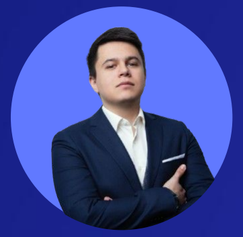
GROUP-IB

January, 2025

INTELLIGENCE INSIGHTS. EUROPE

Highlighting month-to-month trends and insights (November - December)

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, or emerging technique, providing actionable insights for proactive defenses.



ANTON USHAKOV
Head of Cyber Threat Intelligence

Key Insights

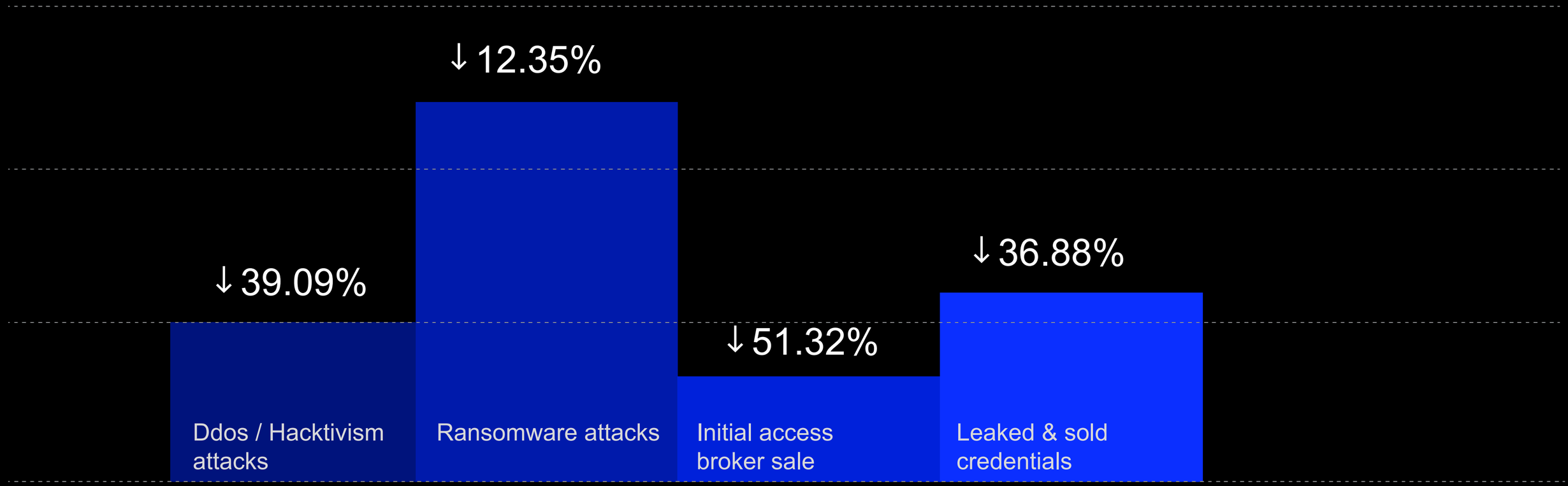
GROUP-IB

- In December 2024, the Clop ransomware group leveraged critical vulnerabilities, CVE-2024-50623 and CVE-2024-55956, in Cleo's file transfer software to gain unauthorized access and steal data from multiple organizations.
- ClickFix attacks gained significant traction and widespread adoption among threat actors due to its surprising effectiveness and were used for distribution of Lumma C2, Vidar, Rhadamanthys, XWorm, AMOS, Stealc.
- Black Basta became #1 ransomware actor in Europe in December while RansomHub and Akira kept their positions as #2 and #4 most active ransomware groups in Europe.
- Manufacturing, constructions and education sectors remained in Top-5 industries targeted by ransomware.
- Accounts of cloud services available for sale on underground markets are still the most common type of credentials that could be used to access corporate resources.
- Access to companies in the UK is still the most popular offer among Initial Access Brokers .

THREAT LANDSCAPE OVERVIEW

GROUP-IB

Month over Month Comparison
(November - December)



DDOS AND HACKTIVISM BY COUNTRY

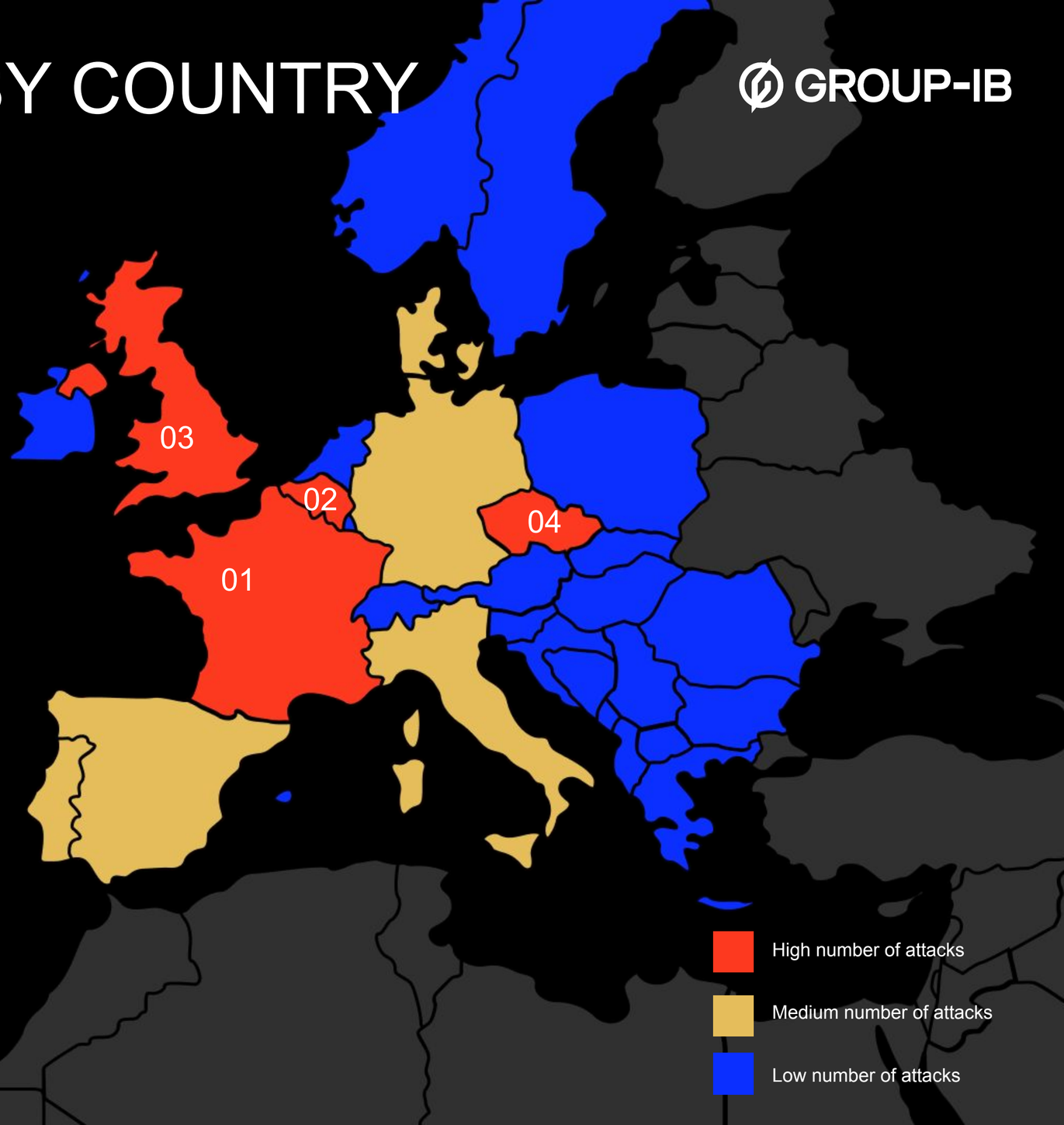
GROUP-IB

Key Events

- HIZBULLAH CYB3R TEAM and Mr Hamza announced DDoS attacks targeting multiple websites in Belgium including website of Belgian Federal Police, Bever municipality, the Province of Flemish Brabant, the Province of East Flanders, and the Wallonia Federation - Brussels.
- Mr Hamza, Penta Force and RedAtlas announced DDoS attacks targeting financial organizations in Czech Republic including Prague Stock Exchange and Czech National Bank.
- DarkStormTeam announced DDoS attack on the Ministry of Internal Affairs of Ukraine.

Most attacked countries

France	Belgium	UK	Czech
25 attacks	20 attacks	13 attacks	9 attacks
+66.67%	+1900.00%	-27.78%	+12.5%



RANSOMWARE ACTIVITIES

Key Events

- Akira ransomware attacked Pražské služby, a company based in Prague, which deals with the comprehensive collection, sorting, utilization and disposal of waste, maintenance of roads and public spaces, ensuring the passability and walkability of roads and sidewalks, traffic signs and energy production in the capital city of Prague.
- RansomHub ransomware attacked INIA: national center of the Spanish National Research Council (CSIC), dedicated to Research, Development and Innovation in agricultural, livestock, food, forestry and environmental matters.

↓ 12.35%

71 Ransom incidents

GROUP-IB

Most active threat actors

Black Basta

11 attacks
+ 175%

RansomHub

9 attacks
- 43.75%

Qlin

7 attacks
+ 40%

Akira

5 attacks
- 37.5%

Brain Cipher

5 attacks
+ 0%

Most targeted industries

Manufacturing

8 attacks
- 20%

IT

5 attacks
+ 25%

Architecture

5 attacks
+ 400%

Construction

5 attacks
- 16.67%

Education

3 attacks
- 40%

INITIAL ACCESS BROKER SALE ON DARK WEB

↓ 51.32%

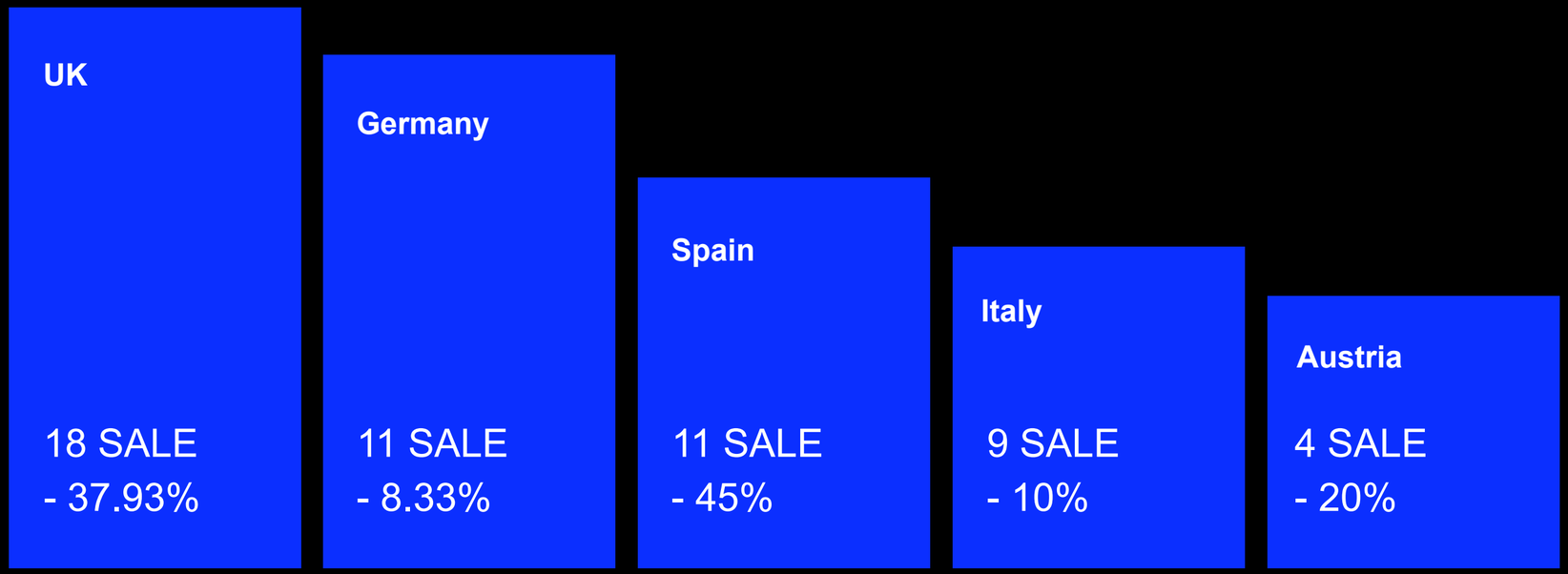
74 Sale

GROUP-IB

Key Events

- LockBit Ransomware group announced LockBit 4.0 update and new affiliate program.
- U.S. authorities announced charges against alleged developer for the LockBit ransomware group.

Most targeted countries



LEAKED & SOLD CORPORATE CREDENTIALS

GROUP-IB

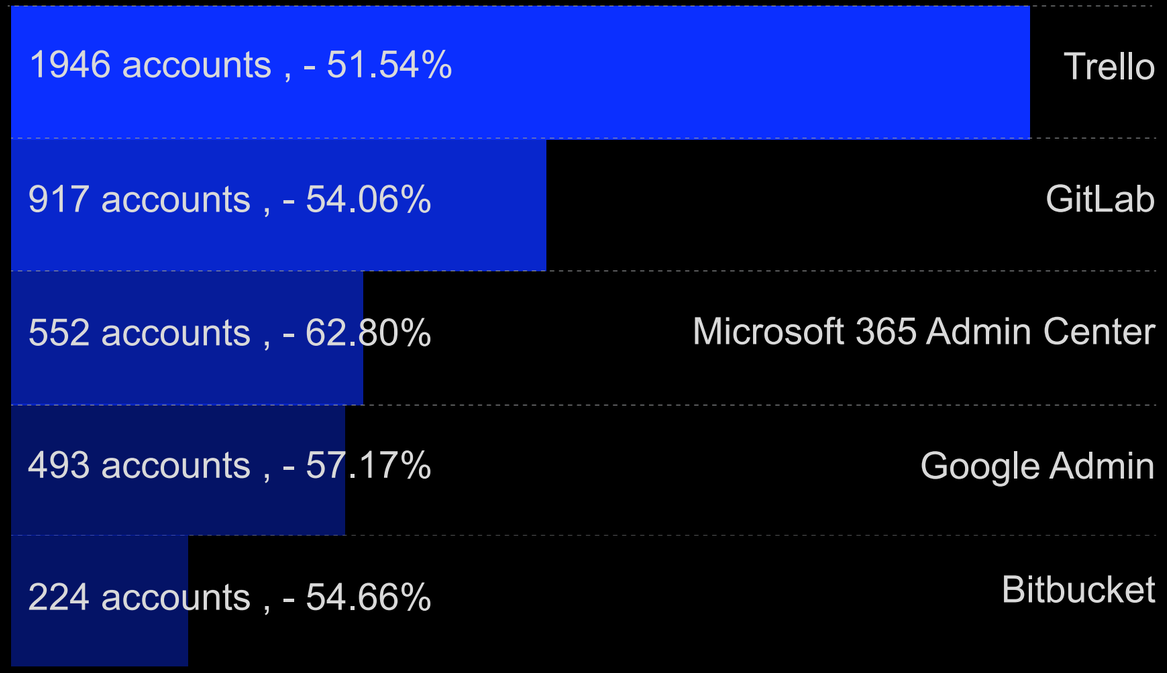
Key Events

- On the 24th of November 2024 the source code for Banshee MacOS Stealer was leaked.
- ClickFix attacks gained significant traction and widespread adoption among threat actors due to its surprising effectiveness and were used for distribution of Lumma C2, Vidar, Rhadamanthys, XWorm, AMOS, Stealc.

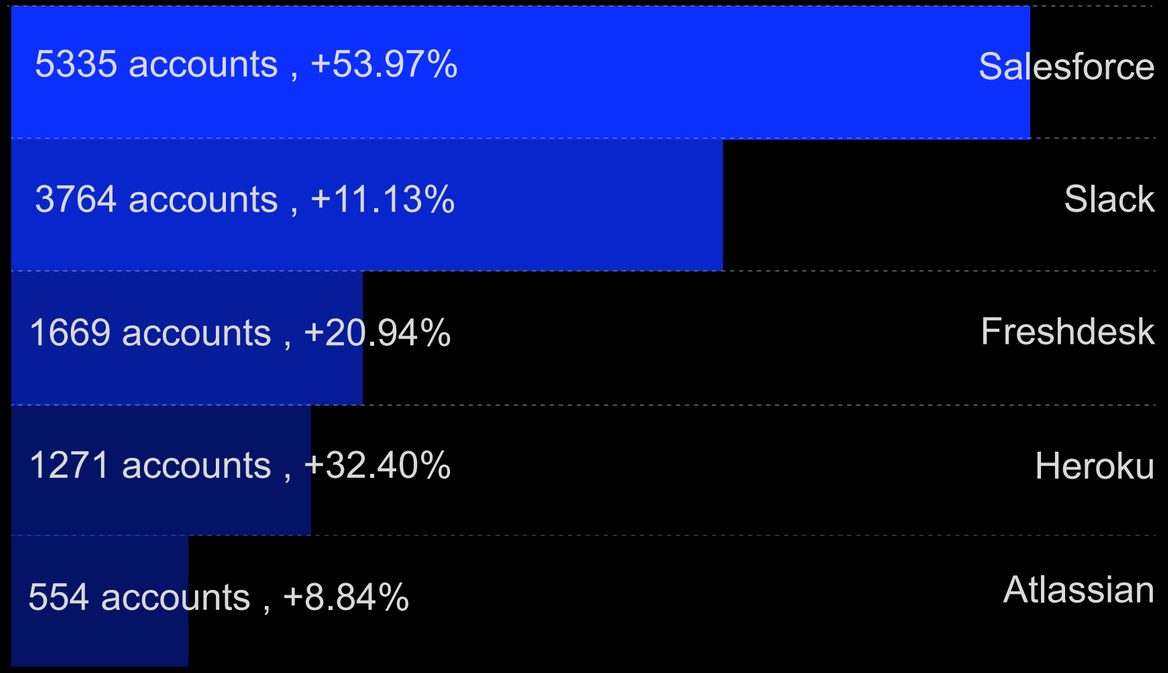
↓ 56.18%
Compromised account

↑ 30.70%
on sale on dark web markets

Services with the most compromised accounts



Services with the most on sale accounts



ADVERSARY OF THE MONTH

GROUP-IB

Threat actor group

Clop

Targeted industries:

- Manufacturing
- Information technology
- Financial services
- Software
- Education
- Healthcare
- Transportation
- Retail

Period of Activity:	2019 - Present
Targeted countries:	Worldwide
Attribution:	Unknown
Intent:	Financially-motivated

Attack Summary

In December 2024, the Clop ransomware group leveraged critical vulnerabilities – CVE-2024-50623 and CVE-2024-55956 in Cleo's file transfer software to gain unauthorized access and steal data from multiple organizations.

Key Observations

- Clop deployed Malichus backdoors for prolonged network infiltration.
- The group indicated selective deletion of sensitive government, medical, and research data to avoid escalation.
- Data exfiltrated in the Cleo breaches is reportedly deleted from their servers as part of internal policy shifts.

STAY SMART. STAY CONNECTED. STAY SECURED

[Talk to our team]

RECENT RESOURCES

Read now

Read now

MEET US AT EVENTS