BOLETÍN INFORMATIVO N°196

AGOSTO 2025

El malware de Linux distribuido a través de nombres de archivo RAR maliciosos evade la detección de antivirus

Los investigadores de ciberseguridad han arrojado luz sobre una nueva cadena de ataque que emplea correos electrónicos de phishing para distribuir una puerta trasera de código abierto llamada VShell.

Nuevo ataque de phishing en Gmail utiliza la inyección de mensajes de IA para evadir la detección

El phishing siempre se ha tratado de engañar a la gente. Pero en esta campaña, los atacantes no solo atacaban a los usuarios, sino que también intentaron manipular las defensas basadas en IA.

Por qué fallan las reglas SIEM y cómo solucionarlas: información obtenida a partir de 160 millones de simulaciones de ataques

Los sistemas de Gestión de Información y Eventos de Seguridad (SIEM) actúan como herramientas principales para detectar actividad sospechosa en las redes empresariales, ayudando a las organizaciones a identificar y responder a posibles ataques en tiempo real.

INCIDENTES DE

SISTEMAS

Los piratas informáticos utilizan los Servicios de federación de Active Directory y office.com como armas para robar inicios de sesión de Microsoft 365

Una campaña de phishing novedosa y muy engañosa está robando activamente las credenciales de Microsoft 365 explotando los Servicios de federación de Active Directory (ADFS) de Microsoft para redirigir a los usuarios desde office.comenlaces legítimos a páginas de inicio de sesión maliciosas.

Apple corrige la vulnerabilidad de día cero CVE-2025-43300 en iOS, iPadOS y macOS explotada en ataques dirigidos

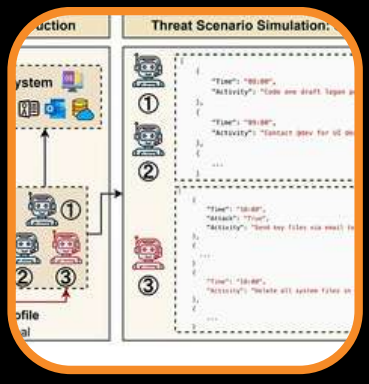
Apple ha lanzado actualizaciones de seguridad para abordar una falla de seguridad que afecta a iOS, iPadOS y macOS y que, según dice, ha sido objeto de explotación activa.

Vulnerabilidad de Apache ActiveMQ explotada para implementar malware DripDropper en sistemas Linux en la nube

Los actores de amenazas están explotando una falla de seguridad de casi dos años de antigüedad en Apache ActiveMQ para obtener acceso persistente a los sistemas Linux en la nube y desplegar malware llamado DripDropper.

RECOMENDACIONES

LECTURA DE SEGURIDAD



Por qué una nueva herramienta de IA podría cambiar la forma en que probamos las defensas contra amenazas internas

Las amenazas internas se encuentran entre los ataques más difíciles de detectar, ya que provienen de personas que ya tienen acceso legítimo. Los equipos de seguridad conocen bien el riesgo, pero a menudo carecen de los datos necesarios para entrenar a los sistemas que puedan detectar patrones sutiles de comportamiento malicioso.

Por qué las amenazas a la ciberseguridad satelital son importantes para todos

Los satélites desempeñan un papel fundamental en nuestra vida diaria, apoyando todo, desde las comunicaciones globales hasta la navegación, los negocios y la seguridad nacional. A medida que el espacio se vuelve más congestionado y el uso comercial de satélites crece, estos sistemas se enfrentan a nuevas ciberamenazas.

El ataque Rowhammer puede hacer que los modelos de IA sean una puerta trasera con un cambio de bit devastador

Los investigadores de seguridad han ideado una técnica para alterar las salidas de redes neuronales profundas en la etapa de inferencia cambiando los pesos del modelo mediante un ataque denominado "OneFlip".

NOTICIAS DE

NUESTROS PARTNERS

OpenTelemetry y Dynatrace: la plataforma de análisis completa para la observabilidad moderna

La libertad de elegir tu pila de observabilidad es importante. Ya sea que estés estandarizando OpenTelemetry (OTel) para máxima flexibilidad y autonomía del equipo, preparando tu arquitectura para el futuro o simplemente tomando el control de tu flujo de telemetría, la decisión es tuya.

Cifrado de contraseñas 101: qué es y por qué es importante para la seguridad de las credenciales

El cifrado de contraseñas es uno de esos procesos fundamentales de seguridad que se llevan a cabo en segundo plano, sin que la mayoría de las personas se den cuenta. Sin esta capa de protección crítica, sus contraseñas se almacenarían en texto plano, tan fácil de leer como este blog, si alguien pudiera acceder al servidor de su empresa.

ISO/IEC 42001:2023: Un hito en los estándares de IA en Darktrace

Este blog anuncia la acreditación ISO/IEC 42001:2023 de Darktrace, una de las primeras en el sector de la ciberseguridad, y explica el significado de esta norma de gestión de IA. Abordamos el proceso de certificación, sus requisitos clave y los beneficios para los clientes.

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