Security Summit Milano 2017

Sessione Plenaria del 14.03.2017

Clusit
Associazione Italiana
per la Sicurezza Informatica

SECURITY
TECHNOLOGIES
MANAGEMENT COMPLIANCE
SUMMIT

Rapporto Clusit 2017 sulla sicurezza ICT in Italia

Apertura dei lavori: Gabriele Faggioli, Presidente Clusit

Modera: Alessio Pennasilico, Clusit

Intervengono alcuni degli autori:

- Andrea Zapparoli Manzoni, Clusit
- Davide Del Vecchio, Clusit
- Stefano Buttiglione, Akamai

Partecipano alla Tavola Rotonda:

- Gastone Nencini, Trend Micro
- Andrea Piazza, Microsoft
- Federico Santi, Hewlett Packard Enterprise
- Francesco Teodonno, IBM
- Alessandro Vallega, Oracle

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

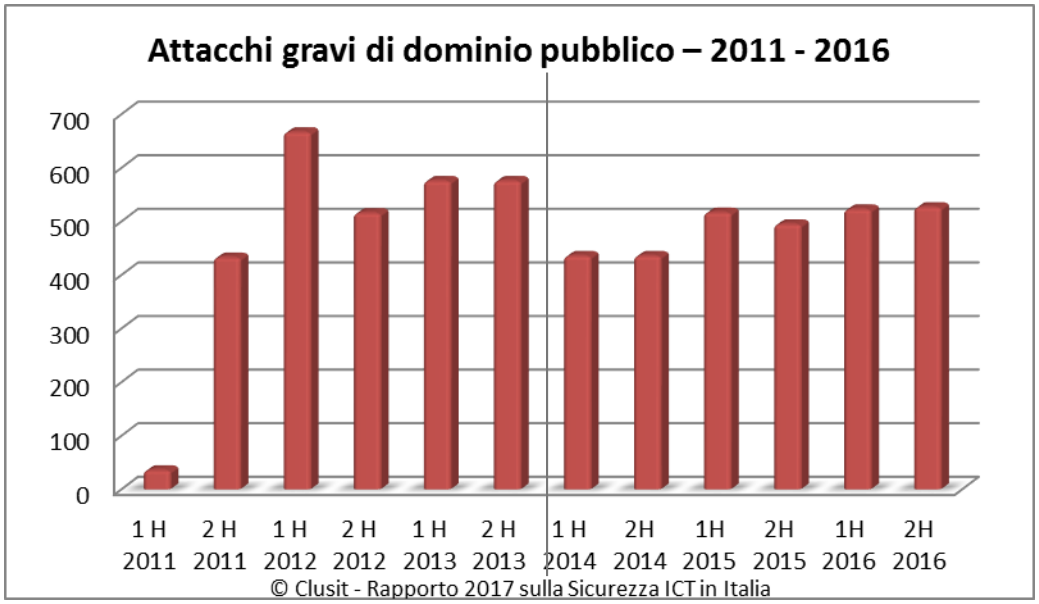
Analisi Clusit dei principali attacchi a livello globale

Quali sono i numeri del campione ?

In media negli ultimi 72 mesi abbiamo analizzato e classificato come gravi 81 incidenti al mese, ogni mese (87,5 al mese nel 2016)

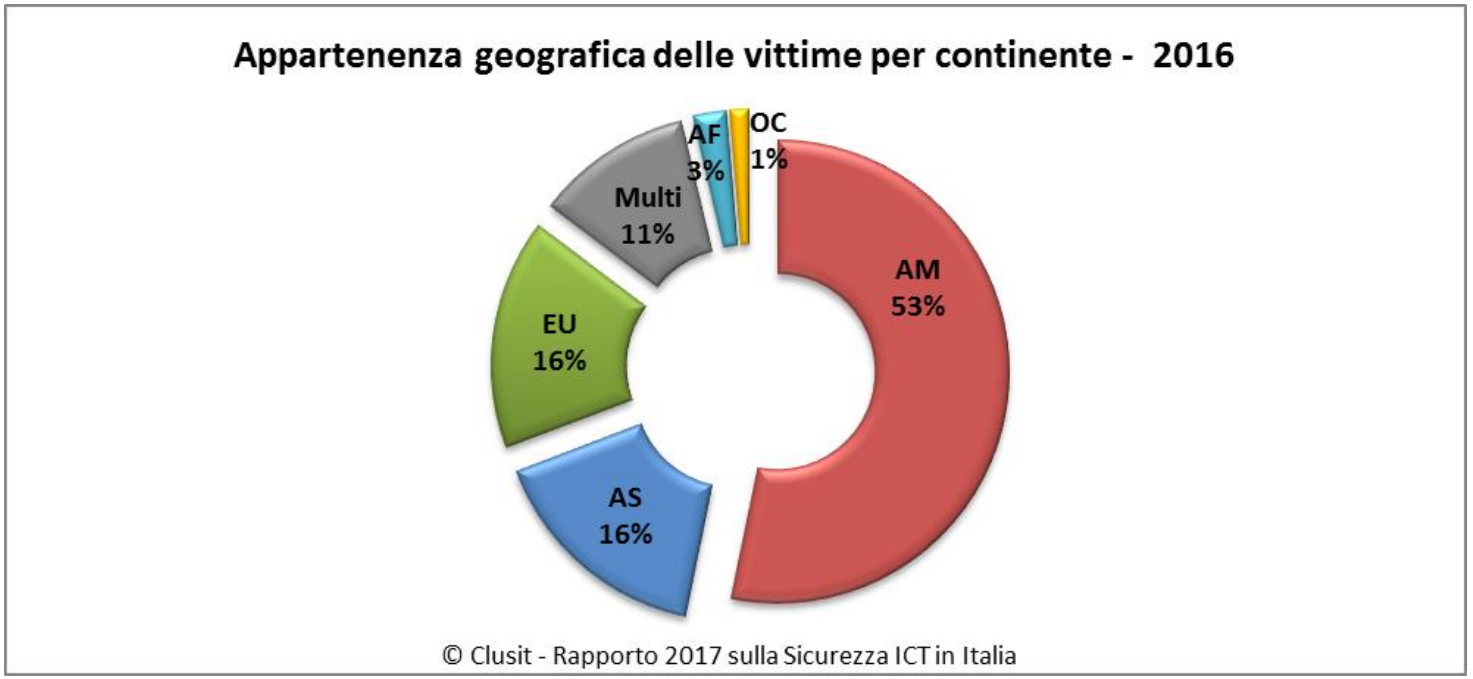
- 5.738 attacchi analizzati dal gennaio 2011 al dicembre 2016.

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



(*) 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 primo semestre 2016, nel secondo semestre in percentuale diminuiscono leggermente le vittime di area americana (dal 55% al 53%), mentre crescono gli attacchi verso realtà basate in Europa (dal 13% al 16%) ed in Asia (dal 15% al 16%).

Da notare che gli attacchi contro realtà asiatiche equivalgono a quelli contro realtà europee. La categoria “Multinational” rimane sostanzialmente stabile al 11% (era il 9% nel 2015), ad indicare la tendenza a colpire bersagli sempre più importanti, di natura transnazionale.

Tipologia e distribuzione degli attaccanti

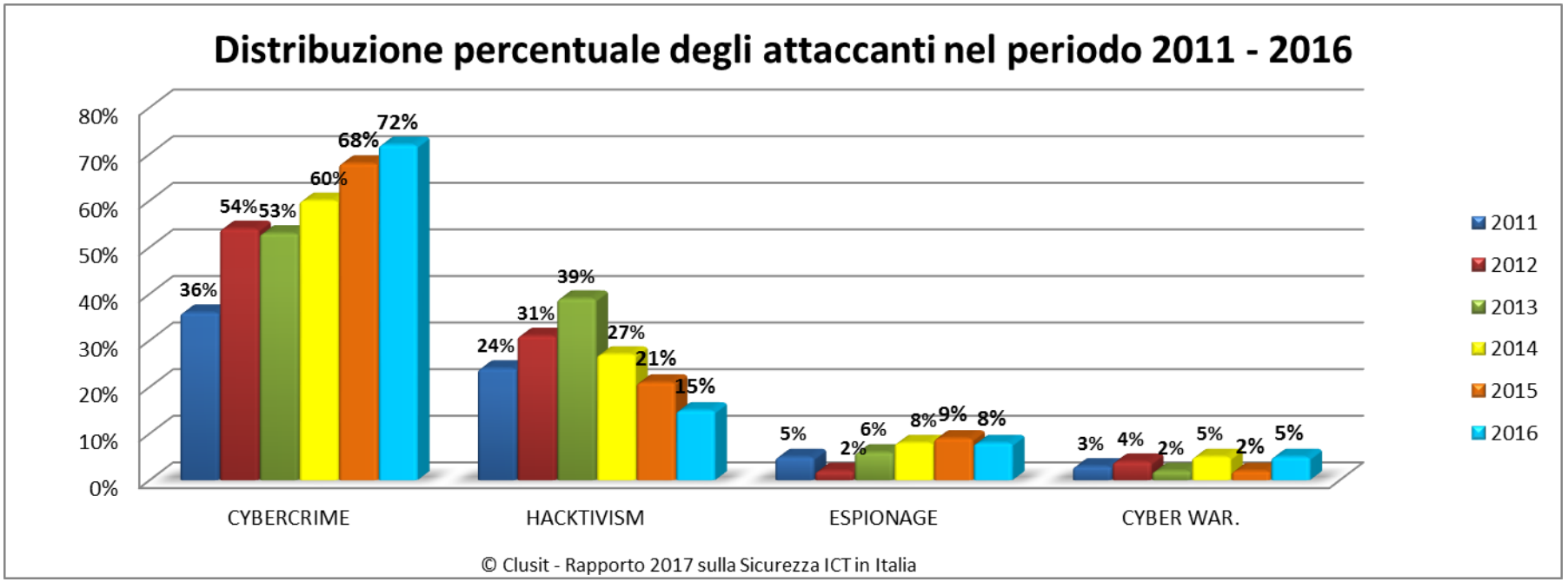
ATTACCANTI PER TIPOLOGIA	2011	2012	2013	2014	2015	2016	Variazioni 2016 su 2015	Trend 2016
Cybercrime	170	633	609	526	684	751	9,80%	↑
Hacktivism	114	368	451	236	209	161	-22,97%	↓
Espionage / Sabotage	23	29	67	69	96	88	-8,33%	↘
Cyber warfare	14	43	25	42	23	50	117,39%	↑
TOTALE	**469**	**1.183**	**1.152**	**873**	**1.012**	**1.050**	**+3,75%**	↗

In termini assoluti, nel 2016 le categorie “Cybercrime” e “Cyber warfare” fanno registrare il numero di attacchi più elevato degli ultimi 6 anni.

Dal campione emerge chiaramente che, con l’esclusione delle attività riferibili ad attacchi della categoria “Hacktivism” che diminuisce sensibilmente (-23%) rispetto al 2015, nel 2016 gli attacchi gravi compiuti per finalità “Cybercrime” sono in aumento (+9,8%), così come quelle riferibili ad attività di “Cyber warfare” (+117%), mentre rimangono sostanzialmente stabili, in lieve calo, gli attacchi del gruppo “Cyber Espionage” (-8%).

Va sottolineato che, rispetto al passato, oggi risulta più difficile distinguere nettamente tra queste due ultime categorie: sommando gli attacchi di entrambe, nel 2016 si assiste ad un aumento del 16% rispetto all’anno precedente (138 contro 119).

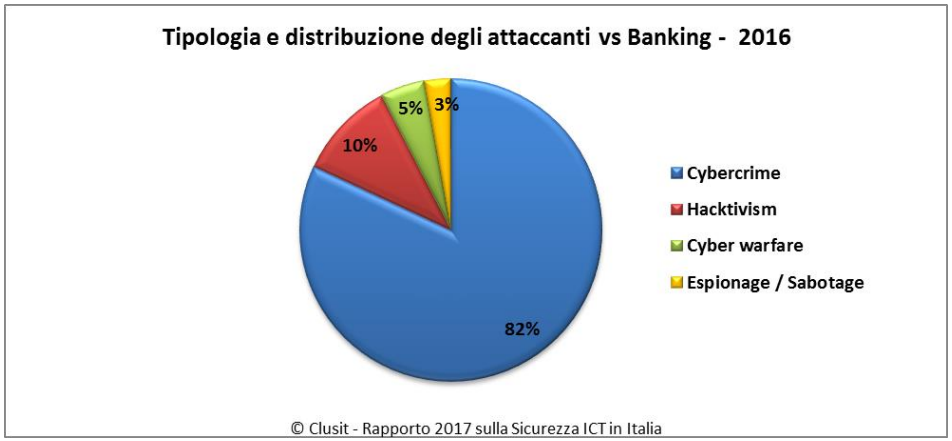
Tipologia e distribuzione degli attaccanti (6 anni)

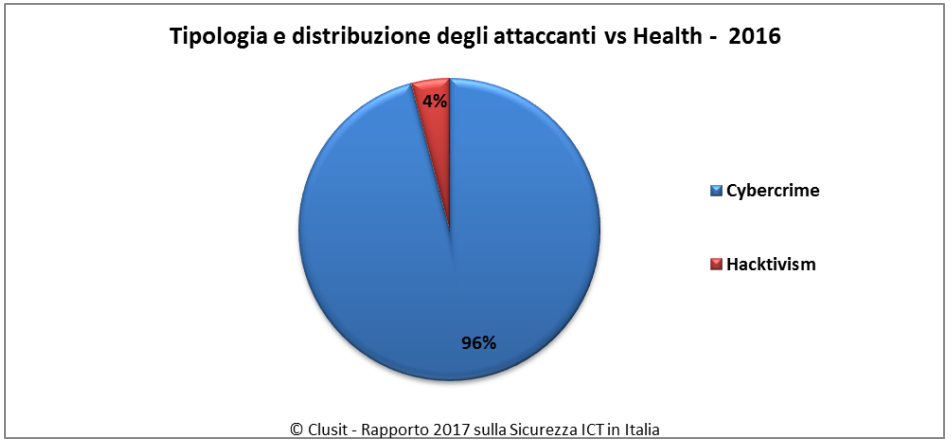


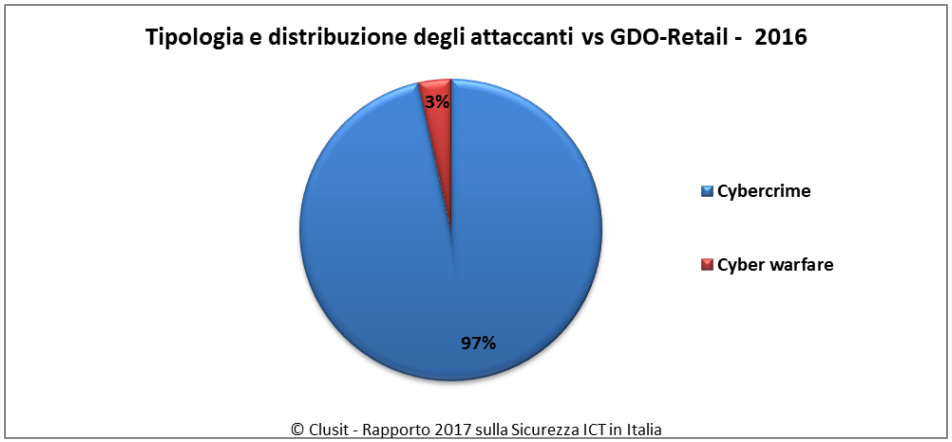
Il Cybercrime passa dal 68% al 72% del totale, mentre l'Hacktivism diminuisce di 23 punti percentuali rispetto al suo picco del 2013, passando da oltre un terzo a meno di un sesto dei casi analizzati.

Per quanto riguarda le attività di Espionage, rispetto alla percentuale degli attacchi gravi registrati nel 2015 la quota di attacchi nel 2016 è in lieve calo (dal 9% al 8% del totale), mentre l'Information Warfare risulta essere in forte crescita (nonostante la scarsità di informazioni pubbliche in merito), dal 2% al 5%.

Tipologia e distribuzione attaccanti nei settori a maggior crescita degli attacchi



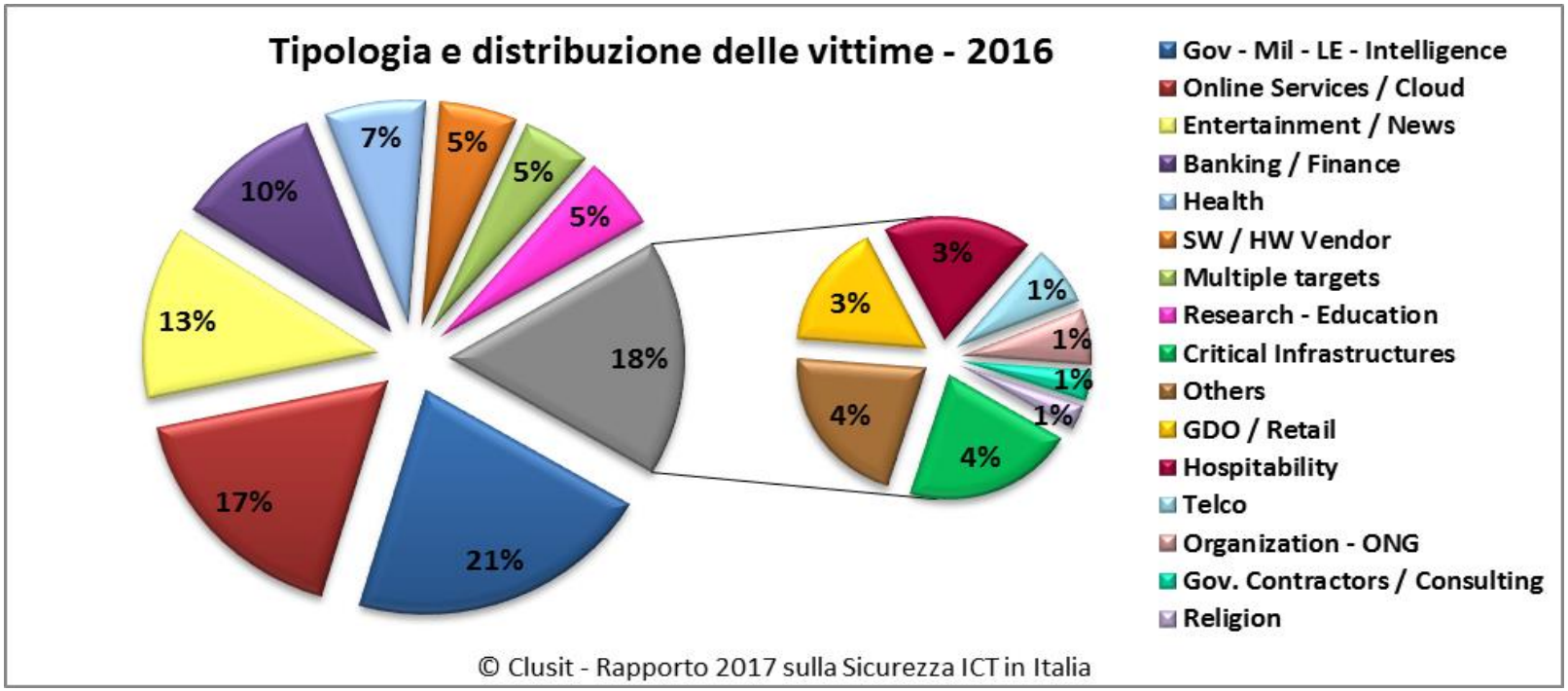




Quest'anno per la prima volta presentiamo le statistiche relative ad alcune categorie di vittime verticali, con un'attenzione particolare verso i primi 3 settori per tasso di crescita degli attacchi rispetto all'anno precedente (Health, Banking e GDO).

La distribuzione degli attaccanti mostra variazioni importanti a seconda della tipologia di bersaglio, il che suggerisce la necessità per ogni settore di adottare contromisure differenti, e di investire in modo mirato le proprie risorse, in conseguenza del proprio specifico Threat Model.

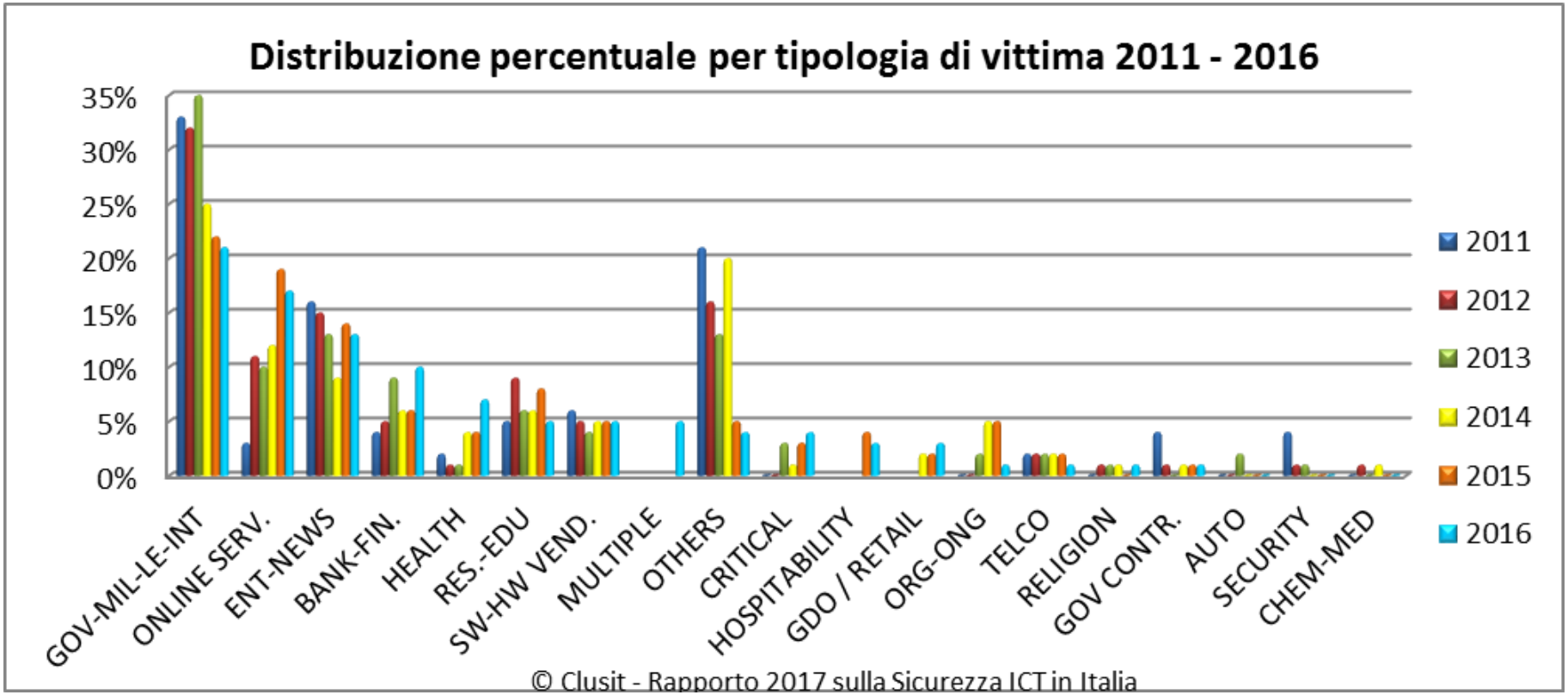
Distribuzione vittime nel mondo (2016)



Al primo posto assoluto, in leggera diminuzione, ancora il settore governativo in senso esteso, con un quinto degli attacchi (21%). La categoria “Online Services / Cloud” nel 2016 si conferma al secondo posto (17%). Al terzo posto la categoria “Entertainment/News” (13%), a seguire “Banking/Finance” (10%) e “Health” (7%).

Il nuovo gruppo di attacchi ricondotti a “Multiple targets” si inserisce a pari merito tra le categorie “Software/Hardware vendor” e “Research/Education” (5% ciascuno del totale), mentre la categoria “Others” (principalmente a causa dell’introduzione della nuova categoria “Multiple targets”), scende al 4%.

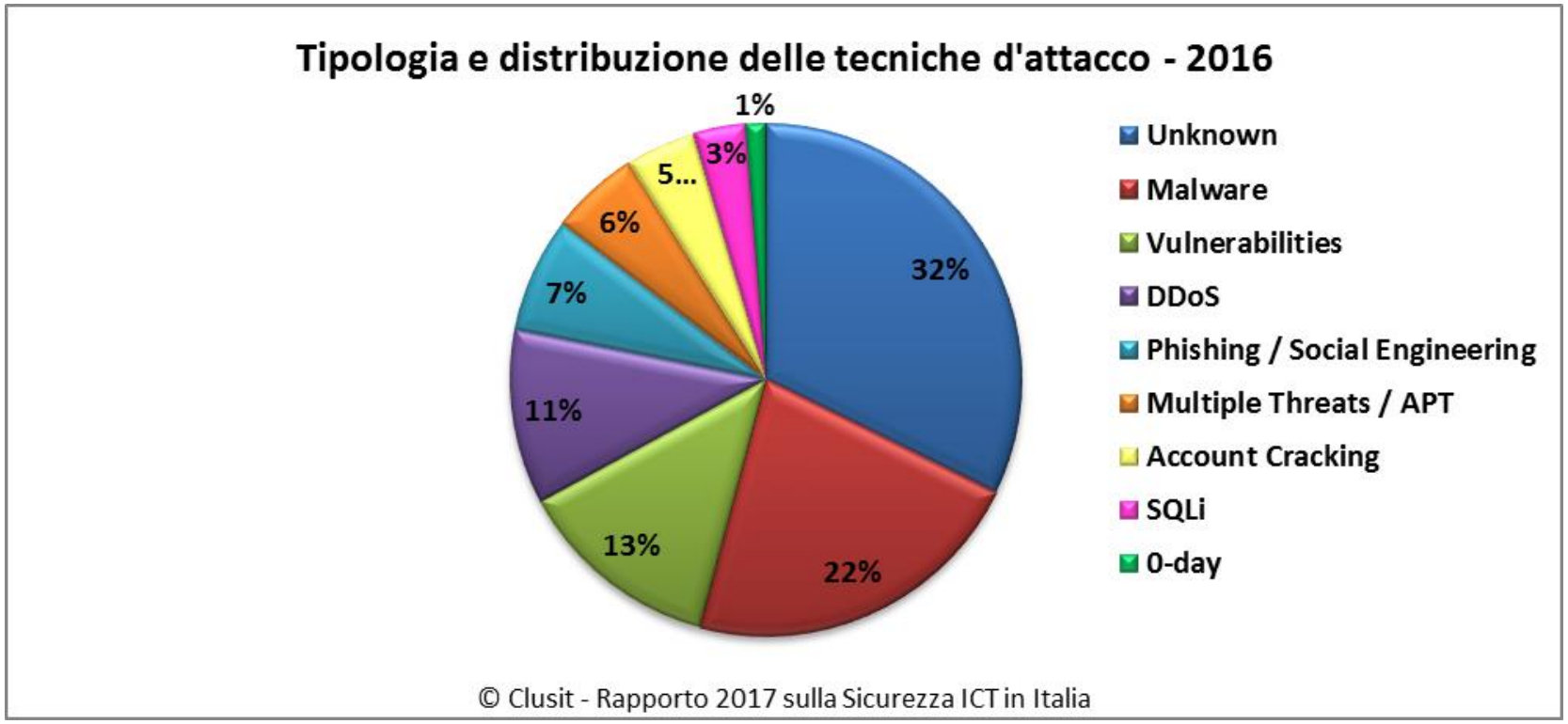
Distribuzione vittime nel mondo (6 anni)



Rispetto al 2015, nel 2016 la crescita percentuale maggiore di attacchi gravi si osserva verso le categorie “Health” (+102%), “GDO/Retail” (+70%) e “Banking / Finance” (+64%), seguite da “Critical Infrastructures” (+15%).

Rimangono stabili, sia pure con un leggero calo, gli attacchi verso i settori “Gov” (tipicamente con finalità di Espionage o di Hacktivism), “Entertainment / News”, “Online Services / Cloud”, e “Software/Hardware vendor.

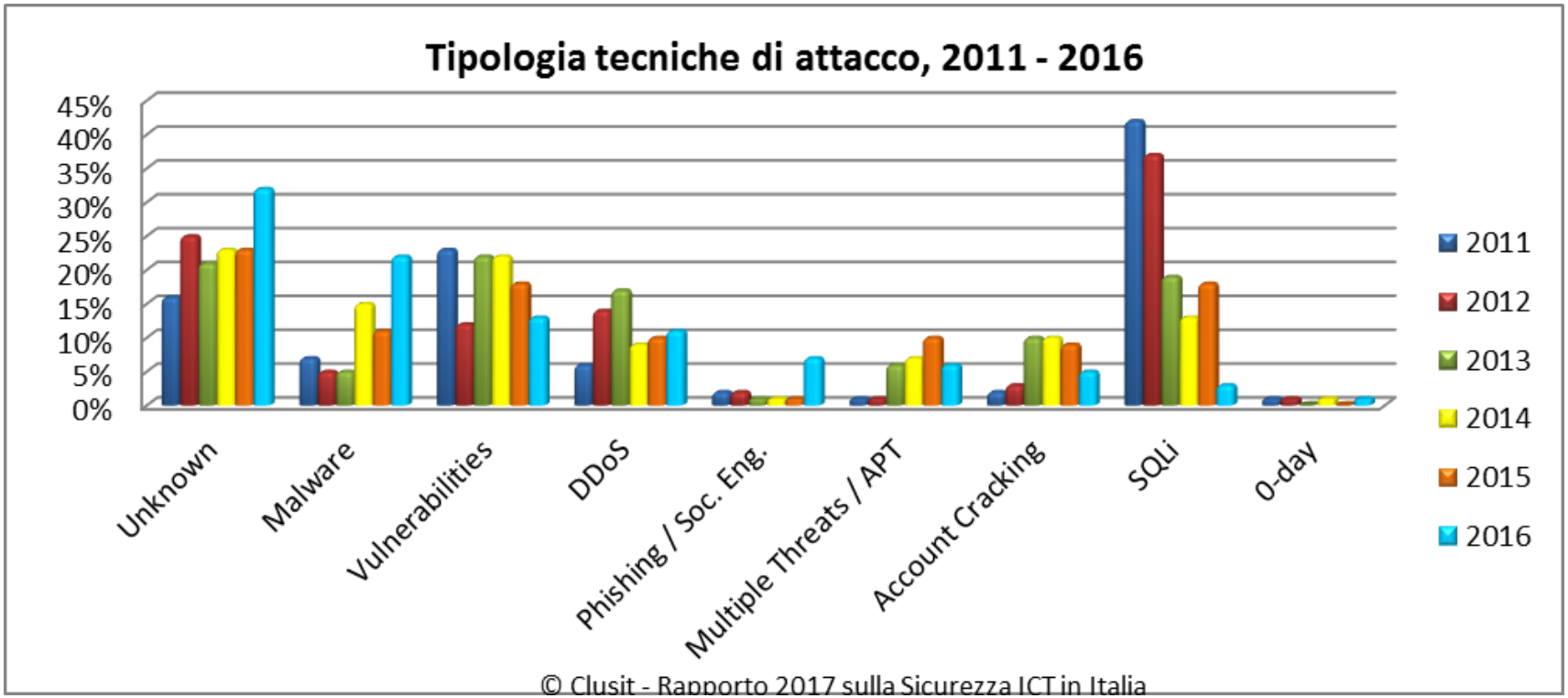
Tecniche di attacco nel mondo (2016)



Diminuiscono sensibilmente le SQLinjection, che nel 2016 passano dal 18 al 3% del totale. Crescono invece fortemente gli attacchi realizzati a partire da attività di Phishing e Social Engineering, che passano dal 1% al 7% del totale.

Sostanzialmente stabili dal punto di vista numerico gli attacchi DDoS (11%), che però nel corso del 2016 hanno in alcuni casi raggiunto volumi di traffico vicini o superiori al Gigabit per secondo, un record assoluto.

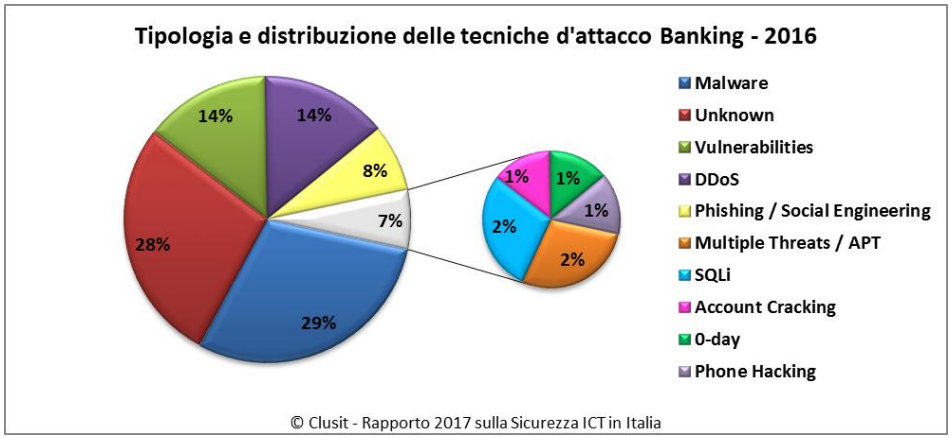
Tecniche di attacco nel mondo (6 anni)

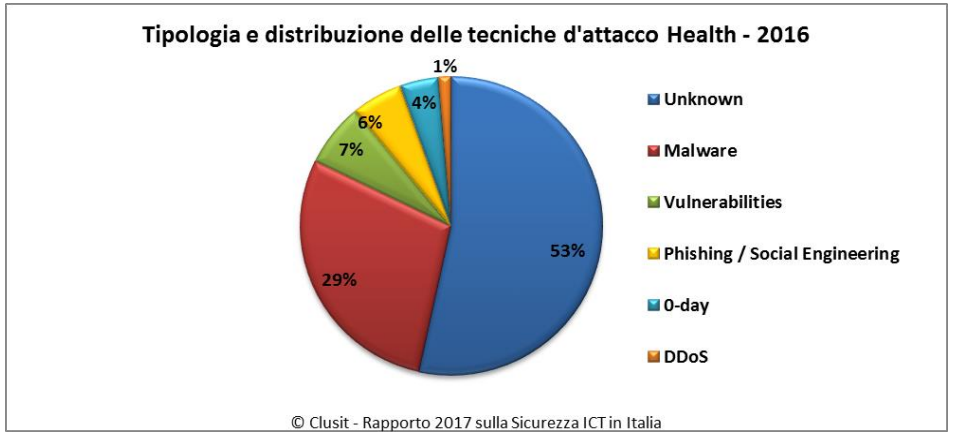


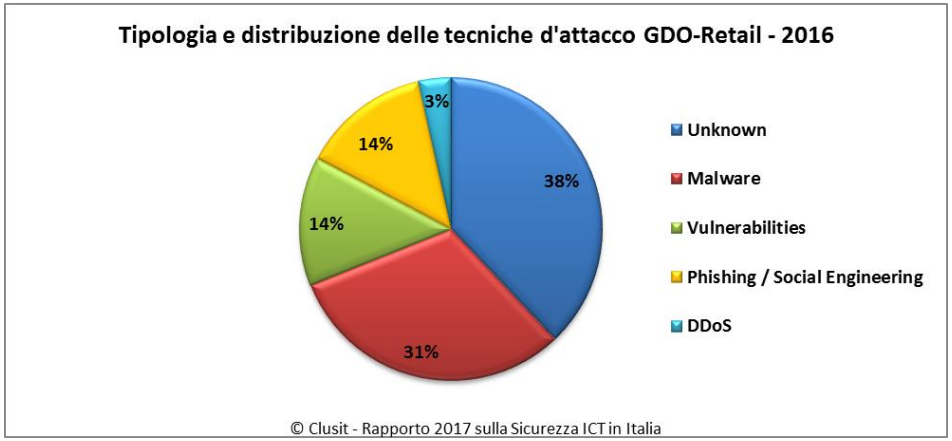
Ritornano ad aumentare il "Malware" comune (+116%), i DDoS (+13%) e l'utilizzo di vulnerabilità "0-day", (+ 333%, per quanto su un numero di incidenti noti limitato), e soprattutto cresce percentualmente in maniera notevolissima la categoria "Phishing/Social Engineering" (+1.166%).

Il fatto che la somma delle tecniche di attacco più banali (SQLi, DDoS, Vulnerabilità note, phishing, malware "semplice") rappresentino ben il 56% del totale (era il 57% nel 2015), implica che gli attaccanti riescono ancora a realizzare attacchi di successo contro le loro vittime con troppa semplicità e costi molto bassi.

Tipologia e distribuzione tecniche di attacco nei settori a maggior crescita degli attacchi







Quest'anno per la prima volta presentiamo le statistiche relative ad alcune categorie di vittime verticali, con un'attenzione particolare verso i primi 3 settori per tasso di crescita degli attacchi rispetto all'anno precedente (Health, Banking e GDO).

Anche la distribuzione delle tecniche di attacco mostra variazioni importanti a seconda della tipologia di bersaglio, il che suggerisce la necessità per ogni settore di adottare contromisure differenti, e di investire in modo mirato le proprie risorse, in conseguenza del proprio specifico Threat Model.

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

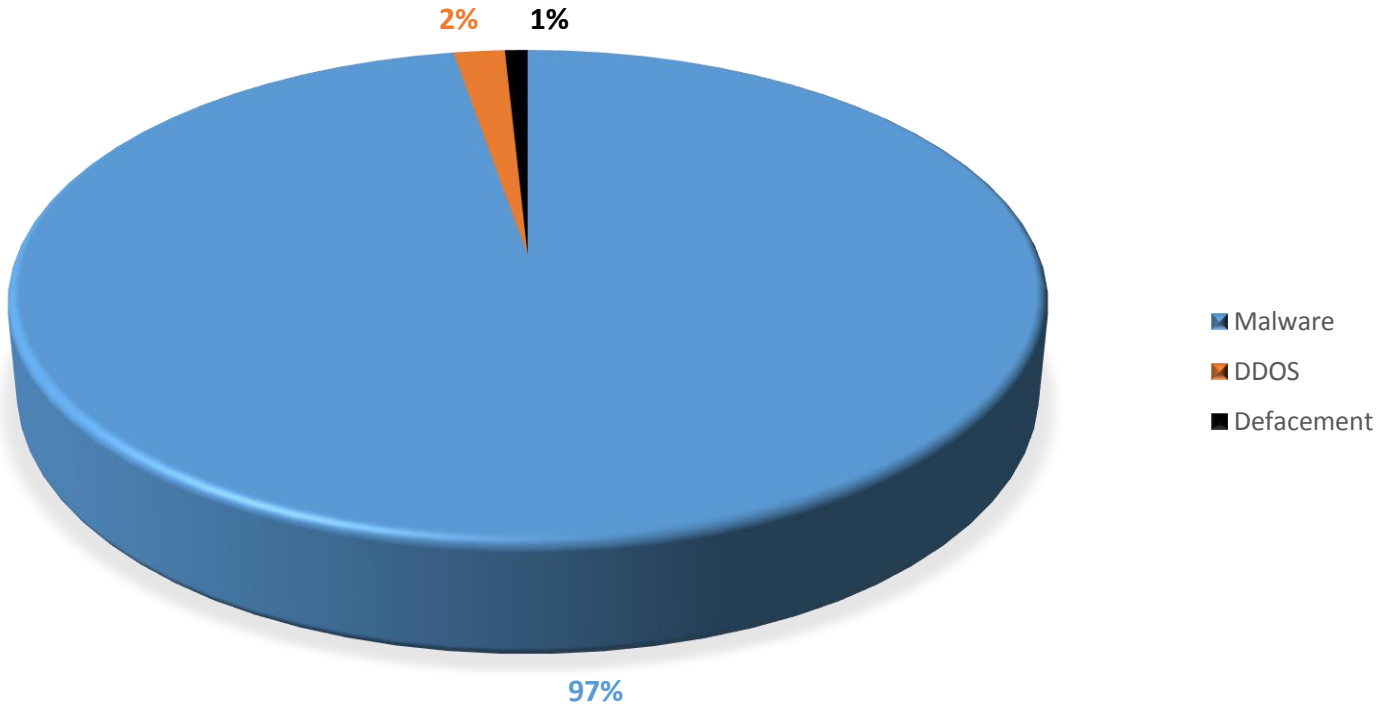
La base dati

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

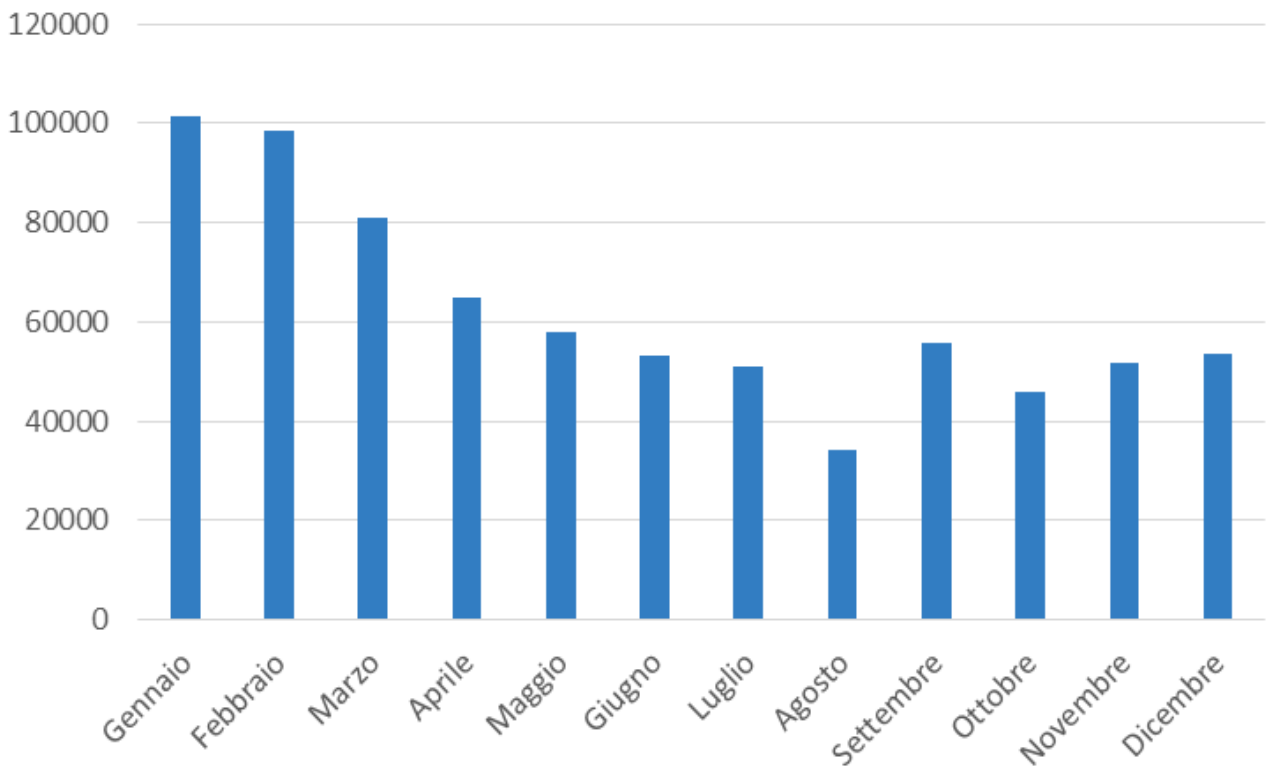
6 milioni di indirizzi IP pubblici

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

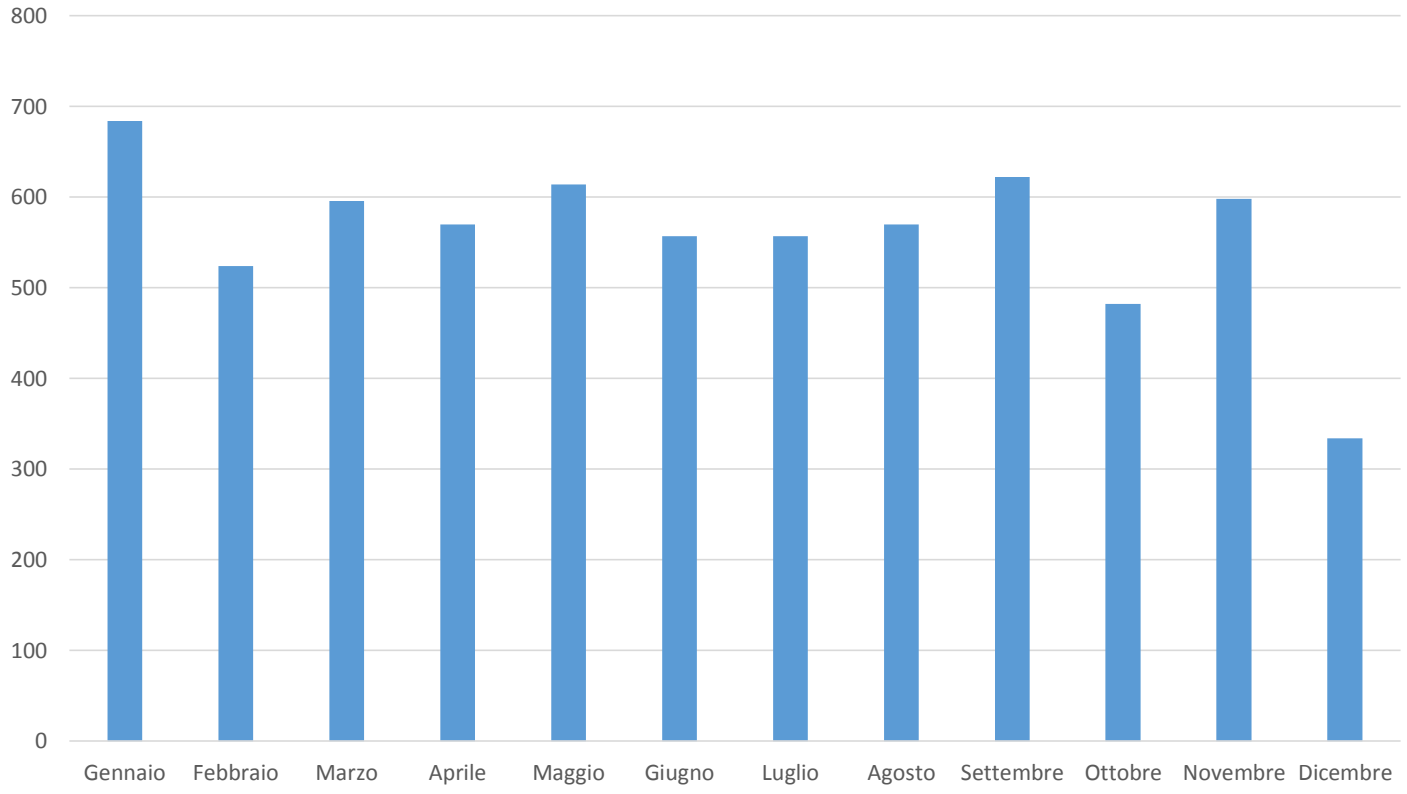
Tipologie di attacchi rilevati



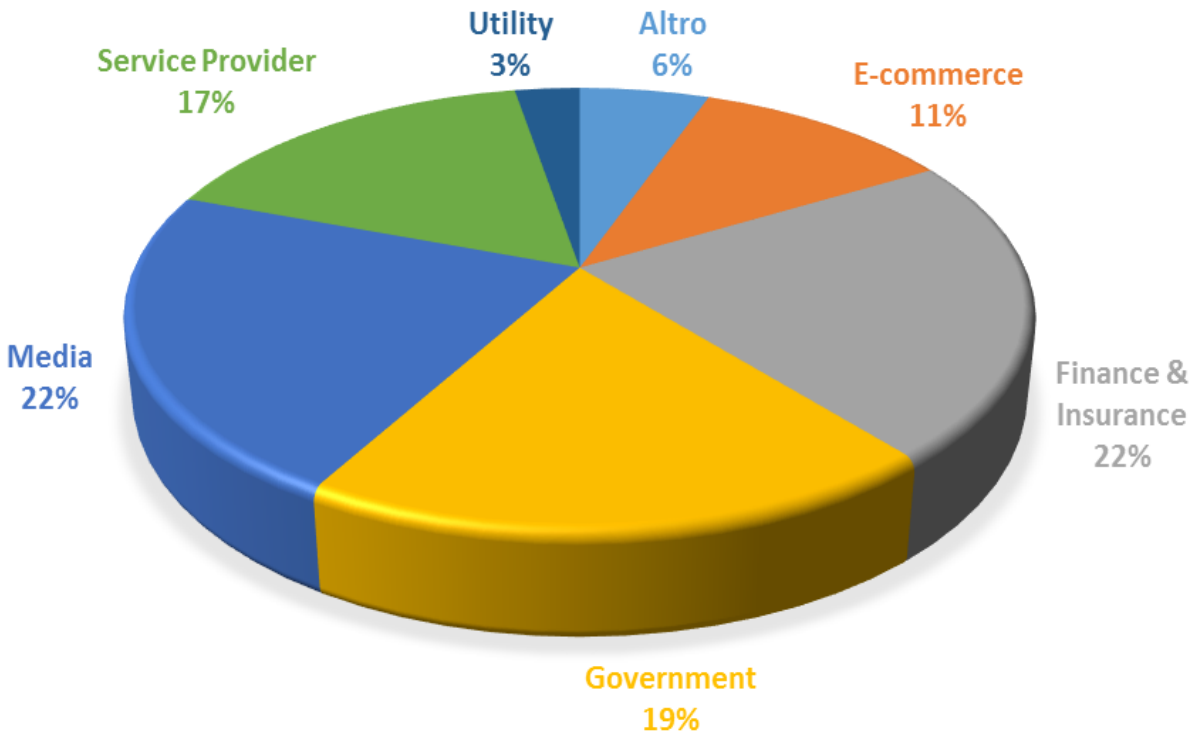
Rilevazione mensile dei malware



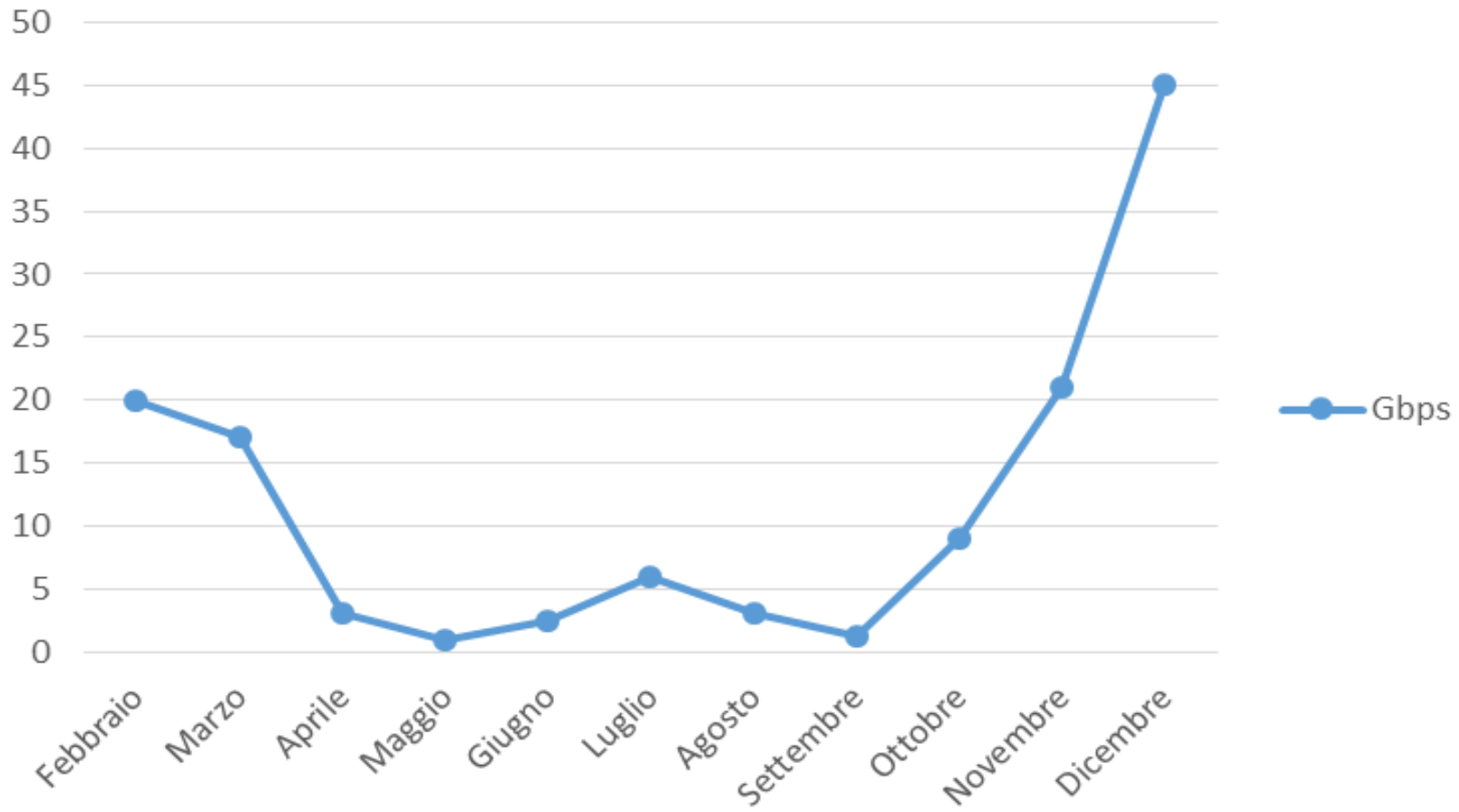
Distribuzione mensile 'anomalie' DDoS



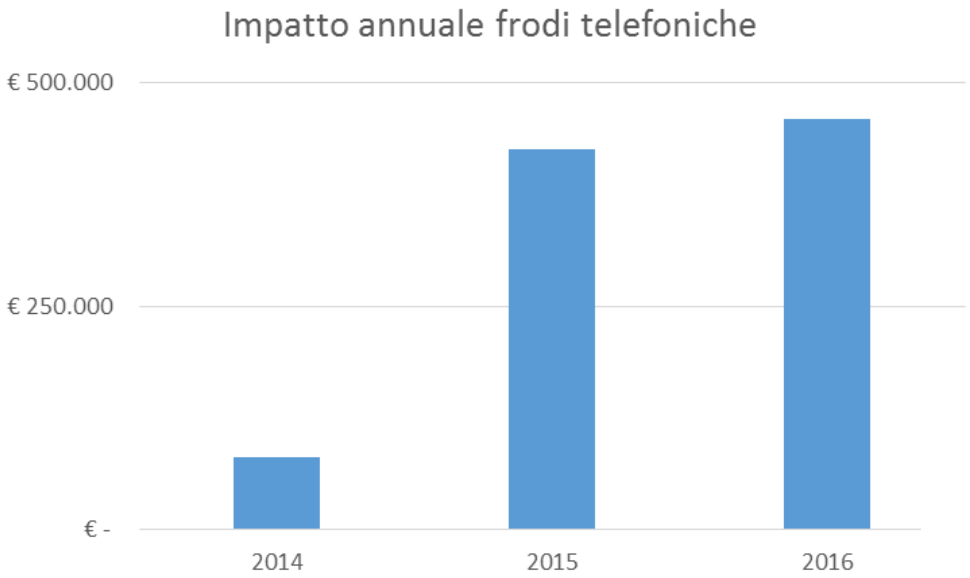
Target di possibili attacchi DDoS

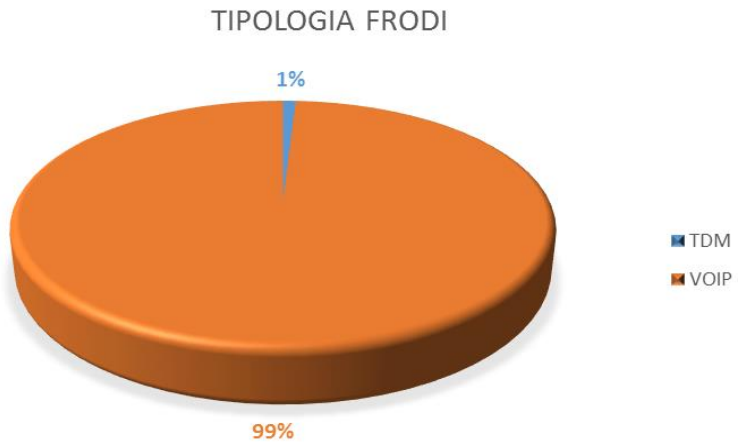


Picchi di traffico relativi ad attacchi DDoS mitigati



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:

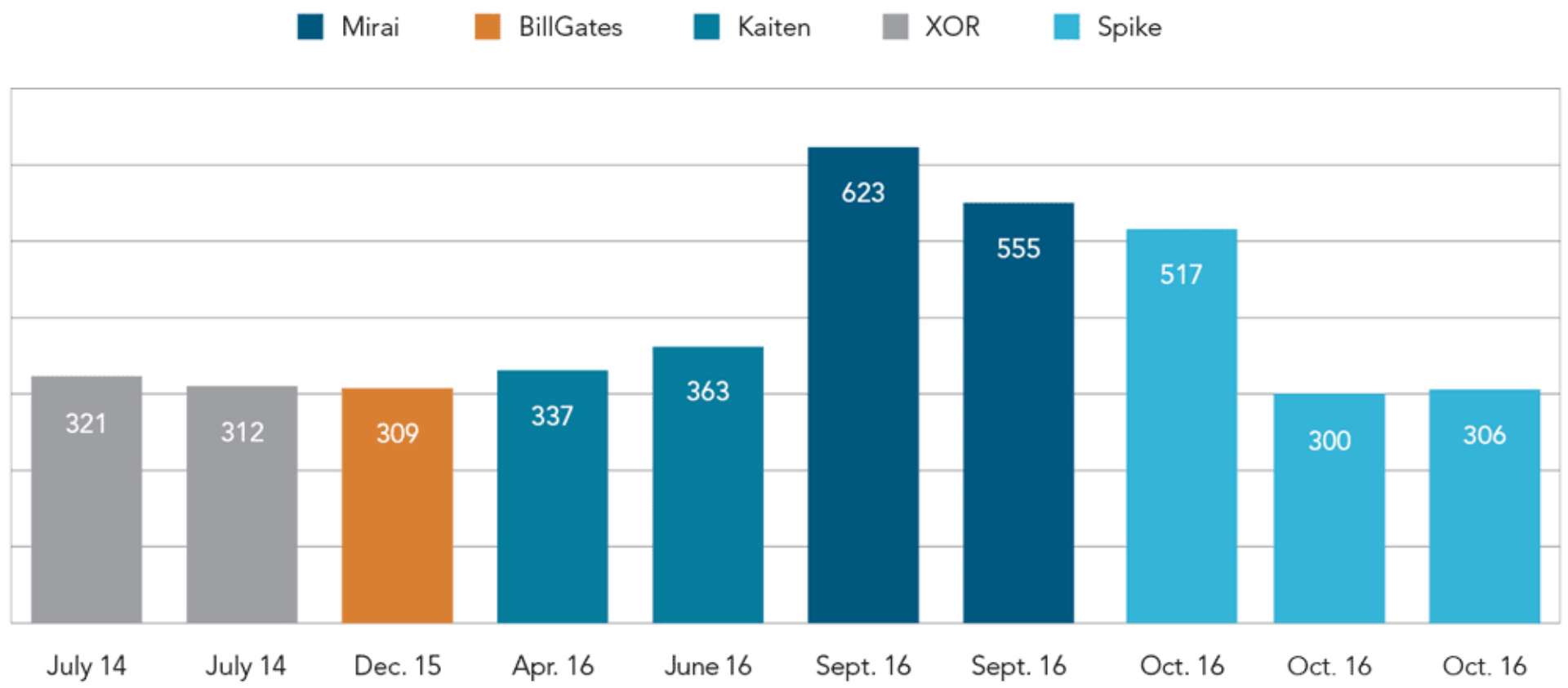
«misure minime di sicurezza ICT» emanate da AgID per le infrastrutture del Settore Pubblico

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

Quando inizieranno anche gli altri ISP?

Rapporto 2016
sullo stato di Internet e analisi globale degli attacchi DDoS e applicativi Web

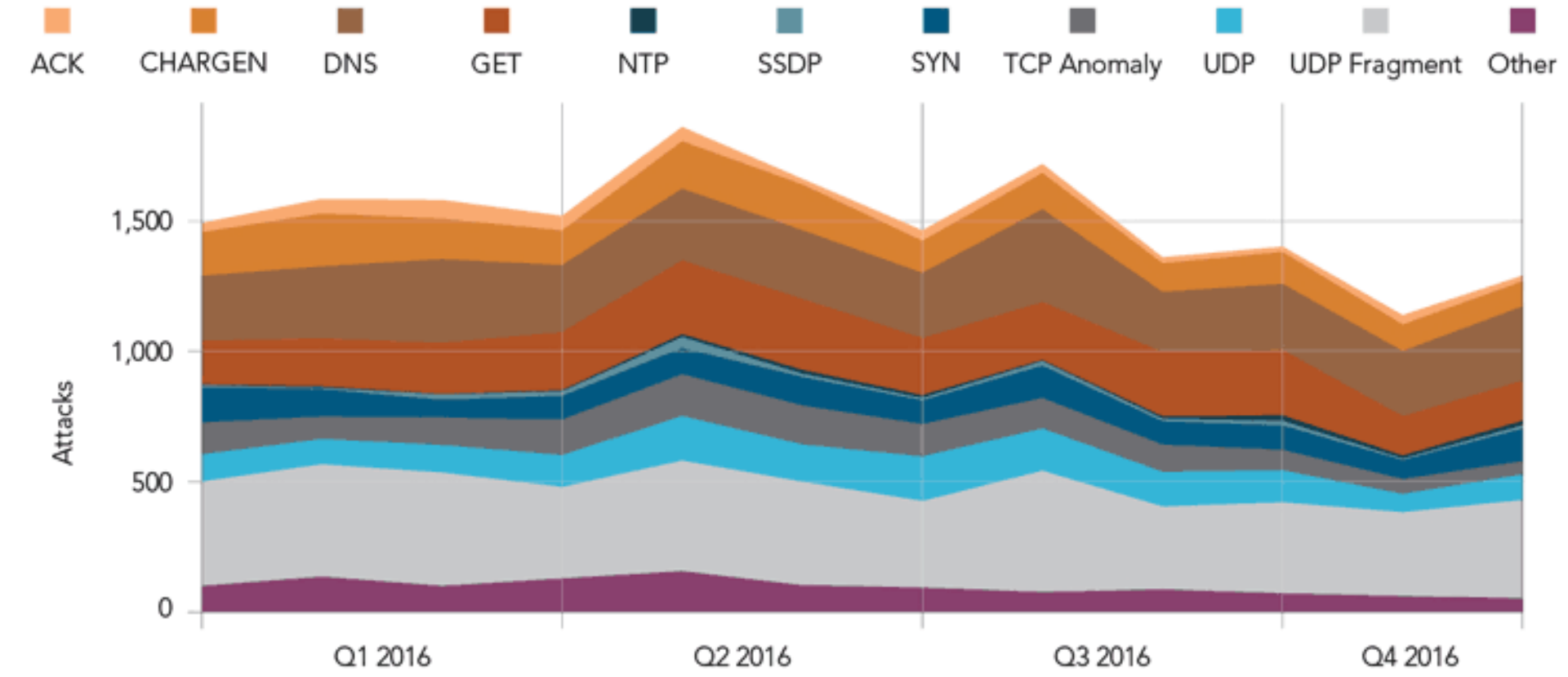
Rapporto Clusit 2017 sulla sicurezza ICT in Italia



Un anno record per la dimensione degli attacchi: 7 oltre i 300 Gbps solo nel 2016.

Kaiten/Mirai ma non solo: Spike, BillGates, XOR

Rapporto Clusit 2017 sulla sicurezza ICT in Italia



Frammentazione UDP, flood UDP, DNS Reflection, corrispondono al 54% del totale

Gli attacchi NTP Reflection, analizzati nel nostro report, sono in discesa

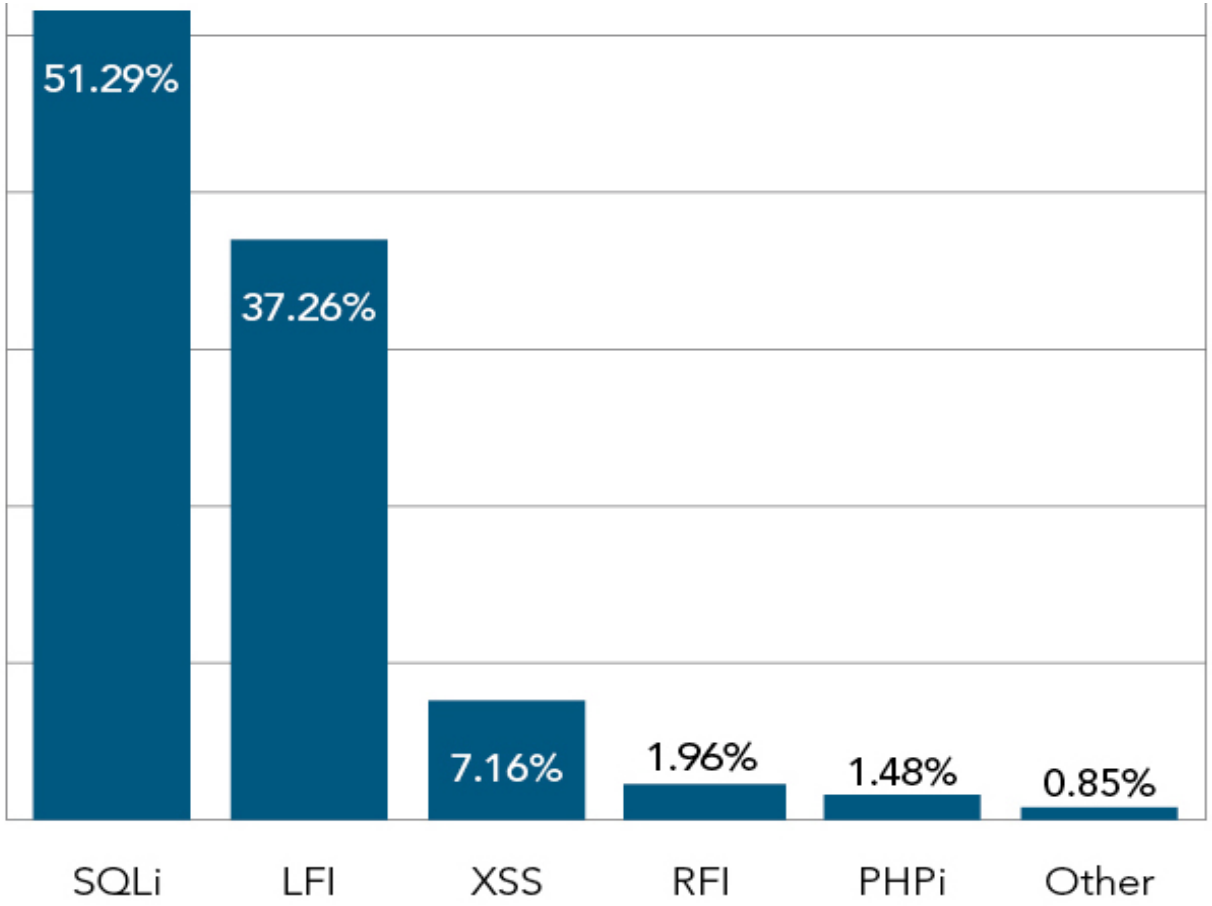
Rapporto Clusit 2017 sulla sicurezza ICT in Italia

Top 5 Source Countries for DDoS Attacks, Q1–Q4 2016

Q1 2016		Q2 2016		Q3 2016		Q4 2016	
Country	Percentage Source IPs	Country	Percentage Source IPs	Country	Percentage Source IPs	Country	Percentage Source IPs
China	16%	China	40%	China	19%	U.S.	24%
	115,478		306,627		81,276		180,652
U.S.	10%	U.S.	12%	U.S.	14%	U.K.	10%
	72,598		95,004		59,350		72,949
Turkey	6%	Taiwan	4%	U.K.	10%	Germany	7%
	43,400		28,546		44,460		49,408
Brazil	5%	Canada	3%	France	6%	China	6%
	36,472		20,601		23,980		46,783
South Korea	4%	Vietnam	3%	Brazil	3%	Russia	4%
	31,692		20,244		13,502		33,211

Le botnet IoT hanno mostrato la reale posizione delle sorgenti di attacco

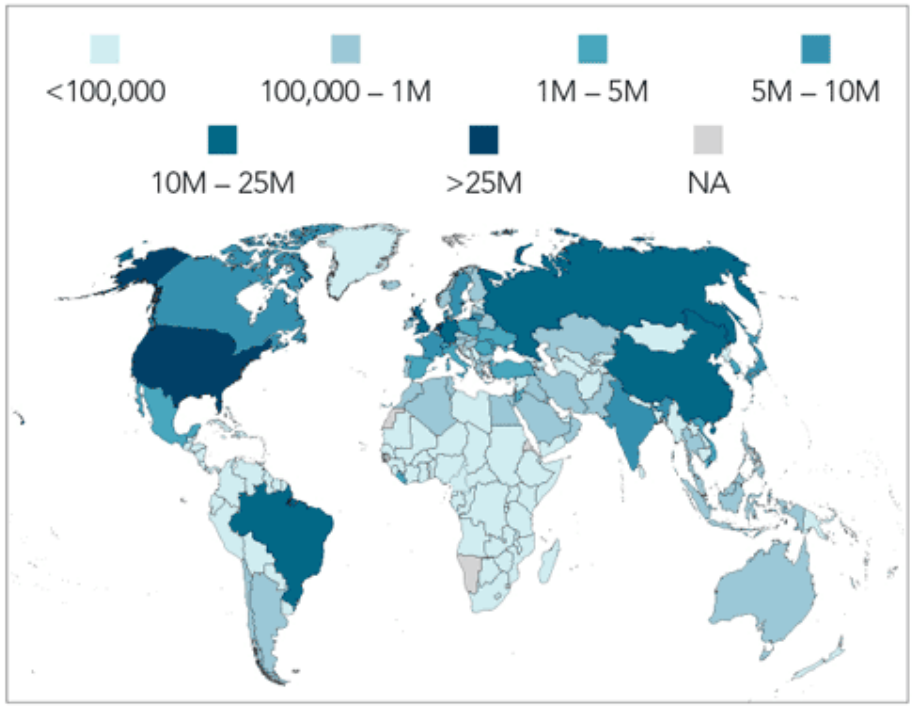
Rapporto Clusit 2017 sulla sicurezza ICT in Italia



Tre vettori compongono il 96% del totale degli attacchi applicativi

Il 68% degli attacchi sono stati eseguiti su protocollo HTTP invece che HTTPS

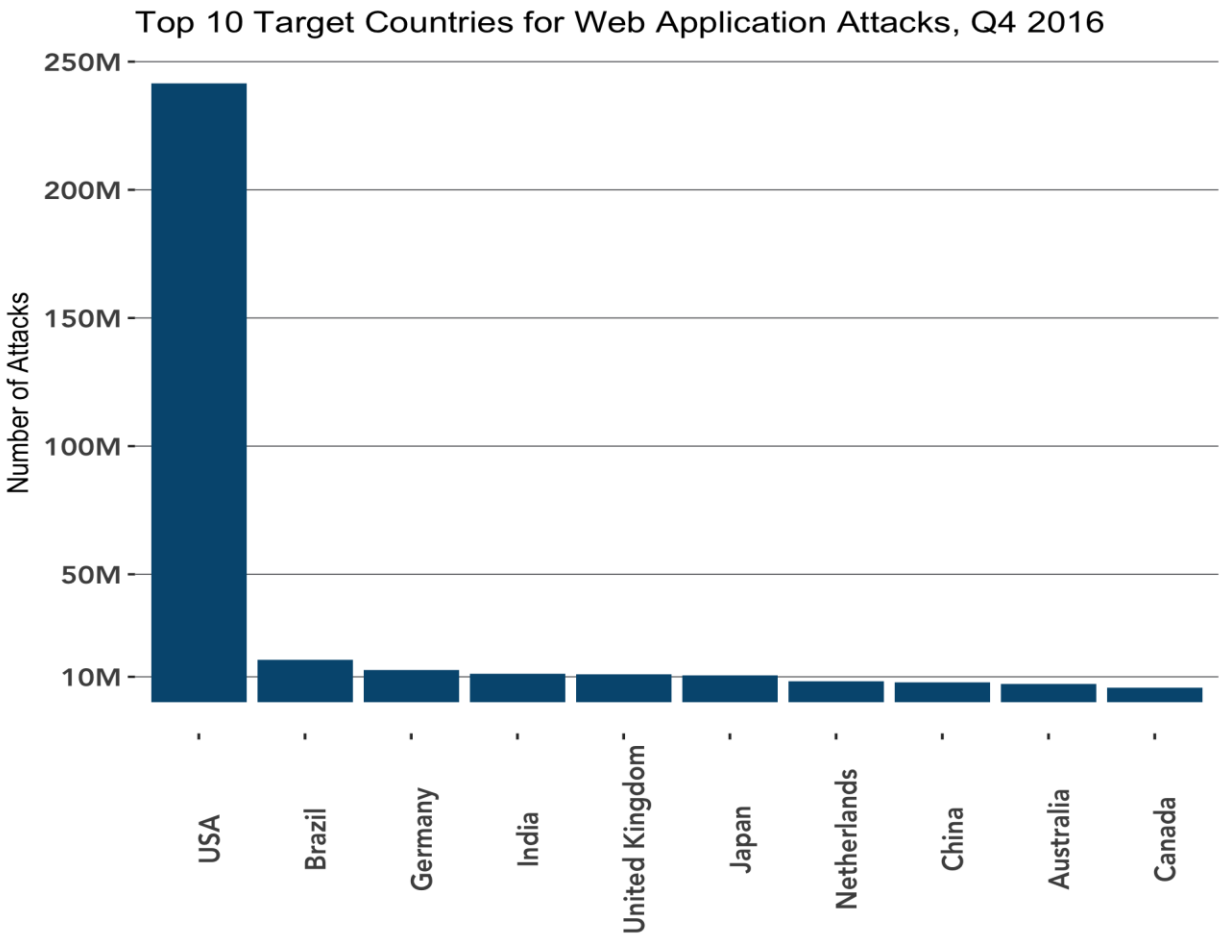
Rapporto Clusit 2017 sulla sicurezza ICT in Italia



Country	Attacks Sourced	Percentage
U.S.	97,918,896	28%
Netherlands	61,499,919	17%
Germany	32,384,205	9.2%
Brazil	19,379,729	5.5%
Russia	16,643,150	4.7%
China	14,275,358	4.0%
U.K.	11,908,055	3.4%
Lithuania	9,793,507	2.8%
France	8,772,176	2.5%
India	8,638,666	2.4%

Gli Stati Uniti sono la principale sorgente di attacchi applicativi web (28%)
Seguono Olanda (17%), Germania (9.2%), Brasile (5.5%)

Rapporto Clusit 2017 sulla sicurezza ICT in Italia



Moltissime organizzazioni, e le loro infrastrutture, hanno sede negli Stati Uniti

L'Olanda, nonostante sia una principale sorgente di attacco, non è tra i primi paesi colpiti

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