Security Summit Milano 2015

Sessione Plenaria del 17.03.2015

Clusit
Associazione Italiana
per la Sicurezza Informatica

SECURITY
TECHNOLOGIES
MANAGEMENT COMPLIANCE
SUMMIT

Rapporto Clusit 2015 sulla sicurezza ICT in Italia

Intervengono alcuni degli autori:

- Andrea Zapparoli Manzoni, Clusit
- Davide Del Vecchio, FASTWEB, Clusit
- Pier Luigi Rotondo, IBM
- Paolo Bufarini, Akamai

Partecipano:

- Gastone Nencini, Trend Micro
- Federico Santi, HP Security Services
- Alessandro Vallega, Oracle Italia
- Stefano Volpi, Cisco

Panoramica degli attacchi informatici più significativi del 2014 e tendenze per il 2015

- Analisi dei principali attacchi a livello internazionale
- Analisi degli attacchi italiani
- Analisi FASTWEB della situazione italiana in materia di cyber-crime e incidenti informatici
- Alcuni elementi sul cyber-crime in Europa e nel Medio Oriente

  (a cura di IBM)
- Rapporto 2014 sullo stato di Internet ed analisi globale degli attacchi DDoS (a cura di Akamai)
- La Polizia Postale e delle Comunicazioni e il contrasto al cyber crime
- Il Nucleo Speciale Frodi Informatiche della Guardia di Finanza e il contrasto alle attività illecite su Internet

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

FOCUS ON

- Internet of (Hacked) Things
- M-Commerce
- Bitcoin, aspetti tecnici e legali della criptovaluta
- Doppia autenticazione per l'accesso ai servizi di posta elettronica
- Lo stato della sicurezza dei siti web della pubblica amministrazione
- Il Regolamento generale sulla protezione dei dati: novità per i cittadini, le imprese e le istituzioni
- Cloud e sicurezza: profili legali
- Return on Security Investment
- L'impatto della Direttiva 263/agg.15 di Banca d'Italia sugli operatori del settore bancario

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

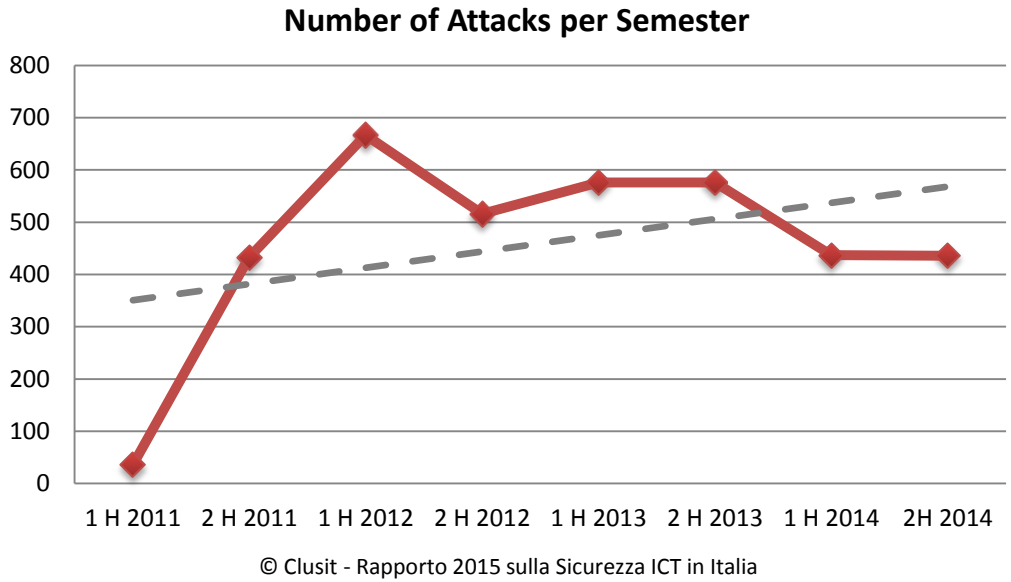
Analisi Clusit della situazione nazionale ed internazionale

Quali sono i numeri del campione ?

Negli ultimi 48 mesi abbiamo analizzato in media 78 incidenti gravi al mese, ogni mese (72 al mese nel 2014, con i nuovi criteri)

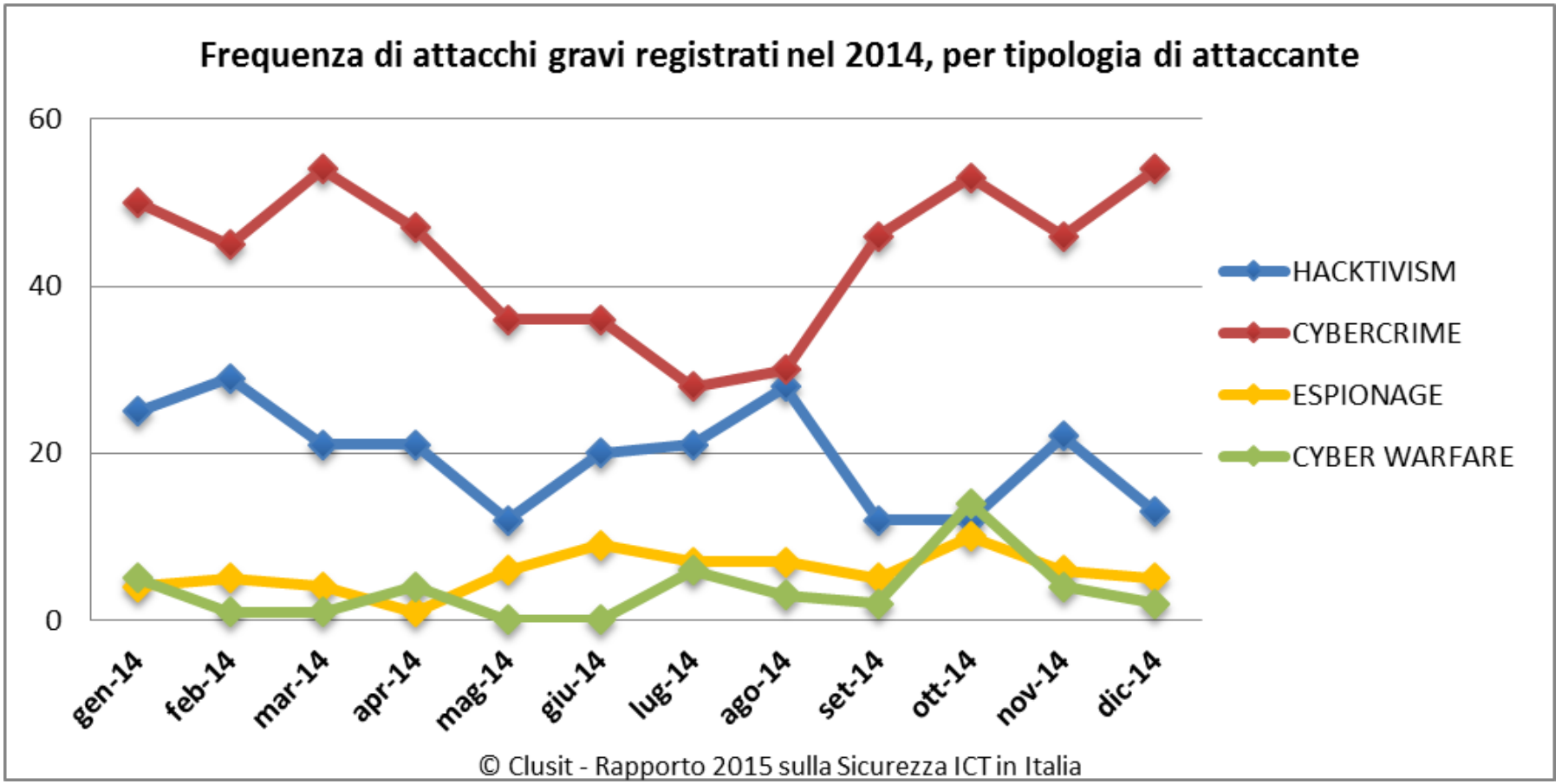
- 3.677 attacchi analizzati dal gennaio 2011 al dicembre 2014.

- 469 nel 2011
- 1.183 nel 2012
- 1.154 nel 2013
- 873 nel 2014 (*)

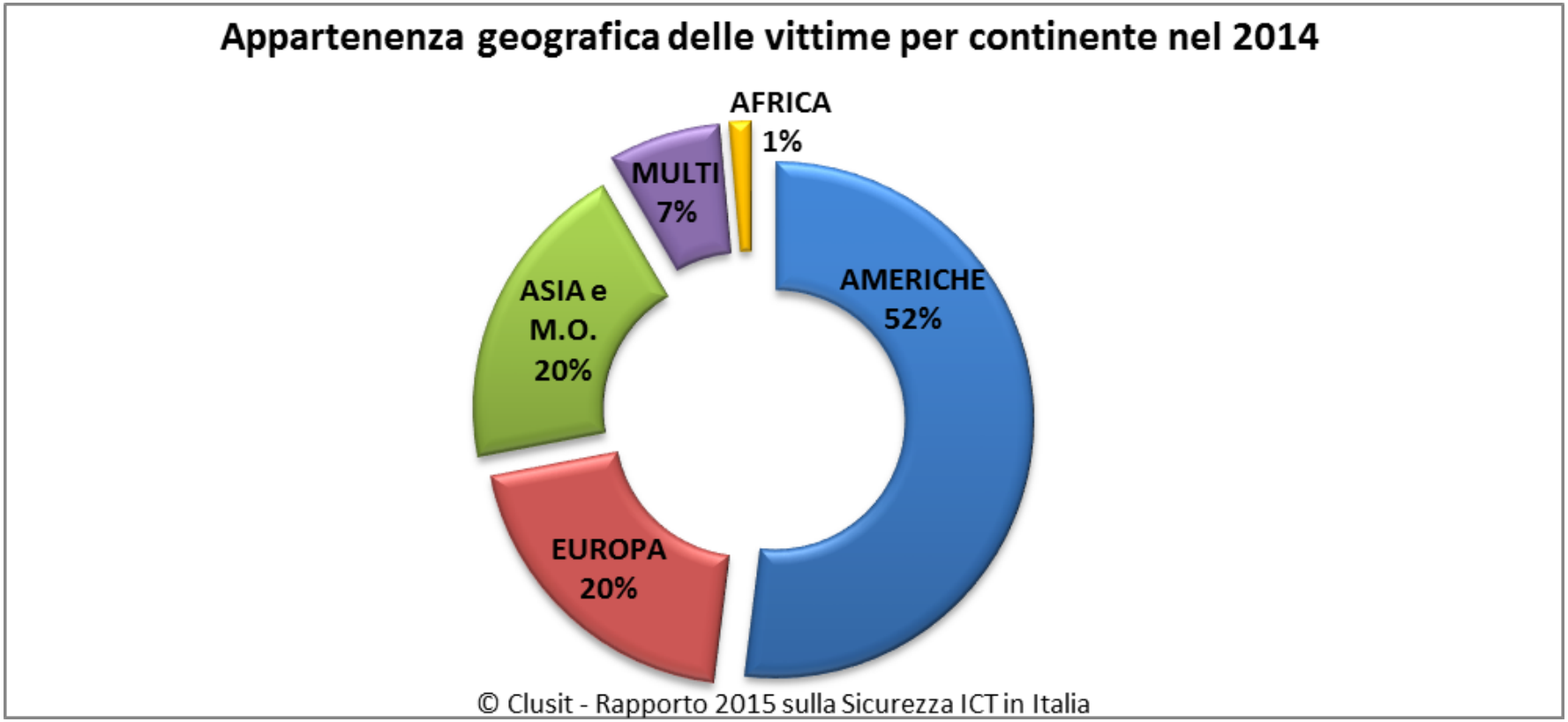


(*) Nel 2014 il numero assoluto di attacchi gravi che abbiamo registrato è diminuito perché abbiamo reso più restrittivi i criteri di classificazione per allinearli al livello crescente di minaccia. Con i criteri precedenti sarebbe aumentato di circa il 10%.

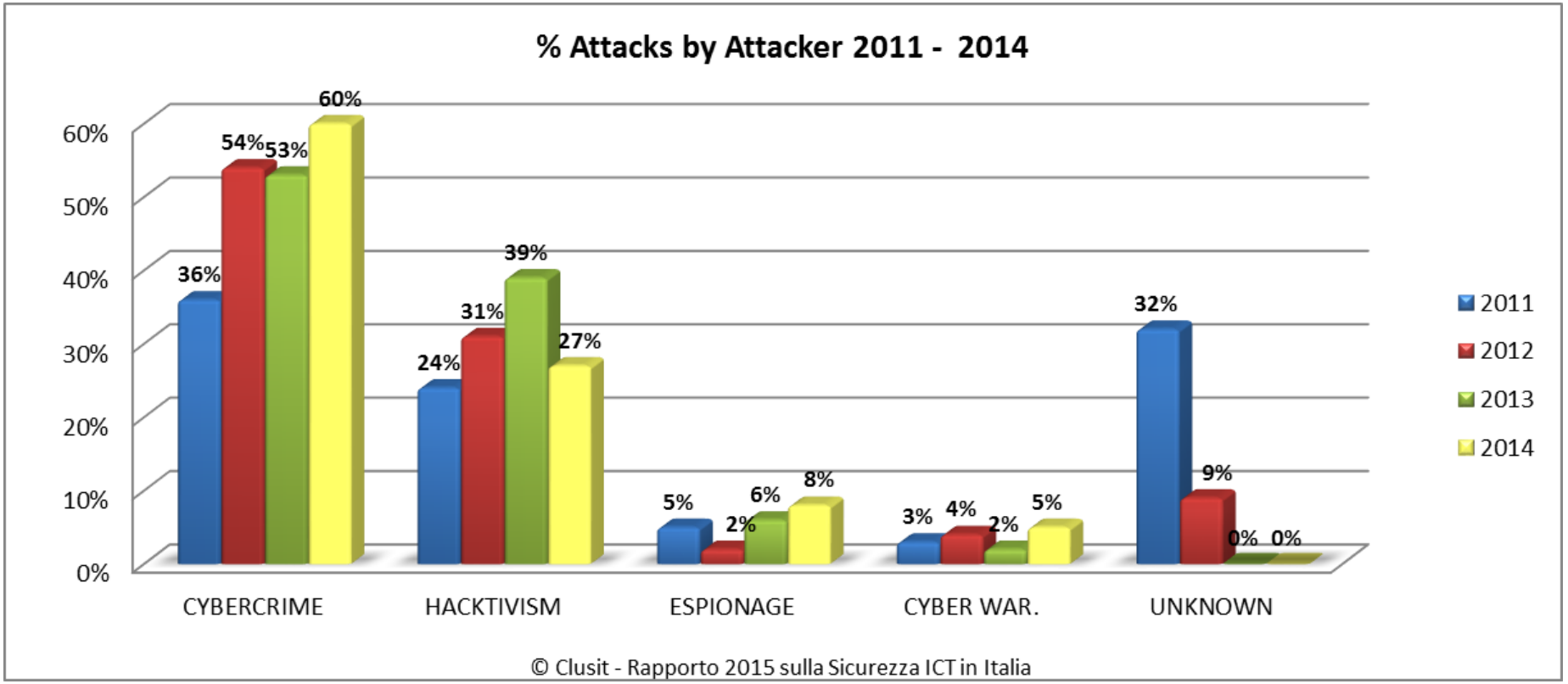
Distribuzione attacchi nel tempo



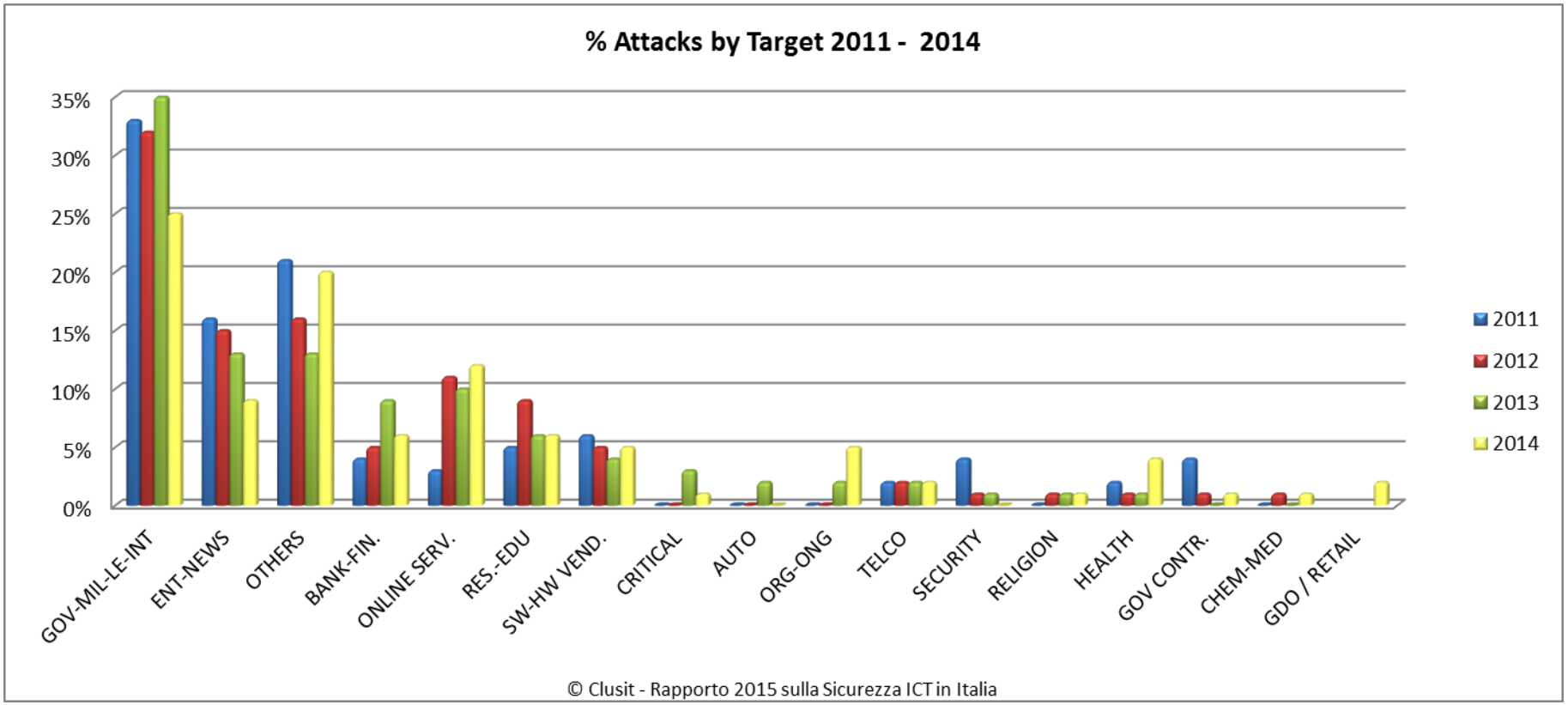
Distribuzione attacchi per area geografica



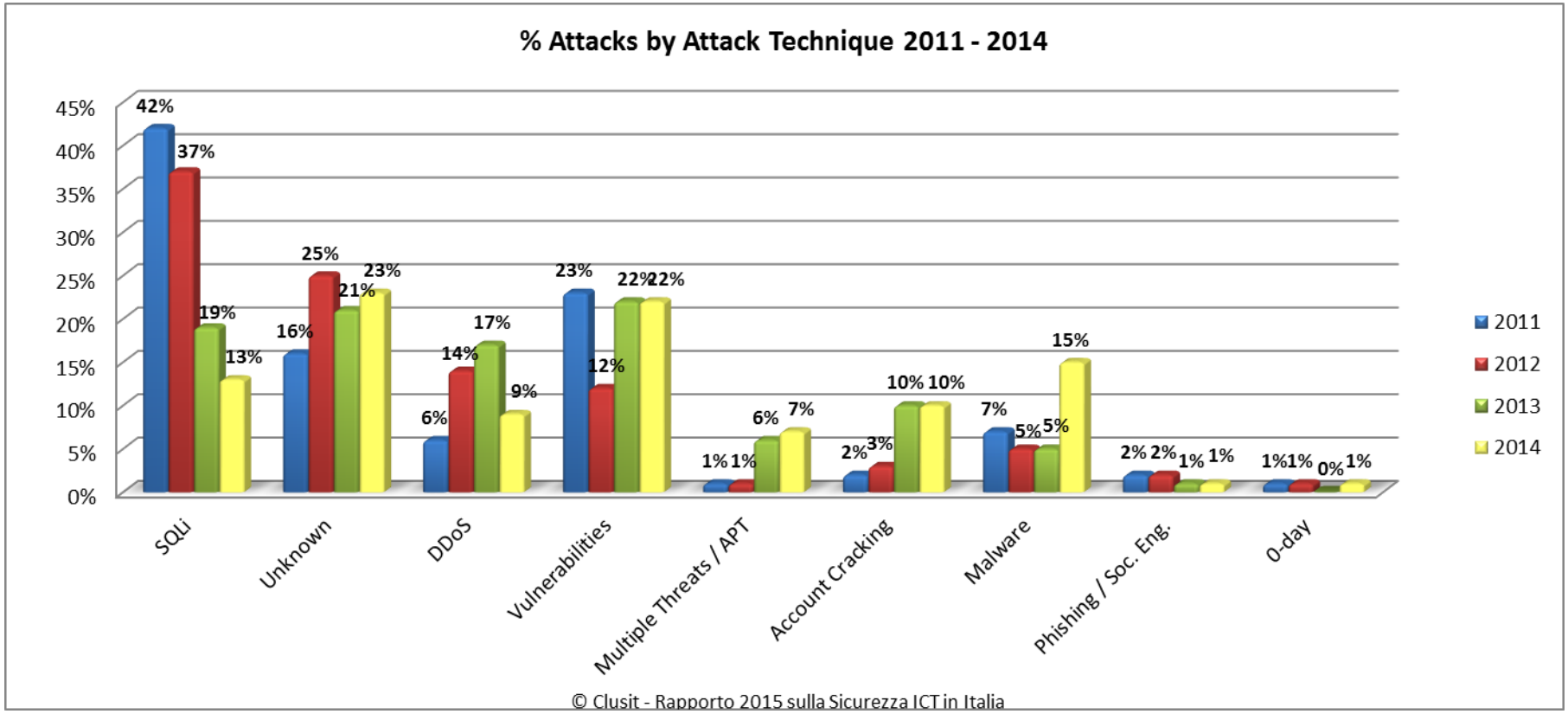
Distribuzione attaccanti nel mondo



Distribuzione vittime nel mondo



Tecniche di attacco a livello mondo



Analisi FASTWEB della situazione nazionale

Perché quest'analisi ?

La sensibilità su questi argomenti nasce più dalle informazioni apprese attraverso i mass media, che tramite i canali specializzati paper scientifici, corsi, congressi, etc).

Ne scaturisce un'idea vaga di come e dove investire il budget dedicato ad affrontare questi problemi così che spesso si rischia di essere guidati più dalle sensazioni che dal livello effettivo di rischio.

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

Eventi di Sicurezza

Base di dati:

circa 6 milioni di indirizzi IPv4

2013	2014
Eventi sicurezza: circa 172 mila	Eventi Sicurezza: oltre 5 milioni

+2900%

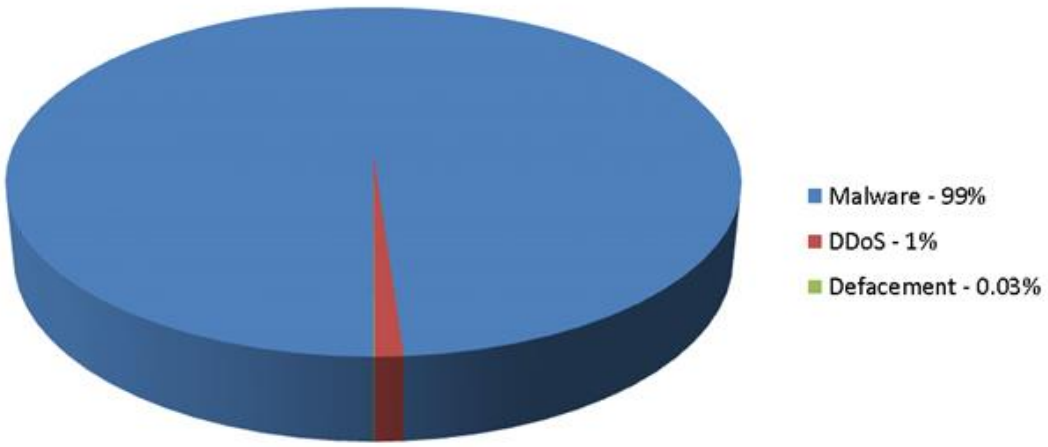
Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

Eventi Sicurezza

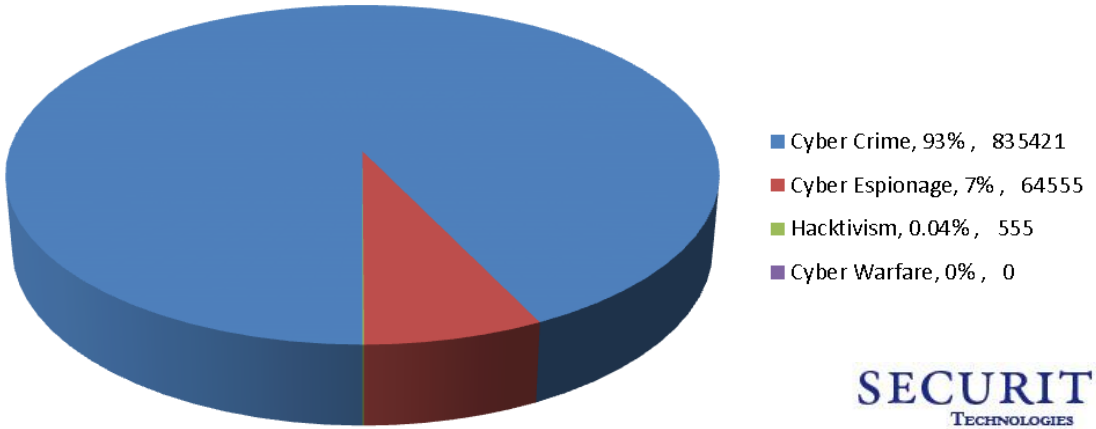
Base di dati: 5 milioni di eventi

Tipologie di attacchi informatici rilevati



Dati FASTWEB relativi all'anno 2014

Motivazione attacchi informatici



Dati FASTWEB relativi all'anno 2014

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

Attacchi DDoS

2013 2014

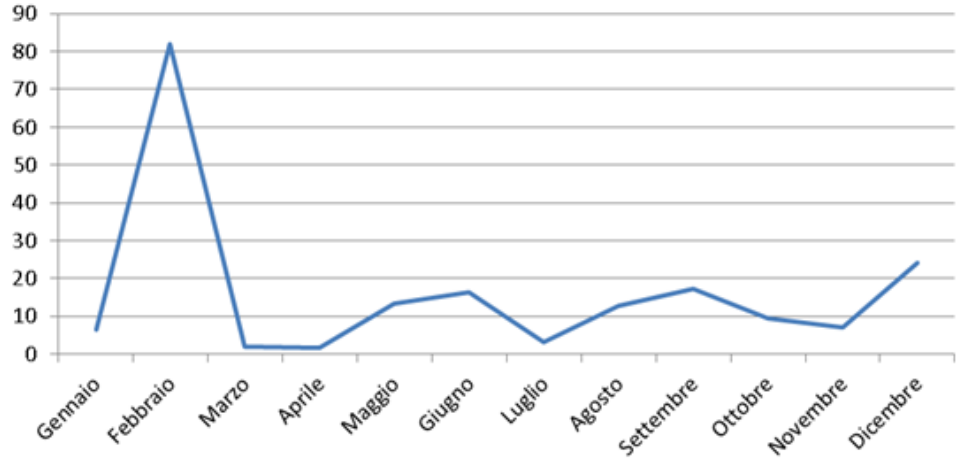
circa 1000 attacchi → oltre 16 mila attacchi

+1600%

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

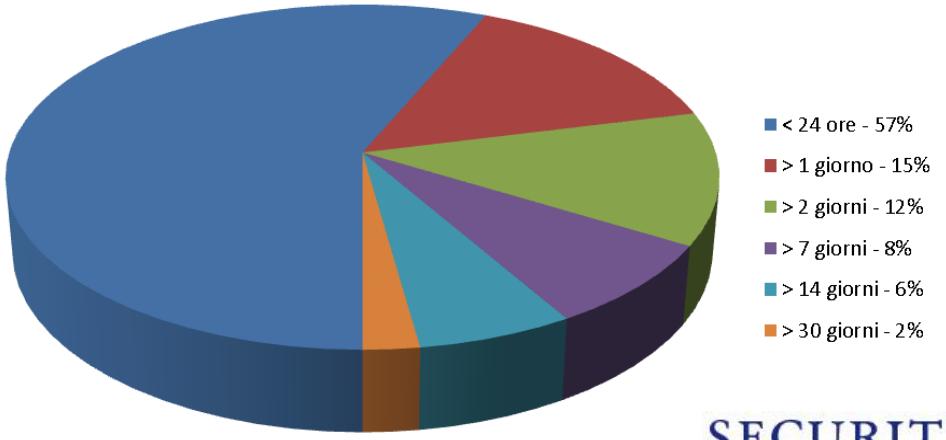
Attacchi DDoS



Dati FASTWEB relativi all'anno 2014

Tipologie di attacchi informatici rilevati. (Media: 9,5 Gbps)

Tipologie di attacchi informatici rilevati. (Media: 3 giorni)



Dati FASTWEB relativi all'anno 2014

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

Considerazioni Finali

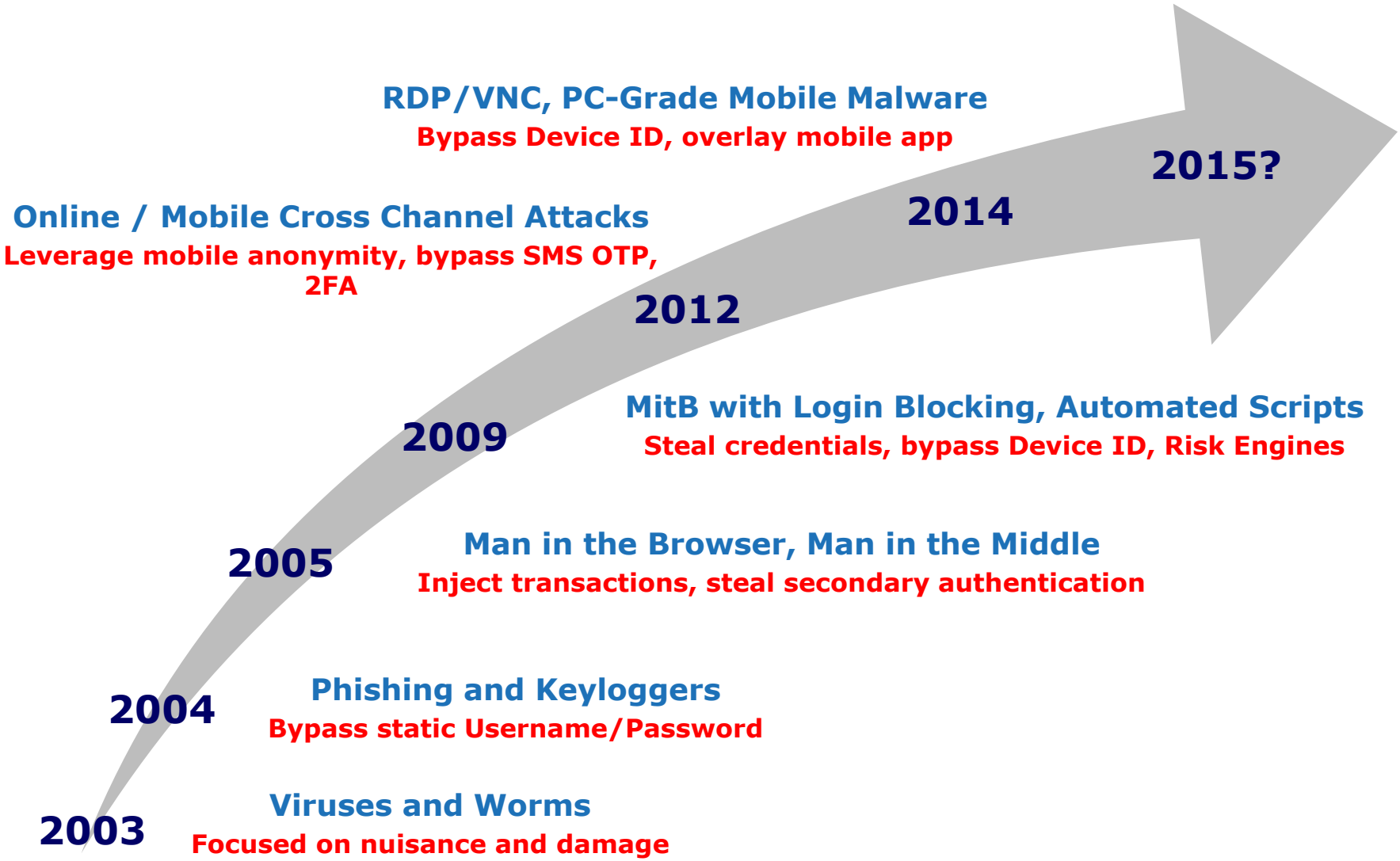
Necessario uno sforzo congiunto tra tutti gli attori coinvolti: forze dell'ordine, ISP, hosting/housing provider, etc, poichè il fenomeno ha assunto una dimensione sempre più grande, su scala nazionale ed internazionale, colpendo ogni ambito lavorativo, con particolari conseguenze per le piccole/medie aziende ed i privati cittadini che sono maggiormente inconsapevoli dei rischi derivanti dal trascurare tale minaccia.

Clusit
Associazione Italiana per la Sicurezza Informatica

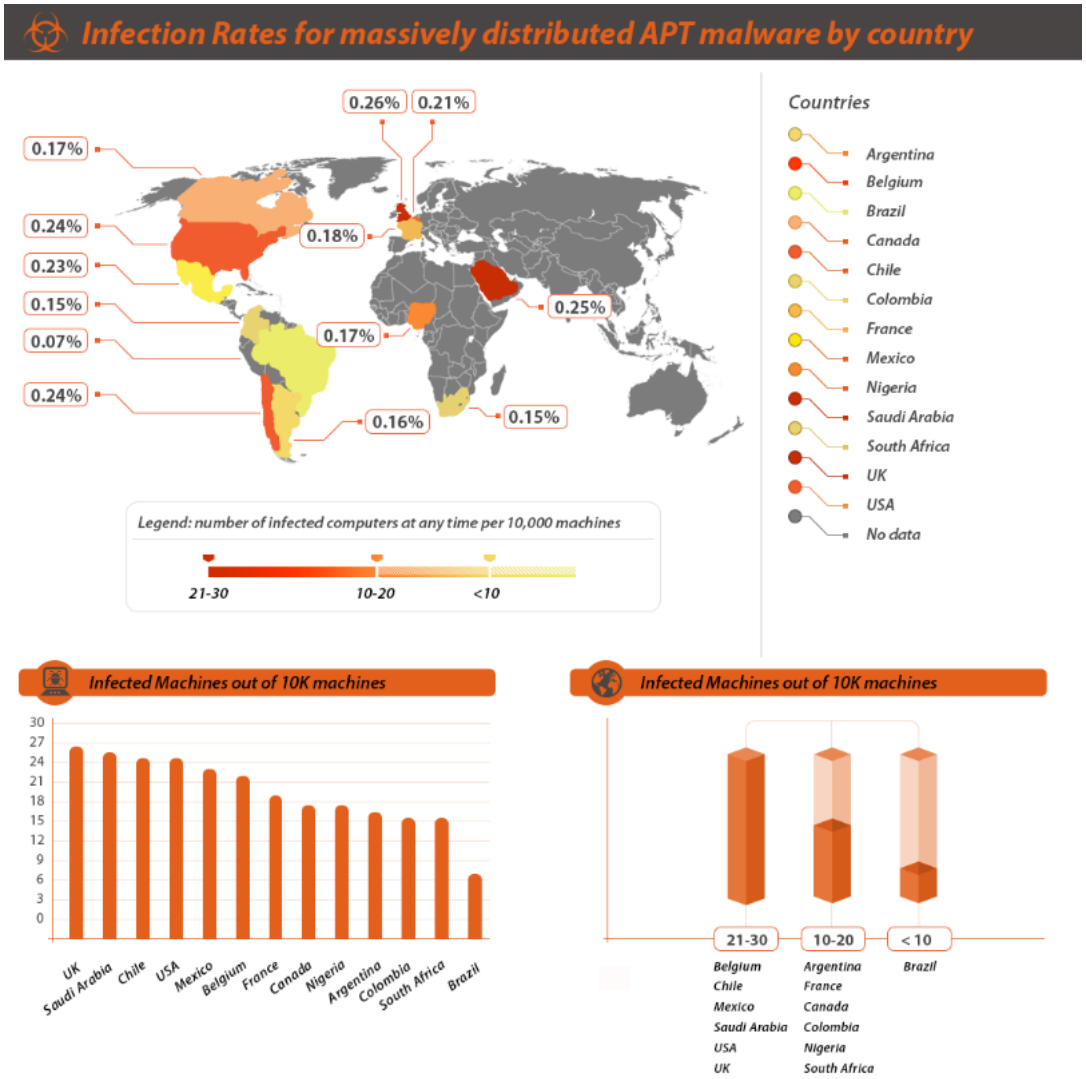
SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

Alcuni elementi sul cyber-crime in Europa e nel Medio Oriente

Evoluzione delle tecniche di attacco

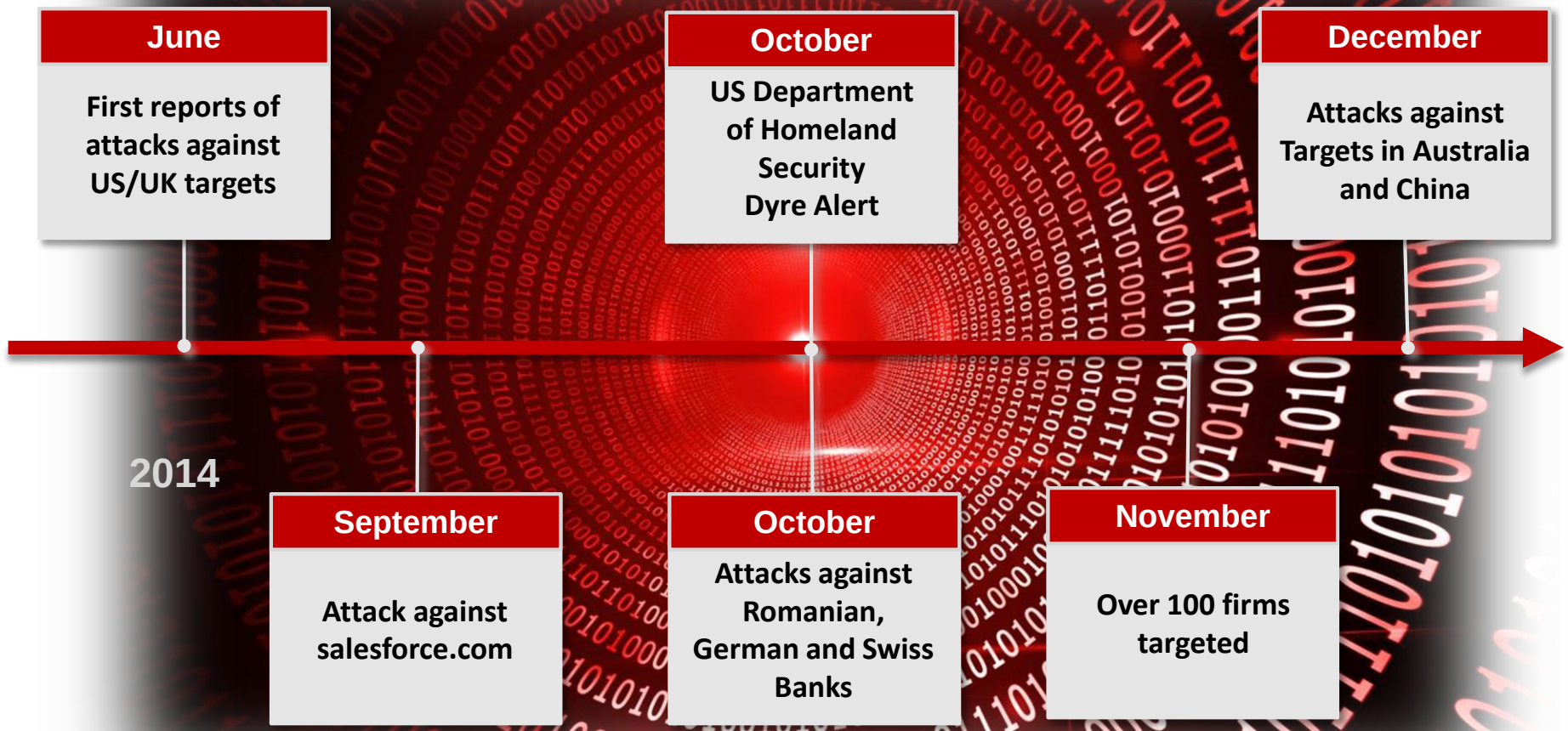


Percentuale di computer infetti da malware APT



Fonte: IBM Security - © 2014 IBM Corporation

Dyre – Da attacco locale a minaccia globale



Rapporto 2014
sullo stato di Internet ed analisi globale degli attacchi DDoS

The Akamai Intelligent Platform

Un piattaforma Cloud distribuita in tutto il mondo che gestisce la crescente complessita' della rete Internet -

- 170.000 > server, 200 carrier
- 15 -30 % del traffico Internet
- 25 Tbps di picco
- 19 Millioni di hit per secondo

Monitoraggio delle minacce a livello globale

- I team Akamai PLXsert e CSIRT monitorano le minacce informatiche a livello globale e analizzano questi attacchi. Attraverso ricerche, indagini digitali e analisi post-evento, Akamai crea un quadro globale delle minacce alla sicurezza, delle vulnerabilità e dei trend, che viene condiviso con i clienti e la community impegnata nella sicurezza.
  - **2 trilioni di hits al giorno**
  - **780 milioni di indirizzi IPv4 osservati a trimestre**
  - **260+ terabytes di file di log compressi**
  - **10 Terabytes di dati giornalieri su attacchi**
  - **2 Petabytes di dati di sicurezza archiviati**
  - **45 giorni di ciclo di vita del dato**

Minacce emergenti

- Nel 2014 si sono verificati numerosi eventi significativi riguardanti la sicurezza in Internet, che sono stati successivamente utilizzati per attacchi su vasta scala.
- La diffusione dei dispositivi con funzionalità Internet e l'espansione dell'Internet of Things (IoT) comporteranno anche l'ampliamento della superficie di attacco a disposizione dei pirati informatici
- Le nuove risorse dell'ecosistema DDoS influiranno sulle campagne indotte dal malcontento sociale e da rivalità geopolitiche e sulle campagne sponsorizzate da stati.
- L'ecosistema dei crimini DDoS motivato da scopi di lucro si espanderà per sfruttare l'opportunità

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

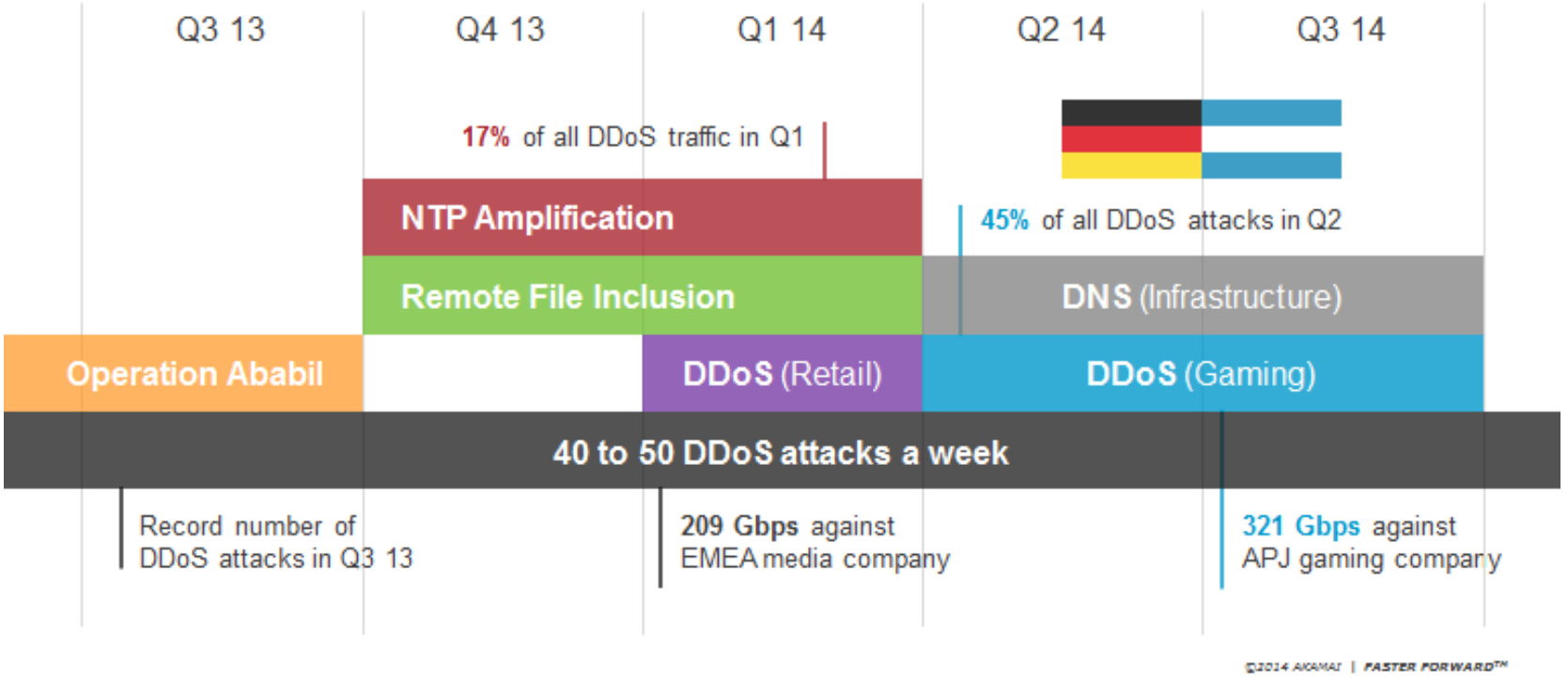
Analisi e trend

- Le campagne di attacchi DDoS da record verificatesi nel 2014 hanno registrato un notevole aumento percentuale della media dei picchi di banda rispetto all'anno precedente.
- Un fattore che ha contribuito a tale aumento è stato un attacco di 321 Gbps (gigabit al secondo), mentre un altro è rappresentato dall'utilizzo di nuovi vettori di attacco
- Rispetto all'anno precedente, i volumi degli attacchi sono aumentati del 366%.
- L'elemento principale che ha guidato lo sviluppo delle botnet nel 2014 è stato l'utilizzo su vasta scala delle vulnerabilità del Web pubblico con predominanza degli attacchi basati sulla riflessione.

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

2014: crescente aumento delle minacce



Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

Crescita dei volumi e dell'utilizzo di vettori multipli di attacco

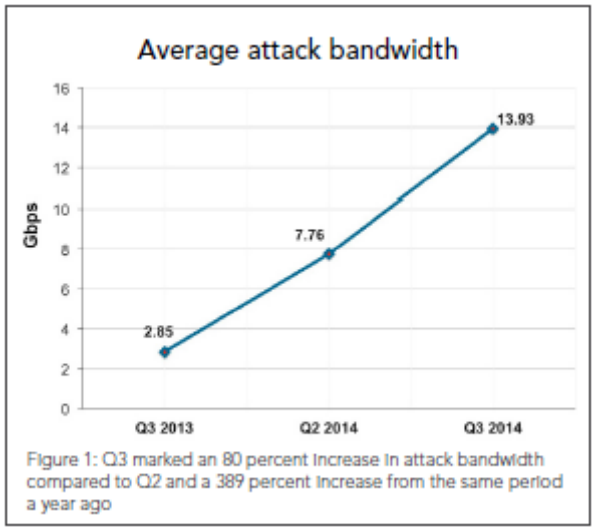


Figure 1: Q3 marked an 80 percent increase in attack bandwidth compared to Q2 and a 389 percent increase from the same period a year ago

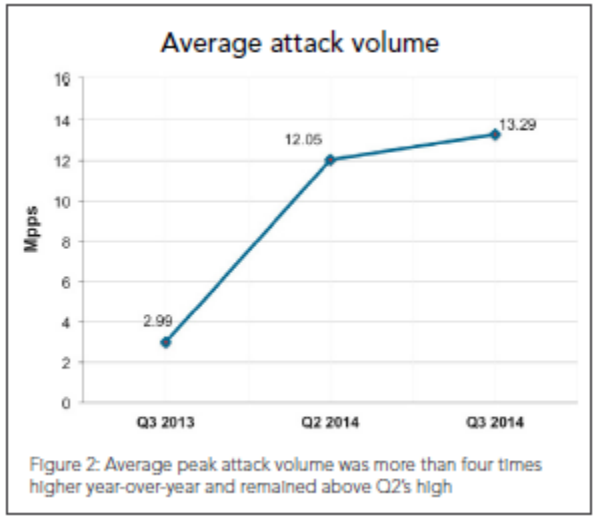


Figure 2: Average peak attack volume was more than four times higher year-over-year and remained above Q2's high

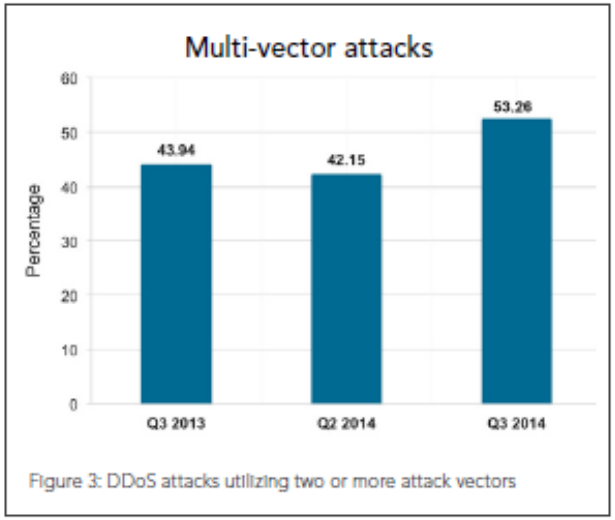


Figure 3: DDoS attacks utilizing two or more attack vectors

Conclusioni

- **I malintenzionati sono costantemente alla ricerca di nuovi modi per espandere le proprie risorse e creare nuovi vettori di attacco DDoS.**
- **I pirati informatici stanno spostando l'attenzione verso i dispositivi embedded (IoT)**
- **I sistemi con potenza di elaborazione di alto livello e la capacità di larghezza di banda elevata resa disponibile attraverso la compromissione di questi dispositivi, nonché le applicazioni basate sul cloud che interagiscono con essi, presentano uno scenario complesso.**
- **È necessario coordinare gli sforzi della community impegnata nella sicurezza per scoprire, gestire e mitigare le vulnerabilità presenti in questi dispositivi e per evitare l'ulteriore espansione di queste campagne malevole.**

Per maggiori informazioni e per chiedere una copia del rapporto in formato digitale:

rapporti@clusit.it

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT