Sep, 2025

INTELLIGENCE INSIGHTS EUROPE

Defend against what’s ahead by uncovering month-over-month trends and insights for Europe’s threat landscape (July - August)

Key insights

- On August 19, 2025, the ransomware group Warlock claimed responsibility for an attack targeting Colt Technology Services — a multinational telecommunications company headquartered in London, United Kingdom.
- In August, Initial Access Brokers listed companies with the following top revenue figures: $75M (Greece), $38M (United Kingdom), and $30M (Germany).
- INTERPOL's "Operation Serengeti 2.0," supported by Group-IB, led to 1,209 cybercriminal arrests across Africa, dismantling over 11,400 pieces of malicious infrastructure and recovering $97.4M for victims.
- NoName057(16) and Z-ALLIANCE were the two most active hacktivist groups performing DDoS attacks targeting companies and organizations in the EU.

Val Shirko
Regional Business Head, Europe

This report offers an overview of the latest threat landscape in Europe, covering key developments such as ransomware attacks, leaked credentials, data breaches, and more. It includes a month-over-month trend analysis to track evolving patterns. Additionally, the report spotlights a newly identified threat actor, campaign, emerging technique, providing actionable insights for proactive defenses.

Click here to take a 1-min survey now to improve the report.

THREAT LANDSCAPE

GROUP-IB

Month over Month Comparison
(July - August)

42%

DDoS / Hacktivism attacks

28%

Ransomware attacks

10%

Initial access broker sale

46%

Leaked & sold credentials

DDOS AND HACKTIVISM BY COUNTRY

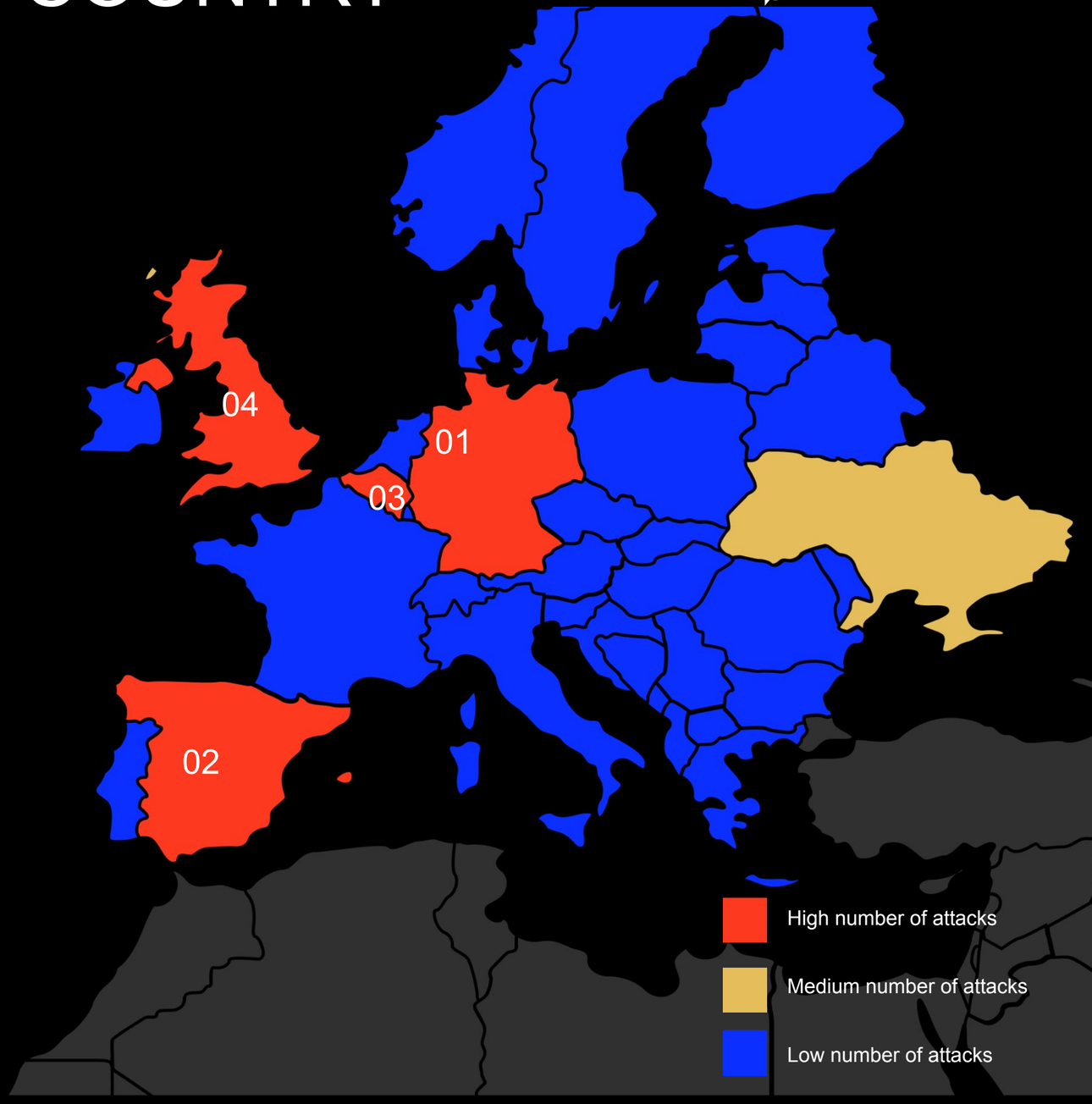
GROUP-IB

Key events

- The threat actor Mr. Hamza claimed responsibility for attacks on Spanish energy companies: Naturgy Energy Group, Red Electrica, SOLARIA Energy and Environment, EDP, Grupo Cobra, Ingeteam.
- NoName057(16) and Z-ALLIANCE were the two most active hacktivist groups performing DDoS attacks targeting companies and organizations in the EU.

Most attacked countries

Germany	Spain	Belgium	UK
65 attacks	48 attacks	22 attacks	22 attacks
+ 7%	+ 700%	+ 340%	+ 144%



RANSOMWARE ACTIVITIES

GROUP-IB

Key events

- On August 19, 2025, the ransomware group Warlock claimed responsibility for an attack targeting Colt Technology Services, a multinational telecommunications company headquartered in London, United Kingdom.
- On August 20, 2025, the ransomware group Qilin claimed responsibility for an attack targeting Ids Ingegneria Dei Sistemi S.p.A. IDS, part of Fincantieri NexTech, is an engineering and systems technologies company that provides research, innovation, and products in electromagnetic engineering, satellite communications, robotics and unmanned systems, and radar technologies for civil and defense applications.

↑ 28%

153 Ransomware incidents

Most active threat actors

Qilin

25 attacks
+ 39%

SafePay

18 attacks
+ 6%

DragonForce

17 attacks
+ 89%

J Group

11 attacks
+ 175%

Warlock

6 attacks
(0 in July)

Most targeted industries

Manufacturing

20 attacks
+ 5%

Professional Services

9 attacks
+ 125%

IT

6 attacks
(0 in July)

Construction

6 attacks
- 25%

Retail

5 attacks
- 55%

INITIAL ACCESS BROKER SALE ON DARK WEB

↓ 10%

36 Sales

GROUP-IB

Initial access to a company's systems can lead to data theft, corporate espionage, or the deployment of malware for various malicious purposes. This page shows the volume and geographic distribution of corporate infrastructure access instances currently for sale on the dark web.

Key events

- The antivirus software most frequently mentioned by Initial Access Brokers was Windows Defender.
- The highest revenue figures among companies put up for sale by Initial Access Brokers in August were: $75M (Greece), $38M (United Kingdom), and $30M (Germany).

Most targeted countries

LEAKED & SOLD CORPORATE CREDENTIALS

GROUP-IB

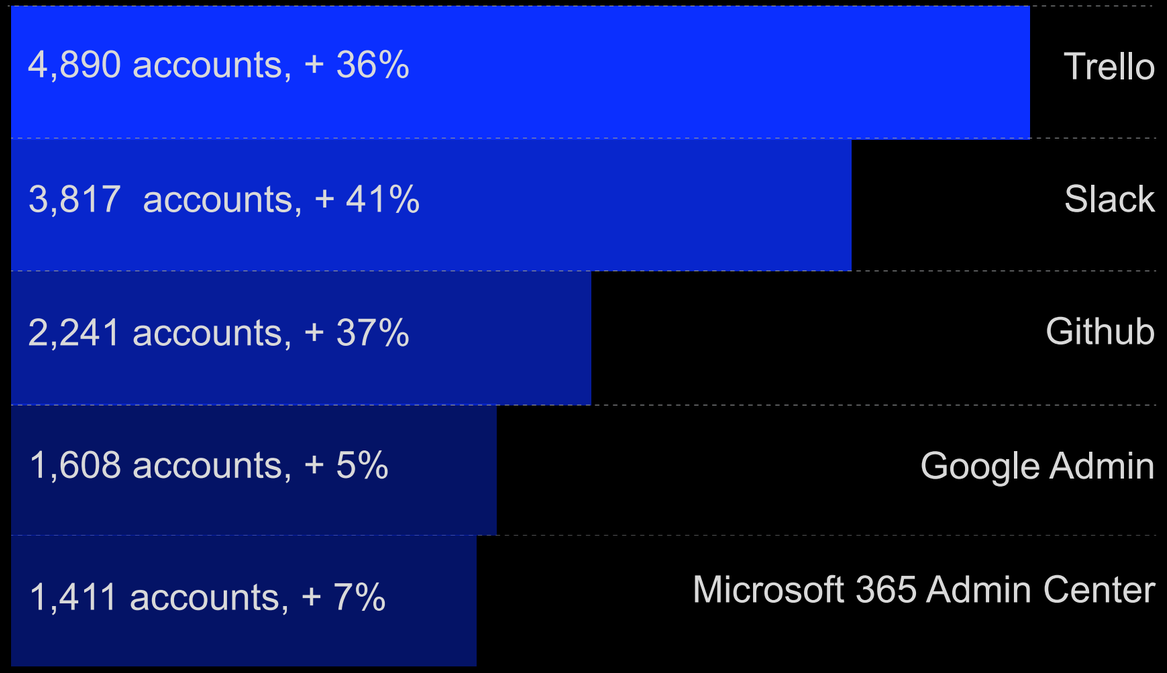
Key events

- Most compromised corporate accounts detected in August were stolen by password stealers and belonged to users in France, Spain, Italy, Poland, and the United Kingdom.
- The most active adversary-in-the-middle phishing framework in August was Tycoon 2FA.

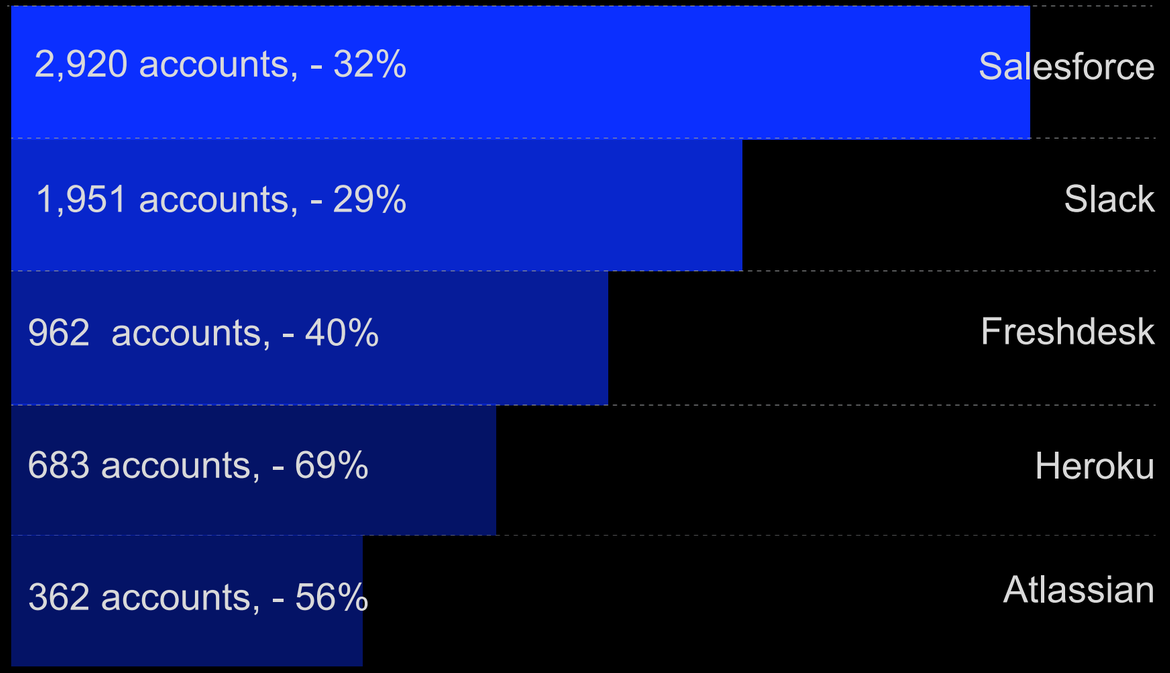
↓ 47%
compromised accounts: 218,777

↓ 35%
on sale on dark web markets: 13,354

Services with the most compromised accounts



Services with the most on sale accounts



OPERATION SPOTLIGHT

GROUP-IB

INTERPOL’s “Operation Serengeti 2.0”

Key outcomes

- INTERPOL’s “Operation Serengeti 2.0,” supported by Group-IB, led to 1,209 cybercriminal arrests across Africa, the dismantling of over 11,400 instances of malicious infrastructure, and the recovery of $97.4 million for victims.
- As an INTERPOL Gateway Partner, Group-IB contributed circumstantial intelligence on a cryptocurrency investment scam, and details of the malicious infrastructure linked to the scheme. Group-IB also provided INTERPOL and its investigators with findings relating to the infrastructure linked to business email compromise (BEC) campaigns, as well as broader intelligence on malicious infrastructure hosted across the African region.

Read more.

Click here to take a 1-min survey now to improve the report.

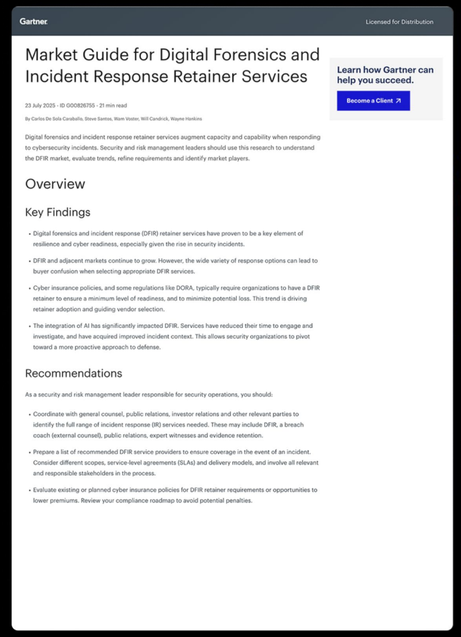
STAY SMART. STAY CONNECTED. STAY SECURED

[Talk to our team]

GROUP-IB

RECENT RESOURCES

Read now



Read Now

MEET US AT EVENTS

Register now