Cyber Security, Fastweb fotografa le principali evoluzioni nel panorama della sicurezza italiana per il Rapporto Clusit 2024

Milano, 6 marzo 2024 – Anche quest'anno Fastweb contribuisce a fotografare la situazione del cyber crime in Italia fornendo un'analisi dei fenomeni più rilevanti elaborata dal proprio Security Operations Center (SOC) attivo 24 ore su 24 e dai propri centri di competenza di sicurezza informatica. Per la prima volta anche 7Layers, società acquisita da Fastweb nel 2020 e specializzata in soluzioni avanzate di cybersecurity, ha collaborato al report.

L'analisi inserita all'interno del Rapporto Clusit 2024, il report dell'Associazione Italiana per la Sicurezza Informatica sulla sicurezza ICT, evidenzia quest'anno il consolidamento di alcune tendenze osservate in passato e la nascita di nuovi trend derivanti anche della progressiva integrazione dell'Intelligenza Artificiale all'interno delle tecniche e degli strumenti di attacco così come di difesa.

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 attivi, si sono registrati oltre 56 milioni di eventi di sicurezza, in linea, per la prima volta da anni, con il dato del 2022.

Se nel 2023 la totalità degli eventi di sicurezza rilevati è rimasta stabile, sul fronte degli attacchi DDoS (Distributed Denial of Service) si registrano invece 2.300 eventi significativi (+28% rispetto al 2022) e circa 13.000 anomalie riconducibili a possibili attacchi alla rete di Fastweb con un deciso aumento pari al 32% e in controtendenza con la contrazione del biennio precedente degli attacchi ad alto impatto (oltre 100 Gbps di banda utilizzata) a dimostrazione di come il progressivo aumento delle capacità di difesa delle organizzazioni spinge i criminali informatici a sviluppare attacchi sempre più gravi e impattanti, mentre diminuiscono le anomalie a basso impatto (-40%). I settori più colpiti rimangono ancora il settore Finance/Insurance e la Pubblica Amministrazione, che insieme costituiscono oltre il 55% dei casi. L'aumento più significativo è quello del settore del Gambling, cresciuto dal 2% del 2022 a quasi il 12% del 2023.

L'incidenza dell'Intelligenza Artificiale e la sua crescente pervasività sia come strumento di attacco che difesa rappresenta una nuova frontiera della cybersecurity che sta già dispiegando i suoi effetti.

L'AI ha contribuito infatti a migliorare la capacità di identificare e raccogliere informazioni sugli attori degli attacchi cyber incrementando significativamente anche l'efficacia degli strumenti di riconoscimento di pattern malevoli contenuti nelle mail, con una riduzione fino al 70% degli eventi "falsi positivi" rilevati, parallelamente però si assiste ad un aumento degli attacchi che sfruttano l'AI per aumentare l'efficacia degli attacchi. Gli eventi malevoli legati al "credential phishing", per esempio, che mirano a persuadere le vittime a rivelare informazioni sensibili tramite contenuti e comunicazioni verosimili registrano infatti un aumento dell'87% mentre gli attacchi di social engineering che sfruttano l'AI e il fattore umano per generare, ad esempio, messaggi audio falsi per convincere le persone a fornire informazioni personali o a eseguire alcune azioni come per esempio comunicare i propri dati personali, sono in aumento del 13% rispetto al 2022.

A fronte di questi fenomeni, anche nel 2023 si registra però il costante aumento della consapevolezza rispetto ai rischi informatici da parte di aziende e PA nel contrasto alle strategie di attacco dei criminali informatici testimoniato da un' ulteriore riduzione, pari all'8%, del numero dei server che espongono su internet servizi critici (38.000 nel 2023) oltre che dall'utilizzo di strumenti di ricerca e monitoraggio che hanno contribuito a migliorare l'identificazione delle minacce.

Rispetto al 2022 prosegue nel 2023 la flessione (-3%) nel volume di malware e botnet e del numero delle famiglie di software malevoli (-29%) così come della quantità di famiglie di malware e botnet sconosciute (-70% rispetto al 2022), anche grazie alla maggiore efficacia degli strumenti zeroday di difesa presenti sul mercato.

Grazie alla collaborazione con 7Layers, il report include quest'anno anche il monitoraggio relativo alle minacce informatiche rilevate e contrastate tramite il servizio di Managed Detection and Response (MDR) che ha permesso di identificare i macro trend delle tecniche di attacco più comunemente utilizzate dai criminali informatici. Al primo posto con il 19% del totale si posizionano gli attacchi "Multiple" caratterizzati da scenari complessi e tattiche di attacco diversificate, seguiti dagli attacchi "Exfiltration" con il 15% che puntano alla sottrazione di dati sensibili, mentre gli attacchi di tipo "Initial Access" realizzati per individuare potenziali vulnerabilità rappresentano il 13% degli attacchi. Eventi ad alto impatto e che possono causare danni significativi come ransomware o cryptominer contribuiscono invece al 9%.

Per informazioni:

FASTWEB Ufficio Stampa
Roberta Dellavedova
Tel. + 348 14 71 722
roberta.dellavedova@fastweb.it