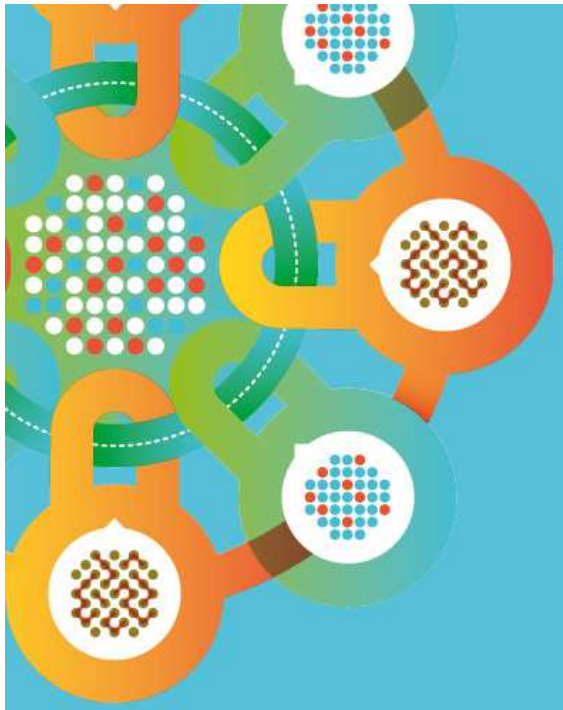


IBM Forum Segrate - Milano

18 settembre: Missione Sicurezza

Identifica e combatti i rischi con la Security Intelligence IBM

Andrea Zapparoli Manzoni

Rapporto Clusit 2012 sulla sicurezza ICT in Italia

Andrea Zapparoli Manzoni

- Founder, CEO, iDialoghi
- Italian OSN (National Security Observatory) Member
- Clusit Lecturer (SCADA, Social Media, Mobile, OSInt, etc)
- ICT Security Author (ROSI, DLP, Social Media, SCADA…)
- Co-author of the first Italian Report on Cybercrime 2012
- Lecturer at the Master in Homeland Security course
- Cybercrime and Cyber Warfare analyst, etc.

Rapporto Clusit sulla Sicurezza ICT in Italia – Prima edizione

https://www.securitysummit.it/page/rapporto_clusit

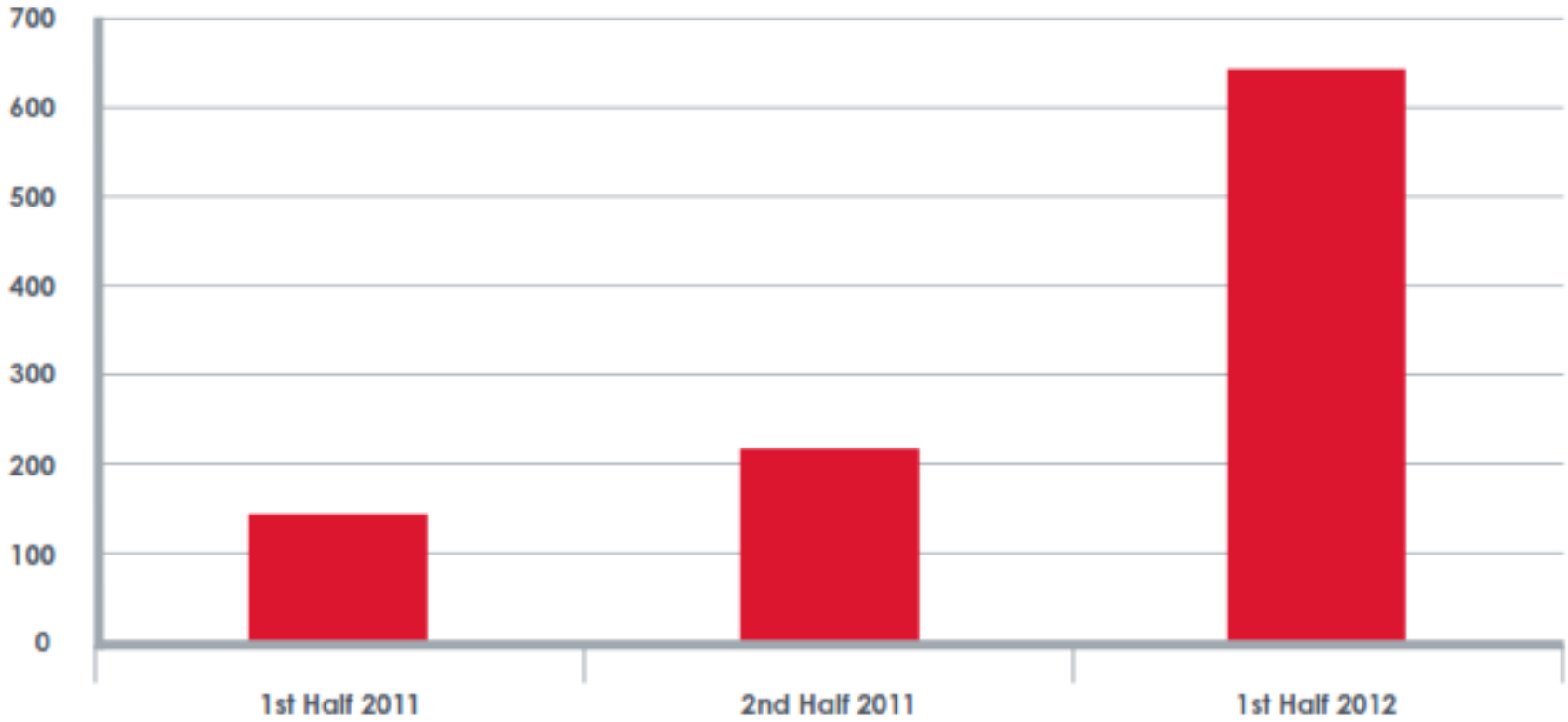
Contenuti

- Panoramica degli eventi (cybercrime e incidenti informatici) più significativi del 2011 e del 2012, verificatisi in Italia e nel mondo, con un'analisi delle tendenze per il 2012 e oltre.

- Analisi del mercato italiano della sicurezza ICT e tendenze degli investimenti delle aziende. Analisi e prospettive del mercato del lavoro nel settore.

- 7 "Focus on": Mobile Security, Social Media Security, Cloud Security, Normative per il trattamento dei dati personali: le novità degli ultimi 12 mesi, Lo stato della Sicurezza ICT nella Pubblica Amministrazione italiana, Protezione di reti e sistemi di controllo in ambito Industriale (e Infrastrutture), Lo stato della sicurezza ICT nella Piccole e Medie Imprese italiane.

La situazione, in una slide

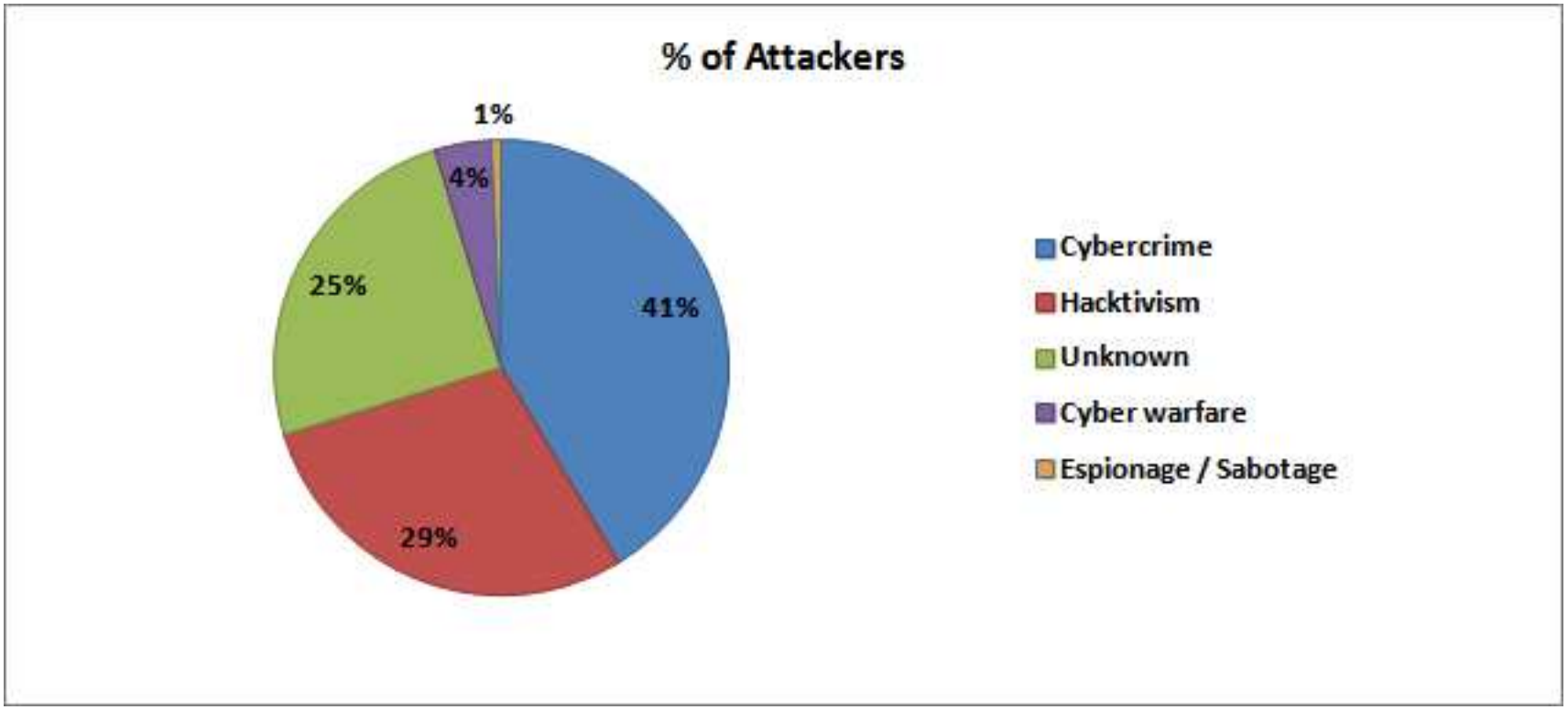


Fonte: Clusit – analisi di 982 attacchi significativi 2011 – 1H 2012

Panoramica cybercrime – Analisi dei principali incidenti a livello internazionale

- La crescita nel numero, nella gravità e nel costo degli attacchi ha assunto nel 2010-11 un andamento **esponenziale**… e il 2012 conferma il trend **(+ 300%** in 6 mesi).
- **Tutti** i settori sono attaccati, non è più un "problema altrui". E' solo questione di tempo.
- Gli Hacktivist, per quanto molto visibili, non sono il problema. E' il **cybercrime transnazionale organizzato** che incassa 10Md $ all'anno producendo danni diretti ed indiretti per quasi 400Md $ (**40:1**)
- Le **organizzazioni** e gli **utenti** (governativi, business, privati) sono del tutto **impreparati** e non si rendono conto della velocità di evoluzione dei fenomeni. NB spam e virus sono preistoria…
- Altri **3 anni** (36 mesi) con questi andamenti e il problema diventerà, molto semplicemente, *intrattabile*.

Chi sono gli attaccanti



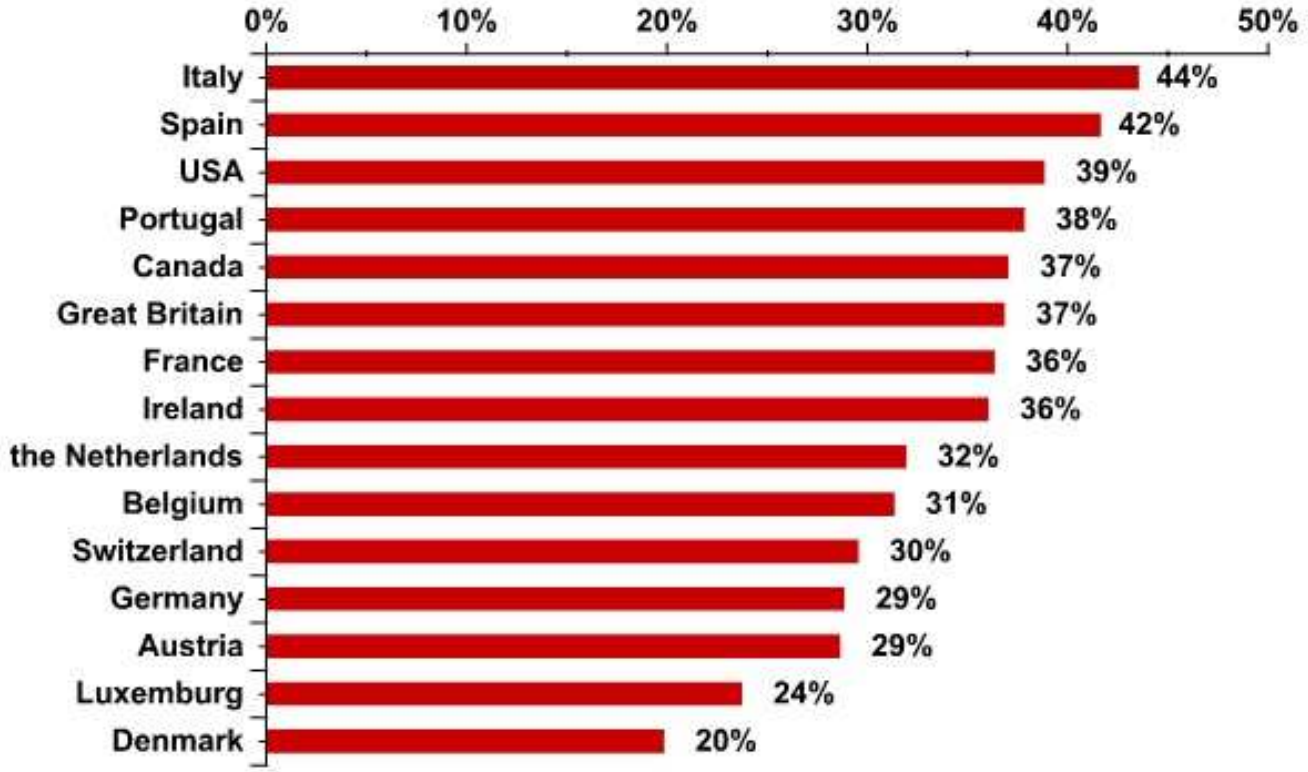
Fonte: Clusit – analisi di 982 attacchi significativi 2011 – 1H 2012

Panoramica cybercrime – Analisi della situazione italiana

- I **navigatori attivi** in Italia sono 25 milioni (dicembre 2011).
- Gli **utenti di Social Network** sono l'87% degli utenti online
- Gli **smartphone** in Italia sono 20 milioni (novembre 2011)
- In un contesto del genere, solo **il 2%** degli Italiani dichiara di avere piena consapevolezza dei rischi informatici e di prendere opportune contromisure… In caso di attacco, **pochissimi** denunciano.
- Mancano i dati, ma per analogia con altri Paesi (dove i dati ci sono) in Italia il **costo** degli incidenti informatici si può valutare in alcuni miliardi di euro / anno (perdite dirette ed indirette).
- Siamo un Paese avanzato, ma **non** abbiamo politiche di ICT Security efficaci (educazione, prevenzione, gestione degli incidenti) e **non** investiamo.

Panoramica cybercrime – Analisi della situazione italiana

- Risultato: nel 2012, *milioni* di italiani saranno **attaccati** e *centinaia di migliaia* (privati ed aziende) saranno **vittime** del cybercrime.



Principali tendenze per il 2012 e oltre

- **Cybercrime** : In mancanza sia di barriere all'ingresso che di forme efficaci di contrasto e disincentivazione, altri gruppi si uniranno certamente a quelli già oggi in attività, facendo aumentare sia il numero dei crimini informatici (ROI > 750% / mese), sia quello dei crimini tradizionali veicolati e/o commessi con l'ausilio di sistemi informatici.
- **Hacktivism** : sempre più di massa, potenzialmente sempre più distruttivo. In particolare aumenteranno attacchi DDoS e leakage di dati riservati.
- **Cyber Espionage**: il più grande trasferimento di ricchezza della storia umana. Attacchi sempre più sofisticati sponsorizzati da governi, corporations e gruppi criminali in un contesto di "tutti contro tutti".
- **Cyberwarfare** : non ci sarà la cyber war, almeno per 2-3 anni, ma tutti si prepareranno attivamente a combatterla, investendo ingenti risorse. Ci saranno schermaglie ed incidenti con frequenza crescente.

Analisi del mercato italiano della sicurezza ICT (e mercato del lavoro)

- L'andamento del mercato del lavoro nel nostro settore: dopo una leggera flessione nel 2011, nel 2012 dovrebbe rimanere stabile.
- Le figure professionali più richieste: consulenti, analisti, security auditor. Seguono le figure tecniche.
- Quali i prerequisiti determinanti al momento dell'assunzione: le certificazioni vendor neutral (CISSP, CISM, ISO27001...). Segue l'Esperienza di almeno 5 anni e poi la Laurea.

Survey – Il campione intervistato

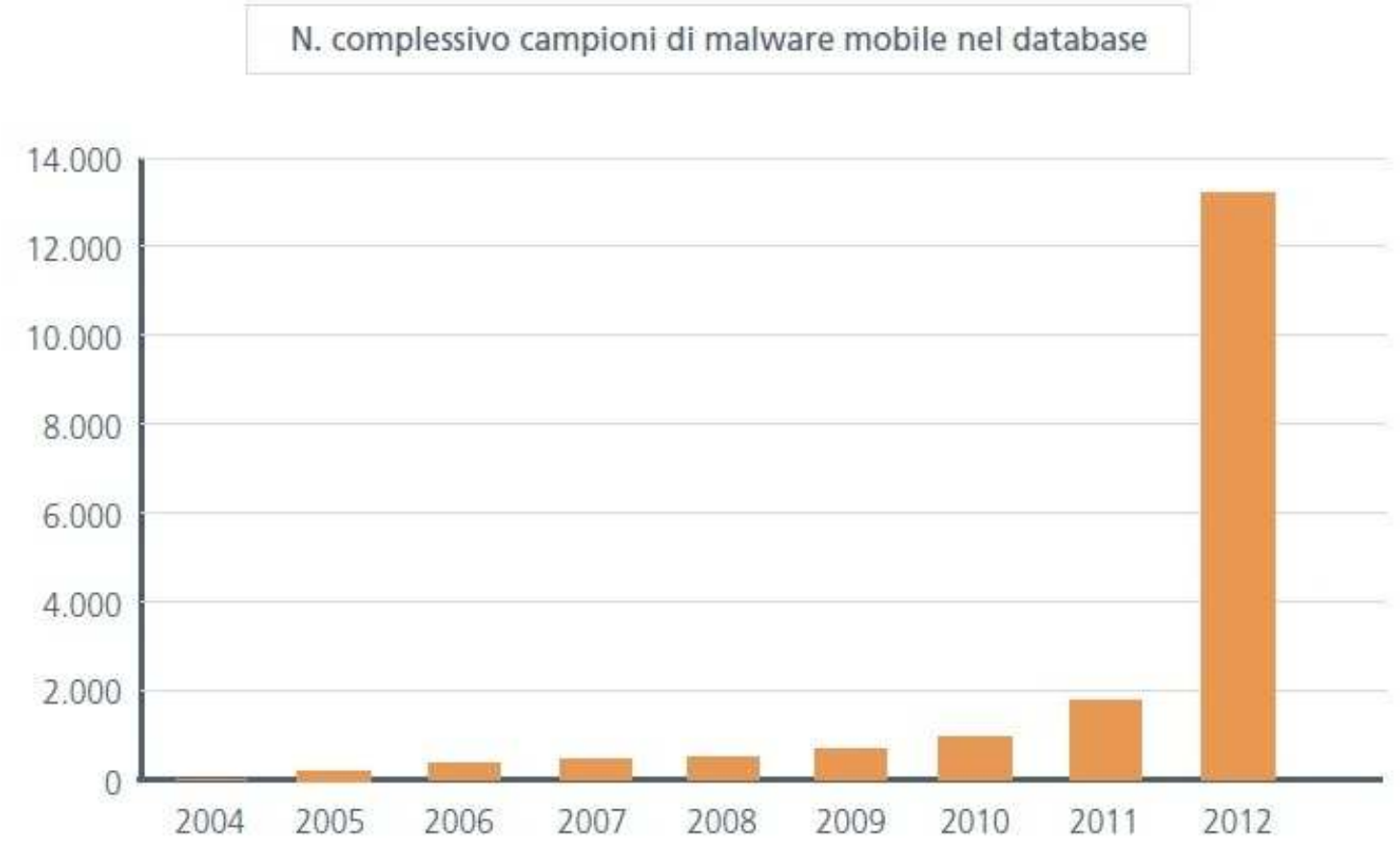
- 142 aziende italiane di ogni dimensione
- 77 che offrono prodotti e servizi di ICT security (vendors)
- 65 User, appartenenti a tutti i settori economici.

Focus On: Mobile Security

- **Premessa** : per la natura transnazionale della cybercriminalità, per il fatto che Internet non ha confini, per il fatto che queste piattaforme sono ancora acerbe, e che questi device sono stati pensati per un uso ludico, e non certo come strumenti ai quali affidare i propri segreti ed i propri affari (credenziali di accesso, dati finanziari, dati sensibili, reti di relazioni, etc), i device mobili sono oggi **molto difficili da proteggere**.

- **Conseguenza**: Gli attacchi sono più sofisticati ed aggressivi di quanto sia possibile fare con i PC. Inoltre nella maggior parte dei casi (>90%) i device non dispongono di protezioni anti-malware (anzi spesso sono gli stessi utenti a manometterli, rendendoli ancora più vulnerabili). Non si tratta solo di infezioni da malware, ma anche e soprattutto di frodi ed attacchi basati su tecniche di "social engineering", veicolate principalmente tramite spam e tramite i messaggi che arrivano dai Social Networks (contro i quali un antivirus non può nulla). Il 2012 sarà l'anno della Mobile Insecurity.

Focus On: Mobile Security



Focus On: Social Media Security

- **Numeri** : I SN hanno complessivamente 2 miliardi di utenti nel mondo (800 milioni solo Facebook, la metà mobili), i quali hanno instaurato tra loro circa 300 miliardi di collegamenti e trascorrono *200.000 anni / uomo al giorno* sui Social Network (45.000 su Facebook).
- **Luci e Ombre** : Le aspettative miracolose alimentate dal marketing in merito ai vantaggi derivanti dall'uso dei Social Network (ed il loro straordinario sviluppo) hanno **fin'ora** mascherato la realtà della corrispondente crescita esponenziale di attività di spionaggio, di ogni genere di attività di criminali, agenzie, mercenari, terroristi, corporation…
- **Minacce**: i SN sono un amplificatore ed un "luogo" di aggregazione senza precedenti. E' **troppo** facile colpire gli utenti social e le piattaforme non sono all'altezza del compito di proteggerli.
- **Rischi** : Decine di milioni di vittime all'anno. Costi astronomici. Situazione di "Far West" sempre più diffusa. Effetto "boomerang".

Grazie!

Per maggiori informazioni:

pgiudice@clusit.it

a.zmanzoni@idialoghi.com