UNIVERSITÀ
POLITECNICA
DELLE MARCHE

Facoltà di Ingegneria

"(Conoscere la) Cybersecurity: un'esigenza per scuola e famiglia".

Franco Chiaraluce

Dipartimento di Ingegneria dell'Informazione

f.chiaraluce@univpm.it

LO SPAZIO CIBERNETICO

Decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017

Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali

(Gazzetta Ufficiale n. 87 del 13 aprile 2017)

Lo **spazio cibernetico (cyber spazio)** è «l'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti, nonché delle relazioni logiche, comunque stabilite, tra di essi»

Il cyber spazio è «la cosa più complessa e articolata che l'uomo abbia mai concepito, unione di migliaia di reti dati e di stratificazioni di software che interconnettono uomini e cose in giro per il mondo»

[cfr. Roberto Baldoni, già direttore dell'ACN, l'Agenzia per la Cybersicurezza Nazionale]

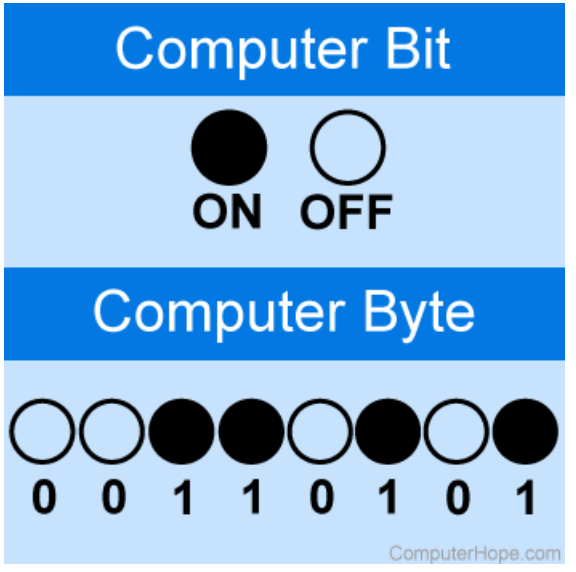
CODIFICA BINARIA

- All'interno di un computer le informazioni sono codificate usando la rappresentazione binaria, basata su un alfabeto di due soli simboli: 1 e 0.

UNIVERSITÀ POLITECNICA DELLE MARCHE

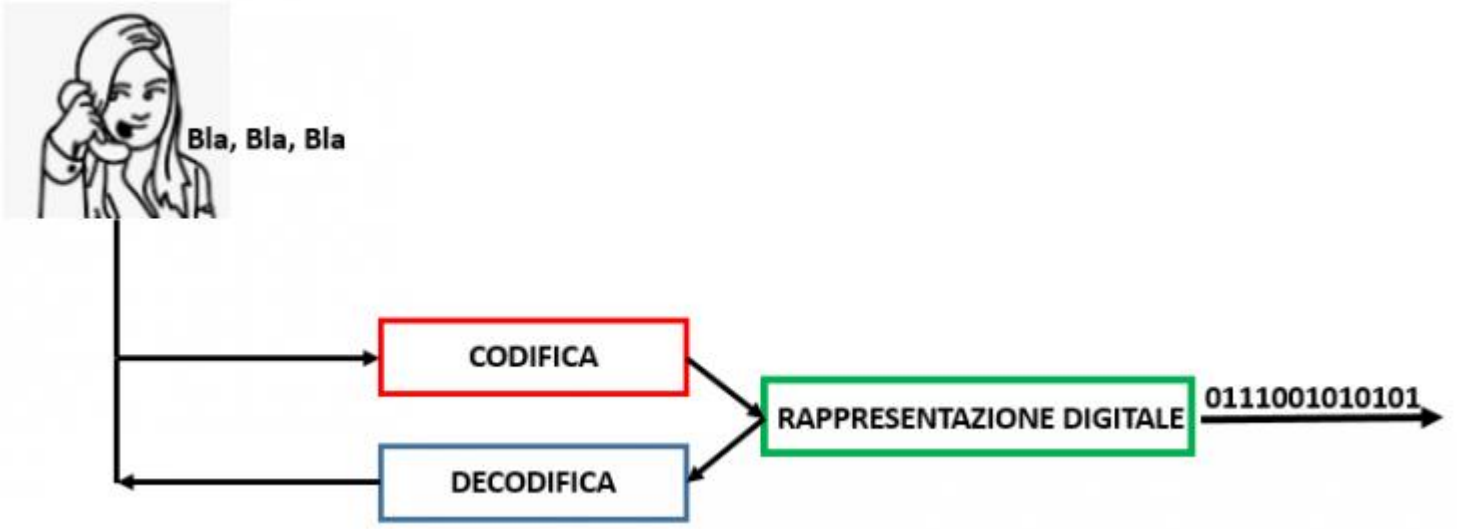
IL BIT

- In informatica, l'unità di misura elementare dell'informazione, che viene rappresentata alternativamente con le cifre 0 e 1, in quanto corrisponde a una scelta tra due possibili alternative.



UNIVERSITÀ POLITECNICA DELLE MARCHE

INFORMAZIONE E CODIFICA



UNIVERSITÀ POLITECNICA DELLE MARCHE

INFORMAZIONE E CODIFICA

Capitolo I
Breve storia della pubblicità

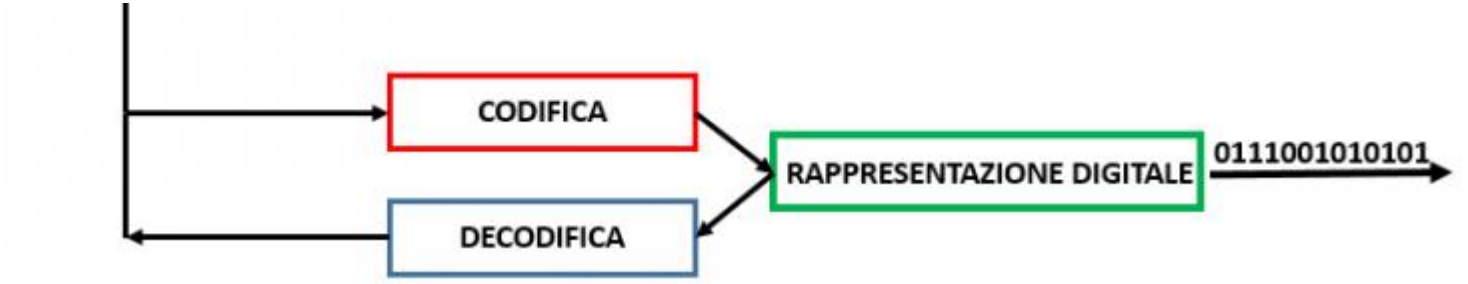
1. Sulla soglia

La pubblicità ha origini molto più remote di quanto si possa pensare. Già nelle società post-arcaiche (si vedano gli scavi archeologici dell'antica Roma o di Pompei), le varie botteghe avevano dei dipinti – antenati delle odierne insegne – che rappresentavano il lavoro o le merci che si potevano trovare all'interno.
Questo sistema rimase in uso finanche dopo il Medioevo, quando cioè l'avvento di una classe di ricchi possidenti non nobili trasformò la società, con la necessità di una scolarizzazione diffusa (prima solo la classe nobiliare poteva accedere all'istruzione).
Solo dopo l'invenzione di Gutenberg e la nascita dei primi quotidiani, nascono i primi box pubblicitari, mentre gli strati meno colti utilizzavano ancora il metodo più antico conosciuto dall'essere umano: la voce (o quello che oggi chiamiamo "passaparola"). Fred Vargas ci fornisce un interessante esempio di banditore[1]:

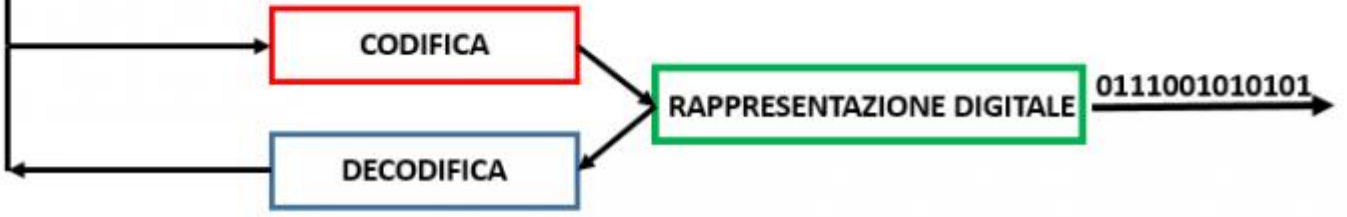
> «(...) raccoglieva nell'ora una notevole quantità di messaggi, in media una sessantina al giorno – e molti di più la mattina della sera, poiché la notte era propizia ai depositi furtivi –, ognuno in una buona chiusa e zavorrata da una moneta di cinque franchi. Cinque franchi per poter sentire il proprio pensiero, la propria frustrazione, la propria ricetta lasciata al vento di Parigi non era poi così caro. All'inizio Jean aveva provato con una tariffa minima, ma alla gente non piace «dar svendere le proprie frasi per una moneta da un franco».

Ma da quando possiamo incominciare a parlare di pubblicità? C'è sostanziale accordo nell'atto di nascita della pubblicità "moderna", quella che si sviluppa con l'avvento dei primi quotidiani, situandola nel **1631**, quando apparve per la prima volta

[1] Fred Vargas, *Parti in fretta e non tornare*, Torino, Einaudi, 2004, p. 13



INFORMAZIONE E CODIFICA



UNIVERSITÀ POLITECNICA DELLE MARCHE

CODIFICA ASCII

Dec	Hex	Oct	Binary	Char	Dec	Hex	Oct	Binary	Char	Dec	Hex	Oct	Binary	Char	Dec	Hex	Oct	Binary	Char
0	00	000	0000000	NUL (null character)	32	20	040	0100000	space	64	40	100	1000000	@	96	60	140	1100000	`
1	01	001	0000001	SOH (start of header)	33	21	041	0100001	!	65	41	101	1000001	A	97	61	141	1100001	a
2	02	002	0000010	STX (start of text)	34	22	042	0100010	"	66	42	102	1000010	B	98	62	142	1100010	b
3	03	003	0000011	ETX (end of text)	35	23	043	0100011	#	67	43	103	1000011	C	99	63	143	1100011	c
4	04	004	0000100	EOT (end of transmission)	36	24	044	0100100	$	68	44	104	1000100	D	100	64	144	1100100	d
5	05	005	0000101	ENQ (enquiry)	37	25	045	0100101	%	69	45	105	1000101	E	101	65	145	1100101	e
6	06	006	0000110	ACK (acknowledge)	38	26	046	0100110	&	70	46	106	1000110	F	102	66	146	1100110	f
7	07	007	0000111	BEL (bell (ring))	39	27	047	0100111	'	71	47	107	1000111	G	103	67	147	1100111	g
8	08	010	0001000	BS (backspace)	40	28	050	0101000	(	72	48	110	1001000	H	104	68	150	1101000	h
9	09	011	0001001	HT (horizontal tab)	41	29	051	0101001	)	73	49	111	1001001	I	105	69	151	1101001	i
10	0A	012	0001010	LF (line feed)	42	2A	052	0101010	*	74	4A	112	1001010	J	106	6A	152	1101010	j
11	0B	013	0001011	VT (vertical tab)	43	2B	053	0101011	+	75	4B	113	1001011	K	107	6B	153	1101011	k
12	0C	014	0001100	FF (form feed)	44	2C	054	0101100	,	76	4C	114	1001100	L	108	6C	154	1101100	l
13	0D	015	0001101	CR (carriage return)	45	2D	055	0101101	-	77	4D	115	1001101	M	109	6D	155	1101101	m
14	0E	016	0001110	SO (shift out)	46	2E	056	0101110	.	78	4E	116	1001110	N	110	6E	156	1101110	n
15	0F	017	0001111	SI (shift in)	47	2F	057	0101111	/	79	4F	117	1001111	O	111	6F	157	1101111	o
16	10	020	0010000	DLE (data link escape)	48	30	060	0110000	0	80	50	120	1010000	P	112	70	160	1110000	p
17	11	021	0010001	DC1 (device control 1)	49	31	061	0110001	1	81	51	121	1010001	Q	113	71	161	1110001	q
18	12	022	0010010	DC2 (device control 2)	50	32	062	0110010	2	82	52	122	1010010	R	114	72	162	1110010	r
19	13	023	0010011	DC3 (device control 3)	51	33	063	0110011	3	83	53	123	1010011	S	115	73	163	1110011	s
20	14	024	0010100	DC4 (device control 4)	52	34	064	0110100	4	84	54	124	1010100	T	116	74	164	1110100	t
21	15	025	0010101	NAK (negative acknowledge)	53	35	065	0110101	5	85	55	125	1010101	U	117	75	165	1110101	u
22	16	026	0010110	SYN (synchronize)	54	36	066	0110110	6	86	56	126	1010110	V	118	76	166	1110110	v
23	17	027	0010111	ETB (end transmission block)	55	37	067	0110111	7	87	57	127	1010111	W	119	77	167	1110111	w
24	18	030	0011000	CAN (cancel)	56	38	070	0111000	8	88	58	130	1011000	X	120	78	170	1111000	x
25	19	031	0011001	EM (end of medium)	57	39	071	0111001	9	89	59	131	1011001	Y	121	79	171	1111001	y
26	1A	032	0011010	SUB (substitute)	58	3A	072	0111010	:	90	5A	132	1011010	Z	122	7A	172	1111010	z
27	1B	033	0011011	ESC (escape)	59	3B	073	0111011	;	91	5B	133	1011011	[	123	7B	173	1111011	{
28	1C	034	0011100	FS (file separator)	60	3C	074	0111100	<	92	5C	134	1011100	\	124	7C	174	1111100	|
29	1D	035	0011101	GS (group separator)	61	3D	075	0111101	=	93	5D	135	1011101	]	125	7D	175	1111101	}
30	1E	036	0011110	RS (record separator)	62	3E	076	0111110	>	94	5E	136	1011110	^	126	7E	176	1111110	~
31	1F	037	0011111	US (unit separator)	63	3F	077	0111111	?	95	5F	137	1011111	_	127	7F	177	1111111	DEL

UNIVERSITÀ POLITECNICA DELLE MARCHE

CODIFICA DI IMMAGINI

Quanti pixel?

1 bit
2 toni

2 bit
4 toni

8 bit
256 toni

Quanti bit per pixel?

Es: un'immagine di 400x400 pixel a 256 toni/colori occupa 160,000 byte

L'ERA DEI BIG DATA

- 1 byte (B) = 8 bit
- 1 kilobyte (kB) = 1000 B
- 1 megabyte (MB) = 1000 kB
- 1 gigabyte (GB) = 1000 MB
- 1 terabyte (TB) = 1000 GB
- 1 petabyte (PB) = 1000 TB
- 1 exabyte (EB) = 1000 PB
- 1 zettabyte (ZB) = 1000 EB = **10^{21} B**

UNIVERSITÀ POLITECNICA DELLE MARCHE

L'ERA DEI BIG DATA

Year	Data in Volume	Percentage change over the previous Year
2025*	181 zettabytes	23.13%
2024*	147 zettabytes	22.5%
2023	120 zettabytes	23.71%
2022	97 zettabytes	22.78%
2021	79 zettabytes	23.05%
2020	64.2 zettabytes	56.59%
2019	41 zettabytes	24.24%
2018	33 zettabytes	26.92%
2017	26 zettabytes	44.44%
2016	18 zettabytes	16.13%
2015	15.5 zettabytes	24%

Source: Statista, Exploding topics.

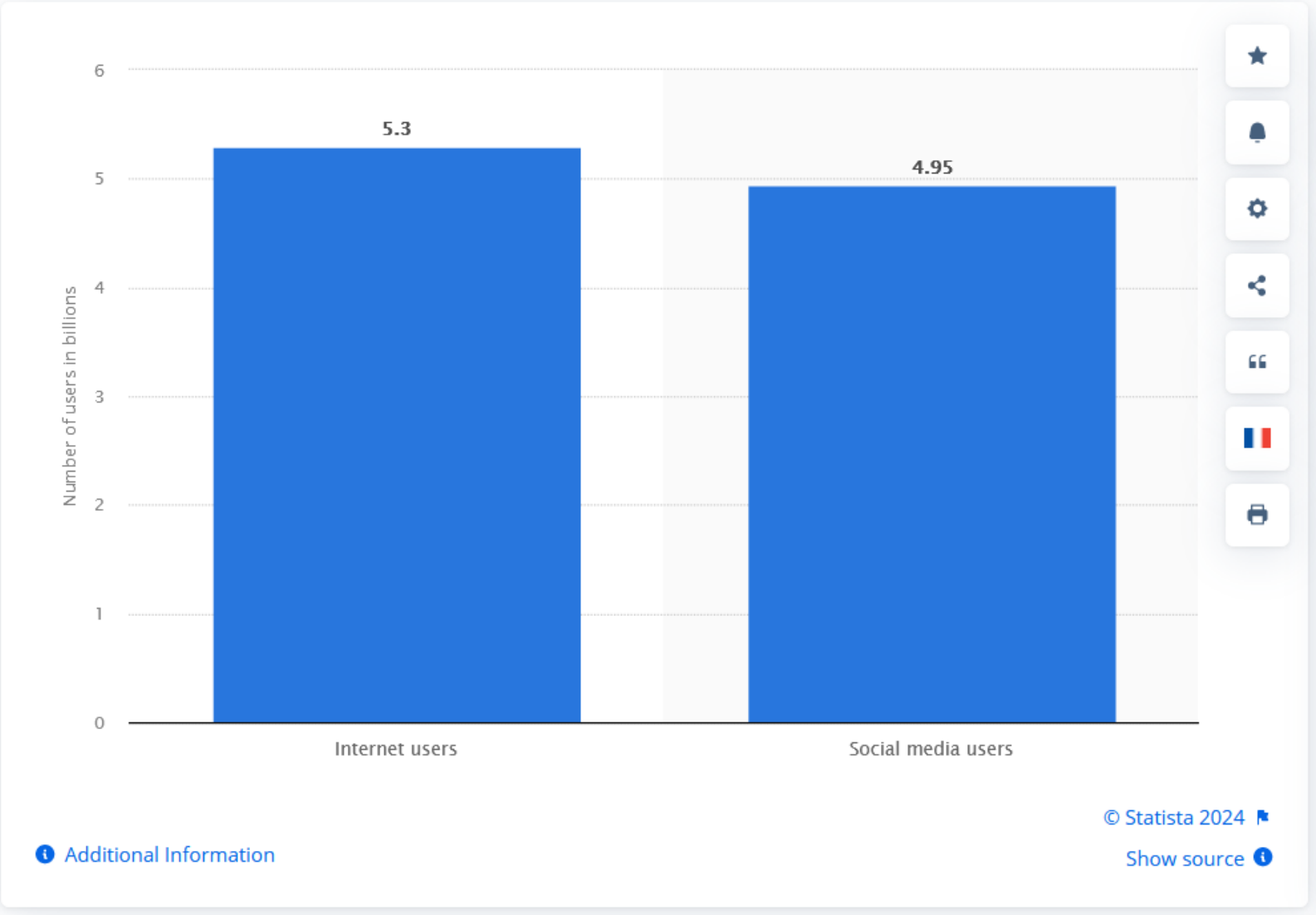
UNIVERSITÀ POLITECNICA DELLE MARCHE

L'ERA DEI BIG DATA

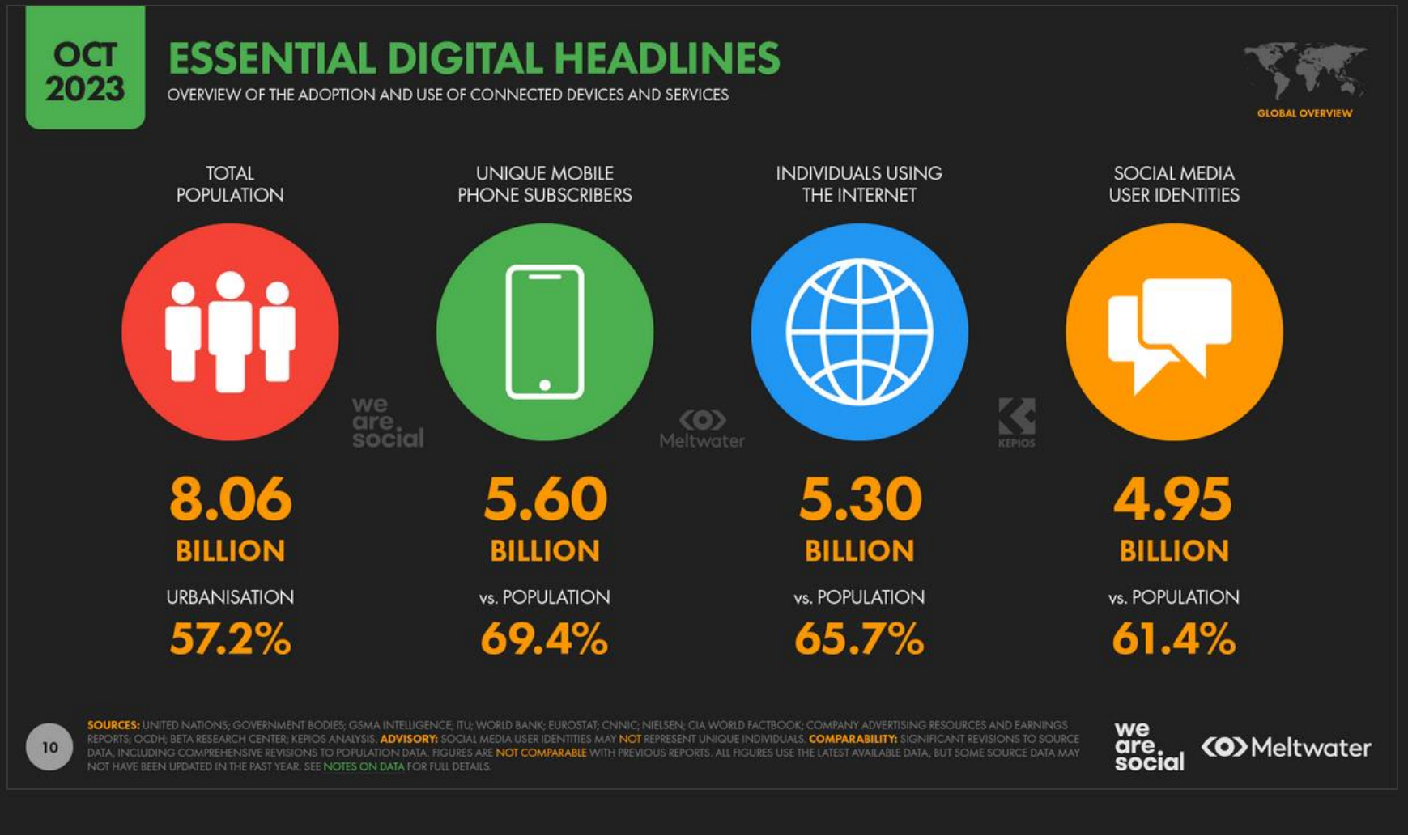
Year	Data in Volume	Percentage change over the previous Year
2025*	181 zettabytes	23.13%
2024*	147 zettabytes	22.5%
2023	120 zettabytes	23.71%
2022	97 zettabytes	22.78%
2021	79 zettabytes	23.05%
2020	64.2 zettabytes	56.59%
2019	41 zettabytes	24.24%
2018	33 zettabytes	26.92%
2017	26 zettabytes	44.44%
2016	18 zettabytes	16.13%
2015	15.5 zettabytes	24%

Source: Statista, Exploding topics.

L'ERA DEI BIG DATA

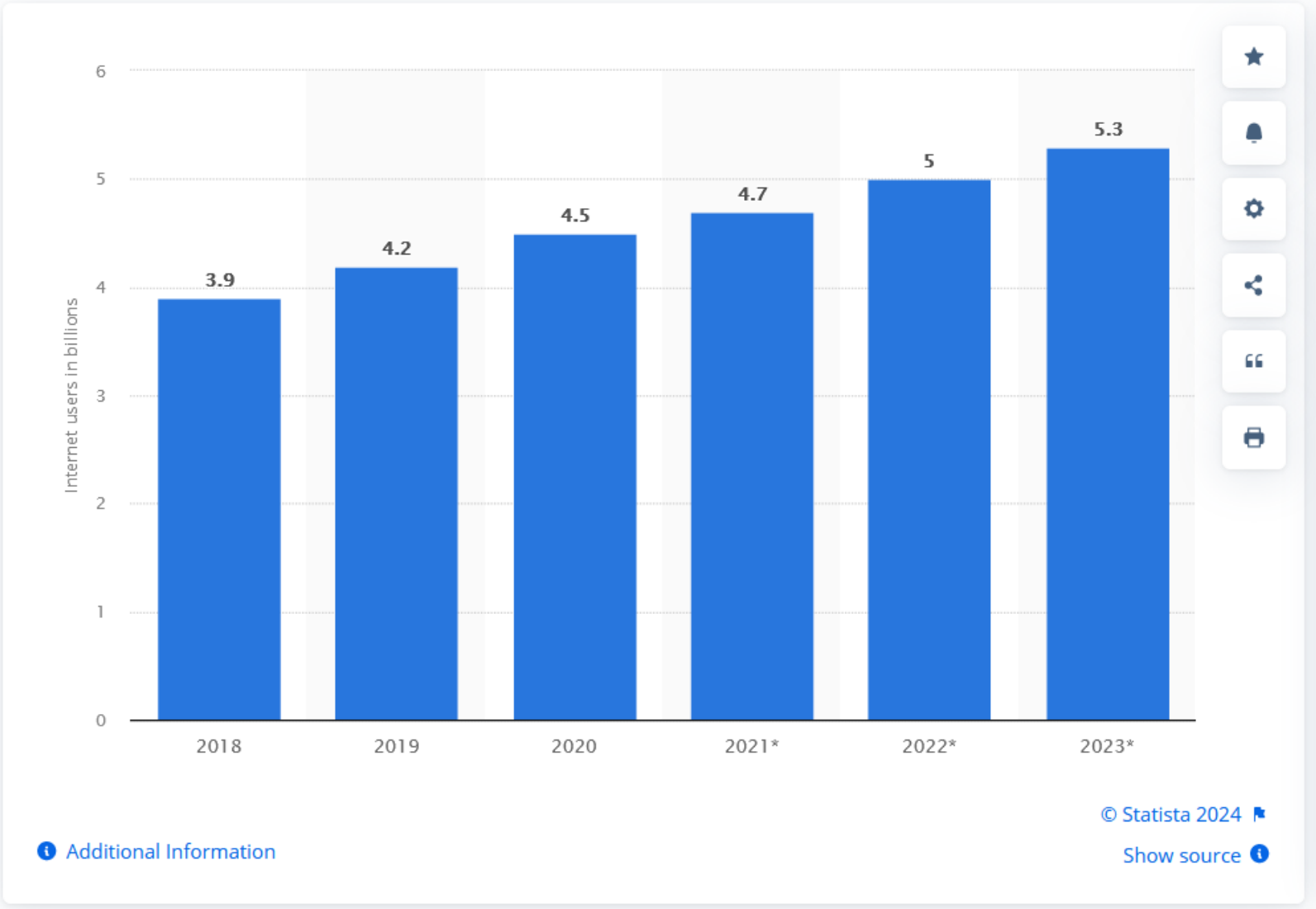


L'ERA DEI BIG DATA



UNIVERSITÀ POLITECNICA DELLE MARCHE

L'ERA DEI BIG DATA



UNIVERSITÀ POLITECNICA DELLE MARCHE

L'ERA DEI BIG DATA

- Ogni utente di Internet produce big data.
- Ogni secondo vengono effettuate circa 100,000 ricerche su Google.
- Il 91.9% delle ricerche online utilizza Google.
- Il tempo medio di utilizzo quotidiano di Internet è di 6 ore e 58 minuti.

L'ERA DEI BIG DATA

Activity	Amount of activity done in 60 seconds.
Emails sent	241 million
WhatsApp messages sent	41.6 million
Global hours spent online	25.1 million
Searches on Google	6.3 million
Facebook posts liked	4 million
Reels sent via DM on Instagram	694,000
X (Twitter) posts sent	360,000
Taylor Swift song streamed	69,400
Hours of content watched on Twitch	48,000
LinkedIn resumes submitted	6,060

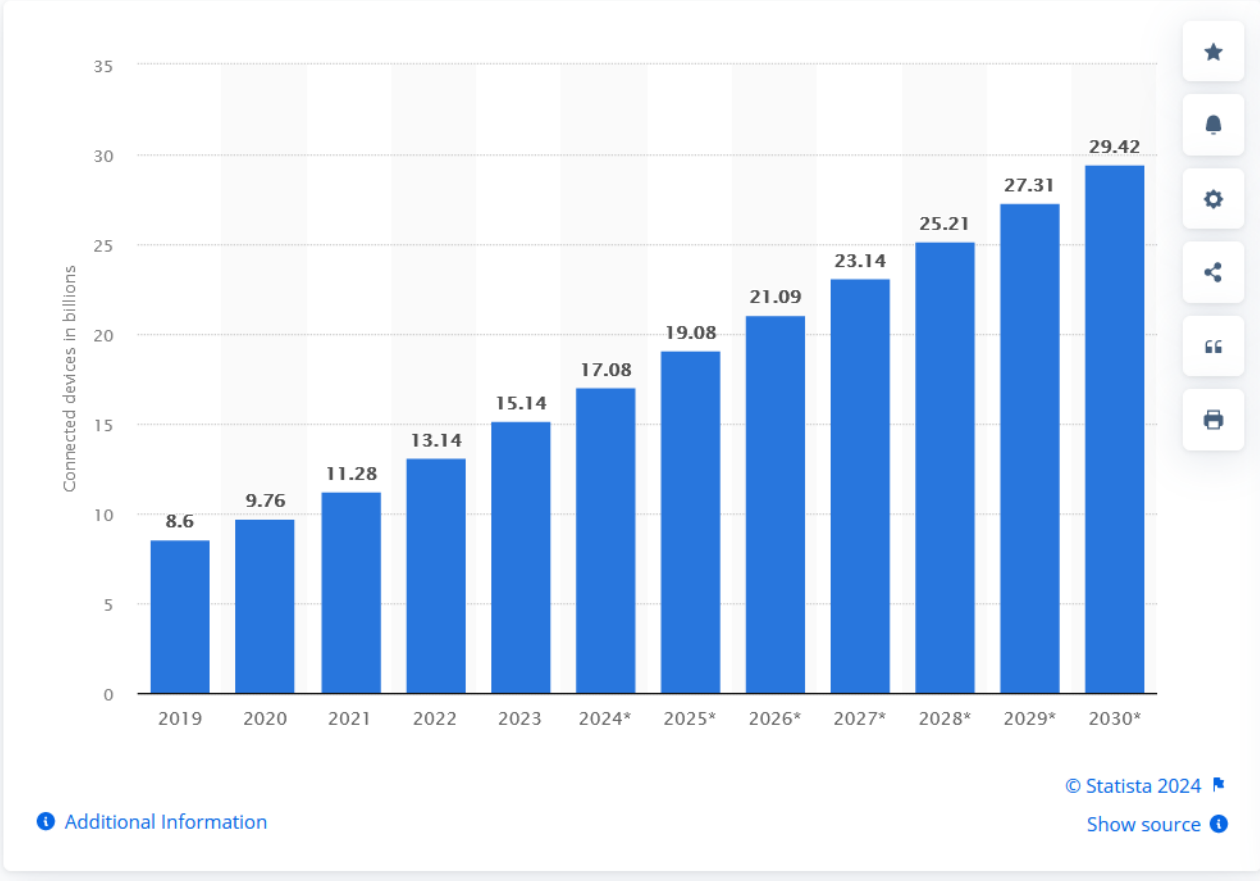
Source: Statista.

UNIVERSITÀ POLITECNICA DELLE MARCHE

L'ERA DEI BIG DATA

Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030

(in billions)

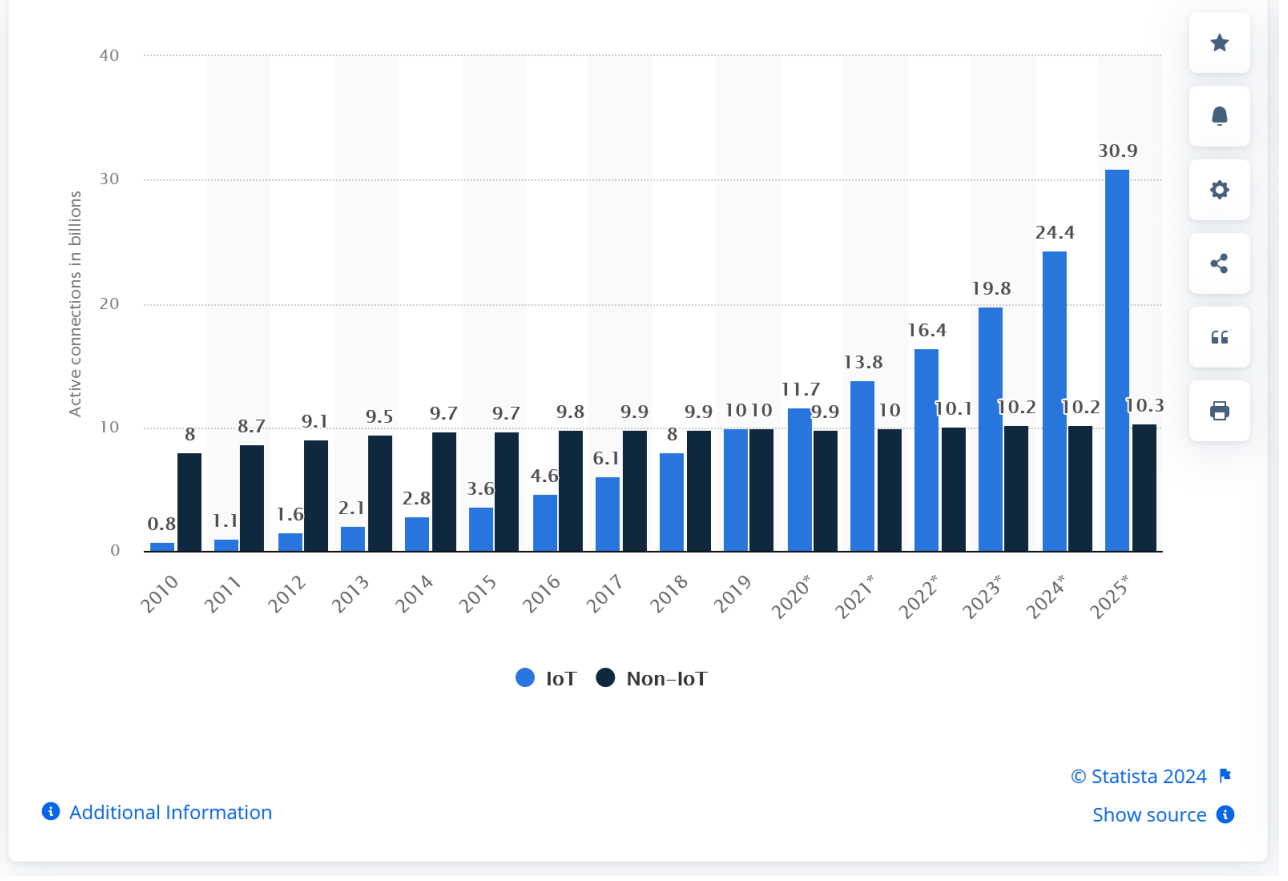


UNIVERSITÀ POLITECNICA DELLE MARCHE

L'ERA DEI BIG DATA

Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025

(in billions)



HOME AUTOMATION

UNIVERSITÀ POLITECNICA DELLE MARCHE

INDUSTRY 4.0

DATI BIOMEDICALI

DATI BIOMEDICALI

https://www.visualcapitalist.com/big-data-healthcare/

SMART OBJECTS

Corriere della Sera **Domenica 12 Novembre 2017**

CRONACHE 25

007 domestici

L'ASPIRAPOLVERE
Esistono molti robot di nuova generazione, come il Botvac D7, riescono a mappare tutta la casa. I dati possono essere condivisi con altre aziende

LA BAMBOLA
Cayla è dotata di un microfono collegabile via Bluetooth a qualsiasi smartphone nel raggio di 10 metri. In Germania è stata ritirata, perché è facilmente hackerabile: qualsiasi estraneo potrebbe ascoltare i bambini o entrare in contatto con loro

LA TV INTELLIGENTE
La smart tivù Samsung permette il riconoscimento vocale: alcuni comandi vocali possono essere trasmessi a un servizio di conversione da voce a testo fornito da terze parti

IL SEGGIOLINO CON SENSORI
BebèCare è prodotto da Chicco e Samsung: permette di controllare il bimbo dallo smartphone. Il seggiolino ha un sensore di movimento e telecamera a 360°: le informazioni potrebbero essere intercettate

CdS

Gli oggetti che ci spiano in casa

UNIVERSITÀ POLITECNICA DELLE MARCHE

SUPERFICIE DI ATTACCO

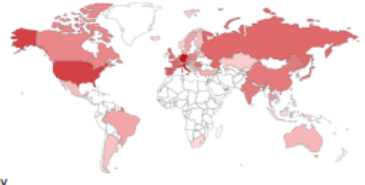
SHODAN | Original Siemens Equipment | Explore | Pricing | Enterprise Access

Exploits | Maps

TOTAL RESULTS

1,406

TOP COUNTRIES



Germany	323
Italy	192
United States	131
Spain	74
France	60

TOP ORGANIZATIONS

Digital Ocean	189
Deutsche Telekom AG	188
Envia Tel GmbH	36
Orange	28
Telefonica de Espana	15

TOP PRODUCTS

Conpot	349

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

RELATED TAGS: scada siemens iot

200.34.109.221
telelabplc.lag.itesm.mx
admin162.lag.itesm.mx
Instituto Tecnológico y de Estudios Superiores de
Added on 2019-12-09 09:46:19 GMT
Mexico, Ahumada

ics

```
Copyright: Original Siemens Equipment
PLC name: Storage Warehouse
Module type: CPU 315F-2 PN/DP
Unknown (129): Boot Loader          A
Module: 6ES7 315-2FH13-0AB0  v.0.4
Basic Firmware: v.2.6.5
Module name: CPU 315F-2 PN/DP
Serial number of module: S C-W2G100722008
Plant identification:
Basic Ha...
```

165.22.123.49
Digital Ocean
Added on 2019-12-09 09:50:55 GMT
United States, New York

honeypot cloud

```
Serial number of memory card: MMC 267FF11F
Location designation of a module:
Copyright: Original Siemens Equipment
Manufacturer and profile of a CPU module: *
PLC name: SNAP7-SERVER
Module type: CPU 315-2 PN/DP
Unknown (129): Boot Loader          A
Module: v.0.0 v.0.4
Basic Firmw...
```

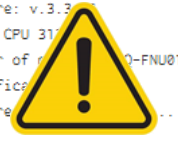
82.77.52.86
unused.static.rdsor.ro
RCS & RDS Business
Added on 2019-12-09 10:48:14 GMT
Romania, Oradea

ics

```
Copyright: Original Siemens Equipment
PLC name: osorhei11
Module type: CPU 313C
Unknown (129): Boot Loader          A%
Module: 6ES7 313-5BG04-0AB0  v.0.5
Basic Firmware: v.3.3
Module name: CPU 31
Serial number of
-FNU015662015
Plant identifica
```

Articolo 615 ter - Codice Penale

«Accesso abusivo ad un sistema informatico o telematico»



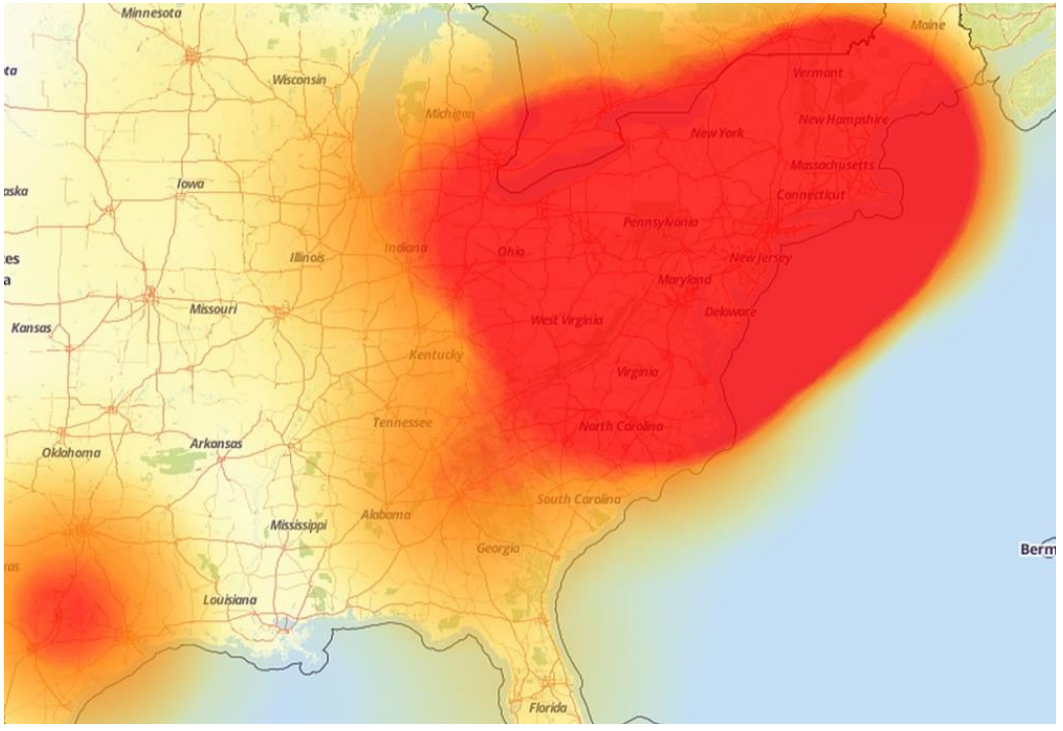
21 OTTOBRE 2016: DYN CYBERATTACK

Attacco partito da **dispositivi IoT**:

- webcam
- router domestici
- videocamere per bebé
- strumenti medici
- smart TV
- ...

Vittime:

- Twitter
- Spotify
- Cnn
- New York Times
- Financial Times
- Boston Globe
- The Guardian
- Netflix
- Airbnb
- Visa
- eBay
- Reddit
- Amazon
- …



PERDITE DELL'ORDINE DI MILIONI DI DOLLARI

Robert Page, lead penetration tester at Redscan: "The relative ease at which DDoS attacks are to execute suggests that the perpetrators are most likely **teenagers looking to cause mischief** rather than malicious state-sponsored attackers."

SECONDO RAPPORTO CLUSIT 2023 (AGGIORNAMENTO OTTOBRE 2023)

https://clusit.it/rapporto-clusit/

SECONDO RAPPORTO CLUSIT 2023

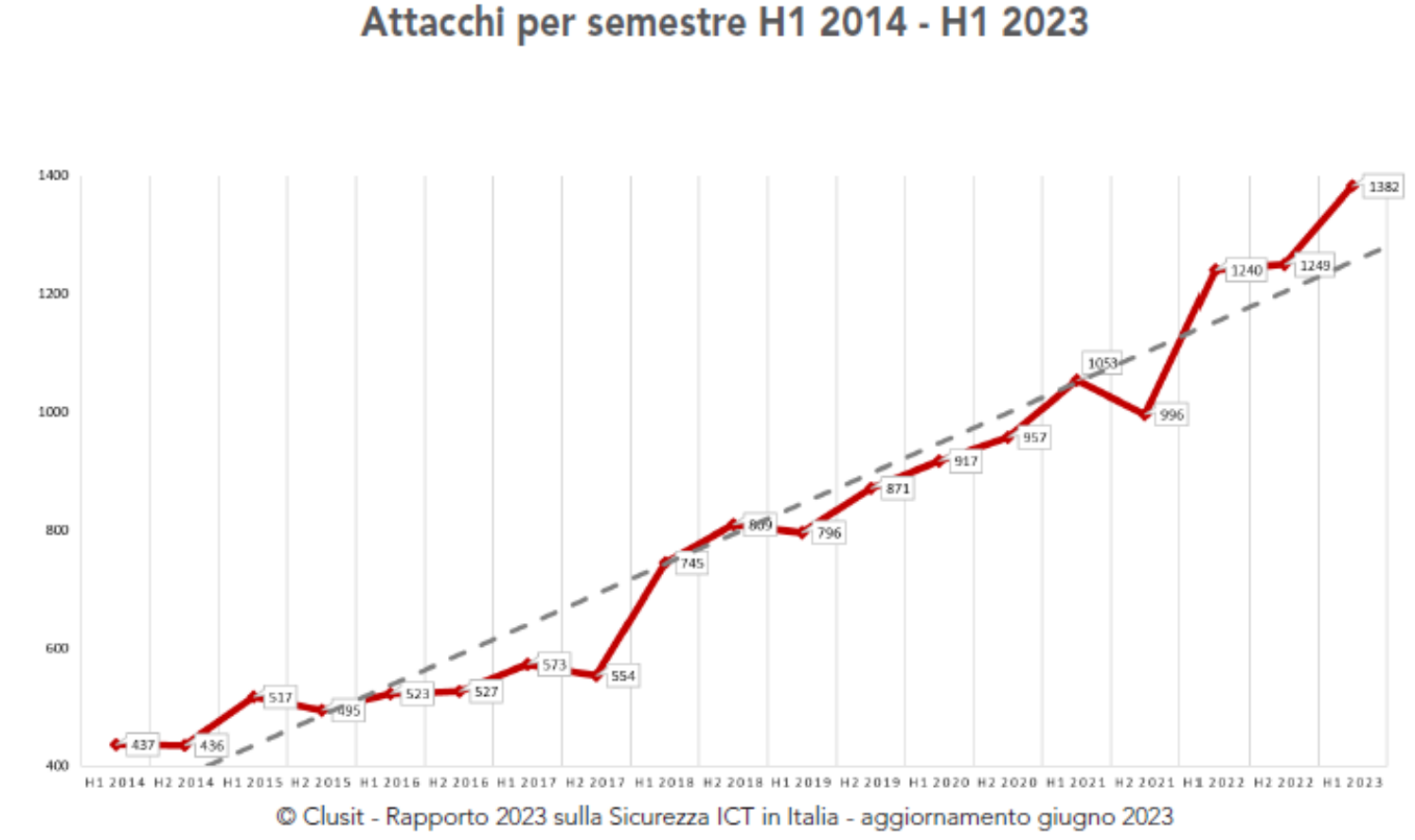


Fig. 1: *Andamento dei cyber attacchi per semestre da H1 2014 a H1 2023*

- Numero di attacchi noti <u>di particolare gravità.</u>

SECONDO RAPPORTO CLUSIT 2023

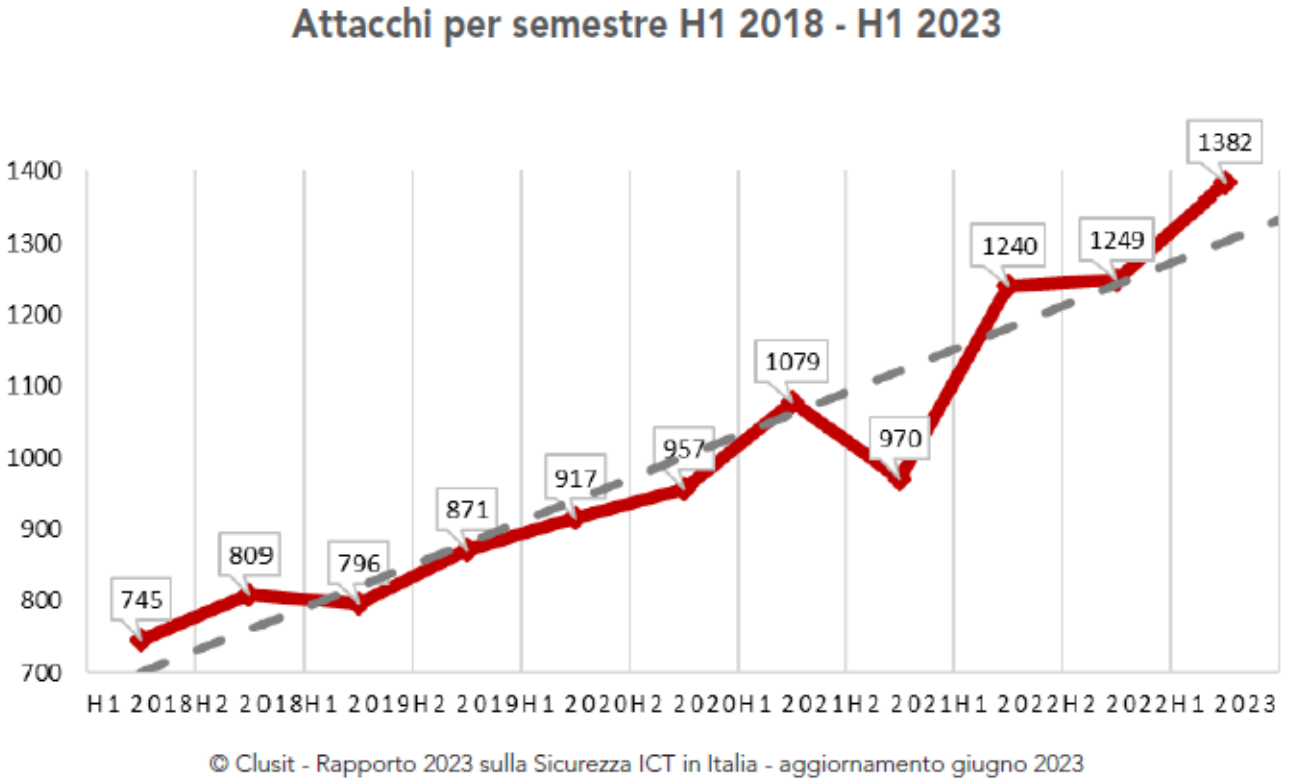


Fig. 2: *Andamento dei cyber attacchi nel periodo 2018 – H1 2023*

- Nel periodo che prenderemo in esame, tra gennaio 2018 e giugno 2023 si sono verificati un totale di 11.015 cyber attacchi gravi, suddivisi come mostrato in Fig. 2.

SECONDO RAPPORTO CLUSIT 2023

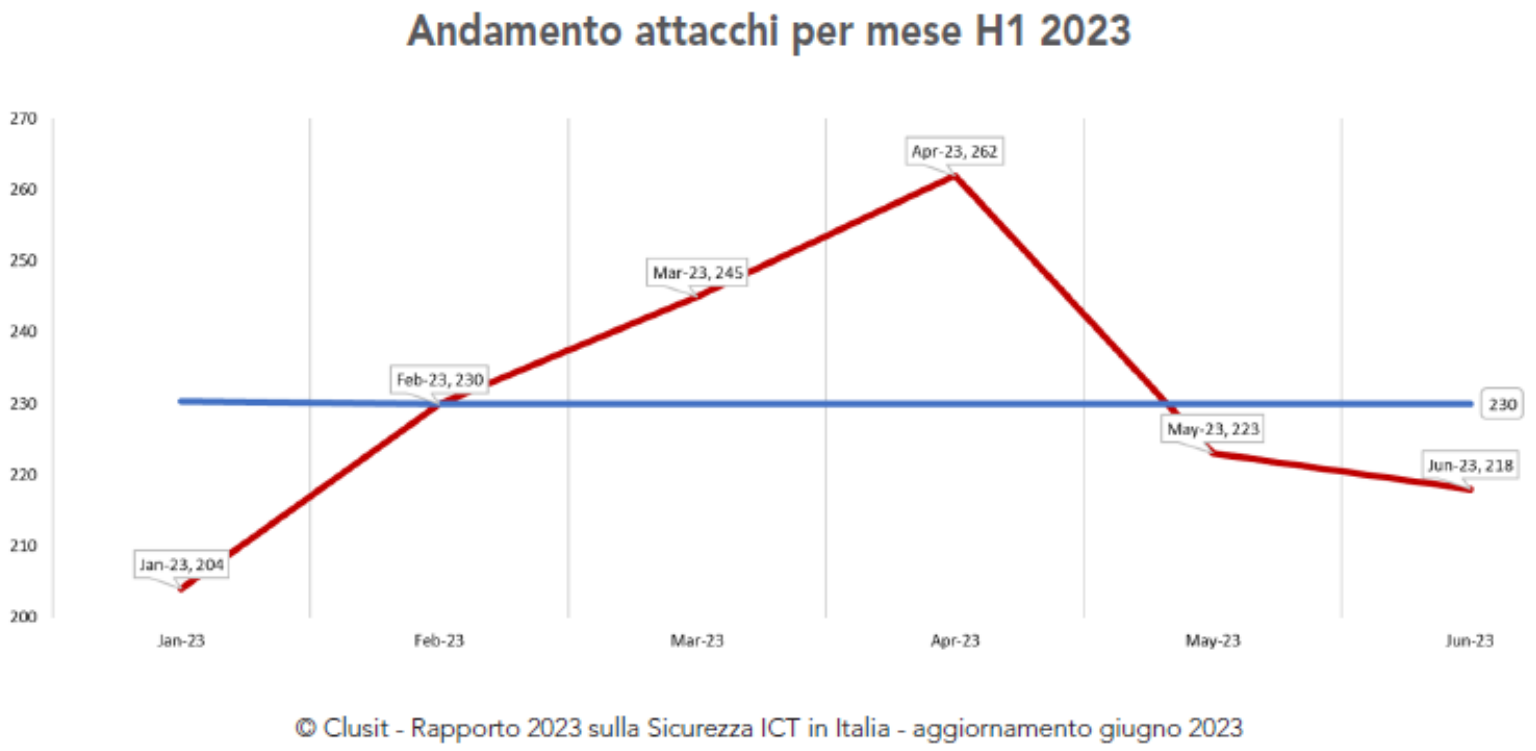


Fig. 3: *Numero di attacchi per mese nel primo semestre 2023*

SECONDO RAPPORTO CLUSIT 2023

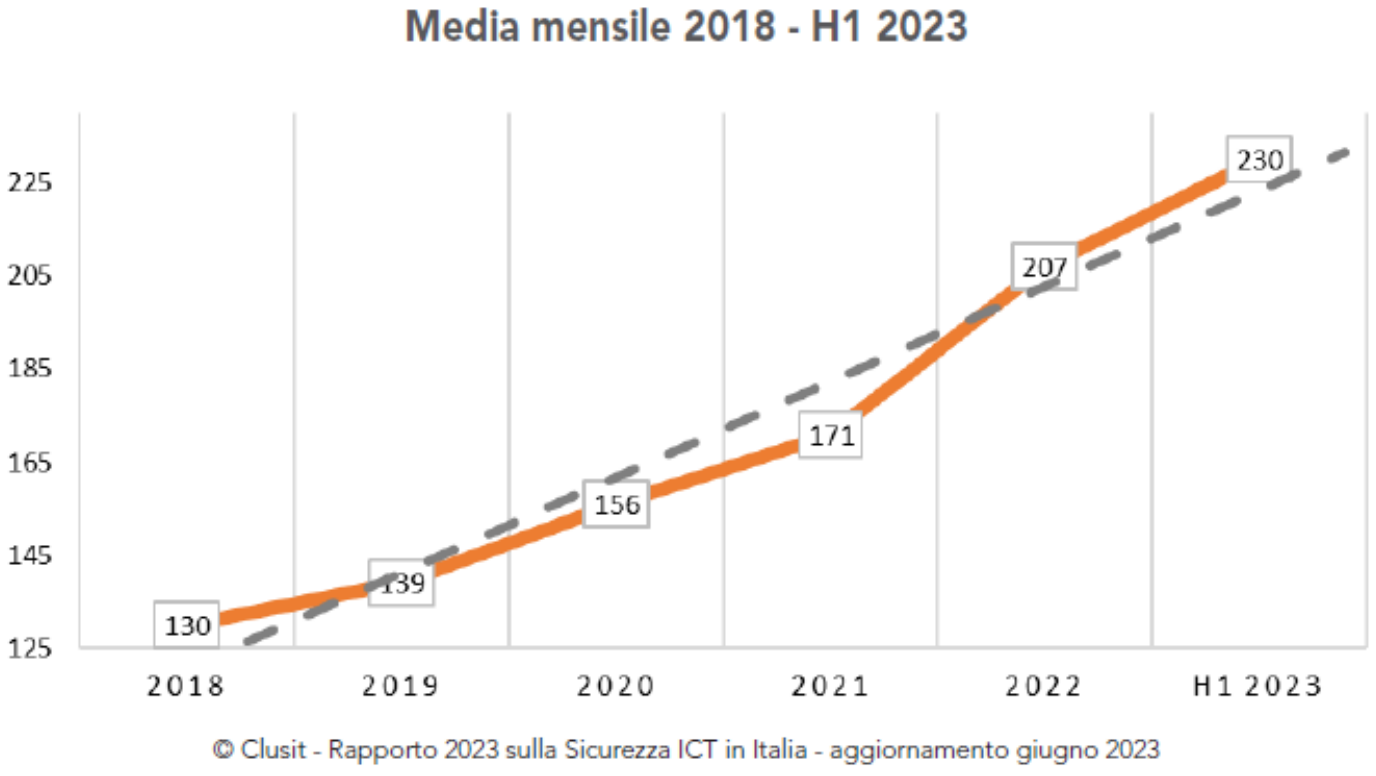


Fig. 4: *Andamento delle medie mensili nel periodo 2018-H1 2023*

HACKER

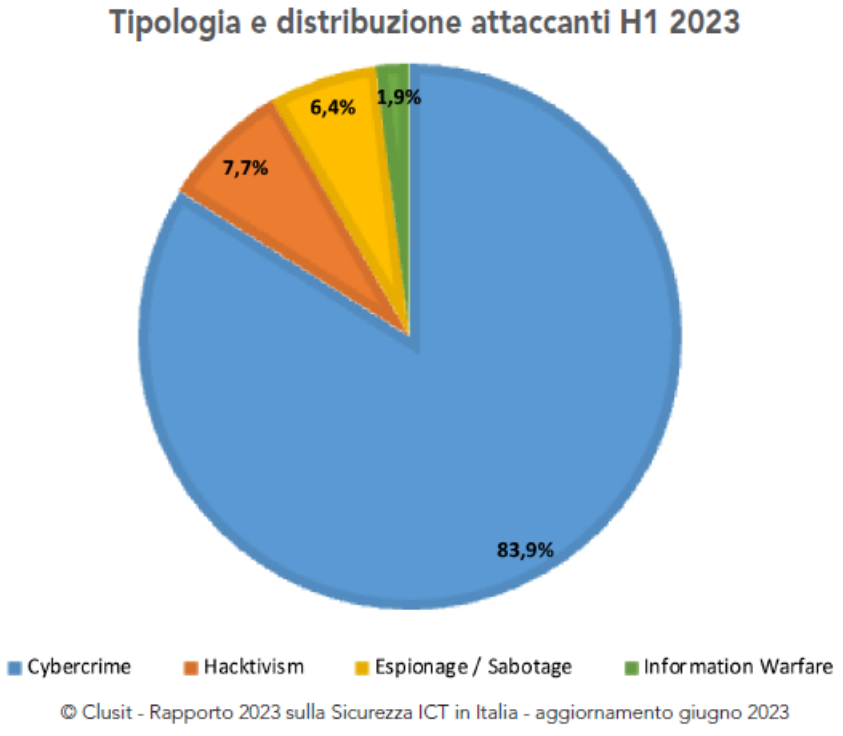
- **Definizione originale:** Qualcuno con una conoscenza approfondita del mondo dei computer e dell'informatica – e di conseguenza in grado di entrare nelle profondità del sistema.

HACKER

- **Black hat hacker (Cracker):** hacker attivamente impegnato in qualsiasi tipo di operazione criminale informatica. Il suo obiettivo è ottenere un guadagno economico tramite azioni di cyberspionaggio o altri scopi dannosi per le organizzazioni.
- **White hat hacker (Hetical hacker):** conduce test e attacchi a siti Web e ai software per identificare possibili falle. Una volta rilevate le criticità, il white hat invia le notifiche direttamente al fornitore (o a un CERT), in modo che questo possa rilasciare una patch per correggere il difetto.
- **Grey hat hacker:** opera in un regime di ambiguità etica. In sintesi, non compromette i sistemi con l'obiettivo malevolo di rubare dati ma è disposto a usare anche metodi illegali per trovare difetti o per rendere pubbliche le vulnerabilità o, ancora, vendere exploit zero-day ai governi o alle agenzie di intelligence.

TIPOLOGIE DI ATTACCHI

- **Cyber crime**
  - Crimine commesso via computer, reti o dispositivi hardware
- **Cyber espionage**
  - Attività volta ad ottenere informazioni industriali e commerciali da aziende competitor in maniera illecita
- **Hacktivism**
  - Hacking per scopi politici o sociali
- **Information warfare**
  - Uso di tecnologie informatiche per assumere posizioni di vantaggio nell'ambito di un conflitto (dichiarato o sommerso)



DISTRIBUZIONE DELLE VITTIME PER CATEGORIA

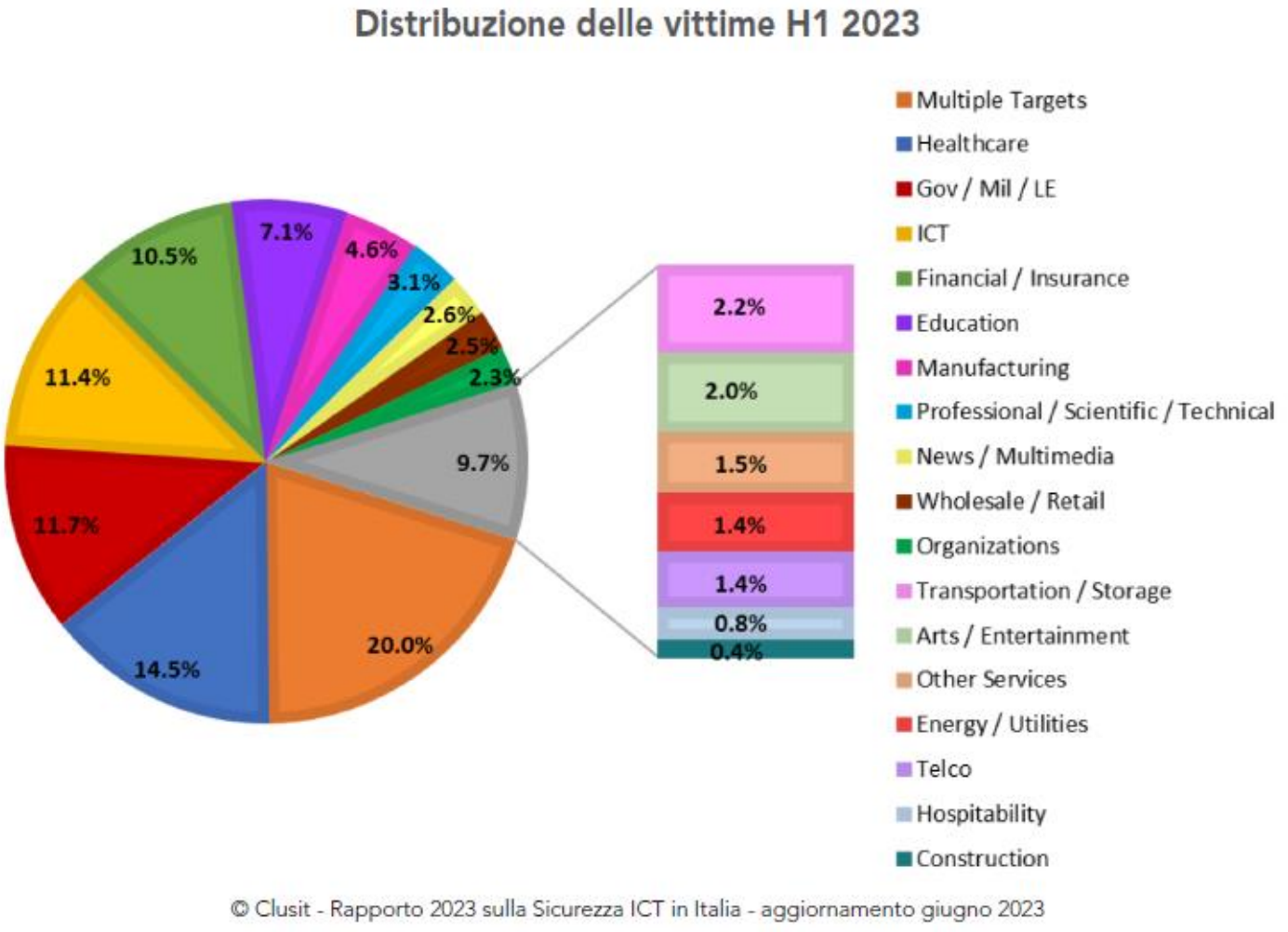
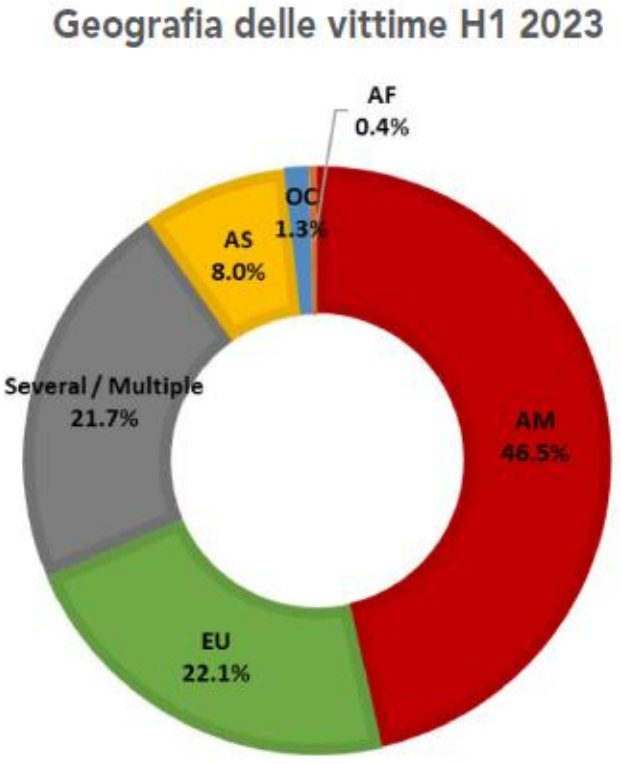


Fig. 7: *Andamento percentuale della tipologia di vittime nel primo semestre 2023*

DISTRIBUZIONE DELLE VITTIME PER AREA GEOGRAFICA



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia - aggiornamento giugno 2023

Fig. 10: *Distribuzione geografica delle vittime nel primo semestre 2023*

UNIVERSITÀ POLITECNICA DELLE MARCHE

DISTRIBUZIONE DELLE TECNICHE DI ATTACCO

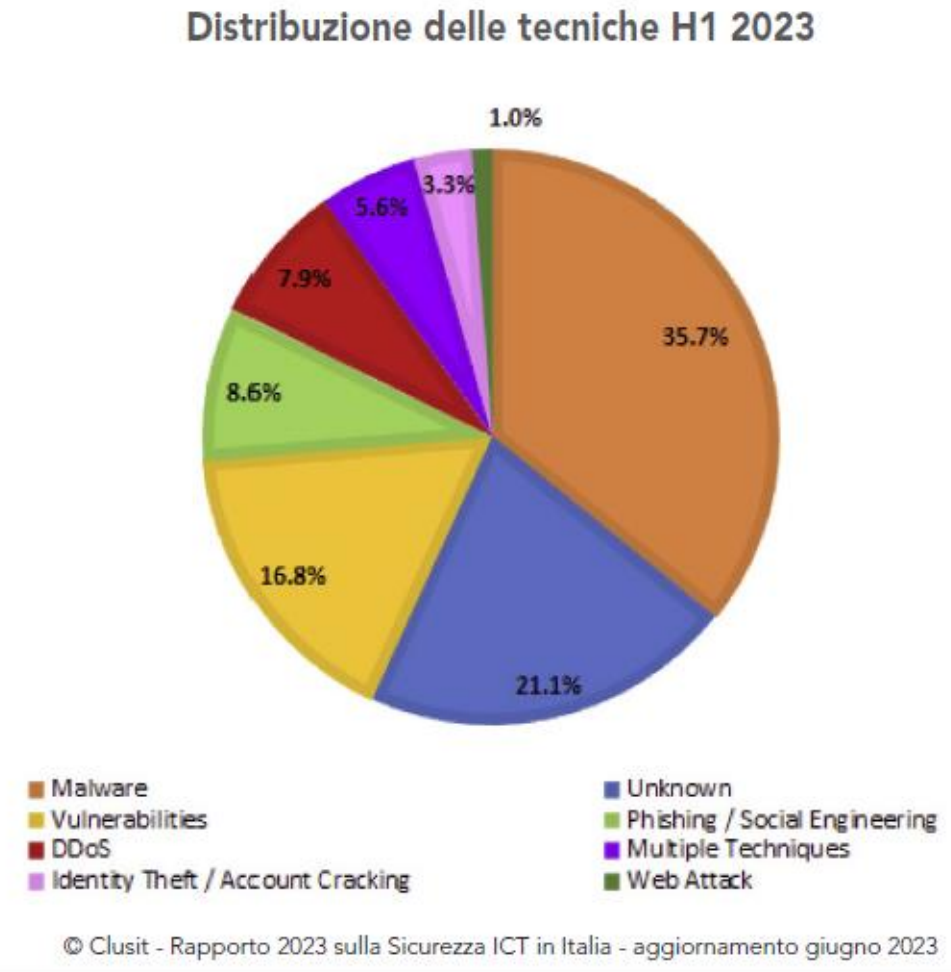
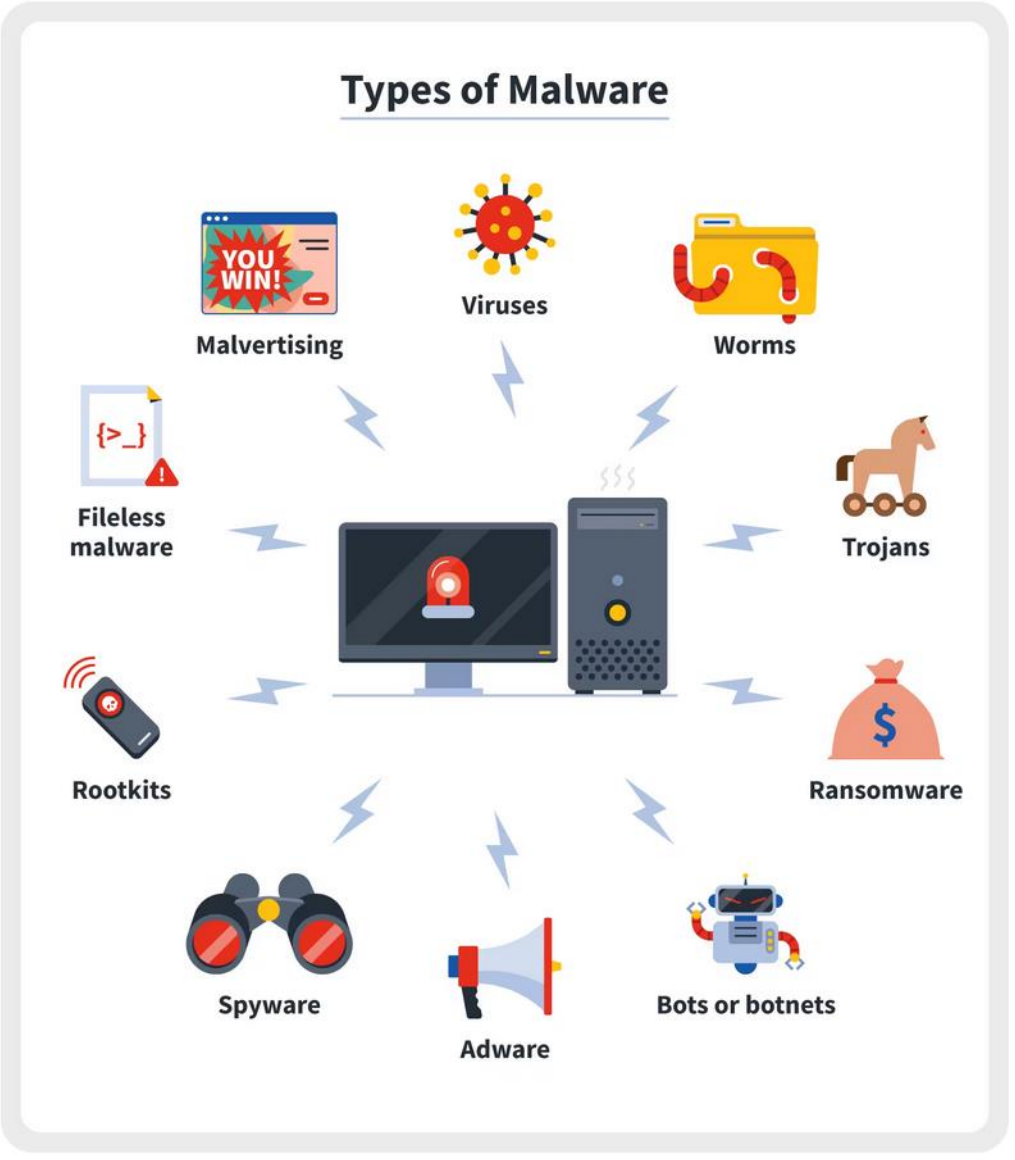
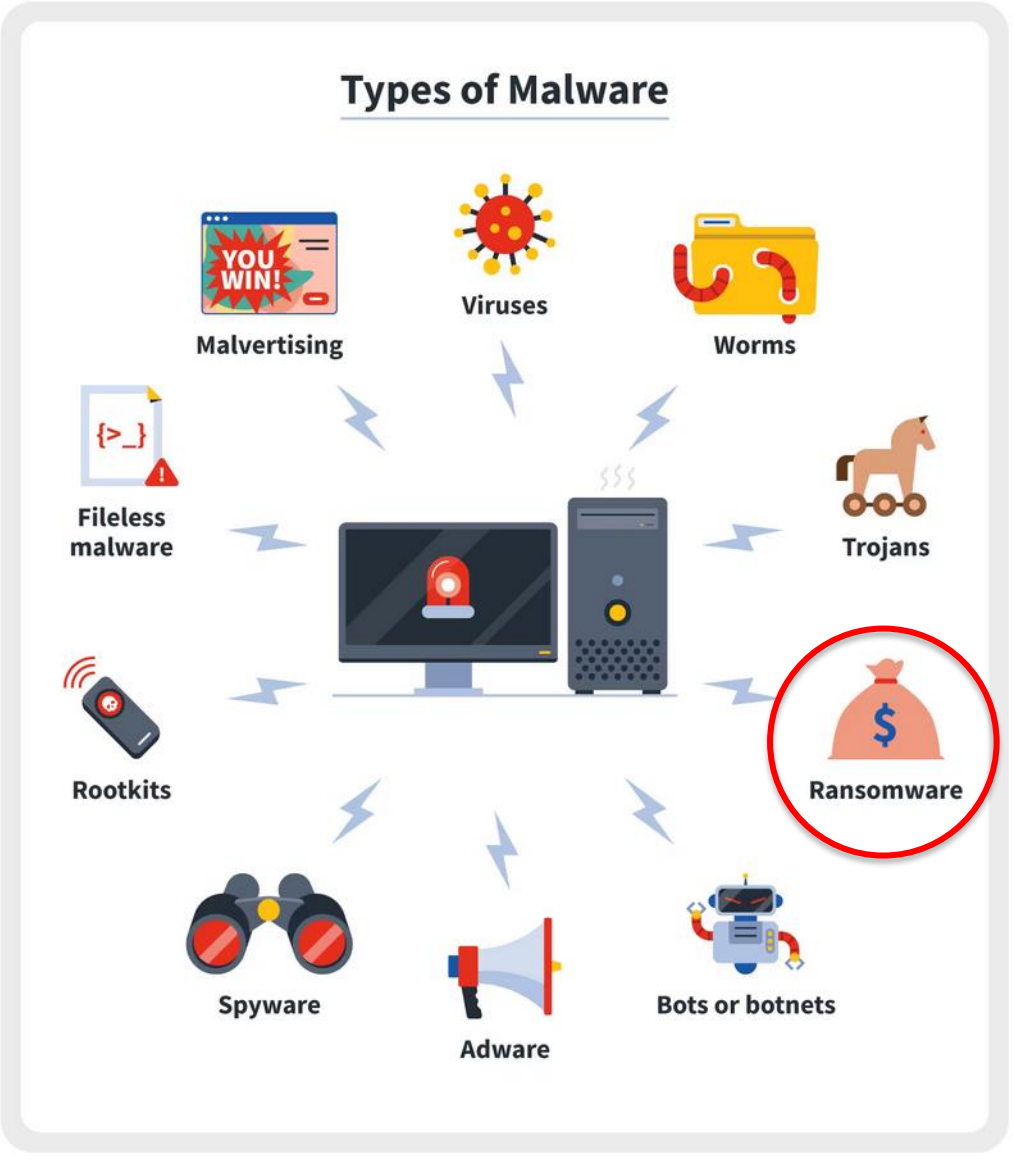


Fig. 11: *Distribuzione delle tecniche di attacco nel primo semestre 2023*


Types of Malware
YOU WIN!
Malvertising
Viruses
Worms
{>_}
Fileless malware
Trojans
Rootkits
Ransomware
Spyware
Adware
Bots or botnets


Types of Malware
YOU WIN!
Malvertising
Viruses
Worms
{>_}
Fileless malware
Trojans
Rootkits
Ransomware
Spyware
Adware
Bots or botnets

«SEVERITY» DEGLI ATTACCHI

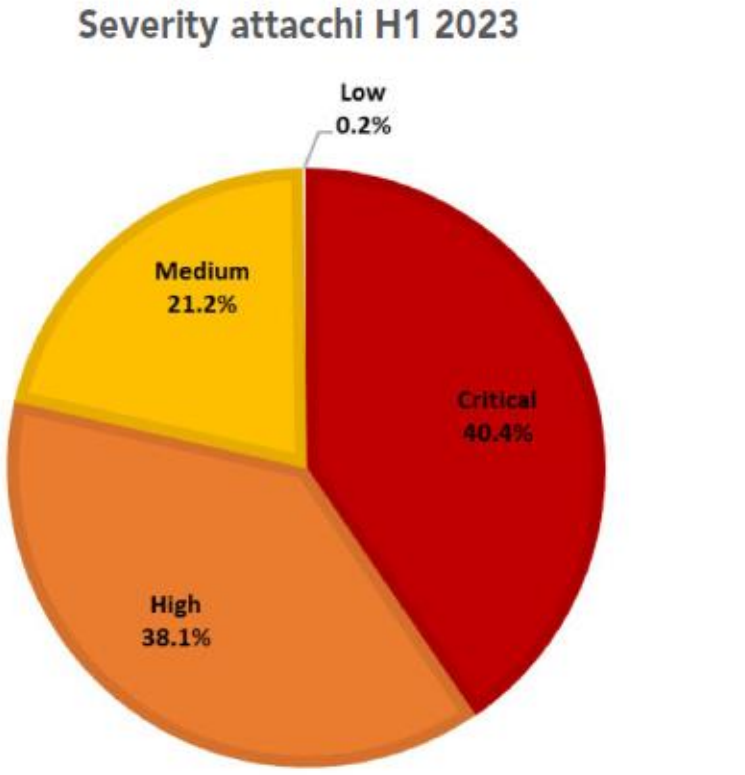


Fig. 14: *Distribuzione della Severity nel H1 2023*

UNIVERSITÀ POLITECNICA DELLE MARCHE

«SEVERITY» DEGLI ATTACCHI

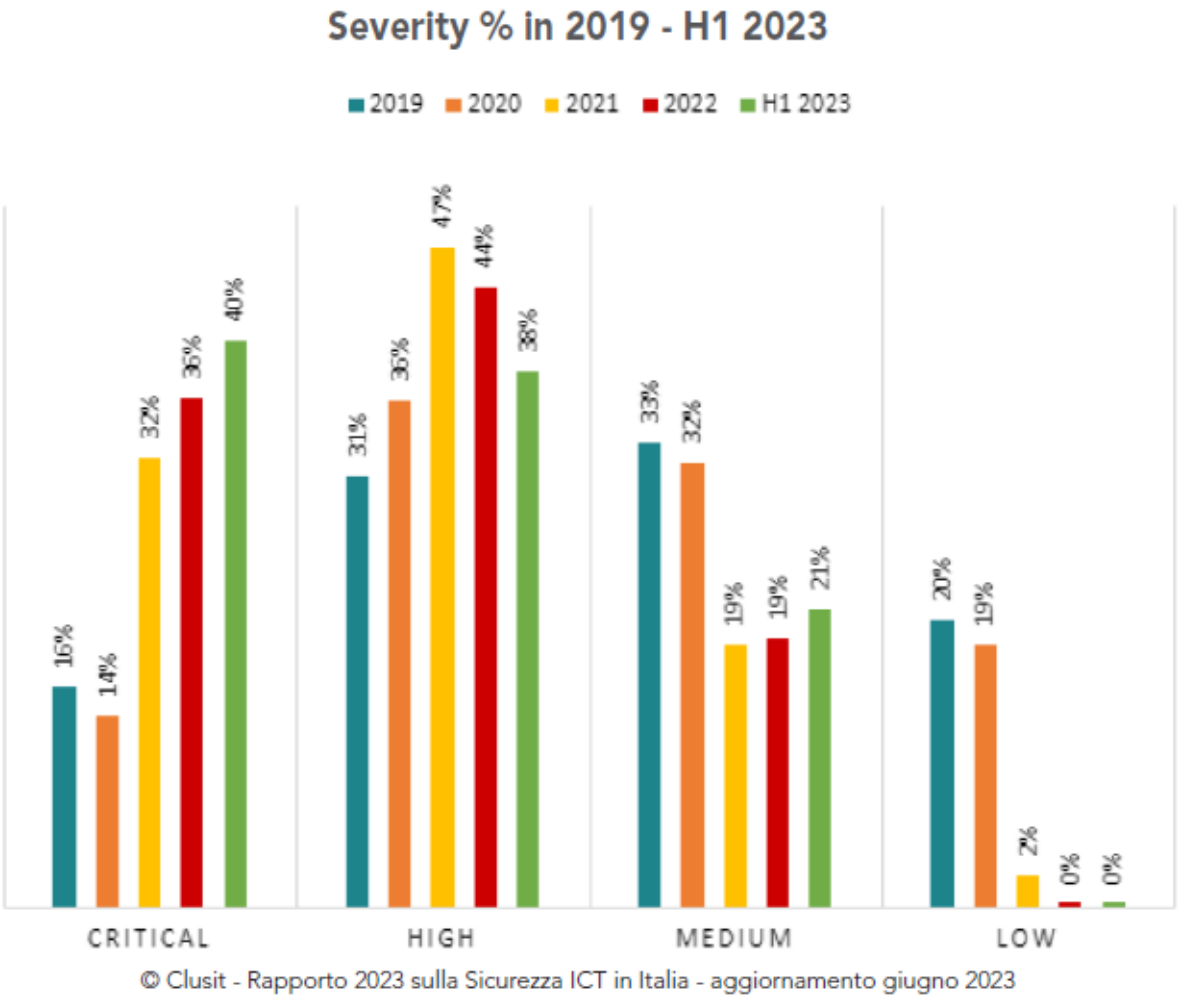


Fig. 13: *Andamento percentuale della Severity degli attacchi nel periodo 2019-H1 2023*

SEVERITY PER TIPOLOGIA DI ATTACCANTE

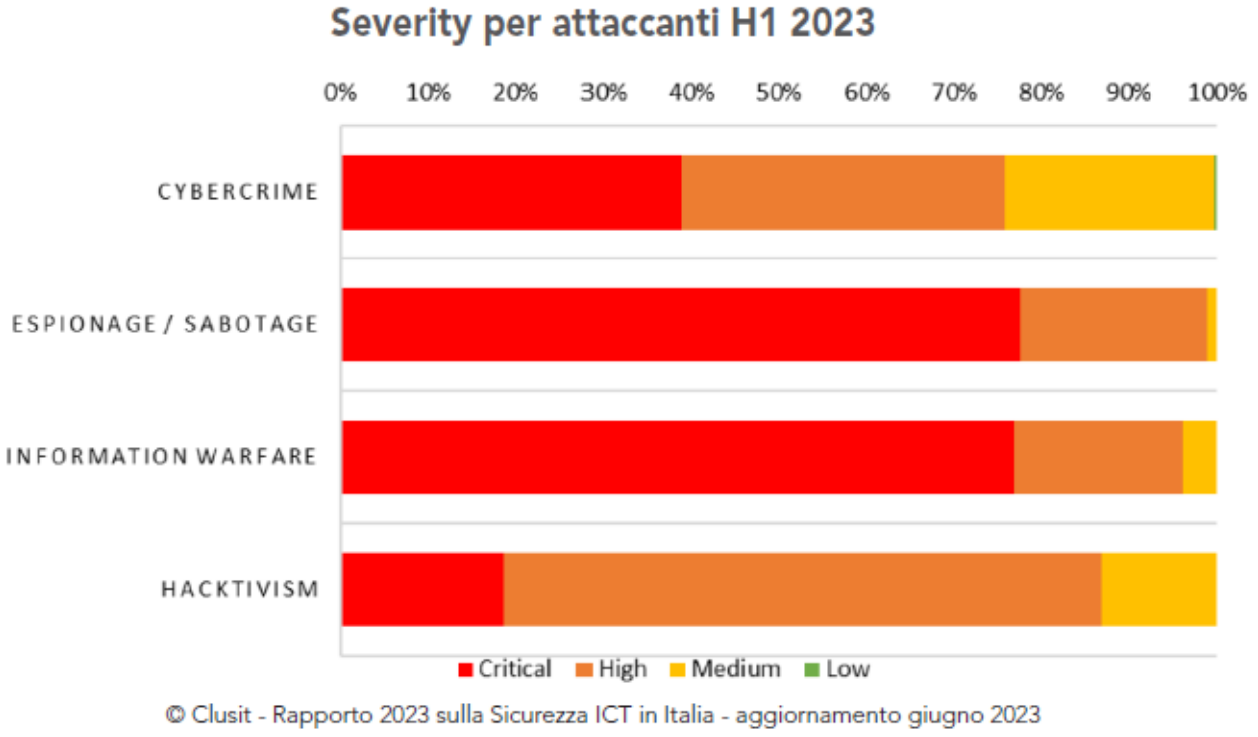


Fig. 15: *Distribuzione della Severity per attaccanti nel primo semestre 2023*

SEVERITY PER TECNICHE DI ATTACCO

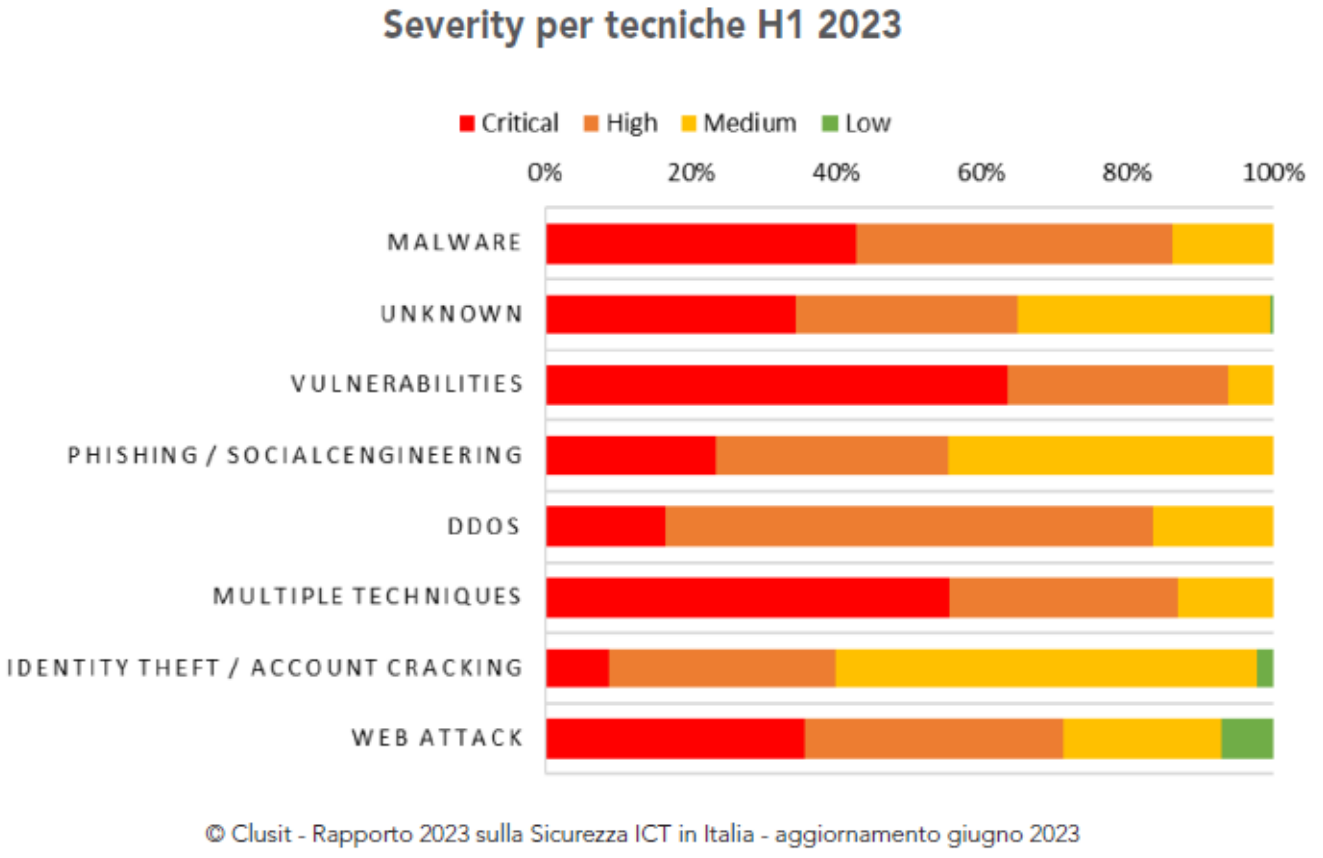


Fig. 19: *Distribuzione della Severity per tecniche di attacco nel primo semestre 2023*

ANALISI DEGLI ATTACCHI IN ITALIA

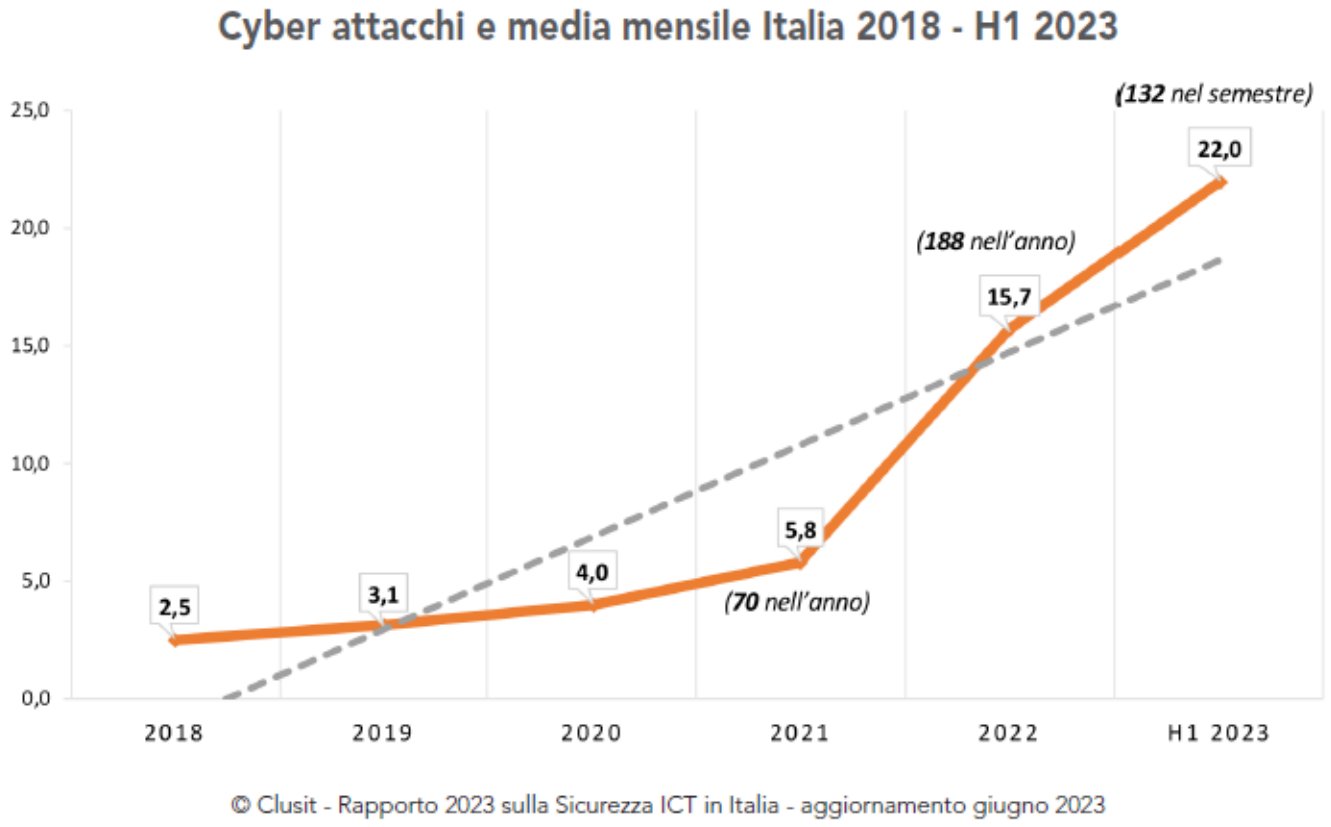


Fig. 21: *Distribuzione dei cyber attacchi e media mensile in Italia nel periodo 2018-H1 2023*

UNIVERSITÀ POLITECNICA DELLE MARCHE

ANALISI DEGLI ATTACCHI IN ITALIA

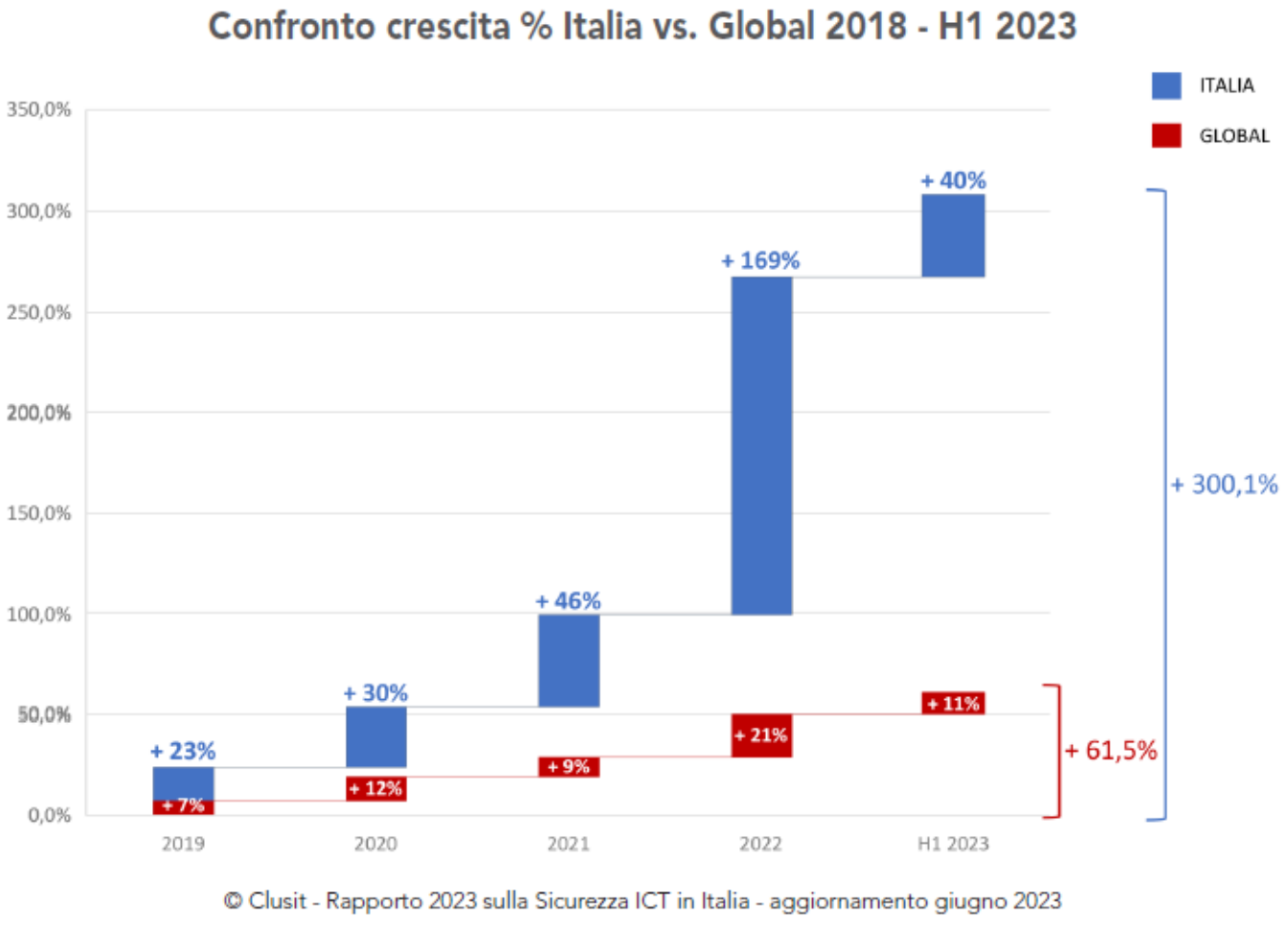


Fig. 22: *1Confronto crescita percentuale Italia vs. Global nel periodo 2018-H1 2023*

Analisi degli attacchi in Italia: Distribuzione delle vittime per categoria

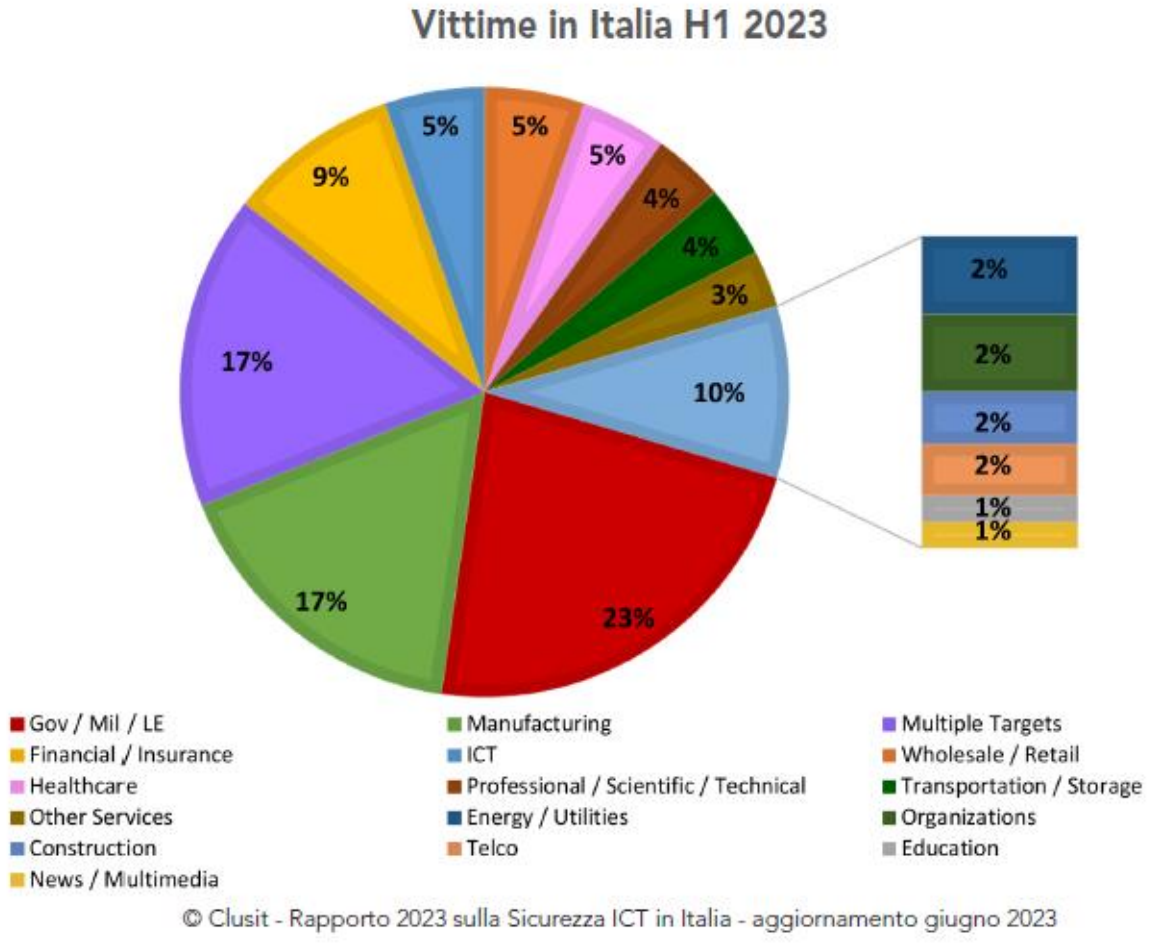


Fig. 26: *Distribuzione delle vittime in Italia nel primo semestre 2023*

Analisi degli attacchi in Italia: Distribuzione delle tecniche di attacco

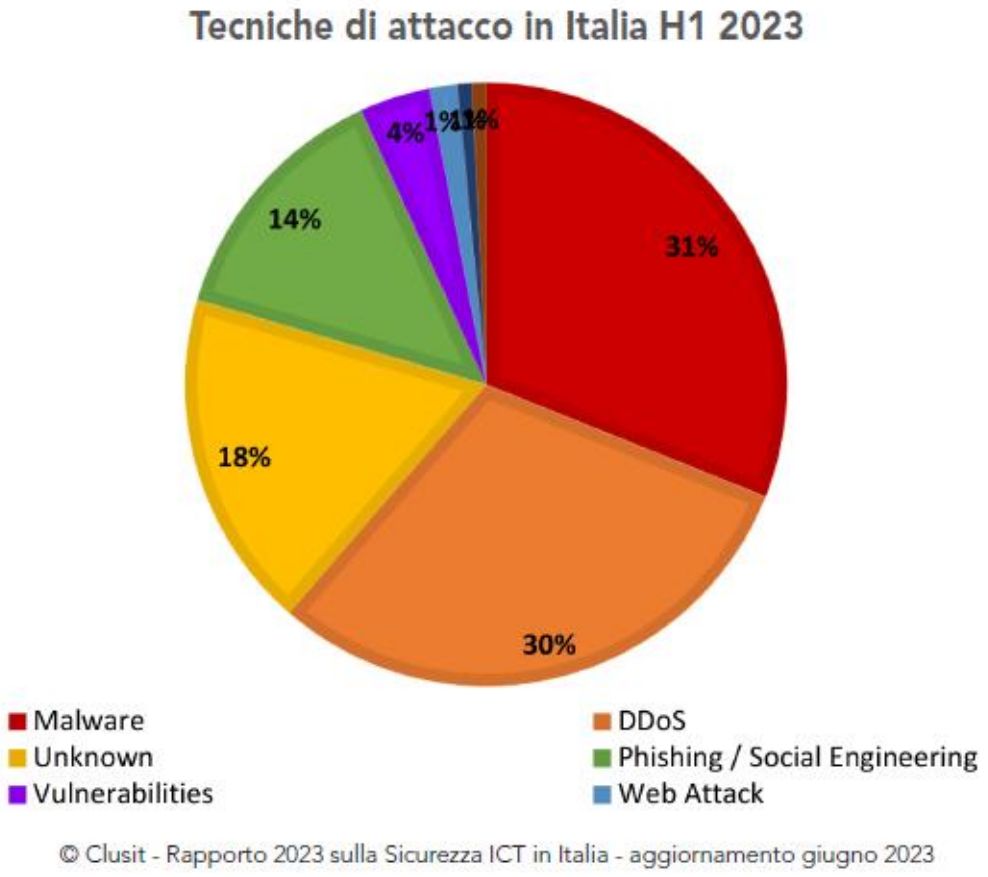
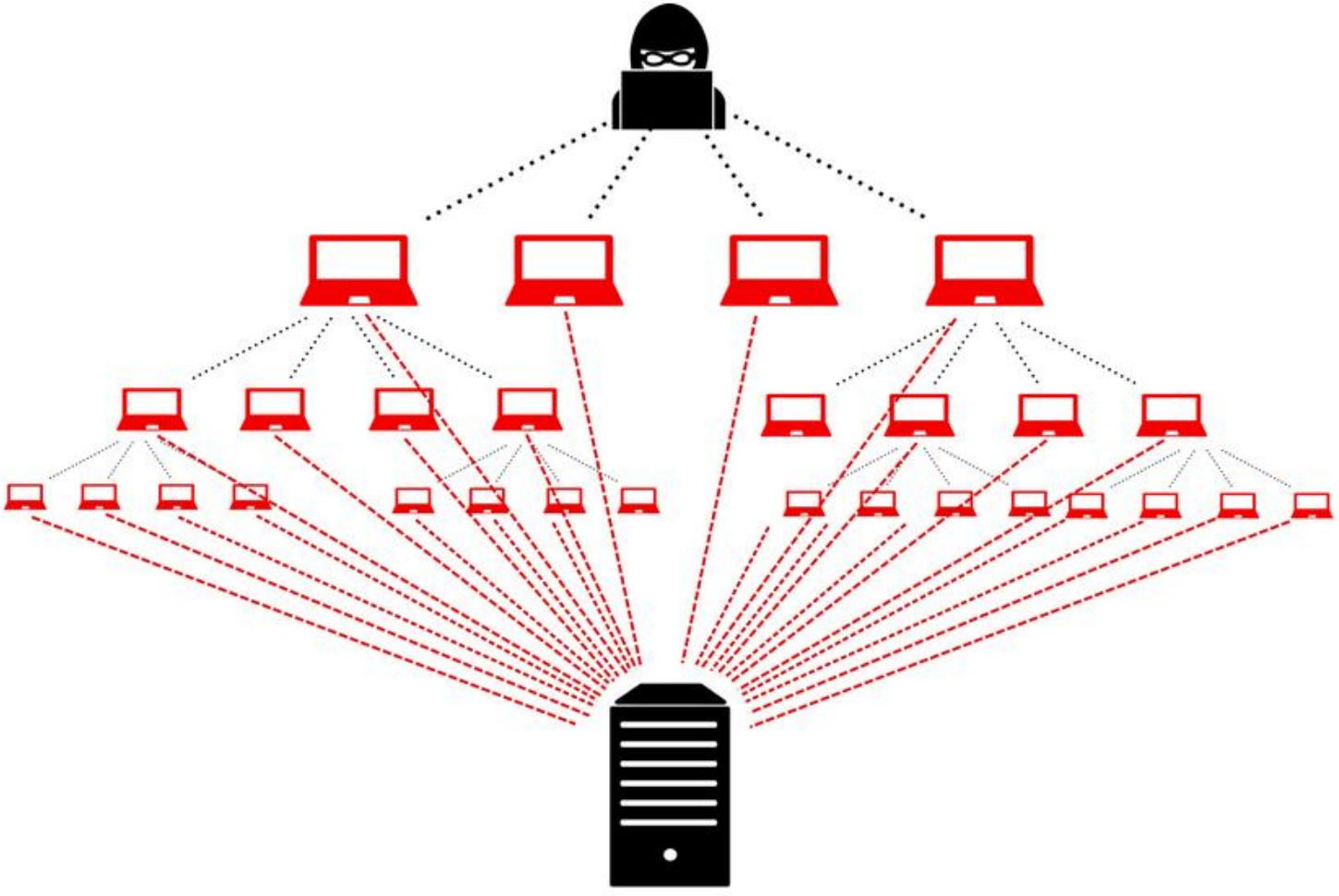


Fig. 28: *Tecniche di attacco in Italia nel primo semestre 2023*

UNIVERSITÀ POLITECNICA DELLE MARCHE

ATTACCHI DDOS



DDoS attack creation

ANALISI DEGLI ATTACCHI IN ITALIA: DISTRIBUZIONE DELLE TECNICHE DI ATTACCO

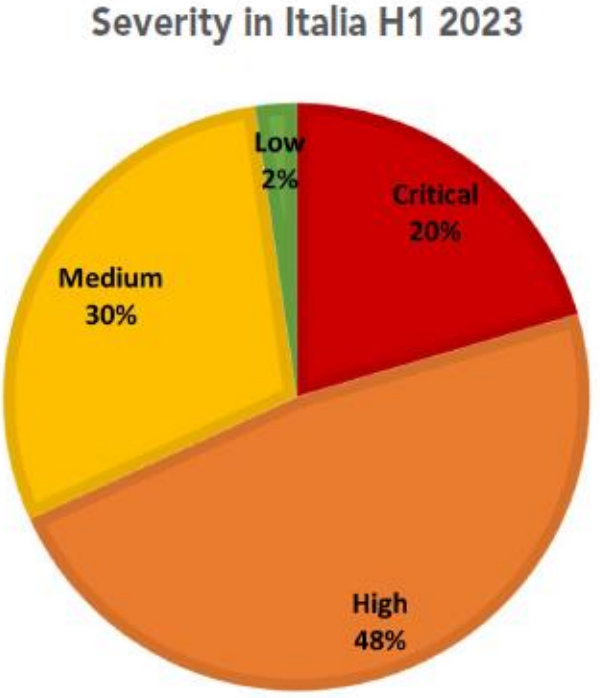
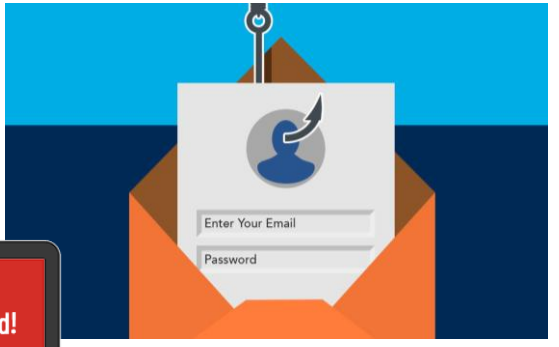


Fig. 30: *Severity degli attacchi in Italia nel primo semestre 2023*

- Dall'analisi dei dati, possiamo concludere che in Italia sono aumentati gli attacchi "di disturbo", con severity limitata, che riescono però sempre più spesso ad andare a buon fine.

EVOLUZIONE DEGLI ATTACCHI

- Phishing (bulk/spear)



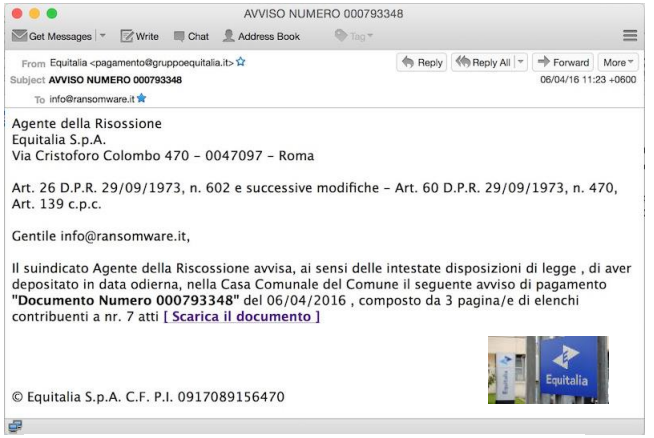
- Ransomware

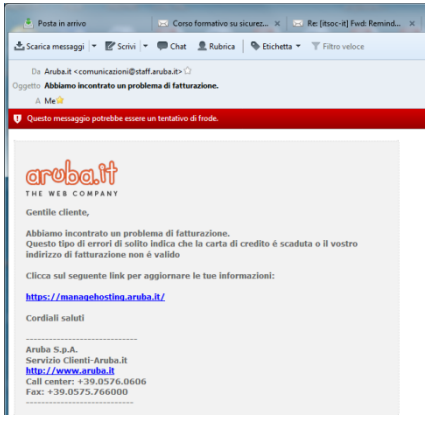
- Social engineering

- Phone hacking

PHISHING

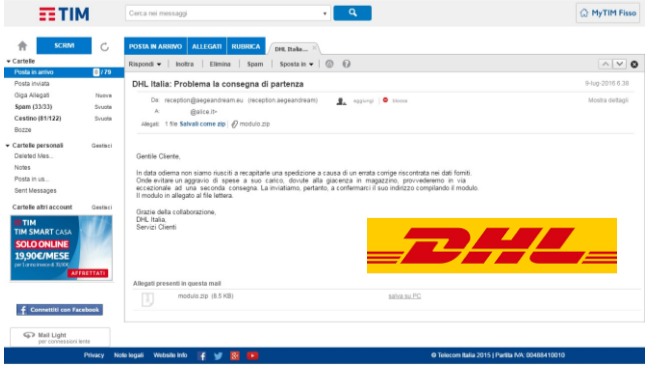

Enel
ENEL SERVIZIO ELETTRICO - Servizio di Maggior Tutela
DATI CLIENTE
Numero cliente: 566 880 539
Codice Fiscale: ZDRW641 4UHQ
BOLLETTA PER LA FORNITURA DI ENERGIA ELETTRICA
N. fattura 19591426 del 6/07/2016 Bimestre giugno-luglio 2016
Totale da pagare entro il 31/05/2016: euro 497,32
DATI FORNITURA
RIEPILOGO IMPORTI FATTURATI

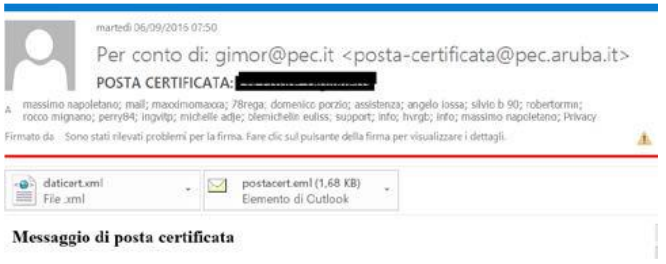

AVVISO NUMERO 000793348
From Equitalia <pagamento@gruppoequitalia.it>
Subject AVVISO NUMERO 000793348
To info@ransomware.it
06/04/16 11:23 +0600
Agente della Risossione
Equitalia S.p.A.
Via Cristoforo Colombo 470 - 0047097 - Roma
Art. 26 D.P.R. 29/09/1973, n. 602 e successive modifiche - Art. 60 D.P.R. 29/09/1973, n. 470, Art. 139 c.p.c.
Gentile info@ransomware.it,
Il suindicato Agente della Riscossione avvisa, ai sensi delle intestate disposizioni di legge , di aver depositato in data odierna, nella Casa Comunale del Comune il seguente avviso di pagamento "Documento Numero 000793348" del 06/04/2016 , composto da 3 pagina/e di elenchi contribuenti a nr. 7 atti [Scarica il documento]
Equitalia
© Equitalia S.p.A. C.F. P.I. 0917089156470


aruba.it
THE WEB COMPANY
Gentile cliente,
Abbiamo incontrato un problema di fatturazione.
Questo tipo di errori di solito indica che la carta di credito è scaduta o il vostro indirizzo di fatturazione non è valido
Clicca sul seguente link per aggiornare le tue informazioni:
https://managehosting.aruba.it/
Cordiali saluti
Aruba S.p.A.
Servizio Clienti-Aruba.it
http://www.aruba.it
Call center: +39.0576.0606
Fax: +39.0575.766000


Recapito Elettronico Fattura
Ti inviamo in allegato il Conto Telefonico Completo all'interno del quale puoi trovare la Fattura nr.
dell'importo di 146,16euro.
Ti ricordiamo che puoi scaricare il tuo Conto Telefonico Completo nella sezione "190 Fai da te" del sito www.vodafone.it (scopri come).
Per maggiori informazioni sulle voci del tuo Conto Telefonico visita la sezione dedicata su www.vodafone.it.
Cordiali Saluti.
Servizio Clienti Vodafone


TELECOM
TIM
Gentile
ti informiamo che la tua fattura TIM di Giugno 2016 relativa alla linea è stata appena emessa ed è disponibile online.
Si prega di scaricare il fattura
Ti ricordiamo che in MyTIM Fisso nella sezione Il mio profilo puoi richiedere di ricevere la fattura TIM esclusivamente online. Risparmierai così le spese di spedizione postale.
Ti aspettiamo presto su www.tim.it
Grazie
Servizio Clienti tim.it
Attenzione:ti invitiamo a non rispondere a questo messaggio: questa casella di posta elettronica non è abilitata alla ricezione.


TIM
DHL Italia: Problema la consegna di partenza
DHL
TIM SMART CASA
SOLO ONLINE
19,90€/MESE


martedì 06/09/2016 07:50
Per conto di: gimor@pec.it <posta-certificata@pec.aruba.it>
POSTA CERTIFICATA:
daticert.xml
File .xml
postacert.eml (1,68 KB)
Elemento di Outlook
Messaggio di posta certificata

SOCIAL ENGINEERING

1. **Phishing**
2. **Pretexting**

   Il criminale contatta la vittima telefonicamente simulando una situazione particolare (creazione di un pretesto). Per esempio, si finge un dipendente bancario o di un ufficio pubblico e cerca di instaurare una relazione di empatia con la vittima, in modo da ottenere le informazioni di cui ha bisogno.

3. **Baiting**

   Questa tecnica adesca le vittime sfruttando la loro curiosità: l'hacker utilizza una vera e propria "esca", lasciando incustodito un supporto di memorizzazione (chiavette USB, cd, hard disk, …) contenente codice maligno. L'obiettivo è indurre la vittima, spinta dalla curiosità, a inserire il dispositivo nel proprio computer, dando così all'hacker l'accesso all'intera rete aziendale.

CYBER2PHYSICAL

4. **Trashing**

   I criminali cercano informazioni sensibili setacciando la spazzatura delle vittime alla ricerca di bollette, estratti conto e altri documenti contenenti dati sensibili. Un altro obiettivo degli hacker possono essere anche sistemi dismessi come smartphone, laptop o dispositivi USB guasti che, se non opportunamente resettati, possono essere fonti di informazioni preziose.

5. **Quid pro quo**

   Questo metodo prevede che il social engineer offra un servizio o un aiuto in cambio di un benefit. Per esempio, il malintenzionato può fingersi un tecnico IT e contattare alcuni dipendenti per offrire loro supporto tecnico in cambio di informazioni (ad es: PW) oppure chiedendo loro di disattivare temporaneamente l'antivirus in modo da installare un programma contenente malware.

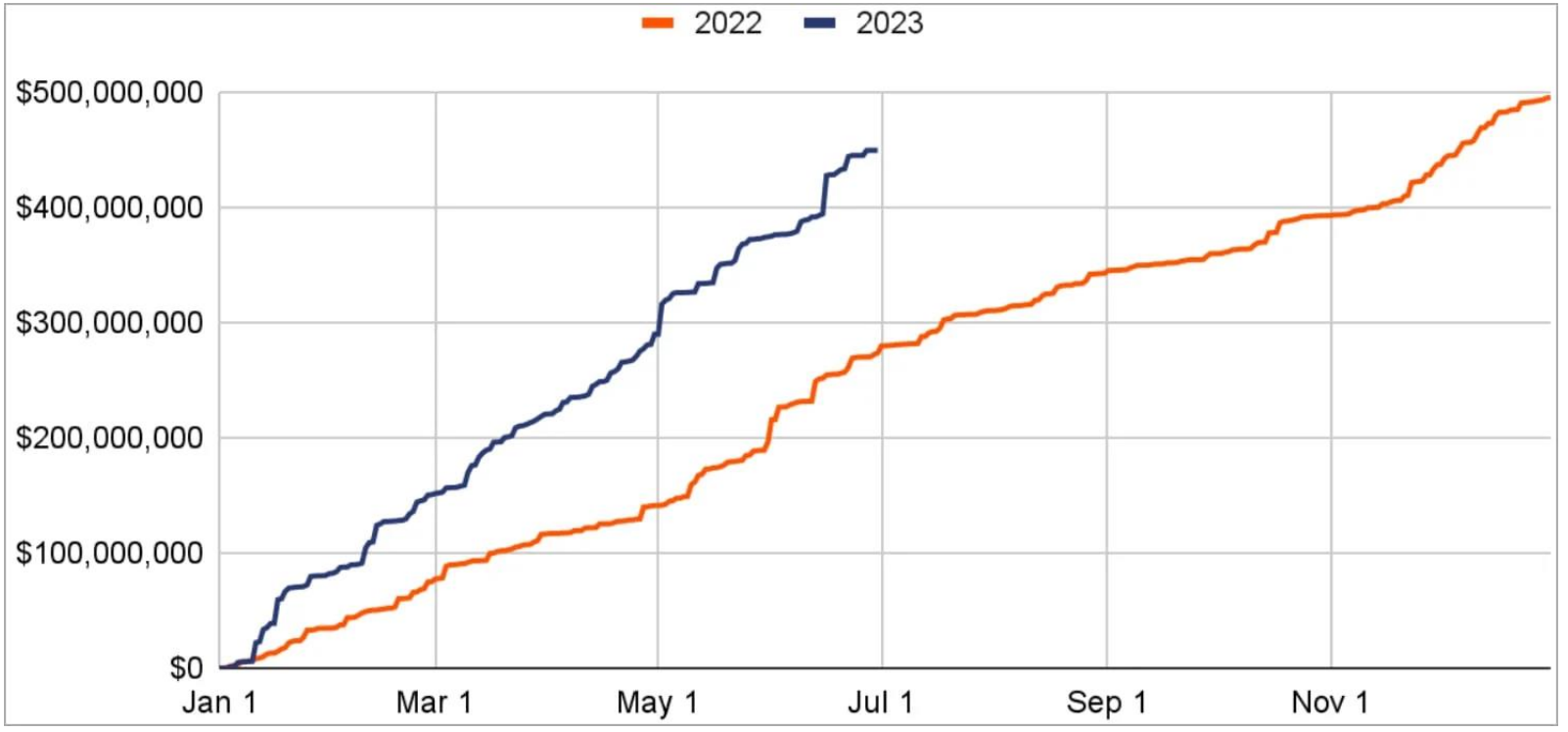
6. Tailgating

Questa tecnica riguarda l'accesso fisico all'interno di un'area riservata: il cybercriminale segue un dipendente autorizzato o chiede di entrare fingendo di aver dimenticato il badge di accesso all'area.

RANSOMWARE

- Tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto da pagare per rimuovere la limitazione.
- Alcuni ransomware bloccano il sistema e intimano l'utente a pagare per sbloccare il sistema.
- Altri cifrano i file dell'utente chiedendo di pagare per riportare i file cifrati in chiaro.

RANSOMWARE



- Se il ritmo di crescita dei guadagni da ransomware sarà stato confermato alla fine dell'anno, i gruppi ransomware avranno guadagnato circa 900 milioni di dollari dalle loro vittime, poco sotto la cifra record di 940 milioni raggiunta nel 2021.

I numeri

42 milioni di euro

La richiesta di riscatto record **a una sola azienda** *(gruppo REvil ad Acer nel marzo 2021)*

59,5 milioni di euro

La richiesta di riscatto record **per un solo attacco a più aziende** *(gruppo REvil nell'attacco a Kaseya nel luglio 2021)*

RANSOMWARE

- Generalmente l'operazione prevede che prima di procedere con la cifratura dei dati presenti nel sistema possa essere effettuata un'esfiltrazione di tutte le informazioni.

- Nella prima fase gli attacchi ransomware prevedevano quasi esclusivamente la crittografia dei dati che venivano resi indisponibili a tempo indeterminato.

- Successivamente si è aggiunta la divulgazione dei dati nel dark web.

Double extortion

RANSOMWARE

- Oltre a richiedere il riscatto all'azienda e a farne trapelare i dati, ora le richieste di riscatto vengono recapitate anche ai clienti dell'azienda stessa.

- Questo è, ad esempio, avvenuto per l'azienda finlandese Vastaamo, specializzata in supporto psicoterapeutico.

- Molti pazienti hanno riferito di aver ricevuto e-mail con una richiesta di 200 euro in Bitcoin per evitare che il contenuto delle loro discussioni con gli psicologi fosse reso pubblico.

Triple extortion

RANSOMWARE

- La maggior parte degli attacchi arriva da Russia, Cina e Corea del Nord ma ci sono altri focolai in Vietnam, Ucraina, India.

- Grazie a una dashboard costantemente aggiornata è possibile monitorare l'andamento delle rivendicazioni ransomware che impattano sulle vittime italiane.

- Il dato del numero totale di rivendicazioni ransomware contro target italiani nel 2023, aggiornato al 28/12/2023 è **185**.

- Al link:

  https://www.cybersecurity360.it/nuove-minacce/ransomware/attacchi-ransomware-aziende-italiane-oggi/

  è possibile visualizzare la lista delle vittime, insieme ad alcune informazioni sulla quantità di dati diffusa online ed il gruppo criminale che ha rivendicato l'attacco.

Somacis SpA

26-01-2023 – L'attacco viene rivendicato dal gruppo criminale **ALPHV/BlackCat**. Vengono diffusi online 262 GB di dati. Somacis si occupa dal 1972 di soluzioni tecnologiche ed elettronica industriale (fonte dati: **DRM**).

University of Salerno

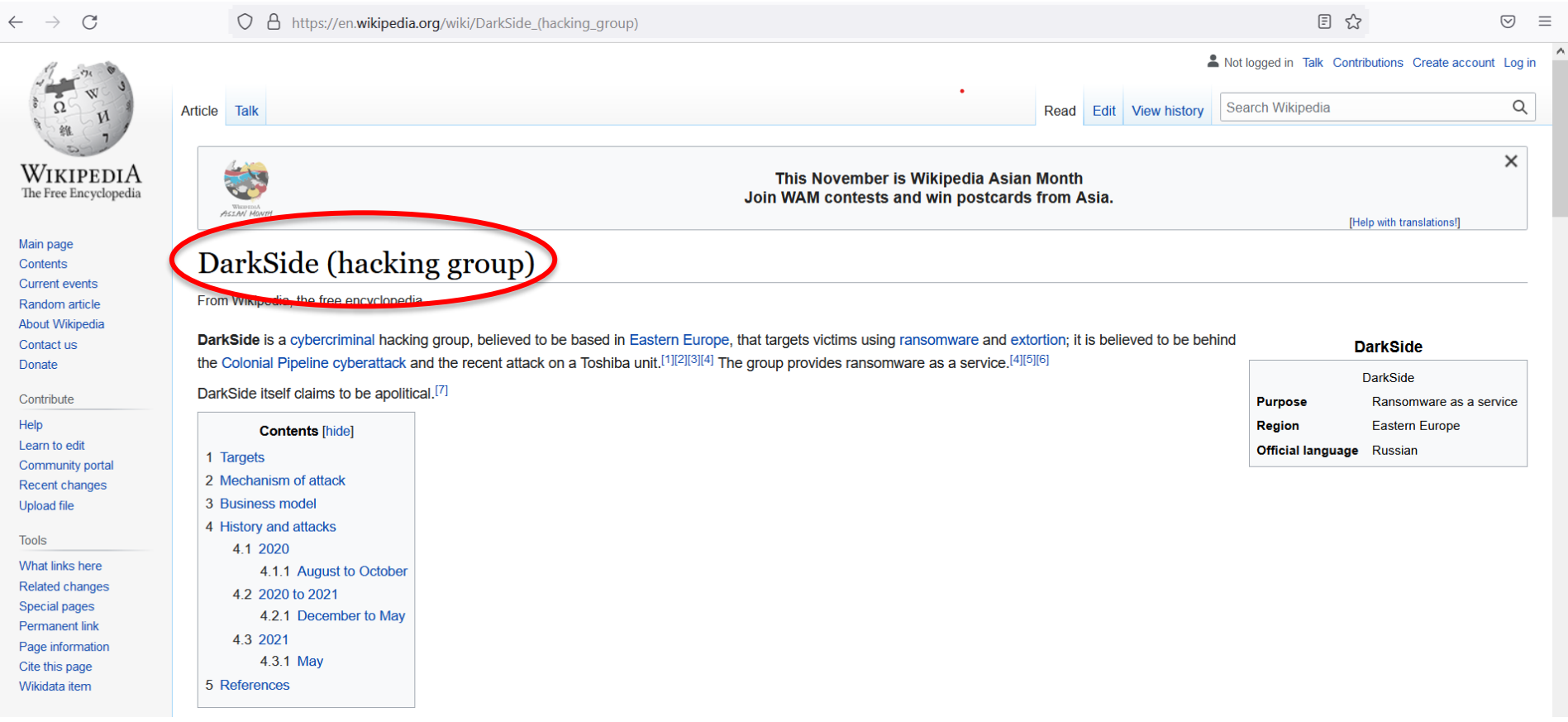
26-07-2023 – L'attacco è stato rivendicato dal gruppo criminale **rhysida**. Azienda operante nel settore Universities (fonte dati: **DRM**)

Omniatel

07-09-2023 – L'attacco è stato rivendicato dal gruppo criminale **noescape**. Azienda operante nel settore Services (fonte dati: **DRM**)

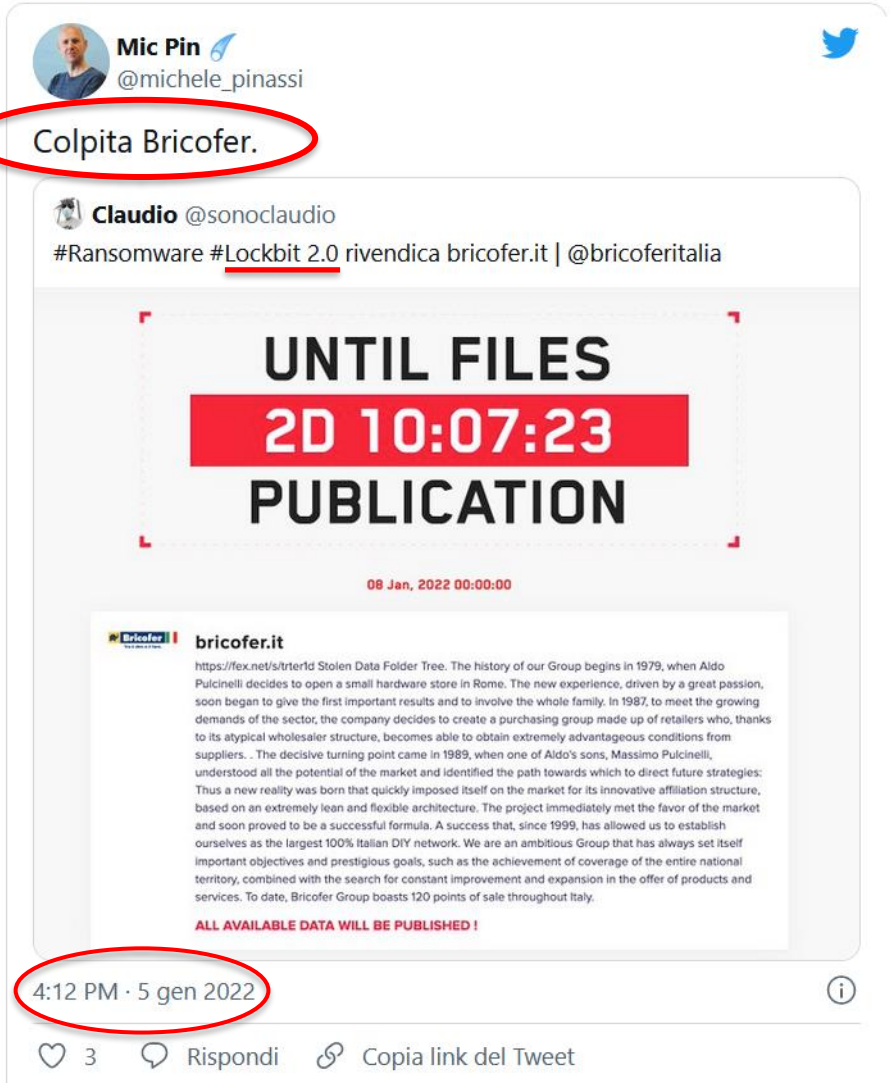
Omniatel

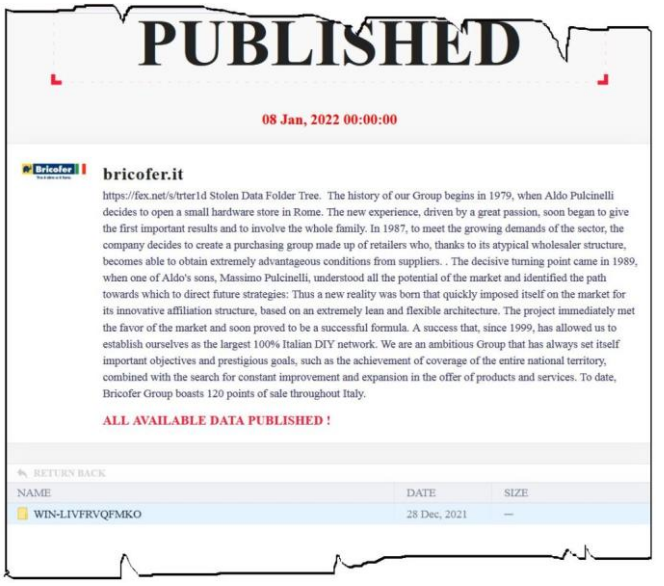
26-09-2023 – L'attacco è stato rivendicato dal gruppo criminale **losttrust**. Azienda operante nel settore Finance (fonte dati: **DRM**)

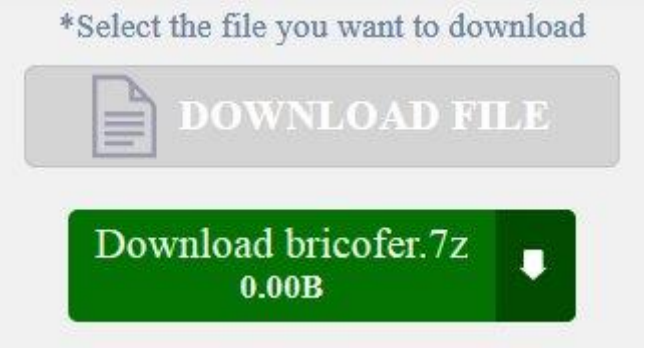


- Il **Ransomware as a Service** (RaaS) è un modello di business utilizzato dagli sviluppatori di ransomware, in cui si affittano varianti di ransomware nello stesso modo in cui gli sviluppatori di software legittimi affittano prodotti SaaS.

RANSOMWARE


Mic Pin
@michele_pinassi
Colpita Bricofer.
Claudio @sonoclaudio
#Ransomware #Lockbit 2.0 rivendica bricofer.it | @bricoferitalia
UNTIL FILES
2D 10:07:23
PUBLICATION
08 Jan, 2022 00:00:00
bricofer.it
https://fex.net/s/trter1d Stolen Data Folder Tree. The history of our Group begins in 1979, when Aldo Pulcinelli decides to open a small hardware store in Rome. The new experience, driven by a great passion, soon began to give the first important results and to involve the whole family. In 1987, to meet the growing demands of the sector, the company decides to create a purchasing group made up of retailers who, thanks to its atypical wholesaler structure, becomes able to obtain extremely advantageous conditions from suppliers. . The decisive turning point came in 1989, when one of Aldo's sons, Massimo Pulcinelli, understood all the potential of the market and identified the path towards which to direct future strategies: Thus a new reality was born that quickly imposed itself on the market for its innovative affiliation structure, based on an extremely lean and flexible architecture. The project immediately met the favor of the market and soon proved to be a successful formula. A success that, since 1999, has allowed us to establish ourselves as the largest 100% Italian DIY network. We are an ambitious Group that has always set itself important objectives and prestigious goals, such as the achievement of coverage of the entire national territory, combined with the search for constant improvement and expansion in the offer of products and services. To date, Bricofer Group boasts 120 points of sale throughout Italy.
ALL AVAILABLE DATA WILL BE PUBLISHED !
4:12 PM · 5 gen 2022
3
Rispondi
Copia link del Tweet

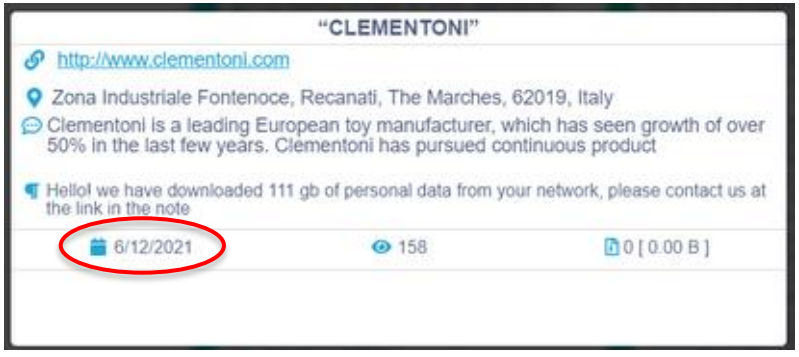

PUBLISHED
08 Jan, 2022 00:00:00
bricofer.it
https://fex.net/s/trter1d Stolen Data Folder Tree. The history of our Group begins in 1979, when Aldo Pulcinelli decides to open a small hardware store in Rome. The new experience, driven by a great passion, soon began to give the first important results and to involve the whole family. In 1987, to meet the growing demands of the sector, the company decides to create a purchasing group made up of retailers who, thanks to its atypical wholesaler structure, becomes able to obtain extremely advantageous conditions from suppliers. . The decisive turning point came in 1989, when one of Aldo's sons, Massimo Pulcinelli, understood all the potential of the market and identified the path towards which to direct future strategies: Thus a new reality was born that quickly imposed itself on the market for its innovative affiliation structure, based on an extremely lean and flexible architecture. The project immediately met the favor of the market and soon proved to be a successful formula. A success that, since 1999, has allowed us to establish ourselves as the largest 100% Italian DIY network. We are an ambitious Group that has always set itself important objectives and prestigious goals, such as the achievement of coverage of the entire national territory, combined with the search for constant improvement and expansion in the offer of products and services. To date, Bricofer Group boasts 120 points of sale throughout Italy.
ALL AVAILABLE DATA PUBLISHED !
RETURN BACK
NAME
DATE
SIZE
WIN-LIVFRVQFMKO
28 Dec, 2021


*Select the file you want to download
DOWNLOAD FILE
Download bricofer.7z
0.00B

RANSOMWARE

Clementoni HACKED

L'Italiana Clementoni, vittima del ransomware Conti.

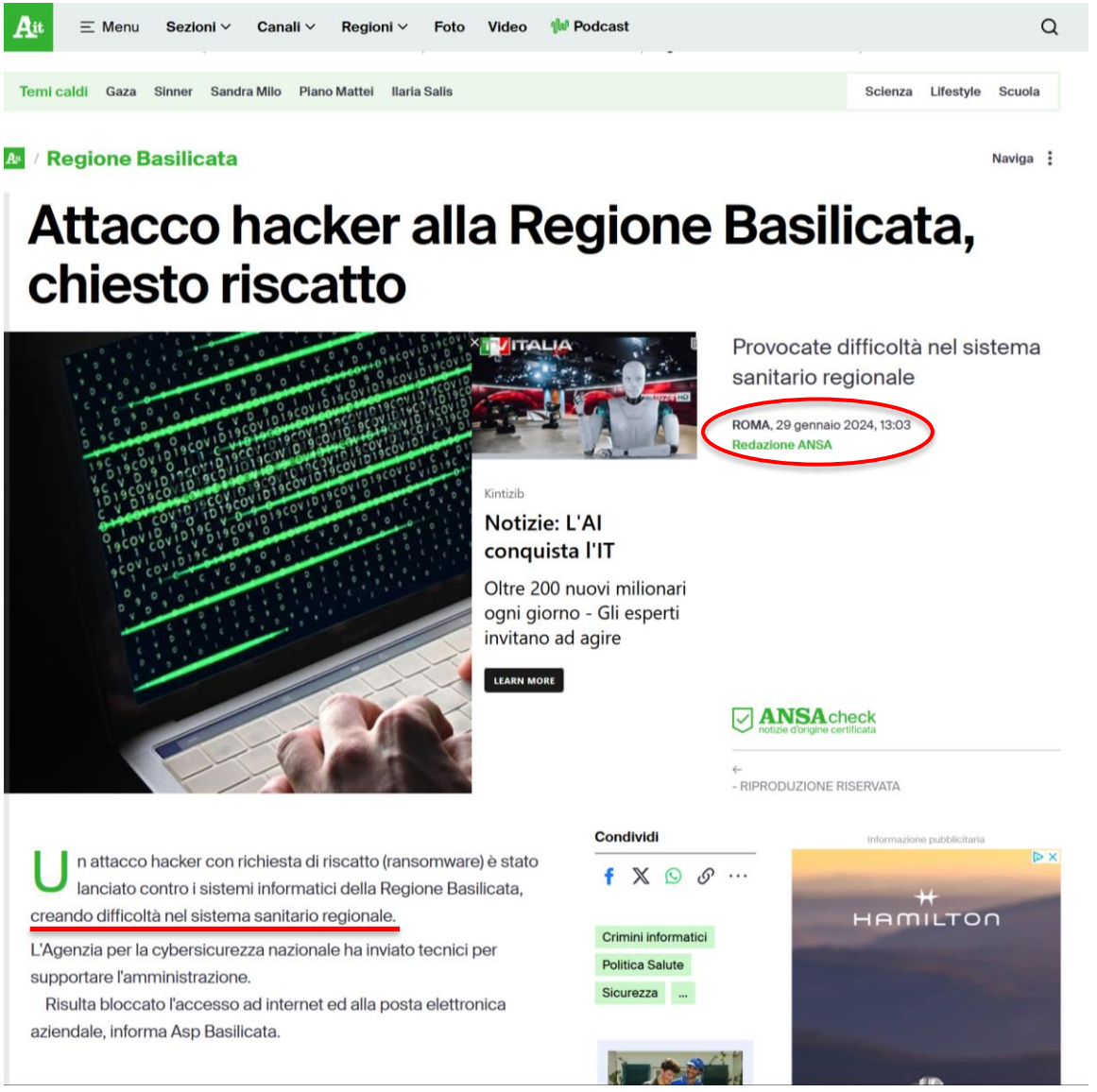


RANSOMWARE

The British Library

- È la più importante biblioteca britannica, una delle cinque istituzioni del Regno Unito che conservano una copia di ogni lavoro pubblicato nel paese. Nei suoi archivi si trovano oltre 170 milioni di opere.
- I criminali hanno sferrato un attacco ransomware ad Ottobre 2023 e chiesto un riscatto di 600mila sterline che la Biblioteca si è rifiutata di pagare.
- Ciò ha provocato la reazione degli hacker che hanno pubblicato centinaia di migliaia di documenti rubati, tra cui i dati personali degli impiegati e degli utenti della biblioteca.
- Gli hacker hanno inoltre venduto sul dark web, per una cifra ignota, il 10% dei file in loro possesso a un singolo offerente.
- Per ripristinare il servizio servirà almeno un anno e la British Library dovrà spendere una cifra stimata attorno ai 7 milioni di euro.

RANSOMWARE



Menu Sezioni Canali Regioni Foto Video Podcast

Temi caldi Gaza Sinner Sandra Milo Piano Mattei Ilaria Salis Scienza Lifestyle Scuola

Regione Basilicata Naviga

Attacco hacker alla Regione Basilicata, chiesto riscatto

Provocate difficoltà nel sistema sanitario regionale

ROMA, 29 gennaio 2024, 13:03
Redazione ANSA

Kintizib
Notizie: L'AI conquista l'IT
Oltre 200 nuovi milionari ogni giorno - Gli esperti invitano ad agire
LEARN MORE

ANSAcheck notizie d'origine certificata

Un attacco hacker con richiesta di riscatto (ransomware) è stato lanciato contro i sistemi informatici della Regione Basilicata, creando difficoltà nel sistema sanitario regionale.
L'Agenzia per la cybersicurezza nazionale ha inviato tecnici per supportare l'amministrazione.
Risulta bloccato l'accesso ad internet ed alla posta elettronica aziendale, informa Asp Basilicata.

Condividi

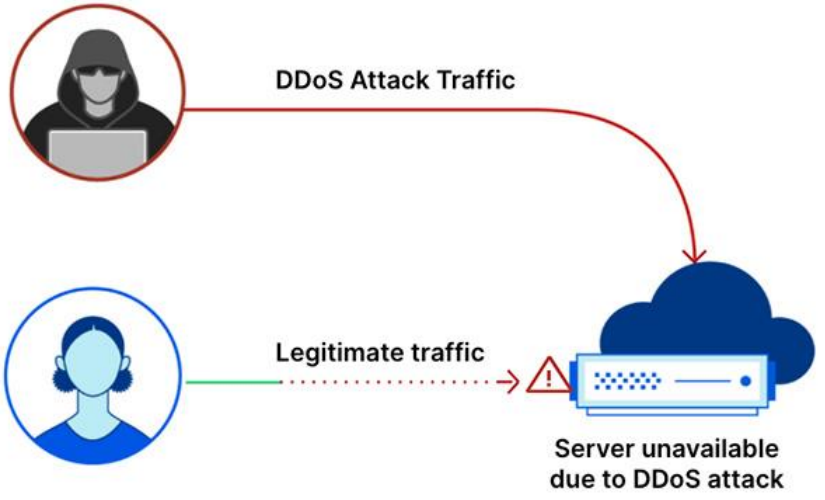
Crimini informatici
Politica Salute
Sicurezza ...

RANSOMWARE

- Recentemente sono apparsi esempi di ransomware (uno di questi è **LockFile**) che usano la *crittografia intermittente*.
- LockFile, in particolare, crittografa in modo intermittente 16 byte in un documento.
- La crittografia intermittente può avere successo contro i software di protezione ransomware che eseguono l'ispezione del contenuto con l'analisi statistica per rilevare la crittografia.
- La crittografia intermittente aiuta il ransomware ad eludere il rilevamento da parte di alcune soluzioni di protezione perché un documento crittografato sembra statisticamente molto simile all'originale non crittografato.

NON SOLO RANSOMWARE

- Nuova tendenza: esecuzione di attacchi DDoS accompagnata da richieste monetarie in cambio dell'annullamento dell'attacco.



- Più di un attacco DDoS su cinque è ormai accompagnato da una richiesta di riscatto.
- Gli attaccanti si avvalgono spesso di botnet a noleggio.

EVOLUZIONE DEGLI ATTACCHI: RUOLO DELL'INTELLIGENZA ARTIFICIALE

- Deepfakes

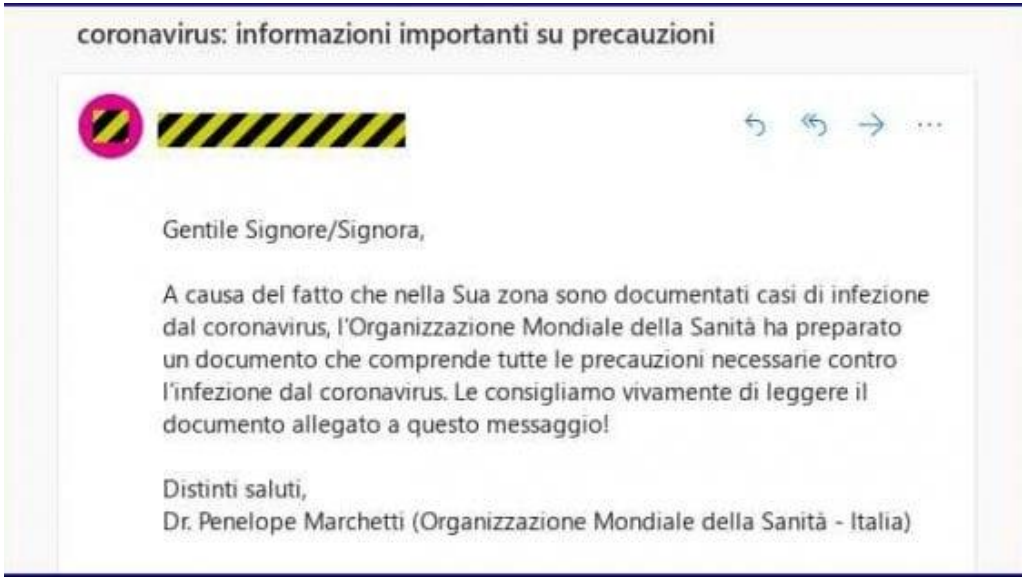
- In uno studio del Parlamento europeo si legge: "Sul web bisogna comportarsi come se ogni giorno fosse il primo d'aprile".

UNIVERSITÀ POLITECNICA DELLE MARCHE

CYBERSECURITY E COVID-19

- Eventi come lo tsunami nell'Oceano Indiano del 2004 e l'epidemia di virus Zika sono stati utilizzati come esche per attacchi cyber.

- L'emergenza Covid-19 ha fornito un'ulteriore opportunità di questo tipo, sfruttando la psicosi:
  - tentativi di **ingegneria sociale** a tema virale
  - vendita di **prodotti sanitari** contraffatti
  - diffusione di **disinformazione**



CYBERSECURITY E COVID-19

- Inoltre, un numero senza precedenti di persone **ha lavorato (e continua a lavorare) da remoto**, spesso per la prima volta.

- Le aziende si affrettano a fornire terminali ai dipendenti, distribuire software ed implementare piattaforme di collaborazione.

- Spesso l'accesso avviene da **macchine private** poco sicure ed attaccabili.

- Ma anche in assenza di attacchi, un dipendente in **smart working** potrebbe ad esempio inviare documenti aziendali sulla propria posta elettronica personale per lavorarci da casa.

- Se tali documenti contengono dati personali (ad es. di clienti o altri dipendenti), ciò già si inquadra come **data breach** (GDPR).

CYBERBULLISMO

https://www.miur.gov.it/bullismo-e-cyberbullismo

Governo Italiano

ACCESSO

Ministero dell'Istruzione e del Merito

Seguici su:

Cerca nel sito

Home > URP > Argomenti più richiesti > Studenti > Scuola > Bullismo e Cyberbullismo >

Bullismo e cyberbullismo

Il cyberbullismo è la manifestazione in Rete di un fenomeno più ampio e meglio conosciuto come bullismo. Quest'ultimo è caratterizzato da azioni violente e intimidatorie esercitate da un bullo, o un gruppo di bulli, su una vittima. Le azioni possono riguardare molestie verbali, aggressioni fisiche, persecuzioni, generalmente attuate in ambiente scolastico. Oggi la tecnologia consente ai bulli di infiltrarsi nelle case delle vittime, di materializzarsi in ogni momento della loro vita, perseguitandole con messaggi, immagini, video offensivi inviati tramite smartphone o pubblicati sui siti web tramite Internet. Il bullismo diventa quindi cyberbullismo. Il cyberbullismo definisce un insieme di azioni aggressive e intenzionali, di una singola persona o di un gruppo, realizzate mediante strumenti elettronici (sms, mms, foto, video, email, chat rooms, instant messaging, siti web, telefonate), il cui obiettivo è quello di provocare danni ad un coetaneo incapace di difendersi.

URP

- L'ufficio
- Argomenti più richiesti
- Studenti
- Famiglie
- Personale Scuola
- Come faccio a
- Officina Urp
- Risorse
- Cerca gli URP sul territorio

CYBERBULLISMO

- Il cyberbullismo è la manifestazione in Rete di un fenomeno più ampio e meglio conosciuto come bullismo.
- Quest'ultimo è caratterizzato da azioni violente e intimidatorie esercitate da un bullo, o un gruppo di bulli, su una vittima.
- Le azioni possono riguardare molestie verbali, aggressioni fisiche, persecuzioni, generalmente attuate in ambiente scolastico.

- Oggi la tecnologia consente ai bulli di infiltrarsi nelle case delle vittime, di materializzarsi in ogni momento della loro vita, perseguitandole con messaggi, immagini, video offensivi inviati tramite smartphone o pubblicati sui siti web tramite Internet.
- Il bullismo diventa quindi cyberbullismo.

CYBERBULLISMO

Il cyberbullismo definisce un insieme di azioni aggressive e intenzionali, di una singola persona o di un gruppo, realizzate mediante strumenti elettronici (sms, mms, foto, video, email, chat rooms, instant messaging, siti web, telefonate), il cui obiettivo è quello di provocare danni ad un coetaneo incapace di difendersi.

CYBERBULLISMO

Differenze tra bullismo e cyberbullismo

Bullismo	Cyberbullismo
Sono coinvolti solo gli studenti della classe e/o dell'Istituto;	Possono essere coinvolti ragazzi ed adulti di tutto il mondo;
generalmente solo chi ha un carattere forte, capace di imporre il proprio potere, può diventare un bullo;	chiunque, anche chi è vittima nella vita reale, può diventare cyberbullo;
i bulli sono studenti, compagni di classe o di Istituto, conosciuti dalla vittima;	i cyberbulli possono essere anonimi e sollecitare la partecipazione di altri "amici" anonimi, in modo che la persona non sappia con chi sta interagendo;
le azioni di bullismo vengono raccontate ad altri studenti della scuola in cui sono avvenute, sono circoscritte ad un determinato ambiente;	il materiale utilizzato per azioni di cyberbullismo può essere diffuso in tutto il mondo;

CYBERBULLISMO

Differenze tra bullismo e cyberbullismo

Bullismo	Cyberbullismo
le azioni di bullismo avvengono durante l'orario scolastico o nel tragitto casa-scuola, scuola-casa;	le comunicazioni aggressive possono avvenire 24 ore su 24;
le dinamiche scolastiche o del gruppo classe limitano le azioni aggressive;	i cyberbulli hanno ampia libertà nel poter fare online ciò che non potrebbero fare nella vita reale;
bisogno del bullo di dominare nelle relazioni interpersonali attraverso il contatto diretto con la vittima;	percezione di invisibilità da parte del cyberbullo attraverso azioni che si celano dietro la tecnologia;
reazioni evidenti da parte della vittima e visibili nell'atto dell'azione di bullismo;	assenza di reazioni visibili da parte della vittima che non consentono al cyberbullo di vedere gli effetti delle proprie azioni;
tendenza a sottrarsi da responsabilità portando su un piano scherzoso le azioni di violenza.	sdoppiamento della personalità: le conseguenze delle proprie azioni vengono attribuite al "profilo utente" creato.

UNIVERSITÀ POLITECNICA DELLE MARCHE

VULNERABILITÀ

20 PASSWORD PIÙ COMUNI IN ITALIA NEL 2023

Rank	Pawwword	Time to crack it	Count
1	admin	< 1 second	38,369
2	123456	< 1 second	14,335
3	password	< 1 second	12,476
4	Password	< 1 second	10,281
5	12345678	< 1 second	5,831
6	123456789	< 1 second	4,049
7	password99	< 1 second	3,847
8	qwerty	< 1 second	2,688
9	UNKNOWN	17 minutes	2,539
10	12345	< 1 second	2,464
11	ciaociao	2 seconds	1,992
12	francesco	< 1 second	1,463
13	1234567890	< 1 second	1,346
14	Windows1	5 seconds	1,321
15	Windows10	20 seconds	1,262
16	riccardo	< 1 second	1,192
17	corrado	< 1 second	1,162
18	francesca	11 seconds	1,134
19	andrea	< 1 second	987
20	juventus	< 1 second	975

https://nordpass.com/most-common-passwords-list/?ftag=YHF4eb9d17

20 PASSWORD PIÙ COMUNI NEL MONDO NEL 2023

Rank	Pawwword	Time to crack it	Count
1	123456	< 1 second	4,524,867
2	admin	< 1 second	4,008,850
3	12345678	< 1 second	1,371,152
4	123456789	< 1 second	1,213,047
5	1234	< 1 second	969,811
6	12345	< 1 second	728,414
7	password	< 1 second	710,321
8	123	< 1 second	528,086
9	Aa123456	< 1 second	319,725
10	1234567890	< 1 second	302,709
11	UNKNOWN	17 minutes	240,377
12	1234567	< 1 second	234,187
13	123123	< 1 second	224,261
14	111111	< 1 second	191,392
15	Password	< 1 second	177,725
16	12345678910	< 1 second	172,502
17	000000	< 1 second	168,653
18	admin123	11 seconds	159,354
19	********	< 1 second	152,497
20	user	1 second	146,233

https://nordpass.com/most-common-passwords-list/?ftag=YHF4eb9d17

PASSWORD PIÙ COMUNI NEL MONDO NEL 2023

- Anche la password “P@ssw0rd”, nonostante la sua apparente originalità, può essere decifrata in meno di un secondo ed è stata utilizzata, nel database oggetto dell’analisi, 135.424 volte.

- Le password più popolari sono sequenze numeriche. Tuttavia, facendo scorrere il dito sulla fila superiore di tasti della tastiera, ottieni “qwertyuiop“: questa password è stata utilizzata 79.434 volte.

- Negli Stati Uniti le password più popolari sono “123456”, “password” e “admin”. Ma la sedicesima password più popolare, “sh**bird”, è stata utilizzata 4.230 volte e richiede cinque minuti per essere decifrata.

PASSWORD PIÙ COMUNI NEL MONDO NEL 2023

- Diverse piattaforme influenzano le abitudini di creazione delle password.
- Pertanto, la quarta password più popolare sui siti di e-commerce come Amazon è “amazon” .
- Per i siti di streaming, una delle password più popolari è “netflix”.

Le Regole d'Oro per la gestione delle Password

1	Usare password sempre diverse
2	Usare password complesse: non meno di 8-10 caratteri, con numeri, lettere (sia maiuscole che minuscole) e simboli speciali
3	Cambiare spesso le password, anche se non sono state violate
4	Non creare alcun file, né sull'hard disk né online in qualche spazio in cloud, che contiene tutte le nostre password
5	Usare, quando è possibile la cosiddetta autenticazione a due fattori

UNIVERSITÀ
POLITECNICA
DELLE MARCHE

Procedura Semplice per Memorizzare Password Complesse

MfLe’ni25MegacnC!

UNIVERSITÀ POLITECNICA DELLE MARCHE

Procedura Semplice per Memorizzare Password Complesse

Mio figlio Luca è nato il 25 Marzo e gioca a calcio nel Camerano!

MfLe’ni25MegacnC!

UNIVERSITÀ POLITECNICA DELLE MARCHE

PASSWORD «FAMOSE»

- Victor Gevers afferma di aver fatto appena cinque tentativi prima di indovinare la password Twitter di Donald Trump: al quinto è entrato nel suo account con "***MAGA2020!***", con "*MAGA*" che sta per "*Make America Great Again*", lo slogan elettorale del presidente.
- Nel 2016 Gevers riuscì ad indovinare la password di Twitter di Trump che, all'epoca, era "*your'fired*". Cioè "*sei licenziato*", la frase che Trump ripeteva in continuazione nel reality show "*The Apprentice*", di cui era protagonista.

UNIVERSITÀ POLITECNICA DELLE MARCHE

LE REGOLE D'ORO PER LA GESTIONE DELLE PASSWORD

"The only secure password is the one you can't remember"
(Troy Hunt – 2011)

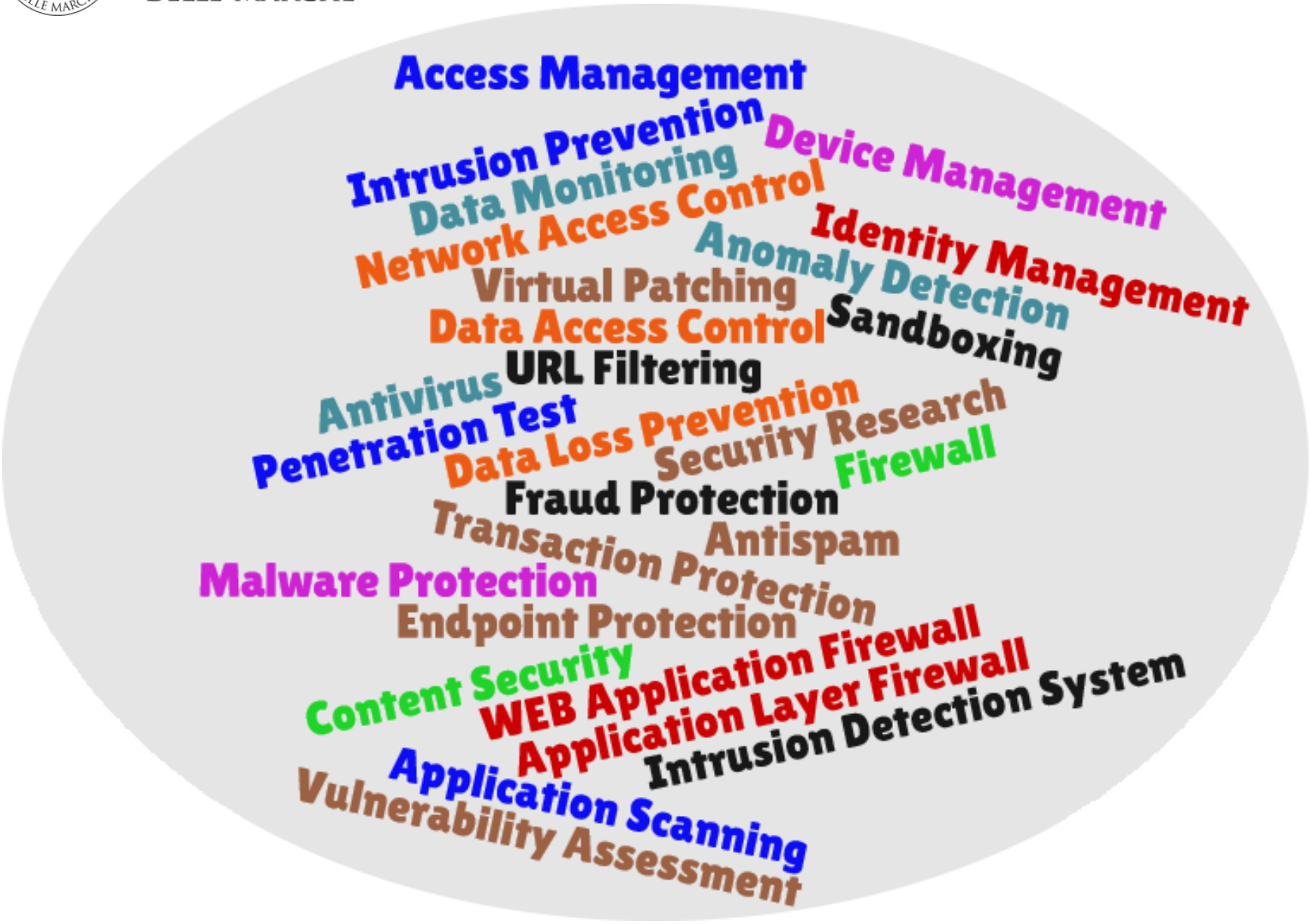
UNIVERSITÀ POLITECNICA DELLE MARCHE

PASSWORD MANAGER

- Sono programmi e app che archiviano in modo sicuro e crittografato le credenziali (username e password) di accesso ai servizi web (e non solo) in una sorta di cassaforte (“Vault”) virtuale, rendendola disponibile all’utente quando ne avrà bisogno.

- Sono protetti da una Master Password, che serve per aprirli e diventa perciò l’unica password che occorre ricordare.

DA DOVE INIZIARE?



NORME OBBLIGATORIE

NORME OBBLIGATORIE

- The Cyber Resilience Act (CRA) aims to safeguard consumers and businesses buying or using products or software with a digital component.
- The European Cyber Resilience Act is **a legal framework that describes the cybersecurity requirements for hardware and software products with digital elements placed on the market of the European Union**.
- Manufactures are now obliged to take security seriously throughout a product's life cycle.

NORME E STRUMENTI FACOLTATIVI

Framework Nazionale per la Cybersecurity e la Data Protection

cini Cybersecurity National Lab

Information Security Management ISO 27001 Certified

CIS Controls™

RECOVER IDENTIFY PROTECT DETECT RESPOND

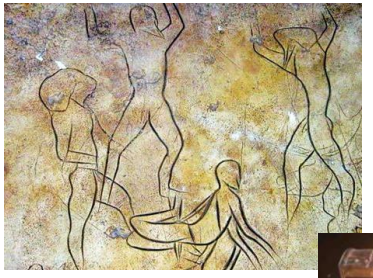
NIST National Institute of Standards and Technology U.S. Department of Commerce Cybersecurity Framework

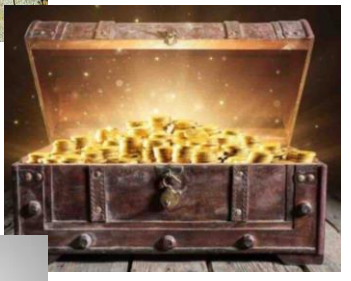
enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

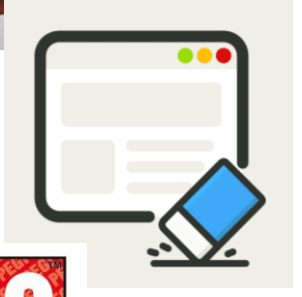
COME AZZERARE IL RISCHIO CYBER

Uso consapevole della tecnologia

COMANDAMENTI







1. Online è per sempre
2. Non è tutto oro ciò che luccica
3. Nulla è gratis
4. I dispositivi ti ricordano
5. (non) hai l'età?

UNIVERSITÀ POLITECNICA DELLE MARCHE

ALTRE REGOLE AUREE

- Da un'intervista a Gianluca Galasso, Direttore Servizio Operazioni dell'Acn (in data 5 Gennaio 2024):

- Le truffe online sono quasi sempre le stesse e i truffatori sfruttano sempre il principio della fiducia ingenua della vittima. Molte di queste truffe sono basate infatti sull'ingegneria sociale, cioè sulla conoscenza della psicologia delle persone e dei loro interessi.
- … facendo leva sula stanchezza e la distrazione delle persone, i delinquenti possono indurle ad avviare un'azione, come scaricare un allegato infetto o cliccare sul link verso un sito clone dove digitare ID e password per ottenere un servizio che però non gli sarà dato. Anche lì gli ruberanno i dati per usarli a piacimento.

UNIVERSITÀ POLITECNICA DELLE MARCHE

ALTRE REGOLE AUREE

- Da un'intervista a Gianluca Galasso, Direttore Servizio Operazioni dell'Acn (in data 5 Gennaio 2024):

- Altri tipi di truffa si basano su schemi piramidali dove la leva è il desiderio della vittima di ottenere soldi facili e quindi la si induce a investire in cryptomonete oppure, dopo avere instaurato una relazione di tipo romantico, chiederle un prestito che non verrà restituito.
- Tra gli strumenti utilizzati per eseguire le truffe negli ultimi tempi si è registrato anche un ampio ricorso agli sms, ovvero messaggi inviati al proprio smartphone da utenti apparentemente leciti (ad esempio operatori finanziari) contenenti link ai quali accedere per digitare i dati che contestualmente vengono carpiti.

UNIVERSITÀ POLITECNICA DELLE MARCHE

ALTRE REGOLE AUREE

- Da un'intervista a Gianluca Galasso, Direttore Servizio Operazioni dell'Acn (in data 5 Gennaio 2024):

- Tali forme di attacco possono avere buone possibilità di successo poiché, nelle nostre intense routine quotidiane facciamo tutti un utilizzo continuo e spesso distratto degli apparecchi mobili, tanto da aumentare il rischio di commettere le fatali disattenzioni.

UNIVERSITÀ POLITECNICA DELLE MARCHE

ALTRE REGOLE AUREE

- Da un'intervista a Gianluca Galasso, Direttore Servizio Operazioni dell'Acn (in data 5 Gennaio 2024):

- Per i cittadini la prima cosa da fare è diventare consapevoli che la Rete si presta a questo tipo di frodi sia perché consente l'anonimato, sia perché non ha confini territoriali.
- Purtroppo, le stesse leggi non consentono sempre di perseguire facilmente i delinquenti quando operano da paesi con cui non ci sono protocolli di collaborazione giudiziaria adeguati.
- E poi ci vuole buon senso: É vero che la Rete ci ha abituati ad avere molte cose senza pagarle direttamente, ma è abbastanza difficile che uno ti voglia regalare un iPhone perché sei l'utente numero 10mila che ha visitato quel certo sito.
- … quando una cosa è troppo bella per essere vera, non è vera.

ALTRE REGOLE AUREE

- Da un'intervista a Gianluca Galasso, Direttore Servizio Operazioni dell'Acn (in data 5 Gennaio 2024):

- Per le aziende si deve partire dall'uso di software e hardware sicuri, poi si implementano politiche di accesso ai sistemi secondo la logica del privilegio minimo (cioè non tutti possono operare allo stesso modo sui sistemi), ci si dota di sistemi anti-intrusione e di altri sistemi di difesa per le singole postazioni, per i server e per le reti aziendali e, per le realtà più complesse, si realizzano vere e proprie centrali operative per il monitoraggio della funzioni vitali dell'intera infrastruttura digitale (Security Operation Center).
- É importante anche fare degli audit interni e favorire l'igiene cibernetica dei propri impiegati e dei propri clienti.

ALTRE REGOLE AUREE

- Da un'intervista a Gianluca Galasso, Direttore Servizio Operazioni dell'Acn (in data 5 Gennaio 2024):

- Con igiene cibernetica ci riferiamo a un insieme di regole di sicurezza che vanno dall'aggiornamento dei sistemi operativi dei dispositivi digitali con cui si lavora, ad esempio, all'uso di antivirus e anti-malware, fino alle copie di backup offline di dati e informazioni.
- La formazione dei dipendenti è cruciale.
- Alcune realtà la addestrano con iniziative di gamification, rendendo cioè le esercitazioni di sicurezza simili a un gioco per favorire il coinvolgimento e l'apprendimento degli utenti.
- Dobbiamo anche ricordare che siamo un paese del G7, altamente digitalizzato, con una industria moderna e un forte settore bancario; pertanto, è inevitabile essere vittima di attacchi informatici. I criminali vanno dove ci sono profitti da fare.

CAPITALE UMANO

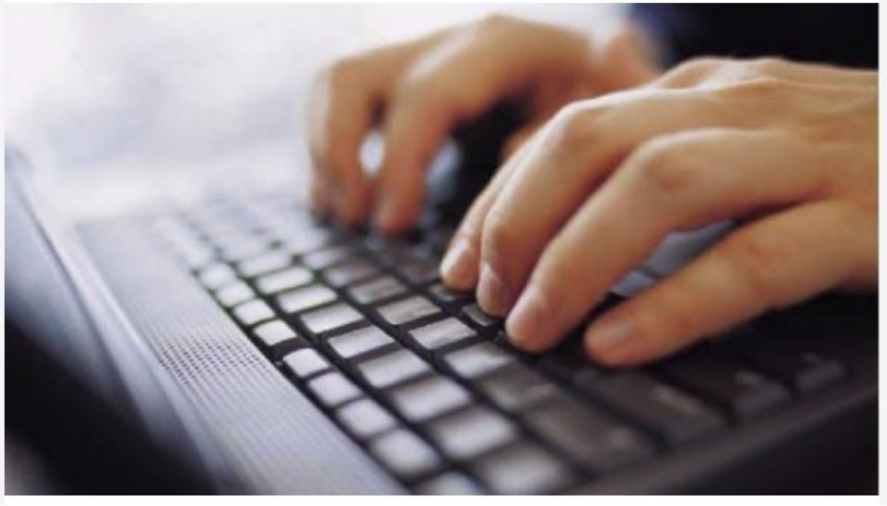
28 LUGLIO 2016 15:16

Allarme sicurezza: mancano esperti in "cyber security"

I governi non investono abbastanza nella formazione di personale qualificato in sicurezza informatica. Lo dice uno studio americano

(269) LEGGI DOPO COMMENTA

Oltre **200 mila posizioni di lavoro** rimaste vacanti nei soli Stati Uniti. Competenze preziose come **rilevamento delle intrusioni** e **mitigazione degli attacchi** sembrano non attrarre i giovani informatici. Nonostante l'ampia offerta – e il bisogno di **combattere il terrorismo** anche sulla rete – in paesi come Francia, Germania e Regno Unito **nessuno vuole lavorare nel settore della sicurezza online**. A rivelarlo è uno studio della **Intel Security Group** in collaborazione col **Center for Strategic and International Studies (Csis)**.



06 giugno 2017 | 16:22

L'economia digitale offre 85mila posti di lavoro ma mancano le competenze per occuparli. Programmatori e specialisti in sicurezza informatica tra le professioni più richieste. E c'è domanda di innovazione

Dall'economia digitale 85 mila nuovi posti di lavoro nel triennio 2016-2018. Ma mancano i professionisti per riempirli. È quanto emerge dalla terza edizione dell'Osservatorio delle Competenze Digitali, condotto dalle associazioni Ict Aica, Assinform, Assintel e Assinter Italia, promosso da Miur e Agid.

Le associazioni denunciano la mancanza di una "strategia di lungo periodo che coinvolga aziende e sistema formativo", di una "visione d'insieme" e di "risorse per rendere la pubblica amministrazione adeguata al cambiamento".

https://www.tomshw.it/business/cresce-la-domanda-di-esperti-in-cybersecurity-in-italia-100mila-posizioni-da-colmare

B2BLABS Hardware Videogiochi Mobile Elettronica EV Scienze B2B Offerte

Cresce la domanda di esperti in cybersecurity: in Italia 100mila posizioni da colmare

Anche in Italia continua la ricerca di esperti in cybersecurity, ma l'offerta scarseggia: sono più di 100mila le posizioni aperte per i talenti della sicurezza informatica.

Quando acquisti tramite i link sul nostro sito, potremmo guadagnare una commissione di affiliazione. Scopri di più

ML a cura di Marina Londei
Editor
Pubblicato il 21/09/2023 alle 14:00

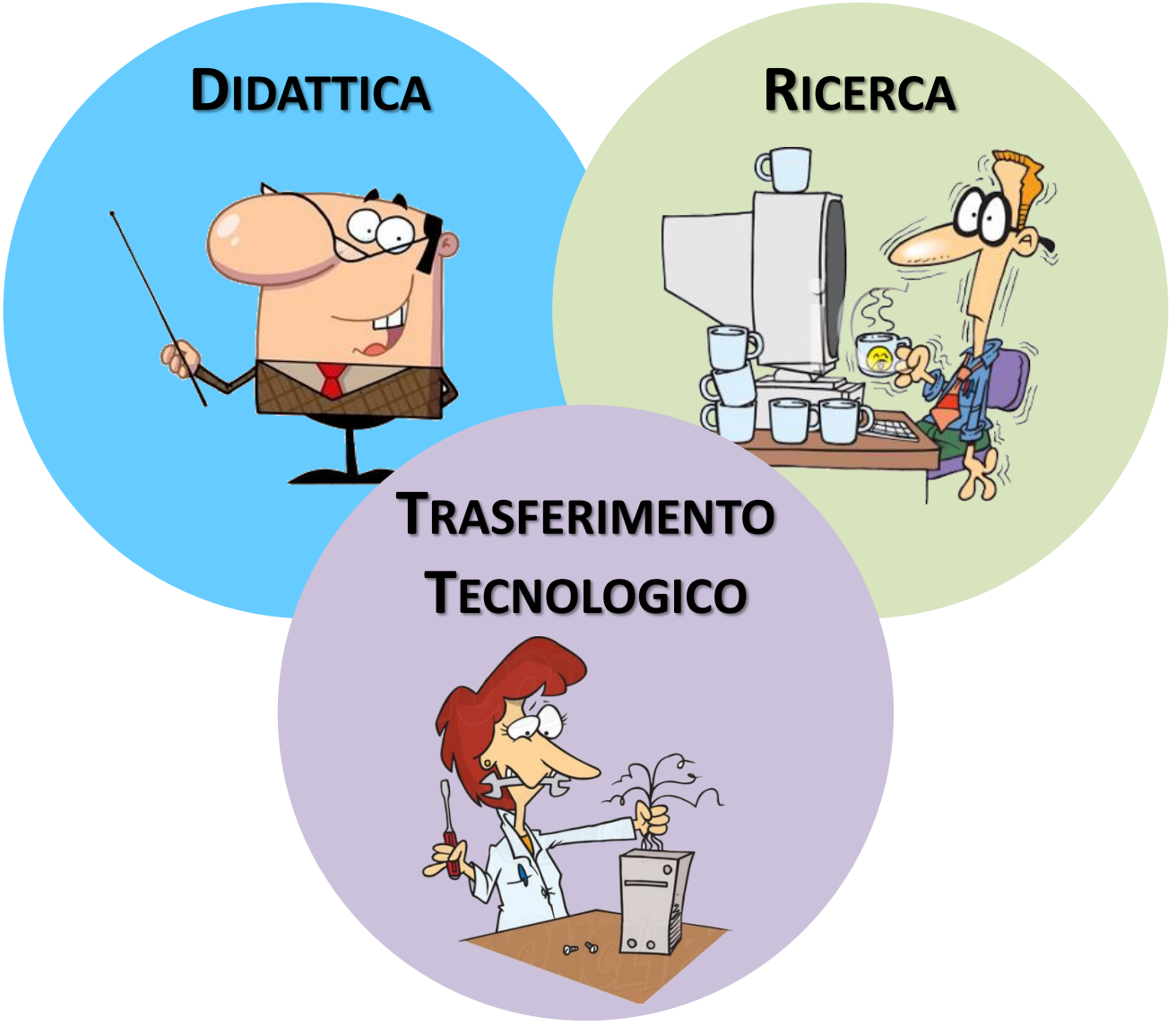
La ricerca di talenti esperti in cybersecurity non si arresta: **l'aumento del numero e della varietà di minacce ha fatto crescere esponenzialmente la domanda, ma l'offerta rimane scarsa.**

Non perdere gli ultimi aggiornamenti
NEWSLETTER TELEGRAM

I PIÙ LETTI DI OGGI
#1 I nuovi incentivi auto non stanno funzionando, si vendono solo auto a benzina
#2 Una pubblicazione social sbagliata fa licenziare tutto il team, succede in MSI

UNIVERSITÀ POLITECNICA DELLE MARCHE

ATTIVITÀ IN UNIVPM

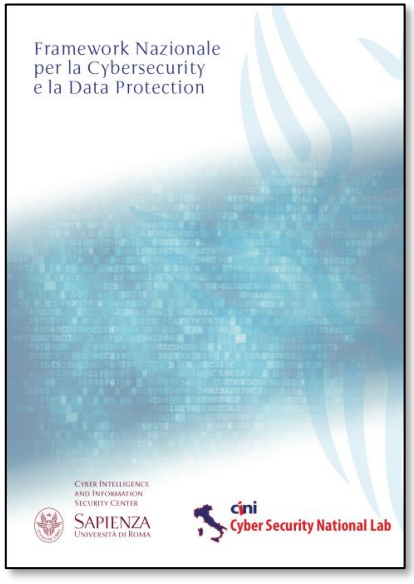


UNIVERSITÀ POLITECNICA DELLE MARCHE

LAB NAZIONALE DI CYBERSECURITY

cini Cyber Security National Lab

- **Oltre 500 professori e ricercatori**
- **51 nodi locali presso università e centri di ricerca**



CYBER CHALLENGE
CyberChallenge.IT

CENTRO DI RICERCA E SERVIZIO PER LA PRIVACY E LA CYBERSECURITY

Il Centro di Ricerca e Servizio per la Privacy e la Cybersecurity (CRiSPY) dell'Università Politecnica delle Marche è stato istituito nel 2019 allo scopo di riunire in un unico centro competenze interdisciplinari negli ambiti dell'Ingegneria dell'Informazione, delle Scienze Giuridiche ed Economiche e della Medicina per svolgere attività di ricerca e progettuale nel settore della protezione dei dati e della cybersecurity.

L'associazione di promozione sociale De Componendis Cifris o, in forma abbreviata De Cifris, si propone di animare la comunità crittografica italiana, sia nelle sue componenti accademiche, che nelle sue ramificazioni nel mondo del lavoro e dell'impresa.

Tra gli obiettivi, si prefigge di:

- Incentivare in Italia lo studio e la ricerca nell''ambito della crittografia a livello accademico e applicativo, con particolare attenzione alle aree della Matematica, dell'Informatica e dell'Ingegneria.
- Sostenere la realizzazione di qualificati progetti di ricerca che richiedano il coinvolgimento e la collaborazione di numerosi studiosi appartenenti a discipline anche molto diverse.
- Divulgare l'uso responsabile della crittografia, favorendo il formarsi di una cultura propria e autonoma.
- Contribuire al rafforzamento della cooperazione internazionale in questo settore, in ambito scientifico e del suo impiego, anche con principi di solidarietà.

La De Cifris auspica che l'Italia possa sviluppare cifrari robusti e flessibili, adatti all'era moderna, e che emergano talenti dedicati alle scienze crittografiche. L'associazione intende coinvolgere enti del mondo accademico, così come centri di ricerca, aziende, studenti universitari, liberi professionisti, e più in generale tutti coloro che condividono questa visione.

Fra le varie iniziative proposte si evidenziano numerosi seminari, diffusi anche tramite le pagine YouTube e LinkedIn dell'associazione.


ANCHARIA
cybersecurity
CONCENTRATI SUL TUO LAVORO, ALLA SICUREZZA CI PENSIAMO NOI
PREVENZIONE DEGLI ATTACCHI
Forniamo servizi concepiti per individuare, valutare e risolvere criticità e vulnerabilità presenti nei sistemi, nelle applicazioni e nelle reti aziendali. Tra le nostre principali attività rientrano il Penetration Test, il Vulnerability Assessment, la Cloud Security Assessment e le simulazioni di campagne di phishing.
CONFORMITÀ NORMATIVA
Offriamo supporto alle aziende nel raggiungere la conformità normativa in ambito di sicurezza informatica e tutela dei dati, con un focus specifico sull'adesione al Regolamento GDPR, alla Direttiva NIS 2 e al sistema di gestione ISO 27000.
RISPOSTA AGLI INCIDENTI
Ancharia si impegna a offrire alle aziende servizi di rilevamento e risposta agli incidenti informatici, individuando problemi e anomalie e intervenendo in caso di cyber attacchi.
CONSULENZA
Servizi progettati per assistere le aziende nel valutare la propria postura cyber, identificare rischi e lacune rispetto ai principali framework di riferimento, colmare tali divari e garantire che il personale sia preparato adeguatamente per affrontare le minacce cibernetiche in costante evoluzione.

CYBER CHALLENGE
CyberChallenge.IT

- Programma nazionale di allenamento e selezione di **ethical hackers**
- CyberChallenge.IT è il primo programma di addestramento in cybersecurity per studentesse e studenti universitari e delle scuole superiori organizzato dal Cybersecurity National Lab
- **Edizione 2024** appena partita

CYBER CHALLENGE
CyberChallenge.IT

- Programma nazionale di allenamento e selezione di **ethical hackers**

- **Edizione 2023**:
  - 4720 candidati tra 16 e 23 anni
  - 43 nodi locali (503 scuole affiliate)
  - 944 ammessi
  - Formato il Team Italiano di Cyberdefender per la **European Cyber Security Challenge**

- **Edizione 2024** appena partita

Calendario CyberChallenge.IT 2024

Cosa	Quando	Dove
Adesioni delle sedi	**Entro 31/12/2023**	**Online**
Iscrizioni online	**04/12/2023 - 08/02/2024**	**Online**
Pretest	10/02/2024	Online
Test di ammissione	13/02/2024	Online
Percorso formativo	Feb - Mag 2024	Presso ogni sede
Gare locali	29/05/2024	Presso ogni sede
Cerimonie di premiazioni locali	In base alla sede	In base alla sede
Gara nazionale	04/07/2024	Torino
Recruitment Fair nazionale	05/07/2024	Torino
Cerimonia di premiazione nazionale	05/07/2024	Torino
CyberChallenge.IT Workshop	06/07/2024	Torino
Ritiro della Nazionale Italiana	08/09/2024 - 15/09/2024	Lucca
European Cybersecurity Challenge 2024	07/10/2024 - 11/10/2024	Torino

- Tutte le informazioni sul sito: https://cyberchallenge.it/

SAFER INTERNET DAY

6 Febbraio 2024

- https://www.saferinternetday.org/in-your-country/italy

Franco Chiaraluce

Dipartimento di Ingegneria dell'Informazione

f.chiaraluce@univpm.it

linkedin.com/in/dipartimento-di-ingegneria-dell-informazione-univpm-356559228

https://www.instagram.com/dii_univpm/