Mainsoft®

BOLETÍN INFORMATIVO

#229 | Julio 2026

JFrog confirma que los modelos de OpenAI explotaron la vulnerabilidad de día cero de Artifactory antes de la brecha de seguridad de Hugging Face.

JFrog ha confirmado que los modelos de OpenAI explotaron una vulnerabilidad de día cero en Artifactory, una instalación autoalojada, al intentar acceder a internet desde un entorno de evaluación sellado.

ver artículo >>

Chaos Ransomware Uses msaRAT to Route C2 Traffic Through Headless Chrome and Edge

The Chaos ransomware group ran its command-and-control through the victim's own browser. Cisco Talos on Thursday detailed msaRAT, the Rust implant behind it, found on a compromised Windows machine ahead of the encryptor

ver artículo >>

La botnet Tengu reinicia los dispositivos Linux comprometidos cuando los defensores terminan su proceso.

Una nueva botnet derivada de Mirai, llamada Tengu, puede utilizar el mecanismo de vigilancia de hardware de un dispositivo Linux comprometido para provocar un reinicio cuando los defensores finalizan su proceso principal.

ver artículo >>

INCIDENTES DE SISTEMAS

Se ha publicado una prueba de concepto sobre una vulnerabilidad de desbordamiento de búfer en Nginx que permite a los atacantes ejecutar código arbitrario.

Un desbordamiento de búfer de montón de alta gravedad en NGINX Plus y NGINX Open Source puede permitir que atacantes no autenticados bloqueen los procesos de trabajo y, bajo ciertas condiciones, ejecuten código arbitrario

ver artículo >>

Cómo el ataque DCSync ayuda a los hackers a robar silenciosamente hashes de contraseñas de Active Directory

Active Directory es el núcleo de la identidad en la mayoría de las empresas, y su secreto más valioso es el hash de la contraseña de cada cuenta de usuario, servicio y máquina.

ver artículo >>

RECOMENDACIONES DE LECTURA DE SEGURIDAD

Coca-Cola confirma que unos hackers robaron datos en el ataque de ransomware contra FairLife.

Coca-Cola ha confirmado que el ataque de ransomware contra su filial láctea Fairlife implicó el robo de datos de la empresa, semanas después de que el incidente detuviera temporalmente la producción en sus instalaciones de Estados Unidos.

ver artículo >>


Hugging Face breach re
open-weights debate, ra
questions

The first publicly documented cyberattack run end-to-
was an OpenAI benchmark test that escaped its sand
Face.

In an incident post-mortem compiled with the input fr
several hundred members of Cloud Security Alliance's
nonprofit organization laid out the most salient points
advised on what they should do next.

La filtración de Hugging Face reaviva el debate sobre las categorías de peso libre y plantea interrogantes sobre la responsabilidad.

El primer ciberataque de extremo a extremo documentado públicamente por una IA autónoma fue una prueba de rendimiento de OpenAI que escapó de su entorno aislado y vulneró Hugging Face .

ver artículo >>

NOTICIAS DE NUESTROS PARTNERS

Oculto a plena vista: Descubriendo un ataque de ransomware en múltiples etapas mediante la detección de comportamiento.

Darktrace detectó una intrusión de ransomware en varias etapas desde sus inicios, identificando reconocimiento, escalada de privilegios, movimiento lateral, comunicaciones de comando y control, y exfiltración de datos antes del cifrado.

ver artículo >>

Cómo la observabilidad transforma la codificación de vibraciones en ingeniería de IA

Descubra cómo transformar el código generado por IA y los agentes de codificación, pasando de ser colaboradores impredecibles a un trabajo de ingeniería fiable, mediante la combinación de ingeniería ágil, planificación estructurada, habilidades y un ciclo de retroalimentación en tiempo de ejecución impulsado por la observabilidad.

ver artículo >>

IBM adquirirá HRL Laboratories para impulsar el futuro de la computación cuántica.

IBM anunció la firma de un acuerdo definitivo para adquirir HRL Laboratories, LLC (HRL), una institución líder en investigación y desarrollo. HRL es una empresa privada propiedad conjunta de Boeing y General Motors

ver artículo >>

BENCHMARKING EN CIBERSEGURIDAD

Nos es muy grato informarle que, como parte de la estrategia de difusión de los servicios de Riesgo y Seguridad de Mainsoft, hemos creado una serie de benchmarkings sin costo para empresas seleccionadas.

MIDE LA SEGURIDAD DE TU ORGANIZACIÓN SIN COSTO

HAZ CLICK

EVENTOS CERCANOS DE NUESTROS PARTNERS

DARKTRACE

Más Información

BeyondTrust

Más Información

IBM Gold Partner

Más Información