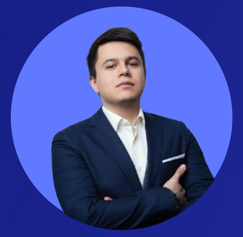
GROUP-IB

February, 2025

INTELLIGENCE INSIGHTS EUROPE

Defend against what's ahead by uncovering month-on-month trends and insights for Europe's threat landscape (January - February)

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.



ANTON USHAKOV
Head of Cyber Threat Intelligence

Key Insights

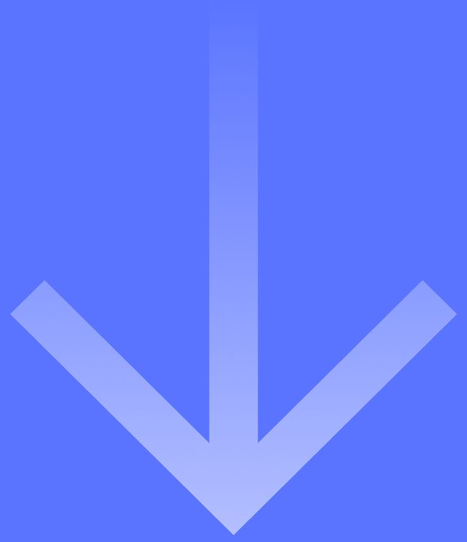
- RansomHub stayed the most active ransomware group active in Europe for the last two months.
- Access to companies in the UK and Spain was the most popular offer among Initial Access Brokers in February.
- Hacktivists focused on attacking websites in France and Germany in February.
- Accounts of cloud-based services available for sale on underground markets are still the most common type of credentials that could be used to access corporate resources.

THREAT LANDSCAPE

GROUP-IB

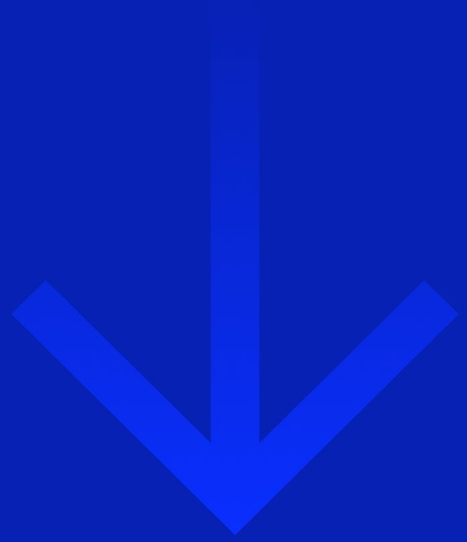
Month over Month Comparison
(January vs February)

7%



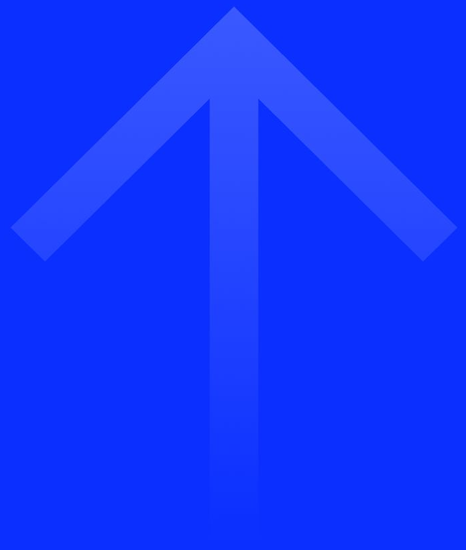
DDoS / Hacktivism attacks

62%



Ransomware attacks

32%



Initial access broker sale

9%

Leaked & sold credentials

DDOS AND HACKTIVISM BY COUNTRY

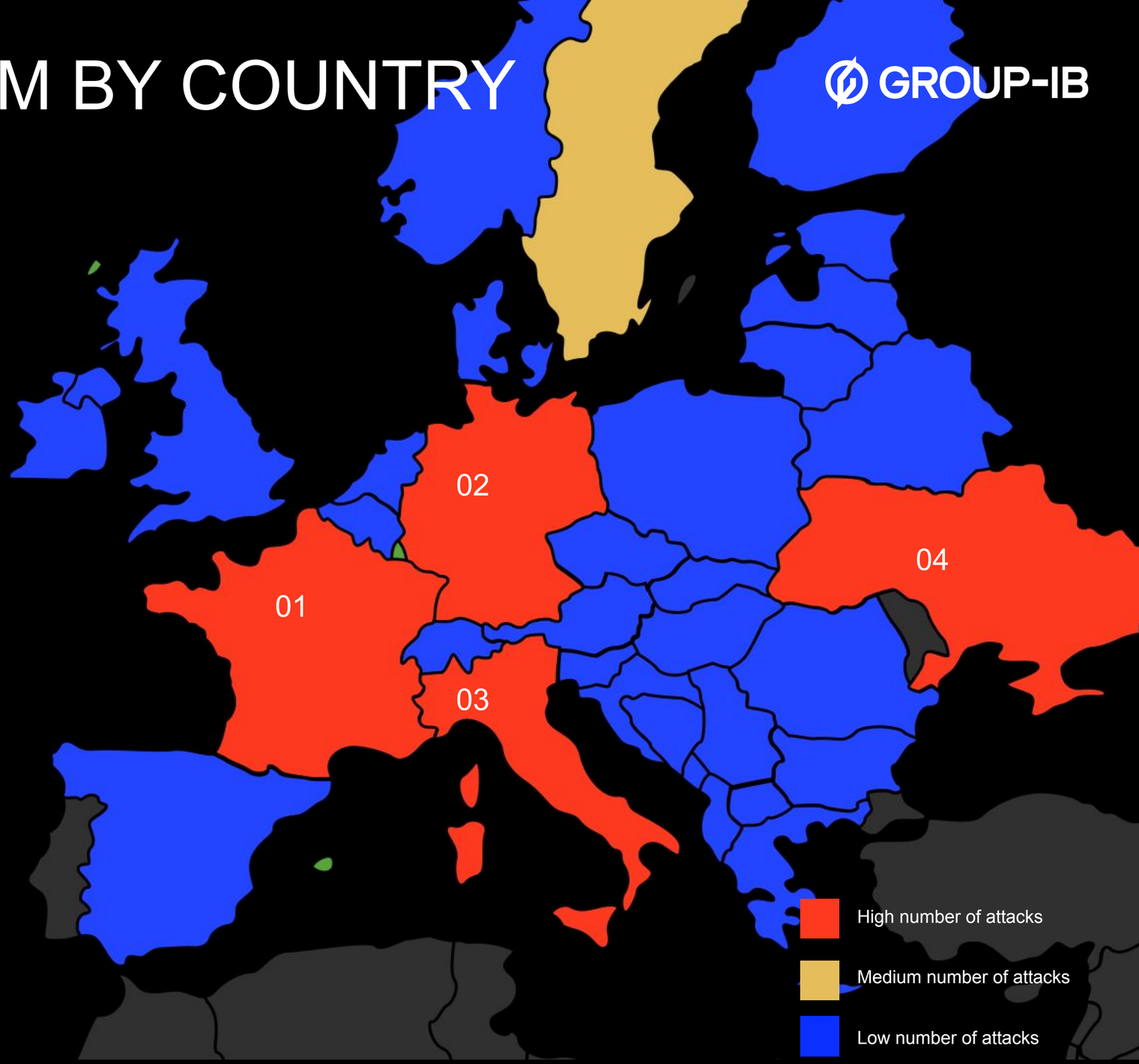
GROUP-IB

Key Events

- Mr Hamza and NoName057(16) were the most active hacktivists conducting attacks on websites in Europe.
- Most hacktivist attacks primarily targeted government websites as well as those of financial companies and services.

Most attacked countries

France	Germany	Italy	Ukraine
13 attacks	12 attacks	9 attacks	9 attacks
+8%	+300%	+80%	+350%



RANSOMWARE ACTIVITIES

Key Events

- New ransomware group Linkc was detected in February 2025
- New Ransomware-as-a-Service (RaaS) affiliate program Anubis was detected in February 2025.
- Law enforcement seized 8Base Ransomware DLS, arrested 4 suspects.
- New ransomware group Kraken allegedly related to Hellokitty was detected in February 2025.

↓ 62%

53 Ransomware incidents

GROUP-IB

Most active threat actors

RansomHub

8 attacks
- 33%

Funksec

6 attacks
+ 50%

Termite

6 attacks
+ 500%

Play

4 attacks
(January at 0)

Cl0p

4 attacks
- 56%

Most targeted industries

IT

4 attacks
- 33%

Professional services: legal

4 attacks
+ 33%

Manufacturing

3 attacks
- 63%

Transportation: logistics

3 attacks
(January at 0)

Financial Services

2 attacks
- 100%

INITIAL ACCESS BROKER SALE ON DARK WEB

↑ 32%

120 Sales

GROUP-IB

The initial access to a company's system could potentially result in data theft, corporate espionage, or malware installed in the infrastructure for various other malicious purposes. The slide represent amount and geography of accesses to corporate infrastructure currently on sale in DarkWeb.

Key Event

Alleged Sarcoma operators were recruiting initial access brokers for long-term cooperation on underground forums.

Most targeted countries

LEAKED & SOLD CORPORATE CREDENTIALS

GROUP-IB

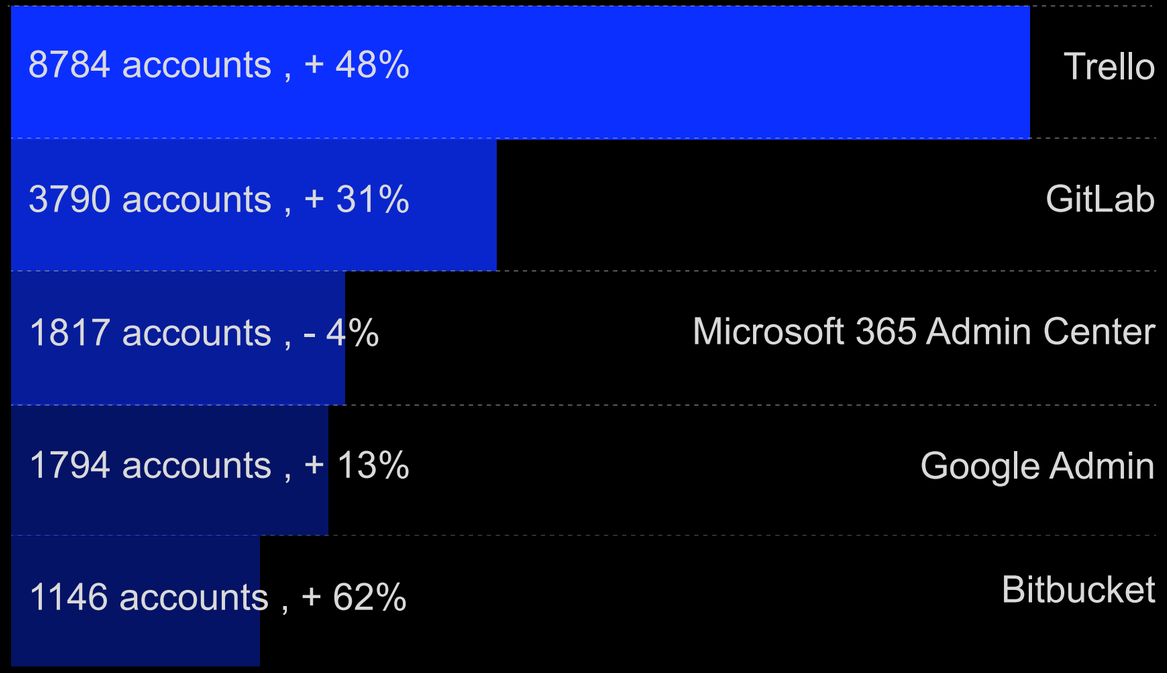
Key Events

- Most of detected compromised corporate accounts in the Europe belong to users from France, Italy and Spain.
- Based on statistics of compromised corporate accounts available for sale, the most popular source of credentials in February was Lumma Stealer.

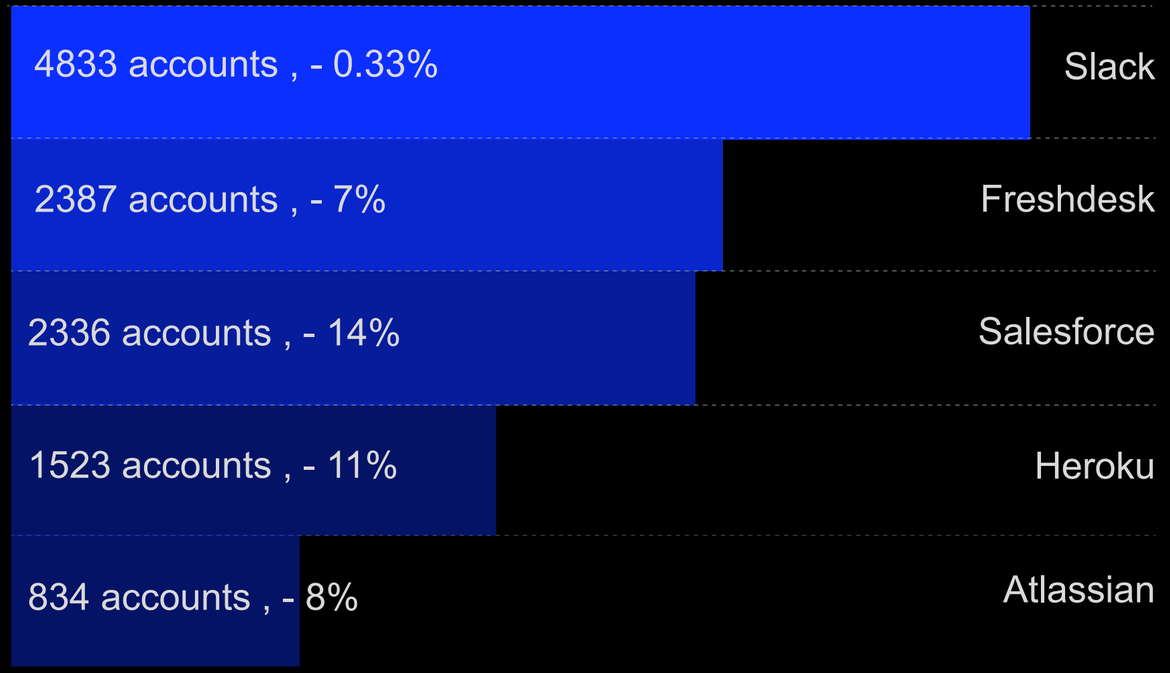
↑ 16%
Compromised account: 96,877

↓ 12%
on sale on dark web markets: 23,107

Services with the most compromised accounts

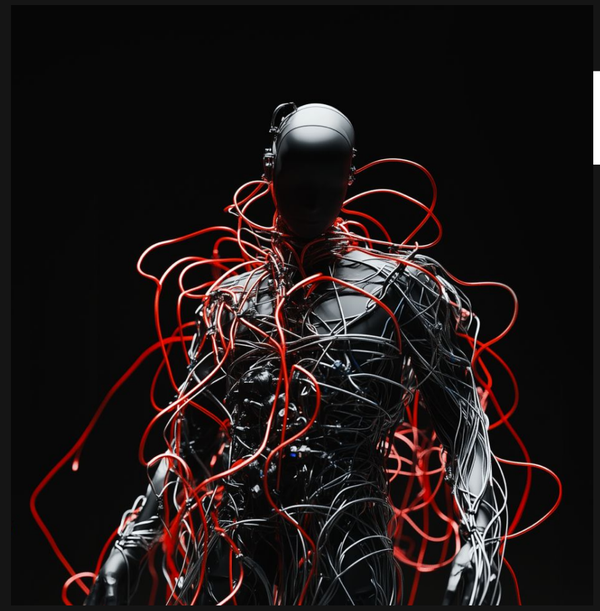


Services with the most on sale accounts



ADVERSARY OF THE MONTH

GROUP-IB



Threat actor group

RansomHub

Targeted industries:

- Agriculture
- Automotive
- Consumer Goods
- Education
- Financial services
- Food and Beverages
- Government
- Healthcare
- Hospitality
- Information Technology & Software
- Legal Services
- Logistics and Shipping
- Manufacturing
- Media & Entertainment
- Pharmaceutical
- Real Estate
- Retail and E-commerce
- Telecommunications

Period of Activity:	Feb 2024 - Present
Targeted countries:	Worldwide
Attribution:	Unknown
Intent:	Financially-motivated

Key Observations

- RansomHub’s operators strategically advertised the group’s partnership program on RAMP underground forum.
- RansomHub’s operators took advantage of the impact of law enforcement operations on LockBit and ALPHV to release a partnership program and recruit affiliates of these groups.
- The threat actors likely acquired the ransomware and web application source code from the Knight (aka Cyclops) group.
- Affiliates may eventually threaten and report cyber incidents to regulators such as PDPL (Personal Data Protection Law).

Read more in our recent blog.

STAY SMART. STAY CONNECTED. STAY SECURED

GROUP-IB

[Talk to our team]

RECENT RESOURCES

Read now

Read now

MEET US AT EVENTS