

# CYBERFACTORY 4.0

16 DICEMBRE 24  
1 GENNAIO 25

## IN EVIDENZA

**CYBER 4.0, 30 DICEMBRE 2024**

### Futuri scenari di cybersecurity per il 2025

Il panorama della cybersecurity nel 2025 si presenta come un contesto in rapida evoluzione, influenzato da dinamiche geopolitiche, innovazioni tecnologiche, sfide legislative e la crescente interconnessione delle infrastrutture digitali. Questo articolo analizza le tendenze emergenti e le sfide che definiranno la sicurezza informatica nei prossimi anni, fornendo un'analisi approfondita per i professionisti del settore.



[LEGGI TUTTO](#)

**UNITED NATIONS, DECEMBER 24, 2024**

### UN General Assembly adopts landmark convention on cybercrime

The United Nations General Assembly adopted today a new convention to prevent and combat cybercrime, concluding a five-year negotiation process. The UN Convention against Cybercrime aims to prevent and combat cybercrime more efficiently and effectively, including by strengthening international cooperation and by providing technical assistance and capacity-building support, particularly for developing countries.



[LEGGI TUTTO](#)

**PRESIDENZA DEL CONSIGLIO DEI MINISTRI, 16 DICEMBRE 2024**

### Stati generali della diplomazia, l'intervento del Sottosegretario Mantovano

[...] Secondo l'Artificial Intelligence Index Report 2024 dell'Università di Stanford, l'Italia si colloca al 4° posto in Europa per il numero di laureati magistrali in materie informatiche, e al 3° per il numero di dottori di ricerca, dopo Germania e UK. Siamo però deboli quanto alla capacità di trasferire l'innovazione sviluppata negli ambienti accademici e della ricerca nel mondo industriale. Il che rischia di non valorizzare il capitale umano a disposizione, che anche per questo decide di emigrare.



[LEGGI TUTTO](#)

## CYBER 4.0



**CYBER 4.0, 16 DICEMBRE 2024**

### Cyber 5.0 finanzia il progetto SPOTLIGHT

Sistemi & Automazione (S&A) annuncia con orgoglio che il suo progetto SPOTLIGHT è stato selezionato per ricevere un finanziamento mirato nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR). L'iniziativa si colloca tra le attività strategiche promosse da CYBER 4.0 – Cybersecurity Competence Center, volte a rafforzare l'innovazione tecnologica e la sicurezza digitale in Italia.

[LEGGI TUTTO](#)

**UNICAMPUS, 2 DICEMBRE 2024**

### UCBM tra le eccellenze europee selezionate da Virtual Routes con il supporto di Google.org per un'iniziativa di formazione in cybersecurity

[...] Progettato per rispondere alle crescenti esigenze di cybersecurity, il programma di formazione includerà aggiornamenti sulle tecnologie emergenti e attività di coinvolgimento comunitario. Sotto la guida del Prof. Luca Faramondi e sfruttando l'esperienza maturata nel corso di Laurea Magistrale in Sistemi Intelligenti, il progetto garantisce una formazione pratica e orientata allo sviluppo professionale. Le attività pratiche si svolgeranno presso il Cyber Shot Lab, un laboratorio congiunto tra UCBM e Cyber 4.0 (il Centro di Competenza del Ministero per l'Innovazione e il Made in Italy), che consente agli studenti di lavorare su infrastrutture di test che riproducono scenari reali.

[LEGGI TUTTO](#)

## IN ITALIA



**GARANTE PRIVACY, 20 DICEMBRE 2024**

### ChatGPT, il Garante privacy chiude l'istruttoria. OpenAI dovrà realizzare una campagna informativa di sei mesi e pagare una sanzione di 15 milioni di euro

Il Garante per la protezione dei dati personali ha adottato nei giorni scorsi un provvedimento correttivo e sanzionatorio nei confronti di OpenAI in relazione alla gestione del servizio ChatGPT.

Il provvedimento, che accerta le violazioni a suo tempo contestate alla società californiana, arriva all'esito di un'istruttoria avviata nel marzo del 2023 e dopo che l'EDPB (Comitato europeo per la protezione dei dati) ha pubblicato il parere con il quale identifica un approccio comune ad alcune delle più rilevanti questioni relative al trattamento dei dati personali nel contesto della progettazione, sviluppo e distribuzione di servizi basati sull'intelligenza artificiale.

[LEGGI TUTTO](#)

**CYBERSECURITY ITALIA, 24 DICEMBRE 2024**

### Quali sono stati gli attacchi informatici più gravi del 2024?

Il 2024 è stato segnato da una serie di attacchi informatici di portata senza precedenti, colpendo governi, infrastrutture critiche, aziende e privati in tutto il mondo. Questi episodi hanno dimostrato quanto sia cruciale investire nella cybersecurity e migliorare la cooperazione internazionale per fronteggiare minacce sempre più sofisticate. Di seguito, una panoramica degli attacchi più gravi del 2024.

[LEGGI TUTTO](#)



**CYBERSECURITY ITALIA, 18 DICEMBRE 2024**

### La Farnesina si prepara ad una svolta cyber, Tajani: "Presto una riforma del ministero" e nomina Diego Brasioli Inviato Speciale per la Cybersicurezza

L'annuncio del ministro Tajani: "Ho dato mandato al segretario generale di preparare una riforma del ministero per adattarlo ai cambiamenti, con una parte dedicata alla sfida cibernetica e alle minacce ibride". Nominato l'ex ambasciatore del Lussemburgo, Diego Brasioli, Inviato Speciale per la Cybersicurezza e capo dell'Unità per l'innovazione tecnologica e la sicurezza cibernetica."

[LEGGI TUTTO](#)



**HD BUSINESS, 17 DICEMBRE 2024**

### La cybersecurity al centro del dibattito: l'Italia si prepara alla sfida della NIS2

Si è tenuta ieri presso la Sala Stampa della Camera dei deputati la presentazione dell'Osservatorio sulla Cybersicurezza, focalizzata sulla recente direttiva europea NIS2. L'evento, promosso dall'ANGI (Associazione Nazionale Giovani Innovatori) in collaborazione con Tinexta Cyber, ha visto la partecipazione di importanti esponenti del mondo politico e imprenditoriale.

[LEGGI TUTTO](#)



## NEWS INTERNAZIONALI

**CYBERSECURITY 360, 23 DICEMBRE 2024**

### Analisi del rischio e d'impatto dei sistemi di IA: la metodologia europea HUDERIA

Lo scorso 28 novembre 2024, il Committee on Artificial Intelligence (CAI) del Consiglio d'Europa ha adottato la metodologia HUDERIA che ha come obiettivo quello di delineare un approccio strutturato per la valutazione del rischio e dell'impatto dei sistemi di intelligenza artificiale (IA) dal punto di vista dei diritti umani (human rights – HU), della democrazia (democracy – DE) e dello Stato di diritto (rule of law – R) ("HUDERIA"). La metodologia è stata pensata per essere utilizzata sia da attori pubblici che privati per aiutare a identificare e affrontare i rischi e gli impatti sui diritti umani, la democrazia e lo Stato di diritto durante l'intero ciclo di vita dei sistemi di IA.

[LEGGI TUTTO](#)



**U.S. DEPARTMENT OF JUSTICE, DECEMBER 20, 2024**

### United States Charges Dual Russian and Israeli National as Developer of LockBit Ransomware Group

A superseding criminal complaint filed in the District of New Jersey was unsealed today charging a dual Russian and Israeli national for being a developer of the LockBit ransomware group. In August, Rostislav Panev, 51, a dual Russian and Israeli national, was arrested in Israel pursuant to a U.S. provisional arrest request with a view towards extradition to the United States. Panev is currently in custody in Israel pending extradition on the charges in the superseding complaint.

[LEGGI TUTTO](#)



**SECURELIST, DECEMBER 19, 2024**

### Lazarus group evolves its infection chain with old and new malware

Over the past few years, the Lazarus group has been distributing its malicious software by exploiting fake job opportunities targeting employees in various industries, including defense, aerospace, cryptocurrency, and other global sectors. This attack campaign is called the DeathNote campaign and is also referred to as "Operation DreamJob". We have previously published the history of this campaign.

[LEGGI TUTTO](#)



**PROOF POINT, DECEMBER 19 2024**

### Security Brief: Threat Actors Gift Holiday Lures to Threat Landscape

As the holiday season ramps up globally, threat actors have begun to take advantage of people's desires for deals, jobs, and end of year bonuses. Proofpoint researchers have observed an increase in timely, themed content delivering malware, fraud, and credential phishing campaigns. For example, on 18 November, researchers identified a "Winter Holiday Promotion" campaign purporting to be from an airline. The messages were sent in both Spanish and English and contained compressed executables that led to the installation of Remcos RAT.

[LEGGI TUTTO](#)



**KREBS ON SECURITY, DECEMBER 18, 2024**

### How to Lose a Fortune with Just One Bad Click

Adam Griffin is still in disbelief over how quickly he was robbed of nearly \$500,000 in cryptocurrencies. A scammer called using a real Google phone number to warn his Gmail account was being hacked, sent email security alerts directly from google.com, and ultimately seized control over the account by convincing him to click "yes" to a Google prompt on his mobile device.

[LEGGI TUTTO](#)



**INTERPOL, DECEMBER 18, 2024**

### Inside INTERPOL's probe into cyber-enabled human trafficking

An innovative new operation to tackle the emerging trend of human trafficking facilitated by technology, including social media, apps and other digital platforms, has been launched by INTERPOL and the Organization for Security and Co-operation in Europe (OSCE). The initiative is a response to a worrying pattern of victims being trafficked from Latin America, lured by fake or deceptive job offers. They are then taken to another country, increasingly in Europe, where they are subject to exploitation, mainly through prostitution. This first-of-its-kind operation took place from 19 to 22 November 2024, during which the participating officers were supported by INTERPOL's capabilities in human trafficking, facial recognition, cybercrime and criminal analysis.

[LEGGI TUTTO](#)



**COUNCIL OF EUROPE, DECEMBER 12, 2024**

### Convention on Cybercrime: Ecuador becomes the 77th Party and Peru signs the Second Protocol on electronic evidence

Today, 12 December 2024, ECUADOR deposited the instrument of accession to the Convention on Cybercrime (ETS 185). With Ecuador, the Convention now has 77 Parties while two have signed it and 18 have been invited to accede. Moreover, Peru signed the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS 224). With this, 48 States have signed it of which two are already Parties.

[LEGGI TUTTO](#)



**FBI, DECEMBER 23, 2024**

### FBI, DC3, and NPA Identification of North Korean Cyber Actors, Tracked as TraderTraitor, Responsible for Theft of \$308 Million USD from Bitcoin.DMM.com

The Federal Bureau of Investigation, Department of Defense Cyber Crime Center, and National Police Agency of Japan are alerting the public to the theft of cryptocurrency worth \$308 million U.S. dollars from the Japan-based cryptocurrency company DMM by North Korean cyber actors in May 2024. The theft is affiliated with TraderTraitor threat activity, which is also tracked as Jade Sleet, UNC4899, and Slow Pisces. TraderTraitor activity is often characterized by targeted social engineering directed at multiple employees of the same company simultaneously.

[LEGGI TUTTO](#)



## Nuove Pubblicazioni

ENISA, Annual Report – Trust Services Security Incidents 2023, December 20, 2024

CSIRT Italia, Report su minaccia ransomware, 19 Dicembre 2024

CSIRT Italia, La Settimana Cibernetica del 22 dicembre 2024

European Data Protection Board, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, December 17, 2024

U.S. House of Representatives, Bipartisan House Task Force Report on Artificial Intelligence, December 2024

## Prossimi Eventi

UCBM, Cybersecurity Seminar Program 2025, Martedì 28 Gennaio 2025 ore 14.00, Sala Conferenze PRABB