INFORMATION BULLETIN

Cybercrime Monitoring

October 15–31, 2025

EXECUTIVE SUMMARY

This report presents the findings from monitoring and analysis of cybercrime activities observed between October 15 and 31, 2025. The threat landscape remains driven by exploitable vulnerabilities and the improper exposure of internet-facing services.

KEY FINDINGS

- Incident Types: Exposures of Personal Data and Relevant Mentions of organizations and individuals were the most recurrent, underscoring the critical need for safeguarding sensitive information and managing digital reputation.
- Most Affected Sectors: The Military, Government, and Financial sectors experienced the highest concentration of incidents, reflecting their strategic value and attractiveness to cybercriminals.
- Predominant Vulnerabilities: Recurring attack vectors included publicly accessible SSH services, software downloads via P2P networks, and open FTP servers—all exploitable for unauthorized access and data dissemination.
- Data Sources (OSINT): The majority of intelligence originated from Telegram and Pastebin, highlighting the necessity of continuous monitoring of these platforms.
- Notable Incidents: Significant events included targeted attacks against airport infrastructure and the emergence of a new banking malware, dubbed Herodotus, specifically targeting Brazilian users.
- Hacktivist Activity: Cyber campaigns increasingly reflect political and ideological motivations, with hacktivist and digital activist groups leveraging these drivers in their operations.

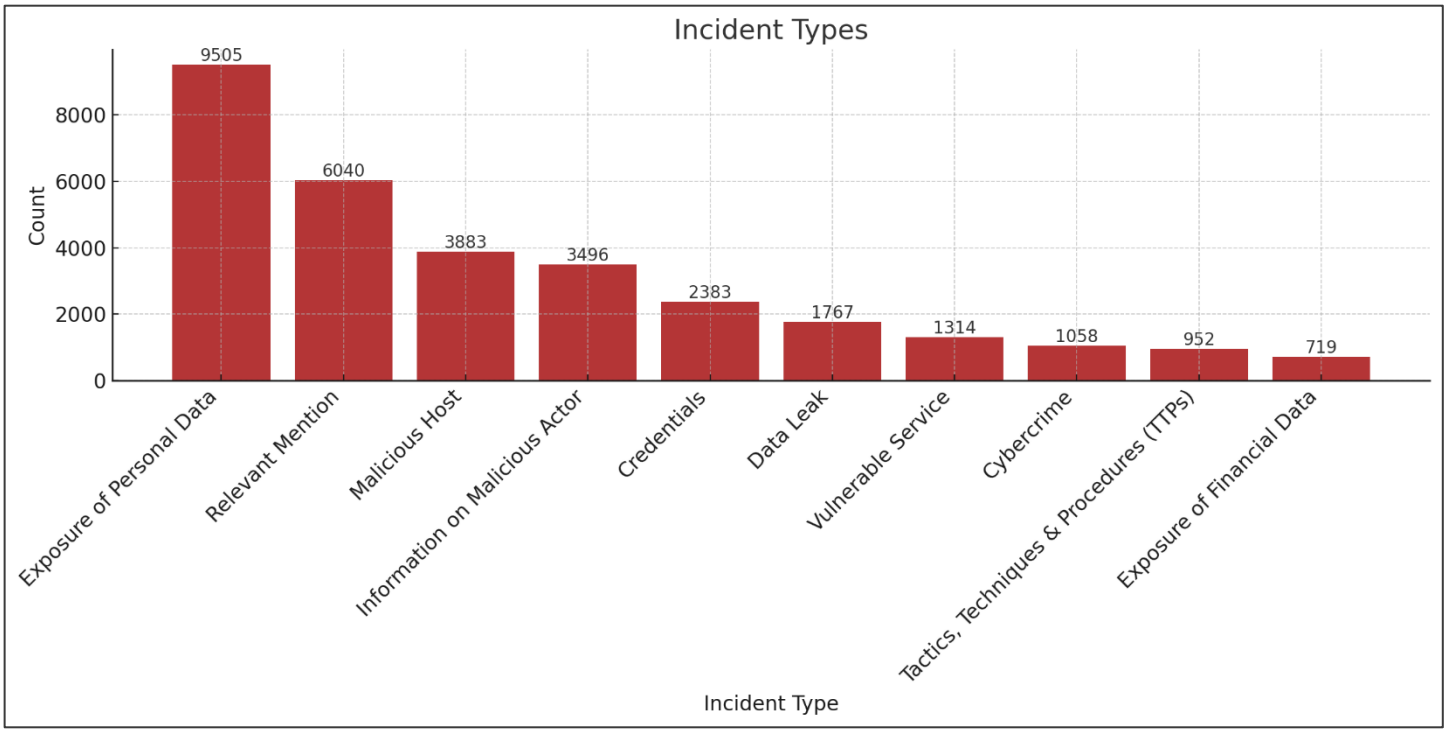
SOURCES

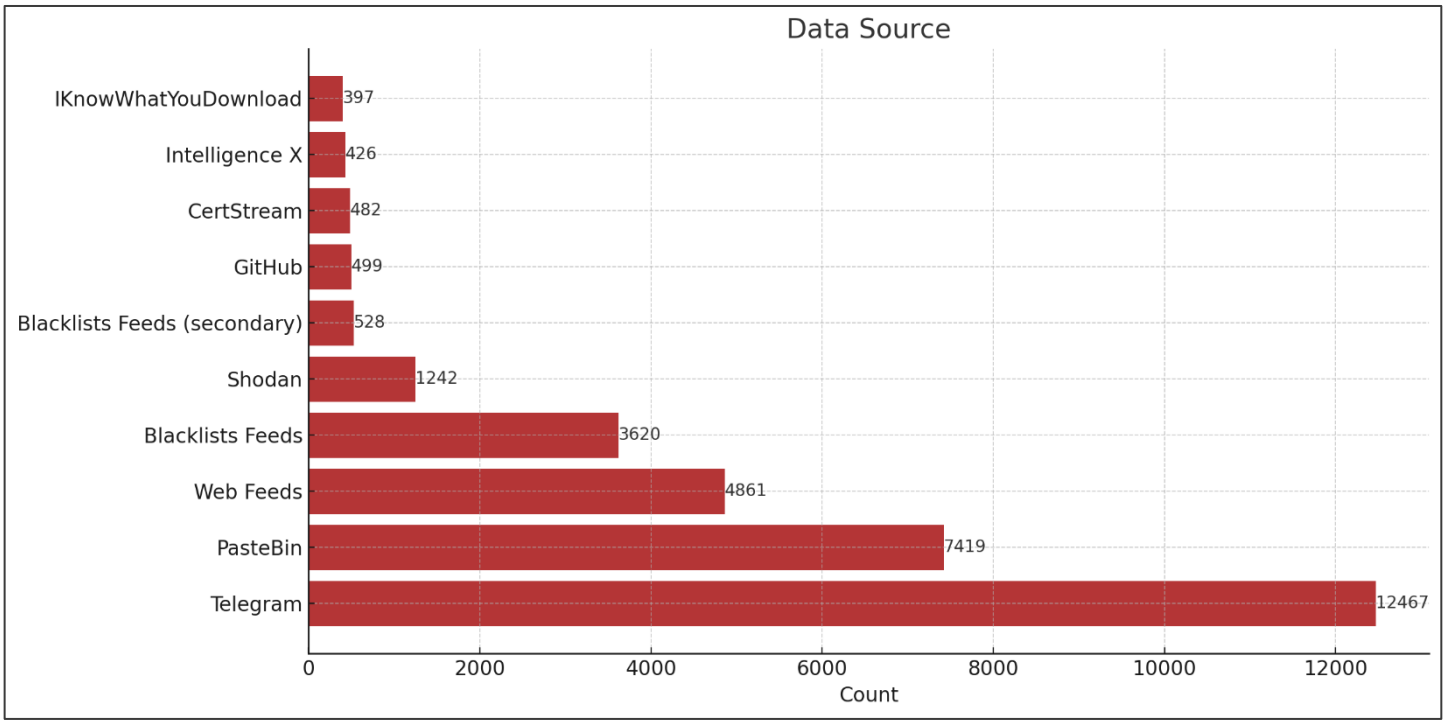
- Proprietary Neural™ platform.

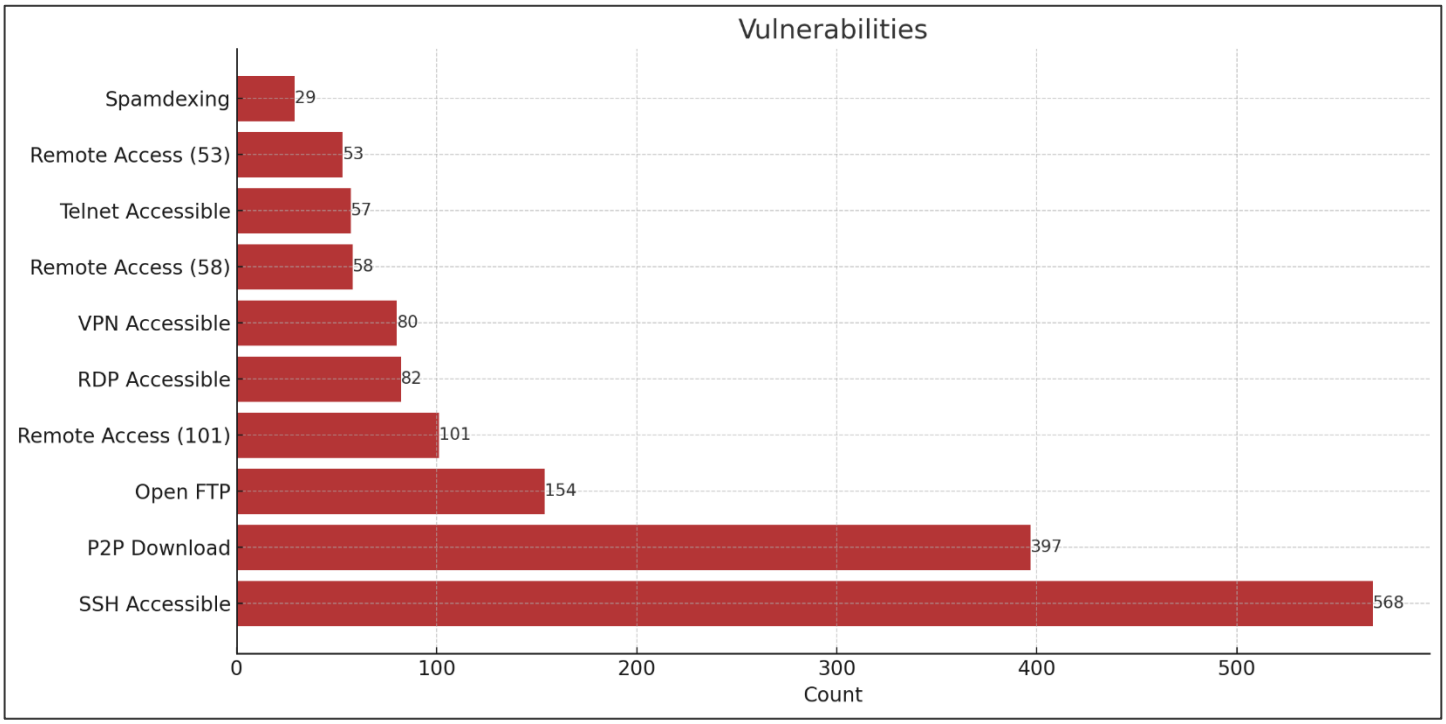
INCIDENTS BY THE NUMBERS

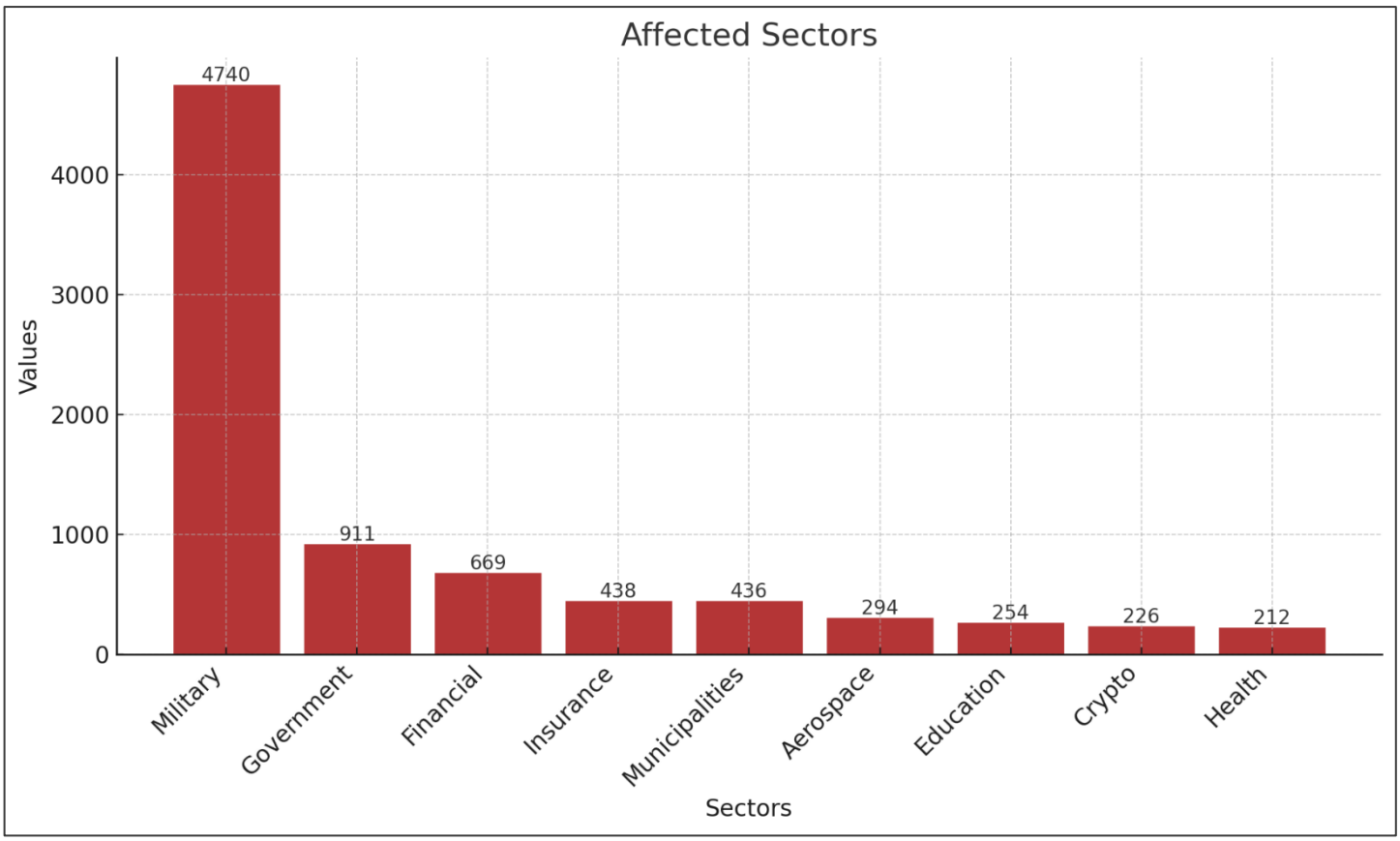
Observed Incidents: 34,283

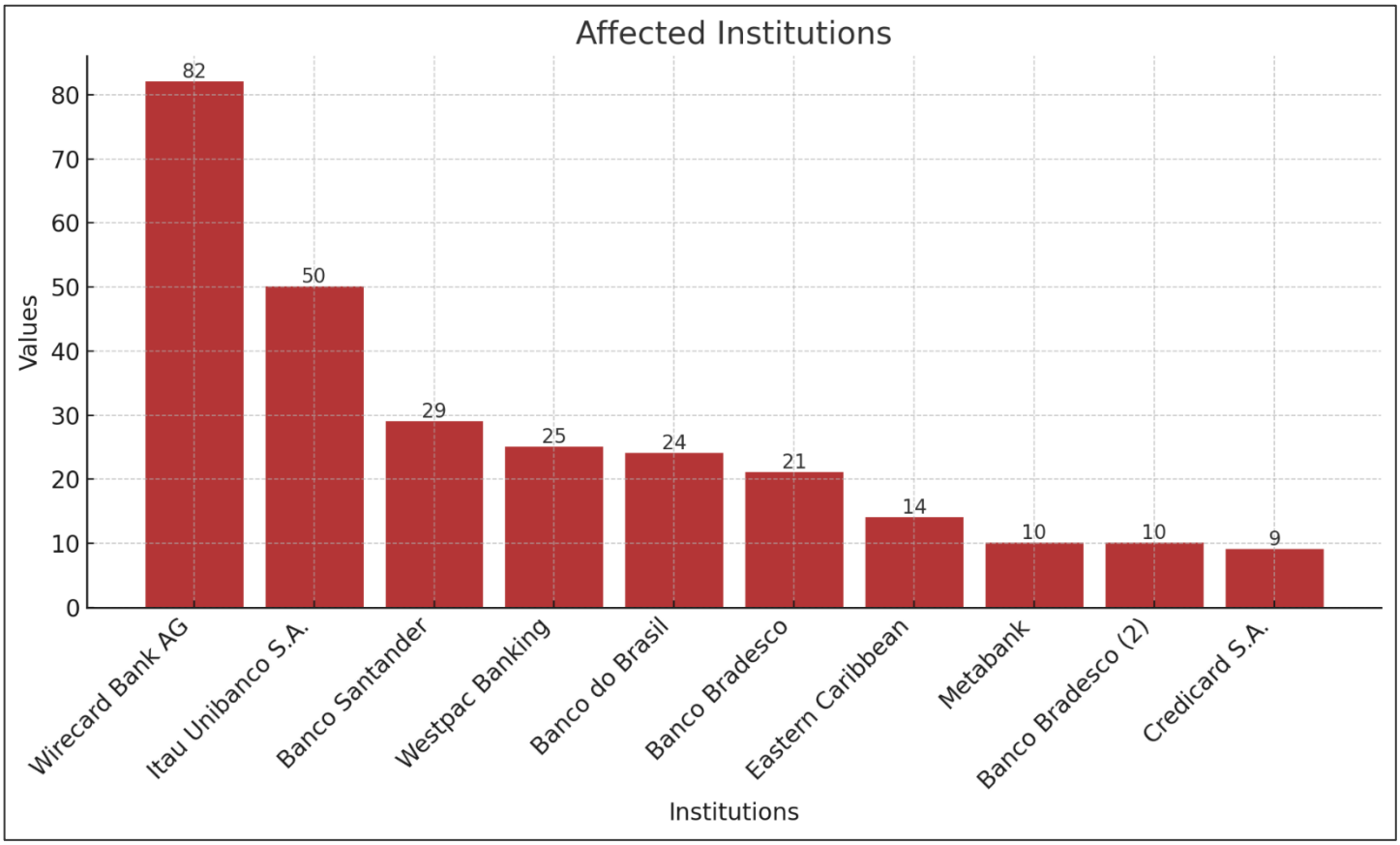
Involved Actors: 2,344






Vulnerabilities
Spamdexing
Remote Access (53)
Telnet Accessible
Remote Access (58)
VPN Accessible
RDP Accessible
Remote Access (101)
Open FTP
P2P Download
SSH Accessible
29
53
57
58
80
82
101
154
397
568
0
100
200
300
400
500
Count


Affected Sectors
Values
0
1000
2000
3000
4000
4740
911
669
438
436
294
254
226
212
Military
Government
Financial
Insurance
Municipalities
Aerospace
Education
Crypto
Health
Sectors



DETECTED VULNERABILITIES

In the second half of October 2025, exposure vectors remained consistent: remote access services and legacy protocols continued to dominate among the identified risks. Most incidents involved unprotected exposed services (SSH, RDP, VPN, Telnet) and file transfer/sharing services (P2P, FTP), as well as web interfaces used to manage industrial and security equipment. This pattern reinforces that misconfigurations, lack of system hardening, and weak credential management persist as primary enablers for malicious actors.

In such cases, it is recommended to prioritize basic cyber hygiene controls (strong authentication and MFA, patching/updating, attack surface reduction), network segmentation, and continuous monitoring to reduce exposure and detection time.

Key Observed Vulnerabilities

Accessible SSH (568 occurrences, 1.66%)

- Tactic: Direct exposure of SSH services to the internet without compensating controls.
- Techniques: Brute-force attacks, credential stuffing, use of poorly protected or leaked private keys, and exploitation of accounts with elevated privileges.
- Observed procedures: Initial server access, privilege escalation, lateral movement within the network, and deployment of backdoors or persistence tools.
- Recommended mitigations: Disable password-based authentication, implement MFA/OTP, use bastion hosts or jump servers, restrict access via ACLs/whitelists, rotate and secure SSH keys, and monitor login attempts.

P2P Downloads (397 occurrences, 1.16%)

- Tactic: Use of P2P networks to distribute and execute malicious code, as well as to evade detection.

- Techniques: Sharing of malicious binaries, trojans disguised as popular files, P2P channels as C2 vectors, and fragmented data exfiltration.
- Observed procedures: Installation of malicious agents on workstations, lateral movement across the corporate environment, and exfiltration of unencrypted data.
- Recommended mitigations: Block P2P traffic at perimeter/endpoint levels, inspect traffic, implement DLP controls, and provide user awareness training.

Open FTP (154 occurrences, 0.45%)

- Tactic: FTP servers available without proper authentication or configured with overly permissive access rights.
- Techniques: Unmonitored uploads/downloads, use of anonymous accounts, and brute-force attacks on credentials.
- Observed procedures: Storage and movement of sensitive data via FTP, deployment of web shells, and establishment of persistence points.
- Recommended mitigations: Disable legacy FTP, migrate to SFTP/FTPS, audit accounts and permissions, and implement centralized logging.

Remote Access to Web Interface – Industrial System (101 occurrences, 0.29%)

- Tactic: Exposure of industrial management panels and interfaces (SCADA/ICS) without access controls.
- Techniques: Exploitation of known vulnerabilities in HMIs/PLCs, weak authentication, and injection attacks on web interfaces.
- Observed procedures: Manipulation of operational parameters, disruption of industrial processes, and risks to physical safety and operational continuity.
- Recommended mitigations: Isolate OT networks, use MFA-enabled administrative VPNs, implement robust segmentation, and apply virtual patching where immediate updates are not feasible.

Accessible RDP (82 occurrences, 0.24%)

- Tactic: RDP ports exposed without additional protection.
- Techniques: Brute-force attacks, exploitation of protocol vulnerabilities, and use of compromised credentials.
- Observed procedures: Session takeover, ransomware deployment, and lateral movement.
- Recommended mitigations: Disable public-facing RDP, use MFA-enabled VPNs, restrict access via firewalls, and apply geolocation/time-based blocking policies.

Accessible VPN (80 occurrences, 0.23%)

- Tactic: Exposed or misconfigured VPN services.
- Techniques: Exploitation of appliance vulnerabilities, credential stuffing, and bypasses via weak configurations.
- Observed procedures: Unauthorized remote access to internal networks and use as a pivot platform.
- Recommended mitigations: Update appliances, review authentication policies, implement post-authentication segmentation, and monitor session logs.

Remote Access to Firewall Web Admin Interface (58 occurrences, 0.17%)

- Tactic: Administrative ports of firewalls and appliances accessible from external networks.

- Techniques: Exploitation of default credentials, unpatched CVEs, and CSRF/SSRF attacks on web interfaces.
- Observed procedures: Modification of firewall rules, opening of ports, and establishment of tunnels for persistent access.
- Recommended mitigations: Restrict administrative access by IP address, enforce MFA, enable comprehensive logging, and separate control/management planes.

Accessible Telnet (57 occurrences, 0.17%)

- Tactic: Use of the legacy, unencrypted Telnet protocol.
- Techniques: Credential sniffing and brute-force attacks.
- Observed procedures: Compromise of legacy devices and use as trojan horses for pivoting.
- Recommended mitigations: Disable Telnet, migrate to secure protocols (e.g., SSH), and inventory legacy devices.

Remote Access to Router (53 occurrences, 0.15%)

- Tactic: Router management interfaces exposed with weak credentials.
- Techniques: Router takeover and NAT/DNS manipulation for hijacking campaigns.
- Observed procedures: Traffic redirection, interception/exfiltration, and establishment of network persistence.
- Recommended mitigations: Apply hardening measures, update firmware, and disable public remote management.

Spamdexing (29 occurrences, 0.08%)

- Tactic: Use of black-hat SEO and abusive indexing to promote malicious or phishing content.
- Techniques: Creation of cloaked pages and abuse of legitimate websites to host malicious content.
- Observed procedures: Amplification of phishing campaigns, increased fraud success rates, and distribution of malicious links.
- Recommended mitigations: Monitor web reputation, rapidly remove compromised content, and track publication vectors.

NOTABLE INCIDENTS

Attacks on Airport Infrastructure

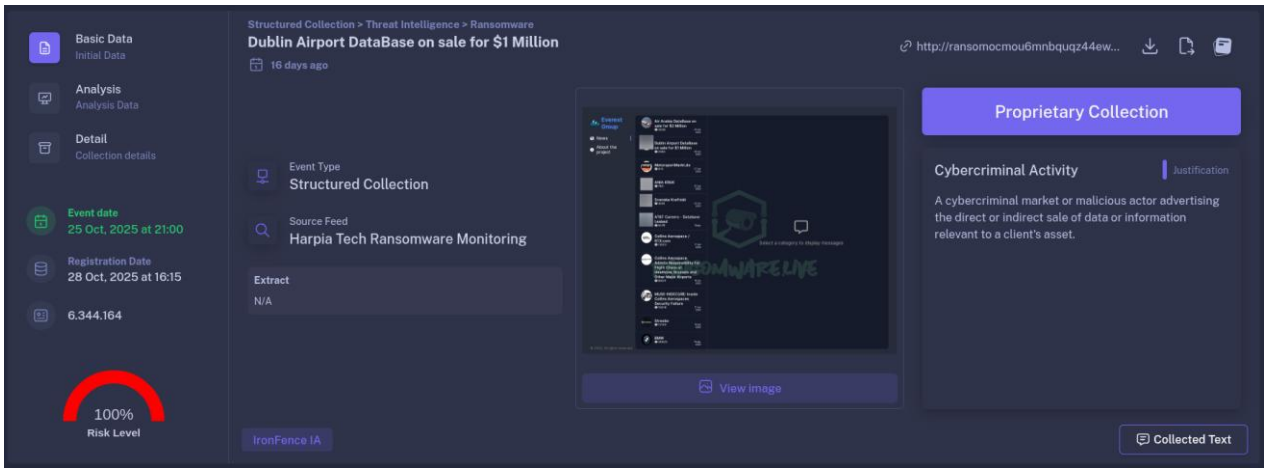
A series of data leaks linked to the aviation sector was identified, published on the Everest ransomware group's website, involving Collins Aerospace, Dublin Airport, and Air Arabia.

According to the group, these incidents resulted in access to extensive repositories of personal, corporate, and operational data. In the Collins Aerospace case, over 50 GB of information was allegedly exposed—including 1.5 million passenger records, employee data, and internal infrastructure files—reportedly obtained via an exposed FTP server. This incident appears linked to the disruptions that affected European airports in September 2025.

Regarding Dublin Airport, Everest claims to have copied a database containing 1.53 million personal records, including complete flight, passenger, and baggage details. The Air Arabia incident allegedly involves approximately 18,900 employee records containing HR information and internal documents.

All three leaks were published in October 2025, reinforcing this group's recent trend of targeting commercial aviation and airport infrastructure.

These cases can be referenced in the Neural™ registry under IDs: 6,344,164; 6,337,872; and 6,317,144.



Main Risks

- Exposure of personal and corporate data: Including passenger records, employee information, and sensitive internal data.
- Operational risk: Potential impacts on check-in systems, baggage logistics, and flight continuity.
- Secondary exploitation: Threat actors may leverage the stolen information for phishing campaigns, social engineering, or lateral movement within airport networks.

Recommendations

- Assess exposure: Confirm whether corporate assets or data related to the affected companies are present in your environment.
- Strengthen server and access security: Review permissions on FTP servers, VPNs, and internal portals accessible to suppliers or partners.
- Monitor mentions and leaks: Track forums and channels where the data might be shared or sold.
- Review contingency plans: Test business continuity and incident response plans involving critical systems.

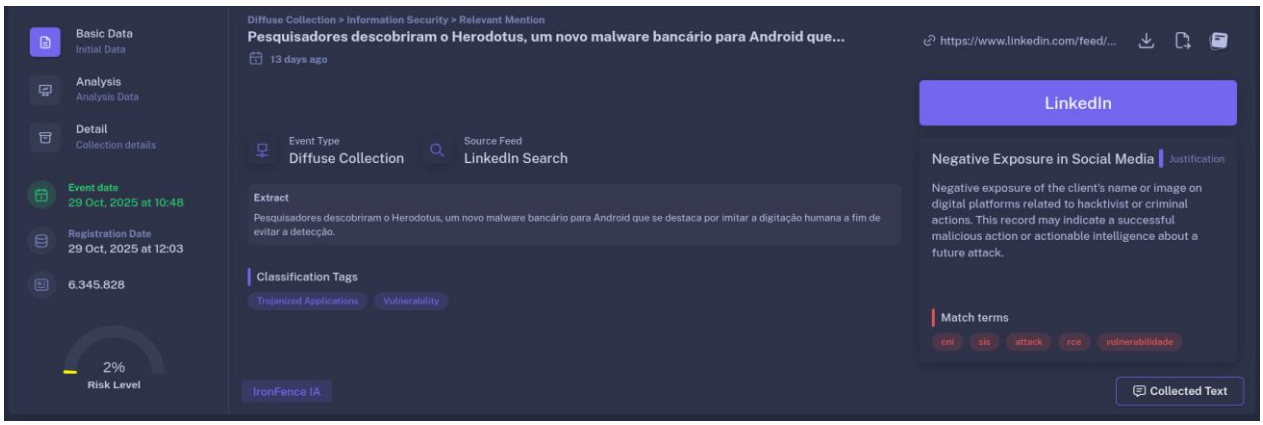
New Banking Malware

A new banking trojan targeting users in South America—particularly Brazil—has been identified, named Herodotus. This malware mimics human behavior to bypass security controls and autonomously execute banking transactions. It inserts random pauses between keystrokes to simulate genuine user activity, thereby evading biometric systems and anti-fraud mechanisms.

Herodotus is classified as a Device-Takeover Trojan, capable of fully compromising an infected device. It can perform clicks, swipe screens, type text, and carry out actions that closely mimic legitimate user behavior. Additionally, it includes typical features of modern banking trojans, such as overlay attacks, SMS and 2FA code theft, and accessibility logging—which enables it to capture passwords and sensitive data displayed on-screen.

Distribution occurs via SMiShing (SMS-based phishing), using messages that impersonate communications from banks and payment companies. In Brazil, the malware masquerades as the "Módulo Segurança Stone" app; in Italy, it appears as "Banca Sicura."

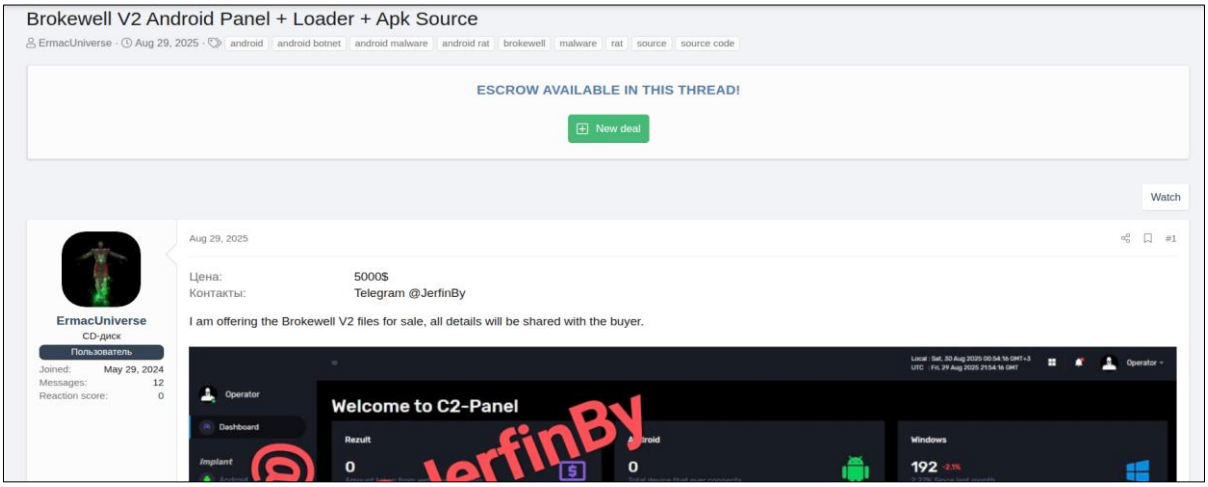
Herodotus is also sold on cybercriminal forums as Malware-as-a-Service (MaaS) by an actor identified as "K1RO," significantly increasing its potential for widespread dissemination.



Extract
Researchers discovered Herodotus, a new Android banking malware that stands out for mimicking human typing to avoid detection.
Negative Exposure in Social Media
Negative exposure of the client's name or image on digital platforms related to hacktivist or criminal actions. This record may indicate a successful malicious action or actionable intelligence about a future attack.

Technical analysis revealed that Herodotus shares portions of code with the Brokewell malware, first discovered by researchers in April 2024. Although not a direct evolution, Herodotus operates by combining segments of Brokewell with original code.

Through our monitoring of cybercriminal forums, we also identified the sharing of Brokewell within Russian-speaking cybercrime communities.



Brockwell malware shared on Russian forum

Main Risks

- Banking credential theft: The malware collects logins, passwords, and authentication codes, enabling unauthorized financial transactions.
- Full device takeover: Attackers can remotely operate the victim's mobile device, accessing apps, messages, and personal data.
- Legitimate disguise: The use of names and interfaces resembling trusted institutions increases infection rates.
- Malware-as-a-Service (MaaS): Herodotus is offered via subscription models, making it easier for other criminal groups to deploy and scale attacks.

Recommendations

- Avoid installing apps outside the Play Store: Herodotus is distributed through external links and installers ("droppers").
- Be wary of SMS messages containing links: Legitimate financial institutions do not send messages requesting the installation of "security modules."
- Review accessibility permissions: Deny accessibility permission requests from unknown apps—these permissions can grant full device control.
- Strengthen authentication: Use authenticator apps (e.g., Google Authenticator, Microsoft Authenticator, Authy) or physical security keys instead of SMS-based two-factor authentication.
- Audit corporate devices: Review policies regarding app installation and the use of accessibility services on employee mobile devices.
- Monitor incidents: Track alerts related to Herodotus and SMiShing campaigns targeting banks and domestic payment processors.

NOTABLE THREAT ACTORS

List of actors with the highest activity between October 15 and October 31, 2025

Actor	Motivation	Type
DimasHxR	criminal	undefined
qilin	ransomware	group
anesmansory	hacktivist	individual
akira	ransomware	group
Katiba Des Kuffars	hacktivist	group
sinobi	ransomware	group
alrahbi5	hacktivist	individual
saleh_binali	hacktivist	individual
ReKaNErrOr	ego	undefined

Anesmansory

In addition to monitoring cybercrime-associated actors, the Neural™ platform also tracks hacktivist and activist groups. This monitoring helps identify relevant mentions of companies, government agencies, and their representatives, enabling early detection of potential threats—including risks to physical facilities, institutional reputation, and the personal reputations of organizational members who may become targets of such actors.

The monitored actor "Anesmansory" is an example of a hacktivist. In the context of ongoing conflicts in the Middle East, he primarily uses the X platform to criticize the United Arab Emirates (UAE), accusing the country of involvement in the deaths of Sudanese civilians and of supporting violence in Sudan. Although his relevance to the South American context is low, this profile was selected to illustrate the importance of monitoring such actors, who can pose risks such as narrative amplification, incitement to protests, and damage to the institutional image of governments and corporations.

Below is the actor's profile in Neural™, accompanied by an analysis of the risks associated with his social media posts, as well as platform-collected records that illustrate key examples of his activity and the potential impacts identified.

Total incidents: 92

✓ Status: Active

Language: Arabic

Motivation: Hacktivist

Capacity: Novice

Actor Registration: 03/12/2025

Last update: 03/12/2025

First Registration: 03/11/2025

Incident Type

Relevant Mention — 97.8% (90 Incidents)

Data Leak — 2.2% (2 Incidents)

Origin

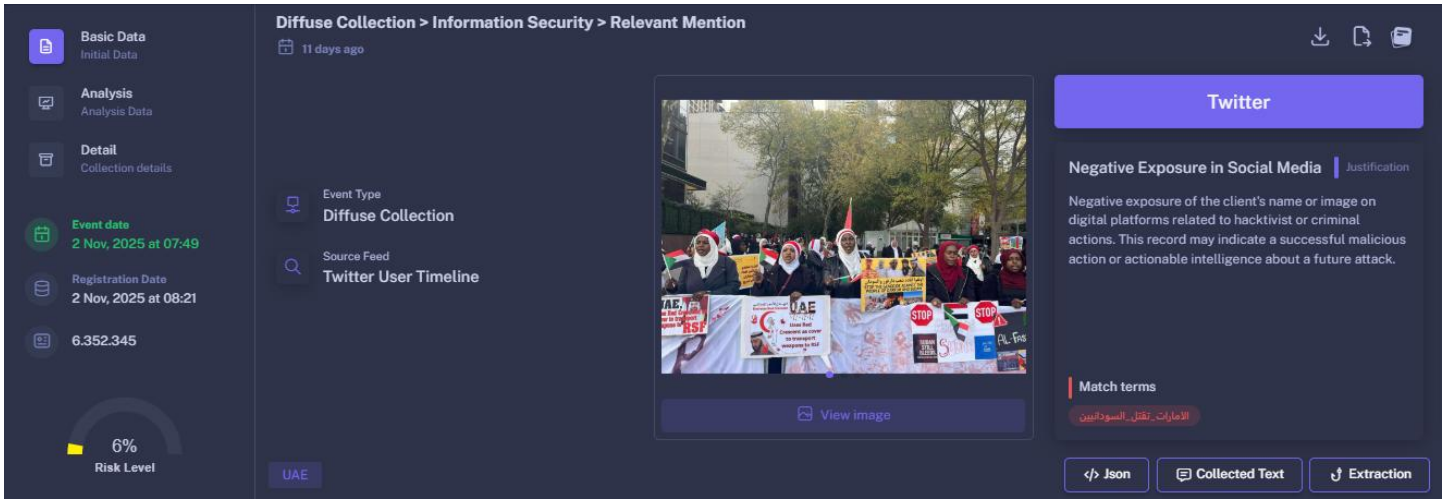
Twitter — 100% (92 Incidents)

Collection Type

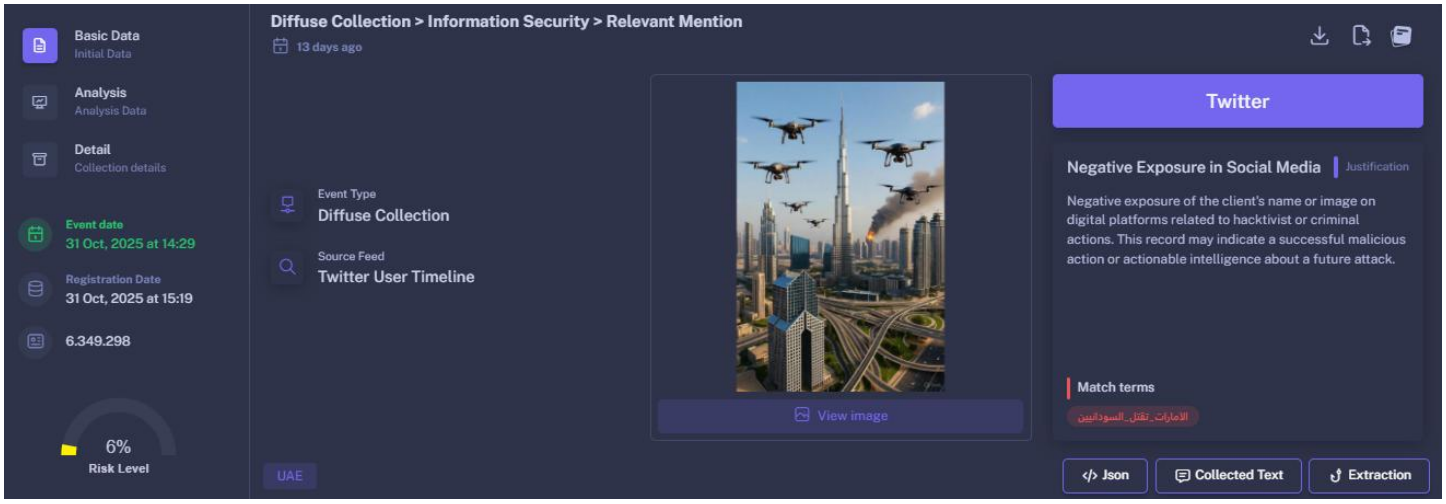
Diffuse Collection — 100% (92 Incidents)

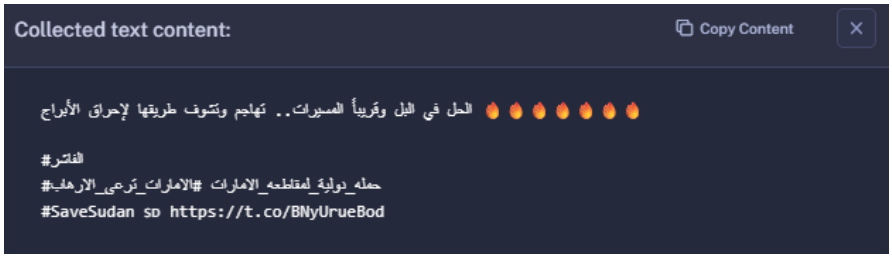
Key Identified Risks

Physical facility risks: Analyzed messages call for protests outside the United Nations headquarters in New York and mobilizations of Sudanese communities in European and Western capitals. Additionally, two specific posts reference attacks against the UAE (including mentions of “burning towers” and rhetoric threatening damage to infrastructure), which increases the risk of directed actions against physical facilities and symbols associated with the United Arab Emirates.

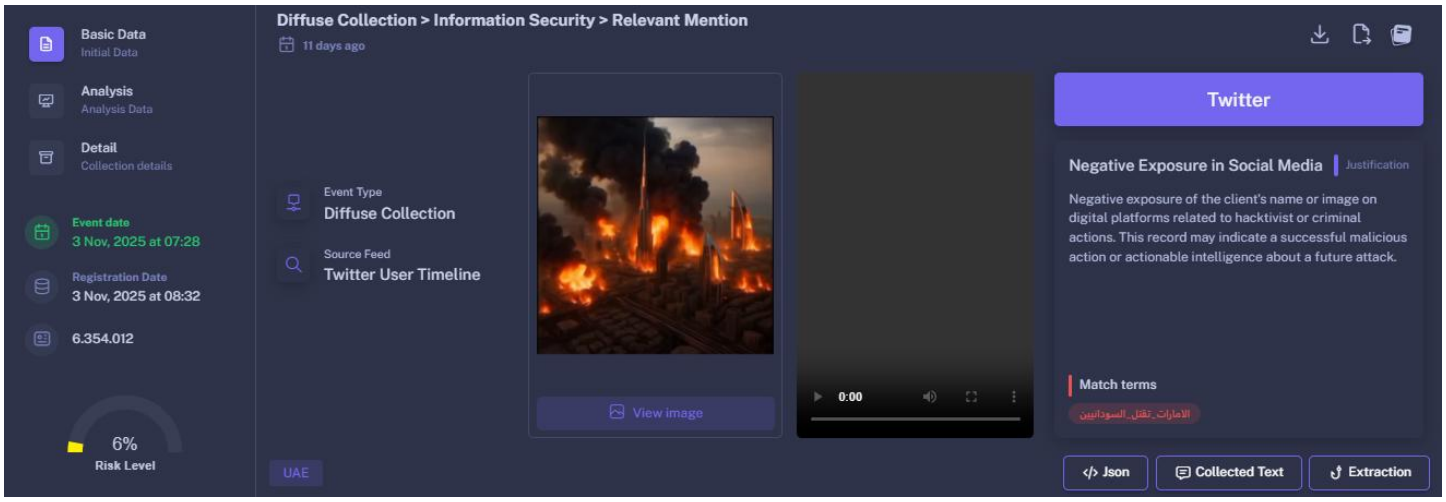


Collected text content:
In front of the United Nations headquarters, New York
Let the world hear our voice rejecting genocide, ethnic cleansing, and Emirati aggression.
We call on Sudanese people in all capitals and cities of European and Western countries to protest and inform the public and parliaments there about the Janjaweed's plan aimed at exterminating and eliminating the Sudanese people. https://t.co/RFOtMwJISL





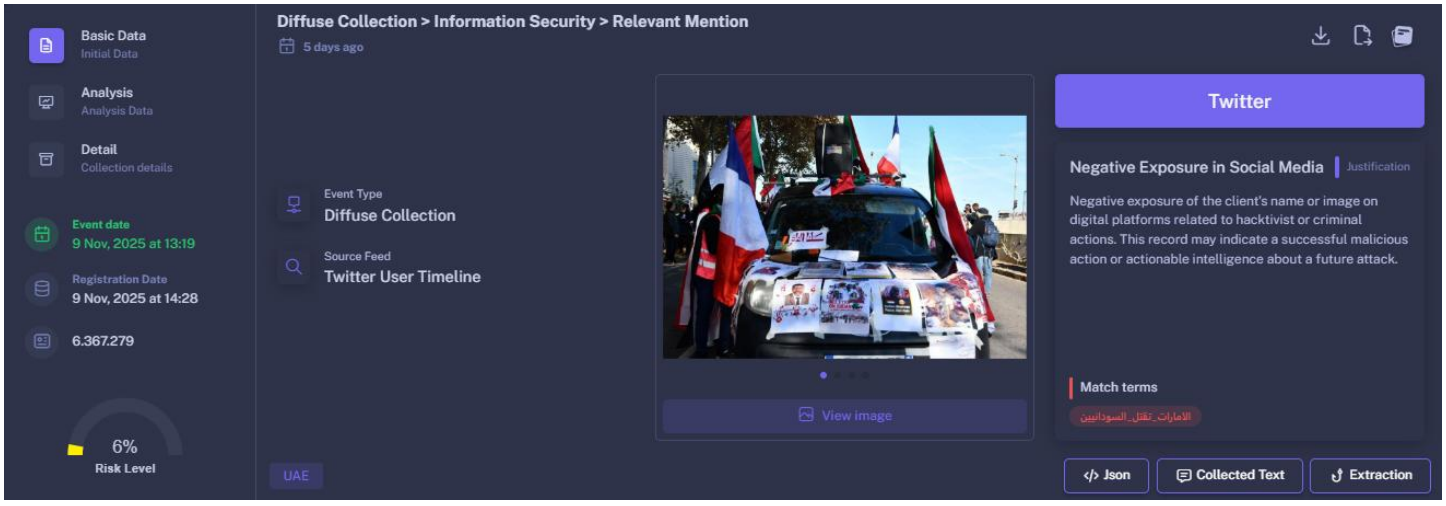
Collected text content:
The solution is in ballistic missiles, and soon the drones...
They will attack and find their way to set the towers on fire 🔥🔥🔥🔥🔥🔥🔥
#AlFashir
#International_Campaign_to_Boycott_UAE
#UAE_sponsors_terrorism
#SaveSudan **sd**

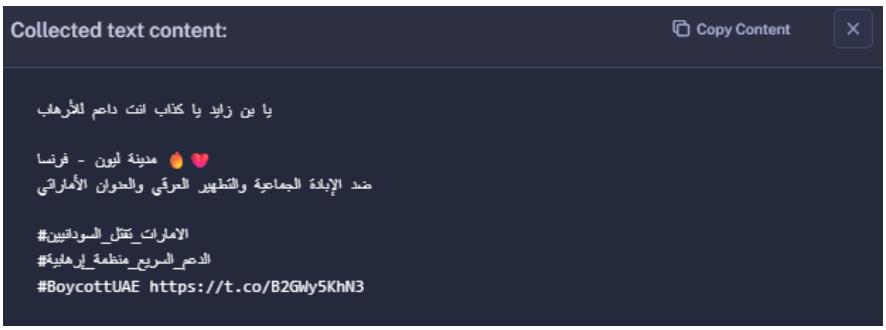


Collected text content:
You will burn just as you burned Sudan 🔥🔥
This is the sentiment of all Sudanese.
And we will return your hostility to you...
And make you drink the deadliest poison...
And we will strike your towers and your homes...
With shells and artillery fire.
#BoycottUAE
#UAE_kills_Sudanese
#UAEKillsSudanesePeople

Reputational Risks

The analyzed messages encourage boycotts of companies from the United Arab Emirates (UAE), particularly airlines such as Emirates and Etihad, and discourage travel to Dubai and Abu Dhabi. They also instruct users to post accusatory comments and criticisms of the UAE government on the official social media profiles of these companies. The use of hashtags such as #BoycottUAE, #KeepEyesOnSudan, and #UAESupportsGenocideInSudan amplifies the reach of these narratives, posing a significant risk to the institutional reputation of the UAE and its leading brands.





Collected text content:
O Ibn Zayed, you liar — you are a supporter of terrorism.
City of Lyon – France 🔥💔
Against genocide, ethnic cleansing, and Emirati aggression

#UAE_kills_Sudanese
#RSF_is_a_terrorist_organization
#BoycottUAE

Collected text content:
This is the Emirates Airlines account — go to it and post comments showing the massacres committed by the UAE in Al-Fashir, using the hashtags:
#BoycottUAE
#UAE_kills_Sudanese
#UAEKillsSudanesePeopl
Hurry before they disable the comment feature.

CONCLUSION

The analyzed data shows that well-known techniques continue to be reused, while emerging threats demonstrate rapid adaptation to the current context by exploiting persistent gaps in digital security. The low technical complexity of these exploits, combined with the broad exposure of essential services, sustains a high likelihood of incidents even without the use of sophisticated attack vectors.

In the public sector and across critical infrastructures, the risk of essential service disruption and leakage of sensitive information reinforces the need for continuous vigilance and more robust response and resilience mechanisms.

This report was developed using data collected through the Neural™ platform, integrating quantitative and qualitative analyses covering tactics, techniques, and procedures (TTPs), relevant incidents, and the most active actors observed during the two-week period.

AwesomeCyber maintains active and continuous monitoring of open sources and clandestine environments with the purpose of anticipating emerging threats, identifying the early activity of malicious actors, and supporting organizations in mitigating cyber risks. This effort aims to strengthen defensive posture, increase security maturity, and ensure greater resilience in an ever-evolving digital landscape.