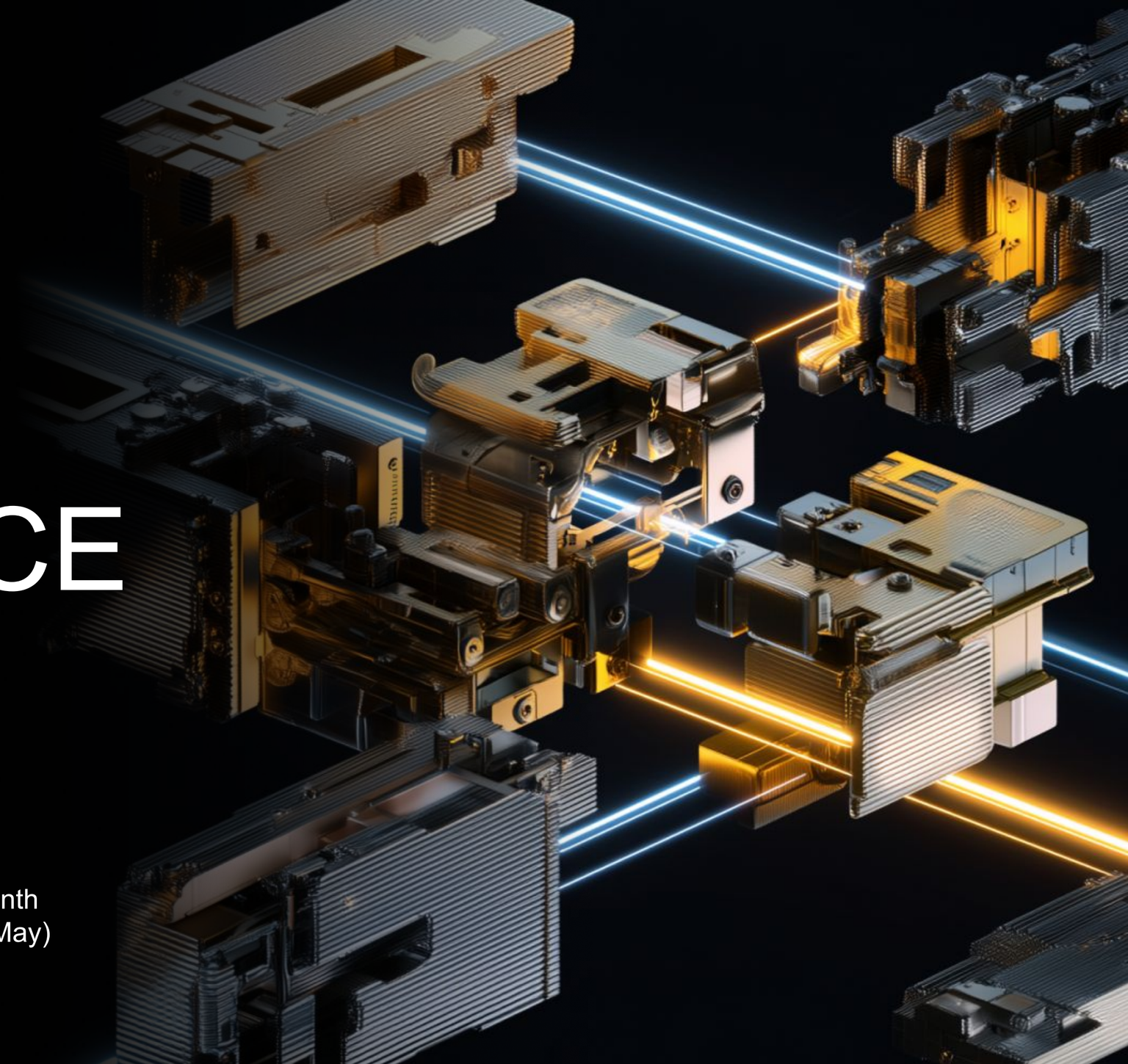
GROUP-IB

June, 2025

INTELLIGENCE INSIGHTS EUROPE

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



Key Insights

- Most of detected compromised corporate accounts in Europe detected in May belong to users from Spain, France, Italy, Poland and the United Kingdom.
- 240 times increase in number of corporate credentials compromised with "acreed" malware and offered for sale on Russian Market.
- IMN Crew ransomware added Croatian Monetary Institute as a victim to group's Dedicated Leak Sites (DLS).
- Group-IB specialists detected multiple campaigns performed by hacktivists groups targeting EU countries, with the most active in May were: OpLithuania, OpPoland, OpFrance.

Val Shirko
Regional Business Head, Europe

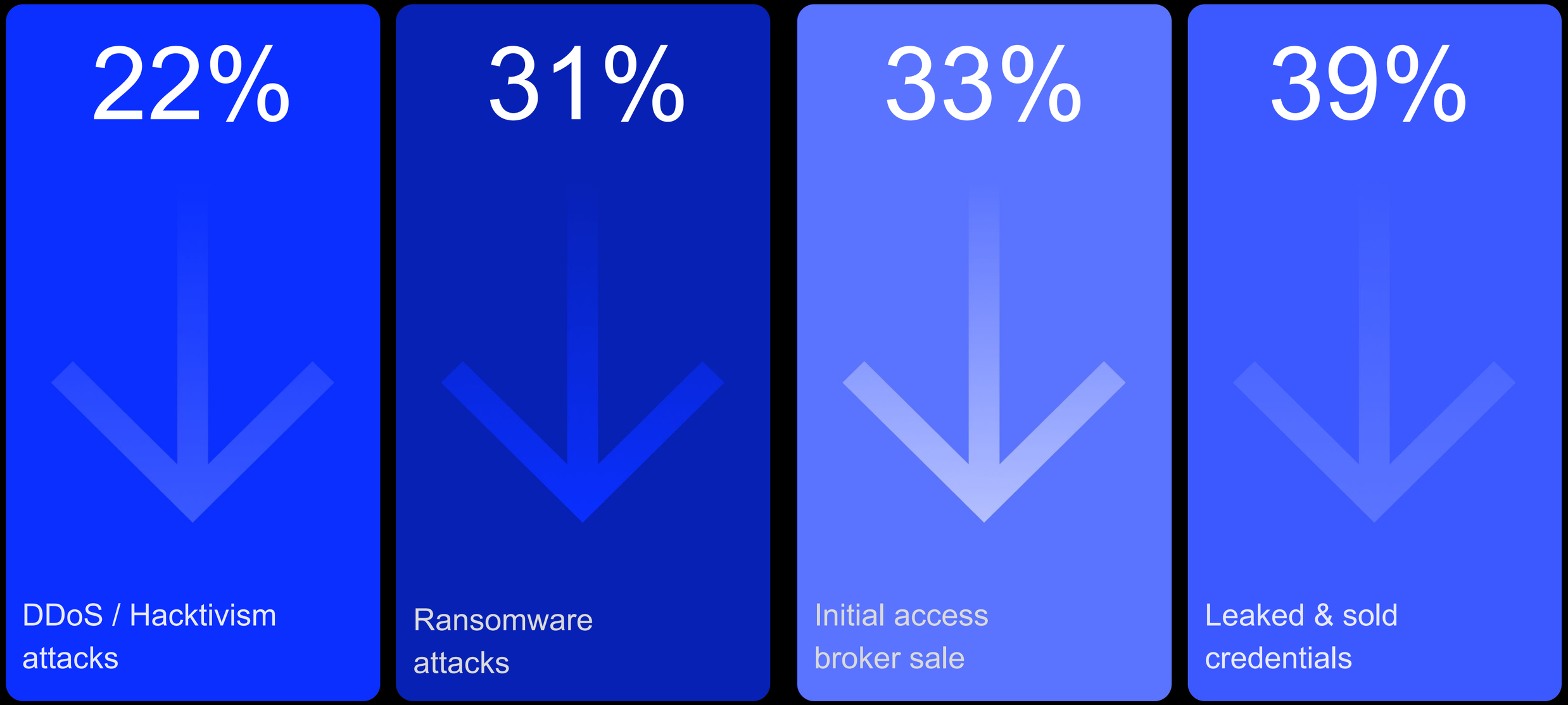
This report offers an overview of the latest threat landscape in Europe, covering key developments such as ransomware attacks, leaked credentials, data breaches, and more. It includes a month-over-month trend analysis to track evolving patterns. Additionally, the report spotlights a newly identified 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
(April VS May)



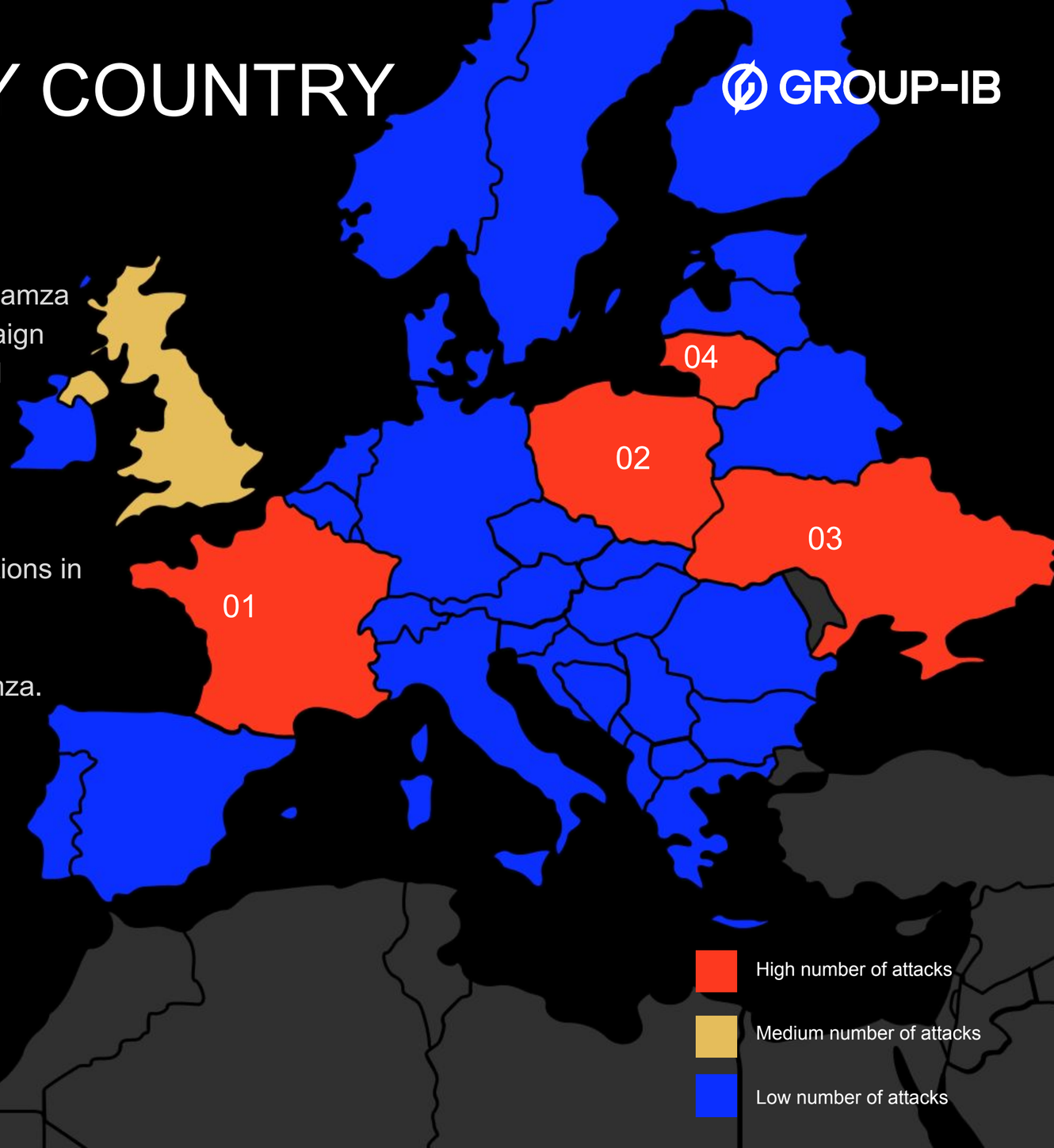
DDOS AND HACKTIVISM BY COUNTRY

Key Events

- Multiple hacktivists groups including NoName057(16), Z-Pentest, Mr Hamza and DarkStormTeam participated in Op_Lithuania / OpLithuania campaign and announced DDoS attacks on various Lithuanian organizations and government agencies.
- Inteid, NoName057(16) and Z-Pentest participated in #Op_poland / #Oppoland campaign targeting Polish companies and government.
- Another DDoS campaign conducted against one of EU countries was OpFrance, targeting websites of companies and government organizations in France.
- Group-IB Threat Intelligence team detected attacks announced by NoName057(16), DarkStormTeam, Keymous, BL4CK CYB3R, Mr Hamza.

Most attacked countries

France	Poland	Ukraine	Lithuania
36 attacks	31 attacks	30 attacks	26 attacks
+260%	- 24%	- 50%	April at 0



RANSOMWARE ACTIVITIES

Key Events

- Rhysida ransomware released new leaked data related to Government of the British Virgin Islands London Office.
- IMN Crew ransomware added Croatian Monetary Institute as a victim to group's dedicated Leak Sites (DLS).
- DataCarry ransomware added Executive Jet Support as a victim to the group's DLS.

↓ 31%

87 Ransomware incidents

GROUP-IB

Most active threat actors

SafePay

24 attacks
+ 118%

Qilin

9 attacks
- 50%

Akira

6 attacks
- 71%

INC Blog

6 attacks
0%

World Leaks

4 attacks
(April at 0)

Most targeted industries

Construction

9 attacks
+ 50%

Software & IT

4 attacks
- 33%

Consumer goods

3 attacks
+ 200%

Insurance

3 attacks
+ 200%

Government

2 attacks
0%

INITIAL ACCESS BROKER SALE ON DARK WEB

↓ 33%

50 Sales

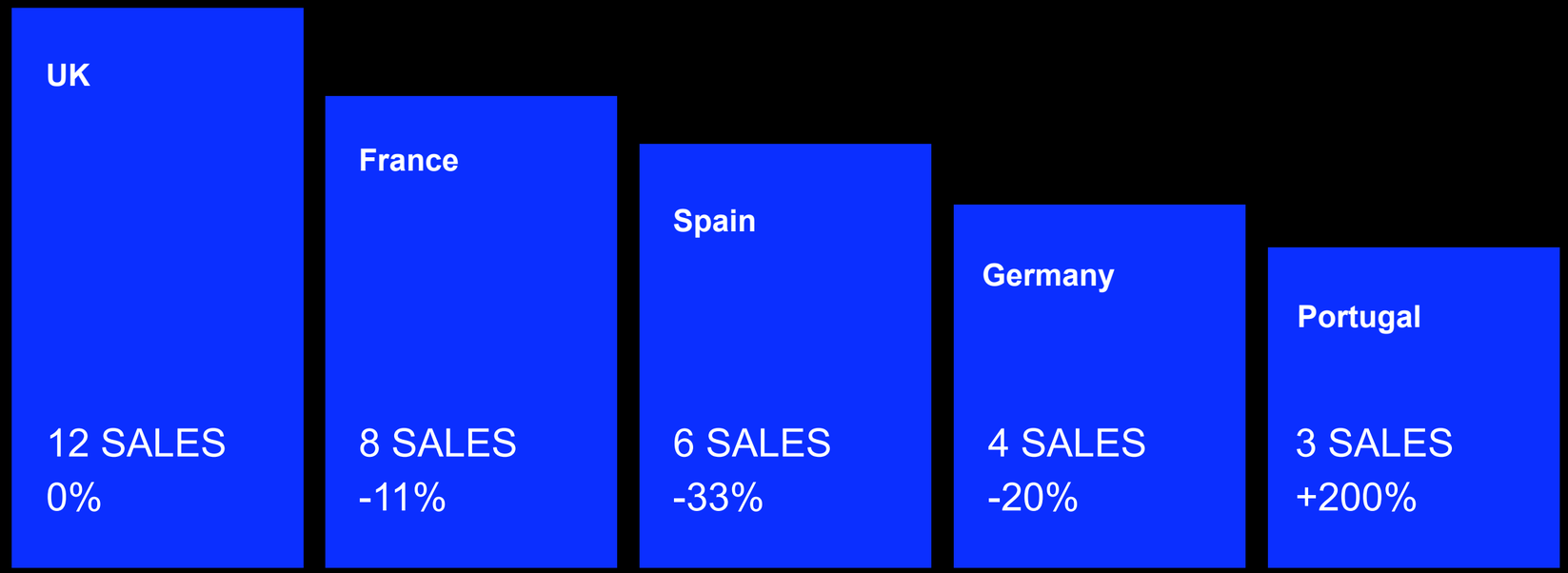
GROUP-IB

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 are tracking the activities of the threat actor – Machine1337 who created multiple threads on underground forums for selling SMS messages.
In May, Machine1337 continued to post new batches of stolen messages for sale related to various popular online services as well as an offer for real-time access to the feeds.

Most targeted countries



LEAKED & SOLD CORPORATE CREDENTIALS

GROUP-IB

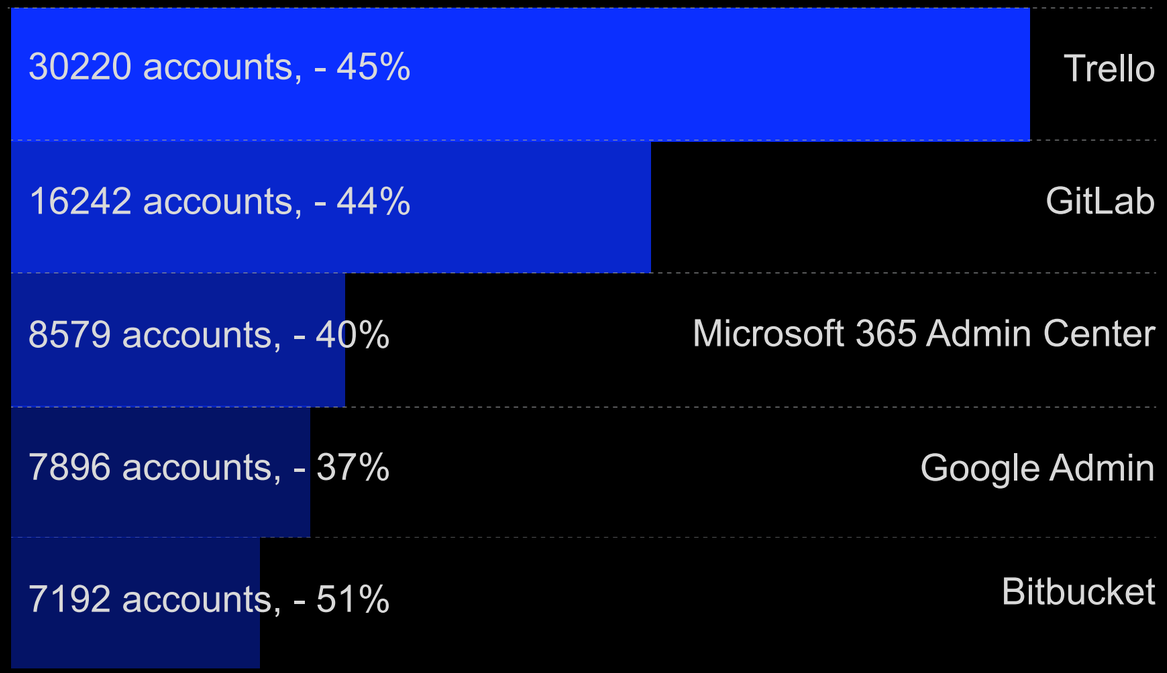
Key Events

- Most of the compromised corporate accounts in Europe detected in May belong to users from Spain, France, Italy, Poland and the United Kingdom.
- Number of corporate credentials compromised with **"acreed"** malware and offered for sale on **Russian Market** increased significantly by more than 240 times in May.

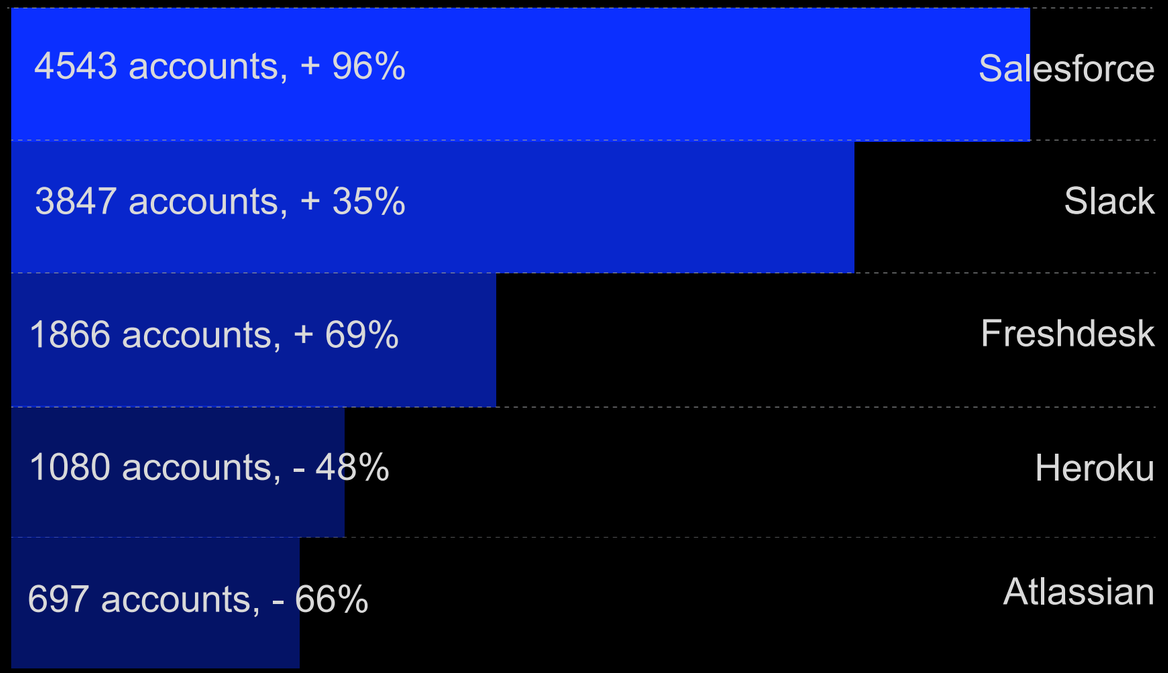
↓ 41%
Compromised account: 460,992

↑ 66%
on sale on dark web markets: 22,563

Services with the most compromised accounts

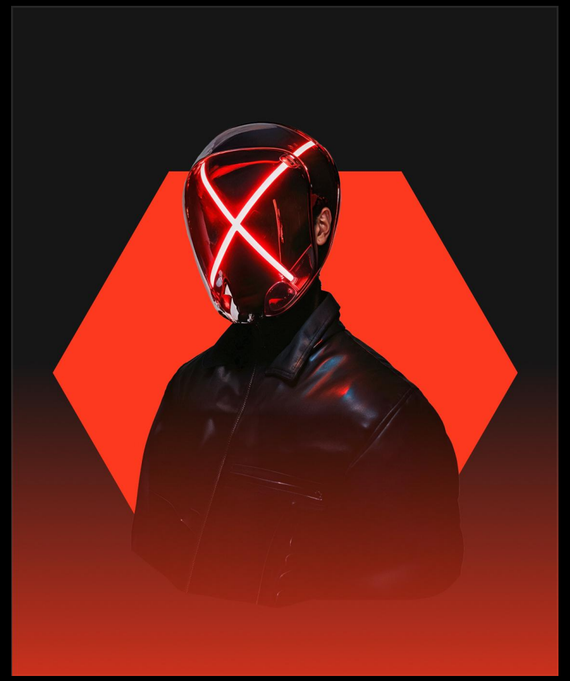


Services with the most on sale accounts



ADVERSARY OF THE MONTH

GROUP-IB



Threat actor group

Devman

(Alias: brokeasf/inifintyink/sozdatellab)

Targeted industries:

Manufacturing	Government and Military
Construction	Telecommunications
Health care	Hospital
Information technology	Pharmaceutical
Human resources services	Media and entertainment
E-commerce	Environmental consulting
Financial services	Transportation
Consumer Goods	

First seen	03 April 2025
Targeted countries:	Worldwide (in Europe: Spain, Italy and France)
Languages:	Russian, English
Intent:	Financially motivated

Key Observations

- The threat actor exploits the EternalBlue vulnerability using Metasploit's msfconsole to gain access and escalate privileges within the victim’s environment.
- Leveraging valid credentials and Mimikatz for credential dumping, the actor ensured persistent access and deeper infiltration into the network.
- The actor used PowerShell and custom scripts for automated file collection, followed by data exfiltration to file storage services via web services, and GPO modification to support the operation.

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

STAY SMART. STAY CONNECTED. STAY SECURED

GROUP-IB

[Talk to our team]

RECENT
RESOURCES

Read now

Listen now

MEET US AT
EVENTS