GROUP-IB

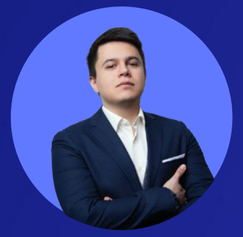
March, 2025

INTELLIGENCE INSIGHTS EUROPE

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

Key Insights

- Threat actor "rose87168" claims to have breached Oracle Cloud's login servers, exfiltrating six million records, including Java KeyStore files and encrypted SSO passwords, potentially affecting over 140,000 tenants.
- On March 30, 2025, an attacker with the nickname “CoreInjection” put up Check Point’s (an Israeli cybersecurity company) sale access and data.



ANTON USHAKOV
Head of Cyber Threat Intelligence

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.

THREAT LANDSCAPE

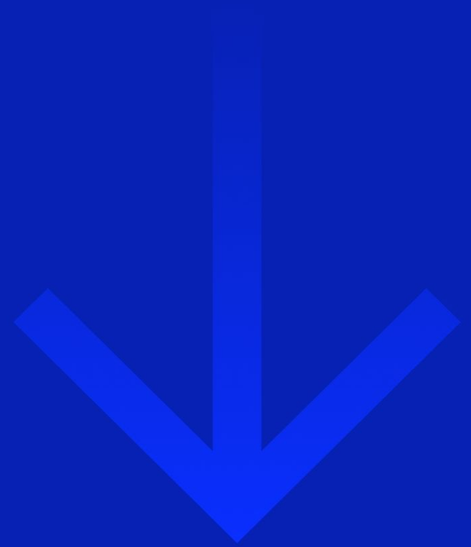
GROUP-IB

Month over Month Comparison
(February vs March)

88%

DDoS / Hacktivism attacks

4%



Ransomware attacks

20%

Initial access broker sale

15%

Leaked & sold credentials

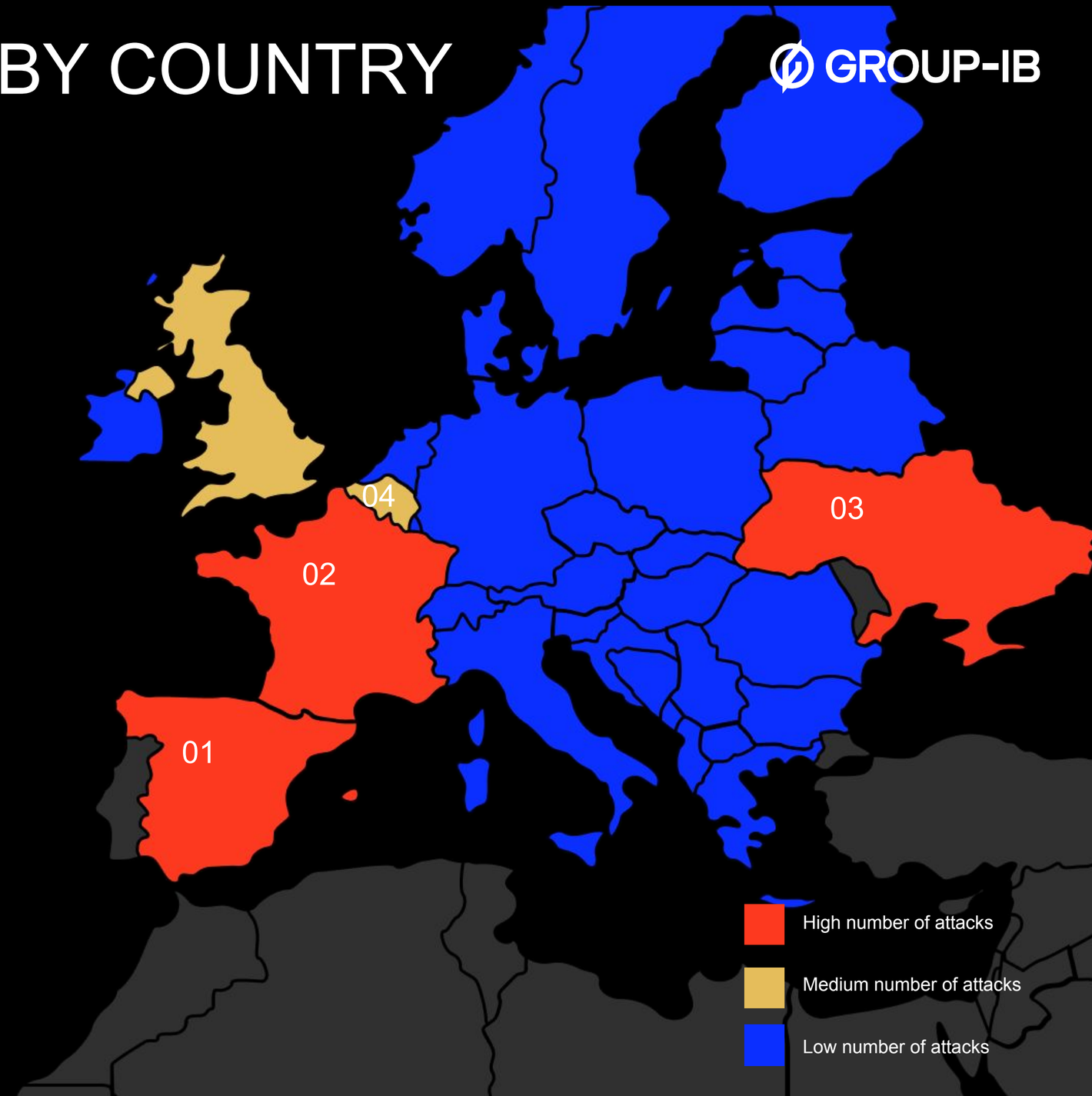
DDOS AND HACKTIVISM BY COUNTRY

Key Events

- Mr Hamza announced DDoS attack on Spanish Prime Minister's Office website.
- TwoNet announced DDoS attack on Indra, one of the leading global defence, aerospace and technology companies.
- Multiple hacktivist groups participated in OpSpain campaign targeting Spanish websites.

Most attacked countries

Spain	France	Ukraine	Belgium
72 attacks	30 attacks	26 attacks	11 attacks
+7100%	+131%	+117%	+267%



RANSOMWARE ACTIVITIES

GROUP-IB

Key Events

- Analysis of attacks claimed by BabukV2 group revealed that group reposts data previously leaked by other threat actors.
- 2025-03-24 Qilin ransomware added Derian House Childrens Hospice website as a victim to their DLS.
- 2025-03-09 Rhysida ransomware added Government Of The British Virgin Islands website as a victim to their DLS.

↓ 4%

93 Ransomware incidents

Most active threat actors

SafePay

14 attacks
+ 600%

Cl0p

10 attacks
+ 67%

Qlin

8 attacks
+ 300%

BabukV2

7 attacks
(February at 0)

Lynx

6 attacks
0%

Most targeted industries

Manufacturing

8 attacks
- 11%

IT

5 attacks
0%

Government and military

4 attacks
(February at 0)

Construction

3 attacks
+ 50%

Education

3 attacks
- 40%

INITIAL ACCESS BROKER SALE ON DARK WEB

↓ 20%

96 Sales

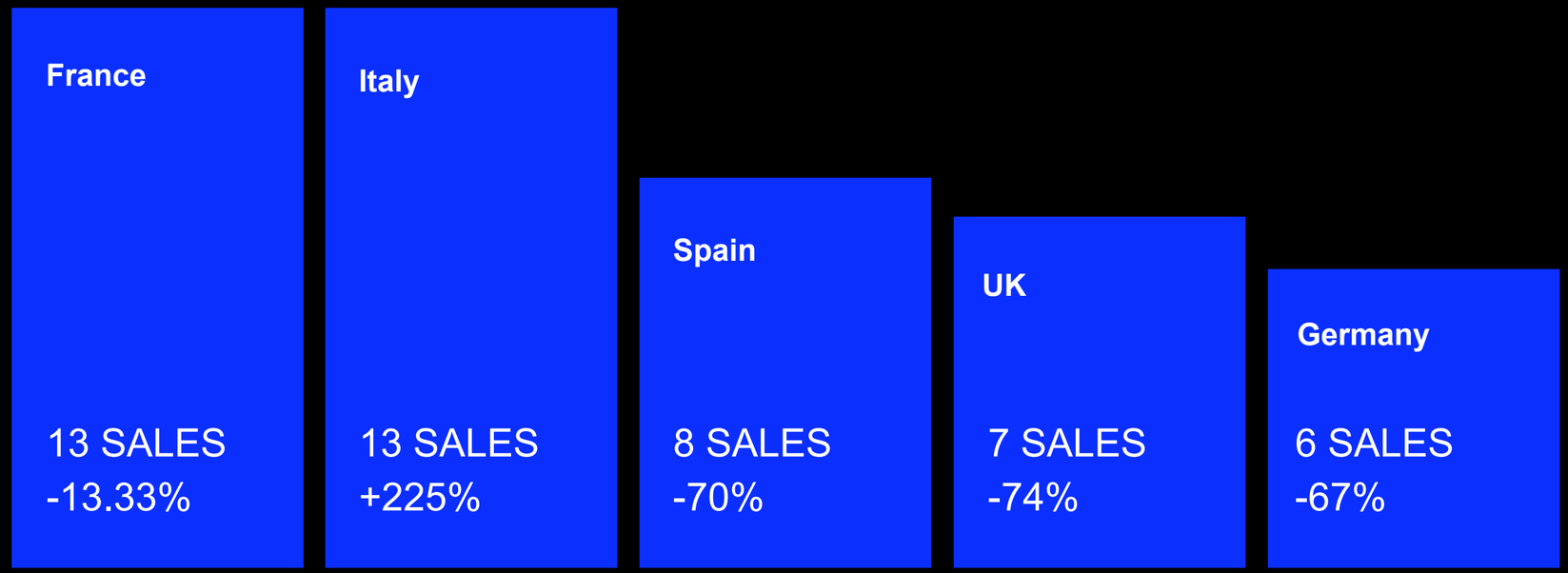
GROUP-IB

Initial access to a company's system can lead to data theft, corporate espionage, or the installation of malware for various malicious purposes. This page illustrates the volume and geographic distribution of corporate infrastructure accesses currently being sold on the dark web.

Key Event

On 2025-03-01 user DataSec posted thread on BreachForums claiming to be selling email access to government and law enforcement agencies from various countries.

Most targeted countries



LEAKED & SOLD CORPORATE CREDENTIALS

GROUP-IB

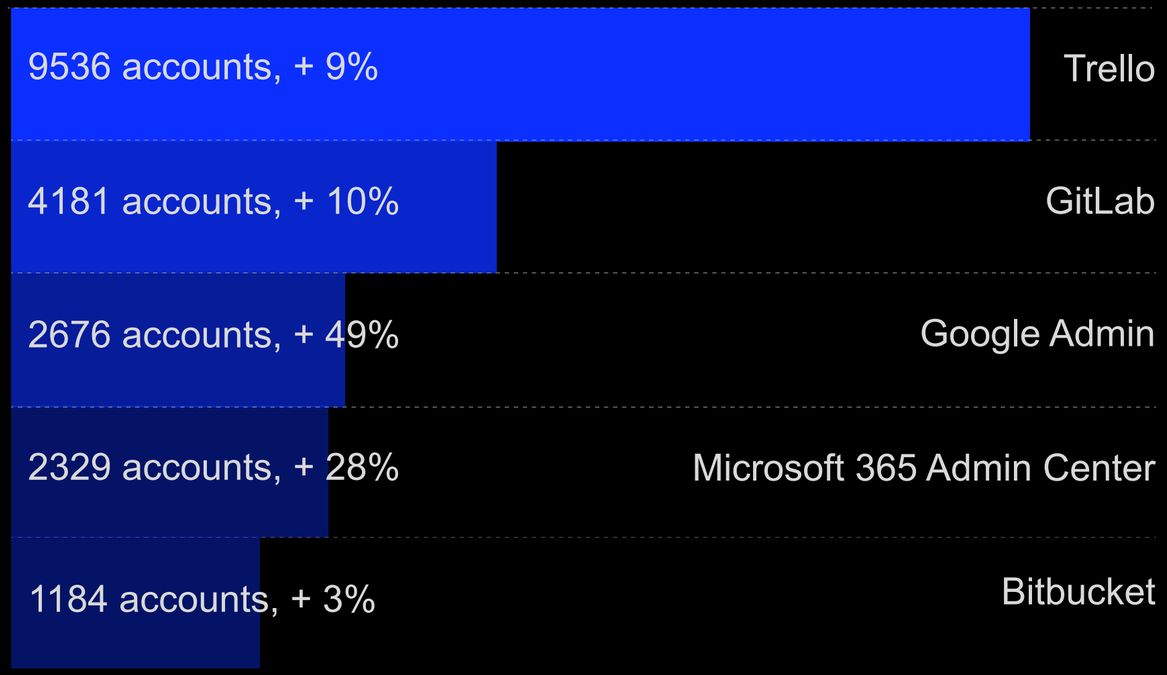
Key Events

- **Users from France, Italy and Spain** have most of the detected compromised corporate accounts in Europe.
- Based on statistics of compromised corporate accounts available for sale, the most popular source of credentials in March was **Lumma Stealer.**

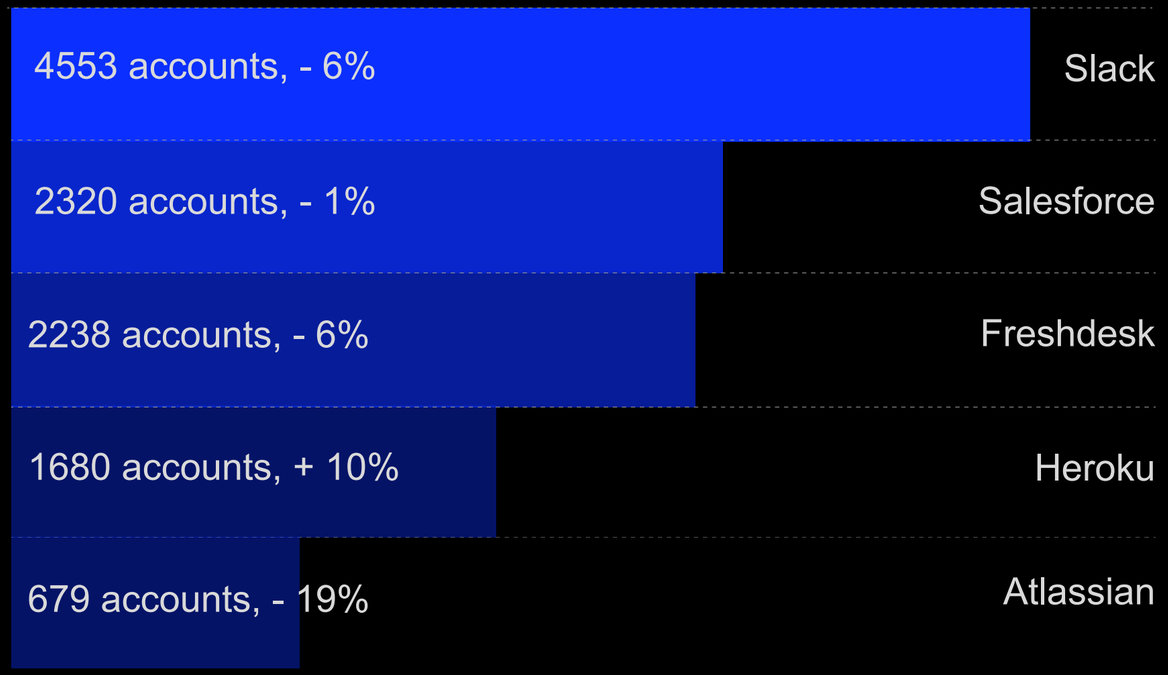
↑ 19%
Compromised account: 115,726

↑ 1%
on sale on dark web markets: 23,238

Services with the most compromised accounts



Services with the most on sale accounts

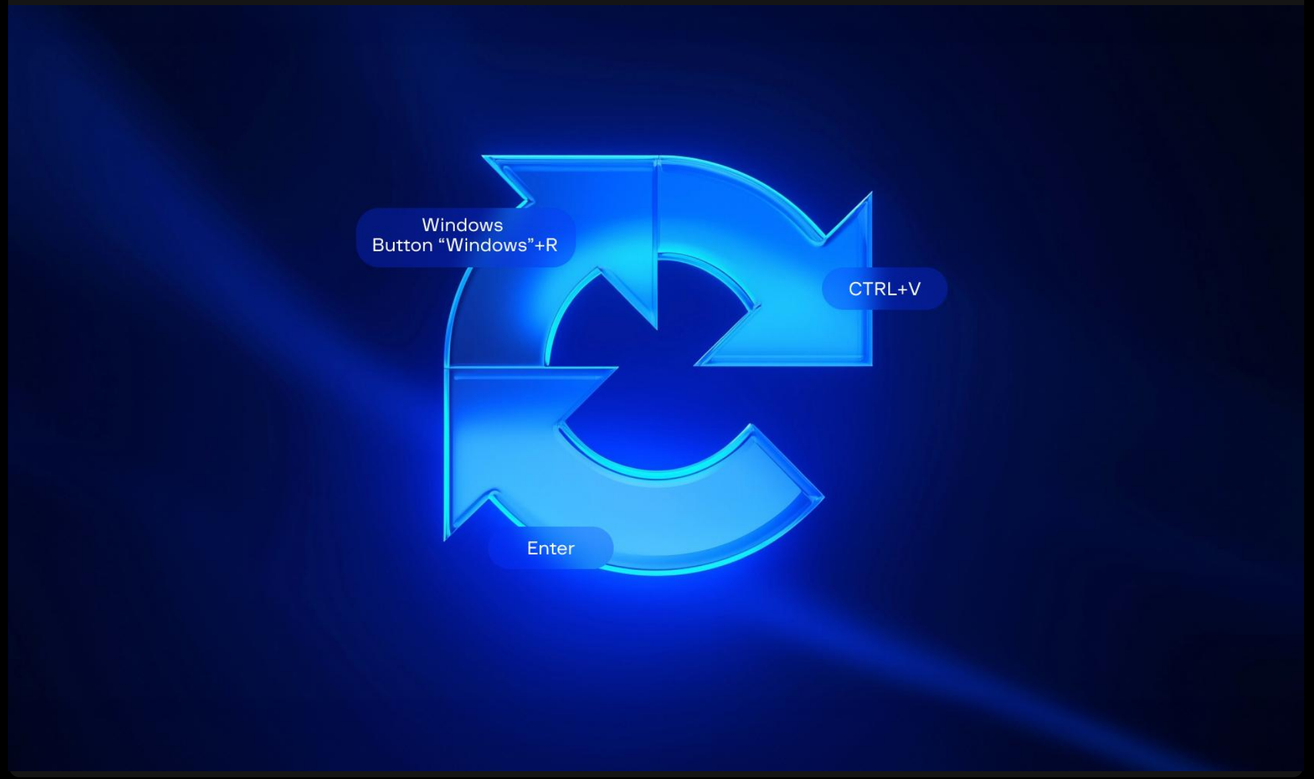


Adversary Technique Spotlight

GROUP-IB

Adversary Technique

ClickFix



Key Observations

- ClickFix manipulates users by presenting fake issues, prompting them to execute malicious commands under the guise of resolving non-existent problems. This approach effectively bypasses many automated security defenses by leveraging human behavior.
- Since its emergence in October 2023, ClickFix has seen widespread adoption among cybercriminals and APT groups.
- Attackers frequently use fake reCAPTCHA pages and bot protection prompts to disguise ClickFix. The Lumma infostealer has been the most commonly distributed malware in these campaigns.

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