CLUSIT: cybercrime fuori controllo,
nel 2017 danni globali per oltre 500 miliardi di dollari

Presentato oggi a Milano il Rapporto Clusit 2018:
i costi della 'insicurezza informatica' quintuplicati in sei anni;
nel 2017 colpito oltre un miliardo di persone nel mondo

Ancora insufficienti gli investimenti in sicurezza informatica in Italia:
"*preoccupante la scarsa attenzione al tema nel dibattito politico alla vigilia delle elezioni*"

Milano, 28 febbraio 2018 – Gli esperti del Clusit, l'Associazione Italiana per la Sicurezza Informatica, lo hanno definito un "**salto quantico**": **l'andamento della cyber-insicurezza ha toccato nel 2017 livelli inimmaginabili ancora pochi anni fa, sia a livello quantitativo, che qualitativo**.

La dodicesima edizione del **Rapporto CLUSIT sulla sicurezza ICT** presentata oggi a Milano evidenzia infatti un trend inarrestabile di crescita degli attacchi e dei danni conseguenti. Sono stati **1.127 gli attacchi "gravi" registrati ed analizzati nel 2017 da Clusit a livello mondiale**, ovvero con impatto significativo per le vittime in termini di perdite economiche, di danni alla reputazione, di diffusione di dati sensibili[1]. Di questi, il 21% è stato classificato dagli esperti Clusit di impatto "critico".

In termini numerici, si assiste ad una **crescita del 240% degli attacchi informatici rispetto al 2011**, anno a cui risale la prima edizione del Rapporto Clusit, e del **7% rispetto al 2016**; tuttavia, a preoccupare gli esperti, è il vero e proprio "**cambiamento di fase" nel livello di cyber-insicurezza globale**, con interferenze pesanti tanto nella geopolitica e nella finanza, quanto sui privati cittadini, vittime nel 2017 di crimini estorsivi su larghissima scala.

Andrea Zapparoli Manzoni, membro del Comitato Direttivo Clusit, sintetizza **in tre punti chiave** i dati analizzati nel Rapporto Clusit 2018: "*il 2017 è stato l'anno del trionfo del Malware[2], degli attacchi industrializzati realizzati su scala planetaria contro bersagli multipli e della definitiva discesa in campo degli Stati come attori di minaccia*".

---

1 Frutto del lavoro di oltre un centinaio di professionisti che operano nell'ambito dell'Associazione per la Sicurezza Informatica in Italia, da sette anni il Rapporto Clusit fornisce ogni anno 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. E' 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 (come auspicabilmente avverrà da quest'anno, quantomeno in Europa, con la piena applicazione del Regolamento GDPR e della Direttiva NIS).

2 Software malevolo, sviluppato con l'obiettivo di infettare computer o dispositivi mobile

"*La situazione che emerge dalla nostra analisi è molto preoccupante*" - prosegue Zapparoli Manzoni - "*perché questo scenario prefigura concretamente l'eventualità di attacchi con impatti sistemici molto gravi".*

Gli attacchi nel 2017: chi viene colpito e perché; le cifre in gioco

In particolare, il Rapporto Clusit 2018 evidenzia il **Cybercrime** (la cui finalità ultima è sottrarre informazioni, denaro, o entrambi), quale **prima causa di attacchi gravi a livello mondiale** (**76% degli attacchi complessivi**, in crescita del 14% rispetto al 2016); sono in netto aumento rispetto allo scorso anno gli attacchi sferrati con finalità di **Information Warfare** (la guerra delle informazioni, che segna **+24%**) e il **Cyber Espionage** (lo spionaggio con finalità geopolitiche o di tipo industriale, a cui va tra l'altro ricondotto il furto di proprietà intellettuale, che cresce del **46%**).

Importanti le cifre in gioco: secondo gli esperti Clusit dal 2011 al 2017 **i costi generati globalmente dalle sole attività del Cybercrime** sono quintuplicati, arrivando a toccare quota **500 miliardi di dollari nel 2017**. Lo scorso anno, truffe, estorsioni, furti di denaro e dati personali hanno colpito quasi **un miliardo di persone nel mondo**, causando ai soli privati cittadini una **perdita stimata in 180 miliardi di dollari**. Sono esclusi da questa quantificazione i danni causati dalle attività di Cyber Espionage e le conseguenze sistemiche generate dalle crescenti attività di Information Warfare, i cui impatti sono difficilmente calcolabili, ma sicuramente crescenti.

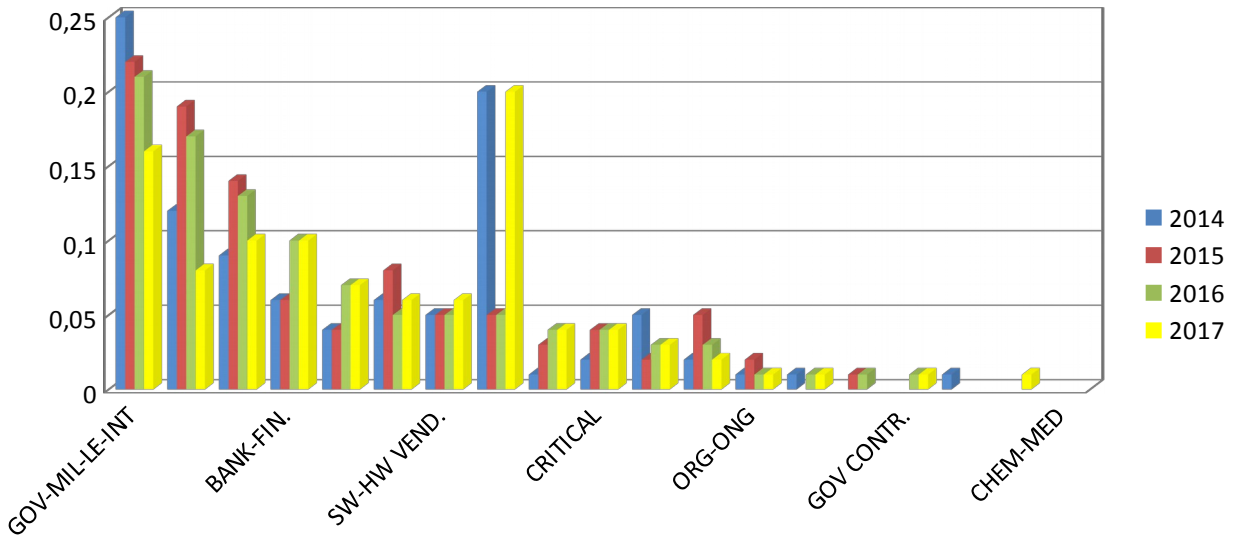
"*Pur essendo ancora la prima causa di attacco a livello globale e rappresentando un problema enorme, il Cybercrime è diventato ormai l'ultimo dei nostri problemi in ambito cibernetico dal punto di vista della sua pericolosità intrinseca. Oggi ci troviamo infatti a fronteggiare problemi ben peggiori*", conferma Andrea Zapparoli Manzoni.

In questo contesto, il Rapporto Clusit 2018 introduce l'analisi dei "livelli di impatto" di ogni singolo attacco in termini geopolitici, sociali, economici, di immagine e di costo. Nel dettaglio, quasi l'80% degli attacchi realizzati per finalità di Espionage e oltre il 70% di quelli imputabili all'Information Warfare sono stati classificati di livello "critico"; le attività riconducibili al cybercrime sono state invece caratterizzate prevalentemente da un impatto di tipo "medio", dovuto presumibilmente alla necessità degli attaccanti di mantenere un profilo relativamente basso, per guadagnare sui "grandi numeri" senza attirare troppa attenzione.

Una novità, nel 2017, è rappresentata dalla tipologia e distribuzione delle vittime: è infatti la categoria dei "**Multiple Targets**[3]" la più colpita: rispetto al 2016 si evidenzia un incremento a tre cifre, pari al **353%**, a conferma del fatto che nessuno può ritenersi escluso dall'essere un obiettivo e che gli attaccanti sono sempre più aggressivi, potendo contare su logiche e mezzi industriali e prescindendo sempre più da limiti territoriali e tipologia di bersaglio per massimizzare il danno inflitto alle vittime e/o il proprio risultato economico.

Sono cresciuti significativamente nel 2017 rispetto all'anno precedente anche gli attacchi nel settore **Research / Education** (+29%), **Software / Hardware Vendors** (+21%), **Banking & Finance** (+11%) e **Healthcare** (+10%).

3 Organizzazioni appartenenti a settori differenti e geograficamente distribuiti



Le tecniche d'attacco

E' il **malware**[4] prodotto industrialmente e a costi sempre decrescenti il principale vettore di attacco nel 2017, in crescita del **95%** rispetto al 2016 (quando già si era registrato un incremento del 116% rispetto all'anno precedente). A questo dato va sommata la crescita della categoria "Multiple Threats / APT" (**+6%**), che include attacchi più articolati e sofisticati, (quasi sempre basati anche sull'utilizzo di malware). Seguono, a testimonianza della logica sempre più "industriale" degli attaccanti, gli attacchi sferrati con tecniche di **Phishing / Social Engineering** su larga scala (**+34%**).

Alla luce dei dati analizzati dal Clusit, nel 2017 gli attacchi gravi sono stati compiuti nella maggioranza dei casi (**68%**) con **tecniche banali**, come SQLi, DDoS, Vulnerabilità note, Phishing, malware "semplice": questo trend è in crescita di 12 punti percentuali rispetto al 2016. Significa, secondo gli esperti Clusit, che gli **attaccanti realizzano attacchi di successo contro le loro vittime con relativa semplicità, a costi sempre minori**.

In decisa crescita anche l'utilizzo di malware specifico per **attacchi alle piattaforme mobile**, che **rappresenta ormai quasi il 20% del malware totale**.

La situazione italiana

Sulla base delle cifre in gioco a livello globale, gli esperti Clusit stimano che **l'Italia nel 2016 abbia subito danni derivanti da attività di cyber crimine per quasi 10 miliardi di euro**[5]: si tratta di un valore dieci volte superiore a quello degli attuali investimenti in sicurezza informatica, che arrivano oggi a sfiorare il miliardo di euro. "*Gli investimenti in sicurezza informatica nel nostro Paese sono ancora largamente insufficienti e ciò rischia di erodere i benefici attesi dal processo di digitalizzazione della nostra società",* afferma Zapparoli Manzoni. "*Ad oggi, alla vigilia delle elezioni, riscontriamo che il dibattito politico in Italia sta dando risposte inadeguate al tema della sicurezza cyber, fondamentale per lo sviluppo e il benessere dei suoi cittadini, nonché per la credibilità e la competitività del nostro Paese sul piano internazionale*".

4 Tipologia che include anche i cosiddetti "**ransomware**"

5 Stima basata su dati rilevati in USA e UK nel 2016; si tratta dei dati più recenti disponibili ad oggi

Il GDPR
Filo rosso dell'anno in corso per quanto riguarda le tematiche della sicurezza cyber, al nuovo regolamento europeo per la protezione dei dati personali sono dedicati quattro capitoli all'interno del Rapporto Clusit 2018. La compliance, evidenziano gli esperti, richiede necessariamente un approccio multidisciplinare in tema di sicurezza delle informazioni, uno dei princìpi a cui il trattamento dei dati personali deve attenersi. In particolare, nel Rapporto Clusit 2018 si parlerà della normativa "ai blocchi di partenza" e delle implicazioni che il GDPR avrà sulle aziende italiane, illustrate da survey esclusiva degli Osservatori *Digital Innovation* della School of Management del Politecnico di Milano. Sarà inoltre presentata una ricerca internazionale sulla privacy dei dati trattati a fini di marketing nei paesi dell'UE e un contributo specifico sulle segnalazioni dei Data Breach nel contesto della nuova normativa.

I "FOCUS ON" del Rapporto Clusit 2018
Come le precedenti edizioni, il Rapporto Clusit 2018 dedica nei cosiddetti "Focus On" approfondimenti a singoli settori e a problematiche particolarmente attuali in tema di sicurezza cyber, a firma di esperti autorevoli. Quest'anno sono in evidenza la Sicurezza Marittima, l'Industria 4.0, il Cloud, la Mail Security, il Business Risk, le attività di Profiling, la diffusione delle criptovalute e la Blockchain, il Ransomware, la Gestione dei Fornitori.

I contributi Fastweb, Akamai e IDC Italia
Il Rapporto Clusit 2018 presenta storicamente anche i dati relativi agli attacchi rilevati dal Security Operations Center (SOC) e relativi agli indirizzi IP appartenenti all'Autonomous System (AS) di **Fastweb**, che ha analizzato la situazione italiana in materia di cyber-crime e incidenti informatici sulla base di oltre 35 milioni di eventi di sicurezza accaduti nel 2017.
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 2016, soprattutto per la diffusione massiva di nuovi malware, ancora sconosciuti e non rilevabili da sistemi tradizionali.

L'analisi degli attacchi all'interno del Rapporto CLUSIT 2018 include inoltre il "Rapporto 2017 sullo stato di Internet ed analisi globale degli attacchi DDoS e applicativi Web", a cura di **Akamai**.

Compongono ancora il Rapporto Clusit le rilevazioni della **Polizia Postale** e del **CERT-PA** per l'anno 2017 e un'importante analisi nell'ambito del settore **Finance**, con tre approfonditi contributi dedicati al Cybercrime in Europa e in Italia e al traffico di carte di credito e di identità degli account bancari.

Segue il contributo inedito di **IDC Italia** relativo a "Il mercato italiano della Sicurezza IT".

Il Rapporto CLUSIT 2018 sarà presentato al pubblico il prossimo 13 marzo in apertura della decima 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, con l'obiettivo di 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 e di ENISA, l'Agenzia dell'Unione Europea per la sicurezza delle informazione e della rete ed 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 b2b.
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