Ottobre è il mese europeo dedicato alla sicurezza informatica (European Cyber Security Month - ECSM), campagna UE volta a promuovere la consapevolezza dei rischi informatici

---

CLUSIT: cybercrime come pandemia, in crescita del 9% nei primi sei mesi del 2016 rispetto al secondo semestre 2015

Presentata oggi al Security Summit di Verona la decima edizione del Rapporto CLUSIT: il mondo di fronte a un nuovo paradigma di cyber security; pensare in termini di "sicurezza informatica" non è più sufficiente.

Crescono del 144% gli attacchi nel settore della Sanità negli ultimi sei mesi; a quattro cifre l'incremento di Phishing e Social Engineering (+ 1500%); Malware e Ransomware a + 129%.

#SecuritySummit #RapportoClusit #CyberSecMonth

Milano, 5 ottobre 2016 – La progressiva digitalizzazione globale e la necessità di iper-connessione espongono sempre più la nostra società agli attacchi cyber: nei primi sei mesi dell'anno, infatti, sono cresciute del 9% le attività compiute con finalità criminale rispetto al semestre precedente. Il dato è evidenziato nella **decima edizione del Rapporto CLUSIT**, che fornisce il quadro aggiornato ed esaustivo della situazione globale della sicurezza informatica.

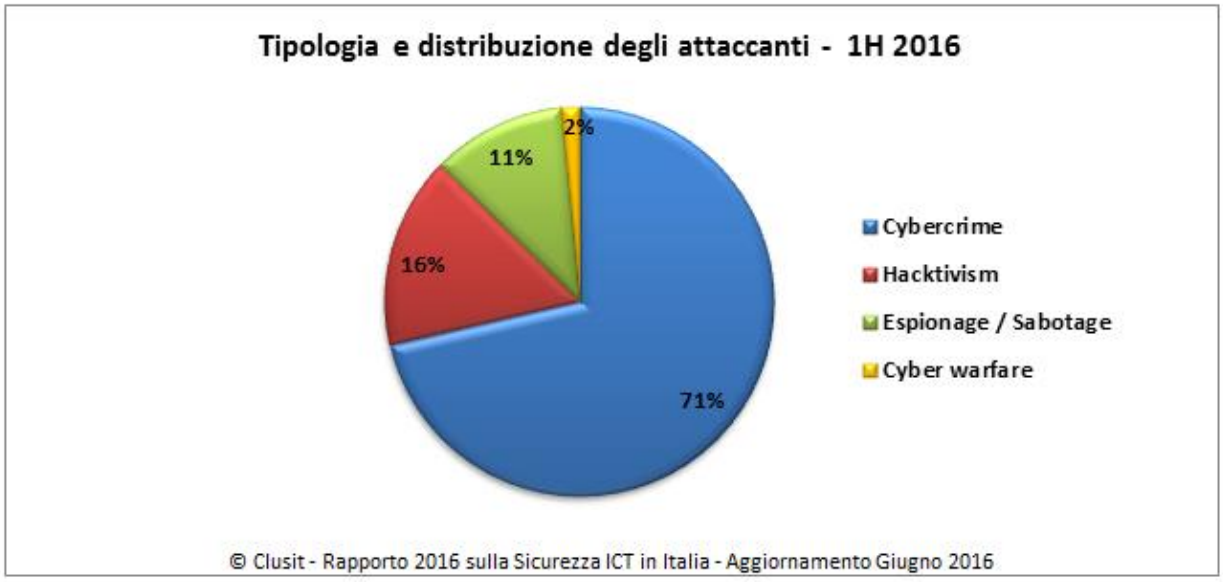
Presentato questa mattina a Verona in apertura di Security Summit, il più importante convegno italiano dedicato alla sicurezza delle informazioni delle reti e dei sistemi informatici, il Rapporto si avvale della collaborazione di oltre cento professionisti impegnati in aziende private e pubbliche e di docenti universitari, che mettono a fattor comune le proprie competenze.

Tra le evidenze, il **cybercrime** si riconferma - secondo un trend in costante ed inesorabile crescita dal 2014 - **prima causa di attacchi gravi a livello globale**, attestandosi al **71%** del totale delle cause di attacco nel semestre appena concluso.
Per lo stesso periodo, nel Rapporto Clusit emerge l'incremento delle aggressioni riferibile alla categoria "**espionage**" (anche in questo caso +9%).

In termini assoluti, nel primo semestre 2016 gli attacchi gravi ascrivibili al Cybercrime e all'Espionage fanno registrare i livelli più elevati degli ultimi sei semestri. Ad aumentare sono soprattutto gli attacchi realizzati con tecniche banali: rispetto alla seconda parte del 2015 tornano infatti ad aumentare i Malware comuni - in particolare i **Ransomware (+ 129%)** - sempre più diffusi e non solo per compiere attacchi "spiccioli", tipicamente realizzati da cyber criminali poco sofisticati, dediti a generare i propri "margini" su grandissimi numeri. A **quattro cifre l'incremento di Phishing e Social Engineering (+ 1500%).**

Gli esperti del Clusit sottolineano però si tratta soltanto della "punta dell'iceberg": il campione su cui si basano le loro analisi è infatti inevitabilmente limitato agli incidenti più eclatanti poiché –

mancando una normativa che ne renda obbligatoria la denuncia[1] (salvo in alcuni ristretti settori regolamentati) - la maggior parte delle aggressioni non diviene mai di dominio pubblico. Le conseguenze più gravi, inoltre, spesso si evidenziano ad anni di distanza. Nel campione di incidenti presi in considerazione nel Rapporto non sono inoltre incluse le attività cybercriminali "spicciole", dal 2015 diffuse in maniera endemica. E' quindi lecito supporre che in generale la crescita di Cybercrime ed Espionage nei primi sei mesi del 2016 sia stata ancora maggiore di quanto effettivamente emerga dal campione considerato.



Il Rapporto Clusit analizza in primo luogo gli **scenari macro-economici e sociologici**: l'Italia ha certamente intrapreso a partire dal 2013 alcune valide iniziative per rafforzare le difese cyber: dal "*Quadro strategico nazionale per la sicurezza dello spazio cibernetico*"[2], al "*Piano nazionale per la protezione cibernetica e la sicurezza informatica*"[3]. Tuttavia, l'insicurezza cibernetica a livello globale - e di pari passo anche in Italia - è cresciuta in modo significativo e le tipologie di aggressori si sono moltiplicate - dal braccio "digitale" dell'Islamic State, ad altri gruppi di spionaggio e information warfare - e le perdite economiche sono aumentate di 4 volte[4].
L'impiego spesso congiunto delle nuove tecnologie - in particolare Social Media, Cloud, Mobile ed Internet of Things - sta contestualmente dando luogo ad una rivoluzione rapidissima dei processi produttivi, degli stili di vita e dei rapporti socio-economici.

Registriamo un incremento della superficie di attacco esposta dalla nostra società digitale, oggi iper-connessa, anche in conseguenza della massiccia adozione di nuove tecnologie facili e a basso costo, che sono intrinsecamente poco o per nulla sicure se confrontate con le capacità di nuocere degli avversari", afferma Andrea Zapparoli Manzoni, membro del Consiglio Direttivo Clusit. "*Tutto questo a fronte di un ampliamento del divario tra percezione dei rischi cyber e realtà:*

[1] https://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn
[2] http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/quadro-strategico-nazionale-cyber_0.pdf
[3] https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/la-cyber-strategy-italiana.html
[4] http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/

nell'ultimo anno la forbice tra la gravità di questi rischi e l'efficacia delle contromisure poste in essere si è infatti ulteriormente allargata", conclude Zapparoli Manzoni.

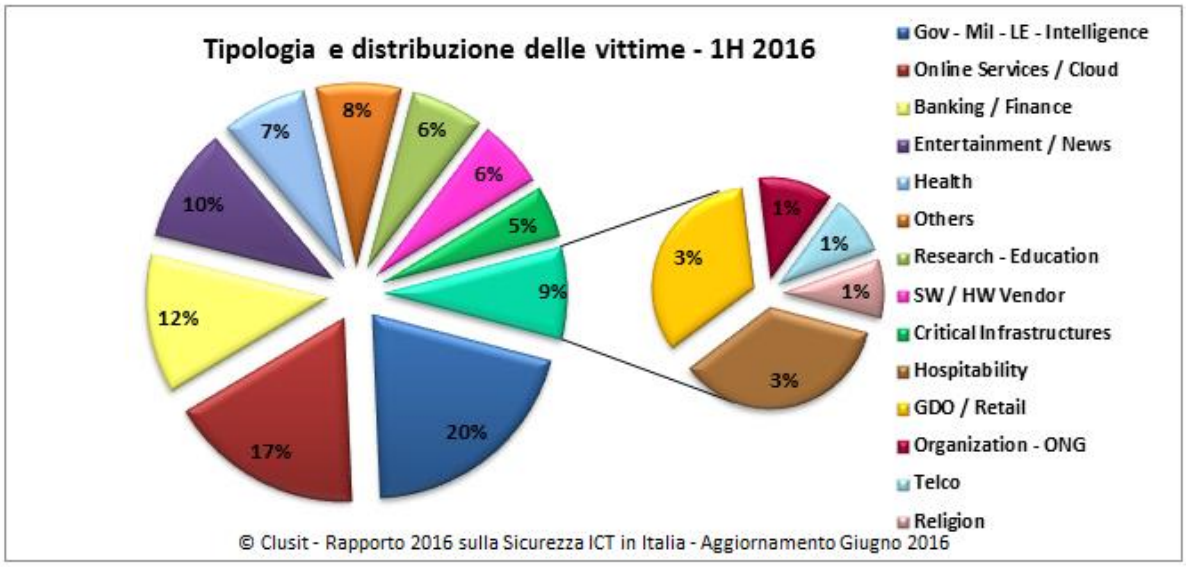
"*Possiamo dire di essere di fronte ad un nuovo paradigma di Cyber Security, che indica un gruppo di attività e competenze multidisciplinari, complesse e sofisticate, molte delle quali non informatiche, che sono oggettivamente di difficile integrazione con le prassi esistenti di gestione dell'ICT e di allocazione dei budget relativi*", afferma Paolo Giudice, Segretario Generale Clusit. "*In questo sta la debolezza delle contromisure messe fino ad oggi in campo da aziende e istituzioni, così come da privati cittadini, che nella maggior parte dei casi si limitano a prevedere un approccio puramente tecnico/informatico*", conclude Giudice.

CHI SUBISCE?

Nel primo semestre 2016 il settore della **Sanità** ha subito l'incremento percentuale più elevato di attacchi gravi (**+ 144%**), con finalità di furto di informazioni ed estorsione tramite Ransomware. Seguono il settore bancario e finanziario (**+93%**), che nel 2016 fa registrare in assoluto il maggior numero di attacchi degli ultimi 11 semestri; le infrastrutture critiche (**+84%**) e la grande distribuzione/commercio (**+ 17%**).

Percentuali positive elevate (+77%) anche per l'ampia categoria "Altri Settori", che raggruppa tutte le organizzazioni non puntualmente classificabili, a dimostrazione del fatto che ormai i bersagli sono allargati.

Sono sostanzialmente stabili gli attacchi verso i settori "Gov" (tipicamente con finalità di Espionage o di Hacktivism), "Entertainment/News", "Online Services/Cloud" (ovvero i principali gestori di Webmail, i Social Network, i siti di e-Commerce e piattaforme Cloud pubbliche) e "Research/Education".



Guardando alla **distribuzione delle vittime**, mantiene il primo posto – come nel 2015 – il "**Government**", che da solo rappresenta il **20%** dei settori presi di mira dai crimini informatici. I servizi "**Online/Cloud**" si confermano al secondo posto (**17%**), e questo evidenzia la maggiore concentrazione degli attacchi gravi verso i settori più esposti e più remunerativi.

A **livello geografico** sono sempre gli Stati Uniti ad essere i più colpiti, con il 55% degli attacchi a livello globale (in crescita di 8 punti percentuali rispetto al 2015). Seguono gli stati asiatici, con il 15% degli attacchi, che per la prima volta dal 2011 superano gli attacchi contro realtà europee (pari al 12% del globale).
In aumento dal 9 al 12% la categoria "Multinational", ad indicare la tendenza a colpire bersagli di dimensioni sempre più importanti e di natura transnazionale.

QUALE DIFESA?
Gli esperti del CLUSIT confermano quale efficace possibilità per fronteggiare le minacce crescenti l'adozione di una logica multidisciplinare di **Cyber Resilience**, in cui convergono compliance e cyber security, governance e risk management, cyber intelligence e crisis management, attività di prevenzione e di reazione rapida, fino alla cooperazione tra pubblico e privato e, più in generale, di condivisione delle informazioni.
Si tratta di comprendere le proprie vulnerabilità e criticità per predisporre un modello di rischio "cyber" accurato e costantemente aggiornato, che consenta di stimare le perdite potenziali al fine di determinare correttamente gli investimenti necessari per la sicurezza. L'Italia è in prima linea, come tanti paesi europei: dinamiche di Cyber Resilience sono state per esempio inserite nell'ambito del Quadro Strategico Nazionale[5].

Per ulteriori informazioni su Security Summit e sul Rapporto Clusit: www.securitysummit.it e **https://www.securitysummit.it/verona-2016/rapporto-clusit/.**
E' possibile richiedere copia digitale del Rapporto CLUSIT 2016 inviando una mail a rapporti@clusit.it.

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.

Per ulteriori informazioni alla stampa:
Ufficio Stampa Security Summit 2016
Daniela Sarti
Tel. 335 459432
email: press@securitysummit.it

5 http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/quadro-strategico-nazionale-cyber_0.pdf