CLUSIT: il 2016 Annus Horribilis della sicurezza cyber

Cresce del 117% nell'ultimo anno la "guerra delle informazioni";
a quattro cifre l'incremento degli attacchi compiuti
con tecniche di Phishing /Social Engineering (+1.166%).

La sanità è il settore più colpito (+102%), con GdO (+70%), Finance /Banche (+64%) e Infrastrutture Critiche (+15%).
Aumentano gli attacchi verso Europa e Asia.

#RapportoClusit

Milano, 22 febbraio 2017 – Sono in deciso aumento i crimini informatici a livello globale: **nel 2016 sono stati 1.050 gli incidenti noti classificati come gravi**, quindi con impatto significativo per le vittime in termini di danno economico, alla reputazione e diffusione di dati sensibili. Contestualmente, è sempre più elevato l'impatto sulla vita delle istituzioni, delle imprese e dei privati cittadini che tali crimini subiscono: si apre così l'undicesima edizione del **Rapporto CLUSIT 2017 sulla sicurezza ICT in Italia**. Frutto del lavoro di oltre un centinaio di professionisti appartenenti a Clusit, l'Associazione Italiana per la Sicurezza Informatica, da sei anni il Rapporto 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.

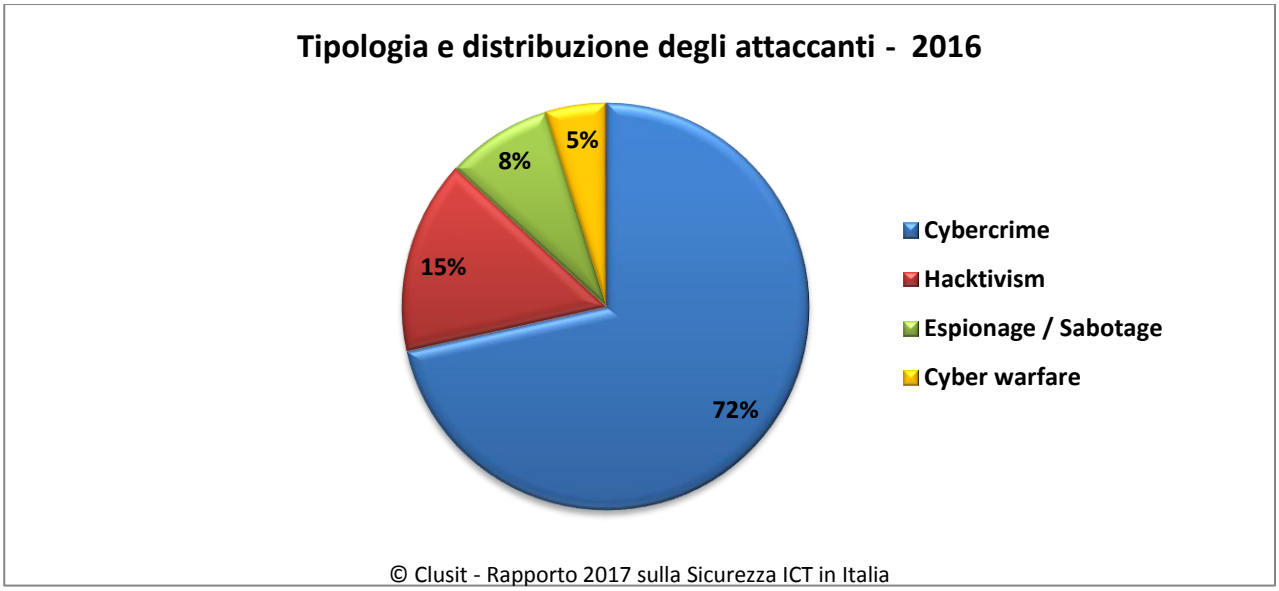
I dati illustrati oggi a Milano in anteprima - l'edizione integrale del Rapporto sarà infatti presentata al pubblico il 14 marzo in apertura di Security Summit - mostrano chiaramente che **il 2016 è stato l'anno peggiore di sempre in termini di evoluzione delle minacce "cyber" e del relativo impatto**.

Il Cybercrime - ovvero i reati compiuti con l'obiettivo di estorcere denaro alle vittime, o di sottrarre informazioni per ricavarne denaro - è causa del 72% degli attacchi verificatisi nel 2016 a livello globale, confermando un trend di crescita costante dal 2011, quando tale tipologia di attacchi reati si attestava al 36% del totale.

"Nel 2016 la cyber-insicurezza globalmente ha raggiunto livelli inimmaginabili ancora pochi anni fa. E' particolarmente evidente dai dati che presentiamo oggi che negli ultimi tre anni il divario tra percezione dei rischi cyber e la realtà, e la forbice tra la gravità di questi rischi e l'efficacia delle contromisure poste in essere si sono ulteriormente allargati", afferma Andrea Zapparoli Manzoni, tra gli autori del Rapporto Clusit 2017. "*Nella situazione attuale, infatti, i rischi cyber non solo stanno crescendo sensibilmente, ma continuano a non essere gestiti in modo efficace, ovvero sono fuori controllo. In quanto tali, per la stessa definizione di rischio, devono essere considerati inaccettabili. Siamo giunti ad una situazione da 'allarme rosso', conclude Zapparoli Manzoni.*

Gli attacchi: chi viene colpito e perché

In particolare, gli attacchi gravi compiuti per finalità di **Cybercrime** sono in aumento del **9,8%**, mentre crescono a tre cifre quelli riferibili ad attività di **Cyber Warfare** – la "guerra delle informazioni" (**+117%**). Appaiono invece in lieve calo gli attacchi con finalità di "**Cyber Espionage**" (**-8%**) **e Hacktivism** (**-23%**). In termini assoluti **Cybercrime e Cyber Warfare fanno registrare il numero di attacchi più elevato degli ultimi 6 anni**.



La maggior crescita percentuale di attacchi gravi nel 2016 è avvenuta nel settore della **sanità** (**+102%**), nella **Grande Distribuzione Organizzata** (**+70%**) e in ambito **Banking /Finance** (**+64%**). Seguono le **Infrastrutture Critiche**, dove gli attacchi gravi sono aumentati del **15%** rispetto allo scorso anno.

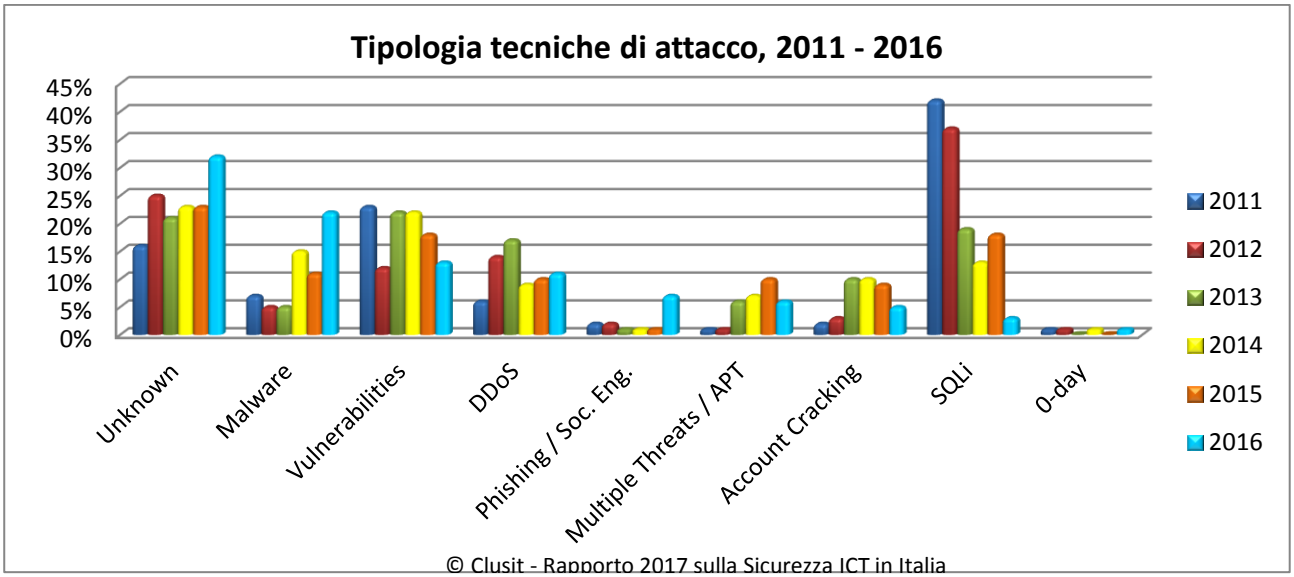
A livello geografico, crescono nel secondo semestre 2016 gli attacchi verso realtà basate in Europa (dal 13% al 16%) e in Asia (dal 15% al 16%), mentre sembrano diminuire leggermente le vittime negli Stati Uniti.
La categoria di organizzazioni target identificata come "Multinational" rimane tuttavia sostanzialmente stabile (11%), confermando la tendenza a colpire bersagli sempre più importanti, di natura transnazionale.

Le tecniche d'attacco

Il 32% degli attacchi viene sferrato con **tecniche sconosciute, in aumento del 45%** rispetto al 2015, principalmente a causa della scarsità di informazioni precise in merito tra le fonti di pubblico dominio.
A preoccupare maggiormente gli esperti del Clusit, tuttavia, è la **crescita a quattro cifre** (**+1.166%**) **degli attacchi compiuti con tecniche di Phishing /Social Engineering,** ovvero mirati a "colpire la mente" delle vittime, inducendole a fare passi falsi che poi rendono possibile l'attacco informatico vero e proprio.

Ma cresce anche il "**Malware**" comune (**+116%**) - tra cui vi sono i cosiddetti "**Ransomware**" – non più solo per compiere attacchi di piccola entità, tipicamente realizzati da cyber criminali poco sofisticati, dediti a generare i propri "margini" su grandissimi numeri, ma anche contro bersagli importanti e con impatti significativi.

In aumento anche gli attacchi compiuti con DDoS (+13%) e l'utilizzo di vulnerabilità "0-day", (+ 333%, anche se in questo caso il numero di incidenti noti è molto limitato).



A livello globale **la somma delle tecniche di attacco più banali** (SQLi, DDoS, Vulnerabilità note, phishing, malware "semplice") **rappresenta il 56% del totale**: questo dato è uno dei più allarmanti, secondo gli esperti del Clusit, poiché rende evidente la facilità di azione dei cybercriminali e la possibilità di compiere attacchi con mezzi esigui e bassi costi.

2016, i 10 attacchi più significativi a livello globale

Come di consueto, gli esperti Clusit descrivono inoltre **i dieci attacchi più significativi** verificatisi nel corso del 2016, particolarmente rappresentativi dello scenario globale e delle tendenze in atto. Per la prima volta in questa "classifica" rientra anche un incidente avvenuto nel nostro Paese: l'attacco di matrice state-sponsored (forse originato dalla Russia), subìto dalla Farnesina nella primavera 2016, che avrebbe provocato la compromissione di alcuni sistemi non classificati.

Le novità e i "FOCUS ON" del Rapporto Clusit 2017

Tra le novità del Rapporto Clusit 2017, tre capitoli dedicati settori che emergono come particolarmente "critici" in termini di sicurezza ICT in Italia: **Finance**, **Pubblica Amministrazione**, **Sanità**. All'**evoluzione delle normative europee** vengono inoltre dedicati quest'anno cinque contributi specifici, a cura di aziende ed esperti del settore.

I "FOCUS ON" prevedono invece approfondimenti relativi a tematiche particolarmente attuali: dagli "**Attacchi Ransomware in Italia**", agli "**Attacchi e difese sulle infrastrutture Private e Hybrid Cloud**", al "**Cyber Risk Management**", alle "**Sfide relative ai captatori informatici, tra proposte**

legislative e rischi di sicurezza", al "**Voto elettronico: potenzialità e rischi lungo la strada della democrazia elettronica**".

I contributi Fastweb, Akamai e IDC Italia

Il Rapporto Clusit 2017 contiene i dati relativi agli attacchi rilevati dal Security Operations Center (SOC) di **Fastweb**, che ha analizzato la situazione italiana in materia di cyber-crime e incidenti informatici sulla base di oltre 16 milioni di eventi di sicurezza accaduti nel 2016. I dati che l'azienda ha condiviso con Clusit a livello di aggregazione statistica (anonimizzati per proteggere la privacy e la sicurezza dei propri clienti), mostrano la diffusione sempre più significativa di varie tipologie di malware nel nostro Paese, a cui nel 2016 va ricondotto il 97% degli attacchi complessivi. Nel Rapporto Clusit 2017 Fastweb evidenzia inoltre l'incremento degli attacchi legati alle piattaforme VOIP volti a Social Engineering e intercettazione, a possibili interruzioni di servizio (DoS e DDoS) e Service Abuse, dove l'infrastruttura della vittima viene utilizzata per generare traffico verso numerazioni a tariffazione speciale. Nel 2016 gli attacchi alle piattaforme VOIP costituiscono il 99% delle frodi telefoniche complessive; i dati - analizzati dal Dipartimento di Fraud Management della Direzione Security di Fastweb - mostrano tuttavia una diminuzione numerica degli episodi rispetto all'anno precedente, a fronte di una quantificazione economica pressoché costante (di poco inferiore a 500.000 euro). Diminuisce percentualmente anche il numero di frodi basate su tecnologia TDM rispetto al totale (meno dell'1% nel 2016, a fronte di valori attorno al 6% nel 2015).

L'analisi degli attacchi all'interno del Rapporto CLUSIT include inoltre il "Rapporto 2016 sullo stato di Internet e analisi globale degli attacchi DDoS e applicativi Web", a cura di **Akamai**, che evidenzia il notevole incremento della dimensione degli attacchi avvenuti nel 2016: nei 12 mesi, infatti, gli attacchi DDoS superiori ai 100 Gbps sono aumentati del 140% rispetto all'anno precedente.

A seguire, le rilevazioni del **CERT Nazionale** e del **CERT-PA** per l'anno 2016.

Anche il capitolo inedito di **IDC Italia** relativo a "Il mercato italiano della Sicurezza IT" contribuisce ad arricchire il Rapporto Clusit 2017. La società di ricerca stima che nel 2016 il valore del mercato del software per la Sicurezza IT (nelle aree della Web Security, del Security & Vulnerability Management, della Network Security, dell'Identity & Access Management e dell'Endpoint Security) abbia superato i 300 milioni di euro. Il mercato delle Appliances per la Sicurezza IT (nelle cinque aree principali VPN, Firewall, IDP, Unified Threat Management, Content) è stato caratterizzato nel 2016 da un valore complessivo sotto i 200 milioni di euro; i servizi per la Sicurezza IT (basata sulla ripartizione tradizionale tra IT Consulting e System Integration/ Implementation) rappresentano una parte essenziale del settore, per cui si prevede il traguardo dei 600 milioni di euro solo dopo il 2019.

Il Rapporto CLUSIT 2016 sarà presentato al pubblico il prossimo 14 marzo alle 9.15 in apertura di Security Summit presso Atahotel Expo Fiera di Milano.

Al sito securitysummit.it è possibile consultare il programma dettagliato del convegno, che quest'anno propone momenti di riflessione dedicati al cinema, alla musica, all'arte come punto di incontro tra Innovazione Tecnologica e Sicurezza Informatica, con l'obiettivo di promuovere la cultura della sicurezza a livello globale.

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

Security Summit è organizzato da:
Clusit - i cui soci rappresentano oltre 500 aziende e organizzazioni - è la principale associazione italiana nel campo della sicurezza informatica. Il 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 svariate 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 alla stampa si prega di contattare l'Ufficio Stampa Security Summit:
Daniela Sarti
Tel. 335 459432
email: press@securitysummit.it