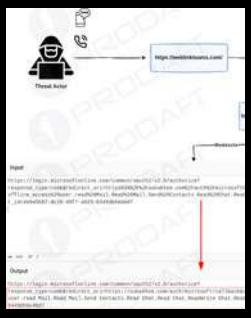
BOLETÍN INFORMATIVO

Mainsoft®

N°175

MARZO 2025



EncryptHub distribuye ransomware y programas ladrones a través de aplicaciones troyanizadas, servicios PPI y phishing

Se ha observado que el actor de amenazas con motivaciones financieras conocido como EncryptHub orquesta sofisticadas campañas de phishing para implementar ladrones de información y ransomware, mientras también trabaja en un nuevo producto llamado EncryptRAT.

Falla de PHP-CGI RCE explotada en ataques a sectores de tecnología, telecomunicaciones y comercio electrónico en Japón

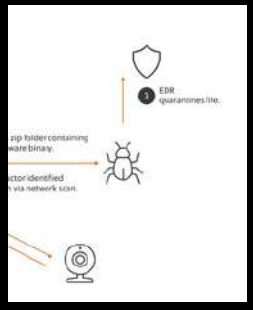
Se ha atribuido a actores de amenazas de procedencia desconocida la responsabilidad de una campaña maliciosa dirigida principalmente a organizaciones en Japón desde enero de 2025.

FIN7, FIN8 y otros utilizan Ragnar Loader para operaciones de ransomware y acceso persistente

Los cazadores de amenazas han arrojado luz sobre un "kit de herramientas de malware sofisticado y en evolución" llamado Ragnar Loader que es utilizado por varios grupos de ciberdelitos y ransomware como Ragnar Locker (también conocido como Monstrous Mantis), FIN7, FIN8 y Ruthless Mantis (ex-REvil).

El ransomware Akira ataca a Windows Server a través de RDP y evade EDR usando una cámara web

El actor de amenazas ha implementado técnicas novedosas para eludir las defensas de seguridad, en particular explotando cámaras web no seguras para eludir las herramientas de detección y respuesta de puntos finales (EDR) al implementar ransomware en redes corporativas.

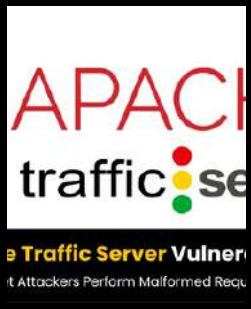


Investigadores de SquareX exponen un ataque OAuth a extensiones de Chrome días antes de una importante vulneración

SquareX , la primera solución de detección y respuesta de navegador (BDR) del sector, es líder en materia de seguridad de navegadores. Hace aproximadamente una semana, SquareX informó sobre ataques a gran escala dirigidos a desarrolladores de extensiones de Chrome que buscaban hacerse con el control de la extensión de Chrome de Chrome Store.

Las vulnerabilidades del servidor de tráfico Apache permiten a los atacantes realizar solicitudes mal formadas

La Apache Software Foundation ha emitido parches urgentes para múltiples vulnerabilidades de alta gravedad en Apache Traffic Server (ATS), su servidor proxy de almacenamiento en caché de nivel empresarial.



Microsoft advierte sobre una campaña de publicidad maliciosa que infecta más de un millón de dispositivos en todo el mundo

Microsoft ha revelado detalles de una campaña de publicidad maliciosa a gran escala que se estima ha afectado a más de un millón de dispositivos en todo el mundo como parte de lo que dice es un ataque oportunista diseñado para robar información confidencial.

RECOMENDACIONES

LECTURA DE SEGURIDAD

Cómo desechar de forma segura tecnología antigua sin dejar ningún riesgo de seguridad

Cada año, millones de equipos tecnológicos antiguos se desechan debido a su antigüedad, a fallos de funcionamiento o para dar paso a otros nuevos, lo que genera riesgos de seguridad relacionados con los datos de estos dispositivos.

Los doce sucios: los 12 peores grupos de ransomware activos en la actualidad

El ransomware está aumentando en todas las industrias. Estas son las operaciones delictivas que los profesionales de la ciberseguridad deben tener en cuenta.

NOTICIAS DE

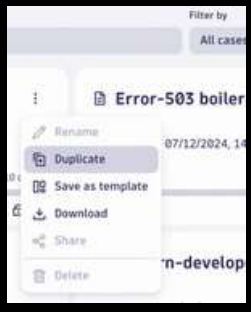
NUESTROS PARTNERS

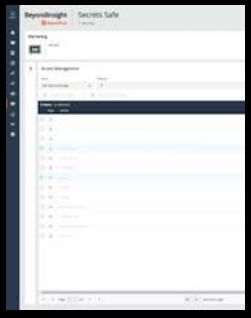
De la contención a la remediación: Darktrace / CLOUD y Cado reducen el tiempo medio de reparación (MTTR)

Darktrace/CLOUD se combina con la captura forense automatizada de Cado para lograr una contención rápida y capacidades de investigación profundas. Obtenga más información sobre cómo acelerar el tiempo medio de reparación aquí.

Casos duplicados: un cambio radical para la productividad y la eficiencia de los investigadores de seguridad

Dynatrace presenta la siguiente gran incorporación a las funciones colaborativas para los investigadores de seguridad. Ahora puede duplicar casos en Security Investigator .





Mejore la seguridad de sus secretos con cajas fuertes compartidas e integraciones en la nube

En este blog, analizaremos las últimas mejoras de BeyondTrust Password Safe y explicaremos por qué son importantes para su organización.

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

CYLANCE — Más Información

IBM Gold Partner — Más Información