Presentato oggi il Rapporto Clusit 2021 sulla sicurezza cyber

Clusit: attacchi informatici in crescita, i danni globali valgono due volte il PIL italiano

Nel 2020 gli attacchi nel mondo sono aumentati del 12% rispetto all'anno precedente; il 10% ha sfruttato il tema Covid-19.
Il 14% degli eventi è dovuto a spionaggio cyber; nel mirino anche lo sviluppo dei vaccini

Milano, 2 marzo 2021 – Nell'anno della pandemia, Clusit - Associazione Italiana per la Sicurezza Informatica - 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**[1]: 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.

[1] Frutto del lavoro di oltre un centinaio di professionisti che operano nell'ambito dell'Associazione per la Sicurezza Informatica in Italia, dal 2011 il Rapporto Clusit fornisce su base semestrale il quadro più aggiornato ed esaustivo della situazione globale dei crimini informatici, evidenziando i settori più colpiti, le tipologie e le tecniche d'attacco più frequenti, sulla base degli attacchi gravi di dominio pubblico rilevati ed analizzati nel periodo in esame.

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.

"Le minacce cibernetiche rappresentano ormai un rischio estremamente serio per Governi, pubbliche amministrazioni, aziende e cittadini" commenta ***Sofia Scozzari****,* ***membro del Comitato Scientifico Clusit e co-autrice della ricerca****. "La varietà, la determinazione, la capacità tecnica e in alcuni casi la 'cattiveria' degli attaccanti hanno raggiunto livelli inauditi, e impressionano a maggior ragione nel contesto della crisi sanitaria globale che stiamo vivendo".*

"La crescita straordinaria delle minacce cyber, in particolare nell'ultimo quadriennio, ha colto alla sprovvista tutti gli stakeholders della nostra civiltà digitale, e rappresenta ormai a livello globale una "tassa" sull'uso dell'ICT che arriva a duplicare il valore del PIL italiano stimato nel 2020[2]*, considerando le perdite economiche dirette e quelle indirette dovute al furto di proprietà intellettuale. È urgente che siano ripensate a fondo le logiche di contrasto e mitigazione di queste minacce, e siano messe in campo le risorse necessarie ad impedire che l'adozione sempre più spinta e capillare dell'ICT, di per sé auspicabile, possa trasformarsi in un boomerang sul piano geopolitico, sociale ed economico" sottolinea* ***Andrea Zapparoli Manzoni, membro del Comitato Direttivo e co-autore dell'analisi Clusit****.*

"*I dati presentati oggi ci mostrano ancora una volta che l'accelerazione continua del cyber crime ha un impatto sempre più elevato sulla nostra società*", afferma **Gabriele Faggioli, presidente di Clusit**. "*Lavoriamo a fianco delle istituzioni per promuovere un processo virtuoso di crescita tecnologica, che parta dalla formazione in età scolastica, passando dal supporto delle start up, alla*

[2] Ovvero, un valore pari a 1.651.595 milioni di euro, stima Istat

condivisione di sapere e collaborazione tra pubblico e privato, al fine di garantire continuità sociale ed economica", conclude Faggioli.

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.

Analisi Fastweb della situazione italiana in materia di cyber-crime e incidenti informatici
Fastweb presenta all'interno del Rapporto Clusit l'analisi dei fenomeni più rilevanti elaborata dal proprio Security Operations Center (SOC) nel corso del 2020. Anche in questo caso, è evidente che la pandemia ha fortemente caratterizzato gli eventi di cybercrime.

Durante l'anno, l'infrastruttura di rete di Fastweb, costituita da oltre 6,5 milioni di indirizzi IP pubblici, ha registrato oltre 36 milioni di eventi di sicurezza. Si tratta di una cifra in netta flessione rispetto al 2019 (iniziata principalmente dopo il primo trimestre del 2020, in corrispondenza con il lockdown e la remotizzazione del lavoro di molte imprese), a fronte tuttavia di una crescita degli attacchi verso gli endpoint, ovvero i dispositivi dei dipendenti. La maggior consapevolezza dei rischi legati agli attacchi informatici in periodo di pandemia ha spinto sicuramente le aziende ad innalzare i propri livelli di protezione per garantire la continuità operativa, portando i criminali informatici a modificare in parte i propri obiettivi: sono stati infatti 85.000 gli attacchi indirizzati ai dispositivi personali, raddoppiati rispetto allo stesso periodo del 2019. Il fenomeno si spiega anche considerando che durante il periodo di emergenza molte aziende non sono riuscite a dotare i propri dipendenti di laptop aziendali, con conseguente utilizzo di dispositivi personali, solitamente maggiormente vulnerabili a malware e virus.

Il Rapporto Clusit 2021 sarà presentato al pubblico il prossimo 16 marzo, in apertura di Security Summit Streaming Edition, il più importante convegno italiano sulla cybersecurity, organizzato da Clusit - Associazione Italiana per la Sicurezza Informatica – con Astrea, Agenzia di Comunicazione e Marketing, specializzata nell'organizzazione di eventi business nel mondo della tecnologia e in particolare della sicurezza informatica.

# # #

Clusit - Associazione Italiana per la Sicurezza Informatica - i cui soci rappresentano oltre 500 aziende e organizzazioni. Clusit collabora, a livello nazionale, con diversi Ministeri, Authority e Istituzioni, con la Polizia Postale e con altri organismi di controllo. Inoltre, svolge un'intensa attività di supporto e di scambio con le Confederazioni Industriali, con numerose Università e Centri di Ricerca e con Associazioni Professionali e dei Consumatori. In ambito internazionale, Clusit partecipa a molte iniziative in collaborazione con i CERT, i CLUSI, la Commissione Europea, ITU (International Telecommunication Union), UNICRI (Agenzia delle Nazioni Unite che si occupa di criminalità e giustizia penale) e sostiene attivamente le attività di ENISA (European Union Agency for Network and Information Security). Ulteriori informazioni sulle attività del 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