Mes: Enero 2026

Resumen mensual

Malware

Destapan una de las mayores operaciones de malware basadas en extensiones de navegador

Resumen: Investigadores de ciberseguridad han descubierto una operación que utilizaba extensiones maliciosas para los navegadores Google Chrome, Mozilla Firefox y Microsoft Edge para obtener información confidencial de los usuarios que las descargaran en sus equipos. Esta operación, asociada al grupo de origen chino conocido como Dark Spectre, se estima que ha afectado a casi 8,8 millones de usuarios, sin haber sido detectada durante más de 7 años.

¿Cómo protegerse?

- ✅ No instales aplicaciones desde orígenes no verificados.
- ✅ Evita guardar contraseñas en el dispositivo, usa un gestor de contraseñas.
- ✅ Usa un antivirus y mantén tus dispositivos actualizados.

Link: https://www.escudodigital.com/ciberseguridad/operacion-masiva-malware-extensiones.html

Nuevo malware amenaza a más de 50.000 usuarios de WhatsApp

Resumen: Una nueva amenaza en forma de programa malicioso que puede acceder a mensajes, archivos multimedia, contraseñas, documentos y contactos almacenados en los dispositivos mediante el abuso de la aplicación de mensajería WhatsApp. El programa, que se presenta como una API de WhatsApp Web llamada Baileys, ha afectado ya a más de 56.000 usuarios.

¿Cómo protegerse?

- ✅ Evita instalar aplicaciones de terceros no aprobadas.
- ✅ Instala un antivirus con análisis en tiempo real en tu dispositivo móvil.
- ✅ Limita los permisos a los que tienen acceso las aplicaciones instaladas.

Link: https://www.20minutos.es/tecnologia/ciberseguridad/cuidado-nuevo-malware-amenaza-mas-50000-usuarios-whatsapp-puede-acceder-todos-chats_6914150_0.html

Maverick, el troyano bancario que utiliza la IA para robar tus datos

Resumen: Un nuevo troyano ha aparecido recientemente, llamado Maverick. Este software malicioso ha sido desarrollado empleando Inteligencia Artificial y cuenta con capacidades para evadir detección por parte de sistemas de seguridad. Se propaga normalmente mediante WhatsApp a través de archivos y enlaces compartidos.

¿Cómo protegerse?

- ✅ Mantén las aplicaciones de tu dispositivo actualizadas para evitar vulnerabilidades.
- ✅ No descargues aplicaciones desde fuentes no oficiales.
- ✅ Evita dar acceso innecesario a tus datos o funciones del dispositivo.

Link: https://www.kaspersky.es/about/press-releases/maverick-el-troyano-bancario-impulsado-por-ia-que-podria-expandirse-internacionalmente

Phishing

Nueva estafa de phishing para el robo de cuentas de Microsoft 365

Resumen: Se ha producido un repunte en el número de ataques contra cuentas de Microsoft 365. Investigadores reportan campañas de suplantación de identidad que presentan a las víctimas mensajes con enlaces de Microsoft, indicando que es necesario introducir códigos de un solo uso adjuntos en estos mensajes. Sin embargo, al hacerlo, los atacantes pueden obtener acceso a la cuenta de Microsoft 365.

¿Cómo protegerse?

✅ Activa la verificación en dos pasos para mayor seguridad en todos los servicios y plataformas.
✅ No accedas a enlaces provenientes de orígenes desconocidos.
✅ Comprueba la autenticidad de las páginas web a las que accedas.

Link: https://www.20minutos.es/tecnologia/ciberseguridad/nueva-estafa-phishing-roba-cuenta-microsoft-365-sin-que-te-des-cuenta-asi-puedes-evitarlo_6913521_0.html

GhostPairing secuestra cuentas de WhatsApp

Resumen: Investigadores de seguridad han detectado una nueva campaña de fraude llamada GhostPairing, donde mediante el uso de ingeniería social, los atacantes convencen a sus víctimas para acceder a un enlace que finge ser un servicio de Meta, la empresa antes conocida como Facebook. De caer en la estafa, las victimas vinculan su cuenta de WhatsApp al dispositivo de los atacantes, lo que les permite espiar conversaciones, acceder a archivos compartidos, y mantener acceso al dispositivo.

¿Cómo protegerse?

✅ No compartas los códigos de seguridad que recibas en tu cuenta, ya que se pueden usar para acceder sin tu permiso.
✅ Evita acceder a enlaces sospechosos recibidos mediante comunicaciones.
✅ Si dudas del remitente, contacta con él mediante otros canales.

Link: https://unaaldia.hispasec.com/2026/01/ghostpairing-una-estafa-secuestra-cuentas-de-whatsapp-sin-robar-contrasenas-ni-duplicar-la-sim.html

Correos falsos de Booking.com distribuyen malware usando la técnica de ClickFix simulando un error de Windows

Resumen: Una campaña de phishing ha aparecido donde suplantando a la entidad Booking.com, actores maliciosos envían a usuarios de la plataforma mediante el uso de correos fraudulentos enlaces a páginas externas ajenas a la compañía. En estas páginas, los atacantes emplean la técnica ClickFix, que convence a los usuarios de realizar ciertas acciones para solucionar problemas que aparecen en la página web.

¿Cómo protegerse?

✅ No ejecutes combinaciones de teclas o comandos solicitados por páginas web.
✅ No accedas a enlaces provenientes de SMS sin verificar su legitimidad.
✅ Nunca des datos personales o bancarios por teléfono ni en páginas no verificadas.

Link: https://www.welivesecurity.com/es/estafas-enganos/phishing-booking-clickfix-malware-windows/

Brechas de seguridad

Un hacker asegura haber pirateado a Endesa y accedido a datos de 20 millones de personas

Resumen: Un ciberdelincuente afirma haber obtenido información extraída mediante un ataque a la compañía Endesa. El hacker declara haber logrado acceso a una base de datos obteniendo así más de 1 terabyte de información de la compañía, incluyendo detalles de más de 20 millones de clientes de Endesa. Entre esta información se incluyen direcciones, datos financieros e información de contacto.

¿Cómo protegerse?

✅ Evita guardar tus datos bancarios en páginas web que lo soliciten.
✅ Activa la autenticación multifactor (MFA) en todas tus cuentas.
✅ Evita dar demasiada información personal al registrarte en sitios web para reducir la probabilidad de que se expongan tus datos en caso de una filtración.

Link: https://www.escudodigital.com/ciberseguridad/endesa-brecha-seguridad-ciberataque.html

Grave brecha de seguridad en Spotify: el 99% de sus canciones han sido pirateadas por un grupo de hackers

Resumen: Spotify ha sufrido una importante brecha de seguridad, donde un grupo de hackers asegura haber obtenido un 99% del contenido almacenado por la compañía. La publicación, compuesta por 256 millones de canciones y 86 millones de archivos de audio, presenta un serio problema legal para la compañía, ya que mucho de este contenido se encuentra protegido por derechos de autor.

¿Cómo protegerse?

✅ Verifica el origen de las comunicaciones que recibas porque, aunque contengan información legitima, pueden ser realizadas por ciberdelincuentes.
✅ No compartas información personal innecesaria al registrarte en servicios.
✅ Mantén tus dispositivos siempre actualizados.

Link: https://www.marca.com/tecnologia/2025/12/24/grave-brecha-seguridad-spotify-99-canciones-han-sido-pirateadas-grupo-hackers.html

La Agencia Espacial Europea confirma una brecha de seguridad en servidores externos

Resumen: La Agencia Espacial Europea (ESA) ha sufrido un incidente de ciberseguridad en el que varios de sus servidores externos han sido comprometidos. La organización indica que, durante el ataque, los ciberdelincuentes se hicieron con información muy limitada, ya que las plataformas afectadas solo se usaban para actividades de ingeniería colaborativa.

¿Cómo protegerse?

✅ Limita la información personal que almacenas en sitios de terceros.
✅ Cambia regularmente tus contraseñas para evitar accesos no autorizados.
✅ Desconfía de mensajes de fuentes no verificadas, aunque usen información real.

Link: https://www.escudodigital.com/ciberseguridad/la-agencia-espacial-europea-confirma-una-brecha-de-seguridad-en-servidores-externos.html

CVEs

Actualizaciones de seguridad de Microsoft: enero de 2026

Resumen: Microsoft ha publicado un paquete de actualizaciones que cubren hasta 112 vulnerabilidades para distintos productos y servicios de la compañía, incluyendo fallos en Windows y la suite de Office. 80 de estas vulnerabilidades han sido calificadas como de alta severidad por la compañía, con las 32 restantes categorizadas como de severidad media.
Gravedad: 🔥 Alta (7.8/10) – Riesgo para usuarios que utilizan productos de Microsoft.
Ejemplo real: Usuarios que utilicen productos de Microsoft y el sistema operativo Microsoft Windows.

✅ **Solución:** Asegurarse que los productos de Microsoft están actualizados a la última versión.

Link: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos/actualizaciones-de-seguridad-de-microsoft-de-enero-de-2026

Actualización de seguridad de SAP de enero de 2026

Resumen: El nuevo paquete de actualizaciones de seguridad de SAP publicado este mes soluciona 17 vulnerabilidades en varios productos, incluyendo S/4HANA y NetWeaver. Los 4 fallos más graves, categorizados como críticos, podrían potencialmente otorgar acceso no autorizados o ejecución de código a atacantes, conllevando serios riesgos para empresas que no actualicen sus sistemas.
Gravedad: 🔥 Crítica (9.9/10) – Riesgo para los usuarios que usen productos de SAP.
Ejemplo real: Usuarios que utilicen S/4HANA o NetWeaver.

✅ **Solución:** Actualizar de manera urgente a las últimas versiones del software para evitar explotación de estas vulnerabilidades.

Link: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos/actualizacion-de-seguridad-de-sap-de-enero-de-2026

Boletín de seguridad de Android: enero de 2026

Resumen: Google ha publicado el paquete de actualizaciones de seguridad correspondientes a enero de 2026 que soluciona una vulnerabilidad crítica afectando a componentes Dolby en el sistema operativo Android. Este fallo podía potencialmente permitir a un atacante evadir ciertas medidas de seguridad, logrando de esta forma el compromiso de los dispositivos vulnerables.
Gravedad: 🔥 Media (5.4/10) – Riesgo para usuarios con dispositivos Android.
Ejemplo real: Usuarios que utilizan móviles Android.

✅ **Solución:** Actualizar el sistema operativo Android a la última versión.

Link:https://www.incibe.es/incibe-cert/alerta-temprana/avisos/boletin-de-seguridad-de-android-enero-de-2026