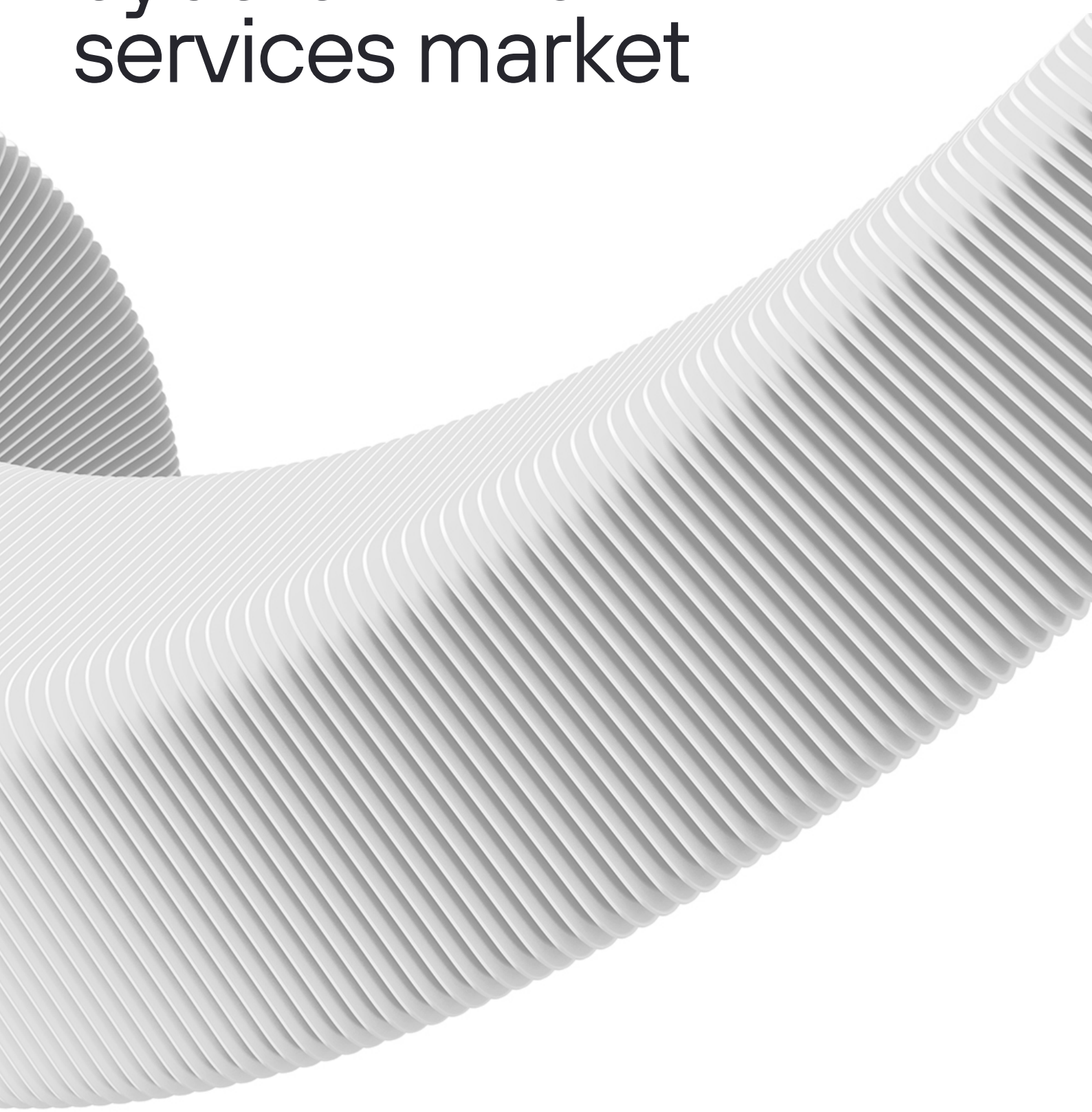


# GCC data in demand on the cybercriminal services market



# Content

Introduction.....	3
Summary.....	3
Materials and methods .....	4
What do buyers on the dark web aim at: Middle East in focus.....	5
Takeaways.....	14
Appendix 1. Sector distribution by country.....	15
Appendix 2. Categories (themes) distribution by country.....	18

# Introduction

Modern businesses are actively using corporate sites, online stores, and web services for various tasks. Their clients provide personal data upon registering on these platforms and make purchases and transactions using their bank cards. They can also keep and transfer confidential information through the provided resources.

However, with the growth of stored data these platforms are becoming the focus of cybercriminal activity. Attackers are trying to gain access to valuable information stored in companies' information systems, which is why we're constantly tracking dark web forums and messengers to assess the potential risks for various systems, as well as the interest in cybercriminal services. This allows us to take appropriate measures and provide reliable protection of information resources to our customers.

In this report we will assess dark web hackers' interest to the GCC region<sup>1</sup>, highlight the most popular topics and sectors, as well as analyze the cost of provided services and products.

<sup>1</sup> Gulf Cooperation Council (GCC), consists of six countries— Saudi Arabia, Kuwait, the United Arab Emirates, Qatar, Bahrain, and Oman.

## Summary

- Among the studied messages, most are related to the UAE (46%) and Saudi Arabia (23%).
- Public and financial sectors attract most attention due to the activity of hackers and ransomware groups.
- Data (33%) and access to the networks of organizations (22%) are the most popular discussion topics on the forums. A third of all data is distributed for free, allowing any dark web user to access and use it in attack.
- In most cases the cost of access to organization's resources is lower than average (100–1,000 \$), that said almost all of them grant administrator privileges.

## Materials and methods

In the course of our research we analyzed 252 Telegram channels and forums on the dark web with a total of 8,884,023 users and 91,484,658 messages. The sample included the biggest multilanguage platforms dedicated to various subjects.

In our research we studied the period from January, 2022 to the end of June, 2023.

We studied messages related to the GCC region: the UAE, Saudi Arabia, Bahrain, Oman, Qatar, and Kuwait.

We analyzed messages by following categories:

- Data, namely personal data, logins and passwords for Internet services, confidential business documentation.
- Access, namely data to get unauthorized access to remote devices in a company infrastructure.
- Spam, namely tools and data required for mass messaging of texts, emails, and calls.
- Cash-out services.
- Carding, namely bank cards data.
- DDoS, namely tools for DDoS attacks and calls to perform DDoS attacks.
- Documents, namely forged documents production.
- Fraud, namely search for fraud schemes and recruiting.
- Traffic forwarding, namely redirecting to phishing sites and downloading malicious files.
- Phishing, namely developing, buying and selling sites to gain access to user's confidential data.

Further in the report information with no specified country refers to the GCC region data.

# What do buyers on the dark web aim at: Middle East in focus

The UAE and Saudi Arabia are the most mentioned countries in published messages and advertisements. These countries are associated with oil industry and financial prosperity, which attracts malicious actors of various kinds.

Figure 1. An advertisement offering access to the infrastructure of an oil and gas company.

1

## access 500kk usa-oe

By [redacted], February 11 in Auctions

byte

●

Paid registration

01

0 posts

Joined

02/11/23 (ID: 142584)

Activity

other

Posted February 11

headquarters usa-dubai

geo dubai uae

rev 500kk 8k employees

development production service +

SECTOR

Energy

INDUSTRY

Oil & Gas

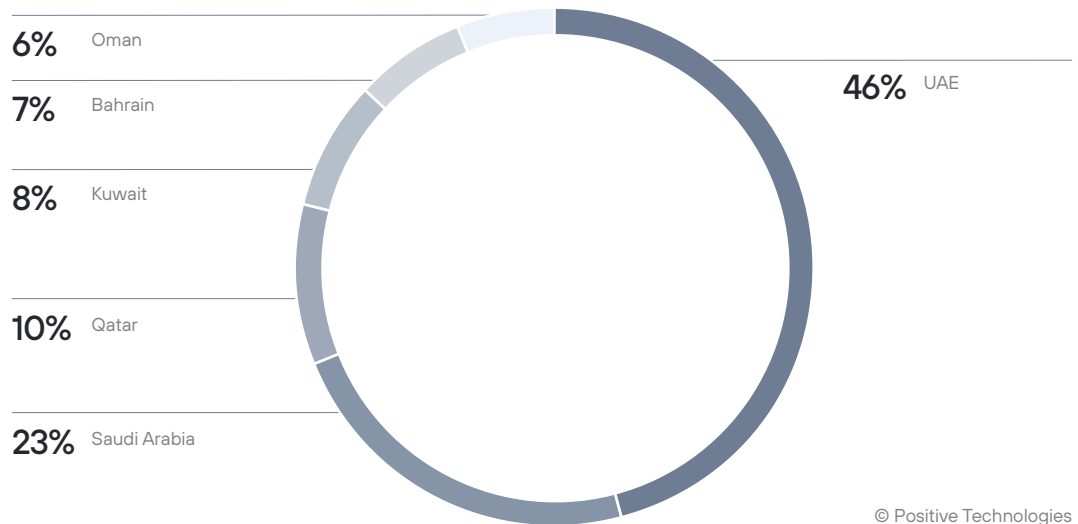
vpn user

start : 1500\$

step : 500\$

blitz : 2500\$

Figure 2. Percentage of forum messages by country




When it comes to the Middle East, messages on the dark web most commonly mention government and financial institutions. Hacktivists attack government agencies because of political motives. Malicious actors of various kinds, including ransomware groups, attack financial institutions. According to our [data](#), every second attack on organizations around the world involves ransomware.

Figure 3. An advertisement offering access to a bank or a bank database.

### Buying Arab banks db/access

👤 06/14/2022



**floppy disk**

User

Registration: 04/12/2022

Messages: 4

Reactions: 0

06/14/2022

---

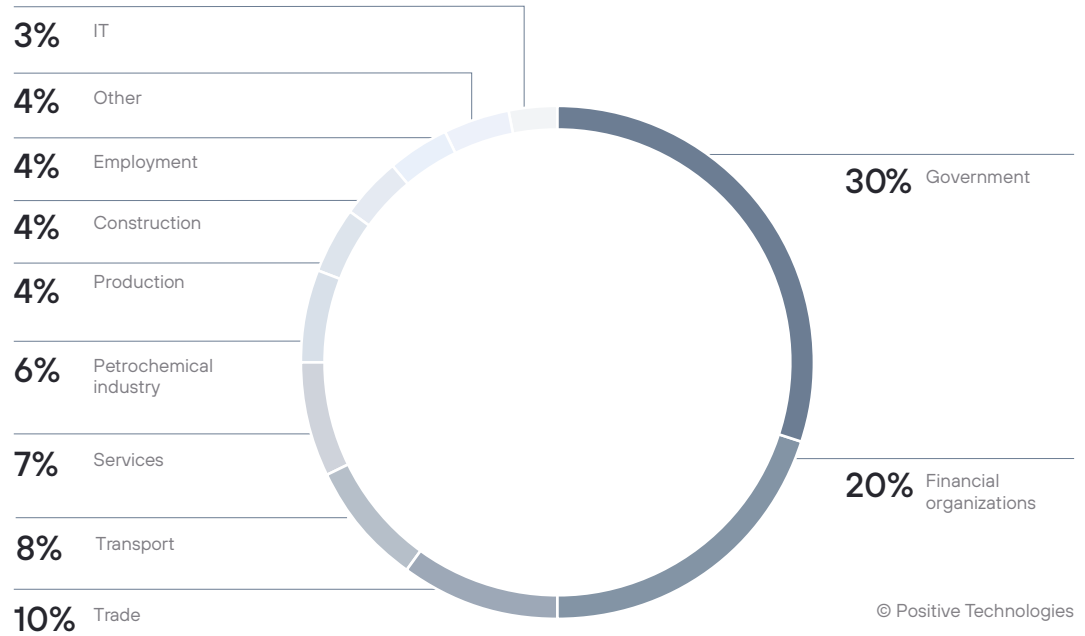
UAE, Saudi, Oman, Qatar, Kuwait, Bahrain

Send DM with your tox or Telegram ID

will post escrow here in new thread

🔔 Complaint

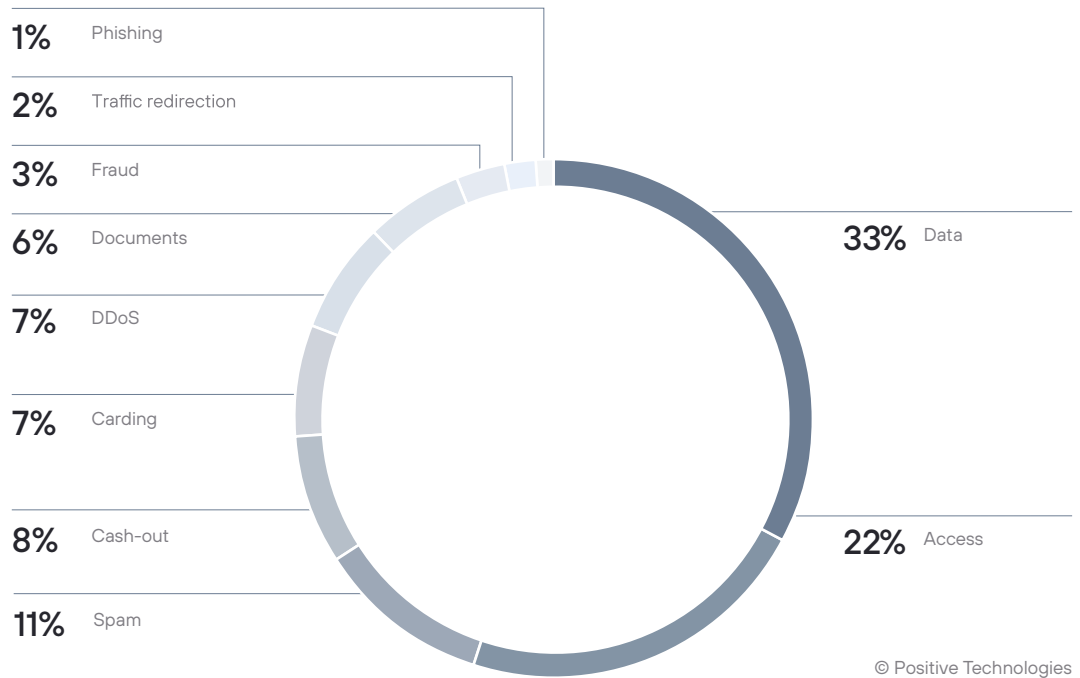
Figure 4. Percentage of forum messages by sector



There is a prevailing interest in such categories as data and access.

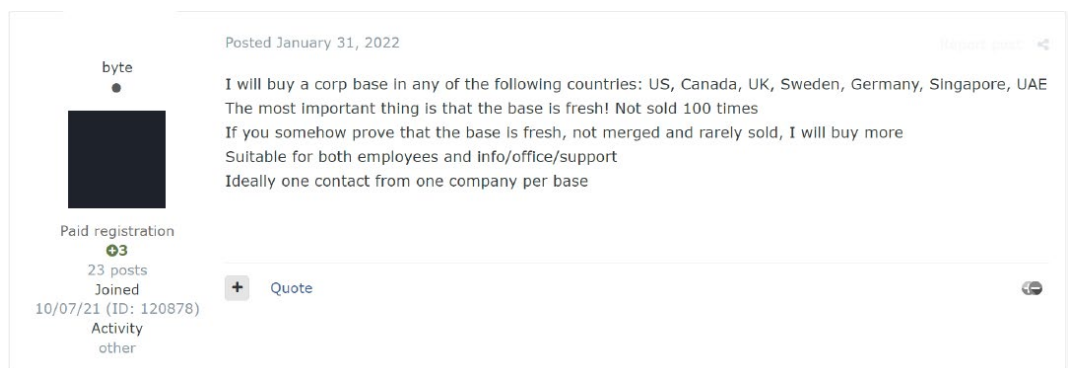
Analysis of messages by categories in general (figure 5) and for every country specifically (appendix 2) shows that data and access always are among the top three categories in the lists.

Figure 5. Percentage of messages by category



A third of all advertisements are related to data: corporate databases and account data, including bank accounts. Attacking corporate web resources, hackers gain information that may contain personal data and credentials of employees and clients. The data may be later used by other malicious actors to attack organizations (for example, in phishing campaigns). According to our [research](#), 43% of successful attacks around the world in 2022 involved social engineering.

Figure 6. An advertisement offering employee databases





Due to hackers and ransomware groups activity, 31% of all data is distributed for free as hackers do not seek financial profit while ransomware actors may publish data for free in case of victim's refusal to pay the ransom. This increases the chances of data being used by other malicious actors in attacks on organizations or their clients.

Figure 7. Advertisement of a UAE company database giveaway

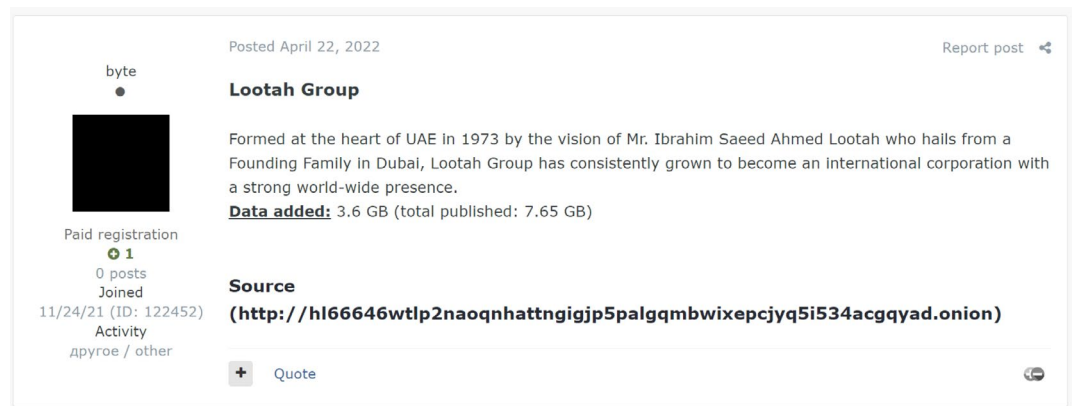
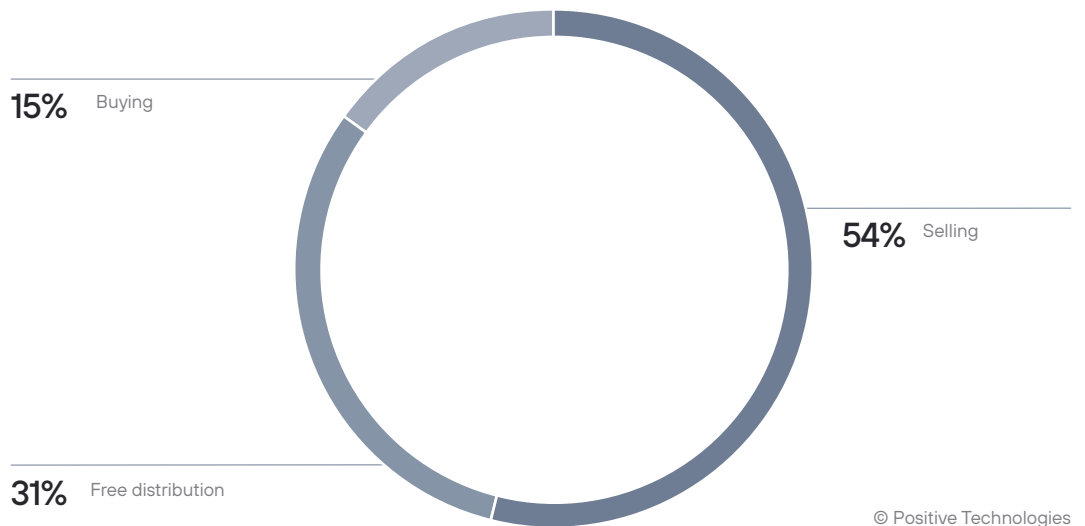


Figure 8. Percentage of messages by type (data category)



© Positive Technologies

22% of all advertisements offer access (figure 5) to infrastructure of organizations in different sectors. Access and data are highly interconnected. Attackers obtain access on forums and use it to infiltrate a company's infrastructure to perform further attacks on the company network. As a result, attackers may gain data that is later sold on forums or distributed for free. For example, if data falls into the hands of hackers or ransomware groups, in most cases it is later distributed for free.

Figure 9. An advertisement offering access

03/08/2023

revenue - 30kk  
country - UAE  
field of activity - Custom Software & IT Services  
privilege - Local Admin  
av -  
pc in the network - 100+  
price - \$ 4000

Complaint

RAID array

User

Registration: 11/28/2020  
Messages: 62  
Reactions: 2  
Deal guarantor: 1

Every third advertisement with an access offer gives an opportunity to connect to a company network with the use of VPN or RDP. Sellers can get access with stealers. According to our [research](#), the number of phishing letters with malicious attachments (credentials stealers) is growing.

Figure 10. An advertisement offering access

Posted November 14, 2022

Report post

gigabyte  
●●●●

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

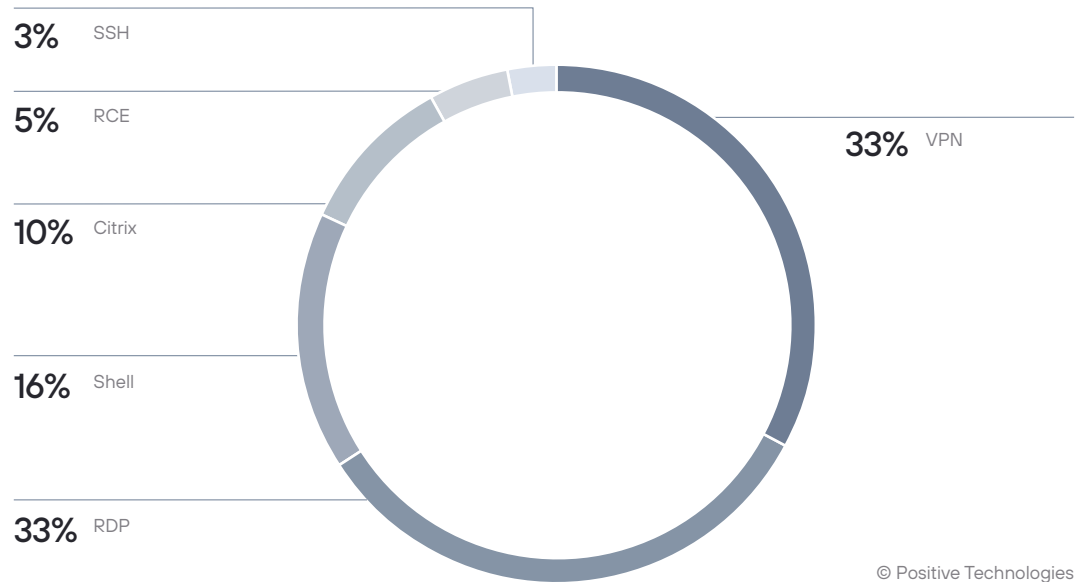
Seller  
070  
121 posts  
Joined  
07/11/22 (ID: 133155)

Activity  
hacking / hacking  
Deposit  
0.005000 \$

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

pps: 48h after last bid

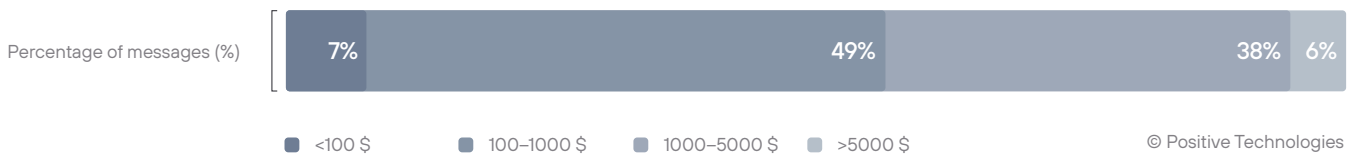
Figure 11. Percentage of messages by access type



16% of messages in the access category discuss using downloaded shell malware to connect to organization resources. 10% of messages discuss using Citrix, a software that provides access to remote desktop, to gain direct access to resources. In rare cases, messages mention using SSH protocol (Secure Shell) to connect to a company’s internal resources, as well as offer access to remote code execution (RCE) in a company’s network.

The cost of access ranges from \$35 to \$40,000. At the same time, in most cases (49%) the cost of access is below average and ranges from \$100 to \$1000.

Figure 12. Access cost distribution

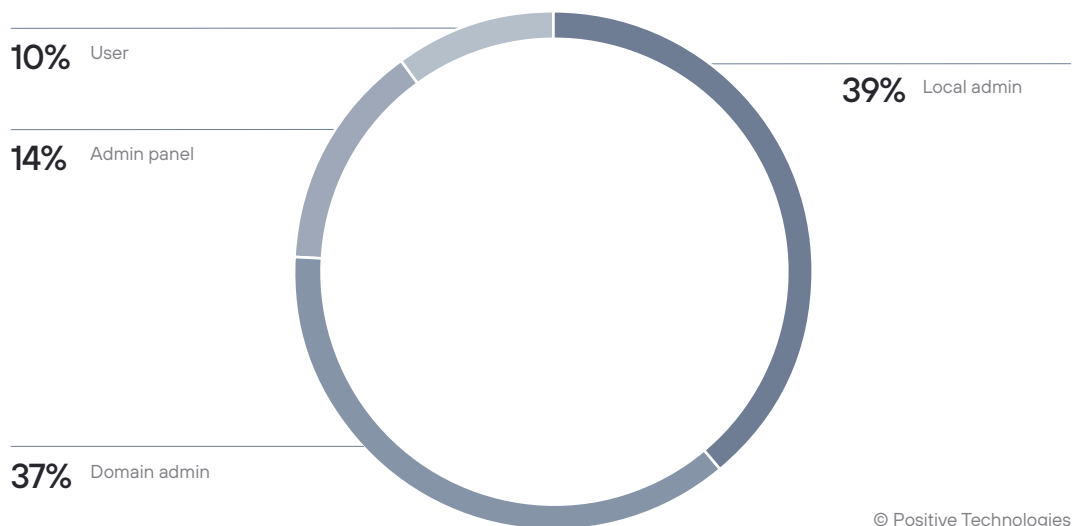


It should be noted that 90% of offers grant administrator permissions. Given this and the low cost of access, even inexperienced attackers with a limited budget may successfully attack organizations. However, there are also expensive offers of access to large companies with high turnover. More sophisticated hackers may use access to these companies to perform complex attacks.

Figure 13. An advertisement offering access



Figure 14. Access privileges offered on the dark web



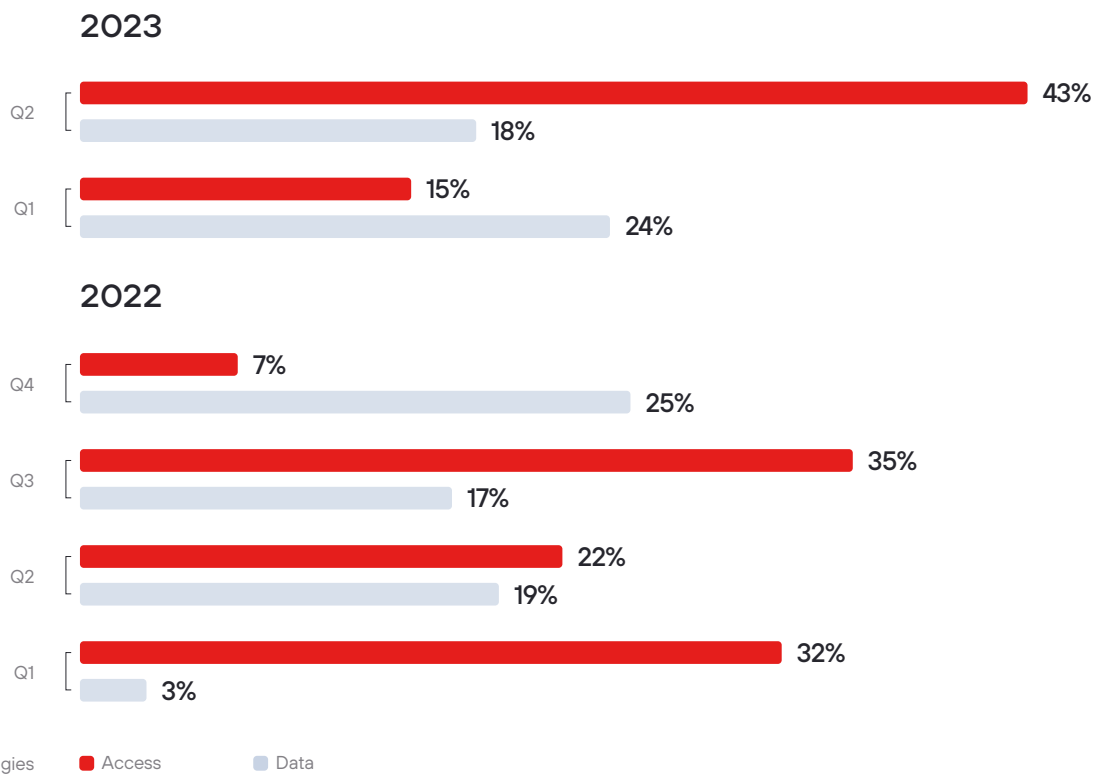
<sup>2</sup> Domain administrator has unlimited access to computers and servers within the domain. Administrator panel or admin panel is a set of functions used to perform certain tasks on a website (for example, to create and edit content, add custom fields to content, and manage users).

Figure 14 shows that only 10% of messages mentioned user access permissions. Generally, this type of access may interest savvy attackers who are able to further modify it on their own. In the remaining cases, messages mentioned privileged types of access such as local administrator, domain administrator, and admin panel<sup>2</sup>.

At the end of 2022 and in the beginning of 2023 the number of messages in the access category reached its maximum.

At the end of 2022 there were few messages in the data category, but in the beginning of 2023 their number increased significantly. This may indicate that data had been obtained through attacks with the use of sold access. As a first step, attackers bought up access rights, which they later used in attacks to obtain data that is now available on the dark web.

Figure 15. Number of messages referring to data and access in 2022 and 2023



## Takeaways

With the large number of messages related to data and access, as well as the low cost of offers, it's easier for attackers to gain initial access to company resources. Inexperienced hackers that don't have substantial funds or skills to bypass network perimeters get an opportunity to perform successful attacks. At the same time, more sophisticated attackers don't have to look for vulnerabilities in a network perimeter. Instead they are able to purchase access and then attack an organization from the inside. All this results in the increase of successful attacks on companies. Therefore, a company's cybersecurity strategy should consider all possible threats and attack scenarios and use cutting-edge security tools, such as:

- [SIEM](#) (security information and event management) systems for monitoring and analyzing security events data from various sources. The combination of SIEM and XDR systems provides centralized threat detection and response.
- [NTA](#) (network traffic analysis) solutions that increase protection by detecting attacks in the early stages.
- [WAF](#) (web application firewall) tools that minimize the risk of a data leak by blocking attacks on web applications.

# Appendix 1.

## Sector distribution by country

Figure 1. Percentage of messages by sector (UAE)

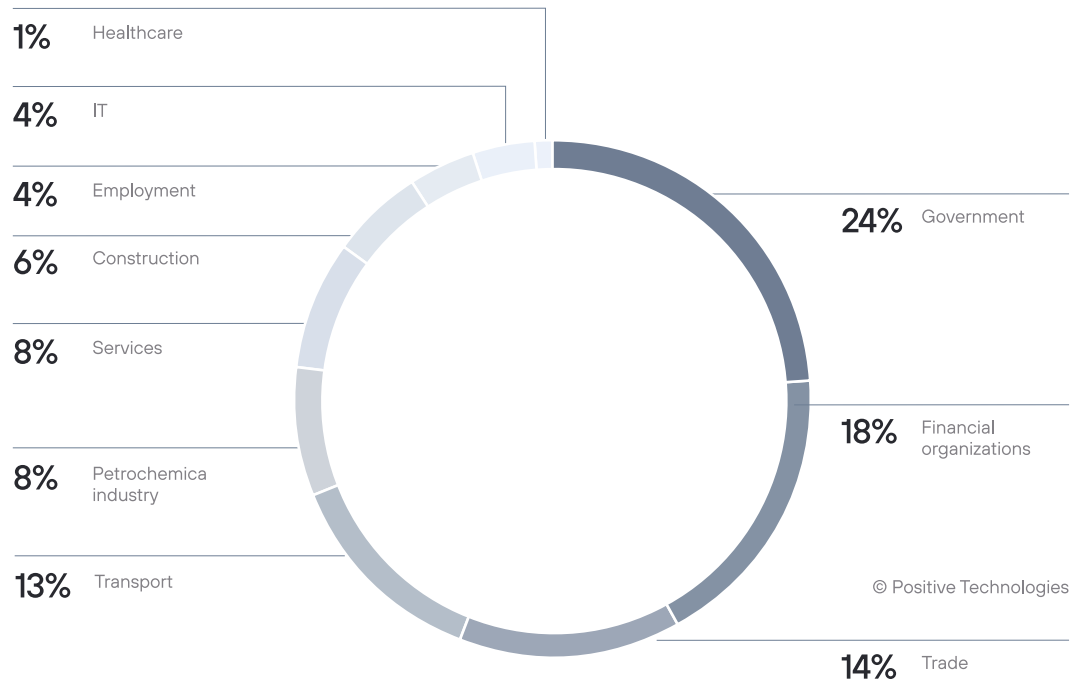


Figure 2. Percentage of messages by sector (Saudi Arabia)

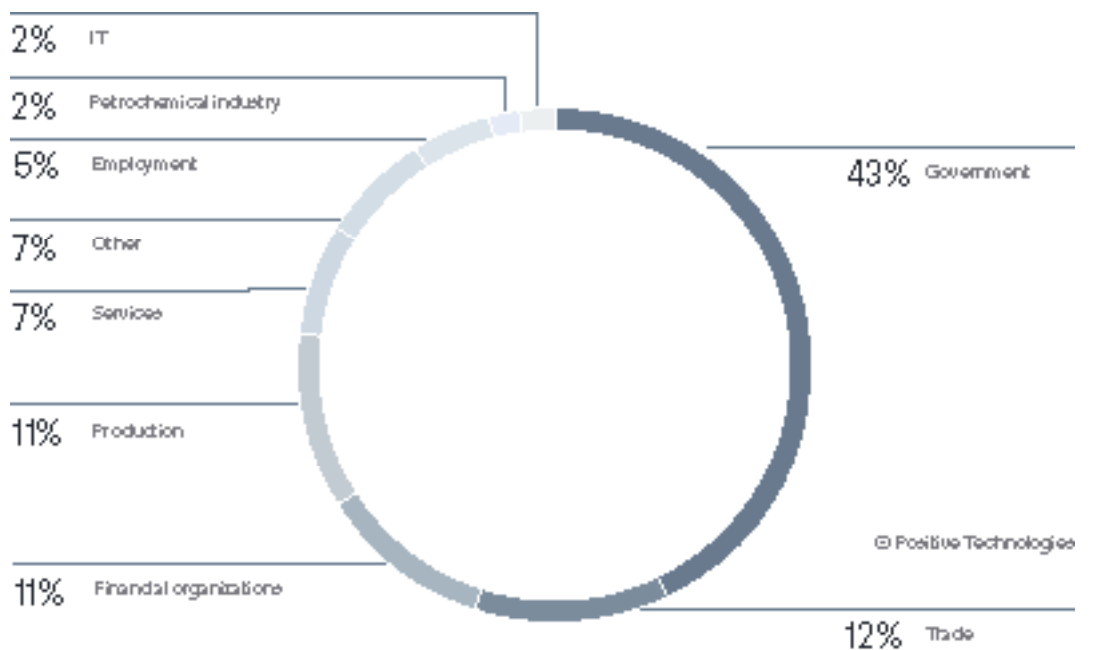


Figure 3. Percentage of messages by sector (Qatar)

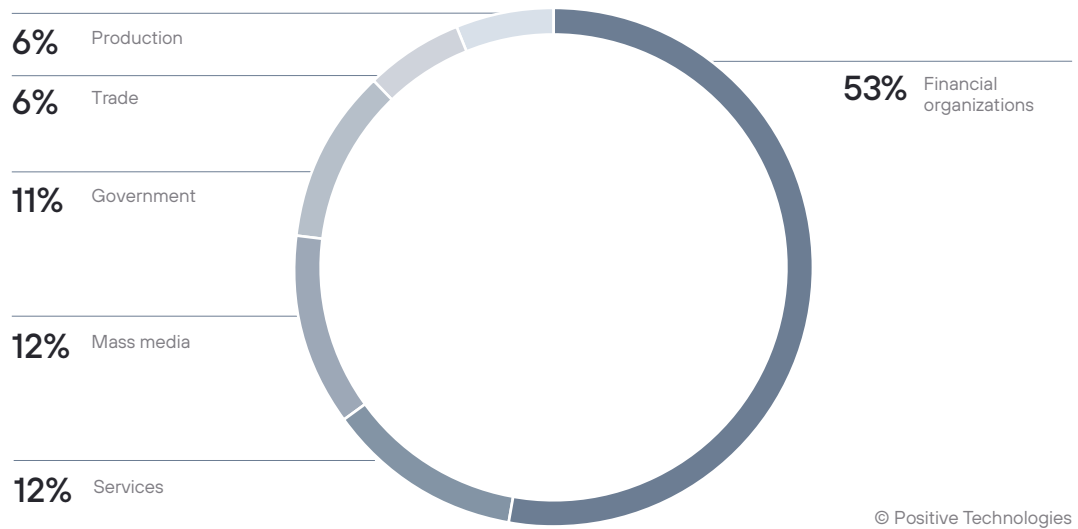


Figure 4. Percentage of messages by sector (Kuwait)

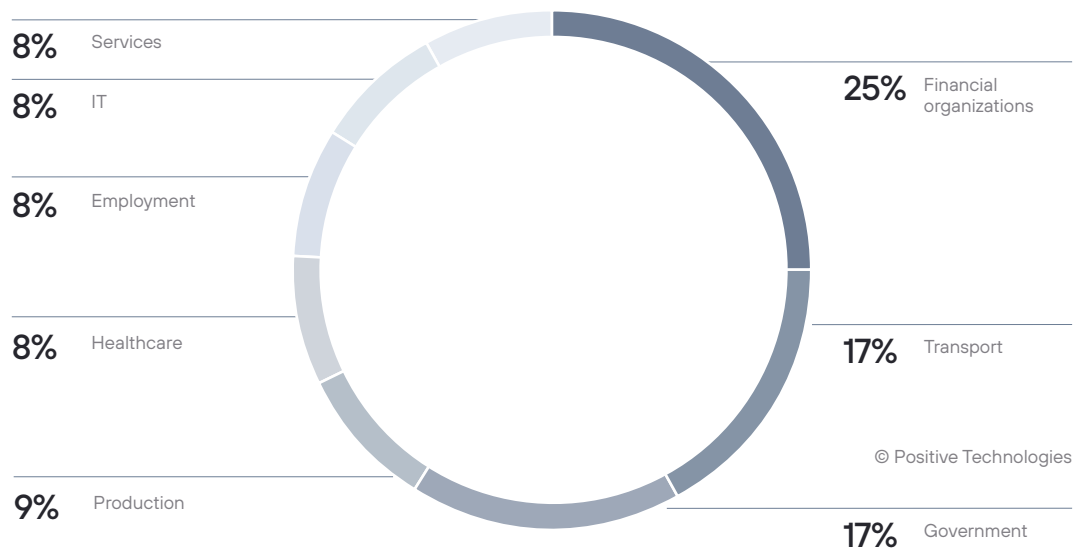




Figure 5. Percentage of messages by sector (Bahrain)

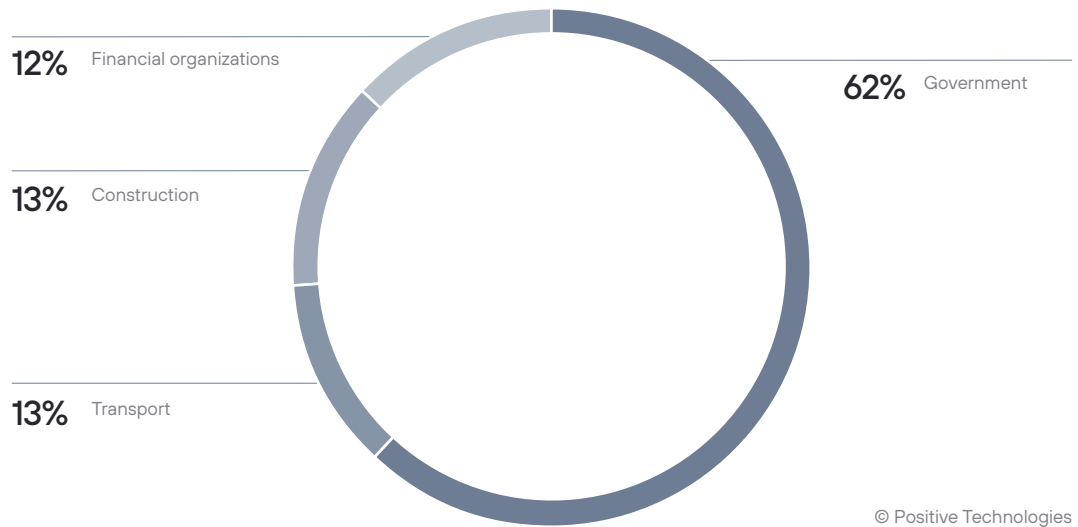
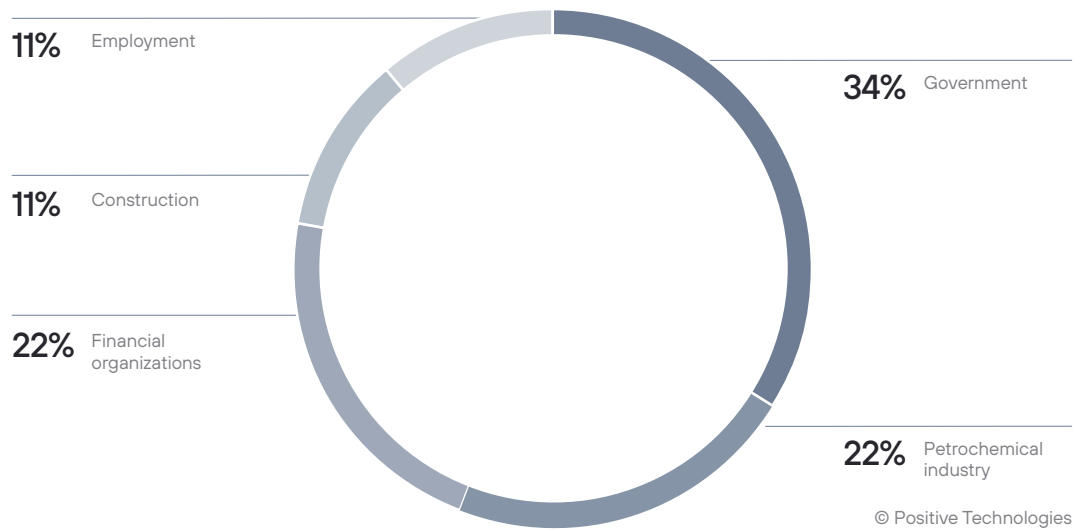


Figure 6. Percentage of messages by sector (Oman)



## Appendix 2.

### Categories (themes) distribution by country

Figure 1. Percentage of messages by category (UAE)

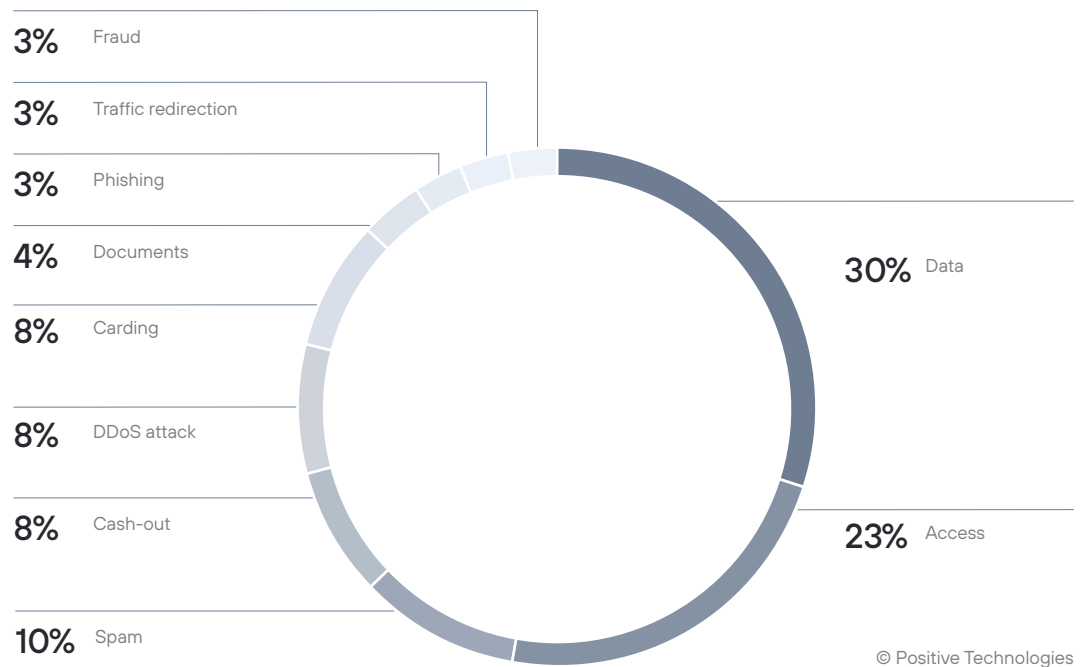


Figure 2. Percentage of messages by category (Saudi Arabia)

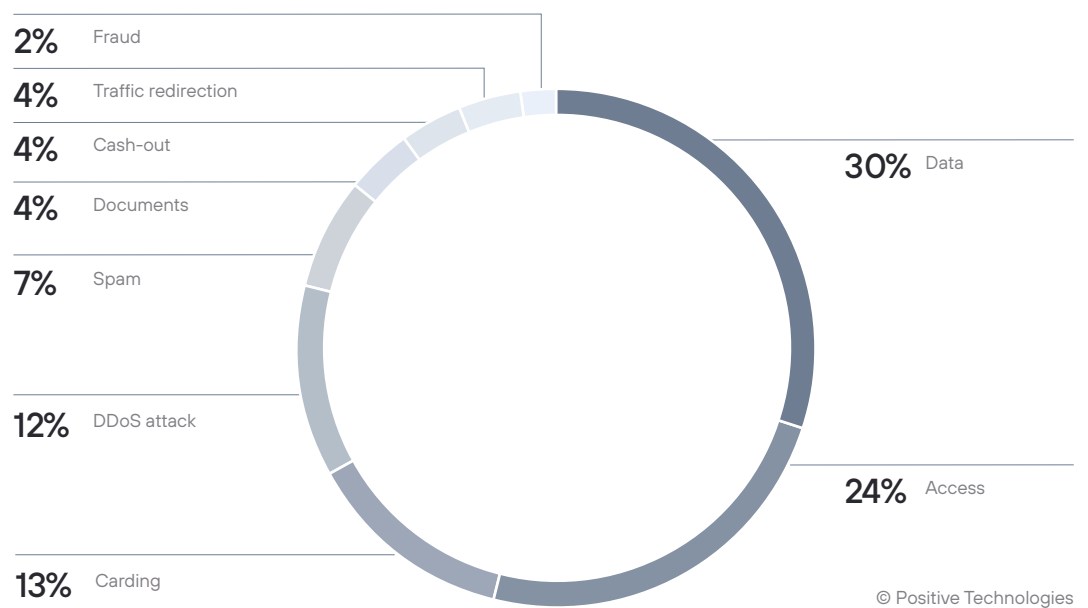


Figure 3. Percentage of messages by category (Qatar)

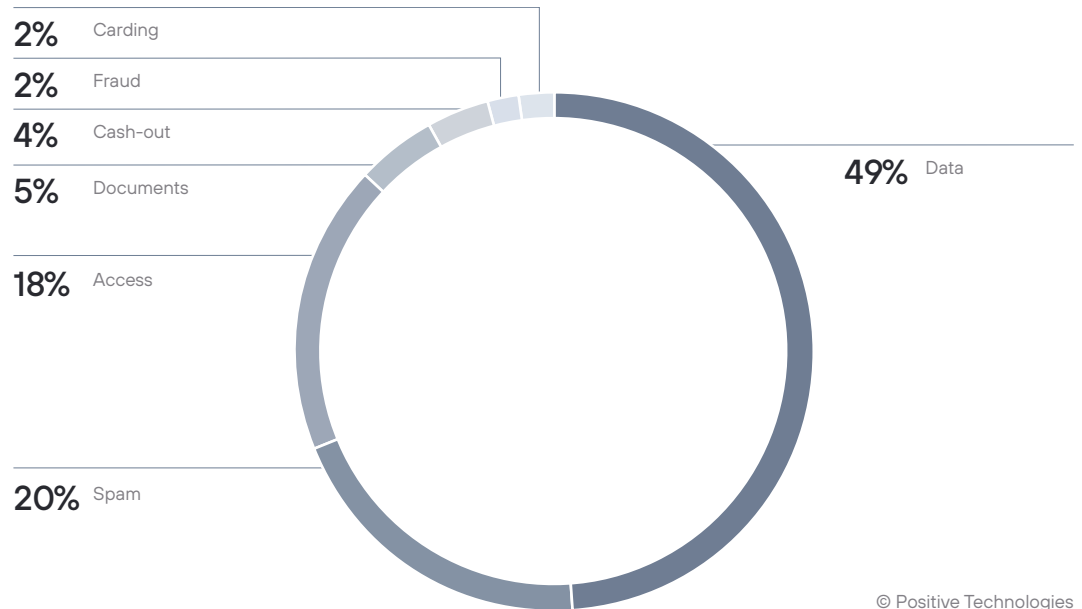


Figure 4. Percentage of messages by category (Kuwait)

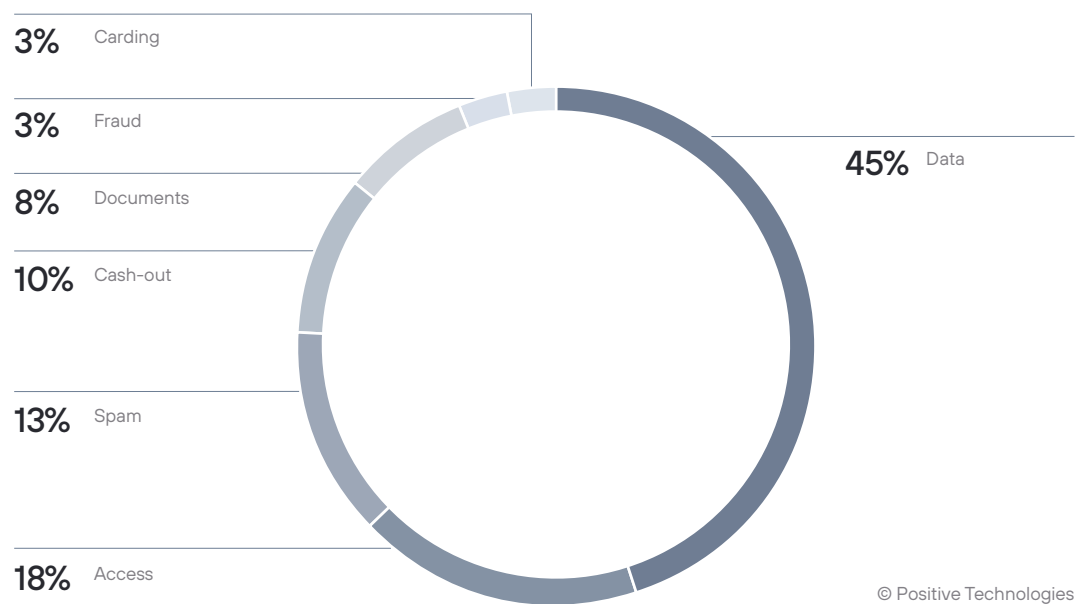


Figure 5. Percentage of messages by category (Bahrain)

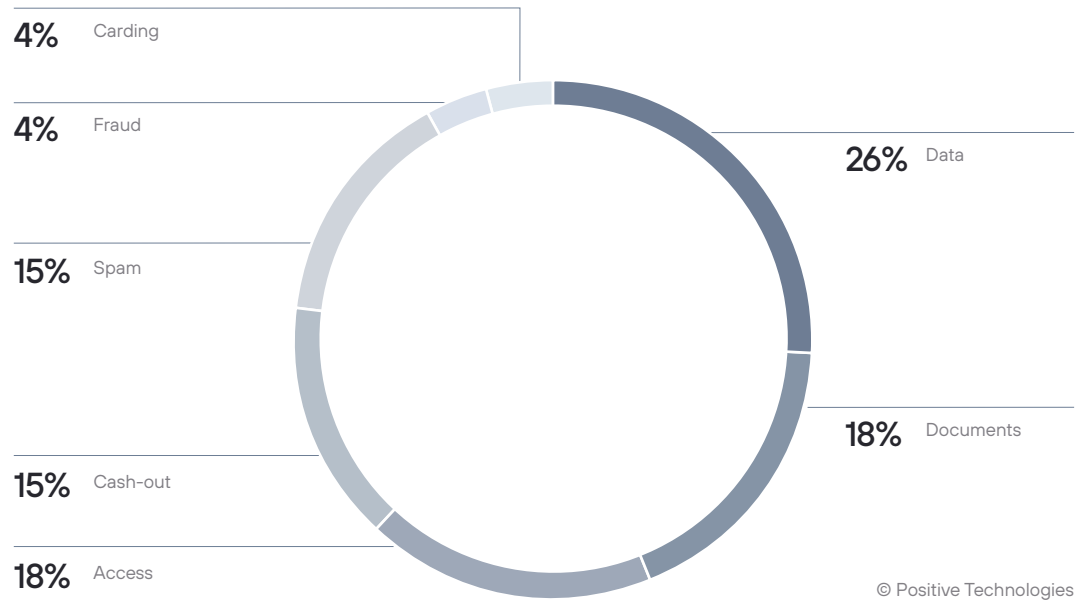
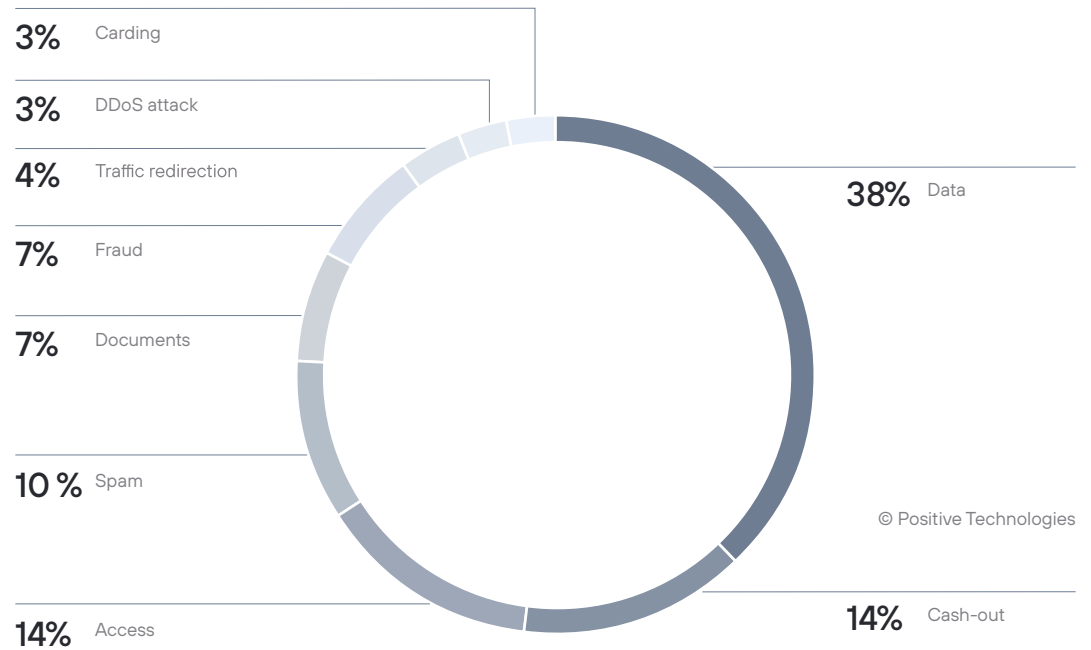


Figure 6. Percentage of messages by category (Oman)





---

[ptsecurity.com](https://ptsecurity.com)  
[pr@ptsecurity.com](mailto: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](https://ptsecurity.com).

---