Verona 4 ottobre 2017

#securitysummit #rapportoclusit #cybersecmonth

Clusit
Associazione Italiana per la Sicurezza Informatica

5th EUROPEAN CYBER SECURITY MONTH Anniversary

ASTREA

Security Summit Verona 2017

Clusit
Associazione Italiana
per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

SECURITY
TECHNOLOGIES
MANAGEMENT COMPLIANCE
SUMMIT

Rapporto Clusit 2017 sulla sicurezza ICT in Italia

Moderano:

Gigi Tagliapietra, Presidente Onorario Clusit

Intervengono:

Alessio Pennasilico, uno degli autori del Rapporto Clusit

Partecipano alla Tavola Rotonda:

- Alberto Mercurio, UNIS&F
- Ettore Guarnaccia, Gruppo Intesa Sanpaolo, Divisione Banca dei Territori
- Gianluca Busco Arre', Panda Security Italia
- Salvatore Marcis, Trend Micro

Panoramica dei cyber attacchi più significativi del 2016

- Analisi dei principali attacchi a livello globale
- Analisi della situazione italiana in materia di cyber-crime e incidenti informatici
- Rapporto sullo stato di Internet ed analisi globale degli attacchi DDoS e applicazioni Web
- La visione del CERT-PA

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

Speciale FINANCE

- Alcuni elementi sul Cyber-crime nel settore finanziario in Europa
- Analisi del Cyber-crime in Italia in ambito finanziario
- Blackmarket – Scenario e focus sul carding in Italia - Anno 2016
- Cyber Risk e Cyber Insurance

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

Speciale PA

- La sicurezza informatica nella Pubblica Amministrazione: che anno è stato il 2016 e cosa ci si aspetta per il 2017

- Monitoraggio e analisi degli eventi di sicurezza nella PA: il case study di Regione Emilia Romagna

- SPID: stato attuale e sviluppi futuri

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

Speciale SANITÀ

- Sicurezza e Privacy in Sanità
- Sicurezza in Sanità, bisogni ed opportunità - Leggi, consolidamento e cose concrete da fare senza budget e con poche risorse
- Dati sanitari protetti (PHI): una nuova miniera d'oro per i cyber criminali

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

EVOLUZIONE DELLE NORMATIVE EUROPEE

- Evoluzione delle normative europee sulla Cyber-Security
- GDPR – Cosa fare ora
- Survey sul nuovo Regolamento Europeo sulla Privacy
- Introduzione alla PSD2 e suoi obiettivi
- Compliance eIDAS

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

Il mercato italiano della sicurezza IT: analisi, prospettive e tendenze secondo IDC

Un’analisi realizzata appositamente per il Rapporto Clusit alla fine del 2016 da

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

FOCUS ON 2017

- Ransomware: un flagello che prende di mira privati e aziende
- Attacchi e difese sulle infrastrutture Private e Hybrid Cloud
- Cyber Risk Management
- Le sfide relative ai captatori informatici, tra proposte legislative e rischi di sicurezza
- Il voto elettronico: potenzialità e rischi lungo la strada della democrazia elettronica

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

Rilevanza strategica e diffusione delle principali aree di Information Security nelle aziende italiane

In chiusura del rapporto, presentiamo i risultati di una Survey realizzata da

Osservatori del Politecnico di Milano

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

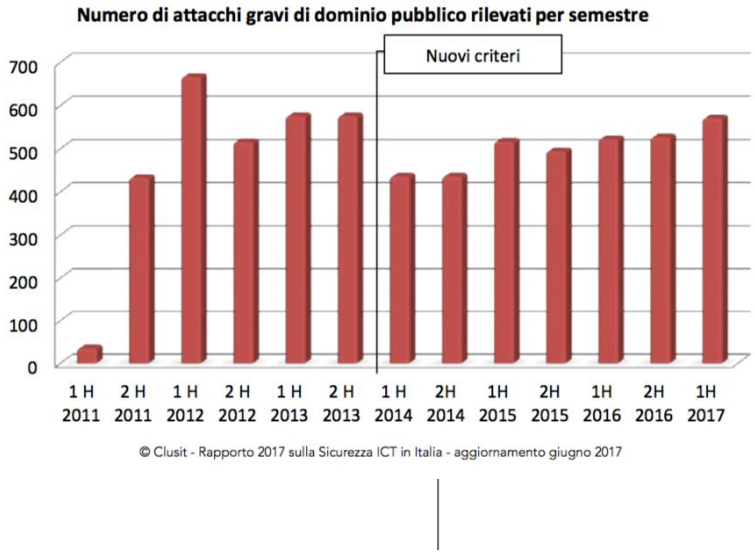
Analisi Clusit dei principali attacchi a livello globale

Quali sono i numeri del campione ?

In media negli ultimi 6 mesi abbiamo analizzato e classificato come gravi 95,2 incidenti al mese, ogni mese (83 al mese negli ultimi 6,5 anni)

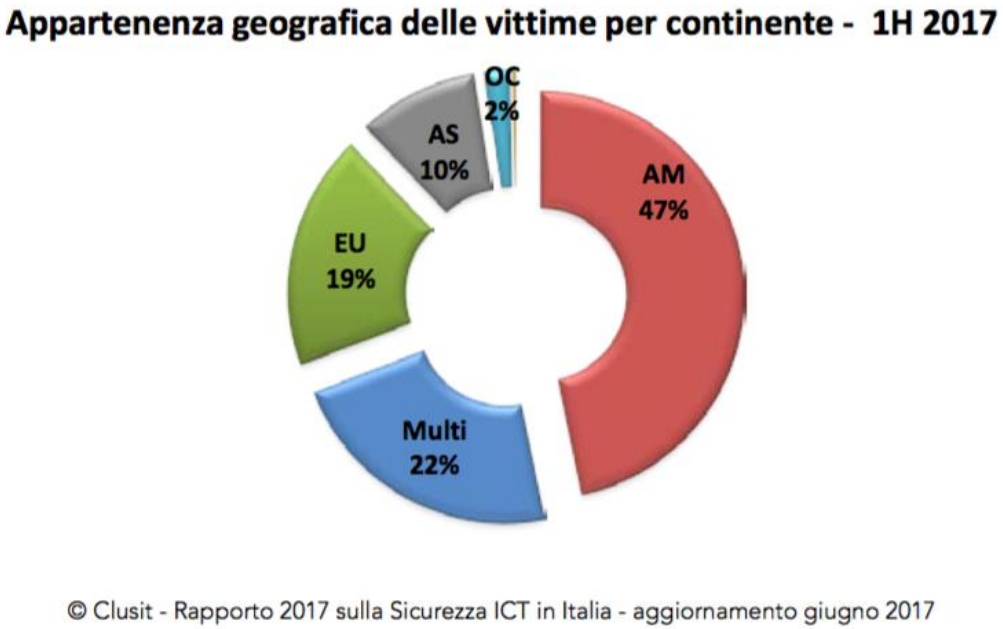
- 6.093 attacchi analizzati dal gennaio 2011 al giugno 2017.

- 469 nel 2011
- 1.183 nel 2012
- 1.154 nel 2013
- 873 nel 2014 (*)
- 1.012 nel 2015
- 1.050 nel 2016
- 571 nel primo semestre 2017



(*) 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%. Nel 2015, pur applicando i nuovi criteri, la crescita rispetto al 2014 è pari al 14% Y/Y. Nel 2016 la crescita è del 3,75% Y/Y (circa +20% rispetto al 2014).

Distribuzione geografica vittime



Rispetto al secondo semestre 2016, nel primo semestre 2017 in percentuale diminuiscono le vittime di area americana (dal 55% al 47%), ed asiatica (dal 16% al 10%).

Crescono gli attacchi verso realtà basate in Europa (dal 16% al 19%) e soprattutto aumentano in modo significativo gli attacchi verso realtà multinazionali (dall'11% al 22%) ad indicare la tendenza a colpire bersagli sempre più importanti, di natura transnazionale.

Tipologia e distribuzione degli attaccanti

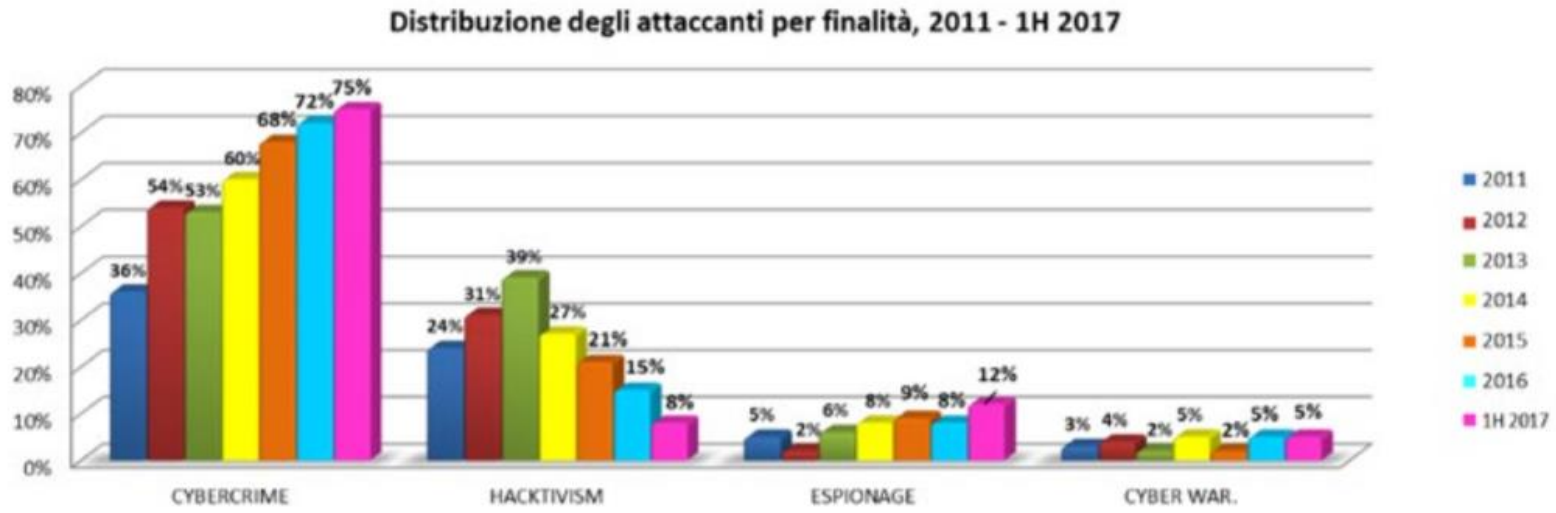
ATTACCANTI PER TIPOLOGIA	2011	2012	2013	2014	2015	2016	2H 2016	1H 2017	1H 2017 su 2H 2016	Trend 2016
Cybercrime	170	633	609	526	684	751	377	427	13,26%	
Hacktivism	114	368	451	236	209	161	78	46	-41,03%	
Espionage / Sabotage	23	29	67	69	96	88	30	68	126,67%	
Information Warfare	14	43	25	42	23	50	42	30	-28,57%	
TOTALE	469	1.183	1.152	873	1.012	1.050	527	571	+8,35%	

Complessivamente, rispetto al secondo semestre 2016, nel primo semestre 2017 il numero di attacchi gravi che abbiamo raccolto da fonti pubbliche ed analizzato cresce del 8,35%In termini assoluti, nei primi mesi del 2017 la categoria “Cybercrime” fa registrare il numero di attacchi più elevato dei 13 semestri presi in esame (247)

Dal campione emerge chiaramente che, con l’esclusione delle attività riferibili ad attac-chi della categoria “Hacktivism” che diminuisce sensibilmente (-41%), rispetto al 2H 2016 nel 1H 2017 gli attacchi gravi compiuti per fnalità “Cybercrime” sono in aumento (+13,26%), così come quelli riferibili ad attività di “Espionage” (+126%), mentre mostra-no un calo gli attacchi noti del gruppo “Information Warfare” (-28,57%).

Va sottolineato che, rispetto al passato, oggi risulta più diffcile distinguere nettamente tra queste due ultime categorie: sommando gli attacchi di entrambe, nel 1H 2017 si assiste ad un aumento del 36% rispetto al semstre precedente (98 contro 72).

Tipologia e distribuzione degli attaccanti (6,5 anni)

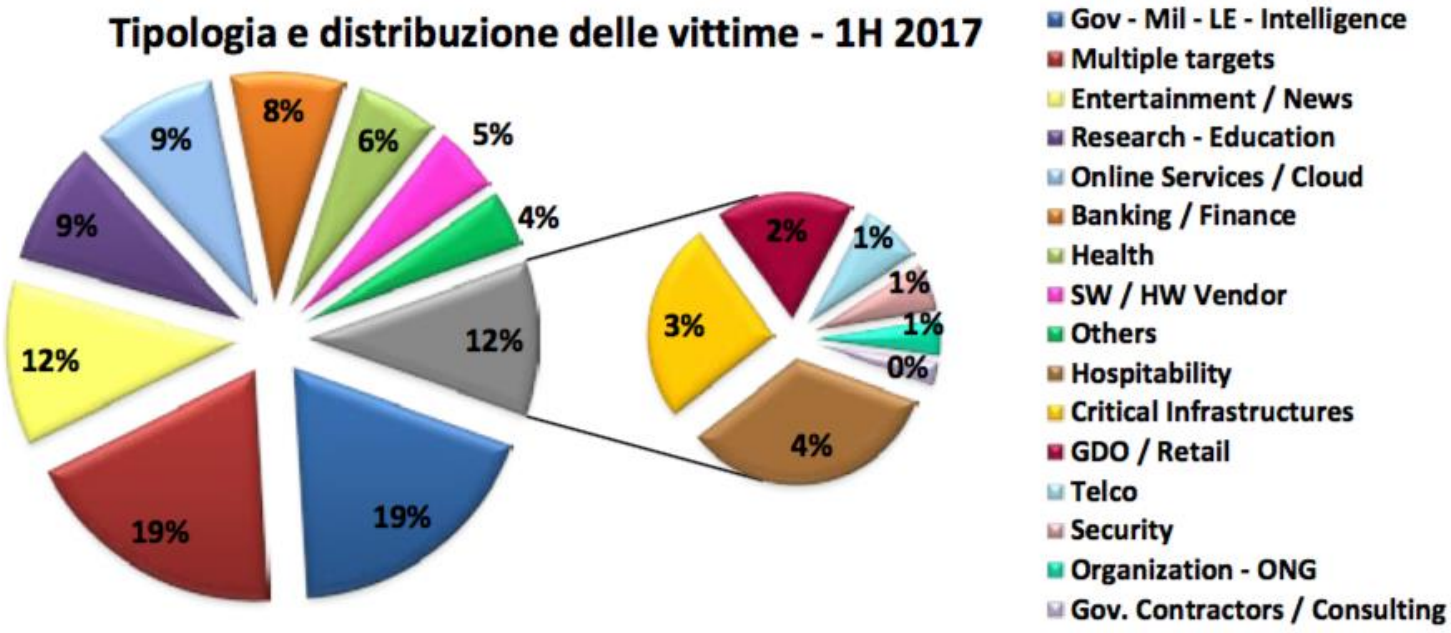


© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia - aggiornamento giugno 2017

Il Cybercrime passa dal 72% al 75% del totale, mentre l'Hacktivism diminuisce di 31 punti percentuali rispetto al suo picco del 2013, passando da oltre un terzo a meno di un decimo dei casi analizzati (8%)

Per quanto riguarda le attività di Espionage, rispetto alla percentuale degli attacchi gravi registrati nel 2016 la quota di attacchi nel 1H 2017 è in forte crescita (dal 8% al 12% del totale), mentre l'Information Warfare risulta stabile (probabilmente per la scarsità di informazioni pubbliche in merito) al 5%.

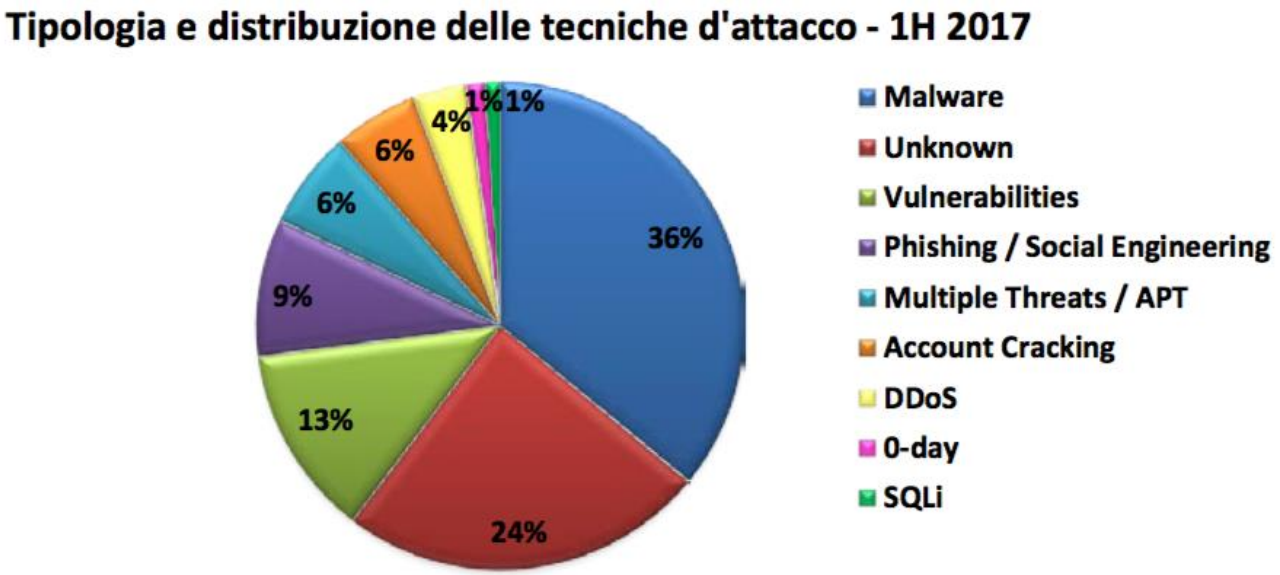
Distribuzione vittime nel mondo (2017 1H)



© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia - aggiornamento giugno 2017

Al primo posto assoluto, in leggera diminuzione, ancora il settore governativo in senso esteso, con un quinto degli attacchi (19%). La categoria “Multiple Targets” nel primo semstre 2017 balza al secondoposto (19%). Al terzo posto la categoria “Entartainment/news” (12%), a seguire “Reasearch – Education” (9%), “Online Services - Cloud” (9%) e “banking / Finance” (8%).

Tecniche di attacco nel mondo (2017 1H)



© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia - aggiornamento giugno 2017

Le SQLInjection rimangono stabili al 13% del totale. Crescono gli attacchi da attività di Phishing e Social Engineering, che passano dal 7% al 9% del totale. Diminuiscono numericamente gli attacchi DDoS (dall'11% al 4%) che però nel primo semestre 2017 hanno raggiunto volumi vicini o superiori al Gigabit per secondo, un record assoluto.

Trends 2017

- "Allarme rosso" (soprattutto per Cybercrime e State sponsored attacks)
- Phishing (via mail, IM e Social), principale vettore di attacco
- Internet of Things / Industry 4.0, il ventre molle del digitale
- Crescenti truffe ed estorsioni nei confronti di privati, Aziende, PA ed Infrastrutture Critiche (p.es. ospedali)
- Consumerization of Cyber Crime
- Crescenti attività di propaganda, PsyOps e alterazione di massa della percezione (alt-truth) supportata anche da cyber attacchi

Analisi FASTWEB della situazione nazionale

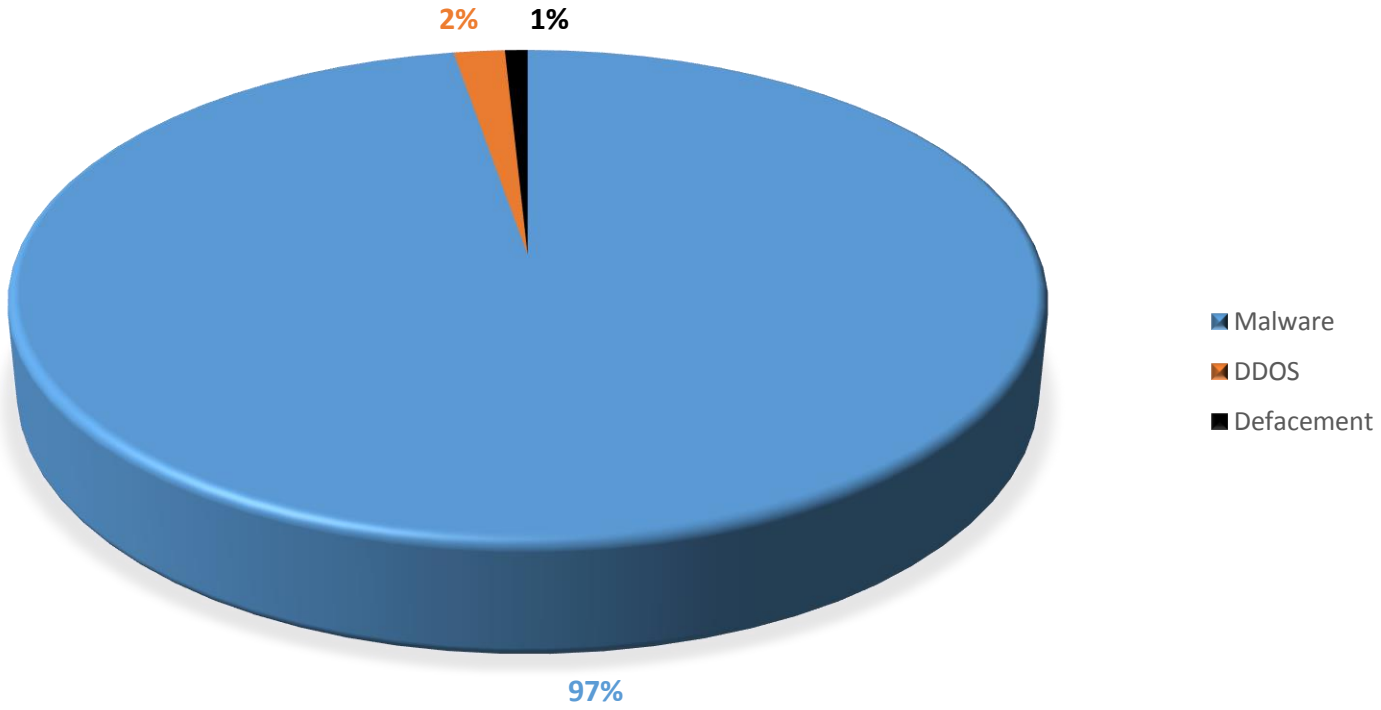
La base dati

16 milioni di eventi di sicurezza (circa il doppio dell'anno precedente)

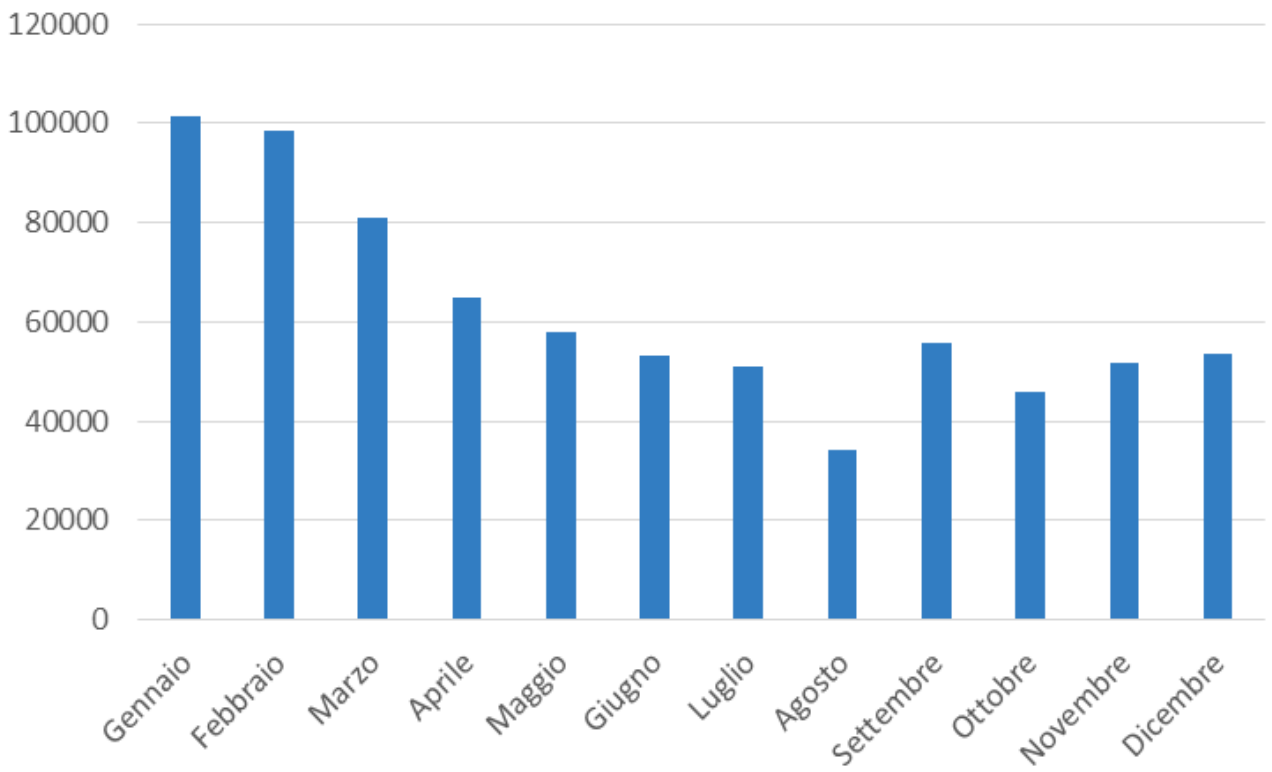
6 milioni di indirizzi IP pubblici

Dati relativi a tutti gli indirizzi IP Fastweb (clienti, Fastweb stessa, FastCloud)

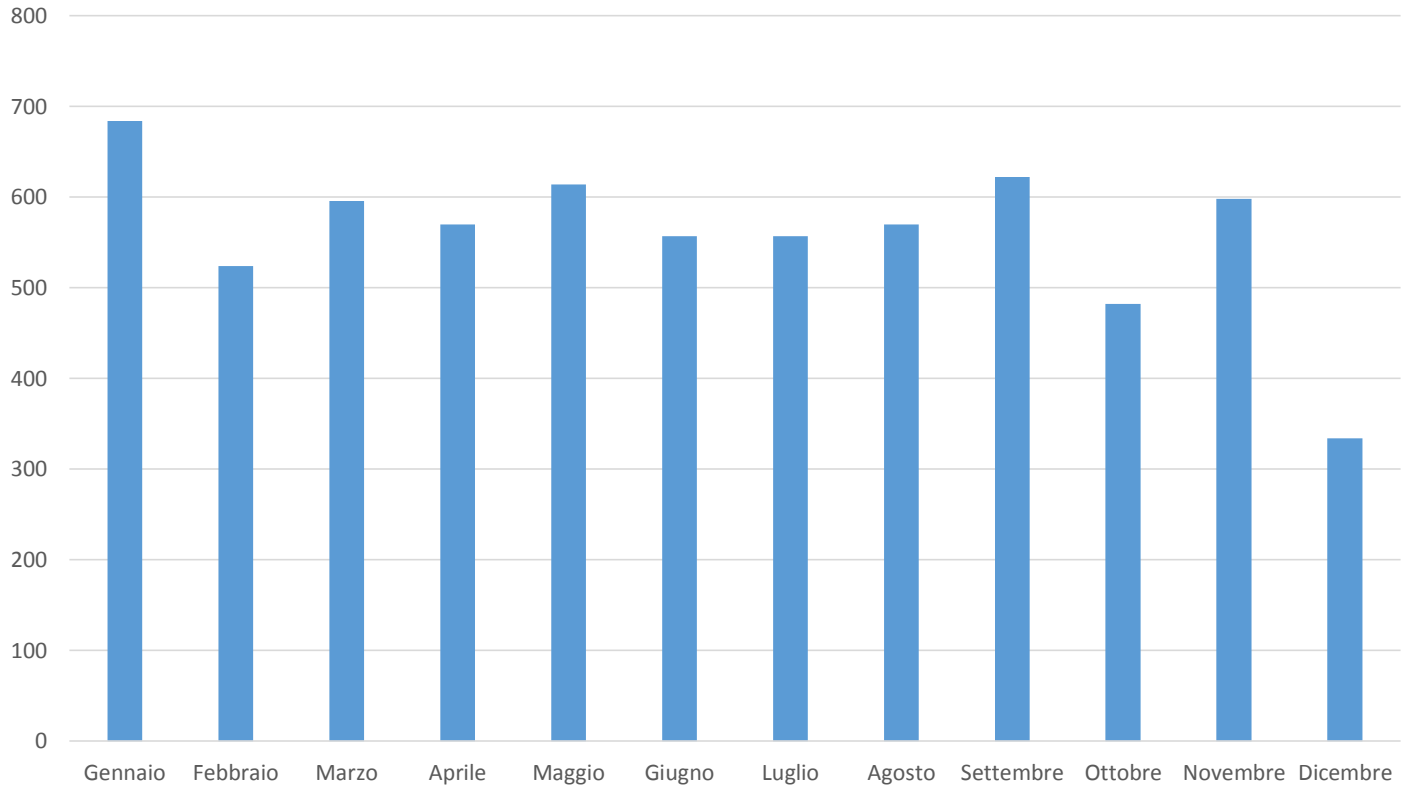
Tipologie di attacchi rilevati



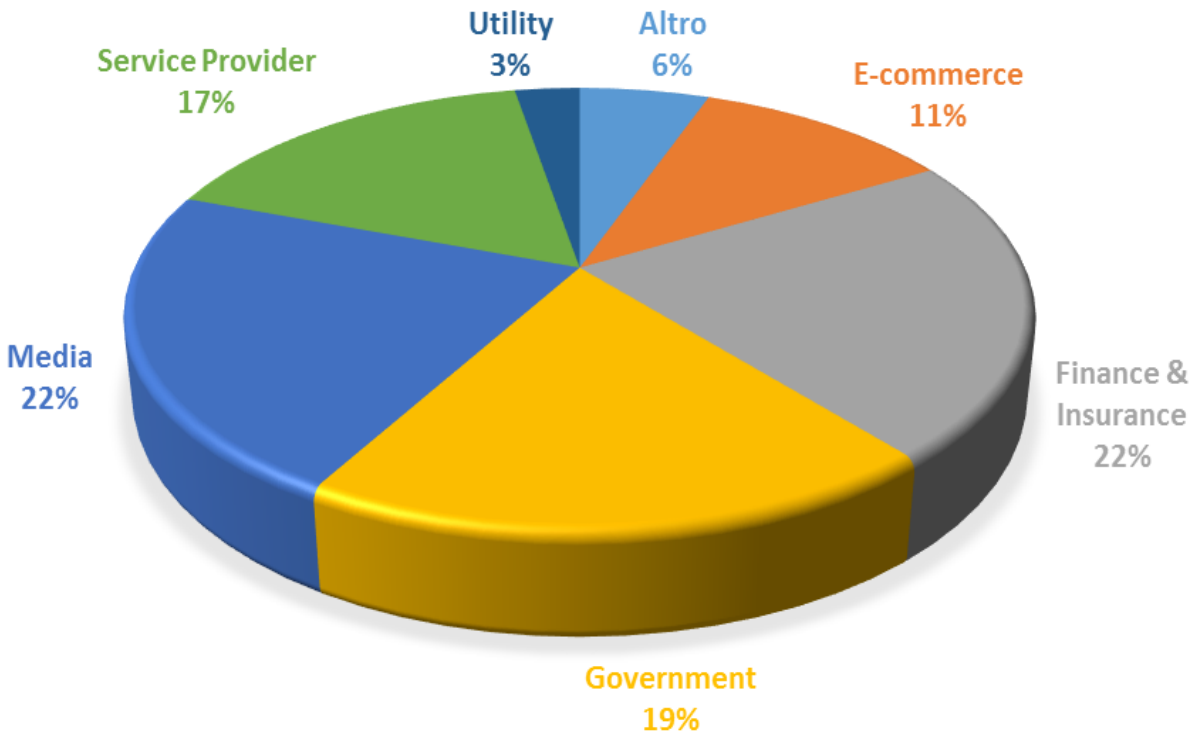
Rilevazione mensile dei malware



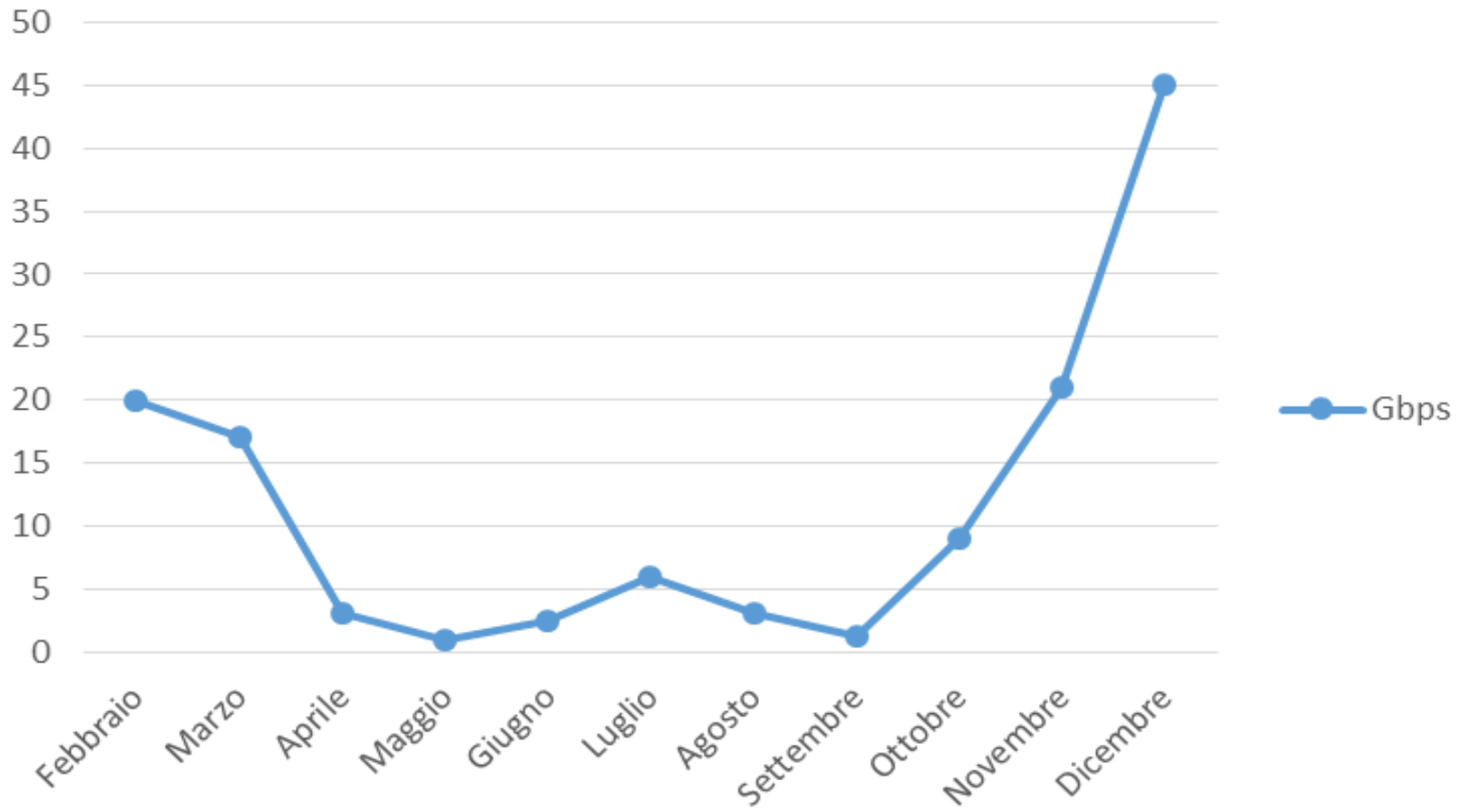
Distribuzione mensile 'anomalie' DDoS



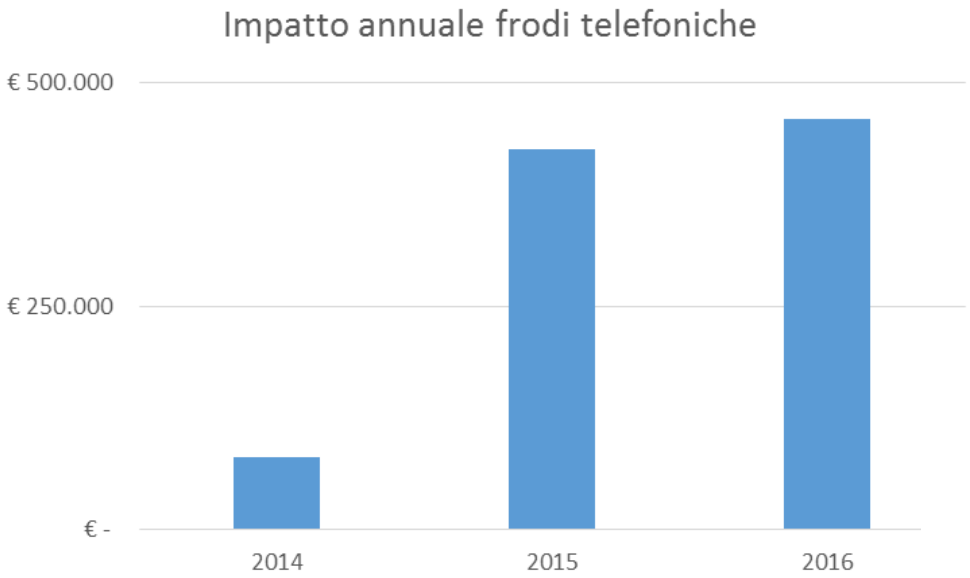
Target di possibili attacchi DDoS

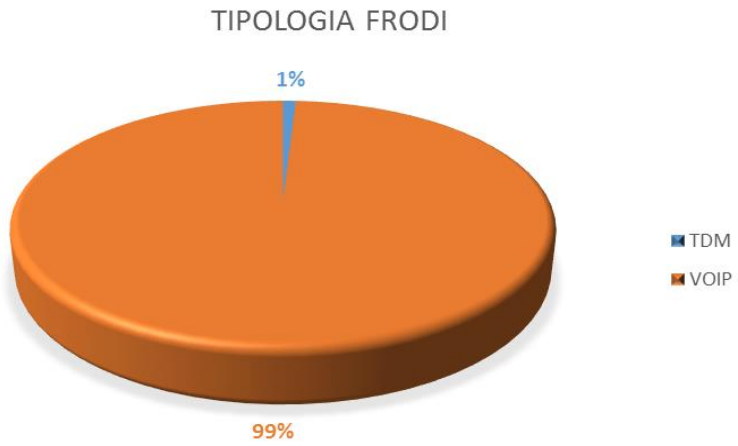


Picchi di traffico relativi ad attacchi DDoS mitigati



Attacchi al VOIP





Conclusioni

Non dimentichiamoci i ransomware!

È aumentato l'interesse e l'attenzione delle aziende

Non solo il settore privato, ma anche il pubblico si muove:

«misure minime di sicurezza ICT» emanate da AgID per le infrastrutture del Settore Pubblico

Nuovo Regolamento Generale sulla Protezione dei Dati Personali (GDPR) definito a livello europeo

Quando inizieranno anche gli altri ISP?

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

Rapporto Clusit 2017 sulla sicurezza ICT in Italia

Moderano:

Gigi Tagliapietra, Presidente Onorario Clusit

Intervengono:

Alessio Pennasilico, uno degli autori del Rapporto Clusit

Partecipano alla Tavola Rotonda:

- Alberto Mercurio, UNIS&F
- Ettore Guarnaccia, Gruppo Intesa Sanpaolo, Divisione Banca dei Territori
- Gianluca Busco Arre', Panda Security Italia
- Salvatore Marcis, Trend Micro

Security Summit Verona 2017

Clusit
Associazione Italiana
per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

SECURITY
TECHNOLOGIES
MANAGEMENT COMPLIANCE
SUMMIT