CLUSIT: cyber crimine, boom di nuove minacce nel 2018; nei primi sei mesi dell'anno aumentano del 31% gli attacchi gravi

Presentata oggi al Security Summit di Verona la nuova edizione del Rapporto Clusit 2018: mai una crescita così rapida e ad ampio raggio dei crimini informatici.

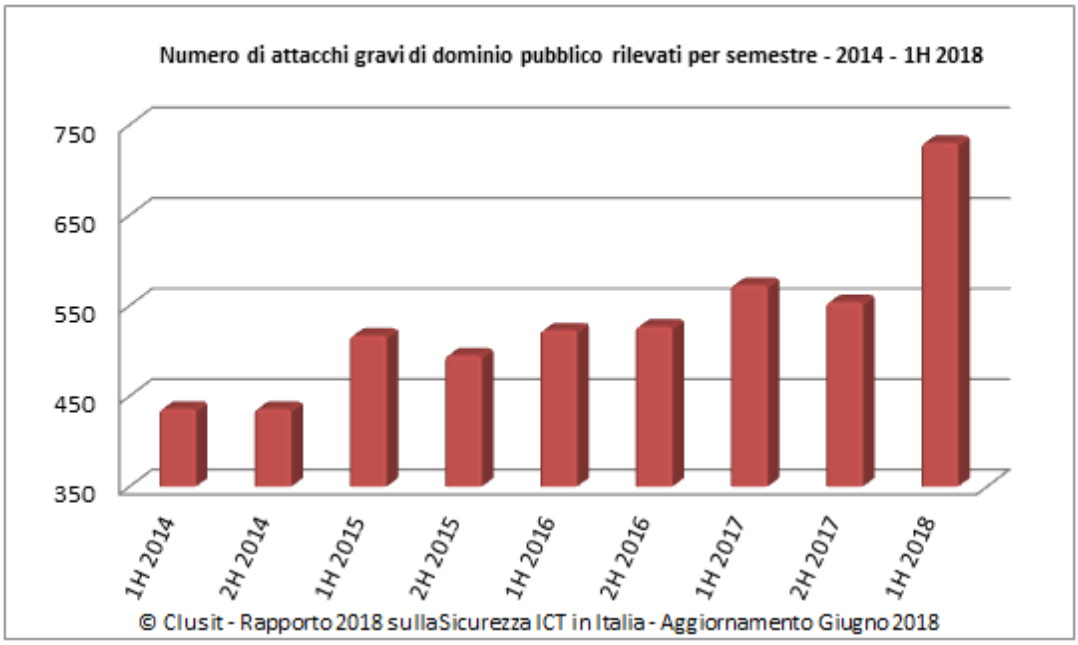
Sviluppati con estrema velocità nuovi e potenti malware, in grado di colpire in maniera indiscriminata, su scala planetaria. Ancora inadeguata la capacità di difesa

Milano, 4 ottobre 2018 – L'andamento dei crimini informatici nei primi sei mesi di quest'anno non lascia spazio alle interpretazioni: con **730 attacchi gravi registrati e analizzati**, che corrispondono ad una **crescita del 31% rispetto al semestre precedente**, il 2018 si appresa a battere il triste primato dello scorso anno, definito l'anno del "salto quantico" della cyber-insicurezza dagli esperti del Clusit, l'Associazione Italiana per la Sicurezza Informatica.

I dati emergono dalla **nuova edizione del Rapporto Clusit**, presentata questa mattina nel corso di **Security Summit di Verona**, il 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 incrementare la cultura sui temi della sicurezza delle informazioni, delle reti e delle infrastrutture informatiche.

Nel corso della presentazione, gli autori del Rapporto Clusit hanno evidenziato che, per numero di attacchi gravi[1] e tipologia, **il primo semestre 2018 è stato il peggiore di sempre**. In particolare, in questo periodo si è registrata una media di **122 attacchi gravi al mese** (rispetto ad una media di 94 al mese nel 2017). Il picco maggiore si è avuto nel febbraio 2018, con 139 attacchi: si tratta del valore mensile in assoluto più alto negli ultimi 4 anni e mezzo.

[1] Il Rapporto Clusit fornisce ogni anno il quadro più aggiornato ed esaustivo della situazione globale sulla base degli attacchi più gravi di dominio pubblico, che rappresentano un campione necessariamente limitato, ma ragionevolmente significativo, rispetto al numero degli attacchi informatici gravi effettivamente avvenuti nel periodo in esame.



Gli attacchi informatici nel primo semestre 2018: chi viene colpito e perché

Nei primi sei mesi del 2018 il **cybercrime** è stato la causa dell'80% degli attacchi informatici a livello globale, risultando **in crescita del 35% rispetto all'ultimo semestre 2017**; ad aumentare maggiormente quest'anno - del **69%** rispetto ai sei mesi precedenti - sono però le attività riferibili al **cyber espionage**.

I crimini informatici sono aumentati percentualmente a tre cifre nei primi sei mesi di quest'anno nel settore "**Automotive**", che segna **+200%**; a tre cifre anche la crescita degli attacchi in ambito "**Research/Education**", con **+128%**. Segue il settore "**Hospitability**": hotel, ristoranti, residence hanno subito da gennaio a giugno 2018 il 69% di attacchi in più rispetto agli ultimi sei mesi dello scorso anno. In decisa crescita anche i crimini nei settori Sanità (**+62%**), nelle Istituzioni (**+52%**) e nei servizi online/Cloud (**+52%**) e nel settore della consulenza (**+50%**).

La categoria maggiormente colpita in senso assoluto nei primi sei mesi di quest'anno, tuttavia, è quella identificata dagli esperti Clusit come "**Multiple Targets**" (18% del totale degli attacchi a livello globale), in aumento del **15%** rispetto ai sei mesi precedenti.

Il fenomeno, che spiega il crescente numero di attacchi gravi compiuti in parallelo dallo stesso gruppo di attaccanti contro numerose organizzazioni appartenenti ai settori più disparati, evidenzia concretamente la logica di tipo "industriale" alla base delle attività dei cybercriminali. Secondo Andrea Zapparoli Manzoni, membro del Comitato Direttivo Clusit, "*Sempre più gli attacchi prescindono sia da vincoli territoriali che dalla tipologia dei bersagli. L'aumento di attacchi gravi perpetrati ai danni di un target disomogeneo e diffuso geograficamente su scala globale dimostra la capacità, la determinazione e l'organizzazione degli attaccanti, che puntano a massimizzare il*

risultato economico con un approccio tipico della criminalità organizzata", conclude Zapparoli Manzoni.

Le tecniche d'attacco

Come di consueto, gli esperti Clusit hanno analizzato le tecniche utilizzate dai cybercriminali per colpire i propri bersagli: a crescere maggiormente in percentuale è l'utilizzo di vulnerabilità "**0-day**", (**+140%** rispetto agli ultimi sei mesi del 2017), dato per altro ricavato da un numero di incidenti noti limitato e quindi, probabilmente, sottostimato. Importante anche l'aumento della categoria "APT", che fa segnare un **+48%**.

È tuttavia il "**Malware semplice**" - prodotto industrialmente a costi sempre decrescenti - **il vettore di attacco più utilizzato** (40% del totale degli attacchi). Questa tecnica segna un incremento del **22%** nei primi sei mesi di quest'anno rispetto al 2017. Ransomware e Cryptominers, compresi nella categoria, rappresentano oggi il 43% del "malware semplice" utilizzato dai cybercriminali. In particolare, i **Cryptominers**, quasi inesistenti fino al 2016, sono stati utilizzati nel primo semestre dell'anno nel **22% degli attacchi realizzati tramite malware** (erano il **7%** nel 2017), superando di poco i Ransomware (+21%), a dimostrazione della dinamicità degli attaccanti, **capaci di creare nuove minacce e cambiare "modello di business" in maniera molto rapida**, a fronte di una velocità di reazione ancora troppo limitata da parte dei difensori.

Negli attacchi sono inoltre sempre molto utilizzate, secondo gli esperti del Clusit, anche le tecniche di **Phishing** e **Social Engineering**, in aumento del **22%** nei primi sei mesi del 2018.

"*Considerato che nel nostro campione analizziamo attacchi particolarmente gravi contro primarie organizzazioni a livello mondiale, è sconcertante che la somma delle tecniche di attacco più banali, come SQLi, DDoS, Vulnerabilità note, Phishing e Malware semplice, rappresenti oggi ancora il **61%** del totale. Significa che gli attaccanti riescono a realizzare attacchi di successo contro vittime*

teoricamente strutturate con relativa semplicità e a costi molto bassi, oltretutto decrescenti", afferma Andrea Zapparoli Manzoni. "*E questa è una delle considerazioni più preoccupanti tra quelle che emergono dalla nostra ricerca*", conclude Zapparoli Manzoni.

****

Security Summit ha il patrocinio della Commissione Europea e di ENISA, l'Agenzia dell'Unione Europea per la sicurezza delle informazioni 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