BOLETÍN INFORMATIVO N°210

DICIEMBRE 2025

RomCom utiliza ataques de actualizaciones falsas de SocGholish para distribuir malware de Mythic Agent

Los actores de amenazas detrás de una familia de malware conocida como RomCom atacaron a una empresa de ingeniería civil con sede en EE. UU. a través de un cargador de JavaScript denominado SocGholish para entregar el Mythic Agent.

El nuevo malware MaaS de Albiriox ataca a más de 400 aplicaciones para cometer fraudes en dispositivos y controlar la pantalla.

Un nuevo malware para Android llamado Albiriox se ha anunciado bajo un modelo de malware como servicio (MaaS) para ofrecer un "espectro completo" de funciones para facilitar el fraude en el dispositivo (ODF), la manipulación de la pantalla y la interacción en tiempo real con los dispositivos infectados.

Los scripts Bootstrap de Python heredados generan un riesgo de adquisición de dominio en múltiples paquetes de PyPI

Investigadores de ciberseguridad han descubierto código vulnerable en paquetes heredados de Python que potencialmente podrían allanar el camino para una vulneración de la cadena de suministro en el Índice de paquetes de Python (PyPI) a través de un ataque de toma de dominio.

Una falla en la administración de API de Microsoft Azure permite la creación de cuentas entre inquilinos, evadiendo las restricciones de administrador.

Una vulnerabilidad de seguridad crítica en el Portal para desarrolladores de Microsoft Azure API Management (APIM) permite a los atacantes registrar cuentas en diferentes instancias de inquilinos, incluso cuando los administradores han deshabilitado explícitamente el registro de usuarios a través de la interfaz del portal.

Una vulnerabilidad crítica en el marco bRPC de Apache permitió a los atacantes bloquear el servidor

Se ha descubierto una vulnerabilidad de seguridad crítica en el marco Apache bRPC que podría permitir a atacantes remotos bloquear servidores enviando datos JSON especialmente diseñados.

RECOMENDACIONES

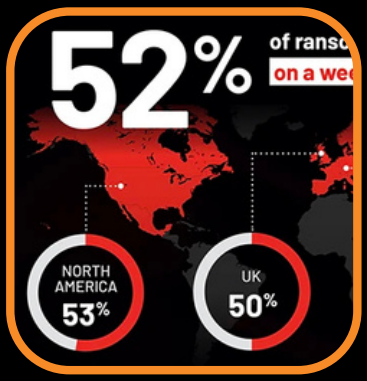
LECTURA DE SEGURIDAD

Por qué la gestión de contraseñas define el éxito de PCI DSS

La mayoría de los CISO pasan sus días lidiando con paneles de control ruidosos y presentaciones de proveedores que prometen un atajo hacia el cumplimiento normativo . Puede resultar abrumador identificar lo que realmente importa.

El fin de semana es el momento cumbre para el ransomware

Según un informe de Semperis , más de la mitad de las organizaciones que sufrieron un ataque de ransomware el año pasado fueron atacadas durante un fin de semana o un día festivo. Estos períodos suelen conllevar escasez de personal, investigaciones más lentas y menos vigilancia en los sistemas de identidad.



Los nuevos ataques de ClickFix utilizan pantallas falsas de Windows Update para engañar a los empleados

Los administradores de Windows y las OSC deben desactivar la capacidad de las computadoras personales de ejecutar automáticamente comandos para bloquear la última versión de los ataques de ingeniería social de ClickFix.

NOTICIAS DE

NUESTROS PARTNERS

Los ataques de phishing aumentan un 620% en el período previo al Black Friday

El Black Friday sigue siendo una excelente oportunidad para los cibercriminales. Los primeros análisis de Darktrace muestran un aumento significativo en el número de atacantes que se hacen pasar por marcas conocidas, así como por las marcas que los estafadores suplantan con más frecuencia.

BeyondTrust obtiene la certificación TX-RAMP Nivel 2 en toda su cartera, lo que fortalece la confianza en la seguridad de la identidad estatal.

La cartera completa de productos de BeyondTrust ahora cuenta con la certificación TX-RAMP Nivel 2, lo que ayuda a las agencias de Texas a simplificar las adquisiciones, cumplir con los requisitos de cumplimiento y fortalecer la seguridad de la identidad con soluciones confiables y auditables.

Información en tiempo real: aproveche las capacidades de observación de Dynatrace dentro de Kiro con tecnología de AWS

En los entornos nativos de la nube actuales, es crucial tener datos de observabilidad en tiempo real al alcance de la mano. Al integrar Kiro con tecnología de AWS con Dynatrace, puede aprovechar las potentes capacidades de monitorización y resolución de problemas asistidas por IA directamente en su flujo de trabajo de desarrollo.

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