Presentata la nuova edizione del Rapporto Clusit 2022 sulla sicurezza cyber

Clusit: scenario di guerra cibernetica globale, oltre un terzo degli attacchi ha impatto critico; più di un quarto colpisce l'Europa

Faggioli, presidente Clusit: "Il conflitto russo-ucraino ci pone davanti alla necessità di rafforzare le infrastrutture critiche; l'Italia deve cogliere l'opportunità della transizione digitale per colmare le proprie lacune sulla sicurezza informatica"

Milano, 9 novembre 2022 – Nei primi sei mesi del 2022 sono stati **1.141 gli attacchi cyber gravi**, ovvero con un impatto sistemico in diversi aspetti della società, della politica, dell'economia e della geopolitica: nel dettaglio, si è registrata una crescita dell'8,4% rispetto al primo semestre 2021, per una media complessiva di **190 attacchi al mese**, con un picco di 225 attacchi a marzo 2022, il valore più alto mai verificato.

I dati sono stati illustrati oggi nell'ambito della presentazione dell'edizione di fine anno del **Rapporto Clusit 2022**[1] a cura di Clusit - Associazione Italiana per la Sicurezza Informatica. Nelle pagine del Rapporto, i ricercatori raccolgono e analizzano i dati relativi agli incidenti informatici su scala globale degli ultimi 12 mesi, proponendo un confronto critico con gli anni precedenti, al fine di fornire una fotografia dei rischi attuali e futuri su cui sviluppare *threat modeling*, studio e gestione del rischio cyber e impostazione di una strategia di difesa a livello aziendale ed istituzionale.

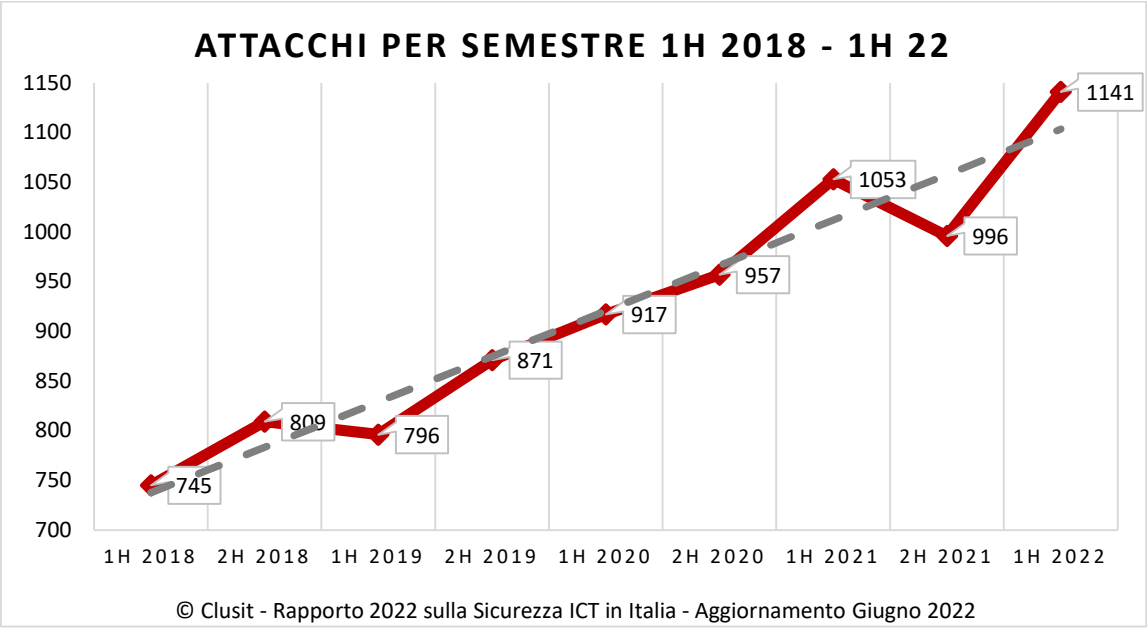
Per dare un'idea in prospettiva, i ricercatori di Clusit hanno identificato, classificato e valutato dal 2011 - data della prima pubblicazione del Rapporto Clusit - ad oggi oltre 15.000 attacchi informatici gravi. Di questi, più della metà (8.285) si sono verificati negli ultimi 4 anni e mezzo, a causa di una accelerazione smisurata delle minacce cibernetiche.

Se confrontati con il primo semestre 2018, gli attacchi da gennaio a giugno 2022 hanno fatto registrare una crescita del 53%. In 4 anni e mezzo la media mensile di attacchi gravi a livello globale è passata da 124 a 190.

[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.

Clusit Associazione Italiana per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency



Negli ultimi quattro anni è avvenuto un vero e proprio cambiamento epocale nei livelli globali di cyber-insicurezza, secondo gli esperti di Clusit, al quale tuttavia non è corrisposto un incremento sufficiente delle contromisure difensive.

"L'Italia deve cogliere l'opportunità della transizione digitale per colmare le proprie lacune in materia di sicurezza informatica", ha affermato **Gabriele Faggioli, presidente di Clusit**. "*Lo scenario geopolitico ci pone con brutalità davanti all'obbligo di avere infrastrutture resistenti ad attacchi esterni che potrebbero minare la capacità di erogare servizi essenziali ai cittadini. Credo che mai come ora sia fondamentale una scelta politica forte, e possibilmente univoca a livello europeo; mai come ora è importante usare al meglio le risorse del PNRR, nel contesto di uno sforzo politico e imprenditoriale collettivo che servirà per superare l'attuale crisi e per affrontare le prossime sfide*", ha concluso Faggioli.

"*Il conflitto tra Russia e Ucraina ha messo in campo strumenti cyber-offensivi altamente sofisticati a supporto di attività di cyber-intelligence e di cyber-warfare: temiamo che questo processo sia difficilmente reversibile e che in prospettiva potrebbe causare conseguenze di inaudita gravità*", ha commentato **Sofia Scozzari, co-autrice del Rapporto e membro del Comitato Scientifico di Clusit** .

"Siamo sulla soglia di una guerra cibernetica globale. D'ora in poi le infrastrutture critiche e molti altri sistemi digitali, meno tutelati a livello normativo ma comunque essenziali per la collettività, saranno bersagli designati, costantemente al centro del mirino di numerosi attori, governativi e non", ha proseguito **Andrea Zapparoli Manzoni, coautore del Rapporto Clusit** e membro del Comitato Direttivo dell'Associazione.

Cresce anche la severità degli attacchi
I ricercatori di Clusit hanno valutato e classificato anche i livelli di impatto dei singoli incidenti, sulla base di aspetti economici, sociali e relativi all'immagine e alle ripercussioni dal punto di vista geopolitico e hanno evidenziato che il trend di crescita degli attacchi riguarda anche la "qualità" degli stessi messa a punto dai cyber criminali, che agisce da moltiplicatore dei danni.

Confermando una tendenza già evidente nel 2021, **gli attacchi gravi con effetti molto importanti** sono stati nel primo semestre 2022 **il 45% del totale**, mentre **quelli con impatto "critico"** arrivano nei primi sei mesi di quest'anno a rappresentare **un terzo di tutti gli attacchi**. Nel complesso, gli attacchi con impatto Critical e High sono stati il **78%** del totale.

Gli attacchi cyber nel primo semestre 2022: chi viene colpito e perché

Le vittime per categoria
I ricercatori di Clusit hanno classificato le vittime di attacchi nel primo semestre del 2022 secondo una tassonomia derivata da standard internazionali[2]: tenendo come base di raffronto il primo semestre 2021, nel primo semestre 2022 la crescita maggiore nel numero di attacchi gravi si osserva verso le categorie "**Multiple targets**" (**+108,3%**): significa, secondo gli autori del Rapporto Clusit, che i cyber criminali tendono ora a colpire in maniera indifferenziata obiettivi molteplici, piuttosto che bersagli specifici.
Questa crescita a tre cifre porta nel primo semestre 2022 la categoria "Multiple Targets" in testa alla classifica delle vittime anche in termini percentuali, rappresentando il **22%** del totale.

In termini di crescita percentuale seguono le categorie "Telecommunication" (**+77,8%**), "Financial / Insurance" (**+76,7%**), "News / Multimedia" (**+50%**), "Manufacturing" (**+34%**), "Other Services" (**+30,8%**) ed "ICT" (**+11,5%**), "Energy / Utilities" (**+5,3%**) ed "Healthcare" (**+2,2%**).

Per quanto riguarda la distribuzione delle vittime, le categorie più colpite dopo i "Multiple targets" sono "**Healthcare**" e "**Gov / Mil / Law Enforcement**", ciascuna con circa il **12%** degli attacchi totali. Al quarto posto segue **Information Technology** - "ICT" (**11%)** e "**Financial / Insurance**" (**9%)**.

Le successive sei categorie merceologiche (che sommate rappresentano il 23% degli attacchi rilevati) sono comprese tra il 6% ed il 2% degli attacchi: secondo i ricercatori di Clusit, questo conferma che gli attaccanti si muovono sempre più a tutto campo, e che tutti sono potenziali bersagli.

[2] I ricercatori di Clusit hanno classificato le vittime di attacchi nel primo semestre del 2022 secondo una tassonomia derivata dagli standard internazionali **ISIC** (International Standard Industrial Classification of All Economic Activities) delle Nazioni Unite e **NACE** della Commissione Europea (Nomenclature statistique des activités économiques dans la Communauté Européenne)

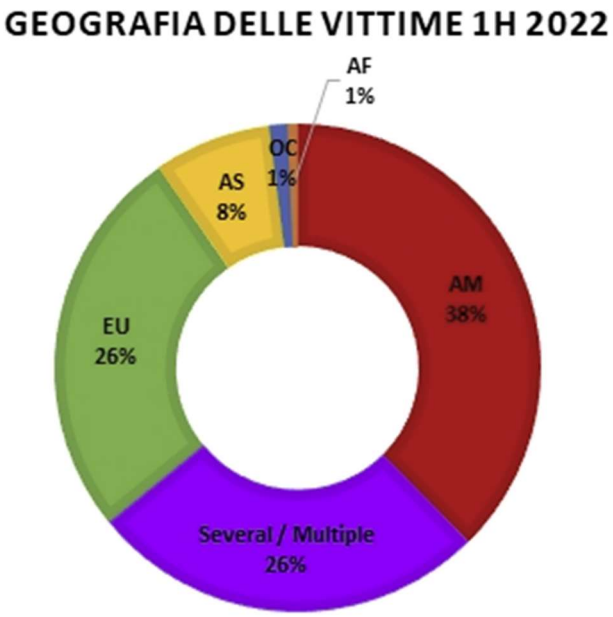
Il conflitto russo-ucraino determina le finalità di attacco
Il primo semestre 2022 ha visto un'impennata del **414%** le attività riferibili agli attacchi della categoria "**Hacktivism**"; quelli relativi all'"**Information Warfare**" sono cresciuti del **119%**. Questi incrementi a tre cifre vanno ricondotti, secondo i ricercatori di Clusit, in primo luogo alla guerra in Ucraina.

Per la stessa motivazione, rispetto al primo semestre del 2021, sono aumentate del **62%** rispetto allo stesso periodo del 2021 degli attacchi con finalità di "**Espionage**".

Dopo il picco straordinario del 2021, nel primo semestre 2022 sono invece diminuiti del 3,4% gli attacchi classificati come attività di "**Cybercrime**", che rimane tuttavia la principale motivazione di attacco a livello globale, rappresentando il **78,4%** degli attacchi globali.

La distribuzione geografica delle vittime
Sono aumentati nel 2022 gli attacchi verso realtà basate in **Europa**, che raggiungono il valore più alto di sempre, con il **26%** degli attacchi complessivi (in crescita dal 21% del 2021). Contestualmente, diminuiscono per la prima volta dal 2011 le vittime di area americana (dal 45% al 38%) e scendono leggermente anche quelli rilevati contro organizzazioni asiatiche (dal 12% all'8%).

Percentualmente aumentano gli attacchi gravi verso bersagli con sedi distribuite in diversi Paesi (categoria "Several / Multiple"), che dal 19% del 2021 salgono al 27%.



Le tecniche d'attacco
Sono otto le macrocategorie analizzate dai ricercatori di Clusit, sulla base di classificazioni internazionali[3]: nel primo semestre di quest'anno hanno prevalso in maniera assoluta gli attacchi perpetrati attraverso "**Malware**" che, pur registrando una leggera flessione dal primo semestre 2021(-4,6%), rappresenta il **38%** del totale. Le **tecniche sconosciute** (categoria "Unknown") sono al secondo posto, con un aumento del **10%** rispetto al primo semestre 2021, superando la categoria "Vulnerabilità" (-26,8%) e "**Phishing / Social Engineering**", che però crescono del **63,8%**.

In conseguenza della natura sempre più complessa degli attacchi, la categoria "**Tecniche Multiple**" sale del **+93,8**%.

In concomitanza con l'aumento di attività riferibili ad Hacktivism ed Information Warfare, rispetto al totale gli attacchi gravi con finalità di "**Distributed Denial of Service**", pur pochi in valori assoluti, crescono di un significativo **308,8%**, così come quelli realizzati tramite "**Identity Theft / Account Hacking**" (**+12,9%**).

Il **22%** di "tecniche sconosciute" è principalmente dovuto al fatto che molti attacchi analizzati (oltre un quinto del totale) diventano di dominio pubblico a seguito di un "data breach", nel qual caso le normative impongono una notifica agli interessati, ma non di fornire una descrizione precisa delle modalità dell'attacco.

Altri contributi del Rapporto Clusit – edizione ottobre 2022

Nell'edizione presentata questa mattina, il Rapporto Clusit ha inaugurato una nuova sezione dedicata agli attori istituzionali con cui l'Associazione collabora attivamente per diffondere la cultura della sicurezza informatica presso Aziende, Pubblica Amministrazione e cittadini. Protagonista del primo appuntamento è **CYBER 4.0**, il Centro di Competenza nazionale ad alta specializzazione per la cybersecurity, attraverso la voce del suo presidente, il Prof. Leonardo Querzoni.

Di rilievo anche il capitolo che presenta l'evoluzione degli attacchi cyber in Italia grazie alle rilevazioni e segnalazioni della **Polizia Postale e delle Comunicazioni,** sulla base delle operazioni svolte nel corso dei primi sei mesi del 2022.

Lo scenario di tensione politica globale è ben delineato all'interno del Rapporto Clusit anche dal contributo "*Geopolitica e Cybersecurity*", a cura di **Carlo Mauceli**, **Microsoft**, che entra nel merito della "guerra informatica a supporto della guerra convenzionale e delle strategie politiche dei singoli Stati", fornendo poi un approfondimento su Russia e Cina.

Experis, società che di ricerca e selezione del personale, fotografa invece nel suo contributo per il Rapporto Clusit le tendenze nel settore della Cybersecurity con l'analisi "**Profili Cyber ultra-specializzati e nuovi trend del mercato del lavoro** (Ultra-specializzazioni, RAL crescenti e strategie di attraction e retention delle aziende)".

[3] Alle 8 macro-categorie si affiancano 54 sotto-categorie derivate dall'analisi dalla Threat Taxonomy dell'ENISA, dalla Open Threat Taxonomy e di diversi altri framework, non esistendo una tassonomia standard per le tecniche di attacco.

Come sempre è inoltre inclusa nel Rapporto Clusit la sezione “FOCUS ON” che prevede in questa edizione approfondimenti specifici su **Operation Technology Security** ed **Effetti della guerra sulla sicurezza delle Infrastrutture Critiche.**

Il Rapporto Clusit 2022 è disponibile gratuitamente sul sito Clusit.

# # #

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