Cybersecurity Database

Informe

ARTEX, la herramienta de ataque con inteligencia artificial señalada por el FBI y el CERT-EU (2026)

ARTEX nació como una herramienta de código abierto para pruebas de penetración automáticas guiadas por modelos de lenguaje, pero desde agosto de 2026 la usan grupos criminales y estatales contra organizaciones de todo el mundo. El CERT-EU dio la alarma el 5 de noviembre y el FBI el 13 de noviembre; el 19 de noviembre la Comisión Europea confirmó una campaña cibernética realizada con una herramienta de IA, que el 23 de noviembre reconoció que había llevado al robo de datos de los usuarios de EU Academy. Qué se sabe, qué normas y estándares cuentan y qué hacer ya.

Edición	Datos a 27 de noviembre de 2026
Versión siempre actualizada	https://www.cybersecuritydatabase.org/es/reports/artex-ai-hacking-tool/
Licencia	CC BY 4.0: libre reutilización citando la fuente

A quién sirve: Para periodistas y para quien trabaja en los sectores afectados: los hechos confirmados por las fuentes oficiales, las normas y estándares relacionados y las medidas recomendadas por las autoridades.

> ARTEX es una plataforma de pruebas de penetración «autónoma»: quien la usa describe el objetivo con palabras y un equipo de agentes basados en modelos de lenguaje realiza por sí solo el reconocimiento, la explotación de fallos y la exfiltración de datos. Publicada en GitHub en julio de 2026 para pruebas autorizadas, desde agosto la usan delincuentes y grupos estatales: según el FBI, algunas intrusiones pasaron del primer contacto a privilegios de administrador en menos de tres horas. El repositorio se retiró el 8 de octubre, pero siguen circulando copias, variantes y una versión comercial. El CERT-EU el 5 de noviembre y el FBI el 13 de noviembre advirtieron de que su difusión acelera los ataques contra los sistemas expuestos en internet. El 19 de noviembre la Comisión Europea confirmó haber sufrido, desde octubre, una «campaña cibernética generada con IA»; el 23 de noviembre confirmó la filtración de nombres y direcciones de correo de los usuarios de la plataforma EU Academy. El 24 de noviembre también Suiza confirmó sus primeros ataques con éxito con agentes de IA contra infraestructuras críticas, y el 26 de noviembre la BSI alemana advirtió de que estas herramientas ya están maduras para un uso a gran escala.

< 3 h
del primer contacto a privilegios de administrador, en algunas intrusiones (FBI)

1600+
consolas de ARTEX expuestas en internet a principios de noviembre (FBI)

2250+
clientes posteriores atacados en el ataque a la cadena de suministro de ConnectWise (FBI)

Qué hacer ya

Las recomendaciones del FBI y del CERT-EU para reducir el riesgo de un ataque con ARTEX o herramientas similares.

1. Hacer inventario de todo lo expuesto en internet, incluidos portales de socios y proveedores, backends de aplicaciones móviles, aplicaciones creadas por cada departamento y servicios antiguos, y apagar lo que no haga falta.
2. Hacer accesibles las consolas de administración de la nube y de la red, las plataformas de copia de seguridad y los demás servicios sensibles solo desde redes de confianza o canales dedicados, no desde internet.
3. Aplicar los parches de urgencia a los sistemas expuestos y no dejar pendientes las vulnerabilidades consideradas leves: una herramienta automática las encadena.
4. Usar autenticación multifactor y mínimo privilegio para cuentas y aplicaciones, y vigilar nuevas credenciales, asignaciones de privilegios e inicios de sesión desde redes nunca vistas.
5. No mostrar mensajes de error detallados a usuarios no autenticados, buscar y sustituir las credenciales que queden en el código y en las pipelines, y limitar la frecuencia de las API y los portales.

6. Conservar los registros de acceso y auditoría, vigilar el uso de herramientas de IA en la propia red y notificar un posible incidente con ARTEX a las autoridades (en Europa el CSIRT nacional, en Estados Unidos el IC3).

Cronología

Fecha	Qué ocurrió	Fuentes
8 de octubre de 2026	El desarrollador «Autumn-27», que había publicado ARTEX en GitHub en julio declarándolo destinado solo a pruebas autorizadas, deja el repositorio no disponible tras las noticias sobre su uso por atacantes. Según el FBI, la herramienta sigue siendo accesible mediante forks, copias archivadas y una versión comercial, ARTEX PRO; se observan ataques con ARTEX al menos desde agosto de 2026.	[1]
5 de noviembre de 2026	El CERT-EU, el servicio de ciberseguridad de las instituciones de la UE, publica el análisis «Beware of ARTEX»: varios actores maliciosos de todo el mundo usan la herramienta, y el CERT-EU ha observado contra las instituciones que protege actividades similares, guiadas por IA, muy probablemente realizadas con ARTEX. La disponibilidad pública de la herramienta, advierte, acelerará su adopción.	[2]
13 de noviembre de 2026	El FBI difunde el aviso FLASH-20261113-001 sobre ARTEX, con las técnicas observadas, indicadores de compromiso y recomendaciones. Los sectores afectados van de los servicios financieros a la administración pública, de la defensa a los semiconductores, de la energía a la sanidad; entre las campañas citadas, un ataque a entidades financieras surcoreanas y el compromiso de la cadena de suministro de ConnectWise Cloud Backup. El FBI pide notificar al IC3 los incidentes con ARTEX.	[1]
19 de noviembre de 2026	En el briefing de mediodía el portavoz de la Comisión Europea confirma una «campaña cibernética» contra la Comisión, detectada el 22 de octubre y confirmada el 26 de octubre tras las primeras comprobaciones: por precaución se apagaron varias aplicaciones y la mayoría ya se ha restablecido. Fue una campaña «generada con IA», con una herramienta de IA disponible públicamente; por ahora no hay pruebas de una violación de datos de todo el personal ni peticiones de rescate conocidas. La Comisión está en contacto con el CERT-EU y con el Supervisor Europeo de Protección de Datos y no señala al responsable.	[5]
23 de noviembre de 2026	La Comisión confirma que la campaña afectó también a la plataforma EU Academy, que ofrece cursos en línea sobre las políticas de la UE a usuarios externos: se filtraron datos personales de los usuarios, entre ellos nombres y direcciones de correo. El alcance aún se está investigando; se ha suspendido el acceso público a la plataforma, se avisó a los usuarios con un mensaje en el sitio y se informó al Supervisor Europeo de Protección de Datos. No habrá atribución hasta que concluya la investigación.	[6]

Fecha	Qué ocurrió	Fuentes
24 de noviembre de 2026	El Centro Nacional de Ciberseguridad suizo (NCSC) confirma los primeros casos en Suiza de ataques realizados con agentes de IA («Agentic Offensive Frameworks») contra empresas y operadores de infraestructuras críticas de al menos dos sectores: en todos los casos conocidos los atacantes lograron comprometer los sistemas. Según el NCSC, los agentes de IA accesibles desde internet, como ARTEX o CyberStrikeAI, casi se han duplicado desde octubre de 2026; recomienda instalar las actualizaciones críticas de los sistemas expuestos en un plazo de 24 horas.	[3]
26 de noviembre de 2026	La Oficina Federal alemana de Seguridad de la Información (BSI) advierte de que los «Agentic Offensive Frameworks» como ARTEX, CAIRN o PentAGI han pasado del experimento al uso operativo y, según sus propios análisis, confirma su alto grado de madurez. Funcionan incluso con modelos de libre acceso y reducen mucho los conocimientos necesarios; la BSI prevé un fuerte aumento de la calidad y la cantidad de los ataques y considera que las infraestructuras accesibles desde internet serán comprometidas si no se corrigen las vulnerabilidades. Pide eliminar contraseñas débiles o por defecto e interfaces sin proteger, contar con un plan de emergencia y cerrar de inmediato las vías de ataque más sencillas.	[4]

Países afectados y estado de las normas de la UE

País	Casos notificados	SRI 2	CER
Unión Europea	El CERT-EU ha observado contra las instituciones, órganos y agencias de la UE actividades guiadas por IA, muy probablemente realizadas con ARTEX. La Comisión Europea confirmó una campaña «generada con IA», detectada el 22 de octubre, con una herramienta de IA disponible públicamente, sin nombrarla; según la prensa, el CERT-EU identificó ARTEX. Varias aplicaciones internas se apagaron por precaución (según la prensa, durante más de diez días los sistemas de nóminas, vacaciones y reembolsos médicos y los servicios de traducción: The Record, 19 de noviembre). El 23 de noviembre la Comisión confirmó el robo de nombres y direcciones de correo de los usuarios externos de la plataforma EU Academy, ahora cerrada al público. [2] [5] [6] [7]	–	–
Corea del Sur	Según el FBI, ataques con ánimo de lucro realizados con ARTEX contra entidades financieras surcoreanas llevaron a la exfiltración de los datos personales de unas 67.000 personas. [1]	–	–

País	Casos notificados	SRI 2	CER
Suiza	El NCSC suizo ha recibido las primeras notificaciones de ataques realizados con agentes de IA contra organizaciones y operadores de infraestructuras críticas de al menos dos sectores, todos con éxito; comparte con los operadores de infraestructuras críticas los indicadores técnicos para detectarlos. [3]	–	–
Alemania	La BSI señala que se multiplican los incidentes en los que se sospecha, y en parte se ha demostrado, el uso de estas herramientas, y confirma según sus propios análisis el alto grado de madurez de los «Agentic Offensive Frameworks». [4]	Transpuesta, en vigor	Transpuesta, en vigor

El estado de SRI 2 y de la CER procede de las páginas de transposición del sitio y se actualiza con los datos.

Cómo funciona ARTEX

Según el FBI, ARTEX es una plataforma multiagente escrita en Go que convierte objetivos descritos en lenguaje natural en comandos ejecutados por agentes especializados, con una intervención humana mínima una vez fijado el objetivo. No contiene un modelo propio: se conecta a modelos de lenguaje externos, comerciales o de código abierto. En las instancias controladas por los atacantes analizadas por el FBI predominan los modelos de origen chino, elegidos por coste y capacidad y por la ausencia de límites visibles cuando la petición se presenta como una prueba de penetración.

La herramienta es especialmente eficaz en los sistemas periféricos: portales de socios y proveedores, backends de aplicaciones móviles, aplicaciones para empleados, servicios antiguos, integraciones con terceros. Entre las técnicas observadas por el FBI están el uso de credenciales de nube expuestas, aserciones SAML sin firmar, fallos XXE y SSRF, contraseñas de administrador escritas en el código y el paso de un proveedor comprometido a sus clientes a través de las relaciones de confianza.

Lo importante, para el FBI y el CERT-EU, no es un fallo nuevo sino la velocidad: un grupo pequeño con pocos conocimientos puede llevar a cabo varias intrusiones a la vez y completar el ataque antes de que los defensores reaccionen, aunque el tráfico que genera es ruidoso y puede activar alertas.

Por qué se habla de ello

Es uno de los primeros casos documentados por autoridades de varios países en que un agente de IA al alcance de cualquiera se usa a gran escala para ataques reales, y el primero que afecta directamente a la Comisión Europea. Para las

organizaciones cambia la escala de tiempo: los fallos conocidos pero no corregidos y los sistemas olvidados en internet se encuentran y explotan en horas, no en semanas.

El caso reabre también el debate sobre las herramientas de doble uso: ARTEX nació para pruebas autorizadas, y el mismo tipo de automatización sirve a quien defiende para encontrar antes sus propias debilidades. Por eso el CERT-EU recomienda vigilar el uso de herramientas de IA en la propia red y no dejar pendientes los fallos considerados leves.

Qué dicen las normas

Los actos de la base de datos que afectan a la seguridad de las instituciones de la UE, a los sistemas de IA y a la gestión del riesgo cibernético.

Reglamento (UE, Euratom) 2023/2841 por el que se establecen medidas destinadas a garantizar un elevado nivel común de ciberseguridad en las instituciones, los órganos y los organismos de la Unión

El reglamento sobre ciberseguridad de las instituciones, órganos y organismos de la Unión: exige a cada uno medidas de gestión del riesgo y la notificación de los incidentes significativos al CERT-EU, que actúa como su servicio común. Es el marco del ataque a la Comisión y de la alerta del CERT-EU.

Directiva (UE) 2022/2555 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva SRI 2)

Para las empresas y entidades de los sectores esenciales e importantes, NIS 2 exige gestión de vulnerabilidades, seguridad de la cadena de suministro y notificación rápida de incidentes (arts. 21 y 23): las medidas que ARTEX pone a prueba, con ataques que duran horas.

Reglamento (UE) 2024/1689 por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial)

El Reglamento de inteligencia artificial exige a los proveedores de modelos de IA de uso general con riesgo sistémico evaluar y mitigar los riesgos sistémicos y garantizar un nivel adecuado de ciberseguridad (art. 55); entre los riesgos sistémicos, el considerando 110 cita las capacidades cibernéticas ofensivas, como el descubrimiento y la explotación de vulnerabilidades. El caso muestra por qué importan.

Los estándares de referencia

Los estándares de la base de datos más útiles para reducir la superficie de ataque y gobernar el uso de la IA.

CIS Controls v8.1 – Controles de seguridad críticos del CIS

Los controles 1 y 2 (inventario de activos y software), 7 (gestión continua de vulnerabilidades) y 12 (gestión de la infraestructura de red) son la primera defensa frente a una herramienta que busca precisamente los sistemas olvidados.

OWASP Top 10:2025 – OWASP Top 10:2025 – Los diez riesgos de seguridad más críticos de las aplicaciones web

Los fallos explotados por ARTEX según el FBI (control de acceso, configuraciones erróneas, SSRF, credenciales en el código) son categorías del OWASP Top 10: una lista para revisar portales y aplicaciones web expuestos.

NIST CSF 2.0 – Marco de ciberseguridad del NIST (CSF) 2.0

El marco para organizar la defensa: inventario y gestión de proveedores (Govern e Identify), protección de los accesos, detección y respuesta rápidas (Detect y Respond), que deben estar listas cuando los ataques duran pocas horas.

NIST AI RMF 1.0 – Marco de gestión de riesgos de la inteligencia artificial (AI RMF 1.0)

El marco del NIST para gestionar los riesgos de los sistemas de IA: útil para quien desarrolla o usa agentes de IA, también en pruebas de seguridad, para definir usos permitidos, controles y responsabilidades.

ISO/IEC 42001:2023 – Tecnologías de la información – Inteligencia artificial – Sistema de gestión

El sistema de gestión de la IA: reglas internas sobre qué herramientas de IA pueden usarse, por quién y con qué controles, como pide el CERT-EU cuando recomienda vigilar el uso de la IA en la propia red.

Fuentes del análisis

1. **Fuentes oficiales:** Federal Bureau of Investigation (FBI), FLASH-20261113-001 – Threat Overview of ARTEX Autonomous Penetration Testing Framework ↗, 13 de noviembre de 2026.https://www.ic3.gov/csa/2026/261113.pdf
2. CERT-EU, From Penetration Testing to Cyber Threat: Beware of ARTEX ↗, 5 de noviembre de 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 de noviembre de 2026.https://www.bacs.admin.ch/en/26-ki-agenten-1-en
4. Bundesamt für Sicherheit in der Informationstechnik (BSI), Hoher Reifegrad von Agentic Offensive Frameworks verschärft Bedrohungslage ↗, 26 de noviembre de 2026.https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Offensive-agentische-KI_261115.html
5. European Commission – Audiovisual Service, EC Midday press briefing of 19/11/2026 – Cybersecurity: Cyber campaign against the European Commission, Q&A ↗, 19 de noviembre de 2026.https://audiovisual.ec.europa.eu/en/media/video/I-298222
6. European Commission – Audiovisual Service, EC Midday press briefing of 23/11/2026 – Cybersecurity: Cyber campaign against the European Commission, Q&A ↗, 23 de noviembre de 2026.https://audiovisual.ec.europa.eu/en/media/video/I-298395
7. **Prensa:** The Record (Recorded Future News), European Commission confirms cyberattack, says hackers used AI tool ↗, 19 de noviembre de 2026.https://therecord.media/european-commission-confirms-cyberattack-using-ai

Para una respuesta práctica

- A quién y en qué plazo notificar un incidente, país por país
- Las autoridades nacionales y los CSIRT de cada país
- La página de su sector: leyes de la UE, actos específicos y normas

Fuentes y datos

Resumen «qué se sabe» basado en el aviso FLASH del FBI, en el análisis del CERT-EU, en las declaraciones del portavoz de la Comisión Europea en los briefings de mediodía del 19 y el 23 de noviembre y, donde se indica, en medios de comunicación. Vale para los hechos conocidos en la fecha indicada. Prevalecen las fuentes citadas.

- Página interactiva: SRI 2 https://www.cybersecuritydatabase.org/es/transposition/nis2/
- Página interactiva: REC https://www.cybersecuritydatabase.org/es/transposition/cer/
- Página interactiva: Normas y marcos https://www.cybersecuritydatabase.org/es/standards/
- Datos abiertos (JSON): documents.json https://www.cybersecuritydatabase.org/api/v1/documents.json

Cómo citar

Cybersecurity Database, «ARTEX, la herramienta de ataque con inteligencia artificial señalada por el FBI y el CERT-EU (2026)», datos a 27 de noviembre de 2026, https://www.cybersecuritydatabase.org/es/reports/artex-ai-hacking-tool/. Licencia CC BY 4.0.