



INTELLIGENCE INSIGHTS

September-November Edition

INTRODUCTION

This report contains information on the most significant cybersecurity events that occurred worldwide and in the META region over the specified period of time.

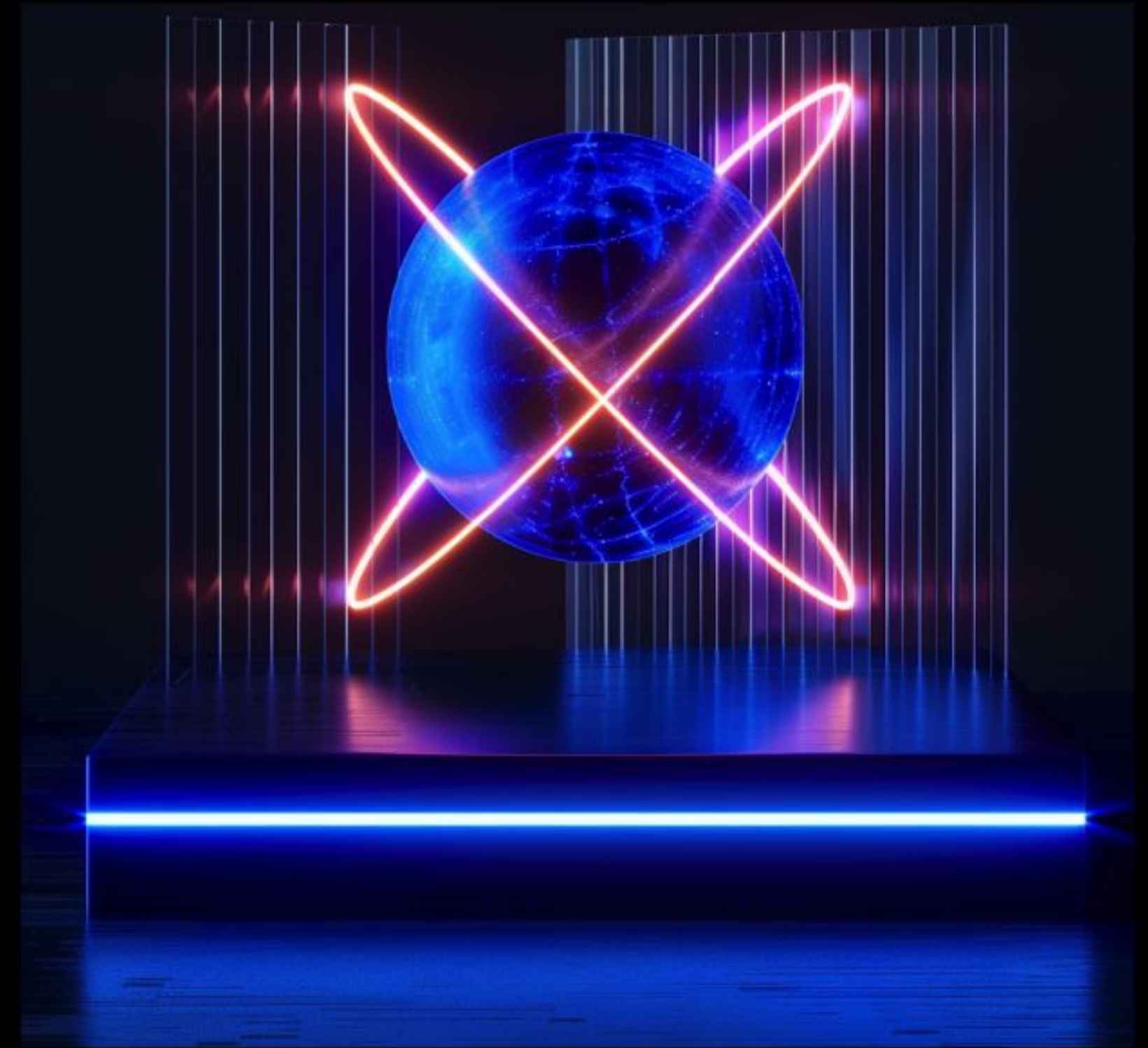
2 notable events of the period:



On 29/09/2025 an unknown source [has started leaking internal data from the Iranian threat actor](#) on a GitHub repository. The leaked files are exposing the Iranian APT affiliated with the Counterintelligence Division (Unit 1500) of the IRGC-IO, known as Charming Kitten.



In mid-September 2025, [Red Hat detected unauthorized access](#) to a self-managed GitLab instance used by Red Hat Consulting, later confirming a security incident after an extortion group calling itself Crimson Collective claimed responsibility. The group says it exfiltrated about 570 GB of data from ~28,000 repositories, including Customer Engagement Reports (CERs) that may contain client architecture diagrams, configuration data, and even authentication tokens for roughly 800 organizations worldwide, though Red Hat has not confirmed the full scope of these claims and stresses that product source code repos were not affected.



Global trends and their context:

1. Jaguar Land Rover (JLR) incident

Jaguar Land Rover (JLR) suffered a major cyberattack starting around 31 August–1 September 2025 that forced a global shutdown of manufacturing and retail IT systems for about five weeks, halting production at plants in the UK and overseas and leaving staff at home while systems were rebuilt. The responsibility for the incident was taken by the Scattered Lapsus\$ Hunters threat actor.

2. RedHat incident

In mid-September 2025, Red Hat detected unauthorized access to a self-managed GitLab instance used by Red Hat Consulting, later confirming a security incident after an extortion group calling itself Crimson Collective claimed responsibility. The group says it exfiltrated about 570 GB of data from ~28,000 repositories, including Customer Engagement Reports (CERs) that may contain client architecture diagrams, configuration data, and even authentication tokens for roughly 800 organizations worldwide, though Red Hat has not confirmed the full scope of these claims and stresses that product source code repos were not affected.



Global trends and their context:

3. APT35 leakage

On 29/09/2025 an unknown source has started leaking internal data from the Iranian threat actor on a GitHub repository. The leaked files are exposing the Iranian APT affiliated with the Counterintelligence Division (Unit 1500) of the IRGC-IO, known as Charming Kitten.

This leak, if confirmed authentic, constitutes a high-value intelligence source for CTI teams, particularly in the Middle East. It provides rare visibility into APT35's internal processes, targeting logic, toolsets, and strategic priorities — insights that can directly inform threat hunting, detection engineering, and defensive strategy.

4. Nation State Actor UNC5221 Compromised F5's Internal Network

In August 2025, F5, a leading cybersecurity and application delivery company, detected unauthorized access to its internal systems by a highly sophisticated nation-state threat actor. The intrusion, which involved persistent access and file downloads, targeted the BIG-IP product development environment and engineering knowledge management platforms. This incident underscores ongoing challenges in securing software supply chains, with no immediate operational disruptions reported by F5.



Global trends and their context:

5. Shai-Hulud Supply Chain Attack: The Second Coming Timeline of the Shai-Hulud Campaign

A rapidly growing npm supply-chain attack linked to the Shai-Hulud cluster has compromised major packages from vendors such as Zapier, ENS Domains, PostHog, and Postman. More than 770 packages and 25,000+ malicious GitHub repos across hundreds of accounts are now involved, with the campaign accelerating by roughly 1,000 repos every 30 minutes. The malware exfiltrates developer secrets, tokens, and project files into attacker-controlled GitHub repos, and a new preinstall-phase variant extends the blast radius across dev machines and CI/CD environments. The latest samples even include a destructive payload that deletes files if token theft is not possible—escalating the threat from pure espionage to destructive behavior.



Global trends and their context:

6. Credentials exposed on JSONFormatter & CodeBeautify

A recent report by [watchTowr](#) shows that many developers unwittingly leak sensitive credentials — passwords, API keys, tokens and internal configs — by pasting them into public web-tools like JSONFormatter or CodeBeautify. Analysis of over 80,000 submissions uncovered thousands of real secrets linked to high-value sectors such as finance, government and cloud providers. Because these tools offer public “share” or “recent items” links, anyone can access those submissions, meaning simple developer convenience is unintentionally exposing organizations to full compromise.

7. LANDFALL Spyware: Analysis of a Zero-Click Exploit Targeting Samsung Galaxy Devices

A new commercial-grade Android spyware family, designated LANDFALL, [was identified](#) during the analysis of malicious activity targeting Samsung Galaxy devices. The spyware was delivered through exploitation of a zero-day vulnerability (CVE-2025-21042) within Samsung’s Android image-processing library.

Activity associated with this campaign was observed beginning in mid-2024 and continued until the vulnerability was remediated through a security patch in April 2025. Although the flaw has since been mitigated, analysis indicates that the operation forms part of a broader pattern involving zero-click exploits and activities attributed to private-sector offensive actors (PSOAs) in the Middle East region.



Key regional trends with a brief description:

1. Unmasking MuddyWater's New Malware Toolkit Driving International Espionage

A recent MuddyWater campaign — [documented by Group-IB](#) — uses phishing emails with weaponized documents to deploy new bespoke backdoors (e.g. “Phoenix v4”) and custom loaders. Once executed, the malware establishes persistence, steals credentials, and enables remote access to compromised systems. The campaign targets governmental, diplomatic and telecom-sector organizations — especially across the Middle East and North Africa — as part of ongoing state-linked espionage efforts.

2. Unmasking MuddyWater's New Malware Toolkit Driving International Espionage

MuddyWater has launched a new global espionage campaign using phishing emails from compromised mailboxes to deliver malicious Word documents that install their custom backdoor Phoenix v4. Once installed, Phoenix v4 gives the attackers stealthy, persistent remote-access to networks — enabling data exfiltration and long-term surveillance. The campaign primarily targets governments, diplomatic services, telecoms and international organizations, especially across the Middle East and North Africa.

Middle East, Türkiye,
Africa & Pakistan

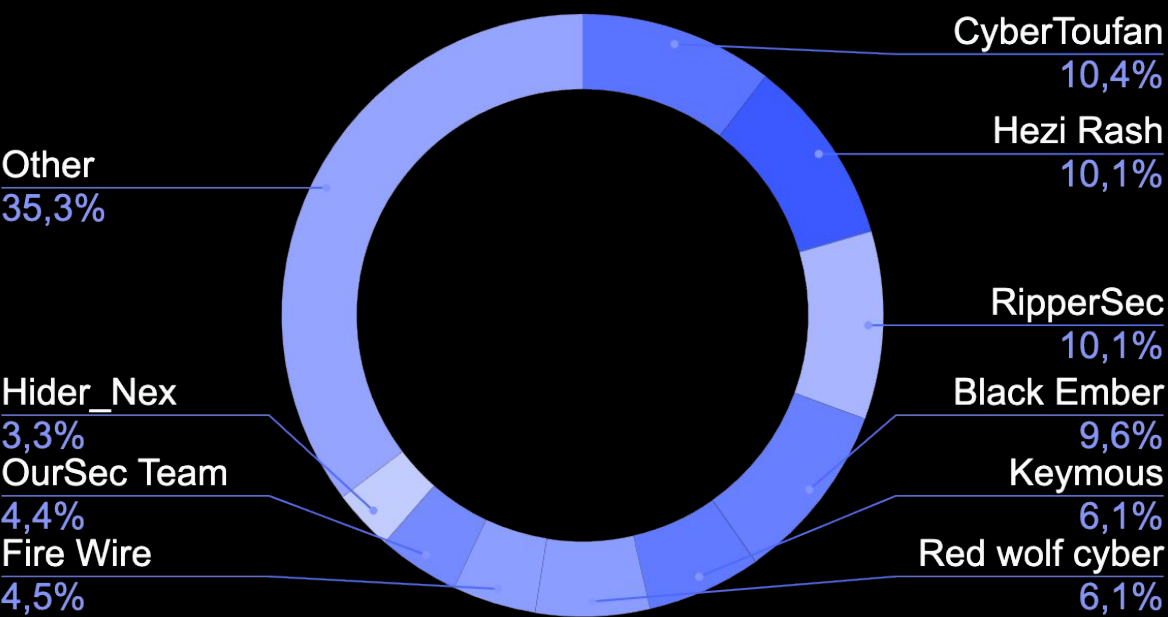


STATISTICS: HACKTIVISM

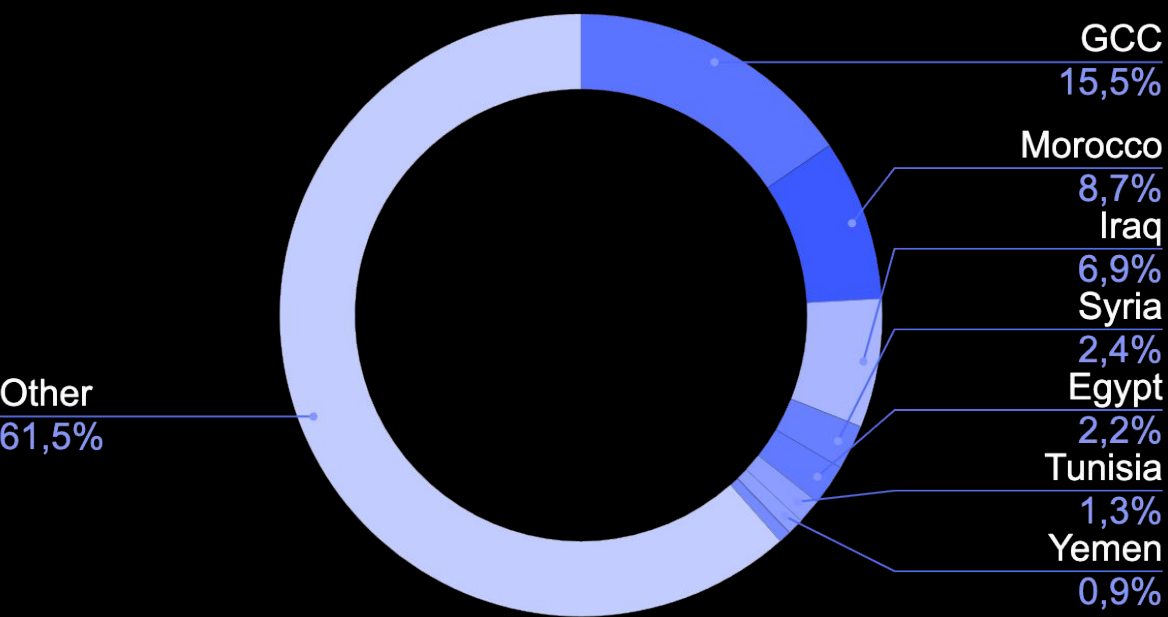
Hacktivism is the use of hacking techniques to support political or social agendas. Usually hacktivist groups are low-skilled hackers who perform DDoS, Defacement, and Data Breaches (mostly leveraging compromised accounts) attacks.

During the specified period, **912** hacktivist events were discovered. The most active groups in the region were **CyberToufan** (10.4%), **Hezi Rash**, and **RipperSec** (10.1%). Among the most attacked countries are **GCC countries** (15.5%), **Morocco** (8.7%), and **Iraq** (6.9%). The top attacked sectors are **Government and military** (34%), **Education** (9.4%), and **Financial services** (8.1%).

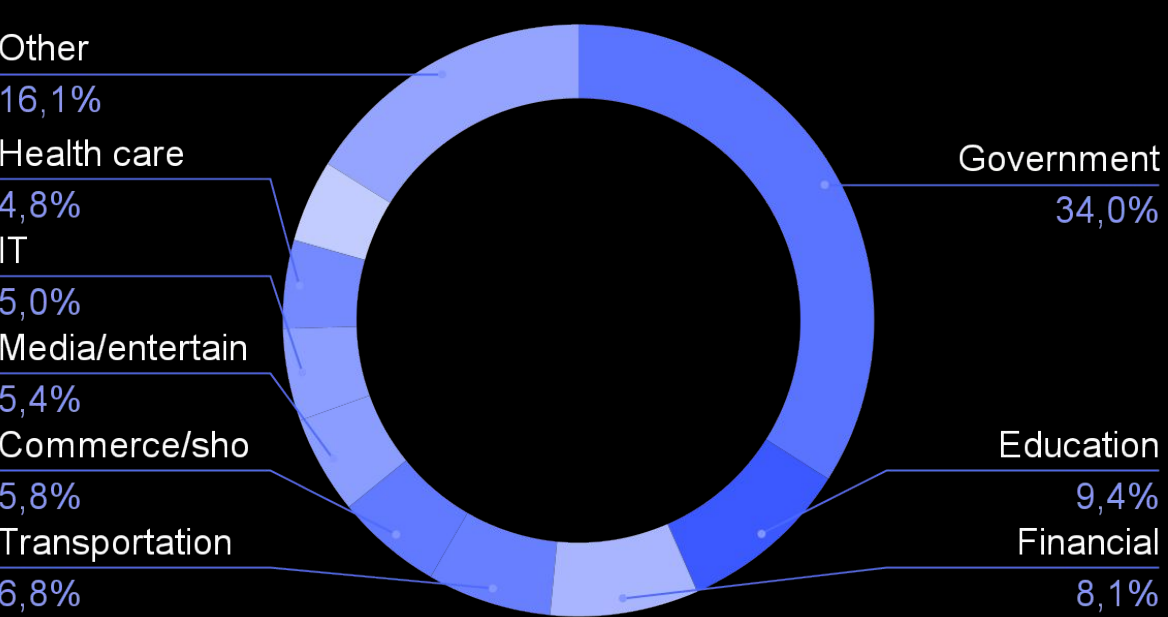
Hacktivists events by Threat Actors



Hacktivists events by countries



Hacktivists events by sectors



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 specified period of time in the META region were as follows:

76 Ransomware incidents

Most active threat actors



Most targeted industries

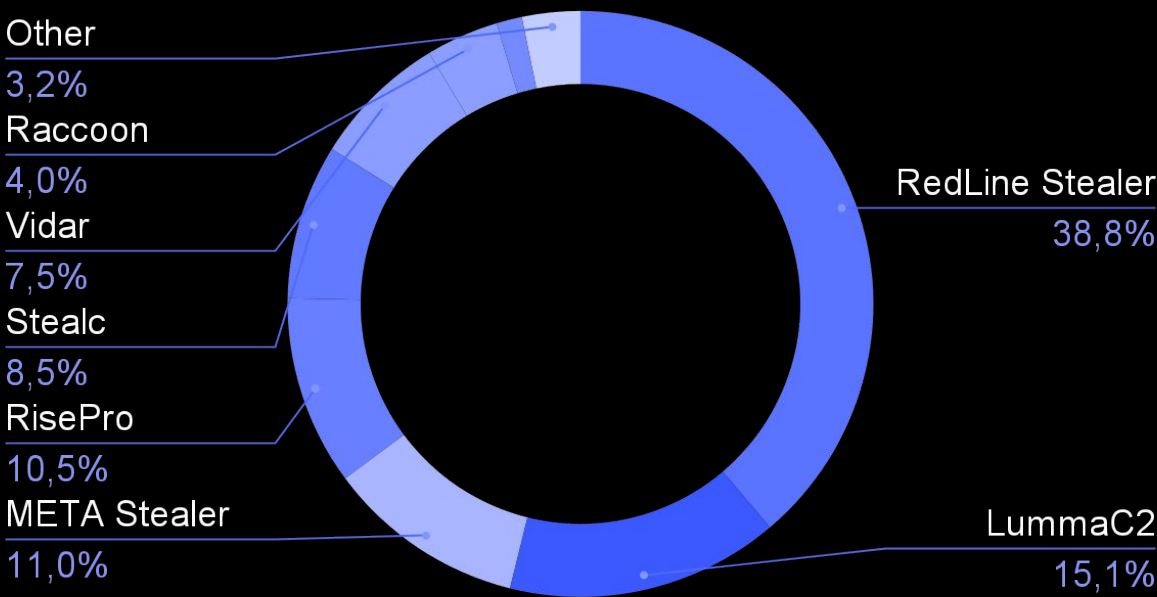


STATISTICS: COMPROMISED DATA

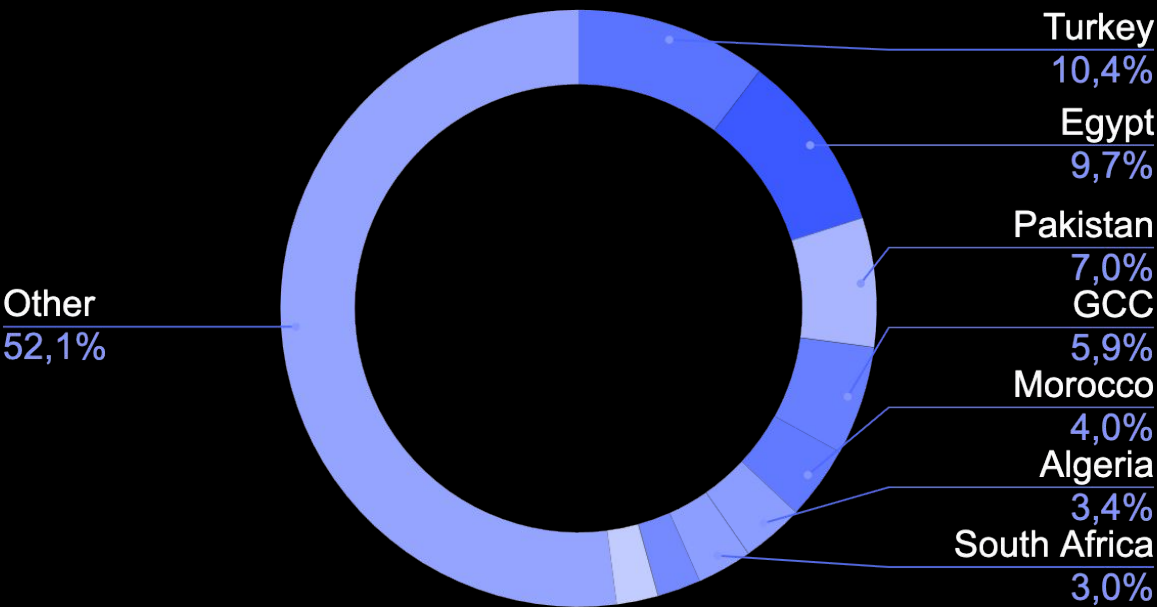
Compromised accounts are a significant threat because they allow unauthorized access to sensitive personal or corporate information, leading to potential financial loss, identity theft, and reputational damage. Additionally, compromised accounts can be used to launch further attacks, causing operational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

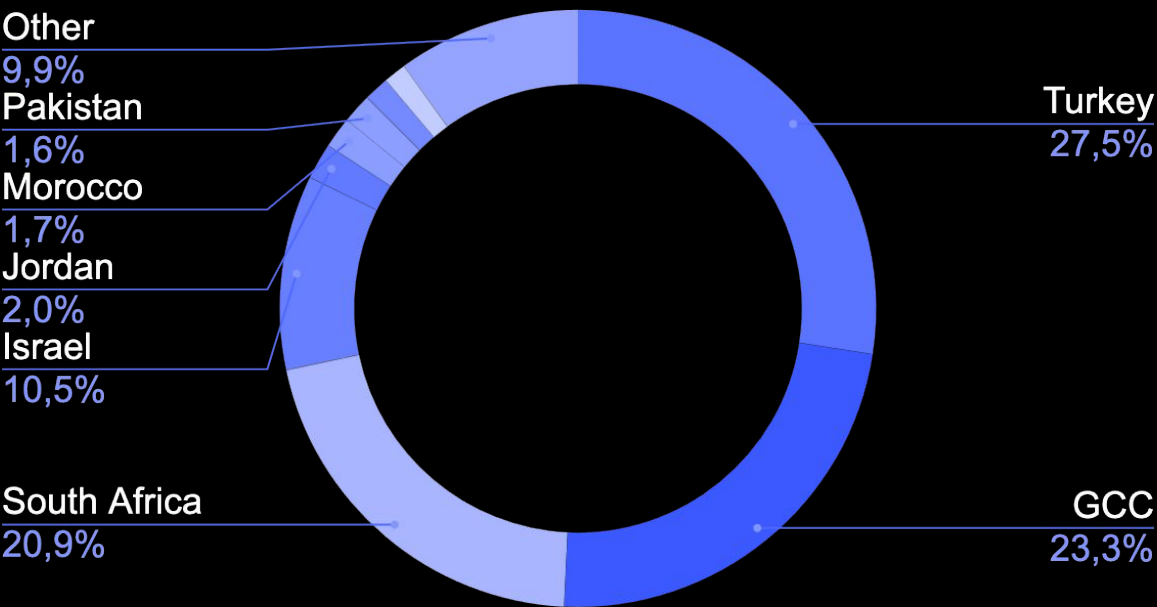
Compromised accounts by malware



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 risk and security management strategies accordingly.

STAY SMART. STAY CONNECTED. STAY SECURED

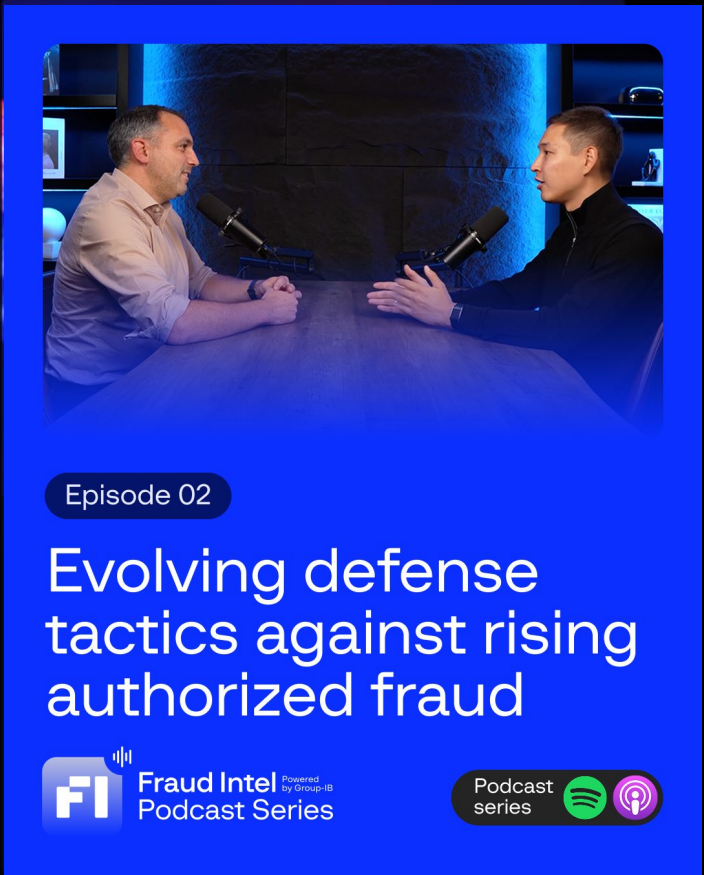


[Talk to our team](#)

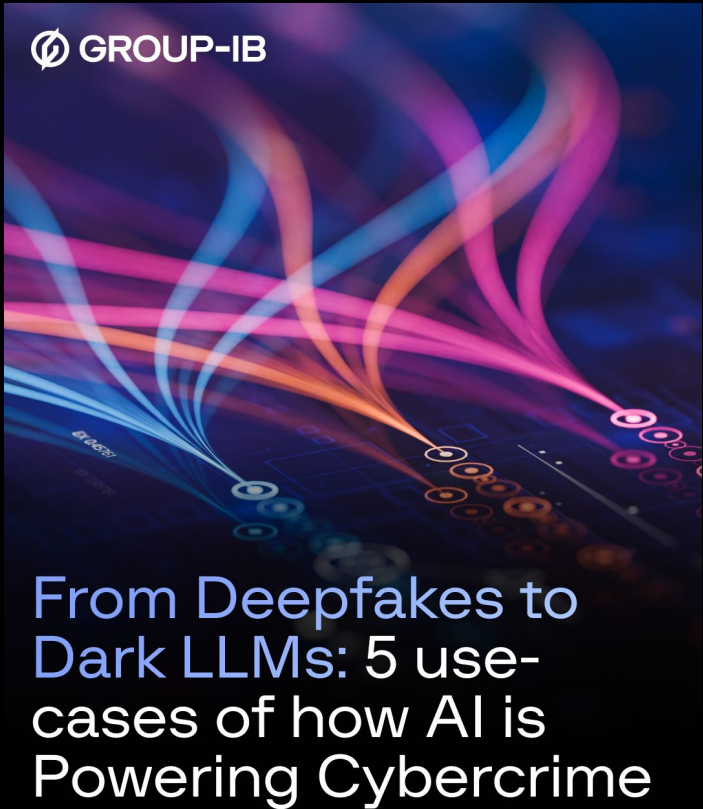
RECENT
RESOURCES



[Read now](#)



[Watch now](#)



[Read now](#)