Mainsoft®

BOLETÍN INFORMATIVO

#216 | Abril 2026

Investigadores detectan el malware ZionSiphon dirigido a sistemas de agua y desalinización de tecnología operativa (OT) israelíes.

Investigadores de ciberseguridad han detectado un nuevo programa malicioso llamado ZionSiphon que parece estar diseñado específicamente para atacar los sistemas israelíes de tratamiento y desalinización de agua

ver artículo >>

Los webhooks de n8n se utilizan indebidamente desde octubre de 2025 para distribuir malware mediante correos electrónicos de phishing.

Se ha observado que los ciberdelincuentes utilizan n8n , una popular plataforma de automatización de flujos de trabajo de inteligencia artificial (IA), como arma para facilitar sofisticadas campañas de phishing y distribuir cargas útiles maliciosas o identificar dispositivos mediante el envío de correos electrónicos automatizados.

ver artículo >>

La variante Mirai de Nexcorium explota la vulnerabilidad CVE-2024-3721 para secuestrar grabadoras de vídeo digital (DVR) de TBK y crear una botnet DDoS.

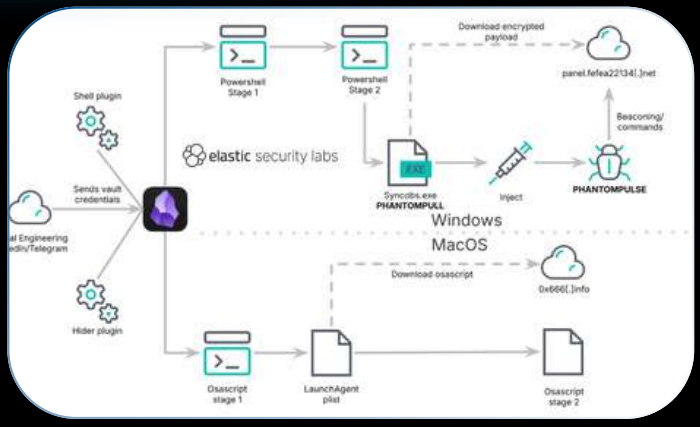
Según los hallazgos de Fortinet FortiGuard Labs y Palo Alto Networks Unit 42, los ciberdelincuentes están explotando fallos de seguridad en los grabadores de vídeo digital (DVR) TBK y en los routers Wi-Fi TP-Link al final de su vida útil (EoL) para desplegar variantes de la botnet Mirai en dispositivos comprometidos.

ver artículo >>

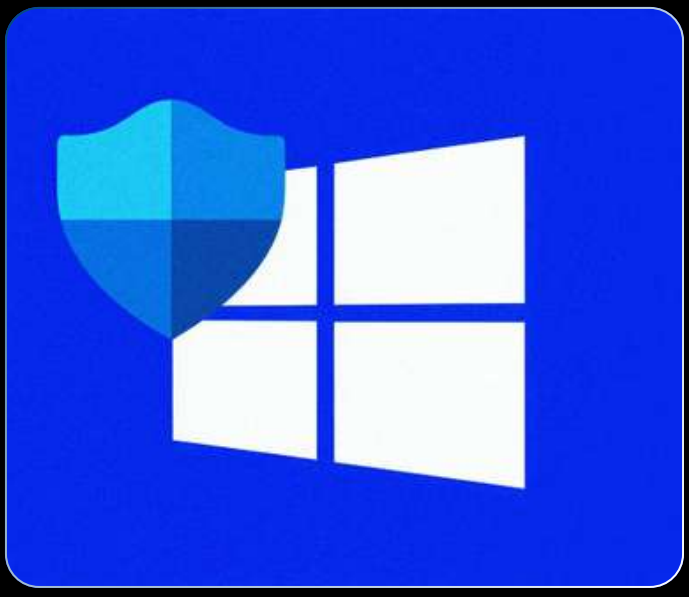
El abuso del plugin Obsidian permite la distribución de PHANTOMPULSE RAT en ataques dirigidos a finanzas y criptomonedas.

Se ha detectado una "novedosa" campaña de ingeniería social que abusa de Obsidian, una aplicación multiplataforma para tomar notas, como vector de acceso inicial para distribuir un troyano de acceso remoto a Windows previamente no documentado llamado PHANTOMPULSE en ataques dirigidos a personas de los sectores financiero y de criptomonedas.

ver artículo >>



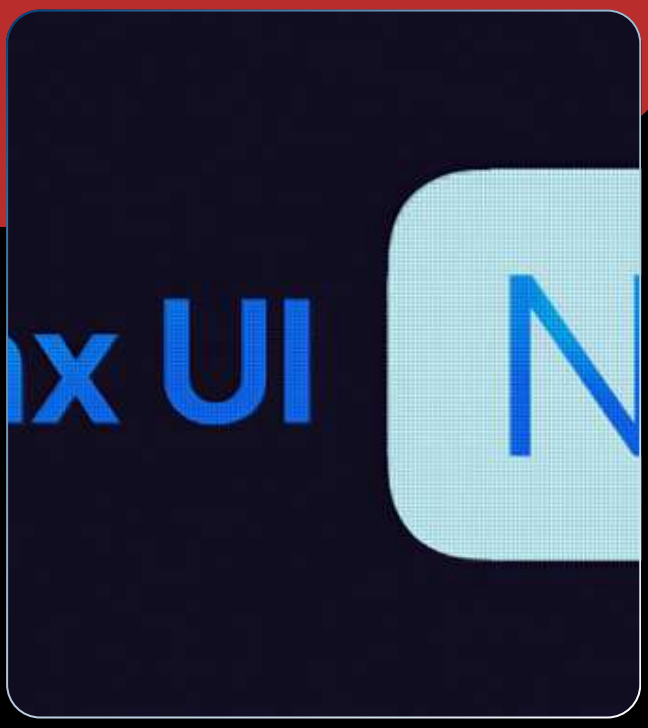
INCIDENTES DE SISTEMAS



Tres vulnerabilidades de día cero de Microsoft Defender están siendo explotadas activamente; dos aún no han sido parcheadas.

Huntress advierte que los ciberdelincuentes están explotando tres fallos de seguridad recientemente descubiertos en Microsoft Defender para obtener privilegios elevados en sistemas comprometidos.

ver artículo >>



Una vulnerabilidad de nginx-ui (CVE-2026-33032), que se explota activamente, permite el control total del servidor Nginx.

Una vulnerabilidad de seguridad crítica recientemente descubierta que afecta a nginx-ui, una herramienta de gestión de Nginx basada en web y de código abierto, está siendo explotada activamente

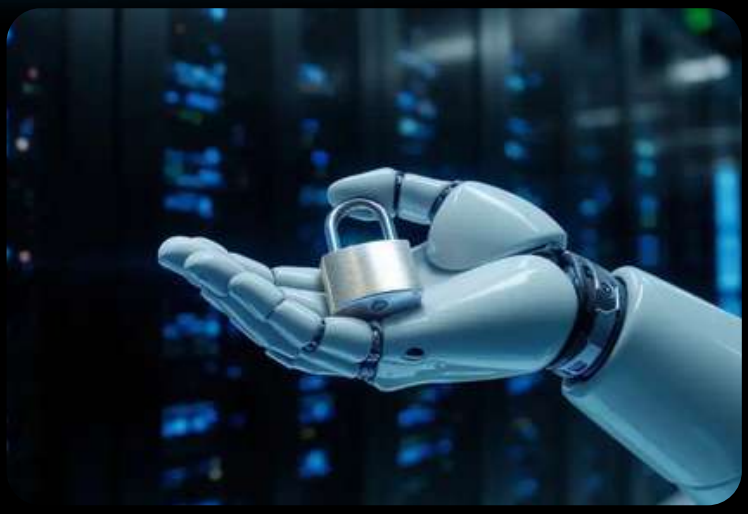
ver artículo >>

RECOMENDACIONES DE LECTURA DE SEGURIDAD

Resumen semanal: Hackeo de Vercel, fraude de notificaciones push, abuso de QEMU, aparición de nuevos RAT para Android y más.

El resumen del lunes muestra el mismo patrón en distintos lugares. Una herramienta de terceros se convierte en una puerta de entrada y luego conduce al acceso interno. Una ruta de descarga segura se cambia brevemente para distribuir malware. Las extensiones del navegador funcionan con normalidad mientras extraen datos y ejecutan código. Incluso los canales de actualización se utilizan para distribuir cargas útiles. No se trata de romper sistemas, sino de minar la confianza.

ver artículo >>



Detrás de la expectación generada por Mythos, Glasswing solo tiene una vulnerabilidad CVE confirmada.

A medida que crece la expectación en torno al modelo de IA ofensiva de Anthropic, el análisis de VulnCheck encuentra solo una vulnerabilidad CVE confirmada vinculada directamente al Proyecto Glasswing, lo que plantea interrogantes sobre cómo debería medirse el impacto de Mythos en el mundo real.

ver artículo >>

NOTICIAS DE NUESTROS PARTNERS

Lograr una mayor observabilidad para Alibaba Cloud en entornos multi-nube con Dynatrace.

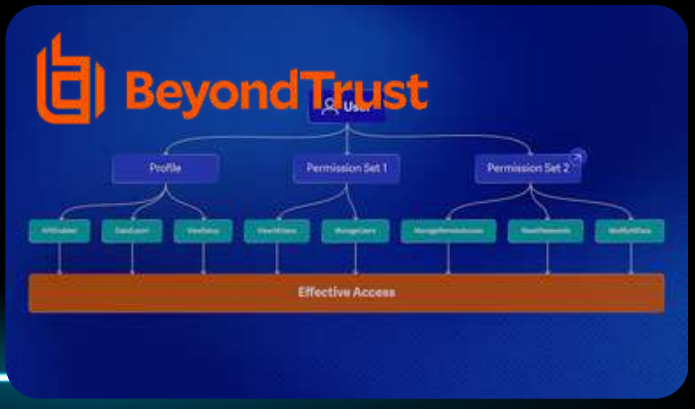
La arquitectura multinube es ahora la norma. Cada nube ofrece ventajas únicas, y Alibaba Cloud suele desempeñar un papel fundamental para las organizaciones con clientes u operaciones en China y la región de Asia-Pacífico. Para aprovechar al máximo la flexibilidad de los entornos multinube, los equipos necesitan una visión clara de cómo se integra su infraestructura.

ver artículo >>

Por qué la IA conductual es la respuesta a los Mythos

La IA está acelerando los ciberataques más allá del ritmo de las actualizaciones, lo que pone de manifiesto una creciente brecha entre el descubrimiento y la corrección de vulnerabilidades. Este blog analiza por qué la seguridad basada en la prevención ya no puede hacer frente a las amenazas impulsadas por la IA. También describe cómo la IA conductual de Darktrace permite a las organizaciones detectar y contener ataques al instante, incluso cuando las vulnerabilidades son desconocidas o no están parcheadas.

ver artículo >>



Riesgo de acceso a Salesforce: cómo los permisos ocultos crean puntos ciegos de seguridad

Descubra el poder y los privilegios ocultos en su organización. Aprenda cómo los permisos dispersos, las aplicaciones conectadas y las API generan riesgos de acceso a Salesforce.

ver artículo >>

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