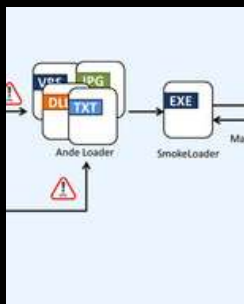


DICIEMBRE 2024



El malware SmokeLoader resurge y ataca a la industria manufacturera y las TI en

Las entidades taiwanesas de los sectores de fabricación, atención médica y tecnología de la información se han convertido en el objetivo de una nueva campaña que distribuye el malware SmokeLoader.

Claves sobre el ciberataque a la Agencia Tributaria: quién está detrás del grupo Trinity

La compañía de ciberseguridad HackManac ha publicado en la red social X (antes Twitter) que el grupo de hackers Trinity asegura haber podido acceder a la base de datos de la Agencia Tributaria (AEAT, por sus siglas).



Las ciberamenazas al comercio minorista aumentan casi un 25% antes del Black

En 2024, los ciberdelincuentes han lanzado más de 38 millones de ataques de phishing, suplantando grandes mercados, bancos y minoristas tecnológicos. Los datos de tarjetas de pago robados se comercializan activamente en foros de la dark web, con precios que oscilan entre 70 y 315 dólares. Así lo ponen de relieve los expertos de Kaspersky.



INCIDENTES DE SISTEMAS



8 millones de usuarios de Android afectados por el malware SpyLoan en aplicaciones de préstamos en Google Play

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.

Se encuentra vulnerabilidad crítica en la herramienta de monitoreo de red Zabbix

Una vulnerabilidad de gravedad crítica en la herramienta de monitoreo de red empresarial de código abierto Zabbix podría llevar a un compromiso total del sistema.



Los piratas informáticos utilizaron un currículum vitae modificado para infectar a un usuario y trasladarlo a entornos de servidores

En marzo de 2024 se detectó un sofisticado ciberataque que reveló una intrusión compleja que comenzó con un currículum vitae armado y culminó con la vulneración de varios servidores.

RECOMENDACIONES

LECTURA DE SEGURIDAD



El uso de la IA Generativa y la evolución del Ransomware provocarán ciberataques

El uso de la inteligencia artificial generativa ha provocado grandes cambios en el ámbito de la ciberseguridad. Los ciberdelincuentes han hecho uso de esta herramienta para ataques de phishing dirigidos

La vulneración de OPCC afecta a 1.7 millones de personas, un soldado estadounidense es sospechoso de haber pirateado Snowflake

Historias notables que podrían haber pasado desapercibidas: el impacto de la violación de datos de OnePoint Patient Care se duplica, un soldado estadounidense puede haber estado involucrado en el hackeo de Snowflake, Cloudflare perdió registros de clientes.



Sin contraseñas y sin claves: el futuro de la gestión de acceso (privilegiado).

Los secretos enumerados anteriormente suelen estar protegidos con soluciones de gestión de acceso privilegiado (PAM) o similares. Sin embargo, la mayoría de los proveedores de PAM tradicionales apenas hablan sobre la gestión de claves SSH. La razón es simple: no tienen la tecnología para hacerlo correctamente.

NOTICIAS DE NUESTROS PARTNERS



¿Arrestar al actor que amenaza los Datos Públicos Nacionales marcará alguna diferencia?

El arresto del Departamento de Defensa de los Estados Unidos, el cerebro detrás de la colosal filtración de datos públicos nacionales, fue una victoria para las fuerzas del orden. Pero también plantea algunas preguntas fundamentales.

Replanteamiento de la seguridad de los endpoints: el papel de la IA en la detección de amenazas

Descubra cómo las empresas pueden aprovechar la IA para mejorar la inteligencia ante amenazas y los mecanismos de respuesta para proteger los puntos finales. También analizaremos los aspectos éticos y prácticos de la implementación de la IA...



Seguridad en la nube: cómo abordar los desafíos habituales de los CISO con soluciones avanzadas

Este blog destaca cómo Darktrace/CLOUD aprovecha la IA de autoaprendizaje para abordar desafíos críticos de seguridad en la nube (como configuraciones incorrectas, complejidad del entorno híbrido, protección de suites de productividad y fatiga del agente) al brindar visibilidad unificada

BENCHMARKING EN CIBERSEGURIDAD

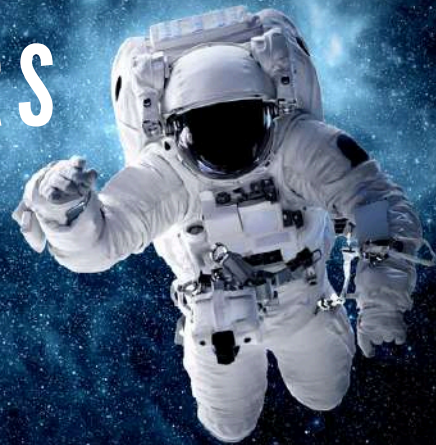
Nos es muy grato informarle que, como parte de la estrategia de difusión de los servicios de Riesgo y Seguridad de Mainssoft, hemos creado una serie de benchmarkings sin costo para empresas seleccionadas.

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](#)

