Italia e PA 2024

Rapporto

2024

sulla sicurezza ICT
in Italia

SECURITY SUMMIT

Rapporto Clusit

Italia e PA

2024

SECURITY SUMMIT

ASTREA Advanced Security, Training Research, Events Agency

Via Copernico, 38 - 20125 Milano

Sommario

Indice dei Grafici

Executive summary

Gli attacchi condotti dalla criminalità organizzata verso l'Italia sono in aumento più che nel resto del mondo. I dati del fenomeno sono particolarmente impressionanti: nell'ultimo quinquennio gli attacchi significativi registrati nel nostro Paese sono complessivamente decuplicati, mentre quelli specificamente rivolti verso la Pubblica Amministrazione sono aumentati di circa sei volte. Fra il 2022 e il 2023 il numero di attacchi condotti ai danni di soggetti italiani è cresciuto del 65%, mentre nel resto del mondo solo del 12%. Nel 2023 ben l'11% degli attacchi registrati nel mondo ha avuto luogo nel nostro Paese, mentre nel 2012 erano meno dell'8% e nel 2011 meno del 3,5%.

L'Italia sta quindi subendo un attacco sistematico e senza precedenti, le cui concause possono verosimilmente essere identificate sia in una digitalizzazione tardiva e affrettata delle nostre imprese ed amministrazioni, sia e soprattutto nella atavica mancanza di una corretta e consolidata cultura della sicurezza nella maggior parte degli operatori economici e produttivi nazionali, che sono costituiti da imprese e pubbliche amministrazioni di dimensioni piccole e piccolissime.

Introduzione e scenario

Questo aggiornamento del Rapporto Clusit 2024 vuole approfondire l'analisi sulla situazione degli attacchi rivolti verso il nostro Paese, ed in particolare su quelli specificamente indirizzati verso la Pubblica Amministrazione.

In questi ultimissimi anni purtroppo l'Italia è sottoposta ad un livello di attacchi assai rilevante, e soprattutto caratterizzato da un tasso di crescita molto più sostenuto rispetto a quello rilevato negli altri Paesi del mondo. In effetti sino al 2022 il Rapporto Clusit non presentava dati specifici sugli attacchi verso l'Italia, in quanto i relativi numeri erano così ridotti da essere considerati statisticamente non significativi: purtroppo però la situazione si è aggravata così rapidamente che a partire dal Rapporto 2023 (relativo ai dati del 2022) abbiamo ritenuto necessario presentare in un'apposita sezione i dati italiani, che oramai non erano più trascurabili. In effetti il numero complessivo di attacchi significativi condotti verso il nostro Paese è praticamente decuplicato in soli cinque anni, passando dai meno di quaranta nel 2019 agli oltre trecento del 2023; di questi, quelli specificamente rivolti alla Pubblica Amministrazione sono aumentati di circa sei volte, passando dai meno di dieci del 2019 ai quasi sessanta del 2023.

Alla luce di questo fenomeno, praticamente unico nel panorama mondiale, abbiamo dunque ritenuto necessario produrre un aggiornamento specifico per analizzare la situazione nazionale in modo più dettagliato. A tal proposito facciamo osservare che i dati analizzati in questo approfondimento sono quelli relativi a tutto il 2023, perché quelli relativi agli attacchi condotti verso la Pubblica Amministrazione italiana nel primo trimestre 2024 sono al momento scarsi e comprendono solo un ristretto numero di casi di attivismo di matrice politico-ideologica (attacchi DDoS); abbiamo quindi preferito mantenere la consistenza e soprattutto la significatività dell'analisi considerando solo i dati dell'anno precedente, e svolgendo su di essi alcuni approfondimenti riguardanti il settore pubblico che non erano stati sviluppati nel Rapporto generale presentato a marzo 2024.

La situazione generale in Italia

Negli ultimi anni, in particolare dal 2021, l'Italia ha iniziato ad essere colpita da un significativo numero di attacchi, diretti verso tutti i settori di attività pubblici e privati. E da allora il nostro Paese sembra essere diventato una delle vittime preferite della grande criminalità cibernetica internazionale, come dimostrato dalla crescita vertiginosa del numero di attacchi da un anno all'altro.

Osservando il grafico di **Figura 1**, che riporta il numero annuale di attacchi significativi rilevati in Italia dal 2009, appare evidente come la loro crescita sia stata complessivamente più che lineare, con una forte impennata fra il 2021 e il 2022. In effetti gli attacchi sono cresciuti di quasi un ordine di grandezza nel quinquennio, passando dai 37 del 2019 ai 310 del 2023.

Questi elevati tassi di crescita del numero di attacchi purtroppo non si riscontrano nel resto del mondo, e sono dunque un fenomeno anomalo che sta caratterizzando quasi solo il nostro Paese. Ciò è bene evidenziato dal grafico di **Figura 2**, nel quale sono messi a confronto gli incrementi relativi (anno su anno) del numero di attacchi in Italia (linea azzurra) e nel mondo (linea rossa) a partire dal 2019. Osservandolo si vede infatti chiaramente come i tassi medi di incremento annuale su tutti i Paesi siano rimasti compresi fra il 9% e il 21% circa nel quinquennio, mentre in Italia sono andati da un minimo del 30% ad un massimo di quasi il 170%: dunque una crescita dalle tre alle otto volte maggiore rispetto all'incremento medio globale dell'anno corrispondente.

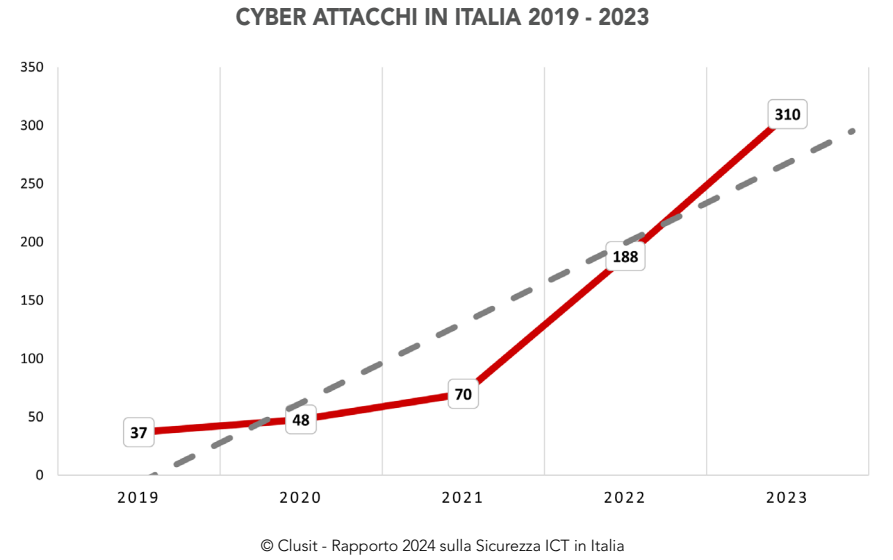

Figura 1 - Numero di attacchi rilevati in Italia negli ultimi cinque anni

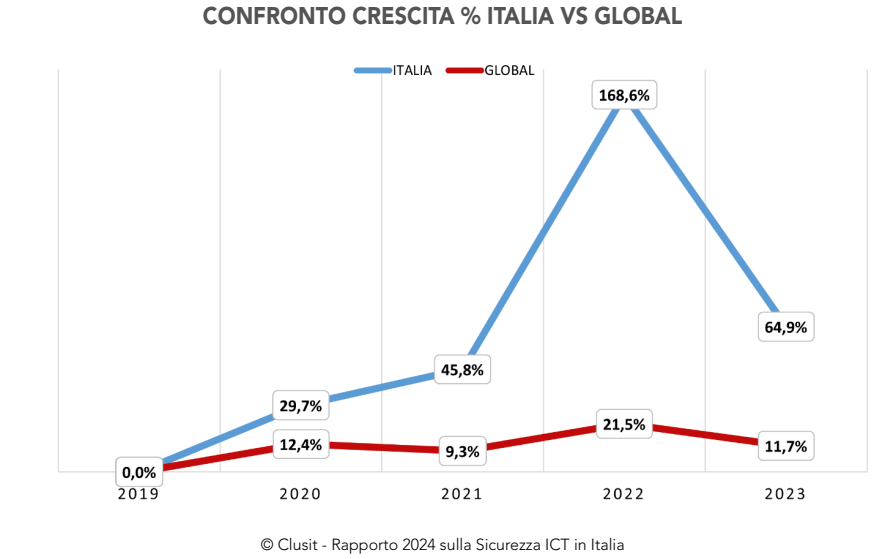

Figura 2 - Incrementi anno su anno del numero di attacchi dal 2019 in Italia e nel resto del mondo

Un'altra chiave di lettura sul fenomeno la fornisce il grafico di **Figura 3**, che riporta l'andamento del rapporto tra il numero di attacchi rilevati in Italia e il numero di attacchi globali: ovvero la frazione del numero complessivo di attacchi avente come oggetto l'Italia.

La curva, in forte salita, dimostra assai chiaramente che il numero di attacchi rivolti verso il nostro Paese cresce ad un ritmo significativamente maggiore rispetto a quelli globali. In particolare si evince dai numeri che sino al 2021 l'Italia raccoglieva meno del 3,5% degli attacchi mondiali, ma nel 2022 questa quota è raddoppiata raggiungendo quasi l'8% e nel 2023 ha superato l'11%: in altre parole, lo scorso anno più di un attacco su dieci a livello mondiale ha interessato l'Italia.

Figura 3 - Rapporto tra numero di attacchi rilevati in Italia e nel mondo *(ossia quota parte di attacchi verificatisi in Italia)*

È altresì importante notare come, in questa rapidissima crescita del fenomeno, non si osservi una specifica localizzazione degli attacchi verso specifici ambiti di attività delle vittime: tutte le organizzazioni, sia pubbliche che private, appaiono infatti egualmente colpite, anche quelle appartenenti a settori che fino a due o tre anni fa erano stati toccati solo marginalmente o addirittura per nulla dal cybercrime.

Ciò si vede chiaramente osservando il grafico di **Figura 4**, che riporta la distribuzione del numero di attacchi avvenuti in Italia negli ultimi cinque anni in funzione del settore di attività delle organizzazioni colpite: è evidente la forte crescita, in taluni casi anche esponenziale, che caratterizza tutti i settori. Tra quelli più colpiti risultano particolarmente significativi i casi della Pubblica Amministrazione (prima colonna) e dell'industria manifatturiera (seconda colonna): la prima è infatti passata da meno di dieci attacchi significativi nel 2019 a quasi sessanta nel 2023, con un incremento di oltre sei volte; mentre la seconda è passata da due a più di quaranta, con un incremento di oltre venti volte. Ma sono ancor più impressionanti i casi dei settori trasporti, finanziario e della vendita al dettaglio, che non avevano praticamente avuto attacchi sino al 2021 e solamente negli ultimi due anni sono passati a contarne alcune decine. Più graduale, ma non per questo meno significativo, l'incremento degli attacchi nel settore sanitario: un fenomeno iniziato già diversi anni fa, e caratterizzato da una crescita costante.

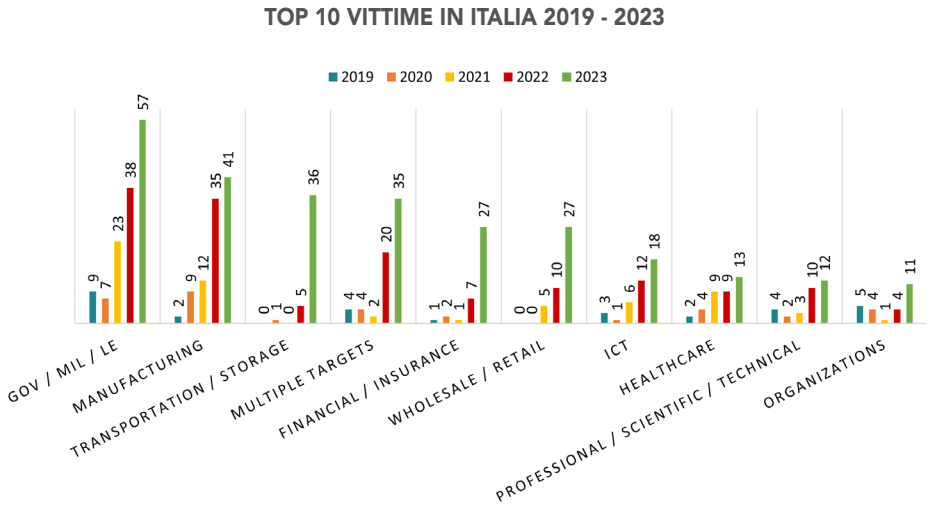

Figura 4 - Distribuzione degli attacchi in Italia rispetto al settore di attività delle organizzazioni colpite

Analizziamo ora il fronte della minaccia, aiutandoci col grafico di **Figura 5** nel quale sono riportati i numeri degli attacchi in funzione della natura e/o delle motivazioni degli attaccanti. Vediamo così che la stragrande maggioranza degli attacchi registrati nel nostro Paese è di matrice puramente criminale, e che questo fenomeno è in

crescita esponenziale: si è infatti passati dai meno di dieci attacchi nel 2019 ai quasi duecento del 2023, con un incremento di oltre venti volte.

Gli altri tipi di obiettivi sono e rimangono secondari e pressoché trascurabili, con l'unica evidente eccezione dell'anomalo picco di attacchi di matrice ideologico-politica verificatosi nel 2023, a fronte di un numero basso e soprattutto costante di eventi analoghi registrati negli anni precedenti. In questo particolare dato si legge chiaramente l'effetto della congiuntura geo-politica internazionale dello scorso anno, legata ai due grandi conflitti che stanno tuttora interessato i territori circum-europei: quello russo-ucraino e quello israelo-palestinese. Entrambi infatti hanno suscitato, nel nostro Paese più che in altri, azioni di protesta e/o iniziative pro o contro l'una o l'altra parte, le quali sono sfociate anche in attacchi cibernetici di natura ideologica e dimostrativa, tipicamente veicolati mediante massicci Denial of Service.

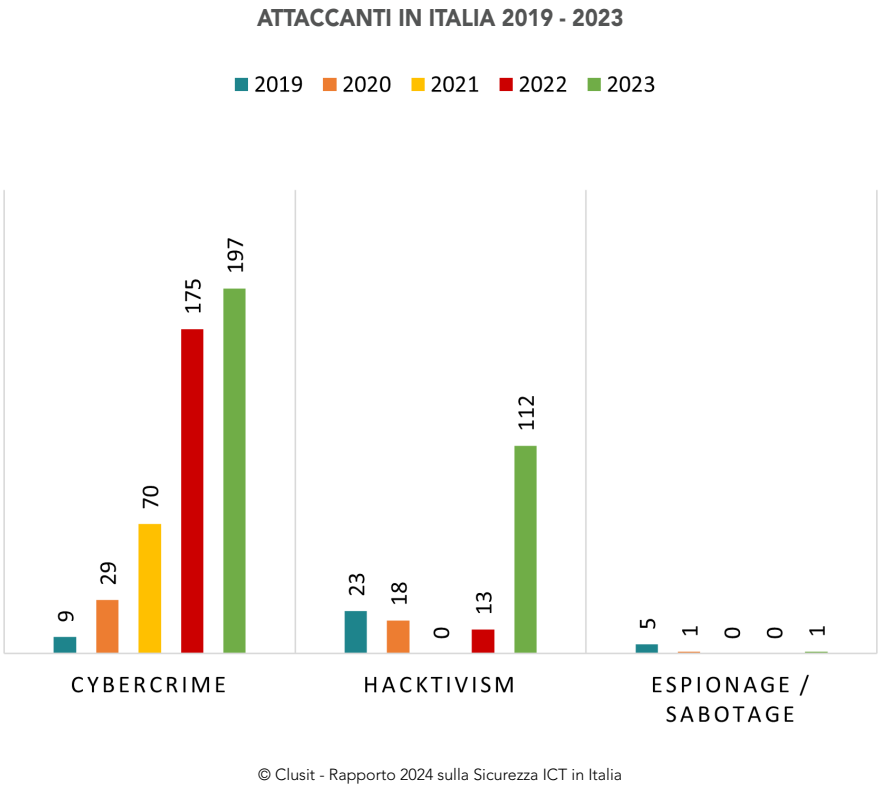

Figura 5 - Distribuzione degli attacchi in Italia rispetto alla tipologia e/o motivazione dell'attaccante

Per quanto riguarda infine le tecniche offensive adottate dagli attaccanti, vediamo dal grafico di **Figura 6** che la stragrande maggioranza è costituita dall'impiego di *malware*, saldamente al primo posto con una crescita nel quinquennio di quasi tredici volte. Al secondo posto, in fortissima crescita relativa, le tecniche di attacco basate sul fattore umano, ossia il cosiddetto *social engineering*: truffe, inganni e raggiri diretti verso le persone che, veicolati anche grazie ai *social network*, si sono moltiplicati negli ultimi due anni mentre erano scarsamente rilevanti in quelli precedenti.

Naturalmente la forte ed anomala presenza di attacchi DDoS nell'ultimo anno è relativa a quei fenomeni di attivismo ideologico-politico già discussi trattando del grafico precedente. Vale infine la pena di ricordare che la categoria "unknown" non rappresenta attacchi "di natura sconosciuta" ma raccoglie semplicemente tutti quei casi in cui la modalità di attacco non è stata resa nota.

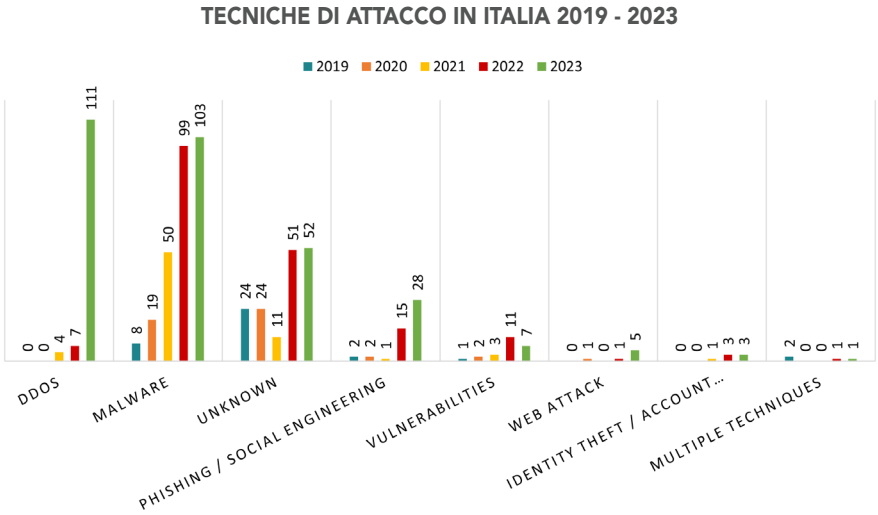

Figura 6 - Distribuzione degli attacchi in Italia rispetto alla tecnica impiegata

La situazione della Pubblica Amministrazione

Stante questa preoccupante situazione complessiva che caratterizza il nostro Paese, andiamo ora a vedere in maggiore dettaglio i dati riguardanti il settore pubblico. E per cogliere meglio l'aspetto evolutivo del fenomeno estendiamo l'analisi comprendendo i dati degli ultimi sei anni, dal 2018 al 2023.

Il grafico di **Figura 7** riporta il numero assoluto di attacchi significativi aventi come obiettivo la Pubblica Amministrazione: si nota chiaramente il cambio di passo avvenuto nel 2021, che ne ha portato il numero a crescere di oltre sette volte nel solo ultimo triennio.

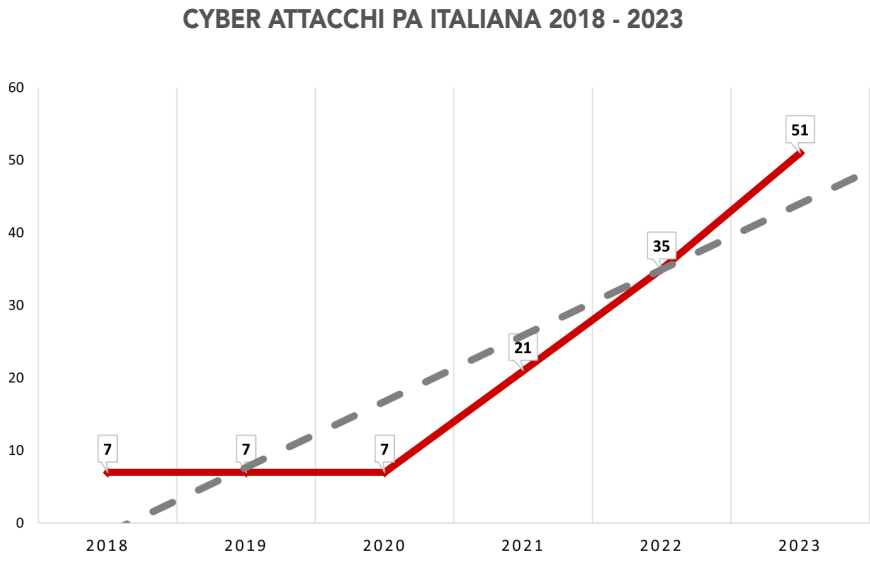

Figura 7 - Numero di attacchi significativi aventi per obiettivo la Pubblica Amministrazione italiana

È interessante confrontare questo andamento con quello degli attacchi generali condotti verso l'Italia, per evidenziare in particolare i rispettivi tassi di crescita annuali. Lo facciamo grazie al grafico di **Figura 8** che riporta, appunto, le variazioni relative anno su anno del numero di attacchi condotti in Italia verso il solo settore pubblico (linea azzurra) e verso tutti i settori (linea rossa), considerando unitario il dato del 2018. Naturalmente la linea rossa di questo grafico rappresenta il medesimo andamento della linea azzurra che abbiamo già visto nel grafico di Figura 2, solo estesa indietro al 2018.

Ebbene, le curve mostrano che la nostra Pubblica Amministrazione è stata in effetti colpita dalla nuova ondata di attacchi con un anno di anticipo rispetto agli altri settori: un fenomeno che era stato largamente previsto negli anni precedenti da molti analisti, i quali avevano correttamente indicato il settore pubblico come maggiormente a

rischio rispetto a quello privato. Attualmente comunque il numero di attacchi verso la Pubblica Amministrazione sembra crescere ad un ritmo leggermente inferiore rispetto agli altri settori, i quali sono probabilmente considerati maggiormente lucrativi da parte delle organizzazioni criminali in cerca di profitto immediato.

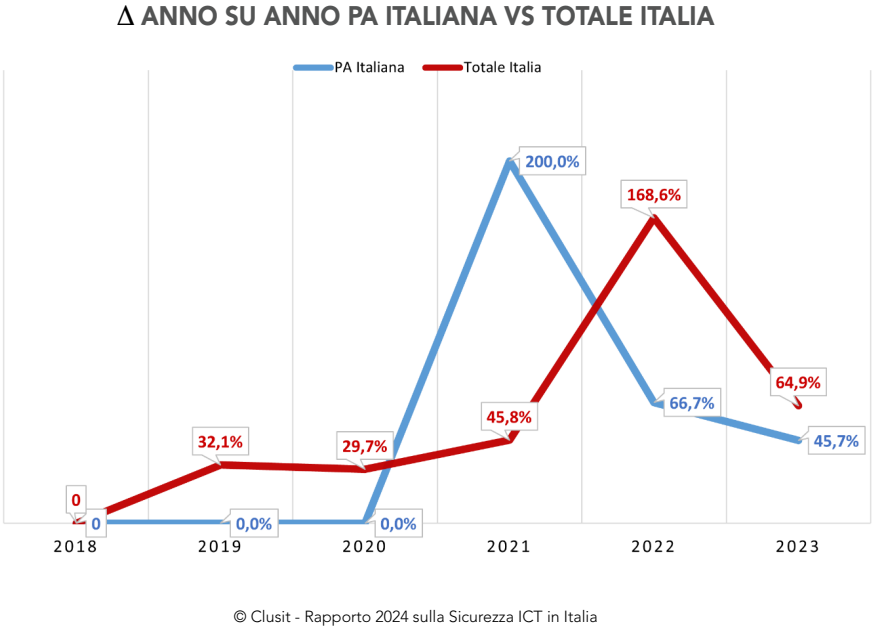

Figura 8 - Incrementi anno su anno del numero di attacchi dal 2018 in Italia nel solo settore pubblico e in tutti i settori

Vogliamo a questo punto comprendere quanto incidano gli attacchi verso il settore pubblico sul numero complessivo di attacchi rivolti verso il nostro Paese. Il grafico di **Figura 9** rappresenta appunto l'andamento nel tempo della frazione di attacchi italiani riguardanti la Pubblica Amministrazione, e ci mostra come questa sia grosso modo compresa tra il 15% e il 30% del totale. In pratica il settore pubblico raccoglie in media da un attacco su tre a un attacco su sei.

Dal picco del 2021 la situazione sembra migliorare, ma il confronto incrociato con gli altri grafici chiarisce che il fenomeno è purtroppo solo apparente: gli attacchi verso il settore privato non stanno infatti diminuendo, ma semplicemente accade che gli attacchi generali stanno crescendo più di quelli diretti verso il settore pubblico e quindi il peso di questi ultimi diminuisce rispetto al totale complessivo.

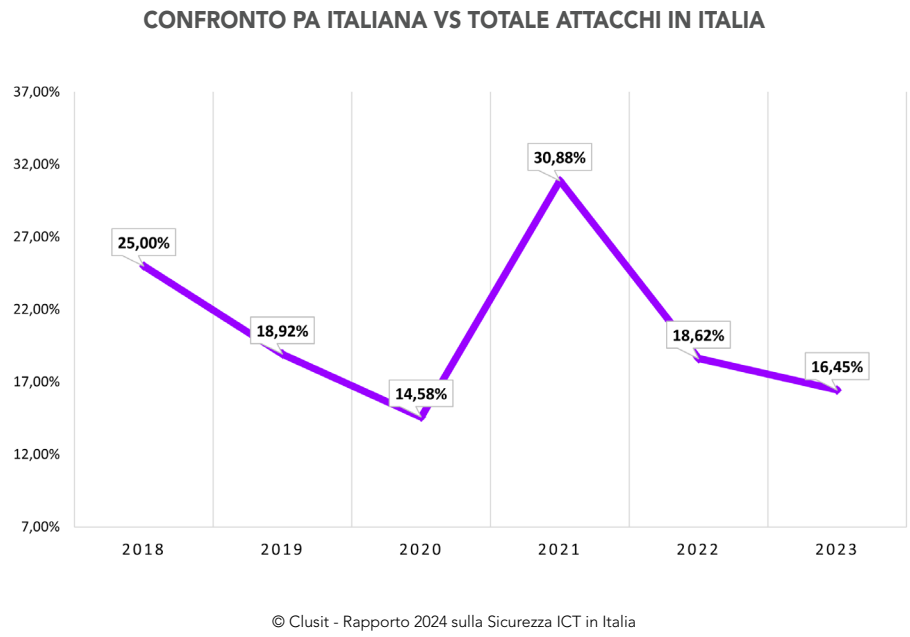

Figura 9 - Rapporto tra numero di attacchi verso la Pubblica Amministrazione e numero complessivo di attacchi in Italia

Passando al fronte della minaccia, aiutandoci col grafico di **Figura 10** vediamo quali sono le tipologie e/o le motivazioni degli attaccanti che si rivolgono contro il settore pubblico. Ancora una volta troviamo al primo posto la criminalità, diventata dirompente dal 2021 in poi e in leggero calo nel 2023. Riconosciamo anche in questo grafico il picco di azioni dimostrative condotte nel 2023 verso obiettivi governativi a seguito della situazione geo-politica internazionale, come già visto nelle analisi precedenti.

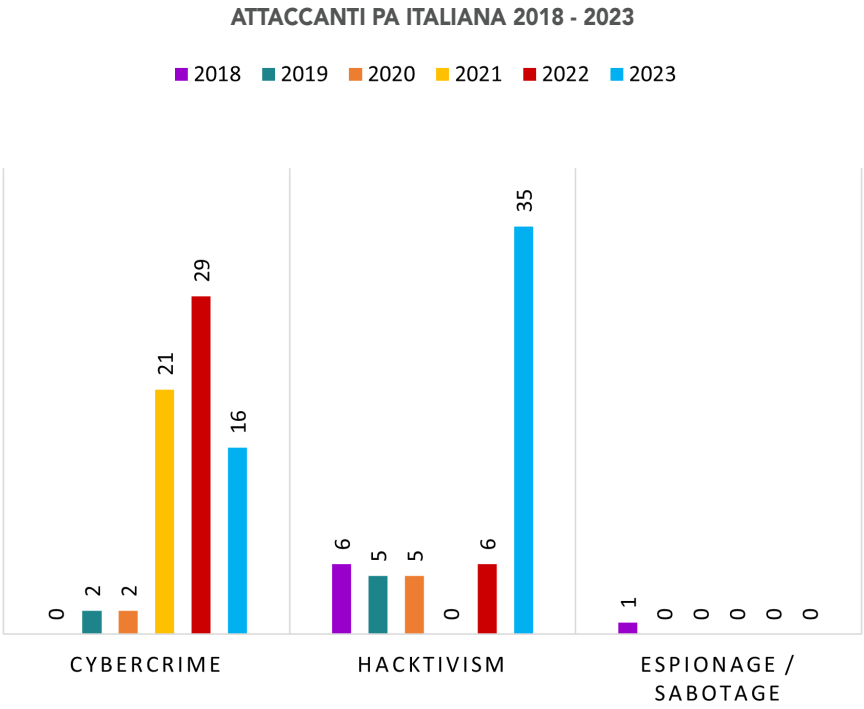

Figura 10 - Distribuzione degli attacchi verso il settore pubblico rispetto alla tipologia e/o motivazione dell'attaccante

Per quanto riguarda le modalità di attacco, il grafico di **Figura 11** ci mostra che anche nel settore pubblico l'utilizzo di *malware* è al primo posto, anche se se ne evidenzia una importante flessione nel 2023. Questa può essere spiegata con il recente e forte spostamento dal piano puramente criminale a quello dimostrativo-ideologico degli attacchi condotti verso la Pubblica Amministrazione, fenomeno già evidenziato nel grafico precedente e confermato in questo dal forte picco di attacchi DDoS individuati nel 2023. Rimangono invece relativamente poco significativi gli attacchi basati su tecniche di *social engineering*, le quali sembrano invece essere molto più utilizzate nei confronti delle vittime appartenenti al settore privato.

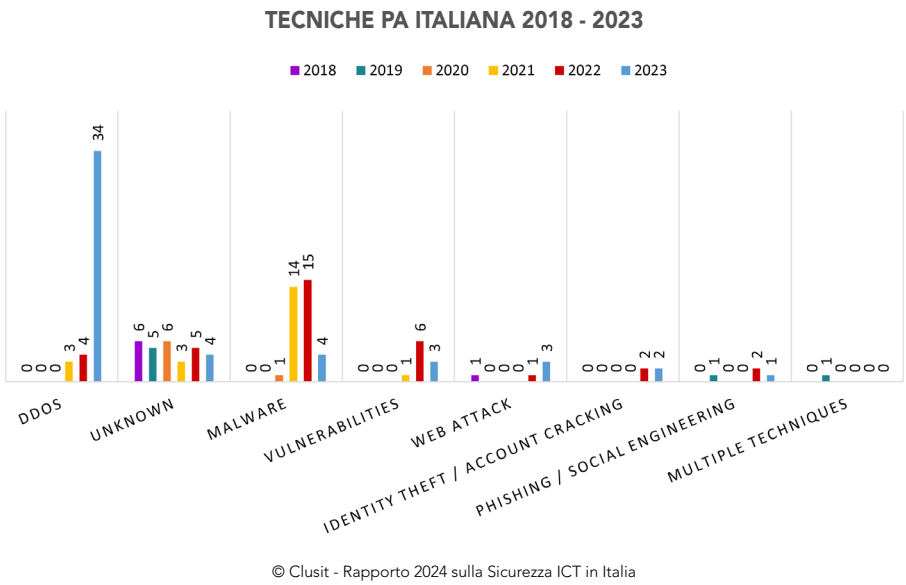

Figura 11 - Distribuzione degli attacchi verso il settore pubblico rispetto alla tecnica impiegata

Un ultimo aspetto importante da valutare è quello relativo alla *severity* degli attacchi, ossia al livello di gravità e conseguenze degli stessi. Analizzando il grafico di **Figura 12** notiamo come, al di là di una evidente anomalia nel 2023 che merita qualche ragionamento specifico, la maggioranza degli attacchi condotti verso la Pubblica Amministrazione rimanga di severità *critica* e *elevata*, con entrambe le categorie in crescita.

L'apparente inversione di tendenza visibile nel 2023, che vede una forte diminuzione degli attacchi aventi severità *critica* ed un corrispondente incremento di quelli aventi severità *alta* e *media*, non fa che confermare quanto già detto a proposito dei grafici precedenti: riflette infatti il forte incremento degli attacchi di tipo Denial of Service di natura puramente ideologica e dimostrativa, e quindi intrinsecamente meno gravi rispetto ad attacchi criminali veri e proprio quali intrusioni o ransomware.

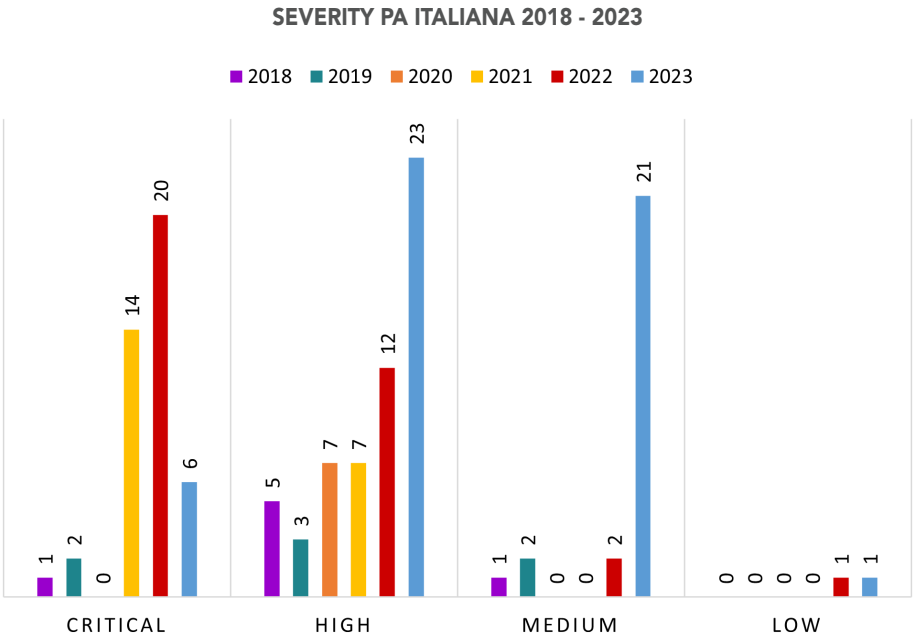

Figura 12 - Livello di gravità degli attacchi verso il settore pubblico

Considerazioni conclusive

L'Italia si trova dunque, da circa tre anni a questa parte, sotto un attacco sistematico e massiccio da parte della criminalità cibernetica internazionale, caratterizzato da un'intensità che non ha pari nel resto del mondo.

Le cause di questo improvviso cambio di prospettiva nel panorama nazionale sono certamente complesse e multiformi, ma volendo semplificare al massimo possono ragionevolmente essere ricondotte ad una digitalizzazione tardiva e affrettata avvenuta repentinamente in moltissimi settori produttivi del nostro Paese, soprattutto quelli composti da imprese piccole e piccolissime che fino a tempi assai recenti non erano connesse. Questa digitalizzazione, favorita sia da improvvisi fattori esogeni come il lockdown e la conseguente necessità di lavorare a distanza, sia da fattori endogeni come gli incentivi economici per l'aggiornamento delle capacità produttive, è stata in molti casi condotta in modo superficiale e poco strutturato: e spesso, anche e soprattutto in mancanza di specifiche e sistematiche direttive istituzionali, senza tenere

in giusta considerazione quei fondamentali aspetti di sicurezza informatica che purtroppo ancora oggi appaiono come tematiche distanti e incomprensibili a molti medi e piccoli imprenditori nonché alla pubblica amministrazione locale.

Altri Paesi avevano affrontato la transizione al digitale molto prima di noi, in tempi in cui la minaccia non era così agguerrita come lo è oggi, e hanno avuto così modo e tempo di formarsi una cultura più sistematica della gestione del rischio cibernetico. Il nostro Paese invece ha dovuto farlo d'improvviso, senza quindi aver potuto maturare quel retroterra culturale che dovrebbe essere patrimonio sia delle persone che delle organizzazioni, e che non riguarda solo gli ambiti più tecnici della sicurezza delle reti e dei sistemi ma consta soprattutto di quagli aspetti generali di comprensione del rischio, di educazione digitale, di resilienza operativa.

Di ciò si è ovviamente avvantaggiata la grande criminalità cibernetica transnazionale che, evolutasi anch'essa nel tempo, ha rapidamente imparato a sviluppare sempre nuove e più efficaci strategie di attacco. Oggi le vittime preferite sono gli anelli deboli della filiera produttiva, ossia proprio quelle imprese e amministrazioni piccole e piccolissime che non si proteggono per ignoranza e sono quindi più facili da colpire, e vengono usate sia come fonte di profitto diretto sia come mezzo per triangolare gli attacchi verso i soggetti più grandi. Così le organizzazioni criminali hanno trovato nel nostro Paese il terreno ideale su cui concentrare le proprie attività, ed i risultati purtroppo si leggono chiaramente nei dati degli attacchi.

Nota metodologica

Per tutte le informazioni relative alla raccolta, analisi e pubblicazione dei dati fare riferimento al relativo capitolo del Rapporto CLUSIT 2024.

Autori

Il Team che analizza e revisiona i dati dei Rapporti Clusit è costituito da:

Luca Bechelli
Giorgia Dragoni
Corrado Giustozzi
Alessio Pennasilico
Pier Luigi Rotondo
Sofia Scozzari
Claudio Telmon
Anna Vaccarelli
Andrea Zapparoli Manzoni

Clusit
Associazione Italiana per la Sicurezza Informatica

Il Clusit, **nato nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano**, è la più numerosa e autorevole associazione italiana nel campo della sicurezza informatica. Oggi rappresenta oltre **700 organizzazioni**, appartenenti a tutti i settori del Sistema-Paese.

Gli obiettivi

- Diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini.
- Partecipare alla elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica, sia a livello nazionale che europeo.
- Contribuire alla definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza.
- Promuovere l'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

Le attività e i progetti in corso

- Formazione specialistica: i Webinar CLUSIT.
- Ricerca e studio: Premio "Innovare la Sicurezza delle Informazioni" per la migliore tesi universitaria arrivato alla 19a edizione.
- Le Conference specialistiche: i Security Summit Streaming Edition, i Security Summit On Site (a Milano, Roma, Cagliari e Verona), gli Atelier della Security Summit Academy, Le Tavole Rotonde Verticali (Energy & Utilities, Health Care, Finance, Manufacturing).
- I Gruppi di Lavoro della Clusit Community for Security.
- Rapporti Clusit: Rapporto annuale, con aggiornamento semestrale, sulla sicurezza ICT in Italia, in produzione dal 2012.
- Il Mese Europeo della Sicurezza Informatica, iniziativa di sensibilizzazione promossa ogni anno nel mese di ottobre in Italia da Clusit.
- Il progetto "SicuraMente Clusit" con attività di formazione nelle scuole sul territorio.

Il ruolo istituzionale

In ambito nazionale, Clusit opera in collaborazione con: Presidenza del Consiglio, numerosi ministeri, Banca d'Italia, Polizia Postale e delle Comunicazioni, Arma dei Carabinieri e Guardia di Finanza, Autorità Garante per la tutela dei dati personali, Cyber 4.0 - il Centro di Competenza nazionale ad alta specializzazione per la cybersecurity, Start 4.0, Università e Centri di Ricerca, Associazioni Professionali e Associazioni dei Consumatori, Confindustria, Confcommercio e CNA.

I rapporti internazionali

In ambito internazionale, Clusit partecipa a svariate iniziative in collaborazione con: i CERT, i CLUSI, Università e Centri di Ricerca in oltre 20 paesi, Commissione Europea, ENISA (European Union Agency for Cybersecurity), ITU (International Telecommunication

Union), OCSE, UNICRI (Agenzia delle Nazioni Unite che si occupa di criminalità e giustizia penale), le principali Associazioni Professionali del settore (ASIS, CSA, ISACA, ISC², ISSA, SANS) e le associazioni dei consumatori.

Security Summit è il più importante appuntamento italiano per tutti coloro che sono interessati alla sicurezza dei sistemi informatici e della rete e, più in generale, alla sicurezza delle informazioni.
Progettato e costruito per rispondere alle esigenze dei professionals di oggi, Security Summit è un convegno strutturato in momenti di divulgazione, di approfondimento, di formazione e di confronto. Aperto alle esperienze internazionali e agli stimoli che provengono sia dal mondo imprenditoriale che da quello universitario e della ricerca, il Summit si rivolge ai professionisti della sicurezza e a chi in azienda gestisce i problemi organizzativi o legali e contrattuali dell'Ict Security.

SECURITY SUMMIT ACADEMY

La **partecipazione è libera e gratuita**, con il solo obbligo dell'iscrizione online.
Il Security Summit è organizzato dal Clusit e da Astrea, agenzia di comunicazione ed organizzatore di eventi di alto profilo contenutistico nel mondo finanziario e dell'Ict.

SECURITY SUMMIT VERTICAL

Certificata dalla folta schiera di **relatori** (**più di 700** sono intervenuti nelle scorse edizioni), provenienti dal mondo della ricerca, dell'Università, delle Associazioni, della consulenza, delle Istituzioni e delle imprese, la manifestazione è stata frequentata da oltre **20.000 partecipanti**, e sono stati rilasciati circa **15.000 attestati** validi per l'attribuzione di oltre **48.000 crediti formativi** (CPE).
Nel 2023 i Security Summit sono stati oggetto di oltre **800 articoli e servizi su web, cartaceo, Radio e TV**.

L'edizione 2024

Il 2024 inizia con una edizione tutta in presenza, dal **19 al 21 marzo, a Milano**.
Seguiranno: il 19 giugno il Security Summit di **Roma**, il 18 settembre il Security Summit di **Cagliari**, il 24 ottobre il Security Summit di **Verona** e il 7 novembre un Security Summit Streaming Edition. Continueranno inoltre gli **Atelier della Security Summit Academy**, che si terranno tutto l'anno e gli **Eventi Verticali**, programmati il 28 maggio (**Energy & Utilities**), il 19 giugno (**Health Care**) e il 7 novembre (**Manufacturing**).

Informazioni

- **Agenda e contenuti:** info@clusit.it, +39 349 7768 882
- **Altre informazioni:** info@astrea.pro
- **Informazioni per la stampa:** press@securitysummit.it
- **Sito web:** www.securitysummit.it/

SECURITY SUMMIT

www.securitysummit.it