Security Summit Milano 2018

Sessione Plenaria del 13.03.2018

Clusit
Associazione Italiana
per la Sicurezza Informatica

SECURITY
10 ANNI
TECHNOLOGIES
MANAGEMENT
COMPLIANCE
SUMMIT

Rapporto Clusit 2017 sulla sicurezza ICT in Italia

Moderano: Gabriele Faggioli, e Alessio Pennasilico

Intervengono alcuni degli autori:

- Andrea Zapparoli Manzoni, Clusit
- Davide Del Vecchio, Clusit
- Marco Pacchiardo, Akamai

Partecipano alla Tavola Rotonda:

- Gianluca Busco Arrè, Panda Security Italia
- Carlo Mauceli, Microsoft
- Gastone Nencini, Trend Micro
- Domenico Raguseo, IBM Italia
- Alessandro Vallega, Oracle Italia

Panoramica dei cyber attacchi più significativi del 2017

- 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**

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY 10 ANNI
TECHNOLOGIES
MANAGEMENT COMPLIANCE
SUMMIT

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”.

Clusit
Associazione Italiana per la Sicurezza Informatica

10 ANNI
SECURITY
TECHNOLOGIES
MANAGEMENT
COMPLIANCE
SUMMIT

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

Clusit
Associazione Italiana per la Sicurezza Informatica

10 ANNI
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 2017 da

IDC
ANALYZE THE FUTURE

Clusit
Associazione Italiana per la Sicurezza Informatica

10 ANNI
SECURITY
TECHNOLOGIES
MANAGEMENT
COMPLIANCE
SUMMIT

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

Clusit
Associazione Italiana per la Sicurezza Informatica

Analisi Clusit dei principali attacchi a livello globale

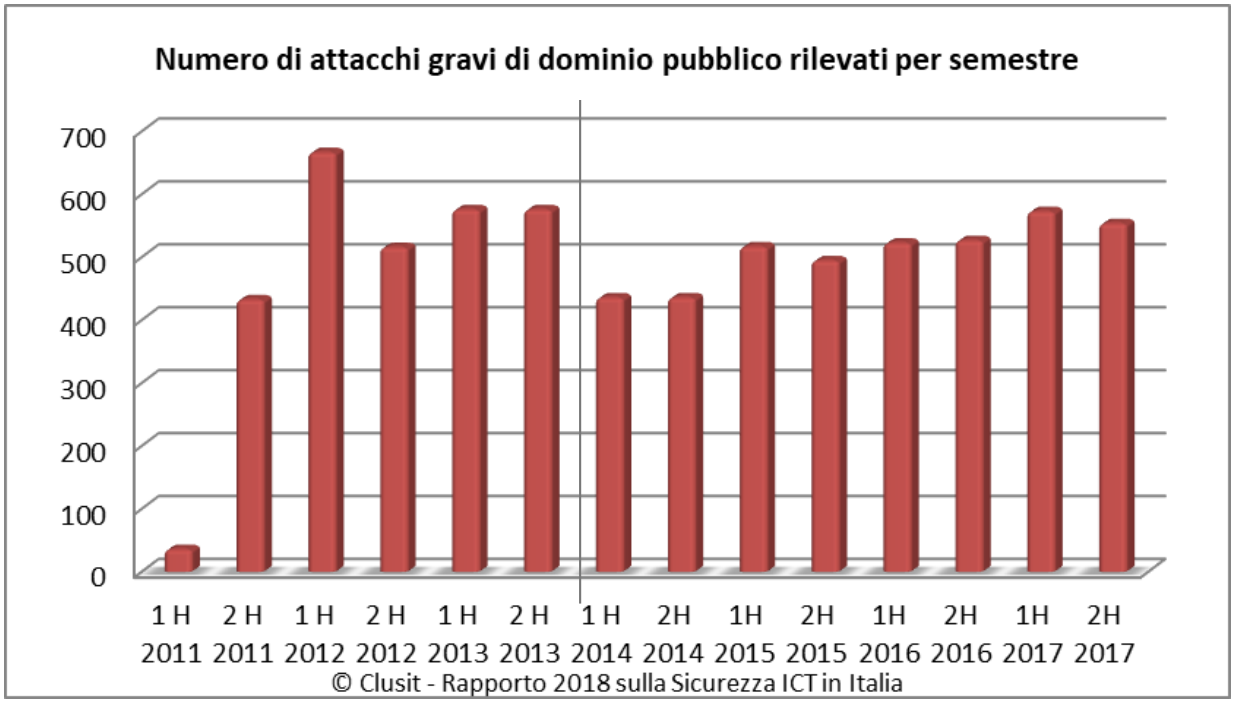
Quali sono i numeri del campione ?

In media negli ultimi 84 mesi abbiamo analizzato e classificato 83 attacchi gravi di dominio pubblico al mese (94 al mese nel 2017)

- **6.865** attacchi gravi analizzati dal gennaio 2011 al dicembre 2017.

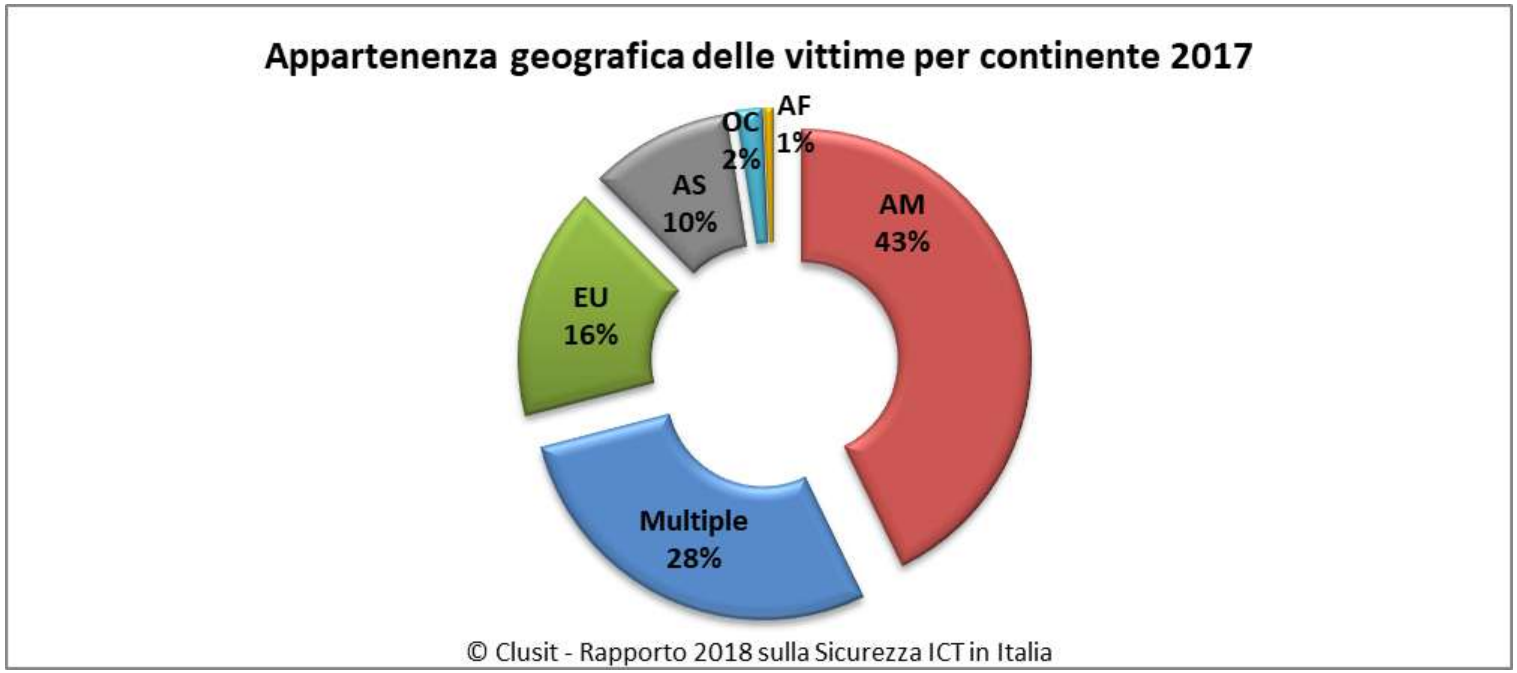
- 469 nel 2011
- 1.183 nel 2012
- 1.154 nel 2013

- 873 nel 2014 (*)
- 1.012 nel 2015
- 1.050 nel 2016
- **1.127 nel 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). Nel 2017, la crescita rispetto al 2014 è del 30%.

Distribuzione geografica vittime



Rispetto al 2016, nel 2017 diminuiscono leggermente le vittime di area americana (dal 53% al 43%), mentre rimangono invariati gli attacchi noti verso realtà basate in Europa (16%) e diminuiscono quelli contro bersagli in Asia (dal 16% al 10%).

La categoria "Multinational" cresce sostanzialmente (dall'11% del 2016 al **28%** del 2017, era il 9% nel 2015), ad indicare la tendenza a colpire in modo trasversale bersagli sempre più importanti, di natura transnazionale.

Tipologia e distribuzione degli attaccanti

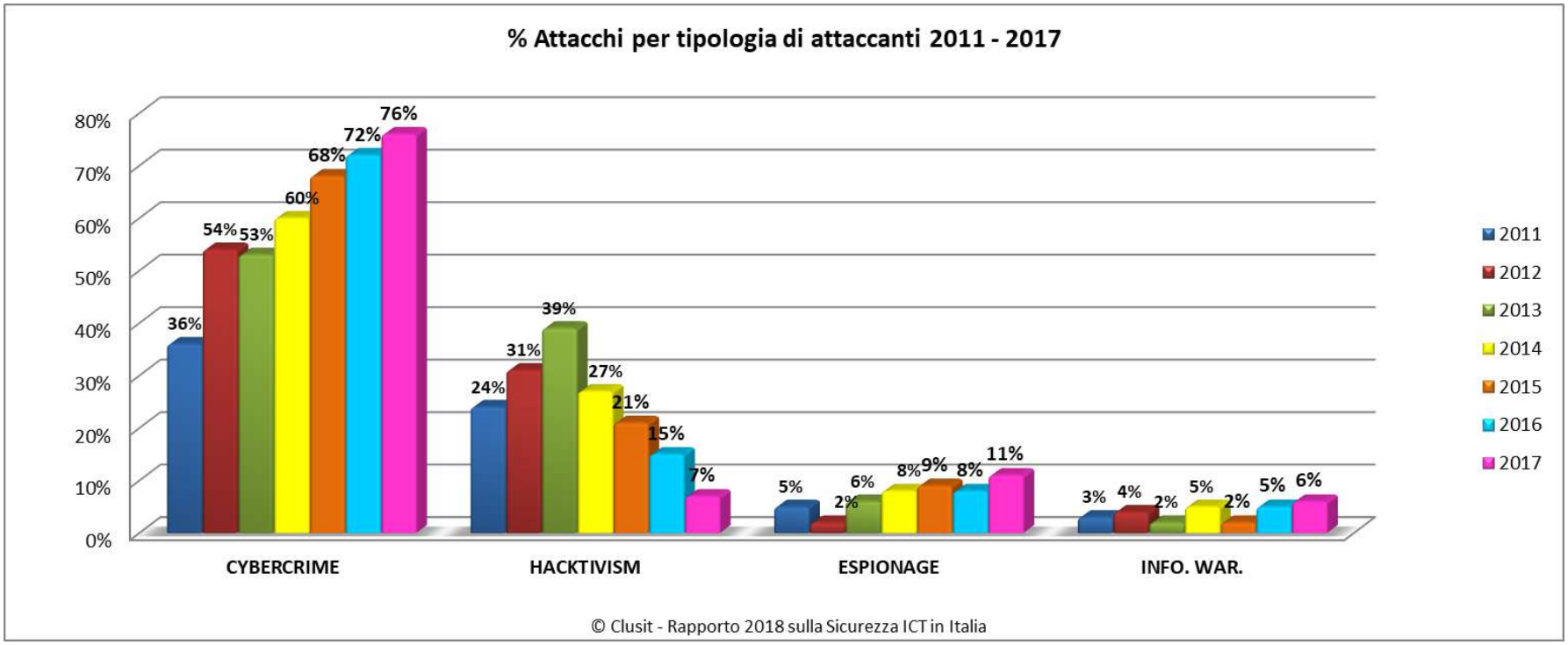
ATTACCANTI PER TIPOLOGIA	2014	2015	2016	2017	Variazioni 2017 su 2016	Trend 2017
Cybercrime	526	684	751	857	14,11%	↑
Hacktivism	236	209	161	79	-50,93%	↓
Espionage / Sabotage	69	96	88	129	46,59%	↑
Information Warfare	42	23	50	62	24,00%	↑
TOTALE	**873**	**1.012**	**1.050**	**1.127**	**+7,33%**	↗

In termini assoluti, nel 2017 le categorie "Cybercrime", "Cyber Espionage" e "Information Warfare" fanno registrare il numero di attacchi più elevato degli ultimi 7 anni.

Dal campione emerge chiaramente che, con l'esclusione delle attività riferibili ad attacchi della categoria "Hacktivism" che diminuisce sensibilmente (-50%) rispetto al 2016), nel 2017 gli attacchi gravi compiuti per finalità "Cybercrime" sono in aumento (+14%), così come quelli riferibili ad attività di "Information warfare" (+24%), mentre crescono sensibilmente gli attacchi del gruppo "Cyber Espionage" (46%).

Va sottolineato che, rispetto al passato, oggi risulta più difficile distinguere nettamente tra queste due ultime categorie: sommando gli attacchi di entrambe, nel 2017 si assiste ad un aumento del 38% rispetto all'anno precedente (191 contro 138).

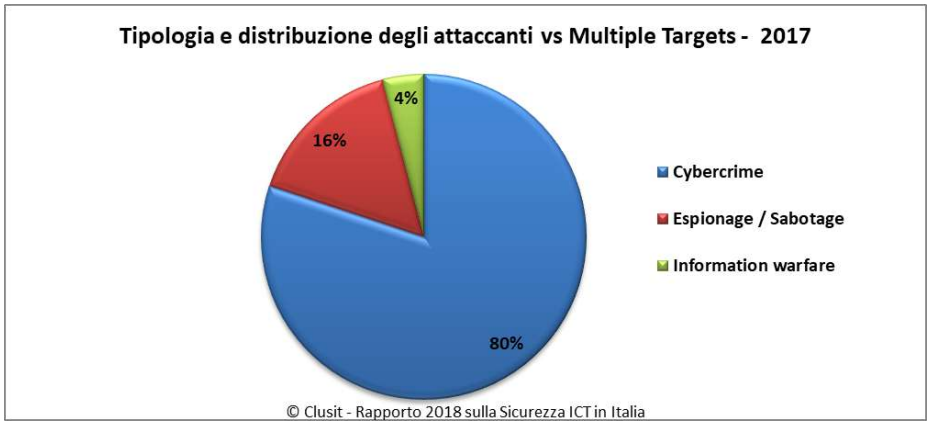
Tipologia e distribuzione degli attaccanti (7 anni)

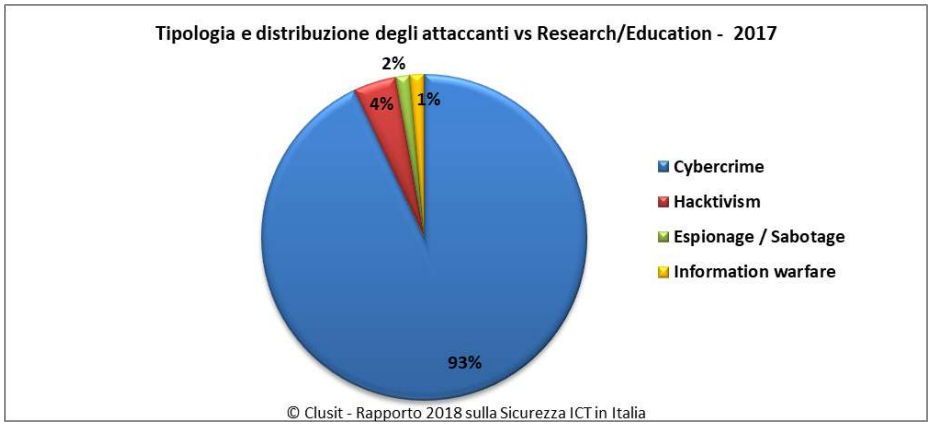


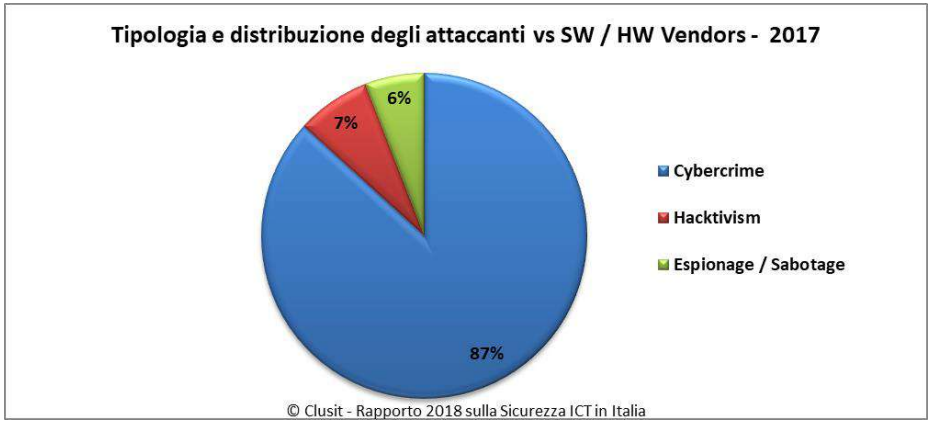
Il Cybercrime passa dal 72% al **76**% del totale, mentre l'Hacktivism diminuisce di 32 punti percentuali rispetto al suo picco del 2013, passando da oltre un terzo a meno di un decimo dei casi analizzati.

Per quanto riguarda le attività di Espionage, rispetto alla percentuale degli attacchi gravi registrati nel 2016 la quota di attacchi nel 2017 è in aumento dal 8 all'11%, mentre l'Information Warfare risulta essere in crescita (nonostante la scarsità di informazioni pubbliche in merito), dal 5% al 6%.

Tipologia e distribuzione attaccanti vs i settori a maggior crescita degli attacchi



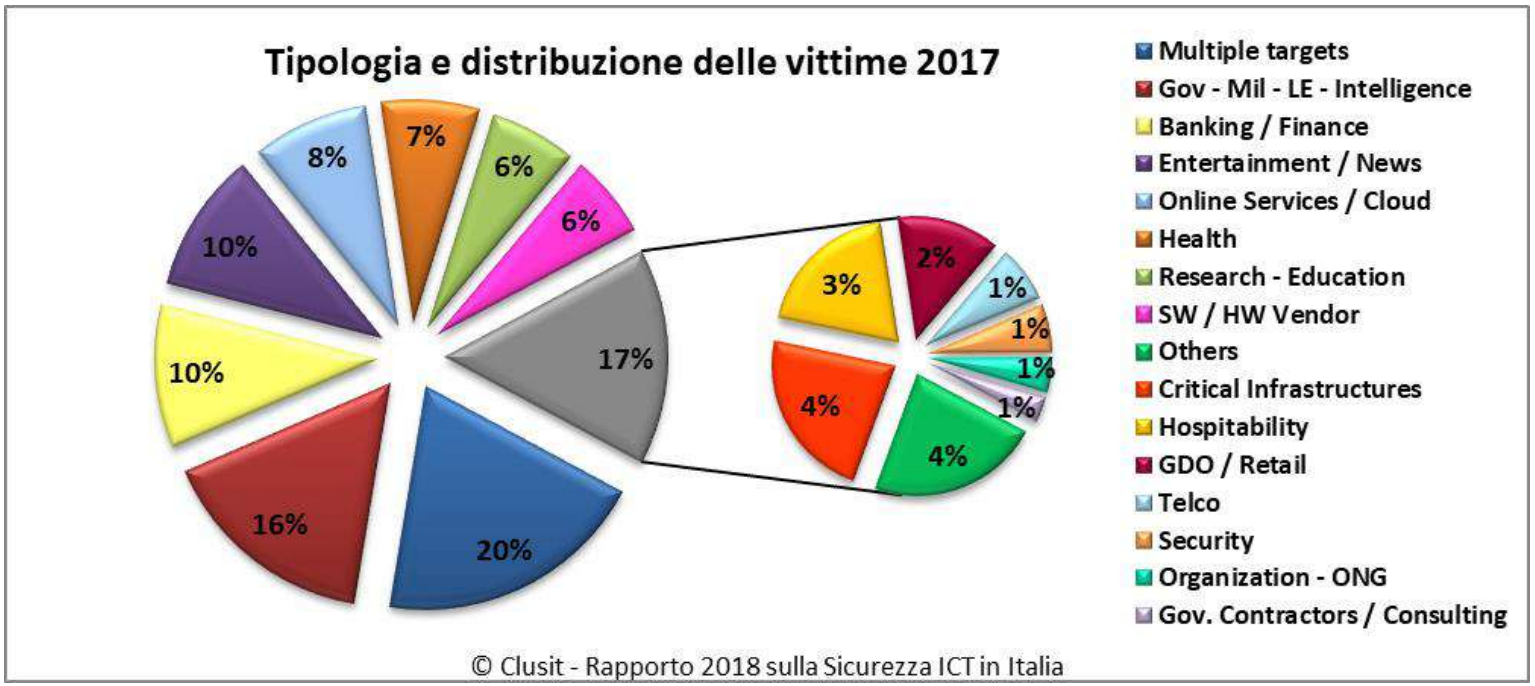




Anche quest'anno presentiamo le statistiche relative ad alcune categorie di vittime verticali, con un'attenzione particolare verso i primi 3 settori per tasso di crescita degli attacchi rispetto all'anno precedente (Multiple Targets, Research/Edu e HW-SW Vendors).

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 (ovvero, non esistono soluzioni universali).

Distribuzione vittime nel mondo (2017)

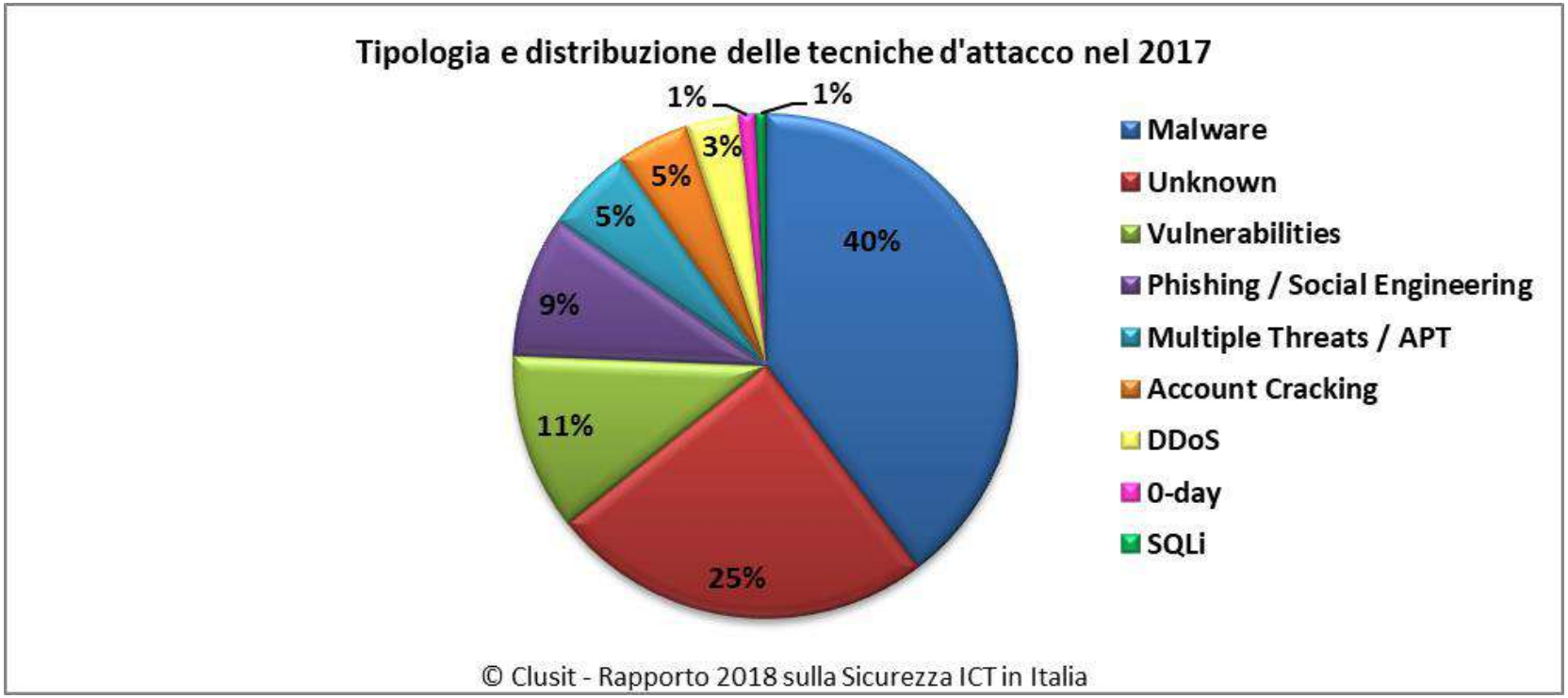


Nel 2017 al primo posto assoluto balza la categoria “Multiple Targets” (20%), superando per la prima volta il settore “Gov”, in diminuzione al 16%, che fin dal 2011 è sempre stato al primo posto nel nostro studio. Rispetto al 2016, nel 2017 “Banking/Finance” sale al terzo posto (10%) insieme a “Entertainment/News” (10%), seguiti da “Online Services / Cloud” (8%) e “Health” (7%). Salgono al 6% “Software/Hardware Vendor” e “Research/Education”, mentre la categoria “Others” (anche a causa dell’introduzione della nuova categoria “Multiple Targets”), scende al 4%.

Distribuzione vittime nel mondo (2017)

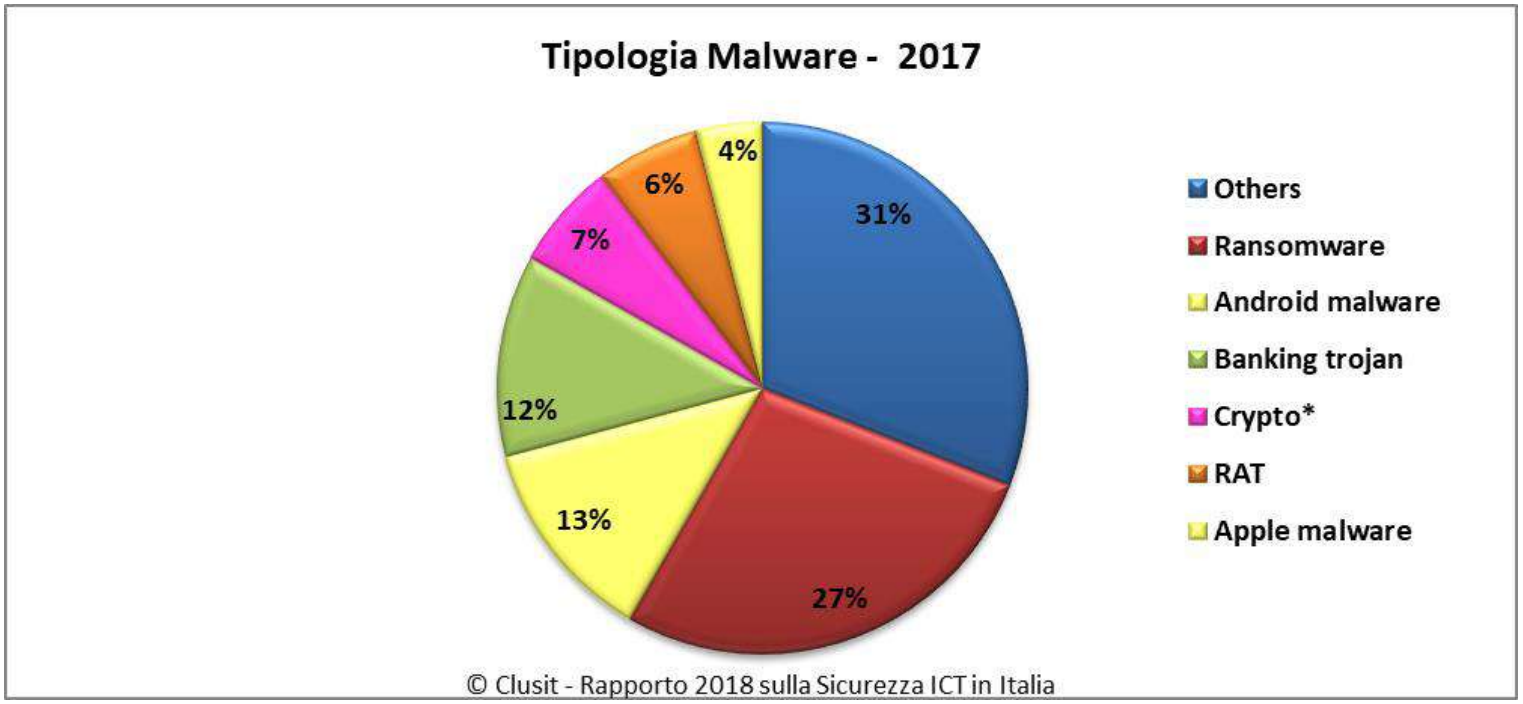
VITTIME PER TIPOLOGIA	2014	2015	2016	2017	Variazioni 2017 su 2016	Trend 2017
Institutions: Gov - Mil - LEAs - Intelligence	213	223	220	179	-18,64%	↓
Others	172	51	38	40	5,26%	↗
Entertainment / News	77	138	131	115	-12,21%	↘
Online Services / Cloud	103	187	179	95	-46,93%	↓
Research - Education	54	82	55	71	29,09%	↑
Banking / Finance	50	64	105	117	11,43%	↑
Software / Hardware Vendor	44	55	56	68	21,43%	↑
Telco	18	18	14	13	-7,14%	↘
Gov. Contractors / Consulting	13	8	7	6	-14,29%	↘
Security Industry	2	3	0	11	-	↗
Religion	7	5	6	0	-	↓
Health	32	36	73	80	9,59%	↑
Chemical	5	2	0	0	-	→
Critical Infrastructures	13	33	38	40	5,26%	↗
Automotive	3	5	4	4	-	→
Org / ONG	47	46	13	8	-38,46%	↓
Multiple Targets	-	-	49	222	353,06%	↑
GDO / Retail	20	17	29	24	-17,24%	↘
Hospitability	-	39	33	34	3,03%	↗

Tecniche di attacco nel mondo (2017)



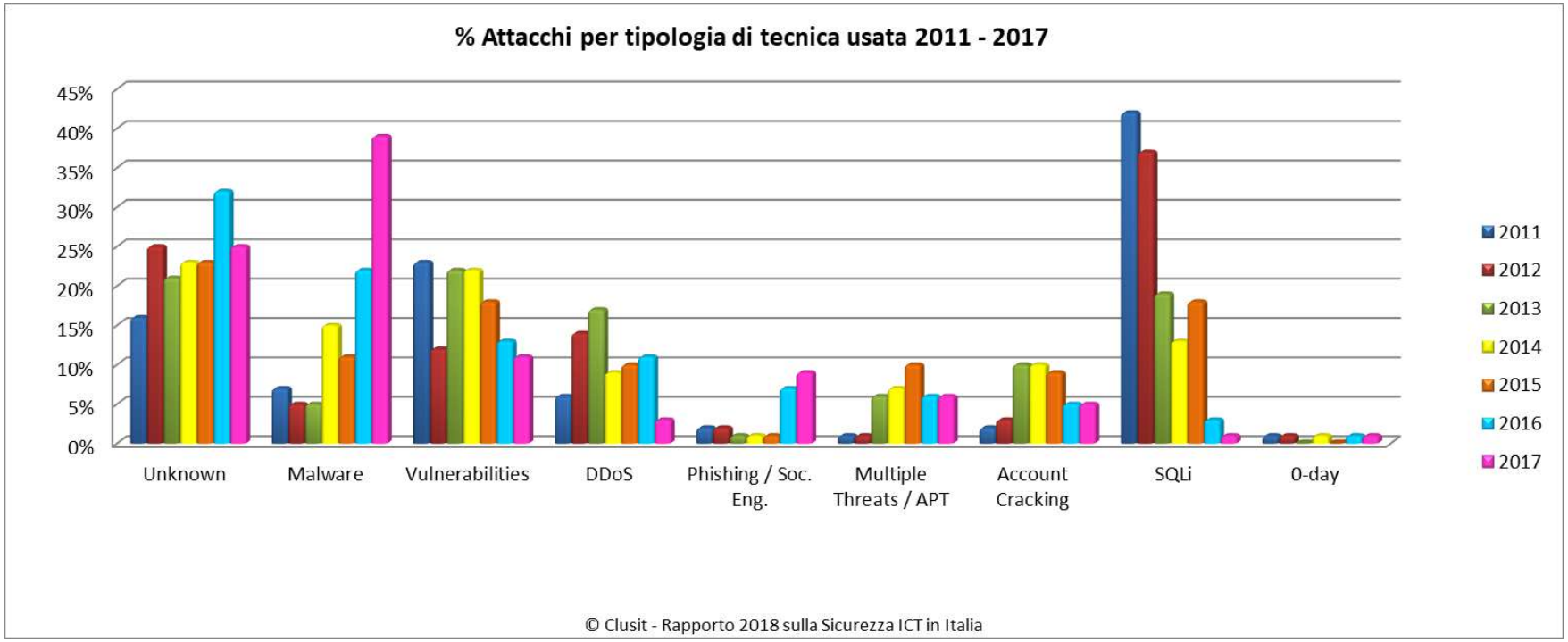
Per la prima volta dal 2011, nel 2017 le tecniche sconosciute (categoria "Unknown") passano al secondo posto con il **25%** del totale (erano il 32% nel 2016), superate dalla categoria "Malware" (**40%**). L'uso di Malware come vettore di attacco aumenta sensibilmente anche nel 2017, facendo segnare una crescita del **95%** rispetto al 2016. In sostanza ormai gli attaccanti possono fare affidamento sull'efficacia del malware "semplice", prodotto industrialmente a costi decrescenti, e delle tecniche di Phishing / Social engineering (**+34%**), per conseguire la gran maggioranza dei loro obiettivi.

Tipologie di malware utilizzate (2017)



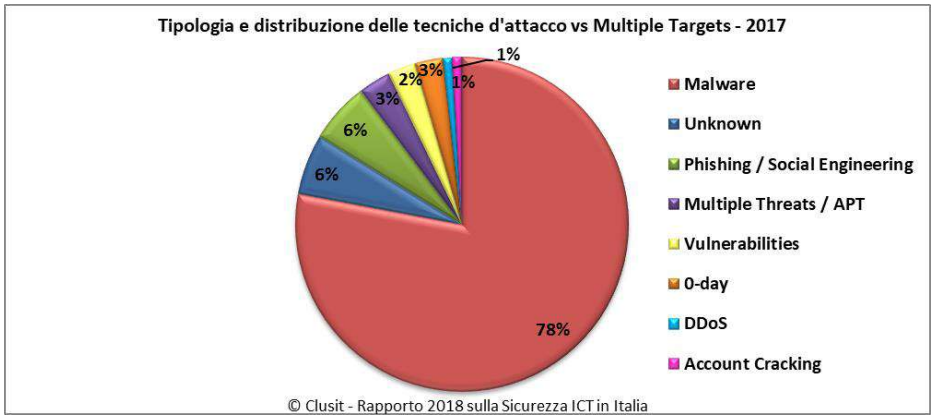
Dal grafico si possono osservare alcuni fenomeni interessanti, tra questi che il malware per le principali piattaforme mobile rappresenta ormai quasi il **20%** del totale, che il Ransomware rappresenta quasi un terzo del malware totale (**27%**), e che i Cryptominers, quasi inesistenti in passato, nel corso del 2017 sono arrivati a rappresentare il **7%** del totale.

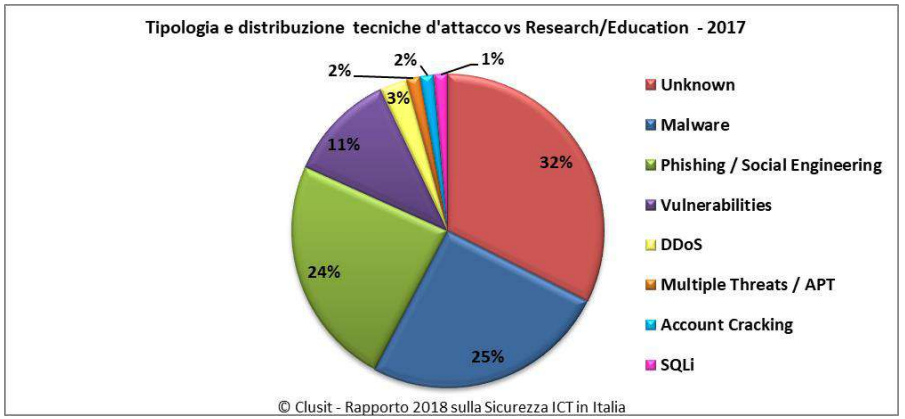
Tecniche di attacco nel mondo (7 anni)

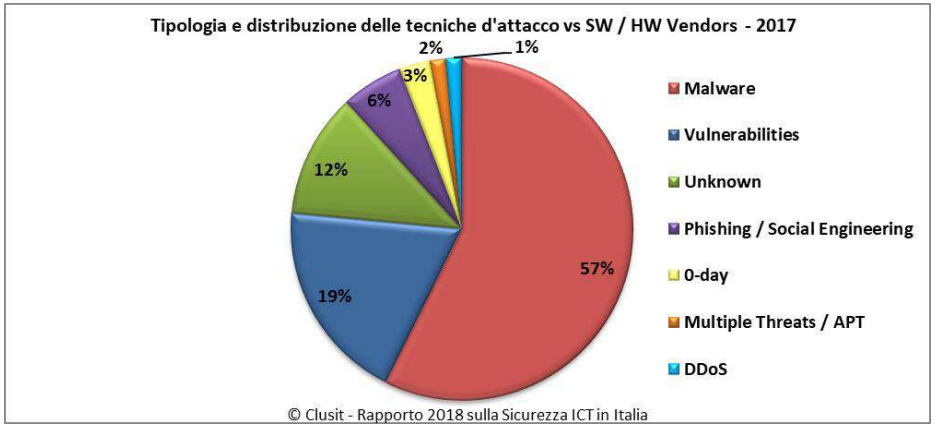


Considerato che stiamo analizzando gli attacchi più gravi del periodo, compiuti contro primarie organizzazioni pubbliche e private, spesso di livello mondiale, il fatto che la somma delle tecniche di attacco più banali (SQLi, DDoS, Vulnerabilità note, Phishing, malware "semplice") rappresenti ben il **68%** del totale (era il 56% nel 2016), implica che gli attaccanti *riescono ancora a realizzare attacchi di successo contro le loro vittime con relativa semplicità e a costi molto bassi, oltretutto decrescenti.*

Tipologia e distribuzione tecniche di attacco nei settori a maggior crescita degli attacchi (2017)



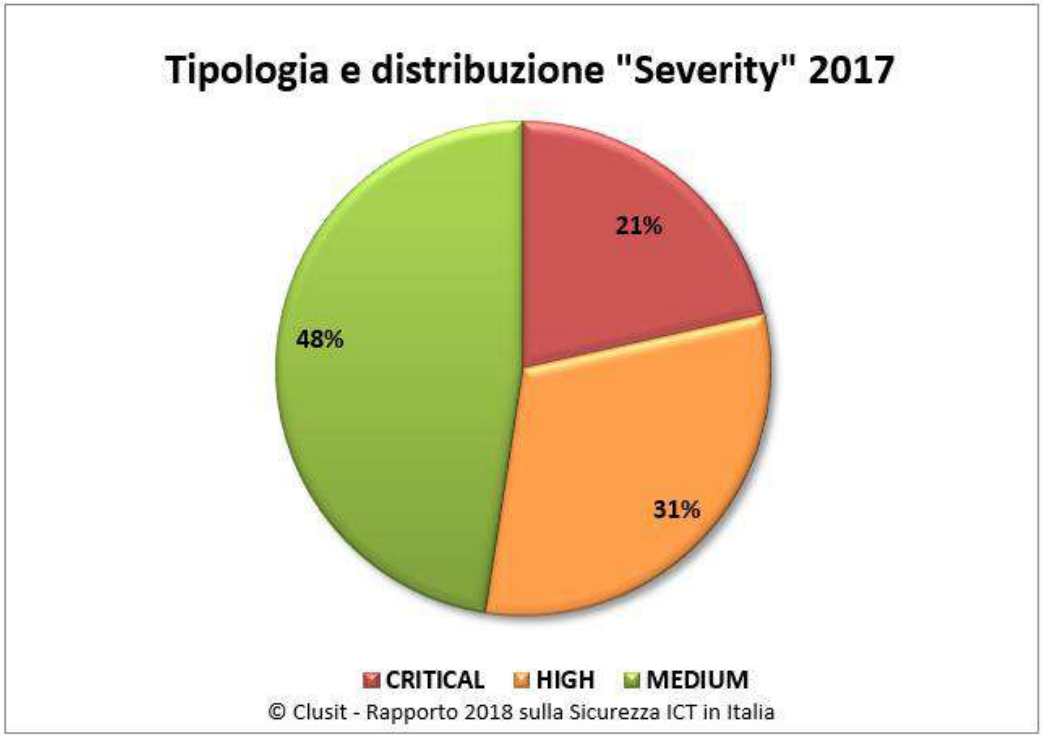




Anche quest'anno presentiamo le statistiche relative ad alcune categorie di vittime verticali, con un'attenzione particolare verso i primi 3 settori per tasso di crescita degli attacchi rispetto all'anno precedente (Multiple Targets, Research/Edu e HW-SW Vendors).

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.

Valutazione degli impatti ("Severity") 2017



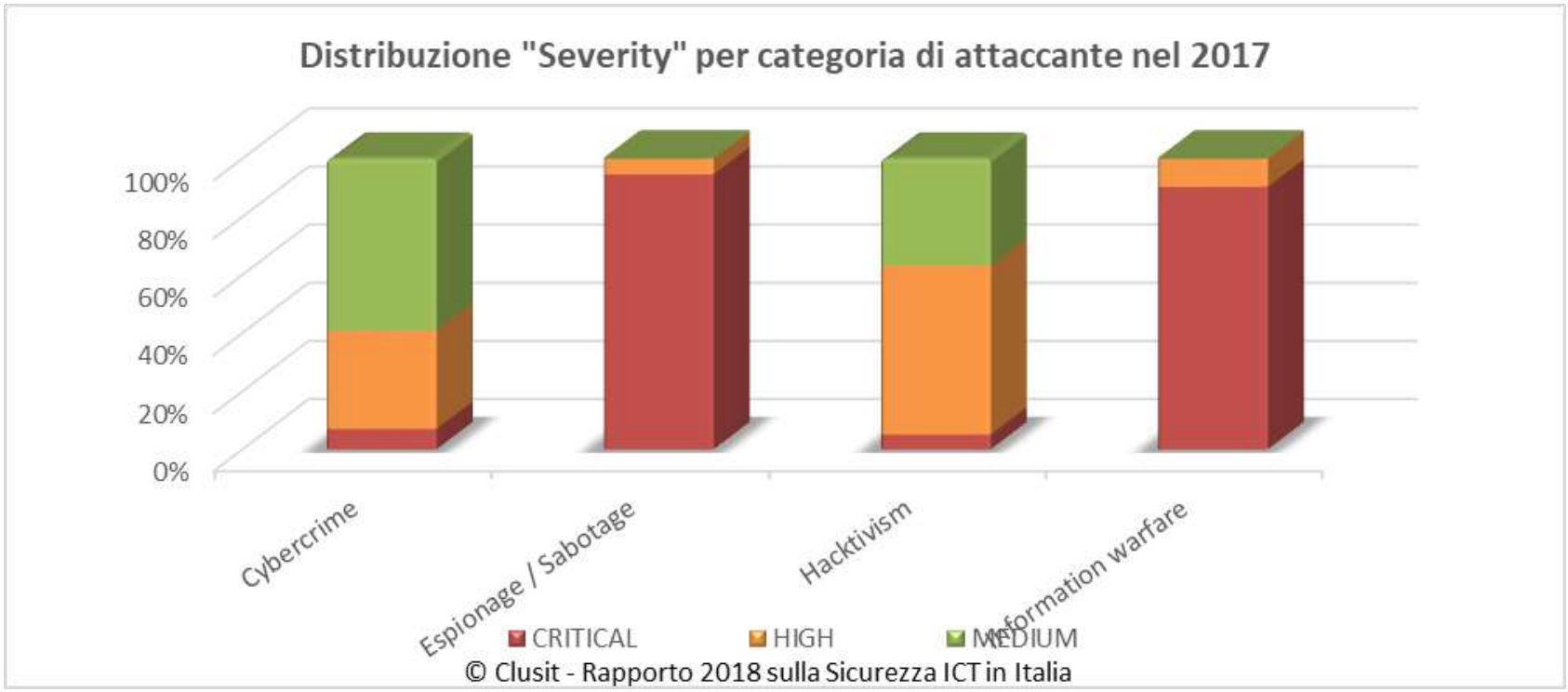
Per la prima volta quest'anno abbiamo definito tre categorie o livelli di impatto (considerato che stiamo comunque analizzando un campione di attacchi già tutti definiti come "gravi"): Medio, Alto e Critico.

Le variabili che contribuiscono a comporre la valutazione dell'impatto per ogni singolo attacco analizzato sono molteplici, ed includono: impatto geopolitico, sociale, economico (diretto e indiretto), di immagine e di costo/opportunità per le vittime.

Gli attacchi con impatto "Medio" rappresentano nel nostro campione quasi la metà del totale (**48%**), quelli di livello "Alto" un terzo (**31%**) e quelli di livello "Critico" un quinto (**21%**).

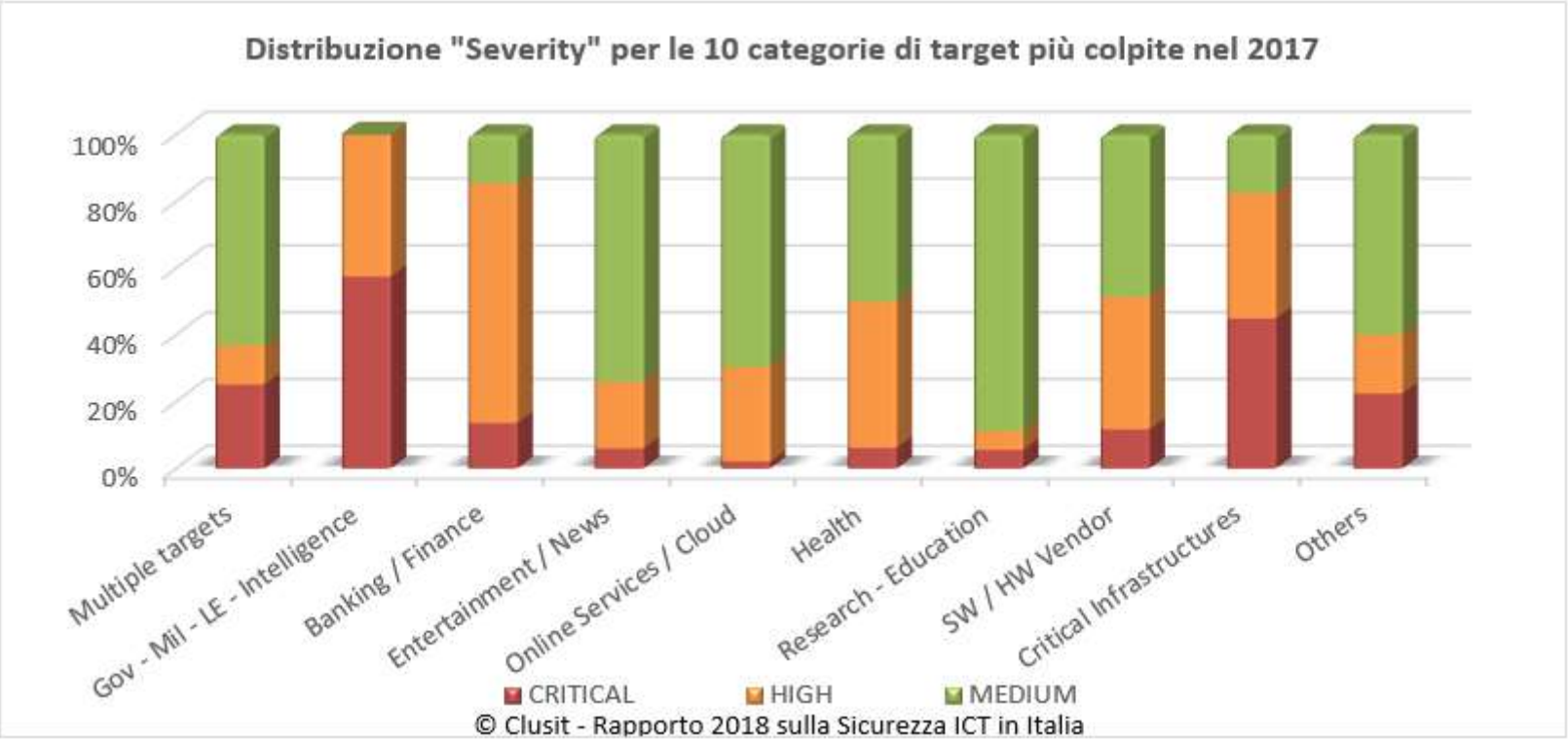
Raggruppando i dati per le consuete categorie (Attaccanti, Vittime e Tecniche di attacco) emergono ulteriori elementi di interesse.

Valutazione degli impatti per tipo di attaccante - 2017



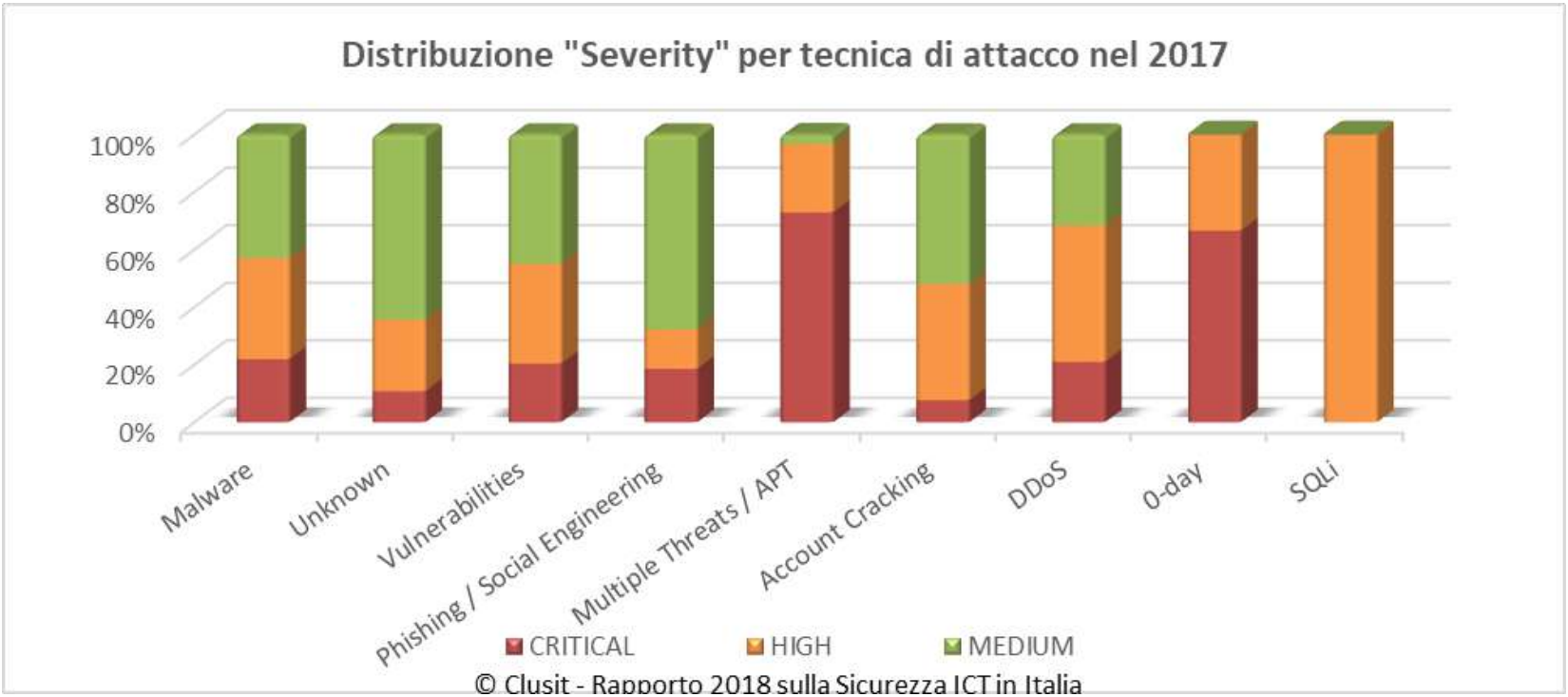
Da questo punto di osservazione il Cybercrime, pur rappresentando un problema enorme e facendo la parte del leone nel nostro campione per le ragioni sopra esposte, è ormai diventato l'ultimo dei nostri problemi in ambito cibernetico dal punto di vista della sua pericolosità intrinseca, nel senso che purtroppo ormai ci troviamo a fronteggiare problemi ben peggiori.

Valutazione degli impatti per tipo di vittima - 2017



Si può notare come le categorie “Gov” e “Critical Infrastructures” abbiano subito il maggior numero di attacchi con Severity “Critica”, mentre le categorie con il maggior numero di attacchi con impatti di livello “Alto” sono “Banking/Finance” e “Healthcare”.

Valutazione degli impatti per tecniche usate - 2017



Gli attacchi con impatto più critico sono quelli realizzati tramite APT e 0-day (quindi più sofisticati e stealth, spesso con motivazioni geopolitiche e finalità di Espionage e Information Warfare).

Molto simili in percentuale gli attacchi con impatto “Critico” realizzati tramite Malware, Vulnerabilità note, Phishing e DDoS, mentre prevalgono gli impatti di tipo “Alto” nel caso di attacchi condotti tramite tecniche di Account Cracking, DDoS e SQL injection.

Trends 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

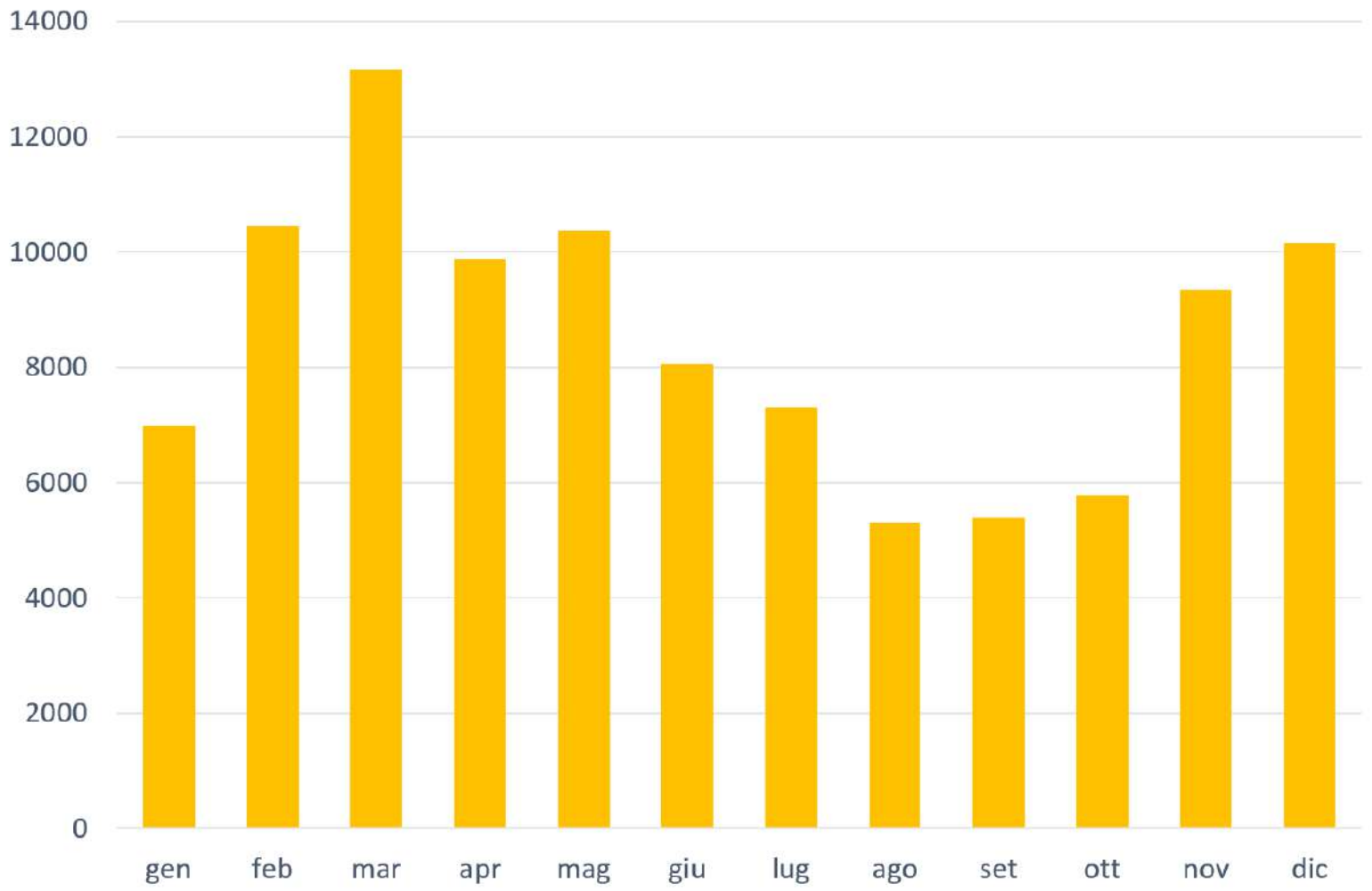
La base dati

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

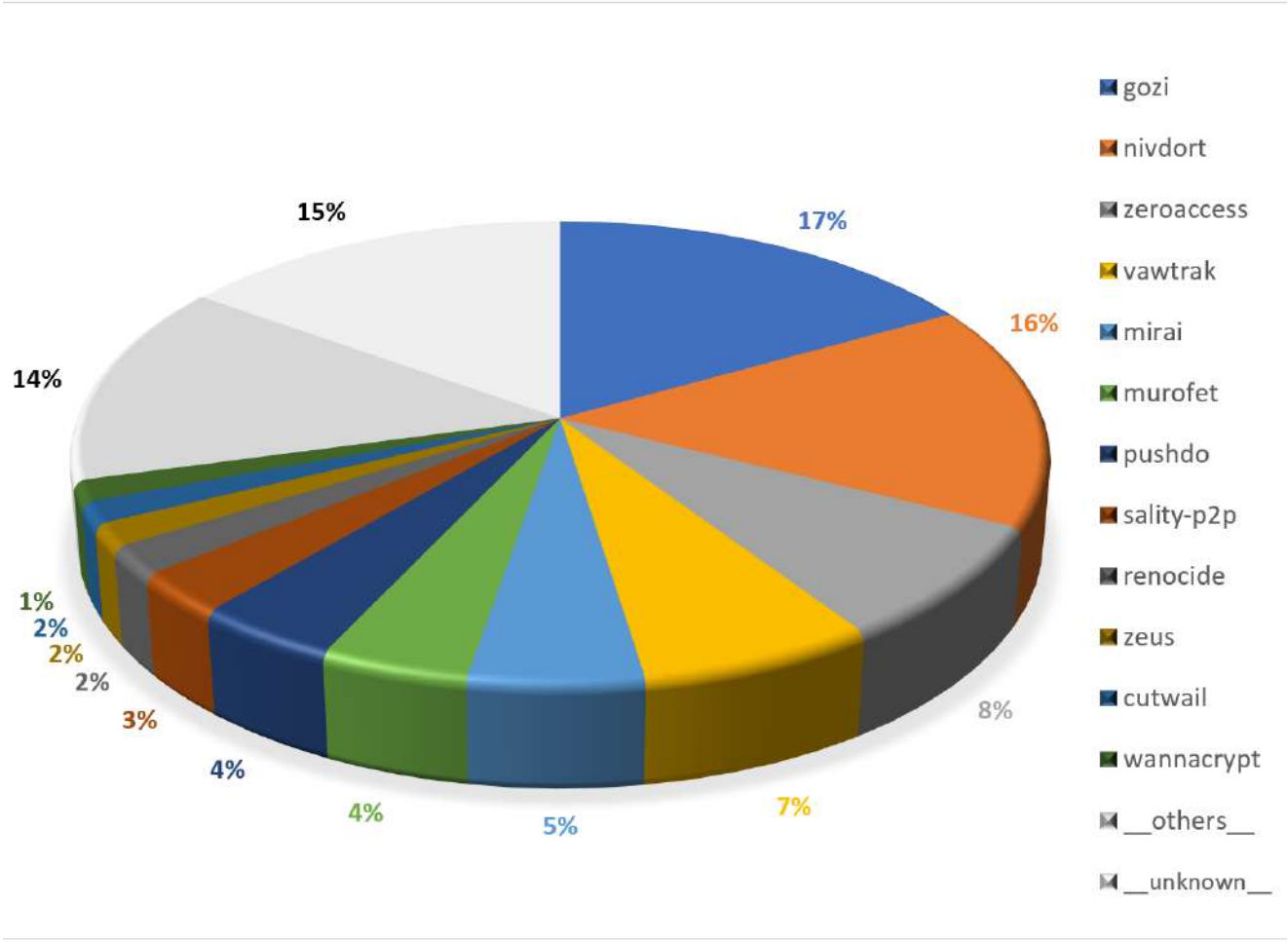
6 milioni di indirizzi IP pubblici (stesso perimetro)

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

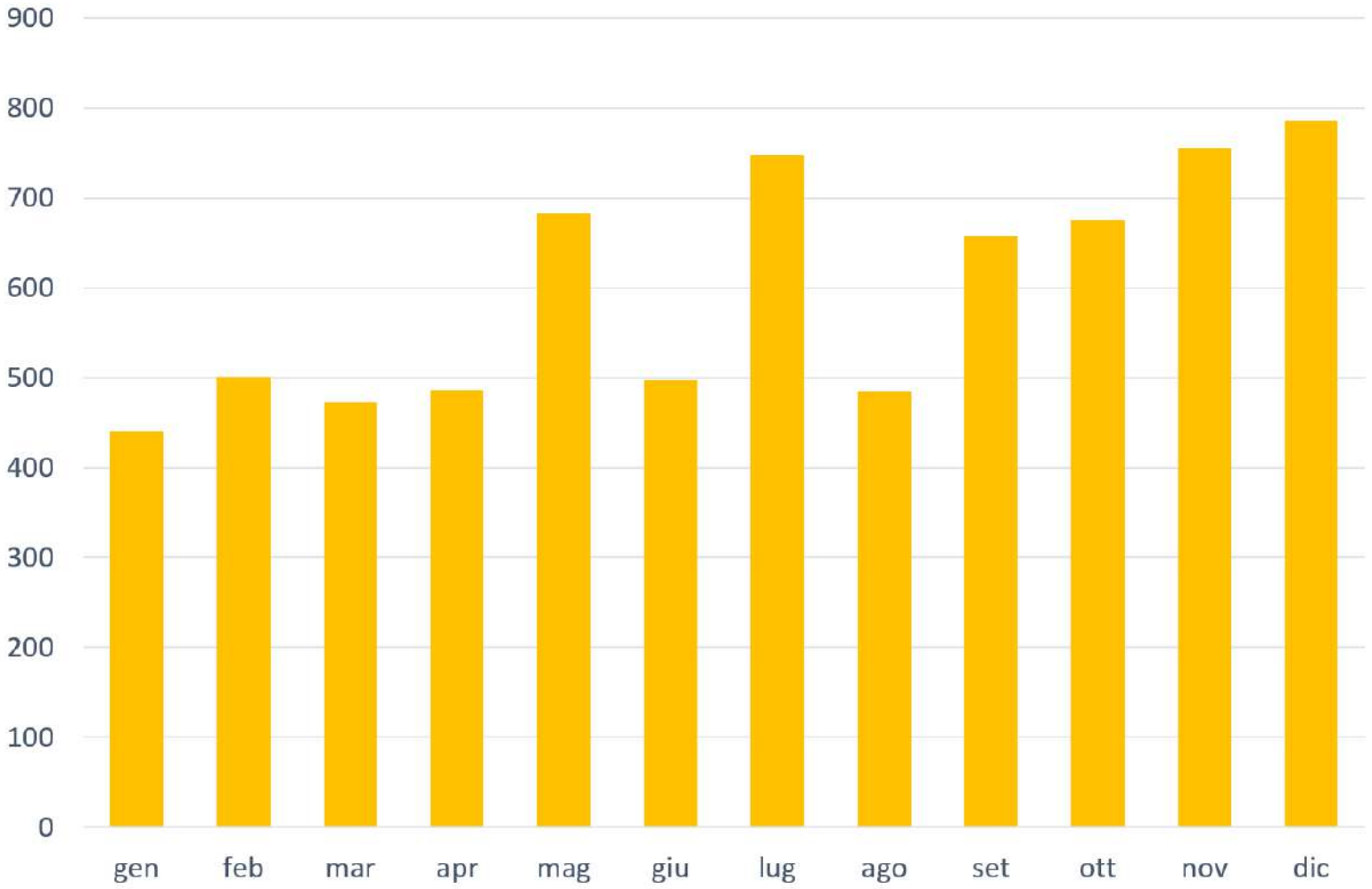
Rilevazione mensile dei malware



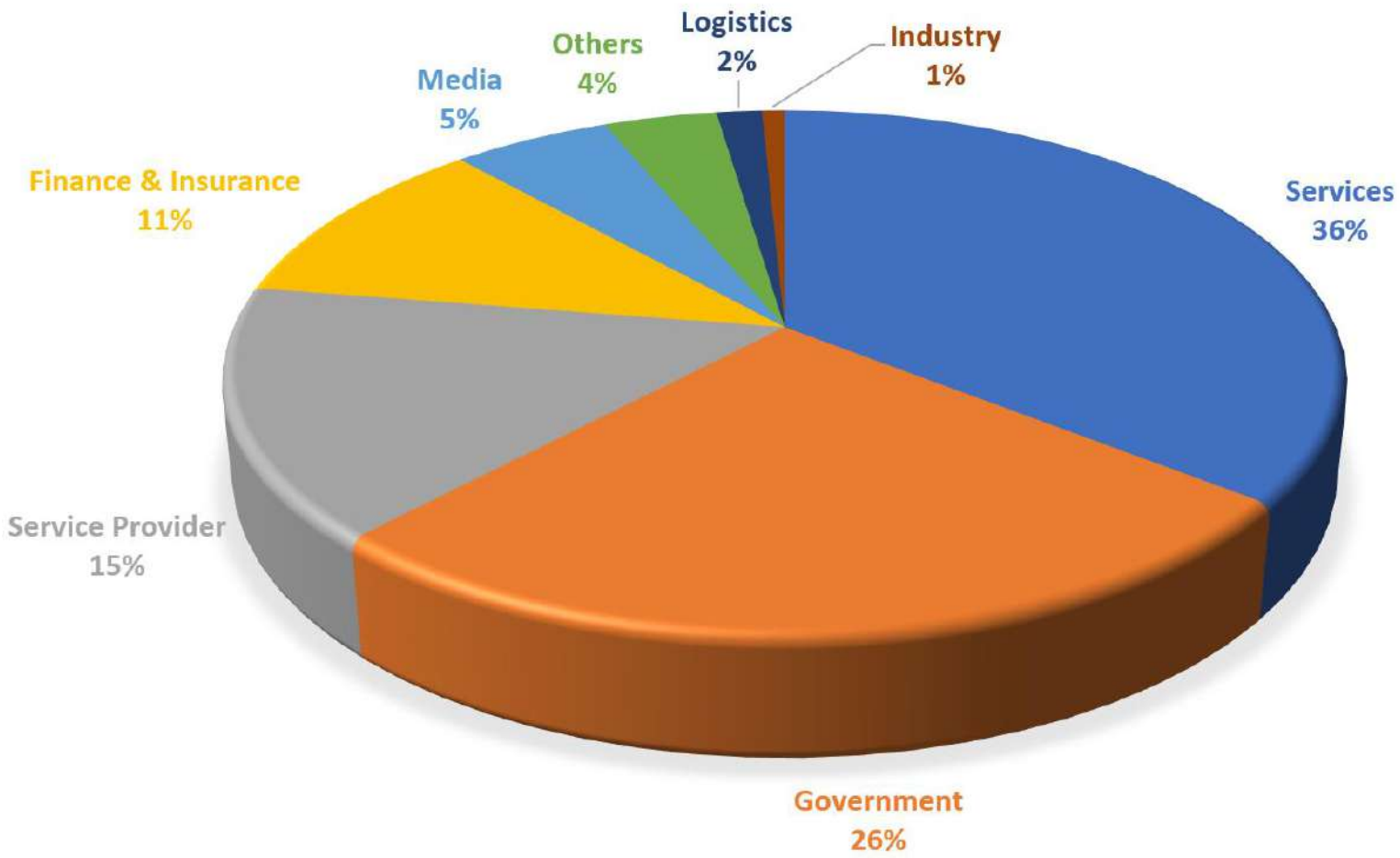
Famiglie malware



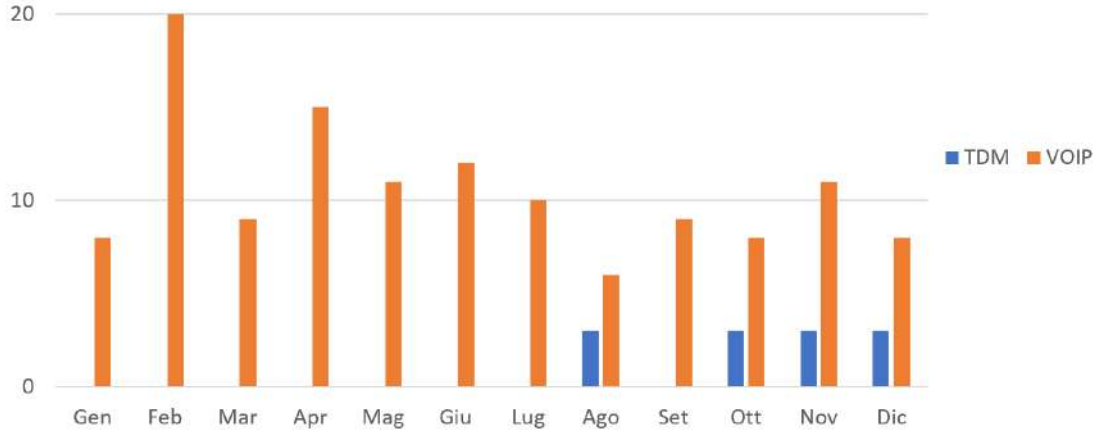
Distribuzione mensile 'anomalie' DDoS

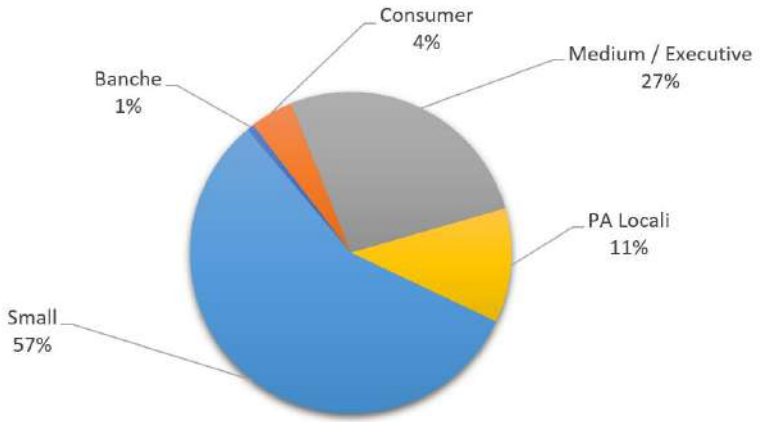


Target di possibili attacchi DDoS



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!)

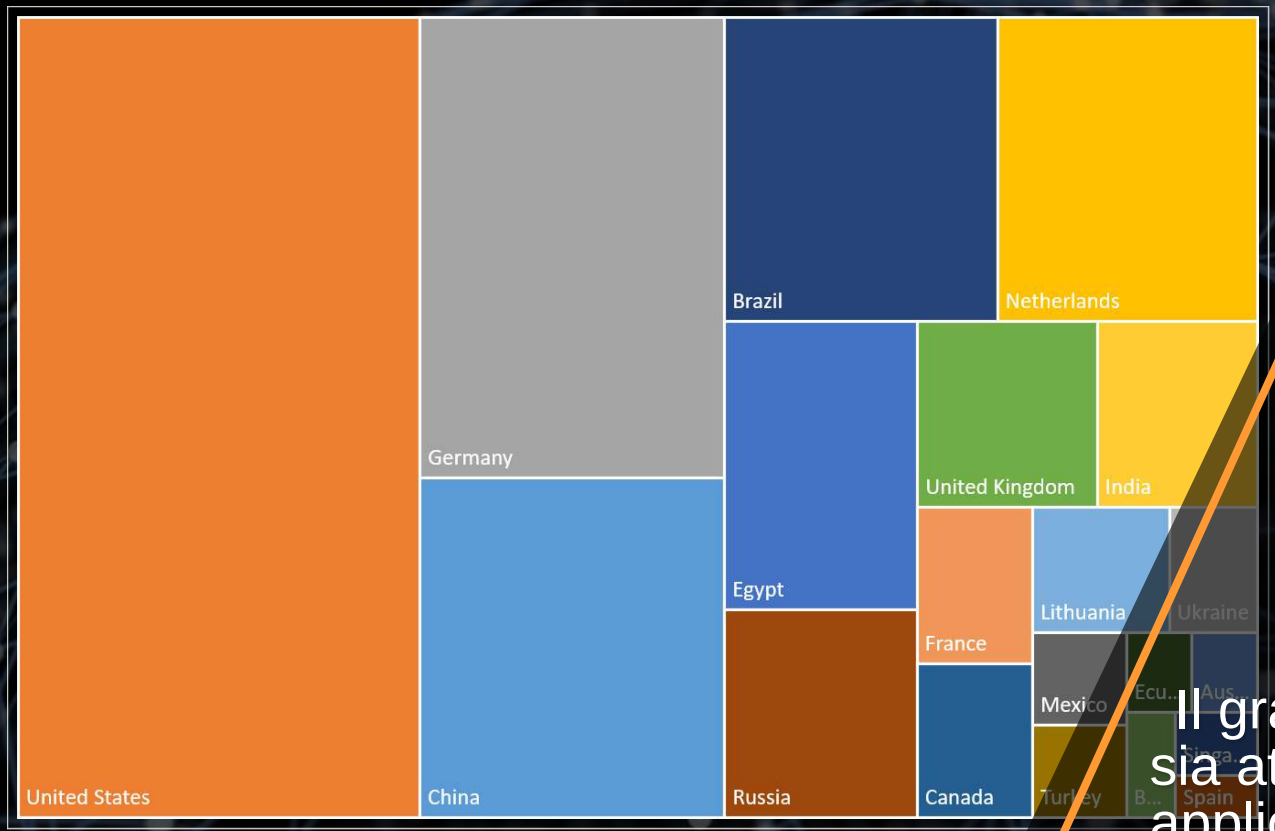
Attacchi letali per le aziende

Sempre più compromissioni tramite IoT

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

Rapporto 2017
sullo stato di Internet e analisi globale degli attacchi DDoS e applicativi Web

Attacchi
DDoS



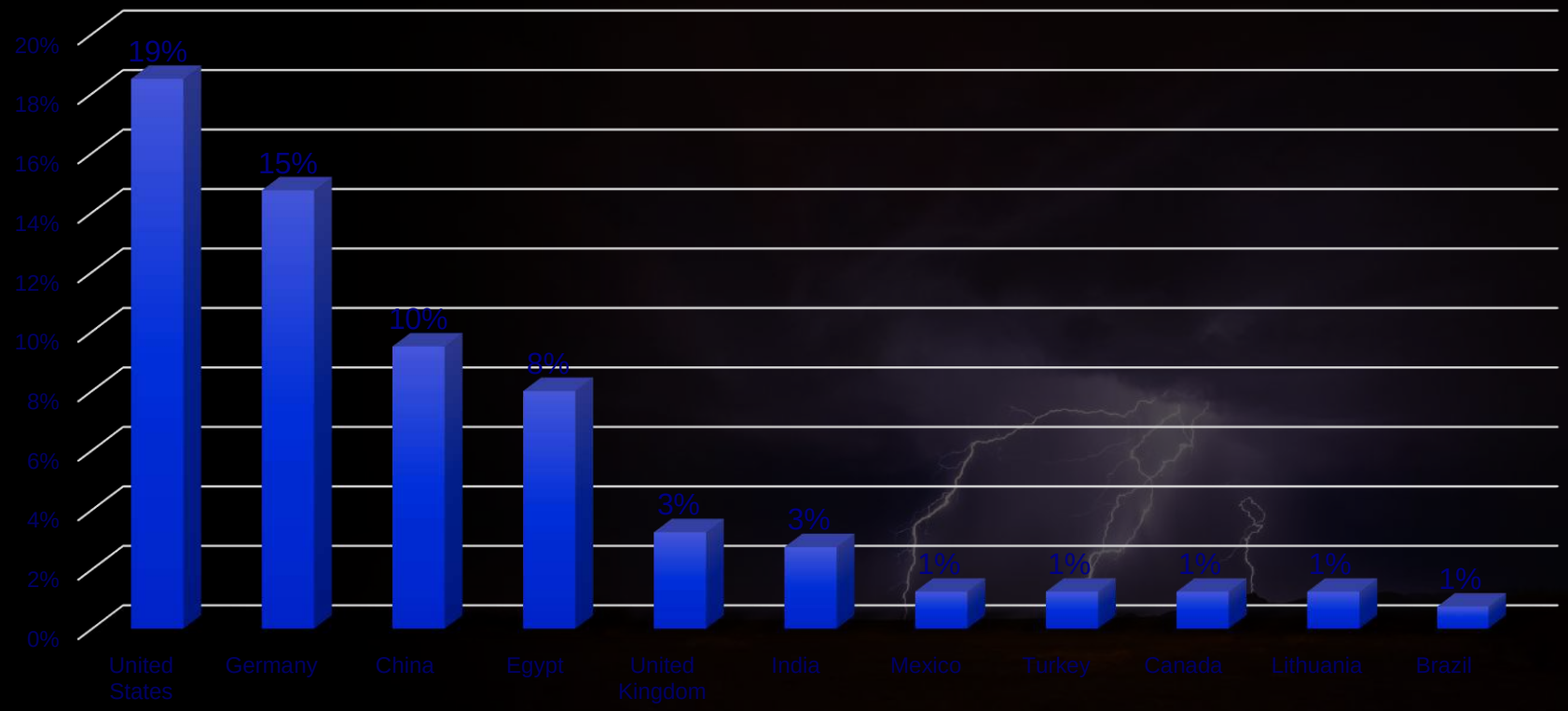
Prime 3 nazioni generano più del 50% degli attacchi

Le prime tre nazioni sono di 3 differenti continenti

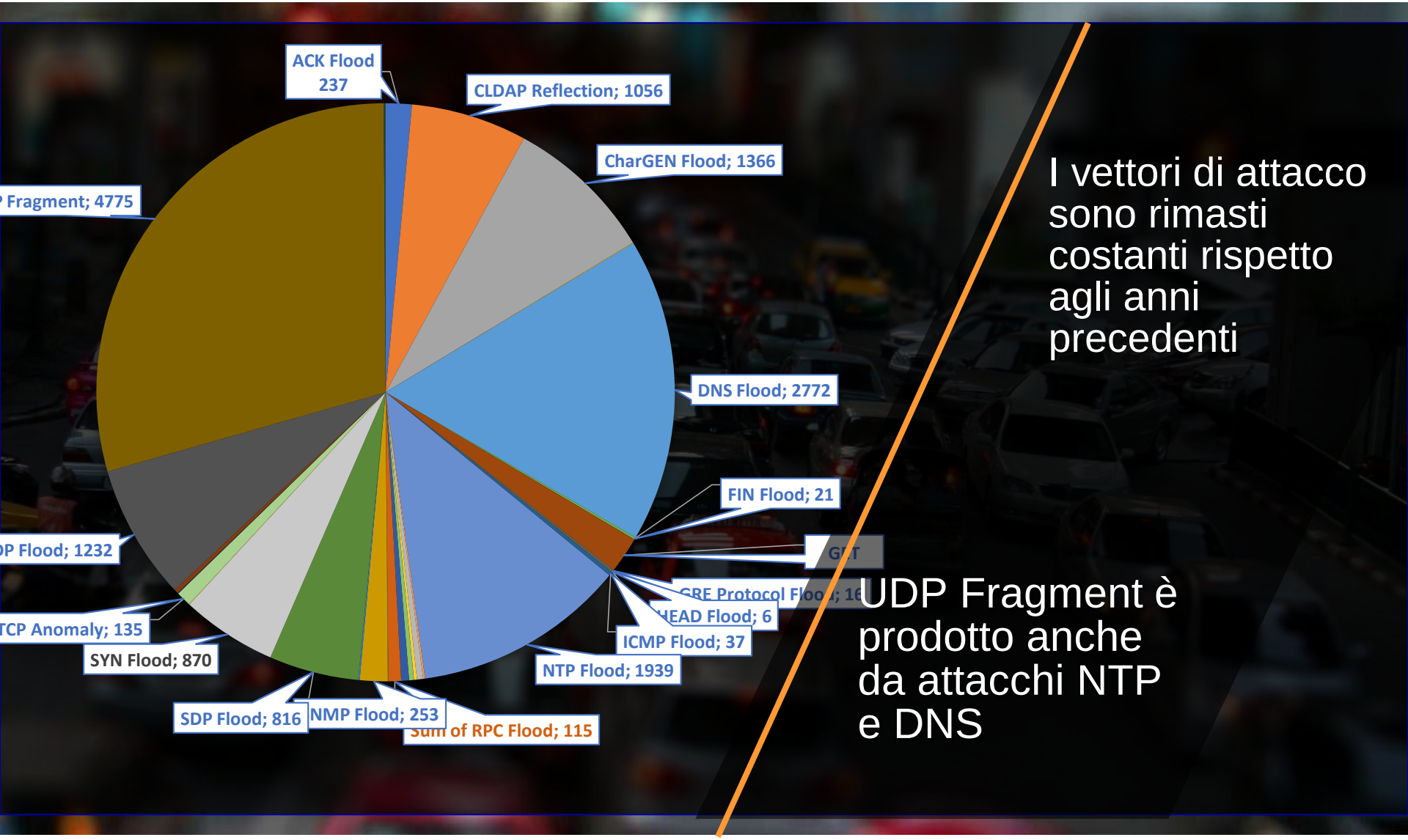
Il grafico mostra sia attacchi applicativi che volumetrici

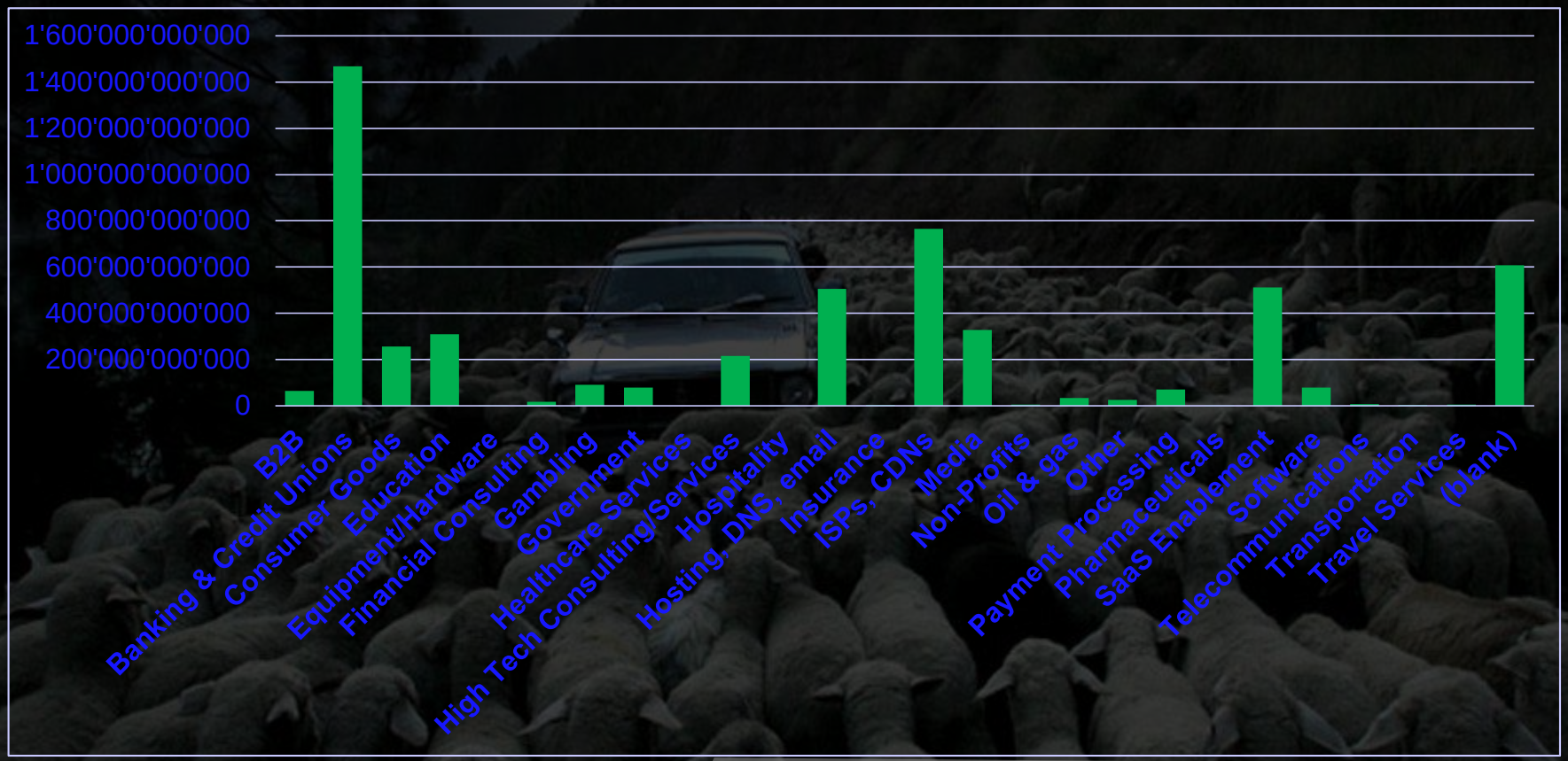
Attacchi Applicativi

Attacci Denial of Service

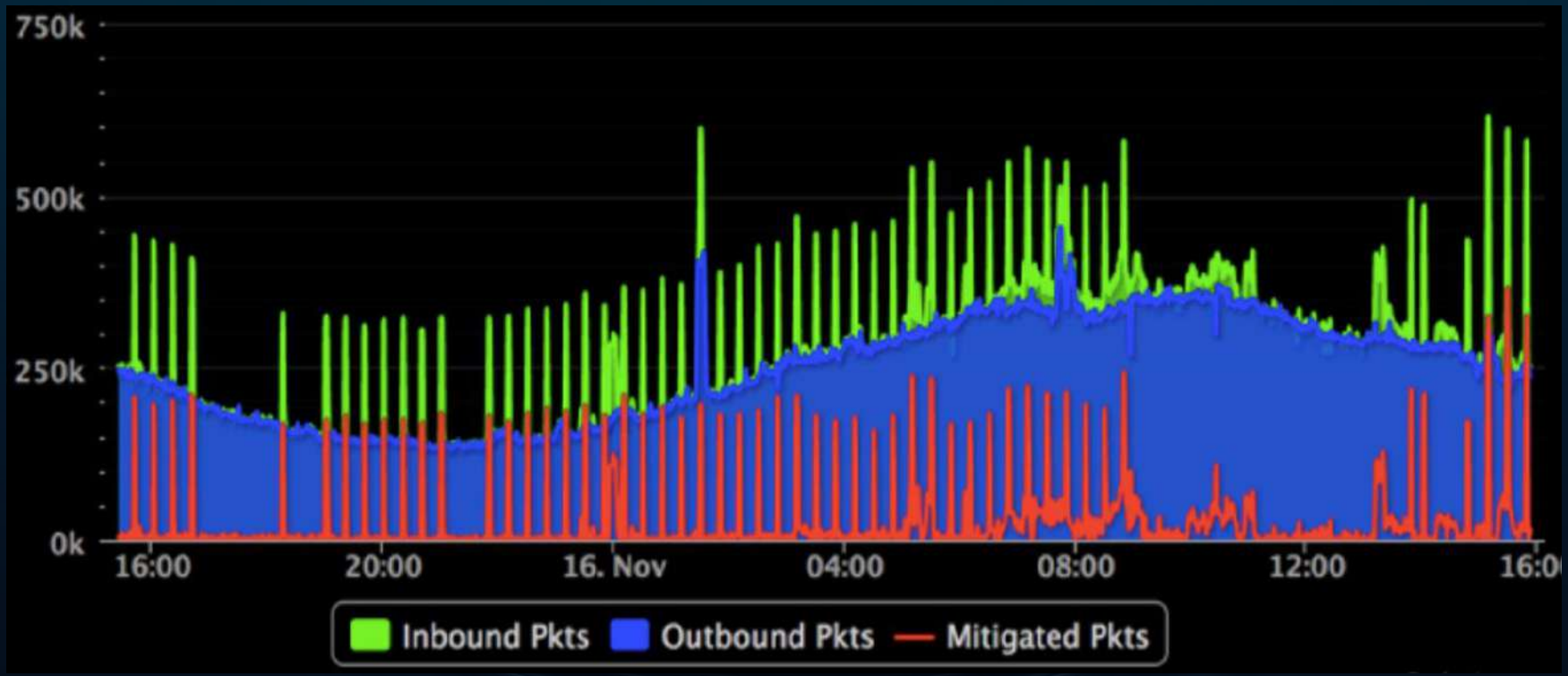


1 milione di IP hanno contribuito a diffondere Satori, una botnet per Account Take over

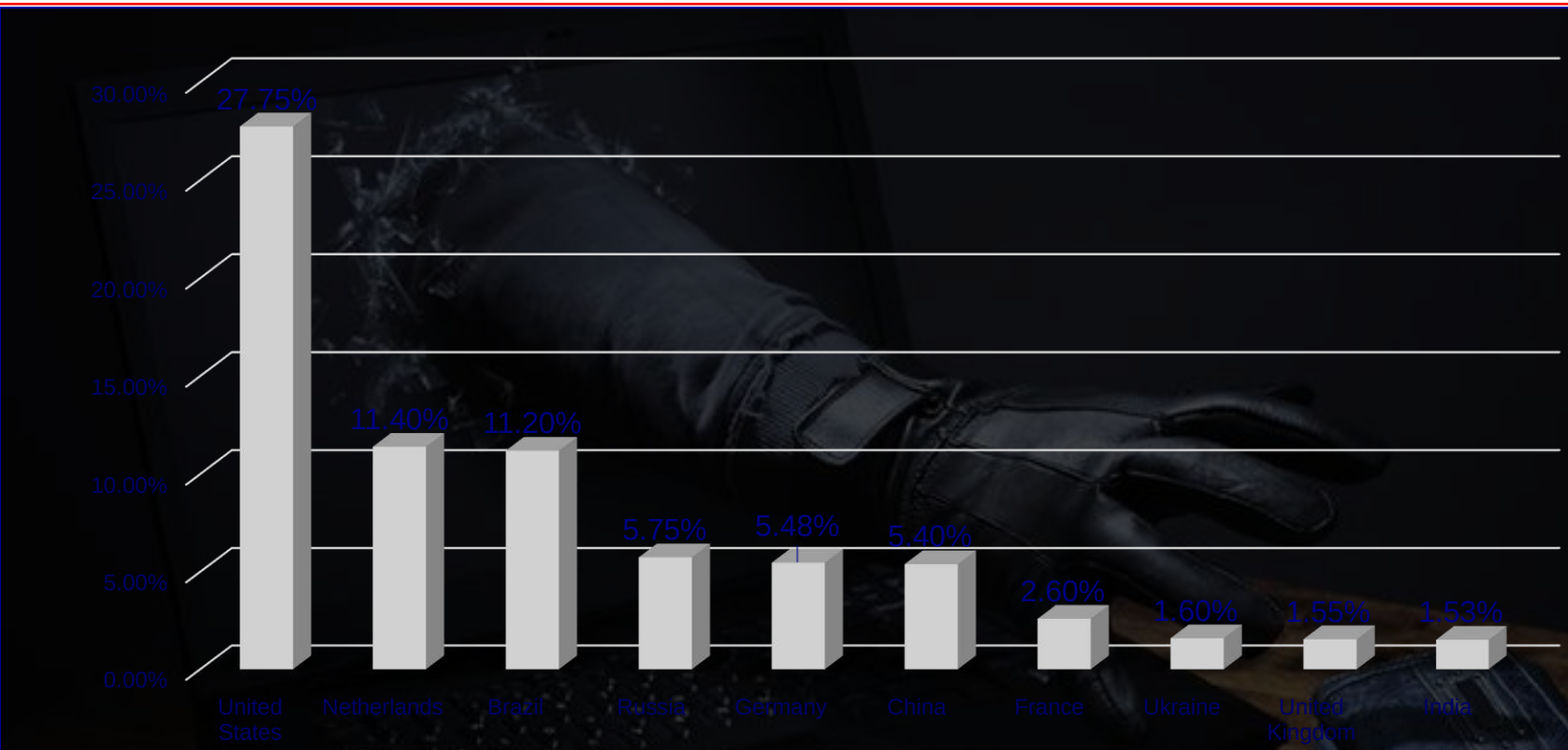

ACK Flood 237
CLDAP Reflection; 1056
CharGEN Flood; 1366
Fragment; 4775
DNS Flood; 2772
FIN Flood; 21
P Flood; 1232
GET
HEAD Flood; 6
ICMP Flood; 37
TCP Anomaly; 135
SYN Flood; 870
NTP Flood; 1939
SDP Flood; 816
NMP Flood; 253
Sum of RPC Flood; 115
I vettori di attacco sono rimasti costanti rispetto agli anni precedenti
UDP Fragment è prodotto anche da attacchi NTP e DNS



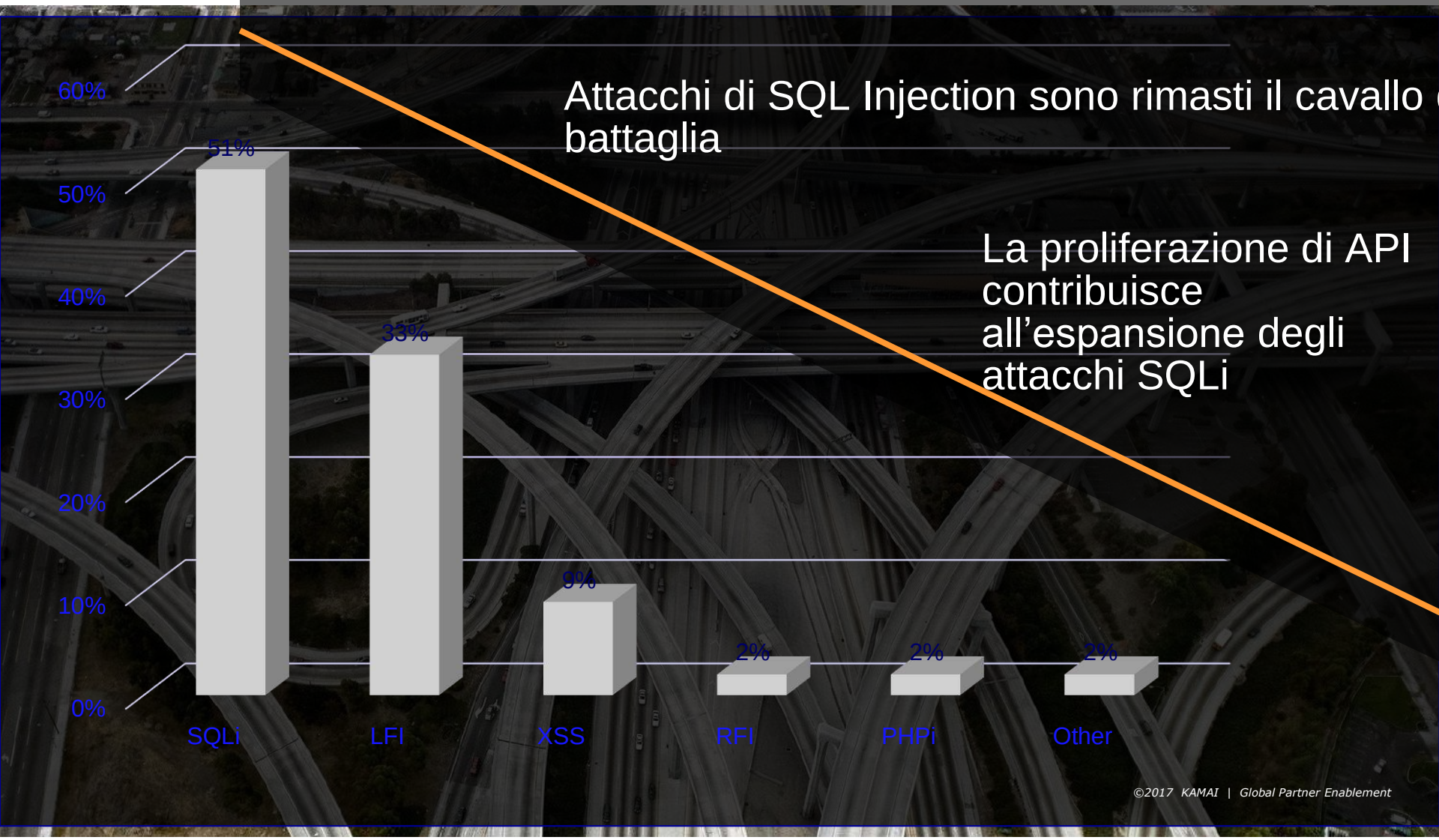
Un singolo cliente attaccato più di 2000 volte

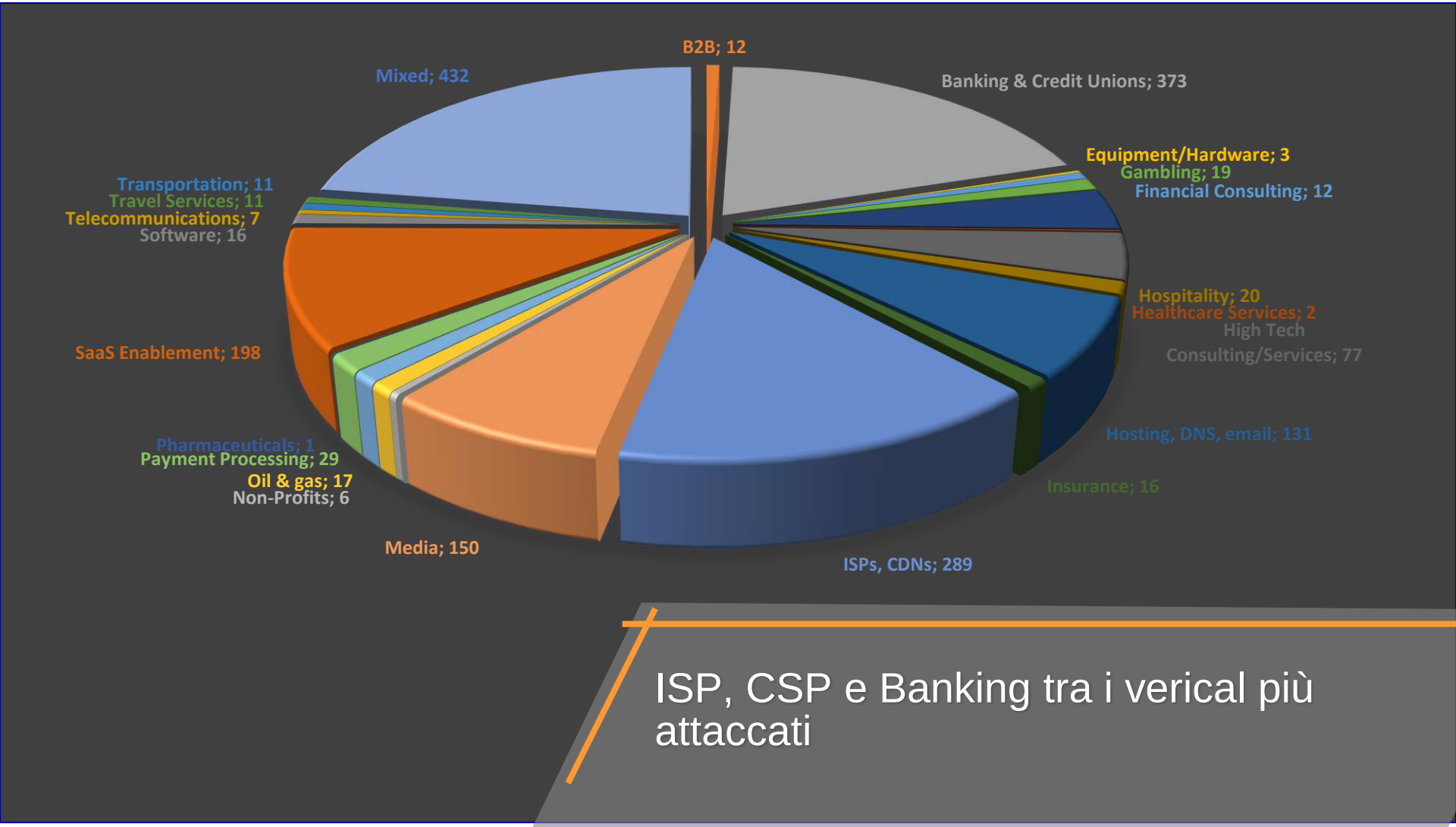


Attacchi “Hit & Run” – eseguiti in breve tempo e ripetuti, prima che si possano mettere in atto le contromisure



Più del 10% di incremento di attacchi web based rispetto all'anno precedente


Attacchi di SQL Injection sono rimasti il cavallo
battaglia
La proliferazione di API
contribuisce
all'espansione degli
attacchi SQLi
60%
50%
40%
30%
20%
10%
0%
51%
33%
9%
2%
2%
2%
SQLi
LFI
XSS
RFI
PHPi
Other
©2017 KAMAI | Global Partner Enablement



ISP, CSP e Banking tra i verical più attaccati

Per scaricare il rapporto in formato digitale:

https://clusit.it/rapporto-clusit

Clusit
Associazione Italiana
per la Sicurezza Informatica