kaspersky

2024

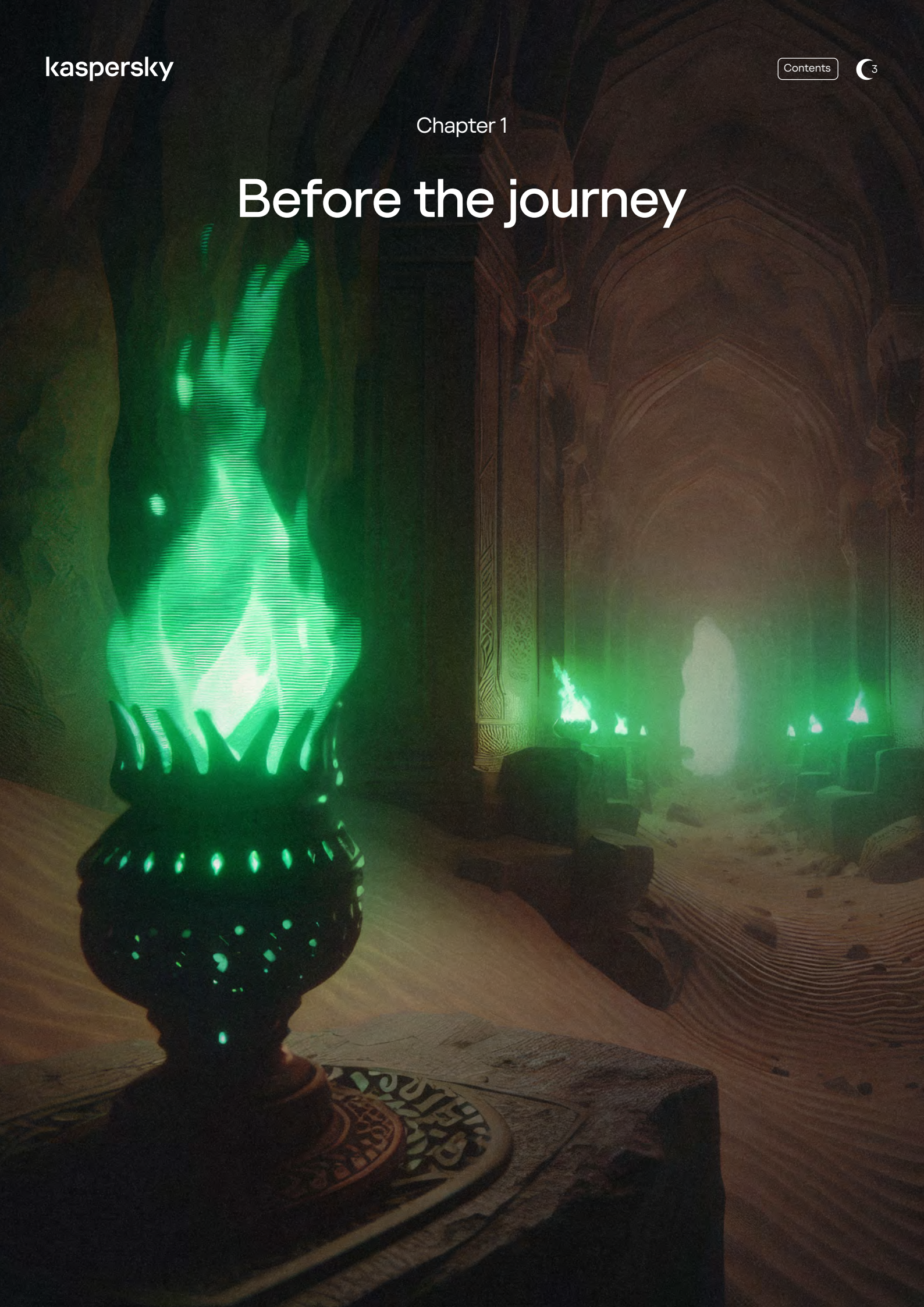
Analytical report

Whispers from the Dark Web Cave

Cyberthreats to the Middle East

Chapter 1

Before the journey



Before the journey

Today, when a multitude of illicit activities are conceived, initiated, discussed, and developed in the dark web, when malicious actors (groups, individuals, and services in the black and gray markets, etc.) exhibit constantly evolving approaches, tactics, techniques, and tools, it is essential to monitor cyber threats.

The rationale behind this report is to highlight the most severe and pervasive threats that dark web cybercriminals posed to the organizations and, in particular, the governments of Arab countries in the first half of 2024. More specifically, it will identify what the potential risks and consequences are. This will allow organizations and governments to stay a step ahead of the cybercriminals and, thus, prevent attacks or other fraud before they compromise network infrastructure or operational integrity.

Data was collected and analyzed for the following countries:


Bahrain


Egypt


Iraq


Jordan


Kuwait


Lebanon


Oman


Palestine


Qatar


Saudi Arabia


Syria


United Arab Emirates

We analyzed publications, posts, and messages on various resources from all layers of the dark web, including:


An archive of web intrusions and defaced web resources


Chats and channels in Telegram (both public and private)


Cybercriminal forums (publicly available ones and those with limited or private access)


Blogs of ransomware groups


Shadow marketplaces


Other onion resources used by cybercriminals

Setting foot on treacherous sands

The dark web [1], usually refers to a hidden part of the Internet that is not indexed by search engines (such as Google). More descriptively, the dark web can be compared with a vortex in the desert sand — as you go deeper, you traverse different layers that differ mainly in how accessible they are.

1

Dark web

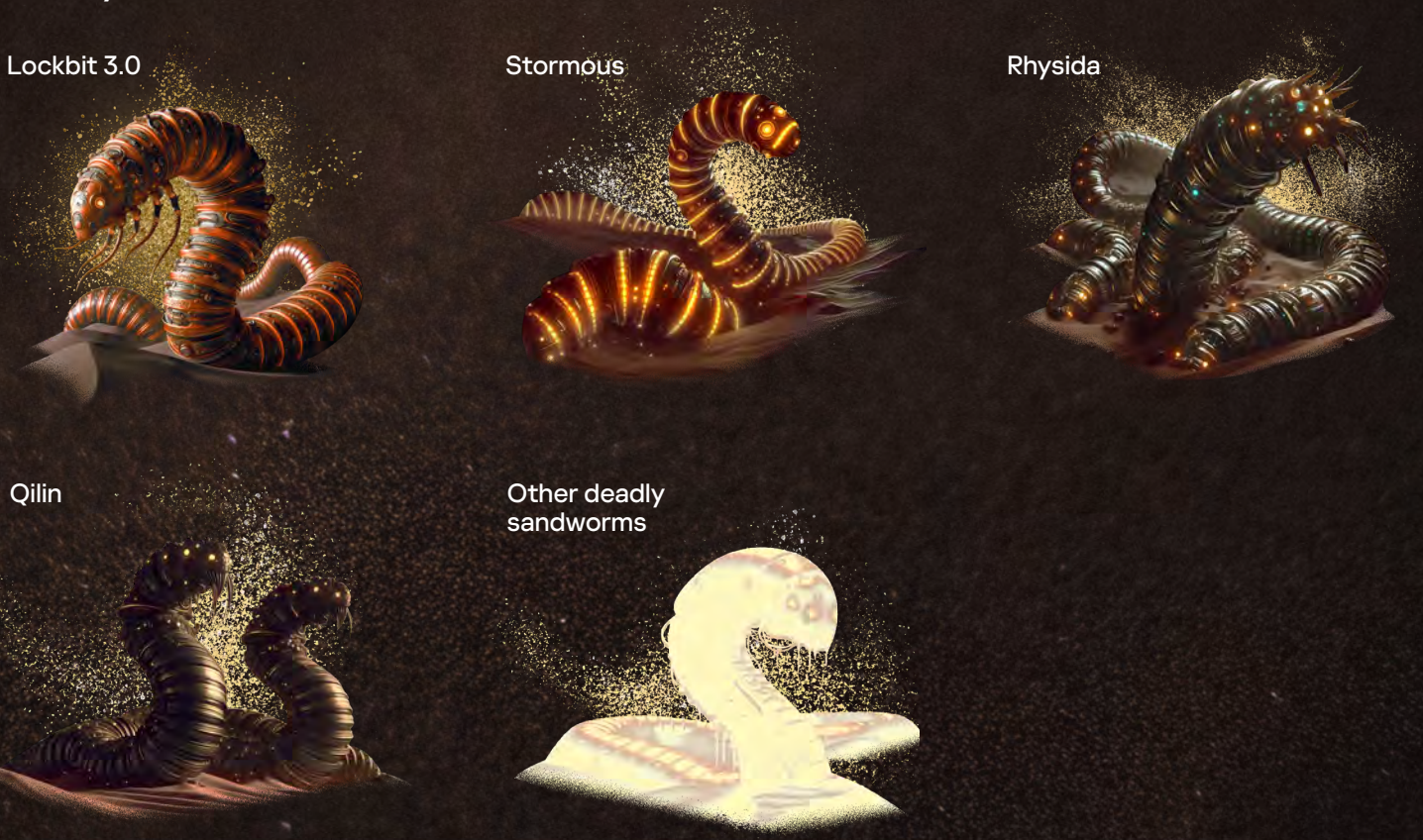
Major hazards

Our investigation shows that the main cyber threats that the governments and organizations in the Middle East face are the following:

Ransomware groups

There were **19 ransomware groups** operating in the region in H1 2024. An analysis of posts on their blogs shows that they executed at least 45 attacks against various companies mainly in the UAE and Saudi Arabia. The most active gangs were Lockbit 3.0, Stormous, Rhysida, and Qilin. Together, they are behind the attacks on 58% of the organizations affected. As for the industries targeted, our research revealed that the top 3 were the public sector, construction, and business services [2].

Deadly sandworms



2

Companies in the business services industry do not create or deliver any certain product, but support other businesses providing consulting, marketing, research, construction, financial, legal, and other services.

Hacktivists

Hacktivist activities are on the rise this year, forming one of the most critical threats in the Middle East and primarily to the UAE, Saudi Arabia, Egypt, Jordan, and Bahrain. Initially, such activity tended to take the form of denial of service, but attacks have recently become more destructive, aiming to completely compromise the target organizations and leak data. For example, in the spring, hacktivists disrupted mobile networks in Bahrain for two days [3] and hacked various government entities in the region [4, 5, 6, 7].

3 Bahrain telecom DDoS

4 Cyberattack on the UAE

5 Anonymous targeted UAE Gov

6 Egypt ministry breach

7 Anonymous striked KSA

Top-5 countries most threatened by hacktivists

Shadow jewelry fair

Initial corporate accesses (entry points into the corporate networks) to companies and organizations across the Middle East are hot targets for cybercriminals. They are exploited by various cybercriminals or groups (such as ransomware gangs, hacktivists, or APT groups) to further develop their attacks. In total, for the first half of 2024, we discovered over 40 ads offering corporate access to government, education, manufacturing, transportation, financial, healthcare, IT, and other organizations as well as posts selling access to various corporate devices, servers, and systems.

Industries under attack in H1 2024

Malicious whistleblowers

Info stealers aim to gather as much sensitive data as possible from infected devices, which may then be published by attackers operating malware as logs in the dark web. In total, we discovered and analyzed almost 10 million records related to users or resources in the Middle East published in various malware logs in H1 2024. The most notable examples of malware on the market are RedLine, Lumma, and RisePro. Together, they account for about 82% of the total activity.

Top-3 Info stealers

RedLine

Lumma

RisePro

Cave raiders

Multiple publications on data breaches (including both leaked data and documents) were discovered. In total, for H1 2024, cybercriminals shared or traded 125 corporate-related databases leaked from organizations in different industries, but primarily from government agencies (25% of all breaches), education institutions, and retail companies. Saudi Arabia, Iraq, and Egypt are the top 3 countries by the number of databases shared.

Top-3 industries suffered from data breaches in H1 2024

Government

Education

Retail

Top-3 countries by the number of databases shared

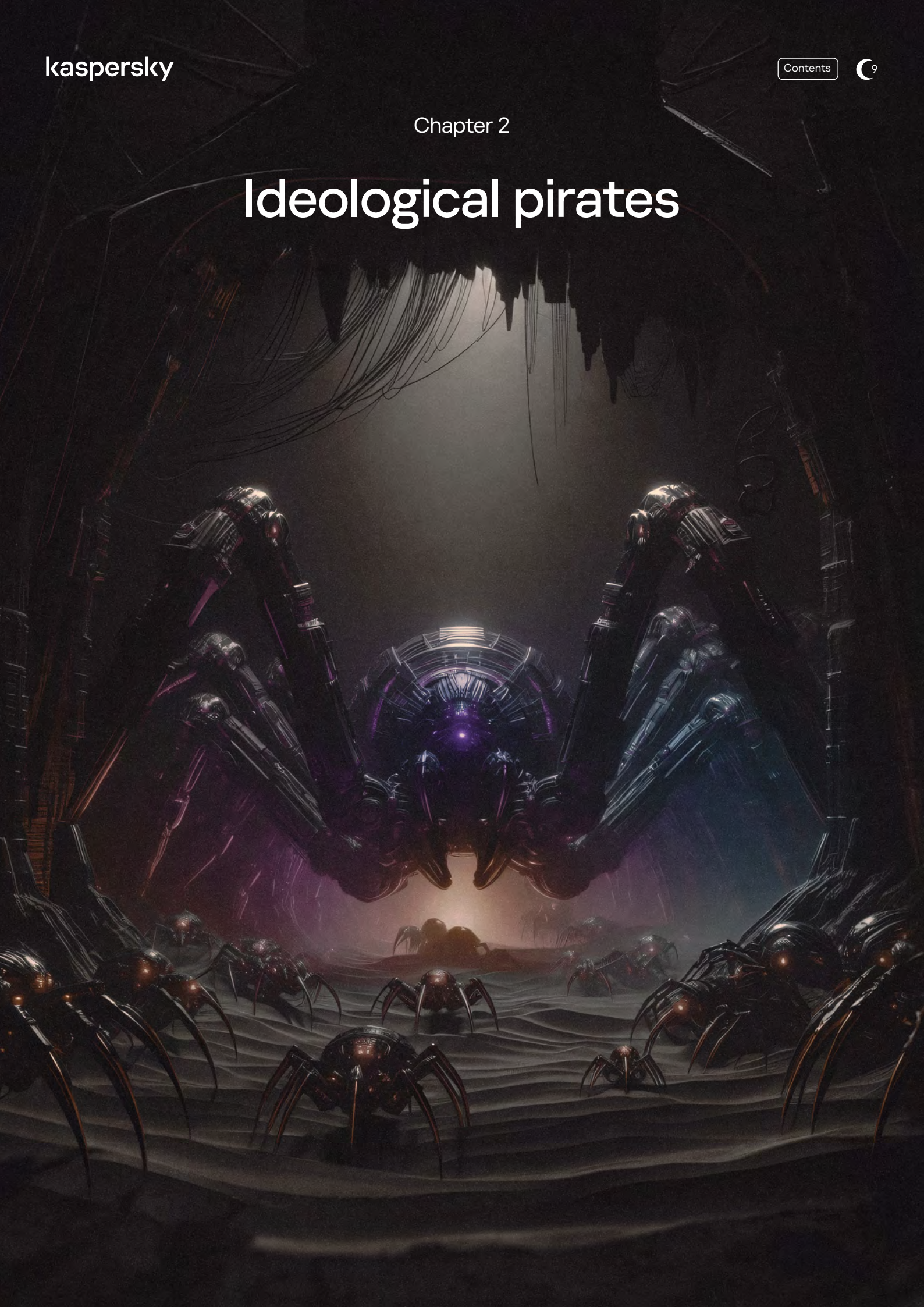
Saudi Arabia

Iraq

Egypt

Chapter 2

Ideological pirates



Ideological pirates

In the simplest terms, hacktivists are ideologically motivated cybercriminals or groups who, due to their principles, convictions, or beliefs, carry out attacks on specific targets or regions in reaction to certain social or political issues and events. Naturally, however, motivations vary from financial gain, espionage, confidential data theft, or other such gain, to personal animosity and so on.

Hacktivist movements have long been active in the Middle East — waves of ideologically motivated attacks occur all the time with varying severity. One of the most infamous umbrella groups is Anonymous. It is in fact not just a group of cybercriminals but an international cybercriminal community primarily known for carrying out cyberattacks against government agencies worldwide.

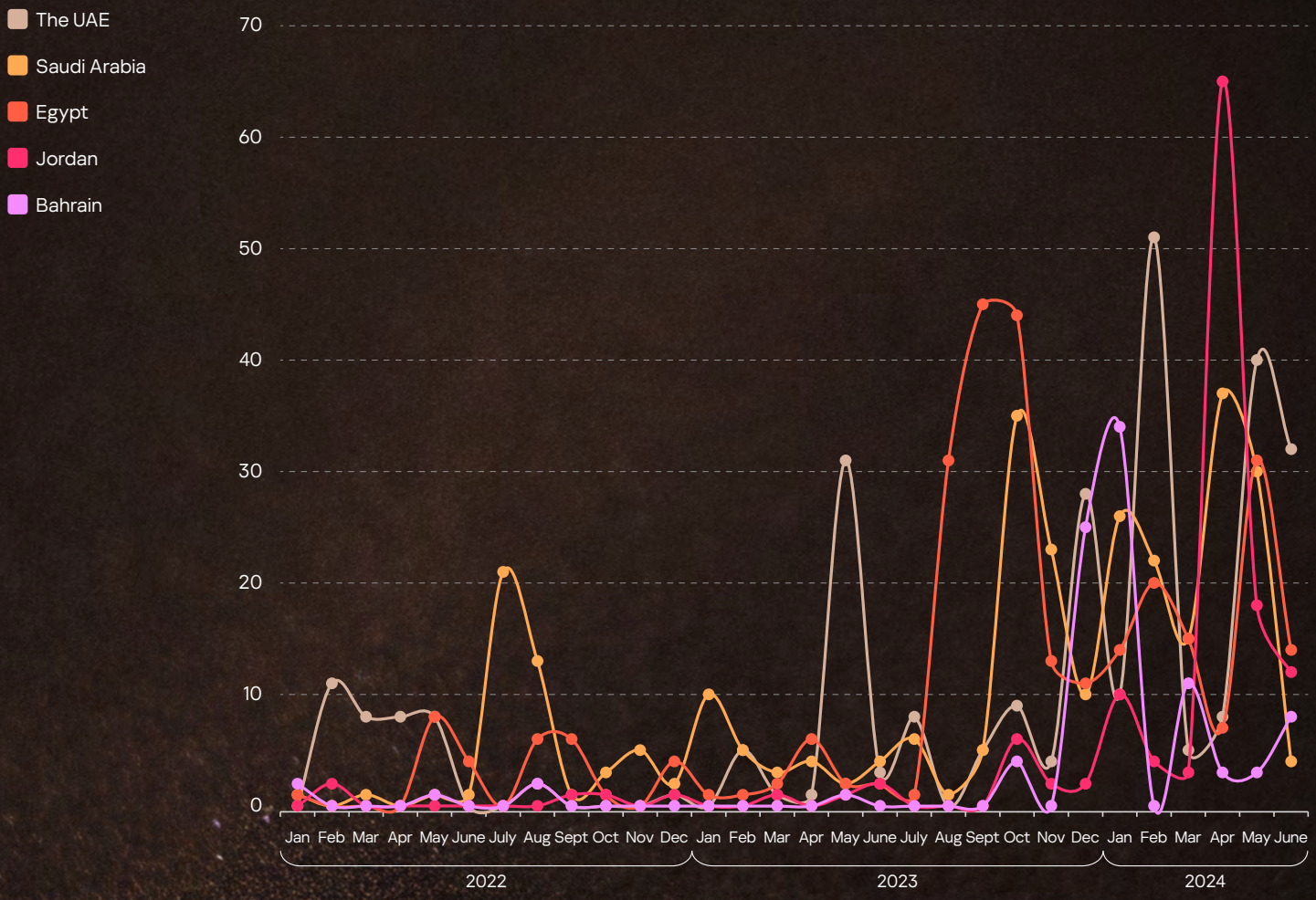
However, hacktivist activity today is fundamentally different than what it was in the past:

It has gone global — hacktivists have formed two opposing coalitions in relation to the Israel-Palestine conflict in the region. Meanwhile, there are smaller groups who target organizations, industries, or countries regardless of geopolitics, but simply to spread chaos.

Attacks have become more destructive — they used to focus on denial of service, website defacement, or doxing, but now, the focus is shifting to more critical outcomes like data leaks and the wholesale compromise of network infrastructure.

We observed more than 11 movements and various actors primarily targeting the UAE, Saudi Arabia, Egypt, Jordan, and Bahrain in H1 2024. The distribution of hacktivism-related messages by month from 2022 is presented in the chart below.

Figure 1 | Distribution of hacktivism-related messages from 2022 to H1 2024. Top-5 affected countries



Various organizations, including critical infrastructure firms, government agencies, and anything tied to main government domains (gov.tld) faced such malicious activity in H1 2024, as did countless other companies in the countries in question.

Figures 2, 3, 4 | Examples of attack announcements for different countries

Among the most critical attacks were the hacking of Saudi and Emirati government infrastructure [8, 9], a leak of data from Egyptian state resources [10] in May, the disruption of mobile networks in Bahrain for two days in March [11], and the shut-down of Thuraya [12], an international mobile-satellite service (MSS) provider based in the UAE in January 2024.

8
Cyberattack on the UAE

9
Anonymous striked KSA

10
Egypt ministry breach

11
Bahrain telecom DDoS

12
Telecommunications

Figures 5, 6 | Disruption of mobile networks in Bahrain for two days in March 2024

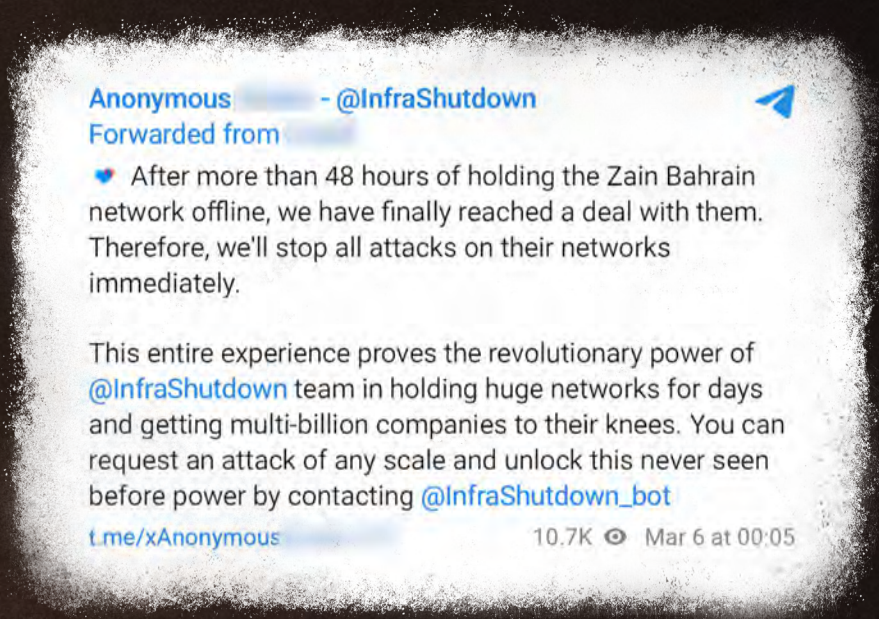


Figure 7 | General update on the status of attacks on Saudi Arabia

Figure 8 | Announcement of the critical attack on the MSS provider Thuraya

Chapter 3

Shadow jewelry fair

Shadow jewelry fair

Common ways to gain initial corporate access

Via a combination of VPN and RDP

Via different shells (web, reverse, etc.)

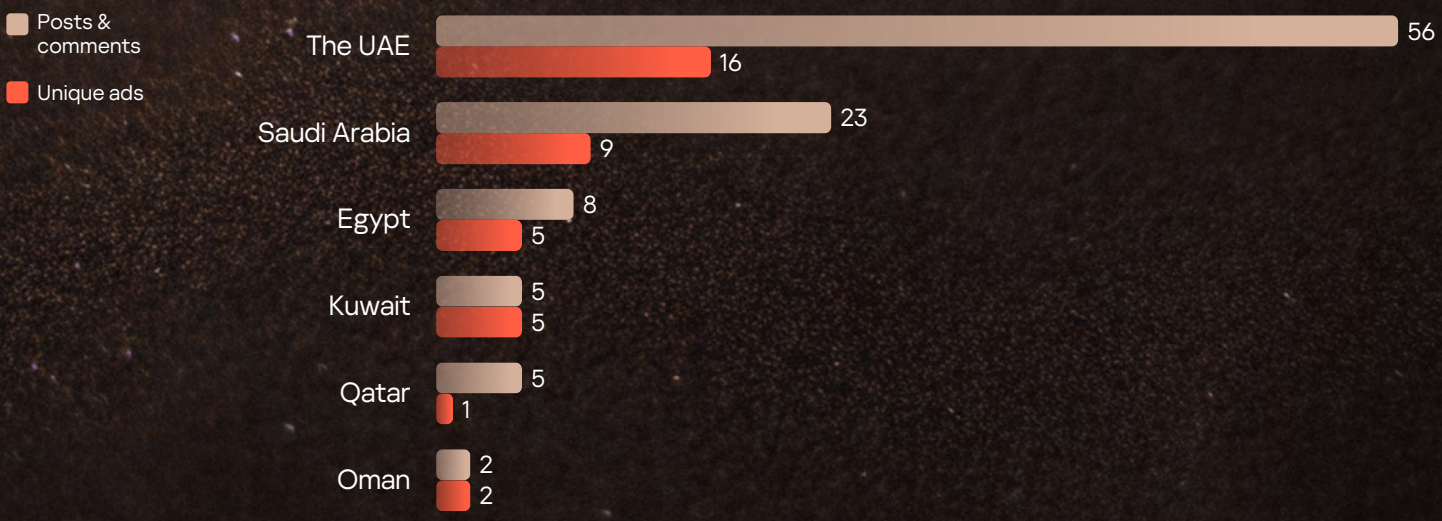
With info on the exploitation of RCE vulnerabilities and SQL injections

Initial access brokers are cybercriminals who specialize in obtaining initial access to the internal networks of different companies and then selling such entry points to other threat actors (e.g., ransomware groups). They do not develop attacks themselves for various reasons ranging from a lack of the technical skills or motivation to do so to the belief that their role in such attacks is relatively low-risk.

There are several common ways to gain initial corporate access: via a combination of VPN and RDP (Remote Desktop Protocol) to access separate corporate devices, servers, or systems available from external networks (control panels, firewalls, etc.), via different shells (web, reverse, etc.) or with info on the exploitation of RCE (remote code execution) vulnerabilities or SQL injections. If you want to get into more detail, take a look at our research on the initial access market in the dark web published in Securelist.

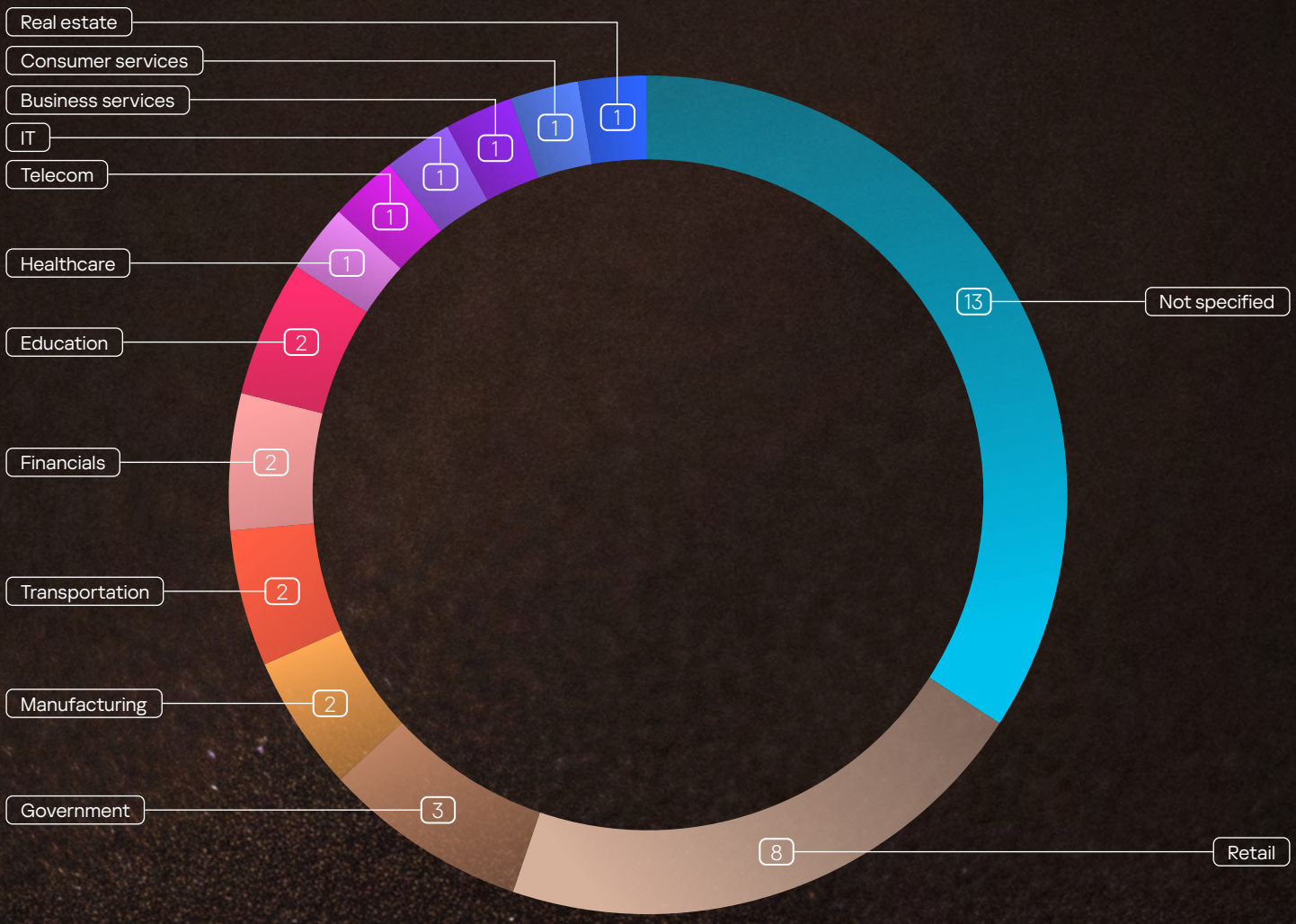
For the first half of 2024, we observed 38 unique ads offering initial access to organizations in various industries – government, healthcare, IT, manufacturing, financial, and others. We also found some posts selling packs of access to compromised corporate devices, servers, and systems (like various VPN clients that are usually used in corporate networks). However, since some cybercriminals have a reputation in the community as good initial access brokers, some malicious actors can also request access data directly. Such deals might be made without recourse to the dark web.

Figure 9 | Ads on initial accesses published in the dark web in H1 2024



Cybercriminals do not compromise themselves by publishing explicit details on the companies affected, just generalities like which country the HQ is in, the revenue, industry, and number of employees or hosts in the network (sometimes). Forewarning the companies in such a way would be self-defeating for cybercriminals who are going to attack these companies.

Figure 10 | Affected industries



Figures 11, 12 | Examples of posts from initial access brokers

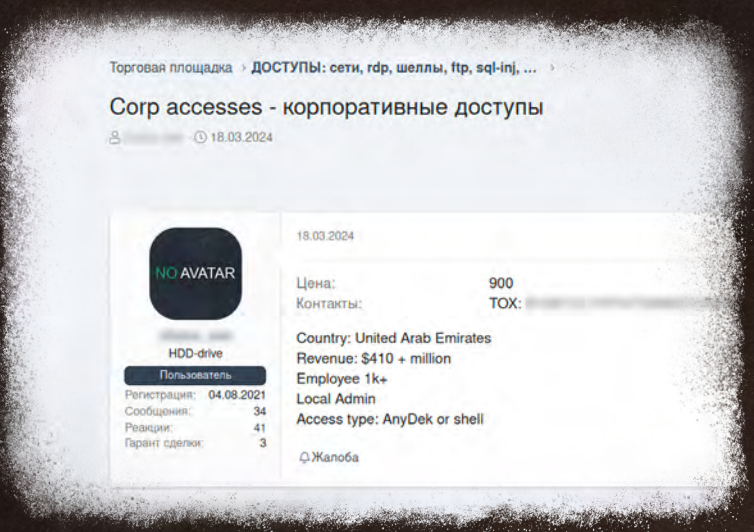
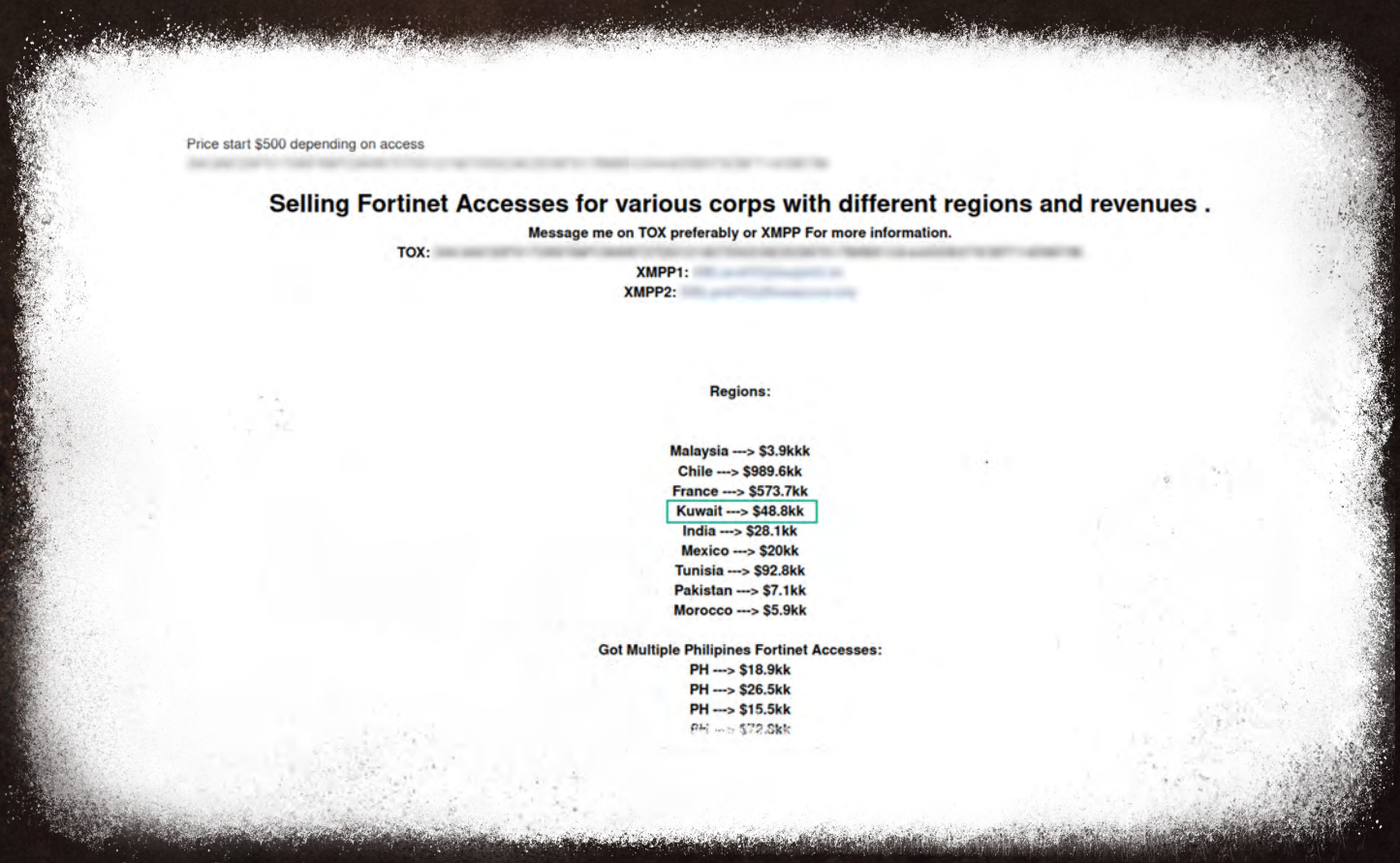


Figure 13 | Sale of accesses to Fortinet VPN clients



Chapter 4

Deadly sandworms

Deadly sandworms

In recent years, we have observed a rise in ransomware attacks targeting everyone — governments, high-profile institutions, critical infrastructure, enterprises, and small businesses. When we talk about ransomware attacks today, it's not about whether or not they will occur but how to safeguard against them or reduce their impact. After all, the main attack goal is to retrieve all sensitive data and encrypt the files and disks on all systems in the victim infrastructure.

Ransomware groups have become more organized and structured; everyone has a certain role delegated as needed given the prevailing objectives. Some are responsible for selecting targets and obtaining initial access — this intersects with what the initial access brokers described in the previous section do, and indeed, ransomware groups periodically buy corporate access in the dark web despite the restrictions on some forums [13]. Other members of the group carry out attacks and develop them across the victim networks, and yet others maintain blogs mainly in the private sections of the dark web but sometimes on public platforms. They publish information in ransomware blogs on all the latest successful hacks and, if no ransom is paid, publish the stolen data.

Moreover, in recent years, major ransomware players have launched Ransomware-as-a-service (RaaS) models, which lowers the entry threshold while significantly increasing the number of ransomware-related incidents. As such, the range of these attacks continues to expand year after year, making it critical to monitor all information security events, alerts, and incidents to trace potential attacks before it's too late.

13

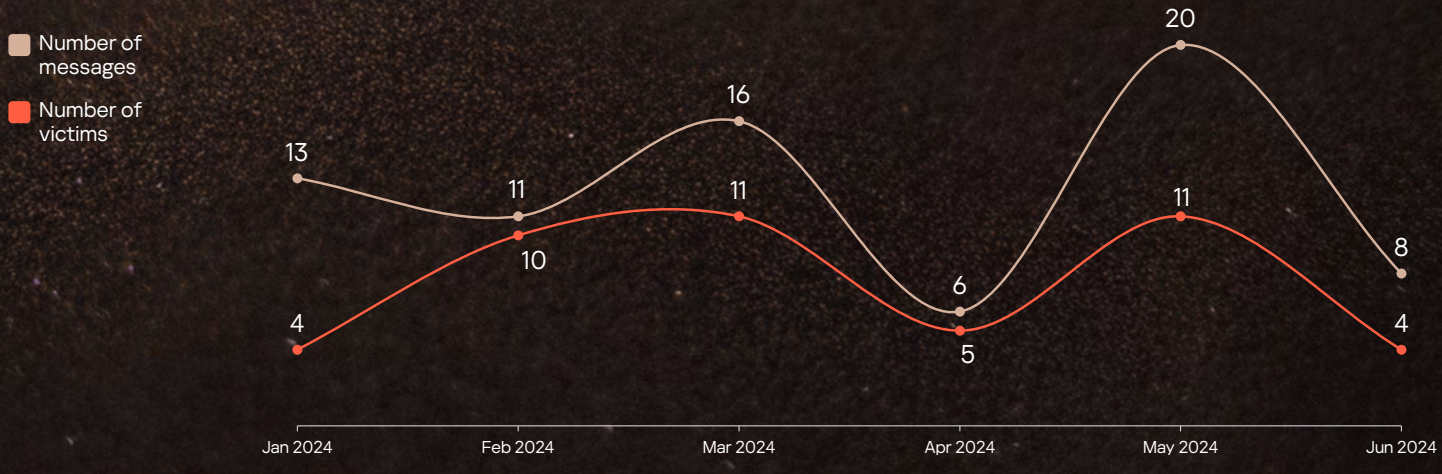
As a rule, dark web forums prohibit deals involving ransomware gangs.

Whispers from the Dark Web Cave — Cyberthreats to the Middle East

In total, for the first half of 2024 alone, 45 organizations in the Middle East covered here faced ransomware attacks. In the previous year, 63 fell victim in the same region for the whole year, 36 in the first half. Our analysis shows that the number of ransomware attacks in the Middle East increased year-to-year with some decline in the second half of the year.

Figure 14 | Ransomware attacks targeting ME countries from 2022 to H1 2024

Figure 15 | Ransomware attacks targeting ME countries in H1 2024



The most active ransomware groups in H1 2024 were Lockbit 3.0, Stormous, Rhysida, and Qilin — together, they attacked 58% of the organizations affected.

Statistics on ransomware attacks in H1 2024 for the Middle Eastern countries covered here are presented in the figure below. The UAE and Saudi Arabia suffered the greatest number of attacks from ransomware groups.

Top-4 ransomware groups

Lockbit 3.0

Stormous

Rhysida

Qilin

Figure 16 | Ransomware actors targeting ME countries in H1 2024

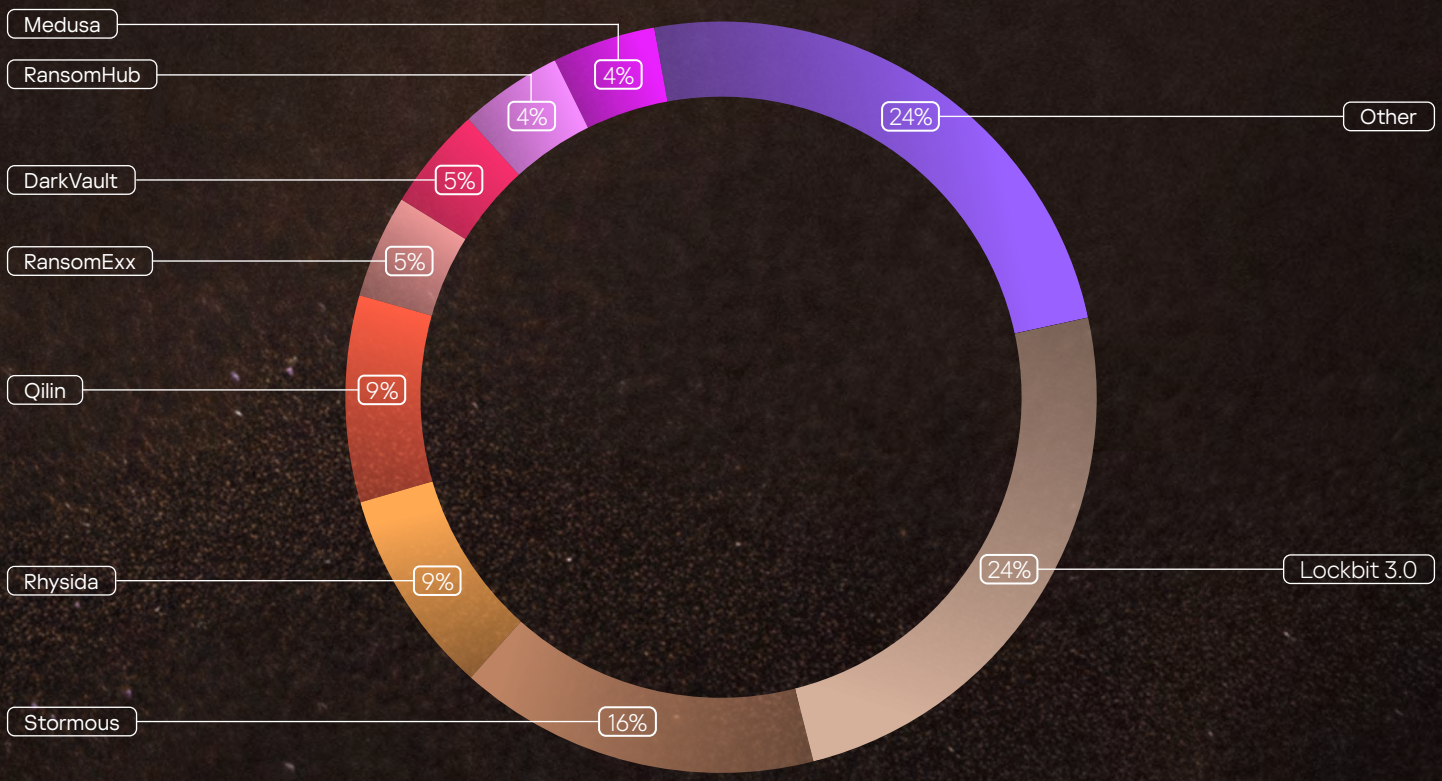


Figure 17 | Ransomware attacks in H1 2024. Statistics by countries

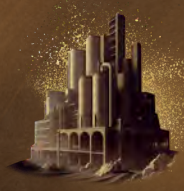
Ransomware gangs tend to be financially motivated, so they usually choose their victims based on potential gain as estimated from factors like revenue, industry, and so on. However, geopolitical events (such as the Israeli regional conflict) may cause them to shift their focus and areas of attack. Our research shows that government entities were the most affected by extortion in H1 2024. Construction companies and organizations providing business services rounded out the top 3.

Ransomware gangs usually choose their victims based on potential gain

Top-3 industries affected by extortion in H1 2024

Government

Construction



Business services

Figure 18 | Ransomware attacks in H1 2024. Statistics by countries

Chapter 5

Malicious whistleblowers

Malicious whistleblowers

An info (or, more generally, data) stealer is a form of malware, the main purpose of which is to covertly collect sensitive data from an infected device and send it for extraction. Such programs gather user credentials, financial data (either entered by users or stored on the system in a browser or elsewhere), website cookies, or personal or system details, or even take screenshots. The main threat that info stealers pose is not the infection itself, but how they intend to use the data they steal. Valid accounts or other authentication data (such as API keys, session cookies, tokens, or secrets) are in high demand on the dark web as they are used as entry points, initial vectors for further attacks, and info stealers are one of the ways threat actors can obtain them.

Since the malware-as-a-service (MaaS) model emerged on the dark web, info stealers have spread through the cybercrime field like a plague. Malware developers and operators build scalable complex network systems and sell access to their malicious infrastructure, with support, to a wide range of cybercriminals who don't have the technical skills to manage malicious botnets. Thus, subscribers gain access to the malware and only need to find and infect their victims. We analyzed the business model and market last year, see our detailed research, Understanding Malware-as-a-Service, published in Securelist.

Attackers use info stealers to collect a huge amount of log files from infected devices and then sell or distribute them on the dark web. If they mainly want to boost their reputation, they may only charge a nominal fee. However, cybercriminals tend not to publish fresh logs right after obtaining them. First, they spend time carefully analyzing the data they have collected to identify anything useful in their other activities (e.g., valid accounts for corporate systems and services, data on banking cards or e-wallets, and so on). Only then do they publish the logs on the dark web. That is why data leaked by info stealers is published with a time lag and why we still find data from 2022 and earlier in logs published in 2024.

Whispers from the Dark Web Cave — Cyberthreats to the Middle East

More than 40% of all info stealer activity in the Middle Eastern countries covered involves RedLine. Lumma (or LummaC2) malware, which only appeared on the info stealer market in the late 2022, takes second place with 22%.

Top-3 info stealers

RedLine

Lumma

RisePro

In total, almost 9.7 million lines (or records) of stolen user accounts were found in the logs of different info stealers published just in the first half of 2024. The total over the last four years is over 27 million lines of user credentials, which is just under three times more.

We conducted a special analysis of the records from major government entities. About 4.4 million lines in the logs published in H1 2024 contain the account info of employees of state institutions or were used to access various government resources (public services both for citizens and corporations).

Figure 19 | Info stealers activity

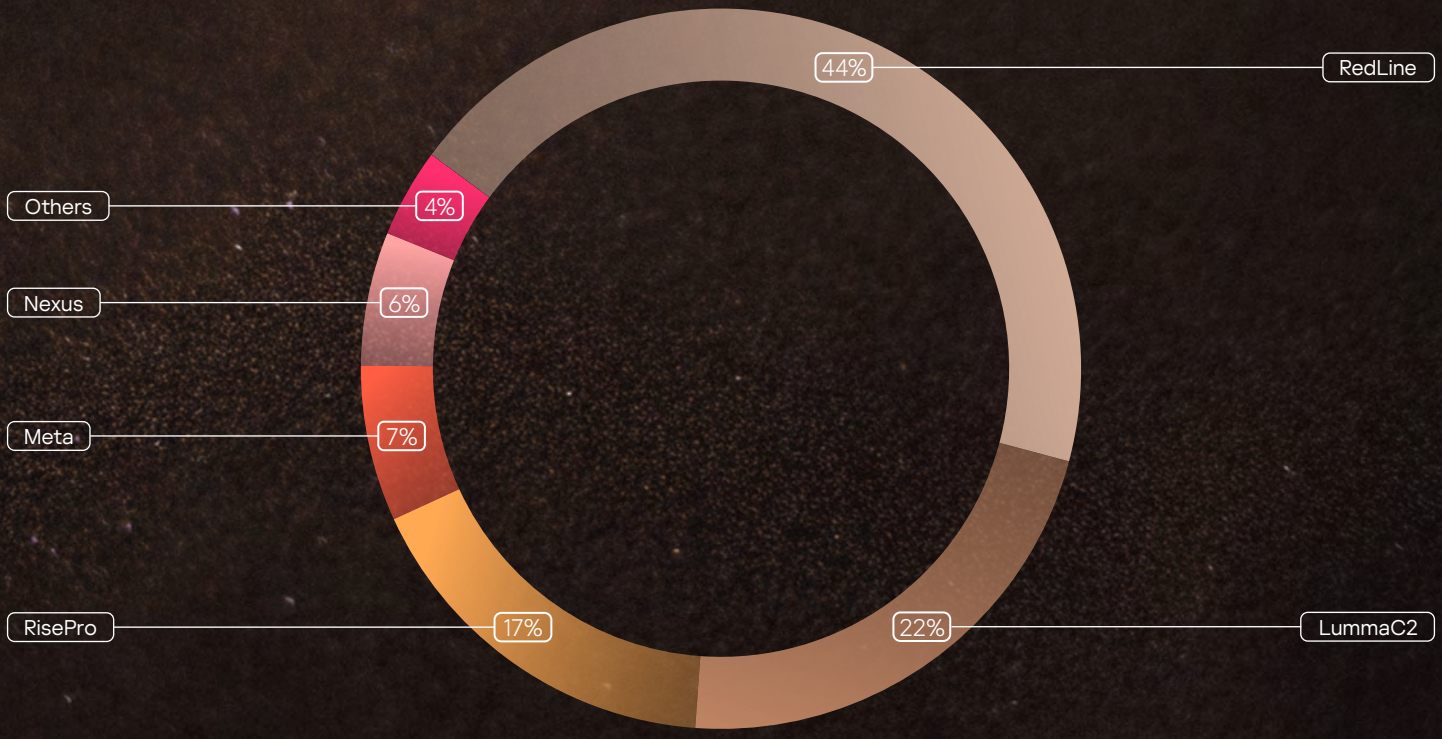
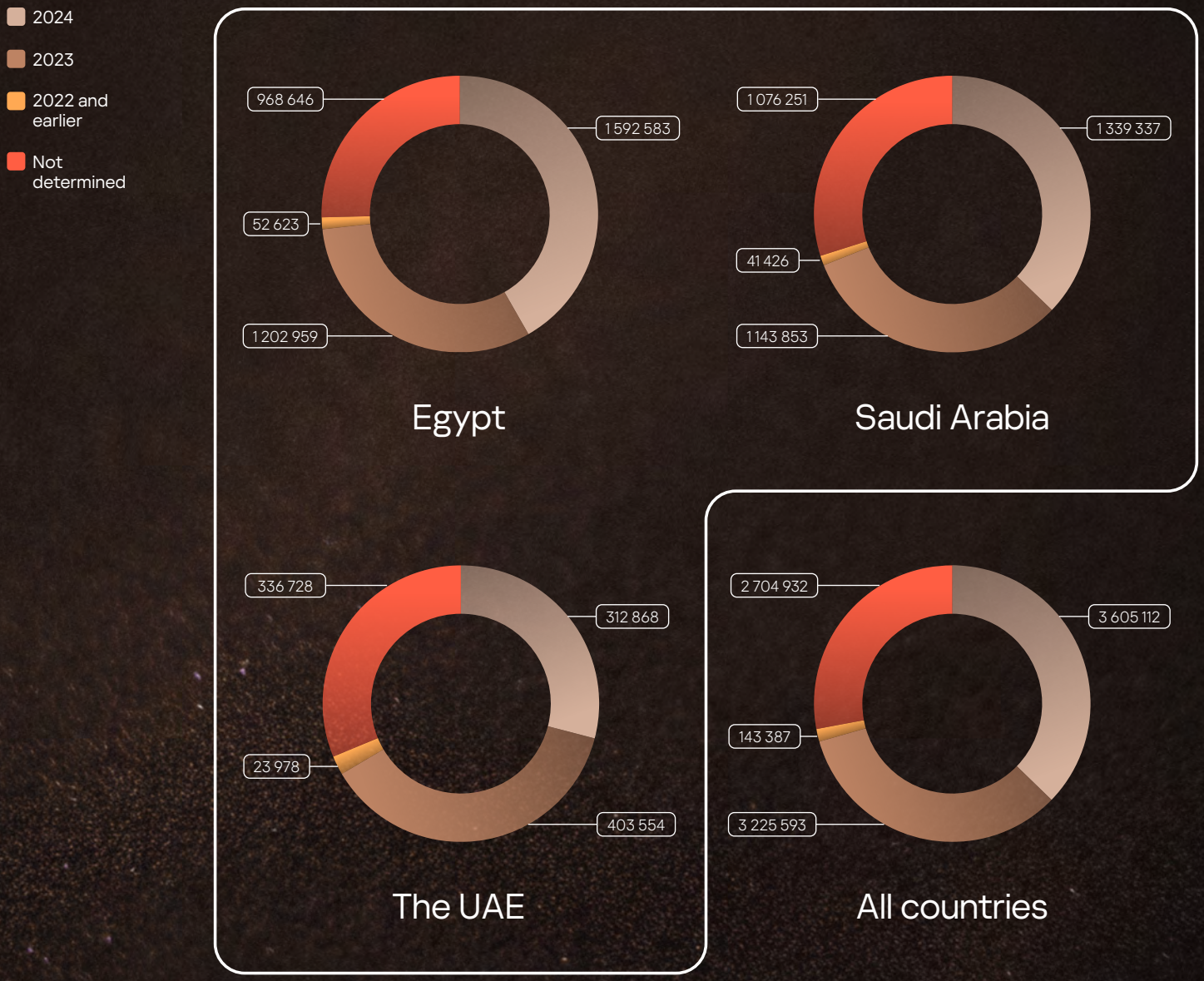


Figure 20 | Records from info stealers' logs published in the dark web in H1 2024

The statistics show that overall, info stealers are highly widespread in Egypt, Saudi Arabia, and the UAE. As for government resources, the top three countries are the same.

The following diagram shows that a third of all records published in malware logs in H1 2024 contain accounts leaked in 2023, while a few records are from 2022, 2021, or earlier.

Figure 21 | Statistics on years of account compromise. Records published in H1 2024. Top-3 countries



Chapter 6

Cave raiders

Cave raiders

Another common activity among cybercriminals is sharing or selling data breaches, including lists of credentials to various resources, databases with sensitive information (personal on staff or clients, financial data, etc.), confidential corporate documents, and anything else that might come in handy in future attacks.

The data offered is usually divided into three main groups:

1

The first type, associated with the most severe threat, is data leaked from companies, applications, or services as a result of intentional activity (of hackers or malicious employees — insiders) or even leaked incidentally (due to insecure behavior or mistakes on the part of employees). Obviously, such breaches are considered more valuable because the leaked info is more useful and reliable, hence sensitive, thereby providing more attack opportunities.

2

The next type involves combinations from, and reposts of, previous breaches still in demand. Cybercriminals usually set a short expiration date for shared files, so the content is only available for a limited time.

3

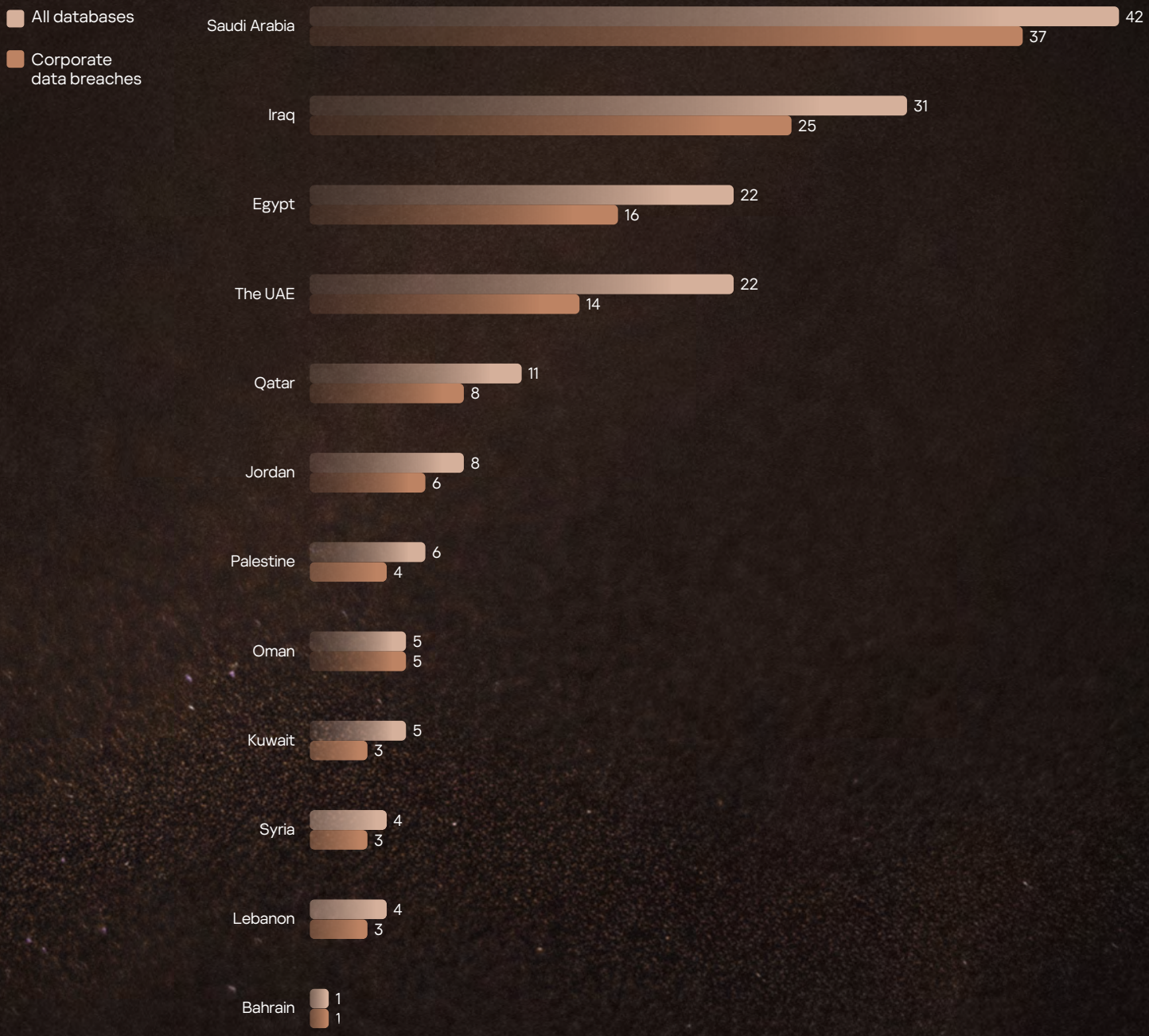
The last group includes target lists containing information on specific groups of victims — by volume of income, residence, industry, or ownership type (e.g., car, apartment, house, real estate, etc.).

Cybercriminals use breached data to commit a huge range of fraud: from common spam and phishing activities targeting staff, clients, partners, or other affiliated people to blackmail, targeted attacks using victim profiling, social engineering, and supply-chain attacks.

For the region and period in question, over 160 databases with information on citizens, companies, or entities were being traded or distributed. According to their descriptions, 125 of them came from corporate data breaches.

Our research shows that Saudi Arabia, Iraq, Egypt, the UAE, and Qatar are the top 5 countries by the number of atabases distributed in the period from January to June 2024.

Figure 22 | Databases by countries distributed in the dark web in H1 2024



Governments were affected the most

Compared by industry, public institutions were affected the most — 32% of all corporate data breaches and 25% of all leaked databases in the region were connected with Governments, which correlates with the level of hacktivist activity. 22% of all leaks contain information on citizens (there are some unspecified databases with personal data and target lists combined according to various parameters).

Education institutions, retail (and e-commerce), financial companies, and organizations providing consumer services also feature prominently.

Figure 23 | Corporate data breaches. Statistics by industries

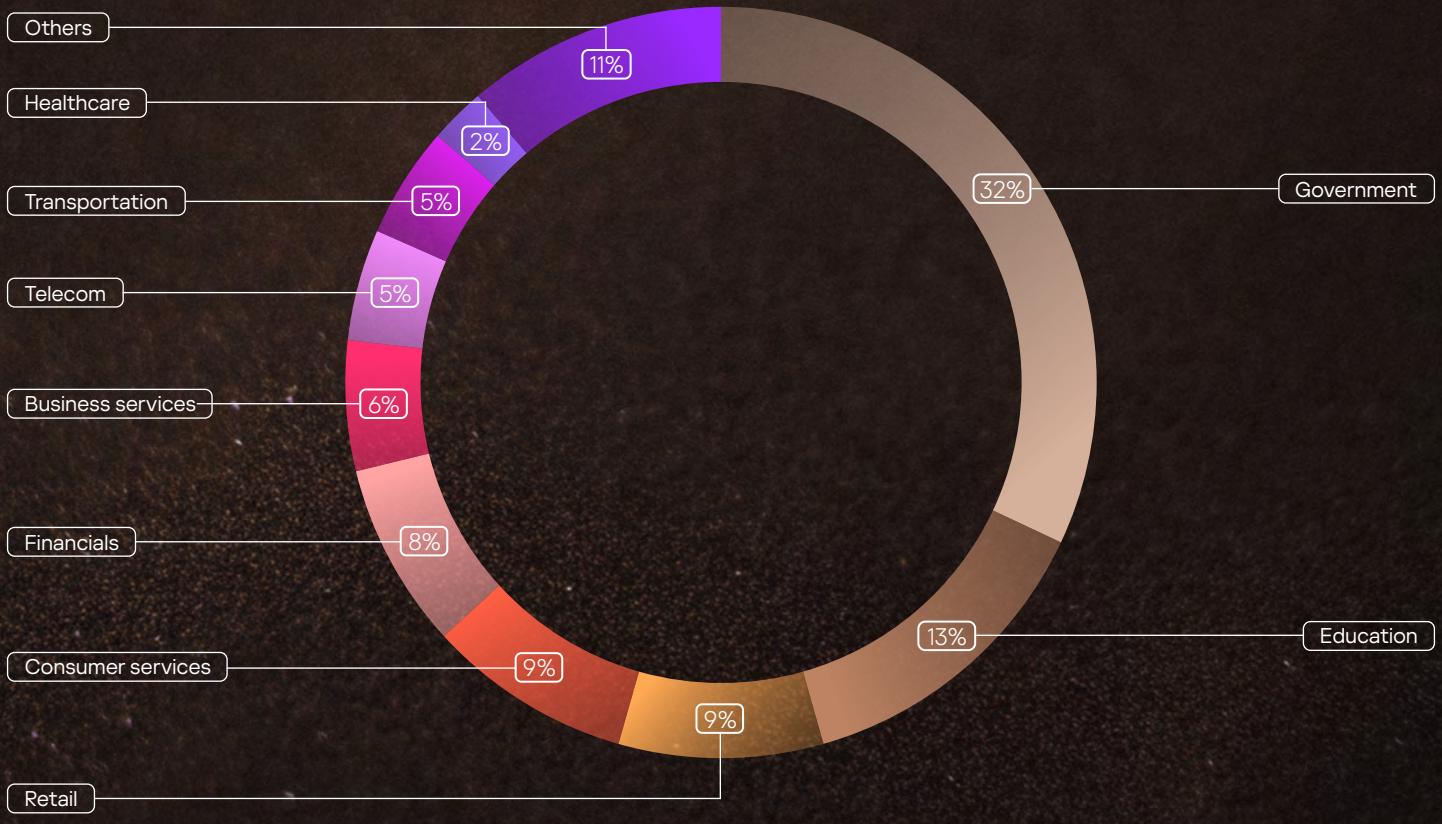
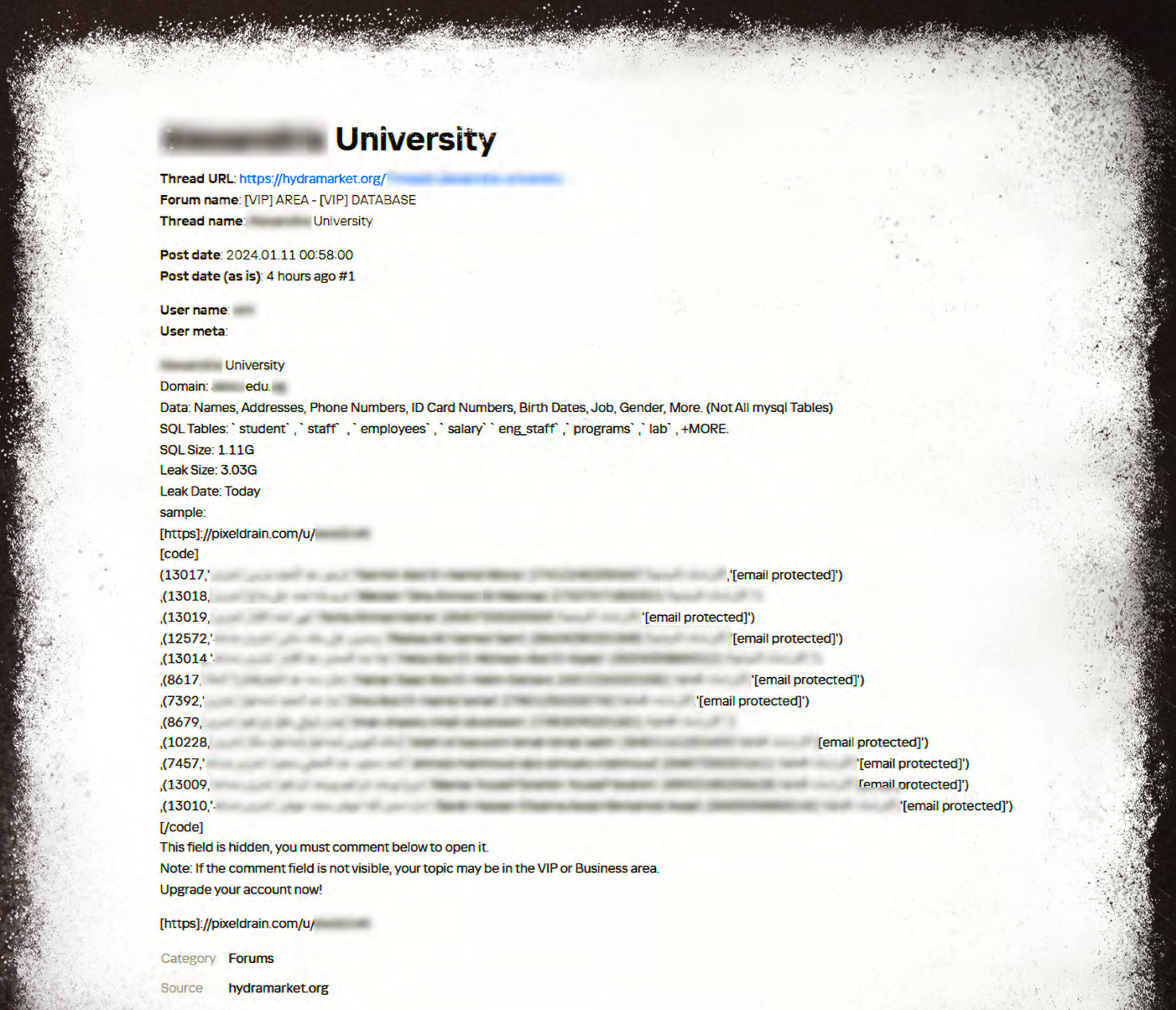


Figure 24 | Example of publication sharing data breaches (source — the Threat Lookup service of the Kaspersky Threat Intelligence portal[14])



[redacted] University

Thread URL: https://hydramarket.org/[redacted]
Forum name: [VIP] AREA - [VIP] DATABASE
Thread name: [redacted] University

Post date: 2024.01.11 00:58:00
Post date (as is): 4 hours ago #1

User name: [redacted]
User meta:

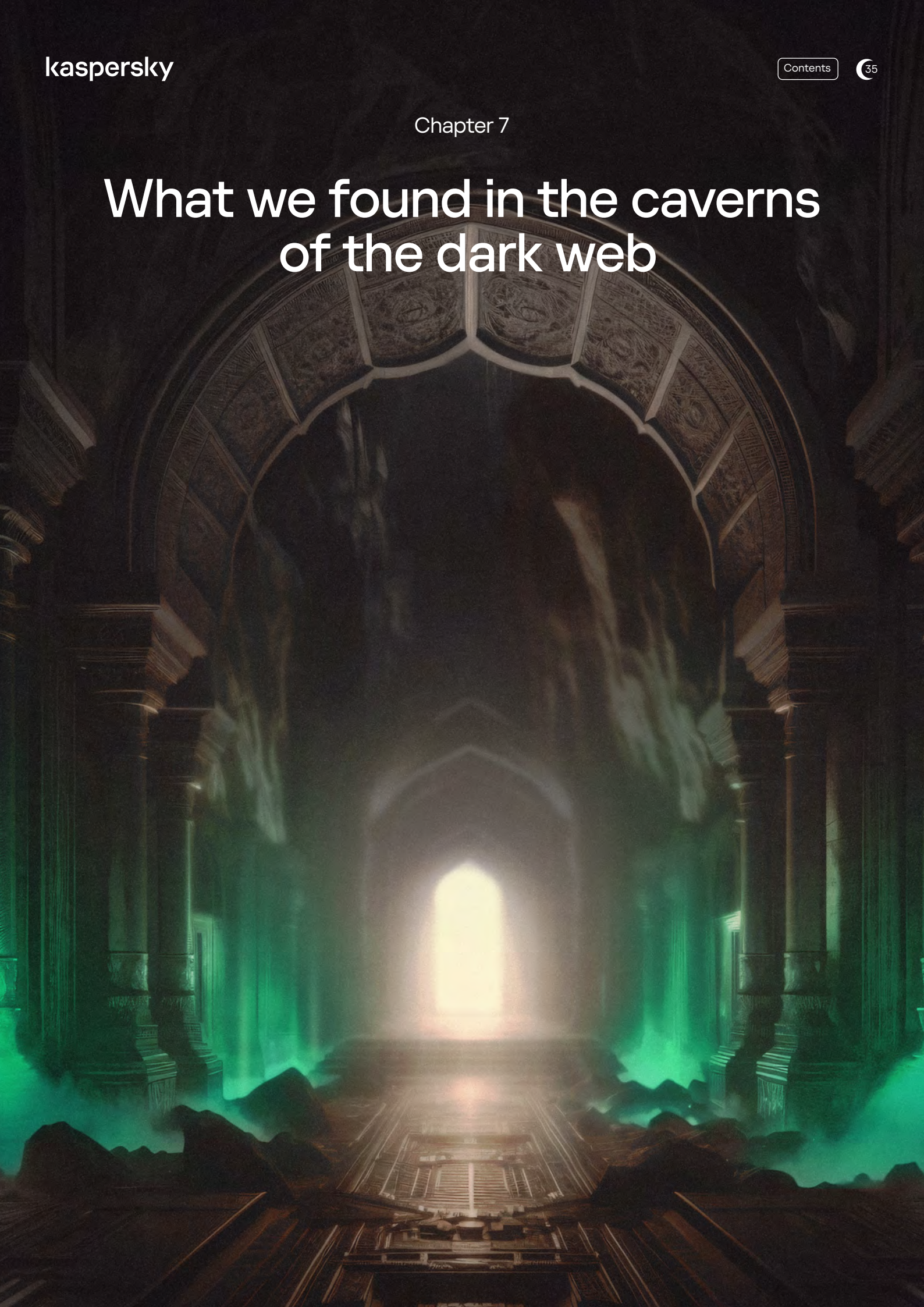
[redacted] University
Domain: [redacted]edu.[redacted]
Data: Names, Addresses, Phone Numbers, ID Card Numbers, Birth Dates, Job, Gender, More. (Not All mysql Tables)
SQL Tables: `student` , `staff` , `employees` , `salary` `eng_staff` , `programs` , `lab` , +MORE.
SQL Size: 1.11G
Leak Size: 3.03G
Leak Date: Today
sample:
[https]://pixeldrain.com/u/[redacted]
[code]
(13017,'[redacted]','')
,(13018,[redacted]
,(13019,[redacted]'')
,(12572,'[redacted]')
,(13014 '[redacted]
,(8617,[redacted]'')
,(7392,'[redacted]'')
,(8679,[redacted]
,(10228,[redacted]')
,(7457,'[redacted]'')
,(13009,[redacted]')
,(13010,'[redacted]'')
[/code]
This field is hidden, you must comment below to open it.
Note: If the comment field is not visible, your topic may be in the VIP or Business area.
Upgrade your account now!

[https]://pixeldrain.com/u/[redacted]

Category Forums
Source hydramarket.org

Chapter 7

What we found in the caverns of the dark web



What we found in the caverns of the dark web

The truth is that the dark web community is evolving daily alongside the global trends in IT and cybersecurity. Attackers are constantly honing their strategies, tactics, techniques, and tools while also inventing new ones. Vigilance is key to securing a company's network infrastructure from attacks — to be one step ahead of any potential adversary. These days, when it comes to cyberattacks, the question is "when", but not "if".

This report highlights five prevalent cybersecurity threats in the Middle East — hacktivism, ransomware attacks, initial access brokering, the ubiquity of info stealers, and the breach of data from corporations and other targets.

Whispers from the Dark Web Cave — Cyberthreats to the Middle East

The full list of cyberthreats affecting businesses and public institutions in the region covered is long, with some specific to certain industries or organizations. And there is no magic pill to protect against all threats, but there is a strategy that works. Put simply, it is about being proactive in defending against possible threats using robust cybersecurity tools combined with intelligence-driven monitoring of internal security events and perceived threats from the dark web. Naturally, when malicious indicators are detected a prompt response is key.

To inquire about threat monitoring services for your organization, please contact us via the Kaspersky Digital Footprint Intelligence website or directly at dfi@kaspersky.com.

Digital Footprint Intelligence

If you are already facing an incident, our Kaspersky Incident Response service will help you respond and minimize the consequences, particularly by identifying compromised nodes and protecting your infrastructure from similar attacks in the future. If you want to **uncover covert cyberattacks** or ensure that your environment has not been penetrated, consider our Kaspersky Compromise Assessment service.

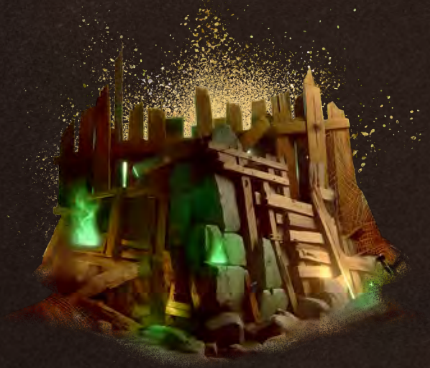
Incident Response

Compromise Assessment

If you intend to evaluate and improve the security posture of your organization, a Kaspersky Security Assessment will include a variety of services, from penetration tests to red teaming.

Security Assessment

Protection strategy



Asset inventory and patch management

First, you need to know what exactly should be protected and ensure that attackers do not have opportunities to exploit known vulnerabilities.

Comprehensive security solutions

Use multi-pronged security controls on all components of your network infrastructure for the best visibility across the environment and, thereby, timely detection and prevention of various forms of attack.

Security awareness among staff is vital

Regardless of the security controls used, the human factor remains one of the main vulnerabilities.

Total monitoring and assessment.

To protect your environment from a malicious attack, you have to detect it first – that's why all devices, servers, systems, services, applications, and traffic should be monitored for suspicious events.

Threat Intelligence (TI)

Constantly stay up to date on TI data, including actual TTPs used by attackers and tailor your security controls accordingly.

Dark web monitoring

Forewarned is forearmed — knowledge about potential attack vectors, cybercriminal interests and plans, and the threats posed by them is crucial to fine-tuning your defenses accordingly or taking timely counter and remedial measures.

Analytical report

Whispers from the Dark Web Cave

#kaspersky
#bringonthefuture

Cyberthreats to the Middle East

www.kaspersky.com

kaspersky