Presentata la nuova edizione del Rapporto Clusit 2021 sulla sicurezza cyber

Clusit: escalation di attacchi cyber nel primo semestre dell'anno

+24% di attacchi gravi rispetto allo stesso periodo del 2020, il 74% ha effetti molto critici o devastanti. Danni economici oltre il 6% del PIL mondiale.

Milano, 9 novembre 2021 – I primi sei mesi del 2021 mostrano un aggravamento della situazione sul fronte della sicurezza cyber: lo evidenziano i dati della nuova edizione del Rapporto Clusit 2021 presentata questa mattina nel corso di Security Summit Streaming Edition, l'evento di riferimento per la cybersecurity in Italia organizzato da Clusit, Associazione Italiana per la Sicurezza Informatica, con Astrea, agenzia specializzata nell'organizzazione di eventi nell'ambito della sicurezza informatica.

Per il primo semestre 2021 sono stati analizzati **1.053 gli attacchi cyber gravi**, ovvero con un impatto sistemico in diversi aspetti della società, della politica, dell'economia e della geopolitica. Si tratta del **24% in più** rispetto allo stesso periodo del 2020, per una **media mensile di attacchi gravi pari a 170**, contro i 156 del 2020. Questa escalation, secondo i ricercatori di Clusit è tra l'altro probabilmente sottostimata, poiché il campione analizzato comprende esclusivamente attacchi di pubblico dominio e, tra questi, alcune classi di incidenti sono sistematicamente sottorappresentate.

Nel primo semestre 2021 sono in aumento del 21% gli attacchi gravi compiuti per finalità di "**Cybercrime**", ovvero per estorcere denaro alle vittime, che oggi rappresentano **l'88% del totale**. Sono inoltre cresciuti del **18%** gli attacchi riferibili a "**Information Warfare**", la cosiddetta "guerra delle informazioni"; in diminuzione, invece, quelli classificati come attività di "**Cyber Espionage**" (-36,7%), dopo il picco straordinario del 2020 dovuto principalmente allo spionaggio relativo allo sviluppo di vaccini e cure per il Covid-19, come evidenziato nel Rapporto Clusit dello scorso anno.

Gli esperti di Clusit la definiscono ormai "un'emergenza globale". **Le perdite stimate per le falle della cybersecurity sono pari a 6 trilioni di dollari per il 2021[1] ed incidono ormai per una percentuale significativa del GDP mondiale, con un tasso di peggioramento annuale a 2 cifre ed un valore pari a 3 volte il PIL italiano**.

"*Da anni siamo di fronte a problematiche che per natura, gravità e dimensione travalicano costantemente i confini dell'ICT e della stessa Cyber Security ed hanno impatti profondi, duraturi e sistemici su ogni aspetto della società, della politica, dell'economia e della geopolitica*", afferma Andrea Zapparoli Manzoni, co-autore del Rapporto Clusit e membro del Comitato Direttivo Clusit.

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

In riferimento al nostro Paese, Zapparoli Manzoni afferma inoltre: "*Auspichiamo che il PNRR, che complessivamente alloca circa 45 miliardi di euro per la transizione digitale, possa rappresentare per l'Italia l'occasione di mettersi al passo e colmare le proprie lacune anche in ambito cyber, per portare a una significativa riduzione della superficie di attacco esposta dal Paese*".

Cyber attacchi nel primo semestre 2021: chi è stato colpito e perché

Utilizzando una tassonomia delle vittime basata su standard interazionali[2], i ricercatori Clusit hanno ricondotto gli attacchi gravi individuati a venti settori merceologici.

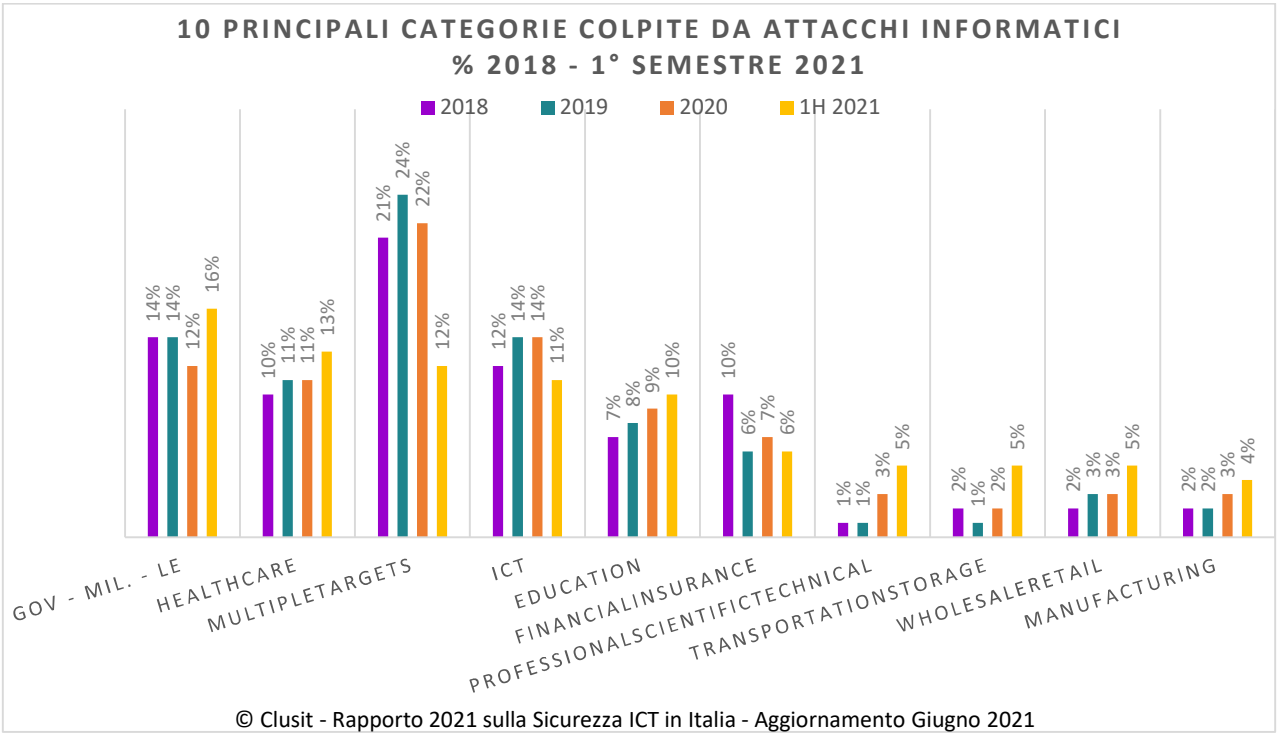
In termini assoluti, rispetto al secondo semestre 2020, da gennaio a giugno 2021 si osserva l'incremento più elevato degli attacchi gravi nelle categorie:

- **Transportation / Storage: +108,7%**
- **Professional, Scientific, Technical: +85,2%**
- **News & Multimedia: +65,2%**
- **Wholesale / Retail: +61,3%**
- **Manufacturing: +46,9%**
- **Energy / Utilities: +46,2%**
- **Government: (+39,2%)**
- **Arts / Entertainment: +36,8%**
- **Healthcare: +18,8%**

La categoria "**Multiple Targets**" (si tratta di attacchi gravi compiuti in parallelo dallo stesso gruppo di attaccanti contro numerose organizzazioni appartenenti a categorie differenti) registra invece una **diminuzione del 23,4%** rispetto al secondo semestre 2020. Siamo di fronte a un **cambio di strategia** da parte degli attaccanti rispetto allo scorso anno: secondo gli esperti Clusit l'aumento di attacchi gravi mirati verso singoli bersagli rappresenta un importante campanello di allarme, in particolare perché caratterizzati da tecniche di tipo ransomware con l'aggravante della "double extortion", cioè della minaccia di diffondere i dati rubati alle vittime qualora non paghino il riscatto.

In termini percentuali la categoria "**Government**" rappresenta il 16% del totale e si **conferma al primo posto tra le vittime**, come nel precedente semestre. Al secondo posto, ancora la **Sanità**, con il **13%** degli attacchi totali, ed al terzo "**Multiple Targets**", che in questo semestre rappresenta il **12%** delle vittime. Le altre categorie merceologiche in crescita - che sommate compongono il 50% degli attacchi rilevati - sono comprese tra l'11 ed il 4% degli attacchi, dimostrando ancora una volta che gli attaccanti si muovono a tutto campo, e che tutti sono potenziali bersagli.

[2] **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 grafico delle principali categorie colpite tra il 2018 ed il 1H 2021 mostra la variazione di incidenza tra la categoria Multiple Targets e le altre, che sono quasi tutte in crescita.

Distribuzione geografica degli attacchi:
Nel primo semestre del 2021 aumentano sensibilmente gli attacchi verso realtà basate in **Europa**: **un quarto degli attacchi sono infatti diretti verso quest'area**, in crescita di 10 punti percentuali rispetto allo stesso periodo dello scorso anno. Rimangono sostanzialmente invariate le percentuali di vittime di area americana e quelle appartenenti ad organizzazioni asiatiche. Diminuiscono invece percentualmente gli attacchi gravi verso bersagli con sedi distribuite in diversi Paesi, che rappresentano il 16% nel primo semestre 2021, rispetto al 25% dello stesso periodo del 2020.

Le tecniche d'attacco
Anche in questo caso, i ricercatori Clusit si basano su una tassonomia derivata da framework internazionali[3], articolata su otto macrocategorie.

"**Malware**" è la categoria che nei primi sei mesi di quest'anno mostra numeri assoluti maggiori: rappresenta infatti il **43%** del totale, in crescita del **10,5%**. Le **tecniche sconosciute** (categoria "Unknown") sono al secondo posto, in aumento del **13,9%** rispetto al secondo semestre 2020, superando la categoria "**Vulnerabilità note**", che è per altro in preoccupante crescita (**+41,4%**) e "**Phishing / Social Engineering**", in leggero calo (**-13%**). Aumentano dell'**11,6**% gli attacchi gravi condotti con "**Tecniche Multiple**". Infine, gli attacchi gravi con finalità di "**Denial of Service**"

[3] Non esistendo una tassonomia standard per le tecniche di attacco, le 55 sotto-categorie delle 8 macro categorie identificate dagli esperti Clusit sono state derivate dall'analisi dalla Threat Taxonomy dell'ENISA, dalla Open Threat Taxonomy e di diversi altri framework.

diminuiscono (**-42,9%)**, così come quelli realizzati tramite "**Identity Theft / Account Hacking**" (**-29,5%**).

In sostanza - commentano gli esperti Clusit - gli attaccanti possono ancora fare affidamento sull'efficacia del Malware, prodotto industrialmente a costi decrescenti, e sullo sfruttamento di vulnerabilità note, per colpire più della metà dei loro obiettivi, ovvero il **59%** dei casi analizzati.

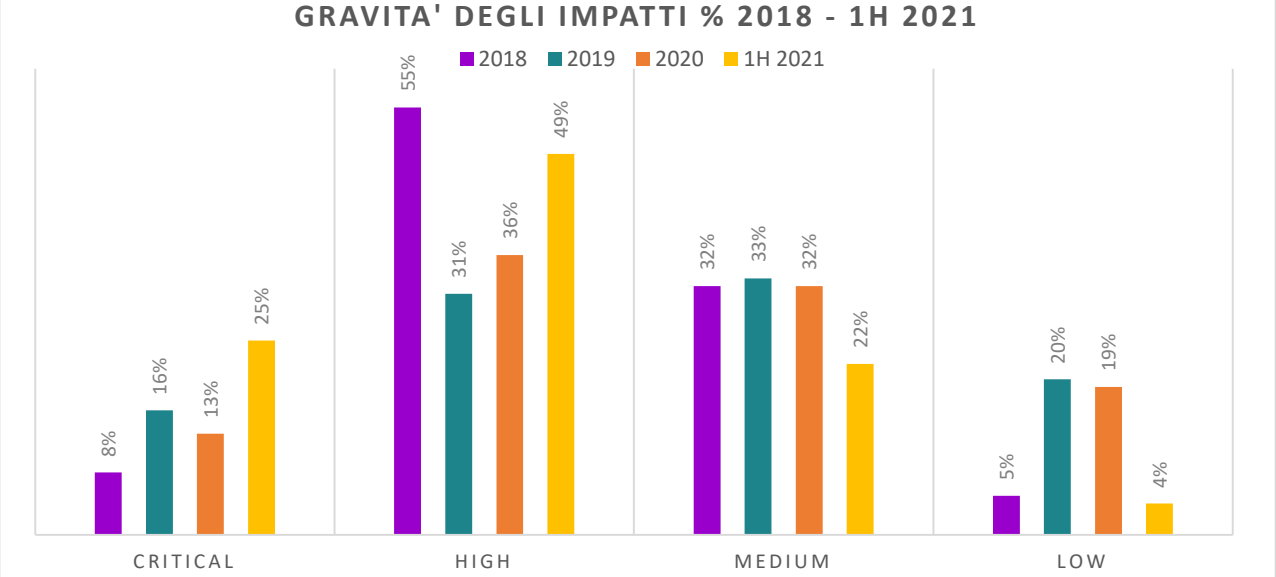
Il **22%** di attacchi realizzati con "tecniche sconosciute" (che crescono del **13,9%**) è dovuto al fatto che un quinto degli attacchi diventano di dominio pubblico a seguito di un "data breach": in questo caso, le normative impongono una notifica agli interessati, ma non di fornire una descrizione precisa delle modalità dell'attacco.

La gravità degli attacchi

Il Rapporto Clusit 2021 valuta poi la "severity" degli attacchi analizzati, secondo quattro categorie, con l'obiettivo di individuare come evolvono gli **impatti** degli attacchi, partendo dalla constatazione che spesso questa valutazione non coincide con l'aumento del numero di attacchi da parte di una specifica categoria di attaccanti o verso una certa categoria di vittime. Le variabili che contribuiscono a comporre questa valutazione per ogni singolo attacco analizzato sono molteplici ed includono l'impatto geopolitico, sociale, economico - diretto e indiretto - e di immagine.

Nel primo semestre 2021 gli attacchi gravi con effetti "molto importanti" e "critici" sono il **74% del totale.** Nel 2020 questa percentuale era il **49%**.

Il 22% degli attacchi analizzati sono di impatto significativo, quelli con impatto basso solo il **4%**.



© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2021

Il grafico mostra la valutazione degli impatti degli esperti Clusit rispetto agli attacchi degli ultimi 3 anni e mezzo.

La seconda edizione del Rapporto Clusit 2021 presentata oggi nel corso di Security Summit Streaming Edition include inoltre **L'analisi degli attacchi in Italia nel periodo gennaio-giugno 2021** svolta da **Fastweb** sulla base dei dati rilevati dal Fastweb Security Operations Center (SOC), che ha registrato nel semestre 36 milioni di eventi malevoli, in aumento del 180% rispetto allo stesso periodo dell'anno precedente.

All'interno del Rapporto Clusit anche un contributo che illustra le attività di prevenzione e di contrasto alla criminalità informatica in generale svolte dalla **Polizia Postale e delle Comunicazioni** nel primo semestre dell'anno, un contributo della **Polizia Criminale** e del **CERT di Banca d'Italia.**

Sono inoltre presenti approfondimenti sul cybercrime nel **settore finanziario** a livello globale e italiano. Vengono poi presentate due indagini inedite in merito a

- **La percezione delle aziende e organizzazioni italiane in merito alle minacce informatiche, all'impatto degli attacchi ed alla capacità di difesa**
- **L'efficienza delle strutture sanitarie italiane per affrontare i rischi di sicurezza informatica**

oltre a un approfondimento sul **mercato del lavoro nel settore della cybersecurity**: professionisti più richiesti, competenze e certificazioni, gender diversity.

Come in ogni edizione, è particolarmente ricca la sezione "**Focus On**", con contributi relativi a:

- La sicurezza dell'e-mail tra nuove tecnologie e best practice
- SD-WAN: vantaggi e rischi
- Sistemi di controllo industriali, analisi della cybersecurity e del cybercrime
- Sicurezza per la rete di accesso: dall'OnPrem al Cloud
- Continuità aziendale, ripristino di emergenza, resilienza informatica: il cloud ibrido come leva strategica
- Digital transformation: un'opportunità per affrontare correttamente la sicurezza fin dalle basi

# # #

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