Security Summit Milano 2019

Sessione plenaria del 12 Marzo

Clusit
Associazione Italiana
per la Sicurezza Informatica

SECURITY
TECHNOLOGIES
MANAGEMENT
COMPLIANCE
SUMMIT

Rapporto Clusit 2019 sulla sicurezza ICT in Italia

Moderano: Gabriele Faggioli e Alessio Pennasilico

Intervengono alcuni degli autori:

- Andrea Zapparoli Manzoni, Clusit
- Marco Raimondi, Fastweb
- Rodolfo D'Agostino, Akamai

Partecipano alla Tavola Rotonda:

- Angelo Bosis, Oracle Italia
- Gianluca Busco Arrè, Panda Security Italia
- Gastone Nencini, Trend Micro Italia
- Domenico Raguseo, IBM Italia
- Federico Santi, DXC Technology

Clusit

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

Contenuti del Rapporto #1

- **Analisi cyber**
  - Panoramica dei cyber attacchi più significativi del 2017
  - Attacchi rilevati dal SOC di Fastweb
  - Analisi globale degli attacchi DDoS e applicativi web
  - Rilevazioni e segnalazioni della Polizia Postale e delle Comunicazioni
  - Rilevazioni e segnalazioni della Guardia di Finanza
  - Rilevazioni e segnalazioni del Cert Nazionale
- **Analisi Finance**
  - Elementi sul Cyber-crime nel settore finanziario in Europa
  - Analisi del Cyber-crime in Italia in ambito finanziario nel 2018
  - Sviluppo di un sistema di cyber threat intelligence (a cura del CERT di Banca d'Italia)
  - Carding – Scenario ed evoluzione dei canali di vendita nel 2018
- **Analisi GDPR**
  - Stato di adeguamento al GDPR delle aziende italiane (Osservatori del Politecnico di Milano)
  - 2019: data protection 4.0
  - La terza fase del GDPR
  - Cifratura dei dati personali
- **Il mercato italiano della sicurezza IT:** analisi, prospettive e tendenze secondo IDC

Contenuti del Rapporto #2

- **Tecnologie emergenti: Intelligenza Artificiale**
  - Intelligenza Artificiale: il Buono, il Brutto, il Cattivo
  - L'Intelligenza Artificiale è sicura?
  - L'intelligenza artificiale come strumento "dual use" nella cybersecurity
- **Tecnologie emergenti: Blockchain**
  - Blockchain & Supply Chain: una catena del valore sicura, distribuita e trasparente
  - Possibili problemi nella gestione degli smart contracts
  - Il 2018 dei Crypto Exchange
- **Focus On**
  - Programmi di security awareness: una necessità non più rimandabile
  - La sicurezza delle imprese è fatta di persone competenti e consapevoli. Un manifesto per la competenza digitale e la consapevolezza in materia di sicurezza online con focus sulla Generazione Z
  - Il panorama delle startup italiane nel settore cybersecurity e legal-tech. Stato dell'arte e valutazioni sul trend evolutivo
  - La logica del profitto alla base dell'aumento del cryptojacking
  - Infrastrutture critiche vulnerabili. Sempre più alto il rischio di attacchi agli impianti idrici ed energetici
  - Attacchi e difese nel Cloud Computing nel 2018

Andrea Zapparoli Manzoni

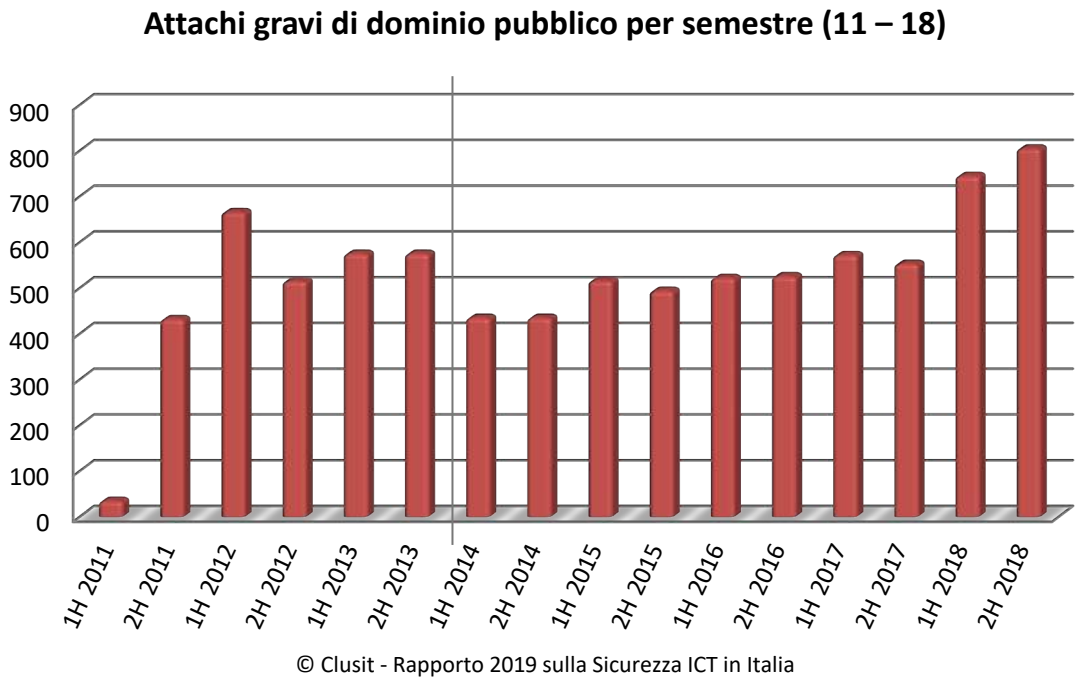
Clusit

Quali sono i numeri del campione ?

In media negli ultimi 96 mesi abbiamo analizzato e classificato 88 attacchi gravi di dominio pubblico al mese (94 al mese nel 2017, 129 nel 2018)

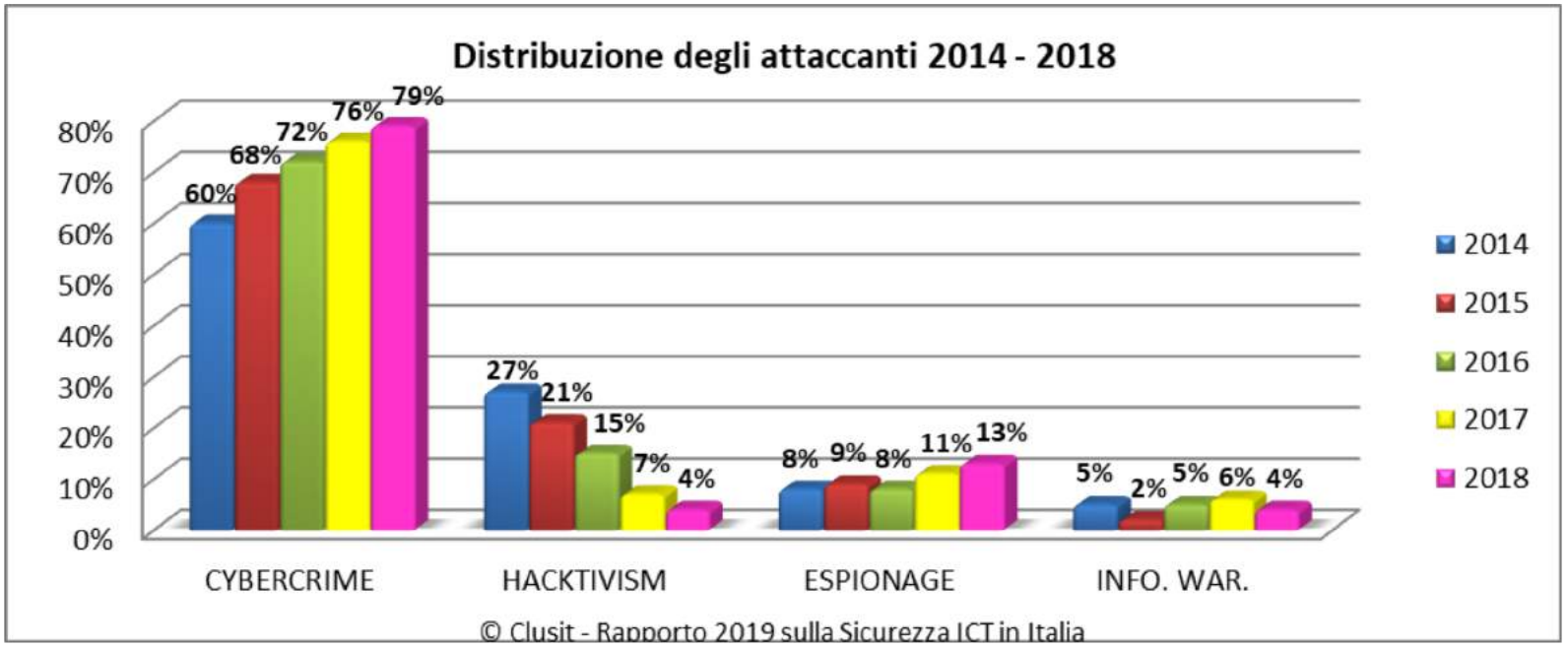
- **8.417** attacchi gravi analizzati dal gennaio 2011 al dicembre 2018.

- 873 nel 2014 (*)
- 1.012 nel 2015
- 1.050 nel 2016
- 1.127 nel 2017
- **1.552 nel 2018**



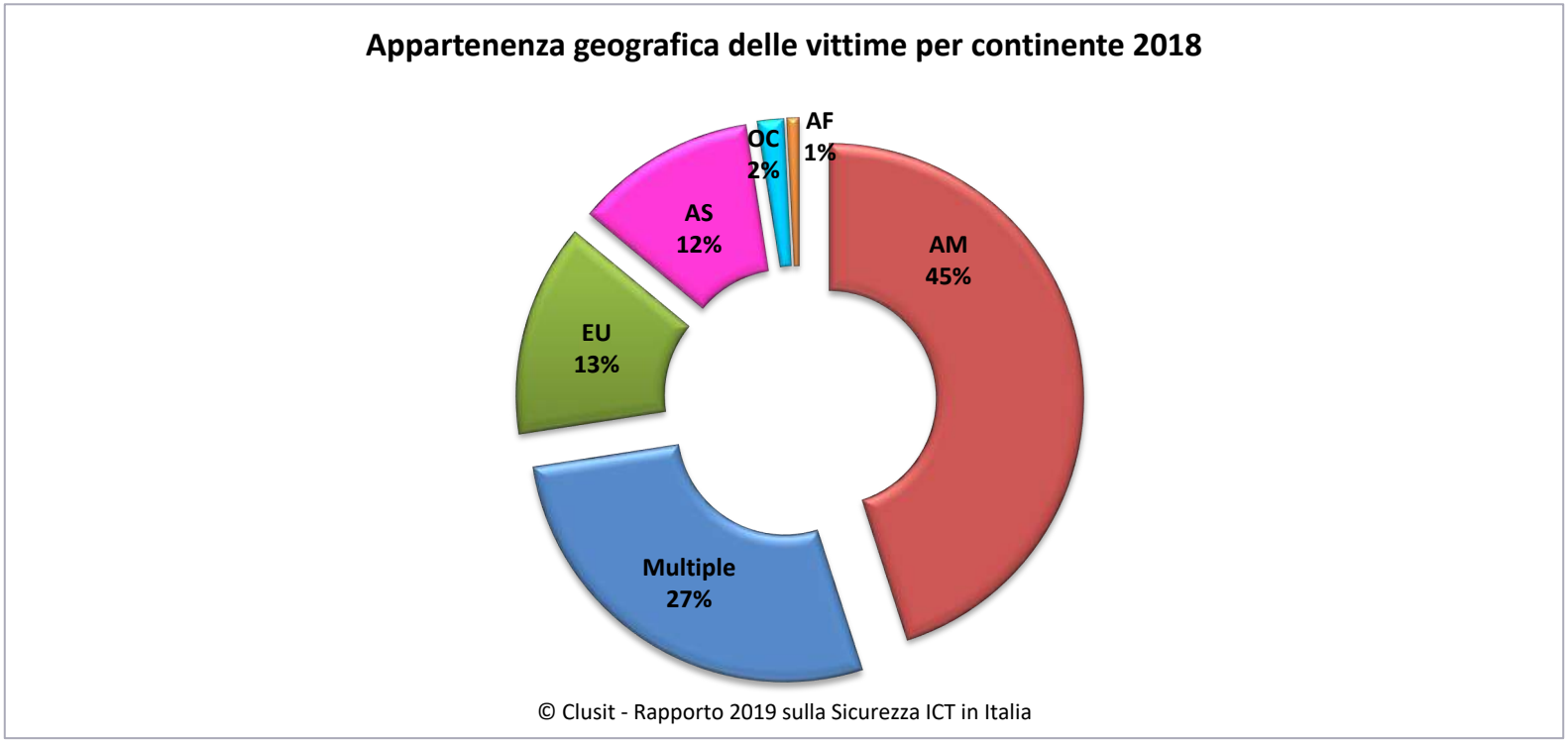
(*) Nel 2014 il numero assoluto di attacchi gravi che abbiamo registrato è diminuito rispetto al triennio precedente perché abbiamo reso più restrittivi i criteri di classificazione, per allinearli al livello crescente di minaccia. Con i criteri precedenti sarebbe aumentato di circa il 10%. Nel 2015, pur applicando i nuovi criteri, la crescita rispetto al 2014 è pari al 14%. Nel 2016 la crescita è del 3,75% (circa +20% rispetto al 2014). Nel 2017, la crescita rispetto al 2014 è del 30%. Nel 2018, la crescita rispetto al 2017 è del 37,7% e rispetto al 2014 è del +77,8%.

Tipologia e distribuzione degli attaccanti



ATTACCANTI PER TIPOLOGIA	2014	2015	2016	2017	2018	2018 su 2017	Trend
Cybercrime	526	684	751	857	1232	43,8%	↑
Hacktivism	236	209	161	79	61	-22,8%	↓
Espionage / Sabotage	69	96	88	129	203	57,4%	↑
Cyber warfare	42	23	50	62	56	-9,7%	↘
Espionage / Sabotage + Cyber Warfare	111	119	138	191	259	35,6%	↑

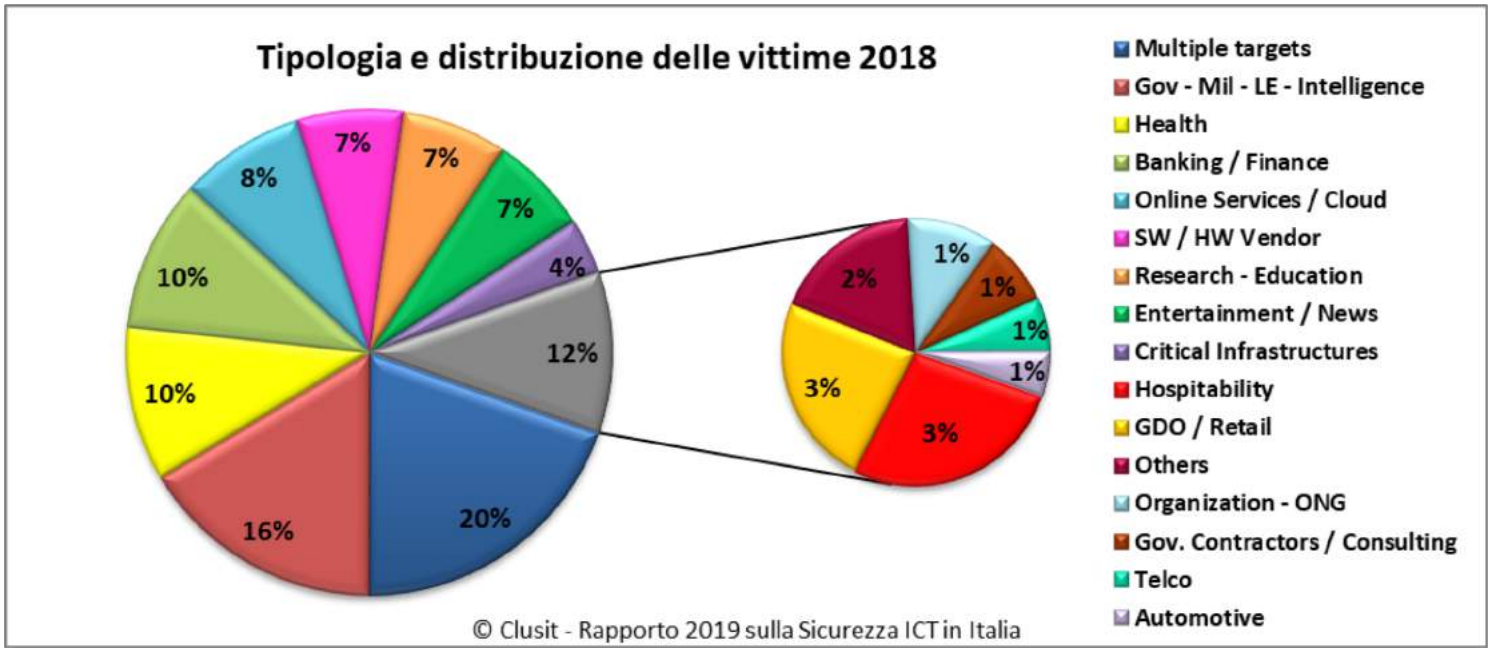
Distribuzione geografica vittime



Nel 2018 aumentano le vittime di area americana (dal 43% al **45%**), mentre, in attesa che GDPR e NIS facciano emergere molti attacchi ad oggi non noti, gli attacchi verso realtà basate in Europa sembrano addirittura diminuire (dal 16% al **13%**) e aumentano quelli rilevati contro organizzazioni asiatiche (dal 10% al **12%**).

Percentualmente rimangono sostanzialmente invariati gli attacchi gravi verso bersagli multipli distribuiti globalmente (categoria "Multiple"), dall'28% del 2017al **27%** del 2018.

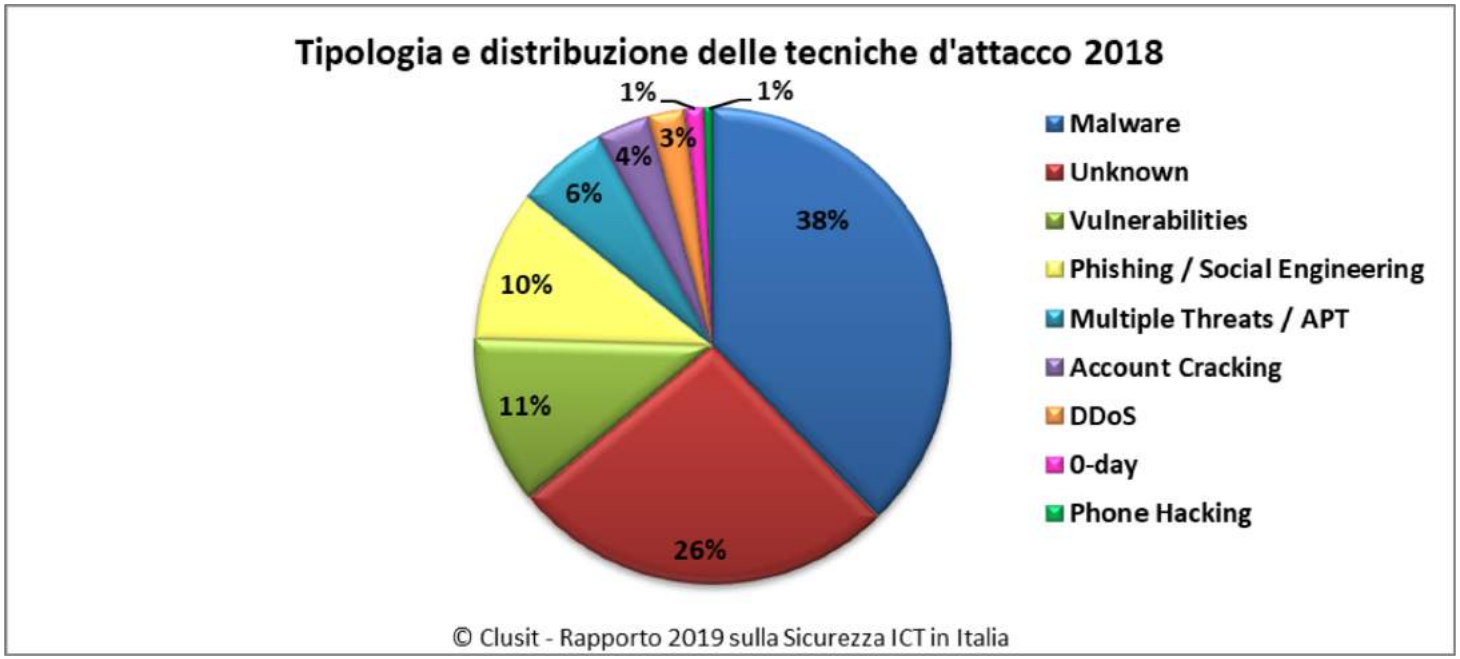
Distribuzione vittime nel mondo



Rispetto al 2017, in termini assoluti nel 2018 il maggiore aumento di attacchi gravi si osserva verso le categorie “Multiple Targets” (**+36,9%**), “Gov” (**+40,8%**) ed “Healthcare” (**+98,8%**), seguite da “Banking / Finance” (**+33,3%**), “Online Services / Cloud” (**+35,8%**) e da “Research / Education” (**+54,9%**).

Degna di nota anche la crescita degli attacchi verso le categorie “Critical Infrastructures” (**+42,5%**), “Software/Hardware vendor” (**+60.3%**) e “GDO/Retail” (**+62,5%**).

Tecniche di attacco nel mondo

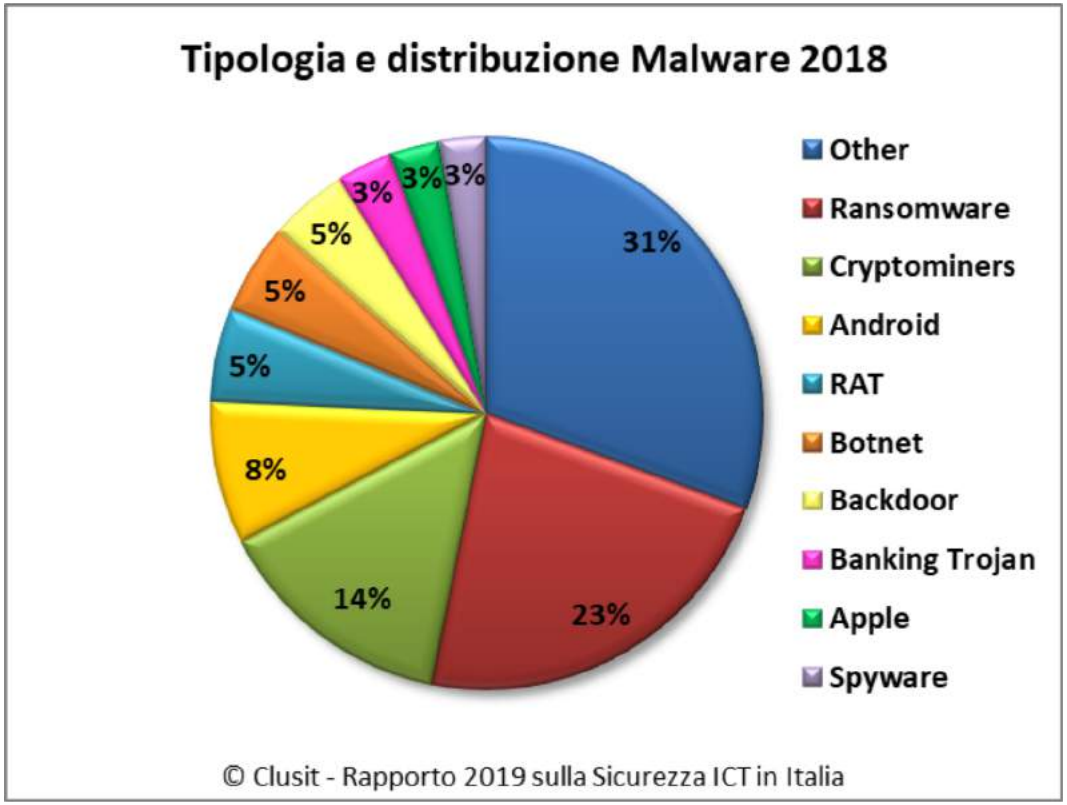


Per la seconda volta dal 2011, nel 2018 le tecniche sconosciute (categoria “Unknown”) passano al secondo posto, pur con una crescita del **47,3%** rispetto al 2017, superate dalla categoria “Malware” (+**31,2%**).

A questo dato va sommata la crescita significativa della categoria “Multiple Techniques / APT” (**+55,6%**).

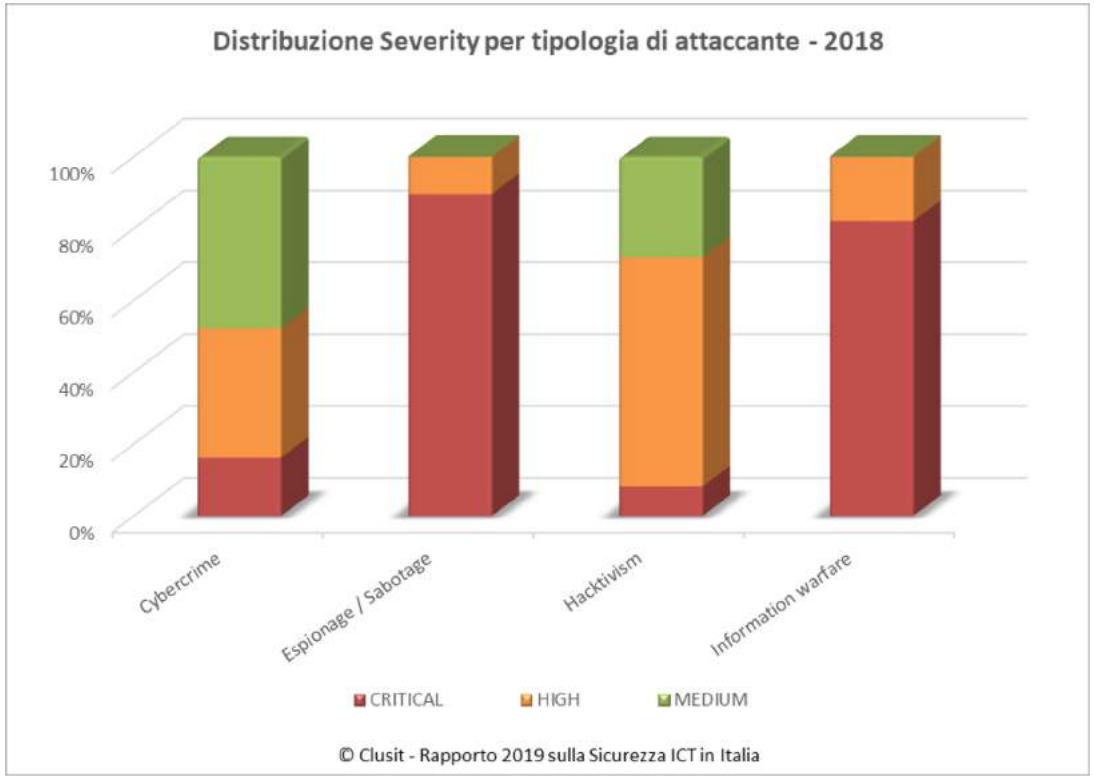
I DDoS rimangono sostanzialmente invariati, mentre le SQL injection finalmente crollano all’ultimo posto facendo segnare un **-85,7%** rispetto al 2017. Lo sfruttamento di vulnerabilità note invece è ancora in crescita (**+39,4%**), così come l’utilizzo di vulnerabilità “0-day”, (**+66,7%**). Ritornano a crescere gli attacchi basati su tecniche di “Account Cracking” (**+7,7%**).

Tipologie di malware utilizzate



Dal grafico si possono osservare alcuni fenomeni interessanti, tra questi che il malware per le principali piattaforme mobile rappresenta ormai quasi il **12%** del totale, che i Ransomware rappresentano quasi un quarto del malware totale (**23%**), e che i Cryptominers, quasi inesistenti in passato, nel corso del 2018 sono arrivati a rappresentare il **14%** del totale (erano il 7% nel 2017).

Valutazione degli impatti per tipo di attaccante - 2018



Non sorprende che il maggior numero di attacchi classificati come “Critici” riguardino le categorie Espionage ed Information Warfare, mentre la prevalenza di attacchi con impatto di tipo “Medio” e “Alto” riferiti ad attività cybercriminali si spiega con la necessità, per questi soggetti, di rimanere relativamente sottotraccia, guadagnando sui grandi numeri più che sul singolo attacco (tranne casi particolari).

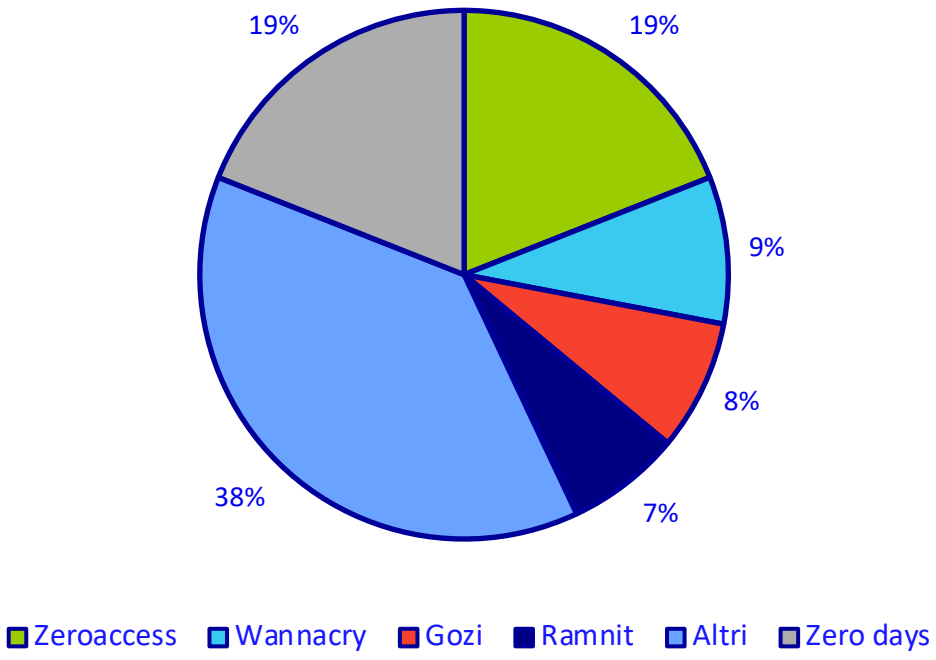
Interessante anche notare come l’Hacktivism, pur in grande diminuzione, presenti un’ampia percentuale di attacchi con impatto di tipo “Alto” ed abbia un valore medio della Severity peggiore rispetto alla categoria Cybercrime (pur essendo numericamente molto meno rappresentato nel campione).

Marco Raimondi

Fastweb

I dati Fastweb relativi al panorama Italiano

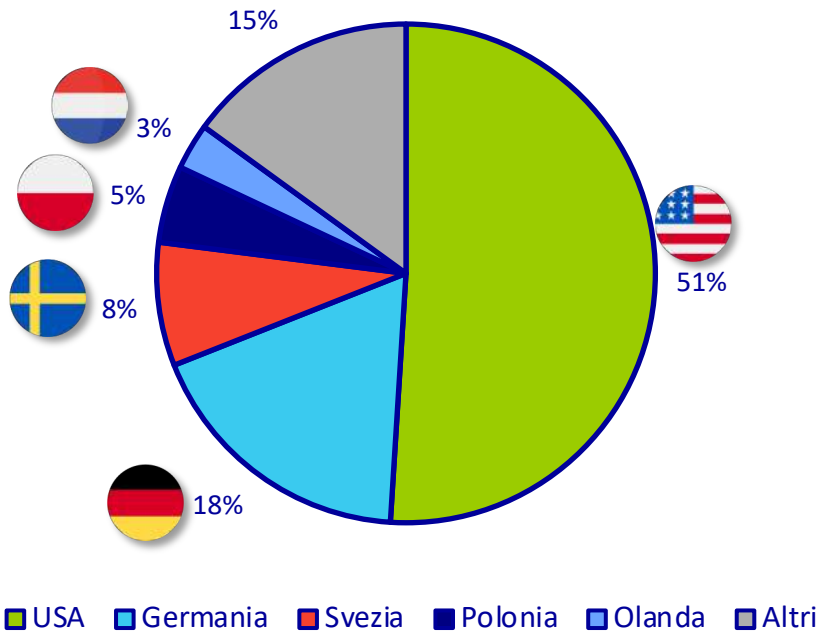
Distribuzione Malware e Botnet 2018



- **212 famiglie** di malware rilevate (+10% vs 2017)
- Il **15% dei malware** totali sono di tipo **finanziario** (Gozi + Ramnit)
- **19% di Zero Days** (+11% vs 2017)

Centri di comando e controllo

I centri di **Command and Control** (C&C) rappresentano i sistemi compromessi utilizzati per l'invio dei comandi alle macchine infette da malware (bot) utilizzate per la costruzione delle botnet.



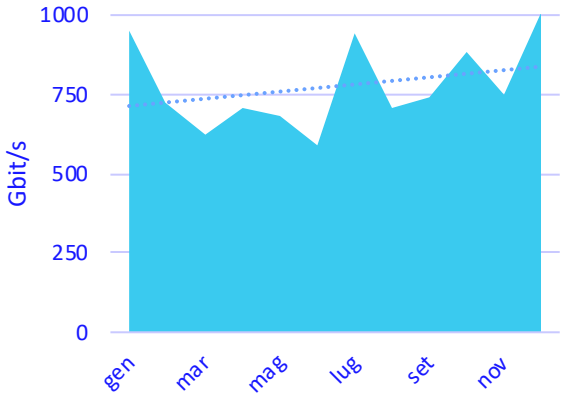
- Gli **Stati Uniti** continuano ad avere una **percentuale rilevante di C&C** anche se in calo rispetto al 2017
- **Crescono** i centri di comando e controllo in **Europa** (+20% vs 2017)
- Questi host spesso sono **«macchine ponte»** per eludere l'indirizzo IP originario (+11% vs 2017)

DDoS: un fenomeno ancora in forte crescita

Banda di un attacco

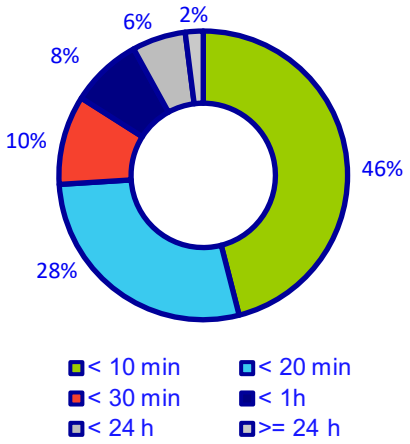
Nell'ultimo anno l'impatto degli attacchi è raddoppiato

Banda complessiva attacchi DDoS



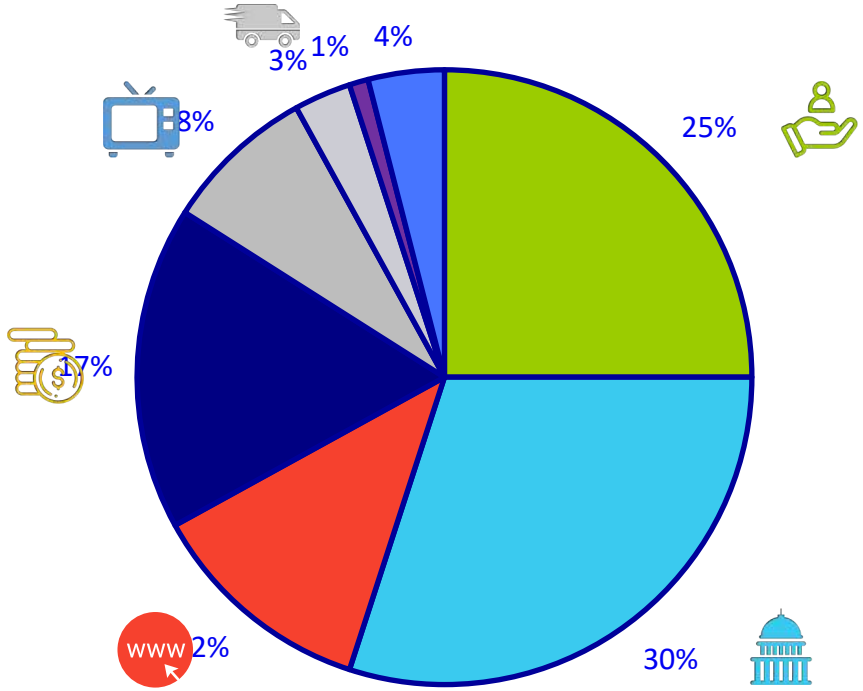
Nel 2018 riscontrate 9300 «anomalie» (+32% vs 2017)

Durata



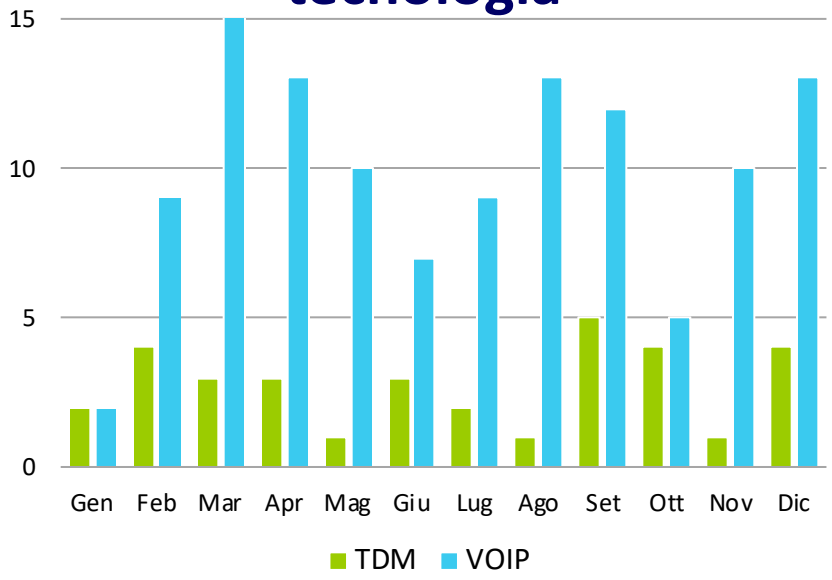
Gli attacchi DDoS nel 92% dei casi durano meno di 1h

DDoS: Attacchi per settori merceologici coinvolti

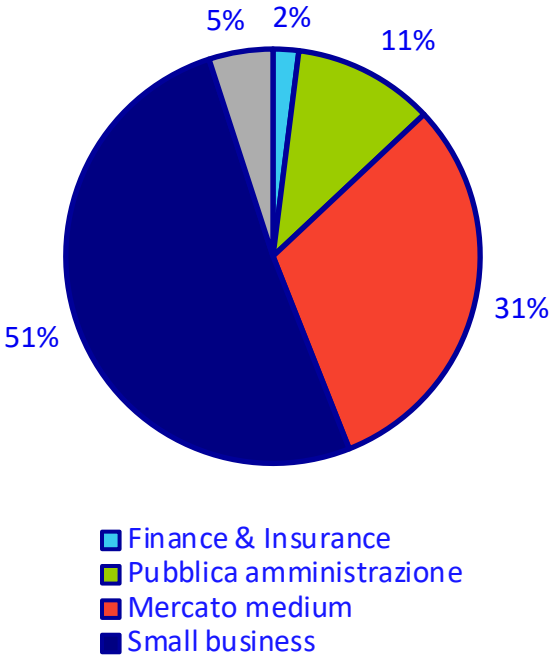


Attacchi ai protocolli VoIP

Attacchi mensili per tecnologia



Settori merceologici/mercati colpiti



Rodolfo D'Agostino

Akamai

Attacchi DDoS e Applicativi

TREND DEL 2018

16.000+ attacchi sulla nostra rete

Numero di attacchi:
+16% YoY (DDoS)
+28% YoY (Attacchi Applicativi)

Dimensione degli attacchi DDoS:
+9% ogni 3 mesi
+200% ogni 2 anni

2016-18: Mirai e varianti
2018: Memcached

MEMCACHED

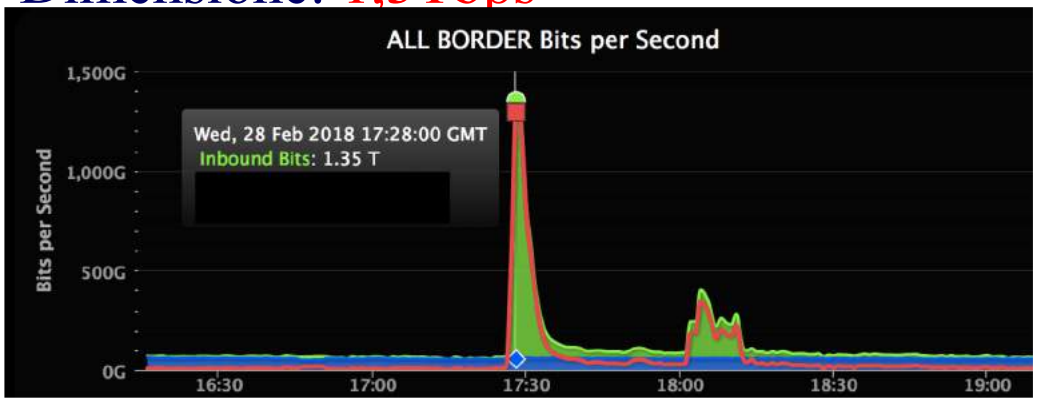
Attacco di riflessione UDP

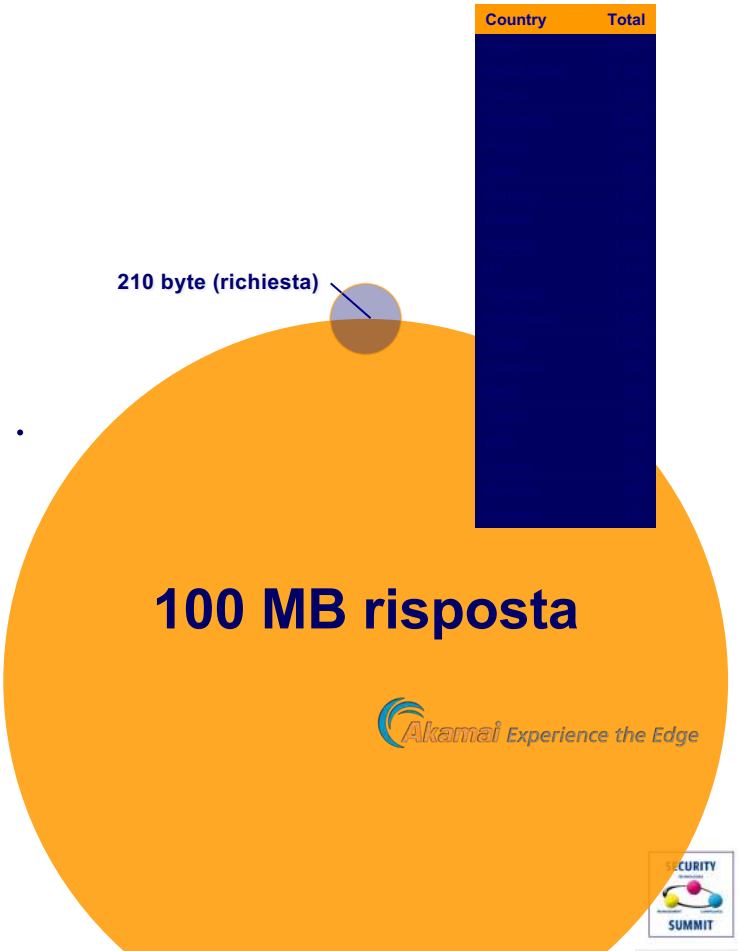
Fattore di amplificazione: 500.000x

Obiettivo: Sito per sviluppo software

Data: Marzo 2018

Dimensione: 1,3Tbps





Attacco ai punti deboli della catena

CREDENTIAL ABUSE

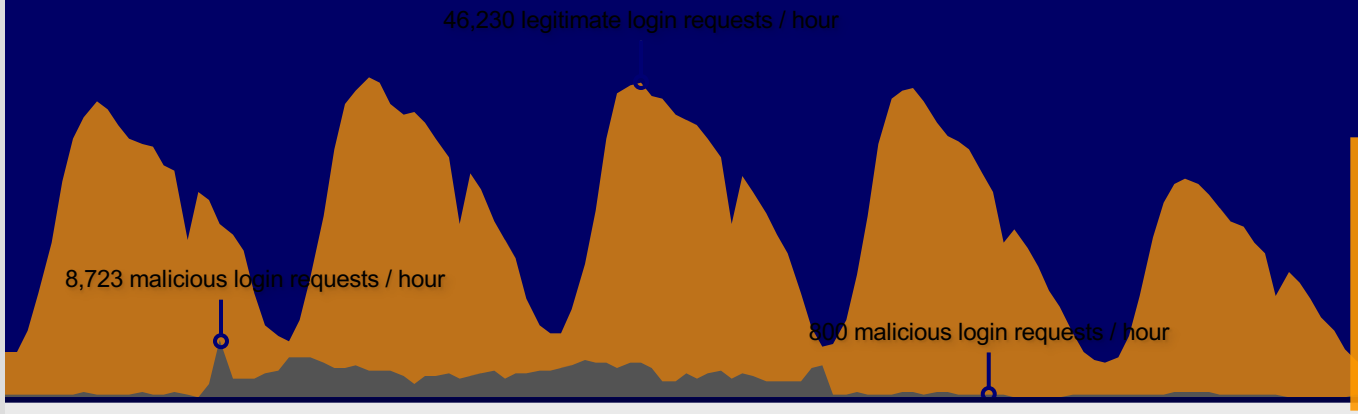
Obiettivo: password e persone.

L'attaccante utilizza combinazioni di login e password (dump) su più siti alla ricerca di match.

Dimensioni (picco):

- Quasi 28 miliardi di accessi tra Maggio e Dicembre 2018
- 300.000 accessi per ora

TOP CREDIT UNION



Botnet #1

- Requests – 94,296 (average 9/min)
- Clients – 2 IPs, same UA

Botnet #2

- Requests – 190,487 (average 59/min)
- Clients – 10k+ IPs, 695 UAs

Botnet #3

Average 0.00035 requests/min per IP

- Requests – 5,286 (average 0.5/min)
- Clients – 1500 IPs, 188 UAs

Legitimate and malicious requests to a login endpoint for a top NA credit union

Human logins
4,251,661

Malicious logins
315,178

IP addresses
19,992

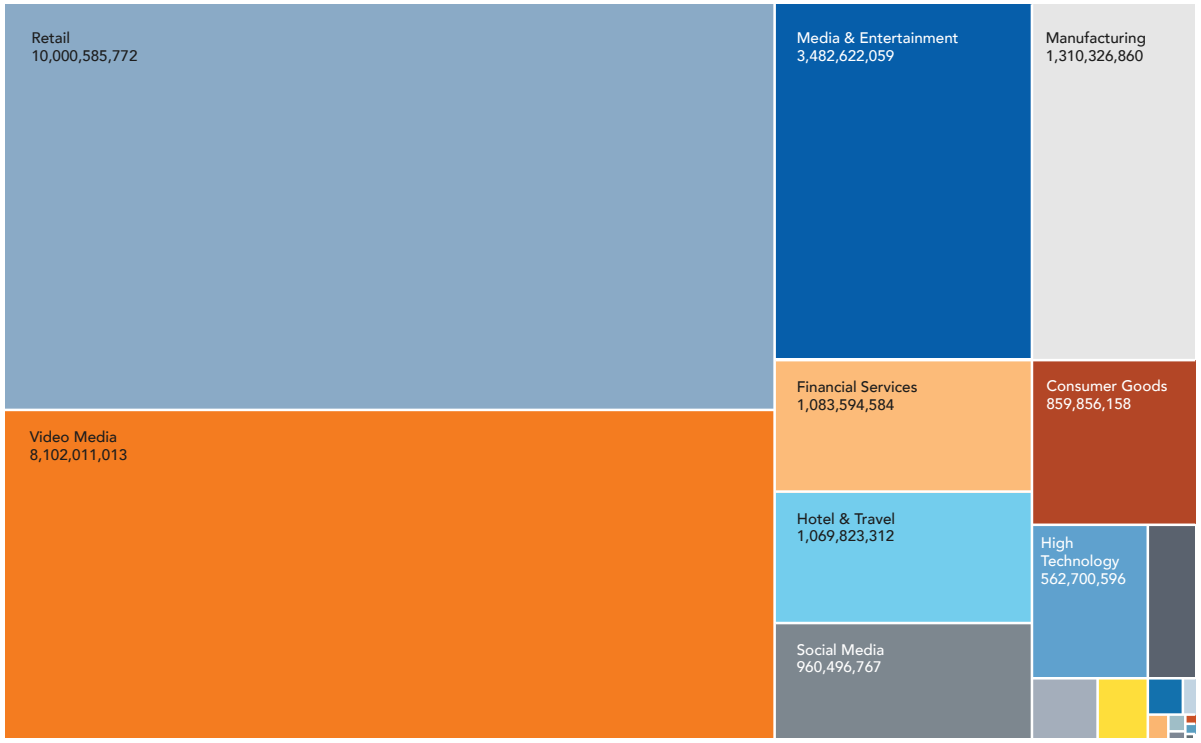
ASNs
1743

User agents
4,382

Akamai Experience the Edge

CREDENTIAL ABUSE

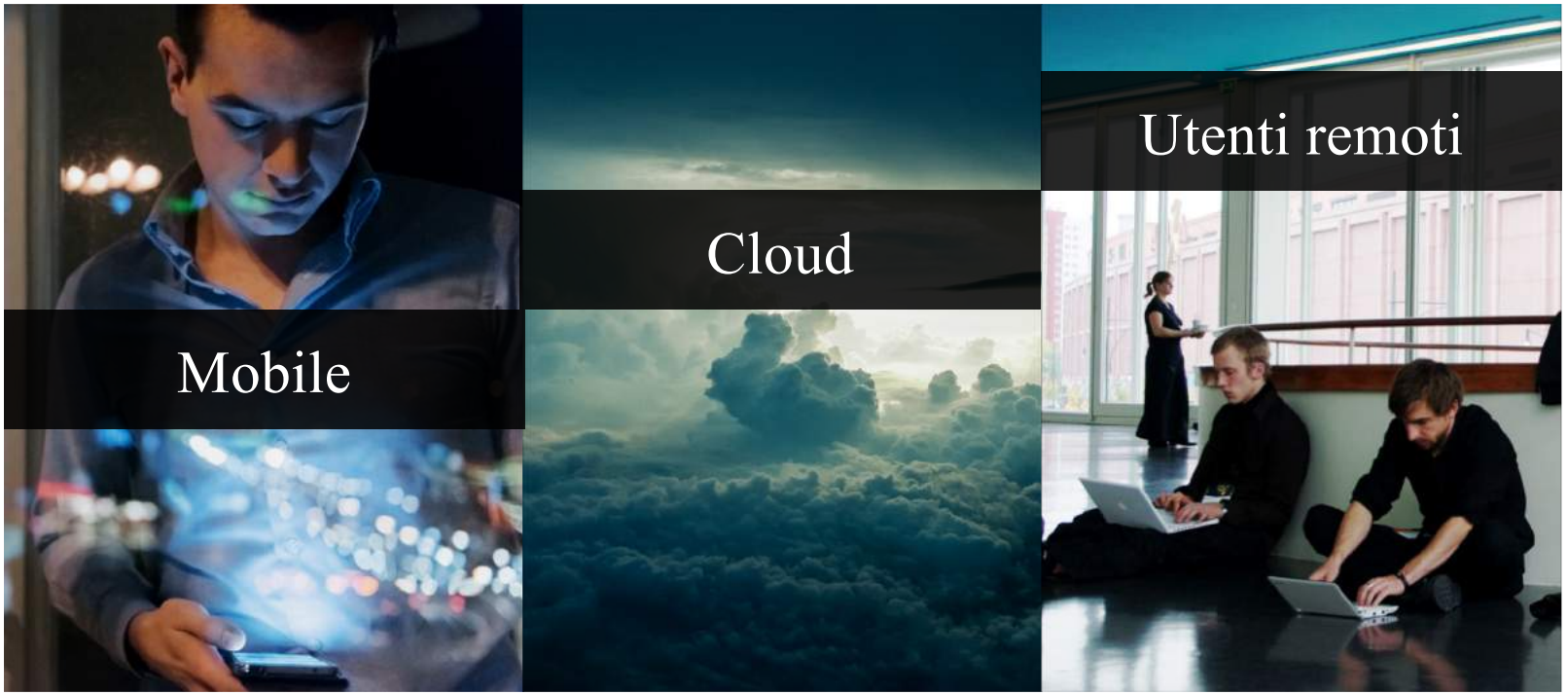
Distribuzione per verticali



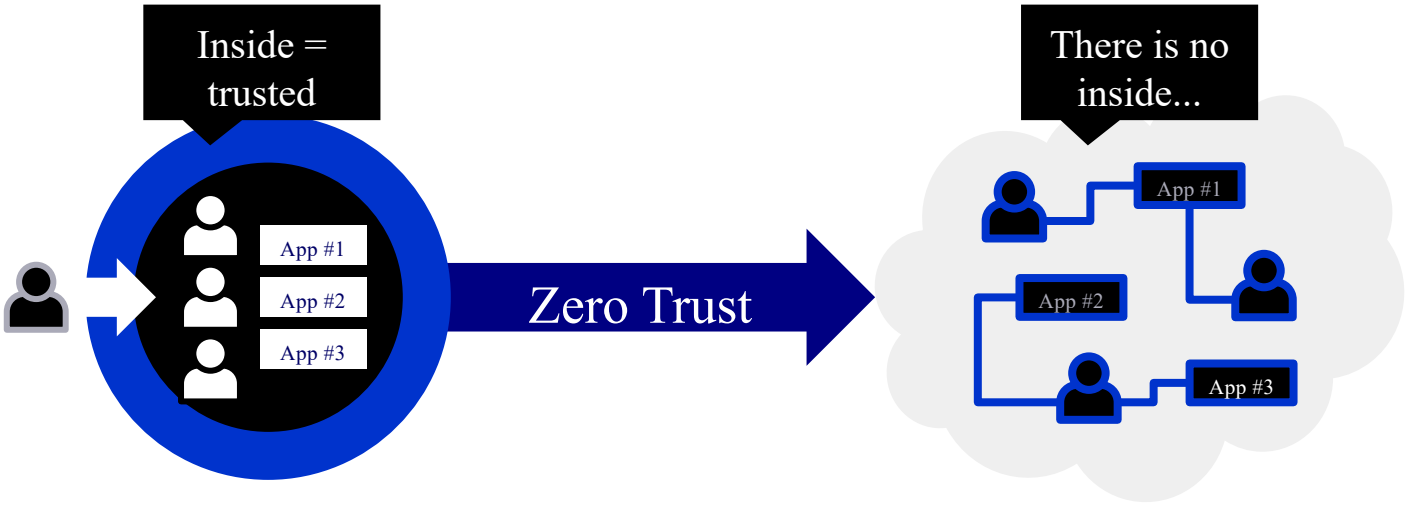
CREDENTIAL ABUSE

Primi 5 paesi sorgenti di attacco

IL MONDO OGGI…



…RICHIEDE UN CAMBIO DI PARADIGMA



Utenti e app interni
Fidati ma verifica
Full network access

Utenti e app ovunque
Verifica e non fidarti
Accesso per applicazioni

Alessio Pennasilico

Clusit

Un commento su Speciali, Novità e Focus On

Siamo in un pericoloso contesto di onde sovrapposte:

- Gli attacchi alle cassaforti non sono finiti (capitolo finance)
- Il GDPR ha raggiunto la «terza fase» ma non ha terminato ancora le prime due (capitolo GDPR)
- Si palesano le sfide di sicurezza e compliance delle nuove tecnologie (capitoli tecnologie emergenti) ripetendo tutti gli errori delle tecnologie precedenti
- Serve ancora tanta awareness e altre cose (focus on)

Speciale GDPR

- Era necessario parlare ancora di GDPR a soli 9 mesi dall'entrata in vigore del nuovo regolamento europeo. Lo facciamo così:

- Ripetiamo e aggiorniamo la **Survey** realizzata dagli Osservatori del Politecnico di Milano sull'impatto del GDPR sulle aziende italiane
- Con il contributo **2019: data protection 4.0** evidenziamo il bisogno di imparare a gestire l'innovazione
- Con **La terza fase del GDPR** descriviamo quali tipi di progetti devono ancora partire
- Con **Cifratura dei dati personali** collochiamo nel giusto contesto la misura tecnologica più discussa

Tecnologie emergenti

Intelligenza artificiale

Blockchain

- Molta attenzione
- Primi prodotti / servizi «da scaffale» presenti sul mercato
- Nuovi rischi da gestire

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

Un’analisi realizzata appositamente per il Rapporto Clusit
alla fine del 2018 da **IDC Italia**

Rapporto Clusit 2019 sulla sicurezza ICT in Italia

Moderano: Gabriele Faggioli e Alessio Pennasilico

Partecipano alla Tavola Rotonda:

- Angelo Bosis, Oracle Italia
- Gianluca Busco Arrè, Panda Security Italia
- Gastone Nencini, Trend Micro Italia
- Domenico Raguseo, IBM Italia
- Federico Santi, DXC Technology

Clusit

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

Per maggiori informazioni:

rapporti@clusit.it

info@astrea.pro

Clusit
Associazione Italiana
per la Sicurezza Informatica

SECURITY
TECHNOLOGIES
MANAGEMENT COMPLIANCE
SUMMIT