Presentazione del Rapporto Clusit 2020

Gabriele Faggioli, Presidente Clusit

Luca Bechelli, Comitato Scientifico Clusit

10 novembre 2020 orario 09.00-11.00 - StreamingEdition

#securitysummit #streamingedition

Streaming Edition 2020

Presentazione del Rapporto Clusit 2020

Andrea Zapparoli Manzoni, Consiglio Direttivo, Clusit

Marco Raimondi, Product Marketing Manager, Fastweb

Domenico Raguseo, Responsabile Unit della CyberSecurity, Exprivia

#securitysummit #streamingedition

Streaming Edition 2020

Presentazione del Rapporto Clusit 2020

Carlo Mauceli, National Digital Officer, Microsoft

Maurizio Taglioretti, Country Manager Sud Europa, Netwrix

Gastone Nencini, Country Manager, Trend Micro Italia

Mauro Cornelli, Security Solution Specialist, Oracle

Ivan De Tomasi, Country Manager Italia, Watchguard

#securitysummit #streamingedition

Agenda 10 Novembre 2020

- Analisi e proposte CLUSIT per il rafforzamento della cyber security in Italia - Sintesi dell'Audizione innanzi alla Commissione Difesa del Senato del 20 Ottobre 2020, Gabriele Faggioli, Presidente Clusit
- I contenuti del Rapporto Clusit 2020 – aggiornamento di Ottobre 2020, Luca Bechelli, CTS Clusit
- Panoramica dei cyber attacchi più significativi del 1° Semestre 2020, Andrea Zapparoli Manzoni, CD Clusit
- Il 1° Semestre dai dati del SOC di Fastweb, Marco Raimondi, Fastweb
- Stato della Cyber Security nel sud Italia – aggiornamento I semestre 2020, Domenico Raguseo, Exprivia

Tavola rotonda moderata da Luca Bechelli, con la partecipazione di

- Mauro Cornelli, Oracle
- Carlo Mauceli, Microsoft
- Ivan De Tomasi, WatchGuard Technologies
- Gastone Nencini, Trend Micro
- Maurizio Taglioretti, Netwrix

Gabriele Faggioli

«PROFILI DELLA SICUREZZA CIBERNETICA ATTINENTI ALLA DIFESA NAZIONALE»

AUDIZIONI INFORMALI SVOLTE PRESSO LA COMMISSIONE DIFESA
SENATO DELLA REPUBBLICA, MARTEDÌ 20 OTTOBRE 2020

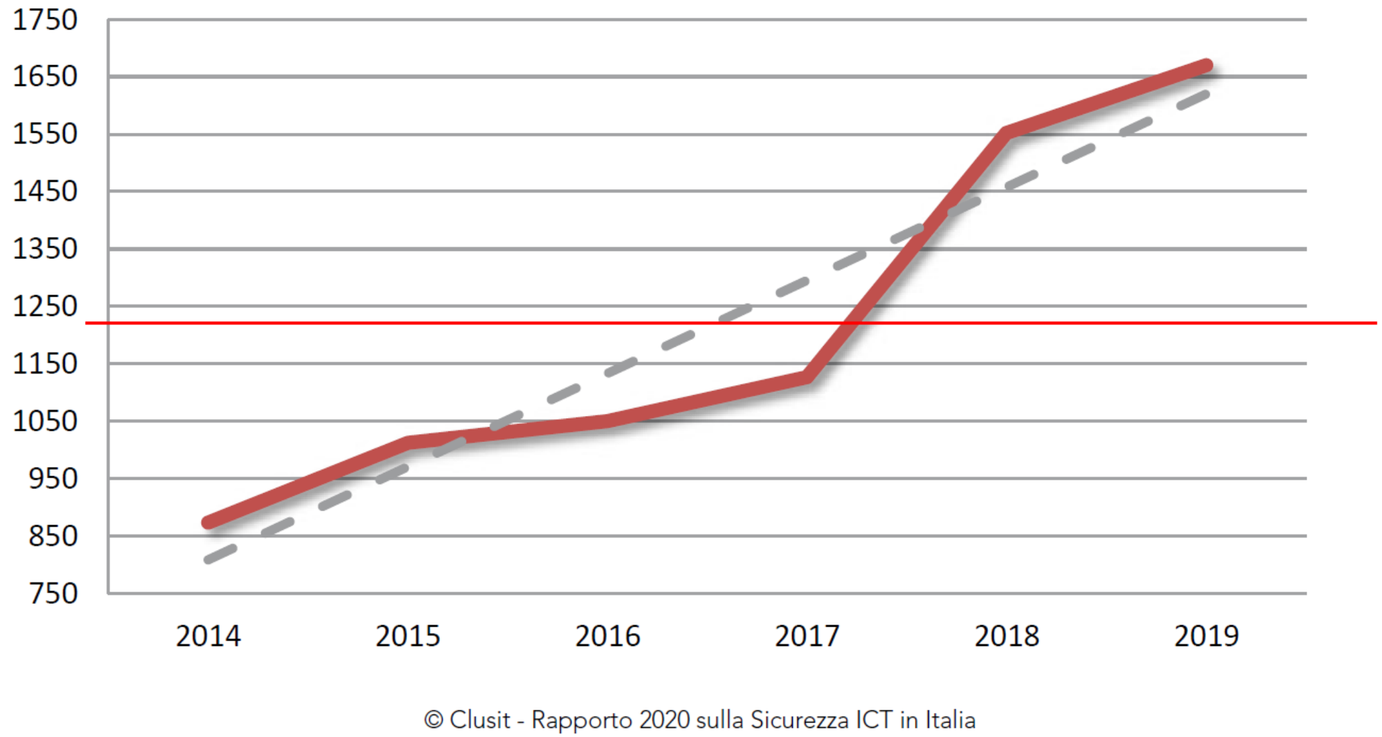
REGISTRAZIONE COMPLETA
HTTP://WEBTV.SENATO.IT/4621?VIDEO_EVENTO=122101

Analisi e proposte CLUSIT per il rafforzamento della cyber security in Italia

Sintesi dell'Audizione innanzi alla Commissione Difesa del Senato
20 Ottobre 2020

#securitysummit #streamingedition

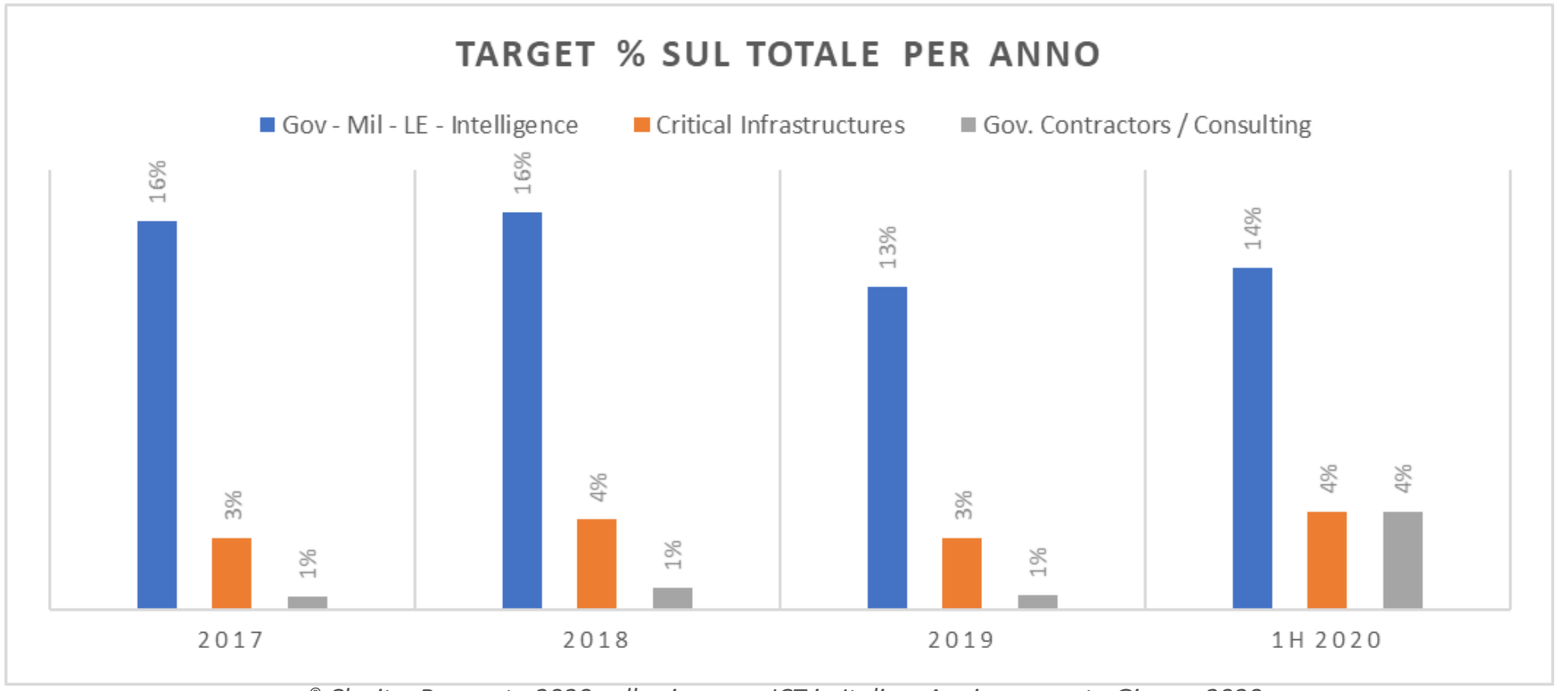
Aumenta la pressione degli attacchi informatici su imprese e Pubbliche Amministrazioni



Rapporto Clusit:

- **+37% di attacchi** rispetto alla media degli ultimi 6 anni
- Dal 2014 al 2019: **+91% attacchi gravi**
- Nel triennio 17-19 il numero degli attacchi gravi cresce di circa +50% rispetto al precedente

L’impatto sugli Enti Governativi e la loro filiera



® Clusit – Rapporto 2020 sulla sicurezza ICT in Italia – Aggiornamento Giugno 2020

- *In tre anni e mezzo si contano 951 attacchi gravi diretti ad Enti Governativi, Infrastrutture Critiche e Gov. Contractors con severity Critica ed Alta (**22%** del totale degli attacchi rilevati nei primi 6 mesi del 2020)*

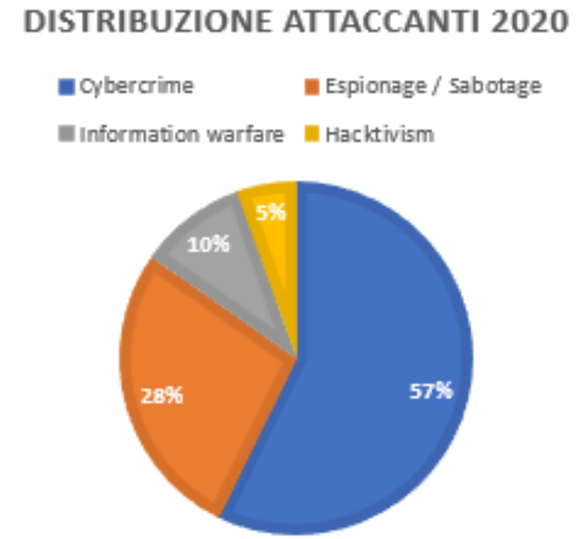
- *Sono molto aumentati gli attacchi verso i **Contractors** nei primi sei mesi del 2020*

Attacchi informatici verso gli Enti Governativi e la loro filiera: non solo information warfare

- Evoluzione degli attacchi dovuti a **Cybercrime** verso **Enti Governativi, Gov. Contractors ed Infrastrutture Critiche**: dal 35% nel 2017 a un 57% nei primi 6 mesi del 2020, in leggera crescita rispetto ai 2 anni precedenti.

- La quota di **Espionage** rimane sostanzialmente costante in tutto il periodo in esame, così come quella di Information Warfare.

- In discesa invece gli attacchi dovuti ad **Hacktivism**, passati dal 12% nel 2017 al 5% nel primo semestre 2020.



® Clusit – Rapporto 2020 sulla sicurezza ICT in Italia

Un ecosistema interconnesso

Il settore militare e quello civile sono caratterizzati da

interessi ed esigenze nazionali convergenti

Non è pensabile perseguire una **resilienza strutturale agli attacchi cyber** senza che l'intero ecosistema Nazionale operi **sinergicamente sia sulla strategia che nelle azioni tattiche**

Le sinergie devono riguardare – tra le altre - l'attuale disponibilità sul mercato e l'uso da parte dei diversi stakeholder di **tecnologie** (di fatto) **dual use**

Le aree di intervento proposte

1. Ricerca e Innovazione di mercato

2. Ecosistema delle imprese e della pubblica amministrazione

3. Consapevolezza dei cittadini

1. Ricerca e Innovazione di mercato

La distribuzione geografica delle startup cybersecurity

254 START UP

254 Startup italiane e internazionali **fondate a partire dal 2015** e **finanziate a partire dal 2018**

Nord America

57,1%

Asia

19,7%

Europa

20,5%

Italia

2%

Altri continenti

2,7%

Osservatorio Cyber Security & Data Protection del Politecnico di Milano

I finanziamenti ricevuti dalle startup cybersecurity

221 **START UP**

3,83 miliardi di $ dal 2018 a oggi
15 milioni di $ a startup
Italia: media 1 mln $ ma una sola ha avuto 2,2 mln $

Nord America

2,4 mld di $

Asia

1 mld di $

Europa

423 mln di $

Italia

5 mln di $

Altri continenti

10 mln di $

Osservatorio Cyber Security & Data Protection del Politecnico di Milano

Quali interventi per favorire l'innovazione?

- Aumentare **investimenti e facilitazioni** per la ricerca e le startup, motore attuale e prospettico della crescita non solo tecnologica, ma anche economica del sistema paese

- Semplificare **l'accesso alla collaborazione pubblico / privato** per la ricerca e le startup

- Per colmare lo skill shortage tipico di questo settore è necessario un programma formativo Nazionale a lungo termine teso a sviluppare e mantenere le competenze e le esperienze necessarie

2. Ecosistema delle imprese e della Pubblica Amministrazione

Dal perimetro nazionale alla filiera

- La definizione del **Perimetro Cibernetico Nazionale** ha dato una svolta innovativa al tema della cyber security che, per essere applicato correttamente, richiede di **intervenire sull'intero ecosistema pubblico-privato**

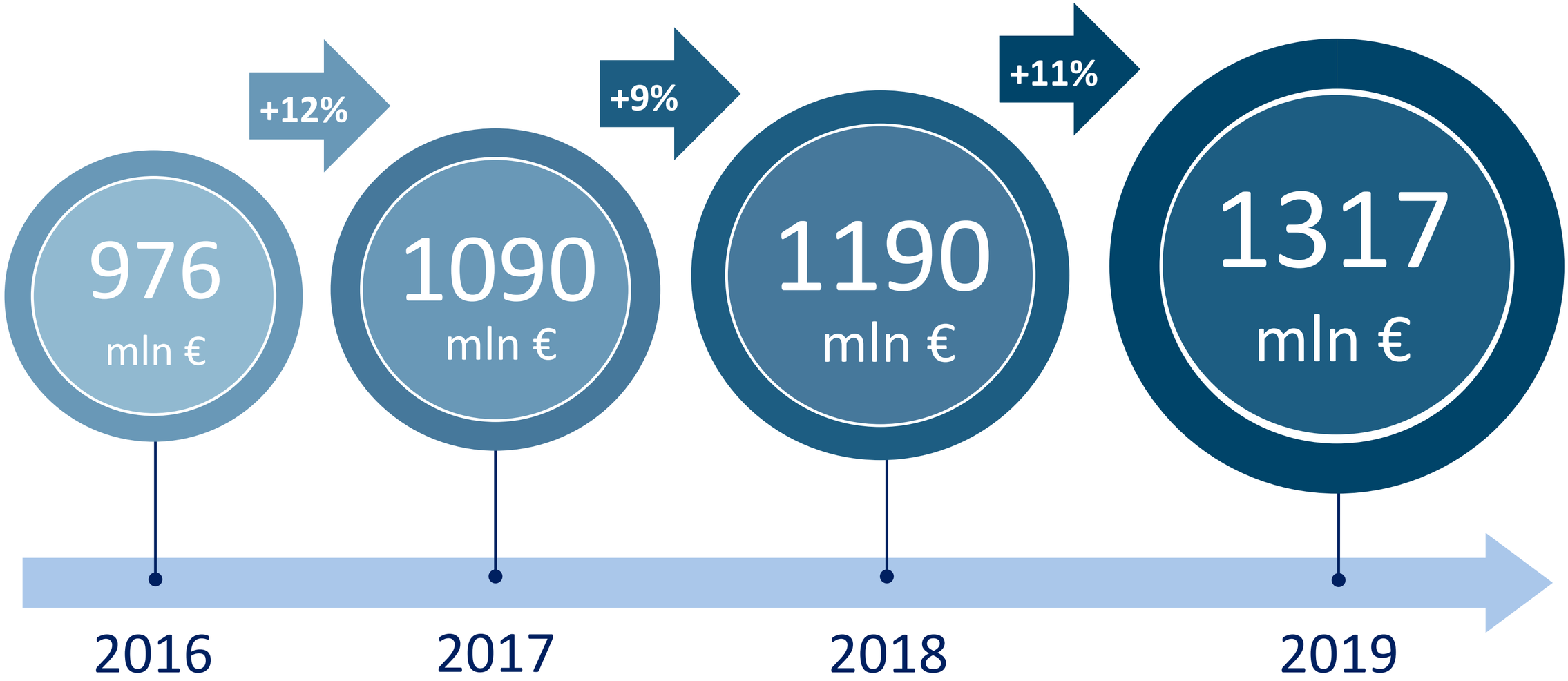
- Prioritaria in tal senso, nonché fondamentale per la tutela dell'intero tessuto socio-economico del Paese, è il **rafforzamento della filiera**, in particolare (ma non solo) con **misure a supporto delle PMI**

Le priorità degli investimenti delle imprese italiane
Cresce la percezione dell'importanza della cyber security

2017	2018	2019	2020
1° Consolidamento applicativo	1° Big Data & Business Intelligence	1° Digitalizzazione e dematerializzazione	1° Big Data & Business Intelligence
2° Big Data & Business Intelligence	2° Digitalizzazione e dematerializzazione	2° Big Data & Business Intelligence	**2° Information Security, Compliance e Risk Mgmt**
3° Digitalizzazione e dematerializzazione	3° Consolidamento applicativo	3° Sviluppo e rinnovo ERP	3° Sviluppo e rinnovo ERP
4° Sviluppo e rinnovo CRM	**4° Information Security, Compliance e Risk Mgmt**	4° Sviluppo e rinnovo CRM	4° Sviluppo e rinnovo CRM
...	5° Industry 4.0	5° eCommerce	5° Data Center, Information Mgmt, virtualizzazione
10° Information Security, Compliance e Risk Mgmt	6° Sviluppo e rinnovo CRM	**6° Information Security, Compliance e Risk Mgmt**	6° Mobile Business

Survey dell'Osservatorio Digital Transformation Academy che ha visto il coinvolgimento di oltre 200 Innovation Manager e CIO di grandi imprese nel 2016, 2017, 2018 e 2019

Gli investimenti riflettono le preoccupazioni delle imprese…



2020: *dato di crescita pressoché invariato (+1-2% - dati preliminari) per effetto della pandemia COVID-19*

…con ampi margini di crescita

Rapporto tra mercato information security e PIL italiano

2017	2018	2019
0,06%	0,06%	0,07%

Rapporto tra mercato information security e mercato digitale italiano*

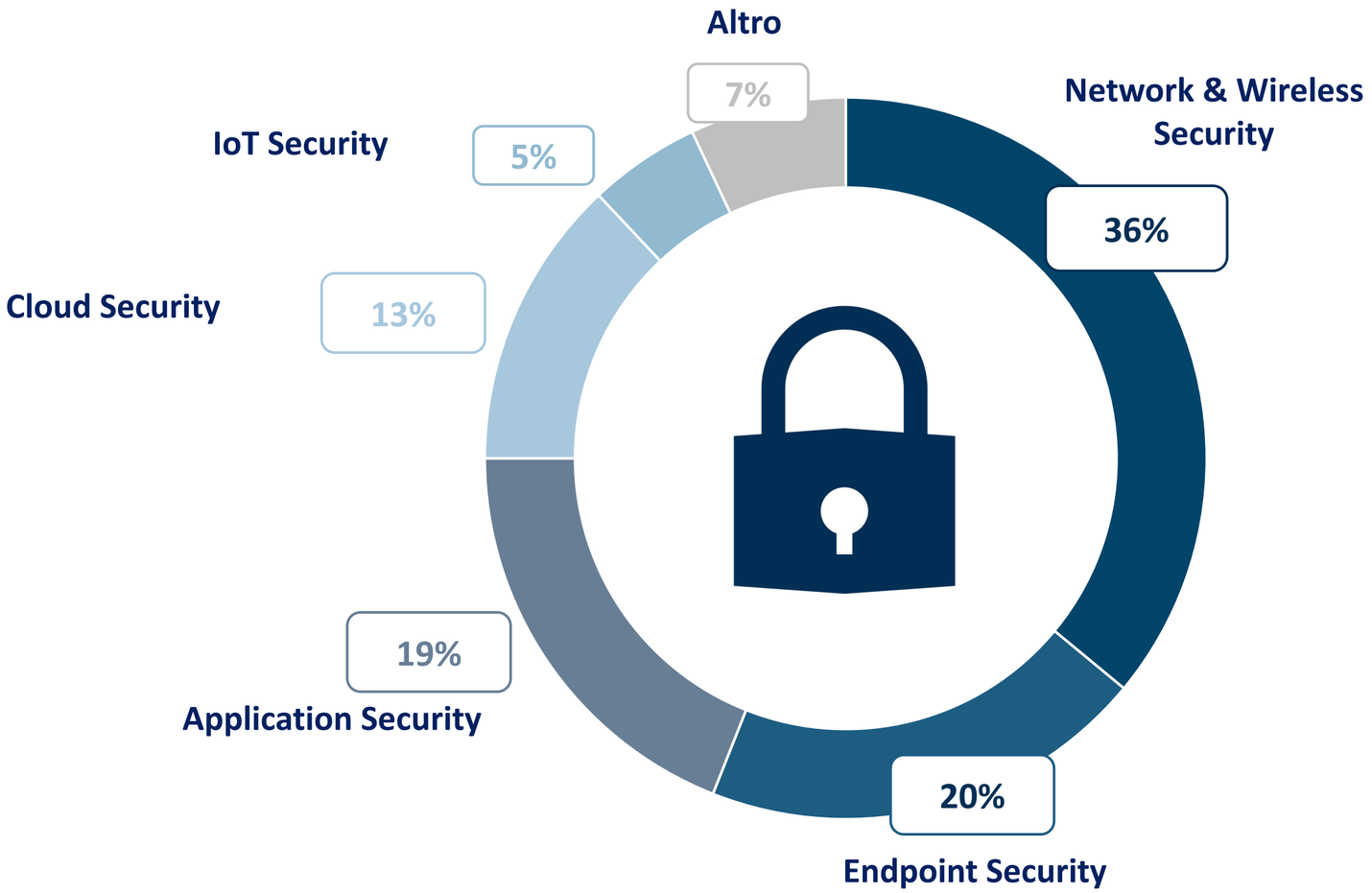
2017	2018	2019
2,8%	2,9%	3,1%

Rapporto tra mercato information security e PIL 2019 (stima): confronto internazionale su 7 Paesi

1. Regno Unito – 0,32%
2. Germania – 0,29%
3. Stati Uniti – 0,23%
4. Francia – 0,20%
5. Giappone – 0,20%
6. Spagna – 0,11%
7. Italia – 0,07%

**Fonte: Assinform; si fa riferimento alla componente business*

La scomposizione del mercato per tipologia di sicurezza (2019)



- A catalizzare le quote maggiori del mercato sono ancora le componenti di sicurezza più tradizionali: ***Network & Wireless Security*** ed ***Endpoint Security***

- Per contro, tra le componenti su cui le aziende dichiarano di voler aumentare i propri investimenti di sicurezza figurano poco le aree più **innovative** legate ai trend del digitale: ***Cloud Security*** e ***IoT Security***

Campione: 180 grandi imprese

Approfittiamo delle opportunità del «new normal»

- Sarebbe necessario avviare e sostenere iniziative di cyber security con **investimenti adeguati ed a lungo termine**, al fine di portare il mercato Italiano ai livelli di degli altri stati dell'Unione in cima alla classifica

  - Per iniziare si potrebbe pensare ad un uso tattico dei fondi stanziati per la gestione dell'emergenza: **il "new normal" è digitale e dovrà prevedere una importante componente di cyber security**, necessaria per la sopravvivenza dell'ecosistema socio-economico

  - Come già fatto per #Industry4.0, **si potrebbe ideare un Piano Nazionale #CyberSecurity4.0** premiando la componente cyber security in tutti i progetti innovativi / di consolidamento, con voci specifiche e misure specifiche

Proteggere se stessi per proteggere l'ecosistema 1/2

Per rafforzare la filiera, sono auspicabili provvedimenti finalizzati a:

- **Supportare la trasformazione organizzativa delle imprese sui mercati di riferimento**, ad esempio prevedendo l'obbligo di dotarsi della figura di *Chief Information Security Officer* (CISO) e, per determinati contesti, di certificazioni «accountable» (es. ISO 27001);

- **Favorire la transizione al cloud**, anche in virtù del "new normal", con modalità che tengano conto di esigenze di cyber security e data protection, anche grazie alle "certificazioni di security", agendo sia sul mondo della domanda che dell'offerta;

- **Accelerare il processo di adozione da parte del mercato di prodotti IoT e tecnologie "cyber sicuri by default"**, sia per il cittadino che acquista a scaffale che per le Organizzazioni pubbliche e private, anche a fronte dei nuovi requisiti normativi (*es. Il Cybersecurity Act obbligherà anche i piccoli produttori a soddisfare requisiti minimi di sicurezza*).

Proteggere se stessi per proteggere l’ecosistema 2/2

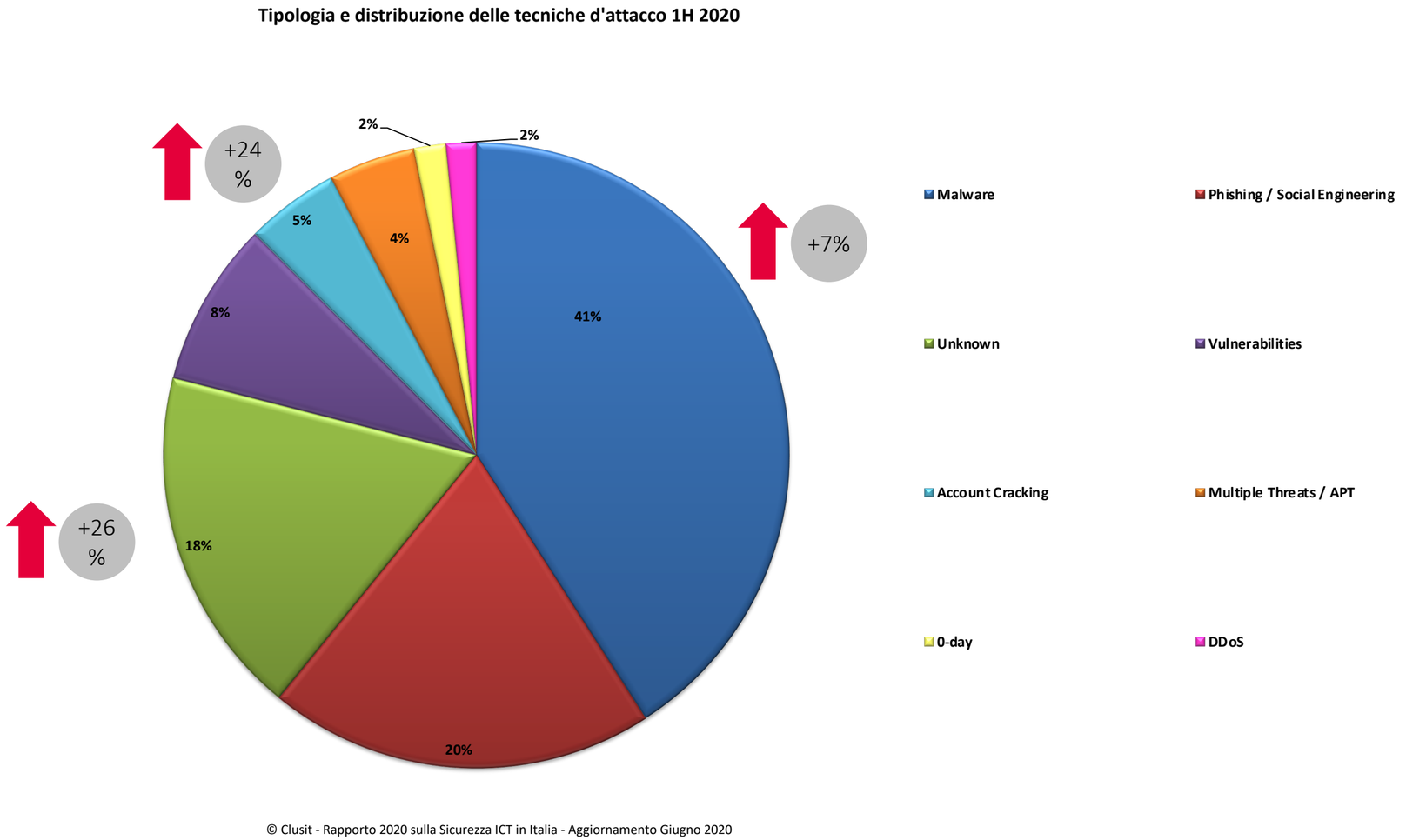
- **Favorire il Partenariato Pubblico Privato per:**
  - Stimolare l'innovazione, anche per le piccole imprese, **aggregandole anche sotto la guida di aziende più strutturate** mantenendo il controllo degli investimenti
  - Assicurare che una percentuale degli investimenti sia dedicata alle PMI, **senza che l'investimento si perda in rivoli di poca efficacia**

3. Consapevolezza dei cittadini

Malware e phishing sono ANCORA (!?!?) la principale minaccia!

Phishing, ransomware, vulnerabilità note, furti di password la fanno da padrone, con oltre l'80% del totale…

E sono attacchi noti dagli anni '90!



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2020

Il fattore umano è decisivo…e l'awareness non può essere lasciata alla discrezionalità di aziende e PA

Nel **55%** dei casi, **esiste un piano di formazione pluriennale, che coinvolge tutta l'organizzazione**, dal Top Management alle Business Line.

Nel **25%** del campione vi è un **piano di formazione indirizzato nello specifico a funzioni con maggiore sensibilità alle tematiche di information security e data protection**, quali IT, Risk Management e Compliance

Il **20%** delle aziende gestisce le **iniziative di formazione in modo spot**, senza un piano strutturato

Osservatorio Cyber Security & Data Protection del Politecnico di Milano

Campione: 698 organizzazioni italiane

Creare consapevolezza nel sistema Paese

- Promuovere un programma organico per creare una **cyber consapevolezza** di base in tutta la cittadinanza (*es. come già fatto per la* ***pubblicità progresso*** *sulla guida responsabile*)

- Favorire le iniziative di **awareness e innalzamento della preparazione** nelle PMI, ad esempio **organizzando percorsi formativi in collaborazione con le Università** su piani definiti dall'Autorità Nazionale, prevedendo **incentivi e sgravi fiscali per l'adozione di misure di sicurezza**

Andrea Zapparoli Manzoni

Membro del consiglio direttivo del Clusit

Managing Director di un centro di ricerca internazionale in materia di Cyber Defense.

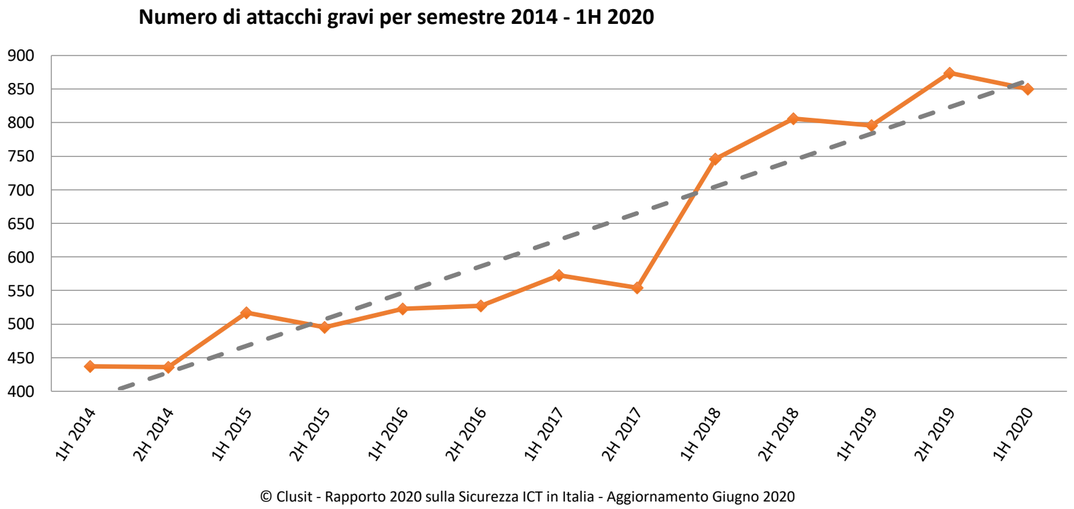
.

Quali sono i numeri del nostro campione?

Negli ultimi 9 anni e mezzo in media abbiamo analizzato e classificato 99 attacchi gravi al mese (129 nel 2018, 137 nel 2019 e 142 nel 1H20)

- **10.938** attacchi gravi analizzati dal gennaio 2011 al giugno 2020 (di cui **8.134** dal 2014).

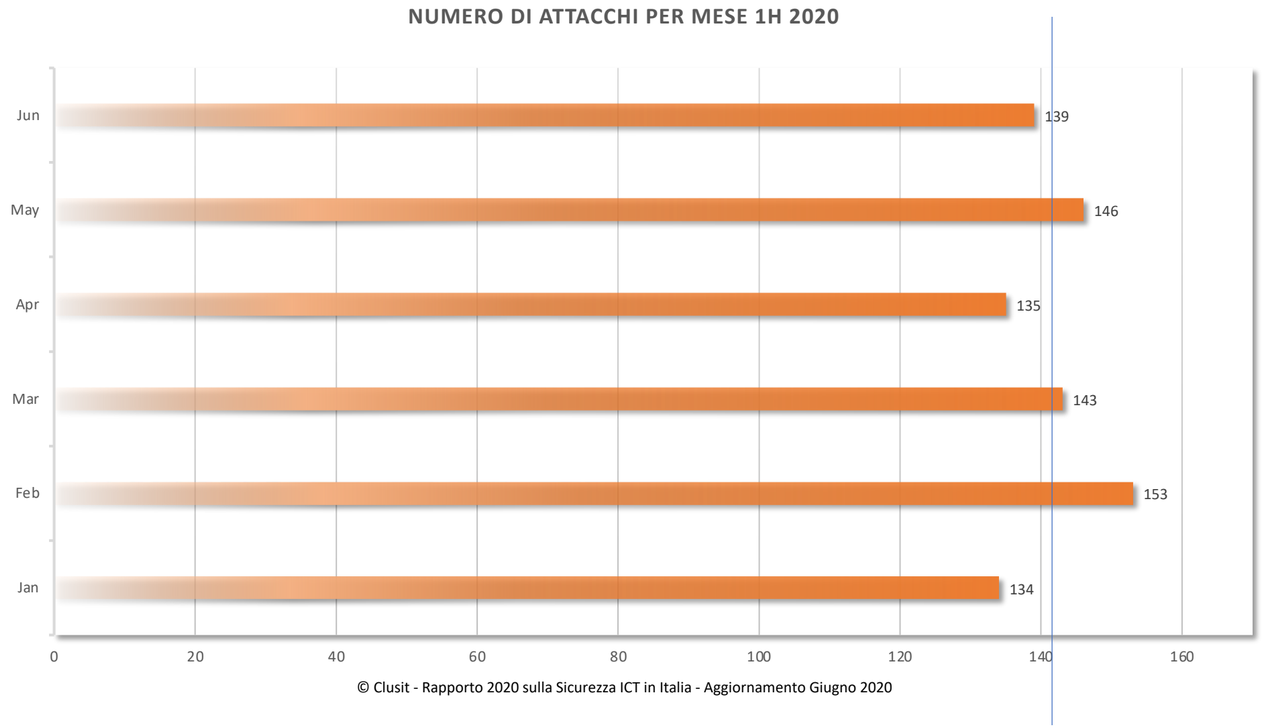
- 873 nel 2014
- 1.012 nel 2015 (+14%)
- 1.050 nel 2016 (+3,75%)
- 1.127 nel 2017 (+7,4%)
- 1.552 nel 2018 (+37,7%)
- **1.670 nel 2019 (+7,6%)**
- **850 nel primo semestre 2020**



Nel 2015 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%. Nel 2019, la crescita rispetto al 2018 è del 7,6%, rispetto al 2014 + 91,2%.

Nel triennio 2017-2019 il numero di attacchi gravi che abbiamo analizzato è cresciuto del +48%. Il numero di attacchi rilevati nel 2019 segna una differenza del +37,5% rispetto alla media degli attacchi per anno degli ultimi 6 anni (1.214)

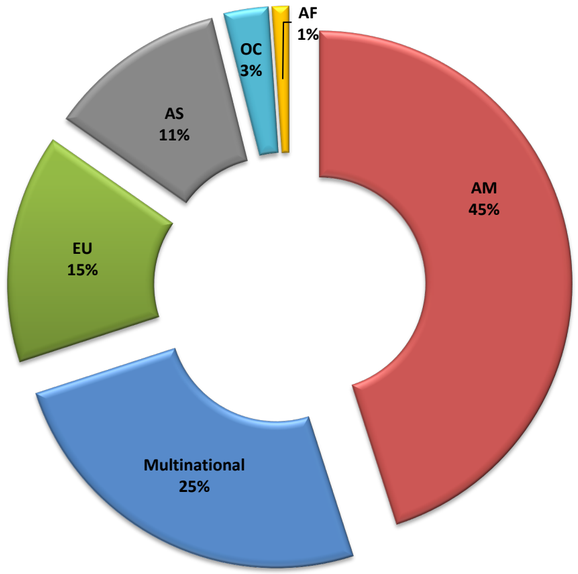
Attacchi rilevati e classificati per mese (1H 2020)



I picchi maggiori (sopra alla media del semestre, pari a 142) si sono avuti in Maggio, Marzo e Febbraio, in corrispondenza con la crisi Covid.

Distribuzione geografica delle vittime (1H 2020)

Appartenenza geografica delle vittime per continente 1H 2020

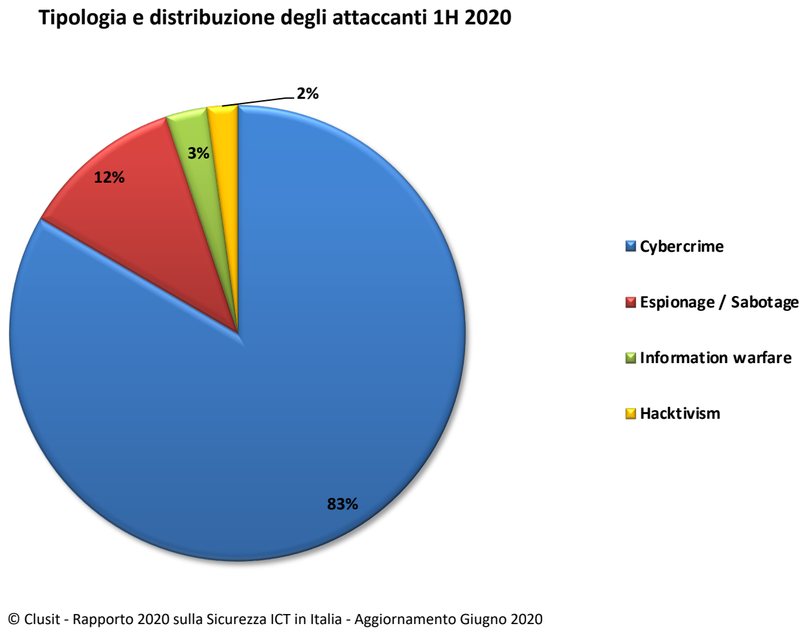


© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2020

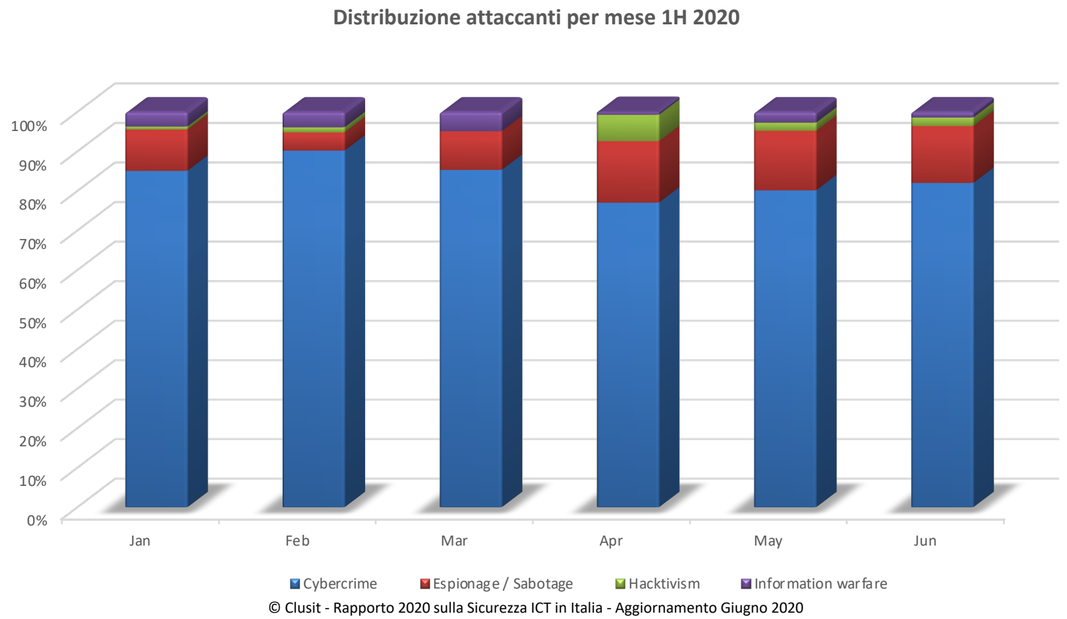
Nel 1H 2020 rimangono sostanzialmente invariate le vittime di area americana (dal 46% al **45%**), mentre gli attacchi verso realtà basate in Europa aumentano (dal 9% al **15%**) e rimangono percentualmente quasi invariati quelli rilevati contro organizzazioni asiatiche (dal 10% al **11%**).

Percentualmente diminuiscono anche gli attacchi gravi verso bersagli con sedi distribuite in diversi Paesi (categoria “Multinational”), che dal 31% del 1H 2019 passano al **25%** del 1H 2020.

Tipologia e distribuzione degli attaccanti (1H 2020)



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2020



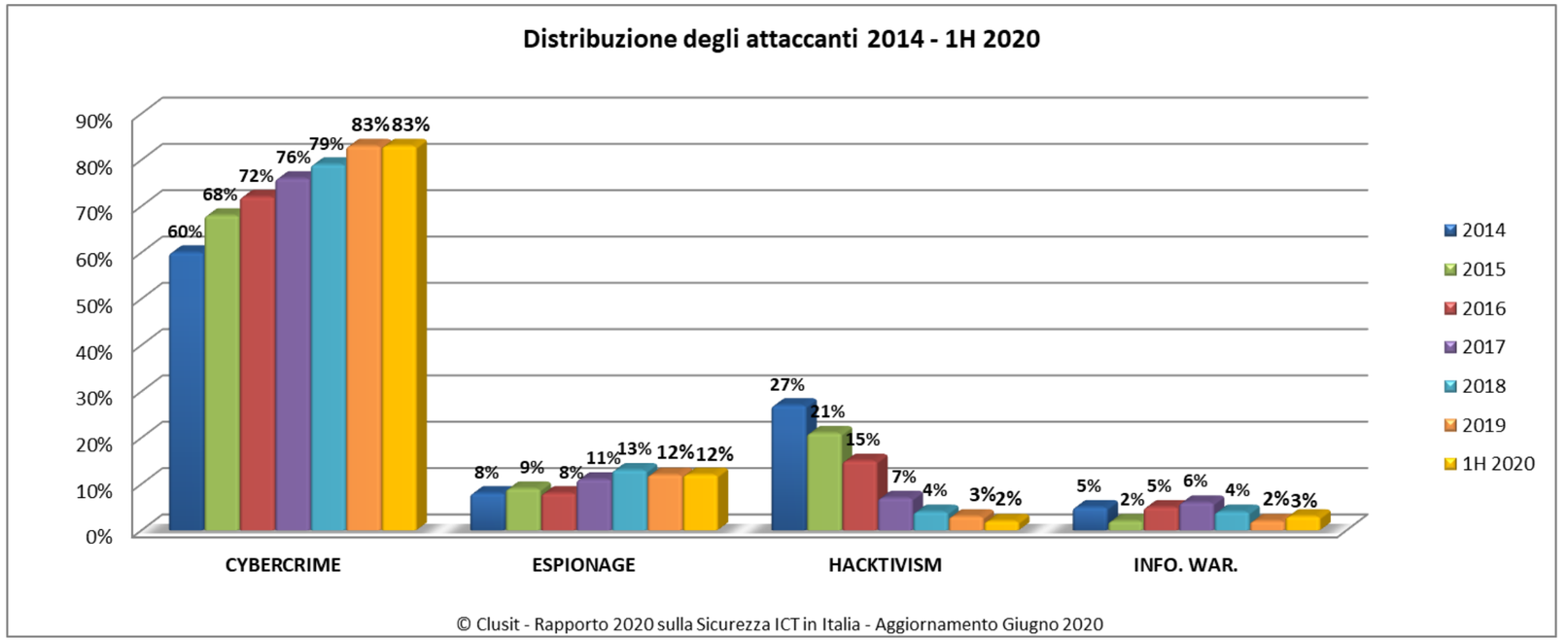
© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2020

In termini assoluti nel 2019 le categorie “Cybercrime”, “Cyber Espionage” e “Information Warfare” fanno registrare il numero di attacchi più elevato degli ultimi 9 anni, tendenza che si conferma anche nel primo semestre 2020.

Dal campione emerge chiaramente che, con l’esclusione delle attività riferibili ad attacchi della categoria “**Hacktivism**” che diminuisce ancora sensibilmente (**-30,8%** in termini percentuali) rispetto al primo semestre 2019, nel primo semestre 2020 sono in aumento sia gli attacchi gravi compiuti per finalità di “**Cybercrime**” (**+7,1%**), che quelli riferibili ad attività di “**Cyber Espionage**” (**+11,4%**) e “**Information Warfare**” (**+25%**).

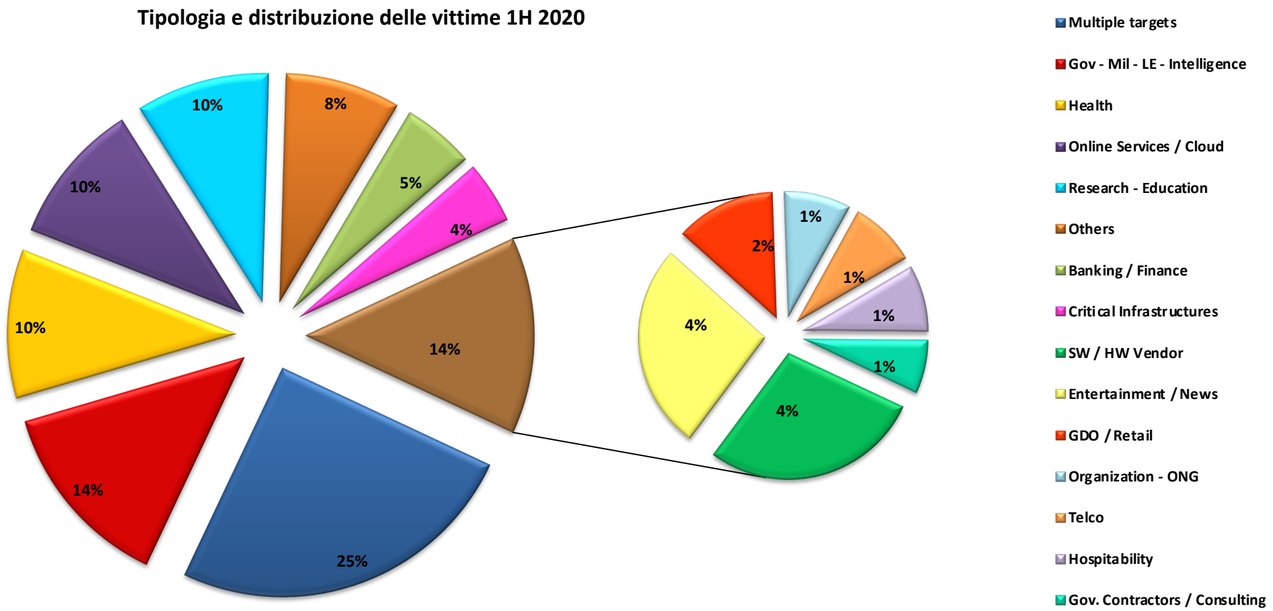
Va sottolineato che, rispetto al passato, oggi risulta più difficile distinguere nettamente tra “Cyber Espionage” e “Information Warfare”: sommando gli attacchi di entrambe le categorie, nel 1H 2020 tali attacchi rappresentano il **15%** del totale, contro il 13% del 1H 2019.

Tipologia e distribuzione degli attaccanti (2014 – 1H 2020)



Percentualmente, per la prima volta nel periodo 2014-2020 considerato, il Cybercrime nel 1H 2020 rimane stabile al 83% del totale, ricordando però che in numeri assoluti è cresciuto del **7.1%** (da 662 attacchi nel 1H 2019 a 709 nel 1H 2020). L'**Hacktivism** diminuisce ulteriormente, passando da quasi un terzo dei casi analizzati nel 2014 al **2%** del primo semestre 2020. Per quanto riguarda le attività di **Espionage** (anche a causa della scarsità di informazioni pubbliche in merito) rispetto al 2019 la loro percentuale rispetto al totale degli attacchi rilevati nel primo semestre 2020 rimane stabile al **12%**, mentre l'**Information Warfare** passa dal 2% al **3%**.

Tipologia e distribuzione vittime (1H 2020)

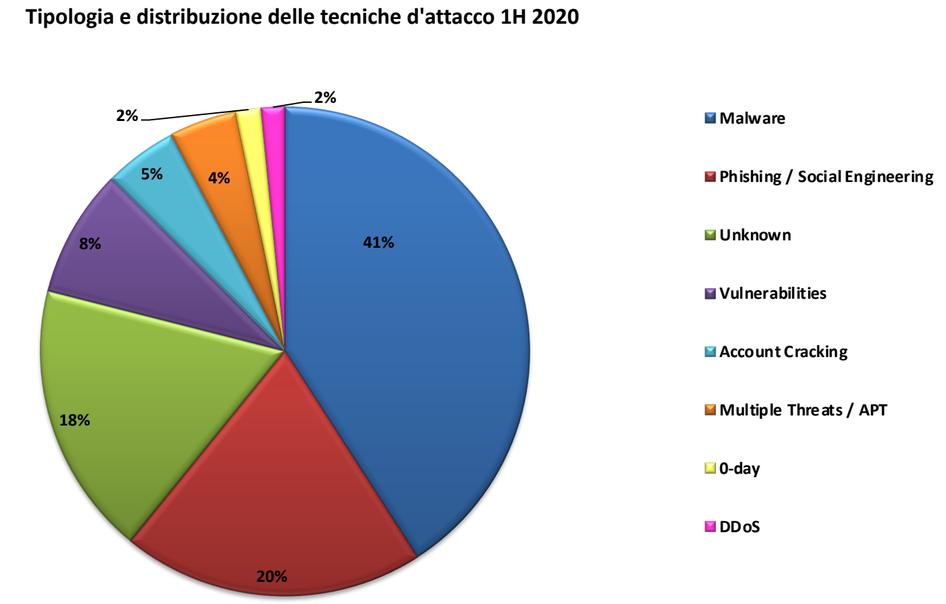


© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2020

Rispetto al primo semestre 2019, in termini assoluti nel 1H 2020 la crescita maggiore nel numero di attacchi gravi si osserva verso le categorie “Multiple Targets” (**+26,3%**), “Research / Education” (**+63,3%**), “Critical Infrastructures” (**+85%**), seguite da “Others” (**+142,9%**) e “Gov Contractors” (**+73,3%**). Aumentano leggermente gli attacchi verso la categoria “Government” (**+5,6%)**. Diminuiscono “Healthcare”, “Banking / Finance” e “Online Services / Cloud”.
La categoria “Multiple Targets” si conferma al primo posto assoluto anche nel 1H 2020 (**25%** del totale, era il 21% nel 1H 2019), superando per il quarto anno di fila il settore “Gov”, che dal 2011 al 2016 è sempre stato al primo posto nel nostro studio, ed ora è al **14%** (era il 13% nel 1H 2019).

Streaming Edition
SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT
20 anni Clusit Associazione Italiana per la Sicurezza Informatica

Tipologia e distribuzione tecniche di attacco (1H 2020)

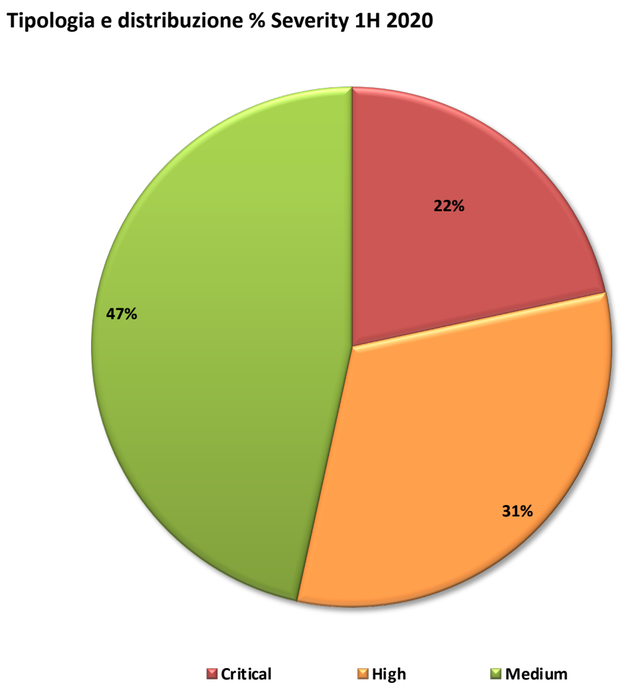


© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2020

Nel 1H 2020 la categoria che mostra numeri assoluti maggiori è “Malware” (**+6,8%**). Le tecniche sconosciute (categoria “Unknown”) scendono al terzo posto, con una diminuzione del **7,8%** rispetto al 1H 2019, superate dalla categoria “Phishing / Social Engineering” (+**26,1%**), che sale per la prima volta al secondo posto in termini assoluti (grazie anche alla diffusione di molte campagne a tema Covid-19, che rappresentano più del 40% del totale della categoria), raggiungendo il **20%** nel periodo (era il 17% nel 1H 2019). Aumenta l’utilizzo di vulnerabilità “0-day”, (**+16,7%**), per quanto quest’ultimo dato sia ricavato da incidenti di dominio pubblico e risulti quindi probabilmente sottostimato. Ritornano a crescere in modo significativo gli attacchi basati su tecniche di “Account Hacking / Cracking” (**+24,2%**).

Streaming Edition
SECURITY SUMMIT
20 anni Clusit Associazione Italiana per la Sicurezza Informatica

Valutazione degli impatti – Severity (1H 2020)



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2020

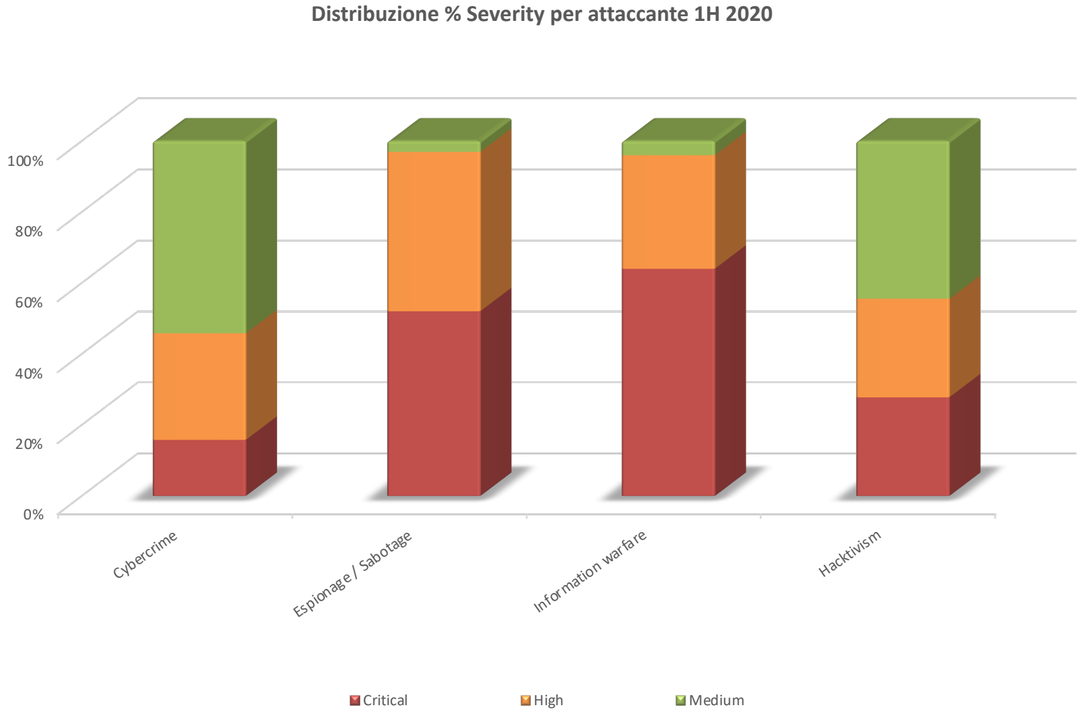
Per il terzo anno abbiamo definito tre categorie o livelli di impatto (considerato che stiamo comunque analizzando un campione di attacchi già tutti definiti come “gravi”): Medio, Alto e Critico.

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.

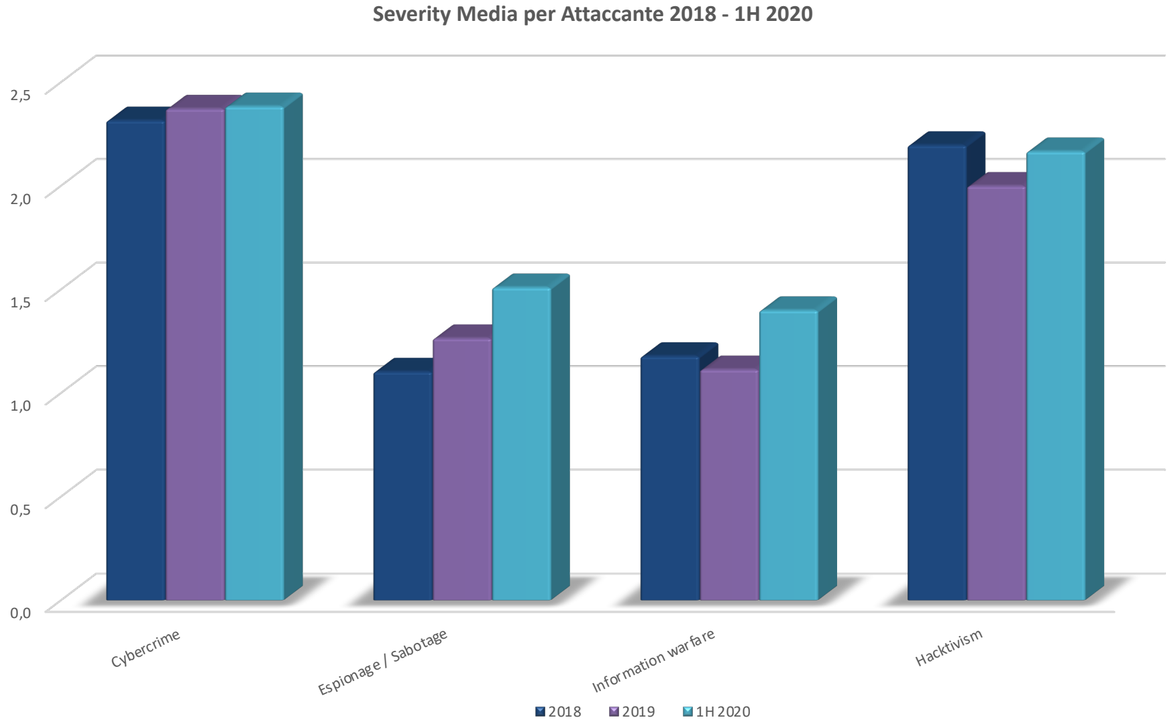
Gli attacchi con impatto “Medio” rappresentano il **47%** del totale (come nel 1H 2019), mentre quelli di livello “Alto” il **31%** (erano il 28%) e quelli di livello “Critico” oltre un quinto con il **22%** (erano il 26%).

Gli attacchi gravi con effetti molto importanti (high) o devastanti (critical) rimangono comunque il **53%** del nostro campione anche nel primo semestre 2020.

Severity per tipologia di attaccanti (1H 2020)



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2020

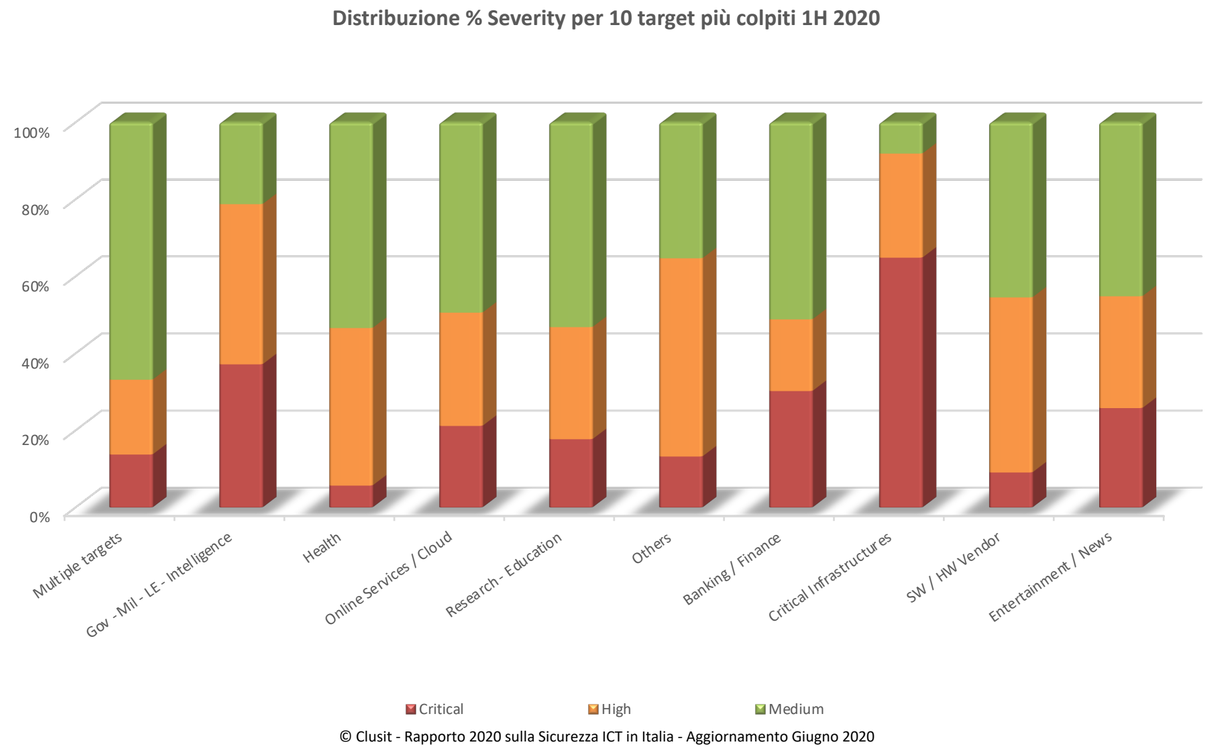


© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2020

Il maggior numero di attacchi classificati come “Critici” riguarda le categorie di attaccanti “Espionage” ed “Information Warfare”. Pur rappresentando l’83% del totale, gli attacchi di matrice cybercriminale hanno complessivamente il tasso di Severity più basso tra tutte le categorie di attaccanti considerate. Interessante anche notare come l’Hacktivism, pur in grande diminuzione, presenti un’ampia percentuale di attacchi con impatto di tipo “Critico” ed abbia un valore medio della Severity peggiore rispetto alla categoria Cybercrime. Dal grafico di sinistra risulta particolarmente evidente il balzo effettuato da Espionage/Sabotage e Information Warfare in termini di Severity nel periodo 2018-2020.

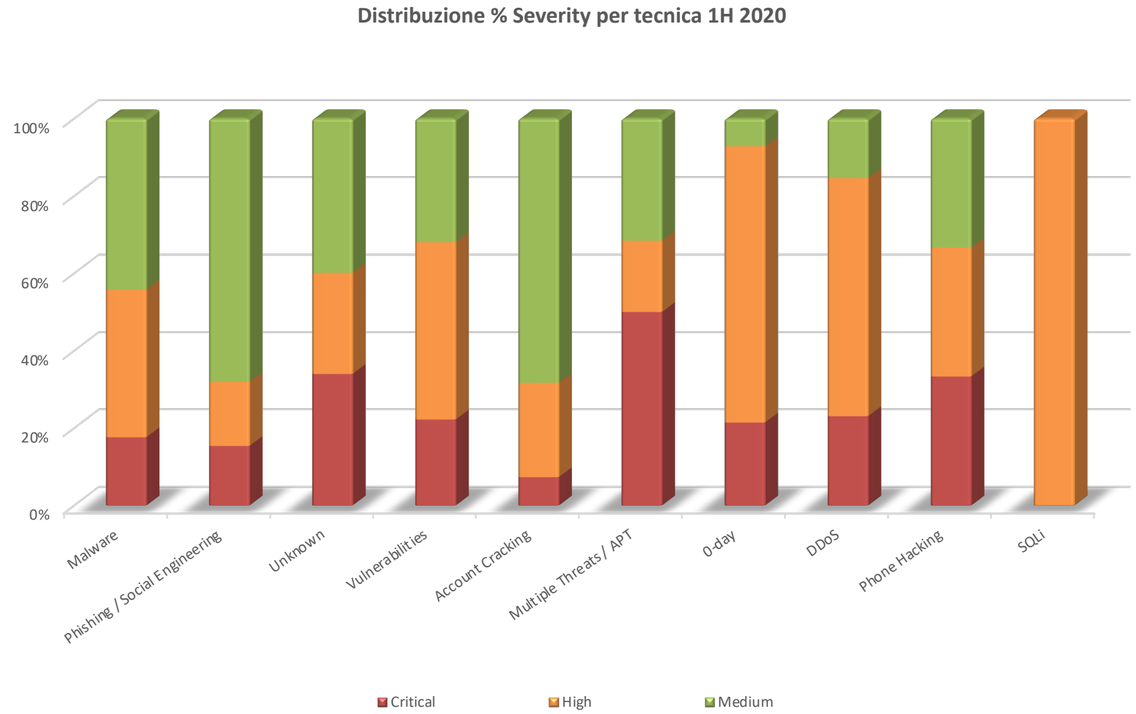
Streaming Edition
SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT
20 anni Clusit Associazione Italiana per la Sicurezza Informatica

Severity per tipologia di vittime (1H 2020)



Per quanto riguarda la distribuzione della Severity in riferimento alle vittime, si può notare come le categorie “Critical Infrastructures” e “Gov” abbiano subito il maggior numero di attacchi con Severity “Critical”, mentre le categorie con il maggior numero di attacchi con impatti di livello “Alto” sono “Healthcare”, “Gov”, “SW/HW vendor” e “Others”. Da notare come, alla luce di questi dati, il «threat model» delle varie categorie di vittime risulti significativamente eterogeneo, il che dovrebbe indurre ad una serie di importanti riflessioni sulla bontà dell’approccio «generalista» alla cyber security.

Severity per tipologia di tecniche di attacco (1H 2020)



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2020

Dal punto di vista delle tecniche di attacco gli incidenti con impatto più critico sono quelli realizzati tramite APT, Phone Hacking, Unknown, DDoS e 0-day (quindi più sofisticati e stealth, spesso con motivazioni geopolitiche e finalità di Espionage e Information Warfare). Gli attacchi realizzati tramite Malware semplice, tecniche di Phishing / Social Engineering e di Account cracking hanno un livello medio di Severity relativamente basso, pur essendo quelli più numerosi. Molto simili in percentuale gli attacchi con impatto “Critico” realizzati tramite Malware e Vulnerabilità note, mentre pur essendo numericamente pochi gli attacchi DDoS del campione mostrano una Severity media piuttosto alta.

Streaming Edition
SECURITY SUMMIT
20 anni Clusit Associazione Italiana per la Sicurezza Informatica

I contenuti del Rapporto Clusit 2020

Aggiornamento di Ottobre 2020

Luca Bechelli – CTS Clusit

#securitysummit #streamingedition

I contenuti del Rapporto

Panoramica dei cyber attacchi più significativi del 2019 e del primo semestre 2020	*segue intervento di Andrea Zapparoli Manzoni – CD Clusit*
• Analisi Fastweb della situazione italiana in materia di cyber-crime e incidenti informatici con aggiornamento **I° Semestre 2020**	*segue intervento di Marco Raimondi - Fastweb*
• Stato della Cybersecurity nel Sud Italia - **secondo studio** realizzato da ricercatori dell'Università degli Studi di Bari e di Exprivia/Italtel	*segue intervento di Domenico Raguseo, Exprivia*
• Attività e segnalazioni della Polizia Postale e delle Comunicazioni nel **1° semestre 2020**	
• Le attività del CERT-AGID (dal CERT-PA al CERT-AGID - aggiornamento **I° Semestre 2020**)	
Speciale Pandemia:	
• La sicurezza dei dati in tempo di pandemia: un approccio strategico a tutela delle organizzazioni	*#alessioèpreoccupato*
• Analisi Clusit dei cyber attacchi a tema Covid-19 più significativi del primo semestre 2020	*Domande o approfondimenti: Sofia Scozzari – sessione 18:00*
• La prima CyberPandemia nella storia dell'umanità	*Domande o approfondimenti: Aldo Di Mattia – sessione delle 11:30*
• Operazione Amuchina – a cura del Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza	
Speciale FINANCE: Elementi sul Cyber-crime nel settore finanziario in Europa"- oltre al contributo inedito del CERT di Banca d'Italia, con i seguenti **aggiornamenti**: Analisi cybercrime nel settore finanziario (Rotondo, IBM), Analisi e trend delle frodi nel settore bancario (Trinchera, CERTFin)	
Il mercato italiano della Sicurezza IT: analisi, prospettive e tendenze secondo IDC	
Focus On: • "Business Continuity & Resilienza, leve fondamentali per una società sempre più globalizzata e digitalizzata" • "Mobile App italiane: una lente di ingrandimento sul loro stato di salute e sulle vulnerabilità più diffuse" • "Sicurezza nel settore sanitario – Perché gli ospedali sono così violabili" • "L'impatto dei deepfake sulla sicurezza delle organizzazioni economiche" • "Tendenze IT che avranno un impatto sui professionisti italiani nel 2020" • Dati inediti forniti dagli Osservatori del Politecnico di Milano sulla "OT Security", **con dati aggiornati al I semestre 2020**	

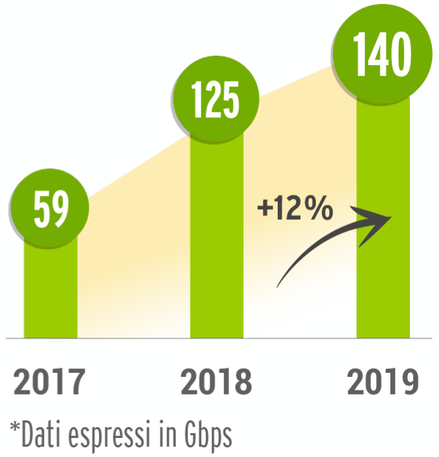
Marco Raimondi

Product Marketing Manager, Fastweb

FASTWEB
un passo avanti

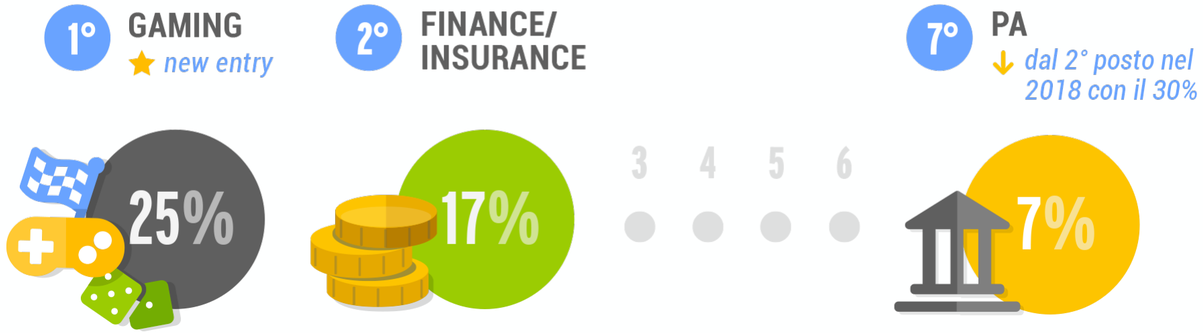
I CYBER ATTACCHI IN ITALIA: alcuni trend del 2019

Continuano a crescere MALWARE e ATTACCHI DDOS



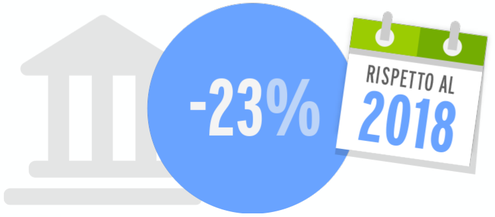
*Dati espressi in Gbps

Cambia la CLASSIFICA dei settori PIÙ COLPITI...

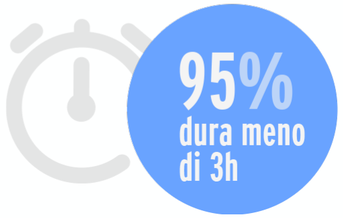


...ma LE MISURE DI DIFESA CYBER si dimostrano uno STRUMENTO EFFICACE di mitigazione

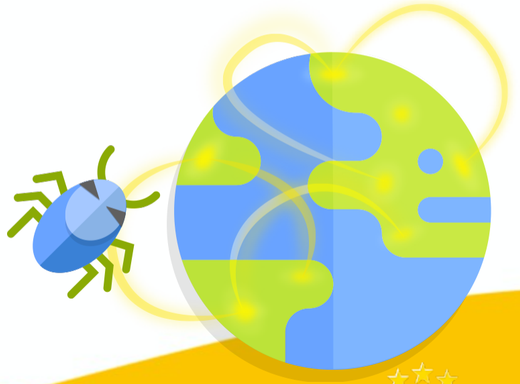
MENO ATTACCHI VERSO LA PA



SI RIDUCE LA DURATA DEGLI ATTACCHI



...e la provenienza degli ATTACCHI diventa "GLOBALE"



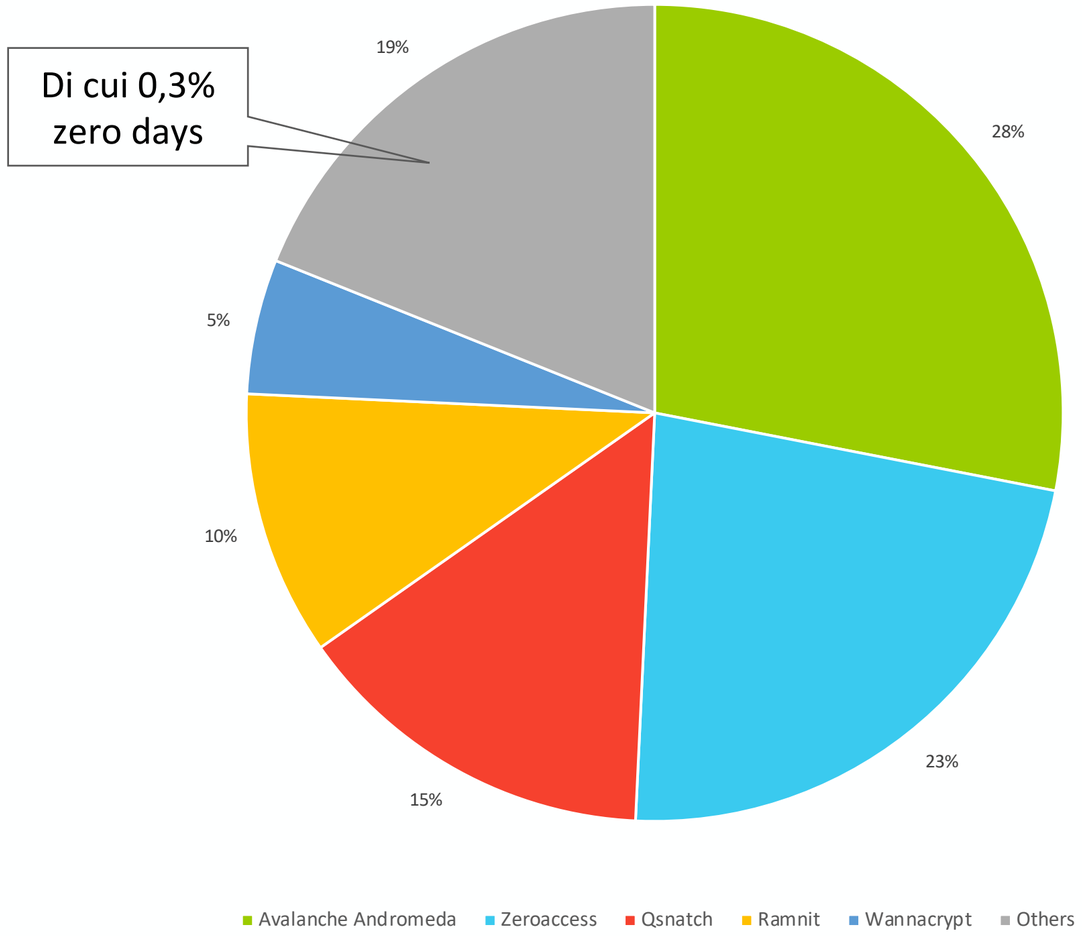
1° USA 83%

2° GERMANIA 8%

20 anni Clusit
Associazione Italiana per la Sicurezza Informatica

FASTWEB
un passo avanti

Distribuzione Malware e Botnet 2019

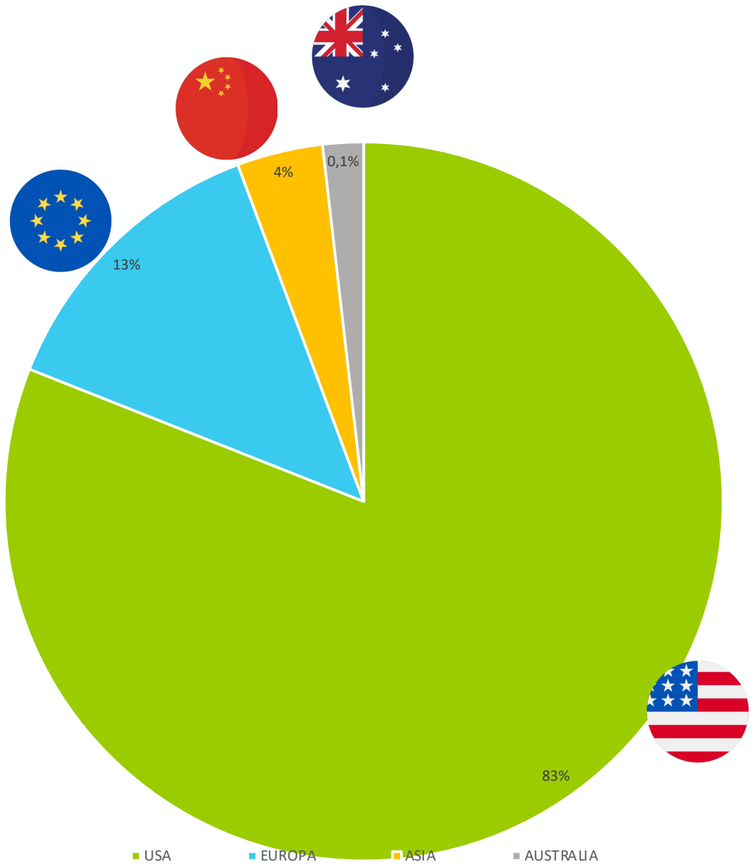


- **165 famiglie** di malware rilevate (-23% vs 2018)
- Il **28% dei malware** totali sono piattaforme di distribuzione di minacce (Avalanche Andromeda)
- **0,3%** di **Zero Days**

20 anni Clusit
Associazione Italiana per la Sicurezza Informatica
FASTWEB
un passo avanti

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.

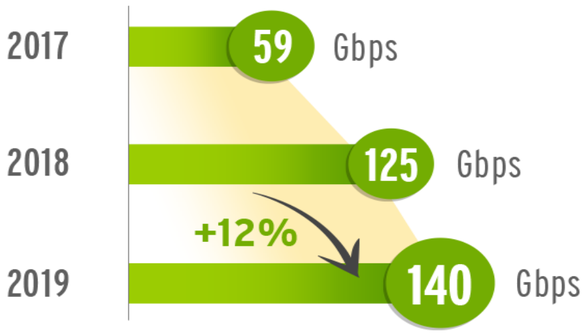


- Gli **Stati Uniti** continuano ad avere una **percentuale rilevante di C&C in aumento** rispetto al 2018
- **Diminuiscono** i centri di comando e controllo in **Asia** (-7% vs 2018)
- Questi host spesso sono **«macchine ponte»** per eludere l'indirizzo IP originario (+7% vs 2018)

20 anni Clusit
Associazione Italiana per la Sicurezza Informatica
FASTWEB
un passo avanti

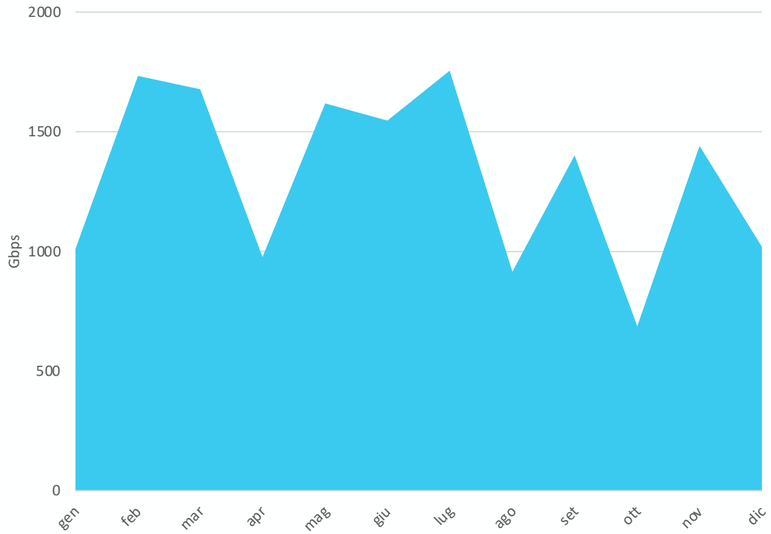
DDoS: Un fenomeno ancora in forte crescita

Banda di un attacco



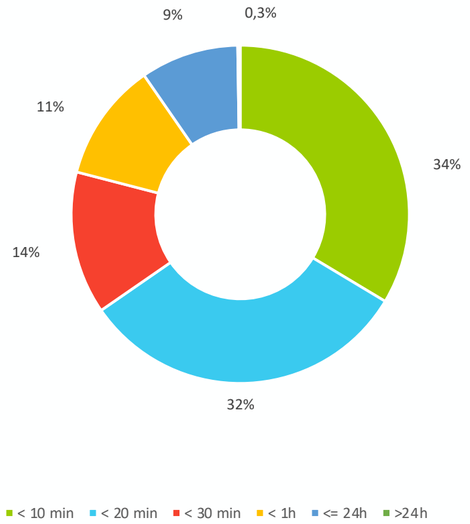
Nell'ultimo anno l'impatto degli attacchi è aumentato del 12%

Banda complessiva attacchi DDoS



Nel 2019 riscontrate 2500 «anomalie» con un incremento di banda mensile del 30% rispetto al 2018

Durata

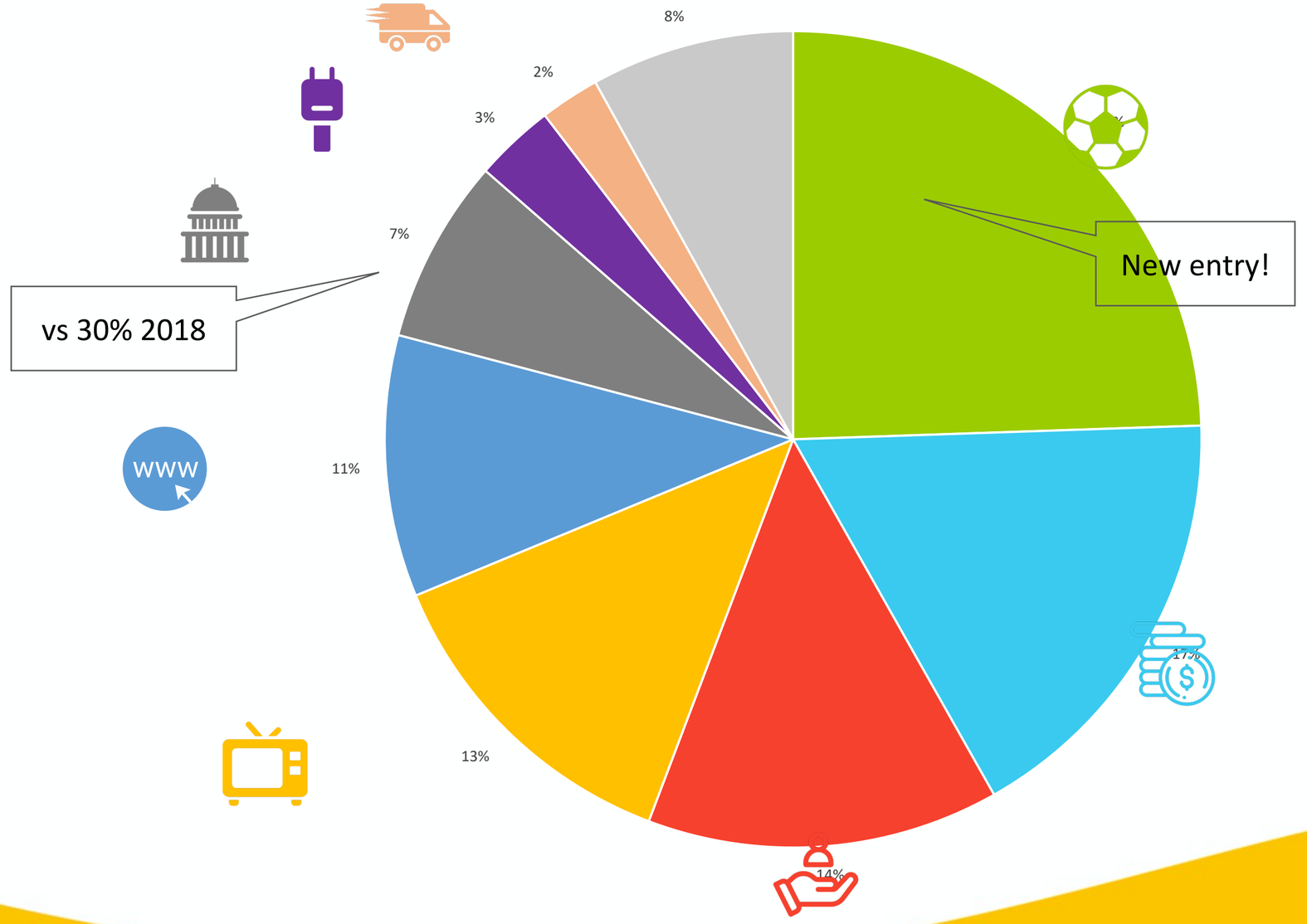


Gli attacchi DDoS nel 95% dei casi durano meno di 3h

20 anni Clusit
Associazione Italiana per la Sicurezza Informatica

FASTWEB
un passo avanti

DDoS: Attacchi per settori merceologici coinvolti



Uno sguardo al 2020 (1 gen/31 ago)

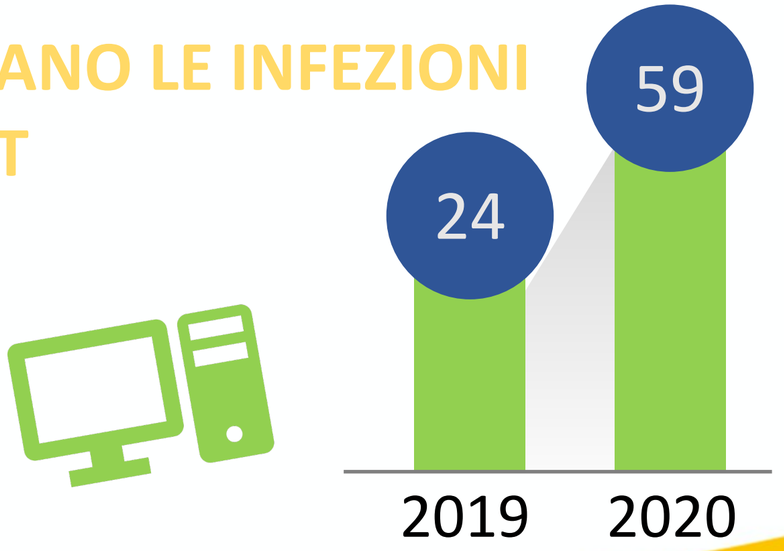
20 MILIONI di eventi malevoli in flessione: **-30%** vs stesso periodo 2019

SMB

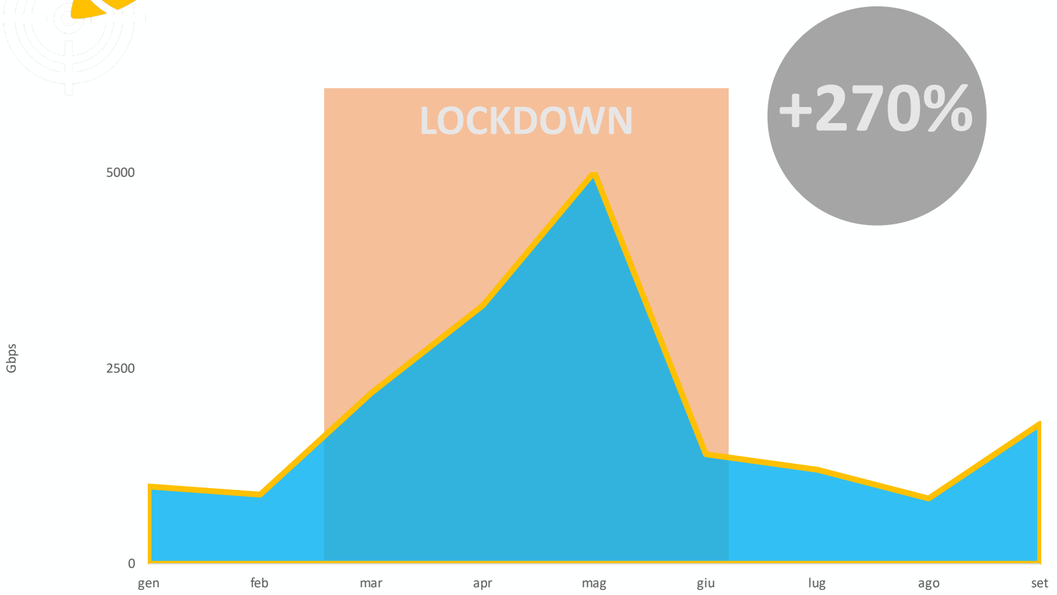
>telnet

I **SERVIZI PERICOLOSI** esposti si **RIDUCONO DEL 25%...**

... ma **AUMENTANO LE INFEZIONI** sugli **ENDPOINT**



ATTACCHI **DDOS IN LOCKDOWN**



FASTWEB
un passo avanti

FASTWEB

un passo avanti

Domenico Raguseo

RESPONSABILE CYBERSECURITY, EXPRIVIA

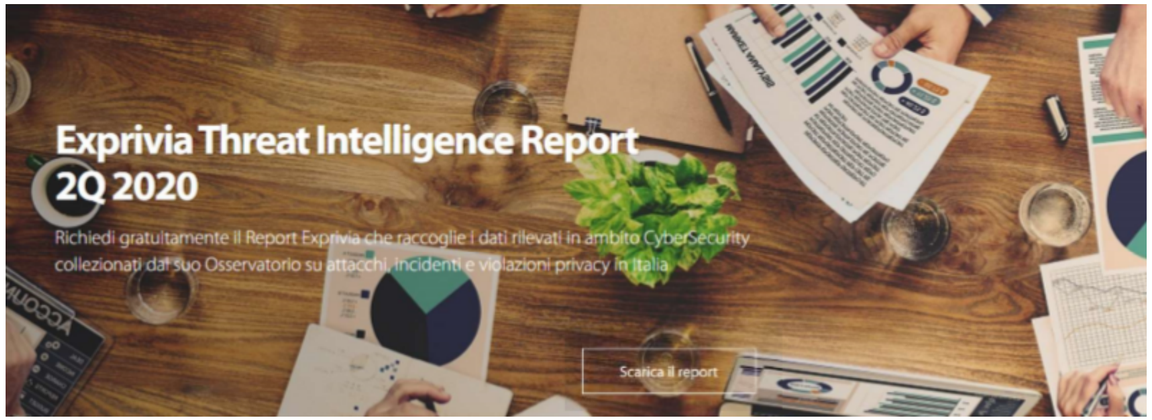
exprivia

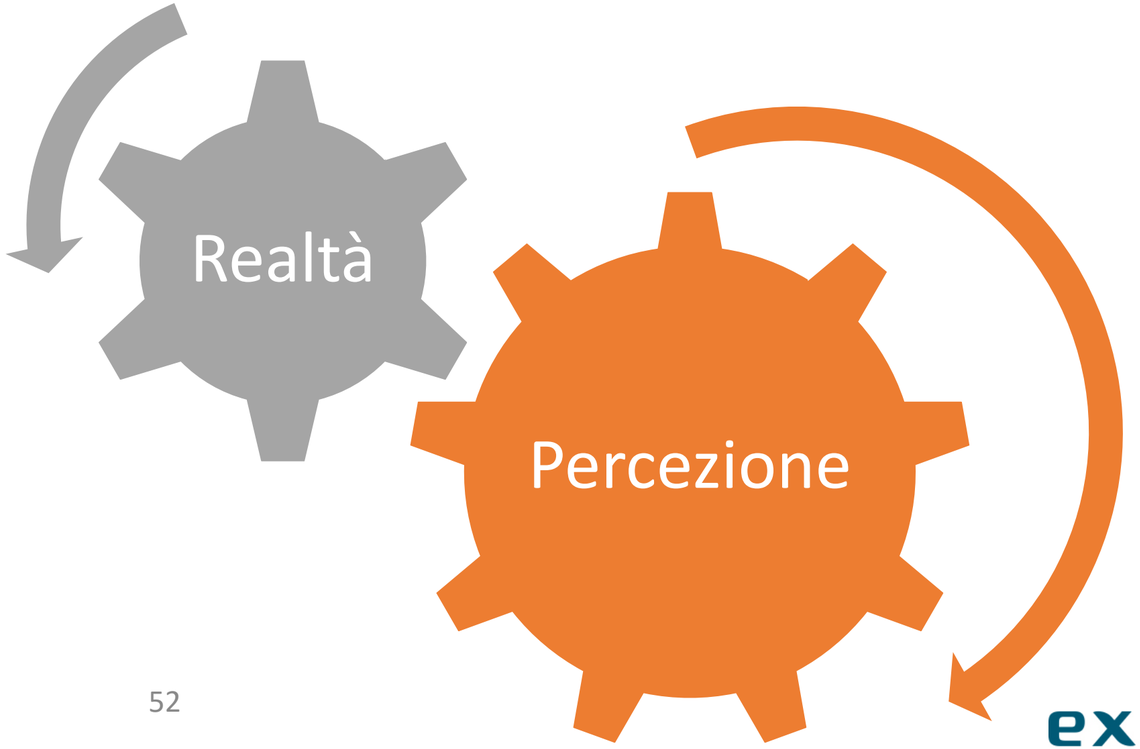
Stato della Cyber-Security nel Sud Italia

Il presente survey ha lo scopo di analizzare il livello di consapevolezza delle aziende e degli enti del Sud Italia sul tema della sicurezza informatica.
Il survey è anonimo.

Grazie per il tempo che ci dedicherai

Vita Santa Barletta (Università degli Studi di Bari)
Danilo Caivano (Università degli Studi di Bari)
Domenico Raguseo (Exprivia|Italtel)





Clusit SECURITY SUMMIT ASTREA
Streaming Edition
10-11-12 novembre 2020

exprivia

percezione – il campione

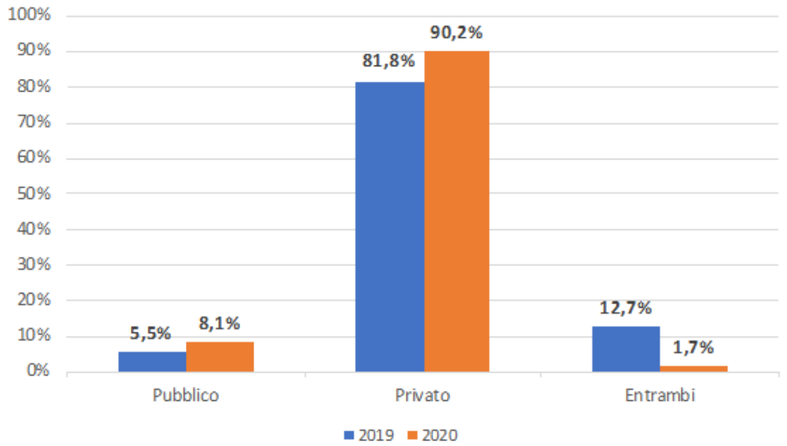


Figura 3. Ripartizione del campione intervistato per tipologia

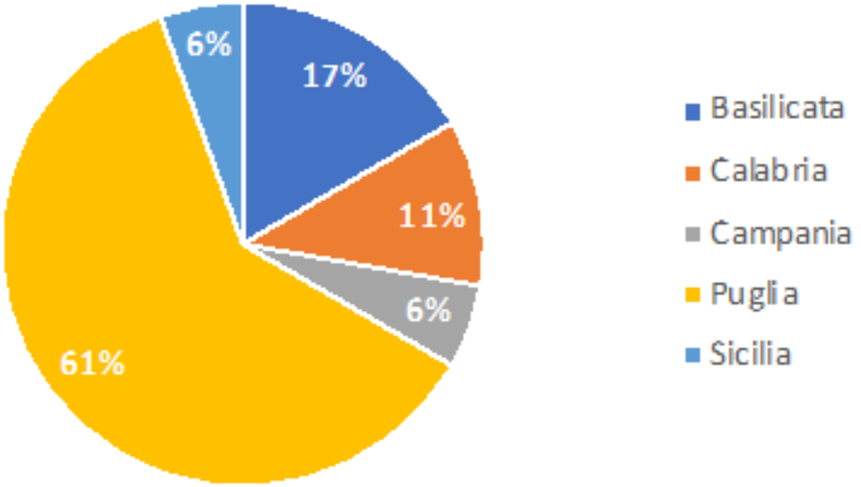


Figura 1. Ripartizione del campione intervistato per regione

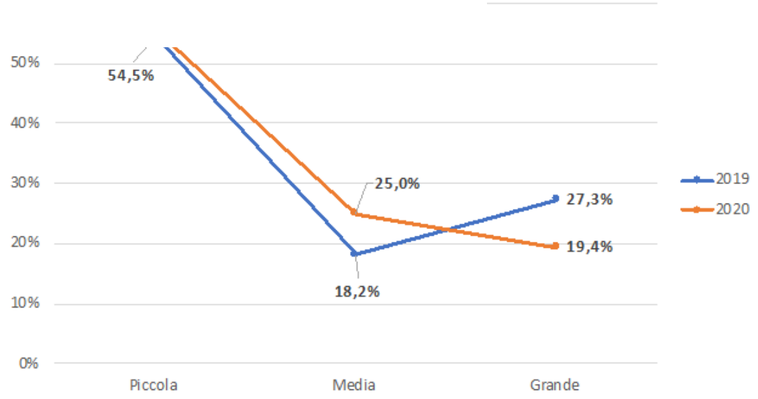


Figura 2. Ripartizione del campione intervistato per dimensione

percezione - danni

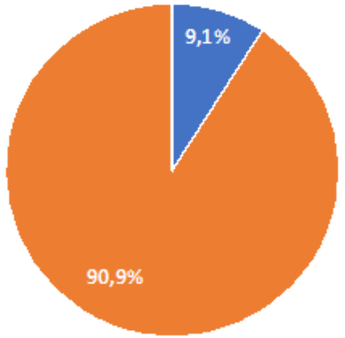


Figura 6. Distribuzione dei soggetti vittima di attacchi durante l'emergenza Covid-19

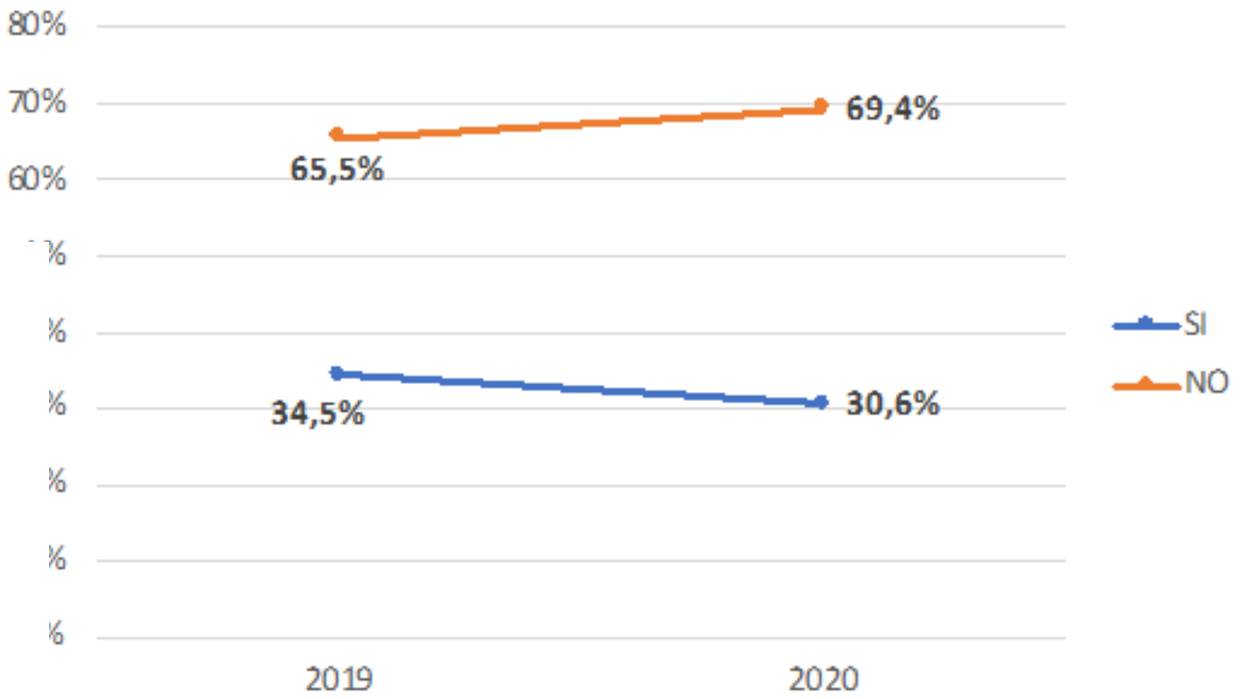


Figura 5. Distribuzione dei soggetti vittima di attacchi

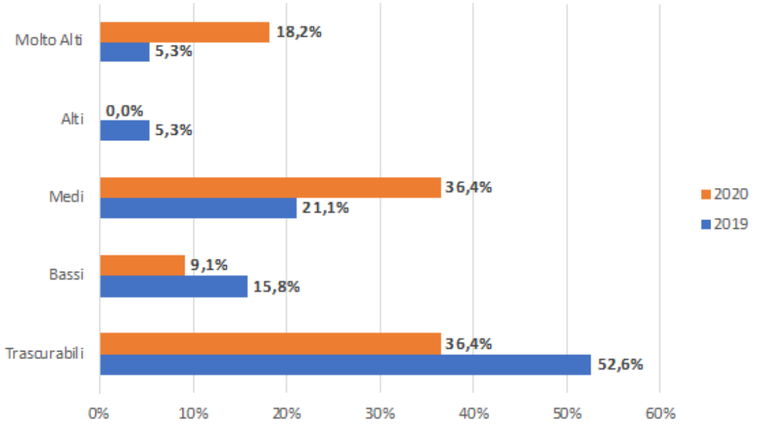


Figura 7. L'azienda/ente come valuta i danni subiti

percezione – capacità di difesa e necessità di formazione

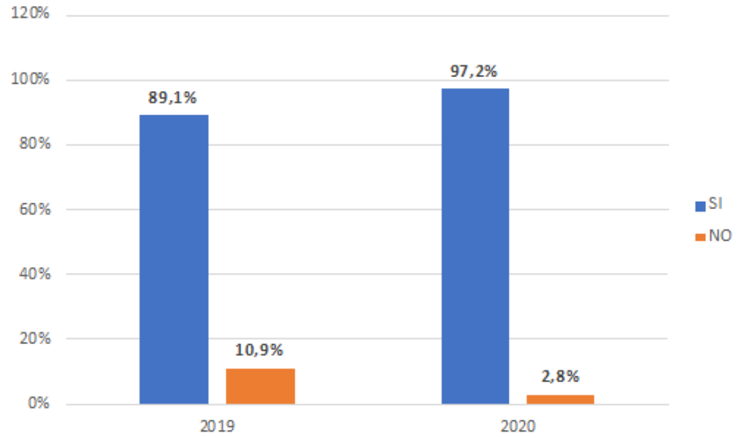


Figura 14. Ripartizione del campione intervistato rispetto all'utilità percepita di corsi di formazione sulla sicurezza informatica

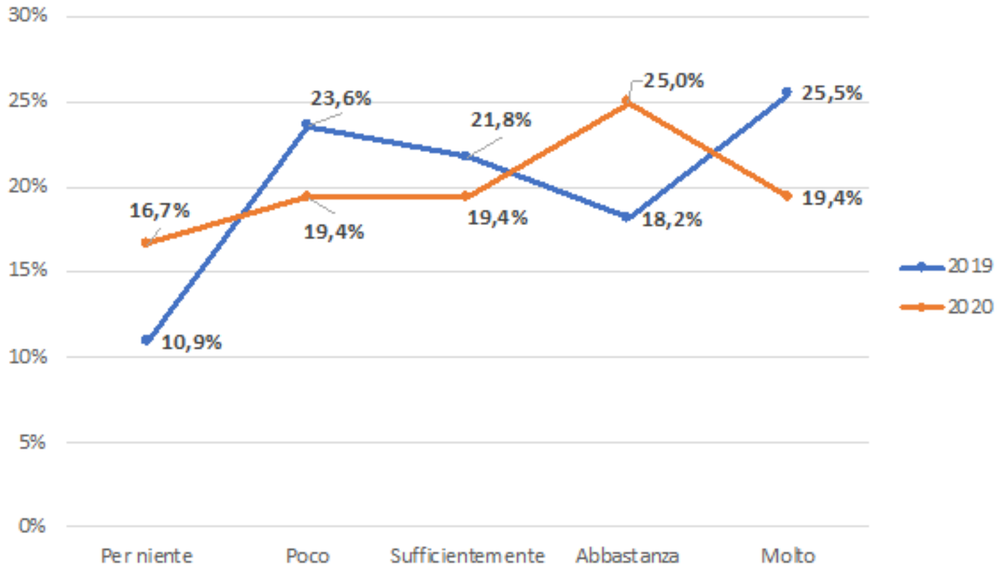
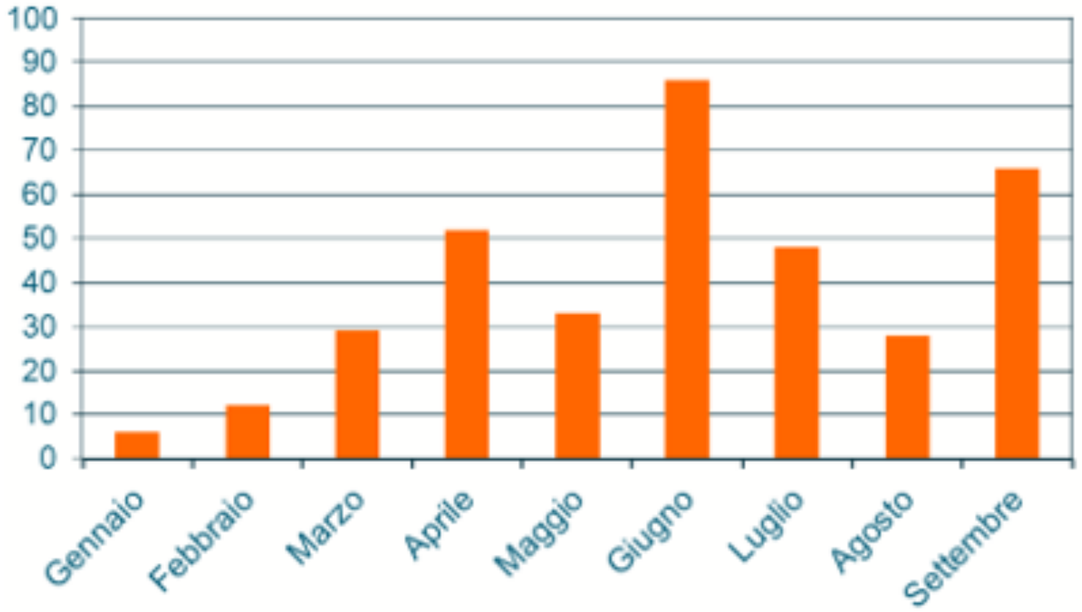


Figura 9. Ripartizione del campione per capacità di difesa da attacchi informatici

realtà – attacchi/incidenti/violazioni privacy



Numero di attacchi, incidenti e violazioni privacy suddivisi in mesi nel 2020 in Italia

Streaming Edition 2020

Tavola rotonda
moderata da Luca Bechelli, con la partecipazione di

- Mauro Cornelli, Oracle
- Carlo Mauceli, Microsoft
- Ivan De Tomasi, WatchGuard Technologies
- Gastone Nencini, Trend Micro
- Maurizio Taglioretti, Netwrix

Per ricevere una copia del rapporto: rapporti@clusit.it

Per chiedere gli attestati : attestati@clusit.it

Per informazioni di carattere generale sulla manifestazione Security Summit scrivere a info@astrea.pro