ASTREA

Security Summit Verona

4 ottobre 2018

Clusit
Associazione Italiana
per la Sicurezza Informatica

SECURITY 10 ANNI
TECHNOLOGIES
MANAGEMENT COMPLIANCE
SUMMIT

Rapporto Clusit 2018 aggiornato al 30 giugno 2018

Modera: Gigi Tagliapietra, Presidente Onorario Clusit

Intervengono alcuni degli autori:

- Alessio L.R. Pennasilico, Clusit
- Luca Bechelli, Clusit

Partecipano alla Tavola Rotonda:

- Corrado Broli, Darktrace
- Gianluca Busco Arrè, Panda Security Italia
- Salvatore Marcis, Trend Micro
- Antonio Pusceddu, F-Secure Italy

Panoramica dei cyber attacchi più significativi del 2017 e del primo semestre 2018

- Introduzione e analisi dei principali attacchi a livello globale
- Analisi **FASTWEB** della **situazione italiana** in materia di cyber-crime e incidenti informatici
- Rapporto 2017 sullo stato di Internet ed analisi globale degli **attacchi DDoS** e applicativi Web
- **Ransomware 2017** in Italia – WannaCry, NotPetya/EternalPetya, BadRabbit… ma non solo
- Le attività nel 2017 della **Polizia Postale e delle Comunicazioni**
- Le segnalazioni del **CERT NAZIONALE** e del **CERT-PA**

Speciale FINANCE

- Elementi sul Cyber-crime nel settore finanziario in **Europa**
- Analisi del Cyber-crime in **Italia** in ambito finanziario nel 2017
- **Carding** – Tecniche di vendita: evoluzioni recenti e future".

Speciale GDPR

- **GDPR** ai blocchi di partenza
- La **notifica del Data breach**: opportunità o adempimento burocratico?
- **Survey** realizzata dagli Osservatori del **Politecnico** di Milano sull'impatto del GDPR sulle aziende italiane

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

- Un’analisi realizzata appositamente per il Rapporto Clusit alla fine del 2017 da

IDC
ANALYZE THE FUTURE

FOCUS ON 2018

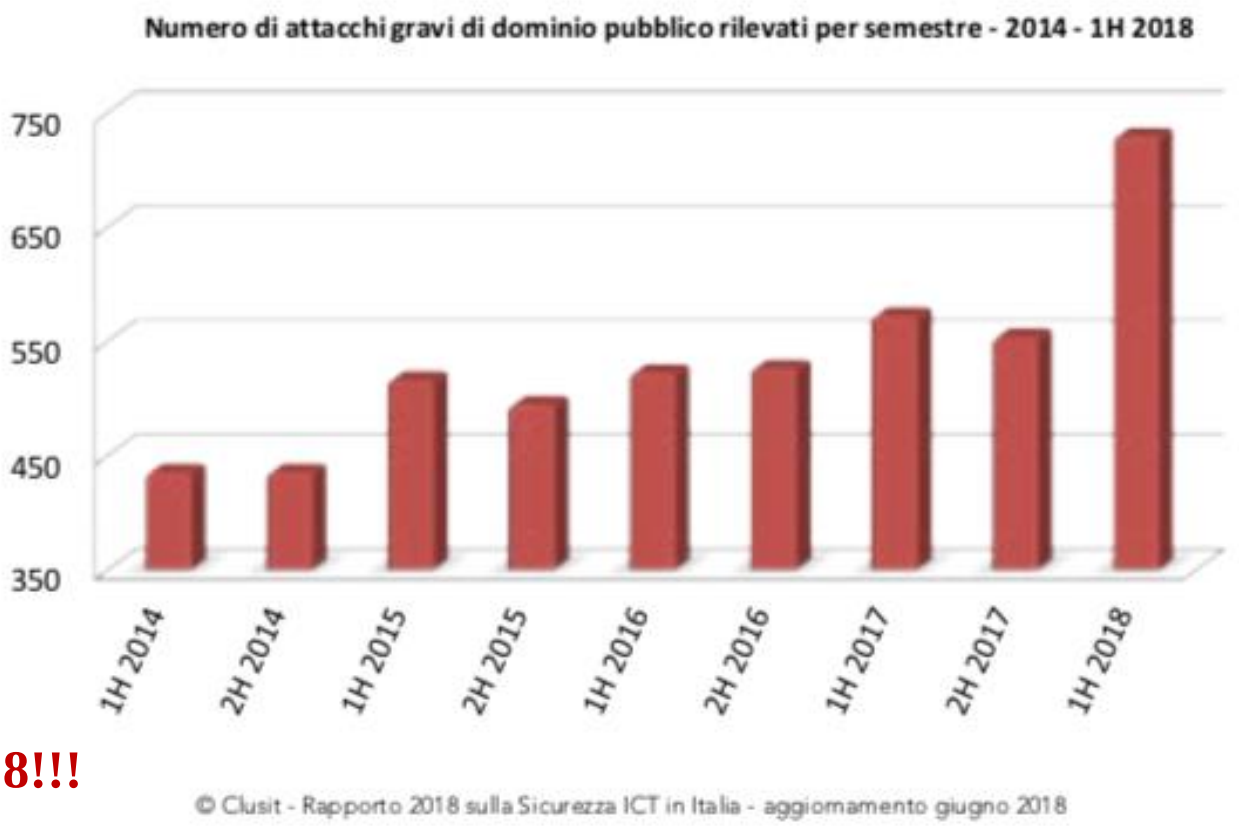
- INDUSTRY 4.0: La nuova frontiera dei cyber criminali nell'anno del GDPR
- Maritime e Sicurezza IT
- Email Security: I trend rilevati in Italia nel corso del 2017
- Attacchi e difese nel Cloud Computing nel 2017
- La Cyber Security, una priorità per il Board
- La governance dei fornitori: adottare un maturity model efficace
- Il fattore umano nella gestione dell'innovazione e dell'information security aziendale (Social Engineering e Social Profiling)
- La diffusione delle criptovalute: rischi ed opportunità in tema di sicurezza e regolamentazione del mercato

Analisi Clusit dei principali attacchi a livello globale

Quali sono i numeri del campione ?

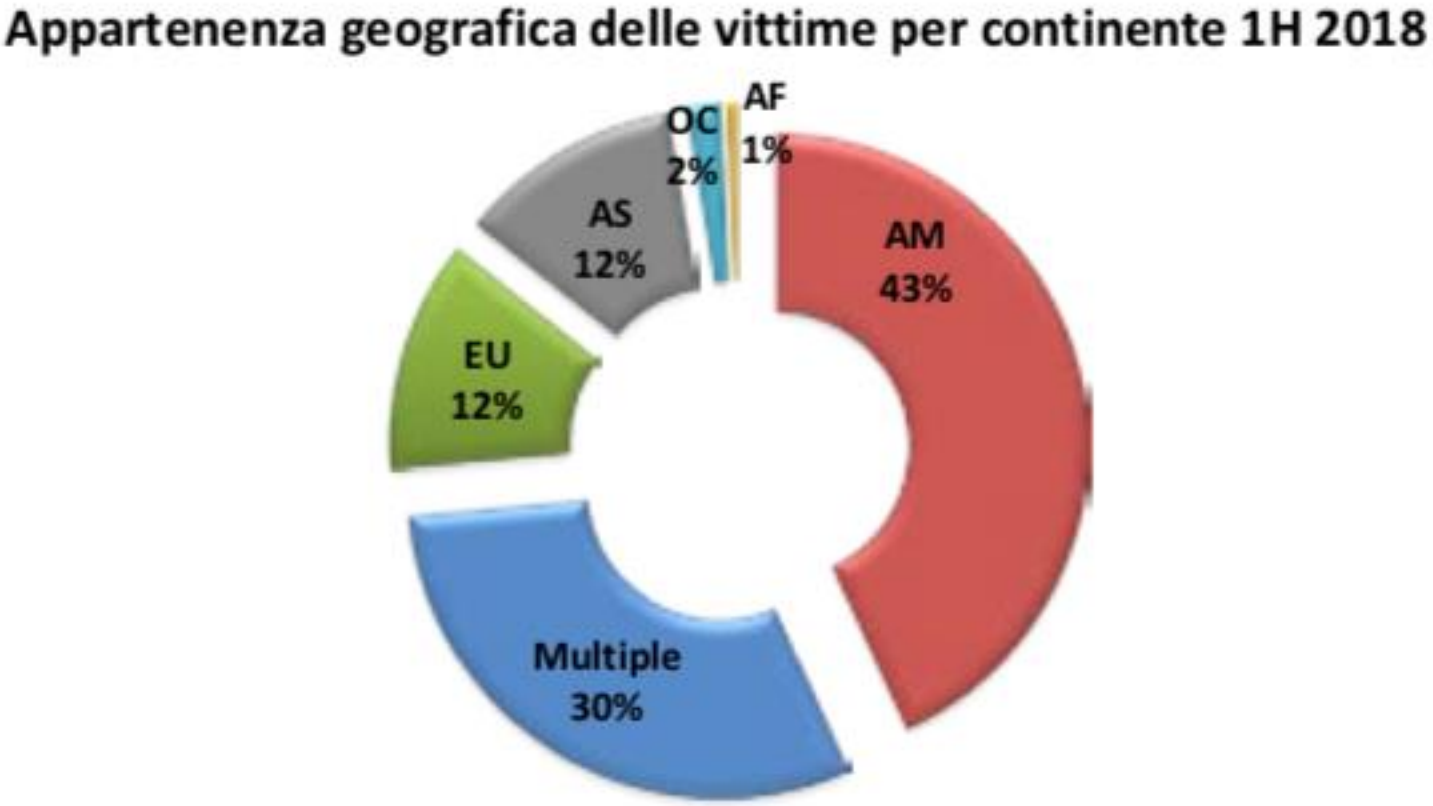
7.595 attacchi gravi analizzati
dal gennaio 2011
al giugno 2018.

- 1.012 nel 2015
- 1.050 nel 2016
- **1.127 nel 2017**



730 attacchi 1H 2018!!!

Distribuzione geografica vittime

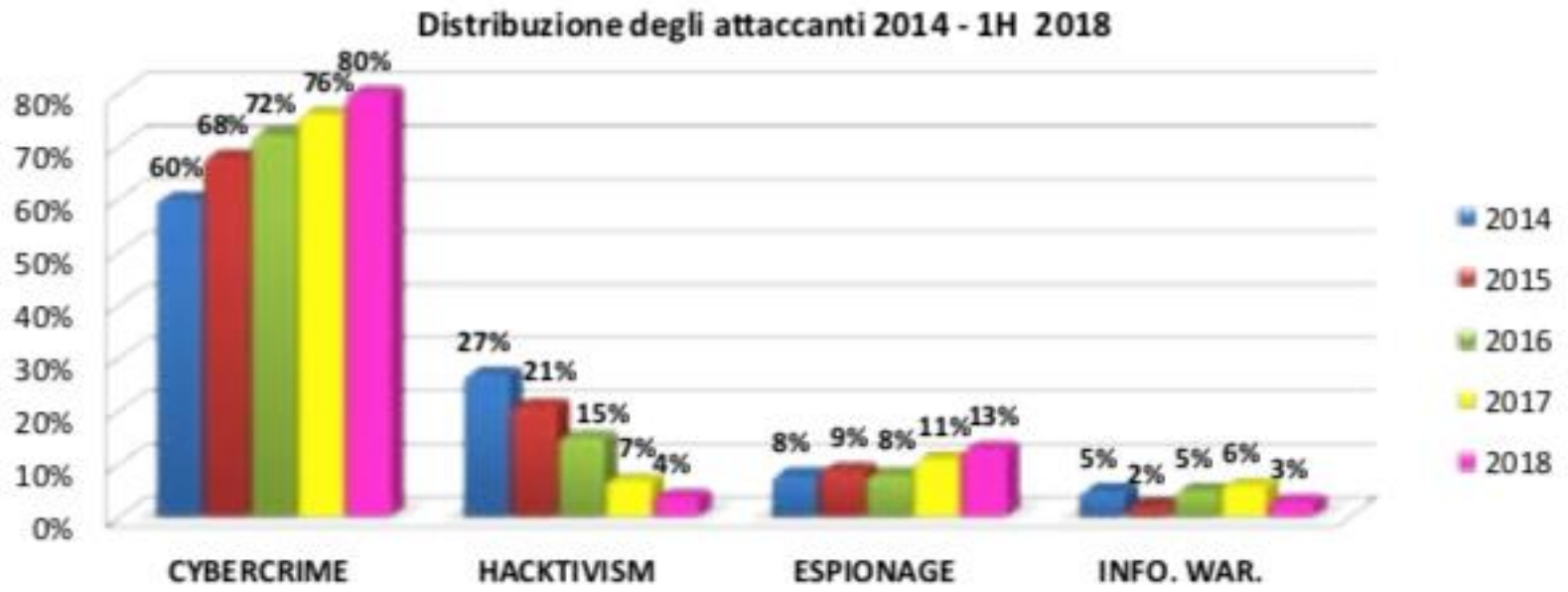


© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia - aggiornamento giugno 2018

Tipologia e distribuzione degli attaccanti

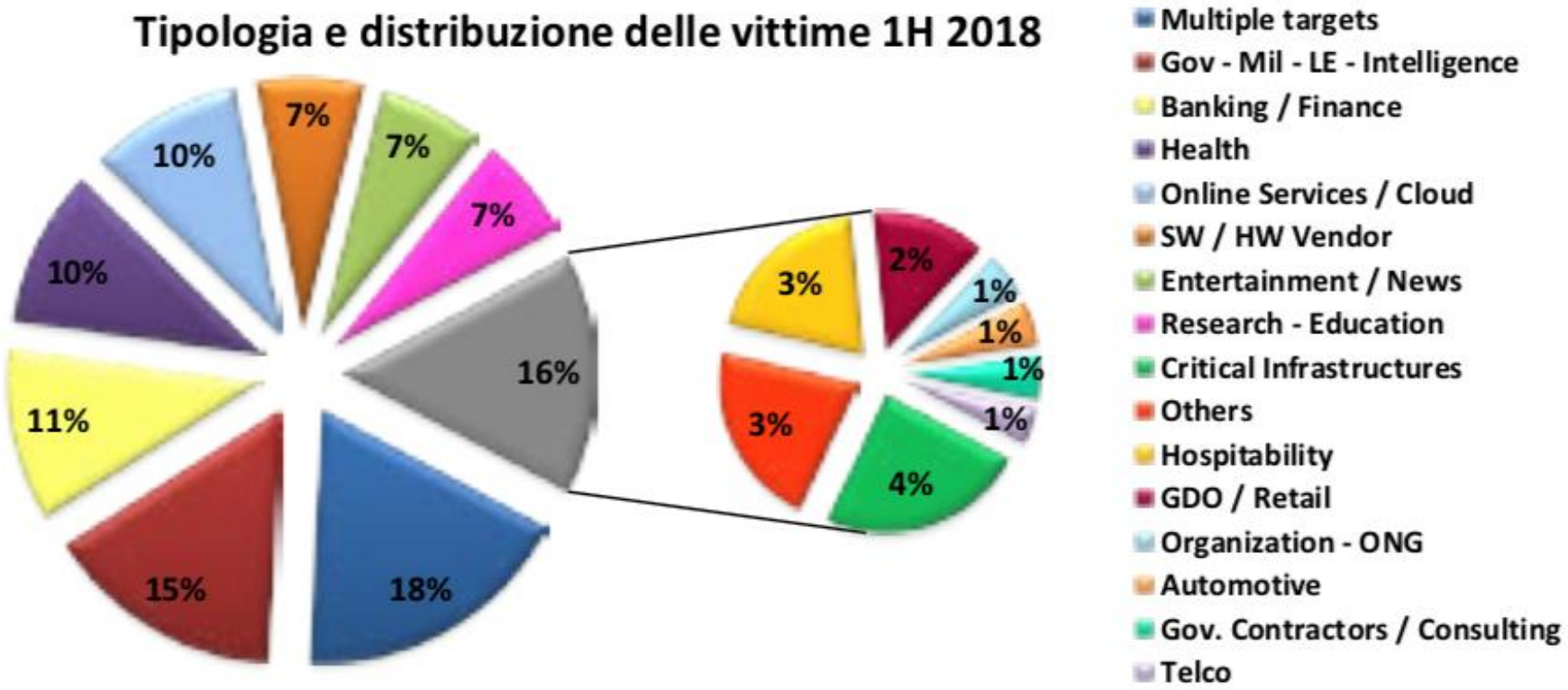
ATTACCANTI PER TIPOLOGIA	2014	2015	2016	2017	2H 2017	1H 2018	Variazioni 1H 2018 su 2H 2017	Trend 1H 2018
Cybercrime	526	684	751	857	434	587	35,25%	↑
Hacktivism	236	209	161	79	34	29	-14,71%	↓
Espionage / Sabotage	69	96	88	129	55	93	69,09%	↑
Information Warfare	42	23	50	62	31	21	-32,26%	↓
TOTALE	873	1.012	1.050	1.127	554	730	+31,77%	↑

Tipologia e distribuzione degli attaccanti



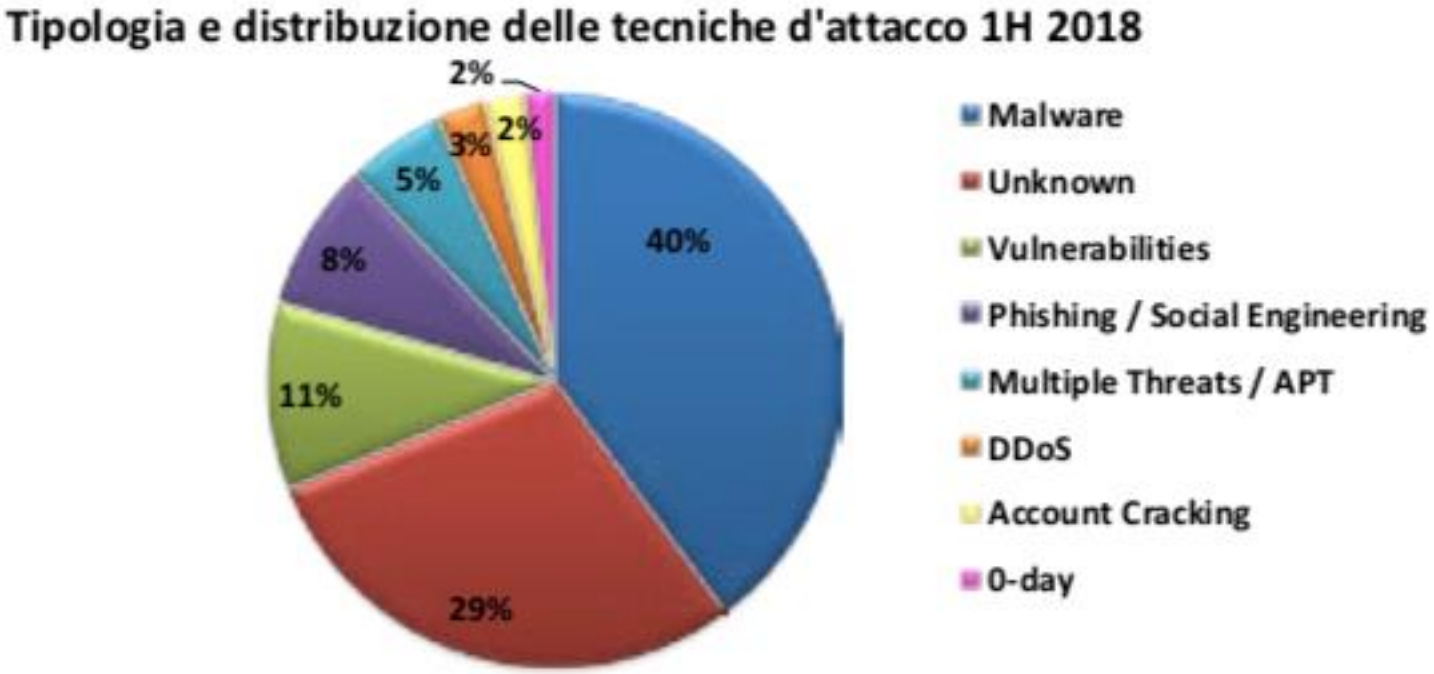
© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia - aggiornamento giugno 2018

Distribuzione vittime nel mondo



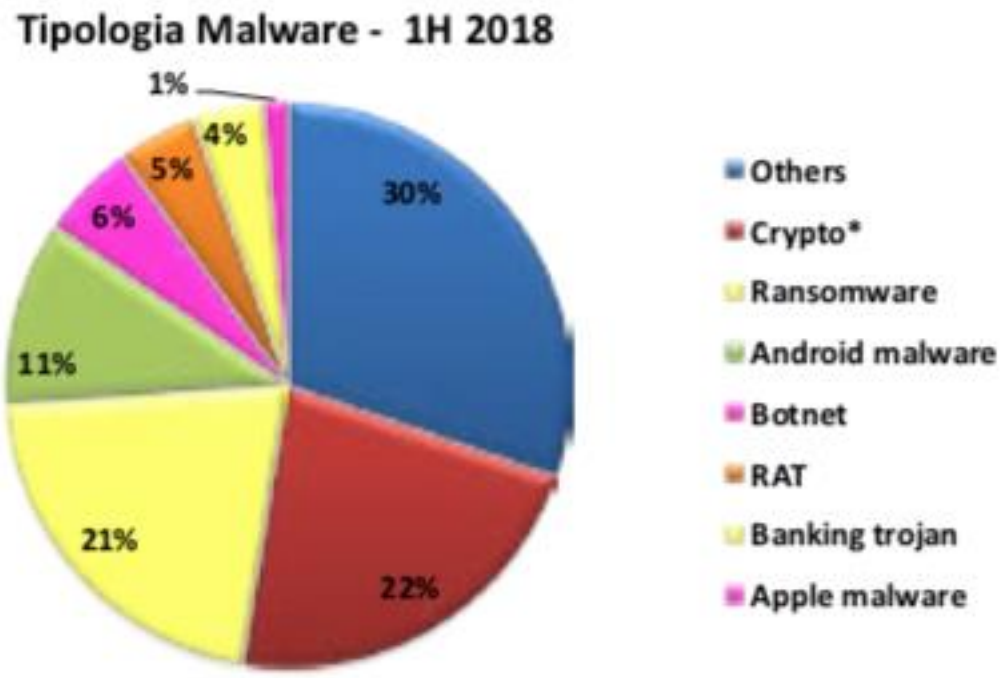
© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia - aggiornamento giugno 2018

Tecniche di attacco nel mondo



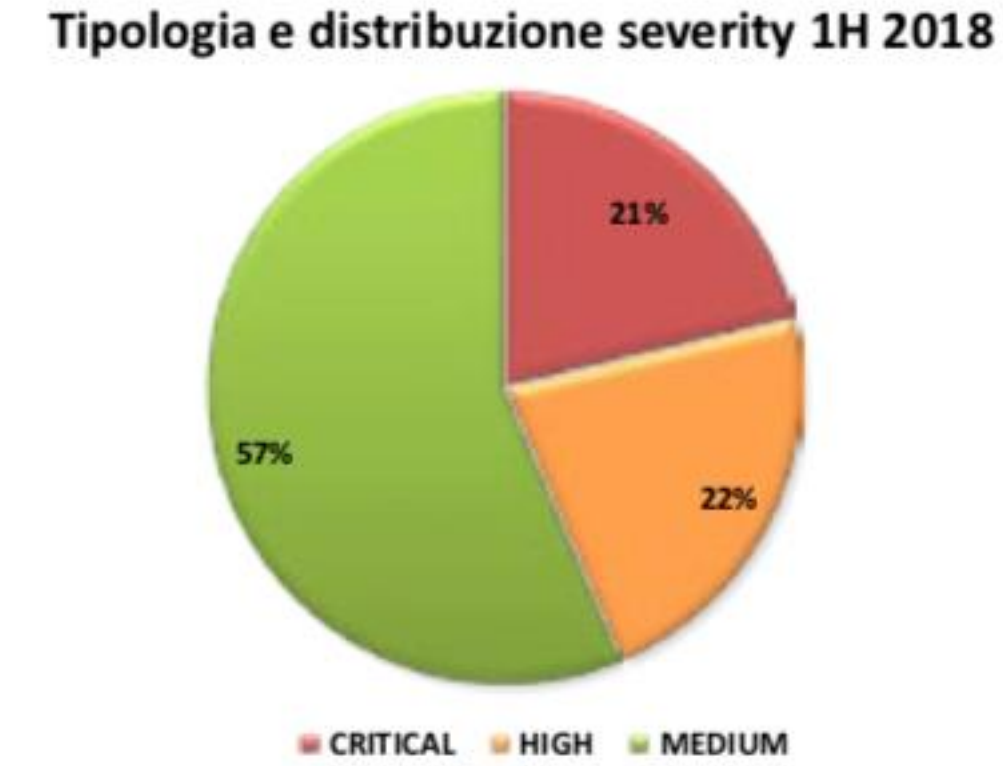
© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia - aggiornamento giugno 2018

Tipologie di malware utilizzate



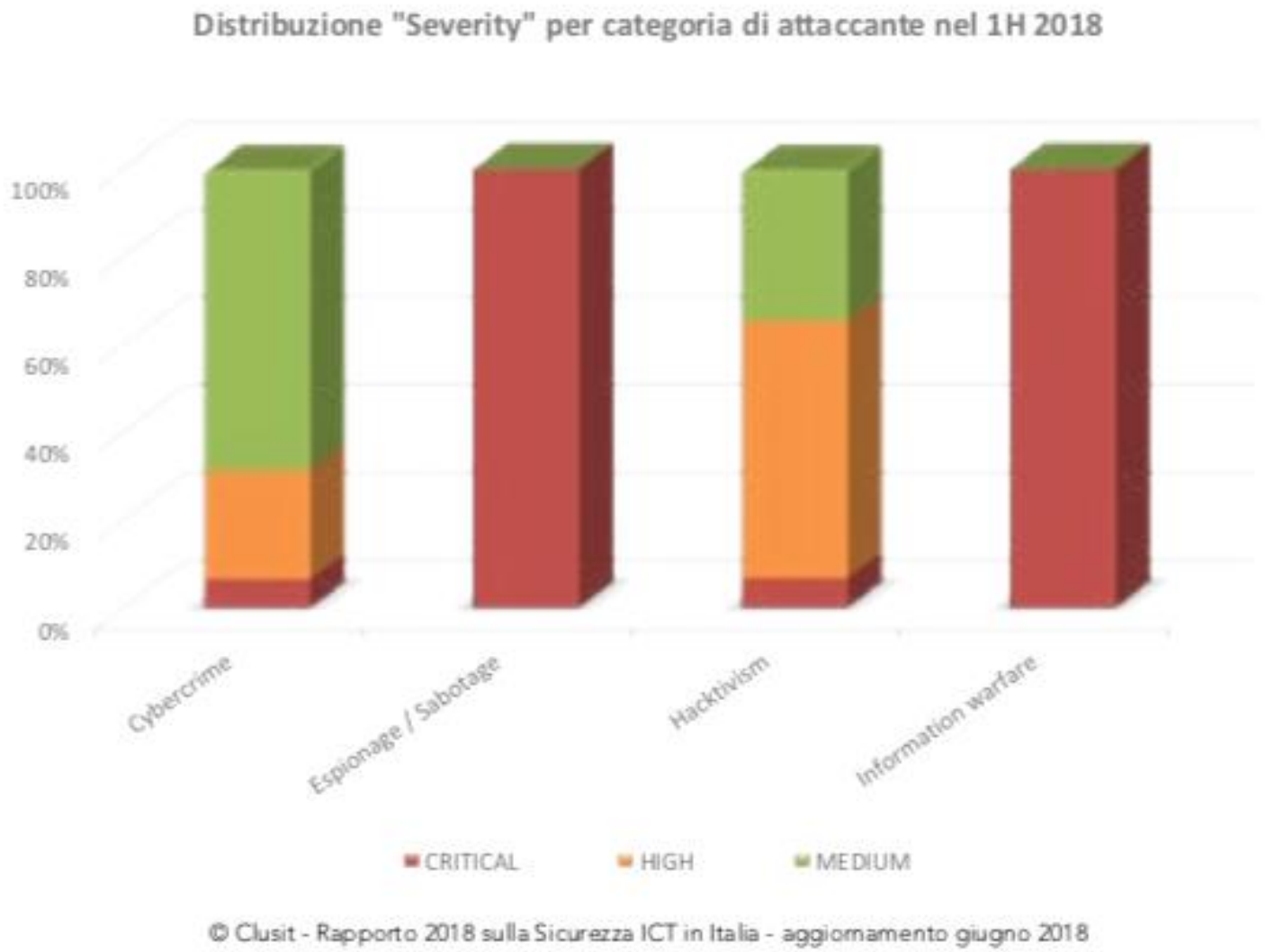
© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia - aggiornamento giugno 2018

Valutazione degli impatti (“Severity”)

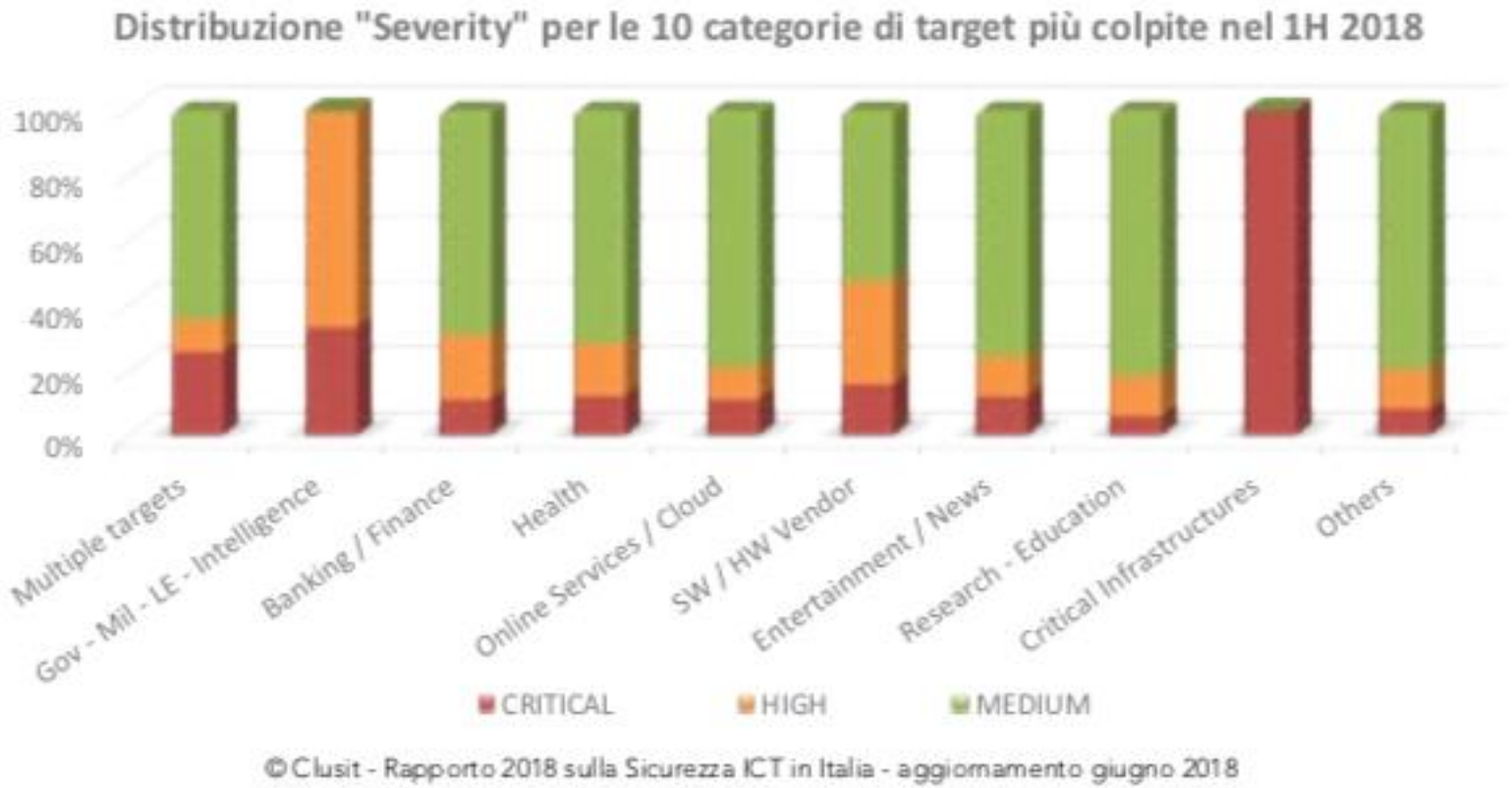


© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia - aggiornamento giugno 2018

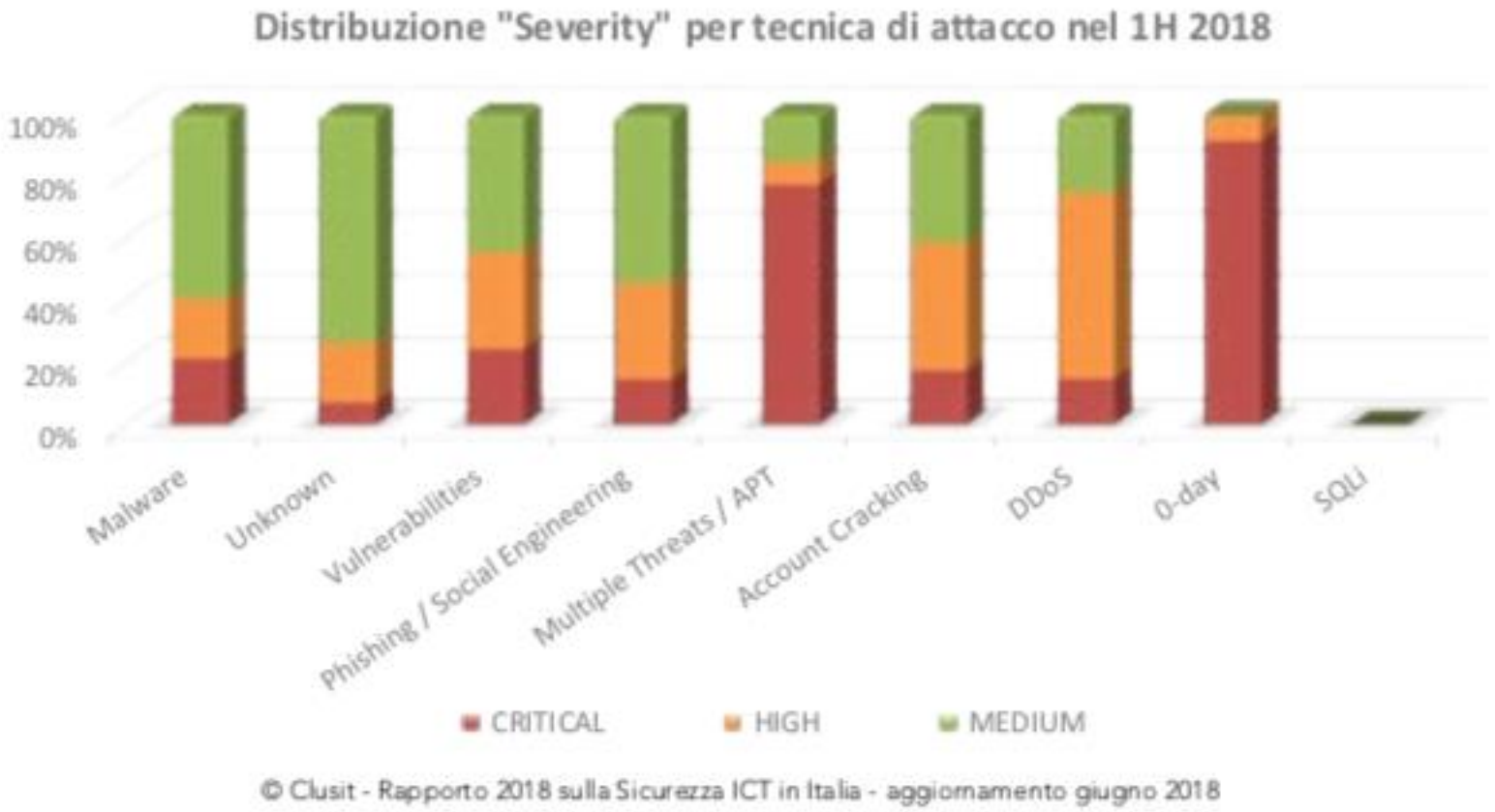
Valutazione degli impatti per tipo di attaccante



Valutazione degli impatti per tipo di vittima



Valutazione degli impatti per tecniche usate



Trend 2018

- «Salto quantico" (soprattutto per Espionage e State sponsored attacks / Information Warfare): siamo in territorio inesplorato
- Phishing (via mail, IM e Social) ancora in crescita
- Malware per piattaforme Mobile sempre più diffuso e sofisticato
- Internet of Things troppo insicuro, rischi sistemici crescenti
- Discesa in campo degli Stati e aumento della (cyber) tensione
- Cyber crime sempre più aggressivo e organizzato
- Crescenti attività di propaganda, PsyOps e alterazione di massa della percezione (alt-truth) supportata anche da cyber attacchi

Analisi FASTWEB della situazione nazionale

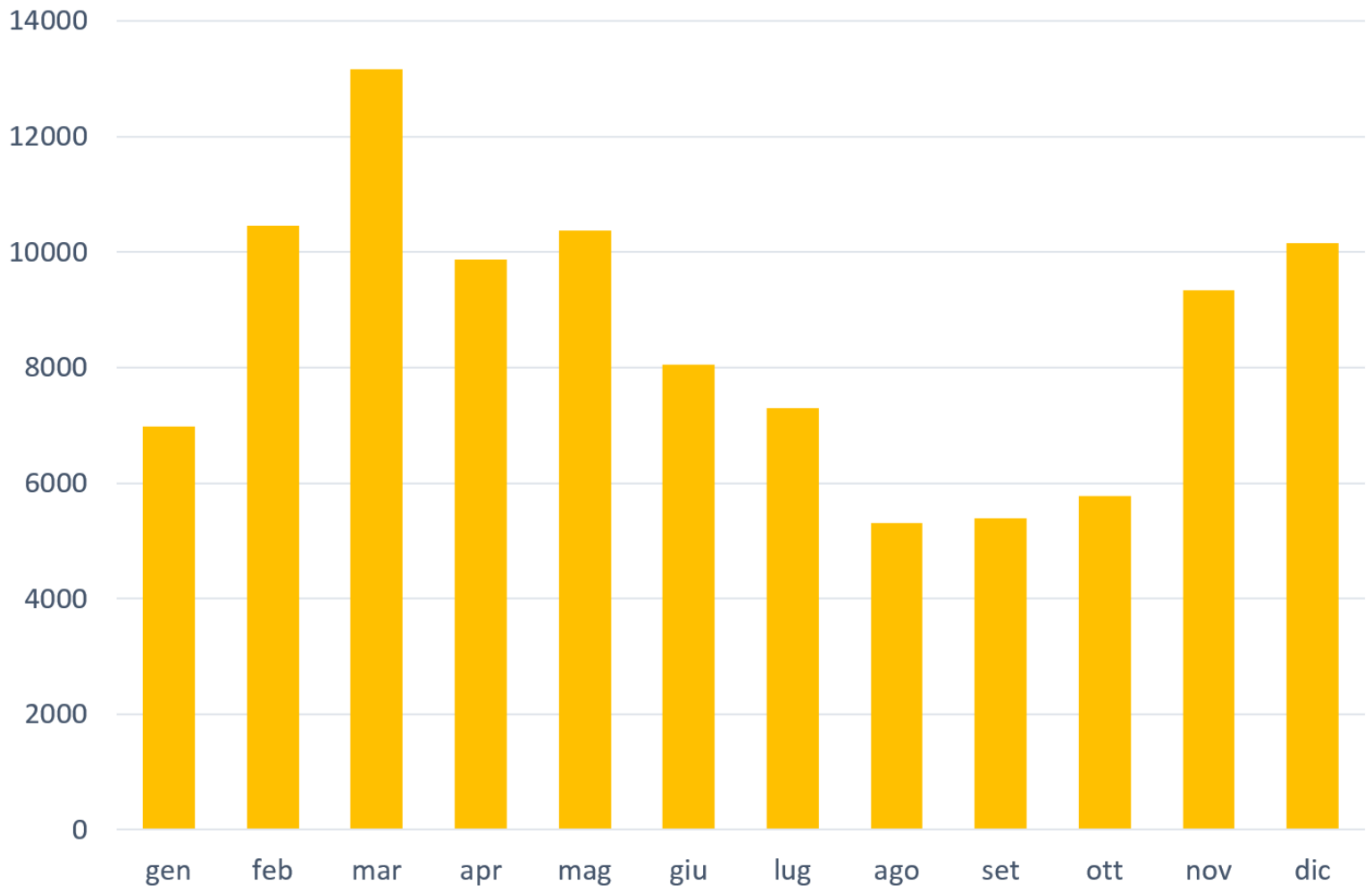
La base dati

35 milioni di eventi di sicurezza (l’anno scorso erano 16)

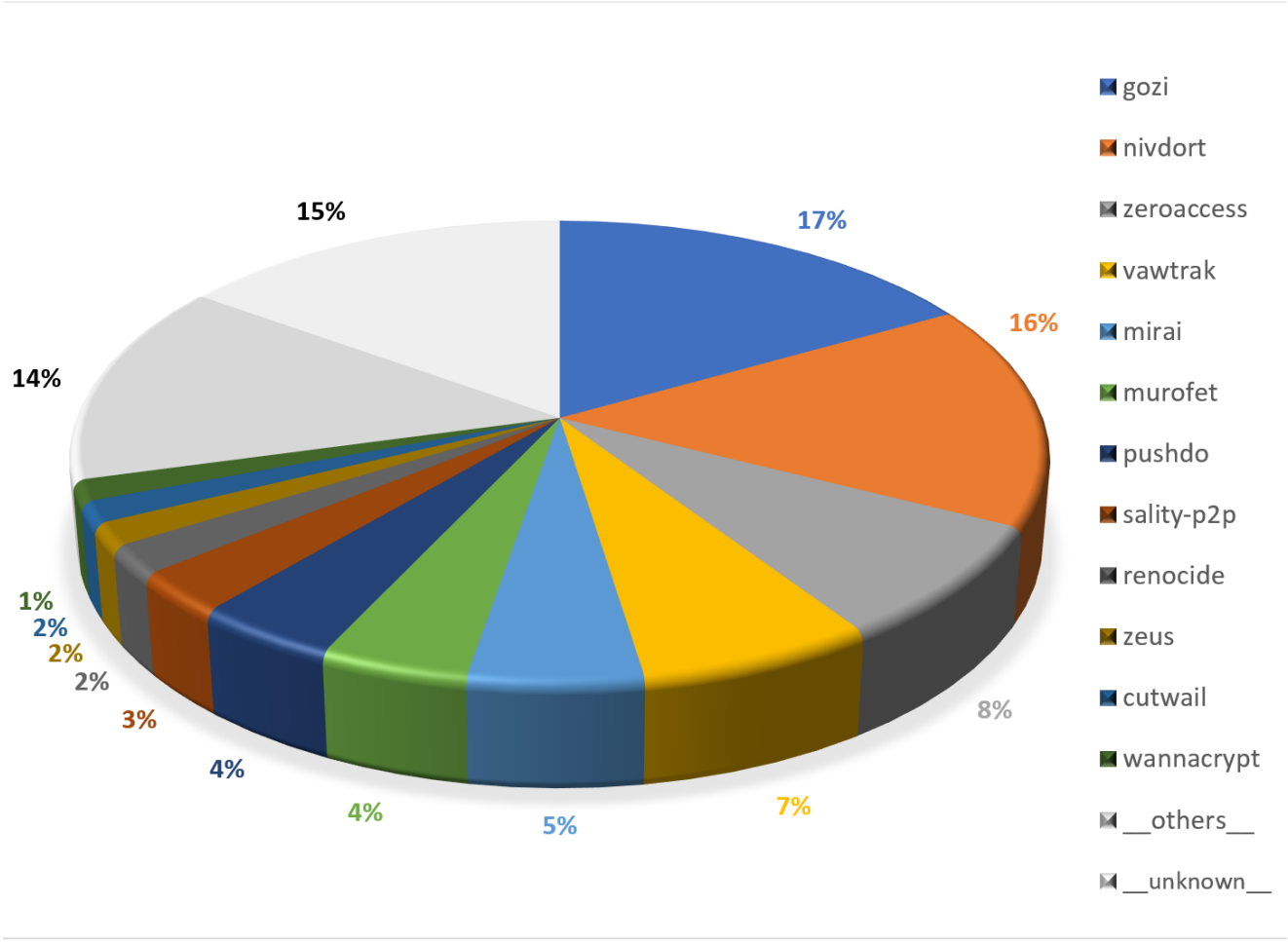
6 milioni di indirizzi IP pubblici (stesso perimetro)

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

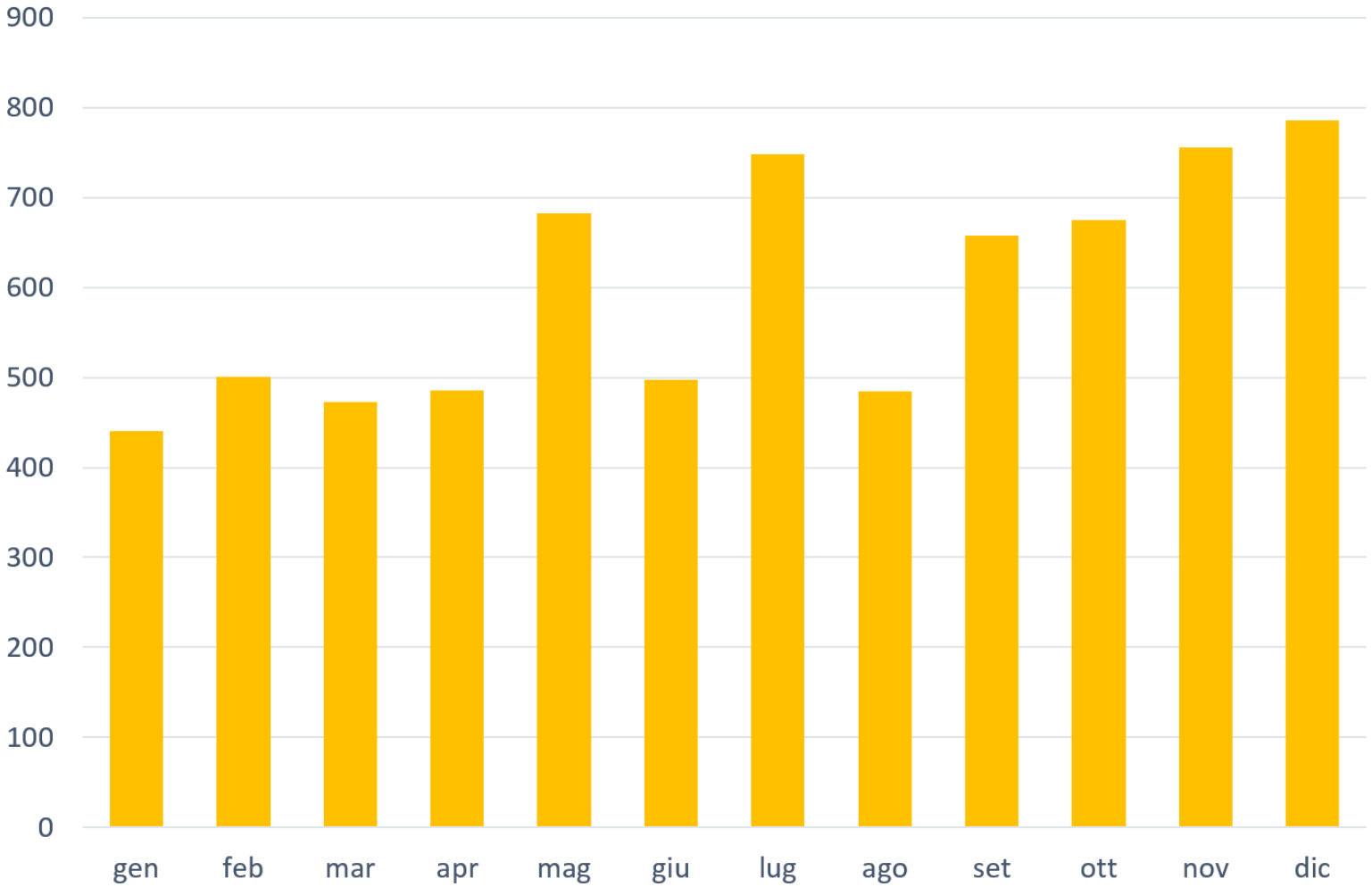
Rilevazione mensile dei malware



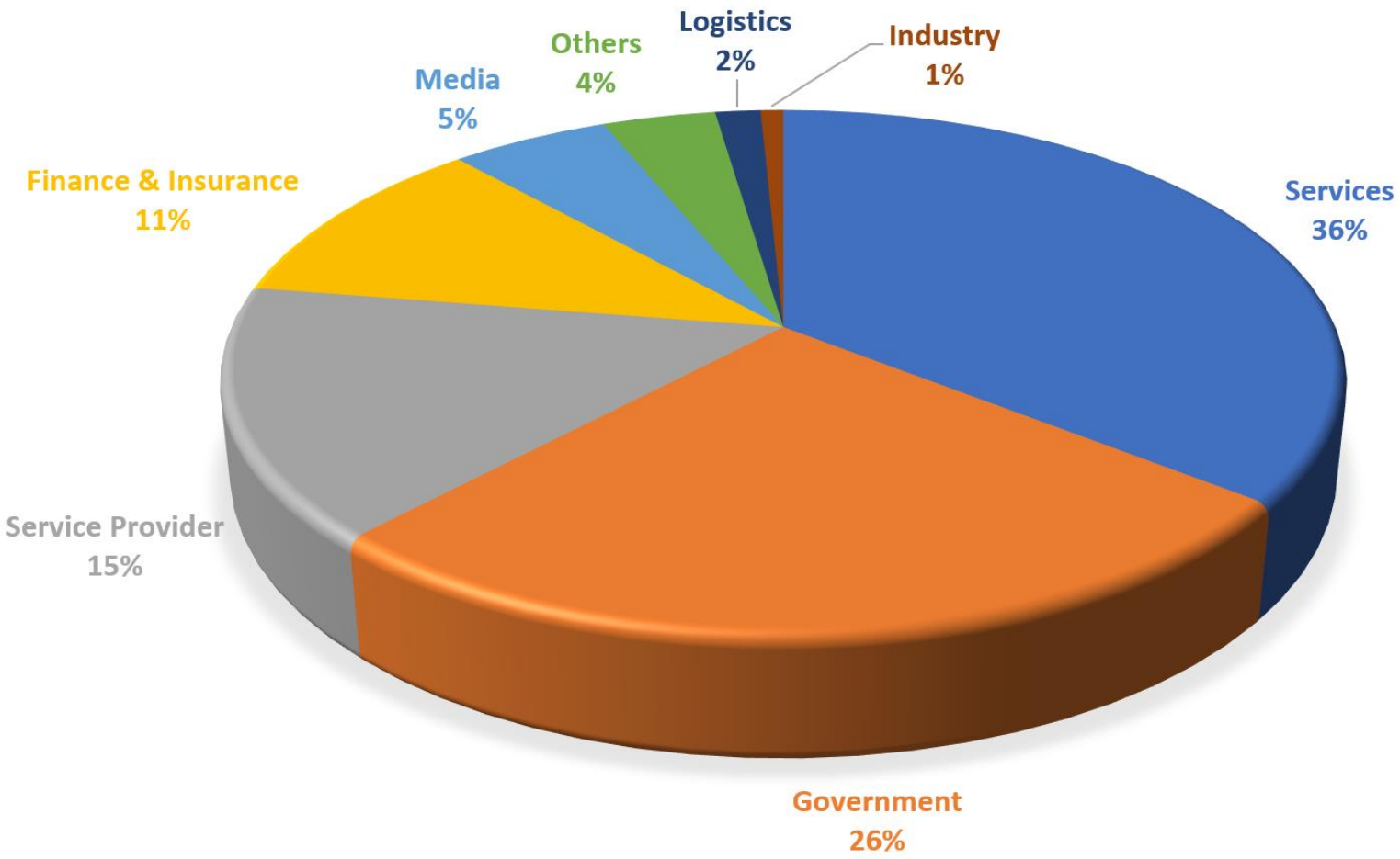
Famiglie malware



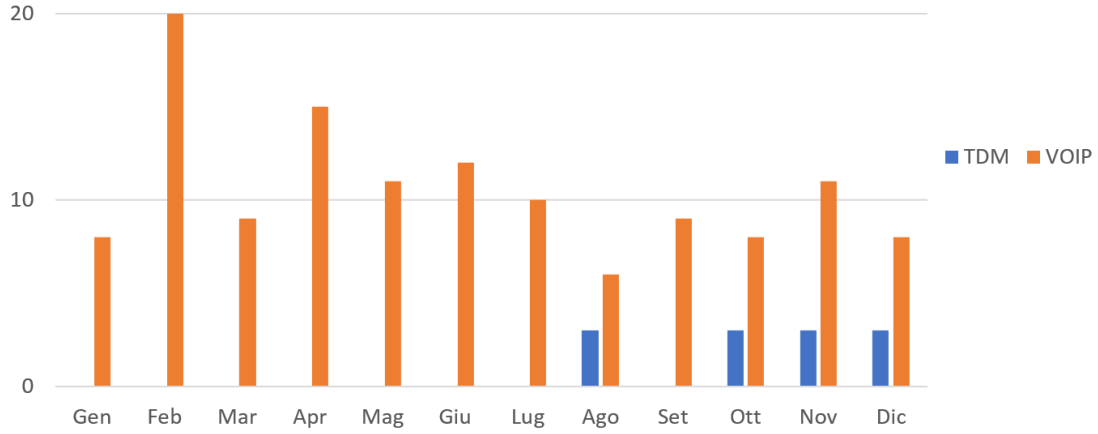
Distribuzione mensile 'anomalie' DDoS

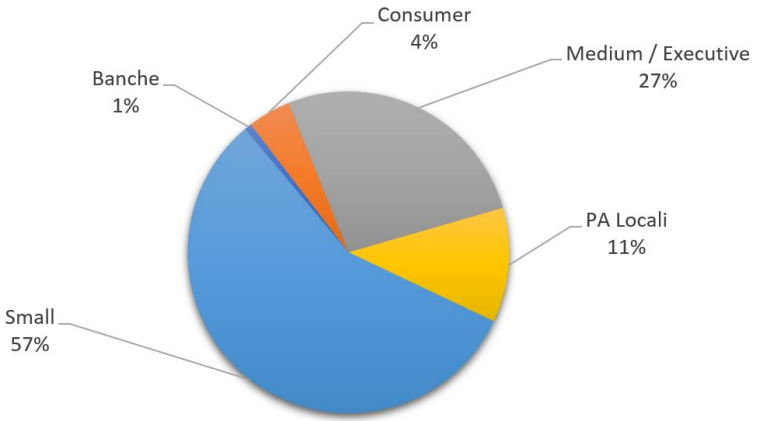


Target di possibili attacchi DDoS



Frodi telefoniche





Conclusioni e previsioni

2017

Ormai la cybersecurity è diventato un tema “pop” (insieme ai bitcoin!)

È stato l’anno degli attacchi al cloud (ma non esattamente per ciò che ci aspettavamo!)

2018

La sfida di quest’anno sarà ottenere più visibilità della security del cloud

Se ne vedranno delle belle grazie al GDPR (multe assicurate!)

Attacchi letali per le aziende

Sempre più compromissioni tramite IoT

Avremmo bisogno di una «convenzione di Ginevra» digitale che difficilmente accadrà quest’anno

Per scaricare il rapporto in formato digitale:

https://clusit.it/rapporto-clusit

Clusit
Associazione Italiana
per la Sicurezza Informatica

10 ANNI
SECURITY
TECHNOLOGIES
MANAGEMENT
COMPLIANCE
SUMMIT