Cybersecurity Database

REPORT

ARTEX, lo strumento di attacco con l'intelligenza artificiale segnalato da FBI e CERT-EU (2026)

ARTEX è nato come strumento open source per i test di penetrazione automatici guidati da modelli linguistici, ma da agosto 2026 lo usano gruppi criminali e statali contro organizzazioni di tutto il mondo. Il 5 novembre CERT-EU e il 13 novembre l'FBI hanno lanciato l'allarme; il 19 novembre la Commissione europea ha confermato una campagna cyber condotta con uno strumento di IA, che il 23 novembre ha portato al furto dei dati degli utenti di EU Academy. Cosa sappiamo, quali norme e standard contano e cosa fare subito.

Edizione	Dati al 26 novembre 2026
Versione sempre aggiornata	https://www.cybersecuritydatabase.org/it/reports/artex-ai-hacking-tool/
Licenza	CC BY 4.0: libero riuso citando la fonte

A chi serve: Per i giornalisti e per chi lavora nei settori colpiti: i fatti confermati dalle fonti ufficiali, le norme e gli standard collegati e le misure raccomandate dalle autorità.

> ARTEX è una piattaforma di test di penetrazione «autonoma»: chi la usa descrive l'obiettivo a parole e una squadra di agenti basati su modelli linguistici esegue da sola ricognizione, sfruttamento delle falle ed esfiltrazione dei dati. Pubblicata su GitHub a luglio 2026 per i test autorizzati, da agosto è usata da criminali e gruppi statali: secondo l'FBI alcune intrusioni sono passate dal primo contatto ai privilegi di amministratore in meno di tre ore. Il repository è stato ritirato l'8 ottobre, ma copie, varianti e una versione commerciale restano in circolazione. CERT-EU il 5 novembre e l'FBI il 13 novembre hanno avvertito che la sua diffusione accelera gli attacchi contro i sistemi esposti su internet. Il 19 novembre la Commissione europea ha confermato di aver subito, da ottobre, una «campagna cyber generata con l'IA»; il 23 novembre ha confermato che sono trapelati nomi e indirizzi email degli utenti della piattaforma EU Academy. Il 24 novembre anche la Svizzera ha confermato i primi attacchi riusciti con agenti di IA contro infrastrutture critiche.

< 3 h
dal primo contatto ai privilegi di amministratore, in alcune intrusioni (FBI)

1600+
console di ARTEX esposte su internet a inizio novembre (FBI)

2250+
clienti a valle presi di mira nell'attacco alla catena di fornitura di ConnectWise (FBI)

Cosa fare subito

Le raccomandazioni dell'FBI e di CERT-EU per ridurre il rischio di un attacco con ARTEX o strumenti simili.

1. Fare l'inventario di tutto ciò che è esposto su internet, compresi portali di partner e fornitori, backend delle app, applicazioni dei singoli reparti e servizi vecchi, e spegnere ciò che non serve.
2. Rendere raggiungibili le console di amministrazione del cloud e della rete, le piattaforme di backup e gli altri servizi sensibili solo da reti fidate o canali dedicati, non da internet.
3. Applicare le patch d'urgenza ai sistemi esposti e non lasciare in sospeso le vulnerabilità giudicate poco gravi: uno strumento automatico le concatena.
4. Usare l'autenticazione a più fattori, il principio del privilegio minimo per account e applicazioni e controllare nuove credenziali, assegnazioni di privilegi e accessi da reti mai viste.
5. Non mostrare a chi non è autenticato messaggi d'errore dettagliati, cercare e sostituire le credenziali rimaste nel codice e nelle pipeline, mettere limiti di frequenza alle API e ai portali.
6. Conservare i registri di accesso e di audit, sorvegliare l'uso di strumenti di IA nella propria rete e segnalare un sospetto incidente con ARTEX alle autorità (in Europa il CSIRT nazionale, negli Stati Uniti IC3).

Cronologia

Data	Cosa è successo	Fonti
8 ottobre 2026	Lo sviluppatore «Autumn-27», che aveva pubblicato ARTEX su GitHub a luglio dichiarandolo destinato ai soli test autorizzati, rende il repository non disponibile dopo le notizie sull'uso da parte di attaccanti. Secondo l'FBI lo strumento resta però accessibile tramite fork, copie archiviate e una versione commerciale, ARTEX PRO; gli attacchi con ARTEX sono osservati almeno da agosto 2026.	[1]
5 novembre 2026	CERT-EU, il servizio di cybersicurezza delle istituzioni dell'UE, pubblica l'analisi «Beware of ARTEX»: diversi attori malevoli in tutto il mondo usano lo strumento, e CERT-EU ha osservato contro le istituzioni che protegge attività simili, guidate dall'IA, con ogni probabilità condotte con ARTEX. La disponibilità pubblica dello strumento, avverte, ne accelererà l'adozione.	[2]
13 novembre 2026	L'FBI diffonde l'avviso FLASH-20261113-001 su ARTEX, con tecniche osservate, indicatori di compromissione e raccomandazioni. I settori colpiti vanno dai servizi finanziari alla pubblica amministrazione, dalla difesa ai semiconduttori, dall'energia alla sanità; fra le campagne citate, un attacco a istituti finanziari sudcoreani e la compromissione della catena di fornitura di ConnectWise Cloud Backup. L'FBI chiede di segnalare gli incidenti con ARTEX a IC3.	[1]
19 novembre 2026	Al briefing di mezzogiorno il portavoce della Commissione europea conferma una «campagna cyber» contro la Commissione, individuata il 22 ottobre e confermata il 26 ottobre dopo le prime verifiche: per precauzione diverse applicazioni sono state spente e la maggior parte è già stata ripristinata. È stata una campagna «generata con l'IA», con uno strumento di IA disponibile pubblicamente; finora nessuna prova di una violazione dei dati di tutto il personale e nessuna richiesta di riscatto nota. La Commissione è in contatto con CERT-EU e con il Garante europeo della protezione dei dati e non indica il responsabile.	[4]
23 novembre 2026	La Commissione conferma che la campagna ha colpito anche la piattaforma EU Academy, che offre corsi online sulle politiche dell'UE a utenti esterni: sono trapelati dati personali degli utenti, fra cui nomi e indirizzi email. La portata è ancora da accertare; l'accesso pubblico alla piattaforma è stato sospeso, gli utenti sono stati avvisati con un messaggio sul sito e il Garante europeo della protezione dei dati è stato informato. Nessuna attribuzione finché l'indagine non sarà conclusa.	[5]
24 novembre 2026	Il Centro nazionale per la cibersicurezza svizzero (NCSC/UFCS) conferma i primi casi in Svizzera di attacchi condotti con agenti di IA («Agentic Offensive Frameworks») contro aziende e gestori di infrastrutture critiche di almeno due settori: in tutti i casi noti gli attaccanti sono riusciti a compromettere i sistemi. Secondo l'NCSC gli agenti di IA raggiungibili da internet, come ARTEX o CyberStrikeAI, sono quasi raddoppiati da ottobre 2026; raccomanda di installare gli aggiornamenti critici dei sistemi esposti entro 24 ore.	[3]

Paesi colpiti

Paese	Casi segnalati
Unione europea	CERT-EU ha osservato contro le istituzioni, gli organi e le agenzie dell'UE attività guidate dall'IA, con ogni probabilità condotte con ARTEX. La Commissione europea ha confermato una campagna «generata con l'IA», individuata il 22 ottobre, con uno strumento di IA disponibile pubblicamente, senza nominarlo; secondo la stampa CERT-EU vi ha riconosciuto ARTEX. Diverse applicazioni interne sono state spente per precauzione (secondo la stampa, per oltre dieci giorni i sistemi per stipendi, ferie e rimborsi medici e i servizi di traduzione: The Record, 19 novembre). Il 23 novembre la Commissione ha confermato il furto di nomi e indirizzi email degli utenti esterni della piattaforma EU Academy, ora chiusa al pubblico. [2] [4] [5] [6]
Corea del Sud	Secondo l'FBI, attacchi a scopo di lucro contro istituti finanziari sudcoreani condotti con ARTEX hanno portato all'esfiltrazione dei dati personali di circa 67.000 persone. [1]
Svizzera	L'NCSC svizzero ha ricevuto le prime segnalazioni di attacchi condotti con agenti di IA contro organizzazioni e gestori di infrastrutture critiche di almeno due settori, tutti andati a segno; condivide con i gestori delle infrastrutture critiche gli indicatori tecnici per riconoscerli. [3]

Come funziona ARTEX

Secondo l'FBI ARTEX è una piattaforma multi-agente scritta in Go che traduce obiettivi descritti in linguaggio naturale in comandi eseguiti da agenti specializzati, con un intervento umano minimo dopo la definizione dell'obiettivo. Non contiene un proprio modello: si collega a modelli linguistici esterni, commerciali o open source. Nelle istanze controllate dagli attaccanti analizzate dall'FBI prevalgono modelli di origine cinese, scelti per costo e capacità e per l'assenza di limiti visibili quando la richiesta è presentata come un test di penetrazione.

Lo strumento è particolarmente efficace sulle parti periferiche: portali per partner e fornitori, backend delle app, applicazioni per i dipendenti, servizi vecchi, integrazioni con terzi. Fra le tecniche osservate dall'FBI ci sono l'uso di credenziali cloud esposte, asserzioni SAML non firmate, falle XXE e SSRF, password di amministratore scritte nel codice e la risalita da un fornitore compromesso ai clienti tramite le relazioni di fiducia.

Il punto, per FBI e CERT-EU, non è una falla nuova ma la velocità: un piccolo gruppo con poche competenze può portare avanti più intrusioni insieme e completare l'attacco prima che i difensori reagiscano, anche se il traffico che genera è rumoroso e può far scattare gli allarmi.

Perché se ne parla

È uno dei primi casi documentati da autorità di più paesi in cui un agente di IA a disposizione di tutti viene usato su larga scala per attacchi reali, e il primo che tocca direttamente la Commissione europea. Per le organizzazioni cambia la misura del tempo: le falle note ma non ancora corrette e i sistemi dimenticati su internet vengono trovati e sfruttati in ore, non in settimane.

Il caso riapre anche il tema degli strumenti a doppio uso: ARTEX è nato per i test autorizzati, e lo stesso tipo di automazione serve a chi difende per trovare prima le proprie debolezze. Per questo CERT-EU raccomanda di tenere d'occhio l'uso degli strumenti di IA nella propria rete e di non

lasciare in sospeso le falle giudicate poco gravi.

Cosa dicono le norme

Gli atti del database che riguardano la sicurezza delle istituzioni UE, i sistemi di IA e la gestione del rischio informatico.

Regolamento (UE, Euratom) 2023/2841 che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione

Il regolamento sulla cybersicurezza delle istituzioni, degli organi e degli organismi dell'Unione: impone a ciascuno misure di gestione del rischio e la notifica degli incidenti gravi a CERT-EU, che ne fa da servizio comune. È la cornice dell'attacco alla Commissione e dell'allarme di CERT-EU.

Direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (Direttiva NIS 2)

Per le aziende e gli enti dei settori essenziali e importanti, NIS 2 chiede gestione delle vulnerabilità, sicurezza della catena di fornitura e notifica rapida degli incidenti (art. 21 e 23): le misure che ARTEX mette alla prova, con tempi d'attacco di ore.

Regolamento (UE) 2024/1689 che stabilisce regole armonizzate sull'intelligenza artificiale (regolamento sull'intelligenza artificiale)

Il regolamento sull'intelligenza artificiale chiede ai fornitori di modelli di IA per finalità generali con rischio sistemico di valutare e attenuare i rischi sistemici e di garantire un livello adeguato di cybersicurezza (art. 55); fra i rischi sistemici il considerando 110 cita le capacità cyber offensive, come la scoperta e lo sfruttamento delle vulnerabilità. Il caso mostra perché contano.

Gli standard di riferimento

Gli standard del database più utili per ridurre la superficie d'attacco e governare l'uso dell'IA.

CIS Controls v8.1 – Controlli di sicurezza critici del CIS

I controlli 1 e 2 (inventario dei sistemi e del software), 7 (gestione continua delle vulnerabilità) e 12 (gestione dell'infrastruttura di rete) sono la prima difesa contro uno strumento che cerca proprio i sistemi dimenticati.

OWASP Top 10:2025 – OWASP Top 10:2025 – I dieci rischi di sicurezza più critici per le applicazioni web

Le falle sfruttate da ARTEX secondo l'FBI (controllo degli accessi, configurazioni errate, SSRF, credenziali nel codice) sono le categorie dell'OWASP Top 10: un elenco da usare per controllare portali e applicazioni web esposte.

NIST CSF 2.0 – Framework di cybersicurezza del NIST (CSF) 2.0

Il quadro per organizzare la difesa: inventario e gestione dei fornitori (Govern e Identify), protezione degli accessi, rilevamento e risposta rapida (Detect e Respond), che con attacchi di poche ore devono essere già pronti.

NIST AI RMF 1.0 – Framework per la gestione del rischio dell'intelligenza artificiale (AI RMF 1.0)

Il quadro del NIST per gestire i rischi dei sistemi di IA: utile a chi sviluppa o usa agenti di IA, anche per i test di sicurezza, per definire usi ammessi, controlli e responsabilità.

ISO/IEC 42001:2023 – Tecnologie dell'informazione – Intelligenza artificiale – Sistema di gestione

Il sistema di gestione per l'IA: regole interne su quali strumenti di IA si possono usare, da chi e con quali controlli, come chiede CERT-EU quando raccomanda di sorvegliare l'uso dell'IA nella propria rete.

Fonti dell'analisi

1. **Fonti ufficiali:** Federal Bureau of Investigation (FBI), FLASH-20261113-001 – Threat Overview of ARTEX Autonomous Penetration Testing Framework ↗, 13 novembre 2026. https://www.ic3.gov/csa/2026/261113.pdf
2. CERT-EU, From Penetration Testing to Cyber Threat: Beware of ARTEX ↗, 5 novembre 2026. https://cert.europa.eu/blog/from-penetration-testing-to-cyber-threat-beware-of-artex
3. National Cyber Security Centre (NCSC), Switzerland, Cyberattacks involving AI agents: First confirmed cases in Switzerland ↗, 24 novembre 2026. https://www.bacs.admin.ch/en/26-ki-agenten-1-en
4. European Commission – Audiovisual Service, EC Midday press briefing of 19/11/2026 – Cybersecurity: Cyber campaign against the European Commission, Q&A ↗, 19 novembre 2026. https://audiovisual.ec.europa.eu/en/media/video/I-298222
5. European Commission – Audiovisual Service, EC Midday press briefing of 23/11/2026 – Cybersecurity: Cyber campaign against the European Commission, Q&A ↗, 23 novembre 2026. https://audiovisual.ec.europa.eu/en/media/video/I-298395

6. **Stampa:** The Record (Recorded Future News), European Commission confirms cyberattack, says hackers used AI tool ↗, 19 novembre 2026.https://therecord.media/european-commission-confirms-cyberattack-using-ai

Per una risposta pratica

- A chi e entro quando notificare un incidente, paese per paese
- Le autorità nazionali e i CSIRT di ogni paese
- La pagina del tuo settore: leggi UE, atti specifici e standard

Fonti e dati

Ricostruzione «cosa sappiamo» basata sull'avviso FLASH dell'FBI e sull'analisi di CERT-EU, sulle dichiarazioni del portavoce della Commissione europea ai briefing di mezzogiorno del 19 e 23 novembre e, dove indicato, su testate giornalistiche. Vale per i fatti noti alla data indicata. Fanno fede le fonti citate.

- Pagina interattiva: Standard e framework https://www.cybersecuritydatabase.org/it/standards/
- Dati aperti (JSON): documents.json https://www.cybersecuritydatabase.org/api/v1/documents.json

Come citare

Cybersecurity Database, «ARTEX, lo strumento di attacco con l'intelligenza artificiale segnalato da FBI e CERT-EU (2026)», dati al 26 novembre 2026, https://www.cybersecuritydatabase.org/it/reports/artex-ai-hacking-tool/. Licenza CC BY 4.0.