Rapporto Clusit 2019 sulla sicurezza ICT

CLUSIT: nel 2018 +38% di attacchi e minacce in continua evoluzione; a rischio la sopravvivenza della società digitale.

A repentaglio la Sanità: attacchi gravi cresciuti del 99% nell'arco di 12 mesi; in aumento del 57% Phishing e Social Engineering.

Milano, 21 febbraio 2019 – Il trend individuato dal 2011 ad oggi dagli esperti di Clusit, l'Associazione Italiana per la Sicurezza Informatica, non lascia spazio alle interpretazioni: gli attacchi con impatto significativo rilevati a livello globale vanno a comporre una curva di crescita che non vede flessioni, con un **picco del +38% nel 2018**, anno in cui si sono registrati **1.552 attacchi gravi**, con una media di 129 al mese.

I dati sono contenuti nella quattordicesima edizione del Rapporto Clusit sulla sicurezza ICT[1]: l'anteprima, presentata oggi a Milano, evidenzia anche che è sempre il **Cybercrime** la **principale causa di attacchi gravi**: il **79%** di questi è stato infatti compiuto allo scopo di estorcere denaro alle vittime, o di sottrarre informazioni per ricavarne denaro (+44% rispetto ai dodici mesi precedenti). Nel 2018 è stata inoltre registrata la crescita del **57%** dei crimini volti ad attività di **spionaggio cyber,** lo spionaggio con finalità geopolitiche o di tipo industriale, a cui va anche ricondotto il furto di proprietà intellettuale.

Le attività di **Hacktivism** e di **Cyber warfare** (la guerra delle informazioni) risultano invece in calo nel 2018, rispettivamente del **23%** e del **10%**, se paragonate all'anno precedente. Va sottolineato che, rispetto al passato, oggi risulta più difficile distinguere nettamente tra "Cyber Espionage" e "Information Warfare": sommando gli attacchi di entrambe le categorie, nel 2018 si assiste ad un aumento del 35,6% rispetto all'anno precedente.

Particolarmente significativa l'analisi dei "**livelli di impatto**" per ogni singolo attacco, in termini geopolitici, sociali, economici, di immagine e di costo: si osserva in generale un deciso **aumento della gravità media degli attacchi** rispetto al 2017. In particolare, l'80% di quelli realizzati con finalità di Espionage e oltre il 70% di quelli imputabili all'Information Warfare sono stati classificati

[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 annualmente il quadro più aggiornato ed esaustivo della situazione globale, evidenziando i settori più colpiti, le tipologie e le tecniche d'attacco più frequenti, sulla base degli attacchi di dominio pubblico – che rappresentano un campione necessariamente limitato, per quanto ragionevolmente significativo, rispetto al numero degli attacchi informatici gravi effettivamente avvenuti nel periodo in esame. È noto infatti che *un buon numero* di aggressioni non diventano *mai* di dominio pubblico, oppure lo diventano *ad anni di distanza,* quando le vittime ne vengono a conoscenza (solitamente quanto più gli attacchi sono sofisticati e gravi), sia perché in molti casi è interesse dei bersagli non pubblicizzare gli attacchi subiti, se non costretti da circostanze o normative particolari.

nel 2018 di livello “critico”; le attività riconducibili al cybercrime sono state invece caratterizzate prevalentemente da un impatto di tipo “medio”. Ciò è dovuto, secondo gli esperti Clusit, alla necessità degli attaccanti di mantenere un profilo relativamente basso, per poter continuare ad agire senza attirare troppa attenzione.

Cyber attacchi nel 2018: chi viene colpito e perché

Negli ultimi dodici mesi la **sanità** ha subito l’incremento maggiore degli attacchi, pari al **99%** rispetto al 2017. Nel 96% dei casi gli attacchi a questo settore hanno avuto finalità cybercriminali e di furto di dati personali.

Segue il **settore pubblico**, con il **41%** degli attacchi in più rispetto ai dodici mesi precedenti e i cosiddetti “**multiple targets**” - i bersagli multipli - che nel 2018 risultano anche i maggiormente colpiti, con **un quinto degli attacchi globali a loro danno**, dato in crescita del **37%** rispetto al 2017. Queste cifre confermano che - come già constatato negli ultimi anni - non solo ormai tutti sono diventati bersagli, ma anche che gli attaccanti sono diventati sempre più aggressivi e sono in grado di condurre operazioni su scala sempre maggiore, con una logica “industriale”, che prescinde sia da vincoli territoriali che dalla tipologia delle vittime.

Nel 2018 sono stati presi di mira anche i settori della **ricerca e formazione**, che vede un **incremento del 55%** degli attacchi rispetto al 2017, dei **servizi online e cloud** e delle **banche**, con l’aumento degli attacchi rispettivamente in crescita del **36%** e del **33%**, sempre rispetto all’anno precedente.

Considerando la gravità dei singoli attacchi nei settori di riferimento, gli esperti Clusit evidenziano che la **sanità** e le **infrastrutture critiche risultano essere i settori per i quali i rischi cyber sono cresciuti maggiormente nel 2018**; pur avendo subito in assoluto un numero di attacchi maggiore, il settore pubblico e i “multiple targets” non mostrano invece peggioramenti significativi in termini di gravità.

Le tecniche d’attacco

È stato ancora il **malware** “semplice”, prodotto industrialmente e a costi sempre decrescenti il principale vettore di attacco nel 2018, in crescita del **31%** rispetto al 2017; All’interno di questa categoria, i **Cryptominers** - pressoché inesistenti in passato - nel corso del 2018 sono arrivati a rappresentare il **14%** del totale (erano il 7% nel 2017); l’utilizzo del **malware per le piattaforme mobile** negli ultimi dodici mesi ha rappresentato quasi il **12%** del totale.

Da segnalare la crescita del **57%** rispetto all’anno precedente degli attacchi sferrati con tecniche di **Phishing e Social Engineering** su larga scala, ancora a testimonianza della logica sempre più “industriale” degli attaccanti.

L’elevato incremento negli ultimi dodici mesi dell’utilizzo di **tecniche sconosciute** (**+47%**) dimostra tuttavia che i cybercriminali sono piuttosto attivi anche nella ricerca di nuove modalità di attacco.

I **DDoS** rimangono sostanzialmente invariati rispetto al 2017, lo sfruttamento di **vulnerabilità note** invece è ancora in crescita (**+39,4%**), così come l’utilizzo di vulnerabilità “**0-day**”, (**+66,7%**), per quanto questo dato sia ricavato da un numero di incidenti noti limitato e risulti probabilmente

sottostimato. Ritornano a crescere gli attacchi basati su tecniche di "**Account Cracking**" (**+7,7%**). Unico dato in calo, le **SQL injection**, che segnano **-85,7%** rispetto al 2017.

Rapporto Clusit 2019: alcune considerazioni di tipo qualitativo

I dati che emergono dall'anteprima del Rapporto Clusit 2019 vanno letti alla luce del "*cambiamento di fase nei livelli globali di insicurezza cyber, causata dall'evoluzione rapidissima degli attori, delle modalità e delle finalità degli attacchi*", come afferma Andrea Zapparoli Manzoni, membro del Comitato Direttivo Clusit, tra gli autori del Rapporto Clusit.

Ovvero, è apparso evidente nel corso degli ultimi dodici mesi il graduale trasferimento dei conflitti sul fronte "cyber" da parte dei singoli Stati, con un innalzamento continuo del livello di scontro in una superficie di attacco di fatto illimitata: secondo gli esperti Clusit la nostra società è entrata in una fase di **cyber guerriglia permanente**, che rischia di minacciare la nostra stessa società digitale.

La rapida evoluzione delle minacce di cyber spionaggio e sabotaggio aggravano lo scenario: la cosiddetta "**guerra della percezione**", che si basa sulla creazione di *fake news* e sulla loro amplificazione attraverso i social media, insieme alle infiltrazioni in infrastrutture critiche e ai furti di informazione per finalità geo-politiche, amplificano infatti notevolmente i livelli di rischio, consentendo ai cybercriminali di finanziarsi per poter compiere poi crimini più importanti.

Ad accrescere le preoccupazioni, il paradigma dell'**Intelligenza Artificiale**: da una parte tecniche di Machine Learning sono utilizzate dai cybercriminali per compiere attacchi in maniera molto efficace e sempre meno costosa; dall'altra, questi sistemi risultano oggi ancora piuttosto vulnerabili, e quindi facilmente attaccabili, anche a causa delle attuali difficoltà di monitoraggio e gestione dei sistemi.

Tra gli aspetti che oggi determinano la fragilità della società digitale, secondo gli esperti Clusit, non sono da trascurare infine le **lacune legislative** e alcuni fenomeni socio-politici che hanno di fatto determinato una **mancanza di trasparenza e di responsabilità sociale** delle multinazionali hi-tech.

"*Saranno le prossime scelte in ambito di sicurezza cibernetica a determinare le probabilità di sopravvivenza della nostra attuale società digitale*", afferma Andrea Zapparoli Manzoni. "*Al cuore della questione c'è una criticità che è sia culturale che economica: abbiamo costruito la nostra civiltà digitale senza tenere conto dei costi correlati alla sua tutela e difesa, secondo un modello di business che non li prevede, se non in modo residuale e, ove possibile, li evita o li minimizza. Di conseguenza queste risorse non sono disponibili, e oggi nel mondo si investe per la cyber security un decimo di quanto si dovrebbe ragionevolmente spendere*", conclude Zapparoli Manzoni.

I contributi Fastweb, Akamai e IDC Italia
Il Rapporto Clusit presenta anche i dati relativi agli attacchi rilevati dal Security Operations Center (SOC) e relativi agli indirizzi IP appartenenti all'Autonomous System (AS) di **Fastweb**[2], che ha analizzato la situazione italiana in materia di cyber-crime e incidenti informatici sulla base di oltre 40 milioni di eventi di sicurezza accaduti nel 2018.

I dati - automaticamente aggregati e anonimizzati per proteggere la privacy e la sicurezza dei Clienti e di Fastweb stessa - mostrano un'evoluzione nella composizione dei Malware e Botnet rispetto al 2017: oltre a diverse minacce già presenti lo scorso anno, sono state rilevate 212 famiglie di software malevoli (+10% rispetto all'anno precedente) e, soprattutto, la diffusione massiva di nuovi malware, non ancora classificati e riconducibili a una famiglia nota.

L'analisi di Fastweb evidenzia inoltre la distribuzione geografica dei centri di comando e controllo dei malware (C&C), che rappresentano i sistemi compromessi utilizzati per l'invio dei comandi alle macchine infette da malware (bot) utilizzate per la costruzione delle botnet. Ben oltre la metà dei centri di C&C relativi a macchine infette appartenenti all'AS di Fastweb nel 2018 sono stati rilevati negli Stati Uniti; negli ultimi dodici mesi è emersa tuttavia la crescita importante dei C&C anche in Europa (+24% rispetto al 2017).

L'analisi degli attacchi all'interno del Rapporto CLUSIT 2019 include il "Rapporto 2018 sullo stato di Internet - Analisi globale degli attacchi di DDoS, applicativi e furto di identità", a cura di **Akamai** e il contributo inedito di **IDC Italia** relativo a "Il mercato italiano della Sicurezza IT: analisi, prospettive e tendenze".

Seguono le rilevazioni e segnalazioni della **Polizia Postale e delle Comunicazioni**, del **Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza** e del **CERT Nazionale** per l'anno 2018.

Completano il Rapporto Clusit 2019 un approfondimento sul settore **Finance**, con un contributo di **Banca d'Italia** dedicato a "cyber intelligence e banche centrali" e gli speciali tematici dedicati a **GDPR**, **blockchain** e **Intelligenza Artificiale**, insieme a "**Focus On**" relativi ad aspetti specifici della sicurezza informatica.

***

Il Rapporto CLUSIT 2019 sarà presentato al pubblico il prossimo 12 marzo in apertura della undicesima edizione di Security Summit, convegno che si propone di analizzare lo stato dell'arte della cybersecurity e di delineare in maniera indipendente le prospettive per i mesi a venire per creare una vera e propria cultura sui temi della sicurezza delle informazioni, delle reti e delle infrastrutture informatiche.

Security Summit ha il patrocinio della Commissione Europea

Security Summit 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

[2] Si tratta di oltre 6 milioni di indirizzi pubblici su ognuno dei quali possono comunicare decine o anche centinaia di dispositivi e server attivi presso le reti dei Clienti.

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