GROUP-IB

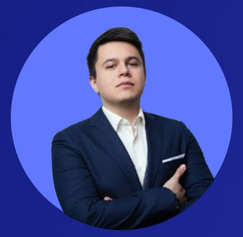
April, 2025

INTELLIGENCE INSIGHTS EUROPE

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

Key Insights

- Group-IB specialists detected threat actor Machine1337 selling stolen SMS messages on underground forums. The data was allegedly exfiltrated from the admin panel of an unknown SMS provider.
- Most of the detected compromised corporate accounts in Europe in April belong to users from Poland, France, Italy, Spain and Germany.
- Activities associated with the newly identified threat actor, J Group, have been detected: victims were found through their data leak sites (DLS), along with ransom notes and encrypted files bearing the '.J' extension.



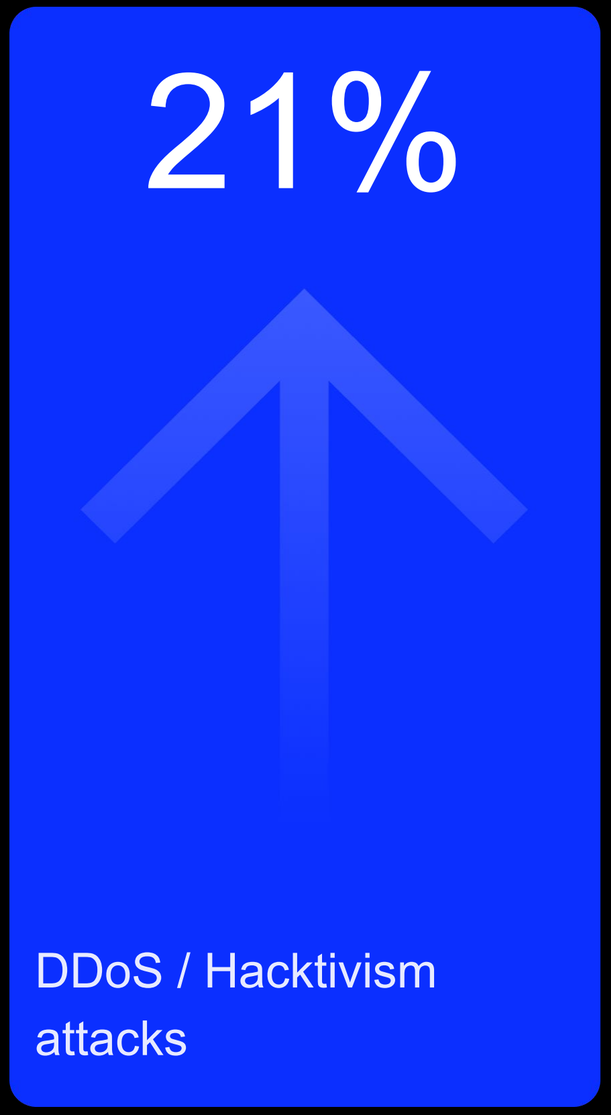
ANTON USHAKOV
Head of Cyber Threat Intelligence

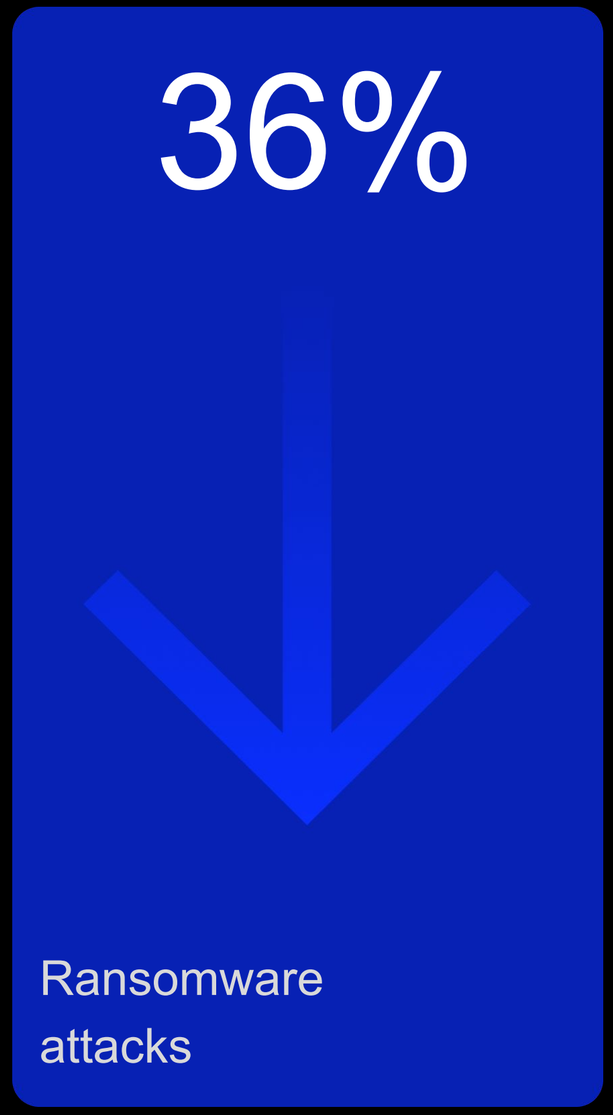
This report offers an overview of the latest threat landscape in Europe, covering key developments such as ransomware attacks, leaked credentials, data breaches, and more. It includes a month-over-month trend analysis to track evolving patterns. Additionally, the report spotlights a newly identified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

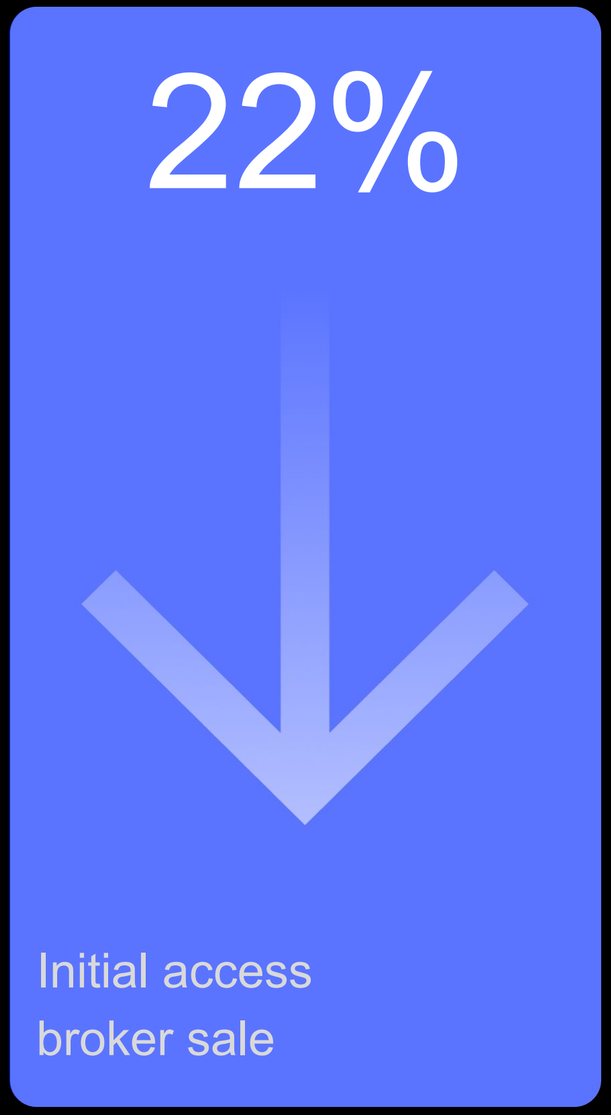
THREAT LANDSCAPE

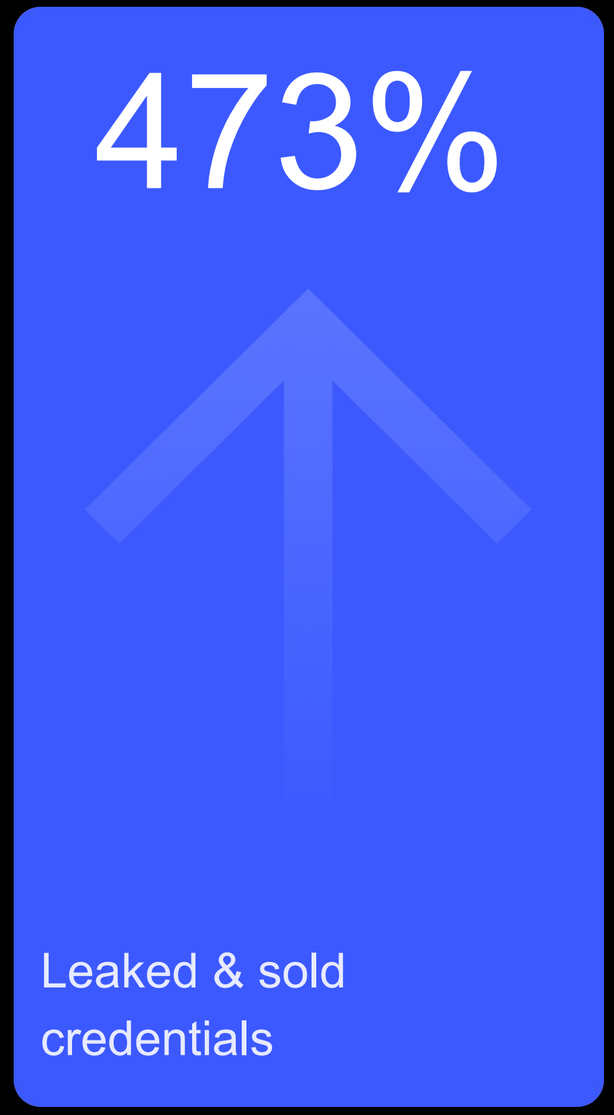
GROUP-IB

Month over Month Comparison
(March VS April)









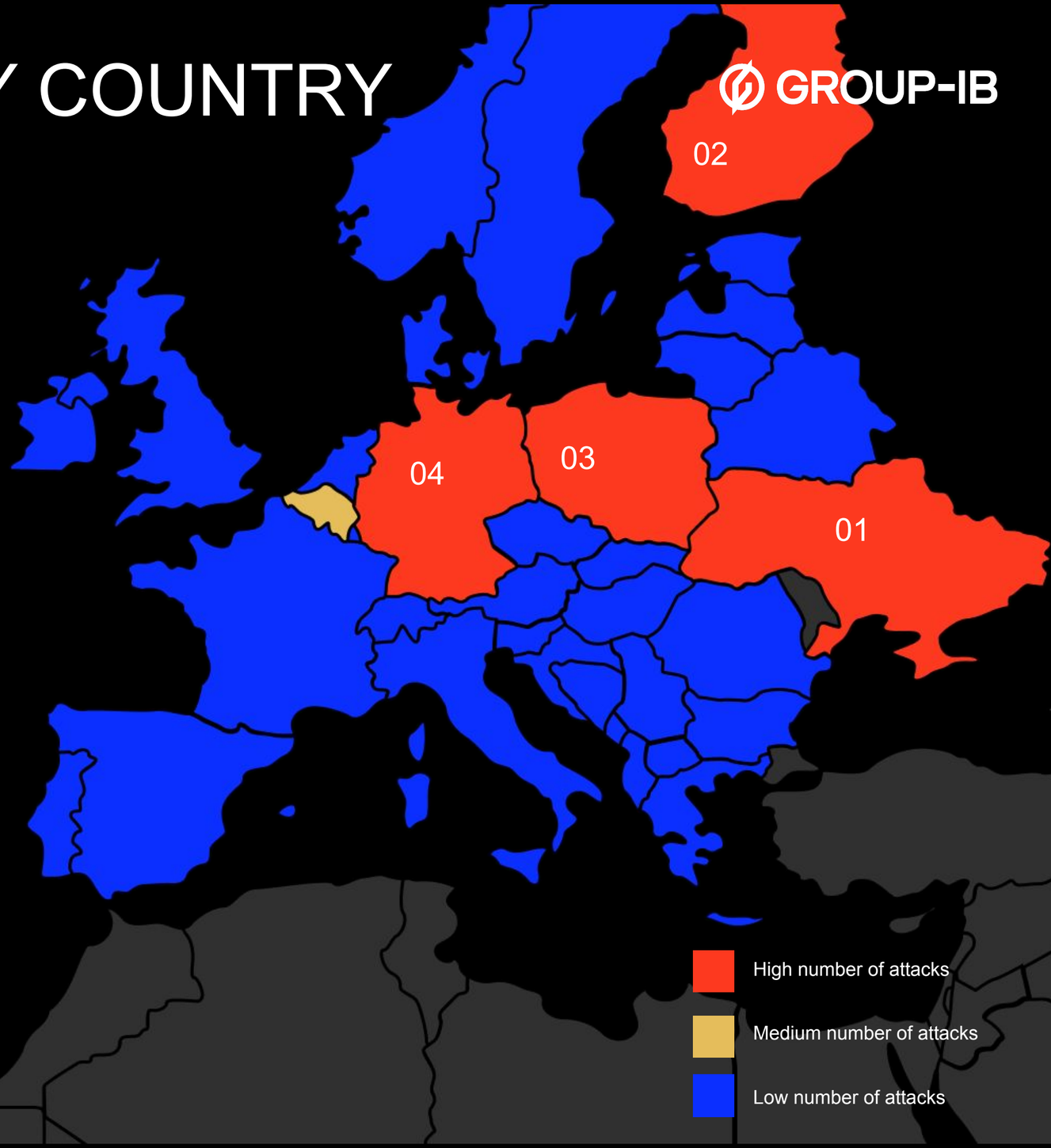
DDOS AND HACKTIVISM BY COUNTRY

Key Events

- In April 2025 AnonSec, NoName057(16), DarkStormTeam participated in attacks targeting government organizations in Finland including websites of political parties, cities and municipalities, ministries, Helsinki Regional Transport Authority and airports.
- Threat actors NoName057(16), DarkStormTeam and Inteid attacked multiple government websites in Germany including websites of the president, ministries and cities.
- In April, Group-IB specialists detected 43 DDoS-related incidents targeting financial organizations, including attacks on the Co-operative Bank and Bunq.

Most attacked countries

Ukraine	Finland	Poland	Germany
60 attacks	41 attacks	41 attacks	32 attacks
+122%	March at 0	March at 0	+1500%



RANSOMWARE ACTIVITIES

Key Events

- Activities associated with the newly identified threat actor, J Group, have been detected: victims were found through their data leak sites (DLS), along with ransom notes and encrypted files bearing the '.J' extension.
- 2025-04-17: Sarcoma Ransomware group added Manchester Credit Union website as a victim to their DLS.

↓ 36%

114 Ransomware incidents

GROUP-IB

Most active threat actors

Akira

20 attacks
0%

Qilin

18 attacks
+ 38%

SafePay

11 attacks
- 35%

Sarcoma

8 attacks
+ 300%

Hunters International

6 attacks
(March at 0)

Most targeted industries

Manufacturing

7 attacks
- 61%

Transportation

7 attacks
+ 133%

Real Estate

5 attacks
+ 25%

Machinery Manufacturing

5 attacks
+ 25%

Software

5 attacks
- 17%

INITIAL ACCESS BROKER SALE ON DARK WEB

↓ 22%

75 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

Group-IB specialists detected threat actor **Machine1337** selling stolen SMS messages on underground forums. The data was allegedly exfiltrated from the admin panel of an unknown SMS provider.

Most targeted countries

LEAKED & SOLD CORPORATE CREDENTIALS

GROUP-IB

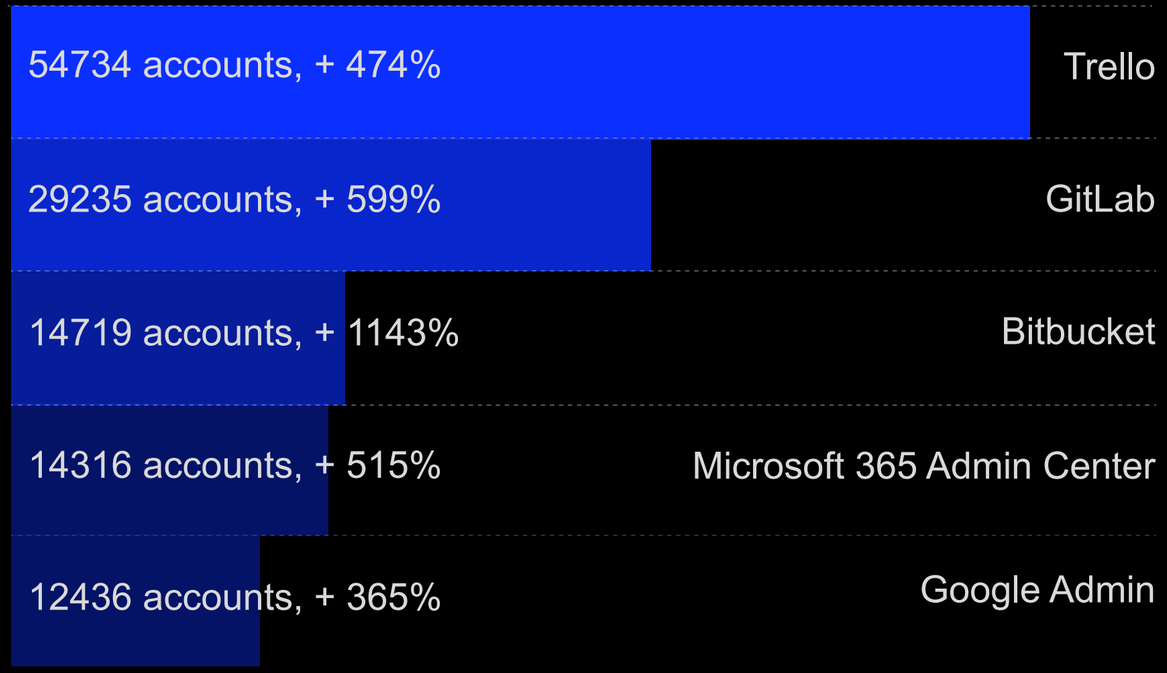
Key Events

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

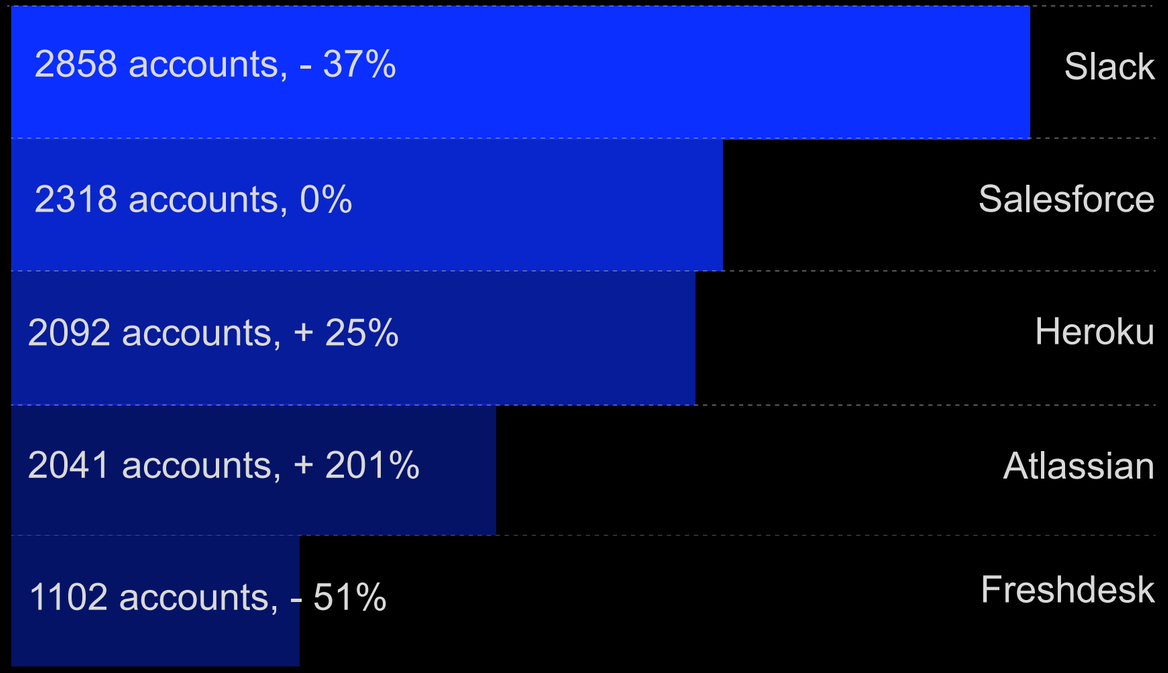
↑ 577%
Compromised account: 783,079

↓ 41%
on sale on dark web markets: 13,606

Services with the most compromised accounts



Services with the most on sale accounts



ADVERSARY OF THE MONTH

GROUP-IB

Threat actor group

Hunters International

Targeted industries:

Real estate

Healthcare

Professional services

Period of Activity:	October, 2023
Targeted countries:	Europe, North America and Asia
Languages:	Russian, English
Intent:	Data exfiltration

Key Observations

- The Hunters International operation was possibly launched in October 2023. Former Hive's operators may have been involved in the Hunters International's administration.
- The group provides its partners with an open source intelligence (OSINT) service with the purpose of extorting victims via telephone calls, emails and social media and other means.
- Hunters International provides a tool named Storage Software, which collects metadata of exfiltrated files and sends information about the files—not the files themselves—to the group's system in order to be presented to the victims as well as to disclose it in the DLS. The tool creates a bridge between the host with the victim's data controlled by the author of the attack, and Hunters International's panels. Once the ransom is paid, the victim is granted access to the Disclosures configured by the criminal, and the victim is able to download and delete the files stored by the criminal from the group's victim panel. The Storage Software establishes network connection via SOCKSv5 proxy, and works on both Windows and Linux.

STAY SMART. STAY CONNECTED. STAY SECURED

GROUP-IB

[Talk to our team]

RECENT RESOURCES

Read now

Listen now

MEET US AT EVENTS