BOLETÍN INFORMATIVO N°203

OCTUBRE 2025

Los investigadores advierten que la botnet RondoDox está utilizando más de 50 vulnerabilidades en más de 30 proveedores.

Las campañas de malware que distribuyen la botnet RondoDox han ampliado su enfoque para explotar más de 50 vulnerabilidades en más de 30 proveedores.

El nuevo malware basado en Rust, "ChaosBot", utiliza canales de Discord para controlar las PC de sus víctimas.

Los investigadores de ciberseguridad han revelado detalles de una nueva puerta trasera basada en Rust llamada ChaosBot que puede permitir a los operadores realizar reconocimientos y ejecutar comandos arbitrarios en hosts comprometidos.

175 paquetes npm maliciosos con 26 000 descargas utilizados en una campaña de phishing de credenciales

Investigadores de ciberseguridad han detectado un nuevo conjunto de 175 paquetes maliciosos en el registro npm que se han utilizado para facilitar ataques de recolección de credenciales como parte de una campaña inusual.

Microsoft bloquea el modo IE después de que hackers convirtieran una función heredada en una puerta trasera

Microsoft dijo que ha renovado el modo Internet Explorer (IE) en su navegador Edge después de recibir "informes creíbles" en agosto de 2025 de que actores de amenazas desconocidos estaban abusando de la función de compatibilidad con versiones anteriores para obtener acceso no autorizado a los dispositivos de los usuarios.

Un nuevo error en Oracle E-Business Suite podría permitir a los piratas informáticos acceder a datos sin iniciar sesión

Oracle emitió el sábado una alerta de seguridad advirtiendo sobre una nueva falla de seguridad que afecta a su E-Business Suite y que, según dijo, podría permitir el acceso no autorizado a datos confidenciales.

El malware Stealit abusa de la función ejecutable única de Node.js mediante instaladores de juegos y VPN.

Los investigadores de ciberseguridad han revelado detalles de una campaña de malware activa llamada Stealit que ha aprovechado la función de aplicación ejecutable única (SEA) de Node.js como una forma de distribuir sus cargas útiles.

RECOMENDACIONES

LECTURA DE SEGURIDAD

Construyendo una estrategia de ciberseguridad sanitaria que funcione

En esta entrevista de Help Net Security, Wayman Cummings, CISO de Ochsner Health , habla sobre cómo desarrollar una estrategia de ciberseguridad para la atención médica, incluso con recursos limitados.

LockBit, DragonForce y Qilin forman un "cártel" para dictar las condiciones del mercado del ransomware

La alianza tiene como objetivo coordinar ataques y compartir recursos a medida que aumenta la presión policial.

Los atacantes no se detienen, atacan y siguen adelante.

Los ciberataques ocurren más rápido que nunca. Intrusiones que antes tardaban semanas o meses ahora se desarrollan en minutos, dejando poco tiempo para reaccionar. Los atacantes actúan con rapidez una vez que obtienen acceso, con el objetivo de ejecutar sus cargas útiles y obtener resultados antes de que los defensores puedan responder, según Elastic.

NOTICIAS DE

NUESTROS PARTNERS

S&P Global e IBM implementan inteligencia artificial agentic para mejorar las operaciones empresariales

S&P Global (NYSE: SPGI) e IBM (NYSE: IBM) anunciaron su asociación para integrar el marco de agente watsonx Orchestrate de IBM en el conjunto de ofertas de S&P Global, comenzando por la gestión de la cadena de suministro.

Dynatrace y Atlassian ofrecen IA agente que transforma la gestión de incidentes de extremo a extremo

Cuando ocurren incidentes, los ingenieros y gestores de incidentes suelen carecer de la visibilidad de producción necesaria para comprender plenamente los problemas subyacentes y actuar con rapidez.

La puerta trasera oculta en los registros de auditoría de Databricks

El equipo de ingeniería de datos de BeyondTrust descubrió una vulnerabilidad en los registros de auditoría de Databricks que puede crear nuevas vías de vulneración. Este blog explora los detalles de esta vulnerabilidad y ofrece medidas prácticas para mitigarla.

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