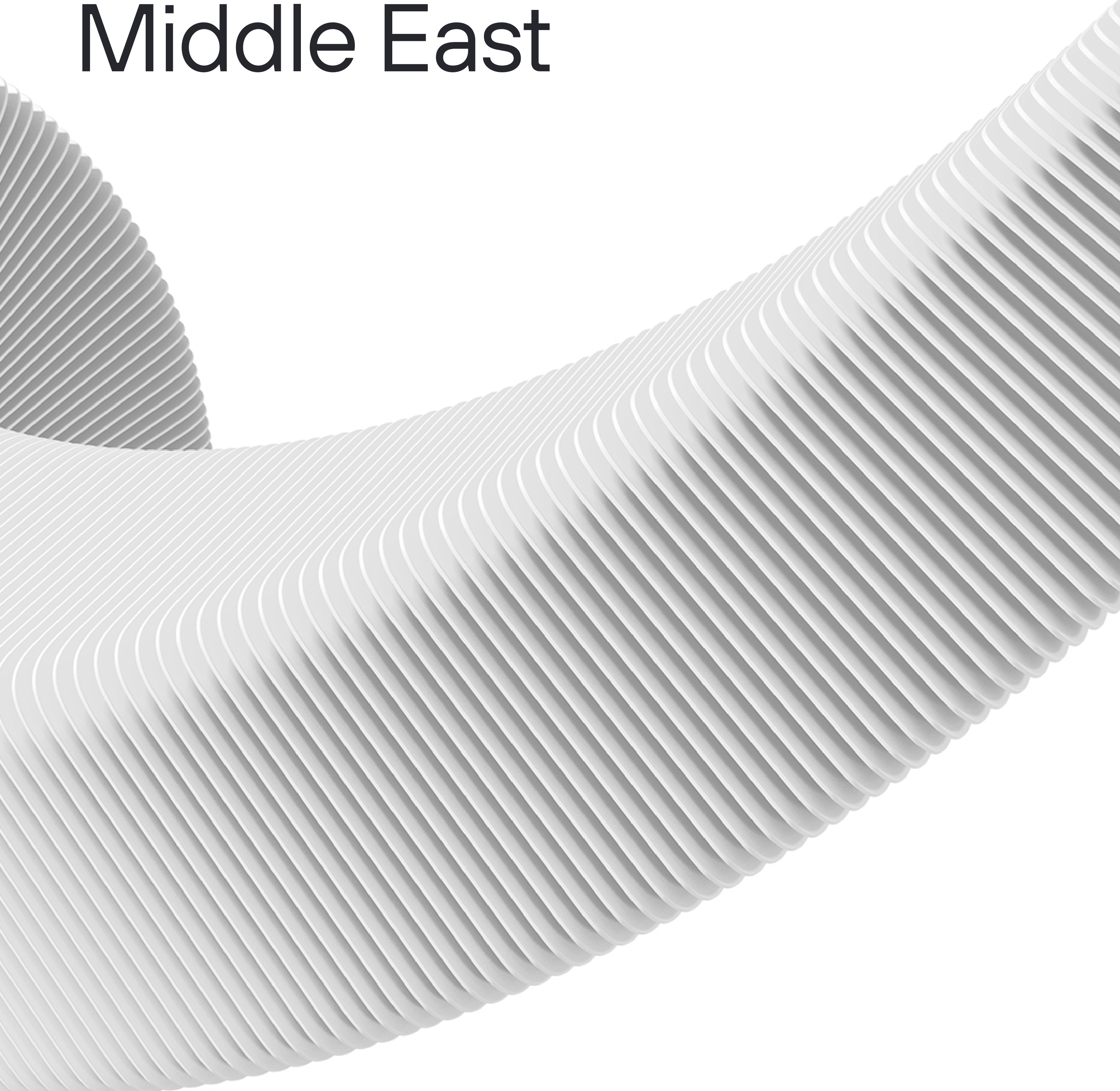
How individuals are attacked in the Middle East



Positive Technologies

ptsecurity.com

Contents

Introduction 3

Who attacks individuals in the Middle East—and why? 3

Social engineering: methods of deceit 4

Look on the dark side: how cybercriminals prepare for attacks 7

Spyware: what it steals and how to defend against it 10

Targeted attacks 13

Conclusions 15

About the report 16

Introduction

The cyberthreat landscape of the Middle East is characterized by the intensity and diversity of attacks targeting not only companies but also individuals. In our research, we examined the most common methods of attacks aimed at individuals in the countries of the Middle East region. How do cybercriminals capitalize on large-scale events like the FIFA World Cup? How to avoid getting scammed when choosing a VPN solution? Kittens and jackals, xenomorphs and pawns—who else is lurking among the cyberdunes of the Middle East? In this article, we will discuss the threats that are relevant for the region.

The unique cyberlandscape of the Middle East is shaped by several factors. First and foremost, we must note the colossal role of the Persian Gulf countries in the global economy. For instance, a fifth of all seaborne oil shipments pass through the Strait of Hormuz alone. The region has experienced rapid technological growth in recent years. By 2020, the UAE, Qatar, Bahrain, and Kuwait topped the rankings of countries with the highest percentage of Internet users. The geopolitical situation also leaves its mark. Furthermore, the diversity in attack methods is also due to the geographical location: in the Middle East, local perpetrators coexist with European and Asian cybercriminals. In such conditions, critical infrastructure, various organizations, and ordinary users all become targets of malicious attacks.

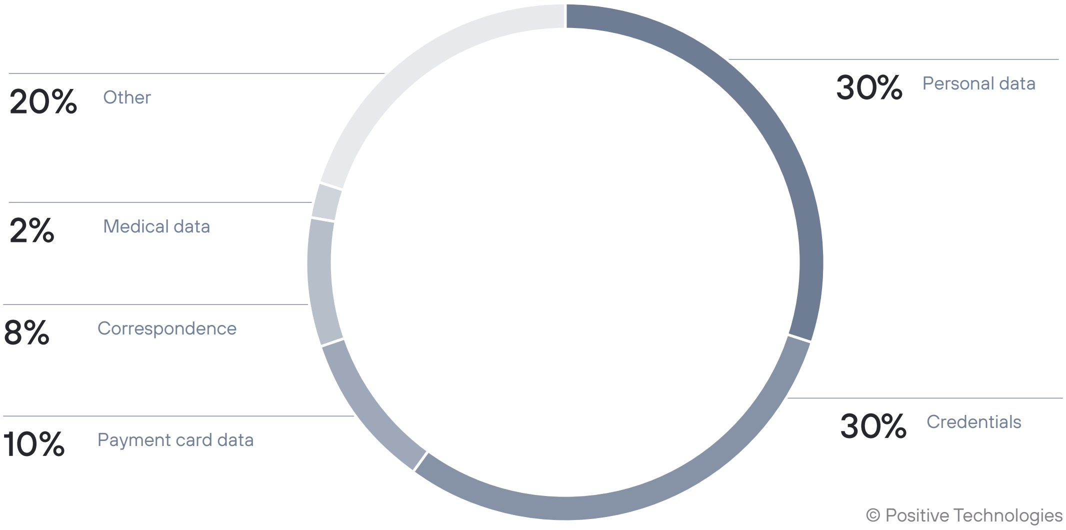
Who attacks individuals in the Middle East—and why?

According to research on current cyberthreats, from the beginning of 2022 to the end of Q1 2023, 20% of successful cyberattacks resulting in negative consequences in the Middle East were directed at individuals. The attackers aimed to steal money and confidential data from users for resale on shadow markets, blackmail, and subsequent attacks.

The socio-political landscape also has its effect on cybercriminal activity. In 39% of successful attacks on individuals, the criminals pursued ideological goals alongside financial gain. Typically, the actions of hacktivists were aimed at drawing attention to social and political issues. Such malicious actors actively maintain social media accounts through which they distribute stolen confidential data, including personal information.

According to our data, 63% of successful attacks on individuals in the Middle East region resulted in leaks of confidential information. The majority of stolen information consisted of personal data (30%) and account credentials (30%). Cybercriminals were also interested in payment card data (10%) and user correspondence (8%).

Figure 1. Types of data stolen in attacks on individuals



© Positive Technologies

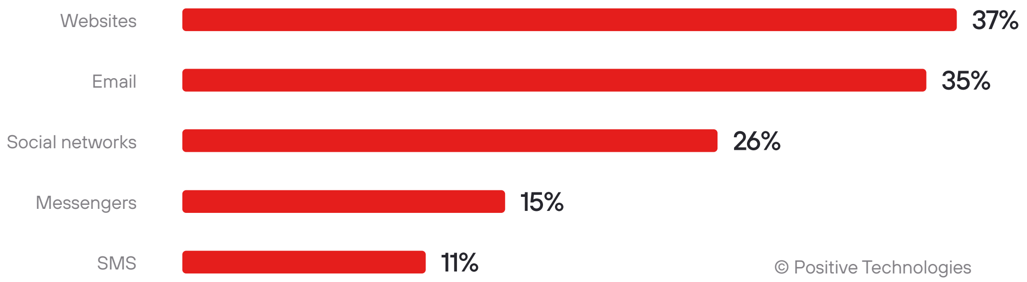
Social engineering: methods of deceit

In the vast majority (96%) of successful attacks on individuals in the Middle East countries, social engineering techniques were employed. Most often, these were mass attacks in which the criminals aimed to reach the maximum number of victims. Typically, the scammers promised some form of benefit and lured victims into rashly installing malicious applications, clicking on malicious links, or transferring funds to the attackers' accounts.

Successful attacks most often involved fake websites and emails, as well as fake social media accounts.

In every fifth (20%) phishing campaign, the attack was multi-pronged, exploiting multiple social engineering channels simultaneously. Criminals led the victims through a series of steps until the device was infected and data stolen. For instance, users could be lured through social media accounts that contained links to a messenger channel from which the victim would install a malicious application.

Figure 2. Social engineering channels used by attackers



© Positive Technologies

In a mass attack, cybercriminals aim to reach as many users as possible. To achieve this, they actively leverage current news about significant global and regional events. Attackers often used the secure HTTPS protocol with valid SSL certificates on their phishing websites to better mask the fraud.

Let's take a look at some of the news topics that cybercriminals exploited in successful attacks on users from the Middle East.

Delivery services

In the UAE, from 2020 to the present, attackers have been disguising messages as notifications from well-known delivery services. During the COVID-19 pandemic, online shopping became very popular, leading to a significant growth in the market for delivering ordered goods to customers. Cybercriminals capitalize on this trend by conducting large-scale phishing campaigns: they create disposable fake websites and send text messages demanding urgent payment for package delivery. The victims who fell for the bait had their funds and credit card information stolen by the perpetrators. It's worth noting that in their attacks, cybercriminals used phishing kits—sets of scripts for rapidly creating websites mimicking well-known delivery brands.

> We recommend to always be vigilant online. If someone demands urgent payment for a service or product, it's most likely a trap. Use official company websites to track your packages. If you're unsure about the sender's authenticity, do not click on links in messages—verify the information yourself from the official source. Treat shortened URL links with caution, as criminals often use them to disguise phishing websites. Avoid making hasty emotional decisions. Take a step back and assess the situation rationally: do you have any outstanding deliveries?

Large-scale events

Cybercriminals find ways to profit during major events. During the 2022 FIFA World Cup in Qatar, scammers created phishing websites, apps, and social media accounts masquerading as official ones, offering match tickets and fan merchandise. The culprits were most active in the Middle East, taking advantage of the geographical proximity to the hosting country. They created fake social media accounts and made job postings, offering work at the stadiums. Users were required to fill out a detailed form with supposedly necessary personal information, which went straight into the criminals' hands.

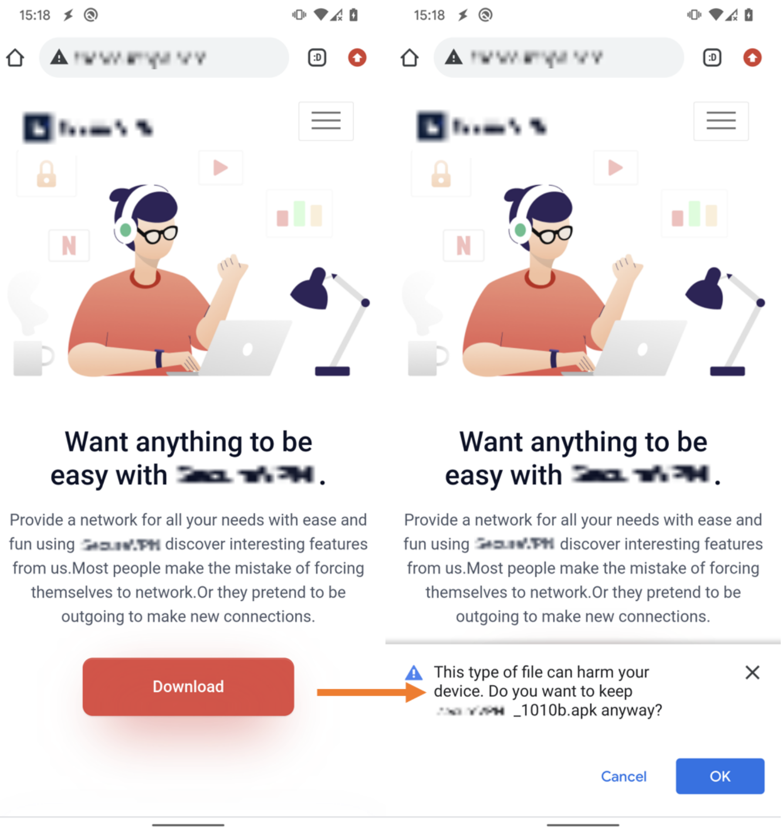
When purchasing goods and services, such as event tickets, make sure that the website is genuinely official. During major events, before buying merchandise and tickets, check if the seller is listed as a partner of the organization responsible for the event. Remember that offering a large discount on a high-demand product is one of the favorite tactics of fraudsters. The same applies to incredible job offers: if it seems too good to be true, it probably is.

VPN

In 2022, the countries in the Persian Gulf region were at the top of the global rankings in terms of the percentage of the population using VPN services. The market of applications and services that exist in a legal gray zone (such as VPNs) attracts cybercriminals spreading malware. They also use advertisements for VPNs in phishing schemes, luring users with lucrative offers and promises of anonymity.

For example, as part of one campaign, cybercriminals created phishing websites offering downloads of supposedly official VPN solutions. However, these downloads actually installed spyware onto the victim's device under the guise of an authentic application.

Figure 3. Phishing website for a fake VPN solution



Want anything to be easy with [redacted].

Provide a network for all your needs with ease and fun using [redacted] discover interesting features from us.Most people make the mistake of forcing themselves to network.Or they pretend to be outgoing to make new connections.

Want anything to be easy with [redacted].

Provide a network for all your needs with ease and fun using [redacted] discover interesting features from us.Most people make the mistake of forcing themselves to network.Or they pretend to be outgoing to make new connections.

This type of file can harm your device. Do you want to keep [redacted] _1010b.apk anyway?

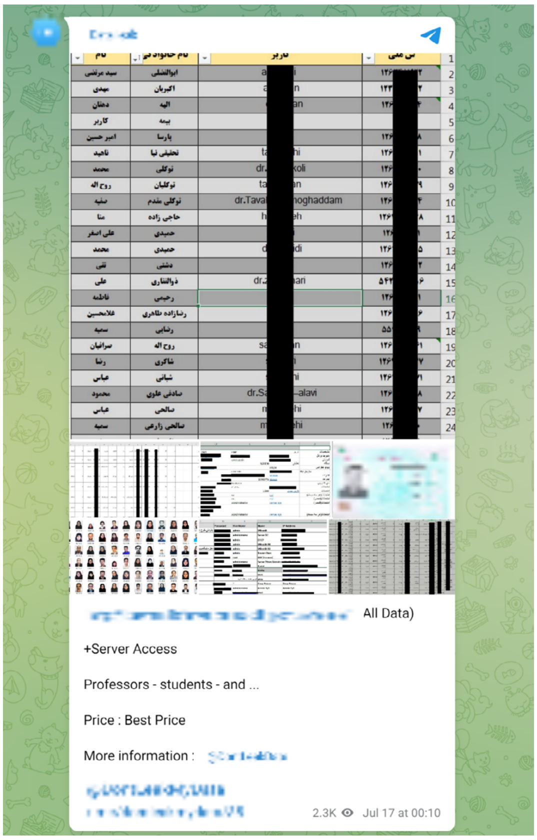
We have prepared a few simple recommendations on how to avoid falling into scammers' traps when installing applications:

- Give preference to solutions that have been in the app store for a while and that have a high rating and authentic comments (written by real users, not bots). Randomly generated usernames, repetitive phrases in reviews, and generic platitudes without specific details about the app's functionality might indicate that the rating is artificially inflated.
- Download installation files only from official sources.
- When you see an enticing offer in an advertisement, go and visit the official company website yourself. If the offer is legitimate, you can go for it without risking your device's security.

Look on the dark side: how cybercriminals prepare for attacks

One of the reasons for the success of social engineering is the numerous data leaks from various organizations. On the dark web, malicious actors sell information about users and also provide stolen data archives for free.

Figure 4. Sale of stolen data



نام	نام خانوادگی	کاربر	ن ملی	1
سید مرتضی	ابوالفضلی	a[redacted]i	۱۲۶[redacted]۲	2
مهدی	اکبریان	a[redacted]n	۱۲۳[redacted]۲	3
دهقان	الهه	[redacted]an	۱۲۶[redacted]۴	4
کاربر	بیمه	[redacted]	[redacted]	5
امیر حسین	پارسا	[redacted]	۱۲۶[redacted]۸	6
ناهید	تحقیقی نیا	ta[redacted]hi	۱۲۶[redacted]۱	7
محمد	توکلی	dr.[redacted]koli	۱۲۶[redacted]۰	8
روح اله	توکلیان	ta[redacted]an	۱۲۶[redacted]۹	9
صفیه	توکلی مقدم	dr.Taval[redacted]noghaddam	۱۲۶[redacted]۴	10
منا	حاجی زاده	h[redacted]eh	۱۲۶[redacted]۸	11
علی اصغر	حمیدی	[redacted]i	۱۲۶[redacted]۱	12
محمد	حمیدی	d[redacted]idi	۱۲۶[redacted]۵	13
تقی	دشتی	[redacted]	۱۲۶[redacted]۲	14
علی	ذوالفقاری	dr.z[redacted]ari	۵۴۴[redacted]۶	15
فاطمه	رحیمی	[redacted]	۱۲۶[redacted]۱	16
غلامحسین	رضازاده طاهری	[redacted]	۱۲۶[redacted]۶	17
سمیه	رضایی	[redacted]	۵۵[redacted]۹	18
سرافیان	روح اله	sa[redacted]an	۱۲۶[redacted]۱	19
رضا	شاکری	s[redacted]i	۱۲۶[redacted]۷	20
عباس	شبانی	s[redacted]hi	۱۲۶[redacted]۱	21
محمود	صادقی علوی	dr.Sa[redacted]–alavi	۱۲۶[redacted]۸	22
عباس	صالحی	m[redacted]hi	۱۲۶[redacted]۷	23
سمیه	صالحی زارعی	m[redacted]ehi	۱۲۶[redacted]۰	24

[illegible] All Data)

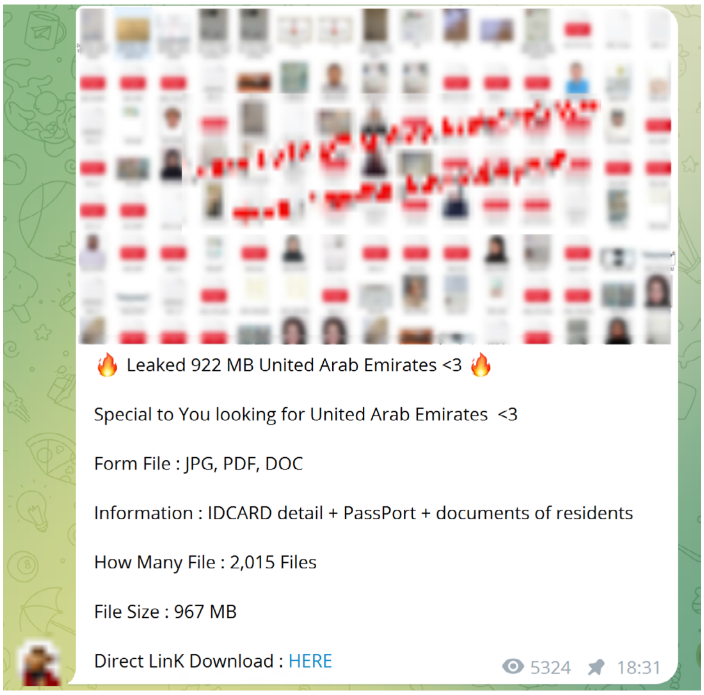
+Server Access

Professors - students - and ...

Price : Best Price

More information : [illegible]

Figure 5. Giveaway of stolen data



🔥 Leaked 922 MB United Arab Emirates <3 🔥

Special to You looking for United Arab Emirates <3

Form File : JPG, PDF, DOC

Information : IDCARD detail + PassPort + documents of residents

How Many File : 2,015 Files

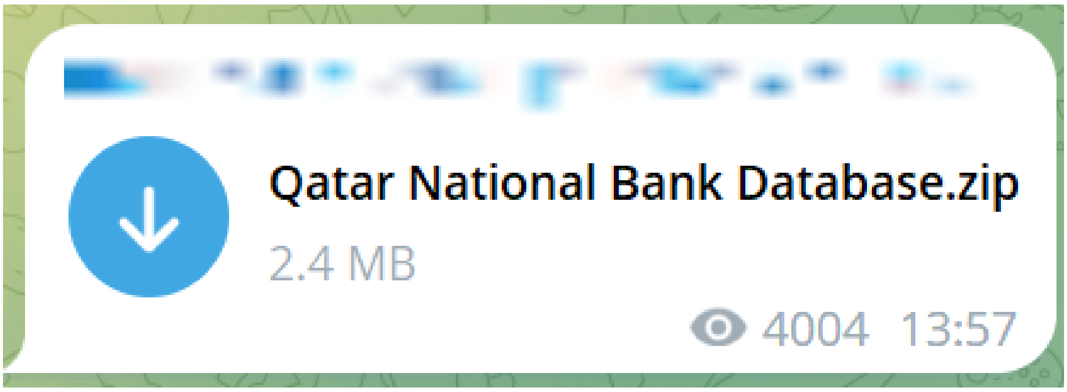
File Size : 967 MB

Direct LinK Download : HERE

5324 18:31

Criminals use the compromised information in subsequent attacks on users. For example, a successful attack on a bank could result in fraudulent actions against its customers.

Figure 6. Distribution of data stolen from a Qatar bank



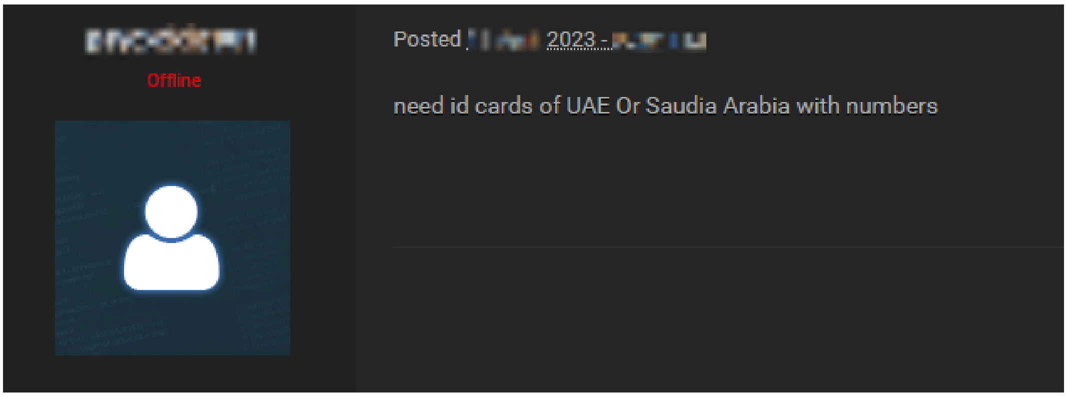
Qatar National Bank Database.zip

2.4 MB

4004 13:57

On dark web forums, we also see a demand for purchasing data. In one of the announcements, a user was looking for ID card data of citizens from the UAE and Saudi Arabia. Such information could be used to carry out targeted attacks against specific individuals.

Figure 7. Purchase of UAE and Saudi ID card data



[redacted]

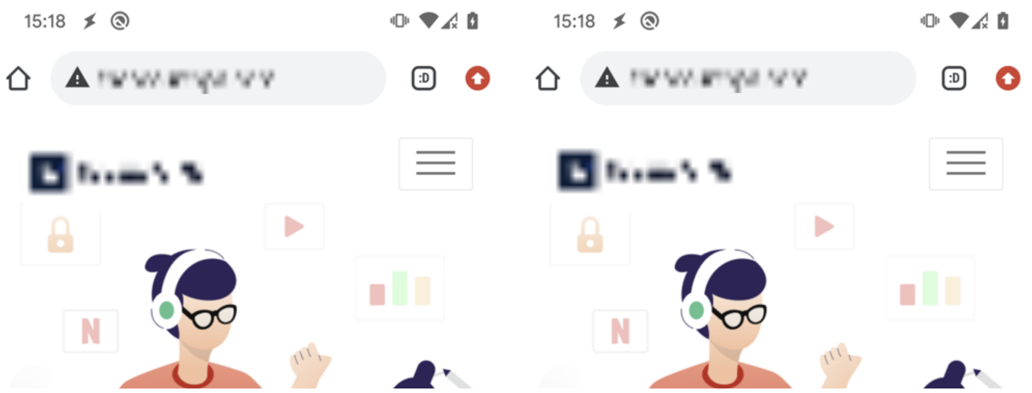
Offline

Posted [redacted] 2023 - [redacted]

need id cards of UAE Or Saudia Arabia with numbers

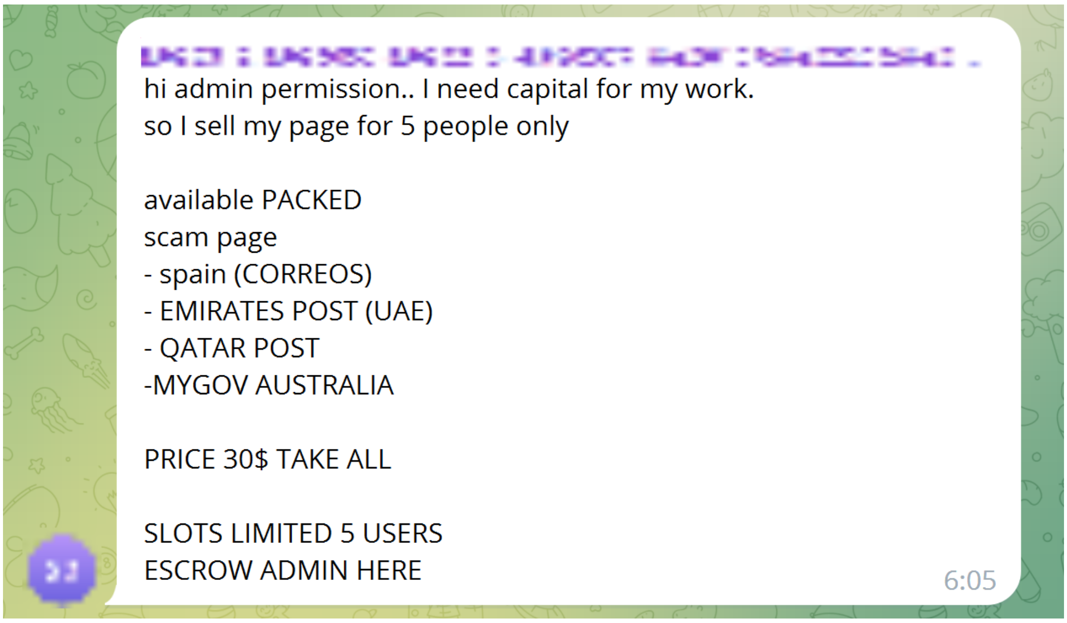
Furthermore, some of the announcements included requests for collaboration. For example, one attacker needed a native Arabic speaker to translate a phishing page for attacking users in the Middle East.

Figure 8. Collaboration proposal



In some ads, the criminals offered ready-made solutions for phishing attacks, including fraudulent websites masquerading as official delivery services such as Emirates Post and Qatar Post. Buying ready-made solutions can enable even inexperienced criminals to carry out successful attacks.

Figure 9. Collaboration proposal



[redacted]

hi admin permission.. I need capital for my work.
so I sell my page for 5 people only

available PACKED
scam page
- spain (CORREOS)
- EMIRATES POST (UAE)
- QATAR POST
-MYGOV AUSTRALIA

PRICE 30$ TAKE ALL

SLOTS LIMITED 5 USERS
ESCROW ADMIN HERE

6:05

Worldwide, social engineering typically exploits common human emotions, whether it's fear, irritation, greed, or hope. Attackers manipulate these emotions, convincing the victim to take impulsive and thoughtless actions. Remember that vigilance is the best defense against social engineering.

Spyware: what it steals and how to defend against it

According to our data, cybercriminals employed malware in seven out of 10 successful attacks on individuals in the Middle East region. More often than not, the attackers infected users' devices with spyware (60% of attacks involving malware). This form of malware collects information from the infected device and then passes it on to the attacker. Depending on the task, spyware can steal personal and financial data, user credentials, as well as files from the device's memory.

For instance, the spyware KingsPawn, discovered in 2023 (including in the Middle East), can not only track the victim's location, record phone conversations, and manipulate files in the smartphone's memory, but also record audio from the infected device's microphone and capture images from both front and rear cameras. The program then erases any traces of malicious activity. Furthermore, KingsPawn is focused on iOS devices and can even generate iCloud TOTPs (time-based one-time passwords) for arbitrary dates. This enables continuous exfiltration of user data directly from cloud storage.

Spyware is designed to be difficult to detect, ensuring it remains on the victim's device for as long as possible. Often, spyware contains additional functions in its code that are characteristic of other types of malware, such as loaders, tools for remote control, stealers, or banking trojans. Loaders are used to distribute malware, including spyware. Their primary objective is to compromise the device and then download and install the targeted malicious payload. As a rule, loaders are designed in such a way that antiviruses do not recognize them as threats, which allows attackers to gain access to a compromised device and control the infected system. These modules help to hide the operation of malware from users and security systems.

Here's a typical spyware infection scenario:

1. Through social engineering, users are tricked into downloading a spyware loader. Cybercriminals distribute their products through phishing websites and emails, instant messengers, and text messages. The loader can be hidden in a seemingly harmless document or embedded within an application. In every fourth attack using spyware (28%), cybercriminals disguise malicious tools as official applications from well-known developers. In some cases, attackers even manage to publish their tools on official app stores.
2. After obtaining the necessary permissions for illicit activity on the device and establishing a connection with the attacker-controlled server, the loader downloads and installs the malicious spy modules.
3. The installed malware collects information from the infected device: it records keyboard inputs, takes screenshots, intercepts credentials from browsers, email clients, messengers, and configuration files, and steals payment data from mobile banking apps. Next, the program sends the information to the attacker. This is done using a communication channel to the control server. Legitimate programs installed on the device can also be used. For example, the spyware CodeRAT, targeting Farsi-speaking developers, used a publicly available Telegram bot API for anonymous file uploads.

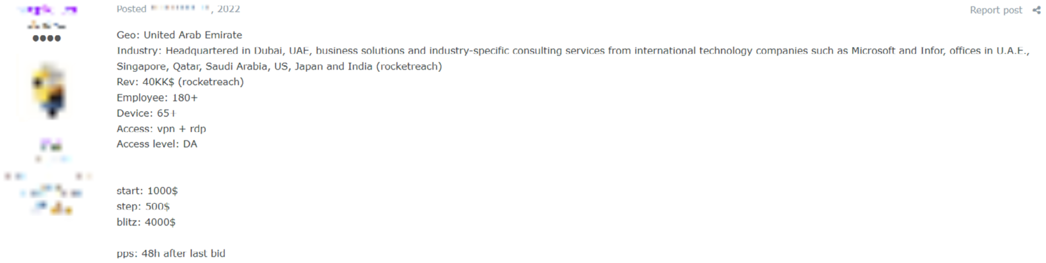
The spyware used by cybercriminals can be roughly divided into two groups. Spyware from the first group is distributed through the malware-as-a-service (MaaS) model or as open-source code. Criminals develop malware and pass it on to other criminals who actively deploy it. Often, these types of malware are used in mass attacks. For instance, at the beginning of 2023, bank customers in the UAE fell victim to a new version of the banking trojan Xenomorph, which stole not only payment data but also actual funds. Furthermore, researchers discovered an advertising website designed to distribute this malware through the MaaS model. Experts believe that attackers intend to carry out large-scale malware distribution in this way.

The second group consists of programs used in targeted, carefully planned multi-stage attacks known as advanced persistent threats (APTs). APT groups are highly skilled criminal teams with substantial funding and technical equipment. They often use tools they've developed themselves, including spyware. In the Middle East, a whole galaxy of such programs is used: PlugX, the Jackal module family, SandStrike, FurBall, and LazaSpy.

Consequences for organizations

With the help of spyware, attackers can compromise not only personal and payment information or data from social media accounts, streaming services, and other resources for personal use. The stolen information may include corporate credentials, organizational network connection details, and other sensitive information. The stolen data is put up for sale on shadow forums. As a result, a highly skilled attacker who gains access to an organization can carry out a successful attack, leading to non-tolerable consequences for the company: disruption of technological and business processes, theft of funds, leakage of confidential information, as well as attacks on customers and partners.

Figure 10. Announcement for the sale of VPN and RDP access


[redacted]

Posted [redacted], 2022

Geo: United Arab Emirate
Industry: Headquartered in Dubai, UAE, business solutions and industry-specific consulting services from international technology companies such as Microsoft and Infor, offices in U.A.E., Singapore, Qatar, Saudi Arabia, US, Japan and India (rocketreach)
Rev: 40KK$ (rocketreach)
Employee: 180+
Device: 65+
Access: vpn + rdp
Access level: DA

start: 1000$
step: 500$
blitz: 4000$

pps: 48h after last bid

In October 2022, ESET researchers analyzed a cyberespionage campaign launched by the POLONIUM group. The group targeted more than a dozen organizations in Israel, including marketing and insurance companies, media, and social services. Experts suggest that the attackers initially gained access to the target systems using compromised VPN credentials, which had been previously exposed to the public.

Earlier in the year, we wrote about the increasing use of spyware in attacks against individuals worldwide. Users in the Middle East should also pay attention to this because the use of spyware in the region during the period from the start of 2022 to Q1 2023 was higher (60%) than the global statistics for 2022 (43%).

The easiest way to protect against spyware is during the infection stage. To keep your data safe, follow these simple and effective tips:

- Do not install applications from unreliable sources. Cybercriminals sometimes manage to place their products in official app stores, so we advise you to always check information about the developer and the upload date, and carefully study the user reviews before installing.
- Use an antivirus. This will help to protect your device from infection in case it encounters any malicious files.
- Keep an eye on the permissions that apps request during installation and do not grant permissions that are clearly unnecessary for the app to work.
- Keep an eye on your device's performance. If your battery suddenly starts draining faster, mobile Internet traffic sharply increases, or Wi-Fi or geolocation services turn on spontaneously, this could indicate spyware activity.
- Do not open suspicious attachments on social networks and in instant messengers, especially if you do not know the sender very well. Archives and files with provocative names, whether with unfamiliar extensions or familiar ones (.pdf,.xls,.doc), could contain malicious scripts or links to phishing resources.
- If you download a program from the Internet, make sure it's from a reliable source. Carefully check the address in the browser bar: phishing site addresses often resemble official ones but with slight modifications that may go unnoticed at first glance, such as an extra letter or one letter replaced with another similar one. Examine the content of the site: cybercriminals might neglect the details, creating only a basic landing page and leaving sections like "Contacts" or "Privacy Policy" empty. Typos and low-resolution images can also be signs of a fake. Pay attention to payment methods. If a website only accepts bank transfers, that's a reason to be suspicious.

Targeted attacks

In targeted attacks, cybercriminals act against a particular group of individuals or a specific user. In such attacks, the criminals change their approach: they first carefully study the victim and then engage in a long and systematic operation.

APT groups: advanced threats

During the period under consideration, APT groups actively targeted not only organizations but also private individuals in the Middle East. These hacker groups intensively exploit vulnerabilities, both known and zero-day, and often are the first to employ new attack methods.

For instance, in mid-2022, the hacker group CharmingKitten used the Multi-Persona Impersonation technique in attacks on individuals. Instead of a single phishing email, the perpetrators engaged in a lengthy exchange of carefully thought-out messages, using multiple fake identities of journalists and colleagues from other countries. At the end of such an exchange, the victim receives an infected document under the pretext of, for example, checking the accuracy of interview responses. Upon opening the file, spyware is loaded onto the device.

Attackers use both publicly available and proprietary tools to successfully compromise even systems considered well-protected.

All APT groups are well-prepared and pose a significant threat to the network. Here are a few examples of APT groups that targeted private individuals in the Middle East:

- CharmingKitten—one of the most well-known and active groups in the region. They employ advanced social engineering techniques in attacks on individuals and use various types of their own malware.
- Bahamut—this group uses malicious fake applications and phishing messages and websites. The criminals have been observed attacking a wide range of different targets. Experts believe that this group works for hire.
- GoldenJackal—since 2019, this group has been spying on officials and diplomats in the Middle East using a whole family of their own malicious modules. The criminals operate covertly, carefully selecting their victims and keeping the number of attacks to a minimum to reduce the risk of exposure.

Hacktivists

Some of the targeted attacks were carried out by hacktivists. In these cases, the criminals attempted to inflict the maximum material and reputational damage on the victim. The primary motive of such attacks was not to gain financial profit but to achieve political goals and draw attention to social or religious issues. Sometimes the cybercriminals targeted a specific individual using various means. After a successful attack, the hacktivists widely disseminated the stolen personal data of the victim.

> We strongly recommend making it a first step to verify the authenticity of interlocutors before engaging in further correspondence. Criminals might present themselves as journalists or employees of real organizations. To avoid being deceived, cross-reference information about the interlocutor with contacts from official sources.

Conclusions

The Middle East is a region where the latest cyberattack techniques are actively employed and well-trained cybercriminals operate.

Users are victims of large-scale phishing campaigns based on major events and current news topics, as well as targeted attacks from various groups and hacktivists. The attackers embedded security certificates into phishing sites and assumed real identities in targeted communications to make the fraud harder to recognize.

The main threat to devices has become spyware infections. Cybercriminals distributed both spyware acquired on dark web and their own programs, which have a wide range of functions. This type of malware was actively used in targeted attacks, often motivated by political reasons.

Ongoing geopolitical tensions, internal political events, and religious conflicts create fertile ground for cybercriminal activities. Hacktivist groups are gradually becoming a more serious threat and their methods are becoming more sophisticated, enabling them to attack increasingly significant targets. The proliferation of ready-made kits and tools for conducting cyberattacks, which don't require high-level skills to use, contributes to the emergence of new attackers.

Many countries in the Middle East region are taking measures to combat cybercriminals, both technically and legislatively. Nevertheless, individuals need to remain vigilant, prioritize their own security when communicating online, closely monitor their devices' activity, and promptly install security updates.

Companies also need to ensure the security of employee and customer data. Data breaches cause reputational and financial damage and put at risk users whose information has been compromised. To prevent cybercriminal actions from having non-tolerable consequences, such as user fraud, we recommend organizations to focus on their resilience to cyberattacks. To maintain cyberresilience, it's essential to regularly assess the effectiveness of security measures and pay special attention to verification of non-tolerable events.

About the report

This report contains information about current information security threats impacting individuals in the Middle East region, based on Positive Technologies own expertise, as well as data from reputable sources. Our study focuses solely on successful cyberattacks or incidents negatively affecting individuals. This report covers incidents in the following countries: Bahrain, Egypt, Israel, Jordan, Iraq, Iran, Yemen, Qatar, Cyprus, Kuwait, Lebanon, United Arab Emirates (UAE), Oman, the State of Palestine, Saudi Arabia, and Syria.

We estimate that most cyberattacks are not made public due to reputational risks. As a consequence, even companies specializing in incident investigation and analyzing hacker activity are unable to calculate the precise number of threats. Our research seeks to draw the attention of individuals and companies who care about the state of information security to the key motives and methods of cyberattacks, as well as to highlight the main trends in the changing cyberthreat landscape in the Middle East.

This report considers each mass attack (for example, phishing emails sent to multiple addresses) as one incident, not several. For explanations of terms used in this report, please refer to the Positive Technologies glossary.

ptsecurity.com
pr@ptsecurity.com

Positive Technologies is an industry leader in results-oriented cybersecurity and a major global provider of information security solutions. Our mission is to safeguard businesses and entire industries against cyberattacks and non-tolerable damage. Over 3,300 organizations worldwide use technologies and services developed by our company.

Positive Technologies is the first and only cybersecurity company in Russia to have gone public on the Moscow Exchange (MOEX: POSI), with 180,000 shareholders and counting.

Follow us on social media (Twitter, Habr) and in the News section at ptsecurity.com.