Anteprima Rapporto Clusit 2024

Rapporto Clusit, cyber attacchi gravi analizzati dal Clusit crescono in Italia più che nel resto del mondo: +65% nel 2023 rispetto al 2022 (+12% a livello mondiale).

Contesto sempre più ostile in termini di minacce digitali verso il nostro Paese, dove nel 2023 è andato a segno l'11% degli attacchi globali.

Il 47% degli attacchi analizzati da Clusit con matrice di hacktivism a livello mondiale è avvenuto a danni dell'Italia.

Il più colpito è il settore governativo/militare; un quarto del totale degli attacchi analizzati dal Clusit rivolti al settore manifatturiero a livello globale riguarda realtà italiane.

Milano, 6 marzo 2024 – È stato presentato questa mattina in anteprima alla stampa il Rapporto Clusit 2024[1] in cui i ricercatori di Clusit, l'Associazione Italiana per la Sicurezza Informatica, delineano in maniera indipendente l'andamento del cybercrime a livello globale e italiano.

Con **2.779 incidenti gravi**[2] **analizzati a livello globale da Clusit**, il 2023 restituisce una fotografia nettamente peggiorativa rispetto ai dodici mesi precedenti, continuando a descrivere una curva degli attacchi in inesorabile crescita, che registra un +12% sul 2022. Mensilmente, è stata rilevata una media di 232 attacchi, con un picco massimo di 270 nel mese di aprile, che rappresenta anche il valore massimo misurato negli anni. **Nell'81% dei casi la gravità degli attacchi è elevata o critica**, secondo la scala di "severity" utilizzata dai ricercatori di Clusit che si basa sulla tipologia di attacco e sugli impatti.

In questo contesto, il nostro Paese appare sempre più nel mirino dei cyber criminali: **lo scorso anno in Italia è andato a segno l'11% degli attacchi gravi globali** mappati dal Clusit (era il 7,6% nel 2022), per un totale di 310 attacchi, dato che marca una **crescita del 65%** rispetto al 2022. Oltre la metà degli attacchi - il 56% - ha avuto conseguenze di gravità critica o elevata. Con uno sguardo agli ultimi cinque anni, emerge inoltre che oltre il 47% degli attacchi totali censiti in Italia dal 2019 si è verificato nel 2023.

Come sempre, nell'illustrare i dati i ricercatori di Clusit hanno evidenziato che si tratta di una fotografia che rappresenta le linee tendenziali del fenomeno e che tuttavia rappresenta soltanto la

[1] Frutto della collaborazione continuativa di oltre cento professionisti nell'ambito di Clusit, il Rapporto Clusit fornisce da quattordici anni il quadro esaustivo della situazione globale della sicurezza informatica, avvalendosi anche del contributo di soggetti pubblici e privati che condividono con Clusit esperienze e ricerche sul campo con informazioni e dati inediti. La presentazione del Rapporto Clusit al pubblico avverrà in apertura di Security Summit, il convegno dedicato ai temi della cyber security in programma a Milano dal 19 al 21 marzo.

[2] Nel Rapporto Clusit sono classificati come "gravi" gli attacchi con un impatto sistemico in ogni aspetto della società, della politica, dell'economia e della geopolitica

punta dell'iceberg, posto che molte vittime tendono ancora a mantenere riservate le informazioni sugli attacchi cyber subìti e che relativamente ad alcune zone del mondo la possibilità di accesso alle informazioni è molto limitata.

Considerando l'andamento del cyber crimine nell'ultimo quinquennio, gli autori del Rapporto Clusit ne hanno evidenziato evoluzione e picchi in termini quantitativi e qualitativi: dal 2018 al 2023 gli attacchi sono cresciuti complessivamente del 79%, con una media mensile passata da 130 a 232.

Questi dati definiscono un quadro preoccupante della capacità di protezione sia delle organizzazioni pubbliche sia delle imprese: è evidente che ad oggi le strategie e le tecniche di difesa utilizzate non sono all'altezza delle possibilità degli attaccanti che fanno sempre più ricorso all'utilizzo di tecnologia di ultima generazione grazie alle risorse economiche a disposizione e alla possibilità di agire liberamente senza limiti.

I trend osservati, in particolare in merito alle tecniche di attacco, indicano che è certamente da tenere monitorato l'utilizzo dell'Intelligenza Artificiale da parte dei cyber criminali per selezionare i target e scansionarli, al fine di trovare falle, per analizzare codici e trovare nuove vulnerabilità e per produrre contenuti per phishing o codice per malware. Si tratta di una tendenza in rapida ascesa, di cui tuttavia i ricercatori di Clusit ritengono sarà possibile osservare gli effetti solo in un prossimo futuro.

"*Le strategie adottate ad oggi, anche a livello normativo a livello sia italiano che europeo, sono state sicuramente utili e importanti per cercare di limitare la crescita del fenomeno. Ma per poter far rallentare il trend e cercare di stabilizzarlo, e possibilmente ridurlo, devono essere concepite e adottate strategie nuove che si fondino sul knowledge sharing, sulla messa a fattor comune degli investimenti e sulla assunzione di responsabilità verso la comunità per chi deliberatamente decide di non proteggere adeguamente la propria struttura con ciò arrecando danno all'intero ecosistema Paese. Non è sostenibile che chiunque possa investire in tecnologia liberamente senza le coperture finanziare necessarie per evitare da un lato l'obsolescenza e dall'altro per garantire la protezione nel tempo delle risorse digitali*", afferma Gabriele Faggioli, presidente di Clusit.

"*Vogliamo mantenere alta l'attenzione anche sulla frammentazione di infrastrutture e servizi che caratterizza la cyber security nel nostro Paese, e che rischiano di produrre una moltiplicazione di sforzi, ciascuno in sé poco efficace, come ampiamente dimostrato dai settori di mercato maggiormente colpiti e anche considerando la spesa complessiva italiana in cybersecurity. Riteniamo quindi particolarmente significative iniziative come quella del Polo Strategico Nazionale e della strategia Cyber Nazionale. Questo, in particolare, in un momento in cui si assiste un forte cambiamento della componente della schiera degli attaccanti, con un preponderante ritorno in primo piano dell'Hacktivism in relazione ad uno scenario geopolitico incerto",* prosegue Faggioli.

"Ricordiamo che il 2024 è un anno in cui si apriranno le urne per 2 miliardi di persone in 70 paesi del mondo, e ciò accade in un momento in cui con l'introduzione della AI nella vita quotidiana pone di nuovo al centro, con alterne fortune ed efficacia, i temi dell'Etica e della Sovranità Digitale, che non possono esistere, tuttavia, senza garanzie sulla sicurezza delle informazioni, senza una adeguata cultura digitale (molto scarsa in Italia come fotografato impietosamente dall'Indice DESI) e senza una adeguata politica industriale che metta al centro gli investimenti in aziende tecnologiche", conclude Faggioli.

Gli obiettivi degli attacchi nel mondo e in Italia

L'analisi dei cyber attacchi noti nel 2023 da parte dei ricercatori di Clusit evidenzia la netta prevalenza di attacchi con finalità di **cybercrime** - ovvero con l'obiettivo di estorcere denaro - che sono stati oltre 2.316 a livello globale, oltre l'**83% del totale**, in crescita del 13% rispetto al 2022.

Questo andamento, commentano gli autori del Rapporto Clusit, sostanzia le indicazioni degli analisti che vedono una commistione tra criminalità "off-line" e criminalità "on-line" volta a reinvestire i proventi delle attività malevole, producendo così maggiori risorse a disposizione di chi attacca, in una sorta di circolo vizioso.

Nel mondo sono quasi triplicati a livello globale gli attacchi con matrice di **hacktivism**, nel 2023 pari all'**8,6% degli attacchi complessivi** (erano il 3% nel 2022), con una variazione percentuale rispetto al totale anno su anno del 184%. In significativa diminuzione, invece, i fenomeni di **espionage** (6,4%, 11% nel 2022) e **information warfare** (1,7%, 4% nel 2022).

Tuttavia, rilevano gli autori del Rapporto Clusit, per quanto riguarda *espionage* e *information warfare* gli attacchi con impatto critico sono aumentati considerevolmente, da valori prossimi al 50% nel 2022 a valori intorno al 70% lo scorso anno. Questo andamento si può con alta probabilità spiegare con riferimento ai conflitti Russo-Ucraino ed Israelo-Palestinese che, almeno sul piano della cyber security, vedono coinvolti molti Paesi.

Per le azioni di *hacktivism* è stata invece rilevata a livello mondiale una significativa riduzione percentuale degli attacchi critici (poco più del 10% sul totale nel 2023, rispetto al 50% del 2022), un andamento costante di quelli ad alto impatto ed un aumento di quelli ad impatto medio. Il fenomeno si spiega, secondo gli autori del Rapporto Clusit, con il consistente aumento degli attacchi afferenti a questa categoria a seguito dell'aggravarsi dello scenario geopolitico, nonché alla natura dimostrativa dei possibili effetti, la cui gravità, in confronto agli obiettivi perseguiti dai criminali informatici verso il mondo pubblico o privato, è spesso intrinsecamente più limitata.

In Italia, nel 2023 gli attacchi perpetrati con finalità di **cybercrime** sono stati pari al **64%**; segue un significativo **36% di attacchi con finalità di hacktivism**, in netta crescita rispetto al 2022 (che aveva fatto registrare il 6,9%), con una **variazione percentuale anno su anno del +761%**. Il 47% circa del totale degli attacchi con finalità "hacktivism" a livello mondiale e che rientrano nel campione rilevato – notano gli esperti di Clusit - è avvenuto ai danni di organizzazioni italiane.

La crescita di attacchi con matrice di hacktivism nel nostro Paese dimostra la forte attenzione di gruppi di propaganda che hanno l'obiettivo di colpire la reputazione delle organizzazioni. Questa tipologia di eventi – perlomeno quelli avvenuti nei primi nove mesi dell'anno, secondo i ricercatori di Clusit - si riferisce per la maggior parte al conflitto in Ucraina, nei quali gruppi di attivisti agiscono mediante campagne dimostrative rivolte tanto al nostro Paese che alle altre nazioni del blocco filo-ucraino. *"Questo tipo di operazioni a sfondo politico e sociale sembrano essere state a livello globale predominanti rispetto a quelle militari o di intelligence, almeno per quanto riguarda la porzione divenuta di pubblico dominio e considerando quanto questo contesto tenda ad emergere difficilmente",* commenta Sofia Scozzari, del Comitato Direttivo Clusit.

Chi viene attaccato, nel mondo e in Italia

A livello mondiale le principali vittime si confermano appartenere alla categoria degli **obiettivi multipli** (19%), che subiscono campagne di attacco non mirate ma dagli effetti consistenti. Segue il **settore della sanità** (14%) che, come fanno notare i ricercatori Clusit, ha visto un **incremento del 30%** rispetto allo scorso anno. Gli incidenti in questo settore hanno inoltre visto un aumento della gravità dell'impatto, critico nel 40% dei casi (era il 20% nel 2022).

Una parte consistente degli attacchi è stata rivolta anche al settore **governativo e delle pubbliche amministrazioni** (12%). Pur con un andamento lineare, il settore pubblico è stato interessato da un incremento del 50% degli incidenti negli ultimi cinque anni, rilevano gli esperti di Clusit. Questo è spiegabile con l'incremento delle attività dimostrative, di disturbo e di fiancheggiamento legate ai conflitti in corso, le quali hanno come obiettivi di elezione soggetti legati alle sfere governative e della difesa di quei Paesi considerati avversari.

Segue il settore **finanza e assicurazioni** (11%). Gli attacchi in questo settore sono cresciuti percentualmente del **62%** rispetto all'anno precedente e hanno avuto **un impatto critico nel 50% dei casi** (era il 40% nel 2022).

In percentuale, sono cresciuti in maniera rilevante anche gli attacchi ai settori **dei trasporti e della logistica (+41%),** del **manifatturiero (+25%)** e del **retail (26%)**, probabilmente - come già evidenziato dagli esperti di Clusit lo scorso anno - a causa della crescente diffusione dell'IoT e dalla tendenza verso l'interconnessione di sistemi, ampiamente impiegati in questi settori e tuttavia spesso non sufficientemente protetti.

In crescita anche la percentuale degli attacchi registrata nel **settore scolastico** (+20%) e del **tempo libero** (+10%); calano invece sensibilmente (-49%) gli attacchi verso il settore dei **media e multimedia**.

Il settore più attaccato **in Italia** nel 2023 è stato invece quello **governativo/ militare**, con il 19% degli attacchi, che ha subito **un incremento del 50% rispetto al 2022**, seguìto dal **manifatturiero**, con il 13%, **cresciuto del 17% rispetto ai dodici mesi precedenti**. Come evidenziato dagli autori del Rapporto Clusit, è interessante notare che **un quarto del totale degli attacchi rivolti al manufacturing a livello globale riguarda realtà manifatturiere italiane**.

Colpito dal 12% degli attacchi, il settore dei **trasporti/logistica** in Italia, ha visto invece un **incremento percentuale anno su anno sul totale degli attacchi del 620%**; analogamente, il settore della **finanza e delle assicurazioni**, verso cui è stato perpetrato il 9% degli attacchi nel 2023, ha visto una **variazione percentuale sul totale del +286% rispetto allo scorso anno**.

Le vittime appartenenti alla categoria degli "**obiettivi multipli**" sono state colpite nel nostro Paese dall'11% degli attacchi, segno di una maggior focalizzazione dei cyber criminali verso settori specifici negli ultimi mesi.

La geografia delle vittime: i continenti più colpiti

La distribuzione geografica percentuale delle vittime segna, secondo i ricercatori di Clusit, la variazione della digitalizzazione nel mondo, riflettendo verosimilmente uno spaccato sulle regioni mondiali che hanno adottato le migliori azioni di difesa. Nel 2023 si confermano, come nel 2022, più numerosi gli attacchi alle **Americhe**, che rappresentano il **44% del totale**. Gli **attacchi rivolti all'Europa hanno rappresentato nel 2023 il 23% degli attacchi globali**, scendendo di un punto percentuale rispetto all'anno precedente ma in **crescita percentuale sul 2022 del 7,5%**. Crescono invece di un punto percentuale rispetto al 2022 gli attacchi in **Asia** - **il 9% del totale** - e rimangono sostanzialmente stabili quelli in **Oceania** e in **Africa,** rispettivamente il **2%** e l'**1%** del totale.

Circa un **quinto degli attacchi** (21%) è avvenuto parallelamente **verso località multiple**, con una riduzione di 6 punti percentuali sul totale degli attacchi rispetto al 2022.

Le tecniche d'attacco, nel mondo e in Italia

Il **malware** rappresenta nel 2023 ancora la tecnica principale con cui viene sferrato il **36%** degli attacchi globali, percentualmente in crescita sul totale del 10% rispetto al 2022. In questa categoria, che comprende diverse tipologie di codici malevoli, il ransomware è in assoluto quella principale e maggiormente utilizzata grazie anche all'elevata resa economica per gli aggressori, che spesso collaborano fra loro con uno schema di affiliazione.

Segue lo sfruttamento di **vulnerabilità** - note o meno - nel **18%** dei casi, in crescita percentuale del 76% sul totale rispetto al 2022. **Phishing e social engineering** sono la tecnica con cui è stato sferrato nel mondo l'**8%** degli attacchi, come gli **attacchi DDoS**, che segnano però una variazione percentuale annua del **+98%.**

In **Italia per la prima volta da diversi anni, la categoria prevalente non è più il malware, bensì** gli attacchi per mezzo di **DDoS**, che rappresentano il **36% del totale degli incidenti registrati nel 2023**, un valore che supera di 28 punti percentuali il dato globale e che segna una variazione percentuale annua sul totale del **1486%**. La forte crescita è probabilmente dovuta, come indicano gli autori del Rapporto Clusit, all'aumento di incidenti causati da campagne di hacktivism: molto spesso la tecnica di attacco utilizzata in questo caso è proprio il DDoS, poiché si punta a interrompere l'operatività di servizio dell'organizzazione o istituzione individuata come vittima.

La percentuale di incidenti basati su tecniche sconosciute è 17%, sostanzialmente in linea con il resto del mondo.

Leggermente superiore l'impatto nel nostro Paese rispetto al resto del mondo gli attacchi di phishing e di ingegneria sociale, pari all'9%, che tuttavia in crescita dell'87% in valore assoluto, dimostrando l'efficacia duratura di questa tecnica. "*Il fattore umano, evidentemente in Italia ancora più che nel resto del mondo, continua a rappresentare un punto debole facilmente sfruttabile dagli attaccanti: rimane quindi fondamentale focalizzare l'attenzione sul tema della consapevolezza, poiché i dati ci dicono che quanto fatto fino ad oggi non è ancora sufficiente*", afferma Luca Bechelli, del Comitato Scientifico Clusit.

Analisi Fastweb della situazione italiana in materia di cyber-crime

Come ogni anno, Fastweb ha contribuito con l'analisi dei trend più rilevanti elaborata sulla base dei dati del proprio Security Operations Center (SOC), attivo 24 ore su 24 e dai propri centri di competenza di sicurezza informatica.

Dall'analisi sull'infrastruttura di rete di Fastweb, costituita da oltre 6,5 milioni di indirizzi IP pubblici, su ognuno dei quali possono comunicare centinaia di dispositivi e server, sono stati registrati nel 2023 oltre 56 milioni di eventi di sicurezza in linea per la prima volta con il dato del 2022.

Nel corso del 2023 si è assistito al consolidamento di alcune delle tendenze già osservate nel panorama dei fenomeni del cybercrime. Nonostante l'elevato numero di attacchi DDOS (oltre 15.000 eventi) e la gravità di eventi informatici malevoli ad alto impatto (+32%) continua a crescere la consapevolezza rispetto ai rischi informatici da parte delle aziende e delle pubbliche amministrazioni, testimoniata da una significativa riduzione della durata degli attacchi e da una riduzione del numero dei server che espongono su internet servizi critici (-8%), oltre che dall'utilizzo di strumenti di ricerca e monitoraggio che hanno contribuito a migliorare l'identificazione delle minacce.

Come si evince dall'analisi, l'Intelligenza Artificiale rappresenta un cambiamento significativo nell'ambito della sicurezza informatica, con vantaggi e sfide che ridefiniscono il panorama della difesa cibernetica. Gli algoritmi avanzati e la capacità di apprendimento continuo contribuiscono ad una protezione più sofisticata e reattiva migliorando notevolmente la capacità di rilevare e mitigare le minacce con una riduzione fino al 70% dei falsi positivi rilevati. Tuttavia, le tecnologie come la GenAI possono essere sfruttate dagli attaccanti per aumentare l'efficacia e l numerosità degli attacchi, come nel caso del credential phishing che nel 2023 è aumentato dell'87% rispetto all'anno precedente.

Per la prima volta, il report include anche il monitoraggio relativo alle minacce informatiche rilevate e contrastate tramite il servizio di Managed Detection and Response (MDR) di 7Layers, società acquisita da Fastweb nel 2020 e specializzata in soluzioni avanzate di cybersecurity.

Gli autori del Rapporto Clusit 2024 hanno evidenziato inoltre i contributi e gli approfondimenti che arricchiscono anche questa edizione:

- le **attività e segnalazioni della Polizia Postale e delle Comunicazioni** nel 2023;
- il contributo in ambito finance: **Elementi sul cybercrime nel settore finanziario in Europa**
- lo Speciale **Cybersecurity in Sanità**: Tra Aumento degli Attacchi e Innovazioni Normative e Tecnologiche, a cura della Community Women For Security
- l'indagine "**Le tendenze della Hybrid Security per il 2024**"

Sono inoltre inclusi nel Rapporto Clusit 2024 undici approfondimenti "**Focus On**" sulle tematiche tecnologiche più attuali in tema di cybersecurity.

Il Rapporto Clusit 2024 sarà presentato al pubblico il prossimo 19 marzo, in apertura di Security Summit, la tre giorni dedicata alla cybersecurity organizzata a Milano da Clusit con Astrea, Agenzia di Comunicazione ed Eventi specializzata nel settore della Sicurezza Informatica.

Clusit è l'Associazione Italiana per la Sicurezza Informatica. Nata nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, rappresenta oggi oltre 600 organizzazioni, appartenenti a tutti i settori del Sistema-Paese. Clusit collabora con la Presidenza del Consiglio, con diversi Ministeri, Authority, Istituzioni e organismi di controllo, tra cui Polizia Postale e delle Comunicazioni, Arma dei Carabinieri e Guardia di Finanza, Agenzia per l'Italia Digitale, Autorità Garante per la tutela dei dati personali. Svolge inoltre un'intensa attività di supporto e di scambio con Cyber 4.0, il Centro di Competenza nazionale ad alta specializzazione per la cybersecurity e con Associazioni Professionali e Associazioni dei Consumatori, Confindustria, Confcommercio e CNA, con Università e Centri di Ricerca. In ambito internazionale, Clusit partecipa a diverse iniziative in collaborazione con i CERT, i CLUSI, con la 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), con le principali Associazioni Professionali del settore, con Università e Centri di Ricerca in oltre 20 paesi. Ulteriori informazioni sulle attività di Clusit sono disponibili sul sito www.clusit.it.

Per ulteriori informazioni si prega di contattare:
Daniela Sarti
Ufficio Stampa Security Summit | Clusit
press@securitysummit.it - dsarti@clusit.it Tel. 335 459432