Attacchi hacker: +12% rispetto allo scorso anno, uno su dieci sfrutta il tema Covid-19

Il 2020 registra un incremento di cyber attacchi del 12% rispetto al 2019.

Il 10% è stato a tema Covid-19.

Nell'anno della pandemia, il rapporto Clusit 2021 registra il record negativo degli attacchi informatici: a livello globale sono stati infatti 1.871 gli attacchi gravi di dominio pubblico rilevati nel corso del 2020, ovvero con un impatto sistemico in ogni aspetto della società, della politica, dell'economia e della geopolitica. In media, si tratta di 156 attacchi gravi al mese, il valore più elevato mai registrato ad oggi (erano 139 nel 2019), con il primato negativo che spetta al mese di dicembre, in cui sono stati rilevati ben 200 attacchi gravi.

In termini percentuali, nel 2020 l'incremento degli attacchi cyber a livello globale è stato pari al 12% rispetto all'anno precedente; negli ultimi quattro anni il trend di crescita si è mantenuto pressoché costante, facendo segnare un aumento degli attacchi gravi del 66% rispetto al 2017.

I dati sono stati illustrati alla stampa questa mattina nel corso della presentazione in anteprima della sedicesima edizione del Rapporto Clusit sulla sicurezza ICT in Italia e nel mondo : gli autori hanno tuttavia evidenziato che lo scenario riportato è certamente meno critico rispetto alla situazione effettiva, per la tendenza complessiva delle vittime a mantenere, ove possibile, riservati gli attacchi cyber subìti, soprattutto in Europa, anche a fronte del vigente Regolamento GDPR e della Direttiva NIS.

Il Cybercrime è stato nel 2020 la causa dell'81% degli attacchi gravi a livello globale; le attività di Cyber Espionage costituiscono invece il 14% degli attacchi: diverse attività di questo tipo risultano correlate alle elezioni USA nella seconda metà dell'anno, con tentativi di influenzare l'opinione pubblica da parte di attori interni ed esterni.

Operazioni di spionaggio sono state rilevate dagli esperti Clusit anche ai danni di molti enti di ricerca ed aziende coinvolte nello sviluppo dei vaccini contro il Covid-19.

Proprio la pandemia ha caratterizzato il 2020 per andamento, modalità e distribuzione degli attacchi secondo gli esperti del Clusit: il 10% degli attacchi portati a termine a partire da fine gennaio è stato a tema Covid-19. In particolare, i cybercriminali hanno sfruttato la situazione di disagio collettivo, nonché di estrema difficoltà vissuta da alcuni settori - come quello della produzione dei presidi di sicurezza (ad esempio, delle mascherine) e della ricerca sanitaria - per colpire le proprie vittime. Diverse operazioni di spionaggio sono state compiute a danno di organizzazioni di ricerca correlate con lo sviluppo dei vaccini.

Nello specifico settore della Sanità, il 55% degli attacchi a tema Covid-19 è stato perpetrato a scopo di cybercrime, ovvero per estorcere denaro; con finalità di "Espionage" e di "Information Warfare" nel 45% dei casi. Sostanzialmente stabili, invece, negli ultimi 12 mesi, gli attacchi globali appartenenti alla categoria

Cyber Warfare – la guerra delle informazioni, che costituiscono il 3% del totale.

Gli attacchi registrati nel 2020 sono stati classificati dagli esperti Clusit anche in base ai loro differenti livelli di impatto, sulla base di una valutazione dei danni dal punto di vista geopolitico, sociale, economico (diretto e indiretto) e di immagine. Nel 2020 gli attacchi rilevati e andati a buon fine hanno avuto nel 56% dei casi un impatto "alto" e "critico"; il 44% è stato di gravità "media".

Gli attacchi correlati a finalità di Cyber Espionage, per quanto numericamente inferiori, risultano avere una gravità più alta della media, e preoccupano per la loro continua crescita.

Cyber attacchi nel 2020: chi è stato colpito e perché - Tra i settori colpiti da attacchi cyber gravi negli ultimi dodici mesi, spiccano (in ordine decrescente):

- "Multiple Targets": 20% del totale. Si tratta di attacchi realizzati in parallelo verso obiettivi molteplici, spesso indifferenziati, che vengono colpiti "a tappeto" dalle organizzazioni cyber criminali, secondo una logica "industriale". Gli attacchi verso questa categoria di obiettivi sono tuttavia in calo del 4% rispetto al 2019;
- Settore Governativo, Militare, Forze dell'Ordine e Intelligence, che hanno subìto il 14% degli attacchi a livello globale;
- Sanità, colpita dal 12% del totale degli attacchi;
- Ricerca/Istruzione, verso cui sono stati rivolti l'11% degli attacchi
- Servizi Online, colpiti dal 10% degli attacchi complessivi.

Sono cresciuti, inoltre, gli attacchi verso Banking & Finance (8%), Produttori di tecnologie hardware e software (5%) e Infrastrutture Critiche (4%). Gli esperti Clusit hanno inoltre registrato nel corso degli ultimi dodici mesi un incremento di attacchi veicolati tramite l'abuso della supply chain, ovvero tramite la compromissione di terze parti, il che consente poi a criminali e spie di colpire i contatti (clienti, fornitori, partner) dell'obiettivo, ampliando notevolmente il numero delle vittime e passando più facilmente inosservati.

Le tecniche d'attacco - Nel 2020 gli attacchi cyber sono stati messi a segno prevalentemente utilizzando Malware (42%), tra i quali spiccano i cosiddetti Ransomware - una tipologia di malware che limita l'accesso ai dati contenuti sul dispositivo infettato, richiedendo un riscatto - utilizzati in quasi un terzo degli attacchi (29%), la cui diffusione è in significativa crescita (erano il 20% nel 2019), sia in termini assoluti che in termini di dimensioni dei bersagli e di ammontare dei danni.

Seguono le "tecniche sconosciute" (in riferimento alle quali prevalgono i casi di Data Breach, per il 20%), mentre Phishing & Social Engineering continuano ad essere la causa di una buona parte degli attacchi (15% del totale); si registra inoltre negli ultimi dodici mesi una crescita degli attacchi sferrati per mezzo di vulnerabilità note (+ 10%), precedentemente in calo (-29% nel 2019 rispetto al 2018).

Dove colpiscono i cybercriminali - Gli attacchi classificati dai ricercatori di Clusit si sono verificati nel 47% dei casi negli Stati Uniti; nel 22% dei casi in località multiple, a dimostrazione della capacità degli attaccanti di colpire in maniera diffusa bersagli geograficamente distanti e/o organizzazioni multinazionali. In Europa gli attacchi sono aumentati negli ultimi dodici mesi del 13%, arrivando a rappresentare il 17% degli attacchi globali. Gli eventi di in-sicurezza cyber hanno colpito per l'11% l'Asia, il 2% l'Oceania e l'1% l'Africa.

Fonte: Federprivacy.org