BOLETÍN INFORMATIVO

Mainsoft®

N°174

MARZO 2025

Microsoft expone a los cibercriminales que están detrás del esquema de abuso de inteligencia artificial de Azure

Microsoft desenmascaró el jueves a cuatro de los individuos que, según dijo, estaban detrás de un esquema de Azure Abuse Enterprise que implica aprovechar el acceso no autorizado a servicios de inteligencia artificial generativa (GenAI) para producir contenido ofensivo y dañino.

Los registros de chat filtrados del ransomware Black Basta revelan el funcionamiento interno y los conflictos internos

Más de un año de registros de chat internos de una banda de ransomware conocida como Black Basta se han publicado en línea en una filtración que proporciona una visibilidad sin precedentes de sus tácticas y conflictos internos entre sus miembros.

JavaGhost aprovecha los permisos de Amazon IAM para desencadenar un ataque de phishing

La Unidad 42, el equipo de inteligencia de amenazas de Palo Alto Networks, ha identificado un sofisticado grupo de actores de amenazas llamado JavaGhost que ha evolucionado desde la desfiguración de sitios web hasta la ejecución de campañas de phishing persistentes utilizando entornos de AWS comprometidos.

Los PDF CAPTCHA falsos difunden Lumma Stealer a través de Webflow, GoDaddy y otros dominios

Los investigadores de ciberseguridad han descubierto una campaña de phishing generalizada que utiliza imágenes CAPTCHA falsas compartidas a través de documentos PDF alojados en la red de distribución de contenido (CDN) de Webflow para distribuir el malware ladrón Lumma.

INCIDENTES DE SISTEMAS

Vulnerabilidad de Apache Derby permite a atacantes eludir autenticación con inyección LDAP

Una vulnerabilidad de seguridad crítica (CVE-2022-46337) en Apache Derby, una base de datos relacional de código abierto implementada completamente en Java, ha expuesto los sistemas a ataques de elusión de autenticación a través de la inyección LDAP.

CISA advierte que una vulnerabilidad crítica del Centro de socios de Microsoft está bajo ataque

La falla sin parchear CVE-2024-49035 permite una escalada de privilegios no autenticados, lo que plantea riesgos para la cadena de suministro.

Trigon: se revela un nuevo exploit para la vulnerabilidad de día cero del kernel de iOS

Los investigadores de seguridad han publicado un nuevo y sofisticado exploit del kernel dirigido a los dispositivos iOS de Apple , denominado Trigon, que aprovecha una vulnerabilidad crítica en el subsistema de memoria virtual del kernel XNU.

RECOMENDACIONES

LECTURA DE SEGURIDAD

Cómo funcionan los ataques con códigos QR y cómo protegerse

Los códigos QR se han convertido en una parte integral de nuestra vida cotidiana debido a su simplicidad. Si bien existen desde hace muchos años, su uso se disparó durante la pandemia de COVID-19, cuando las empresas recurrieron a ellos para menús, pagos y check-ins sin contacto.

OSPS Baseline: Prácticas recomendadas de seguridad para proyectos de software de código abierto

La Open Source Security Foundation (OpenSSF), una iniciativa intersectorial de la Linux Foundation, ha anunciado el lanzamiento inicial de la Línea de base de seguridad del proyecto de código abierto (OSPS Baseline), un marco escalonado de prácticas de seguridad que evolucionan con la madurez de los proyectos de código abierto.

Microsoft presenta demanda contra grupo de hackers LLMjacking que eludió protecciones de IA

La demanda civil contra cuatro miembros de Storm-2139 subraya una tendencia emergente que combina credenciales LLM robadas y jailbreaking de inteligencia artificial para generar ganancias financieras para los ciberdelincuentes y pérdidas para las empresas que explotan.

SOC 3.0 - La evolución del SOC y cómo la IA está potenciando el talento humano

En la actualidad, las organizaciones se enfrentan a incesantes ataques cibernéticos, y las infracciones de alto perfil aparecen en los titulares casi a diario. Si reflexionamos sobre una larga trayectoria en el campo de la seguridad, queda claro que no se trata solo de un problema humano, sino de un problema matemático.

NOTICIAS DE

NUESTROS PARTNERS

La lucha contra el verdadero enemigo: la importancia de la divulgación responsable de vulnerabilidades entre proveedores de seguridad de correo

Este blog explora una capacidad de explotación observada por Darktrace en la reescritura de enlaces de otro proveedor de seguridad de correo electrónico y los pasos que Darktrace tomó para informar y resolver el problema.

Vodafone e IBM trabajan para garantizar la seguridad de los teléfonos inteligentes con criptografía cuántica segura

Vodafone e IBM (NYSE: IBM) anunciaron una colaboración destinada a proteger a los clientes y sus datos de futuros riesgos relacionados con las computadoras cuánticas cuando navegan por Internet en sus teléfonos inteligentes.

Observabilidad de procesos de negocio: una solución de TI para un desafío empresarial

Los procesos de negocio desempeñan un papel fundamental en la transformación digital, ya que permiten a las organizaciones operar de forma más eficiente, adaptarse más rápidamente a los cambios y ofrecer un mejor valor al cliente. Sin embargo, la mayoría de los procesos de negocio siguen sin ser supervisados, o al menos lo son de forma insuficiente.

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

CYLANCE — Más Información

IBM Gold Partner — Más Información