Mes: Octubre 2025

Resumen mensual

Malware

Datzbro, nuevo troyano bancario en Facebook que busca robar tu dinero

Resumen: Datzbro es un nuevo malware distribuido mediante Facebook que tiene como principal objetivo llevar a cabo fraudes financieros. Los ciberdelincuentes se ganan la confianza de sus víctimas con distintas actividades y una vez lo logran, continúan la interacción a través de Messenger o WhatsApp, donde les piden a sus víctimas que descarguen esta aplicación maliciosa.

¿Cómo protegerse?

- ✅ Descarga aplicaciones siempre desde tiendas de aplicaciones oficiales.
- ✅ Evita guardar contraseñas en el dispositivo, usa un gestor de contraseñas.
- ✅ Usa un antivirus y mantén tus dispositivos actualizados.

Link: https://www.20minutos.es/tecnologia/ciberseguridad/un-nuevo-troyano-bancario-usa-deepfakes-esta-red-social-para-robar-tu-dinero-sin-que-notes_6511892_0.html

ClayRat, malware espía para Android que usa el móvil infectado para enviar SMS y llegar a más víctimas

Resumen: Recientemente se ha descubierto una nueva amenaza para dispositivos móviles Android llamada ClayRat. Distribuida a través de sitios web fraudulentos que ofrecen versiones modificadas de aplicaciones populares, ClayRat es capaz de acceder a registros de llamadas, fotografías, mensajes y contactos en el dispositivo.

¿Cómo protegerse?

- ✅ Evita instalar versiones modificadas de aplicaciones móviles que ofrezcan mejoras o funciones de pago gratis porque pueden contener software malicioso.
- ✅ Evita dar acceso innecesario a tus datos o permisos del dispositivo.
- ✅ Instala software antivirus en tu dispositivo para evitar aplicaciones maliciosas.

Link: https://www.europapress.es/portaltic/ciberseguridad/noticia-clayrat-spyware-android-usa-movil-infectado-enviar-sms-llegar-mas-victimas-20251010163324.html

España, víctima de Klopatra: el nuevo troyano bancario que vacía tu cuenta bancaria

Resumen: Un nuevo software malicioso de acceso remoto llamado Klopatra ha comprometido múltiples dispositivos en España e Italia, permitiendo a los responsables obtener credenciales de acceso a cuentas bancarias. Este malware se oculta en aplicaciones IPTV y solicita permisos de accesibilidad, lo que permite evadir la detección y tomar control de los dispositivos móviles infectados.

¿Cómo protegerse?

- ✅ No guardes credenciales ni información de cuentas bancarias en tu móvil.
- ✅ No descargues aplicaciones desde fuentes no oficiales.
- ✅ Evita dar acceso innecesario a tus datos o funciones del dispositivo.

Link: https://www.20minutos.es/tecnologia/ciberseguridad/klopatra-nuevo-troyano-bancario-vacia-cuenta-bancaria-mientras-duermes_6512624_0.html

Phishing

Campaña de smishing que suplanta a entidades bancarias solicitando que les llames

Resumen: El Instituto Nacional de Ciberseguridad (INCIBE) ha informado sobre una nueva campaña de SMS fraudulentos que busca engañar a las víctimas haciéndoles creer que sus bancos van a realizar una transferencia no autorizada. En el mensaje se incluye un número de teléfono al que se insta a llamar con urgencia para cancelar la supuesta operación; sin embargo, dicho número pertenece en realidad a los atacantes.

¿Cómo protegerse?

- ✅ Nunca des datos personales o bancarios por teléfono ni en páginas no verificadas.
- ✅ Desconfía de comunicaciones aparentemente oficiales a través de SMS.
- ✅ No realices transacciones bancarias en páginas web no verificadas.

Link: https://www.incibe.es/ciudadania/avisos/campana-de-smishing-que-suplanta-entidades-bancarias-solicitando-que-les-llames

Una nueva campaña de phishing suplantando a Endesa distribuye el troyano bancario Metamorfo

Resumen: Expertos en ciberseguridad han detectado recientemente una nueva campaña de phishing que usa el nombre de la compañía Endesa para enviar correos a sus víctimas. Estos correos dicen contener una factura pendiente e incluyen un archivo adjunto que contiene el programa malicioso Metamorfo, diseñado para robar credenciales y datos bancarios.

¿Cómo protegerse?

- ✅ No almacenes las credenciales en el navegador web; en su lugar, utiliza un gestor de contraseñas seguro.
- ✅ Emplea contraseñas robustas, evita su reutilización y activa el doble factor de autenticación.
- ✅ Si dudas del remitente, contacta con él mediante canales oficiales.

Link: https://bitlifemedia.com/2025/10/una-nueva-campana-de-phishing-suplantando-a-endesa-distribuye-el-troyano-bancario-metamorfo/

La Guardia Civil desmantela una red de phishing bancario y detiene al principal desarrollador de kits de robo de credenciales en España

Resumen: La Guardia Civil ha logrado detener a un grupo de cibercriminales propietario de una plataforma que ofrecía servicios a demanda para otros ciberdelincuentes, en la que se vendían kits listos para su uso en actividades delictivas como phishing o extorsión a empresas empleando ransomware.

¿Cómo protegerse?

- ✅ Evita usar enlaces recibidos en mensajes, accede mediante canales oficiales.
- ✅ Nunca des datos personales o bancarios por teléfono ni en páginas no verificadas.
- ✅ No instales aplicaciones provenientes de orígenes desconocidos.

Link: https://web.guardiacivil.es/es/destacados/noticias/La-Guardia-Civil-desmantela-una-red-de-phishing-bancario-y-detiene-al-principal-desarrollador-de-kits-de-robo-de-credenciales-en-Espana/

Brechas de seguridad

Discord aclara que el ciberataque a un proveedor externo ha expuesto documentos oficiales de 70.000 usuarios

Resumen: Un proveedor de Discord, una popular plataforma de comunicaciones ha sufrido una brecha de seguridad que ha provocado la exposición de datos confidenciales de más de 70000 usuarios. Entre la información filtrada se incluyen documentos de identidad, fotografías y datos bancarios.

¿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.europapress.es/portaltic/ciberseguridad/noticia-discord-aclara-reciente-ciberataque-proveedor-externo-expuso-documentos-oficiales-70000-usuarios-20251009100731.html

Brecha de ciberseguridad en el CNI: investigan si un 'hacker' español huido a Rusia filtró datos de su cúpula

Resumen: Un ciberdelincuente ha llevado a cabo múltiples filtraciones de datos personales de la cúpula del gobierno, incluyendo al presidente del gobierno y a altos cargos del CNI. La Policía Nacional investiga al presunto ciberdelincuente responsable, que posiblemente se encuentra a la fuga.

¿Cómo protegerse?

✅ Revisa que la autenticación multifactor (MFA) esté activada en todas tus cuentas.
✅ No abras enlaces ni proporciones información personal sin confirmar la autenticidad del remitente.
✅ Evita guardar tus contraseñas en el navegador, usando preferentemente un gestor de contraseñas.

Link: https://www.elespanol.com/espana/20250923/brecha-ciberseguridad-cni-investigan-filtrar-datos-cupula-hacker-espanol-huido-rusia/1003743936123_0.html

Madrileña Red de Gas sufre un ciberataque donde se roban datos de contadores y clientes

Resumen: Madrileña Red de Gas, una de las principales distribuidoras de gas natural en Madrid, ha detectado una brecha de seguridad en su infraestructura informática. Los atacantes lograron acceder a la identidad e información de contacto de sus clientes.

¿Cómo protegerse?

✅ Verifica el origen de las comunicaciones que recibas porque, aunque contengan información legitima, pueden provenir de ciberdelincuentes.
✅ No compartas información personal innecesaria.
✅ Mantén actualizados tus dispositivos y evita hacer clic en enlaces sospechosos.

Link: https://www.eldiario.es/tecnologia/principales-distribuidoras-gas-madrid-sufre-ciberataque-roba-datos-contadores-clientes_1_12622914.html

CVEs

Actualizaciones de seguridad de Microsoft de octubre de 2025

Resumen: Microsoft ha publicado un paquete de actualizaciones de seguridad que corrige 175 vulnerabilidades, de las cuales hay 5 calificadas como críticas, 121 como altas, 46 como medias y 3 como bajas. Las vulnerabilidades afectan a múltiples productos y servicios de Microsoft, incluyendo Windows y Office.
Gravedad: 🔥 Crítica (9.9/10) – Riesgo para usuarios que utilizan productos de Microsoft.
Ejemplo real: Usuarios que utilicen 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-octubre-de-2025

Actualización de seguridad de SAP de octubre de 2025

Resumen: SAP ha publicado un conjunto de actualizaciones de seguridad para solucionar 13 vulnerabilidades: 3 de severidad crítica, 2 de severidad alta, 6 de severidad media y 2 de severidad baja. Estas vulnerabilidades afectan a varios de sus productos y su explotación podría permitir a un atacante ejecutar comandos y acceder a información confidencial.
Gravedad: 🔥 Crítica (10/10) – Riesgo para usuarios que utilizan productos de SAP.
Ejemplo real: Usuarios que utilizan los productos de SAP.

✅ **Solución:** Actualizar los productos de SAP a las últimas versiones disponibles.

Link: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos/actualizacion-de-seguridad-de-sap-de-octubre-de-2025

Múltiples vulnerabilidades en productos de Apple

Resumen: Apple ha publicado una actualización solucionando múltiples vulnerabilidades detectadas en dispositivos iOS y macOS. Una de estas vulnerabilidades, de categoría crítica, permitiría acceso remoto a atacantes, y otra, de categoría alta, se cree que podría estar siendo explotada activamente actualmente.
Gravedad: 🔥 Crítica (9.8/10) – Riesgo para usuarios con dispositivos iOS o macOS.
Ejemplo real: Usuarios que utilizan los productos de Apple.

✅ **Solución:** Actualizar los productos de Apple a la última versión.

Link: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-productos-de-apple-1