UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unimc

La Cybersicurezza nell'era della Guerra Ibrida: il caso NoName057(16) e l'importanza di essere pronti

Dott. Edoardo Scippa

Gesta srl Società Benefit

Mail: scippa@gestaconsulenza.it

Cell: +39 3456443339

Mercoledì 17 Settembre 2025

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Introduzione: gli attacchi cyber

Gli attacchi cyber

Che cos'è un «attacco cyber»?

Attacco terroristico condotto con mezzi tecnologici, attraverso Internet.

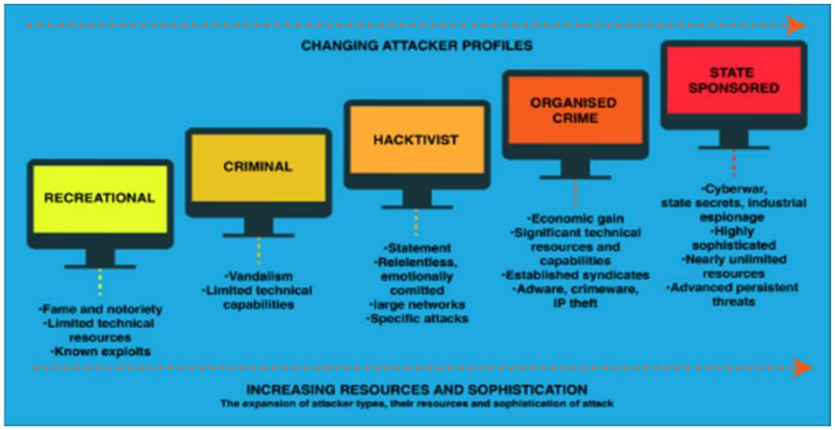
*(*Enciclopedia Treccani, 2008*)*

Any attempt by an individual or organization to use computers or digital systems to steal, alter, expose, disable, or destroy information, or to breach computer systems, networks, or infrastructures.

*(*Asbaş C., Tuzlukaya Ş., "Cyberattack and Cyberwarfare Strategies for Businesses", 2022*)*

Gli attacchi cyber

Tanti **vettori**,
tanti **attaccanti**...



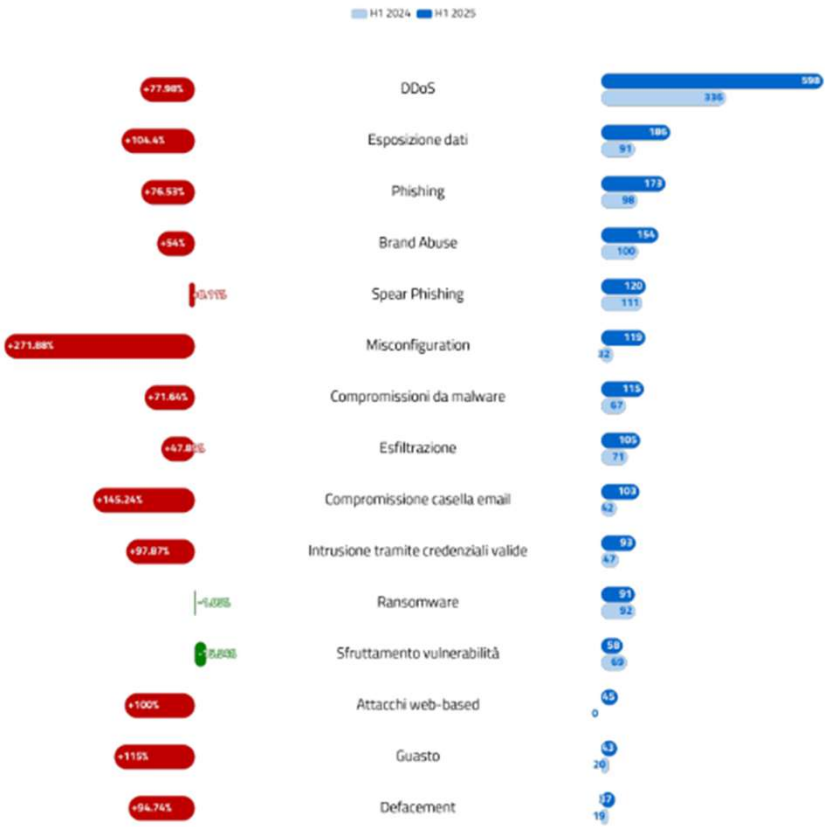
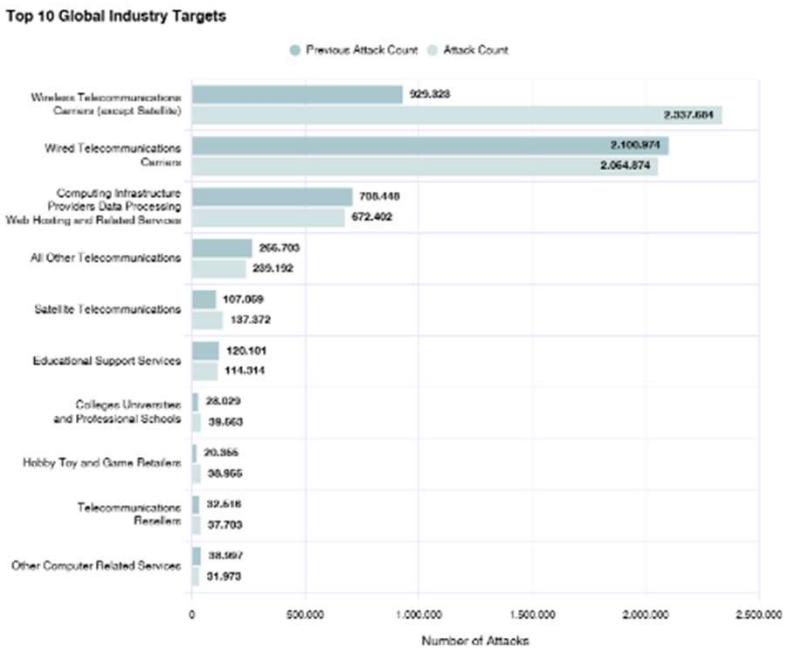


Figura 4 - *tipologie di minacce rilevate negli eventi e variazione percentuale rispetto al 1° semestre 2024*

Gli attacchi cyber

… ed altrettanti **attaccati**.

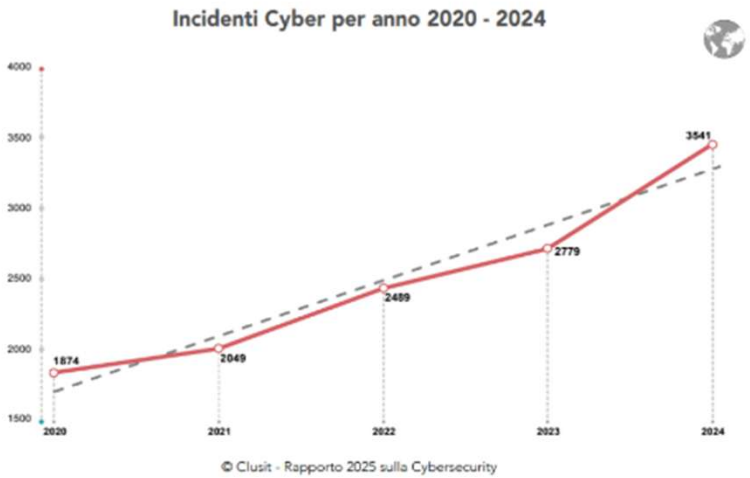


	Pubblica amministrazione centrale	Pubblica amministrazione locale	Servizi finanziari	Telecomunicazioni	Tecnologico	Energia	Trasporti	Vendita al dettaglio	Manifatturiero	Sanitario	Università e ricerca	Altre società private	Comunicazione	Organizzazioni associative	Fornitura di acqua potabile
Esposizione dati	92	80	86	70	56	43	54	33	24	82	99	22	12	6	17
DDoS	102	238	37	29	19	9	61	11	12	2	2		6	10	11
Misconfiguration	30	11	3	4	28	2	5	48	15	4	23	30	14	16	1
Esfiltrazione	4	5	57	11	15	23	20	20	28	6	3	18	2	1	1
Phishing	51	10	10	20	15	16	9	15	20	20	11	9	1	4	1
Compromissioni da malware	8	19	55	20	15	22	14	10	15	6	4	9	1	1	1
Compromissione casella email	29	11	2	22	13	9	7	18	9	18	27	7		2	
Intrusione tramite credenziali valide	17	5	85	12	15	2	5	10	7	8	2	4		1	
Brand Abuse	53	7	6	23	14	18	3	3	11	9	2	6	7	2	1
Spear Phishing	20	4	2	65	9	29	3	4	3	9	1	5		2	
Attacchi web-based	2	29		4	11	20	1	6	8	3	2	10	1	2	
Ransomware	1	6	4	1	13	8	2	7	23	3	2	8	1	1	
Supply chain attack			52	2	2	2	3								
Sfruttamento vulnerabilità	3	7		4	12	2	5	5	7	5	2	6		2	1
Guasto	3	1	3	15	10	6	6			3					
SCADA/ICS attack		3		1	1	9		4	12			2			1
Defacement	1	1			5	1		6	6	2		7	1	1	
DoS	3	10	1		1	5	7	2				1			
Scansione attiva su credenziali	2	3	1	9	2	1	5		1			1	1		1
Diffusione malware tramite email	6		2	5	1	2		2	1		1	2			
Smishing	8		5	1	1	1									
Typosquatting	5			1	1	3				1			5		
Cybersquatting	5				1					1			7		
Scansioni attive sul perimetro di rete	4		1	1	3	2		1	1						
Spam e scam	3				1	1			1	1					

Figura 5 - *numero di vittime per settore e tipologia di minacce*

Gli attacchi cyber

Due uniche certezze: il **danno** ed il trend in continua **crescita**.



© Clusit - Rapporto 2025 sulla Cybersecurity

	2024						2025					
	gennaio	febbraio	marzo	aprile	maggio	giugno	gennaio	febbraio	marzo	aprile	maggio	giugno
Eventi Cyber	89	252	108	114	283	167	205	302	245	163	201	433
Incidenti con impatto confermato	18	21	21	27	45	43	47	48	81	29	51	90
Vittime	80	240	121	111	278	165	201	324	323	260	341	531
Asset potenzialmente compromessi	65	142	0	13	0	0	269	289	1245	426	2171	8
Asset potenzialmente vulnerabili	628	1440	249	1473	1336	214	15000	1207	461	289	532	1027
URL di phishing	13	7	10	34	57	22	104	159	180	262	360	465
Comunicazioni inviate	1930	4142	3026	3823	2758	5545	2406	3260	3877	3733	3440	6428
Alert sito web	48	48	50	49	51	43	47	51	54	67	51	59

inferiore alla media — superiore alla media

- **1.549** eventi cyber, in **aumento** (**+536**);
- **2.367** vittime, in **aumento** (**+1.374**);
- **829** vittime della constituency[1], in **aumento** (**+562**);
- **346** incidenti con impatto confermato, in **aumento** (**+171**);
- **4.408** asset potenzialmente compromessi, in **aumento** (**+4.188**);
- **18.516** asset potenzialmente vulnerabili, in **aumento** (**+13.176**);
- **329** alert sul sito web del CSIRT Italia, in **aumento** (**+40**);
- **23.144** comunicazioni inviate, in **aumento** (**+1.920**);
- **24.098** nuove CVE, in **aumento** (**+4.067**).

La guerra ibrida e gli attacchi cyber

La guerra ibrida e gli attacchi cyber

Che cosa significa «guerra ibrida»?

*Strategia militare, caratterizzata da grande flessibilità, che unisce la guerra convenzionale, la guerra irregolare e la guerra fatta di azioni di attacco e **sabotaggio cibernetico**.*

*(*Enciclopedia Treccani, 2017*)*

Negli anni ’20, la dimensione cyber della guerra ibrida («**cyber warfare**») ha assunto sempre maggiore rilevanza.

La guerra ibrida e gli attacchi cyber

1. Gli attacchi cyber sono diventati veri e propri **strumenti di guerra,** utilizzati dagli **«hacktivisti»** schierati con l'una o l'altra parte del conflitto per **imporre il proprio messaggio** ideologico o **recare danni alle infrastrutture** degli avversari.
2. La «**webizzazione»** di servizi pubblici, comunicazioni, istituti finanziari ed infrastrutture critiche ha reso questi **attacchi più pericolosi**.
3. Questi attacchi hanno un **potenziale** pressoché **illimitato**, in quanto vengono **sostenuti**, economicamente e strutturalmente, **dagli Stati** che gli hacktivisti rappresentano.

La guerra ibrida e gli attacchi cyber

Chi attacca?	Chi viene attaccato?	Quali attacchi?	Quali fini?
Stati **Hacktivisti «sponsorizzati»** Cyberterroristi Spie Cyberpartigiani	**Agenzie governative** Infrastrutture critiche **Soggetti privati** Servizi finanziari **Servizi bancari** **Telecomunicazioni** Media Social Network **Alleati dell'avversario**	**DDoS** ***Malware*** *Deface* ***Slow HTTP Attack*** *Phishing* *Doppelgänger* OSINT Ingegneria sociale *Equipment disruption* Intelligenza artificiale	**Propaganda ideologica** **Disinformazione** **Danni economici** Disagio e panico **Interruzione di servizi strategici** Mobilitazione popolare «*Regime change*»

Meloni e il video fake: il Cremlino allude a un festino con Zelensky. E la propaganda russa se la ride

L'allusione è pesante: la premier italiana coinvolta in un festa a base di cocaina e alcol con il collega ucraino. Un'altra fake news che parte da Mosca e viene rilanciata dai social filo-Putin. E la portavoce Zakharova commenta con ironia

di Luca Arnaù

29 giugno 2026 20:07

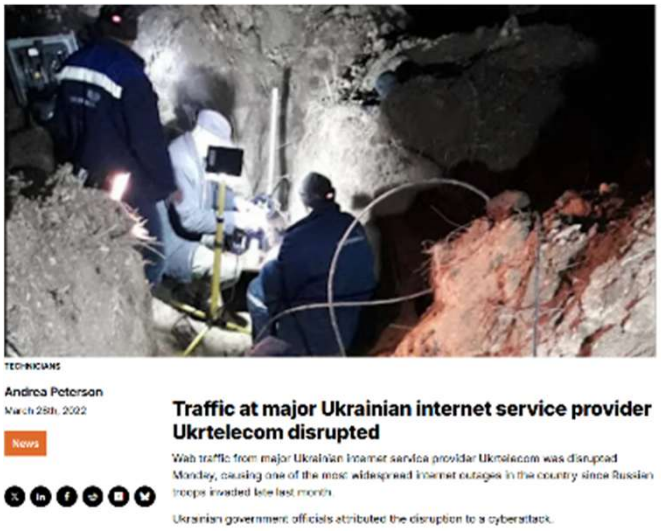
Un'ondata di disinformazione di origine russa punta a interferire sulle elezioni in Germania

L'obiettivo più ampio è la destabilizzazione dell'intera Europa, mentre i leader del Vecchio Continente vengono estromessi dall'avvio degli accordi di pace sull'Ucraina

17/02/2025 Cristiana Raffa

La guerra ibrida e gli attacchi cyber

Qualche esempio: L'invasione russa dell'Ucraina



TECHNICIANS

Andrea Peterson

March 28th, 2022

News

Traffic at major Ukrainian internet service provider Ukrtelecom disrupted

Web traffic from major Ukrainian Internet service provider Ukrtelecom was disrupted Monday, causing one of the most widespread Internet outages in the country since Russian troops invaded late last month.

Ukrainian government officials attributed the disruption to a cyberattack.

CYBERSECURITY | SECURITY NEWSWIRE | CYBERSECURITY NEWS

Russia-Sponsored Cyber Attack Campaign Targets Networking Devices, Critical Infrastructure

By Iordyn Alger, Managing Editor

August 22, 2025

COMPUTING

Russian hackers tried to bring down Ukraine's power grid to help the invasion

As Russia's ground war stalls, hackers attempted to cause a blackout for two million people.

By Patrick Howell O'Neill

April 12, 2022

La guerra ibrida e gli attacchi cyber

Qualche esempio: La controffensiva ucraina

Pro-Ukraine hacker group claims Aeroflot cyber-attack

28 July 2025

Share Save

Laura Gozzi BBC News Joe Tidy BBC News Cyber correspondent

'Cyber partisans' hack Russian TV, broadcast battlefield casualties and 'truth' about war, HUR source claims

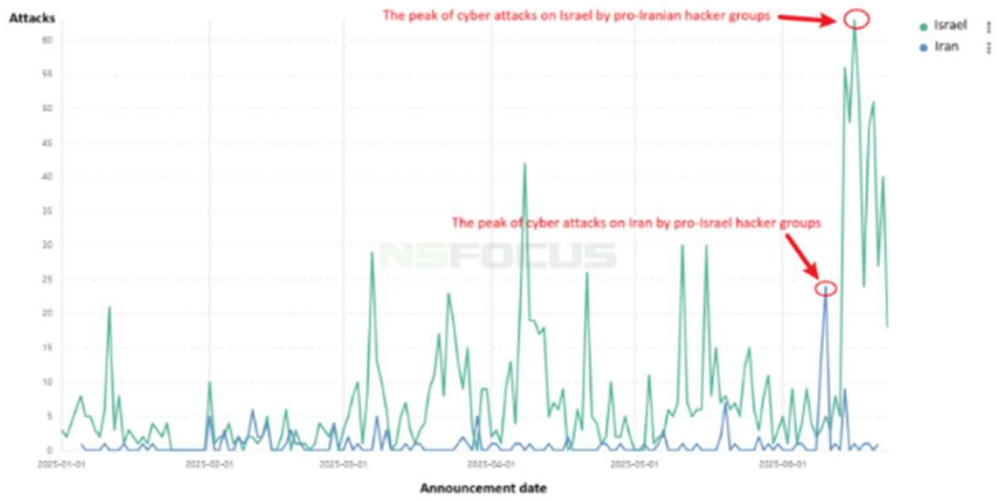
August 25, 2025 12:49 pm • 2 min read

by Kateryna Denisova

Footage from a video allegedly showing an attack on Russia, reportedly broadcast on Russian television on Aug. 24, 2025. (HUR)

La guerra ibrida e gli attacchi cyber

Qualche esempio: La guerra tra Israele e Iran



Un esempio di *cyber warfare*: il caso NoName057(16)

Un esempio di *cyber warfare*: il caso NoName057(16)

Chi è NoName057(16)?

Sono [hacktivisti] *filo-russi e simpatizzanti di Putin. Sono attivi dall'inizio della guerra e si servono di tanti volontari, anche pagati. E sono mossi da motivi esclusivamente politici, contro i "nemici della Russia", "russofobi", colpendo banche, siti istituzionali e servizi collegati a infrastrutture critiche.*

(Il Sole 24 Ore, 2023*)*

Un esempio di *cyber warfare*: il caso NoName057(16)

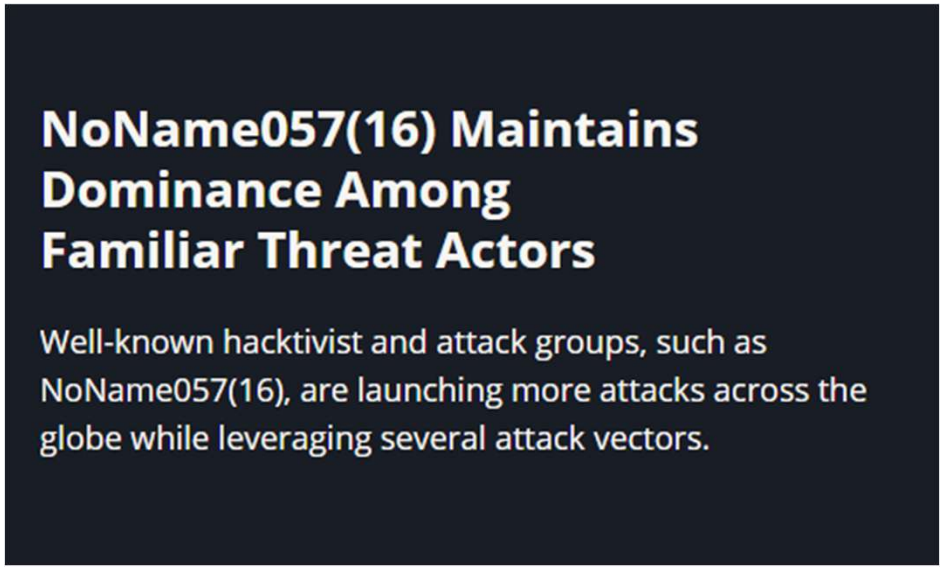
«Stiamo conducendo massicci attacchi alle risorse di propaganda ucraina che mentono sfacciatamente alle persone (sic) *sull'operazione speciale* (sic) *della Russia in Ucraina, così come sui siti web degli hacker del dolore ucraini che cercano di sostenere il regime neonazista* (sic) *di Zelens'kyj e una manciata di tossicodipendenti* (sic) *e nazisti* (sic) *della sua banda! Abbiamo già condotto diversi attacchi riusciti alle risorse ucraine, che hanno paralizzato l'accesso degli utenti ad esse.»*
(Manifesto di NoName057(16), 2022)

Un esempio di *cyber warfare*: il caso NoName057(16)

Tipologia di attacchi:

1. DDos
2. *Malware*
3. *Slow HTTP Attack*
4. Disinformazione

Il gruppo hacktivista ha rivendicato oltre 475 attacchi solo a marzo 2025, il 337% in più rispetto al secondo gruppo hacker più attivo, prendendo di mira siti governativi in Spagna, Taiwan, Ucraina e **ITALIA.**



Un esempio di *cyber warfare*: il caso NoName057(16)

Le offensive in Italia:


Servizio | Cyberwar

Terzo giorno di attacchi hacker filorussi all'Italia, giù molti siti di banche

L'Agenzia per la cybersicurezza nazionale è intervenuta per avvisare i target e dare supporto per il ripristino delle funzionalità

19 febbraio 2025

I soggetti attaccati nel 2025:

1. AdSP MAC
2. Ministero degli Esteri
3. Guardia di Finanza
4. AdRdT
5. Porti di Trieste, Taranto ed Olbia
6. Aeroporti di Malpensa e Linate
7. Intesa Sanpaolo
8. Mediobanca
9. Nexi
10. Benelli Armi S.p.A.
11. Fiocchi Munizioni S.p.A.
12. Danieli & C. SpA

E tanti altri…

Come prevenire e come proteggersi?

Come prevenire e come proteggersi?

Morale della favola:

NESSUNO È INTOCCABILE

(*Enti Pubblici, Soggetti privati, Canali di comunicazione e mediatici*)

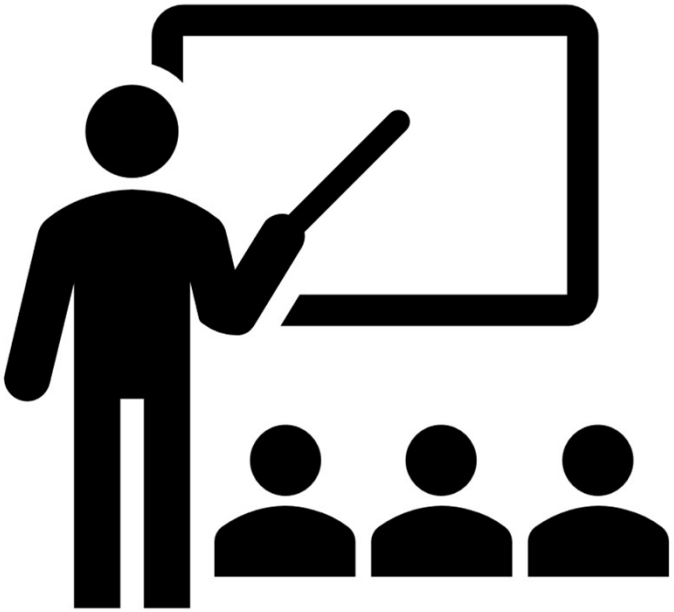
Di conseguenza:

TUTTI DOBBIAMO ESSERE PRONTI

In che modo?

PREVENZIONE E PROTEZIONE

Come prevenire e come proteggersi?



La Prevenzione

1. Analisi e valutazione dei rischi
2. *Vulnerability assessment e penetration test*
3. Definizione di policy aziendali sulla cybersicurezza
4. Formazione e sensibilizzazione
5. Mappatura degli accessi

Come prevenire e come proteggersi?

La Protezione

1. Piano di risposta agli incidenti
2. Policy di *crisis management* e *disaster recovery*
3. Comunicazione tempestiva degli incidenti
4. Firewall, antivirus e crittografia
5. Virtual Private Network

Come prevenire e come proteggersi?

Le misure migliorative

1. Data Protection Impact Assessment (DPIA) e Statement of Applicability (SoA)
2. Sinergia con NIS 2 e AI Act
3. Sistemi di Gestione ISO 27001
4. Consulenze da parte di professionisti

GESTA®
FORNITORI D'ECCELLENZA

Come prevenire e come proteggersi?

E ogni tanto, qualche vittoria…

Arrestati gli hacker di NoName. Maxi operazione in tutta Europa: "Sabotavano per conto di Mosca"

di Giuliano Foschini

In Italia hanno colpito ministeri, infrastrutture e la Finanza. "Reclutati via Telegram, sono tutti simpatizzanti di Putin"

L'ascolto è riservato agli abbonati premium

17 LUGLIO 2025 ALLE 01:00

2 MINUTI DI LETTURA

GRAZIE PER L'ATTENZIONE!

Bibliografia

- Rapporto CLUSIT 2025, Clusit – Security Summit, Marzo 2025
- Operational Summary 1° Semestre 2025: dati ed indicatori della minaccia cyber in italia, Agenzia per la Cybersicurezza Nazionale, 04 Agosto 2025
- NETSCOUT DDoS Threat Intelligence Report / January 2025 to June 2025, NETSCOUT Inc., 27 Agosto 2025

Sitografia

- https://www.futurelearn.com/info/courses/cyber-security-landscape/0/steps/60317
- https://cyberpeaceinstitute.org/news/cyber-dimensions-of-a-hybrid-warfare/
- https://therecord.media/traffic-at-major-ukrainian-internet-service-provider-ukrtelecom-disrupted
- https://www.securitymagazine.com/articles/101858-russia-sponsored-cyber-attack-campaign-targets-networking-devices-critical-infrastructure
- https://www.bbc.com/news/articles/c87e0ydy3d4o
- https://kyivindependent.com/cyber-partisans-hack-russian-tv-to-show-the-truth-about-the-war/
- https://nsfocusglobal.com/the-hacktivist-cyber-attacks-in-the-iran-israel-conflict/
- https://edition.cnn.com/2025/06/18/middleeast/pro-israel-hackers-iran-crypto
- https://www.ilsole24ore.com/art/terzo-giorno-attacchi-hacker-all-italia-giu-molti-siti-banche-AG8vHpzC
- https://www.repubblica.it/tecnologia/2025/02/17/news/nonanme_hacker_russi_ddos_attacco_come_funziona-424009406/
- https://www.repubblica.it/esteri/2025/07/17/news/europol_hacker_russia_arresti-424735666/
- https://www.lacnews24.it/italia-mondo/meloni-e-il-video-fake-il-cremlino-allude-a-un-festino-con-zelensky-e-la-propaganda-russa-se-la-ride-xspg3lnh