BOLETÍN INFORMATIVO

Mainsoft®

N°177

MARZO 2025

El ransomware Medusa utiliza un controlador malicioso para desactivar el antimalware con certificados robados

Se ha observado que los actores de amenazas detrás de la operación ransomware como servicio (RaaS) Medusa utilizan un controlador malicioso denominado ABYSSWORKER como parte de un ataque de "traiga su propio controlador vulnerable" (BYOVD) diseñado para deshabilitar las herramientas antimalware.

Se teme que el nuevo día cero de Windows haya sido objeto de abuso en un espionaje generalizado durante años

La vulnerabilidad permite a los atacantes ejecutar comandos arbitrarios de forma remota utilizando archivos de acceso directo de Windows creados con líneas de comando maliciosas.

VSCode Marketplace elimina dos extensiones que implementan ransomware en etapa temprana

Investigadores de ciberseguridad han descubierto dos extensiones maliciosas en el Marketplace de Visual Studio Code (VSCode) que están diseñadas para implementar ransomware en desarrollo para sus usuarios.

Se corrige una falla crítica de ejecución remota de código en los servidores de respaldo de Veeam

Veeam Software, proveedor de soluciones de resiliencia de datos, lanzó un parche crítico para su producto Veeam Backup & Replication. La actualización corrige un problema de deserialización que puede provocar la ejecución remota de código como usuario SYSTEM en el servidor Windows subyacente.

CISA marca la vulnerabilidad crítica de copia de seguridad de NAKIVO como explotada activamente

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) ha agregado una vulnerabilidad parcheada de alta gravedad que afecta al software de respaldo y replicación de NAKIVO a su catálogo de vulnerabilidades explotadas conocidas (KEV).

Vulnerabilidad crítica de Chrome permite a atacantes ejecutar código arbitrario

Google ha confirmado una falla de seguridad crítica en Chrome que afecta a miles de millones de usuarios en plataformas Windows, Mac, Linux y Android.

RECOMENDACIONES

LECTURA DE SEGURIDAD

APT Aquatic Panda, vinculado a China: campaña de 10 meses, 7 objetivos globales y 5 familias de malware

El grupo de amenaza persistente avanzada (APT) vinculado a China, conocido como Aquatic Panda, ha sido vinculado a una "campaña de espionaje global" que tuvo lugar en 2022 contra siete organizaciones.
.

Cómo proteger su empresa de las ciberamenazas: Dominando el modelo de responsabilidad compartida

La ciberseguridad no es solo una prioridad en la agenda de su empresa. Es un pilar fundamental para la supervivencia. A medida que las organizaciones migran cada vez más sus operaciones a la nube, comprender cómo proteger sus activos digitales se vuelve crucial.

El riesgo oculto en SaaS: por qué las empresas necesitan una estrategia de salida de identidad digital

Ante restricciones comerciales repentinas, sanciones o cambios de políticas, confiar en proveedores de SaaS fuera de su región para servicios de identidad es una apuesta que las empresas ya no pueden darse el lujo de correr.

NOTICIAS DE

NUESTROS PARTNERS

Proveedor global de tecnología transforma la detección de amenazas de correo electrónico con Darktrace

Para fortalecer sus operaciones distribuidas y complejas, este líder tecnológico global implementó Darktrace/EMAIL para monitorear, detectar y mitigar posibles amenazas de correo electrónico. Lea el blog para descubrir sus resultados.

IBM contribuye con proyectos clave de código abierto a la Fundación Linux para promover la participación de la comunidad

IBM está contribuyendo con tres proyectos de código abierto (Docling, Data Prep Kit y BeeAI) a la Fundación Linux . Esta iniciativa demuestra no solo el potencial de crecimiento de estos proyectos, sino también el compromiso continuo de IBM con la IA de código abierto.

Espionaje móvil: Lo que los gobiernos deben saber para prevenir la interceptación y el espionaje

Las recientes y notorias filtraciones de las principales redes globales de telecomunicaciones y el aumento del espionaje móvil revelan una amenaza creciente, a menudo subestimada, para la seguridad nacional y organizacional. Es decir, las redes y herramientas de comunicación que hacen que las comunicaciones globales sean accesibles, conectadas y eficientes también están exponiendo datos sensibles a riesgos sin precedentes.

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