



## Rapporto CLUSIT 2016: sicurezza informatica oggi a livelli di rischio inaccettabile

**Il Cybercrime cresce del 30% nell'ultimo anno e aumentano del 39% gli attacchi con finalità di spionaggio.**

**Anche le infrastrutture critiche nel mirino dei cyber-criminali, con un incremento degli attacchi pari al 154%.**

**Inarrestabile la diffusione dei ransomware, che generano vere e proprie campagne di estorsione informatica**

**Gli esperti del CLUSIT – l'Associazione per la Sicurezza Informatica in Italia – delineano il quadro aggiornato della situazione globale e delle prospettive della sicurezza informatica sulla base dei più importanti eventi del 2015**

**#SECURITYSUMMIT #RAPPORTOCLUSIT**

Milano, 1° marzo 2016 – Governi, istituzioni, aziende e privati cittadini sempre più a rischio “cyber”: i crimini informatici nel nostro Paese e nel mondo fanno registrare il numero di attacchi gravi più elevato degli ultimi 5 anni: **1.012** solo quelli di dominio pubblico nel 2015 (contro gli 873 del 2014).

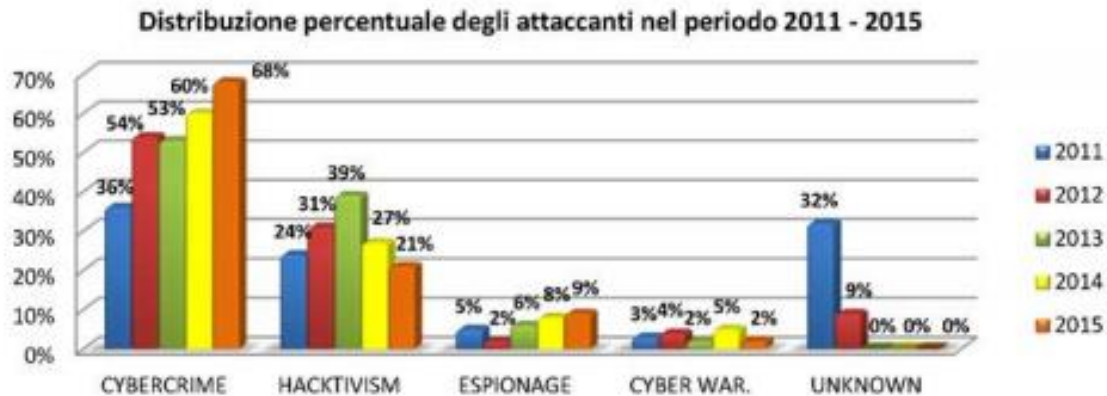
Una crescita a doppia cifra che definisce il rischio “cyber” attuale come inaccettabile secondo gli esperti del CLUSIT - l'Associazione Italiana per la Sicurezza Informatica - che presenterà al [Security Summit di Milano](#) il prossimo 15 marzo l'atteso **Rapporto CLUSIT 2016**.

Frutto del lavoro di oltre un centinaio di professionisti, il Rapporto evidenzia la crescita inarrestabile degli attacchi compiuti con finalità criminali: il **Cybercrime** segna infatti un **+ 30%** nel 2015 rispetto all'anno precedente.

Nel 2015 è esplosa in maniera dirompente nel nostro Paese la diffusione - già segnalata come importante nell'anno precedente - dei **ransomware** e, in particolare, dei più insidiosi **crypto-ransomware**: si tratta di codici che criptano i documenti presenti nei sistemi degli utenti finali (aziende, ma anche comuni cittadini), chiedendo il pagamento di un vero e proprio riscatto per riottenerli in chiaro. Si ha già evidenza dell'esistenza di gruppi criminali che gestiscono servizi di “ransomware as a service”, mettendoli a disposizione per vere e proprie campagne di **estorsione informatica**.

A livello di attività criminale, è notevole anche il tasso di incremento annuo delle attività di “Espionage”, pari al 39%; a questo proposito, gli esperti del CLUSIT notano inoltre che proprio sul settore governativo si è concentrato nel 2015 un quinto degli attacchi noti a livello mondiale.

**Nel 2015 Cybercrime ed Espionage fanno registrare il numero di attacchi più elevato in valore assoluto degli ultimi 5 anni.**



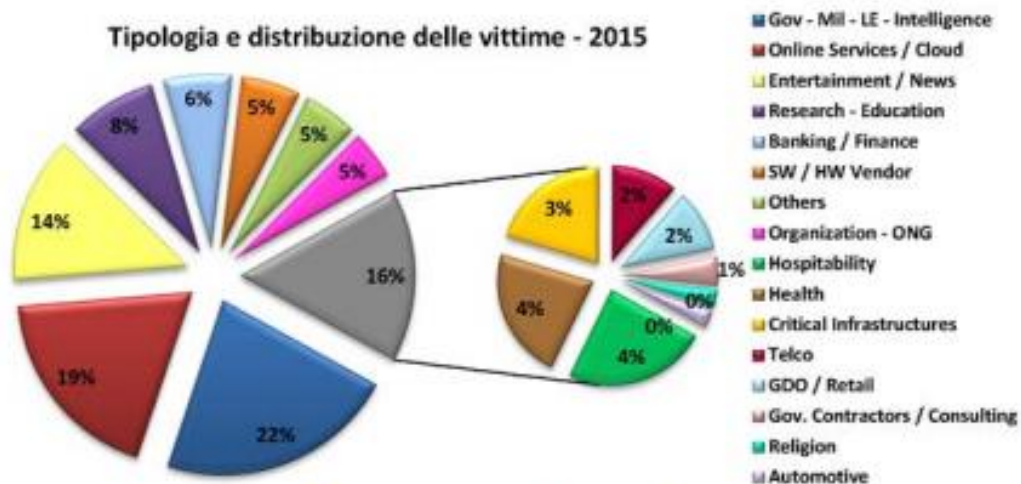
© Clusit - Rapporto 2016 sulla Sicurezza ICT in Italia

Il Rapporto CLUSIT 2016 evidenzia inoltre un'impennata delle aggressioni note alle **infrastrutture critiche**. Pur rappresentando soltanto il 3% degli attacchi a livello globale, nel 2015 l'incremento in questo comparto è stato del **154%** rispetto al 2014.

I **servizi Cloud** – categoria che comprende i principali sistemi di Webmail, i Social Network, siti di e-Commerce e piattaforme Cloud pubbliche - registrano un aumento dell'**81%** rispetto al 2014 e il più elevato valore assoluto ad oggi consuntivato.

Colpiti in maniera evidente anche i settori dell'**informazione e del gioco**: media online, piattaforme di blogging e gaming nel 2015 hanno subito un incremento degli attacchi pari al **79%** rispetto all'anno precedente.

Tra i settori più bersagliati anche l'**Automotive**, in cui gli attacchi nel 2015 sono stati circa il **67%** in più rispetto ai dodici mesi precedenti. Nel mirino dei criminali informatici ci sono inoltre il settore **Ricerca ed Educazione**, in cui si è registrato un incremento degli attacchi pari al **50%**, per lo più con finalità di spionaggio. Nel 2015 compare per la prima volta nell'analisi dei ricercatori del CLUSIT il settore dell'**Ospitalità** – organizzazione alberghiere, ristoranti, residence e collettività – in cui gli attacchi vengono tipicamente sferrati per colpirne gli utenti.



© Clusit - Rapporto 2016 sulla Sicurezza ICT in Italia

Campanello d'allarme del CLUSIT anche per quanto riguarda le **tecniche d'attacco**: il 57% degli attacchi gravi nel 2015 compiuti contro primarie organizzazioni pubbliche e private è stato sferrato con tecniche tra le più banali - SQLi, DDoS, vulnerabilità note, malware semplice. Secondo gli autori del Rapporto CLUSIT 2016 si tratta di una chiara indicazione della inadeguata capacità di difesa e della pressoché sconfinata libertà di azione delle organizzazioni criminali.

**La crescita complessiva degli attacchi cyber rende evidente che i rischi della sicurezza informatica non sono più controllabili. In quanto tali, secondo gli esperti CLUSIT, devono essere quindi considerati inaccettabili.**

*“L'insicurezza cibernetica è di fatto ormai un problema di ‘salute pubblica’, come una pandemia, che come tale va indirizzato e gestito, con il coinvolgimento e la collaborazione di tutti”,* afferma Paolo Giudice, segretario generale CLUSIT. *“In particolare, negli ultimi tre anni, il divario tra percezione dei rischi cyber e realtà e tra la gravità di questi rischi e l'efficacia delle contromisure poste in essere si è pericolosamente ampliato. Mitigare gli inevitabili impatti di questa pandemia è l'obiettivo primario al quale si deve tendere”,* conclude Giudice.

Il Rapporto CLUSIT presenta quest'anno anche un interessante capitolo relativo all'ecosistema criminale nel **Dark Web**, insieme di contenuti ospitati in siti web con indirizzo IP nascosto, ma accessibili a chiunque lo conosca. Utilizzata per lo più per effettuare transazioni relative alla vendita di sostanze stupefacenti ed a servizi/prodotti per la realizzazione di frodi finanziarie, si stima che **i 35 principali mercati illeciti all'interno del Dark Web registrino un volume di affari tra \$300,000 e \$500,000 al giorno**. Altra piaga del Dark Web sono la **pedo pornografia** (36% dei siti su Dark Web analizzati dagli esperti) e l'utilizzo da parte di **organizzazioni terroristiche quali ISIS ed Al Qaeda** per attività di propaganda.

Il Rapporto CLUSIT 2016 si avvale anche quest'anno del contributo di **Fastweb** sulla **situazione italiana in materia di cyber-crime ed incidenti informatici**. In particolare, l'Azienda ha analizzato i dati relativi agli attacchi rilevati dal proprio Security Operations Center (SOC): oltre 8 milioni di eventi di sicurezza avvenuti nel 2015, ovvero una base dati più ampia di circa il 60% rispetto a quella dell'anno precedente. I dati, preventivamente aggregati ed anonimizzati in maniera automatica per proteggere la privacy e la sicurezza dei clienti e della stessa Fastweb, mostrano che ben il **98,19% delle minacce è da ricondursi alla diffusione di malware**, software malevolo che si installa volontariamente perché l'utente clicca su un link malevolo, o involontariamente, sfruttando vulnerabilità dell'applicativo o del sistema operativo. Una volta avviato, il malware è in grado di ottenere informazioni sensibili, monitorare le azioni dell'utente, codificare i dati con l'intento di estorcere denaro e/o partecipazione alla formazione di botnet che, addirittura, possono essere messe in vendita per effettuare campagne di spam, attacchi di tipo DDoS o altro genere di operazioni malevole.

I dati rilevati dal SOC di Fastweb evidenziano inoltre un incremento notevole degli attacchi verso l'infrastruttura **VOIP** di aziende, tipicamente di piccole dimensioni, verso le quali sono state attuate **frodi telefoniche** volte a generare traffico illecito verso direttrici a tariffazione speciale, per un valore complessivo nell'anno di oltre 429 mila euro.

L'analisi degli attacchi contenuta all'interno del Rapporto CLUSIT è poi completata dal **“Rapporto 2015 sullo stato di Internet ed analisi globale degli attacchi DDoS”**, a cura di Akamai e dal contributo di IBM **“Alcuni elementi sul cyber-crime in ambito finanziario con focus sull'Europa”**. Di particolare rilievo, inoltre, le segnalazioni del **CERT Nazionale** e del **CERT-PA**.

Ad arricchire il Rapporto CLUSIT 2016 concorre inoltre il capitolo inedito di **IDC Italia** su **“Il mercato italiano della Sicurezza IT”**, che attualmente vale circa 850 milioni di euro, comprendendo le principali declinazioni commerciali -dal software, ai dispositivi hardware, fino ai servizi - e per la quale si prevede un tasso medio di crescita al 2018 attorno al 2%. IDC analizza inoltre il passaggio della Sicurezza IT da priorità meramente tecnica a priorità di business, con una interessante analisi sul fronte organizzativo e mercato del lavoro.

Un capitolo del Rapporto CLUSIT è interamente dedicato a **Expo Milano 2015** e alla gestione della sicurezza e degli attacchi avvenuti durante l'Esposizione Universale, con approfondite analisi di **Cisco Systems**, **Poste Italiane** e del **C.N.A.I.P.I.C.** (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche, nucleo speciale in seno alla **Polizia Postale**).

### **I “FOCUS ON” del Rapporto CLUSIT 2016**

Come ogni anno, all'interno del Rapporto CLUSIT vengono delineati da parte dei maggiori esperti italiani specifici scenari tematici, con l'obiettivo di fornire una visione concreta anche sulla gestione della sicurezza informatica, delineando un percorso pratico per la definizione di policy aziendali. Per il 2016 i “FOCUS ON” prevedono contributi relativi alle **coperture assicurative** e al trasferimento del rischio informatico; alla **sicurezza nel mobile** e nell'**e-commerce**; al **furto di credenziali** in ambito aziendale; ai nuovi modelli di **prevenzione** e di **gestione degli incidenti**; alle sfide nel campo della **robotica**; della sicurezza del **Database**.

**Il Rapporto CLUSIT 2016 sarà presentato al pubblico il prossimo 15 marzo alle 9.30 in apertura di Security Summit**, presso [Atahotel Expo Fiera](#) di Milano.

A questo link il programma dettagliato e la possibilità di registrarsi gratuitamente: <https://www.securitysummit.it/milano-2016/>

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

**Security Summit è organizzato da CLUSIT**, la principale associazione italiana nell'ambito della sicurezza informatica, i cui soci rappresentano oltre 500 aziende e organizzazioni. 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](http://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](http://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](mailto:press@securitysummit.it)