BOLETÍN INFORMATIVO N°201

SEPTIEMBRE 2025

Microsoft detecta phishing impulsado por IA: archivos SVG creados por LLM superan en inteligencia a la seguridad del correo electrónico

Microsoft está llamando la atención sobre una nueva campaña de phishing dirigida principalmente a organizaciones con sede en EE. UU. que probablemente haya utilizado código generado mediante modelos de lenguaje grandes (LLM) para ofuscar cargas útiles y evadir las defensas de seguridad.

Primer servidor MCP malicioso descubierto robando correos electrónicos en un paquete Postmark-MCP fraudulento

Los investigadores de ciberseguridad han descubierto lo que se ha descrito como el primer caso de un servidor de Protocolo de Contexto de Modelo (MCP) detectado en la práctica, lo que aumenta los riesgos de la cadena de suministro de software.

La nueva campaña de malware COLDRIVER se une al equipo BO y a Bearlyfy en ciberataques centrados en Rusia.

El grupo ruso de amenazas persistentes avanzadas (APT) conocido como COLDRIVER ha sido atribuido a una nueva ronda de ataques de estilo ClickFix diseñados para distribuir dos nuevas familias de malware "liviano" identificadas como BAITSWITCH y SIMPLEFIX.

Lección de la vulnerabilidad RCE de día cero de Cisco ASA, explotada activamente en la naturaleza

El panorama de la ciberseguridad experimentó una escalada significativa en septiembre de 2025, cuando Cisco reveló múltiples vulnerabilidades críticas de día cero que afectaban a sus plataformas Adaptive Security Appliance (ASA) y Firepower Threat Defense (FTD).

Vulnerabilidades de alta gravedad en GitLab permiten a los atacantes bloquear instancias

GitLab ha revelado múltiples vulnerabilidades de denegación de servicio (DoS) de alta gravedad que podrían permitir que atacantes no autenticados bloqueen instancias de GitLab autoadministradas.

Vulnerabilidad de Apache Airflow expone información confidencial a usuarios de solo lectura

Ha surgido una falla de seguridad crítica en Apache Airflow 3.0.3, que expone información de conexión confidencial a usuarios con solo permisos de lectura.

RECOMENDACIONES

LECTURA DE SEGURIDAD

Los grupos de ransomware se están multiplicando, lo que aumenta los riesgos para los defensores

La actividad de ransomware está aumentando de nuevo, con un marcado incremento en el número de víctimas y grupos que lanzan ataques. Un nuevo informe semestral de Searchlight Cyber muestra la rapidez con la que cambia el panorama de amenazas y por qué los CISO deben seguir ajustando sus defensas

Coherencia: el nuevo principio fundamental de la estrategia de gestión del riesgo interno

El control y la vigilancia han sido durante mucho tiempo los principios centrales para reducir el riesgo interno. Sin embargo, garantizar la coherencia organizacional antes de que la desalineación y la desviación de la misión se conviertan en una amenaza sienta una base más sólida contra acciones maliciosas y comportamientos de seguridad laxos.

Resumen semanal: Cisco 0-Day, DDoS récord, LockBit 5.0, errores de BMC, botnet ShadowV2 y más

La ciberseguridad nunca se detiene, y los hackers tampoco. Mientras terminaba la semana pasada, ya había nuevos ataques en marcha.

NOTICIAS DE

NUESTROS PARTNERS

Anunciamos CDR unificado en tiempo real e investigaciones automatizadas para transformar las operaciones de seguridad en la nube

Tras el anuncio de Darktrace / Adquisición e Investigación Forense, nos complace compartir cómo Darktrace / CLOUD está evolucionando para ofrecer un enfoque verdaderamente unificado para la seguridad en la nube.

Ingiera y enriquezca las alertas de seguridad de Microsoft Sentinel con Dynatrace

Dynatrace se integra con Microsoft Sentinel para unificar, visualizar y automatizar los hallazgos de seguridad en todas las herramientas y entornos.

BeyondTrust alcanza los mil millones de sesiones remotas seguras... sin señales de desaceleración

BeyondTrust alcanzó un hito importante: mil millones de sesiones remotas seguras (y seguimos sumando), impulsadas por las soluciones BeyondTrust Remote Support y Privileged Remote Access (PRA).

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