Mainsoft®

BOLETÍN INFORMATIVO

#224 | Junio 2026

El ransomware Gentlemen se cobra 478 víctimas y puede propagarse como un gusano.

Un nuevo análisis de la operación The Gentlemen ha revelado que este grupo de ciberdelincuentes, motivado por intereses económicos, operaba inicialmente como una filial responsable de llevar a cabo ataques de doble extorsión, aprovechando recursos de diversos esquemas de ransomware como servicio (RaaS) como LockBit (también conocido como Tenacious Mantis), Qilin (también conocido como Pestilent Mantis) y Medusa (también conocido como Venomous Mantis).

ver artículo >>

GitHub deshabilitará los scripts de instalación de npm por defecto para detener los ataques a la cadena de suministro.

GitHub ha anunciado lo que ha calificado de "cambios importantes" que llegarán a la versión 12 de npm, uno de los cuales desactiva los scripts de instalación por defecto para combatir las amenazas a la cadena de suministro de software.

ver artículo >>

152 extensiones de fondo de pantalla para Chrome con 105.000 instalaciones vinculadas a adware y tráfico falso.

Investigadores de ciberseguridad han descubierto una red de 152 extensiones de Google Chrome que actúan como complementos de fondo de pantalla animado para nuevas pestañas, con el fin de distribuir una familia de programas potencialmente no deseados (PUP, por sus siglas en inglés).

ver artículo >>

INCIDENTES DE SISTEMAS

Más de 400 paquetes de Arch Linux AUR secuestrados para desplegar el rootkit Infostealer y eBPF.

Esta semana, unos atacantes se apoderaron de más de 400 paquetes del Arch User Repository (AUR) y modificaron sus scripts de compilación para instalar un programa de robo de credenciales en cualquier máquina que los compilara.nte, ya que Google ha corregido 429 vulnerabilidades, incluidas 22 clasificadas como críticas, en Chrome 149.0.7827.53 para Windows, macOS, Linux y Chrome para iOS

ver artículo >>

Una grave vulnerabilidad en Splunk Enterprise permite a los atacantes ejecutar código sin autenticación.

Splunk ha publicado actualizaciones de seguridad para solucionar una vulnerabilidad crítica en Splunk Enterprise que podría ser explotada para realizar operaciones de archivos sin autenticación e incluso ejecutar código de forma remota.

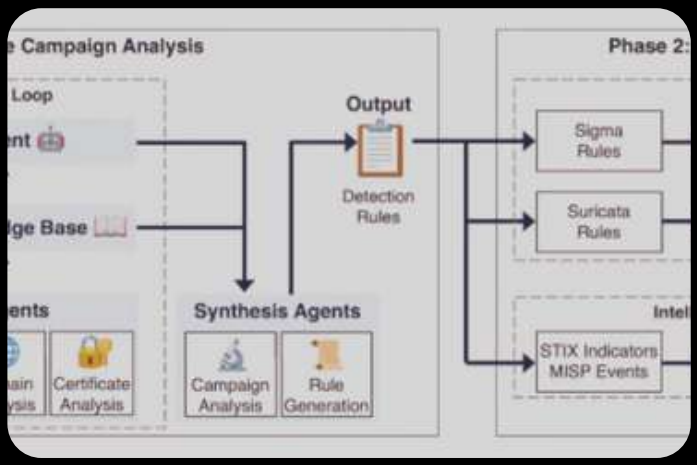
ver artículo >>

Una vulnerabilidad crítica en Wazuh permite a los atacantes manipular las alertas y eliminar las pruebas de seguridad.

Se ha descubierto una vulnerabilidad de seguridad crítica en Wazuh Manager que podría permitir a atacantes remotos manipular alertas de seguridad, eliminar pruebas forenses y alterar datos SIEM en diferentes entornos.

ver artículo >>

RECOMENDACIONES DE LECTURA DE SEGURIDAD



PhishLumos: Desenmascarando campañas de phishing que evaden la detección ocultando contenido

El phishing sigue siendo una de las amenazas más persistentes en ciberseguridad: los seres humanos están cansados, distraídos, confían demasiado y son susceptibles a la urgencia y la autoridad de una manera que ninguna cantidad de capacitación en concientización puede superar por completo.

ver artículo >>

Resumen semanal: Vulnerabilidad de día cero en Chrome, exploits de UniFi, ladrones de macOS, fallos en VPN y más.

Las cosas volvieron a fallar. No como en las películas. Una herramienta antigua quedó expuesta. Se abusó de un paquete abandonado. Una función obsoleta seguía funcionando en producción.

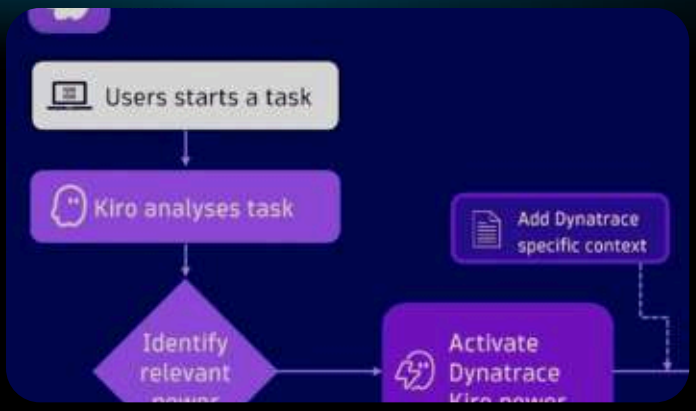
ver artículo >>

NOTICIAS DE NUESTROS PARTNERS

Ciberseguridad para el sector deportivo: las amenazas que afronta una industria digitalizada en 2026.

El 84 % de las organizaciones deportivas sufrieron un incidente cibernético en los últimos 12 meses. A continuación, explicamos qué nos dicen los datos y nuestro análisis sobre por qué el deporte se ha convertido en un objetivo tan frecuente.

ver artículo >>



La observabilidad de Dynatrace ahora es una potencia de Kiro.

En este blog, presentaremos la potencia de Kiro para Dynatrace, mostraremos las ventajas que ofrece a los desarrolladores y explicaremos paso a paso cómo ponerlo en marcha.

ver artículo >>

IBM y ServiceNow amplían su colaboración para aprovechar los datos empresariales para la IA a gran escala.

IBM (NYSE: IBM) y ServiceNow (NYSE: NOW), la plataforma de IA para la reinvención empresarial, anunciaron hoy una colaboración ampliada para abordar dos de las mayores barreras que impiden la implementación a gran escala de la IA empresarial: la falta de datos preparados para la IA y la capa de aplicaciones heredadas.

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