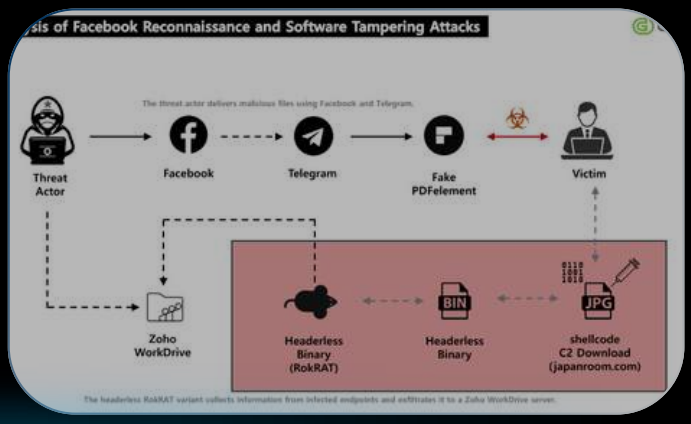
BOLETÍN INFORMATIVO

#215 | Abril 2026

La botnet Masjesu emerge como un servicio de ataques DDoS por encargo dirigido a dispositivos IoT globales.

Investigadores de ciberseguridad han desvelado una red de bots sigilosa diseñada para realizar ataques de denegación de servicio distribuido (DDoS).

ver artículo >>



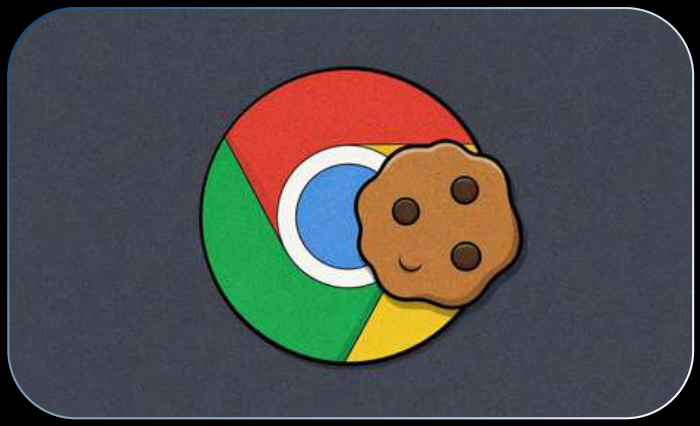
El grupo APT37 de Corea del Norte utiliza ingeniería social de Facebook para distribuir malware RokRAT.

El grupo de hackers norcoreano identificado como APT37 (también conocido como ScarCruft) ha sido señalado como responsable de una nueva campaña de ingeniería social en varias etapas, en la que los ciberdelincuentes contactaron con sus objetivos en Facebook y los agregaron como amigos en la plataforma, convirtiendo este ejercicio de creación de confianza en un canal de distribución para un troyano de acceso remoto llamado RokRAT .

ver artículo >>

Google implementa DBSC en Chrome 146 para bloquear el robo de sesiones en Windows.

Google ha puesto a disposición de todos los usuarios de Windows de su navegador web Chrome las Credenciales de Sesión Vinculadas al Dispositivo (DBSC , por sus siglas en inglés), meses después de haber comenzado a probar esta función de seguridad en fase beta abierta.



ver artículo >>

INCIDENTES DE SISTEMAS

Vulnerabilidad de ejecución remota de código en Marimo explotada en las 10 horas posteriores a su divulgación.

Se descubrió una vulnerabilidad crítica en Marimo, una plataforma de cuadernos Python reactivos de código abierto . Menos de 10 horas después, los atacantes lograron explotar la vulnerabilidad para robar credenciales confidenciales en la nube, lo que pone de manifiesto la extrema rapidez de los ciberdelincuentes actuales.

ver artículo >>

Vulnerabilidad de día cero en Adobe Reader explotada mediante archivos PDF maliciosos desde diciembre de 2025.

Los ciberdelincuentes han estado explotando una vulnerabilidad de día cero previamente desconocida en Adobe Reader mediante documentos PDF manipulados con fines maliciosos desde al menos diciembre de 2025.

ver artículo >>

Vulnerabilidades en Apache Tomcat permiten eludir EncryptInterceptor.

La Apache Software Foundation ha publicado actualizaciones de seguridad de emergencia para solucionar múltiples vulnerabilidades en Apache Tomcat.

ver artículo >>

RECOMENDACIONES DE LECTURA DE SEGURIDAD

Por qué la mayoría de las arquitecturas de confianza cero fallan en la capa de tráfico.

Puedes tener el mejor sistema de identificación del mundo, pero si tu capa de tráfico es un desastre, los hackers simplemente entrarán por una puerta trasera. La verdadera confianza cero requiere proteger la infraestructura de tu red.

ver artículo >>

Los hackers secuestraron las descargas de CPUID y distribuyeron el RAT STX a las víctimas.

Si intentaste descargar algún software del sitio web de CPUID a finales de la semana pasada, es posible que hayas descargado malware en su lugar.

ver artículo >>

Resumen semanal: Espionaje mediante fibra óptica, rootkits de Windows, búsqueda de vulnerabilidades mediante IA y más.

Ha llegado el lunes y el caos acumulado del fin de semana está a punto de estallar. Estamos rastreando una vulnerabilidad crítica de día cero que ha permanecido oculta en sus archivos PDF durante meses, además de una injerencia estatal agresiva en la infraestructura que finalmente está saliendo a la luz.

ver artículo >>

NOTICIAS DE NUESTROS PARTNERS

Integración de los equipos SOC y IR con investigaciones automatizadas de amenazas para el mundo híbrido.

La respuesta a incidentes suele verse afectada tras su detección debido a la fragmentación de las herramientas y la visibilidad limitada. Darktrace unifica la detección y la investigación en entornos locales y en la nube, lo que permite la captura automatizada de pruebas y una respuesta más rápida y clara.

ver artículo >>

Dynatrace adquirirá Bindplane para tomar el control del ciclo de vida de la telemetría.

Dynatrace ha firmado un acuerdo para adquirir Bindplane, una moderna plataforma de telemetría basada en estándares abiertos que actúa como plano de control para datos de diversas fuentes. Juntos, Dynatrace y Bindplane ampliarán la recopilación de datos desde el extremo de la red hasta el análisis, combinando las capacidades de una plataforma de telemetría basada en estándares abiertos con la observabilidad impulsada por IA para brindar a los clientes mayor acceso, flexibilidad y control sobre sus registros, métricas y datos de aplicaciones.

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