TLP:CLEAR

CENTRE FOR CYBERSECURITY BELGIUM

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

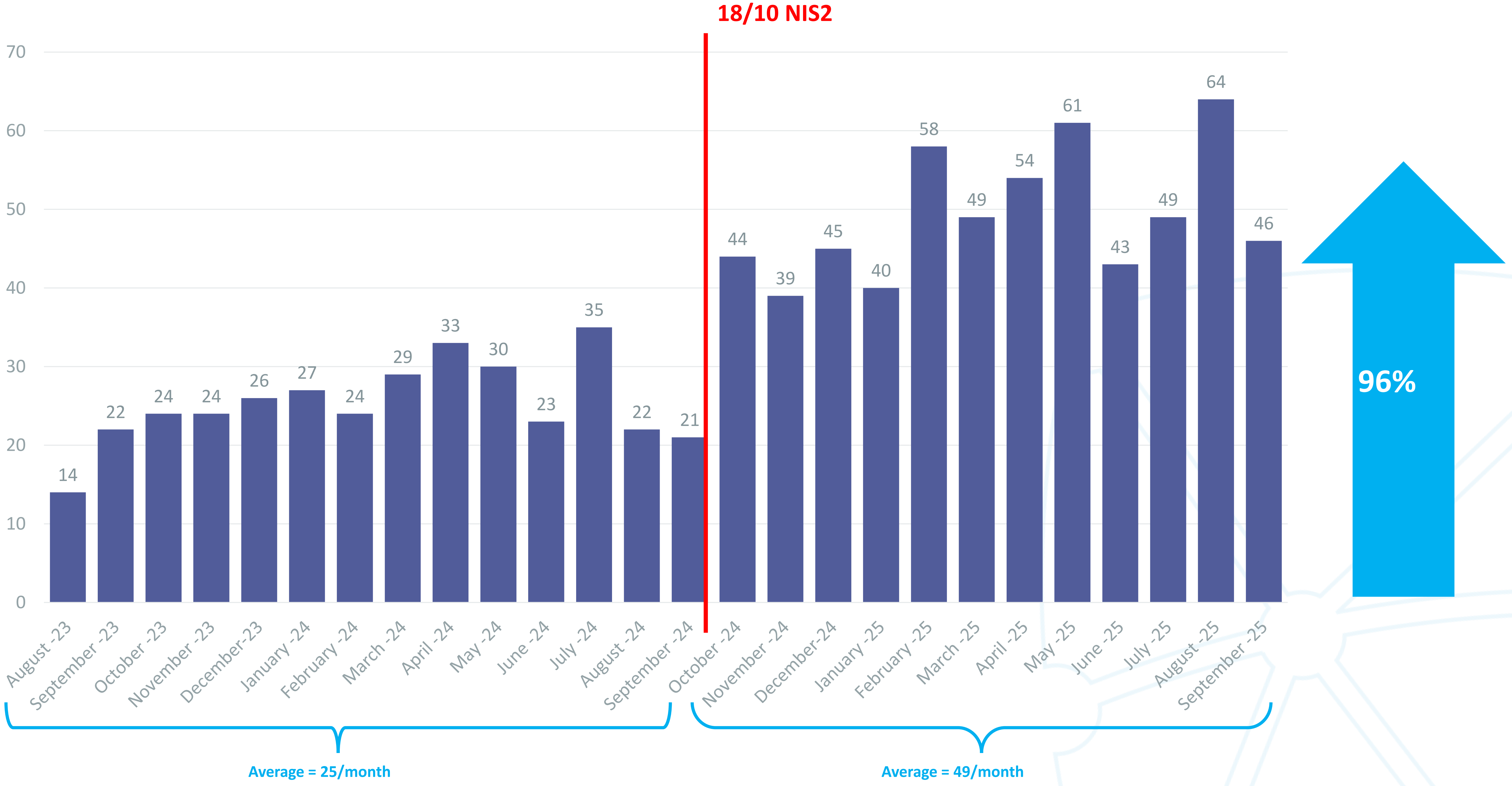
Cyber Threat Landscape Q3 2025: Trends, Metrics, and Recommendations

QCTR Q3 – October 2025

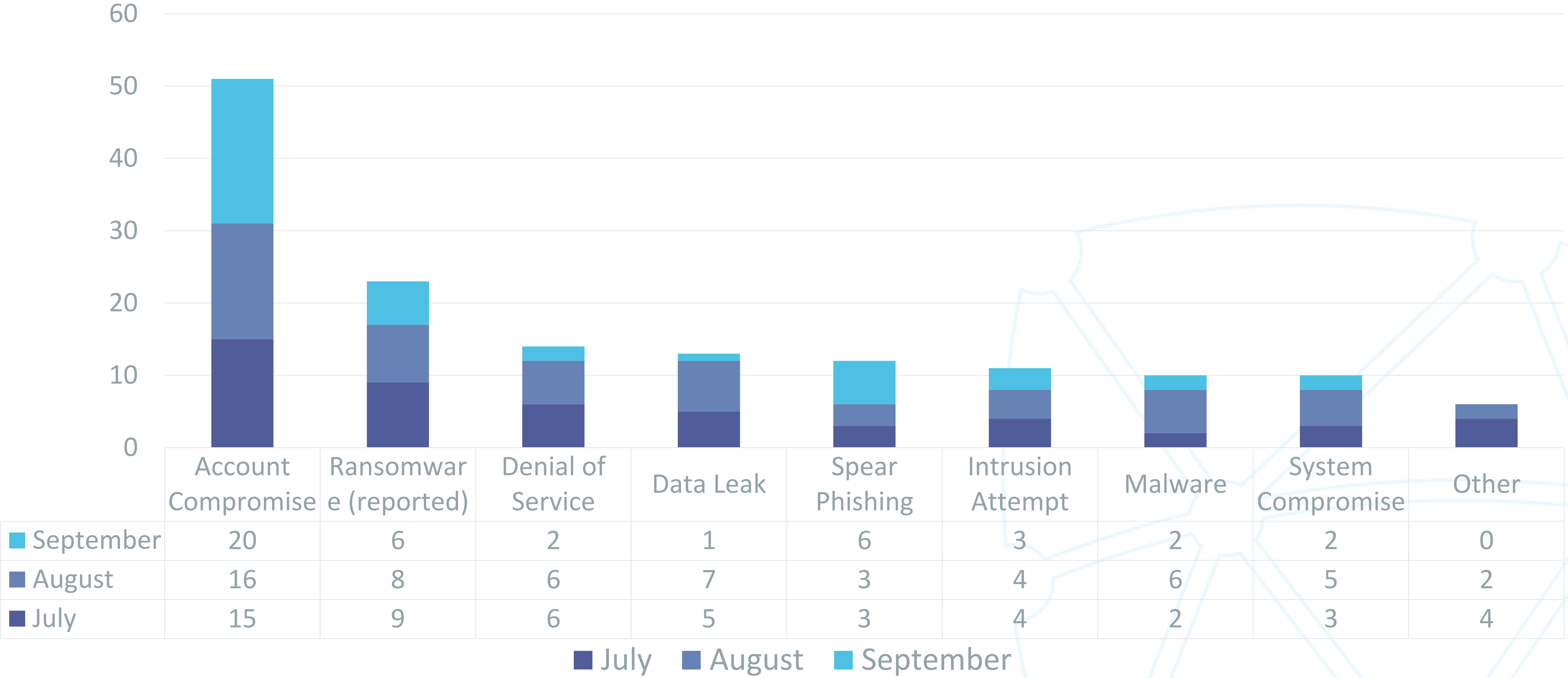
TLP:CLEAR

Evolution of Cyber Incident Notifications in Belgium

Number of notifications received by the CCB



Incident Breakdown by type

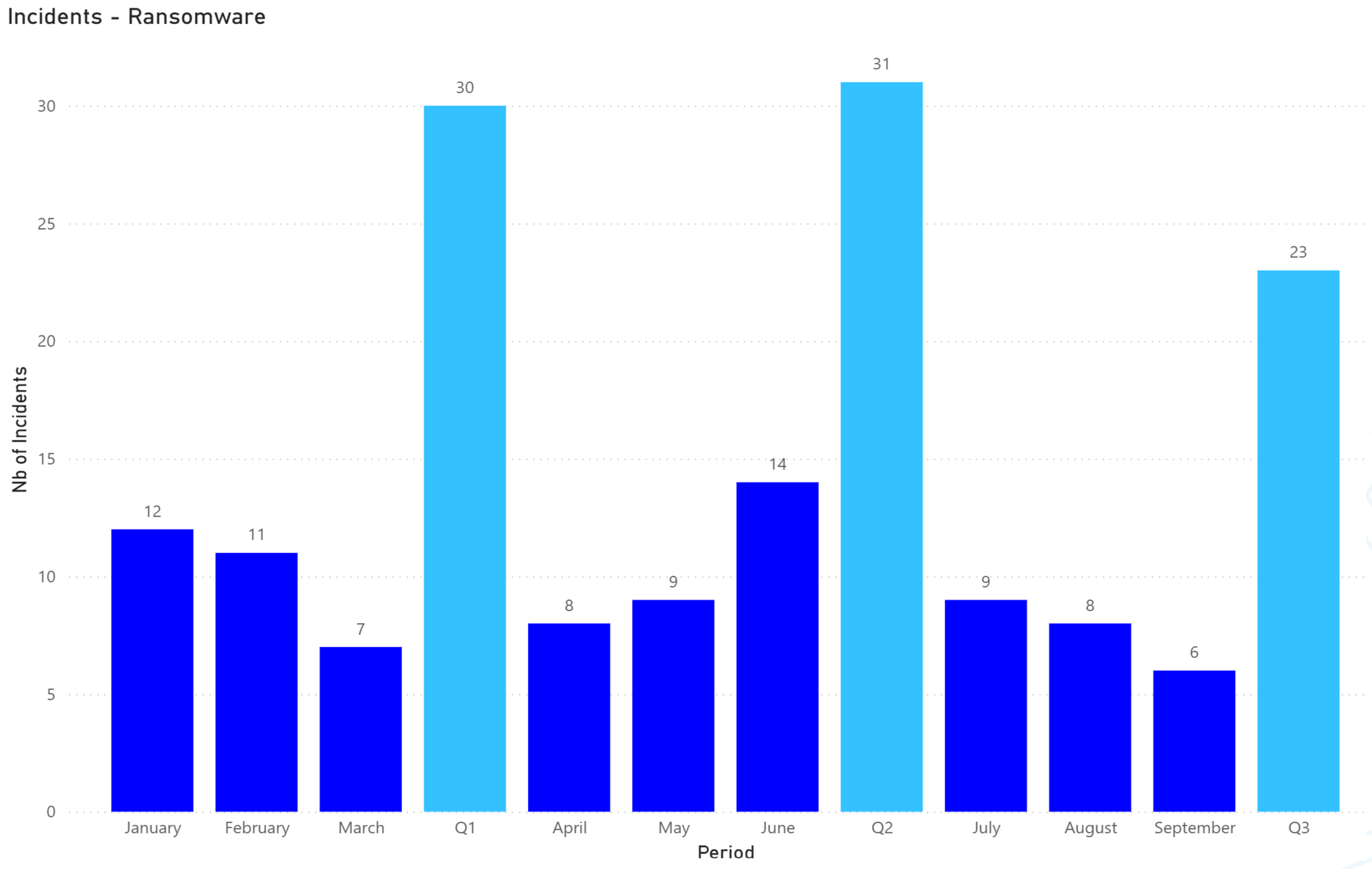


	Account Compromise	Ransomware (reported)	Denial of Service	Data Leak	Spear Phishing	Intrusion Attempt	Malware	System Compromise	Other
September	20	6	2	1	6	3	2	2	0
August	16	8	6	7	3	4	6	5	2
July	15	9	6	5	3	4	2	3	4

—

Ransomware

Ransomware attacks



Number of ransomware related notifications received in 2025

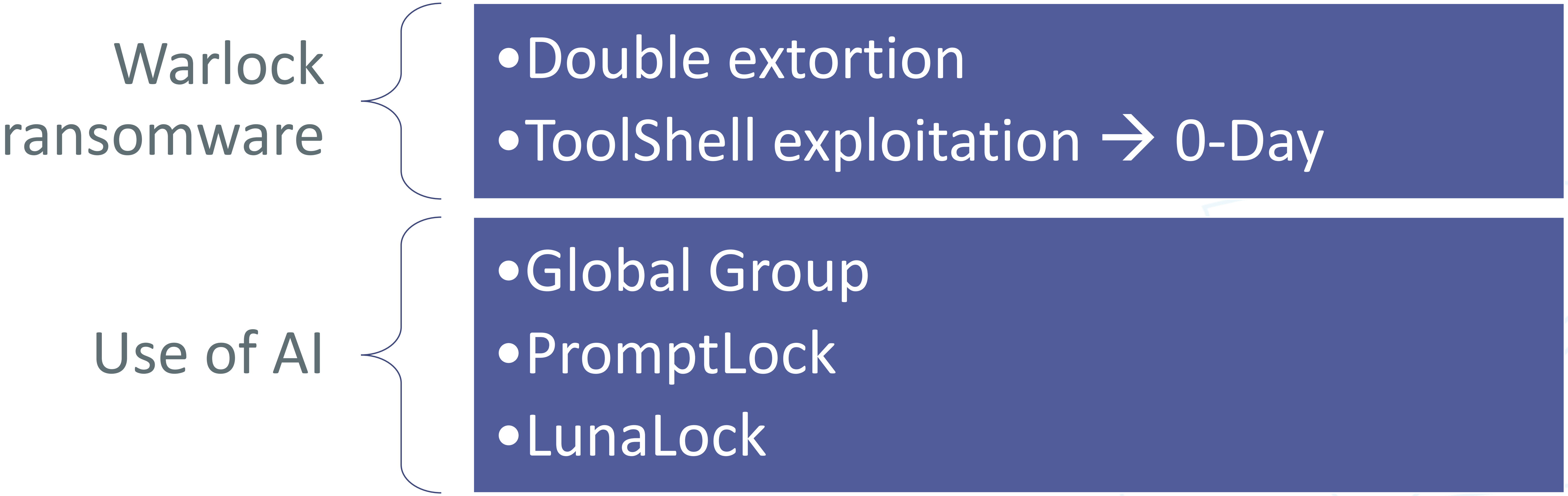
Top actors

- Qilin
- INC Ransom
- Warlock Group

Top sector

- Manufacturing

Ransomware new developments



Warlock ransomware

- Double extortion
- ToolShell exploitation → 0-Day

Use of AI

- Global Group
- PromptLock
- LunaLock

Recommendations - Ransomware

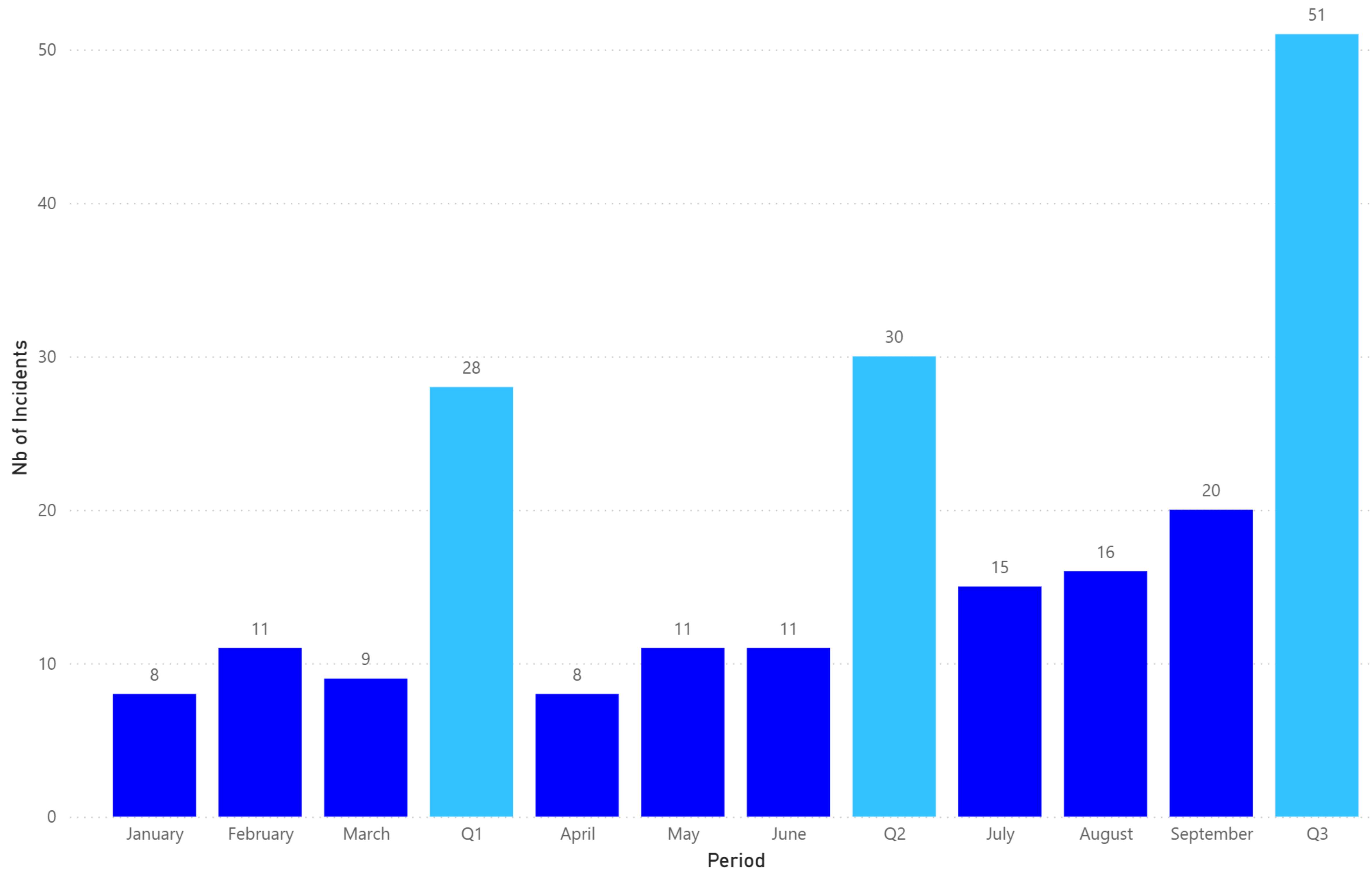
- Backups
  - 3-2-1 strategy
  - Reliability and integrity
  - Verification
- EDR on all devices
- Keep systems up to date

We have multiple reliable backups
Backups were also encrypted

Account Compromises

Account compromises

Incidents - Account Compromises



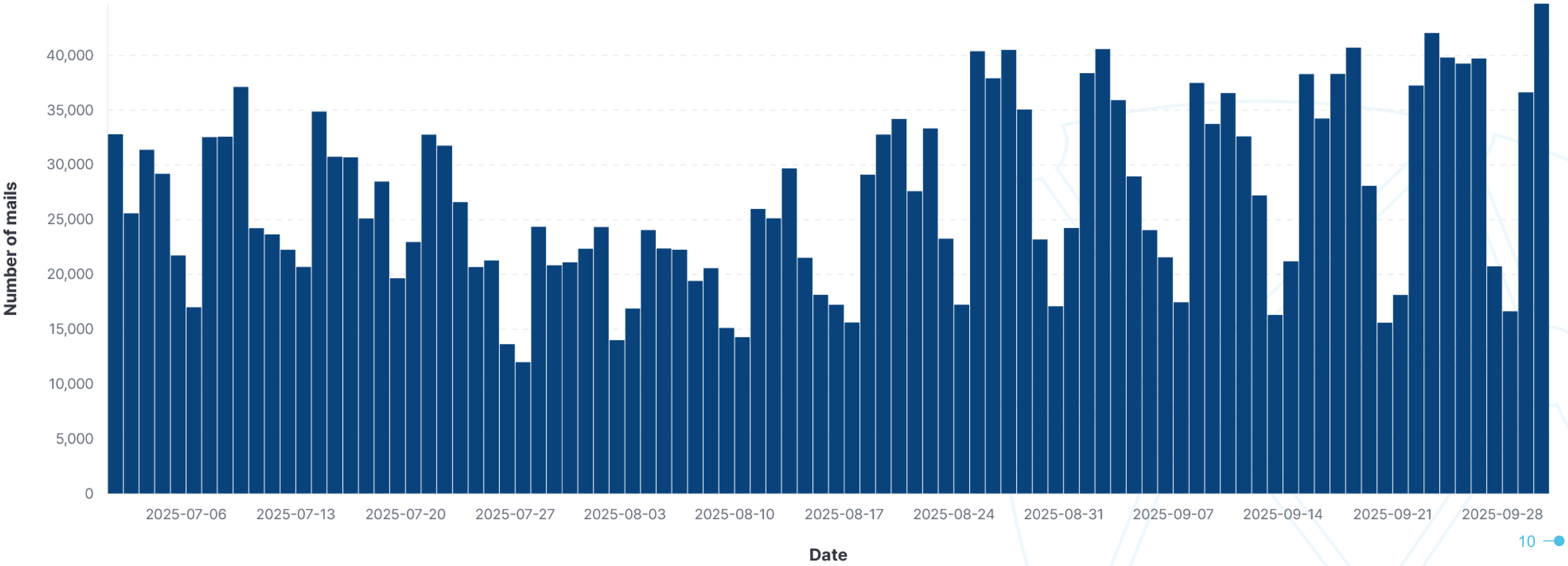
Impact

- Data leaks and exposures
- Service disruptions
- Financial fraud
- Launching further phishing campaigns
- Account compromise is a precursor stage in ransomware operations

TLP:CLEAR

Phishing – suspicious@safeonweb.be

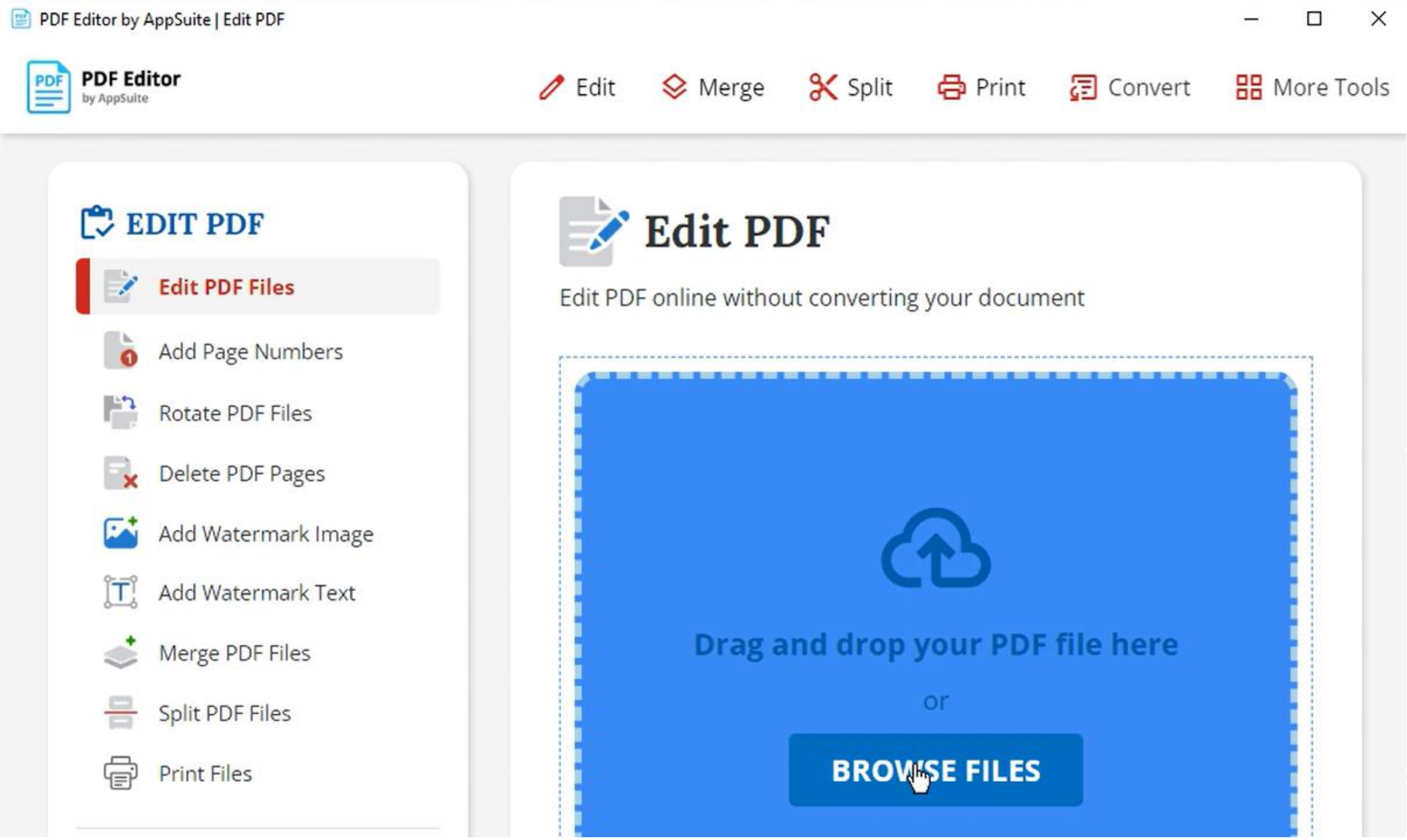
- 2,495,027 mails
- 46,147 unique URLs tagged as malicious
- 4,027 unique domains tagged as malicious



Infostealers

- Lumma
- Rhadamanthys
- Vidar
- Redline

Malicious PDF editor



- Google AD campaign in June + SEO poisoning
- Weaponized in late August
- Credential stealer
- Widely Spread

Recommendations – Account Compromise

- Multi-factor Authentication (MFA)
- Identity and Access Management
- Anomaly detection

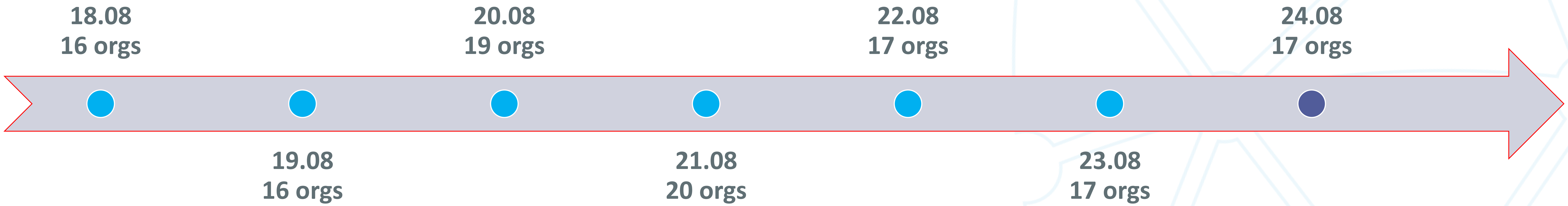
DDoS

DDoS

- Operation Eastwood coordinated by Europol targeted pro-Russian hacktivist group NoName057(16).
  - Between 14 and 17 July
  - Within 1 week, new C2 infrastructure was observed online, followed by new campaigns #FuckEastwood and #TimeOfRetribution were launched
  - Belgium July 25-27, 16 organisations were continuously targeted
    - Government, mobility, energy
    - Low impact

DDoS Campaign - #OpBelgium August 2025

- **Motivation**: The head of the European Commission received the President of Ukraine in Brussels.
- **Modus operandi:** high-volume DDoS attacks launched over extended periods of time.
- **Adversary**: an alliance of pro-Russian hacktivist groups (**NoName057(16)**, Z-ALLIANCE).
- **Victims**: **122 Belgian organisations** added to the list of targets **over 7 days**
  - “traditional” victims (federal and regional bodies, public institutions, ministries, and local municipalities);
  - other sectors: (ex. maritime, banking, energy, research, logistics, postal services, telecommunications, education, media);
- **Impact**: **low**
  - Many of the organisations were able to mitigate the impact by proactively implementing anti-DDoS measures.
  - CCB provided blocklists and recommendations



18.08
16 orgs

19.08
16 orgs

20.08
19 orgs

21.08
20 orgs

22.08
17 orgs

23.08
17 orgs

24.08
17 orgs

Recommendations - DDoS

- Cloud-based/CDN DDoS protection
- Rate-limit & Throttling
- Geofencing and IP blocking
- Firewalls
- Load balancers

Cyber Tips Webinar: DDoS Demystified

https://ccb.belgium.be/events/cyber-tips-ddos-demystified-how-stay-online

APT Activities

0-Days impacting BE

Sharepoint

- CVE-2025-53770
- CVE-2025-53771

Netscaler

- CVE-2025-5777
- CVE-2025-5349
- CVE-2025-6543

Cisco ASA

- CVE-2025-20333
- CVE-2025-20363
- CVE-2025-20362

New player to the party

- DoNot APT (APT-C-35/Origami Elephant)
  - India-linked cyberespionage group
  - European foreign ministries
  - Spear-phishing emails impersonating defense officials to deliver LoptikMod malware
- https://www.trellix.com/blogs/research/from-click-to-compromise-unveiling-the-sophisticated-attack-of-donot-apt-group-on-southern-european-government-entities/

—

Supply Chain

Supply Chain attacks

- Drift AI chatbot plug-in for Salesforce
    - Stolen OAuth tokens
- Collins Aerospace
    - Ransomware
    - Disruptions in several airports in Europe

CENTRE FOR
CYBERSECURITY
BELGIUM

Outlook

Outlook for Q4 2025

No significant changes expected in the coming quarter.

- Ransomware and account compromises will remain the main threats
- Small and medium-sized entities remain popular target
  - Phishing
  - Vulnerability exploitation
- Third party risk and supply chain
- Geopolitical tensions may further shape the cyber threat landscape.

TLP:CLEAR

CENTRE FOR
CYBERSECURITY
BELGIUM

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Rue de la Loi / Wetstraat 18 - 1000 Brussels

www.ccb.belgium.be

Contact: Intelligence@ccb.belgium.be

.be