BOLETÍN INFORMATIVO

Mainsoft

N°169

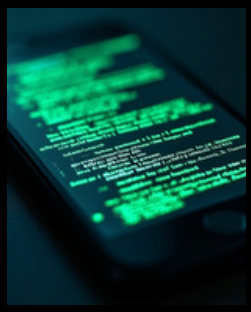
ENERO 2025

Ransomware en ESXi: la mecanización de los ataques virtualizados

En 2024, los ataques de ransomware dirigidos a servidores VMware ESXi alcanzaron niveles alarmantes, con una demanda de rescate promedio que se disparó a $5 millones. Con aproximadamente 8000 hosts ESXi expuestos directamente a Internet (según Shodan), el impacto operativo y comercial de estos ataques es profundo.

Un investigador del Proyecto Zero de Google descubre un exploit de clic cero que ataca a dispositivos Samsung

Los investigadores de ciberseguridad han detallado una falla de seguridad ahora parcheada que afecta al decodificador Monkey's Audio (APE) en los teléfonos inteligentes Samsung y que podría provocar la ejecución de código



La autenticación multifactor de Microsoft está bloqueando el acceso de los usuarios de Office 365

Microsoft ha alertado a los usuarios sobre un problema con su sistema de autenticación multifactor (MFA), que ha interrumpido el acceso a ciertas aplicaciones de Microsoft 365.

El ransomware Ako abusa de las llamadas a la API de Windows para detectar las ubicaciones del sistema infectado

Ako, comúnmente conocido como MedusaReborn, es una cepa de ransomware basada en C++ que ha estado activa desde enero de 2020.

INCIDENTES DE

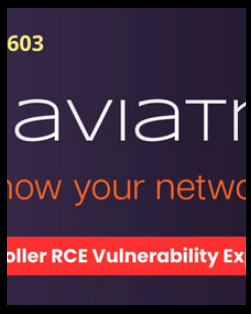
SISTEMAS

Los skimmers de WordPress evitan la detección inyectándose en las tablas de la base de datos

Los investigadores en ciberseguridad advierten sobre una nueva campaña sigilosa de clonación de tarjetas de crédito que apunta a las páginas de pago de comercio electrónico de WordPress insertando código JavaScript malicioso en una tabla de base de datos asociada con el sistema de gestión de contenido (CMS).

Vulnerabilidad RCE del controlador Aviatrix explotada en la naturaleza

Una vulnerabilidad crítica de ejecución remota de código (RCE), CVE-2024-50603, ha sido explotada activamente, lo que plantea riesgos significativos para los entornos de nube.

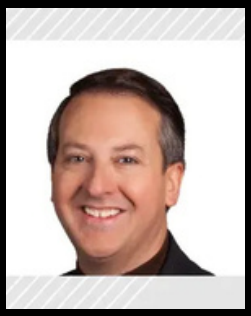


Vulnerabilidad crítica de la zona protegida de macOS (CVE-2024-54498): PoC de explotación publicada en línea

Se lanzó un exploit de prueba de concepto para una vulnerabilidad crítica que afecta a los sistemas macOS, identificada como CVE-2024-54498.

RECOMENDACIONES

LECTURA DE SEGURIDAD

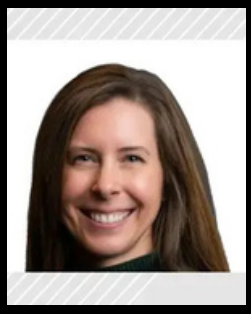


Cómo prevenir el próximo ataque de ransomware con ayuda de la IA

En esta entrevista de Help Net Security, el Dr. Darren Williams, director ejecutivo de BlackFog , habla sobre cómo la capacitación de los empleados desempeña un papel crucial en la prevención de ataques de ransomware.

CISO de GitHub sobre estrategia de seguridad y colaboración con la comunidad de código abierto

En este Help Net Security, Alexis Wales, CISO de GitHub , analiza cómo GitHub integra seguridad en cada aspecto de su plataforma para proteger a millones de desarrolladores y repositorios, garantizando que siga siendo una plataforma confiable para crear software seguro.



Resumen semanal de THN: Principales amenazas de ciberseguridad, herramientas y consejos

El mundo cibernético ha estado en plena efervescencia esta semana y lo importante es mantenerse un paso por delante de los malos. Desde errores de software furtivos hasta trucos de piratería avanzados, los riesgos son reales, pero también lo son las formas de protegerse. En este resumen, analizaremos qué está sucediendo, por qué es importante y qué puede hacer para mantenerse seguro.

NOTICIAS DE

NUESTROS PARTNERS

Seguridad en la nube con agente o sin agente: por qué son importantes los métodos de implementación

Las soluciones de seguridad en la nube se pueden implementar con enfoques basados en agentes o sin agentes, o con una combinación de métodos. Las organizaciones deben evaluar qué método se aplica mejor a los activos y datos que protegerá la herramienta

RISE with SAP en IBM Power Virtual Server para ayudar a acelerar la transformación con SAP S/4HANA Cloud

IBM (NYSE: IBM) y SAP SE (NYSE: SAP) anunciaron el próximo lanzamiento de RISE with SAP en IBM Power Virtual Server , diseñado para que los clientes de IBM Power puedan acelerar su transformación de ERP de la forma más rápida y sencilla. Juntos, IBM y SAP tienen como objetivo ayudar a las organizaciones a realizar una transición y modernizar de forma más fluida sus entornos ERP locales a la nube y a respaldar los procesos comerciales impulsados por IA.

BlackBerry AtHoc “en proceso” para autorización alta de FedRAMP

BlackBerry® AtHoc® ahora figura como "En proceso" para lograr el estado de Alta Autorización del Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP) de la Junta de Autorización Conjunta (JAB). Una vez aprobado, BlackBerry AtHoc será la primera solución de gestión de eventos críticos (CEM) en recibir la autorización de FedRAMP High.

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