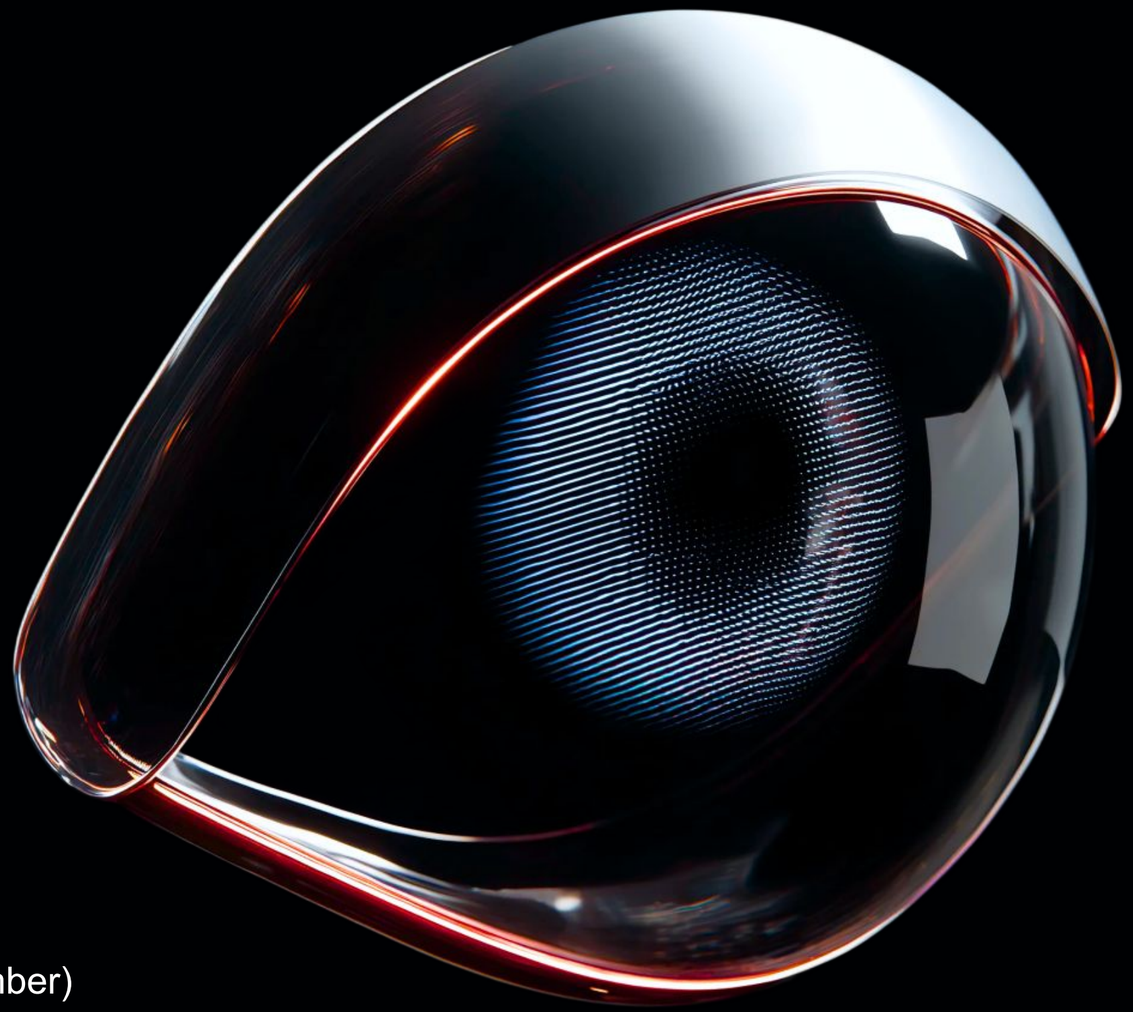
GROUP-IB

Oct, 2025

INTELLIGENCE INSIGHTS EUROPE



Defend against what’s ahead by uncovering month-over-month trends and insights into Europe’s threat landscape (August – September)

Key insights

- On September 26, 2025, the ransomware group Payouts King Group leaked corporate data belonging to Creditinfo Group, a leading provider of credit information and risk management solutions.
- The highest-revenue company listed by Initial Access Brokers was a Serbian firm in the marine shipping and transportation sector, with $206 million in annual revenue.
- Threat actor Hezi Rash claimed responsibility for DDoS attacks targeting four German health-related organizations: the National Association of Statutory Health Insurance Physicians, Hartmannbund; the Association of Physicians of Germany, Virchowbund; the Association of Practicing Physicians of Germany; and the German Society for Hygiene and Microbiology.
- The most active adversary-in-the-middle phishing framework in September was Tycoon 2FA.

Val Shirko
Regional Business Head, Europe

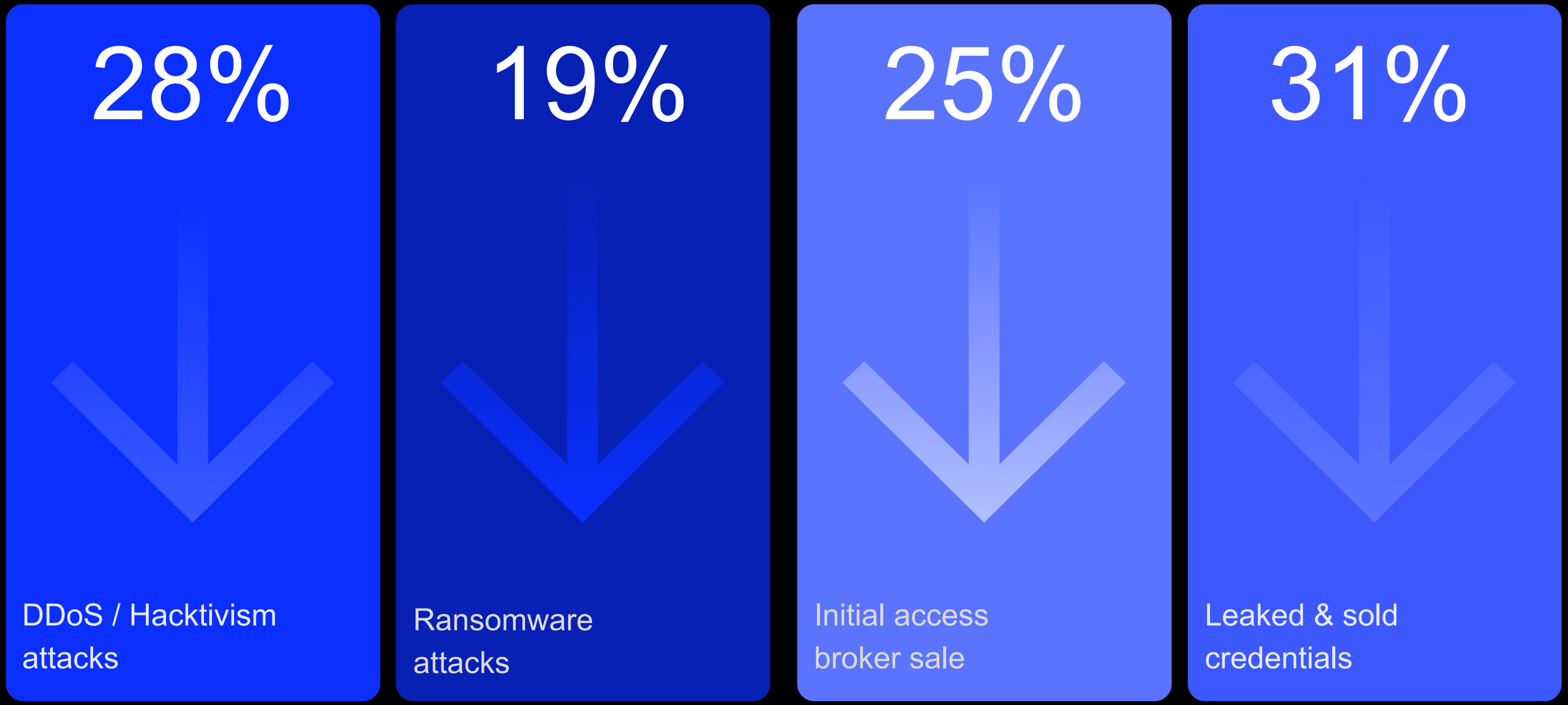
This report offers an overview of the latest threat landscape in Europe, covering key developments such as ransomware attacks, leaked credentials, data breaches, and more. It includes a month-over-month trend analysis to track evolving patterns. Additionally, the report spotlights a newly identified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



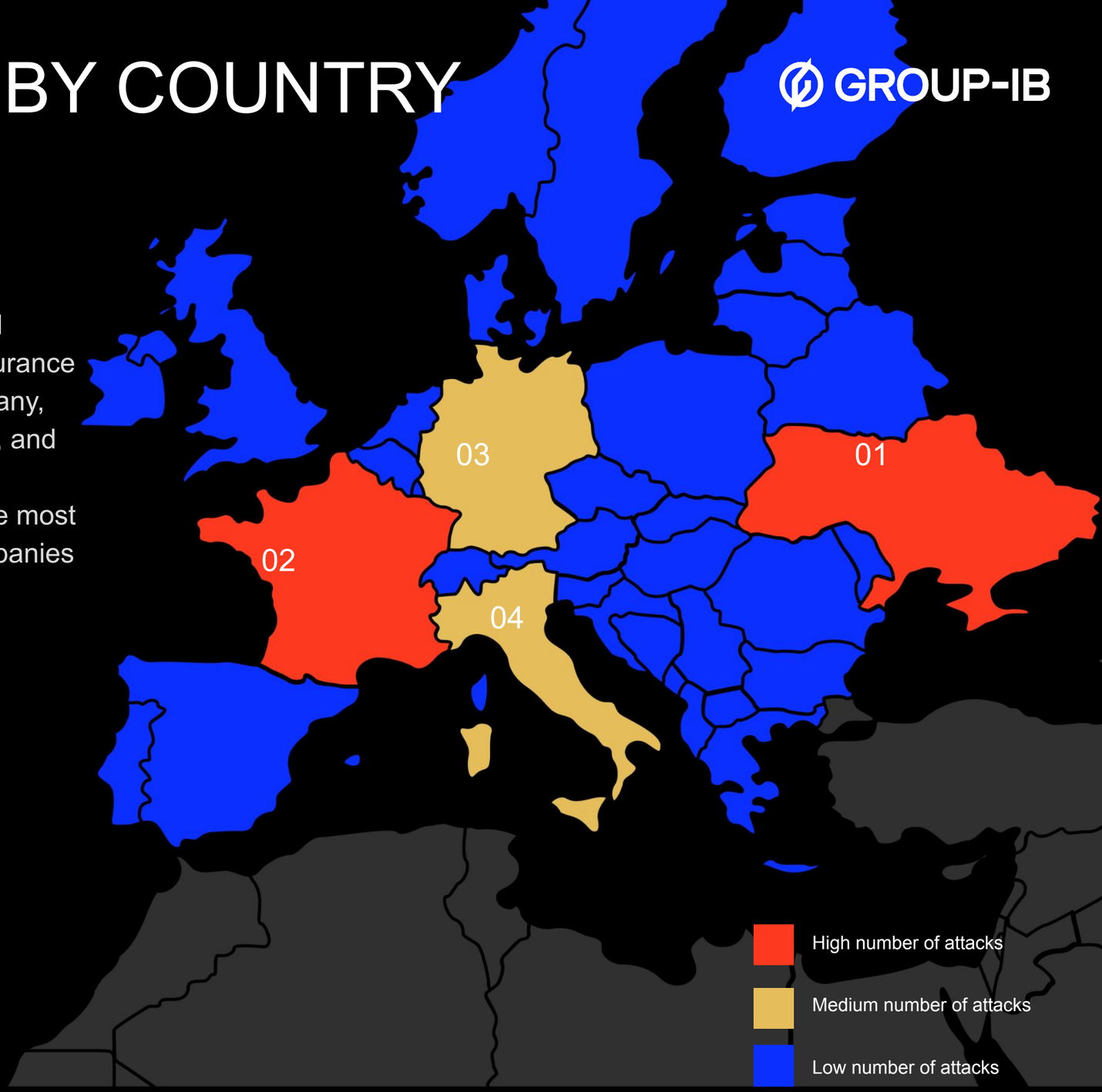
DDOS AND HACKTIVISM BY COUNTRY

Key events

- Threat actor Hezi Rash claimed responsibility for DDoS attacks targeting four German health-related organizations. The affected entities include The National Association of Statutory Health Insurance Physicians, Hartmannbund – Association of Physicians of Germany, Virchowbund – Association of Practicing Physicians of Germany, and the German Society for Hygiene and Microbiology.
- NoName057(16), DarkStormTeam and Hezi Rash were the three most active hacktivist groups performing DDoS attacks targeting companies and organizations in the EU.

Most attacked countries

Ukraine	France	Germany	Italy
29 attacks	27 attacks	16 attacks	15 attacks
+ 32%	+ 50%	- 76%	+ 200%



RANSOMWARE ACTIVITIES

Key events

- On September 26, 2025, the ransomware group Payouts King Group leaked corporate data of Creditinfo Group, a leading service provider for credit information and risk management solutions worldwide.
- On September 26, 2025, the ransomware group Arachna Leak leaked corporate data of Clinica Armstrong Internacional.

↓ 19%

124 Ransomware incidents

GROUP-IB

Most active threat actors

Qilin

19 attacks
- 24%

DragonForce

13 attacks
- 24%

Safepay

9 attacks
- 50%

The Gentlemen

8 attacks
(0 in August)

Lynx

7 attacks
+250%

Most targeted industries

Legal

8 attacks
+ 167%

Manufacturing

7 attacks
- 65%

Machinery manufacturing

6 attacks
+ 500%

Construction

7 attacks
+ 17%

Financial Services

5 attacks
+ 67%

INITIAL ACCESS BROKER SALE ON DARK WEB

↓ 25%

27 Sales

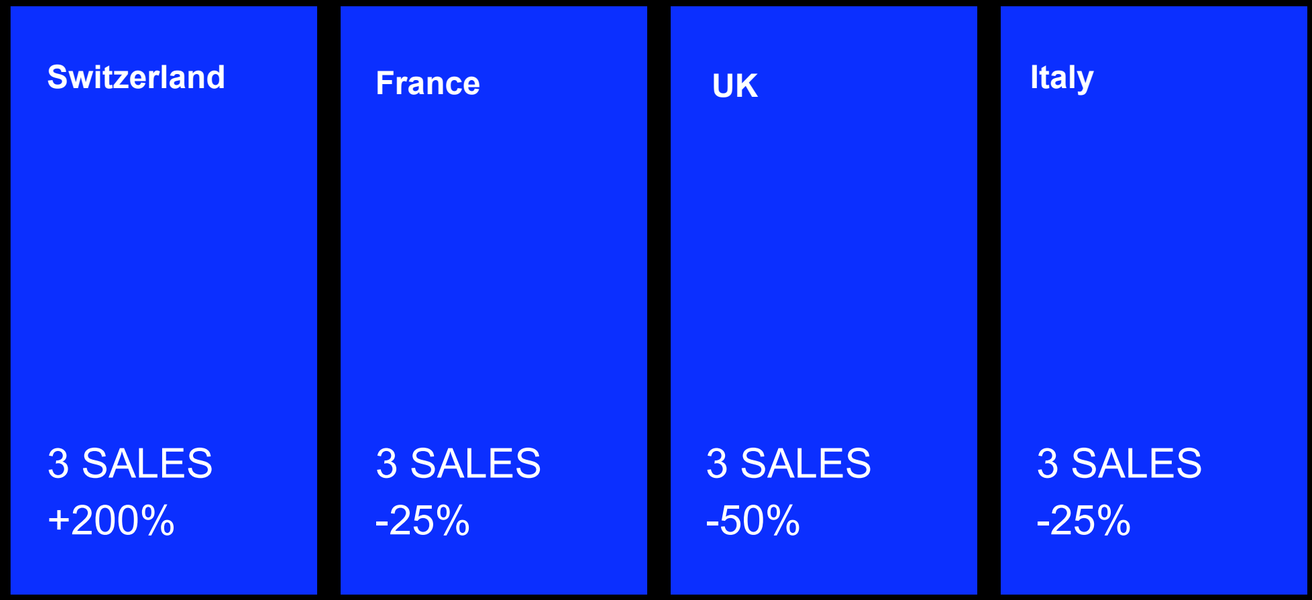
GROUP-IB

Initial access to a company’s systems can lead to data theft, corporate espionage, or the deployment of malware for various malicious purposes. This page shows the volume and geographic distribution of corporate infrastructure access instances currently for sale on the dark web.

Key events

- The highest-revenue company listed by Initial Access Brokers was a Serbian firm in the Marine Shipping & Transportation industry, with $206 million in annual revenue.

Most targeted countries



LEAKED & SOLD CORPORATE CREDENTIALS

GROUP-IB

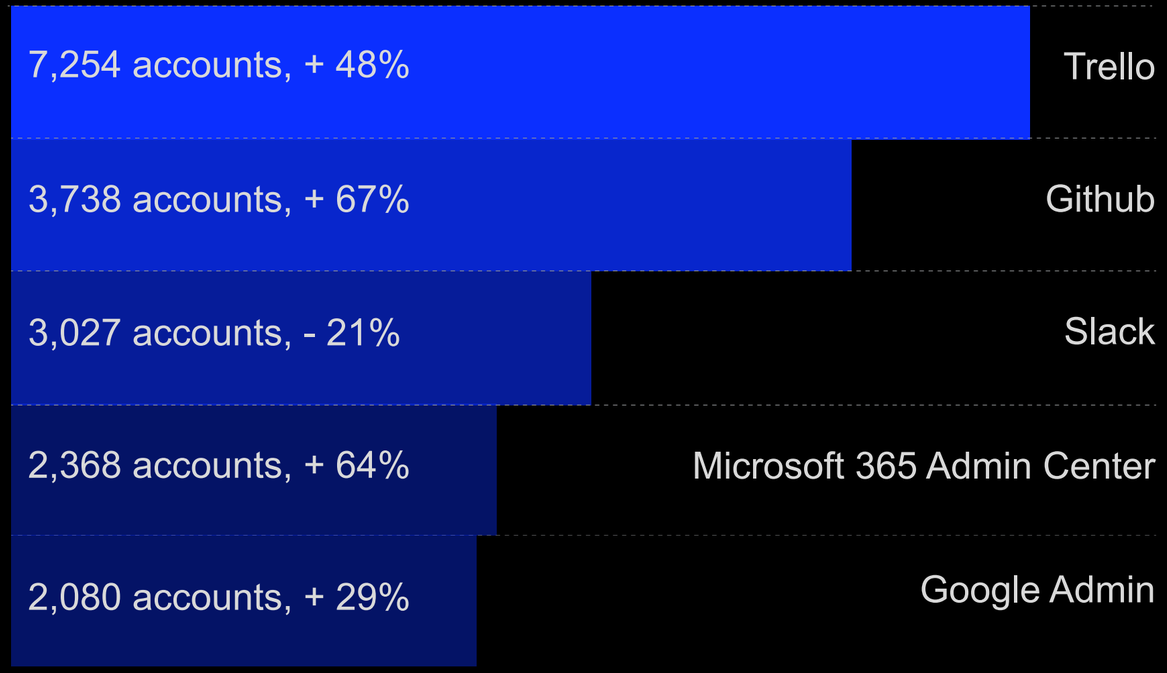
Key events

- Most compromised accounts were stolen via password stealers. Affected users were primarily from France, Spain, Italy, Poland, and Germany.
- The most active adversary-in-the-middle phishing framework in September was Tycoon 2FA.

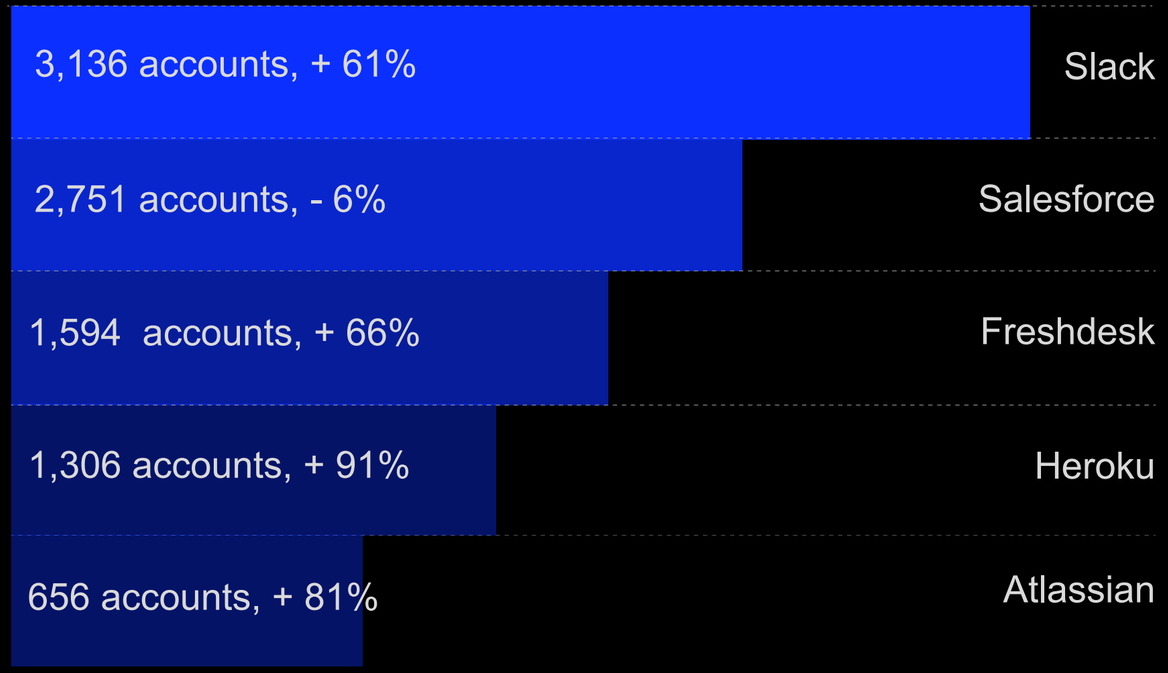
↓ 36%
compromised accounts: 139,092

↑ 51%
on sale on dark web markets: 20,248

Services with the most compromised accounts



Services with the most sold accounts



ADVISORY SPOTLIGHT

GROUP-IB

MuddyWater’s evolution

MuddyWater

Aliases
TEMP.Zagros, Seedworm
Static Kitten, TA450, Boggy
Serpens, Earth Vetala

First seen
2017

Latest activity
Present

LANGUAGES	GEOGRAPHY	INDUSTRY FOCUS	MOTIVATION(S)
English	Middle East	Telecommunications	Espionage
Persian	Turkey	Government	Intelligence Gathering
Arabic	Azerbaijan	Education	Tactical Disruption
Hebrew	Pakistan	Energy	
	United States	Aviation	
	United Kingdom	Information Technology	

Skillset

Linux, Apache, Windows, Nginx, Python, Golang, AWS, PowerShell, RMM, SpearPhishing

Toolset

StealthCache, Phoenix, BugSleep, FakeUpdate, LiteInject, Fooder, CannonRat, Blackout, UDPgangster, Chromium_Stealer, SilentShell, PowerGUI, Atera, PDQ, Action1, ScreenConnect, Level RMM, HackBrowserData, Yamux, go-socks5

Threat Actor Write-up

MuddyWater, also known by aliases TA450 and Seedworm, is a sophisticated threat actor group operating since at least 2017. It is believed to be state-sponsored by the Iranian Ministry of Intelligence and Security (MOIS). The group's primary motivation is espionage and intelligence gathering. MuddyWater targets a variety of industries including government, telecommunications, energy, and critical infrastructure, focusing its efforts in the Middle East, South Asia, and NATO-affiliated countries.

Modus operandi

MuddyWater primarily relies on phishing to gain initial access to systems belonging to organizations and persons of interest, and maintain long term stealthy access while conducting espionage and information gathering for further operation expansion, serving the interests of the Iranian government. They have also conducted destructive operations during times of conflict as a tactical move against Iranian geopolitical adversaries.

Key Insights

- MuddyWater continues to be active in the Middle East, with increased activity in Europe and the United States.
- The group continues to rely on phishing and maldocs for initial access.
- MuddyWater significantly reduced opportunistic RMM campaigns in favor of targeted spearphishing and custom malware.

Read more

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]

As the host of the FIRST Technical Colloquium in Paris, we’re inviting speaker proposals.
Submit your proposal → https://www.first.org/events/colloquia/paris2026/cfs