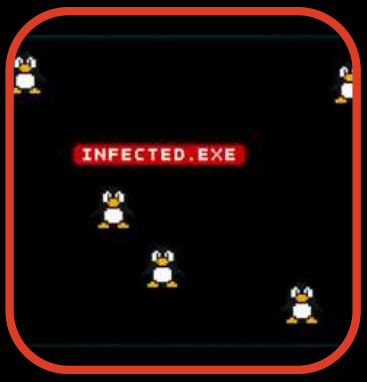
BOLETÍN INFORMATIVO N°205

OCTUBRE 2025

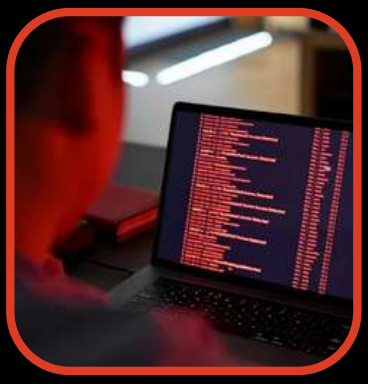


El ransomware Qilin combina la carga útil de Linux con un exploit BYOVD en un ataque híbrido

El grupo de ransomware conocido como Qilin (también conocido como Agenda, Gold Feather y Water Galura) ha cobrado más de 40 víctimas cada mes desde principios de 2025, excepto enero, y el número de publicaciones en su sitio de filtración de datos alcanzó un máximo de 100 casos en junio

Tríada de smishing vinculada a 194.000 dominios maliciosos en una operación global de phishing

Los actores de amenazas detrás de una campaña de smishing continua y a gran escala han sido atribuidos a más de 194.000 dominios maliciosos desde el 1 de enero de 2024, apuntando a una amplia gama de servicios en todo el mundo, según nuevos hallazgos de Palo Alto Networks Unit 42.



Una falla crítica de Microsoft WSUS recientemente parcheada se encuentra bajo explotación activa

Microsoft lanzó el jueves actualizaciones de seguridad fuera de banda para corregir una vulnerabilidad de gravedad crítica del Servicio de actualización de Windows Server (WSUS) con una explotación de prueba de concepto (Poc) disponible públicamente y que ha sido objeto de explotación activa.

Vulnerabilidad de día cero en Chrome explotada activamente en ataques por un conocido grupo de hackers

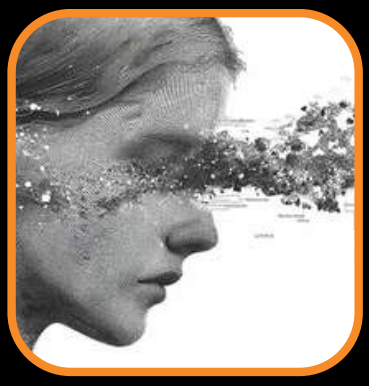
El conocido grupo de hackers Mem3nt0 mori ha estado explotando activamente una vulnerabilidad de día cero en Google Chrome, comprometiendo objetivos de alto perfil en Rusia y Bielorrusia.

Vulnerabilidades críticas de Dell Storage Manager permiten a los atacantes comprometer el sistema

Dell Technologies ha revelado tres vulnerabilidades críticas en su software Storage Manager que podrían permitir a los atacantes eludir la autenticación, divulgar información confidencial y obtener acceso no autorizado a los sistemas.

RECOMENDACIONES

LECTURA DE SEGURIDAD

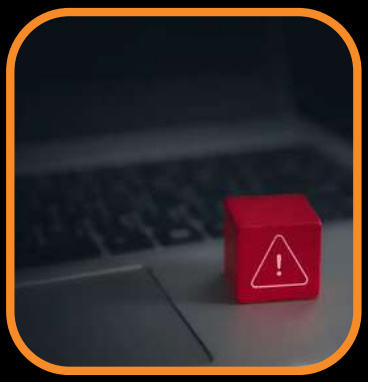


Los grupos de ransomware y extorsión se adaptan a medida que las tasas de pago alcanzan mínimos históricos

Los grupos de ransomware se enfrentan a una crisis económica propia: en el tercer trimestre de 2025, solo el 23 por ciento de las víctimas pagaron un rescate, y en los incidentes de robo de datos que no implicaron cifrado, la tasa de pago se redujo a solo el 19 por ciento, según Coveware.

Los navegadores con IA pueden ser objeto de abuso por extensiones de barra lateral con IA maliciosas: Informe

Los líderes de seguridad de la información deben estar preparados para los ataques de suplantación de la barra lateral de IA, afirman los investigadores.



Resumen semanal: WSUS explotado, LockBit 5.0 regresa, puerta trasera en Telegram, se amplía la brecha de F5

La seguridad, la confianza y la estabilidad, que antes eran los pilares de nuestro mundo digital, son ahora las herramientas que los atacantes usan contra nosotros. Desde cuentas robadas hasta ofertas de trabajo falsas, los ciberdelincuentes siguen encontrando nuevas formas de explotar tanto las fallas del sistema como el comportamiento humano.

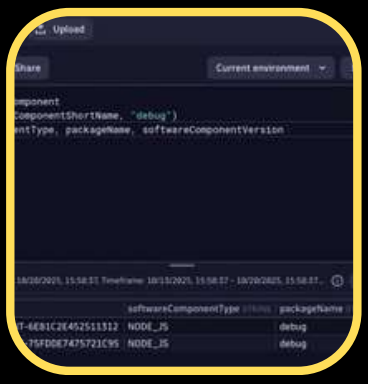
NOTICIAS DE

NUESTROS PARTNERS

Darktrace redefine la NDR: la primera investigación autónoma de amenazas de la industria desde la red hasta el endpoint con inteligencia artificial agenética.

Darktrace ofrece la próxima evolución de NDR, extendiendo un puente pionero en la industria a través de la brecha entre la red y los puntos finales con IA de autoaprendizaje.

Seguridad de la cadena de suministro: Cómo detectar paquetes de software malicioso con Dynatrace



Las cadenas de suministro de código abierto se enfrentan a un número creciente de amenazas de seguridad, desde vulnerabilidades en los pipelines de CI/CD hasta solicitudes de extracción maliciosas, ataques de phishing y malware autopropagante. Para mantenerse a la vanguardia, los equipos necesitan una visibilidad clara de qué componentes se están ejecutando en producción.

IBM anuncia nuevos agentes de IA en Oracle Fusion Applications AI Agent Marketplace

IBM anunció la disponibilidad de nuevos agentes de IA en Oracle Fusion Applications AI Agent Marketplace. Los tres nuevos agentes están diseñados para ayudar a los clientes de Oracle Fusion Cloud Applications a alcanzar nuevos niveles de eficiencia operativa.

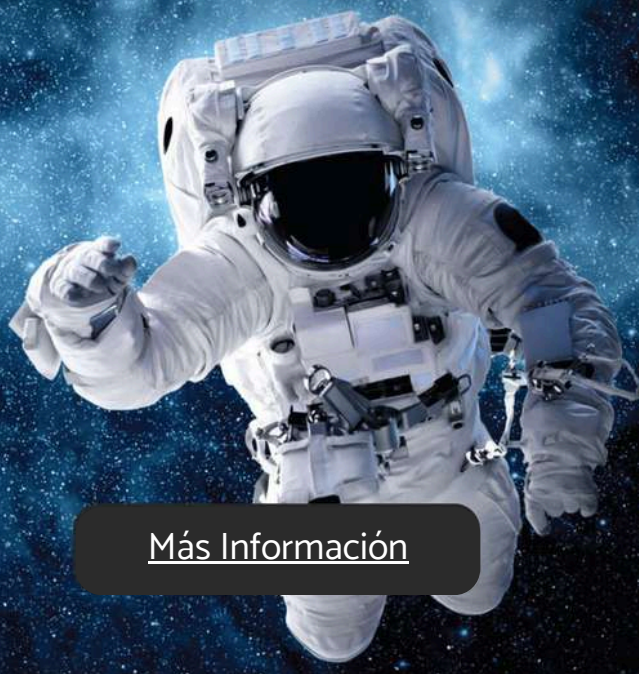
BENCHMARKING EN CIBERSEGURIDAD

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