SECURITY SUMMIT

14-15-16 marzo 2023

Security Summit

Clusit
Associazione Italiana per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

Presentazione
Rapporto Clusit 2023

14 marzo 2023 orario 09.15 - 11:30

#securitysummit #rapportoclusit

INTRODUZIONE

GABRIELE FAGGIOLI

PRESIDENTE
CLUSIT

Agenda

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

Saranno presentati i dati dell'ultimo Rapporto Clusit a cura di
Alessio Pennasilico, CTS Clusit.

Intervengono alcuni degli autori:
- **Sofia Scozzari**, CD Clusit
- **Gabriele Scialò**, Product Marketing Manager - Cybersecurity, Fastweb
- **Giorgia Dragoni**, Ricercatrice Senior, Osservatorio Cybersecurity & Data Protection Politecnico di Milano

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

- **Edoardo Accenti,** Aruba, Hewlett Packard Enterprise company
- **Aldo Di Mattia,** Fortinet
- **Luca Nilo Livrieri,** Crowdstrike
- **Maurizio Taglioretti,** Netwrix

I CONTENUTI DEL RAPPORTO

ALESSIO PENNASILICO

COMITATO SCIENTIFICO
CLUSIT

I contenuti del Rapporto

Panoramica sull'evoluzione del cyber crime in Italia e nel mondo

- Analisi dei principali cyber attacchi noti del 2022 a livello globale
  - Analisi della situazione in Italia
  - Analisi della situazione PA
- Analisi Fastweb della situazione italiana in materia di cyber-crime
- Attività e segnalazioni della Polizia Postale e delle Comunicazioni nel 2022
- E-mail security in Italia
- Sanità, tra cyberattacchi e rischi per la salute

Speciale FINANCE

- Elementi sul cybercrime nel settore finanziario in Europa
- Lo scenario evolutivo della minaccia ransomware

Survey

- Netwrix Cloud Data Security Report 2022
- La gestione del rischio cyber nelle grandi organizzazioni italiane
- La Cybersecurity nelle micro e piccole imprese. Una Survey di CNA Milano e dell'Unione Artigiani Milano

I contenuti del Rapporto

Focus On

- Access Broker e attacchi basati sull'identità: tendenze e protezione
- Infrastrutture Critiche (perimetro di cybersecurity nazionale)
- Cyber Resilienza
- La nuova direttiva NIS 2 tra obbligo normativo e opportunità di migliorare la resilienza
- La Supply Chain come Kill Chain - La sicurezza nell'epoca Zero Trust
- Enterprise Architecture per il supporto all'Information Security Management
- Intelligenza Artificiale - Un approccio alla gestione dei rischi per le aziende
- SOC: scenario attuale e pianificazione per il 2023

Le interviste con i partner istituzionali

- METAVERSO E CYBERSECURITY: intervista e contributo di Agostino Ghiglia, Componente del Garante per la protezione dei dati personali

ANALISI CLUSIT DEI PRINCIPALI ATTACCHI A LIVELLO GLOBALE

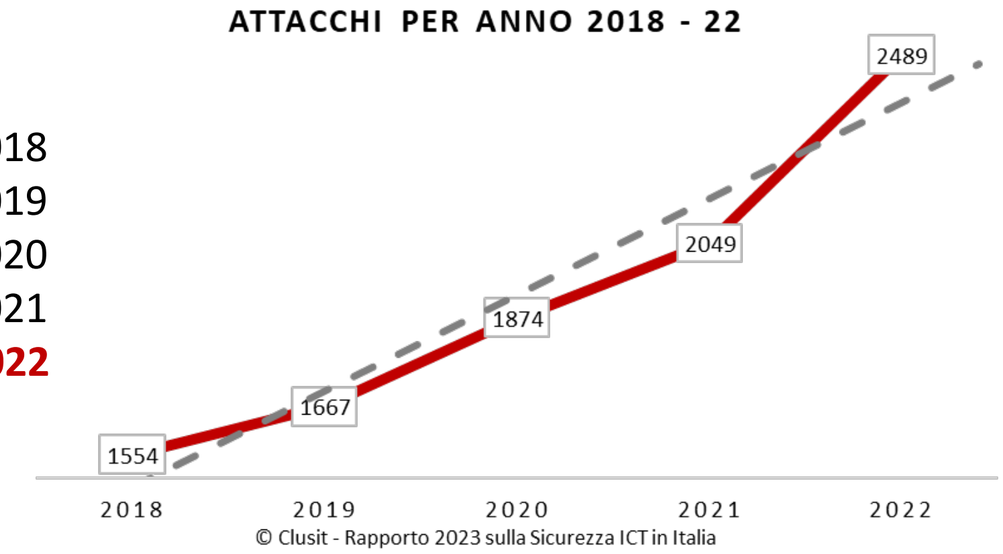
SOFIA SCOZZARI

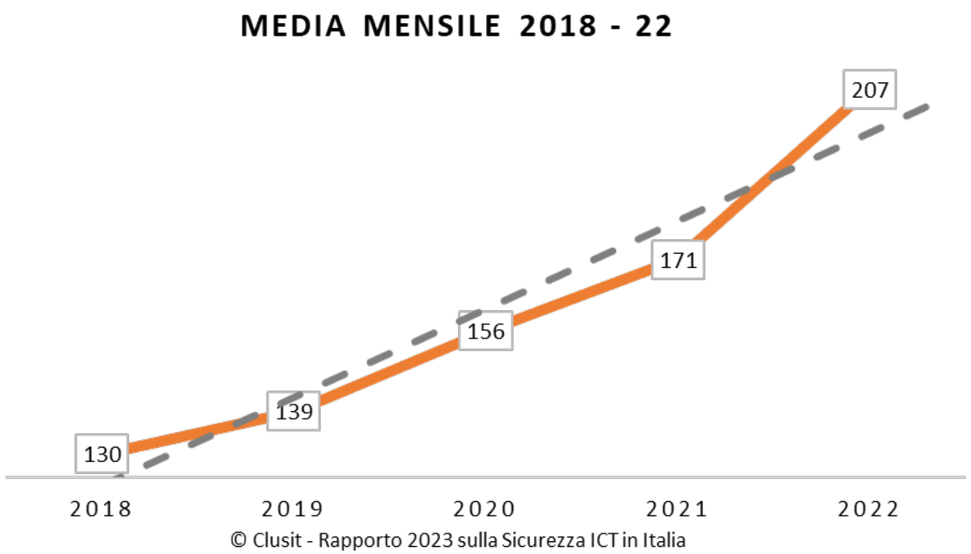
COMITATO DIRETTIVO
CLUSIT

I NUMERI DEL CAMPIONE

Negli ultimi 12 anni abbiamo analizzato e classificato 16.499 cyber attacchi gravi di pubblico dominio, in media 115 al mese.
Negli ultimi 5 anni abbiamo registrato **9.633 incidenti**, il 58% del totale. Gli attacchi sono così suddivisi:

- 1.554 nel 2018
- 1.667 nel 2019
- 1.874 nel 2020
- 2.049 nel 2021
- **2.489 nel 2022**





Dal punto di vista quantitativo, confrontando il 2018 con il 2022 la crescita è stata del **60%** (**+21%** solo nell'ultimo anno) e la media mensile ha raggiunto il record di 207 attacchi al mese.
Dal punto di vista qualitativo, anche la Severity è aumentata significativamente.

NUOVE TASSONOMIE STANDARDIZZATE

La metodologia utilizzata per svolgere questa analisi è stata raffinata ed aggiornata nel tempo, sia dal punto di vista del numero e della qualità delle fonti utilizzate, che della quantità di variabili impiegate per descrivere i diversi fenomeni e delle **tassonomie utilizzate per classificare i dati**, che sono state completamente riviste ed aggiornate per aderire quanto più possibile a **standard riconosciuti a livello internazionale**.

In particolare, il sistema di classificazione dei settori merceologici che abbiamo adottato per mappare le vittime di attacchi informatici è derivato dall'**ISIC (*International Standard Industrial Classification of All Economic Activities*) delle Nazioni Unite** e dalla **NACE della Commissione Europea (*Nomenclature statistique des activités économiques dans la Communauté Européenne*)**, da cui derivano i codici **ATECO** italiani.

20 macro-categorie merceologiche, 163 sotto-categorie

La classificazione delle tecniche di attacco è derivata dalla **Threat Taxonomy** di **ENISA,** dalla **Open Threat Taxonomy** e da **diversi altri framework.**

8 macro-categorie, 59 sotto-categorie

La classificazione degli attaccanti deriva invece dalla nostra esperienza sul campo e rappresenta una **mappatura tra le principali famiglie di "bad actors" e le motivazioni degli attacchi osservati**.

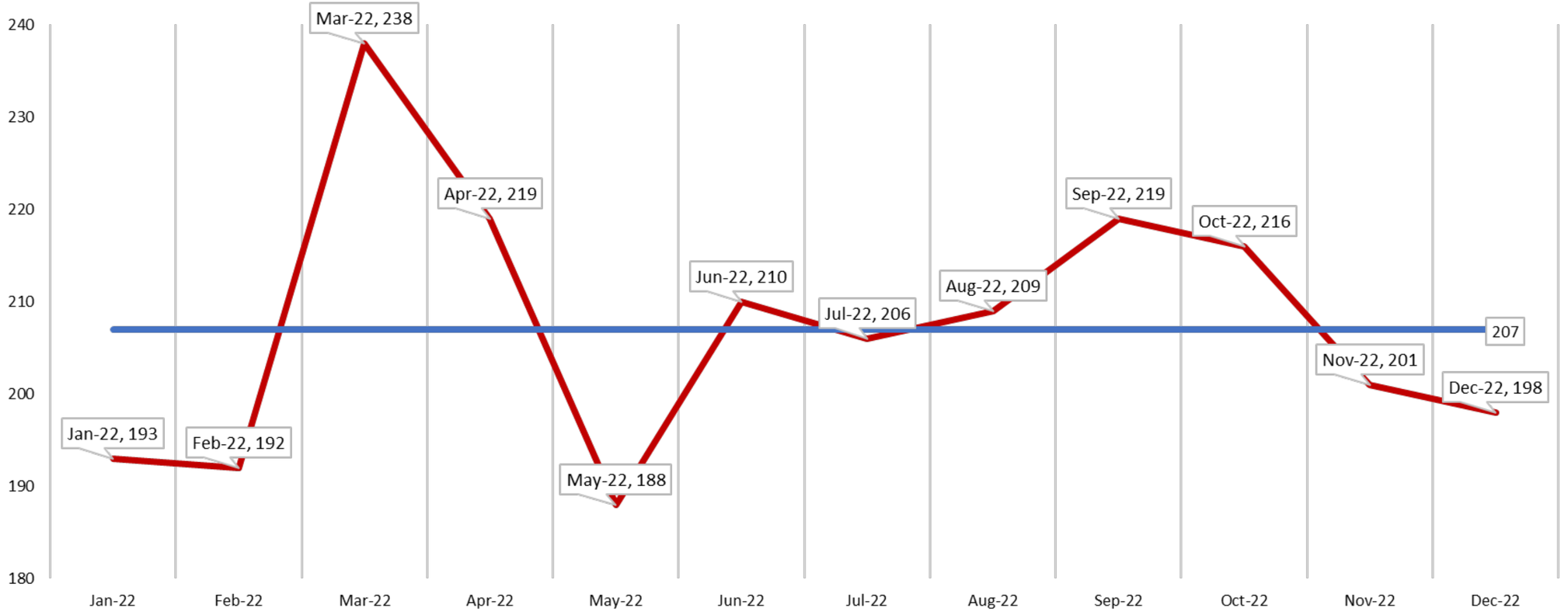
4 macro-categorie, 13 sotto-categorie

Infine, abbiamo aggiunto la valutazione dell'**impatto degli attacchi** (la severity)**,** basandoci su variabili molteplici che includono: impatto geopolitico, sociale, economico (diretto e indiretto), di immagine e di costo/opportunità per le vittime.

4 livelli di severity

ATTACCHI PER MESE NEL 2022

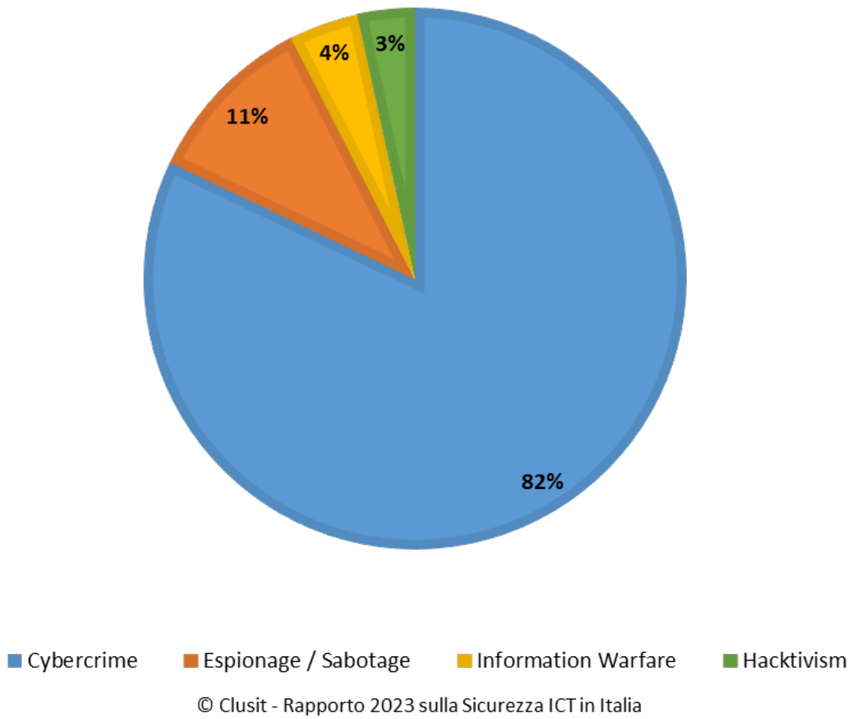
Il picco di Marzo e Aprile è in corrispondenza dell'inizio delle ostilità tra Russia e Ucraina



I 238 attacchi di Marzo rappresentano il record assoluto registrato finora.

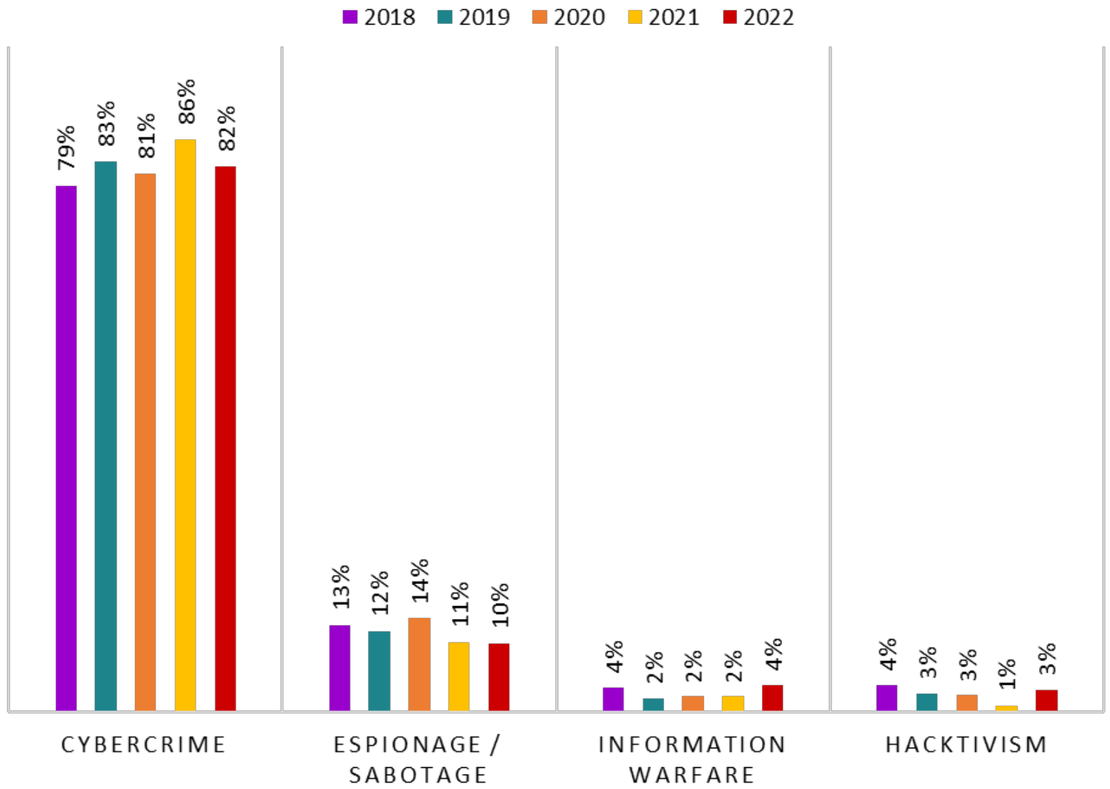
DISTRIBUZIONE DEGLI ATTACCANTI

TIPOLOGIA E DISTRIBUZIONE ATTACCANTI 2022



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

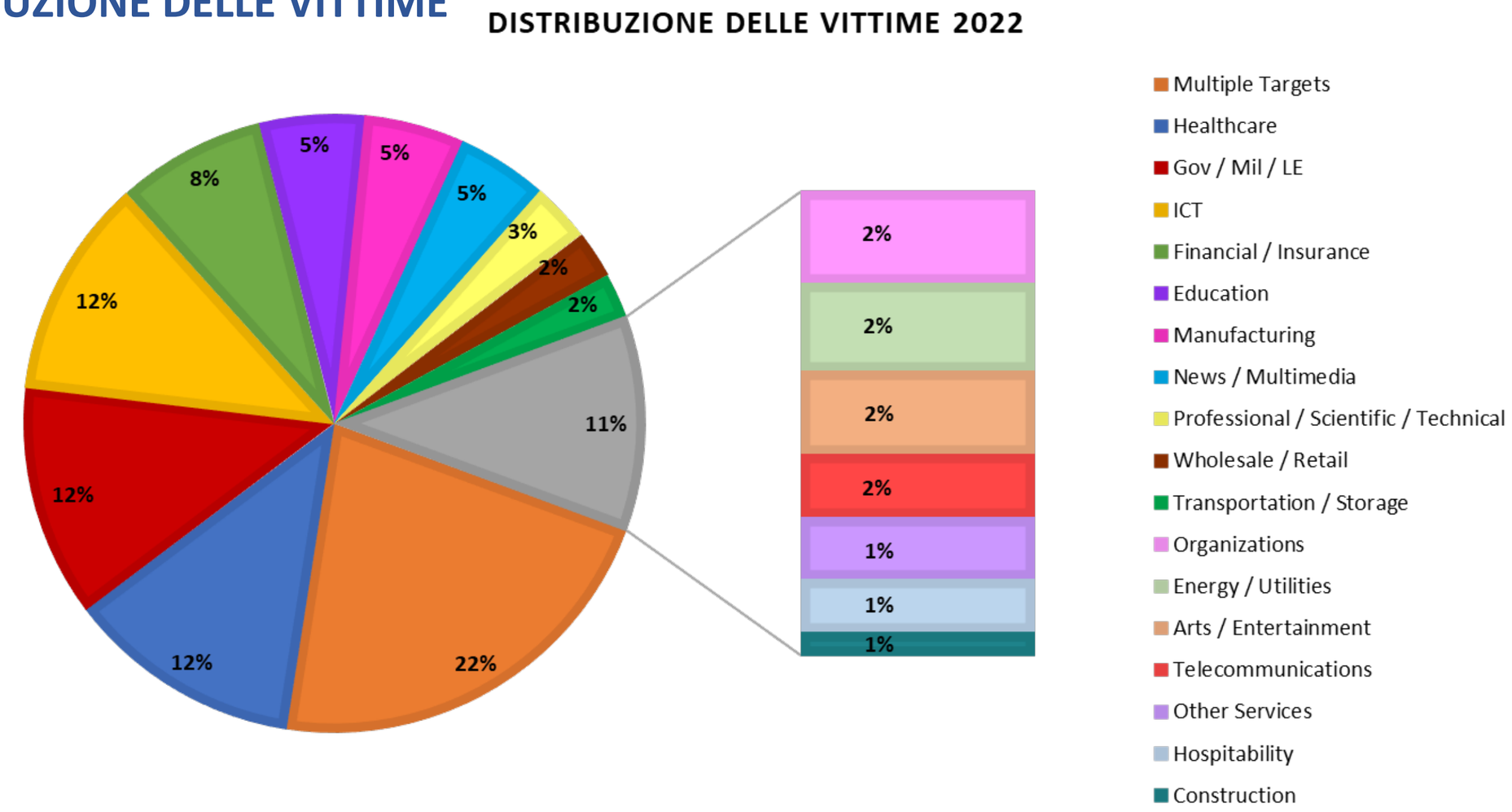
ATTACCANTI % 2018 - 2022



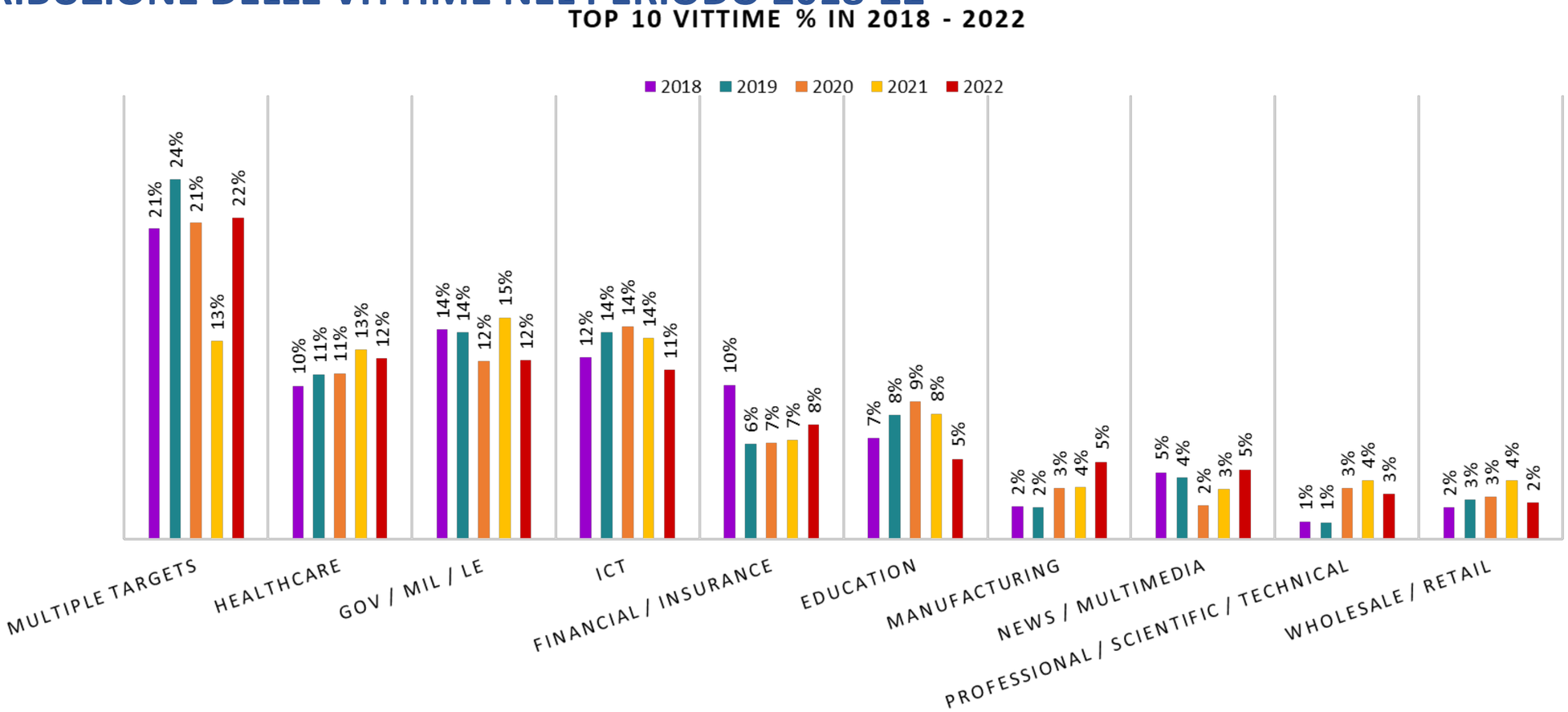
© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

Sebbene diminuisca in percentuale sul totale, in numeri assoluti il **Cybercrime** mostra una crescita del **15%** rispetto al 2021, **Information Warfare** del **110%** e **Hacktivism** del **320%** principalmente a causa del conflitto europeo.

DISTRIBUZIONE DELLE VITTIME

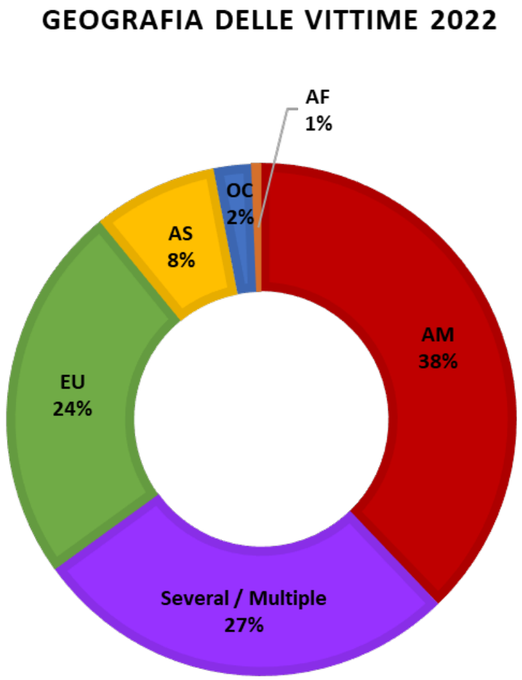


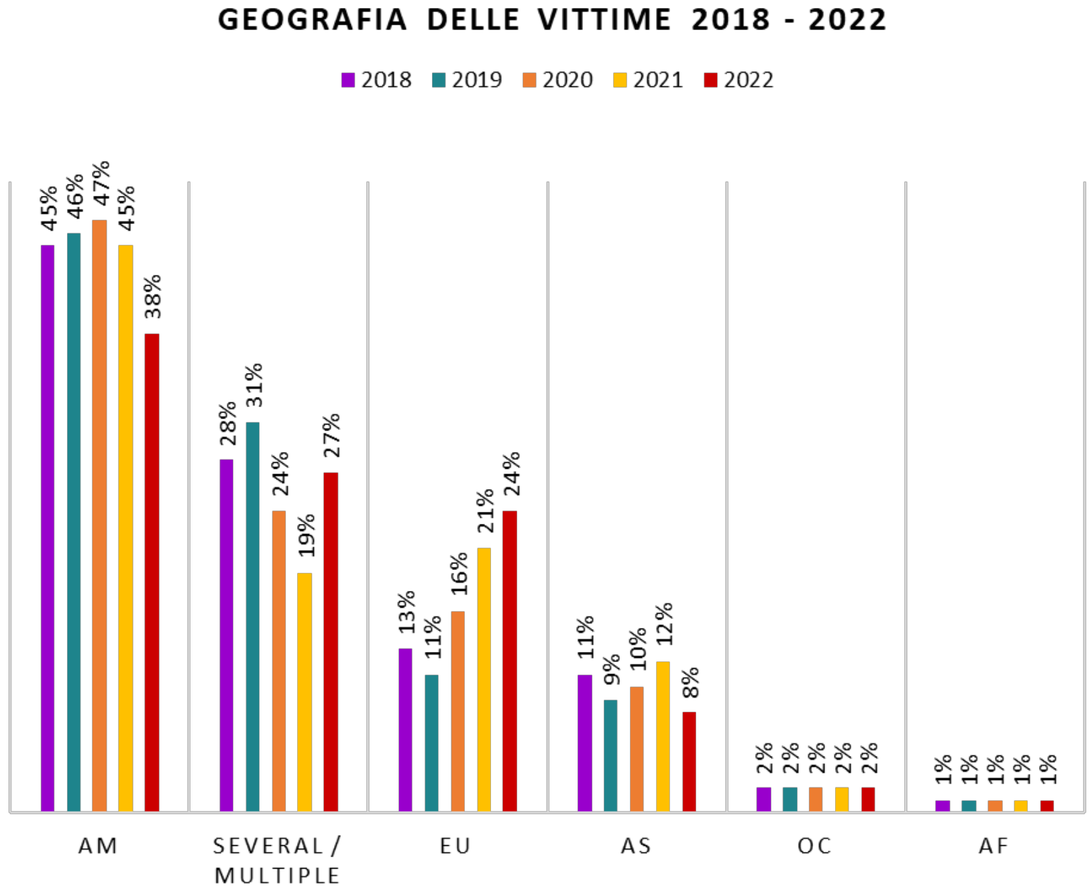
DISTRIBUZIONE DELLE VITTIME NEL PERIODO 2018-22



Aumentano nuovamente le vittime «multiple» (**+97%** rispetto all'anno precedente), **Financial / Insurance** (**+40%**), **Manufacturing** (**+79%**), **News / Multimedia** (**+70%**). **Healthcare** resta il secondo settore più colpito con una crescita del **16%** rispetto al 2021. Il **settore manufatturiero** (**5%** del totale degli attacchi) è un altro record.

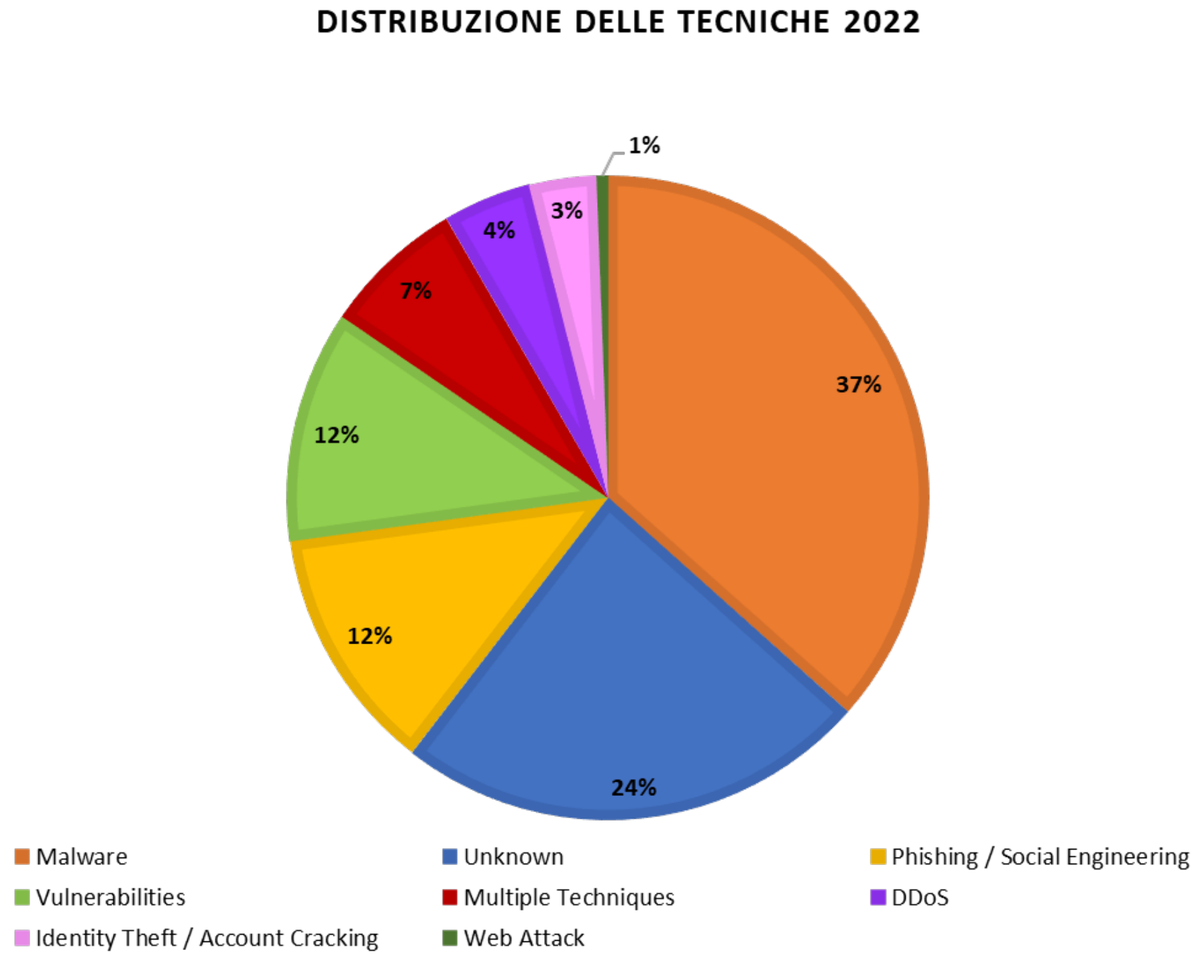
GEOGRAFIA DELLE VITTIME





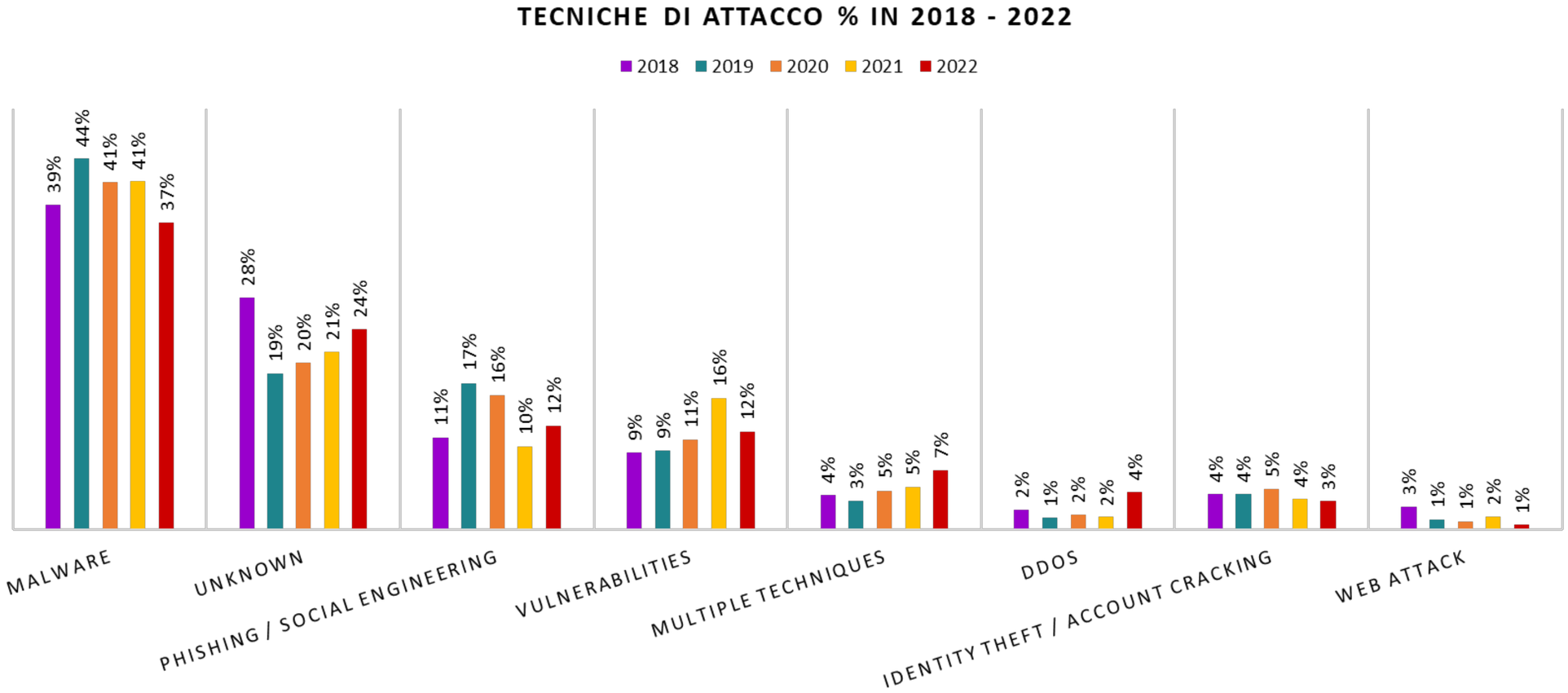
Aumentano gli attacchi verso vittime multinazionali o distribuite in diversi paesi e in **Europa**, che nel 2022 rappresenta **quasi un quarto** del campione (record assoluto finora registrato), mentre diminuiscono in termini percentuali le vittime americane, scese per la prima volta sotto la soglia del 40% (altro record assoluto).

DISTRIBUZIONE DELLE TECNICHE DI ATTACCO



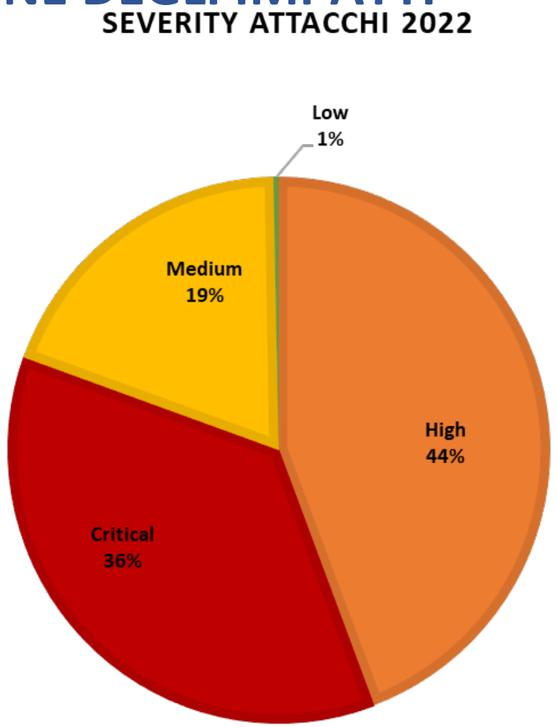
© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

DISTRIBUZIONE DELLE TECNICHE DI ATTACCO NEL PERIODO 2018-22

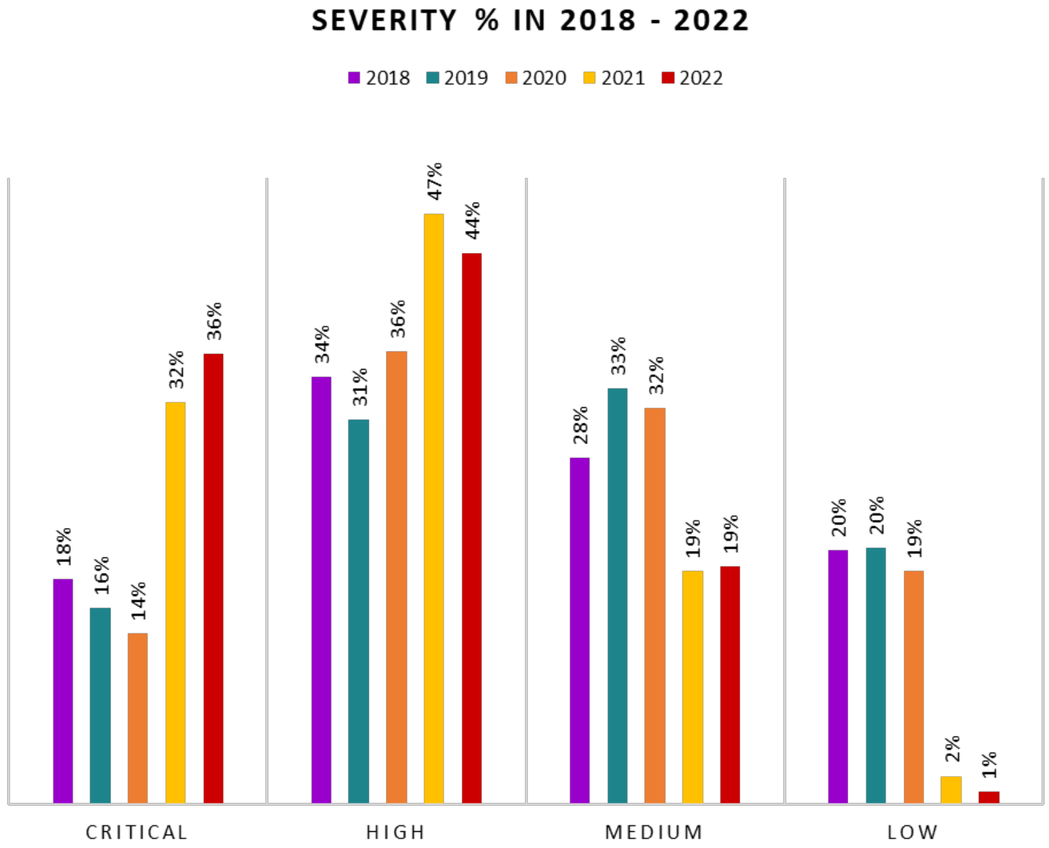


Aumenta leggermente il ricorso a tecniche «sconosciute» (principalmente data breach), mentre crescono notevolmente **Phishing e Social Engineering** (**+52%** rispetto al 2021), **tecniche multiple** (**+72%**, in virtù della natura più complessa degli attacchi) e **DDoS** (**+258%**). Multiple techniques (7%) e DDoS (4%) rappresentano un ulteriore record dell'anno.

VALUTAZIONE DEGLI IMPATTI



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

L'**80%** degli attacchi del 2022 ha avuto un **impatto importante o gravissimo**.
La **severity critica al 36%** è l'ennesimo record assoluto dell'anno.

ANALISI **FASTWEB**

DELLA SITUAZIONE ITALIANA IN MATERIA DI CYBERCRIME

GABRIELE SCIALO'

PRODUCT MARKETING MANAGER - FASTWEB

I trend del cybercrime nel 2022

Gli **investimenti in cybersecurity di aziende e PA e l'efficacia delle misure di sicurezza** hanno permesso di contenere l'avanzata delle minacce informatiche, grazie ad un **approccio strutturato di difesa e tecnologie** a protezione degli asset digitali

+25%

FORTE BALZO DEL NUMERO DEGLI ATTACCHI

OLTRE 56 MILIONI
eventi di **sicurezza in Italia**

-9%

...MA LA CONSAPEVOLEZZA DEI RISCHI CONTINUA A CRESCERE

diminuisce il numero di server e device con servizi esposti su Internet **41.000 SERVER**

GLI SCENARI DI ATTACCO

MALWARE E BOTNET

+22%

In aumento le tipologie di malware individuate ma diminuiscono le infezioni (-3%)

ATTACCHI DDOS

1.800 eventi significativi

-25%

PA + Finance i settori più colpiti, Service Provider al **3° posto** (16%)

DISTRIBUZIONE GEOGRAFICA

Italia al **4°posto** per **provenienza attacchi applicativi**

ATTACCHI EMAIL

URL malevoli
1° tecnica utilizzata nel 92% dei casi

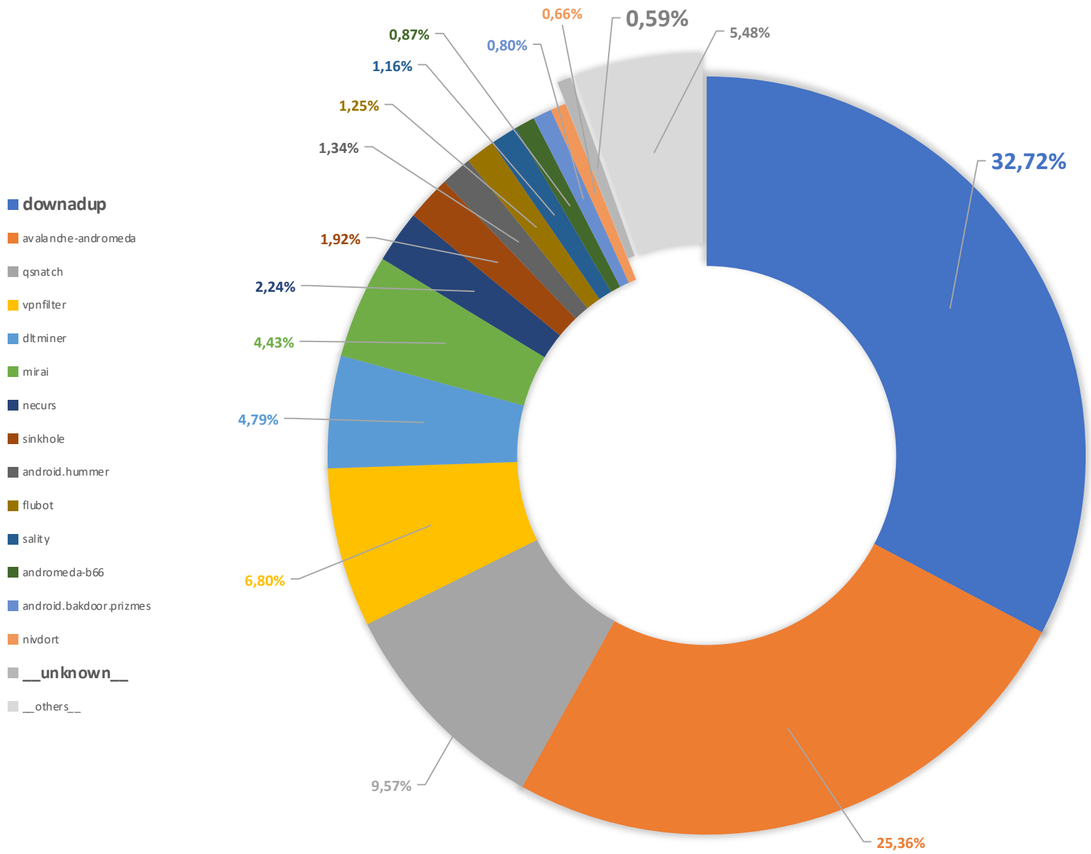
+5%

IA utilizzata per incrementare l'efficacia degli attacchi

Analisi Fastweb per il rapporto Clusit su dati 2022 confrontati al 2021

FASTWEB

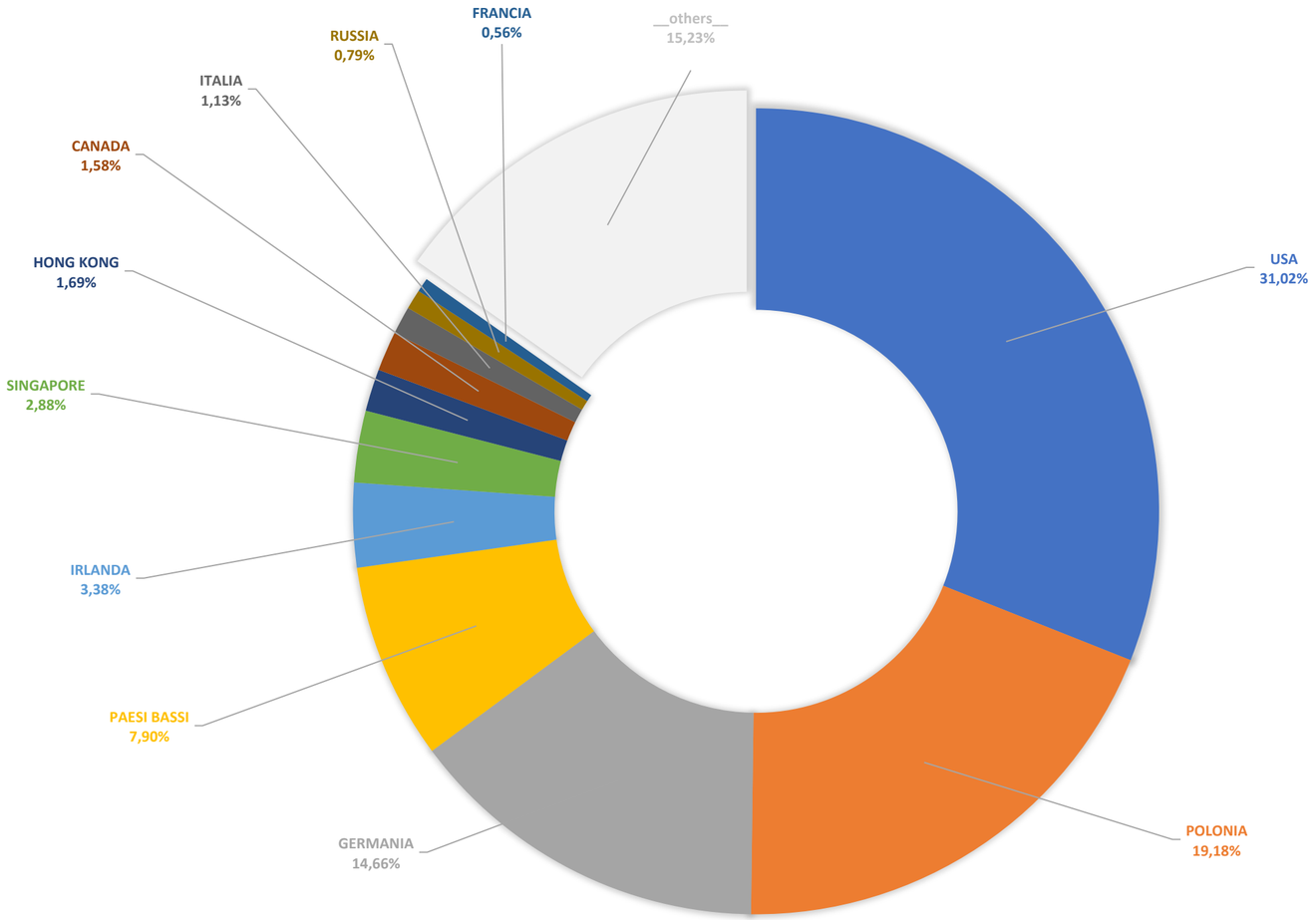
Malware e Botnet | Tipologie e trend



+22% **Tipologie** e **famiglie di malware**

-3% Numerosità di **infezioni** e **attacchi**

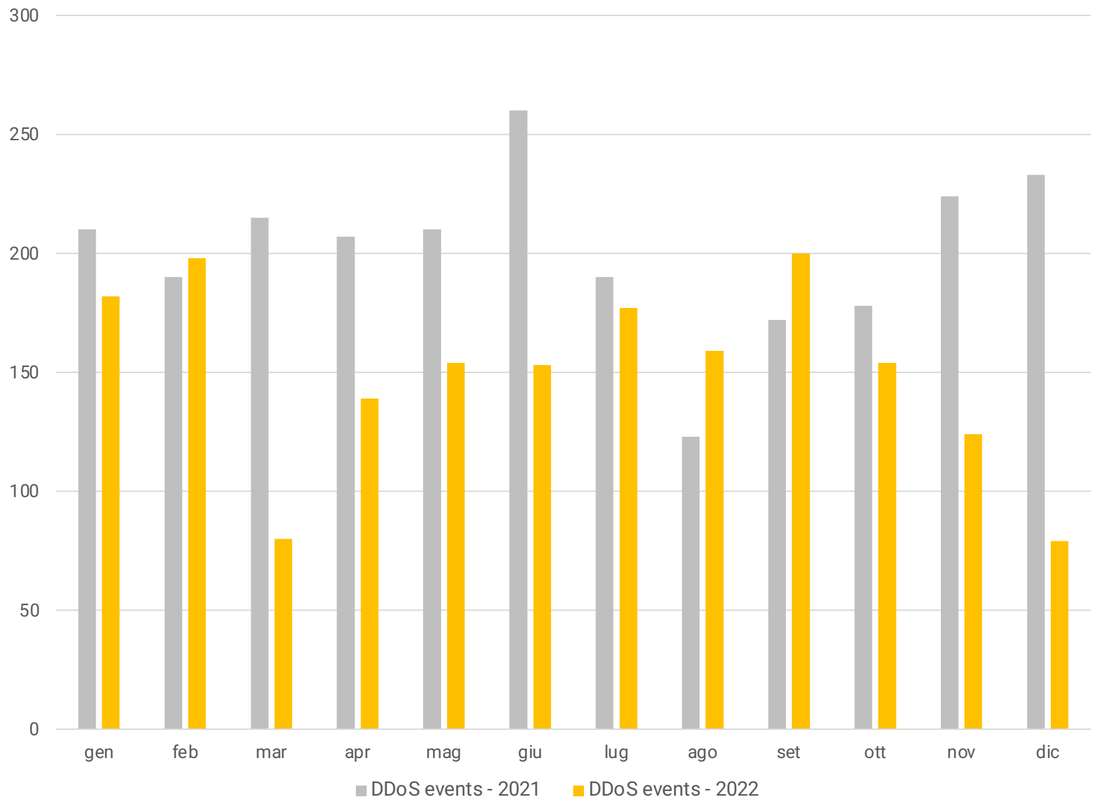
Centri di Comando e Controllo | Distribuzione geografica

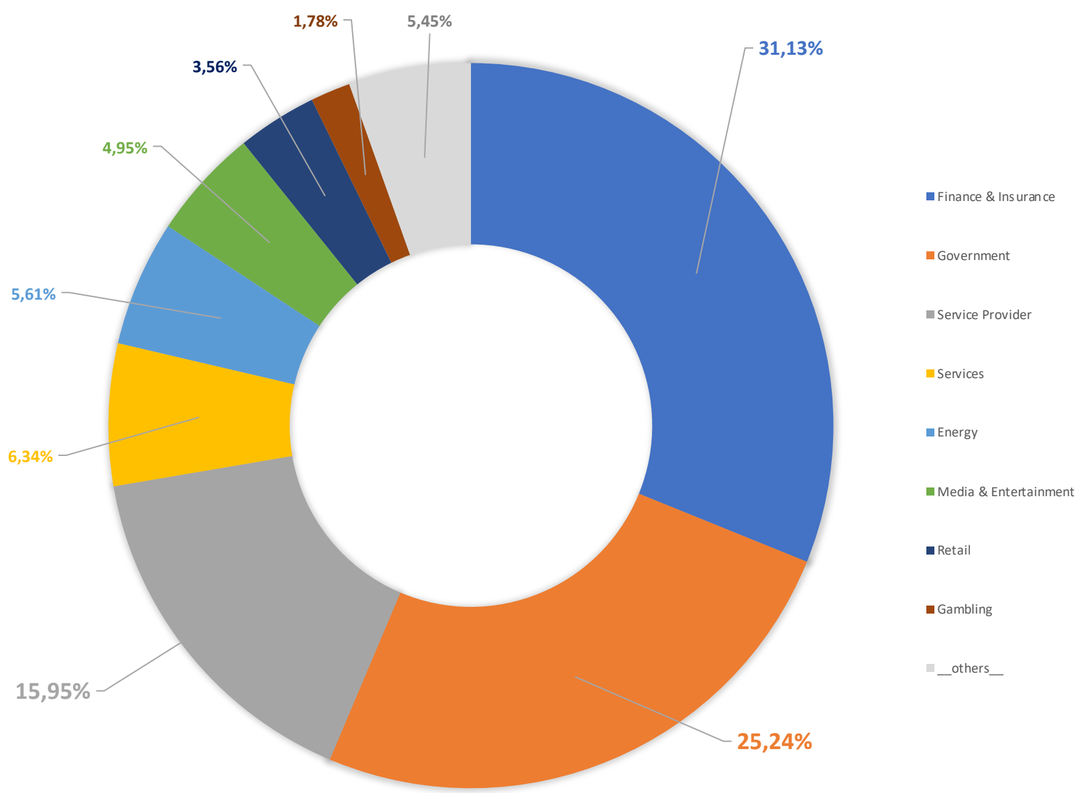


2019 → 2022

80% → 31%

Eventi DDoS | Numerosità, segmenti target e trend



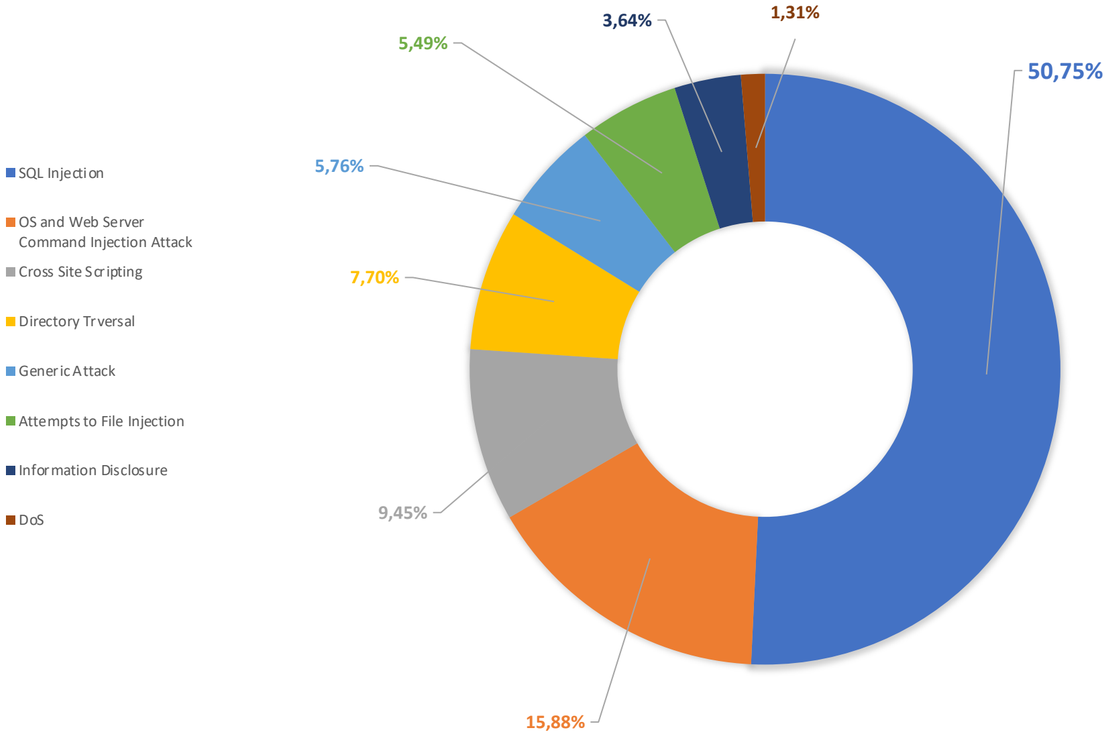


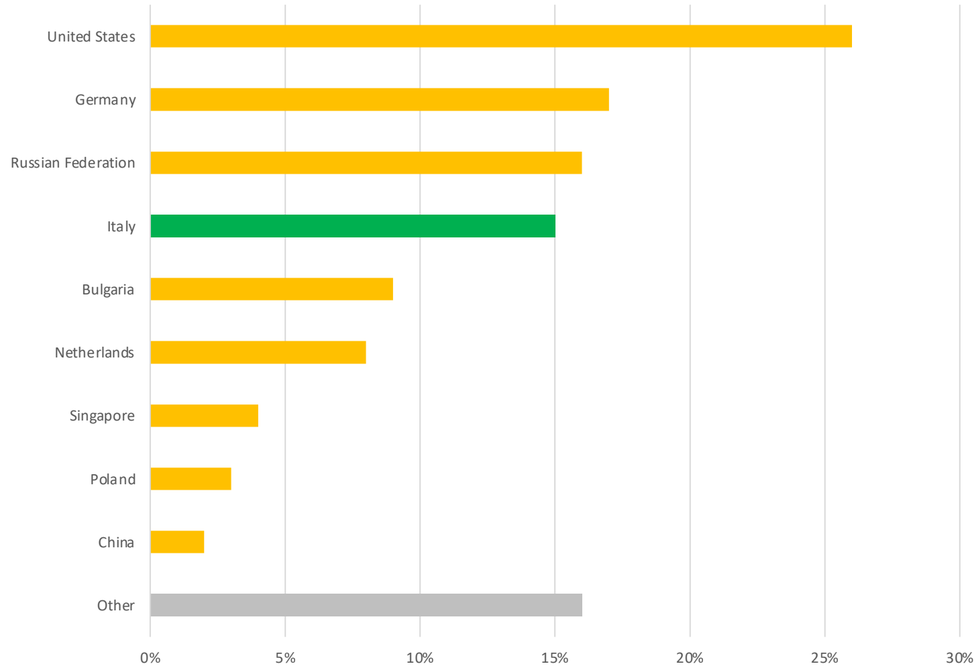
-25% Numerosità **eventi significativi**

+11% Numerosità **anomalie**

93% Attacchi **sotto 1h**

Sicurezza applicativa | Tipologia e distribuzione geografica

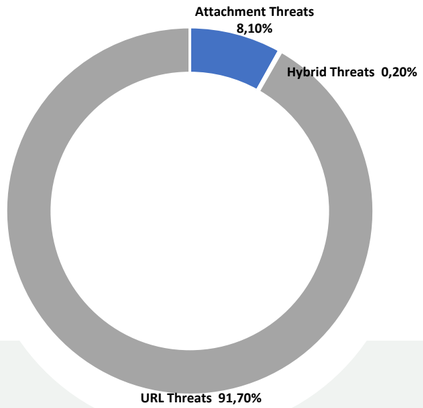




Attività di **Information Gathering**

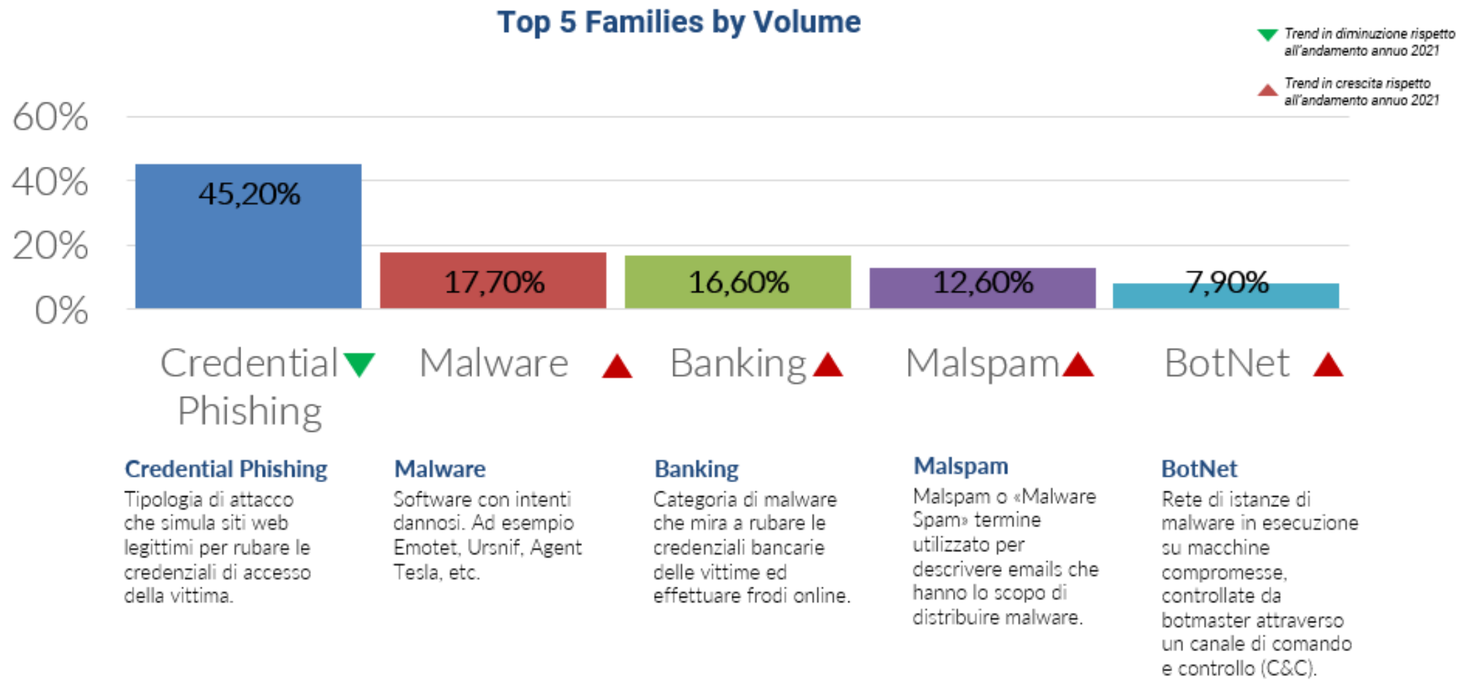
Distribuzione geografica sempre meno influente

Mail Security | Tecniche di attacco e trend



Threat Types by Message Volume

Rappresentazione delle minacce email per tipologia di diffusione



Credential Phishing
Tipologia di attacco che simula siti web legittimi per rubare le credenziali di accesso della vittima.

Malware
Software con intenti dannosi. Ad esempio Emotet, Ursnif, Agent Tesla, etc.

Banking
Categoria di malware che mira a rubare le credenziali bancarie delle vittime ed effettuare frodi online.

Malspam
Malspam o «Malware Spam» termine utilizzato per descrivere emails che hanno lo scopo di distribuire malware.

BotNet
Rete di istanze di malware in esecuzione su macchine compromesse, controllate da botmaster attraverso un canale di comando e controllo (C&C).

+5% Tecnica URL **Malevoli**

Automazione con **Intelligenza Artificiale** e **Machine Learning**

Key Findings

Aumento generalizzato degli **attacchi**

Maggiore **consapevolezza** e **investimenti** mirati

Centralità della **cybersecurity** post pandemia diventa **trend strutturale**

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

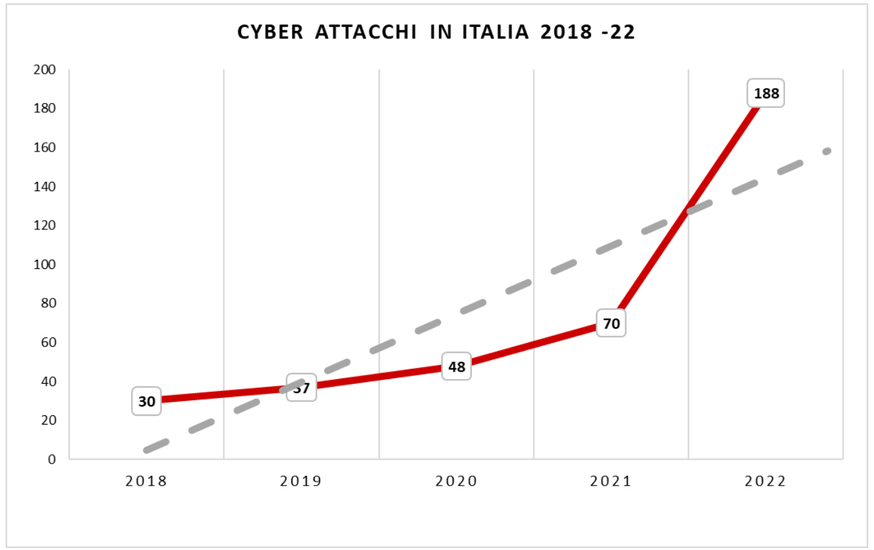
GIORGIA DRAGONI

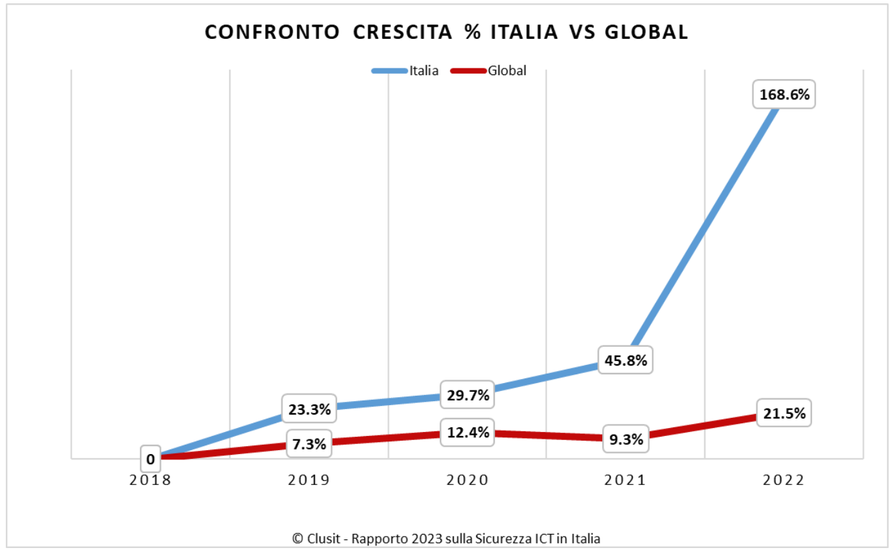
RICERCATRICE SENIOR
OSSERVATORIO CYBERSECURITY & DATA PROTECTION POLITECNICO DI MILANO

I NUMERI DEL CAMPIONE

Negli ultimi 5 anni abbiamo registrato **373 incidenti in Italia**, così suddivisi:

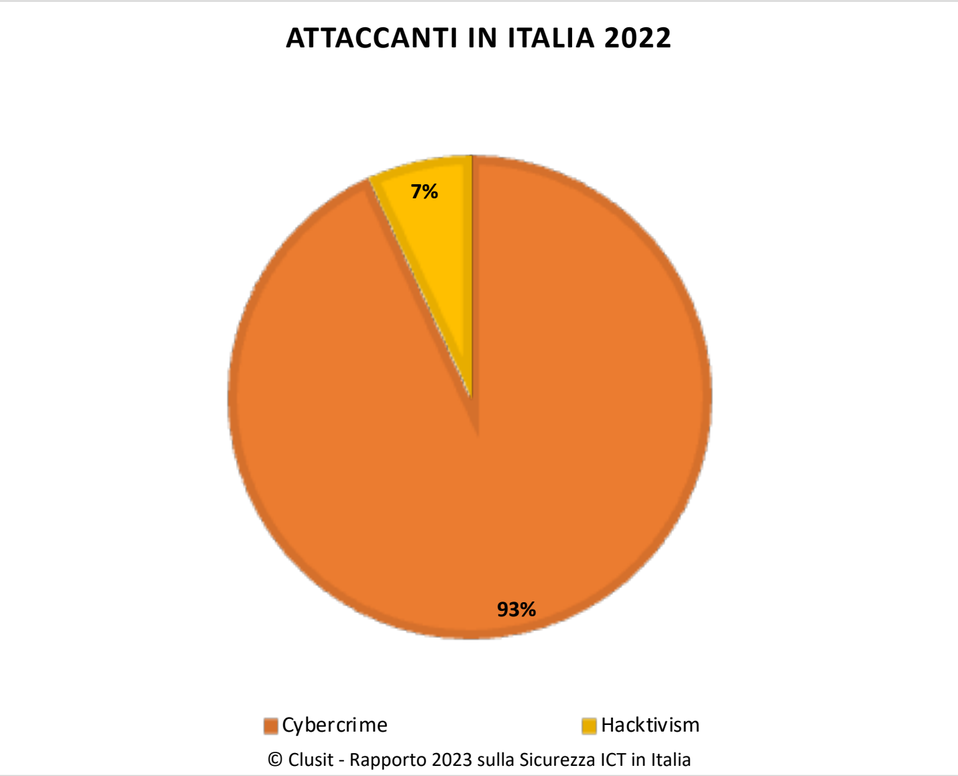
- 30 nel 2018
- 37 nel 2019
- 48 nel 2020
- 70 nel 2021
- **188 nel 2022**

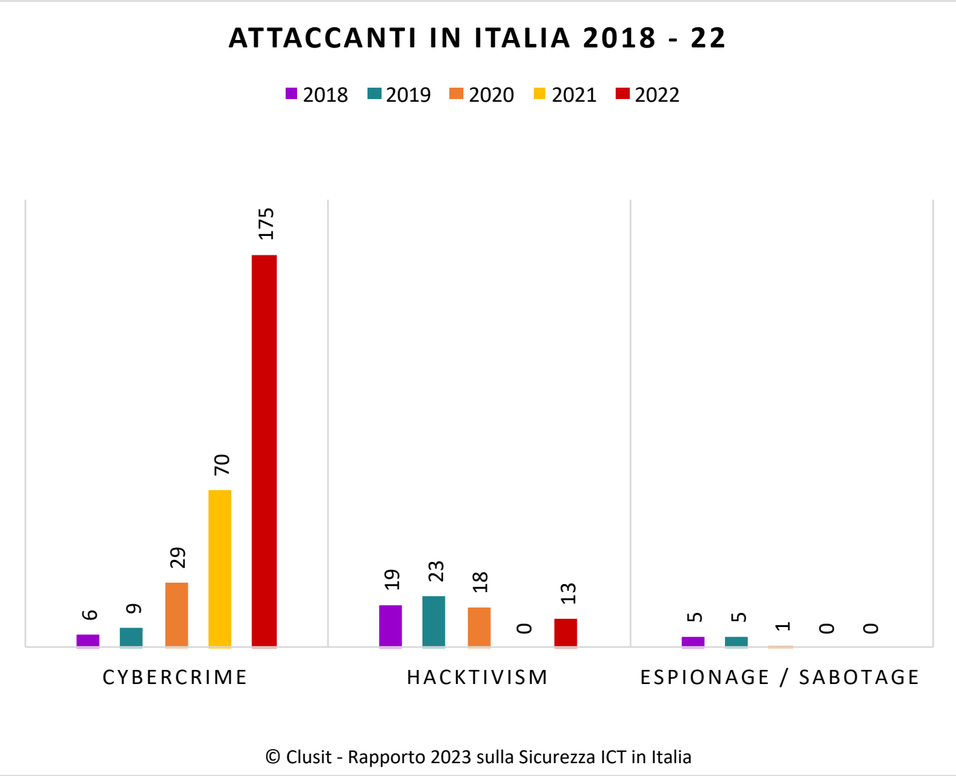




Dal punto di vista quantitativo, confrontando il 2018 con il 2022 la crescita è stata del **527%** (+169% solo nell'ultimo anno) con un ritmo di crescita decisamente superiore di quanto avviene su scala globale.
Gli attacchi in Italia nel 2022 rappresentano il **7,6%** del totale degli attacchi globali, nel 2021 erano il 3,4%.

DISTRIBUZIONE DEGLI ATTACCANTI





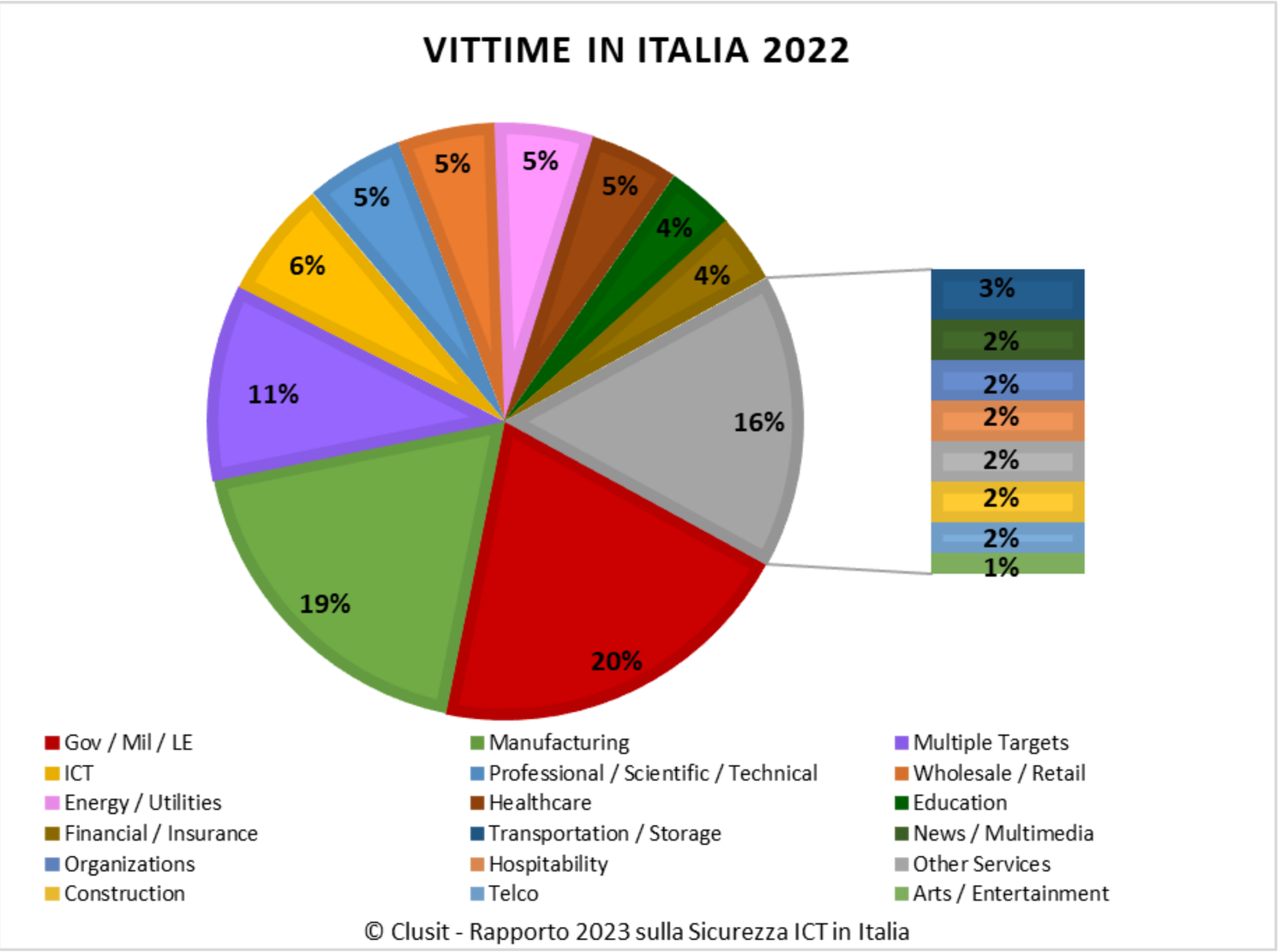
Sebbene diminuisca il peso percentuale del Cybercrime (nel 2021 rappresentava il 100% degli attacchi), in termini assoluti questa categoria ha fatto registrare il numero di attacchi più elevato mai rilevato. Rispetto al 2021, la crescita è pari al **150%.**

DISTRIBUZIONE DELLE VITTIME

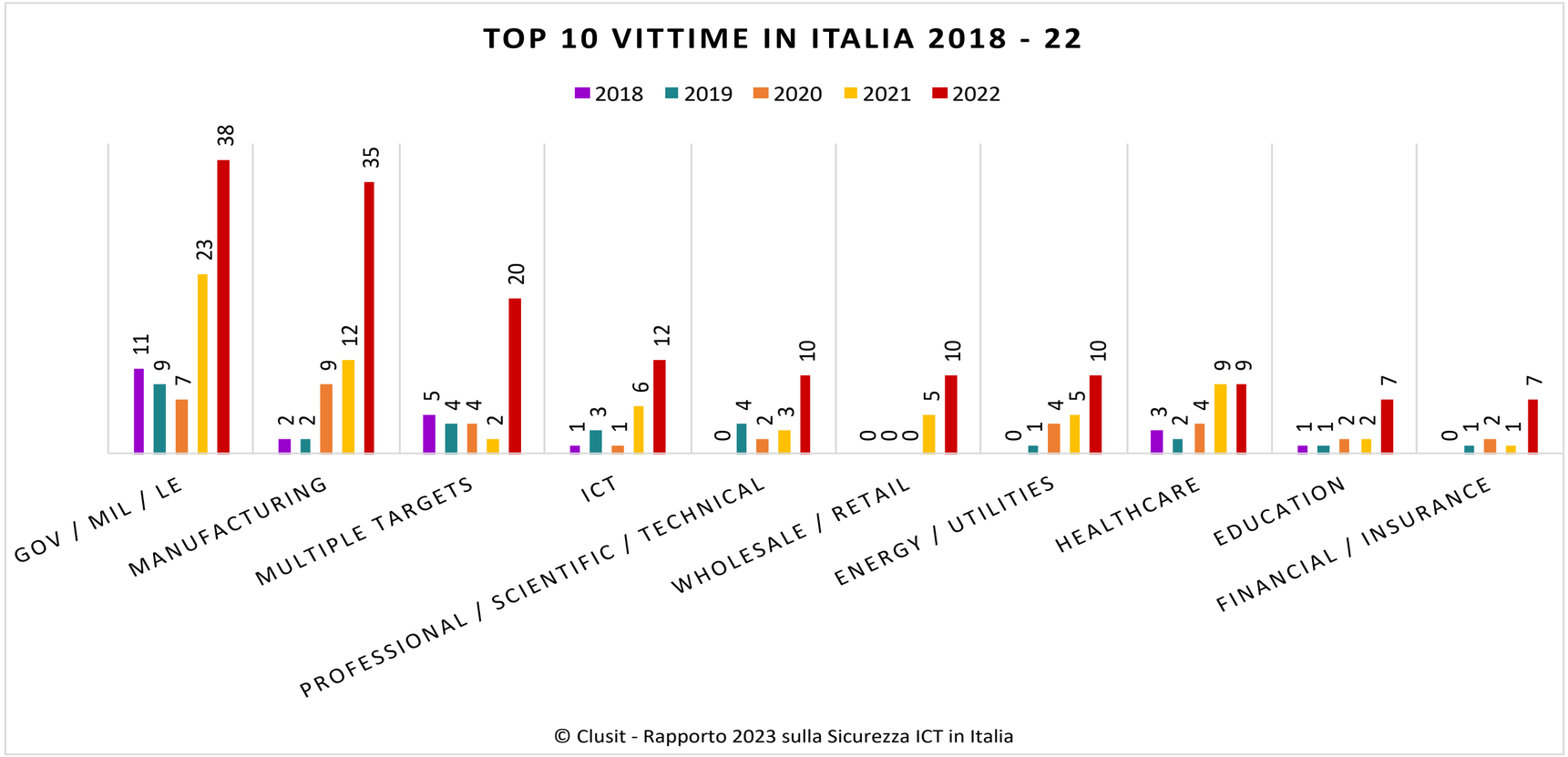
In Italia, i settori per cui si rilevano un maggior numero di attacchi sono:

- Government (20% vs 12% globale)
- Manufacturing (19% vs 5% globale)
- Multiple Targets (11% vs 22% globale)

Gli incidenti rivolti al “Manufacturing” rilevati in Italia rappresentano il **27%** del totale degli attacchi censiti a livello globale nei confronti di questo settore.



DISTRIBUZIONE DELLE VITTIME NEL PERIODO 2018-22



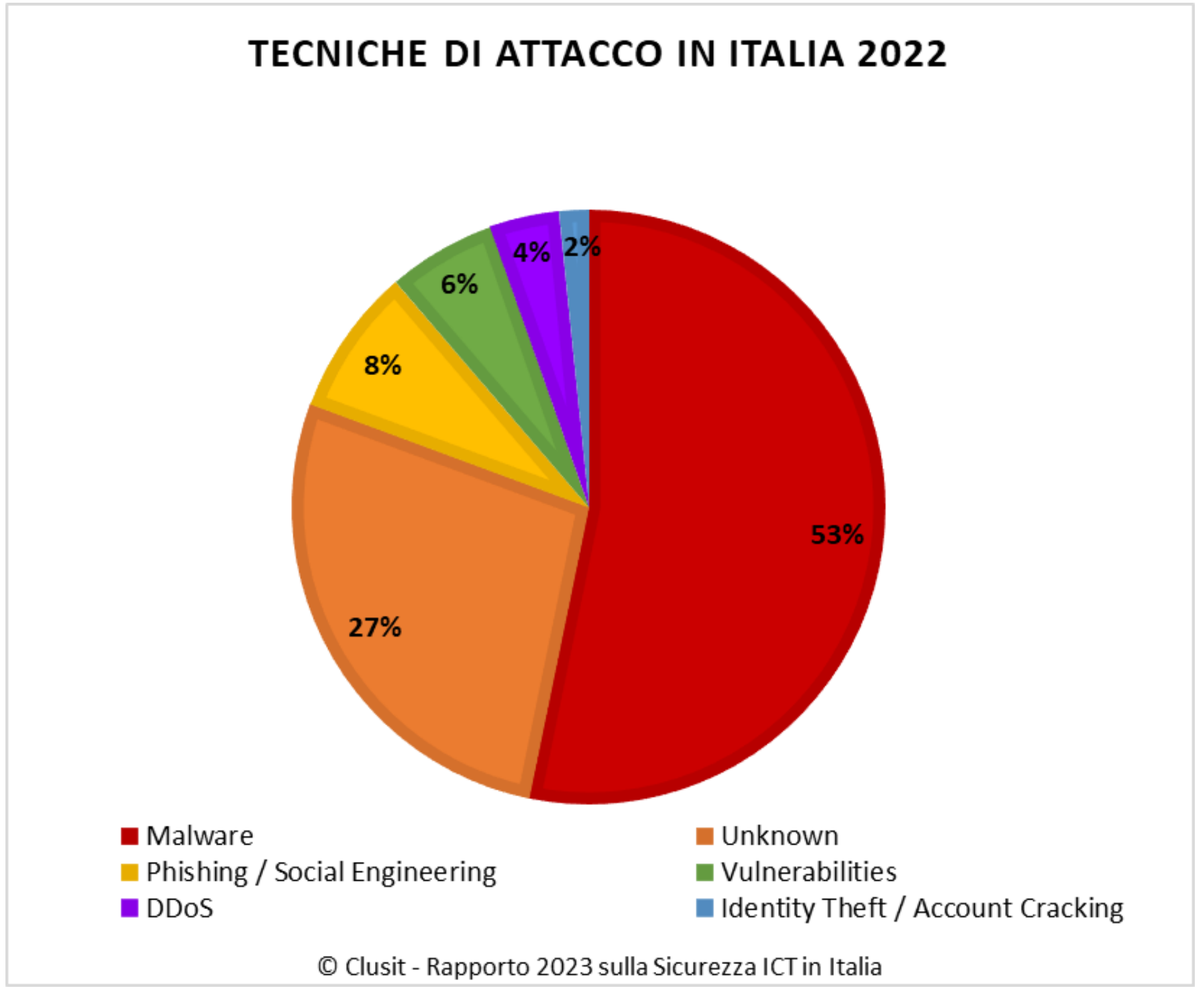
Rispetto al 2021, si rileva un aumento del numero degli attacchi per tutte le aree merceologiche, con una forte crescita della categoria «Multiple Targets» che passa da 2 a 20 attacchi rilevati (**+900%**).

DISTRIBUZIONE DELLE TECNICHE DI ATTACCO

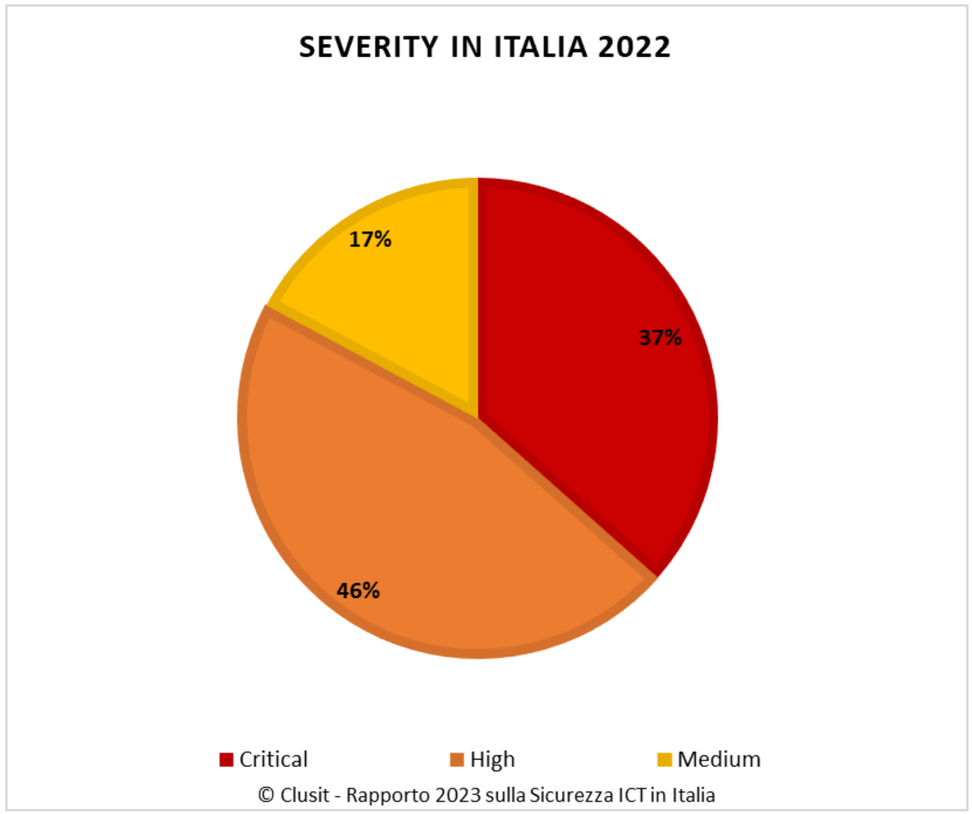
In Italia, tra le tecniche di attacco più utilizzate troviamo:

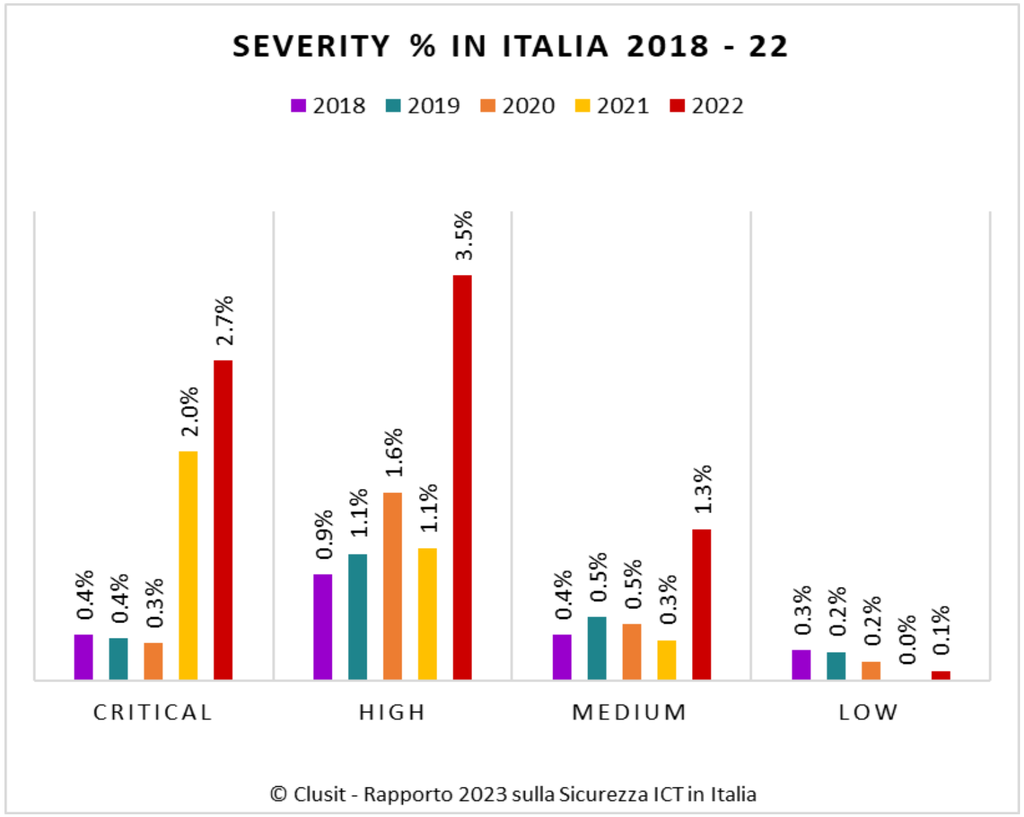
- Malware (53% vs 37% globale)
- Unknown (27% vs 24% globale)
- Phishing / Social Engineering (8% vs 12% globale)

La grande prevalenza del Malware, insieme all'assenza della categoria Multiple Techniques, che include tipicamente gli attacchi più avanzati, fanno pensare che l'aumento degli attacchi in Italia sia con-causato da forti limiti nella capacità di difesa delle vittime



VALUTAZIONE DEGLI IMPATTI





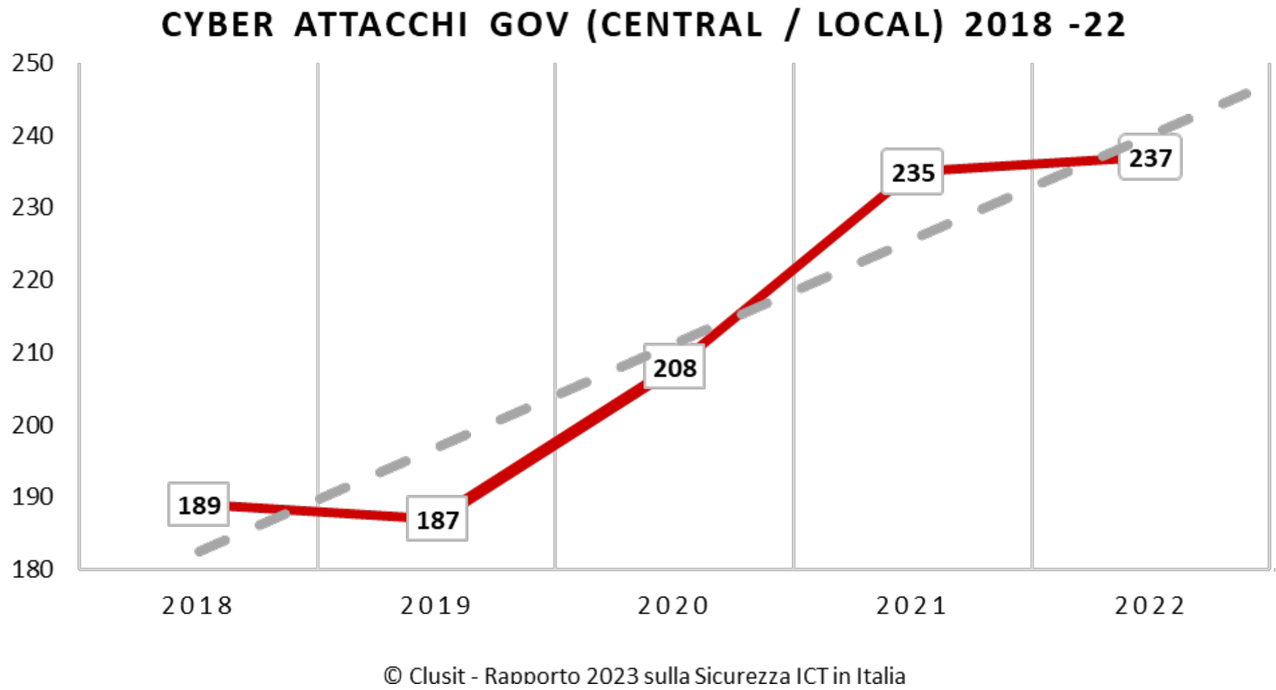
L'**83%** degli attacchi del 2022 in Italia ha avuto un **impatto importante o gravissimo**.
SI rileva un progressivo aumento della severity degli attacchi rispetto al 2021 e agli anni precedenti.

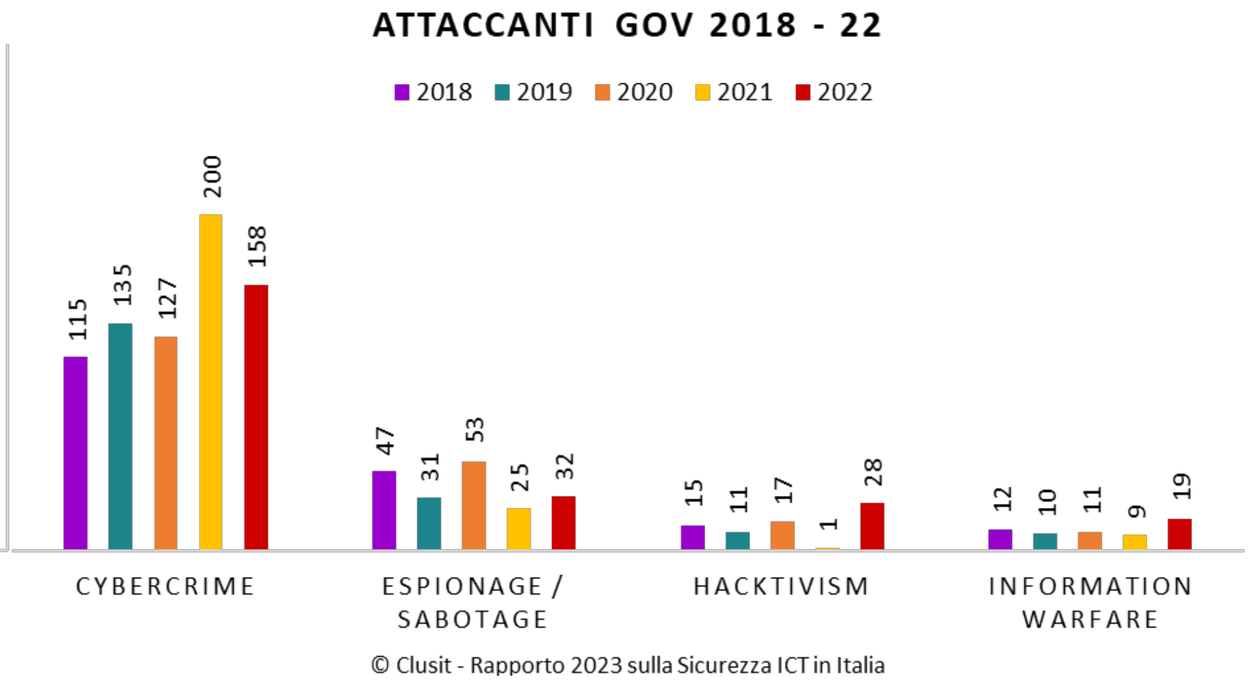
LO SPECIALE CLUSIT DI QUESTA EDIZIONE:
LA SITUAZIONE DELLA **PA (GOVERNO CENTRALE E LOCALE)**

SOFIA SCOZZARI

COMITATO DIRETTIVO
CLUSIT

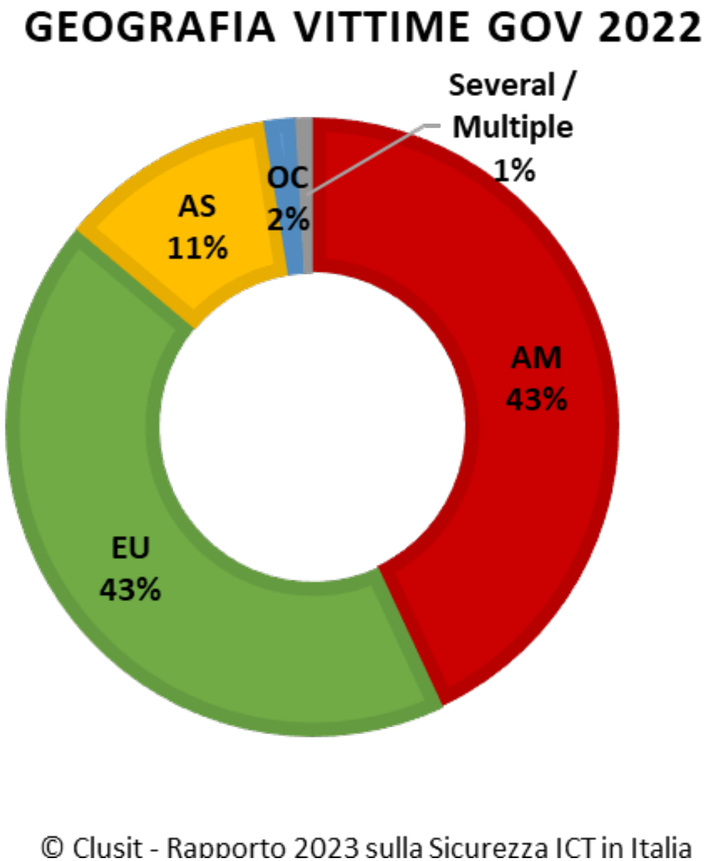
SCENARIO E ATTACCANTI



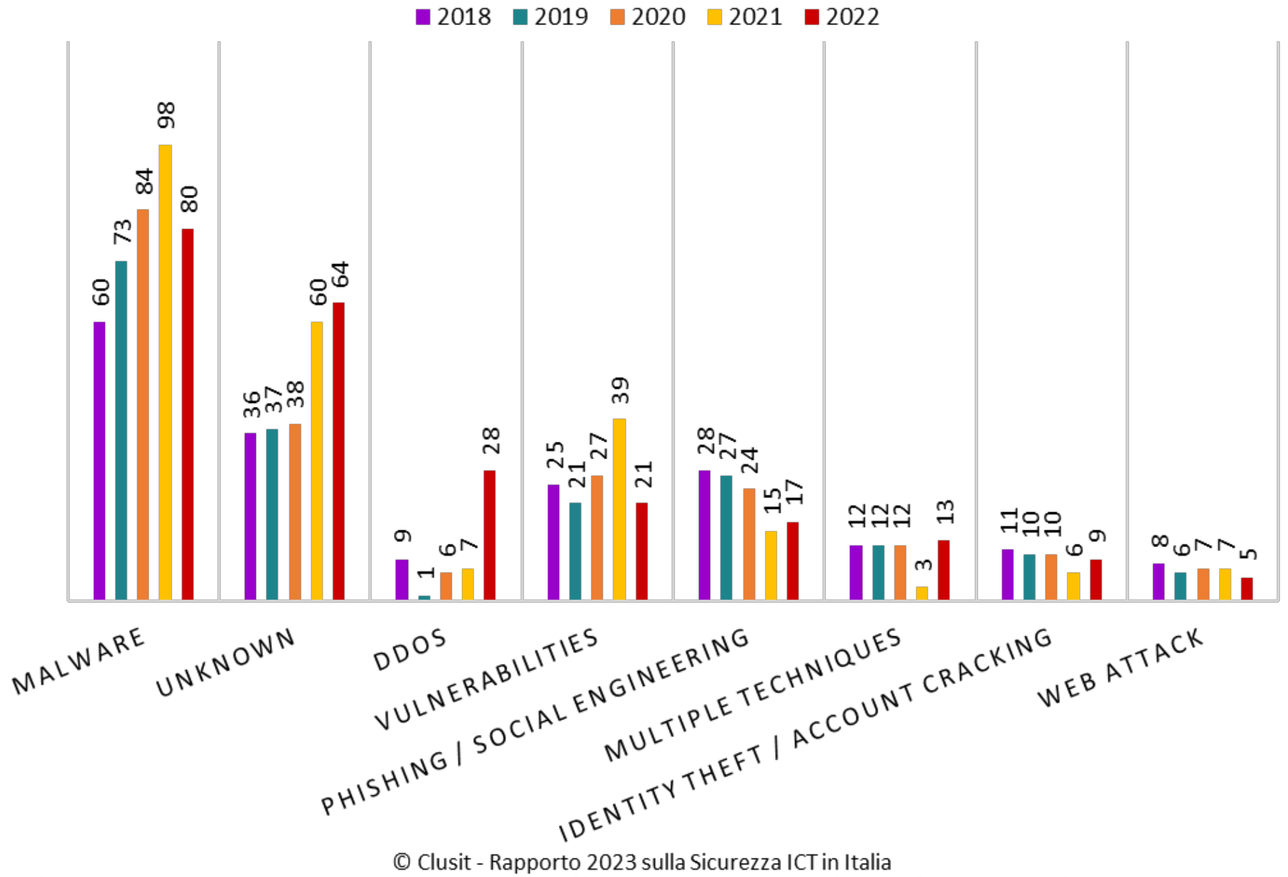


Nel 2022 gli attacchi verso la PA (governo centrale o locale) rappresentano il **9.5% del totale**, in leggero calo rispetto all'anno precedente (erano l'11.5%).

GEOGRAFIA DELLE VITTIME E TECNICHE DI ATTACCO



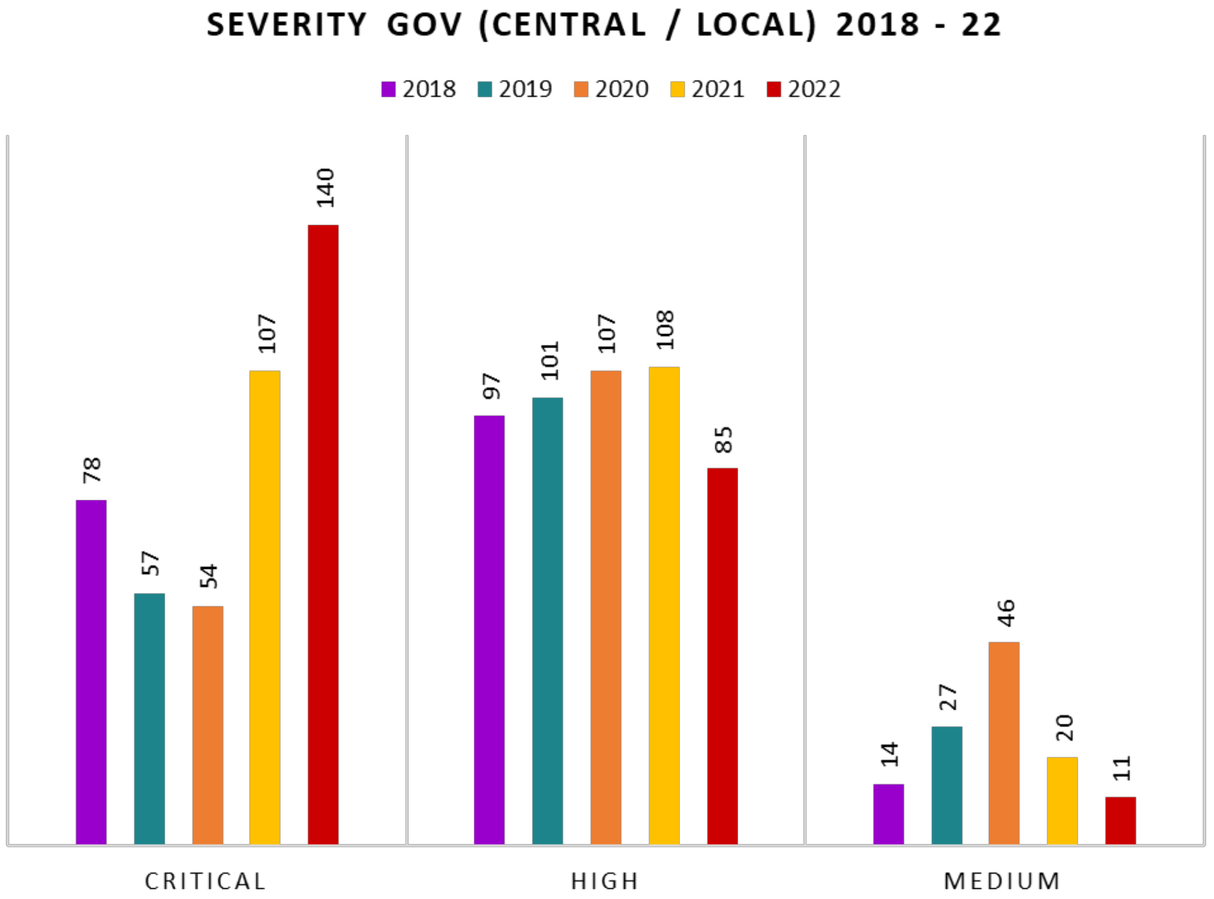
© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

Nel 2022 gli attacchi sono prevalentemente distrubuiti tra il continente americano e quello europeo e il **Malware** è la tecnica preferita nel **34%** dei casi.

SEVERITY DELLA PA



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

Gli incidenti in questo settore hanno impatti gravi o gravissimi nel **95%** dei casi (contro l'80% degli attacchi globali).

TRENDS E PREVISIONI

- L'**anno dei record** (totale attacchi, media mensile, Manufacturing 5%, Multiple Techniques 7% e DDoS 5%, Europa Vs America, severity Critica (36%)

--> in particolare il settore Manufacturing sarà sempre più esposto

- Diminuisce il gap tra **America** (38%) ed **Europa** (24%)

--> l'Europa potrebbe veder crescere il numero di attacchi

- Gli attacchi aumentano in **numeri, frequenza, complessità** (aumentano i fattori multipli), **impatti**

--> I numeri continueranno a crescere

- **Malware** (ransomware) resta la tecnica preferita (37%)

--> il ricorso al ransomware non accenna a diminuire

- **Healthcare** e **Gov. / Mil. / LE** i settori più colpiti dopo Multiple targets
- Attacchi verso la **PA** con severi impatti (95%)
- **Italia** sovrarappresentata nel mondo cyber (7,6% degli attacchi totali) rispetto al PIL (2,2% di quello mondiale), con una crescita importante nell'ultimo anno (+169%)

CONCLUSIONI

- Rafforzare la **governance dei processi di patch & vulnerability management**
- **Security by design** come parte integrante dei processi di sviluppo di nuovi prodotti/soluzioni
- Incrementare ma soprattutto razionalizzare gli **investimenti in Cyber Security**
- **PNRR**: cogliere le opportunità con adeguata priorità alla Cyber Security
- Passare da driver normativi a **processi di valutazione e gestione del rischio**
- Colmare lo **skill gap**
- In particolare in Italia: ridurre la **frammentazione di infrastrutture e servizi** ed evolvere i processi di **monitoraggio, incident response, crisis management e SOC**
- Creare una **cultura della Cyber Security**, patrimonio di tutti i cittadini