Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT
STREAMING EDITION

ASTREA Advanced Security, Training Research, Events Agency

Presentazione Rapporto Clusit 2022 ed. Ottobre Streaming Edition

9 novembre 2022 orario 09.30-11.30

#securitysummit #streamingedition

Agenda

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

Saluto istituzionale e Intervento del Prof. **Roberto Baldoni**, Direttore dell' Agenzia per la Cybersicurezza Nazionale

Intervengono alcuni degli autori:
- **Andrea Zapparoli Manzoni**, CD Clusit

Segue una tavola rotonda, moderata da **Alessio Pennasilico**, CTS Clusit, 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:

- **Aldo Di Mattia**, Fortinet
- **Luca Nilo Livrieri**, Crowdstrike
- **Carlo Mauceli**, Microsoft

INTRODUZIONE

GABRIELE FAGGIOLI

PRESIDENTE CLUSIT

ROBERTO BALDONI

DIRETTORE DELL' AGENZIA PER LA CYBERSICUREZZA NAZIONALE

I CONTENUTI DEL RAPPORTO

ALESSIO PENNASILICO

COMITATO SCIENTIFICO
CLUSIT

I contenuti del Rapporto

Panoramica sull'evoluzione del cyber crime in Italia e nel mondo – Edizione ottobre 2022

- Analisi dei principali cyber attacchi noti nel primo semestre 2022 a livello globale
- Attività e segnalazioni della Polizia Postale e delle Comunicazioni nel primo semestre 2022
- Geopolitica e Cybersecurity

Profili Cyber ultra-specializzati e nuovi trend del mercato del lavoro

(Ultra-specializzazioni, RAL crescenti e strategie di attraction e retention delle aziende)

Focus On
Operation Technology Security – Ultima chiamata

"Effetti della guerra sulla sicurezza delle Infrastrutture Critiche" - una questione di cyber resilience quale calibrata sintesi di risk management, business continuity & cybersecurity

Le interviste con i partner istituzionali
Centro di competenza italiano sulla cybersecurity CYBER 4.0

ANALISI CLUSIT DEI PRINCIPALI ATTACCHI A LIVELLO GLOBALE

ANDREA ZAPPAROLI MANZONI

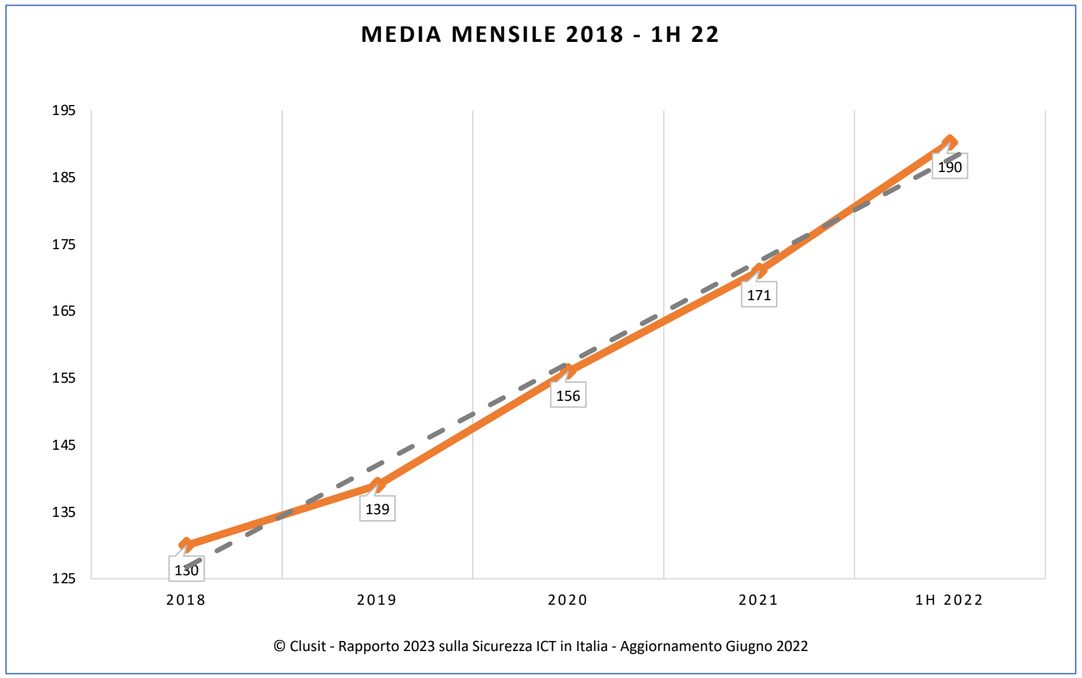
COMITATO DIRETTIVO

CLUSIT

I numeri del campione

Negli ultimi 11 anni abbiamo analizzato e classificato in media 109 attacchi gravi di dominio pubblico al mese. Negli ultimi 4 anni e mezzo sono stati 129 nel 2018, 137 nel 2019, 156 nel 2020, 171 nel 2021 e 190 nei primi 6 mesi del 2022.

- **15.151** attacchi gravi analizzati dal gennaio 2011 al giugno 2022 (di cui oltre metà, **8.285,** dal 2018).
- ...
- 873 nel 2014
- 1.012 nel 2015
- 1.050 nel 2016
- 1.127 nel 2017
- **1.552 nel 2018**
- **1.670 nel 2019**
- **1.871 nel 2020**
- **2.049 nel 2021**
- **1.141 nel primo semestre 2022**



Osservando la situazione dal punto di vista quantitativo, confrontando i numeri del primo semestre 2018 con quelli del 2022 la crescita degli attacchi è stata del 53% (da 745 a 1.141). In 4 anni e mezzo la media mensile di attacchi gravi a livello globale è passata da 129 a 190. Dal punto di vista qualitativo, anche la loro 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, a partire da questa edizione, 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 da quest'anno 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).**

20 macro-categorie merceologiche e 141 sotto-categorie.

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

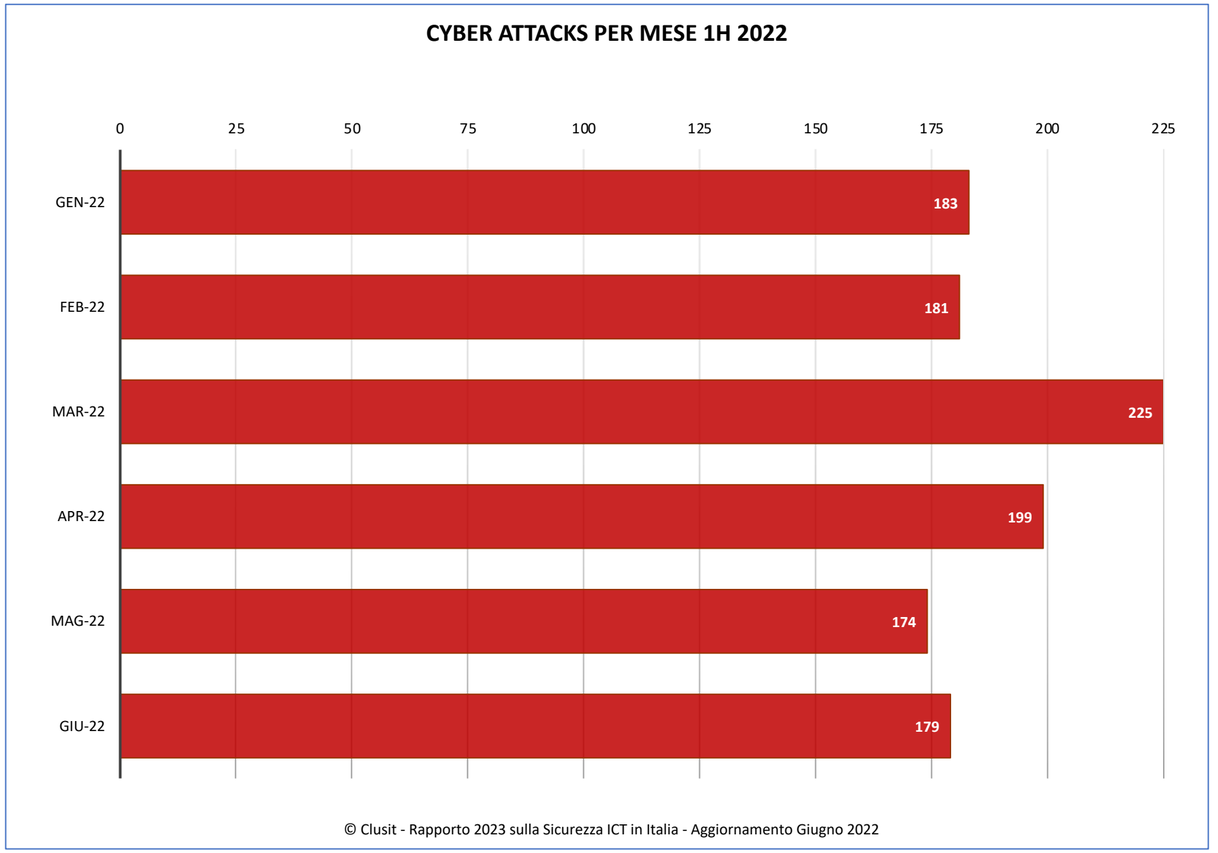
8 macro-categorie e 59 sotto-categorie

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 e 13 sottocategorie

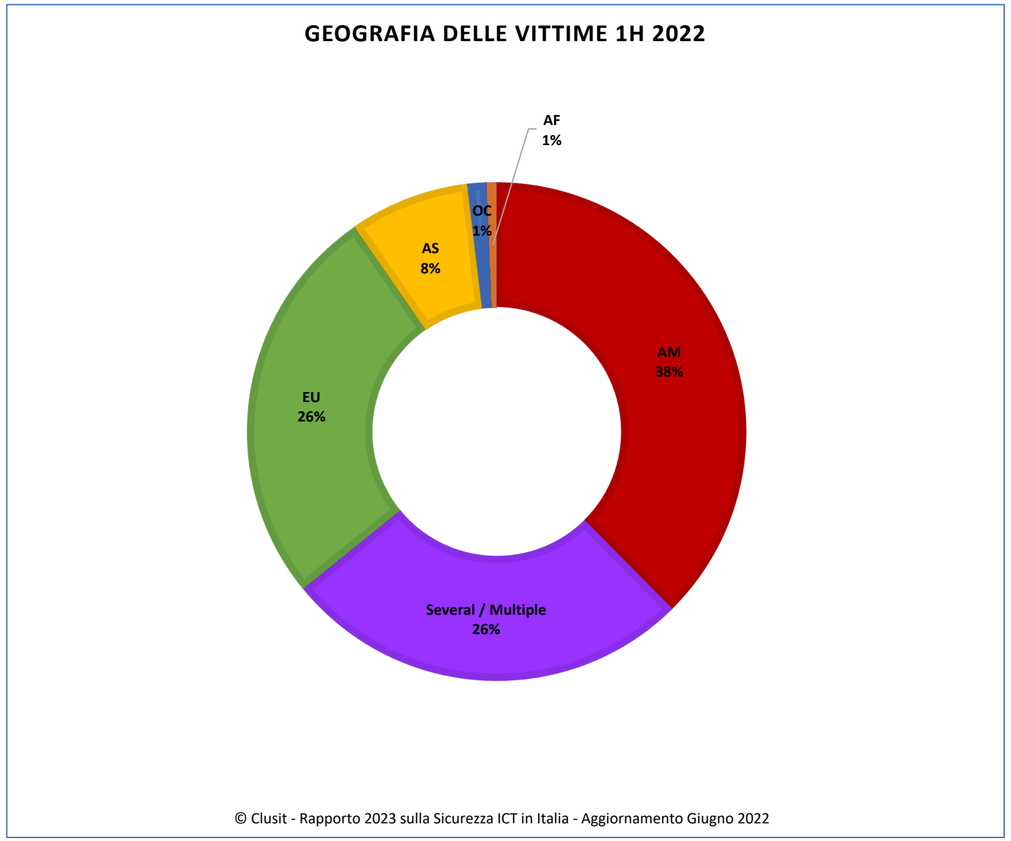
Oltre ad aver rivisto completamente il modello abbiamo anche **riclassificato** tutti gli attacchi del triennio precedente (5.095) per renderli confrontabili con quelli del 2021 (2.049) e del 1H 2022 (1.141) e non perdere così la visione "prospettica" dei fenomeni, che è una delle caratteristiche più distintive di questa ricerca.

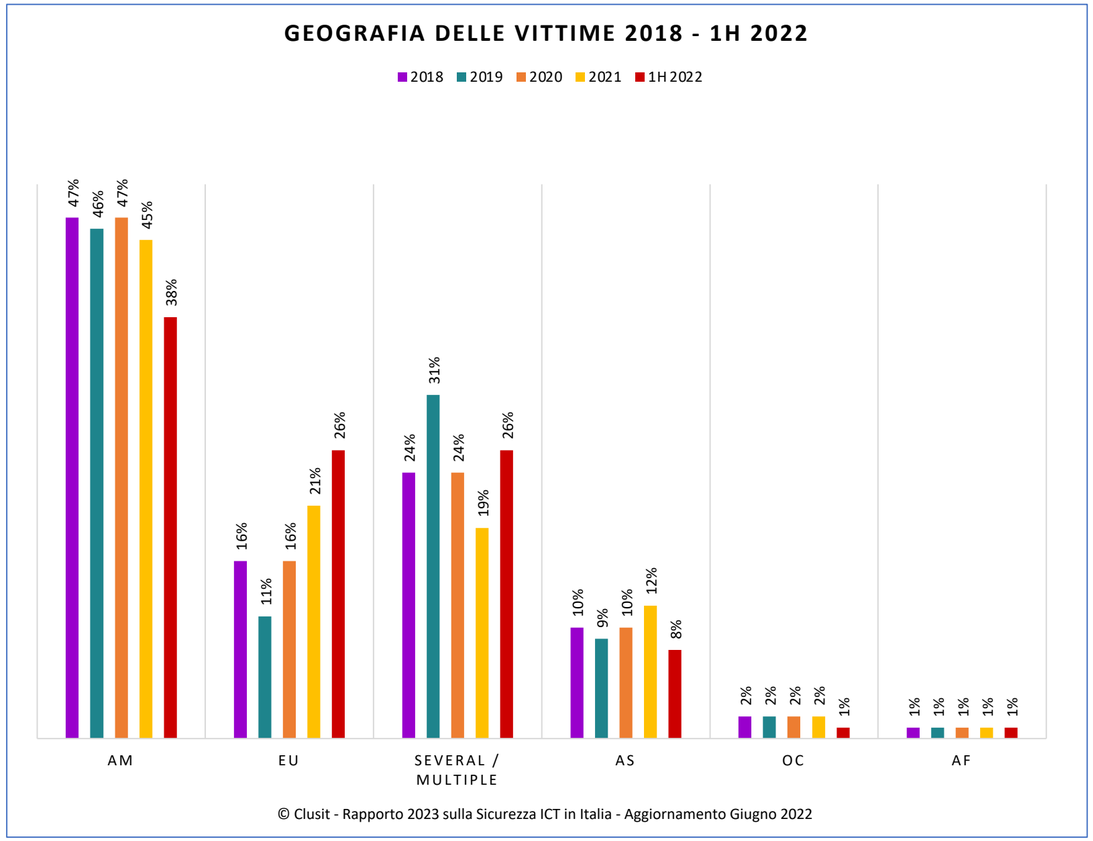
Attacchi per mese nel 1H 2022



Nel 1H 2022 i picchi maggiori (sopra alla media dell'anno) si sono avuti a Marzo e Aprile, in corrispondenza con l'inizio delle ostilità tra Russia e Ucraina.

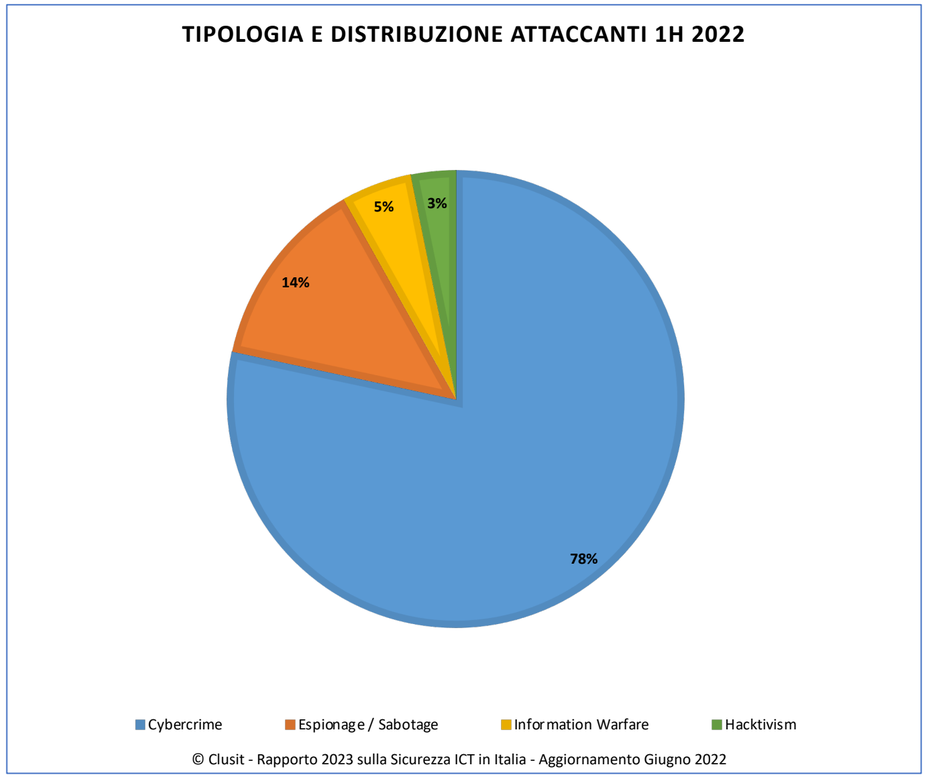
Distribuzione geografica vittime





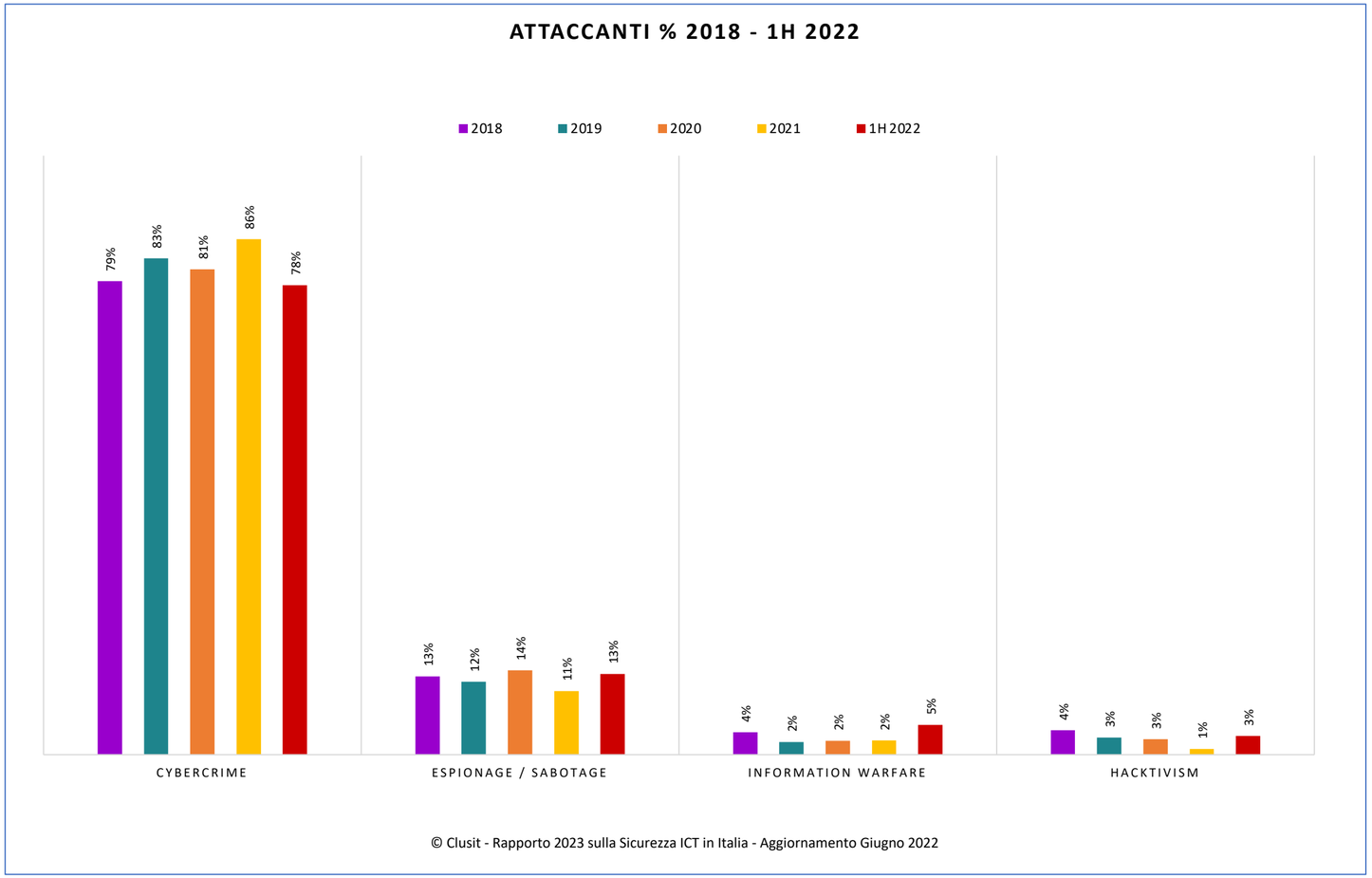
Nel 2022 diminuiscono le vittime di area americana (dal 45% al 38%), mentre gli attacchi verso realtà basate in Europa aumentano sensibilmente (dal 21% al 26%) e scendono leggermente quelli rilevati contro organizzazioni asiatiche (dal 12% al 8%). Percentualmente aumentano gli attacchi gravi verso bersagli con sedi distribuite in diversi Paesi (categoria “Several / Multiple”), che dal 19% del 2021 passano al 26%.

Tipologia e distribuzione degli attaccanti

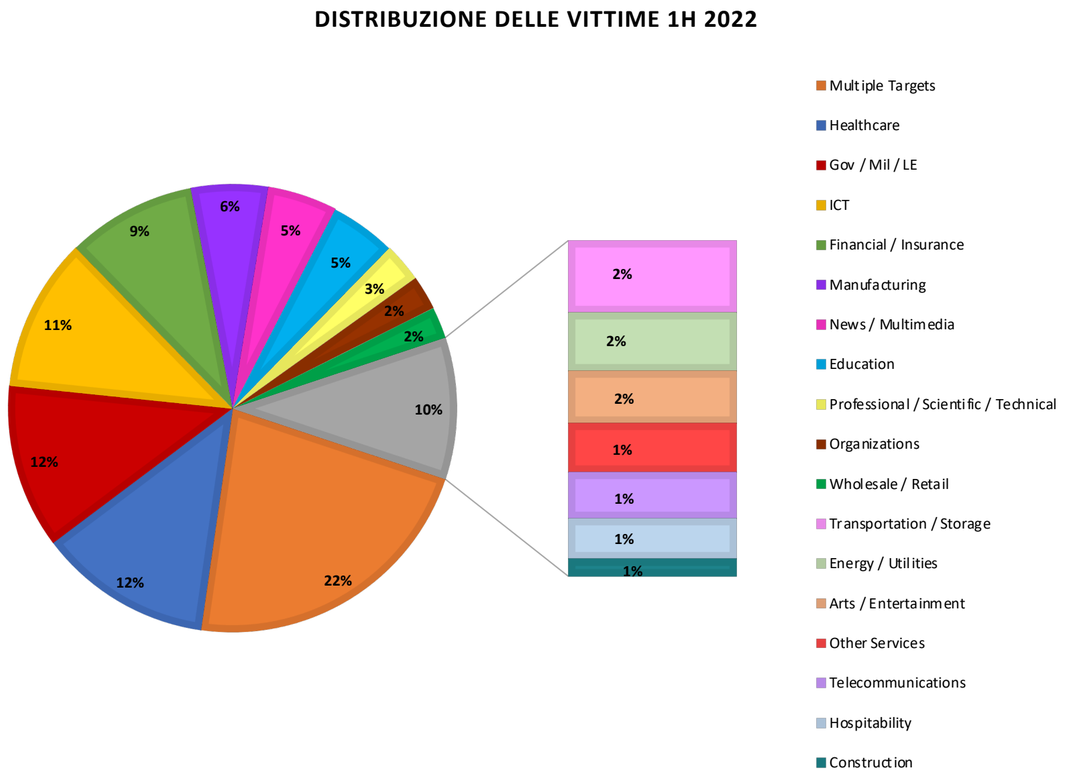


Dal campione emerge chiaramente che rispetto al 2021 le attività riferibili ad attacchi della categoria “Hacktivism” tornano ad aumentare sensibilmente (+414,3%), principalmente a causa della guerra in Ucraina. Per la stessa ragione sono in forte aumento sia gli attacchi compiuti per finalità di “Espionage” (+62,1%) che quelli riferibili a “Information Warfare” (+119,2%). Diminuiscono leggermente gli attacchi classificati come attività di “Cybercrime” (-3,4%) dopo il picco straordinario del 2021.

Tipologia e distribuzione degli attaccanti (2018 – 1H 2022)



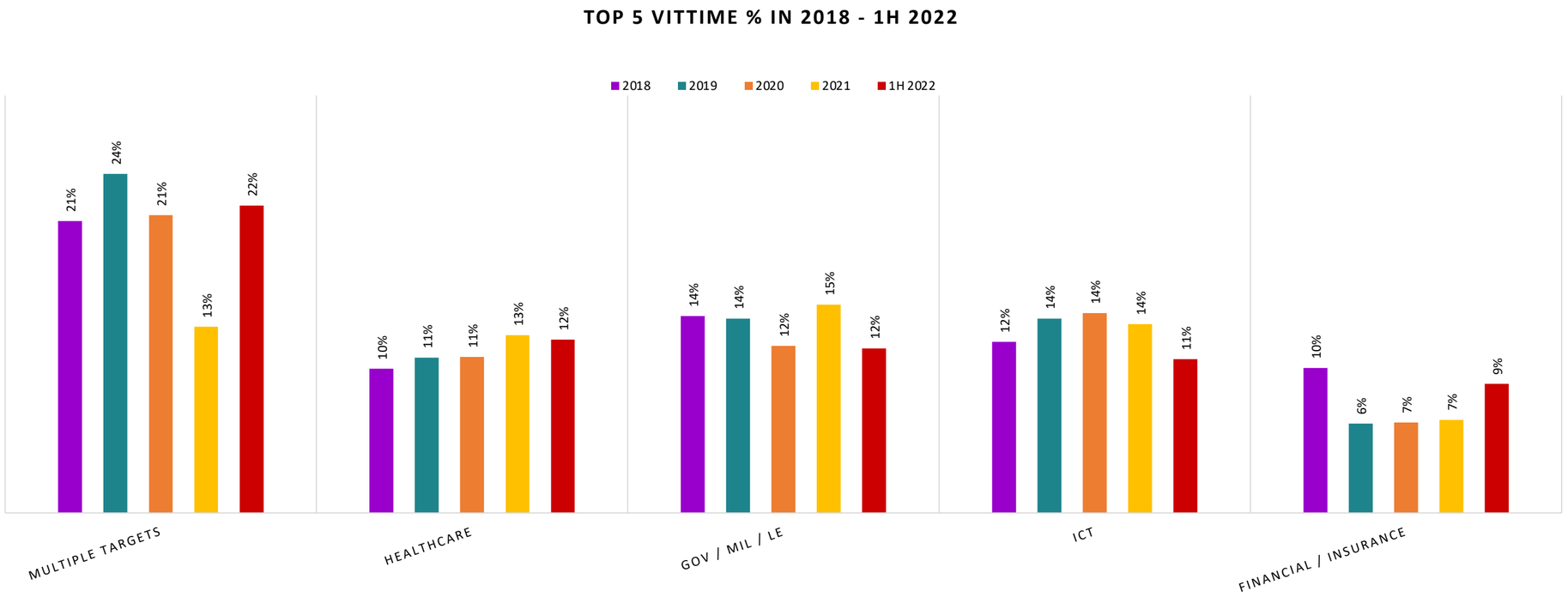
Distribuzione vittime nel mondo (1h 2022)



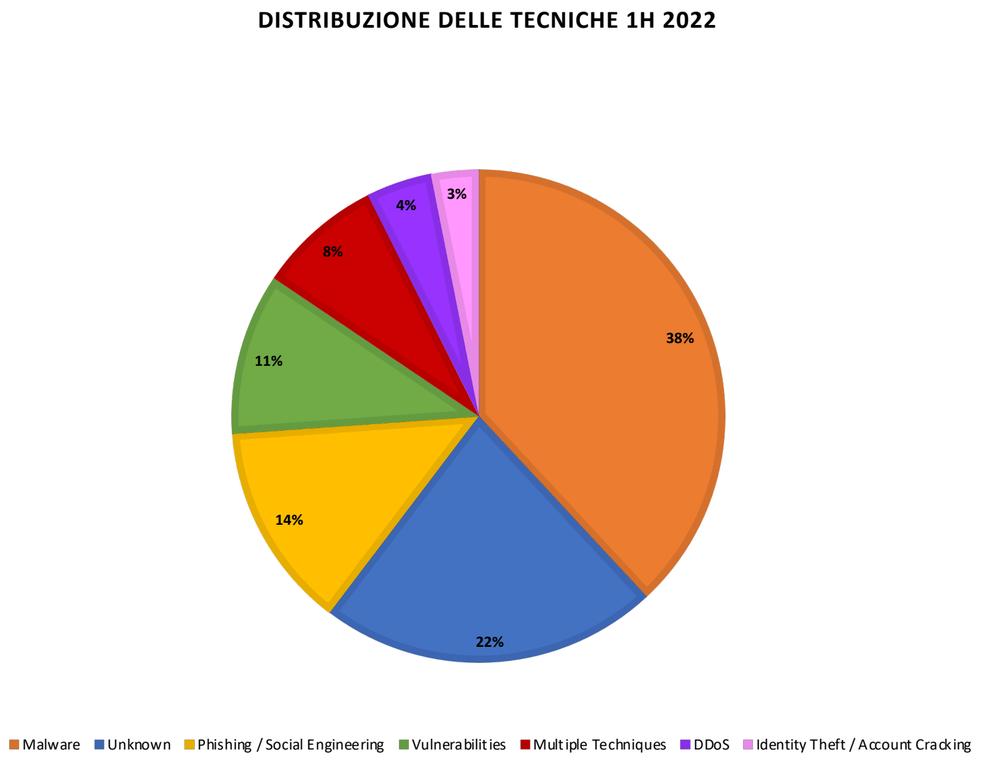
© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2022

In termini percentuali nel primo semestre 2022 la categoria “Multiple Targets” torna al primo posto assoluto (22% del totale). Al secondo e terzo posto “Healthcare” e “Gov / Mil / Law Enforcement”, ciascuna con circa il 12% degli attacchi totali, al quarto “ICT” al 11%, ed al quinto “Financial / Insurance”, al 9%.

Distribuzione vittime nel mondo (2018 - 1h 2022)



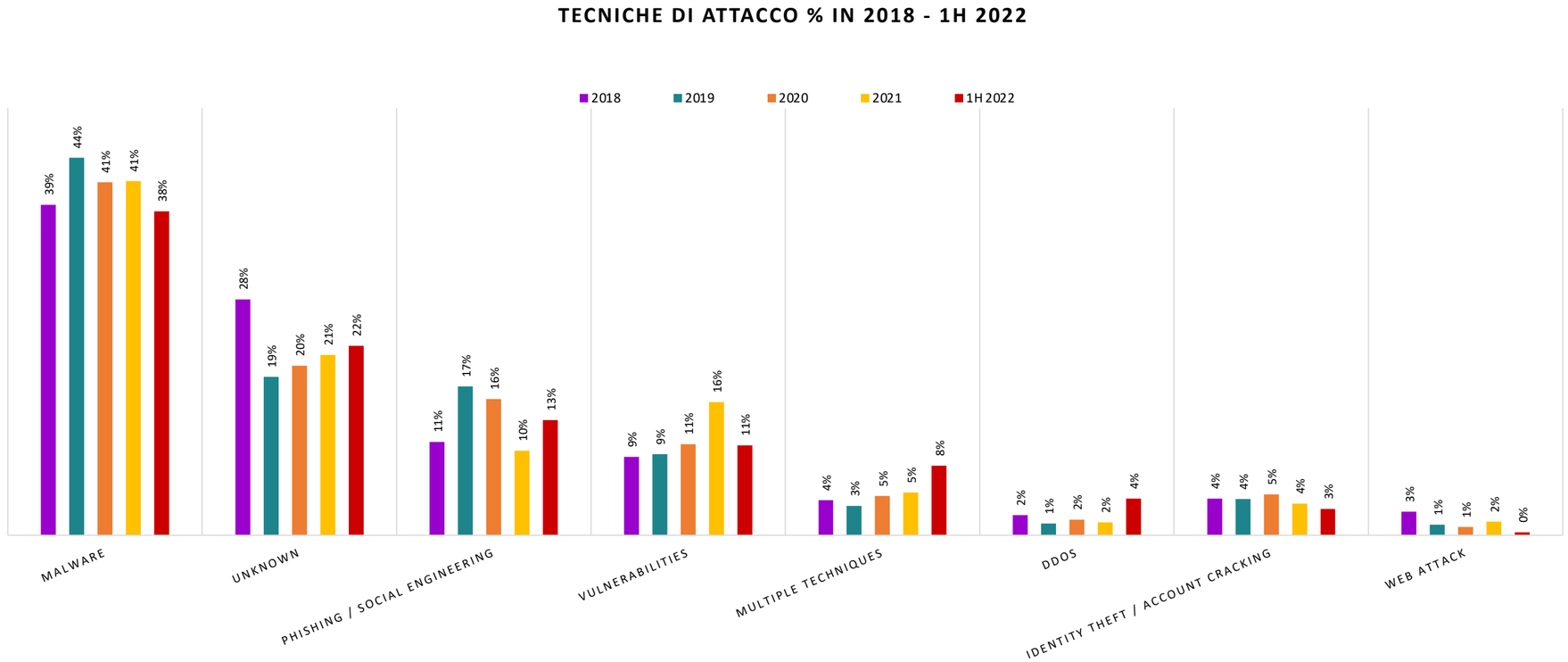
Tecniche di attacco (1H 2022)



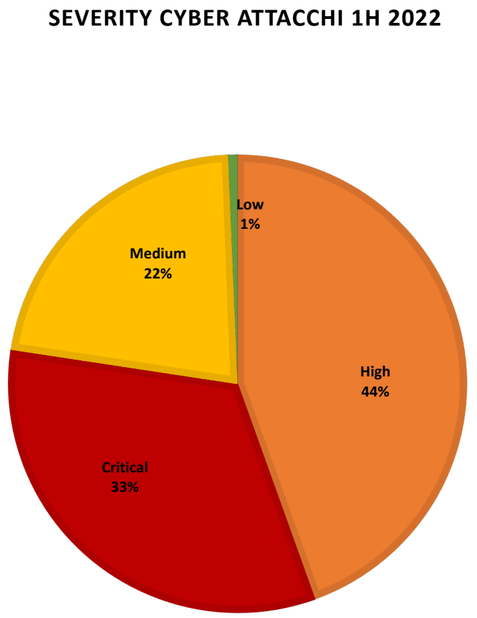
© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2022

Nel primo semestre 2022 la categoria che mostra numeri assoluti maggiori è “Malware”, che sia pure in leggera flessione (-4,6%) rappresenta il 38% del totale. Le tecniche sconosciute (categoria “Unknown”) tornano al secondo posto, con una aumento del 10% rispetto al primo semestre 2021, superando la categoria “Vulnerabilità” (-26,8%) e “Phishing / Social Engineering” (in netta crescita, +63,8%), mentre “Tecniche Multiple” sale del +93,8%, in conseguenza della natura sempre più complessa degli attacchi.

Tecniche di attacco (2018 - 1H 2022)



Valutazione degli impatti (“Severity”) – 1H 2022



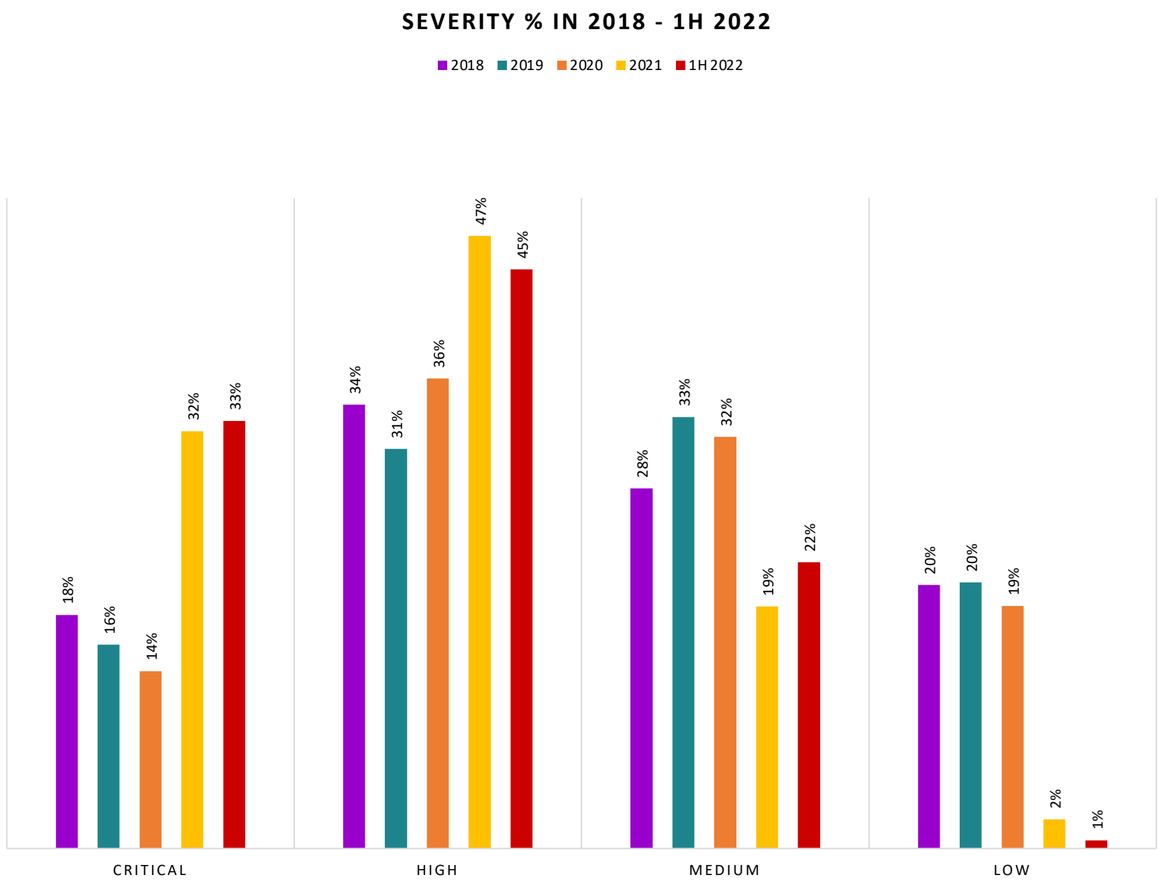
© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2022

Nella nuova classificazione abbiamo definito quattro categorie o livelli di impatto (considerato che stiamo comunque analizzando un campione di attacchi già tutti definiti come “gravi”): Basso, Medio, Alto e Critico.

Le variabili che contribuiscono a comporre la valutazione dell’impatto per ogni singolo attacco analizzato sono molteplici, ed includono: impatto geopolitico, sociale, economico (diretto e indiretto), di immagine e di costo/opportunità per le vittime.

Gli attacchi gravi con effetti molto importanti (High) sono il 44%, quelli devastanti (Critical) il 35%, quelli di impatto significativo (Medium) il 22%, e quelli con impatto basso solo l’1%. Nel primo semestre 2022, gli attacchi con impatto Critical e High sono il 78% del totale.

Valutazione degli impatti (“Severity”) – 2018 - 1H 2022



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2022

Tavola rotonda

modera **Alessio Pennasilico**, CTS Clusit

con gli esperti di security di alcuni dei principali fornitori di prodotti e servizi di sicurezza ICT:

- **Aldo Di Mattia**, Fortinet
- **Luca Nilo Livrieri**, Crowdstrike
- **Carlo Mauceli**, Microsoft

#securitysummit #streamingedition

Q&A

PER MAGGIORI INFORMAZIONI:

RAPPORTI@CLUSIT.IT

GFAGGIOLI@CLUSIT.IT

APENNASILICO@CLUSIT.IT

AZMANZONI@CLUSIT.IT

ADIMATTIA@FORTINET.COM

CARLO.MAUCELI@MICROSOFT.COM

LUCA.NILOLIVRIERI@CROWDSTRIKE.COM

INFO@CLUSIT.IT

INFO@ASTREA.IT

#SECURITYSUMMIT #STREAMINGEDITION