BOLETÍN INFORMATIVO N°193

AGOSTO 2025

La nueva puerta trasera PAM «Plague» expone sistemas Linux críticos al robo silencioso de credenciales.

Los investigadores de ciberseguridad han detectado una puerta trasera de Linux no documentada previamente, denominada Plague , que ha logrado evadir la detección durante un año.

El troyano PlayPraetor para Android infecta más de 11.000 dispositivos mediante páginas falsas de Google Play y metaanuncios.

Investigadores de ciberseguridad han descubierto un troyano de acceso remoto (RAT) naciente para Android llamado PlayPraetor que ha infectado más de 11.000 dispositivos, principalmente en Portugal, España, Francia, Marruecos, Perú y Hong Kong.

El ransomware Akira explota las VPN de SonicWall en un probable ataque de día cero contra dispositivos con todos los parches instalados

Los dispositivos VPN SSL de SonicWall se han convertido en el objetivo de los ataques de ransomware Akira como parte de un nuevo aumento de actividad observado a fines de julio de 2025.

Apple corrige una vulnerabilidad de Safari que también se explota como día cero en Google Chrome

Apple lanzó el martes actualizaciones de seguridad para todo su portafolio de software, incluida una solución para una vulnerabilidad que según Google fue explotada como día cero en el navegador web Chrome a principios de este mes.

Los piratas informáticos pueden manipular las claves de registro de BitLocker a través de WMI para ejecutar código malicioso como usuario interactivo

Una nueva técnica de movimiento lateral que explota la funcionalidad del Modelo de objetos componentes (COM) de BitLocker para ejecutar código malicioso en los sistemas de destino.

Investigadores explotaron instancias de kernelCTF de Google y Debian 12 con un ataque de día cero

Los investigadores explotaron CVE-2025-38001, una vulnerabilidad de uso después de la liberación (UAF) previamente desconocida en la disciplina de colas HFSC de Linux, para comprometer todas las instancias de kernelCTF de Google (LTS, COS y mitigación), así como los sistemas Debian 12 completamente parcheados.

RECOMENDACIONES

LECTURA DE SEGURIDAD

La sorprendente verdad sobre la confianza en la seguridad de la identidad

Según un nuevo informe de BeyondID, las organizaciones que más confían en la seguridad de su identidad suelen ser las menos preparadas. El estudio revela una preocupante brecha entre lo que las organizaciones creen sobre sus programas de seguridad de identidad y su comportamiento real.

Los AIBOM son los nuevos SBOM: el eslabón perdido en la gestión de riesgos de la IA

En esta entrevista de Help Net Security, Marc Frankel, director ejecutivo de Manifest Cyber , analiza cómo los riesgos específicos de la IA que se pasan por alto , como los datos de entrenamiento contaminados y la IA oculta, pueden generar problemas de seguridad que las herramientas convencionales no detectan.

Resumen semanal: VPN de día cero, puerta trasera de cifrado, malware de IA, falla de macOS, hackeo de cajeros automáticos y más

El malware ya no solo intenta ocultarse, sino integrarse. Vemos código que habla como nosotros, registra como nosotros e incluso se documenta como un compañero de equipo útil. Algunas amenazas ahora se parecen más a herramientas de desarrollo que a exploits.

NOTICIAS DE

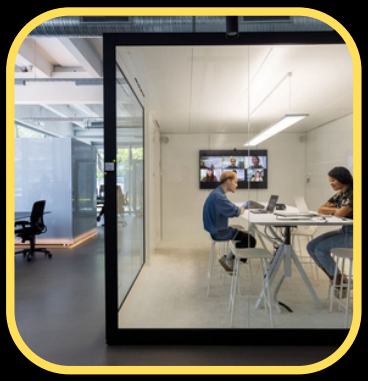
NUESTROS PARTNERS

Dynatrace consigue la certificación High según el Esquema Nacional de Seguridad (ENS) de España

Estamos orgullosos de anunciar que la plataforma Dynatrace® ahora está certificada de acuerdo con el Esquema Nacional de Seguridad (ENS) de España por OCA CERT.

IBM z/OS 3.2 libera el valor de IBM z17

IBM z/OS ha sido la base para las empresas que necesitan confiabilidad, escalabilidad y seguridad inigualables. En 2025, IBM se basará en esta sólida base con z/OS 3.2, la próxima versión del sistema operativo insignia de IBM para mainframe, diseñado para aprovechar al máximo el nuevo IBM z17.



Nuestras reflexiones sobre lo que el acuerdo entre Palo Alto Networks y CyberArk significa para la industria

Un terremoto en Rusia no fue el único cambio radical ocurrido esta semana. El panorama de la ciberseguridad también experimentó un cambio notable: Palo Alto Networks anunció su intención de adquirir CyberArk.

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