July, 2025

INTELLIGENCE INSIGHTS EUROPE

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

Key Insights

- Group-IB uncovered a phishing campaign called “Declaration Trap” targeting European **crypto holders** by impersonating tax authorities like the Dutch Belastingdienst. Fraudulent emails urge victims to submit a fake crypto declaration, leading them to fake portals that steal wallet seed phrases or drain funds via WalletConnect.
- Group-IB team detected phishing campaign targeting apparel, retail and luxury goods companies in France, Switzerland and the USA from cybercrime activity cluster attributed to **Scattered Spider.**
- Group-IB team identified the BuzzToll phishing campaign, attributed to the threat actor **PendingLocust,** which began in April 2024 and remained active as of June 2025. PendingLocust’s main objective is to harvest login credentials and credit card information.
- In June 2025 Group-IB experts discovered four **new ransomware groups**: KaWaLocker, Nemesis, WALocker, Team XXX.

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

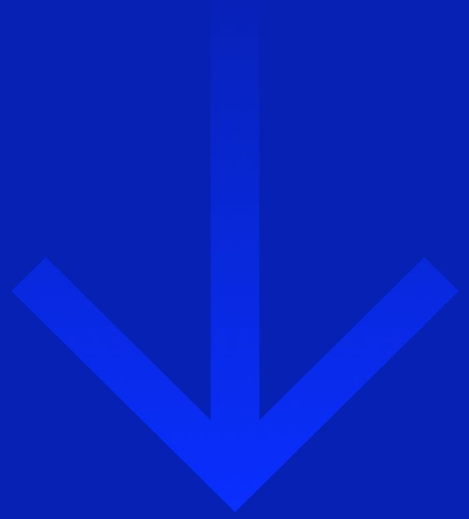
GROUP-IB

Month over Month Comparison
(May vs June)

54%

DDoS / Hacktivism attacks

40%



Ransomware attacks

4%

Initial access broker sale

220%

Leaked & sold credentials

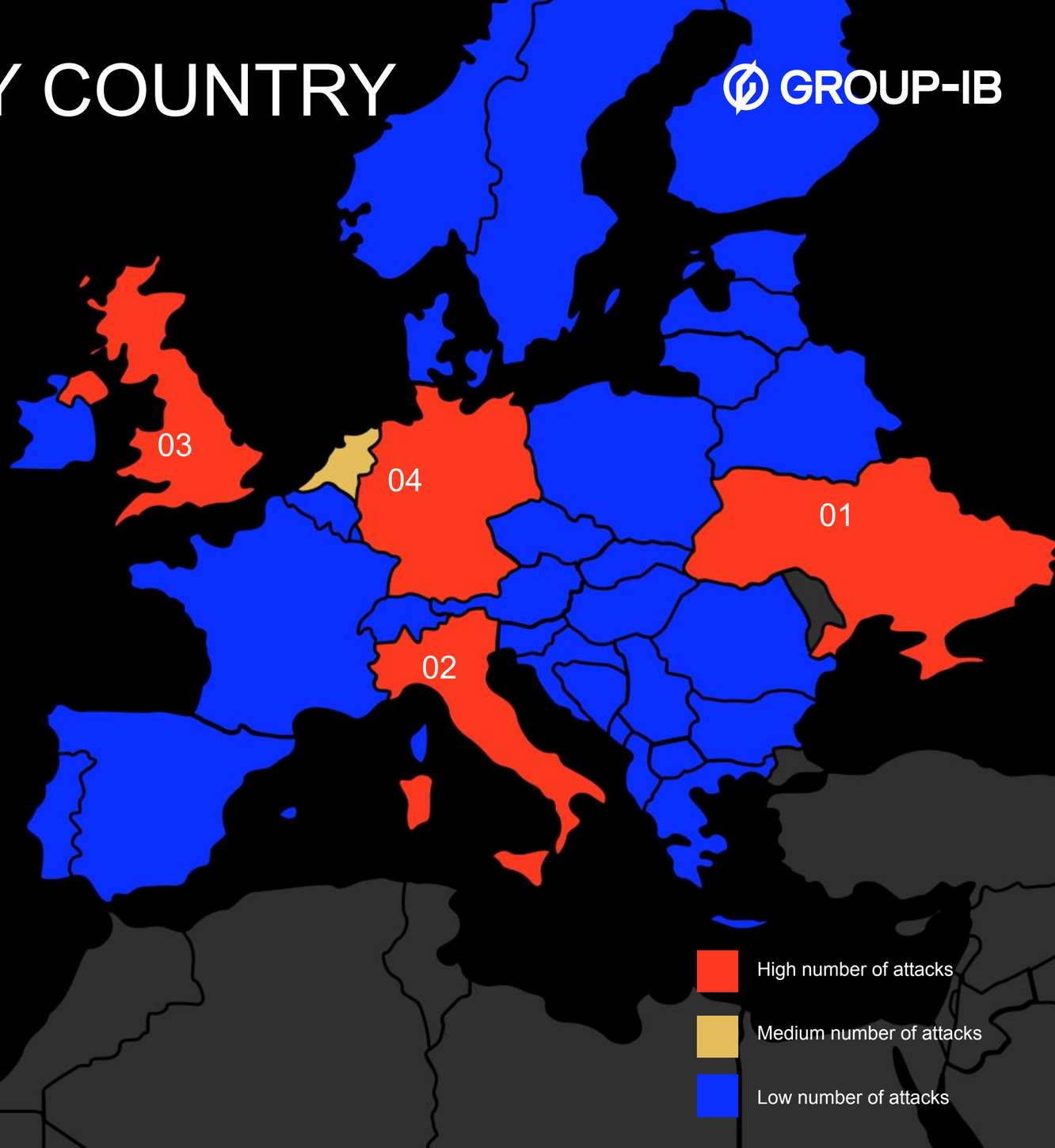
DDOS AND HACKTIVISM BY COUNTRY

Key Events

- NoName057(16) claimed responsibility for DDoS attacks targeting government entities in Italy, Ukraine, Netherlands, Belgium, Lithuania.
- DarkStormTeam announced DDoS attacks targeting companies and government organizations in United Kingdom, Italy, Switzerland, Germany, Spain, France, Portugal and Ukraine.
- Mr Hamza announced attacks targeting organizations in Germany, Albania, France, United Kingdom.

Most attacked countries

Ukraine	Italy	UK	Germany
37 attacks	24 attacks	12 attacks	11 attacks
+ 23%	+ 700%	- 40%	+ 83%



RANSOMWARE ACTIVITIES

GROUP-IB

Key Events

- Dire Wolf Ransomware added EPC Group - a German engineering and construction company - as a victim to group's DLS.
- INC Ransomware added Clinique Alleray Labrouste as a victim to group's DLS.
- Rhysida Ransomware added Coreix Cloud Services Limited - a managed hosting, colocation and network services provider - as a victim to group's DLS.
- In June 2025 Group-IB experts discovered four new ransomware groups: KaWaLocker, Nemesis, WALocker, Team XXX.

↓ 40%

78 Ransomware incidents

Most active threat actors

Qilin

24 attacks
+ 140%

Akira

8 attacks
- 50%

Sarcoma

5 attacks
- 67%

Global

5 attacks
(May at 0)

Payouts King Group

5 attacks
(May at 0)

Most targeted industries

Manufacturing

8 attacks
+ 60%

Real estate: construction

6 attacks
- 14%

Retail

3 attacks
+ 50%

Chemical

2 attacks
0%

Insurance

2 attacks
- 50%

INITIAL ACCESS BROKER SALE ON DARK WEB

↓ 4%

48 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 team detected phishing campaign targeting apparel, retail and luxury goods companies in France, Switzerland and the USA from cybercrime activity cluster attributed to Scattered Spider.

Most targeted countries

LEAKED & SOLD CORPORATE CREDENTIALS

GROUP-IB

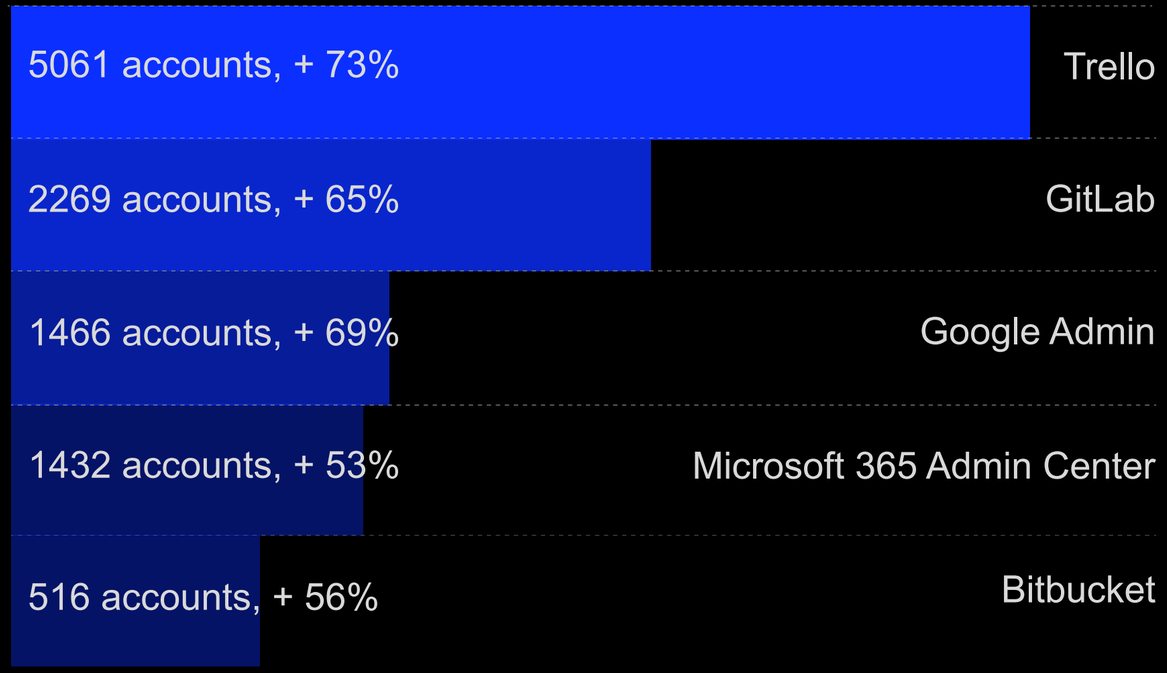
Key Events

- Group-IB team identified the BuzzToll phishing campaign, attributed to the threat actor PendingLocust, which began in April 2024 and remained active as of June 2025. PendingLocust's main objective is to harvest login credentials and credit card information.

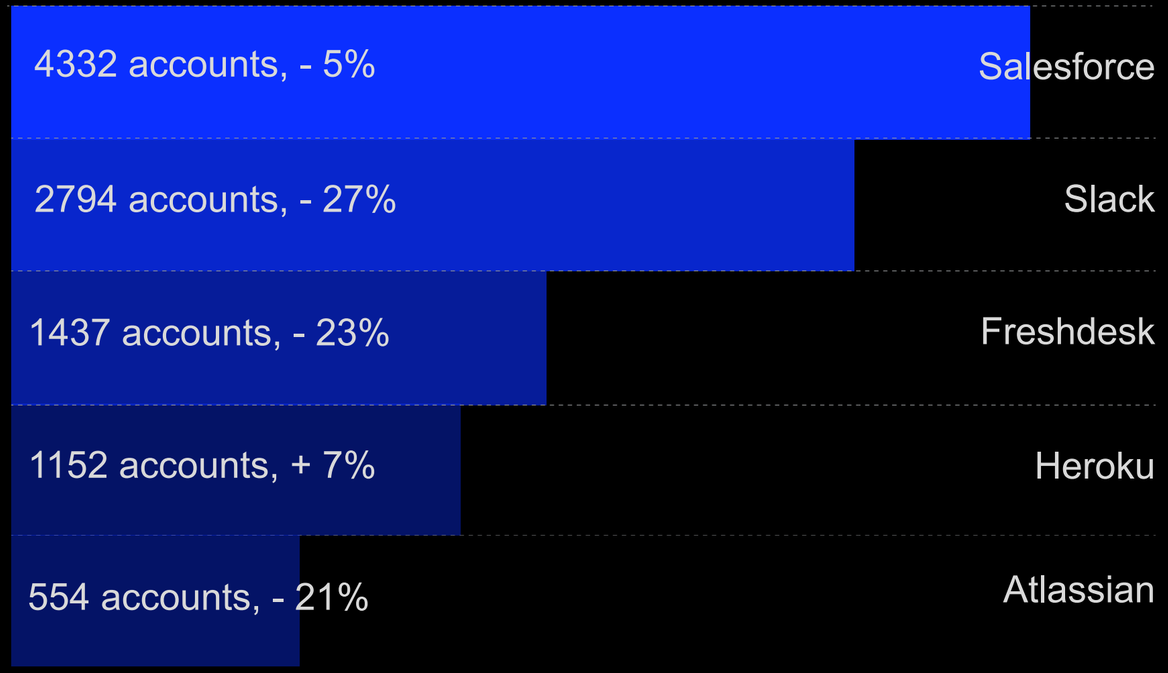
↑ 232%
Compromised account: 1,496,290

↓ 24%
on sale on dark web markets: 17,205

Services with the most compromised accounts



Services with the most on sale accounts



Scam Spotlight

GROUP-IB

Scam case

Crypto Drainers masquerading as European Tax Authorities

Key Observations

- Attackers impersonate European tax authorities like Belastingdienst(Dutch Tax Authority) to target crypto holders.
- Victims are lured via emails demanding urgent crypto tax declarations.
- The phishing websites mimic official government portals using authentic design and branding.
- Two attack paths: seed phrase theft or wallet draining via malicious smart contract transactions.

Read more in our recent blog.

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

STAY SMART. STAY CONNECTED. STAY SECURED

[Talk to our team]

RECENT RESOURCES

Read now

Read Now

MEET US AT EVENTS