Presentata la quindicesima edizione del Rapporto Clusit 2020 sulla sicurezza ICT

Clusit: rischi cyber, situazione di inaudita gravità

Trend persistente nel 2019: +91,2% degli attacchi rispetto al 2014.
Aumentano anche gravità e danni conseguenti. Ma è solo la punta dell'iceberg.

Un quarto degli attacchi compiuti a livello mondiale colpisce in parallelo "bersagli multipli";
in un anno cresciuti del 91,5% gli attacchi a servizi online; del 17% quelli alla sanità.

Sempre più utilizzate le tecniche di Phishing e Social Engineering (+81,9% rispetto al 2018).

Milano, 5 marzo 2020 – Con **1.670** attacchi gravi e una tendenza in crescita del **7%** rispetto al 2018, il 2019 segna un nuovo picco verso l'alto nella rappresentazione della "insicurezza cyber" che viene tracciata ogni anno dagli esperti di Clusit, Associazione Italiana per la Sicurezza Informatica.

Si apre così il **Rapporto Clusit 2020 sulla sicurezza ICT in Italia e nel mondo**[1], che analizza su base semestrale i più gravi cyber attacchi noti avvenuti nel mondo, oggi presentato in anteprima in streaming alla stampa. Gli autori hanno illustrato i principali eventi di sicurezza degli ultimi dodici mesi, i settori più colpiti dalla criminalità sul web, le principali tipologie di attacco, le vulnerabilità più comuni, rapportandoli agli attacchi noti degli ultimi cinque anni e, in particolare a quelli dei dodici mesi precedenti.

Tra gennaio e dicembre 2019 sono stati in media **139 gli attacchi registrati mensilmente a livello mondiale** con impatto sistemico in ogni aspetto della società, della politica, dell'economia e della geopolitica. Si tratta del 47,8% in più rispetto alla media dei 94 attacchi mensili registrati nel quinquennio 2014-2018.

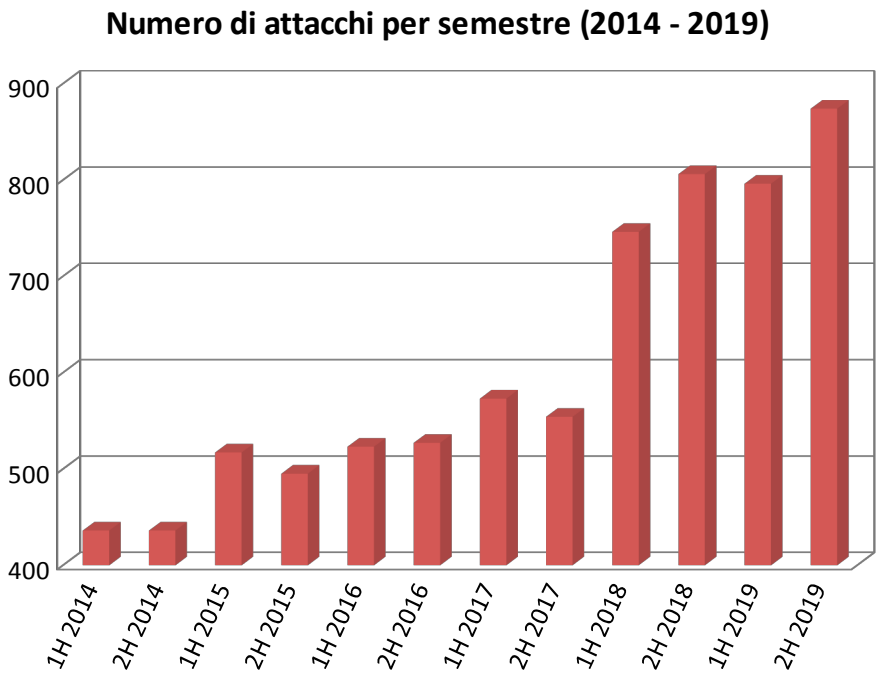
Gli esperti Clusit avvertono, tuttavia, che si tratta solo della punta dell'iceberg: le analisi si riferiscono infatti ad attacchi reali, ovvero effettivamente andati a segno provocando danni importanti. Rimangono quindi esclusi gli attacchi tentati o bloccati. Inoltre, per quanto ormai statisticamente significativo, il campione analizzato nel Rapporto Clusit è necessariamente parziale, data la tendenza generale ad evitare di rendere pubbliche le aggressioni cyber. La stessa entrata in vigore del Regolamento GDPR e della Direttiva NIS nel 2018, non hanno ad oggi portato

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 effettivamente avvenuti nel periodo in esame.

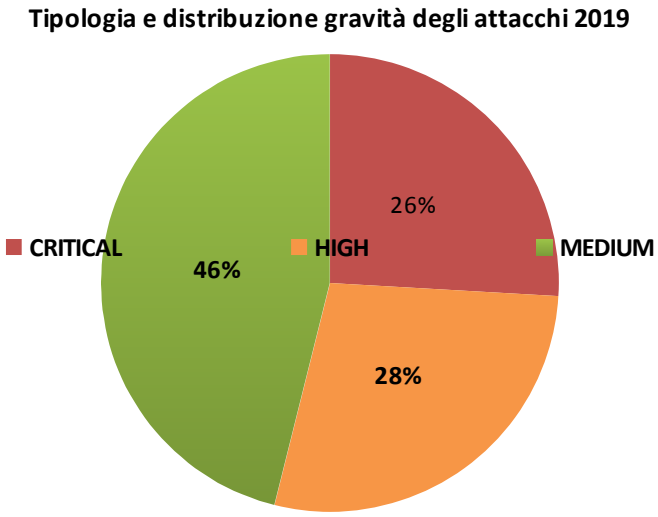
alla rilevazione di un aumento significativo di attacchi gravi di pubblico dominio verso bersagli europei: questo comporta certamente l'evidenza di uno scenario meno critico rispetto alla situazione sul campo.

A seguito delle loro analisi, gli esperti Clusit evidenziano dinamiche che, in particolare nell'ultimo triennio, hanno spinto sempre più soggetti - statuali e non - ed entrare nell'arena della cyber guerra, e questo ha impattato in modo inequivocabile sulla società civile, ovvero sui singoli cittadini, le istituzioni e le imprese. Si tratta di fenomeni che per natura e dimensione travalicano i confini dell'IT e della stessa cyber security. "*Ci troviamo di fronte a un vero e proprio cambiamento epocale nei livelli globali di cyber-insicurezza, causato dall'evoluzione rapidissima degli attori, delle modalità, della pervasività e dell'efficacia degli attacchi*", afferma Andrea Zapparoli Manzoni, del Comitato Direttivo Clusit.

"*Gli attaccanti sono oggi decine e decine di gruppi criminali organizzati transnazionali che fatturano miliardi, multinazionali fuori controllo dotate di mezzi illimitati, stati nazionali con i relativi apparati militari e di intelligence, i loro fornitori e contractors, gruppi state-sponsored civili e/o paramilitari ed unità di mercenari impegnati in una lotta senza esclusione di colpi, che hanno come campo di battaglia, arma e bersaglio le infrastrutture, le reti, i server, i client, i device mobili, gli oggetti IoT, le piattaforme social e di instant messaging (e la mente dei loro utenti), su scala globale, 365 giorni all'anno, 24 ore al giorno",* prosegue Zapparoli Manzoni. "*Viviamo ed operiamo in una situazione di inaudita gravità in termini di rischi cyber, che mette a repentaglio tutti i presupposti sui quali si basa il buon funzionamento dell'Internet commerciale e di tutti i servizi - online e offline - che su di essa fanno affidamento*".



Gli attacchi registrati dagli esperti Clusit sono stati inoltre classificati con differenti **livelli di impatto**, sulla base di variabili di tipo geopolitico, sociale, economico (diretto e indiretto) e di immagine. Nel 2019 gli attacchi andati a buon fine hanno avuto nel 54% dei casi un impatto "alto" e "critico"; il 46% è stato di gravità "media".



Il **Cybercrime**, è ancora nel 2019 **la principale causa di attacchi gravi**: l'**83%** di essi è infatti stato perpetrato con l'obiettivo di estorcere denaro alle vittime. In particolare, lo scorso anno gli esperti Clusit hanno registrato il numero di attacchi di Cybercrime più elevato degli ultimi 9 anni, con una crescita del 162% rispetto al 2014 e del 12,3% rispetto al 2018.

Rimangono sostanzialmente stabili anno su anno gli attacchi gravi riferibili ad attività di **Cyber Espionage** – lo spionaggio cibernetico (+0,5% rispetto al 2018, tuttavia gli esperti evidenziano la scarsità di informazioni pubbliche in merito), che rappresentano la causa del 12% degli attacchi gravi nel 2019; diminuiscono quelli appartenenti alla categoria **Cyber Warfare** – la guerra delle informazioni (-37,5% rispetto al 2018), che costituisce il 2% del totale degli attacchi. Insieme, Cyber Espionage e Cyber Warfare sono però classificabili con una gravità più alta della media, fanno notare gli esperti Clusit.

Cyber attacchi nel 2019: chi è stato colpito e perché

Di seguito i settori maggiormente colpiti da attacchi cyber gravi nel 2019, con rispettive percentuali di crescita rispetto all'anno precedente:

- "**Multiple Targets**": 24% del totale degli attacchi. Si tratta di bersagli multipli che si rivelano obiettivi indifferenziati per un'unica organizzazione criminale che utilizza una logica industriale di attacco. Gli attacchi verso questi obiettivi sono in crescita del 29,9% rispetto al 2018;

- **Settore Pubblico** (15% degli attacchi, in discesa del 19,4%);

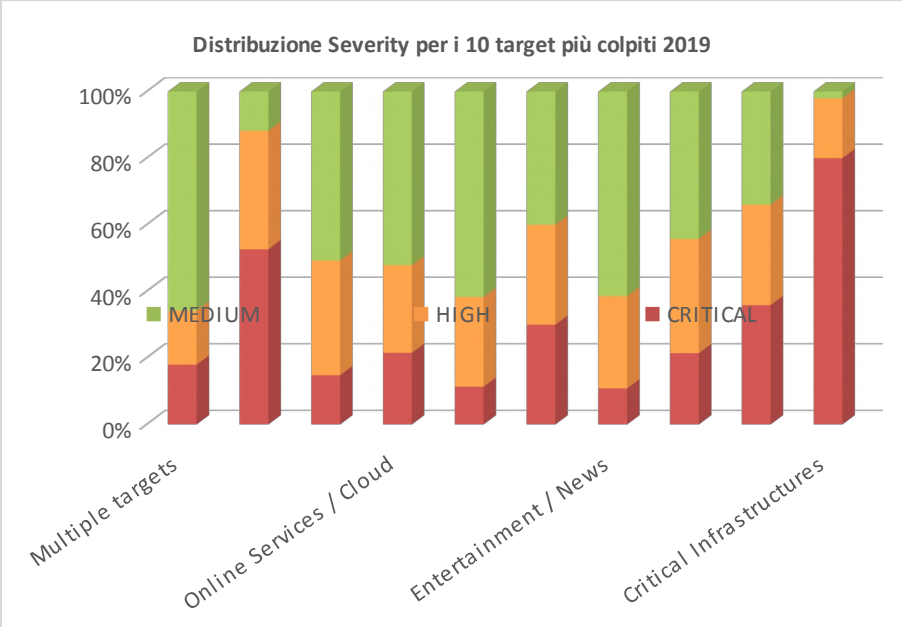
- **Sanità** (12% del totale degli attacchi, +17% rispetto al 2018);

- **Servizi Online** (11% degli attacchi, +91,5%).

Seguono i settori **Ricerca e formazione scolastica** (8% in calo dell'8,3%), **bancario e assicurativo** (6% in calo del 10,2%) e **Intrattenimento/Informazione** (5% in calo del 31,4%), **Commercio e Grande Distribuzione Organizzata** (2% degli attacchi, in crescita del 28,2%), e l'insieme di "**Altri Settori**" (3% del totale attacchi, +76,7%), **Telecomunicazioni** (1% del totale, +54,5%) e **Fornitori di Sicurezza Informatica** (1%; in evidenza qui la crescita a tre cifre: +325%).

La categoria "Multiple Targets" comprende attacchi verso vittime appartenenti a tutte le altre colpite dallo stesso attacco in parallelo, a dimostrazione del fatto che gli attaccanti sono sempre più aggressivi e conducono operazioni su scala sempre maggiore, con una logica "industriale", che prescinde sia da vincoli territoriali che dalla tipologia dei bersagli, puntando solo a massimizzare il risultato economico.

A livello qualitativo, i dati del Rapporto Clusit 2020 evidenziano che le categorie "Infrastrutture Critiche" e "Settore Pubblico", con il settore bancario e finanziario e il settore "altri", hanno subìto nel 2019 il maggior numero di attacchi di impatto "critico", mentre le categorie con il maggior numero di attacchi con impatti di livello "Alto" sono la sanità, i fornitori di Software e Hardware e ancora il Settore Pubblico.



Le tecniche d'attacco

I cybercriminali nel 2019 hanno sferrato attacchi utilizzando **Malware** nel 44% dei casi. Questa tecnica è in crescita del **24,8%** rispetto allo scorso anno; nello specifico, i **Ransomware** - una tipologia di malware che limita l'accesso del dispositivo infettato, richiedendo un riscatto - rappresentano quasi la metà del totale di questa tecnica (46%; in crescita del 21% rispetto al 2018).

Gli esperti Clusit confermano la tendenza dei cybercriminali ad utilizzare tecniche di attacco "semplici", prodotte industrialmente in infinite varianti, a costi decrescenti; allo stesso tempo, tuttavia, appare sempre più elevata la tendenza all'utilizzo di queste tecniche anche da parte di attori statuali e state-sponsored.

Al secondo posto tra le tecniche d'attacco – a rappresentare il **19%** del totale - vi sono varie **tecniche sconosciute**, ma con evidente tendenza alla decrescita (-22,3%) rispetto al 2018.

Le tecniche di **Phishing** e **Social Engineering** segnano invece +**81,9%** rispetto al 2018, arrivando a rappresentare il **17%** del totale. Una quota crescente di questi attacchi basati su Phishing si riferisce, evidenziano gli esperti Clusit, a "*BEC scams*", ovvero frodi via email che colpiscono in maniera specifica le organizzazioni con l'obiettivo di infliggere danni economici, con impatto spesso notevole.

Tutte le altre tipologie di tecniche di attacco sommate rappresentano nel 2019 solo il **12,3%** del totale. Notevole l'incremento percentuale delle categorie "**0day**" (**+50%**) e "**Account Cracking**" (**+53,6%**), mentre appaiono in diminuzione gli attacchi realizzati sfruttando **vulnerabilità note** (**-28,8%**), **DDos** (**-39,5%**) e **tecniche multiple/APT** (**-33,7%**).

Alcuni contributi nel Rapporto Clusit 2020

Analisi della situazione italiana in materia di cyber-crime e incidenti informatici – a cura di Fastweb

Come ogni anno, Fastweb presenta nel Rapporto Clusit i dati relativi agli **attacchi rilevati dal proprio Security Operations Center (SOC)**, che ha analizzato la situazione italiana sulla base di oltre 43 milioni di eventi di sicurezza. I dati - automaticamente aggregati e anonimizzati per proteggere la privacy e la sicurezza dei Clienti e di Fastweb stessa – mostrano che benché il cyber crime sia in costante ascesa, settori come la PA hanno adottato efficaci strumenti di mitigazione.

Lo stato della sicurezza informatica nel Sud Italia – a cura di Università degli Studi di Bari-Exprivia|Italtel

Il Rapporto Clusit 2020 riporta anche un interessante studio quali-quantitativo sullo "Stato della sicurezza informatica nel Sud Italia" condotto dai ricercatori dell'Università degli Studi di Bari con Exprivia|Italtel intervistando un campione eterogeneo di aziende, operanti in diversi settori nel sud Italia. Il 34,5% di queste imprese dichiara di aver subito attacchi informatici nel corso del 2019. A fronte degli attacchi subiti, soltanto il 10,9% dei soggetti si ritiene incapace di difendersi. Il 69% degli intervistati si dice poco o per niente consapevole circa i rischi conseguenti ad un attacco informatico.

Il mercato italiano della Sicurezza IT: analisi, prospettive e tendenze – a cura di IDC Italia

Nel suo contributo, IDC evidenzia che sono soprattutto le grandi organizzazioni a concepire la sicurezza IT sempre più come infrastruttura ormai essenziale e a reputare irrimandabili gli investimenti in cybersecurity. Questo accade soprattutto nel settore manifatturiero, che ha

iniziato a comprenderne il potenziale valore strategico per affrontare le nuove sfide dell'Industria 4.0 e dell'Intelligenza Artificiale.

Entro il 2025 il 25% della spesa in servizi di sicurezza delle imprese italiane sarà destinata allo sviluppo, all'implementazione e al mantenimento di un "trust framework", secondo IDC. Il tema dello "skill shortage" nella sicurezza informatica continuerà tuttavia a rimanere critico: "*Sarà sempre più importante disporre di analisti con competenze anche nelle aree del machine learning, in considerazione del peso sempre maggiore che l'Intelligenza Artificiale giocherà nel monitoraggio, nella detection e nella gestione di eventuali incidenti. La varietà e i volumi degli alert cresceranno in maniera esponenziale e soltanto questi strumenti potranno aiutare le aziende a gestire situazioni anomale, ricorrendo a molteplici fonti per disegnare regole e profili di rischio basati su comportamenti complessi*".

Il Rapporto Clusit 2020 sarà presentato al pubblico il prossimo 17 marzo nel corso di una sessione in streaming che anticiperà il Convegno Security Summit, previsto a Milano e rinviato a seguito dell'ordinanza di Regione Lombardia del 23 febbraio scorso per il contenimento del Coronavirus.

Security Summit prevede nel 2020 appuntamenti a Milano, Treviso Verona e Roma.
È organizzato da:

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

Astrea, Agenzia di Comunicazione e Marketing, specializzata nell'organizzazione di eventi business nel mondo della tecnologia, e in particolare della Sicurezza Informatica. Con sede operativa a Milano, Astrea mette le competenze dei propri professionisti a disposizione delle organizzazioni per sviluppare soluzioni creative ed innovative volte a incrementare visibilità e ad acquisire autorevolezza sui mercati di riferimento. www.astrea.pro

Per ulteriori informazioni si prega di contattare:
Daniela Sarti
Ufficio Stampa Security Summit | Clusit
press@securitysummit.it - dsarti@clusit.it
Tel. 335 459432