RAPPORTO CLUSIT 2019

Il Rapporto CLUSIT 2019, giunto ormai al suo ottavo anno di pubblicazione, inizia con una panoramica degli eventi di cyber-crime più significativi degli ultimi 12 mesi. Si può affermare che il 2018 è stato l'anno peggiore di sempre in termini di evoluzione delle minacce "cyber" e dei relativi impatti, non solo dal punto di vista quantitativo ma anche e soprattutto da quello qualitativo, evidenziando un trend di crescita degli attacchi, della loro gravità e dei danni conseguenti mai registrato in precedenza.
Nell'ultimo biennio il tasso di crescita del numero di attacchi gravi è aumentato di 10 volte rispetto al precedente. Non solo, la Severity media di questi attacchi è contestualmente peggiorata, agendo da moltiplicatore dei danni.

Dal punto di vista numerico, nel 2018 il rapporto ha raccolti e analizzati 1.552 attacchi gravi (+ 37,7% rispetto all'anno precedente), con una media di 129 attacchi gravi al mese (rispetto ad una media di 94 al mese nel 2017, e di 88 su 8 anni).

Anche quest'anno lo studio si avvalso dei dati relativi agli attacchi rilevati dal Security Operations Center (SOC) di FASTWEB, che ha analizzato la situazione italiana sulla base di oltre 40 milioni di eventi di sicurezza. L'analisi degli attacchi è poi completata da due contributi tecnici: il "Rapporto 2018 sullo stato di Internet – Analisi globale degli attacchi di DDoS, applicativi e furto di identità" a cura di Akamai e "Email security: i trend rilevati in Italia nel corso del 2018" a cura di Libraesva.

Seguono le rilevazioni e segnalazioni della Polizia Postale e delle Comunicazioni, del Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza. del CERT Nazionale e del CERT PA.

Vi è un capitolo dedicato al settore FINANCE, con 4 contributi: "Elementi sul Cyber-crime nel settore finanziario in Europa" a cura di IBM; "Analisi del Cyber-crime in Italia in ambito finanziario nel 2018" a cura di Communication Valley Reply**; ""Sviluppo di un sistema di cyber threat intelligence" a cura di Banca d'Italia; "Carding – Scenario ed evoluzione dei canali di vendita nel 2018"** a cura di Lutech**.**

Il 2018 è stato un anno cruciale per la Data Protection e non solo perché il 25 maggio il GDPR è entrato pienamente in vigore: per la prima volta è emersa con chiarezza, nella consapevolezza della pubblica opinione, la relazione fra la protezione dei dati personali e libertà e diritti degli interessati, così spesso richiamati dagli articoli del GDPR. A distanza di 9 mesi dall'entrata in vigore del nuovo Regolamento sono stati raccolti in uno "Speciale GDPR", alcuni contributi che aiutano a capire meglio le cose da fare: "2019: data protection 4.0" di Sergio Fumagalli e "La terza fase del GDPR" di Alessandro Vallega. Lo Speciale contiene i risultati di una survey realizzata dall'Osservatorio Sicurezza & Privacy del Politecnico di Milano sullo stato di adeguamento al GDPR delle aziende italiane. Lo speciale è chiuso da un contributo tecnico su "Cifratura dei dati personali e adeguamento al nuovo Regolamento Europeo" di Paola Meroni.

Tra le novità del Rapporto Clusit 2019, un capitolo dedicato all'Intelligenza Artificiale, con tre contributi: "**Intelligenza Artificiale: il Buono, il Brutto, il Cattivo**" di Fabio Roli; "**L'Intelligenza Artificiale è sicura**?" di Battista Biggio; "**L'intelligenza artificiale come strumento "dual use" nella cybersecurity**" a cura di DXC Technology.

Un altro capitolo è dedicato alla Blockchain, con: "**Blockchain & Supply Chain: una catena del valore sicura, distribuita e trasparente**" di Guido Sandonà e Federico Griscioli; "**Possibili**

problemi nella gestione degli smart contracts" di Alessio Pennasilico e Piero Bologna; "**Il 2018 dei Crypto Exchange**" di Davide Carboni.

Anche in questa edizione del rapporto, troviamo un'analisi del mercato italiano della sicurezza IT, realizzata appositamente da IDC Italia.

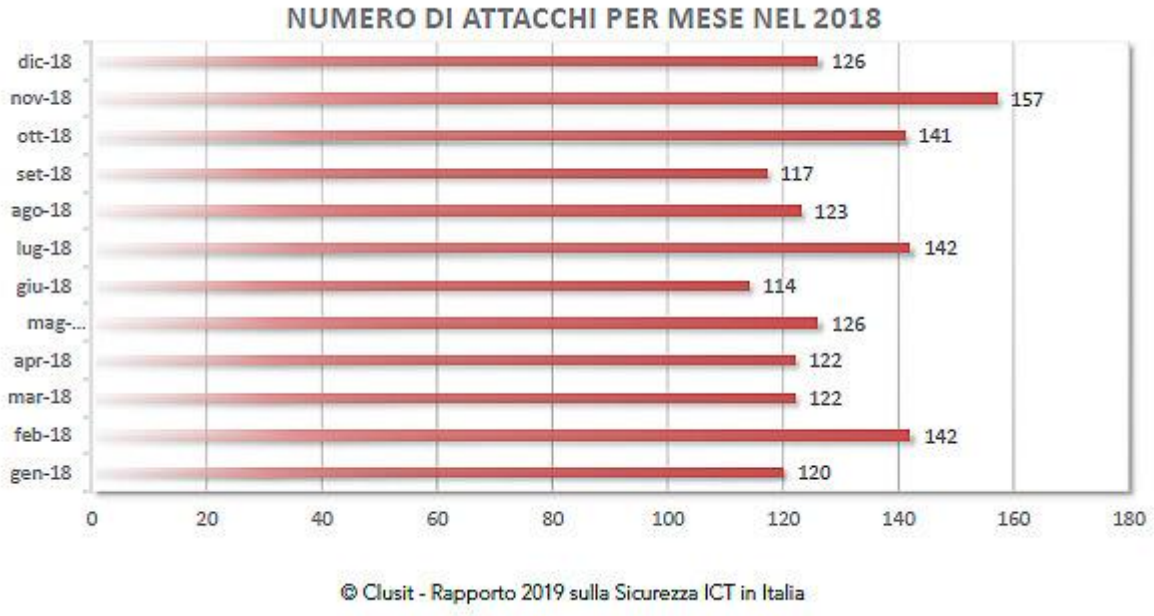
Il rapporto contiene inoltre 6 FOCUS ON:

- "**Programmi di security awareness: una necessità non più rimandabile**" di Garibaldi Conte.
- "**La sicurezza delle imprese è fatta di persone competenti e consapevoli. Un manifesto per la competenza digitale e la consapevolezza in materia di sicurezza online con focus sulla Generazione Z**" di Ettore Guarnaccia.
- "**Il panorama delle startup italiane nel settore cybersecurity e legal-tech. Stato dell'arte e valutazioni sul trend evolutivo**" di Giuseppe Vaciago.
- "**La logica del profitto alla base dell'aumento del cryptojacking"** a cura di Bitdefender.
- "**Infrastrutture critiche vulnerabili. Sempre più alto il rischio di attacchi agli impianti idrici ed energetici**" a cura di Trend Micro.
- "**Attacchi e difese nel Cloud Computing nel 2018**" a cura di Microsoft.

Di seguito alcuni dati estrapolati dalla ricerca.

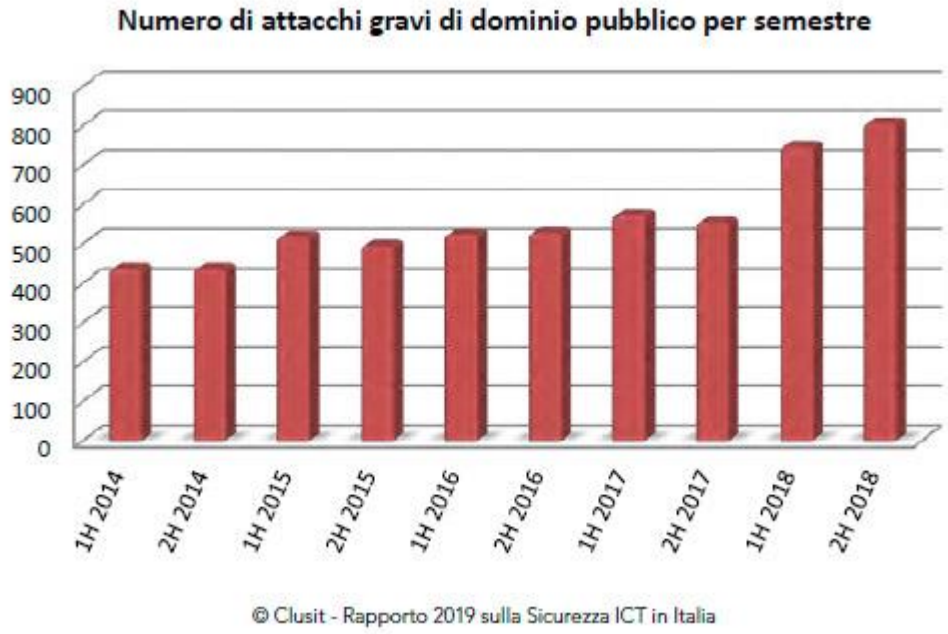
Il 2018 è stato l'anno peggiore di sempre per quanto riguarda gli **attacchi informatici**, superando il 2017.

- Secondo Andrea Zapparoli Manzoni, consiglio direttivo Clusit, è a rischio la sopravvivenza stessa della nostra attuale società digitale e le aziende di ogni dimensione non stanno facendo abbastanza per proteggere i sistemi informativi e i dati, mettendo in pericolo intere catene produttive.
- Le risorse economiche investite nella protezione dai **cyber attack** sono ancora insufficienti, a causa di un livello di awareness ancora pericolosamente basso.
- Gli investimenti in **sicurezza informatica** aumentano, ma non abbastanza da assicurare l'invulnerabilità da attacchi sempre più frequenti, gravi ed efficaci.



- # Il rischio informatico aumenta e gli attacchi hanno impatti sempre maggiori

- Gli attacchi informatici sono raddoppiati in quattro anni: nel 2018, si è registrata una media di 129 attacchi mensili di alto profilo, oltre il 38% in più rispetto al 2017. Per il 2019 si prevede un'ulteriore crescita: picchi che supereranno i 200 attacchi al mese e una media probabilmente oltre i 150 mensili.
- Queste stime contano gli attacchi di pubblico dominio e gli attacchi reali potrebbero essere ancora di più. I dati relativi all'Europa, per esempio, sono ancora sicuramente frammentari e gli effetti propulsivi del Regolamento sulla protezione dei dati personali (GDPR) si vedranno maggiormente solo tra qualche anno.
- Il settore healthcare ha rilevato un aumento del 99% degli attacchi cyber, ma i cyber criminali non risparmiano alcun settore. Si è riscontrata una tendenza in aumento dei rischi per la sicurezza informatica trasversale a tutti i settori, che dimostra aggressioni poco focalizzare a specifici segmenti economici o strategici, ma interessati a colpire trasversalmente ogni settore, danneggiando i sistemi e impadronendosi dei dati spesso per rivenderli.
- La scarsa consapevolezza e spesso anche una competenza insufficiente è testimoniata anche dalla continua crescita, del 57% ogni anno, tanto nel mondo aziendale quanto in quello domestico, di attacchi di phishing e social engineering.



Gli esperti del Clusit, hanno suddiviso gli **attacchi informatici** anche per livelli di impatto, suddividendoli fra medi, alti e critici.

- La severità degli eventi si sta innalzando sensibilmente rispetto al 2017. Il 39% degli attacchi ha un impatto medio, mentre nel 2017 erano il 49%. Gli attacchi ad alto impatto costituiscono il 33% del totale (erano il 31%) e quelli di livello critico quasi un terzo con il 28% (erano il 21%).
- Il maggior numero di attacchi classificati come critici riguarda le categorie **espionage** e **Information Warfare**, a dimostrazione del fatto che gli attacchi informatici hanno natura prevalentemente economica. La prevalenza di attività **cybercriminali** con impatto di livello

medio e alto spiega invece la necessità degli hacker di mantenere un profilo basso per continuare indisturbati, guadagnando più sui grandi numeri che sul singolo attacco.

- Secondo i dati raccolti da Fastweb, nel 2018 gli eventi di sicurezza sono aumentati del 14% rispetto al 2017. I diversi tipi di **malware** sono in crescita del 10%, con 212 famiglie di malware rilevate, e ben il 15% del totale delle e-mail è costituito da **phishing**.

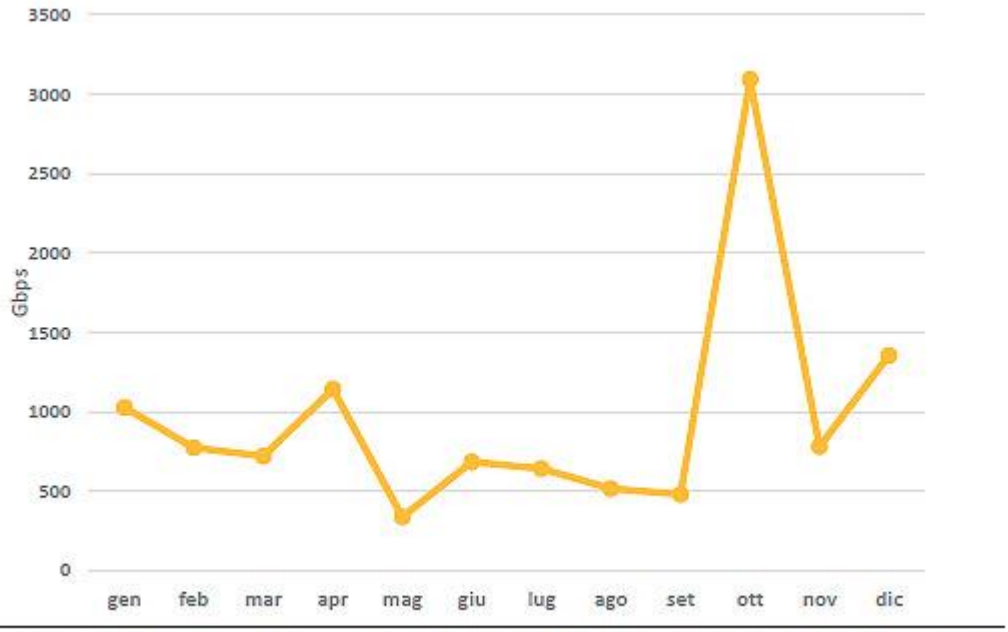


Figura 7 - *Banda totale mensile impegnata negli attacchi DDoS (Dati Fastweb relativi all'anno 2018)*

- Gli attacchi **DDoS** sono cresciuti ad un ritmo ancora maggiore, del 30%. Si tratta di un tipo di attacchi tanto semplici da organizzare quanto efficaci. L'acronimo significa "Distributed Denial of Service", traducibile in italiano come "Interruzione distribuita del servizio" e consiste nel tempestare di richieste un sito, fino a ingolfarlo e renderlo irraggiungibile. Attacchi di questo tipo hanno ancora un grosso impatto, nonostante sia ampiamente raddoppiata la banda usata, che cresce del 200% ogni due anni
- Akamai, azienda per la distribuzione di contenuti via Internet, ha rilevato 16.000 attacchi DDoS nel corso del 2018, il 16% in più rispetto all'anno precedente. Per comprendere la portata di questi attacchi, si ricordi l'attacco DDoS portato da una botnet, una rete di computer infettati da malware, nel marzo 2018: questo attacco ha generato da solo un picco di traffico di 1,3 Tbit, in grado di paralizzare un'intera nazione tra quelle emergenti. Il testo dei pacchetti adottati per l'attacco faceva riferimento a un importo in criptovaluta per interrompere l'attacco, mostrando la natura estorsiva delle azioni perpetrate.
- Sia i cybercriminali che le azioni di difesa della sicurezza informatica utilizzano intelligenza artificiale e machine learning, ma stare al passo delle evoluzioni tecnologiche e delle nuove strategie di attacco è una continua sfida. Occorrono competenze nel settore **sicurezza IT** spesso carenti, anche se il mercato della sicurezza IT in Italia è in crescita e aziende di ogni dimensione iniziano a capire l'importanza e la centralità del tema.