Cognyte LUMINAR

Infosec
Powered by TeleGroup

Illuminating the Cyber Underworld

2024 Major Trends in Cyber Threat Intelligence

Omree Wechsler

Senior Threat Intelligence Analyst

CyberSecurity Group

Cognyte at a glance

30
Years

100+
Countries

~400
Customers

$313.5M
Non-GAAP revenue, traded in Nasdaq (CGNT)

6
Global R&D centers

13
Global offices

1500+
Employees

Note: All figures on this page are for year ending January 31, 2024 (FYE24). GAAP revenue for the year ending January 31, 2024 was $313.4 Million.

LUMINAR Threat Intelligence Group

Proven, well-established methodology that is **fully embedded in the product**

Making sure our products **generate value for a wide range of industries**

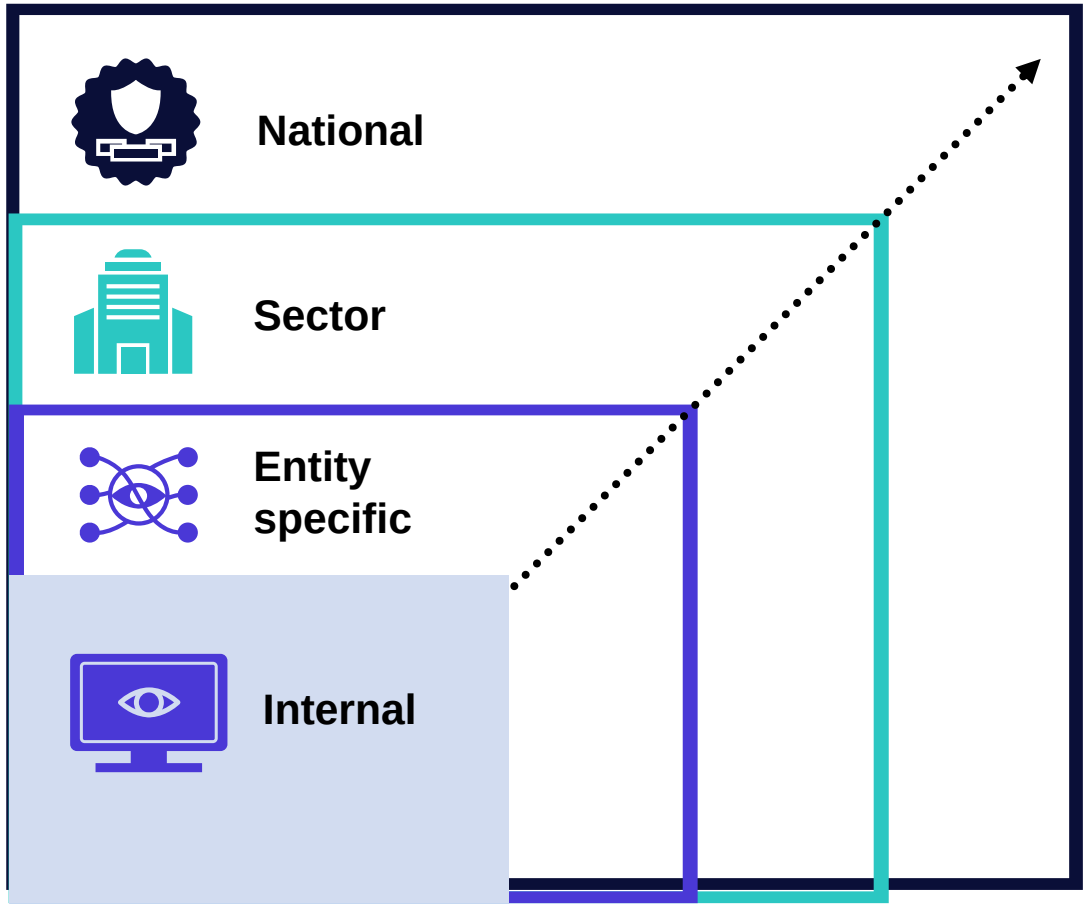
Provide inputs to product roadmap and **design**

Understanding customer's **needs and best-practices**

Extensive cyber **research and analysis experience**

Threat intelligence - key drivers for security leaders

- Limit external exposure to threat actors
- Detect sensitive data leakage
- Identify attack groups targeting the organization, the industry, or the nation



LUMINAR

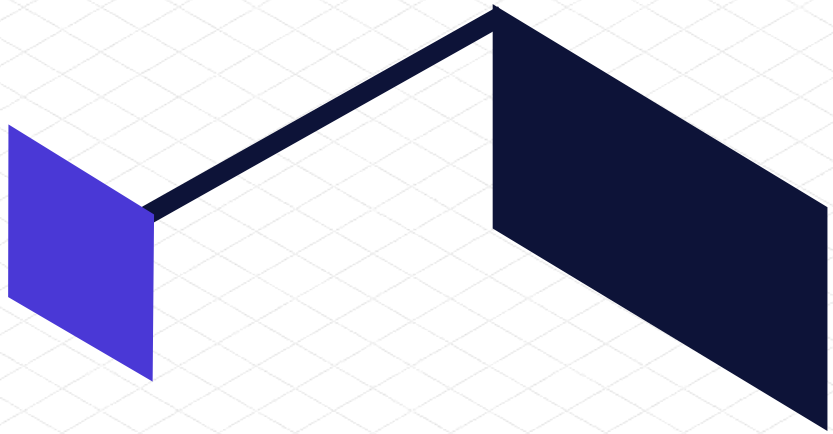
Recognized as an Example Vendor in Gartner's Emerging Tech: The Future of Cyber Threat Intelligence report (August 2024)

Gartner®

https://www.cognyte.com/news/cognyte-recognized-for-its-luminar-solution-in-the-2024-gartner-emerging-tech-the-future-of-cyberthreat-intelligence-research/

The GenAI revolution

- Threat intelligence analysts and SOC teams must speed up risk assessment and analyze raw data at scale
- Leveraging the power of GenAI to accelerate threat intelligence is a natural fit



GenAI technologies can support multiple use cases:

- Contextualizing and enriching threat data
- Identifying and visualizing key security trends
- Sorting and filtering raw data
- Prioritizing threats
- Creating reports

AI-driven CTI findings

Luminar's 2024 Annual Report
Key takeaways

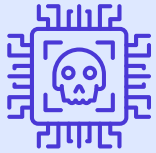
- **Technology and government** are the most targeted industries, amounting to 30% of attacks
- **50%** of attacks documented were **financially-motivated**
- **MOVEit flaw**, alongside two Ivanti Connect Secure zero-days, were the most exploited flaws
- Significant shifts in popularity of **info-stealers,** as recently emerged info-stealing malware took over the vector (accounting for over 70% of infections)
- Multiple **new ransomware variants** are still emerging, almost on a monthly basis, despite law enforcement crackdown

LUMINAR

WE ANALYZED:

1650

cyber feeds



9.4M

sales ads of stolen access credentials

100+

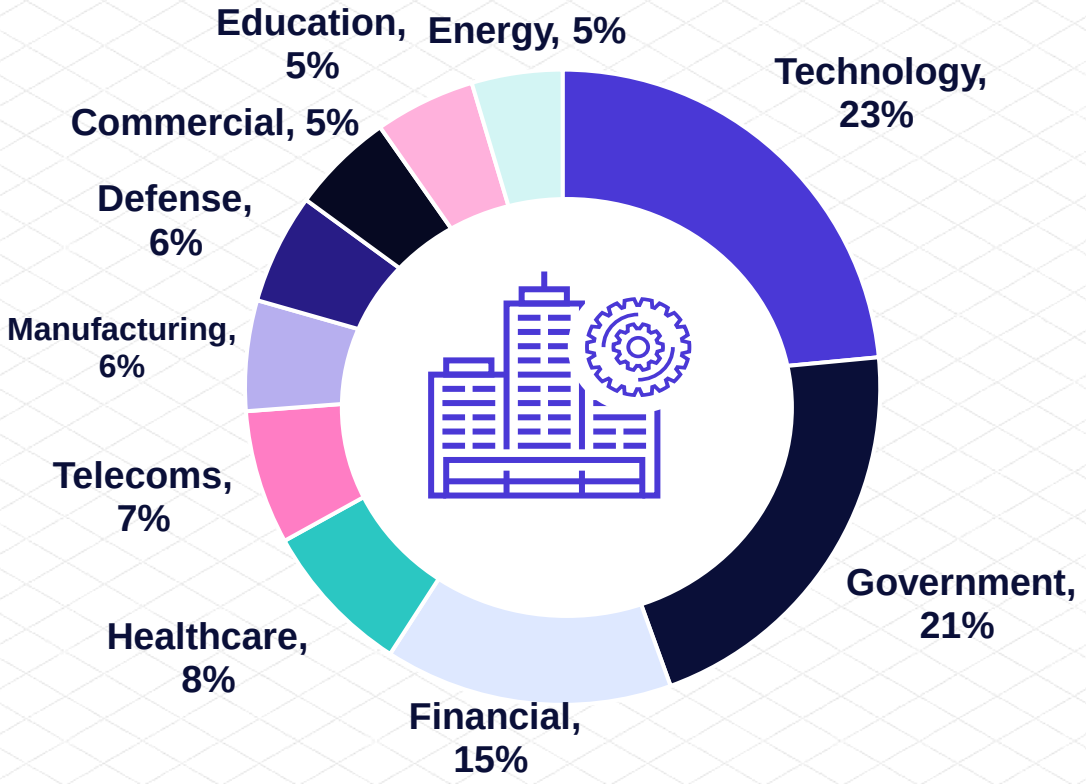
ransomware Dark Web extortion sites

26

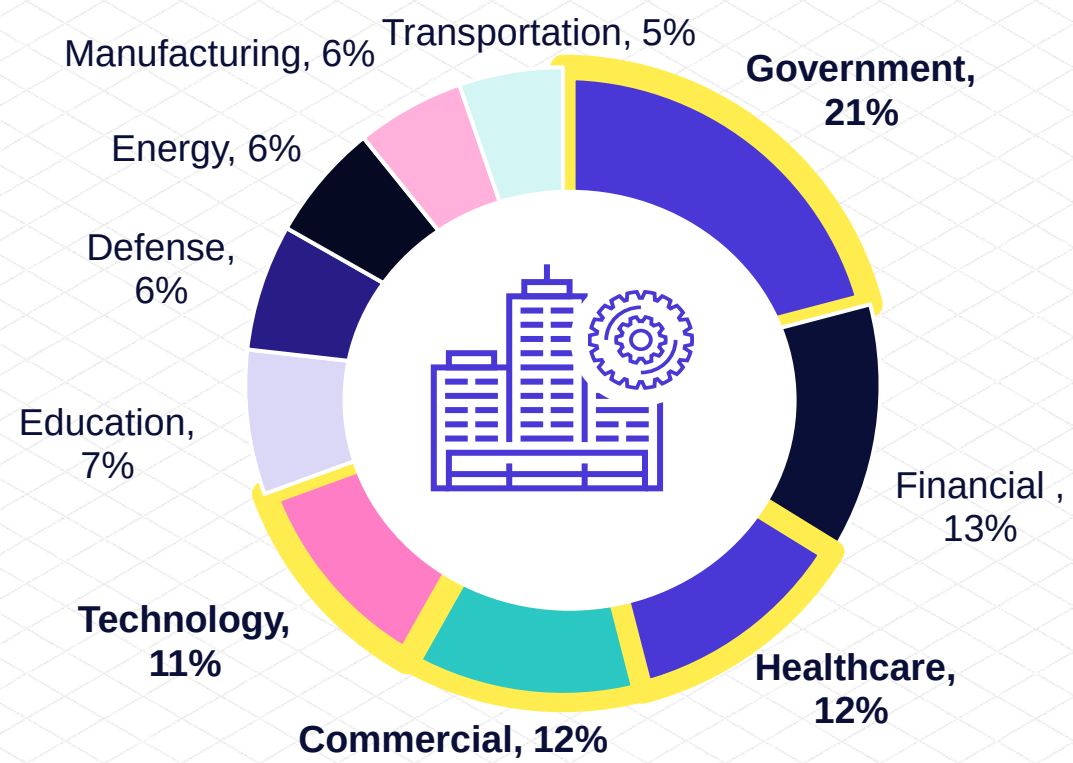
key industries

Top targeted industries: 2023 vs. H1 2024

2023



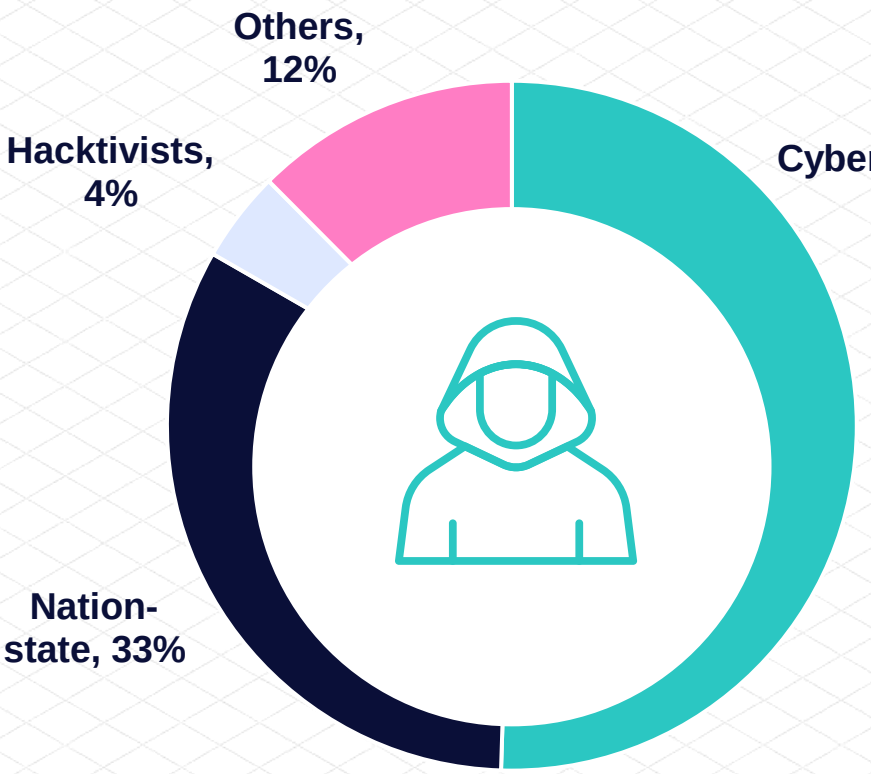
H1 2024



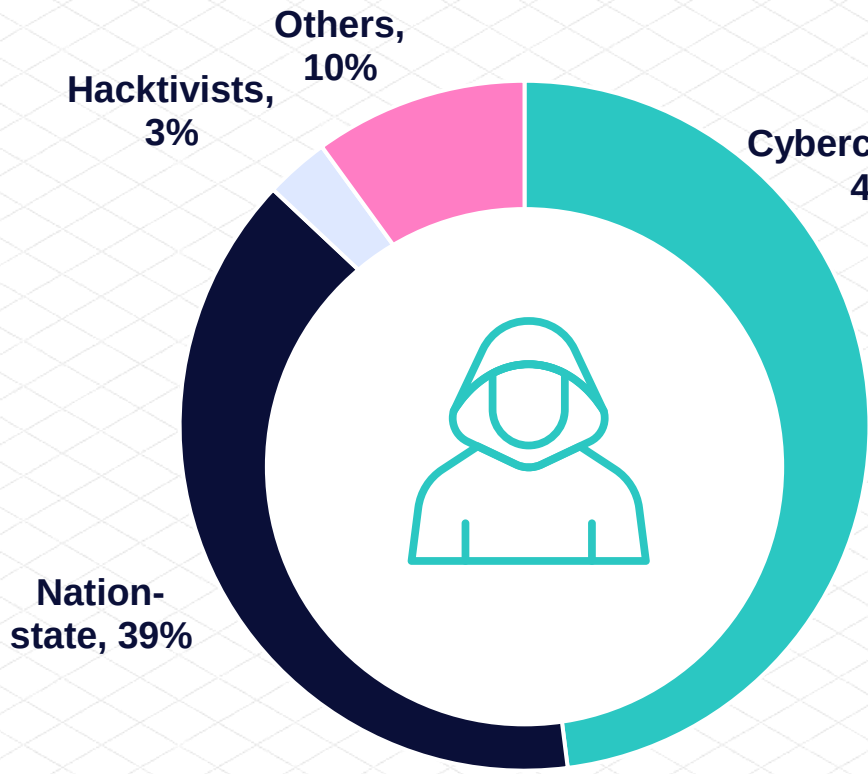
- In H1 2024, cyber attacks against the Technology industry decreased in about 50%, while government entities remained a prime target
- Attacks against the Healthcare industry increased in 50%

Threat actors: 2023 vs H1 2024

2023



H1 2024



+ Cybercrime and financial gain are still the top motivation for conducting cyber attacks
+ During H1 2024, an increase in nation-state APT attacks was seen, mainly against government entities

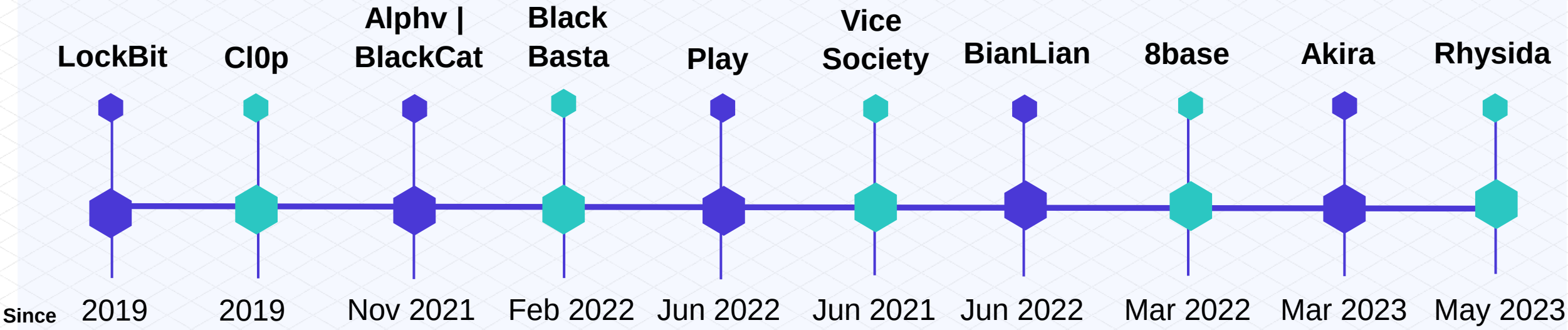
Ransomware

Ransomware attacks

- Ransomware continues to grow and remains one of the biggest threats to organizations, in part fueled by **Ransomware as a Service (RaaS)**
- During 2023, ransomware attacks increased **~40%** worldwide
- Despite significant efforts of law enforcement to crackdown **Ransomware** gangs (such as LockBit in February 2024 and ALPHV/BlackCat in December 2023) the groups managed to continue their operations
- During 2024, numerous new ransomware gangs have appeared, some of which use strains that surfaced in 2023 and were rebranded

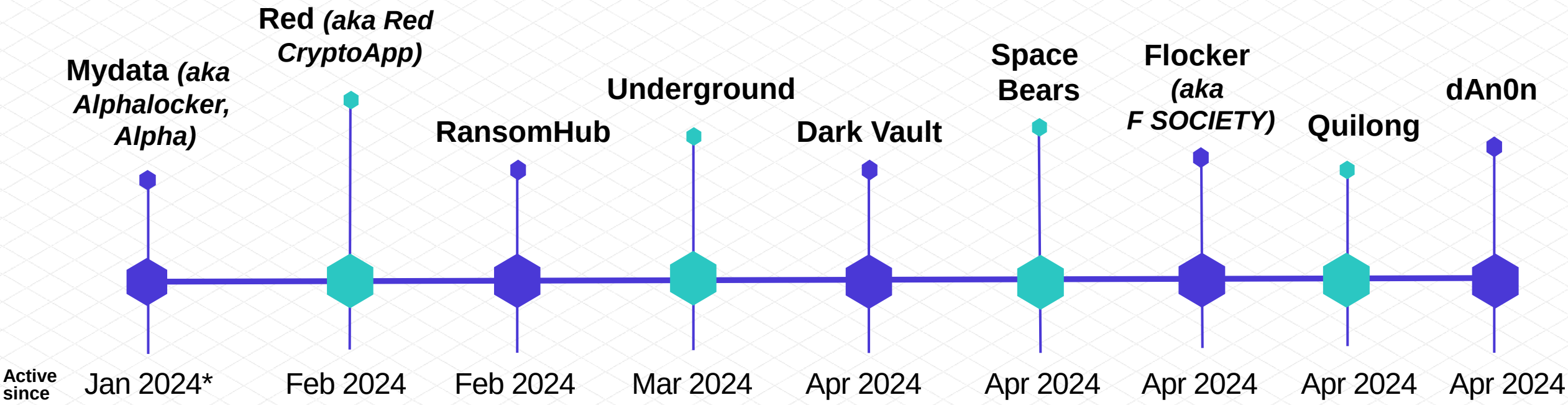
Top 10 active Ransomware groups in 2023

Ransomware Group



- LockBit has been the top ransomware family since 2022
- Newly emerged groups are also active and prominent in the ransomware landscape

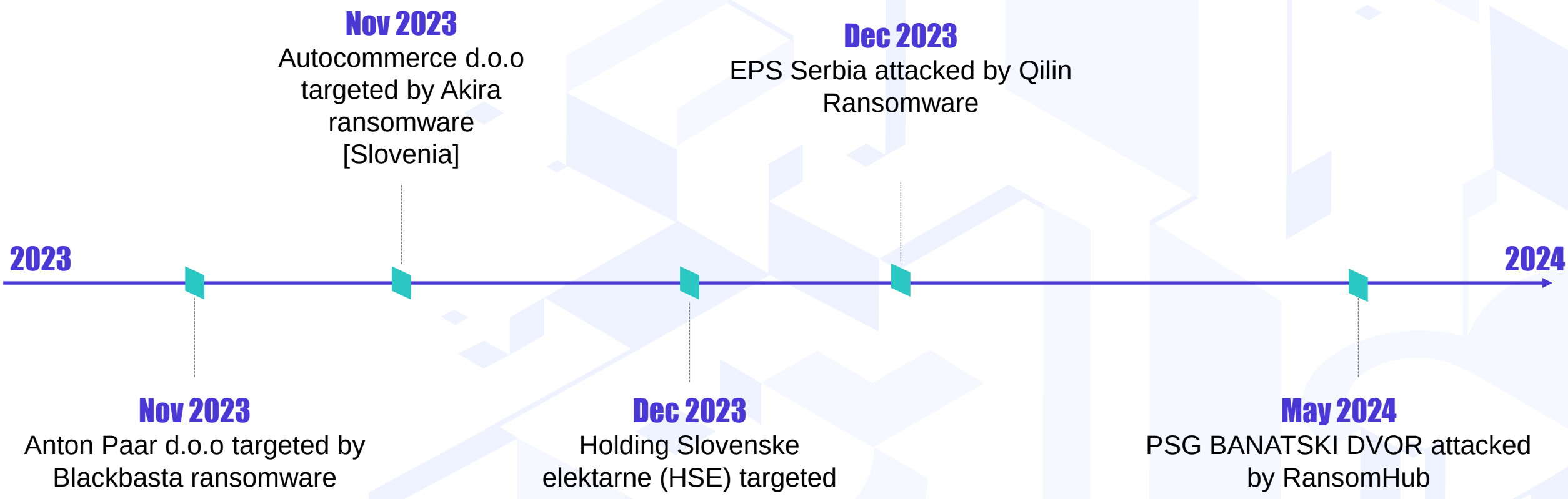
New Ransomware groups that emerged in H1 2024



+ Are law enforcement crackdowns fueling the ransomware ecosystem?
+ During H1 2024, 9 new groups have emerged: 5 of them in April alone

* Leak site titled “Mydata” emerged in January 2024, although Alpha ransomware has been observed since May 2023

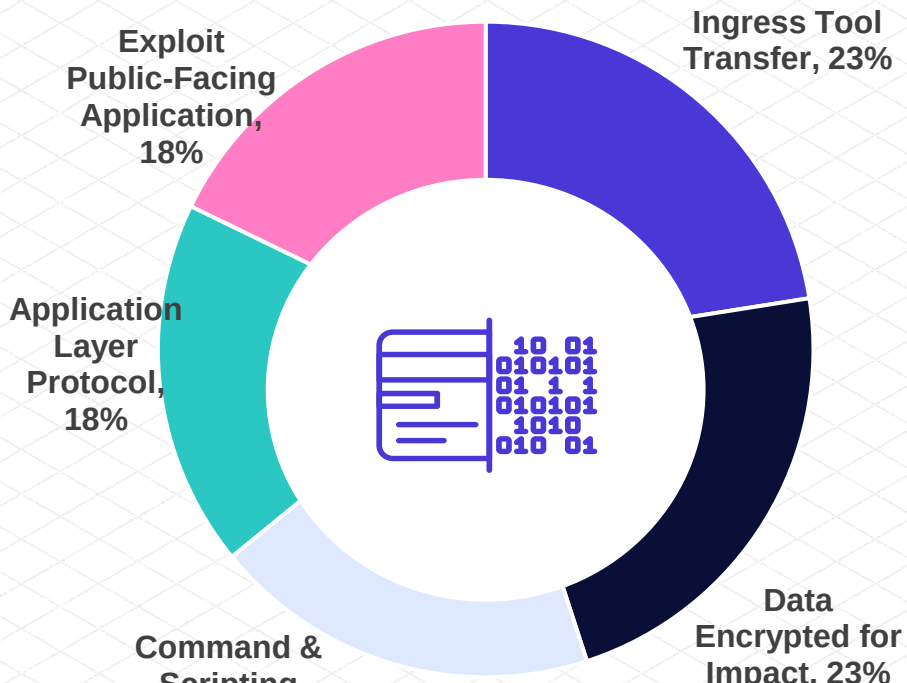
Attacks timeline in the Balkans Region



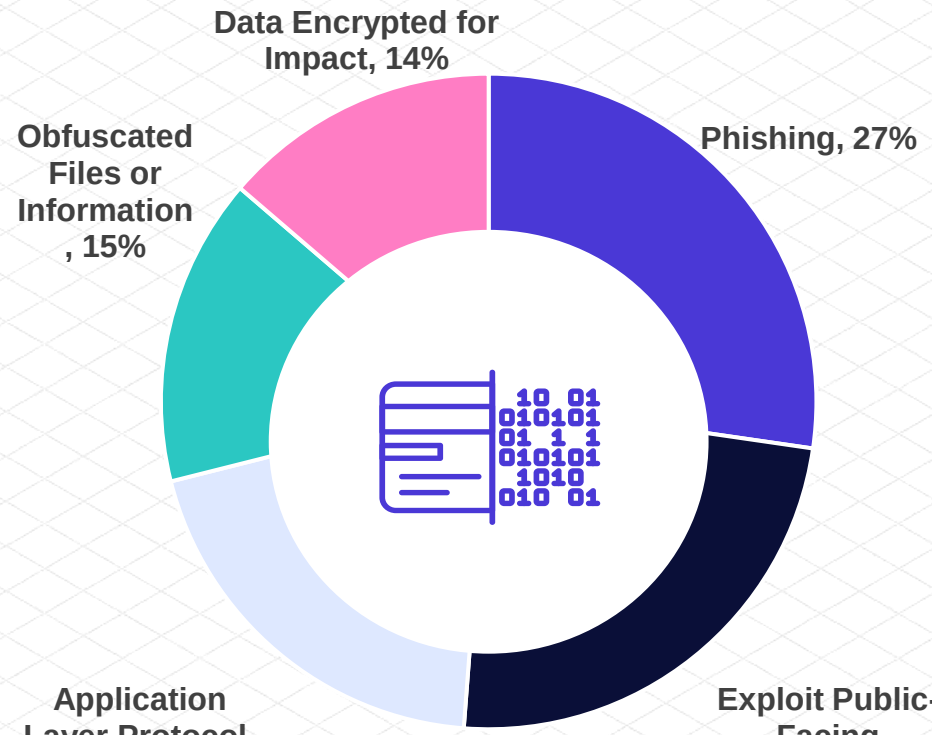
Vulnerability Intelligence

Top used TTPs by attack groups

2023



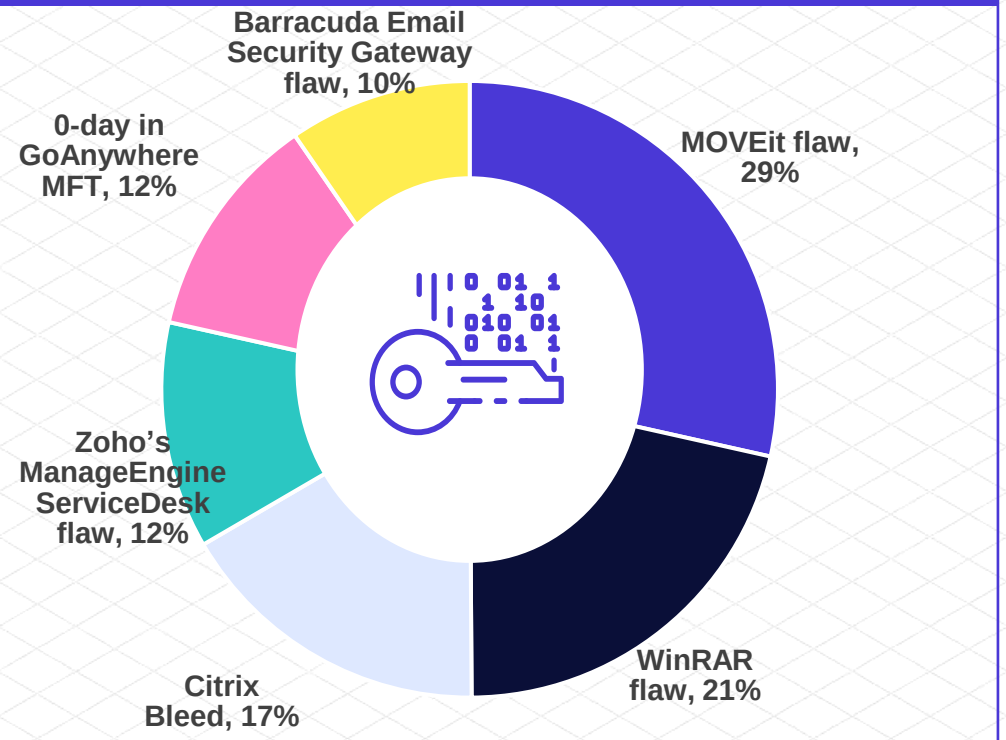
H1 2024



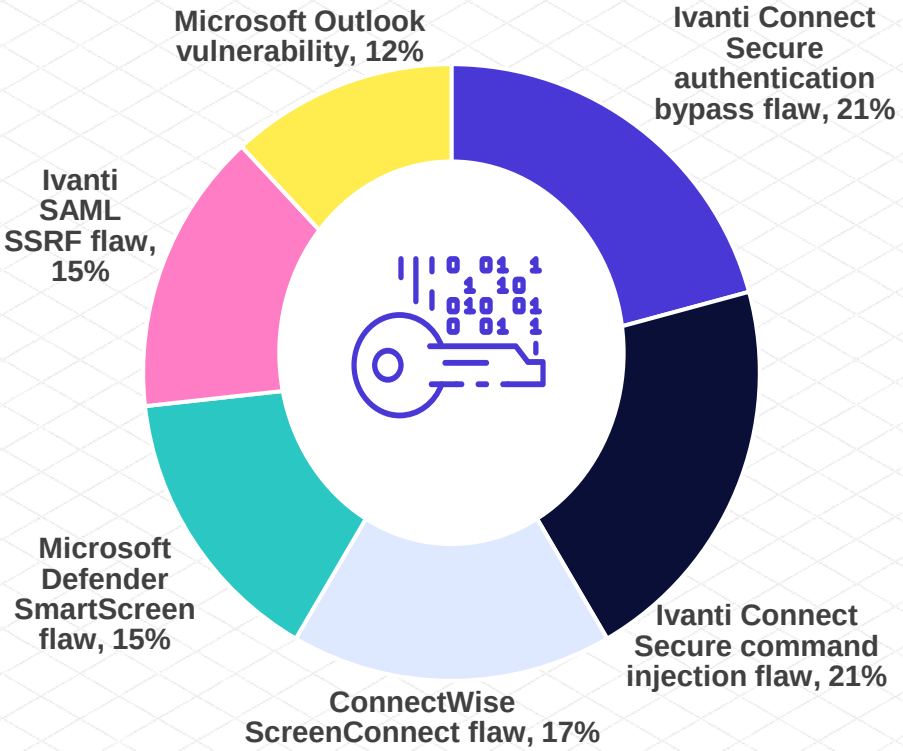
+ During H1 2024, phishing was the leading TTP for various threat actors
+ An increase was seen in hacktivist-related TTPs, due to the geopolitical situation in Europe and the Middle East

Vulnerability intelligence trends

2023 Most Exploited CVEs

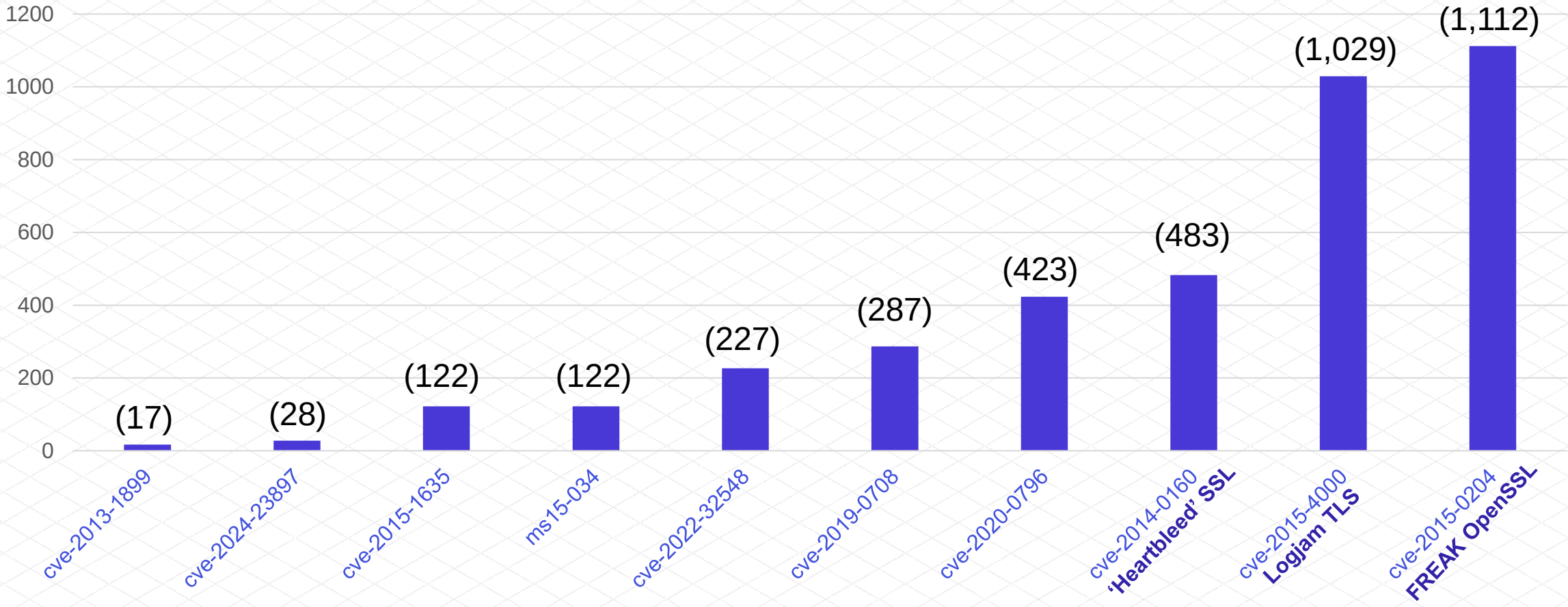


H1 2024 Most Exploited CVEs



+ In 2023, the MOVEit flaw was actively exploited by the Cl0p ransomware group with over 2,600 victims worldwide
+ The two Ivanti Connect Secure zero-days were exploited by Chinese APT groups

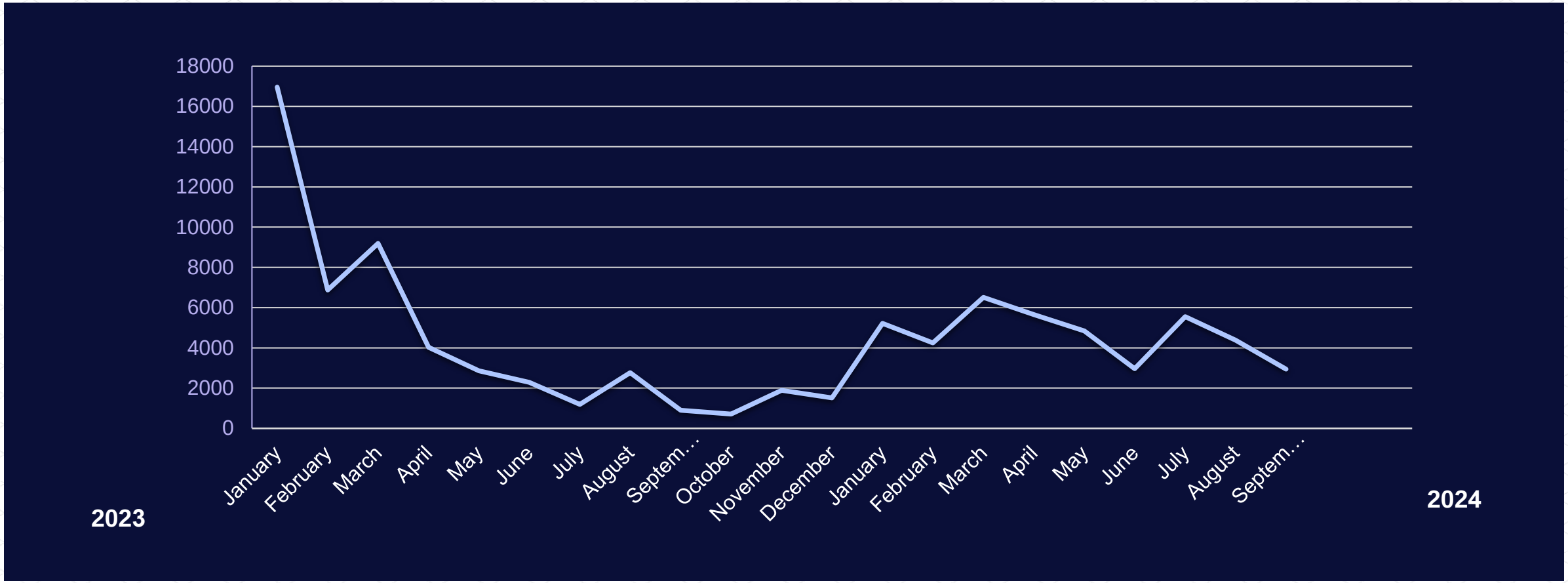
Top 10 vulnerabilities found in servers located in the Balkans



Stolen Access Credentials

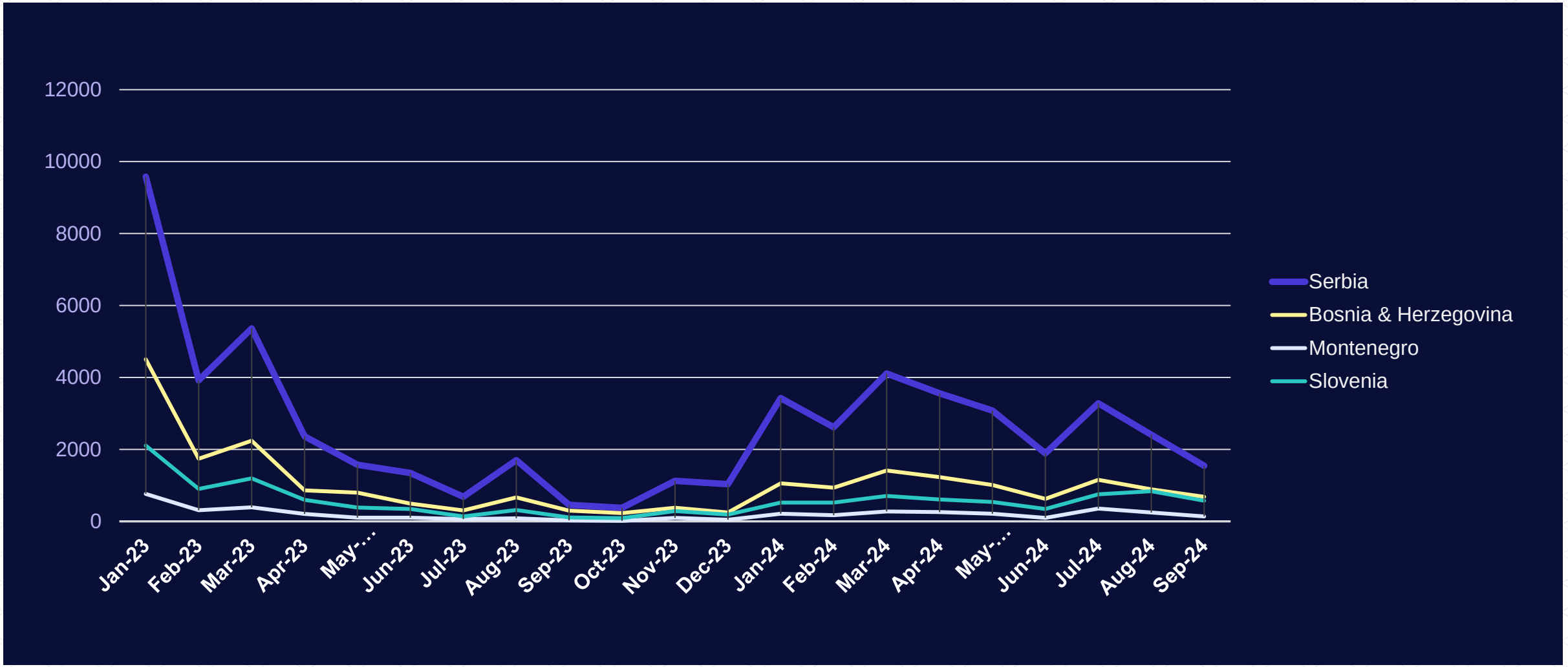
Shifts in info-stealers popularity on Dark Web platforms

Trend of Balkan states stolen access credentials offered for sale (2024 compared to 2023)

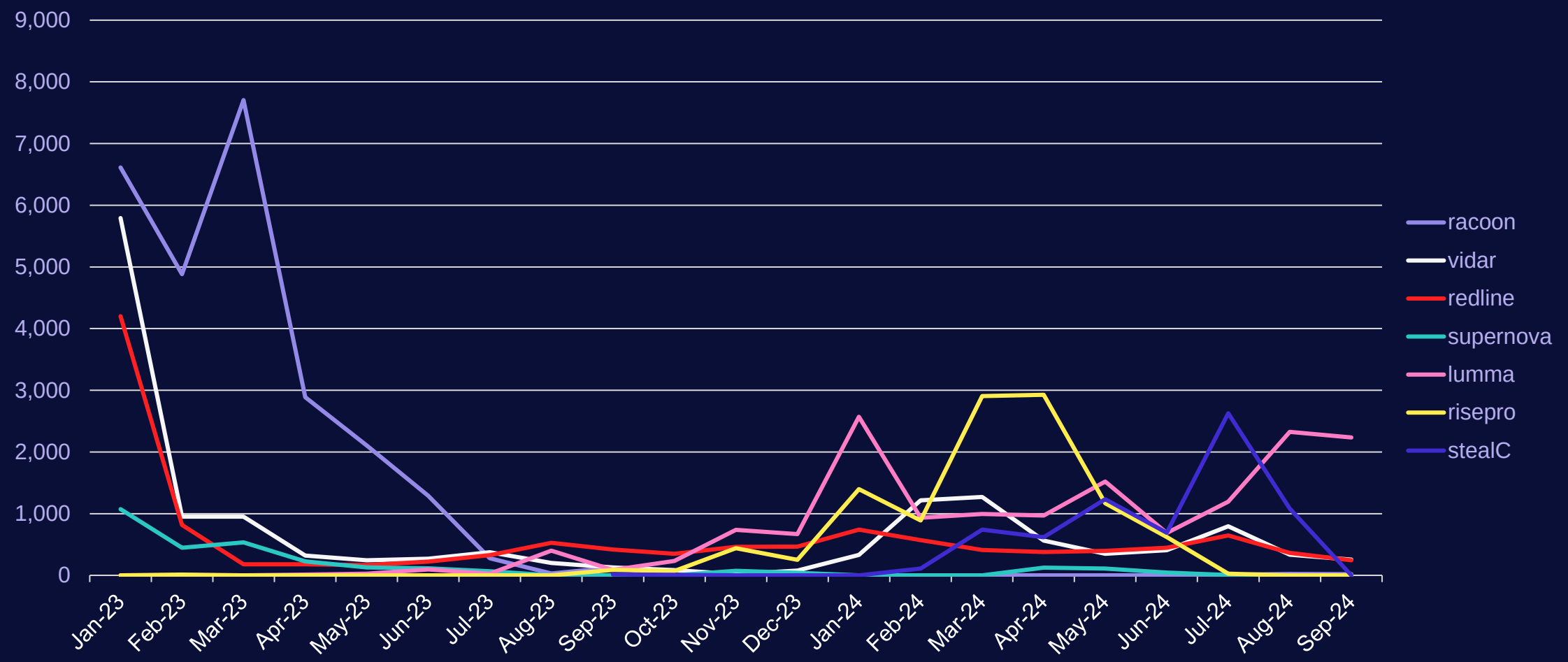


Shifts in info-stealers popularity on Dark Web platforms

Breakdown by Balkan states



Popularity of common infostealers in the Balkans



Shifts in popularity of info-stealers on Dark Web platforms

+ Most popular **info-stealers in H1 2024: RisePro** and **Lumma** (accounting for **53% of infections**)

+ **Previously popular** info-stealers are **in decline**:
- Racoon (99.8%)
- Redline (53%)
- Vidar (44%)

+ **The importance of following the trends:** The easiness of breaching an organization

Cognyte

Thank you

cognyte.com