AGENZIA STAMPA QUOTIDIANA NAZIONALE
Prima Pagina News

Tecnologia - *Rapporto Clusit: impennata di attacchi cyber in Italia: +40% nei primi sei mesi del 2023*

Milano - 09 nov 2023 (Prima Pagina News) **Quasi quattro volte più che nel resto del mondo.**

Sono stati 1.382 gli attacchi cyber nel mondo nel primo semestre del 2023, registrati ed analizzati dai ricercatori di Clusit, Associazione Italiana per la Sicurezza Informatica. Nel corso della presentazione della edizione di fine anno del Rapporto Clusit, che si è svolta questa mattina nel contesto di Security Summit Streaming Edition, il dato è stato accompagnato dalla macroanalisi che ha evidenziato come si tratti del numero di incidenti più elevato di sempre, oltre la linea di tendenza previsionale stimata sulla base dell'andamento dell'ultimo quinquennio. Il primo semestre 2023 segna tuttavia un rallentamento della crescita degli attacchi a livello globale, che si attesta all'11% (era il 21% nell'anno 2022), poco sopra alla tendenza anno su anno registrata negli ultimi cinque anni. In controtendenza, in Italia, nel primo semestre 2023 i ricercatori di Clusit hanno registrato una crescita degli incidenti del 40%, quasi 4 volte superiore al dato globale. Considerando il periodo che va dal 2018 al primo semestre 2023, a livello globale gli incidenti sono aumentati del 61,5%, mentre in Italia la crescita complessiva raggiunge il 300%. Nel complesso dei cinque anni, 505 attacchi noti di particolare gravità hanno coinvolto realtà italiane, di cui ben 132 – ovvero il 26% - si sono verificati nel primo semestre 2023. In questo periodo, nel nostro Paese è andato a segno il 9,6% degli attacchi mondiali. Il picco massimo - del semestre e di sempre - si è registrato ad aprile, con 262 attacchi. "Se nel contesto delle tensioni internazionali e di un conflitto ad alta intensità combattuto ai confini dell'Europa, a fine 2022 anche l'Italia appariva per la prima volta in maniera evidente nel mirino, nel 2023 la tendenza si è decisamente consolidata", ha affermato Gabriele Faggioli, presidente di Clusit, commentando i dati. "Considerato che l'Italia rappresenta il 2% del PIL mondiale e lo 0,7% della popolazione, questo dato fa certamente riflettere".Gli obiettivi degli attacchi nel mondo e in ItaliaL'analisi degli incidenti cyber noti nel primo semestre 2023 evidenzia la crescita costante di attacchi con finalità di Cybercrime, che sono stati oltre 1160 a livello globale (erano 2043 nell'intero anno 2022), pari all'84% del totale. Si assiste inoltre ad un picco degli attacchi riconducibili ad azioni di Hactivism, in crescita dell'8%, mentre sono in calo quelli riconducibili ad Espionage/Sabotage e Information Warfare e rappresentano rispettivamente il 6% e il 2%.Dopo una minima flessione nel 2022, in concomitanza con il raggiungimento dei valori massimi registrati dalle altre tre categorie di attacchi, il Cybercrime riprende dunque il trend di crescita che lo aveva caratterizzato negli anni precedenti, probabilmente a causa dei significativi risvolti economici legati alla sempre maggiore diffusione degli attacchi ransomware. Anche nel nostro Paese la maggioranza degli attacchi noti si riferisce alla categoria Cybercrime, che rappresenta il 69% del totale, con una quota in significativo calo rispetto all'anno precedente (nel 2022

costituiva il 93,1% degli attacchi); tuttavia - evidenziano gli esperti di Clusit - è bene tenere presente che in termini assoluti gli attacchi mantengono un tasso di incessante crescita: sono stati 91 gli incidenti rilevati in Italia solo nei primi sei mesi del 2023.Si attestano nel nostro Paese al 30% gli attacchi classificati come “Hacktivism” nel primo semestre 2023 (la percentuale era pari al 6,9% nel 2022), costituendo una quota molto superiore rispetto a quella globale: oltre il 37% degli attacchi compiuto a livello mondiale con finalità “Hacktivism” è avvenuto nei confronti di organizzazioni italiane. Secondo gli autori del Rapporto Clusit, gli attacchi dimostrativi avvenuti ai danni di enti o aziende italiane sono riconducibili alla situazione geopolitica, con particolare riferimento al conflitto in Ucraina e all'azione di gruppi di attivisti che hanno rivolto campagne al nostro Paese, così come verso altre nazioni del blocco filo-ucraino.Chi viene attaccato nel mondo e in Italia Nel primo semestre dell’anno il 20% degli attacchi globali è stato rivolto ai Multiple Targets – ovvero a bersagli appartenenti a diversi settori, colpiti contemporaneamente con l’obiettivo di mietere il maggior numero di vittime possibile. Seguono Healthcare, con il 14,5% degli attacchi, l’ambito Governativo / Militare / Law Enforcement, colpiti dall’11,7% degli attacchi, il comparto ICT, dall’11,4%, Financial / Insurance dal 10,5% ed Education che è stato bersaglio con il 7,1% degli attacchi globali. Guardando alla distribuzione delle vittime nel nostro Paese, gli esperti di Clusit rilevano che nel semestre il maggior numero di attacchi è stato rivolto ad organizzazioni “Government” (23% del totale), seguita a breve distanza da “Manufacturing” (17%). Da segnalare che gli incidenti rivolti quest’ultimo comparto rilevati in Italia rappresentano il 34% del totale degli attacchi censiti verso il Manufacturing a livello globale.“L’accelerazione verso il digitale, forte dell’impulso dato dalla pandemia, ha coinvolto mai come in questi ultimi tre anni le piccole e medie imprese italiane, che da questi dati risultano evidentemente impreparate a sostenere la crescente pressione dei cyber-attack”, ha commentato Gabriele Faggioli per il quale occorre riflettere sul fatto che le PMI non possono avere le risorse economiche e professionali adeguate così come è possibile per le grandi imprese.Il settore Financial / Insurance ha registrato il maggiore incremento di incidenti gravi nel nostro Paese, con il 9% di attacchi (era il 3,7% nel 2022). Il numero di attacchi rivolti a vittime in questo ambito - notano gli autori del Rapporto Clusit - ha superato nei primi 6 mesi dell’anno il totale degli attacchi avvenuti in tutto il 2022. Al contrario, il posizionamento del settore Healthcare nel novero delle vittime in Italia si mantiene costante e, in controtendenza con il dato globale, dove il mondo della sanità mantiene saldamente il triste primato del settore specifico più colpito, nel nostro Paese fortunatamente ha arrestato da qualche tempo la crescita in classifica. Tuttavia, in valore assoluto, all’aumentare del numero complessivo degli attacchi nel primo semestre 2023, anche questo settore in Italia risulta più colpito che in passato, con un incremento del 33% anno su anno.Dove colpiscono i cyber criminali L’America nel suo complesso ritorna ad essere la zona geografica più colpita, con il 46,5% degli attacchi. L’Europa resta teatro di oltre un quinto delle violazioni globali nei primi sei mesi del 2023, così come nel 2022. Diminuiscono invece nettamente gli attacchi verso vittime in località multiple (-5 punti percentuali), segnale della preferenza dei cybercriminali verso azioni più mirate, secondo gli esperti di Clusit.Le tecniche d’attacco Nel primo semestre 2023 oltre il 35% degli attacchi è andato a buon fine grazie all’utilizzo di Malware, percentuale in leggera flessione rispetto al 2022. Le tecniche sconosciute (categoria

Unknown) sono al secondo posto con il 21%. Gli esperti di Clusit spiegano questo dato evidenziando che oltre un quinto del totale degli attacchi diventano di dominio pubblico a seguito di un data breach, nel qual caso le normative impongono di inviare una notifica agli interessati, che non comprende necessariamente una descrizione precisa delle modalità dell'attacco, spesso genericamente ascritto alla categoria "Unknown". Quasi il 17% degli attacchi nel mondo è stato compiuto nel primo semestre dell'anno sfruttando le Vulnerabilità, categoria che segna una crescita di 4,8 punti percentuali e Phishing / Social Engineering, in diminuzione di 3,4 punti percentuali rispetto al 2022.In concomitanza con l'aumento di attività riferibili ad Hacktivism ed Information Warfare, gli attacchi DDoS, pur pochi in valori assoluti, sono invece cresciuti di 3,8 punti percentuali; quelli realizzati tramite "Identity Theft / Account Hacking" dello 0,3%.Il Malware, insieme al Ransomware, continua a rappresentare la principale tecnica di attacco utilizzata dai criminali anche in Italia (31%), ma in modo molto meno consistente rispetto al 2022 (53%) e di 4 punti percentuali inferiore al dato globale. "Per la prima volta da quando è esploso il fenomeno del ransomware assistiamo a un cambiamento rilevante nelle modalità e nelle finalità perseguite dagli attaccanti, che evidentemente riescono a ottenere con maggiore efficacia i loro scopi utilizzando tecniche diverse", ha affermato Paolo Giudice, segretario generale di Clusit. Sono invece i DDoS a registrare una notevole crescita nel nostro Paese, fanno notare gli esperti di Clusit, passando dal 4% del 2022 al 30% del primo semestre 2023, una quota di 5 volte superiore. L'incidenza di attacchi di questa tipologia in Italia è estremamente più elevata rispetto a quella registrata nel campione complessivo, che si ferma al 7,9%: le vittime italiane hanno subito un numero maggiore di attacchi DDoS, tanto da registrare circa il 37% del totale di tali eventi censito nel campione globale. Gli attacchi DDoS, che mirano a rendere inaccessibile/inutilizzabile un servizio online sovraccaricandone le risorse, sono una delle tecniche più utilizzate dagli hacktivist per raggiungere i loro obiettivi; è quindi evidente, nel panorama italiano, la correlazione tra l'aumento di attacchi che sfruttano questa tecnica e la crescita della quota di incidenti riconducibile proprio alla tipologia Hacktivism - confermano gli autori del Rapporto Clusit - grazie alla quale è possibile interrompere le attività di un'azienda o di un'istituzione, con lo scopo di attirare l'attenzione mediatica su una causa politica o sociale, esercitando così pressione sulla vittima e mettendone in luce la scarsa capacità di difesa. In aumento anche il dato degli attacchi di tipo phishing e ingegneria sociale, che in Italia risulta incidere in maniera maggiore rispetto al resto del mondo (14% vs 8,6% globale): "Questa crescita è indice di una forte necessità di sensibilizzazione e aumento della consapevolezza rispetto alle minacce cyber da parte degli utenti che hanno quotidianamente a che fare con i sistemi informatici", ha confermato Paolo Giudice. La "Severity" degli attacchiAnche nel primo semestre dell'anno in corso gli attacchi con impatti gravi o gravissimi – ovvero con ripercussioni tecnologiche, economiche, legali e reputazionali - sono stati la stragrande maggioranza, arrivando al 78,5% (erano l'80% nel 2022). Gli incidenti con impatti medi sono solo un quinto, mentre sono quasi del tutto scomparsi quelli con impatti bassi. "Investiamo sempre di più in cybersecurity3 , sebbene non ancora abbastanza, ma subiamo anche più danni", ha ribadito Gabriele Faggioli. "È il sintomo che dovremmo rivalutare gli investimenti, oltre che incrementarli, con un approccio al problema radicalmente differente, investendo condivisione della conoscenza, delle risorse e dei costi cyber in un'ottica

di economia di scala".La gravità degli attacchi è stata inoltre analizzata dai ricercatori di Clusit in relazione alla tipologia di attaccanti. Il Cybercrime, nel primo semestre 2023 ha avuto impatti gravi nel 40% dei casi; gli attacchi perpetrati con finalità di spionaggio o cyber warfare mostrano impatti critici che arrivano quasi all'80% dei casi, in decisa crescita rispetto al 2022. La categoria governativa / militare è quella che subisce attacchi di gravità maggiore; in crescita anche l'impatto degli attacchi nel settore Healthcare, che resta un bersaglio conveniente sia per attacchi a sfondo economico che per arrecare danni ai servizi fondamentali della società. In termini di severity, il quadro italiano nei primi 6 mesi del 2023 appare più roseo rispetto al dato globale, con un numero minore di attacchi con severità massima: gli incidenti di tipo "Critical" si fermano al 20% (vs 40% globale), mentre la quota maggiore di attacchi fa riferimento a una severity "High" (48% in Italia vs 38% globale) e "Medium" (30% in Italia vs 21% globale). Completa il quadro un 2% di incidenti con criticità bassa. Questo a conferma – come hanno evidenziato gli autori del Rapporto Clusit – dell'incremento degli attacchi "di disturbo" in Italia, con severity limitata, che riescono però sempre più spesso ad andare a buon fine. "Questo dato è coerente con la crescita dell'Hacktivism e degli attacchi di tipo DDoS, che hanno tipicamente queste caratteristiche. Si tratta comunque di attacchi che possono causare danni economici per le vittime che li subiscono, oltre che avere un effetto rilevante in termini di reputazione, essendo spesso messi in atto con scopo dimostrativo", ha concluso Paolo Giudice.

(Prima Pagina News) Giovedì 09 Novembre 2023

Verbalia Comunicazione S.r.l. Società Editrice di PRIMA PAGINA NEWS
Registrazione Tribunale di Roma 06/2006 - P.I. 09476541009
Iscrizione Registro degli Operatori di Comunicazione n. 21446

Sede legale : Via Costantino Morin, 45 00195 Roma
Redazione Tel. 06-45200399 r.a. - Fax 06-23310577
E-mail: redazione@primapaginanews.it