BOLETÍN INFORMATIVO N°192

JULIO 2025

Chaos RaaS emerge tras el derribo de BlackSuit y exige 300.000 dólares a las víctimas estadounidenses

Los actores de Chaos RaaS iniciaron una inundación de spam de bajo esfuerzo, que escaló a ingeniería social basada en voz para obtener acceso, seguido por el abuso de la herramienta RMM para una conexión persistente y software legítimo de intercambio de archivos para la exfiltración de datos.

Los ciberdelincuentes utilizan aplicaciones falsas para robar datos y chantajear a los usuarios en las redes móviles de Asia

Los dominios falsos, que se hacen pasar por páginas de listados de tiendas de aplicaciones legítimas, se utilizan como señuelo para engañar a los usuarios para que instalen estas aplicaciones, lo que resulta en la exfiltración de listas de contactos e imágenes, todo ello mientras se mantiene una ilusión de legitimidad.

ToolShell: el buffet de explotación que los atacantes aprovechan en SharePoint

A partir del 17 de julio, ToolShell ha sido ampliamente explotado por todo tipo de actores de amenazas, desde cibercriminales de poca monta hasta grupos APT de estado-nación. Dado que SharePoint está integrado con otros servicios de Microsoft, como Office, Teams, OneDrive y Outlook, este compromiso puede proporcionar a los atacantes un asombroso nivel de acceso en toda la red afectada.

Aeroflot cancela medio centenar de vuelos por un ciberataque a sus sistemas de información

Aeroflot ha sufrido un ciberataque este lunes a sus sistemas de información que ha provocado interrupciones en el servicio, con más de 80 retrasos y la cancelación de 60 vuelos en el aeropuerto de Moscú-Sheremétievo.

Encuentran una nueva y potente cepa de ransomware asociada a BlackByte

Los atacantes que se están sirviendo de ella pertenecerían a la conocida operación de ransomware BlackByte. Su nueva cepa, según los investigadores, marcaría una evolución "preocupante" en sus capacidades.

CISA advierte sobre un incremento de los ataques del grupo de ransomware Interlock

Dicha agencia ha emitido un aviso en el que describe cómo Interlock escoge a sus víctimas en función de la oportunidad y ejecuta ataques con motivaciones financieras sirviéndose de vectores como la ingeniería social.

RECOMENDACIONES

LECTURA DE SEGURIDAD

Deepfakes por IA, una mina de oro para los ciberdelincuentes

Los Deepfakes por IA han dejado de ser una función teórica y se han convertido en una «solución» explotable en el mundo real que mina la confianza digital, expone a las empresas a nuevos riesgos e impulsa el negocio comercial de los ciberdelincuentes, asegura un nuevo informe de Trend Micro.

Orden a partir del caos: uso del cifrado de la teoría del caos para proteger OT e IoT

Ravi Monani, ingeniero de diseño de AMD, se propone proporcionar cifrado seguro para dispositivos periféricos pequeños con recursos limitados, como el Internet de las Cosas (IoT), entre otros. La estrategia elegida es controlar el caos, o más específicamente, aprovechar la teoría del caos.

NOTICIAS DE

NUESTROS PARTNERS

Cerrando la brecha de habilidades en respuesta a incidentes y análisis forense en la nube

La rápida migración a recursos en la nube ha puesto a los equipos de seguridad a la defensiva. Si bien intentan aplicar herramientas locales tradicionales a la nube, cada vez es más evidente que no son adecuadas para su propósito. Especialmente en el contexto de la investigación forense y la respuesta a incidentes.

Maximizar la eficiencia de la nube: impulsar la optimización de costos y la sostenibilidad con Dynatrace

A medida que las organizaciones adoptan un futuro basado en la nube y la IA, aumenta la presión para controlar el gasto en infraestructura y, al mismo tiempo, cumplir con los objetivos de sostenibilidad. Como director de tecnología, quiero que mis inversiones se centren en las personas, creando equipos de desarrollo sólidos e innovadores.

Sobrecarga de acrónimos: el primer juego de ciberseguridad para combatir la proliferación de acrónimos

Cuando su pila de seguridad es una maraña de términos como IAM , JIT, UAR, EDR y más, se pierden algunos detalles. Además, para mayor confusión, algunos acrónimos representan múltiples tecnologías o conceptos ampliamente utilizados. Un analista júnior puede interpretar una cosa. Un ingeniero puede asumir otra. ¿El resultado? Falta de comunicación, desalineación y vulnerabilidades reales y explotables en la estrategia de seguridad.

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