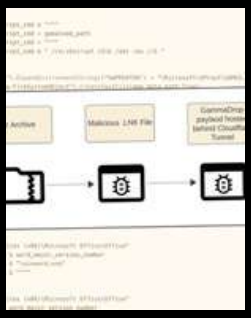
BOLETÍN INFORMATIVO

Mainsoft

N°164

DICIEMBRE 2024



Los piratas informáticos aprovechan los túneles de Cloudflare y DNS Fast-Flux para ocultar el malware GammaDrop

Se ha observado que el actor de amenazas conocido como Gamaredon aprovecha los túneles de Cloudflare como táctica para ocultar su infraestructura de prueba que aloja un malware llamado GammaDrop.

RansomHub: un grupo de ransomware que crece en América Latina y a nivel global

Este grupo que nació a inicios de 2024 se posiciona como una de las bandas más activas y eficaces dentro del mundo del cibercrimen. Conoce cómo trabaja y cuáles han sido sus víctimas más destacadas.

Investigadores descubren vulnerabilidades de inyección rápida en DeepSeek y Claude AI

Han surgido detalles sobre una falla de seguridad ahora parcheada en el chatbot de inteligencia artificial (IA) DeepSeek que, si se explota con éxito, podría permitir que un actor malintencionado tome el control de la cuenta de una víctima mediante un ataque de inyección rápida.

Biblioteca de inteligencia artificial de Ultralytics comprometida: se encuentra un minero de criptomonedas en versiones de PyPI

En otro ataque a la cadena de suministro de software, salió a la luz que dos versiones de una popular biblioteca de inteligencia artificial (IA) de Python llamada ultralytics fueron comprometidas para entregar un minero de criptomonedas.

INCIDENTES DE SISTEMAS

Vulnerabilidad en Qlik Sense Enterprise para Windows permite a atacantes ejecutar código remoto

Se ha descubierto una vulnerabilidad de seguridad crítica en Qlik Sense Enterprise para Windows, que potencialmente permite a los atacantes ejecutar código remoto en los sistemas afectados.Más de una docena de aplicaciones maliciosas para Android identificadas en Google Play Store, que en conjunto se han descargado más de 8 millones de veces, contienen malware conocido como SpyLoan, según nuevos hallazgos de McAfee Labs.

Vulnerabilidad crítica de día cero en Windows explotada en la red: prueba de concepto publicada

Microsoft ha reparado una vulnerabilidad de día cero crítica (CVE-2024-38193) que el conocido grupo de piratas informáticos norcoreanos Lazarus APT explotaba activamente.
Gen Threat Labs descubrió y reportó la falla, que representaba una grave amenaza para los usuarios de Windows en todo el mundo.

Vulnerabilidad crítica (CVE-2024-37071) en IBM Db2 afecta a plataformas Linux y UNIX

IBM ha revelado recientemente una vulnerabilidad de seguridad (CVE-2024-37071) que afecta a su software de base de datos Db2 para plataformas Linux y UNIX.

RECOMENDACIONES

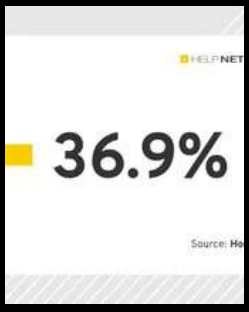
LECTURA DE SEGURIDAD

¿Quién se encarga de qué? Ideas erróneas habituales sobre las responsabilidades de seguridad de SaaS

En esta entrevista de Help Net Security, James Dolph, CISO de Guidewire , aborda conceptos erróneos comunes sobre las responsabilidades de seguridad en entornos de nube, particularmente en SaaS, y cómo estos malentendidos pueden generar riesgos de seguridad.

Empresas afectadas por un flujo constante de correos electrónicos maliciosos

El 36,9% de todos los correos electrónicos recibidos por las empresas (20.500 millones) en 2024 no fueron deseados, según el análisis de Hornetsecurity de más de 55.600 millones de correos electrónicos procesados a través de sus servicios de seguridad entre el 1 de noviembre de 2023 y el 31 de octubre de 2024, y el 2,3% de ellos contenían contenido malicioso, con un total de 427,8 millones de correos electrónicos.



Cómo utilizan Spotify para distribuir malware en podcasts y listas de reproducción

Ciberdelincuentes usan descripciones de podcast y listas de Spotify para distribuir links maliciosos, aprovechando la popularidad el sitio para posicionarse en los resultados de búsqueda de Google.

NOTICIAS DE

NUESTROS PARTNERS

Proteger su nube híbrida: el futuro de la seguridad en la nube en 2025 y más allá

En los próximos años, la seguridad en la nube no solo tendrá que adaptarse a entornos cada vez más complejos a medida que los ecosistemas se vuelven más distribuidos, sino también a amenazas que evolucionan rápidamente, como ataques a la cadena de suministro, vulnerabilidades avanzadas de configuración incorrecta y robo de credenciales.

IBM y AWS aceleran su asociación para ampliar la inteligencia artificial generativa responsable

Durante AWS re:Invent, IBM y AWS darán a conocer nuevos hitos en nuestra colaboración para ayudar a las empresas a adoptar una IA responsable. Juntos, estamos combinando nuestras fortalezas para garantizar que las organizaciones puedan aprovechar el poder de la IA generativa con énfasis en la transparencia, la seguridad y la confianza.

Automatización de las validaciones de AWS Well-Architected Framework con plantillas de Dynatrace CloudFormation

Buenas noticias para los fanáticos de AWS Well-Architected Framework que buscan automatizar las validaciones de sus flujos de trabajo. Las nuevas plantillas de Dynatrace CloudFormation para validar flujos de trabajo Well-Architected ya están disponibles.

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