

#133



BOLETÍN INFORMATIVO MAINSOFT



INCIDENTES DE SEGURIDAD

LA FALLA DEL CANAL LATERAL 'ILEAKAGE' EN APPLE SAFARI PUEDE COMPARTIR CONTRASEÑAS Y MENSAJES

Un grupo de investigadores académicos publicó el miércoles un estudio que muestra cómo lanzaron un ataque que podría obligar a un navegador Apple Safari a mostrar información personal



[*Más Información*](#)

ROUNDCUBE 0-DAY UTILIZADO PARA ROBAR CORREOS ELECTRÓNICOS DE GOBIERNOS EUROPEOS

La banda de ciberespionaje Winter Vibern aprovechó un error de día cero ahora parcheado en el servicio de correo web de código abierto de Roundcube para robar correos electrónicos de entidades gubernamentales y grupos de expertos europeos.

[*Más Información*](#)

PAQUETES MALICIOSOS NUGET DETECTADOS DISTRIBUYENDO MALWARE SEROXEN RAT

Los investigadores de ciberseguridad han descubierto un nuevo conjunto de paquetes maliciosos publicados en el administrador de paquetes NuGet utilizando un método menos conocido para la implementación de malware.

[*Más Información*](#)



VERSIÓN TROYANIZADA DEL SOFTWARE PYCHARM ENTREGADA A TRAVÉS DE ANUNCIOS DE BÚSQUEDA DE GOOGLE



Se ha observado una nueva campaña de publicidad maliciosa que aprovecha un sitio web comprometido para promover versiones falsas de PyCharm en los resultados de búsqueda de Google aprovechando los anuncios dinámicos de búsqueda

[**Más Información**](#)

CSIRT DE GOBIERNO COMPARTE INFORMACIÓN DE NUEVAS VULNERABILIDADES CRÍTICAS EN CISCO IOS XE SOFTWARE WEB UI FEATURE

El CSIRT de Gobierno comparte información de nuevas vulnerabilidades críticas en Cisco IOS XE Software Web UI Feature.



[**Más Información**](#)

CSIRT INFORMA DE VULNERABILIDAD CRÍTICA QUE AFECTA A BIG-IP

El CSIRT de Gobierno comparte información de una nueva vulnerabilidad crítica de seguridad que impacta a BIG-IP

[**Más Información**](#)

CSIRT INFORMA DE VULNERABILIDADES EN NGINX INGRESS PARA KUBERNETES

El CSIRT de Gobierno comparte información de tres nuevas vulnerabilidades de alto riesgo que afectan al controlador NGINX Ingress para Kubernetes

[**Más Información**](#)



EXPOSICIÓN DE DATOS DE SERVICENOW: UNA LLAMADA DE ATENCIÓN PARA LAS EMPRESAS



A principios de esta semana, ServiceNow anunció en su sitio de soporte que las configuraciones incorrectas dentro de la plataforma podrían resultar en un “acceso no intencionado” a datos confidenciales. Para las organizaciones que utilizan ServiceNow.

[Más Información](#)

LOS ATAQUES DE CRIPTOJACKING DE ELEKTRA-LEAK EXPLOTAN LAS CREDENCIALES DE AWS IAM EXPUESTAS EN GITHUB

Una nueva campaña en curso denominada Elektra-Leak ha puesto sus ojos en las credenciales expuestas de gestión de identidad y acceso (IAM) de Amazon Web Service (AWS) dentro de los repositorios públicos de GitHub para facilitar las actividades de cryptojacking.



[Más Información](#)

MILLONES DE REGISTROS MÉDICOS EXPUESTOS TRAS INCIDENTE

La base de datos contenía una gran cantidad de resultados de pruebas médicas que incluían los nombres de los pacientes, los médicos, si la muestra de la prueba se realizó en casa o en un centro médico y una amplia gama de otra información de salud confidencial.



[Más Información](#)



METASPLOIT FRAMEWORK: EXPLOTAR VULNERABILIDADES PUEDE SER BASTANTE FÁCIL



Explotar vulnerabilidades puede parecer complejo, pero el uso de algunas herramientas simplifica mucho el proceso. Descubre cómo funciona la explotación de un fallo con Metasploit.

[Más Información](#)

ARPANET: EL NACIMIENTO DE LA INTERNET MODERNA



Internet es una parte esencial de la vida cotidiana que conecta a miles de millones de personas en todo el mundo y permite la difusión de información, el comercio, la comunicación y colaboración a una escala sin precedentes.

[Más Información](#)

UN INFORME VINCULA A CHATGPT CON UN AUMENTO DEL 1265 % EN LOS CORREOS ELECTRÓNICOS DE PHISHING



El informe SlashNext State of Phishing 2023 ha revelado una tendencia preocupante en el panorama de la ciberseguridad, revelando un aumento del 1265 % en los correos electrónicos de phishing maliciosos desde el cuarto trimestre de 2022.

[Más Información](#)



PRINCIPALES PREDICCIONES DE TENDENCIAS EN CIBERSEGURIDAD PARA 2024: EDICIÓN BEYONDTRUST

A medida que llegamos a la última esquina de 2023, es hora de examinar las tendencias de ciberseguridad que han tomado forma a lo largo del año y comenzar a planificar las que se avecinan en el horizonte



[Más Información](#)



DARKTRACE



DARKTRACE

DARKTRACE/EMAIL EN ACCIÓN: POR QUÉ LA SEGURIDAD DEL CORREO ELECTRÓNICO IMPULSADA POR IA ES LA MEJOR DEFENSA CONTRA CAMPAÑAS SOSTENIDAS DE PHISHING

Desde sus inicios, el correo electrónico ha sido considerado una de las herramientas más importantes para las empresas, revolucionando la comunicación y permitiendo que los equipos globales estén aún más conectados.

[Más Información](#)

CYLANCE

¡EL HACKER ME ROBÓ LA TAREA!

El año escolar 2022-23 fue una lucha cibernética para las escuelas del Reino Unido. La Vice Society, que se cree está detrás de numerosos ataques de ransomware a instituciones educativas en todo el Reino Unido y EE. UU., filtró información sobre necesidades educativas especiales (SEN) de los niños

[Más Información](#)



CYLANCE

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](#)

DARKTRACE



CYLANCE

BeyondTrust

EVENTOS CERCANOS DE NUESTROS PARTNERS

DARKTRACE <https://bit.ly/3Cd0x8g>

CYLANCE <https://bit.ly/3EIP748>

IBM <https://ibm.co/2Z1YVA3>

BEYONDTRUST <https://bit.ly/3EwkngX>



www.mainsoft.cl