GROUP-IB

MIDDLE EAST, TÜRKIYE & AFRICA

INTELLIGENCE INSIGHTS

January, 2025

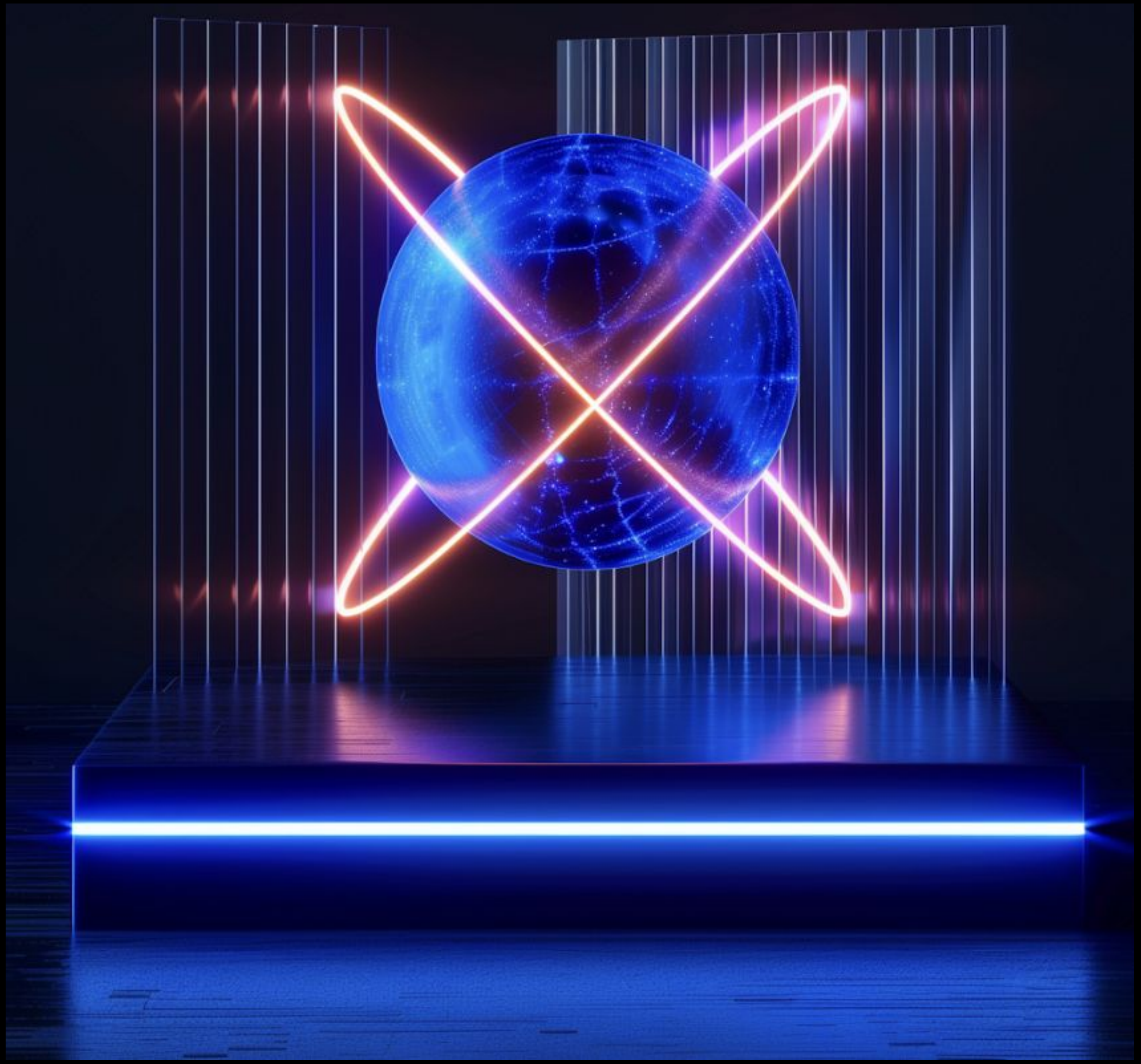
INTRODUCTION

This report contains information on the most significant cybersecurity events that occurred worldwide and in the META region over the last month.

2 notable events of the month:

→ **Group-IB published the blog which highlights the rise of real estate scams in the Middle East, where fraudsters exploit online platforms to deceive victims into paying for non-existent properties.**

→ **Halcyon published the blog details a novel ransomware campaign where the threat actor, dubbed Codefinger, uses compromised AWS credentials to encrypt data in Amazon S3 buckets via Server-Side Encryption with Customer Provided Keys (SSE-C).**



Group-IB specialists discovered multiple phishing and scam campaigns and took active steps to negate their disruptive impact. We want to highlight that **Group-IB customers are well-protected** and aware about such types of threats.

GLOBAL TRENDS

GROUP-IB

Global trends with a brief description:

01 Halcyon published the blog about encryption of the data in Amazon S3 buckets

The blog post "Abusing AWS Native Services: Ransomware Encrypting S3 Buckets with SSE-C" by Halcyon details a novel ransomware campaign where the threat actor, dubbed Codefinger, uses compromised AWS credentials to encrypt data in Amazon S3 buckets via Server-Side Encryption with Customer Provided Keys (SSE-C). This method renders the data irrecoverable without the attacker's encryption key, as AWS does not store these keys, and CloudTrail logs only an HMAC insufficient for decryption.

02 Unveiling OtterCookie: A North Korea-Linked Attack Campaign Targeting Japan

The NTT Security Technical Blog post "Contagious Interview and the Newly Identified Malware OtterCookie" discusses a North Korea-linked attack campaign, "Contagious Interview," which employs a newly identified malware named "OtterCookie." This malware uses Socket.IO to receive remote commands, enabling actions such as executing shell commands, stealing device information, and extracting cryptocurrency wallet keys, with reported cases in Japan emphasizing the need for vigilance.

REGIONAL TRENDS

Key regional trends with a brief description:

01	The Reality of Deception: Exposing Real Estate Scams in the Middle East	Group-IB published the blog which highlights real estate scams in the Middle East: The blog post "The Reality of Deception: Real Estate Scams" by Group-IB highlights the rise of real estate scams in the Middle East, where fraudsters exploit online platforms to deceive victims into paying for non-existent properties. It delves into the operational methods of these scams, the tools and techniques used to detect and disrupt associated money-mule networks, and offers practical advice for individuals to protect themselves from such fraudulent activities.
02	Fake Refund Schemes: Unmasking Social Engineering Scams Targeting Middle Eastern Banking Customers	The blog post "Social Engineering in Action: How Fraudsters Exploit Trust with Fake Refund Schemes in the Middle East" by Group-IB details a sophisticated scam where fraudsters impersonate government officials to deceive banking customers. They exploit individuals who have lodged complaints through a government portal, guiding them to install remote access software, which is then used to steal credit card information and one-time passwords, leading to significant financial losses.

Middle East, Türkiye and Africa

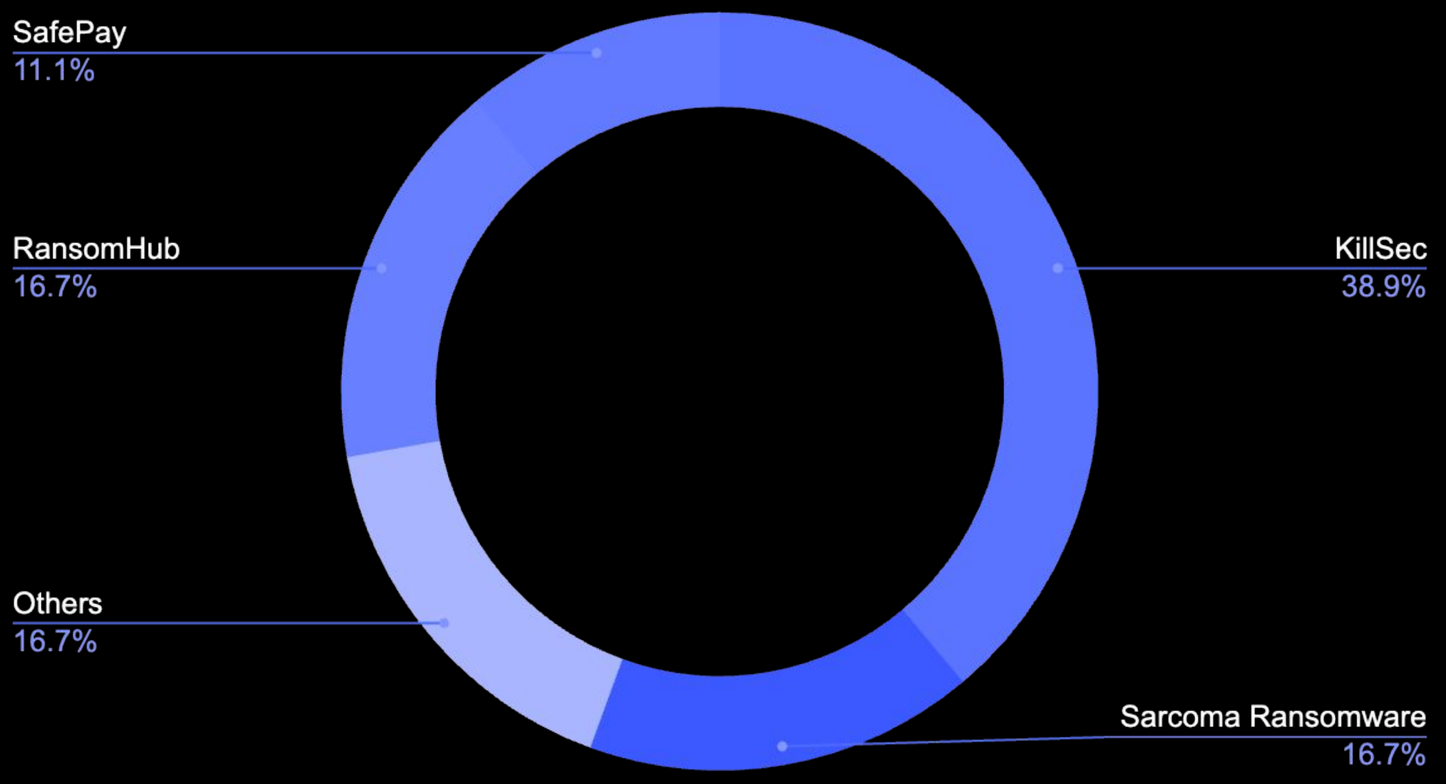
STATISTICS: **ATTACKS**

GROUP-IB

RANSOMWARE ACTIVITIES

Ransomware is a type of malicious software that encrypts the victim's data, rendering it inaccessible. The attacker then demands a ransom payment from the victim to restore access to the data, typically threatening to delete or publicly expose the data if the ransom is not paid. Ransomware statistics for the last month in META region:

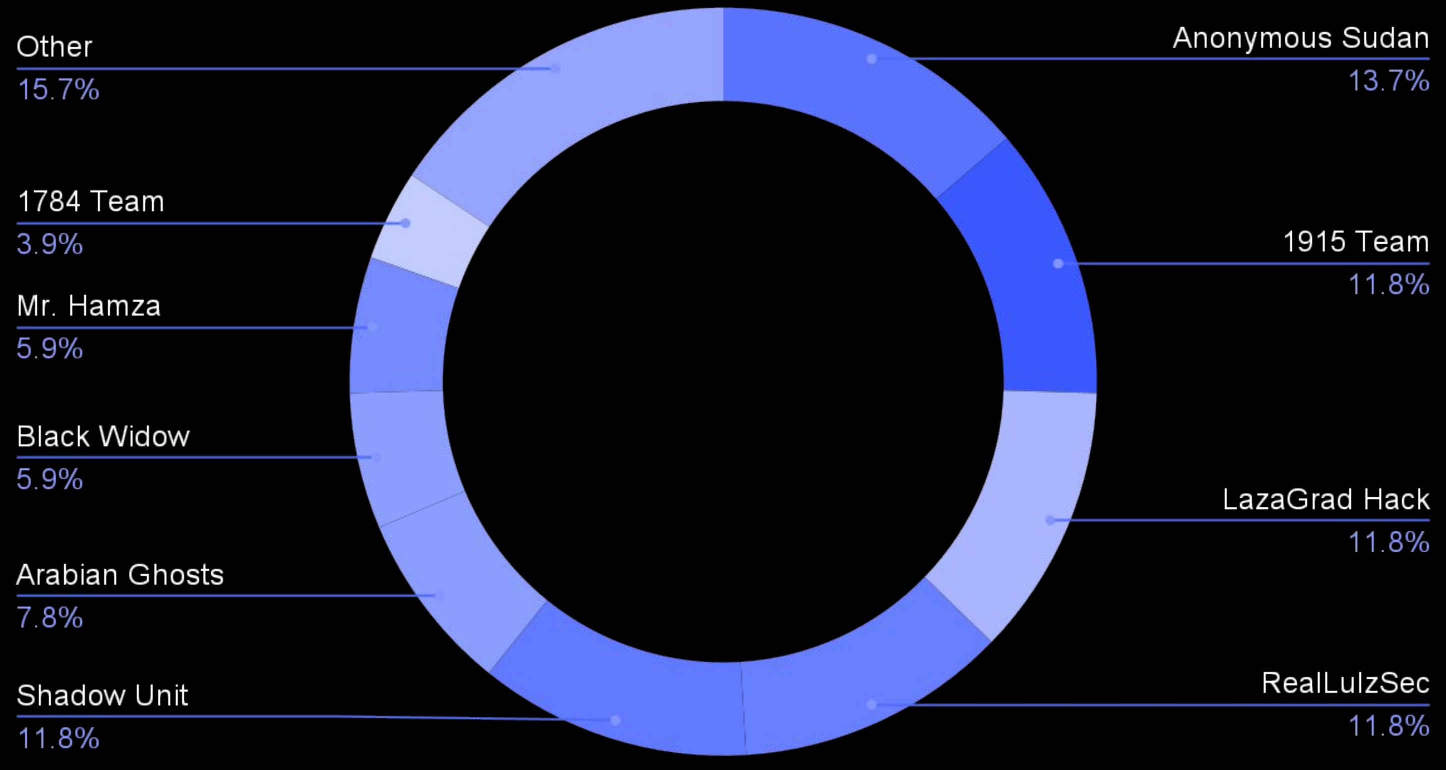
No. of attacks



HACKTIVISM ACTIVITIES

Hacktivism is the use of hacking to promote political or social agendas. Usually hacktivist groups are low-skill hackers who perform DDoS, Defacement, and Data Breaches (mostly leverages compromised accounts) attacks. Unfortunately, during the last year these groups attracted a lot of attention. Below is a brief overview of groups that were active in the region during the previous month.

HACKTIVISM Attacks per group

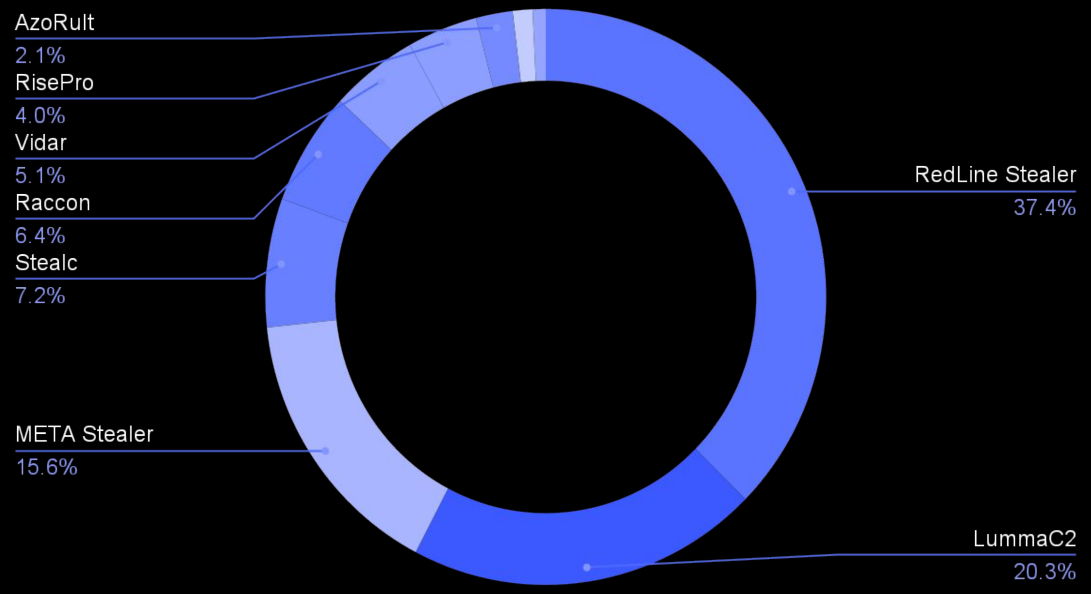


STATISTICS: **COMPROMISED DATA**

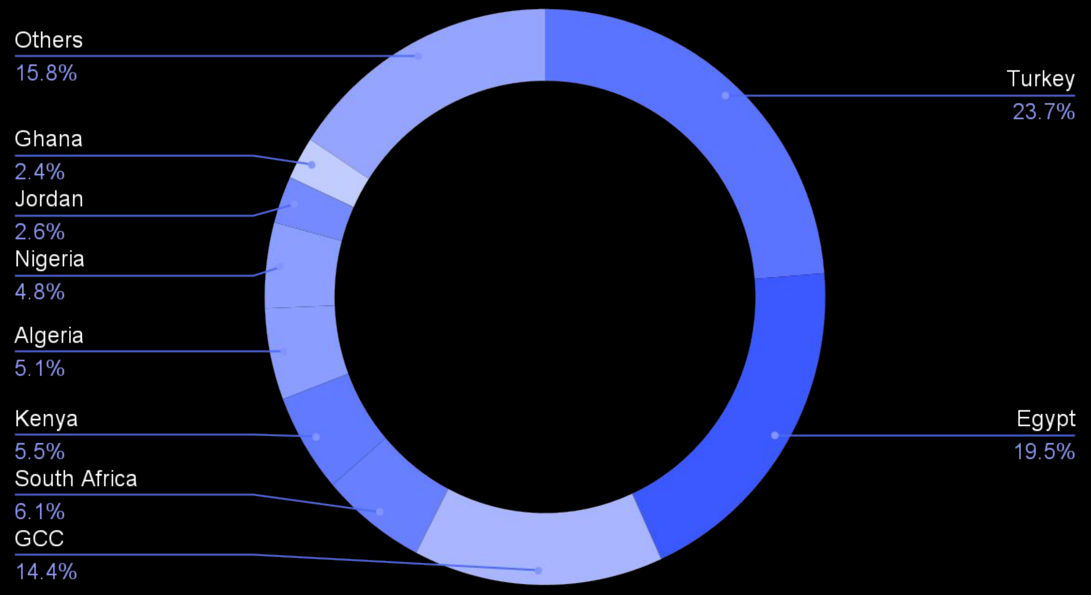
Compromised accounts are a significant threat because they allow unauthorized access to sensitive personal or corporate information, leading to potential financial loss, identity theft, and reputational damage. Additionally, compromised accounts can be used to launch further attacks, causing operational disruptions and exposing organizations to legal and regulatory consequences.

In this part of the report, we provide statistics regarding compromised accounts and compromised cards — all to understand which malware families are the most active in the region.

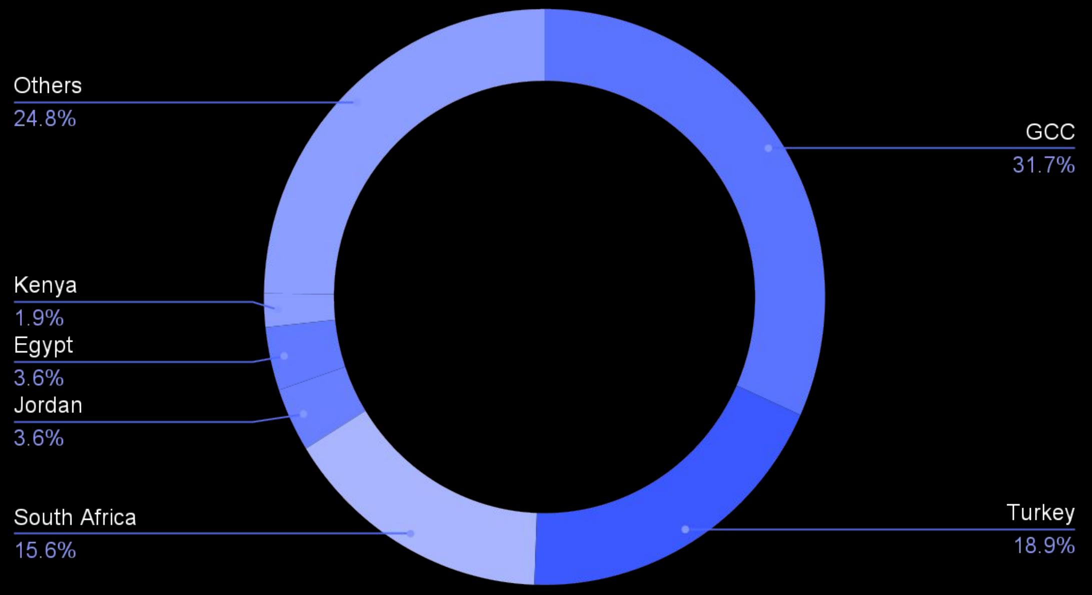
Compromise data by malware



Compromised accounts by country



Compromised bank cards by country



CONCLUSIONS AND RECOMMENDATIONS

The evolving threat landscape poses significant risks to organizations across various sectors. The incidents discussed in this report underscore the need for upgraded security measures and proactive threat management. To safeguard your organization, consider implementing the following recommendations:

ENHANCE SECURITY AWARENESS TRAINING

Regularly educate employees on recognizing phishing attempts, social engineering tactics, and safe online practices.

STRENGTHEN IT INFRASTRUCTURE

Ensure all systems are updated with the latest security patches and employ multi-factor authentication (MFA) to enhance access controls.

CONDUCT REGULAR SECURITY AUDITS

Perform periodic assessments of your IT environment to identify and mitigate potential vulnerabilities.

DEPLOY ADVANCED THREAT DETECTION TOOLS

Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and endpoint detection and response (EDR), to detect and respond to threats in real-time.

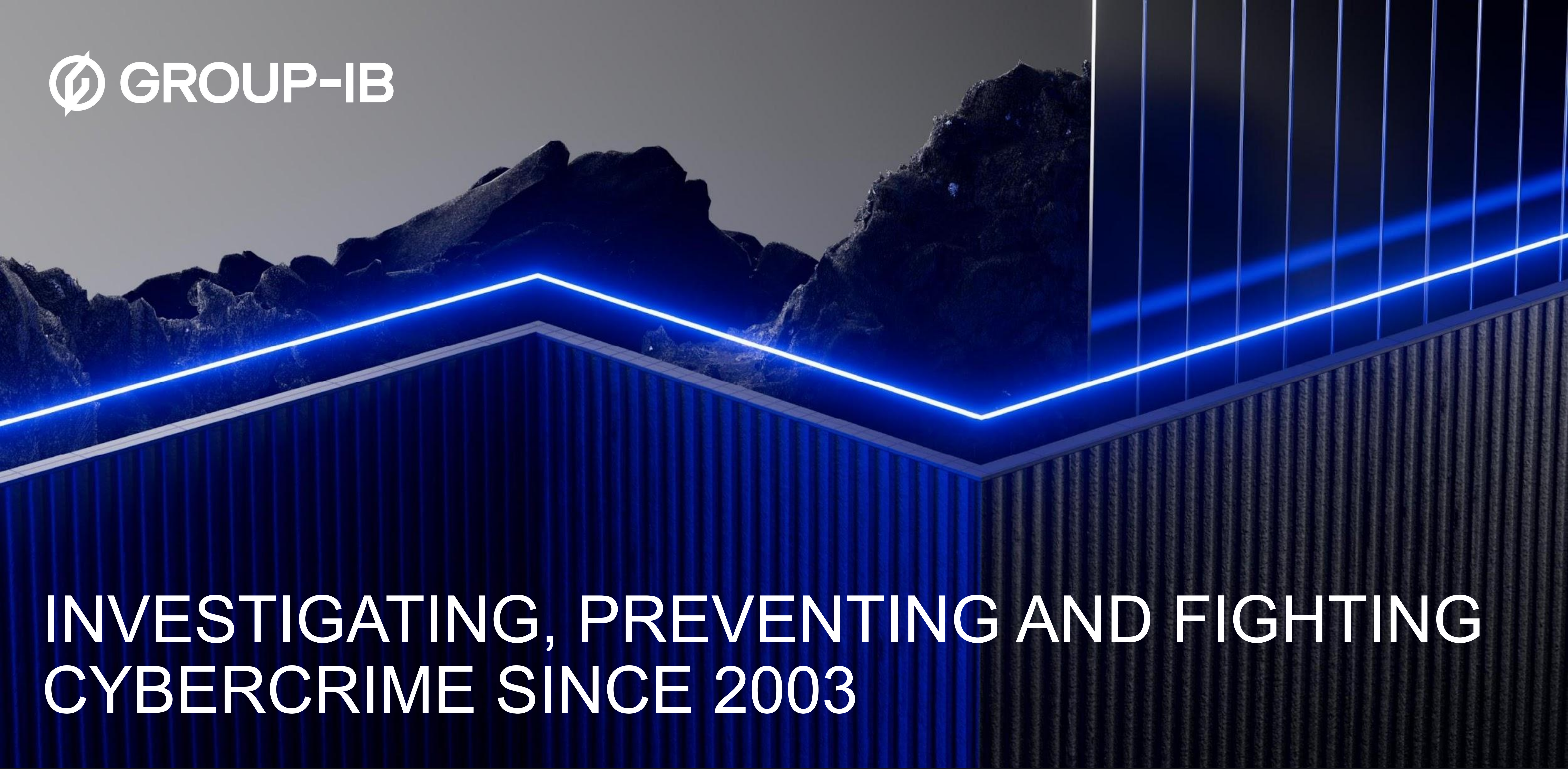
ESTABLISH INCIDENT RESPONSE PROTOCOLS

Develop and regularly update an incident response plan to quickly address and mitigate the impact of security breaches.

COLLABORATE WITH THREAT INTELLIGENCE SERVICES

Leverage threat intelligence services to stay informed about emerging threats and adjust your security strategies accordingly.

GROUP-IB



INVESTIGATING, PREVENTING AND FIGHTING CYBERCRIME SINCE 2003

GROUP-IB.COM
INFO@GROUP-IB.COM

GROUP-IB.COM/BLOG
+971 45681785

LINKEDIN FACEBOOK TWITTER INSTAGRAM