

SECURITY SUMMIT

Security Summit

Milano 19-20-21 marzo 2024



Presentazione del Rapporto Clusit 2024

19 marzo 2024 orario 09.15 – 11.30



INTRODUZIONE

GABRIELE FAGGIOLI

**PRESIDENTE
CLUSIT**

2

Nunzia Ciardi

Vice Direttore Generale

ACN

3

Agenda

Apri i lavori e introduce: **Gabriele Faggioli**, Presidente Clusit

Ospite d'onore: **Nunzia Ciardi**, Vice Direttore Generale, ACN

Intervengono alcuni degli autori, moderati da **Alessio Pennasilico**, CS Clusit

- **Luca Bechelli**, CS Clusit – I contenuti del Rapporto Clusit 2024
- **Sofia Scozzari**, CD Clusit - Analisi Clusit dei principali attacchi a livello globale
- **Giorgia Dragoni**, Ricercatrice Senior, Oss. Cybersecurity & Data Protection Politecnico di Milano, Approfondimento Clusit sulla situazione in Italia
- **Gabriele Scialò**, Product Marketing Manager - Cybersecurity, Fastweb

Segue una tavola rotonda, moderata da **Alessio Pennasilico**, con gli esperti di security di alcuni dei principali fornitori di prodotti e servizi di Cyber Security, che arricchiranno il dibattito con le loro esperienze sul campo:

- **Andrea Negroni**, Aruba, Hewlett Packard Enterprise company
- **Aldo Di Mattia**, Fortinet
- **Luca Nilo Livrieri**, CrowdStrike
- **Stefano Longo**, Microsoft
- **Maurizio Taglioretti**, Netwrix



I CONTENUTI DEL RAPPORTO

LUCA BECHELLI

COMITATO SCIENTIFICO
CLUSIT

5



I contenuti del Rapporto

Analisi Clusit degli incidenti di sicurezza più significativi avvenuti a livello globale (Italia inclusa) nel 2023.

- Attacchi rilevati in Italia dal Security Operations Center (SOC) di FASTWEB.
- Rilevazioni e segnalazioni della Polizia Postale e delle Comunicazioni, rispetto ad attività ed operazioni svolte nel corso degli ultimi 12 mesi.
- **Settore FINANCE:** un'analisi sul Cyber-crime nel settore finanziario in Europa, a cura di IBM.
- **Cybersecurity in Sanità:** Tra Aumento degli Attacchi e Innovazioni Normative e Tecnologiche, realizzato dalle Women for Security.

Survey realizzata da Netwrix, che ha intervistato 1.610 professionisti IT provenienti da 106 paesi, sulle tendenze della Hybrid Security



I contenuti del Rapporto: Focus On

- Il mondo della **sicurezza delle Identità**, a cura di RSA Security Italia
- Attività della **Task Force** Cisco Talos in difesa dell'Ucraina, a cura di Cisco
- Secure Access Service Edge (**SASE**), a cura di Fortinet
- **Cloud adoption e superficie d'attacco**: aumentare la visibilità e la protezione contro gli attacchi nell'infrastruttura e nelle applicazioni Cloud adoption e superficie d'attacco cloud, a cura di CrowdStrike
- Costruire la **cyber resilience per la Space Economy**, a cura di Federica Maria Rita Livelli
- **CSIRT Network**: Incident Response per una Crisis Management di successo in un Contesto Internazionale, a cura di NTT Data
- **Intelligenza Artificiale e Automazione**: le chiavi per rivoluzionare il SOC, a cura di PaloAlto Networks
- La Sicurezza dei sistemi di acquisizione e stampa, a cura di ASSOIT
- Attraverso il tunnel del cambiamento: **l'evoluzione della connessione sicura da VPN a ZTNA**, a cura di HPE Aruba Networking
- Strategie di **data security nell'era dell'AI Generativa**, a cura di Microsoft
- Sviluppo sicuro del **codice software**, a cura di Roberto Obialero



ANALISI CLUSIT DEI PRINCIPALI ATTACCHI A LIVELLO GLOBALE

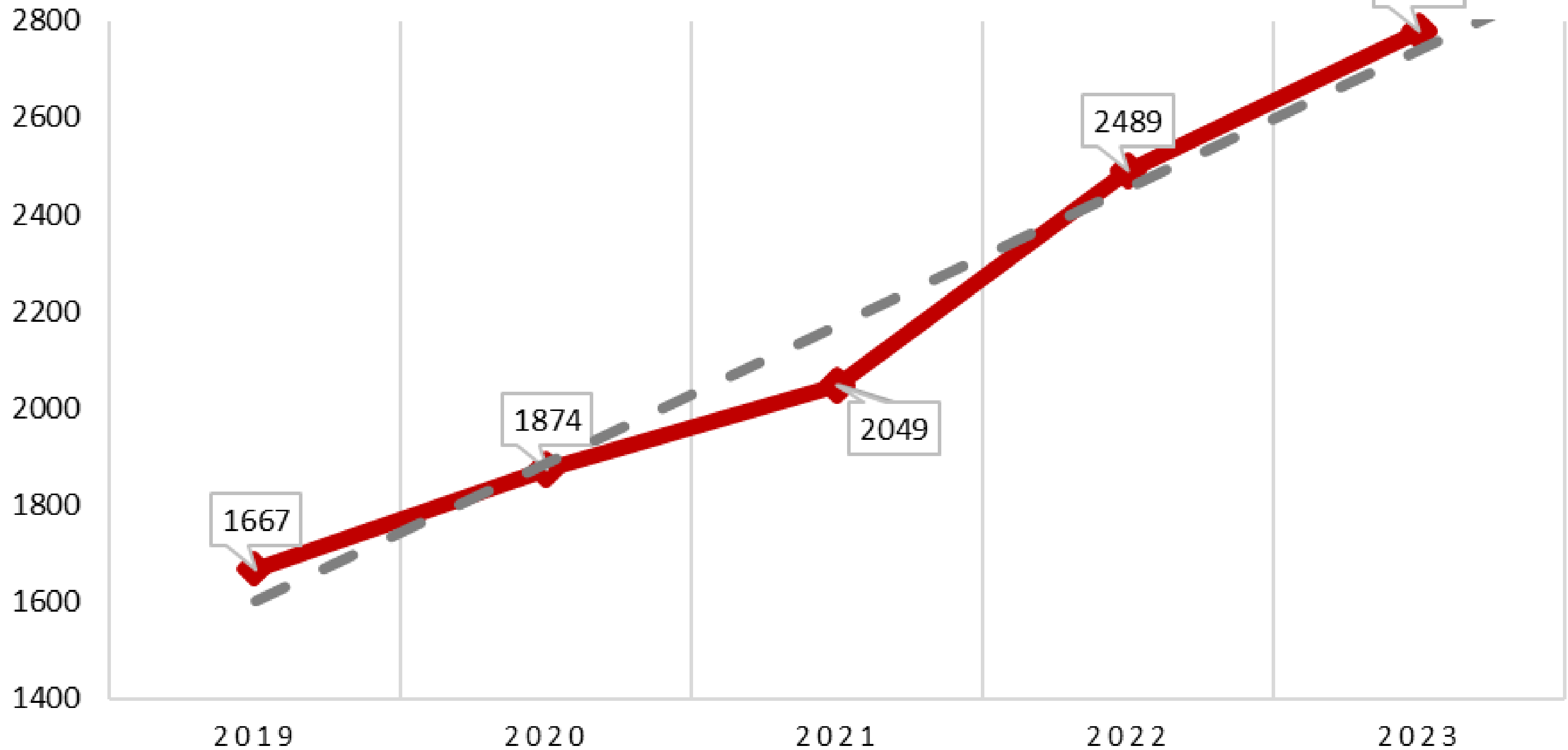
SOFIA SCOZZARI

COMITATO DIRETTIVO
CLUSIT

8



ATTACCHI PER ANNO 2019 - 2023



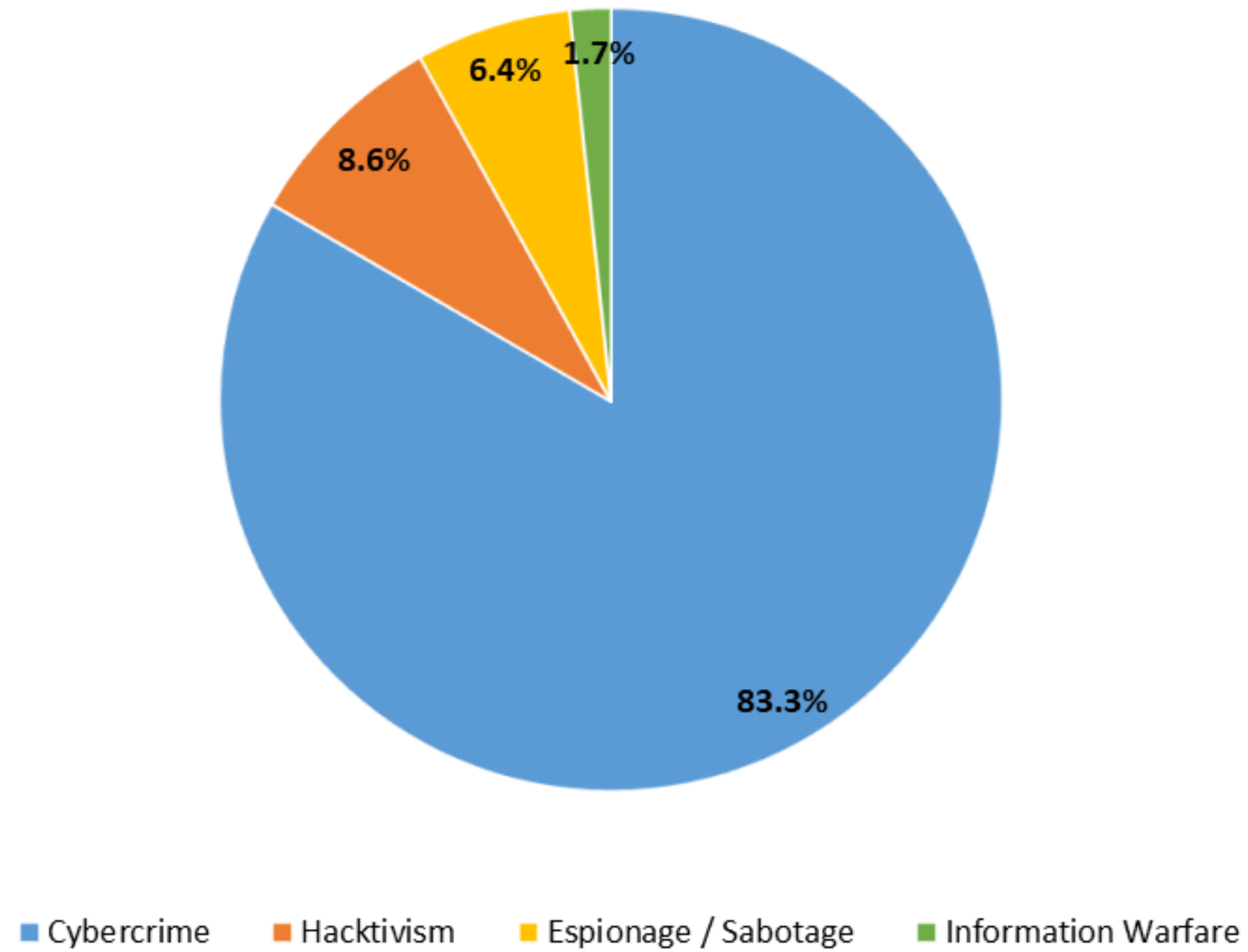
© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

+12%
È la crescita degli incidenti dal 2022 al 2023

56%
Degli incidenti censiti dal 2011 sono avvenuti negli ultimi 5 anni



TIPOLOGIA E DISTRIBUZIONE ATTACCANTI 2023



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia



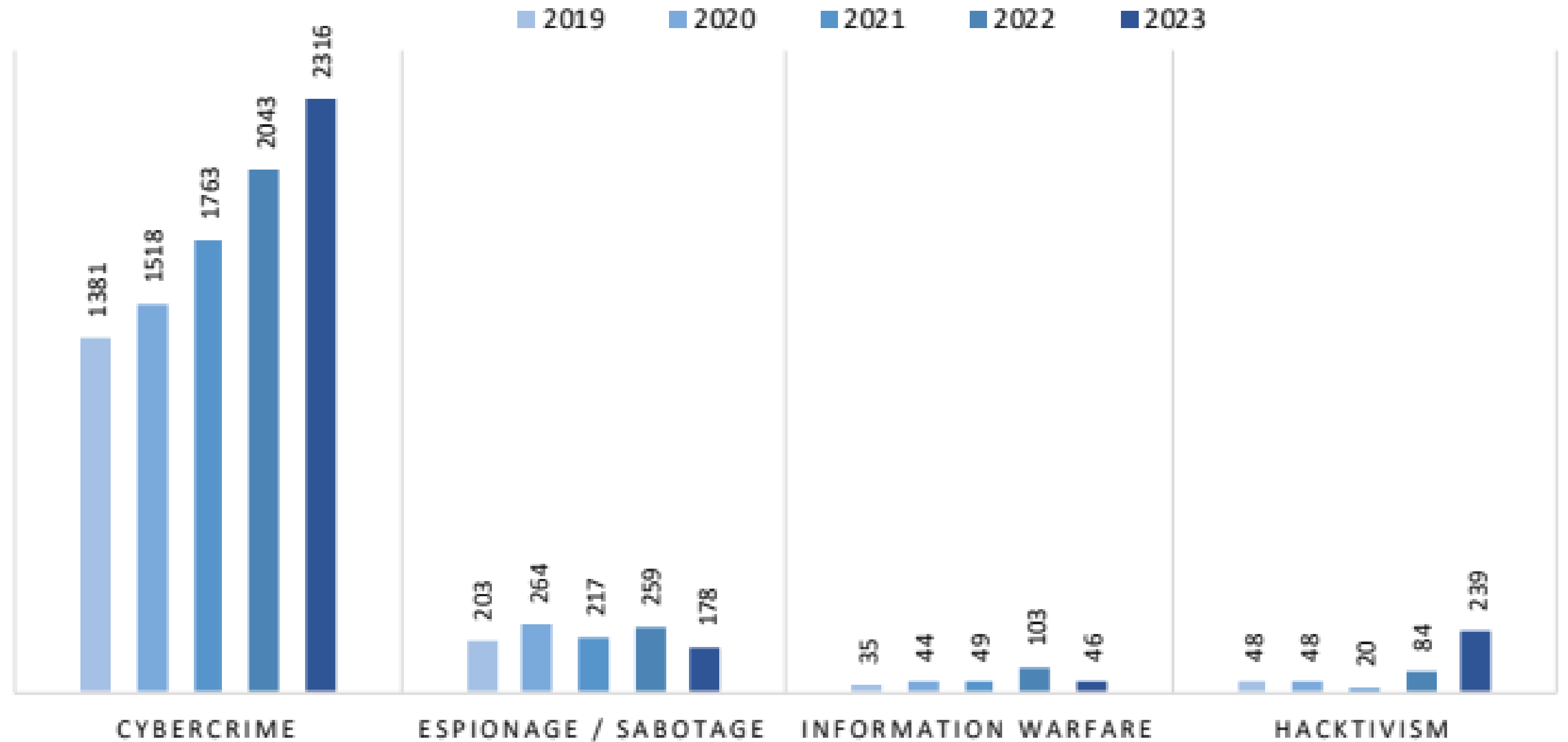
+13%

È la crescita
degli incidenti causati
dal Cybercrime nel
2023

1 su 10

è un incidente con
matrice Warfare o
Hacktivism

ATTACCANTI 2019 - 2023



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia



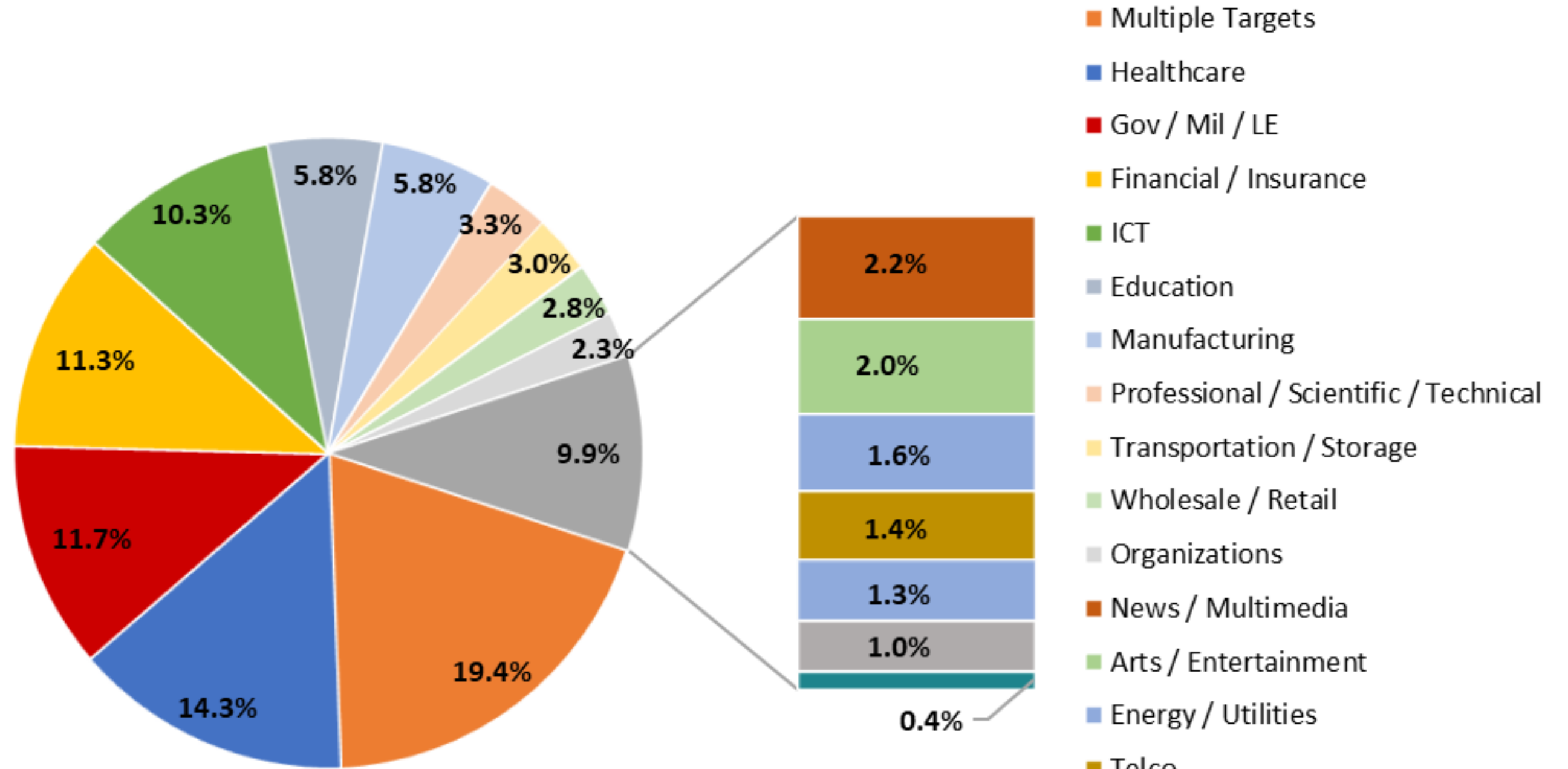
DISTRIBUZIONE DELLE VITTIME 2023

+30%
 È la crescita del numero degli incidenti a danno del settore HealthCare

+50%
 gli incidenti al settore GOV negli ultimi 5 anni

+62%
 è la crescita degli incidenti a danno dei settori Financial/Insurance

+25%
 è la crescita degli incidenti a danno del settore Manufacturing



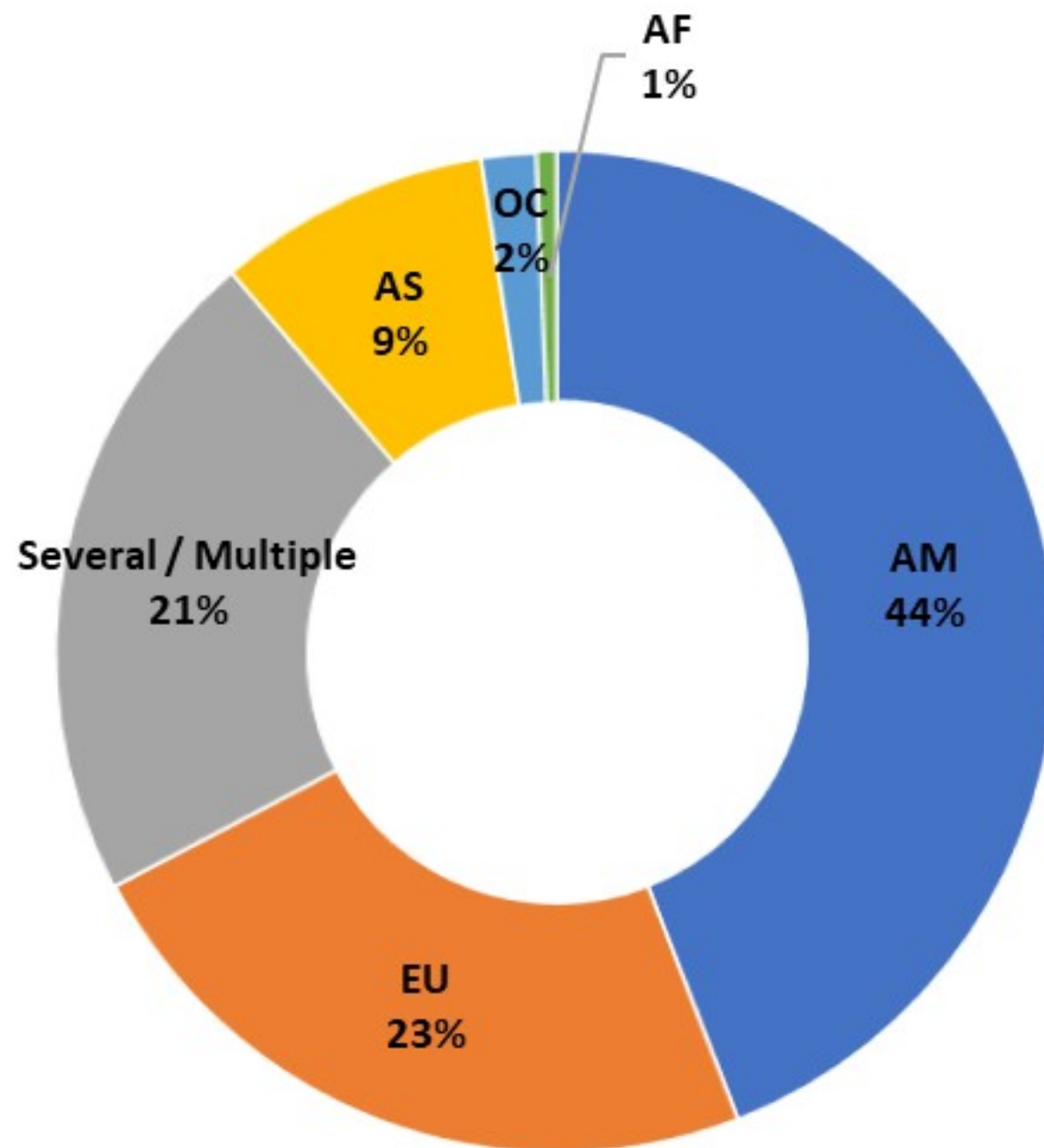
© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia



+7,5%

è la crescita degli incidenti avvenuti nel continente Europeo

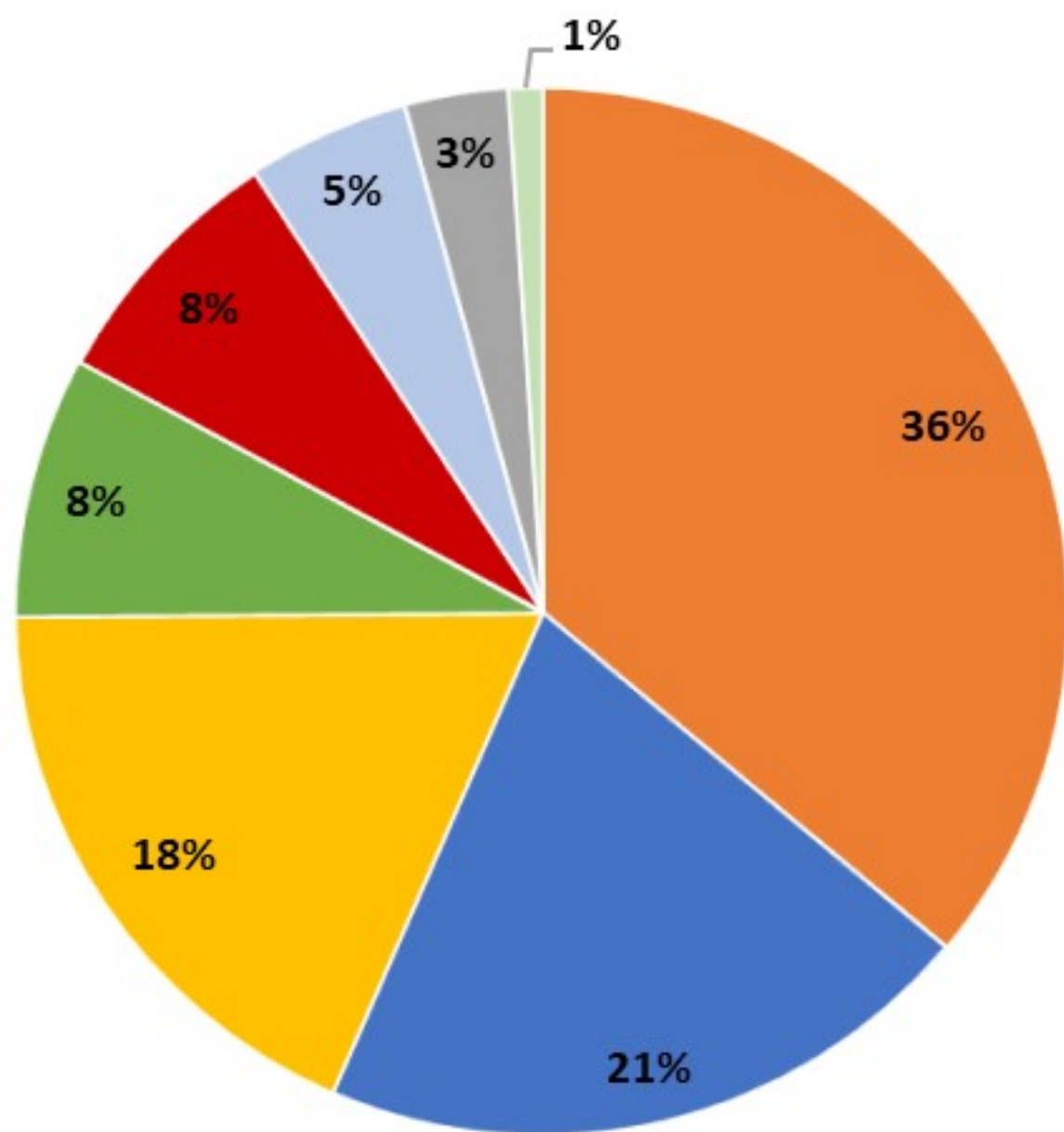
GEOGRAFIA DELLE VITTIME 2023



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia



DISTRIBUZIONE DELLE TECNICHE 2023



- Malware
- Unknown
- Vulnerabilities
- Phishing / Social Engineering
- DDoS
- Multiple Techniques
- Identity Theft / Account Cracking
- Web Attack

+75,9%

è la crescita degli attacchi basati su vulnerabilità note e 0-day

+98%

È la crescita del numero degli incidenti DDOS

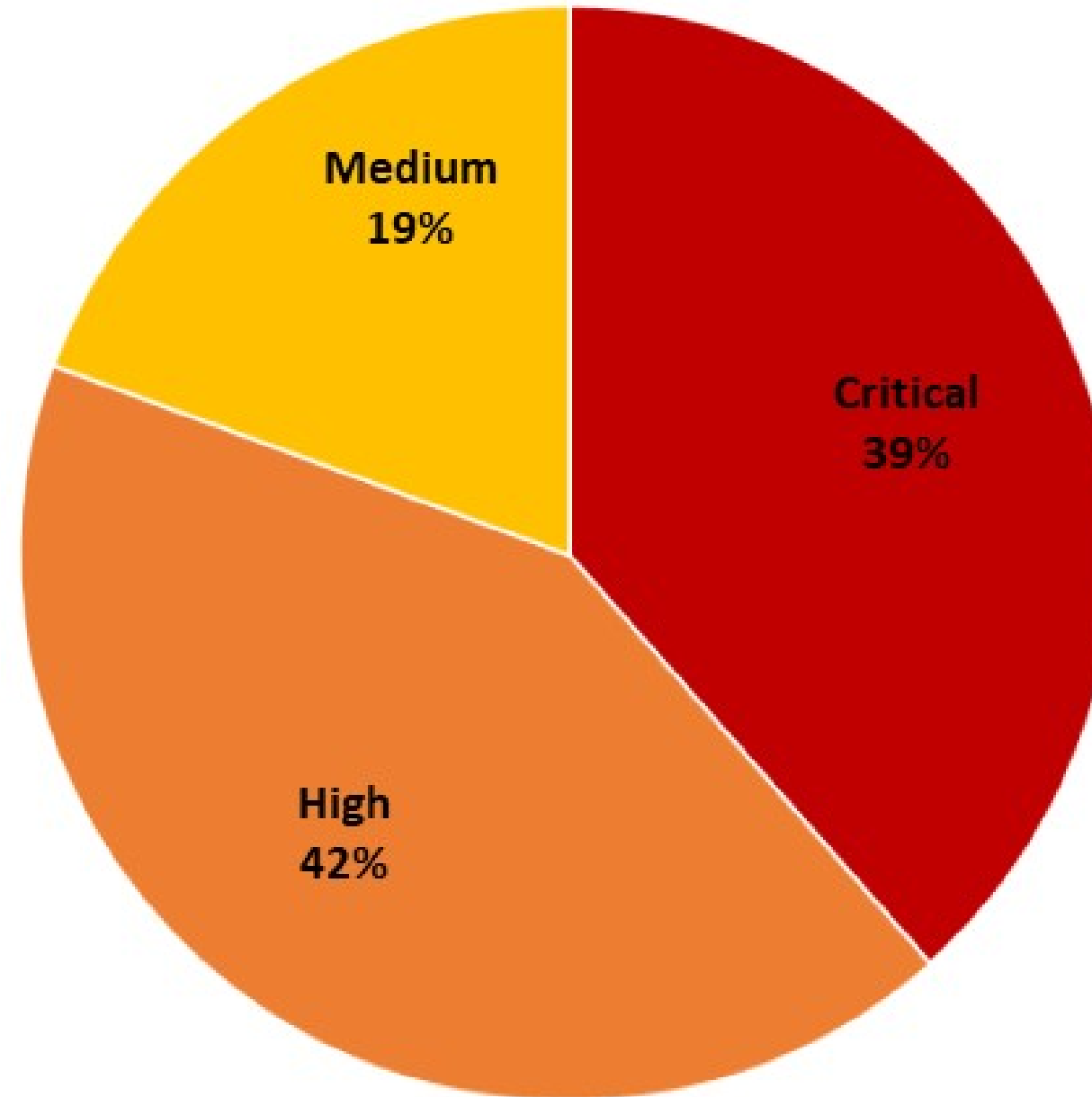
© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia



SEVERITY ATTACCHI 2023

4 su 5

*sono i casi in cui,
quando avvengo, gli
incidenti causano la
massima Severity
(Critical o High)*

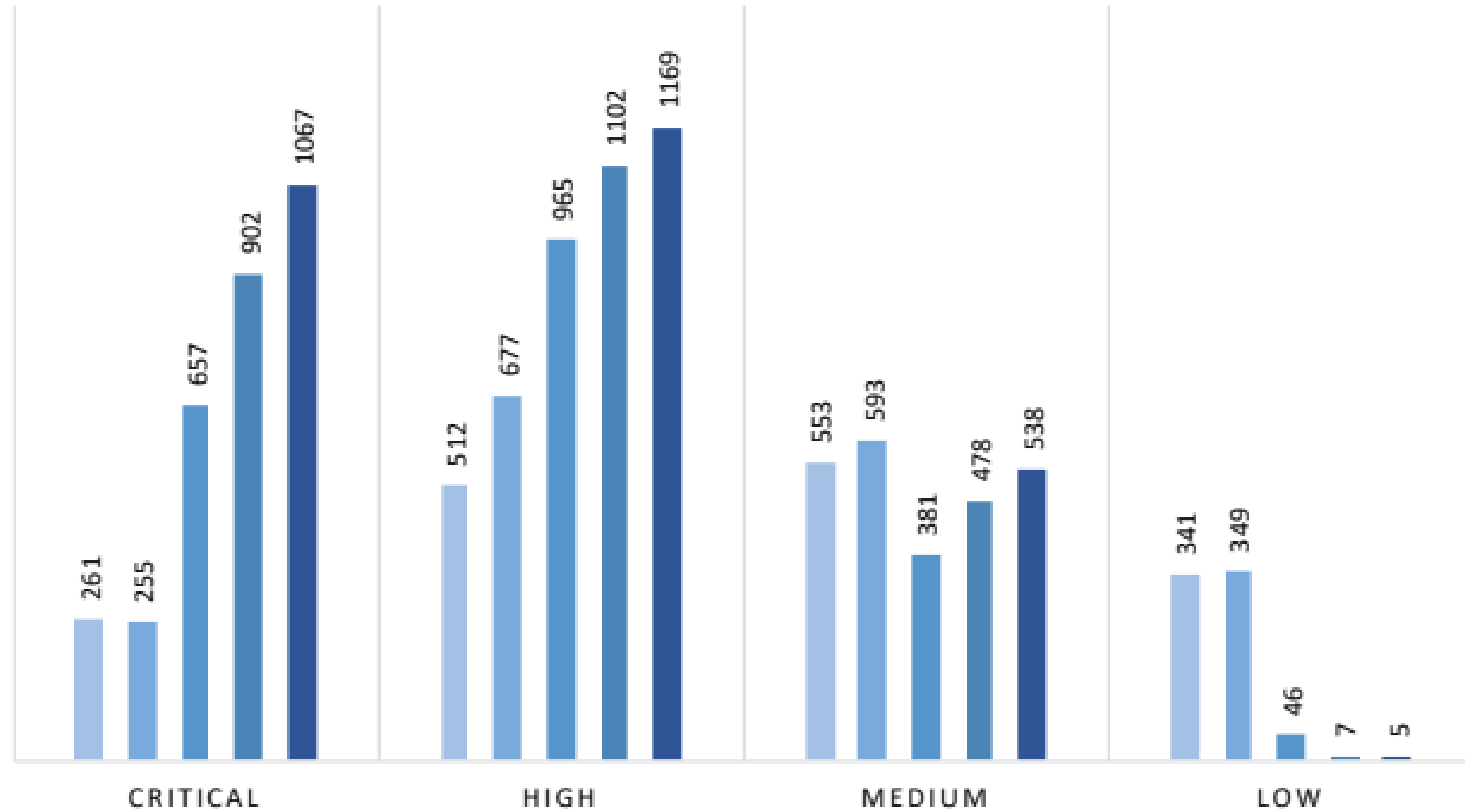


© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia



SEVERITY 2019 - 2023

■ 2019 ■ 2020 ■ 2021 ■ 2022 ■ 2023



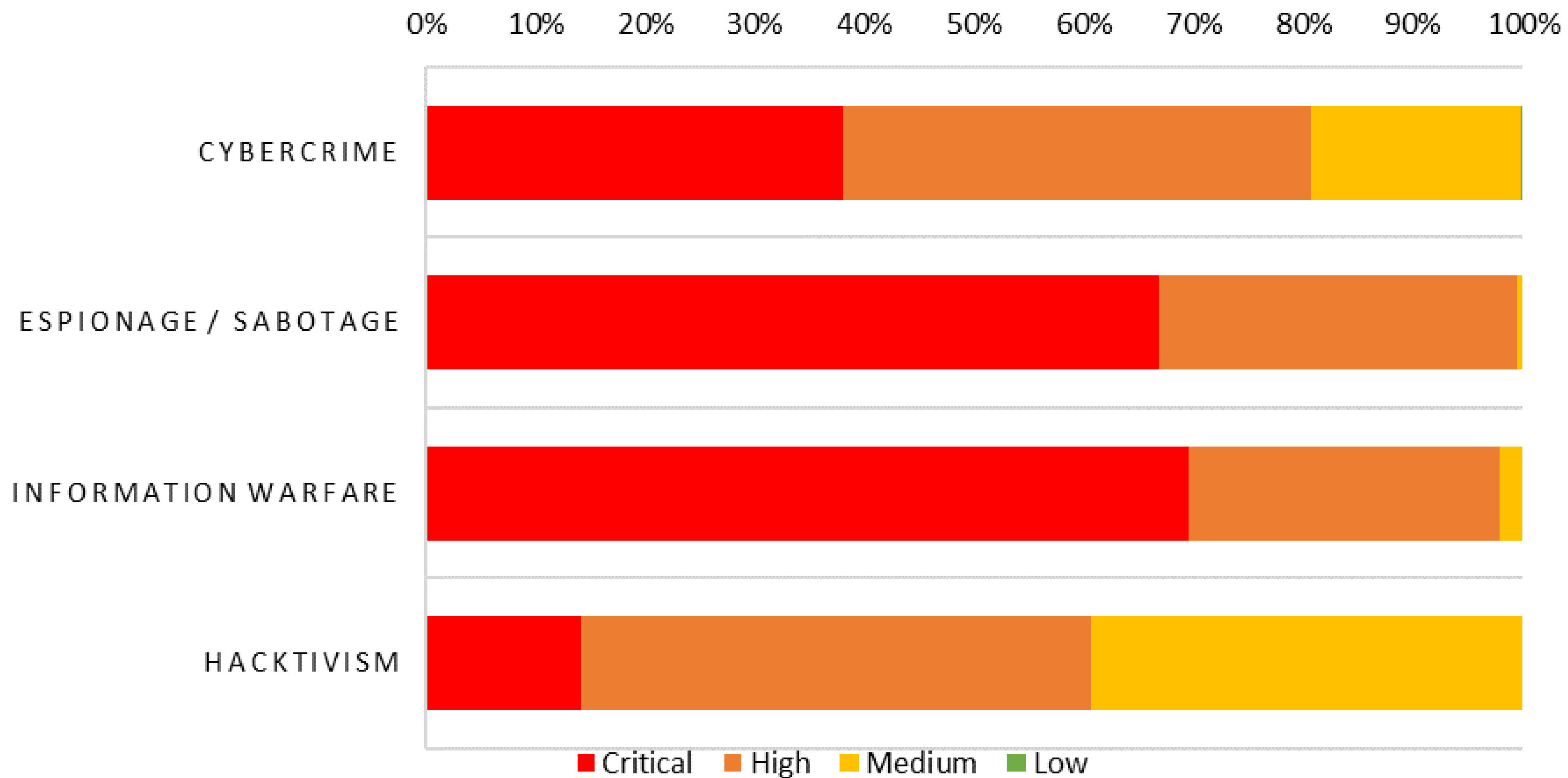
© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia



-39,6%

è la riduzione degli incidenti di severità Critical per attacchi di Hacktivism

SEVERITY PER ATTACCANTI 2023



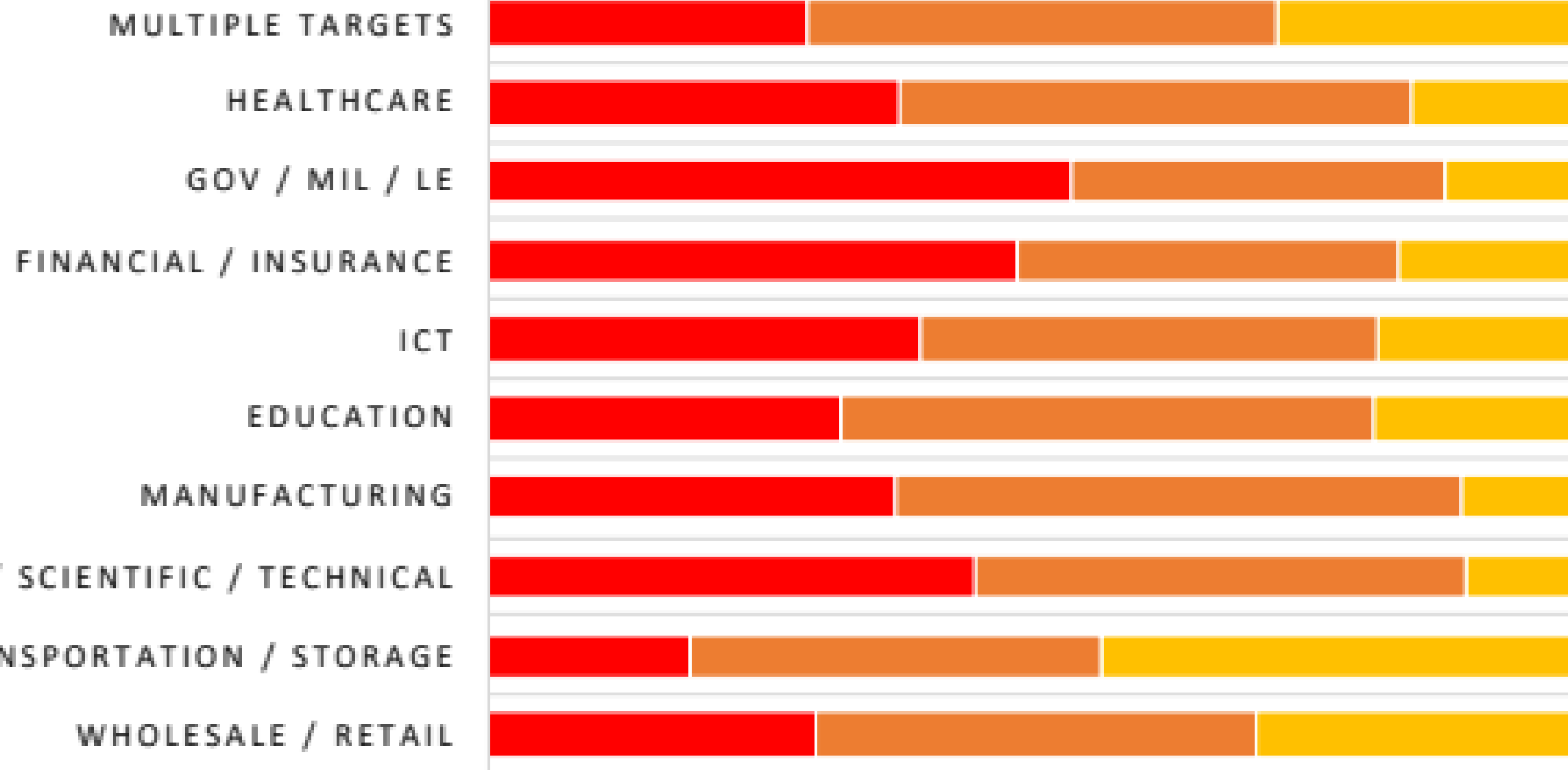
© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia



SEVERITY PER TOP10 VITTIME 2023

■ Critical ■ High ■ Medium ■ Low

0% 20% 40% 60% 80% 100%



53,2%
degli attacchi ai settori GOV/MIL/LE determinano i massimi impatti

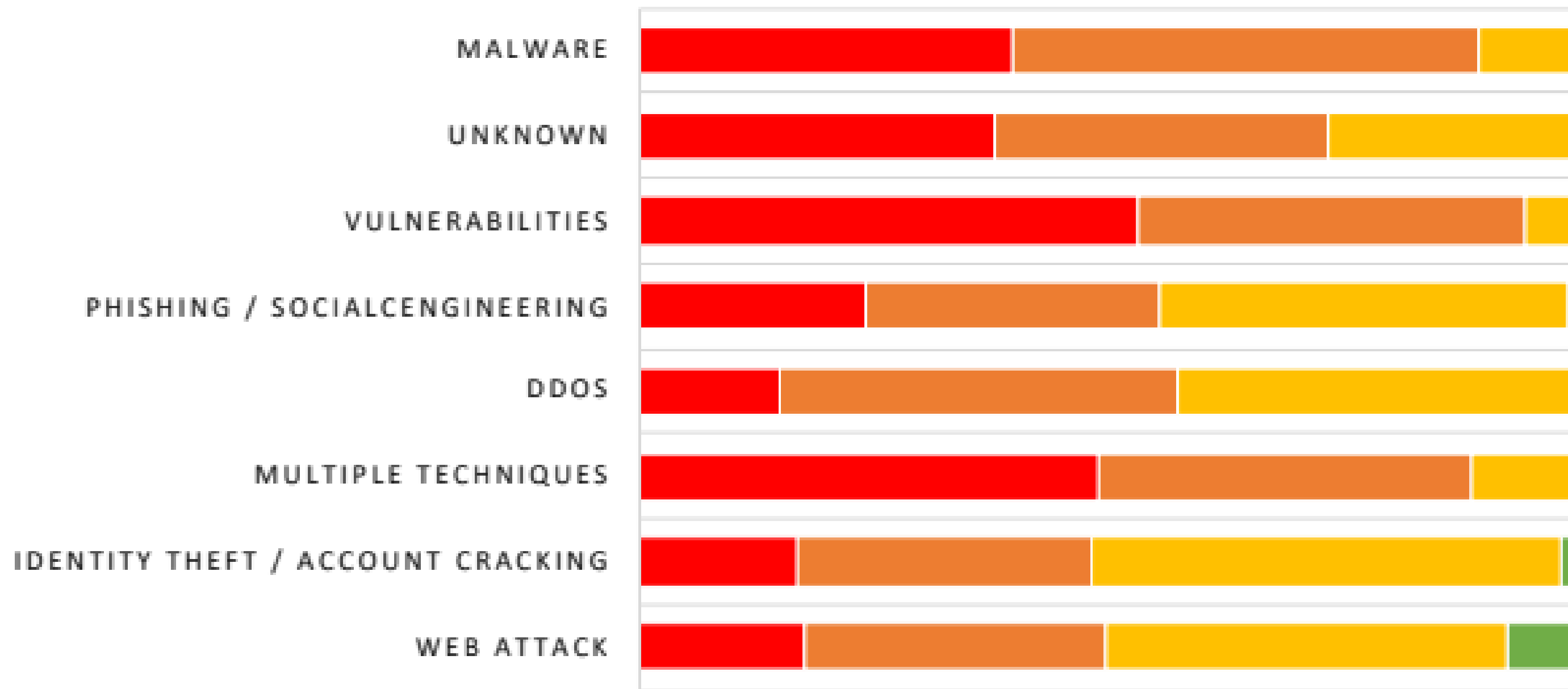
© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia



SEVERITY PER TECNICHE 2023

■ Critical ■ High ■ Medium ■ Low

0% 20% 40% 60% 80% 100%



+10%

la crescita di eventi a
severity «Critical»
di incidenti Malware

© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia



APPROFONDIMENTO **CLUSIT** SULLA SITUAZIONE **IN ITALIA**

GIORGIA DRAGONI

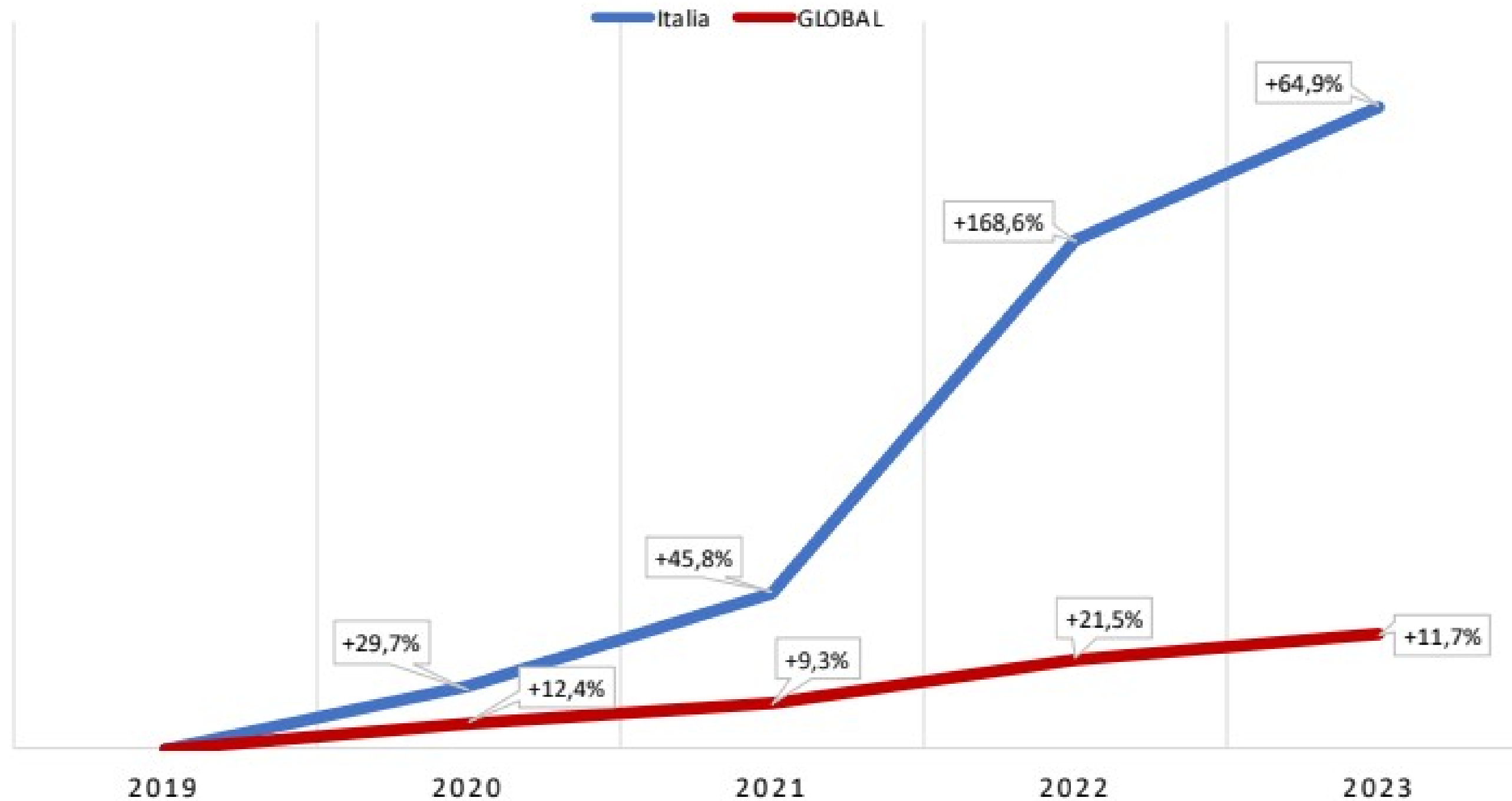
RICERCATRICE SENIOR

OSSERVATORIO CYBERSECURITY & DATA PROTECTION POLITECNICO DI
MILANO

2
1



CONFRONTO CRESCITA % ITALIA VS GLOBAL



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

+65%

è la crescita degli incidenti informatici in Italia nel 2023

11,2%

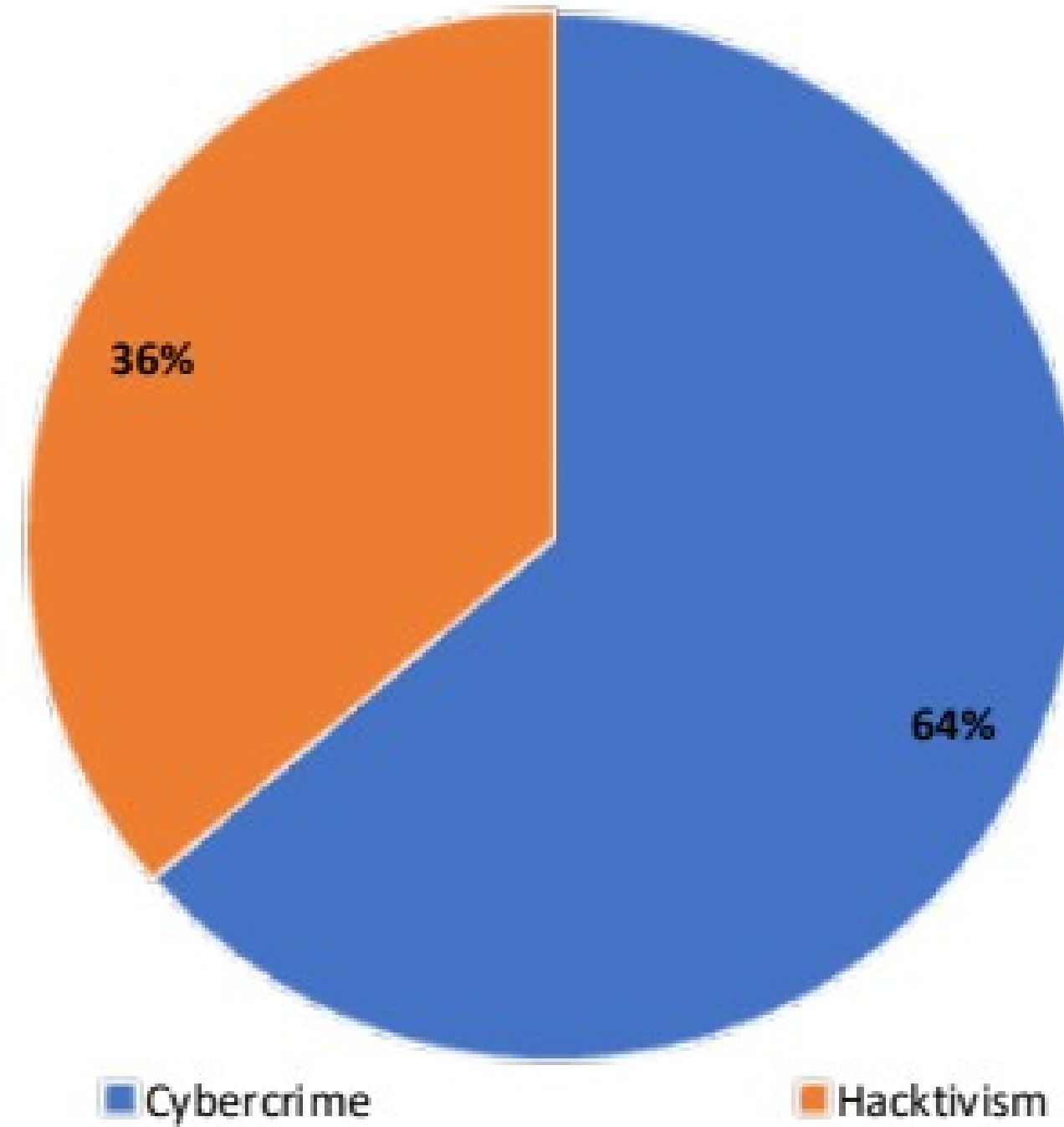
è la quantità di incidenti censiti in Italia rispetto al resto del mondo



ATTACCANTI IN ITALIA 2023

47%

*degli attacchi di
Hacktivism a livello
Global, è avvenuto
a danni dell'Italia*



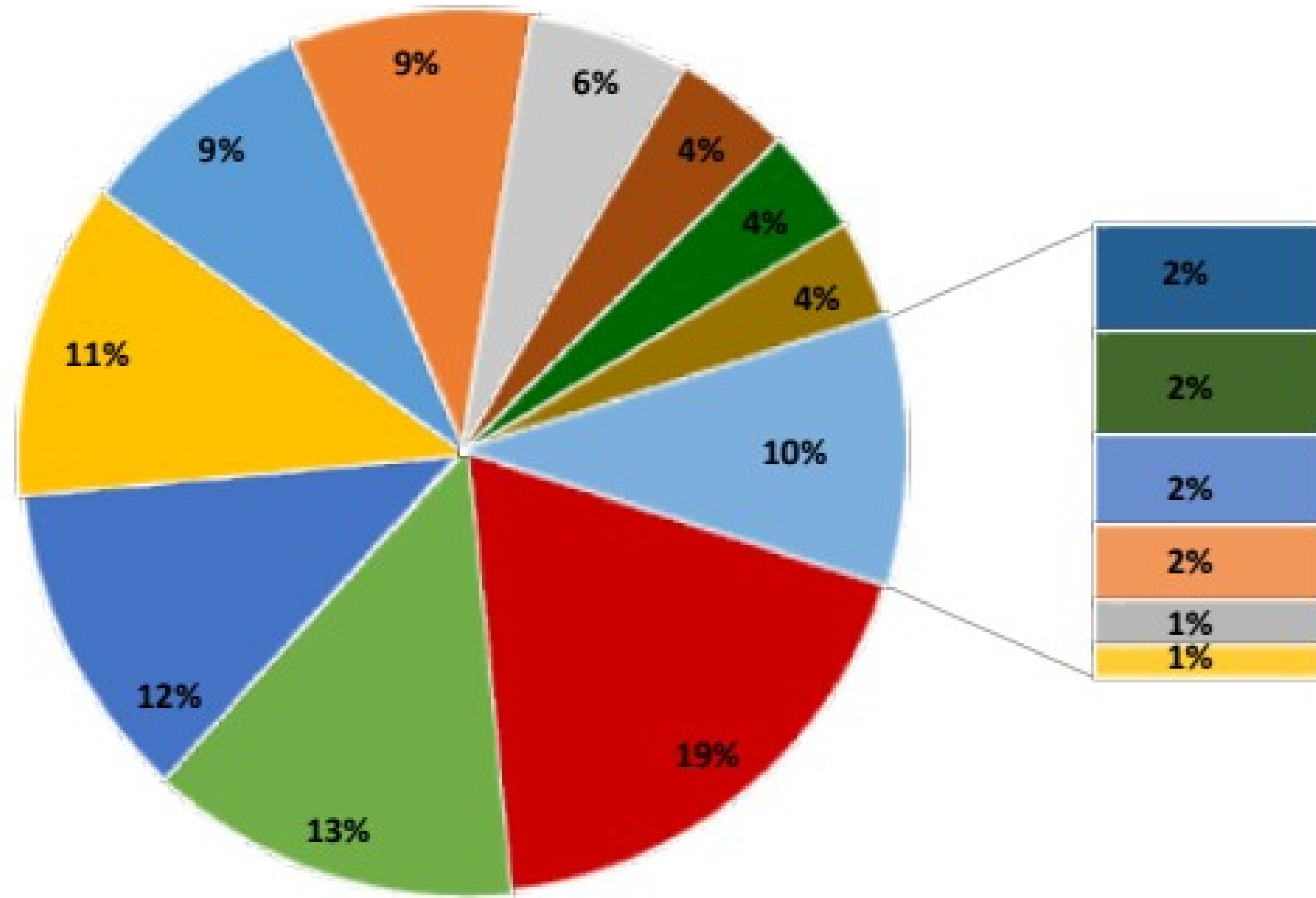
VITTIME IN ITALIA 2023

1° GOV/MIL/LE

il settore più attaccato in Italia nel 2023

2° Manufacturing

al secondo posto, in continuità con il passato



+50%

gli incidenti al settore GOV/MIL/LE in Italia nel 2023

+286%

è la crescita degli incidenti in Italia subiti da Financial/Insurance

- Gov / Mil / LE
- Financial / Insurance
- Professional / Scientific / Technical
- News / Multimedia
- Manufacturing
- Wholesale / Retail
- Organizations
- Other Services
- Transportation / Storage
- ICT
- Energy / Utilities
- Construction
- Multiple Targets
- Healthcare
- Telco
- Hospitability



TECNICHE DI ATTACCO IN ITALIA 2023

DDoS

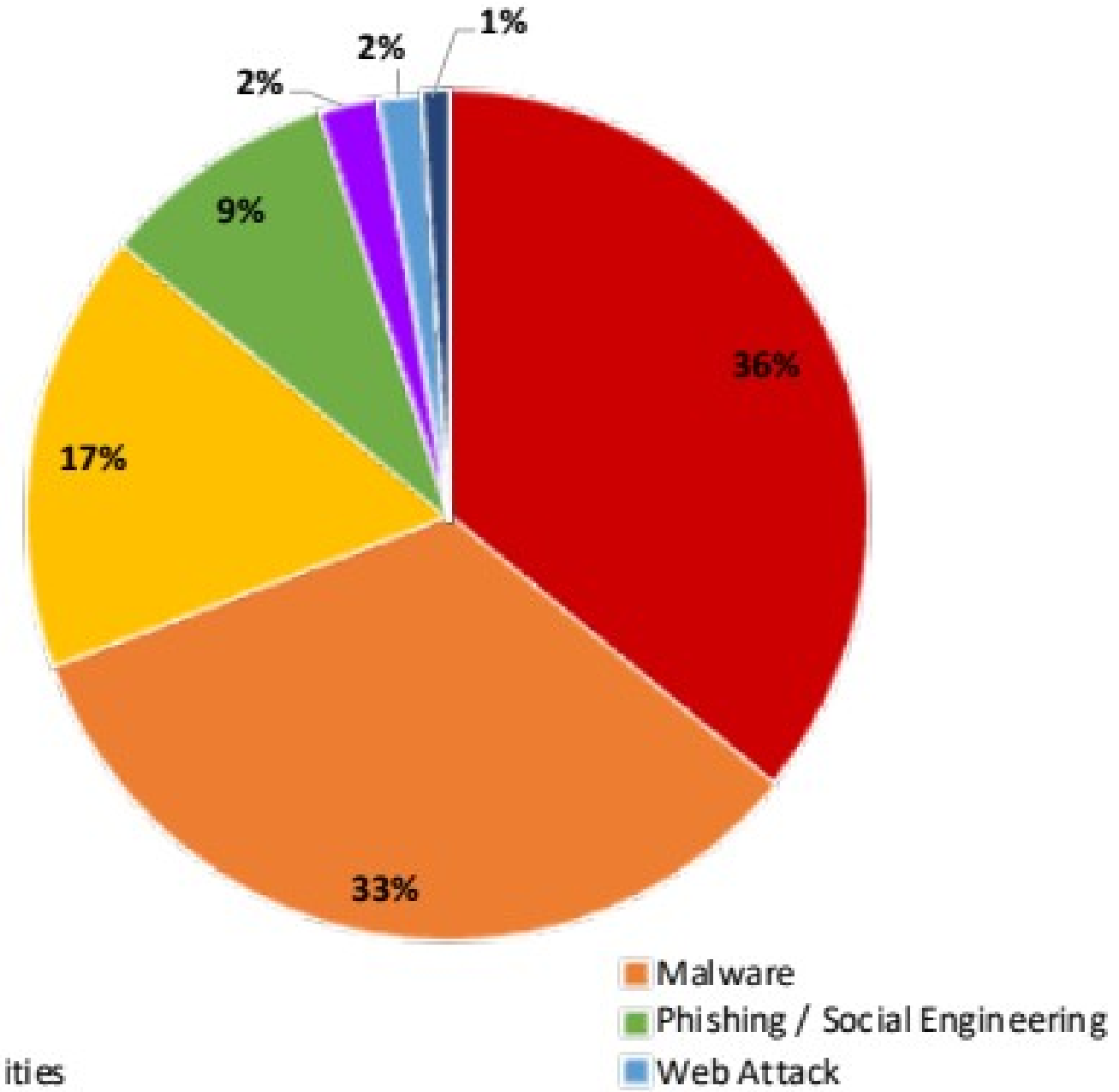
*è la principale
tecnica di attacco
in Italia*

+4%

*è la crescita degli
attacchi basati su
Malware in Italia*

+87%

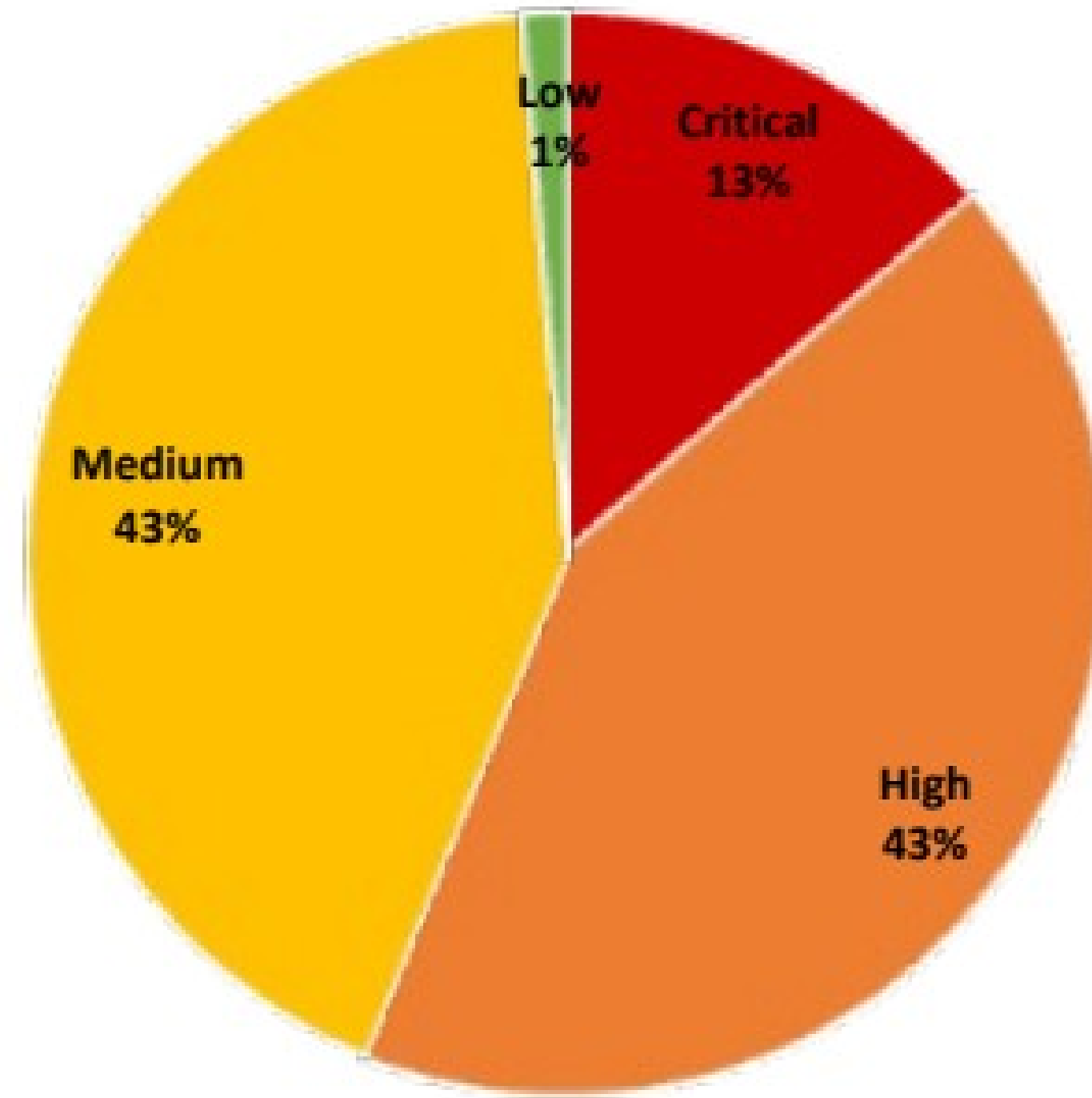
*è la crescita degli
attacchi phishing e
social engineering
in Italia*



© Clusit - Rapporto 202 sulla Sicurezza ICT in Italia



SEVERITY IN ITALIA 2023



+53%

*di attacchi con
severity High in
Italia, nel 2023*

© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia



Take away

- Rafforzare la governance della sicurezza e la capacità di identificare, analizzare, valutare e gestire i rischi
- Sviluppare una cultura della sicurezza che sia parte del patrimonio di conoscenze di tutti i cittadini, a partire dalle nuove generazioni
- Governance dei processi di patch & vulnerability management
- Presidio continuo della sicurezza di prodotti e servizi lungo l'intero ciclo di vita (SSDLC - Secure Software Development LifeCycle)
- Gestione dei processi di sourcing e delle terze parti (anche in ottica ESG)
- Backup & Disaster Recovery & Continuità Operativa
- Rafforzamento della sicurezza del mondo OT
- Prepararsi alla gestione degli incidenti e delle crisi
- Utilizzo dell'AI per «contrastare» la AI
- Ridurre la frammentazione di infrastrutture e servizi



ANALISI **FASTWEB**

DELLA SITUAZIONE ITALIANA IN MATERIA DI CYBERCRIME

GABRIELE SCIALO'

PRODUCT MARKETING MANAGER - FASTWEB

2
8



Oltre 56 Milioni di Eventi di Cybersicurezza Aumenta significativamente la gravità degli attacchi



Attacchi **DDoS** ad alto impatto

+32%

Oltre 100Gbps di banda impiegata



Aggregati mensili di **banda** impiegata in **attacchi DDoS**

+72%

Con un picco nell'ultimo trimestre

Migliora la **capacità difensiva** delle organizzazioni grazie all'**aumentata consapevolezza dei rischi informatici**



-8%

38.000 Server che espongono su internet **servizi critici**



Infezioni **Malware & Botnet**

-3%

Nuove tecnologie che sfruttano l'**Intelligenza Artificiale Generativa** contribuiscono a...

Rafforzare ed espandere le difese



Rilevazione falsi positivi

-70%

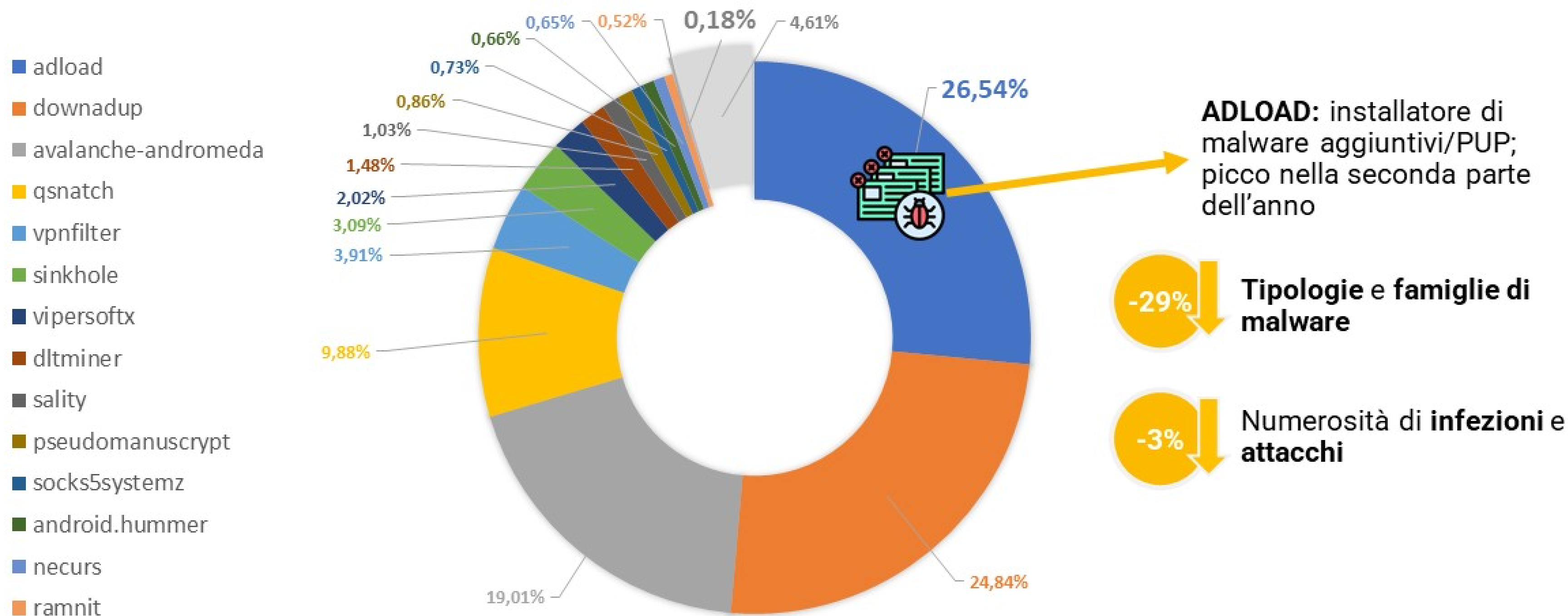
Rendere più efficaci gli attacchi



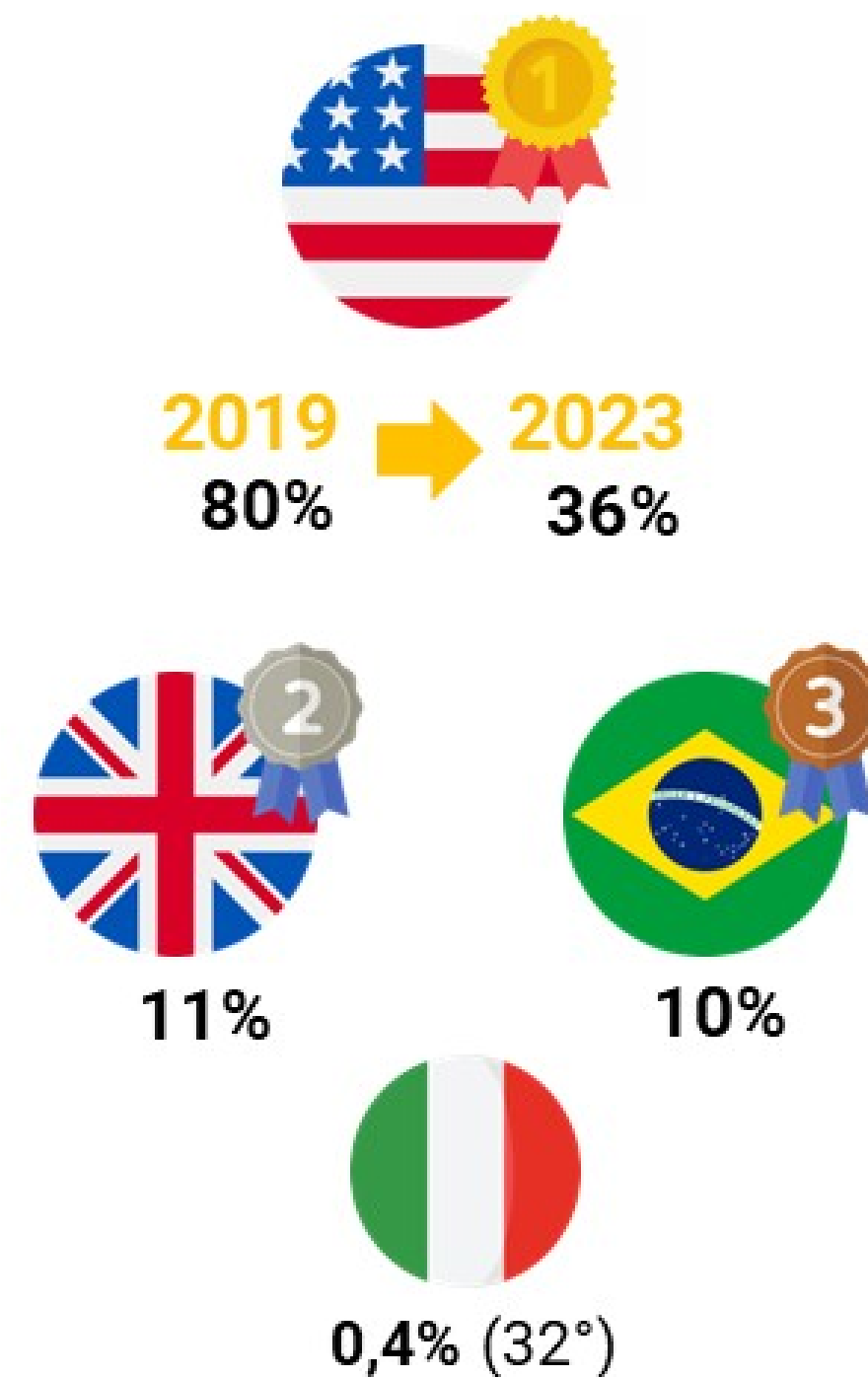
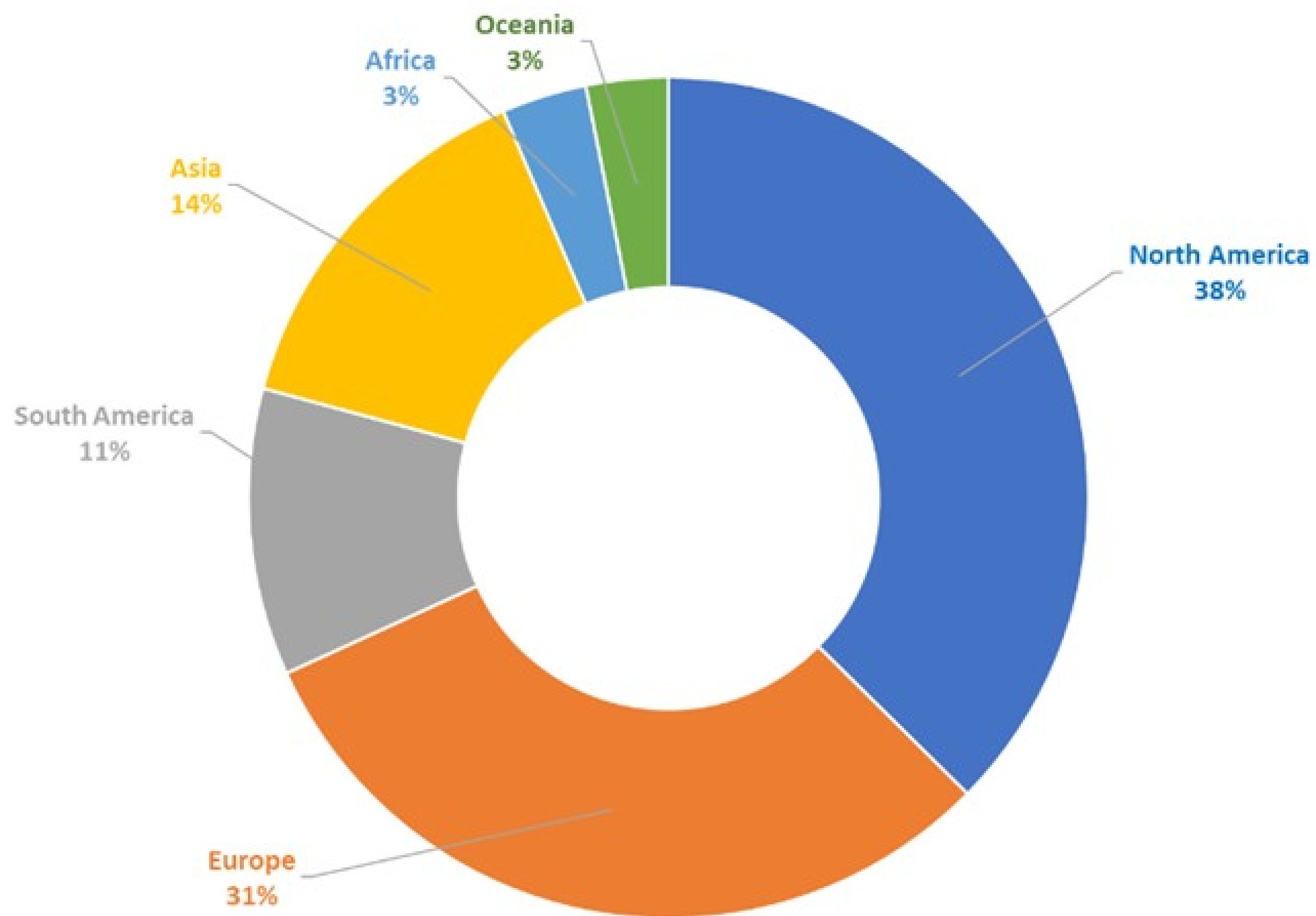
Credential Phishing via email

+87%

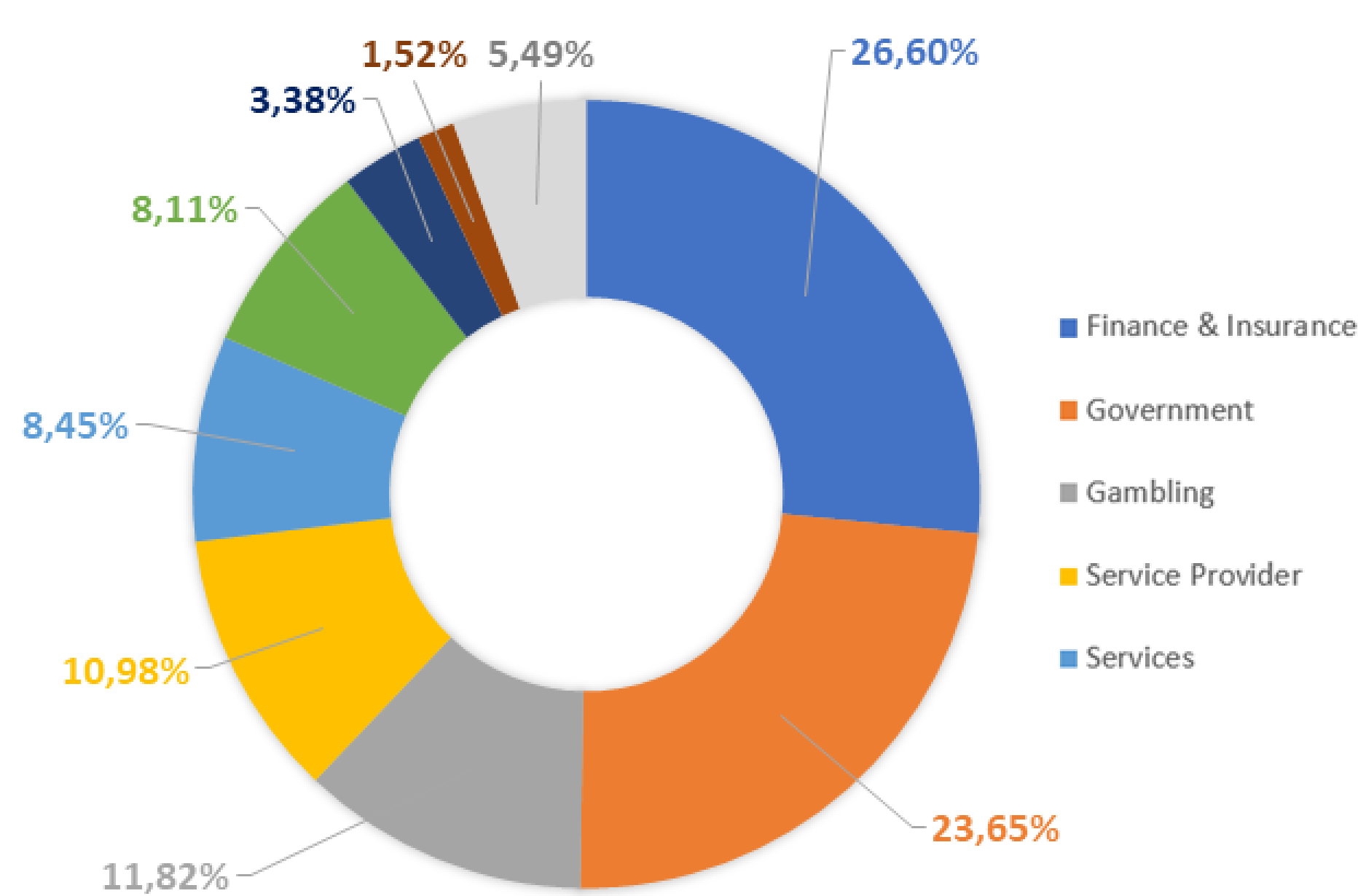
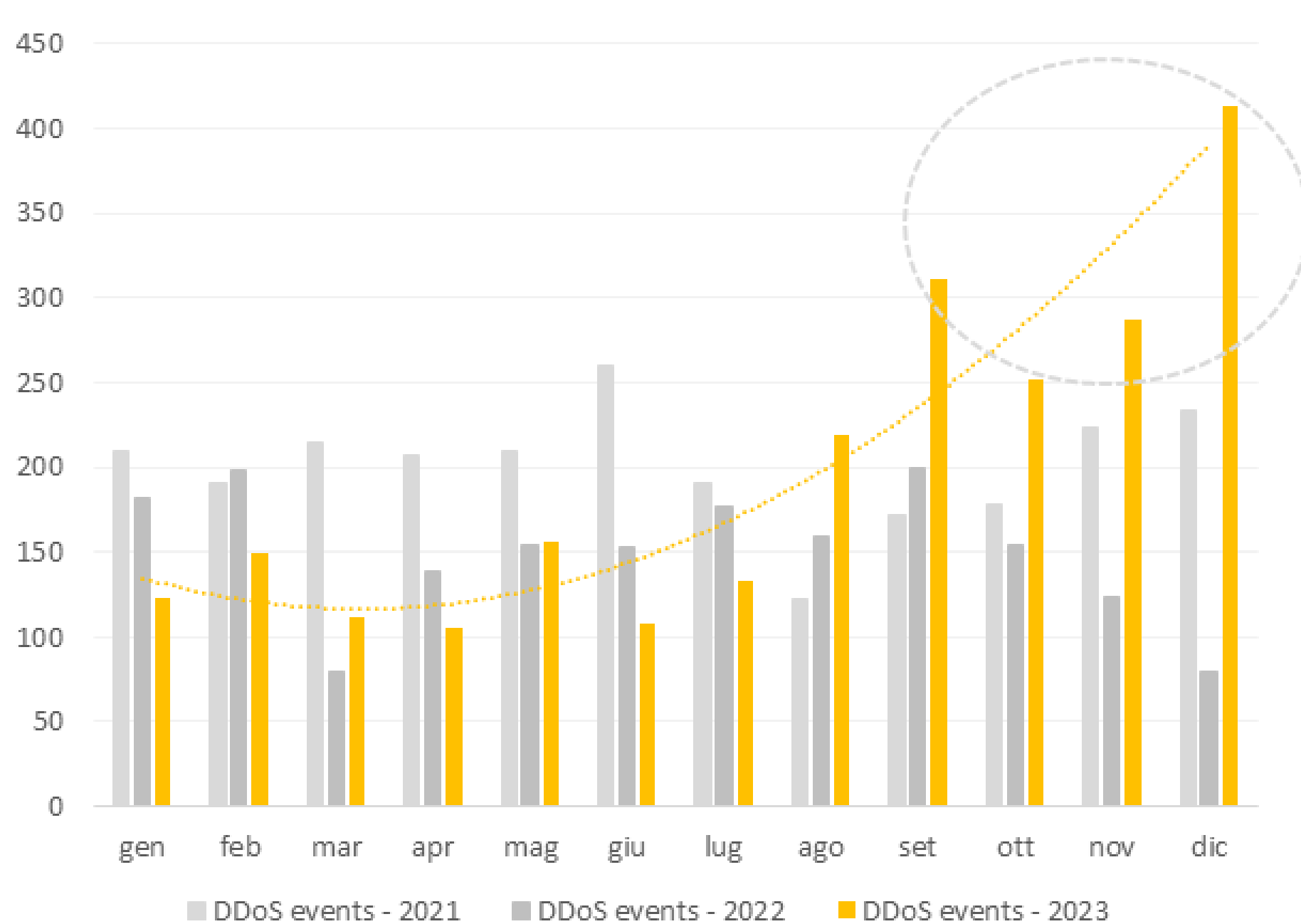
Malware e Botnet | Tipologie e trend



Centri di Comando e Controllo | Distribuzione geografica



Eventi DDoS | Numerosità, segmenti target e trend



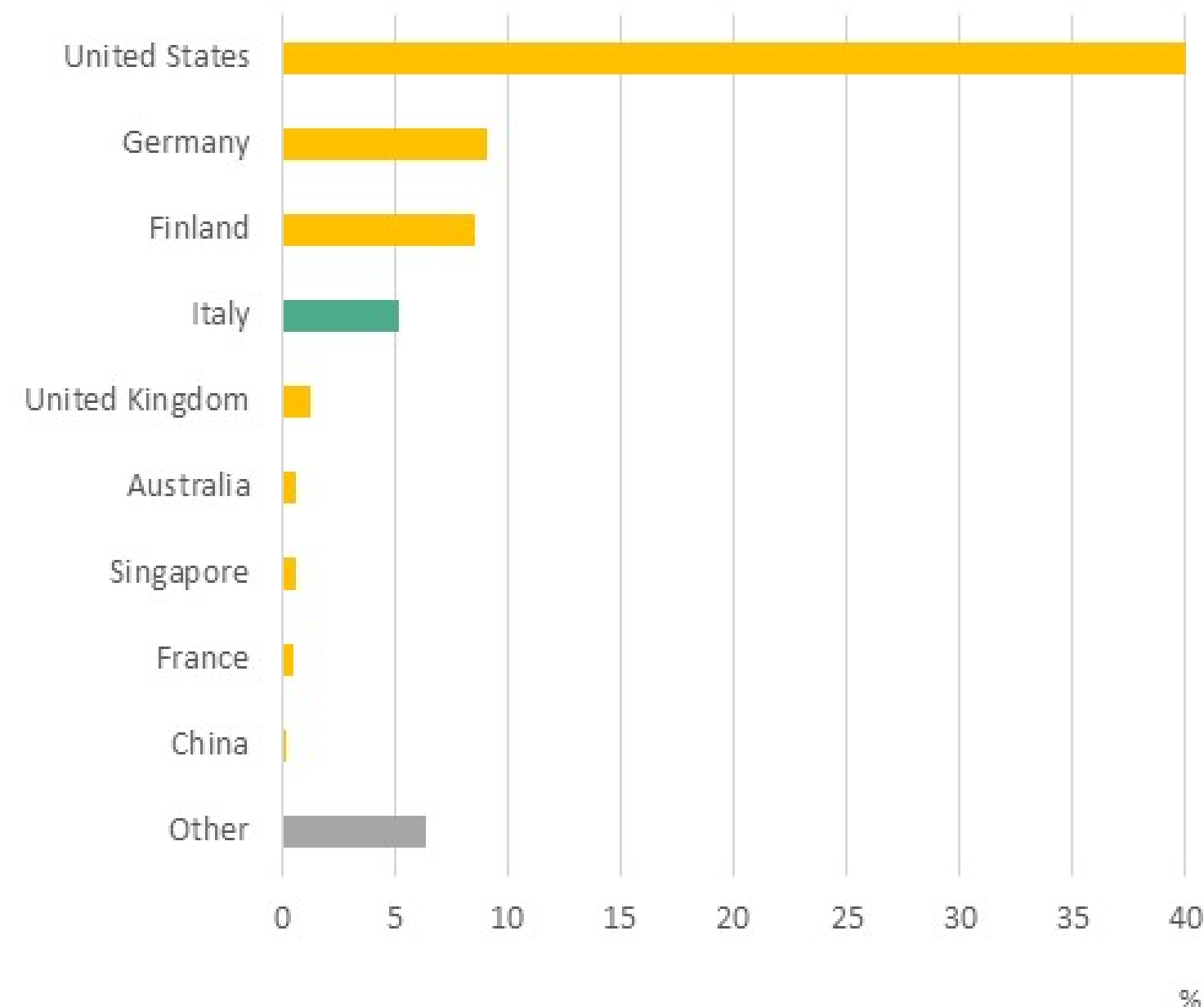
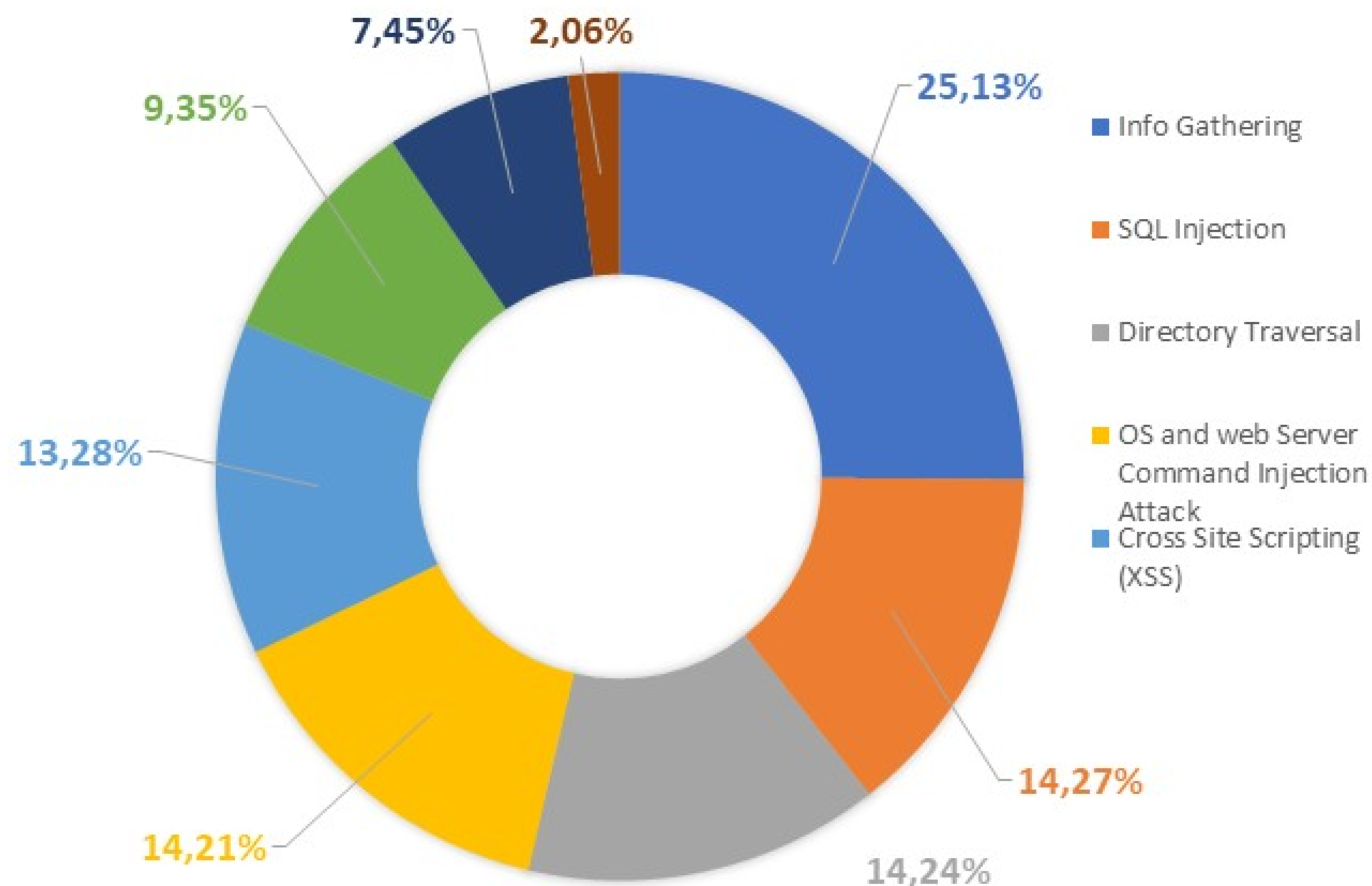
+32% ↑ Numerosità **eventi significativi**

-40% ↓ Numerosità **anomalie**

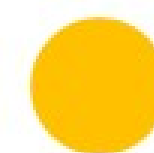
94% Attacchi **sotto 1h**



Sicurezza applicativa | Tipologia e distribuzione geografica



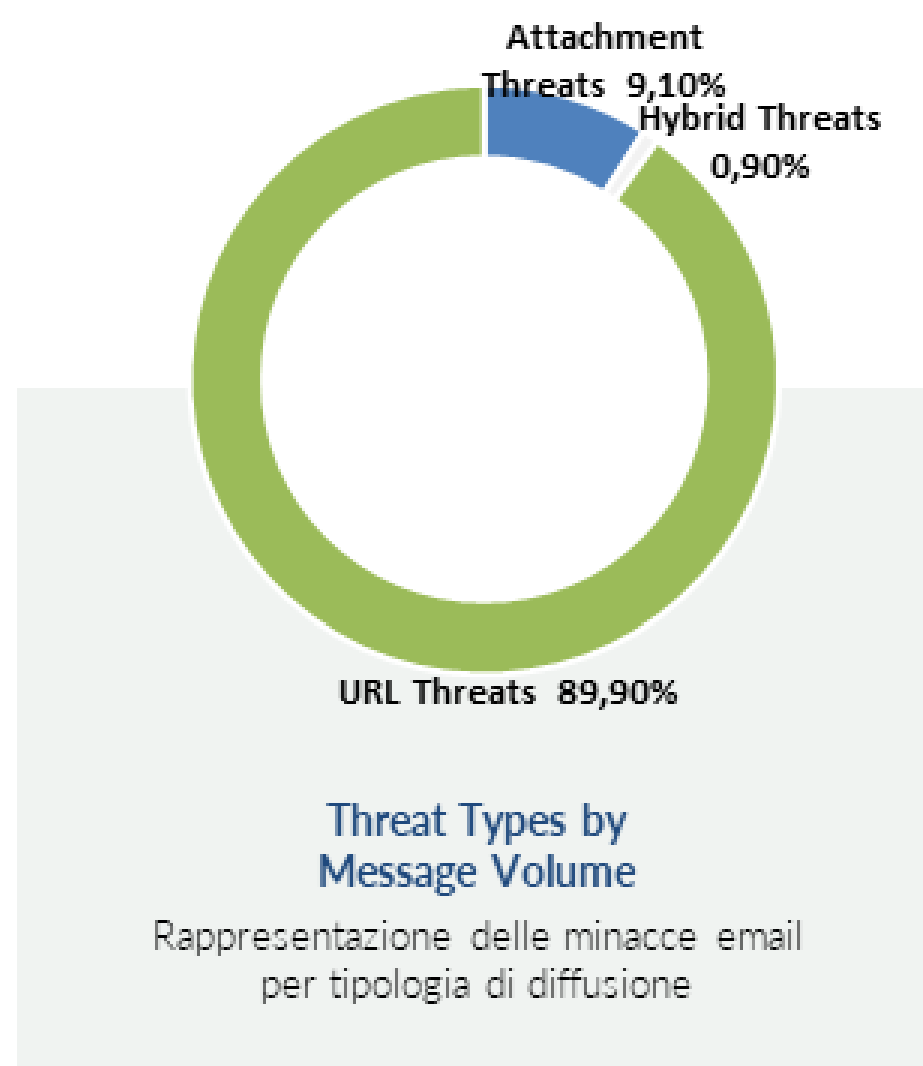
Attività di **Information Gathering**



Distribuzione geografica
sempre meno influente

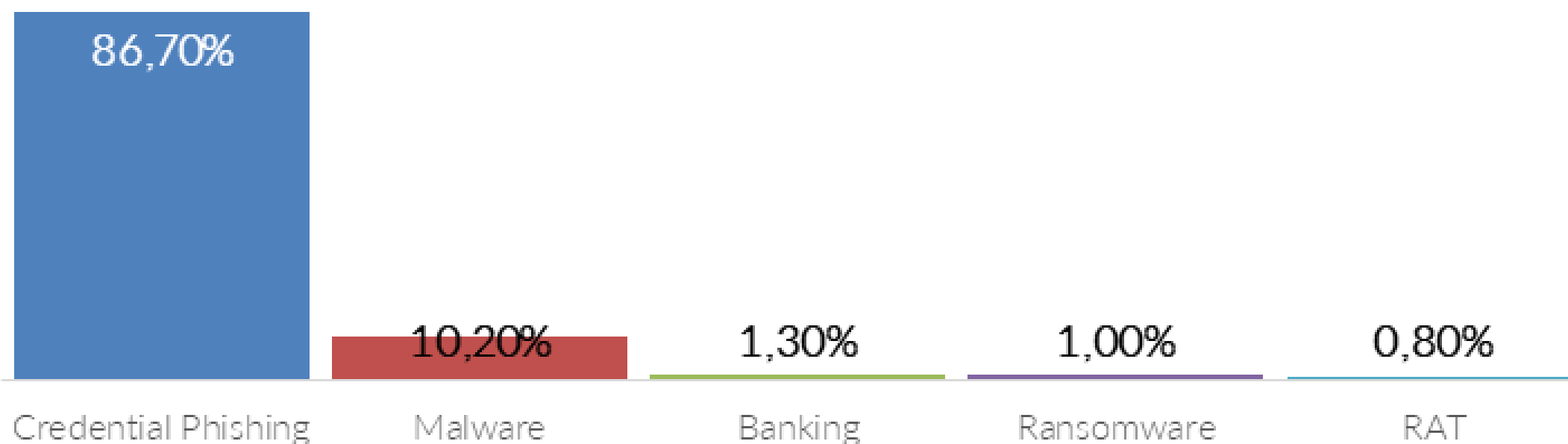


Mail Security | Tecniche di attacco e trend



+11% Tecnica URL Malevoli

Top 5 Famiglie di minacce per volume



Automazione con **Intelligenza Artificiale e Machine Learning**



Attacchi più efficaci
(miglior traduzione, profilazione, deepfake)

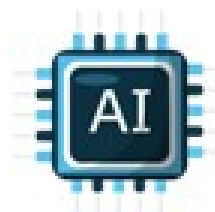


Difese maggiori
(scanning, detection, recognition)

| Key Findings



Aumento della gravità degli **attacchi**



Intelligenza artificiale come **sfida** e **opportunità**



Centralità della **cybersecurity** si conferma **trend strutturale**

Tavola rotonda

Con gli esperti di security di alcuni dei principali fornitori di prodotti e servizi di Cyber Security, che arricchiranno il dibattito con le loro esperienze sul campo:

- **Andrea Negrone**, Aruba, Hewlett Packard Enterprise company
- **Aldo Di Mattia**, Fortinet
- **Luca Nilo Livrieri**, CrowdStrike
- **Stefano Longo**, Microsoft
- **Maurizio Taglioretti**, Netwrix

3
5



Per maggiori informazioni:

rapporti@clusit.it

info@astrea.pro

gfaggioli@clusit.it

apennasilico@clusit.it

sscozzari@clusit.it

lbecchelli@clusit.it

gabriele.scialo@fastweb.it

3
7



SECURITY SUMMIT

