PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4189 di Lunedì 05 marzo 2018

CLUSIT: cresce l'industria del cybercrime nei primi sei mesi dell'anno

Il Rapporto Clusit sulla sicurezza ICT con i dati relativi al primo semestre 2017.

- ***+8,35% di attacchi informatici gravi a livello globale rispetto al semestre precedente***
- ***Aumentano del 253% gli attacchi verso "bersagli multipli indifferenziati" condotti da un'unica forza criminale, secondo una logica "industriale"***
- ***L'Europa è l'unico continente dove cresce la percentuale di vittime***
- ***Utilizzati soprattutto Malware (+86%, di cui oltre un terzo Ransomware) e tecniche di Phishing/Social Engineering (+85%)***
- ***Gli smartphone nel mirino: sempre più diffusi malware specifici per tutte le piattaforme***

Definito "l'Annus Horribilis" della sicurezza informatica, il 2016 ha in realtà ben presto perso il triste primato: la nuova edizione del Rapporto Clusit sulla sicurezza ICT - presentata oggi a Verona nel corso di Security Summit - illustra i dati relativi al primo semestre 2017 e fotografa una situazione decisamente più grave. Da gennaio a giugno di quest'anno, infatti, sono stati 571 gli attacchi gravi di dominio pubblico (ovvero attacchi che hanno avuto un impatto significativo per le vittime, in termini di danno economico, reputazione e diffusione di dati sensibili [1]), che corrispondono ad una crescita dell'8,35% rispetto al secondo semestre 2016.

Gli autori del Rapporto Clusit evidenziano che il primo semestre 2017 è stato il peggiore di sempre, confermando una inesorabile tendenza ascendente dal 2011 ad oggi.

"Nel primo semestre 2017 la cyber-insicurezza ha effettuato un 'salto quantico' a livello globale, raggiungendo livelli in precedenza inimmaginabili", afferma Andrea Zapparoli Manzoni, membro del Comitato Direttivo Clusit - Associazione Italiana per la Sicurezza Informatica - e tra gli autori del Rapporto Clusit 2017. "

Pubblicità
<#? QUI-PUBBLICITA-MIM-[CODE] ?#>

Questo a fronte di investimenti in Sicurezza ICT ancora del tutto insufficienti rispetto al valore del mercato di beni e servizi ICT, nonché alla percentuale di PIL generato tramite l'applicazione dell'ICT da parte di organizzazioni pubbliche e private e dai privati cittadini".

"E' quindi necessario mettere a punto un nuovo modello di investimenti in Cyber Security, commisurandoli adeguatamente alle minacce attuali. Pena una crescente e significativa erosionedei benefici attesi dal processo oggi in atto di digitalizzazione della

società", conclude Zapparoli Manzoni.

I dati presentati oggi dagli esperti Clusit evidenziano una situazione diffusa globalmente: qualsiasi organizzazione, indipendentemente dalla dimensione o dal settore di attività, è a rischio concreto di subire un attacco informatico di entità significativa entro i prossimi 12 mesi.

Oltre il 50% delle organizzazioni nel mondo - si rileva nel Rapporto Clusit aggiornato al primo semestre 2017 - **ha subìto almeno un attacco grave nell'ultimo anno**.

Gli attacchi nel primo semestre 2017: le cause

Sottostima dei rischi e investimenti insufficienti in sicurezza cyber sono le principali cause della curva ascendente dei crimini informatici negli ultimi sei mesi. Contestualmente, si assiste all'inarrestabile espansione della superficie di attacco esposta dalla nostra società digitale: la rapida diffusione di smart working, che si avvale di strumenti quali mobile, cloud e social, spesso utilizzati in maniera indiscriminata mescolando profili personali e lavorativi, e dell'Internet of Things, con apparecchiature per lo più prive delle più elementari misure di sicurezza, costituiscono punti di accesso sempre più immediati verso i sistemi informativi delle organizzazioni. Da evidenziare che ciò avviene oggi anche in contesti produttivi, quali l'Industry 4.0, e per applicazioni critiche come e-health e smart-city.

Gli attacchi nel primo semestre 2017: gli obiettivi

E' il Cybercrime la prima ragione di attacchi gravi nei primi sei mesi dell'anno: i criminali colpiscono le loro vittime nel 75% dei casi con l'obiettivo di estorcere denaro. Questa tipologia di attacco ha registrato una crescita del 13,26% rispetto ai sei mesi precedenti.

In aumento - a tre cifre, sempre sul confronto con la seconda metà del 2016 ? anche i crimini riferibili al Cyber Espionage (+126%). Rispetto al secondo semestre 2016, nei primi sei mesi di quest'anno la crescita percentuale maggiore di attacchi gravi si osserva verso la categoria dei cosiddetti "Multiple Targets" (+253%), che esplicita il crescente numero di attacchi compiuti in parallelo dallo stesso attaccante contro numerose organizzazioni appartenenti a categorie differenti. Seguono i settori "Research/Education" (+138%) e Infrastrutture Critiche (+23%) seguite da "Banking/ Finance" (+12%). Da segnalare la crescita (+16%) dei crimini informatici verso la categoria "Ricettività" (hotel, ristoranti, residence e collettività), che hanno tipicamente la finalità di colpirne i clienti finali.

Gli attacchi nel primo semestre 2017: le tecniche d'attacco

Gli attacchi sferrati con malware comune sono stati nel primo semestre 2017 il 36% del totale, in crescita del 86% rispetto al secondo semestre 2016. Scendendo nel dettaglio, il 27% degli attacchi realizzati tramite malware nel primo semestre dell'anno è stato compiuto utilizzando ransomware; il 20% tramite malware specifico per piattaforme mobile (7% iOS, 13% Android), fenomeno in rapida crescita. Questo trend preoccupa molto gli esperti Clusit, che evidenziano come la maggior parte di questi sistemi non sia provvista di alcuna protezione.

Appare evidente dall'analisi delle tecniche di attacco la sempre maggiore facilità nel reperire strumenti offensivi anche molto sofisticati sul mercato nero e la loro crescente accessibilità in termini economici, secondo logiche prettamente "industriali".

Crescono nel primo semestre dell'anno significativamente rispetto agli ultimi sei mesi del 2016 "Phishing e Social Engineering" (+85%).

Gli attacchi nel primo semestre 2017: la distribuzione delle vittime

Come in passato, anche nel primo semestre di quest'anno è il settore governativo a mantenere il primo posto assoluto nell'elenco delle vittime, con un quinto degli attacchi (19%), insieme alla categoria "Multiple Targets" (19%). Segue la categoria "Entertainment/News" (12%), poi "Research/Education" (9%), "Online Services/Cloud" (9%) e "Banking/Finance" (8%).

A livello geografico, sono in aumento gli attacchi verso realtà basate in Europa (dal 16% del secondo semestre 2016 al 19% del primo semestre 2017); crescono significativamente anche quelli verso realtà multinazionali (dall'11% al 22%), ad indicare la tendenza dei cyber criminali a colpire bersagli sempre più importanti, di natura transnazionale.

Rispetto al secondo semestre 2016, nel primo semestre 2017 diminuiscono invece le vittime di area americana (dal 55% al 47%) ed asiatica (dal 16% al 10%).

Tratto da " CLUSIT: cresce l'industria del cybercrime nei primi sei mesi dell'anno" (pdf)

---

[1] Dal conteggio degli attacchi gravi del primo semestre 2017 sono stati esclusi moltissimi "incidenti minori", così da evitare il confronto disomogeneo tra quelli che hanno causato la perdita ingenti somme di denaro e/o quantità di informazioni e attacchi di lieve entità o verso un numero limitato di soggetti. Anche questo genere di attacchi è tuttavia in rapida crescita. Gli esperti Clusit evidenziano inoltre che il numero di attacchi informatici gravi è calcolato su un campione necessariamente limitato, pur significativo, poiché la maggior parte delle aggressioni non divengono mai di dominio pubblico (mancando ancora una normativa che renda obbligatorio darne notifica), o lo diventano ad anni di distanza.

Questo articolo è pubblicato sotto una Licenza Creative Commons.

---

www.puntosicuro.it