SECURITY SUMMIT
Streaming Edition

Anteprima Rapporto Clusit 2022 sulla sicurezza cyber

Clusit: la mano della criminalità organizzata sul cybercrime; nel 2021 a livello mondiale stimati danni pari a 4 volte il PIL italiano.

Nello scorso anno gli attacchi gravi nel mondo sono aumentati del 10% rispetto al 2020 e sono stati sempre più devastanti. Un quinto degli attacchi ha colpito l'Europa.

Milano, 7 marzo 2022 – Sono sempre inesorabilmente in crescita i crimini informatici, ma evolvono modalità e attori. È la fotografia presentata oggi dai ricercatori di Clusit - Associazione Italiana per la Sicurezza Informatica - che nel **Rapporto Clusit 2022**[1] raccolgono e analizzano i dati relativi agli incidenti informatici su scala globale degli ultimi 12 mesi, proponendo un confronto critico con gli anni precedenti.

Nel 2021 sono stati registrati **2.049 cyber attacchi gravi**[2]: si tratta di un aumento che sfiora il 10% rispetto all'anno precedente, per una media mensile di 171 attacchi, il valore più elevato mai registrato. Nell'illustrare i dati, i ricercatori e gli esperti di Clusit hanno tuttavia evidenziato che certamente la situazione effettiva è ben peggiore, data la tendenza complessiva delle vittime a mantenere, ove possibile, riservati gli attacchi cyber subìti; la tendenza appare evidente ancora oggi in Europa, anche a fronte di normative ormai consolidate, quali il Regolamento GDPR e la Direttiva NIS.

Gli attacchi crescono in quantità e in "qualità": la classificazione dei ricercatori di Clusit si basa anche su una valutazione dei **livelli di impatto** dei singoli incidenti, che tiene in considerazione aspetti di immagine, economici, sociali e le ripercussioni dal punto di vista geopolitico.

---

[1] Frutto del lavoro di oltre un centinaio di professionisti che operano nell'ambito dell'Associazione per la Sicurezza Informatica in Italia, il Rapporto Clusit fornisce dal 2011 su base semestrale il quadro 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. Nel 2022 il Rapporto è giunto alla diciottesima edizione.

[2] I ricercatori di Clusit classificano come "gravi" gli attacchi con un impatto sistemico in ogni aspetto della società, della politica, dell'economia e della geopolitica.

Clusit Associazione Italiana per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

Severità degli attacchi in forte aumento.
Nel 2021 il **79% degli attacchi** rilevati ha avuto un **impatto "elevato"**, contro il 50% dello scorso anno. In dettaglio, il 32% è stato caratterizzato da una severity "critica" e il 47% "alta".
A fronte di queste percentuali, sono diminuiti invece gli attacchi di impatto "medio" (-13%) e "basso" (-17%).

Oltre alla frequenza, nel corso del 2021 è aumentato in maniera netta l'indice di gravità degli attacchi analizzati, agendo da significativo moltiplicatore dei danni, stimati per il 2021 in **6 trilioni di dollari** (da 1 trilione di dollari stimato per il 2020)[3]. *"Si tratta di una crescita drammatica, con un tasso di peggioramento annuale a 2 cifre, per un valore già pari a 4 volte il PIL italiano",* commenta **Andrea Zapparoli Manzoni**, membro del Comitato Direttivo Clusit. "*Non è più possibile procrastinare l'adozione di contromisure efficaci e i necessari investimenti. Le risorse allocate dal PNRR dovranno a nostro parere essere gestite con una governance stringente in ottica cyber security di tutti i progetti di digitalizzazione previsti, valorizzando finalmente le competenze cyber delle risorse umane del Paese"*, conclude Zapparoli Manzoni.

Gli attacchi cyber nel 2021: quali finalità?
Il **cybercrime** si conferma la motivazione dell'**86% dei cyber attacchi**, in crescita rispetto al 2020 (+5%), un trend che non accenna a diminuire. Tra gli attacchi gravi di dominio pubblico, l'**11%** è riferibile ad attività di Espionage e il **2%** a campagne di Information Warfare.

Cyber attacchi nel 2021: chi è stato colpito e perché.
Per la prima volta dopo diversi anni i ricercatori di Clusit rilevano che l'obiettivo più colpito non è più quello dei "Multiple targets", ovvero i cyber criminali non colpiscono più in maniera indifferenziata obiettivi molteplici, ma **mirano a bersagli ben precisi**: al primo posto c'è l'obiettivo **governativo/militare**, con il **15%** degli attacchi totali, in crescita del 3% rispetto all'anno precedente; segue il settore **informatica**, colpito nel **14%** dei casi e stabile rispetto al 2020; gli **obiettivi multipli** (**13%**, in discesa dell'8%) e la **sanità**, che rappresenta il **13%** del totale degli obiettivi colpiti, in crescita del 2% rispetto ai dodici mesi precedenti. L'**8%** del totale degli attacchi è stato rivolto nel 2021 al settore dell'**istruzione**, che rimane sostanzialmente stabile rispetto al 2020 (-1%).

Il quadro complessivo che si evince - spiegano i ricercatori di Clusit - è che **i cyber attacchi nel 2021 sono stati mirati e meglio tarati per colpire bersagli specifici appartenenti a tutti i settori**: "*È interessante notare che la differenza tra le percentuali dei settori più colpiti si assottiglia: per la prima volta non vediamo categorie di vittime prese di mira in modo particolare rispetto ad altre. È invece evidente che i cyber attacchi stanno colpendo tutti i settori, in maniera sostanzialmente uniforme, e al tempo stesso più selettiva, la 'pesca a strascico' indifferenziata sta diminuendo*", afferma **Sofia Scozzari**, membro del Comitato Scientifico Clusit.

3 https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Le tecniche d'attacco.
I **Malware** - e in particolare il **Ransomware** - si riconfermano gli strumenti preferiti dei cyber criminali per generare profitti e rappresentano, come nel 2020, il **41%** delle tecniche utilizzate. Seguono tecniche "**Unknown"[4],** per lo più relative a casi di Data Breach, utilizzate nel **21%** dei casi, le **vulnerabilità note** (**16%** dei casi) e **Phishing / Social Engineering**, tecnica utilizzata nel **10%** degli attacchi.

I cyber criminali da una parte sono sempre più sofisticati e cercano nuove vie per riuscire a penetrare meglio nei sistemi individuati come obiettivi, come per esempio è stato per gli attacchi di phishing a tema Covid-19, o i crescenti attacchi realizzati alterando la supply-chain di importanti organizzazioni, con ripercussioni globali. Tuttavia, sanno anche di poter contare su mezzi più tradizionali, come le vulnerabilità note, che non sempre vengono rimediate con la celerità necessaria.

"*L'aspetto più preoccupante è che, a differenza dei difensori, i criminali oggi collaborano attivamente tra loro*", commenta Sofia Scozzari. "*Si sono ormai consolidati dei cartelli di servizi criminali identificabili, per esempio, come 'Ransomware as a Service'. Significa che chi utilizza il ransomware non è più necessariamente chi lo ha progettato, né un esperto di sistemi come ci aspetteremmo da un 'tradizionale' cyber criminale. Pensiamo che si tratti a questo punto di vera e propria criminalità organizzata, che ha capito quanto i crimini cyber possono essere remunerativi*".

La geografia degli attacchi.
Gli attacchi classificati dai ricercatori di Clusit si sono verificati nel **45% dei casi** ancora nel continente americano (in calo del 2% rispetto al 2020).
Sono invece cresciuti gli attacchi verso l'**Europa**, che superano un quinto del totale (**21%**, +5% rispetto all'anno precedente), e verso l'**Asia** (**12%**, +2% rispetto al 2020). Resta sostanzialmente invariata la situazione degli attacchi verso **Oceania** (**2%**) e **Africa** (**1%**).

Sono invece in diminuzione gli attacchi verso location **multiple**, che costituiscono il **19% del totale (**-5% rispetto al 2020).

"*Anche da queste rilevazioni abbiamo indicazione che gli attacchi cyber nel 2021 sono stati più mirati, con una crescita in Europa ed Asia*", puntualizza Sofia Scozzari.

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 2021 è stato registrato in Italia un aumento generalizzato degli attacchi informatici. In dettaglio, 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, si sono registrati oltre **42 milioni di eventi di sicurezza**, con un **aumento del 16%** rispetto agli eventi rilevati nel 2020.
Tra i trend più rilevanti del 2021 si osserva la continua crescita dei **malware e botnet**, con un numero di server e device compromessi che fa segnare un netto **+58%**. Riguardo alla distribuzione

[4] Tali vettori di attacco risultano "sconosciuti" in quanto non resi pubblici dalle vittime, oppure non ancora individuati al momento della loro classificazione. Al primo caso si riferiscono molti "data breach", dal momento che la normativa prevede un obbligo di notifica che non include anche la descrizione delle modalità dell'attacco subito.

geografica dei malware, nel 2021 si rileva un aumento del **numero di attacchi da server ospitati in Europa rispetto agli Stati Uniti.**

Fastweb, inoltre, quest'anno ha monitorato le minacce afferenti ai **servizi Mail** che vedono una continua crescita. Il vettore d'attacco principale è l'utilizzo di **URL malevoli, con l'87%** sul totale, in **crescita dell'11%**. In aumento, secondo Fastweb, anche i **fenomeni fraudolenti che sfruttano il servizio SMS**, dovuti in particolare alla diffusione di malware, quali Flubot, veicolati attraverso **smishing** (il phishing via SMS) e che espongono inoltre gli utenti a molteplici **rischi in ambito Privacy**.

Il Rapporto Clusit 2022 sarà presentato al pubblico il prossimo 15 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 ed Eventi specializzata nel settore della Sicurezza Informatica.

###

Clusit è l'Associazione Italiana per la Sicurezza Informatica. Nata nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, rappresenta oggi oltre 600 organizzazioni, appartenenti a tutti i settori del Sistema-Paese. Clusit collabora con la Presidenza del Consiglio, con diversi Ministeri, Authority, Istituzioni e organismi di controllo, tra cui Polizia Postale e delle Comunicazioni, Arma dei Carabinieri e Guardia di Finanza, Agenzia per l'Italia Digitale, Autorità Garante per la tutela dei dati personali. Svolge inoltre un'intensa attività di supporto e di scambio con le Associazioni Professionali e Associazioni dei Consumatori, Confindustria, Confcommercio e CNA, con Università e Centri di Ricerca. In ambito internazionale, Clusit partecipa a diverse iniziative in collaborazione con i CERT, i CLUSI, con la Commissione Europea, ENISA (European Union Agency for Cybersecurity), ITU (International Telecommunication Union), OCSE, UNICRI (Agenzia delle Nazioni Unite che si occupa di criminalità e giustizia penale), con le principali Associazioni Professionali del settore, con Università e Centri di Ricerca in oltre 20 paesi. Ulteriori informazioni sulle attività di 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