25/03/2020

IL RAPPORTO CLUSIT: L'ANALISI DI FASTWEB

Di Francesca Romana Tubili

Il Rapporto CLUSIT 2020, giunto ormai al nono anno di pubblicazione, inizia con una panoramica degli eventi di cyber-crime più significativi avvenuti a livello globale nel 2019, confrontandoli con i dati raccolti nei 5 anni precedenti.

Lo studio si basa su un campione che al 31 dicembre 2019 è costituito da 10.087 attacchi noti di particolare gravità, ovvero che hanno avuto un impatto significativo per le vittime in termini di perdite economiche, di danni alla reputazione, di diffusione di dati sensibili, o che comunque prefigurano scenari particolarmente preoccupanti, avvenuti nel mondo (inclusa l'Italia) dal primo gennaio 2011. Sono stati 1.670 gli attacchi cyber messi a segno nel 2019, con una percentuale di crescita del 7,6% sul 2018 e del 91,2% rispetto al 2014. Alessio Pennasilico, membro del comitato tecnico scientifico Clusit, sostiene un forte aumento dell' attenzione riguardo il tema della cyber security e quindi diventano particolarmente rilevanti i dati pubblicati all'interno del report.

Andrea Zapparoli Manzoni, del Comitato direttivo di Clusit, spiega che nei mesi di luglio, agosto, settembre, ottobre e dicembre è presente una significativa accelerazione degli attacchi con il +48% degli attacchi gravi nel triennio 2017-2019. E' un dato significativo poichè normalmente durante la stagione estiva il trend tende a diminuire, ma questo ci fa

capire come le organizzazioni criminali siano strutturate in modo tale da poter garantire attacchi tutto l'anno.

La categoria "Target Multipli" è stata quella più colpita del 2019 superando il settore Gov; al terzo posto abbiamo il settore Healthcare, al quarto Online services e Cloud e al quinto posto Ricerca ed Educazione. L'esperto fa notare che confrontando i dati, emerge che le misure adottate dalle vittime sono diverse, perché differente è la minaccia che incombe. Ad esempio verso i Target Multipli, la percentuale di attacchi riconducibile al cybercrime è dell'84%. Nell'Healthcare, settore le cui strutture sono attaccate perché fragili e spesso costrette a pagare in caso di ransomware per tutelare la continuità e dunque la salute dei pazienti, la percentuale di episodi legati al cyber crime sale al 94%. Tra le tecniche più utilizzate per danneggiare le organizzazioni abbiamo il malware: è stato utilizzato nel 44% degli attacchi, con una crescita del +24%, rispetto all'anno scorso.

Seguono le tecniche sconosciute, i social engineering e attacchi phishing, con una crescita del + 81,9% sul 2018. Al quarto posto ci sono lo sfruttamento delle vulnerabilità e al quinto posto gli attacchi APT.

All'interno del rapporto, anche quest'anno, la situazione italiana è stata analizzata da Fastweb che nel corso del 2019 ha raccolto ed esaminato attraverso il proprio Security Operations Center oltre 43 milioni di attacchi informatici transitati sulla sua infrastruttura.

Accanto a una forte crescita dei malware che coinvolgono per la maggior parte le utenze domestiche, Fastweb rileva una importante e positiva riduzione degli attacchi di natura DDoS verso le Pubbliche Amministrazioni, perchè queste ultime come anche i settori finance/insurance hanno adottato tecniche di difesa per ridurre gli attacchi. La diminuzione

delle durata a meno di 3 ore per il 95% degli attacchi costituisce un chiaro indicatore dell'efficacia delle misure adottate dai centri di competenza per il contrasto al cybercrime.

Un attacco DoS (Denial of Service) è un attacco volto ad arrestare un computer, una rete o anche solo un particolare servizio. Esso viene realizzato utilizzando delle botnet, ovvero decine di migliaia di dispositivi (non più solo computer di ignari utenti), in grado di generare richieste verso uno specifico target con l'obiettivo di saturarne in poco tempo le risorse e di renderlo indisponibile.

Gli effetti di un attacco DdoS sono devastanti sia a causa della potenza e sia perchè ci sono difficoltà per ridurre in tempi brevi l'attacco stesso.

Quanti sono stati gli attacchi DdoS nel 2019 e quali i settori più colpiti? Nel 2019 sono state rilevate oltre 15.000 anomalie riconducibili a possibili attacchi DdoS diretti verso i Clienti Fastweb. Per quanto concerne i settori più colpiti, Il CLUSIT 2020, ha riportato alcuni dei settori merceologici: tra questi abbiamo il mondo del gaming e il mondo del Finance/Insurance, il settore Media, Service Provider e il mondo della Pubblica Amministrazione. Quest'ultimi, avendo considerato i gravi effetti dell'attacco, hanno aumentato la loro consapevolezza, investendo per le loro aziende, per poter garantire un'adeguata protezione; si è osservato quindi che quest'anno oltre l'95% degli attacchi è durato meno di 3 ore.

Per ulteriori informazioni rimandiamo al documento ufficiale:

file:///C:/Users/Francesca/Downloads/Rapporto_Clusit_2020%20(1).pdf