Exchange administrators for remote management. Multiple nation-state threat actors exploited the remote code execution vulnerability against targets in the Middle East, including in the UAE.[47]

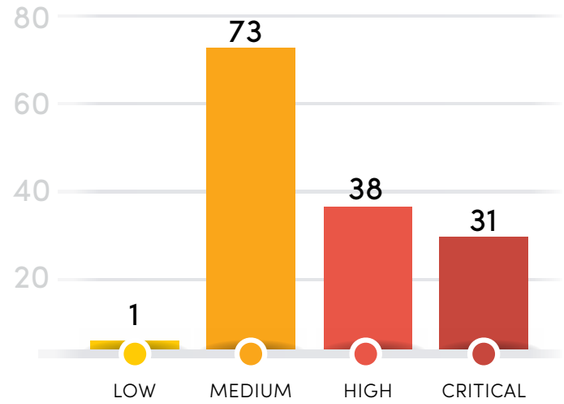


Figure 1. Vulnerabilities with public exploit ranked by severity

Vulnerable instances by affected components

- Digital14's threat analysis showed that the vast majority of instances (66%) pertain to vulnerabilities related to **web applications**. Vulnerabilities related to network services and web servers were also found (Figure 2).
- Of the total instances seen, **nearly 15% of instances were vulnerabilities related to Internet-facing, unpatched IoT devices**. The wide deployment of vulnerable IoT devices can weaken the overall security of an organisation's network.

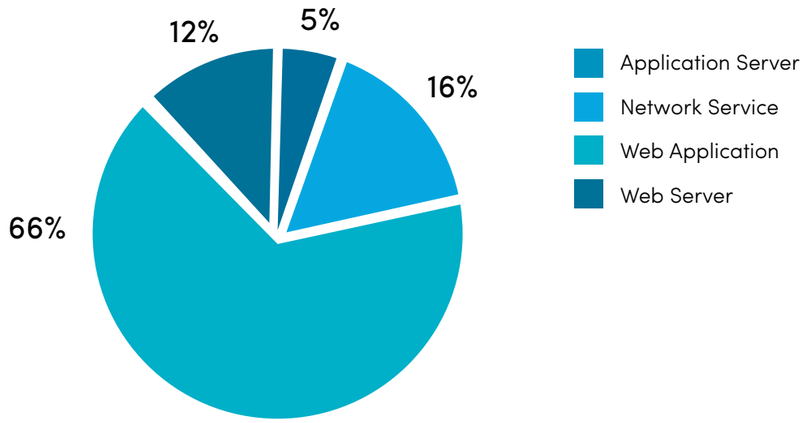


Figure 2. Distribution of instances by affected components

Instances by common weaknesses

- Digital14 analysed vulnerabilities using the common weaknesses enumeration (CWE), an open-source categorisation of software weaknesses and vulnerabilities.
- Nearly **50%** of the weaknesses may lead to **remote code execution**, which could allow threat actors to run code remotely in order to achieve their broader goals, such as exploring a network or stealing data, among others (Figure 3).
- A third (33%) of vulnerable instances are affected by **cross-site scripting flaws** (Figure 3).

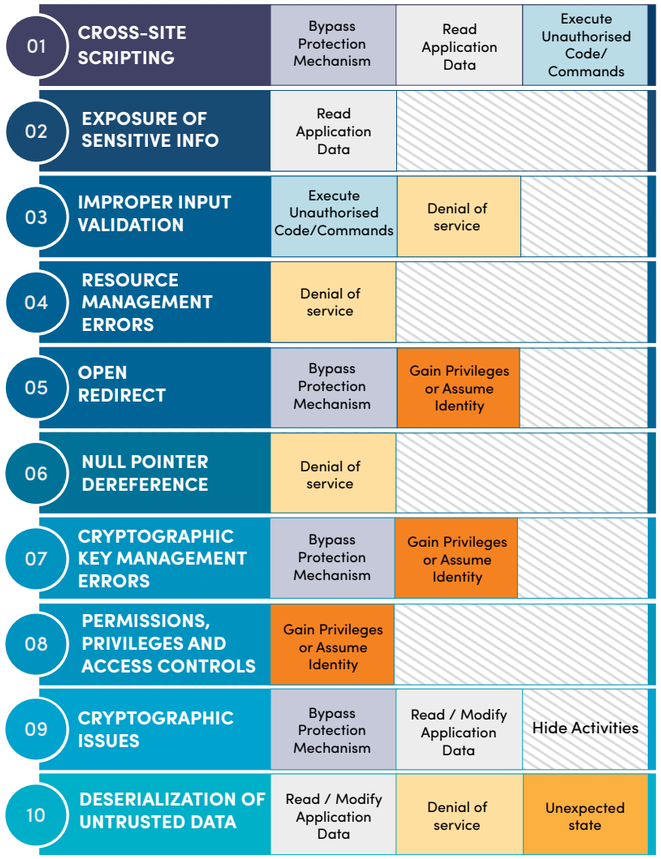


Figure 3. Most common weaknesses

- **Exposure of sensitive information (17%)** and **improper input validation (16%)** were also among the top CWE types observed (Figure 3).
- The top 10 CWEs had the following impacts: Bypass Protection Mechanism; Read Application Data; Denial of Service; Gain Privileges or Assume Identity; Modify Application Data; Execute Unauthorised Code or Commands; Hide Activities; or Unexpected State (Figure 3).

- Additionally, a significant weakness evident from Digital14's analysis was that **11.6% of unique domain names do not use the https protocol**. The non-use or misuse of an SSL certificate may pose considerable risk to UAE organisations that are bound to safeguard the privacy of their customer data; this data is consequently at risk of misuse or theft.

Top exposed ports

Ports are integral to the internet's communication model. Threat actors are therefore constantly in search of exposed ports that could allow access to a network when targeted. Data from Oryx Labs reveals the following top exposed ports (Figure 4), with some notable insights:

- **Port 7547**, which is used by the CPE WAN Management Protocol (CWMP), was the third top exposed port. Port 7547 is commonly used by routers but is also exploited by malicious botnets such as Mirai.

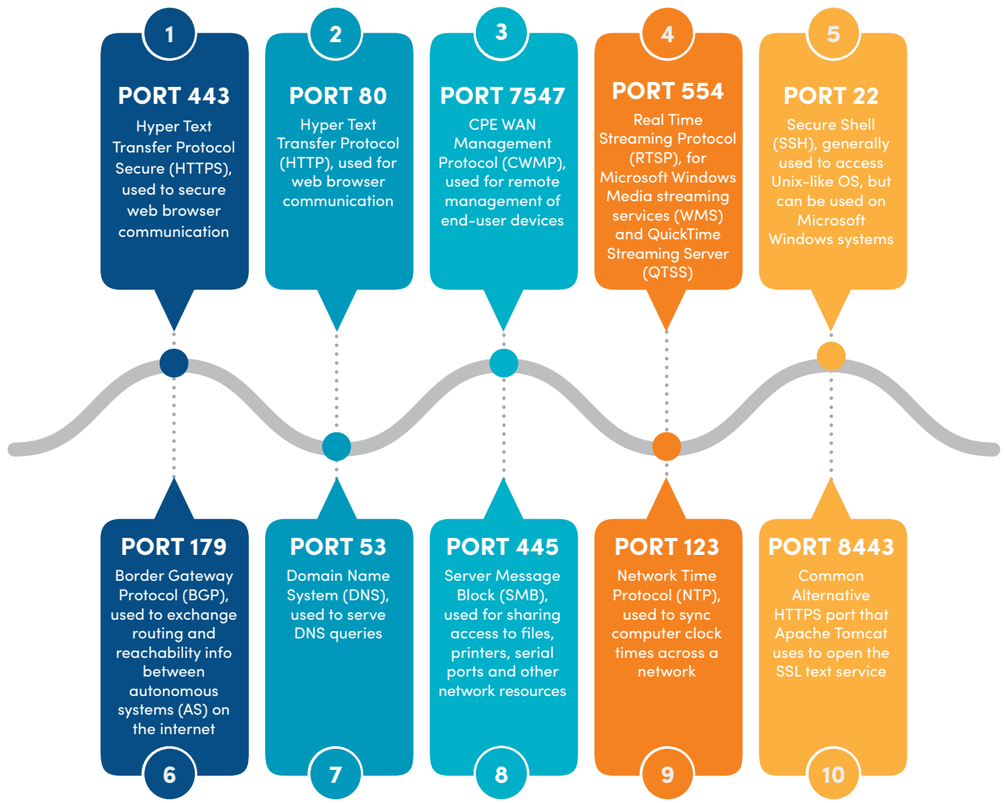


Figure 4. Top exposed ports

- **Port 554** is the fourth top exposed port. It is used for Real Time Streaming Protocol (RTSP) and is commonly exploited by botnets targeting exposed IoT devices.
- **Port 445** is the Server Message Block (SMB) and is one of the top 10 exposed ports. Port 445 was leveraged by the EternalBlue exploit, which was used to spread WannaCry.

Foreign Hosting

- There are nearly **230,000** UAE country code top-level domains.
- Of this total, only 34% are hosted within the UAE and the remaining **66% are hosted outside of the UAE** (Figure 5).
- The majority of the UAE's commercial, government and educational organisations have opted to host their infrastructure outside the UAE rather than using internal providers. Doing so potentially leaves these organisations without full control of their systems, while increasing the risk of threat actors gaining unauthorised access to sensitive organisational data.

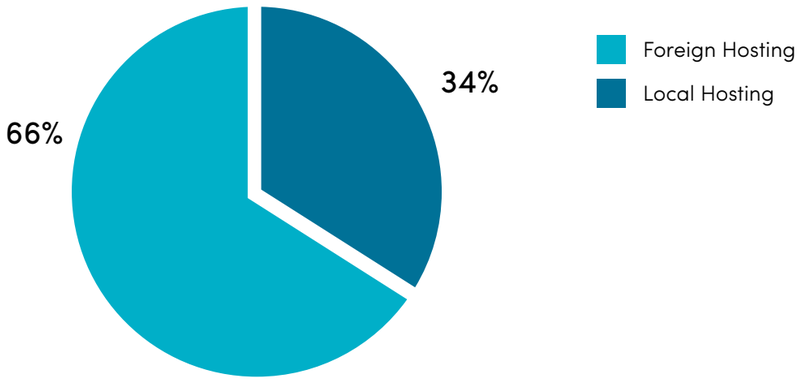


Figure 5. Distribution of geographic web hosting of UAE country code top-level domains

05.

SECURITY WEAKNESSES

Digital14's Cyber Network Defense carried out technical assessments of UAE entities across various sectors. The results are presented in this section. As part of the audit, Digital14 investigated the most predominant security weaknesses and attempted to determine how UAE entities can improve their security posture.

Most frequent weaknesses

Missing Microsoft Windows Operating System Patches

This was the most common security weakness discovered during Digital14's assessments, indicating that UAE organisations need to improve their patch-management processes, especially when it comes to widely used software such as Microsoft products. A widespread disregard for the immediate patching of vulnerable Windows systems presents a substantial attack surface for threat actors (Figure 6).

Password Re-Use

This remains a major weakness in UAE organisations, as observed in nearly half (**47%**) the assessment reports (Figure 6).

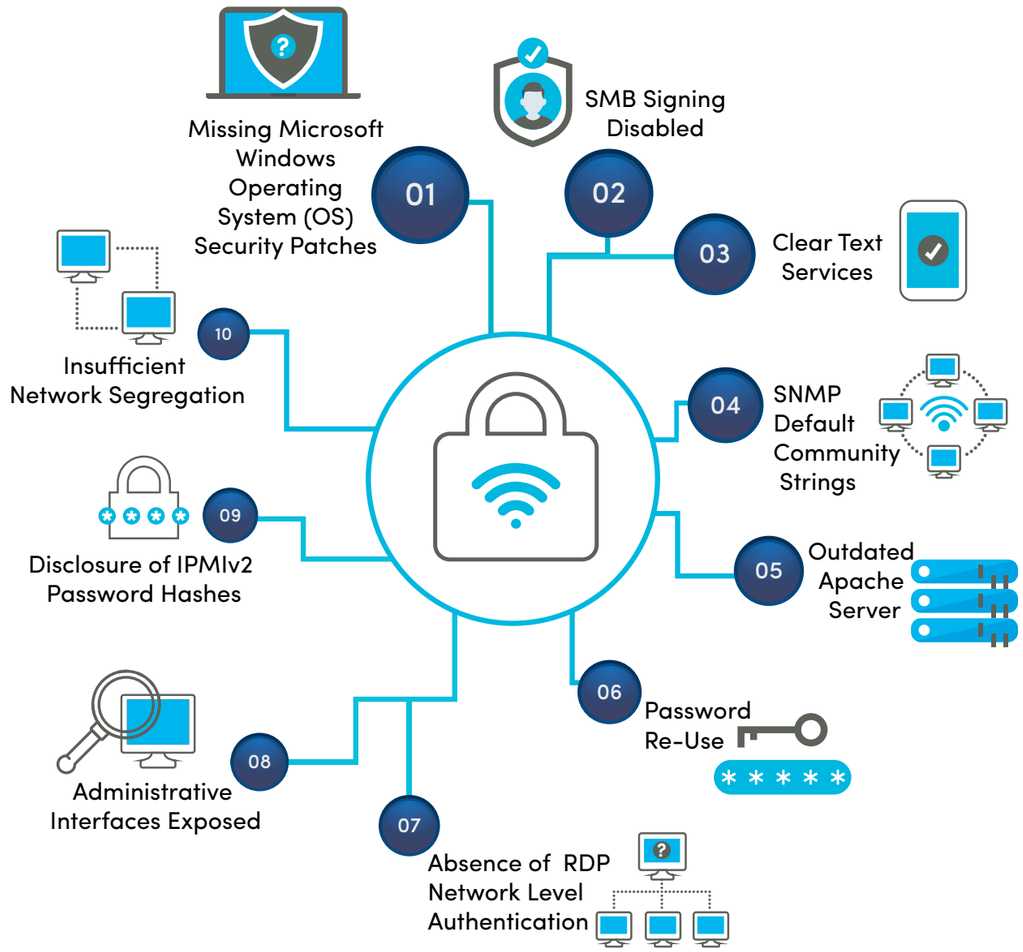


Figure 6. Most frequent security weaknesses

Identified weaknesses, configuration issues and causes

50% of identified weaknesses were **high** and **critical** in terms of severity (Figure 7).

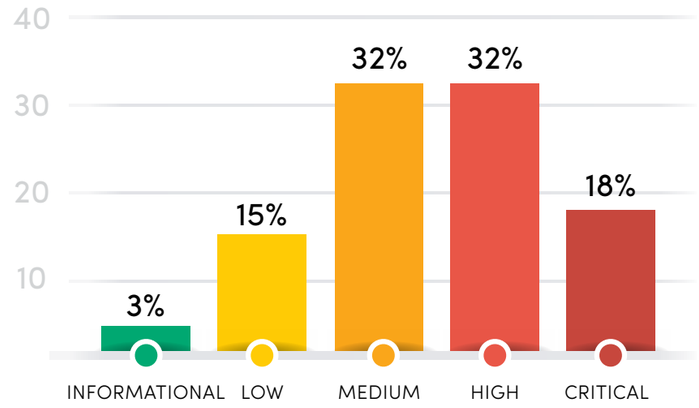


Figure 7. Identified weaknesses ranked by severity

At the top end, these high and critical weaknesses included:

Software Vulnerabilities

The majority of software vulnerabilities that Digital14 perceived concern **remote code execution, information disclosure,** and **unauthenticated access** affecting the software and services below. Such vulnerabilities could allow threat actors to compromise the confidentiality, integrity and availability of sensitive information.

- Cisco
- Microsoft
- Citrix
- Oracle
- F5

Outdated Software

Across a range of operating systems and platforms, Digital14 found that enterprise systems were frequently missing security patches for high-severity vulnerabilities affecting common software provided by different firms, including:

- Apache
- Microsoft Windows OS
- VMWare

Credential Issues

Digital14 observed different issues involving poor or bad password policies and best practices. Such cases include the use of default or weak passwords that can be easily guessed or acquired in a simple dictionary attack. The issue extends to passwords for admin accounts, which could give threat actors administrative privileges once they gain access to the network.

Poor Configuration

Several assessed organisations used default or poor configuration of both software and hardware components for their corporate networks, leading to heightened security risks.

Inadequate Network Segregation

Digital14 observed weaknesses stemming from inadequate network segmentation. Poor internal segmentation permits threat actors to move easily across a network and access its most sensitive areas once they gain access to a single device on the system.

Insecure protocols

Protocols that remain unencrypted and send data as clear-text packets enable threat actors to capture enterprise data in a readable format and subsequently expose sensitive content.

06.

COMMON INCIDENT TYPES

Different types of security incidents, across varying levels of severity, occured in the UAE. Over the past year, the Security Operations Center run by Digital14's Cyber Resilience Service investigated numerous security incidents. These have been broadly categorised into six types and ranked according to the severity scale developed by aeCERT, the UAE's national Computer Emergency Response Team.

During 2020, the most common incident types were **Unauthorised Access** and **Malicious Code**. The former accounted for **40.4%** of incidents. Unauthorised Access is when an individual gains logical or physical access without permission to the network, system, application, data or other resources of an organisation. This category also accounted for almost **34% of severely critical incidents** observed. Incidents with critical security are high-risk attacks that disrupt critical services for a large number of users, involve a serious breach of network security, affect mission-critical infrastructure or services, and damage public confidence in the organisation.

Malicious Code accounted for the second highest number of incidents observed at **39.6%.** Malicious software, commonly known as malware, is any program that infects an operating system or application. Malware may take the form of worms, viruses, trojans, spyware, adware, rootkits, etc. Such programs are typically able to steal sensitive or confidential data, delete documents or even add software not approved by the user (Figure 8).

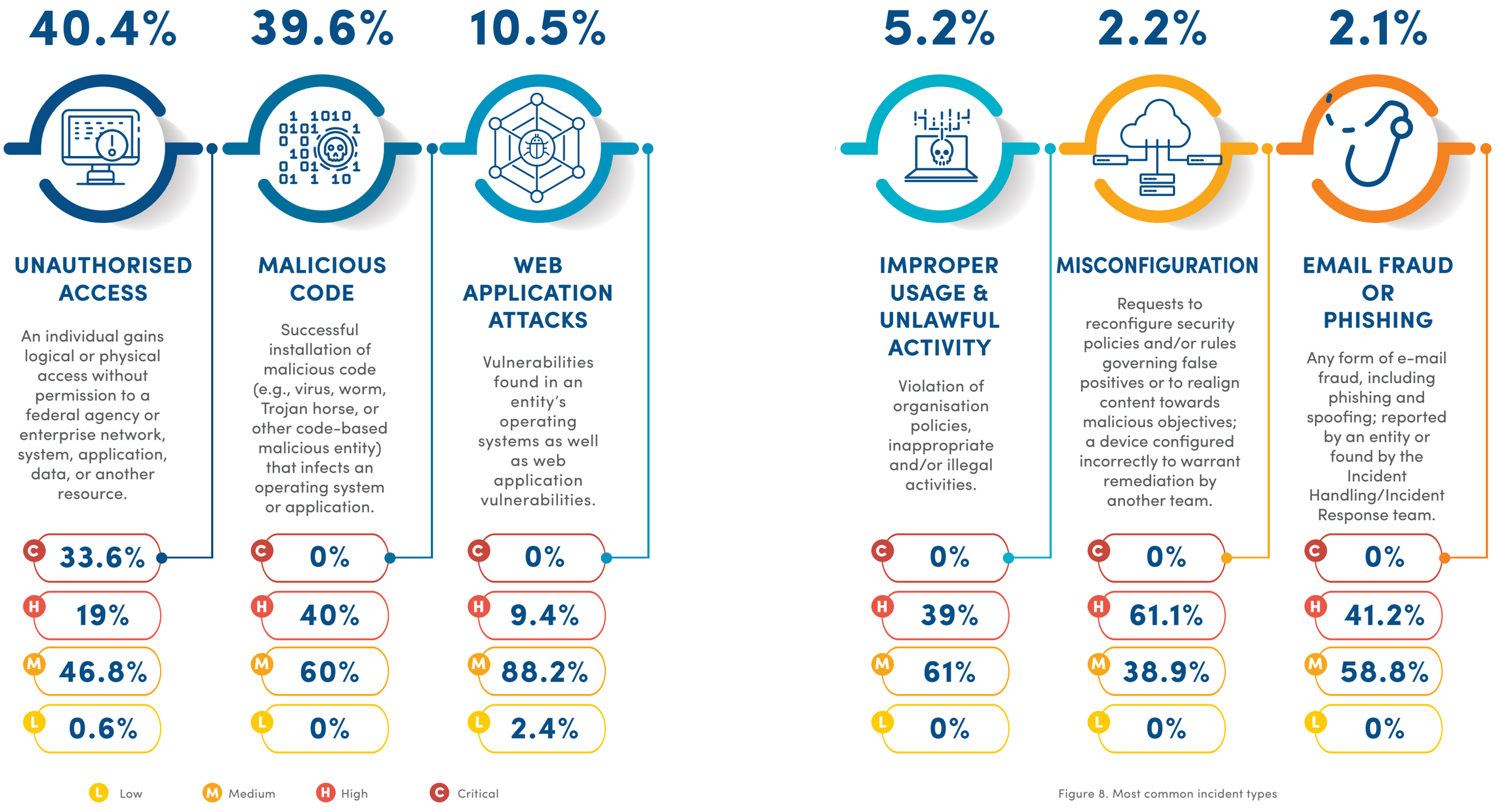


Figure 8. Most common incident types

THREAT VECTORS 07.

Over the course of 2020, Digital14 identified several threat vectors that were successfully leveraged by threat actors to breach the perimeter of targeted organisations. Overall, threat vector activity appeared to be on the increase. In cybersecurity, a threat vector is the means used by a threat actor to gain unauthorised access to a device or network for malicious purposes.[48]

Digital14 noted the following common threat vectors in multiple cybersecurity incident response engagements:

Vulnerability exploitation

The number of discovered vulnerabilities has increased significantly in recent years. In 2020 alone, the US National Institute of Standards and Technology logged a 6% increase in the number of vulnerabilities compared to 2019.[49] Specifically in the UAE, a total of **249,955 vulnerabilities** were found in **800,315 unique instances.** Moreover, Digital14 observed **22,809 vulnerable instances** arising from **143 vulnerabilities with known public exploit**.

The number of threat actors seeking to exploit unpatched vulnerabilities has risen alongside the increase in discovered weaknesses. The situation is intensified by the dangers of a **surging number of vulnerabilities with public exploits** because such flaws can be leveraged by both sophisticated and low-skilled threat actors to conduct targeted and opportunistic attacks. It is also worth mentioning the rise of botnets, which constantly scan the Internet looking for vulnerable systems and automatically attempt to compromise them by executing a wide range of exploits.

During an incident response engagement by the Digital14 Incident Response Team in 2020, two notable malware samples related to recent APT activity in the Middle East region were discovered. The incident commenced with the exploitation of a Microsoft Exchange vulnerability (CVE-2020-0688) to gain access to the target network, harvest credentials, execute commands and exfiltrate data.[50]

Valid accounts

The valid accounts technique involves the use of previously stolen credentials to access the target network. Such compromised credentials may also help bypass access controls placed on different resources and systems within the network and may even be used for persistent access to remote systems and externally available services.[51] Threat actors often gain increased privileges to specific systems or access to restricted areas of the network using valid accounts.

A 2020 study showed that **80% of data breaches are related to the use of lost or stolen credentials**.[52] Observations from several incident response cases handled by Digital14 in 2020 indicate that valid accounts were used to gain initial access to the network of multiple UAE entities, providing threat actors with an entry point to the network to help them achieve their goals.

Supply chain

In December 2020, reports emerged of a supply chain attack by nation-state threat actors using **SolarWinds Orion products**. A supply chain compromise allows adversaries to manipulate products or product delivery mechanisms before they are received by the final consumer in order to extract data or modify enterprise systems.[53] Supply chain attacks are not common, however security experts estimate that the latest SolarWinds attack vector is perhaps the most potentially damaging cyberattack in recent memory.[54] The attack impacted entities across various verticals including government, consulting, technology and telecoms in geographies as diverse as North America, Europe, Asia and the Middle East, including the UAE.[55]

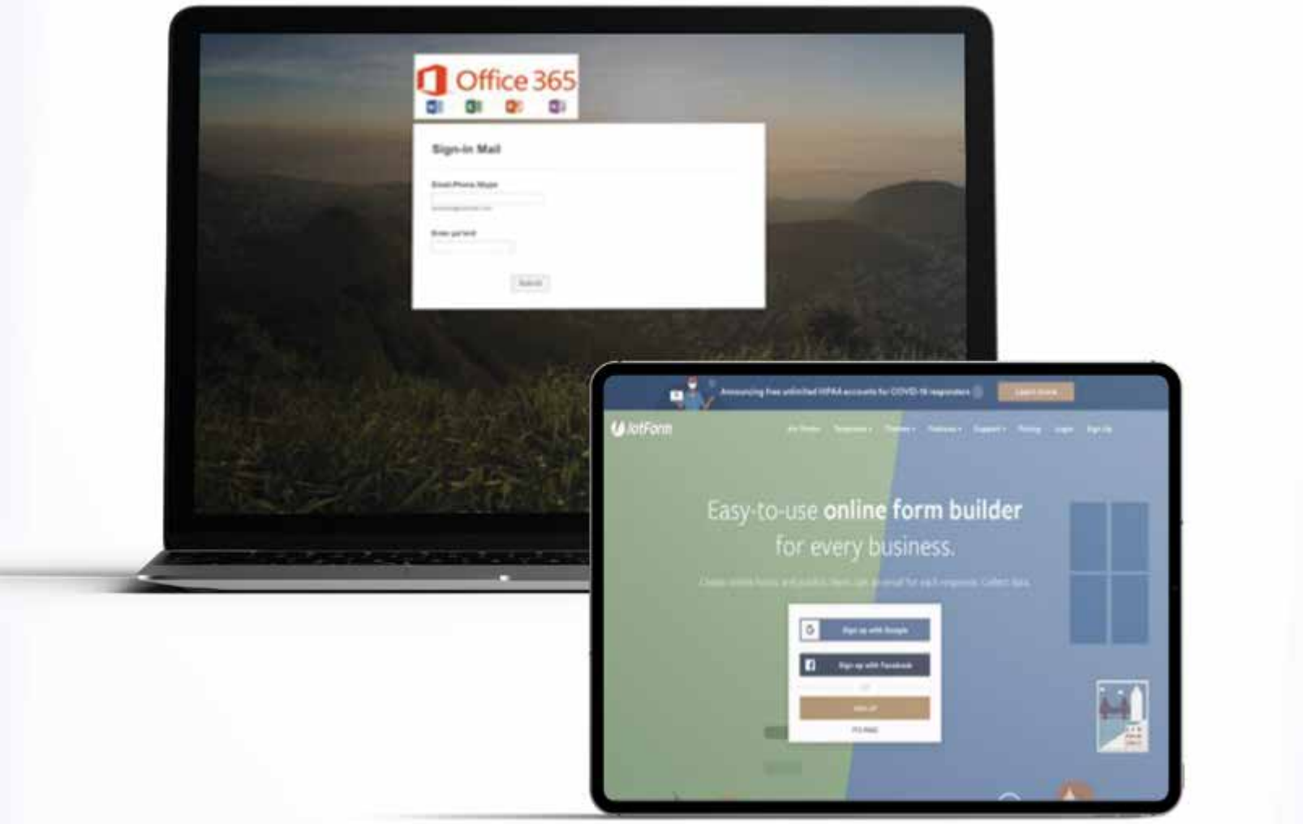


Figure 9. Sample phishing emails discovered by Digital14

Phishing

Phishing is a technique where threat actors target end-users with emails containing malicious attachments or links, typically to execute malicious code on the victim's systems or to gather credentials for further attacks.[56] This commonly used method is extremely effective in gaining access to user data and systems, with the majority of phishing attacks resulting in **loss of data**, followed by **credential/account compromise** and **ransomware infection**, according to an industry study.[57]

The global pandemic has provided fertile ground for malicious actors to launch coronavirus-themed phishing scams. An April 2020 report from the Digital14 Threat Intelligence Center showed that **38 unique malware families** have capitalised on the COVID-19 pandemic during the first quarter of 2020.[58]

Beyond the coronavirus pandemic, Digital14 notes that phishing emails typically pertain to subjects such as recent events, budgets or financial matters, and purchasing. Some phishing emails observed by Digital14 included links to a landing page asking users to provide their Office 365 and JotForm credentials (Figure 9). Additionally, Digital14 detected phishing campaigns that led to the download of Emotet malware. Emotet is an advanced, modular banking Trojan that functions primarily as a conduit for other banking Trojans.[59]

08. Case Study

LESSONS LEARNED

Several different variables contribute to the total impact of a security breach. However, the cost of proactive protection is always lower than the cost of responding to and recovering from a successful breach.

THREAT ACTOR

- APT
- Iranian-linked
- Espionage

INITIAL VECTOR

COMPROMISED CREDENTIALS

Phishing and Credential Reuse

VULNERABILITY

Exploitation of unpatched Microsoft Exchange servers

TACTICS, TECHNIQUES + PROCEDURES

Deployment of custom and highly sophisticated backdoors and web shells

Theft of account credentials

Lateral movements using various techniques

C2 communication via a variety of custom malware

Data exfiltration using custom PowerShell scripts

IMPACT

Data exfiltration aimed at stealing valuable intellectual property and/or confidential data for espionage purposes

Gaining complete access and control over the IT infrastructure

Credential theft, potentially opening the door to additional attacks including supply chain attacks

Operational impact such as service outages or downtime for several weeks

RESPONSE AND REMEDIATION

Incident Response (IR), Post IR monitoring (24x7 for 4 weeks)

Implementation of two factor authentication for virtual private networking and Outlook Web App

Rebuilding Exchange and Active Directory

Reviewing and hardening of the Active Directory

24x7 SOC Monitoring

Web application penetration test (external and internal)

Firewall configuration review and micro-segmentation

Redesign of detection policies - Deployment of endpoint detection and response, and network security monitoring

COST Approximately AED 42 milion

May 2021 — **DWELL TIME** Under six months. — May 2021

RECOMMENDATIONS 09.

Based on the findings outlined in this report, Digital14 recommends the following best practices for UAE organisations to ensure a robust security program:

1. Patch vulnerabilities regularly

Untimely patching exposes organisations to greater risks by providing threat actors with a platform to access their target's network. Patching vulnerabilities immediately as they occur allows the organisation to maintain efficiency by keeping its operating systems and components up to date and protect its assets from unauthorised access.

2. Adopt a defence-in-depth strategy to detect threats

Many of today's advanced threats can evade legacy signature-based threat detection solutions. The use of Security Information and Event Monitoring (SIEM) solutions, Endpoint Detection and Response (EDR) and Network Security Monitoring (NSM) are critical to ensuring that security teams have complete visibility across an organisation's entire environment to investigate, contain, and eradicate materialised threats efficiently and effectively.

3. Perform regular penetration tests

Security weaknesses offer threat actors the opportunity to compromise an organisation. Organisations must therefore understand their current attack surface inside out. Regular penetration testing allows organisations to develop an effective security roadmap and strategy.

4. Maintain password hygiene

Many enterprise users are guilty of password reuse despite continued warnings and successful attacks caused by compromised credentials. Passwords are an integral component of security hygiene but remain a weak link and are the source of many cybersecurity issues. Organisations should implement strong password policies and implement strict rules concerning corporate email accounts for personal use.

5. Implement multi-factor authentication across all infrastructure

Threat actors access sensitive data in multiple ways, beginning with stolen credentials. Multi-factor authentication provides an additional layer of protection for corporate services, ensuring that even if a user's password is compromised, it cannot easily be leveraged by a threat actor.

6. Implement a regular, robust, interactive security awareness program

Humans are the weakest link in the security chain, with functional staff in non-security roles among the greatest offenders. Ensuring that staff are aware of common cybersecurity issues and highlighting the different ways in which users can be targeted or exploited, is a critical component of the overall cyber-security strategy. Regular training and proactive engagement can help ensure that staff are able to identify attempts at phishing, social engineering, and risky internet behaviours.

7. Invest in upskilling cybersecurity staff and building a robust cybersecurity culture

Cybersecurity is a dynamic, fast-paced industry as threat actors continually become more sophisticated and develop new attack techniques. Staying up to date with the latest trends and industry changes is crucial for maintaining cyber resilience. Continuing professional development is key in upskilling cybersecurity operations and risk teams to stay proficient at the highest possible standard. Equally, establishing an effective cybersecurity awareness programme while building a robust and continually maturing cybersecurity culture, is key to combat evolving cyber threats.

8. Implement UAE information assurance standards in regular audits and evidence-based security assessments

UAE entities should implement and stay abreast of the UAE Information Assurance (UAE IA) Standards as part of the Cybersecurity Framework to manage the country's cyberspace.[60] Released in June 2014, the standards contain a detailed list of security controls that go beyond the usual recommendations of similar standards (for both IT and OT environments). UAE IA Standards security assessments should always be conducted by qualified security assessors with both the expertise and the experience to perform a holistic evidence-based review that extends from established policies and procedures through to detailed assessments[61] of both information technology and information security practices.

10. SUMMARY

The cyber threat landscape in the UAE is becoming increasingly complex and hyperconnected because of continuous technological advances. The COVID-19 pandemic has further accelerated these dangers by working as a force multiplier for existing cyber threats, while dispersing new threats as organisations of all kinds shift to remote working. Threat actors have proportionately adapted their tactics to target remote workers, whether by exploiting the fear and uncertainty of the pandemic or by cashing in on opportunities presented by the new remote-working environment.

The UAE remains a very lucrative target for cyber attackers, with cybercrime costing USD1.4bn annually. In line with its reputation for visionary thinking, the country leads the region on numerous fronts, including technological advancements, making it a high-value target for both financially driven and espionage-driven threat actors. It is therefore essential for organisations to urgently understand and manage existing security threats while proactively anticipating developing cyber risks.

As described in this report, websites and systems related to the UAE remain continually exposed to a wide range of cyber threats enacted by nation-state threat actors, cybercriminals, and hacktivists. The COVID-19 pandemic has also led to an increase in phishing and ransomware incidents.

Yet, many of the most common causes of cybersecurity threats seen by Digital14 were the untimely patching of vulnerabilities, the use of outdated and unsupported software, the use of weak passwords, and inadequate configuration management. These are both relatively easy to address and defend in a proactive manner following established best practices – potentially saving millions of dollars in reparative costs following an attack.

Digital14 concludes that cybersecurity approaches in the UAE remain outdated, with organisations ignorant of the expanding risk landscape and the crippling costs associated with potential breaches.

As the UAE marches towards a digital future, organisations are racing to maintain their competitive advantages by adapting new technologies such as cloud computing, artificial intelligence, big data and the industrial Internet of Things. However, the exponential development of a hyperconnected, 'always-on' digital world has concurrently enlarged the threat surface – while introducing blind spots against existing and emerging hazards.

Further, many of the newest threats successfully evade detection using obfuscation techniques. In the process, an organisation's data may be compromised for extended intervals of time, with enterprise activity visible to threat actors and to their potential clients. As numerous incidents have shown, many of these new threats are already active but remain undetected.

Over the medium term, openings for cyber criminals could expand in line with the increasing embrace of new technologies and the continuing uncertainty surrounding the COVID-19 pandemic. It is therefore incumbent on UAE organisations to prioritise the enhancement of their security posture in order to prevent breaches and potentially irreparable damage – whether financial, reputational or even physical.

Organisations and government in the UAE can no longer view cyber protection as a one-time solution but must see it as an ongoing process that steadily strengthens and improves enterprise security. Protecting against current threats is no longer enough – rather, UAE organisations must leverage cybersecurity as the enabler that protects, transforms and nurtures our complex digital ecosystems for the safety and benefit of all stakeholders.

ABOUT DIGITAL14

Delivering trust in a world where cyber risks are a constant threat, Digital14 guides clients on their journeys to reach unprecedented heights and navigate what lies ahead in tomorrow's digital frontier. Digital14, established in 2019, is part of ADQ, one of the region's largest holding companies with a diverse portfolio of major enterprises spanning key sectors of Abu Dhabi's non-oil economy. Being based in the regional and global innovation hub of Abu Dhabi, this provides the ideal platform for Digital14 to accelerate digital advancement and cyber resilience solutions via robust, end-to-end solutions. Whether it is enjoying the freedoms of a protected internet, secure transactions or safe communications – we Protect, Transform, and Nurture today so that everyone can flourish with the freedom to achieve their potential, tomorrow.

For more information, visit https://digital14.com

digital14
protect. transform. nurture.

May 2021

REFERENCES

1. https://www.cnbc.com/2020/12/06/middle-east-facing-cyber-pandemic-amid-covid-19-uae-official-says.html
2. https://www.thenationalnews.com/business/technology/covid-19-pandemic-has-increased-vulnerability-to-cyber-attacks-uae-s-head-of-cyber-security-says-1.1086334
3. Threat vector is a path or tool that a threat actor leverages to attack a target
4. https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf
5. https://securityboulevard.com/2020/06/analysis-of-the-top10-hacktivist-operations/
6. https://press.hp.com/us/en/press-releases/2021/new-study-highlights-100-percent-rise-in-nation-state-cyberattacks.html
7. https://www.cnbc.com/2020/12/06/middle-east-facing-cyber-pandemic-amid-covid-19-uae-official-says.html
8. https://cisomag.eccouncil.org/gcc-countries-to-see-rise-in-state-sponsored-cyberattacks-experts/
9. IBM Cost of Data Breach 2020
10. IBM Cost of Data Breach 2019
11. https://www.cnbc.com/2020/12/06/middle-east-facing-cyber-pandemic-amid-covid-19-uae-official-says.html
12. https://www.tdra.gov.ae/aecert/en/resource-center/statistics.aspx
13. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/a-constant-state-of-flux-trend-micro-2020-annual-cybersecurity-report
14. https://www.sans.org/blog/are-you-prepared-for-double-extortion-attacks-/
15. https://blog.f-secure.com/attack-landscape-update-h1-2021/?_ga=2.244874309.1793370514.1617091149-247904548.1617091149
16. https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf
17. https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors
18. https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF
19. https://ui.threatstream.com/actor/4494
20. https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html
21. https://ui.threatstream.com/actor/28033
22. https://unit42.paloaltonetworks.com/oilrig-novel-c2-channel-steganography/
23. https://attack.mitre.org/groups/G0049/
24. https://ui.threatstream.com/actor/4411
25. https://www.bitdefender.com/files/News/CaseStudies/study/332/Bitdefender-Whitepaper-Chafer-creat4491-en-EN-interactive.pdf
26. https://ui.threatstream.com/actor/60051
27. https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Bahamut&n=1
28. https://www.blackberry.com/us/en/company/newsroom/press-releases/2020/blackberry-uncovers-massive-hack-for-hire-group-targeting-governments-businesses-human-rights-groups-and-influential-individuals
29. https://ui.threatstream.com/actor/24695
30. https://www.clearskysec.com/wp-content/uploads/2020/10/Operation-Quicksand.pdf
31. https://ui.threatstream.com/actor/14723
32. https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf
33. https://attack.mitre.org/groups/G0021/
34. https://blog.certfa.com/posts/charming-kitten-christmas-gift/
35. https://blogs.microsoft.com/on-the-issues/2020/10/28/cyberattacks-phosphorus-t20-munich-security-conference/
36. https://ui.threatstream.com/actor/5115
37. https://portal-digitalshadows.com/search/actor/5282
38. https://portal-digitalshadows.com/intelligence/malware/5297/overview
39. https://portal-digitalshadows.com/intelligence/actors/5160/overview
40. https://www.bleepingcomputer.com/news/security/maze-ransomware-shuts-down-operations-denies-creating-cartel/
41. https://portal-digitalshadows.com/intelligence/actors/4937/overview
42. https://portal-digitalshadows.com/intelligence/malware/4379/overview
43. https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKSEC-2010.pdf
44. oryxlabs.com
45. An instance is a unique combination of a domain parent, IP address, or port
46. https://nvd.nist.gov/vuln/detail/CVE-2020-0688
47. https://www.digital14.com/Microsoft-exchange-vulnerability.html
48. https://www.upguard.com/blog/attack-vector
49. https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=all
50. https://www.digital14.com/Microsoft-exchange-vulnerability.html
51. https://attack.mitre.org/techniques/T1078/
52. https://enterprise.verizon.com/resources/executivebriefs/2020-dbir-executive-brief.pdf
53. https://attack.mitre.org/techniques/T1195/002/
54. https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/
55. https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/
56. https://attack.mitre.org/techniques/T1566/
57. https://www.proofpoint.com/sites/default/files/infographics/pfpt-us-sotp-infographic.pdf
58. Digital14. Cyber Threats In The Midst Of COVID-19 Pandemic. https://digital14.com/insights.html
59. https://us-cert.cisa.gov/ncas/alerts/TA18-201A
60. Measuring Cybersecurity Maturity https://digital14.com/measuring-cybersecurity-maturity.html
61. Measuring Cybersecurity Maturity https://digital14.com/measuring-cybersecurity-maturity.html

KEY

Targeted Industries

- Government
- Finance
- Transportation
- Oil & Gas
- Water and Electricity
- Energy
- Telecommunications
- Technology
- Unknown
- Media
- Civilians
- Manufacturing
- Retail
- Technology
- Healthcare

Attack Vector - MITRE ATTACK

- Phishing-T1566
- Exploit Public Facing Application - T1190
- Unknown
- Valid Accounts - T1078
- PowerShell - T1086
- System Services: Service Execution - T1569
- Application Layer Protocol: Web Protocols - T1071
- Command and Scripting Interpreter: Windows Command Shell - T1059
- Data Encrypted for Impact T1486

Toolset

- Open-source hacking tools