Mes: Agosto 2025

Resumen mensual

Malware

Troyano PlayPraetor en Android

Resumen: Un grupo de investigadores han identificado un software malicioso en teléfonos Android que permite el acceso remoto a los dispositivos infectados. Apodado PlayPraetor, esta campaña dirigida principalmente a España, Portugal, Francia, Marruecos, Perú y Hong Kong, se calcula que ha infectado actualmente más de 11,000 dispositivos. Su objetivo es el robo de información bancaria mediante pantallas de inicio de sesión falsas.

¿Cómo protegerse?

✅ No accedas a enlaces sospechosos ni descargues archivos desde sitios web no verificados.
✅ Aplica una política de contraseñas robusta y activa el doble factor de autenticación.
✅ Usa un antivirus y mantén tus dispositivos actualizados.

Link: https://www.enhacke.com/blog/troyano-playpraetor-en-android-6890c8de88f4c

SparkKitty: el troyano que roba fotos y datos en iPhone y Android

Resumen: SparkKitty es un software malicioso que tiene como objetivo los dispositivos Android e iPhone para realizar el robo de información y criptomonedas. Según los investigadores el modo de infección es mediante aplicaciones maliciosas relacionadas con criptomonedas y apuestas y una versión infectada de la red social TikTok distribuida mediante las tiendas oficiales tanto Google Play como App Store como en páginas de terceros.

¿Cómo protegerse?

✅ No accedas a enlaces sospechosos ni descargues archivos desde sitios web no verificados.
✅ Instala únicamente aplicaciones de los desarrolladores de confianza.
✅ Usa un antivirus y mantén tus dispositivos actualizados.

Link: https://www.kaspersky.es/about/press-releases/sparkkitty-el-troyano-que-roba-fotos-y-datos-en-iphones-y-android

España experimenta cada mes unos 72 ataques de malware por dispositivo

Resumen: Según el informe de la compañía NordVPN, España es uno de los países con más dispositivos infectados. En dicho estudio España ha registrado cerca de 6,7 millones de incidentes en el último trimestre, una cifra que continúa en aumento.

¿Cómo protegerse?

✅ No almacenes las credenciales en el navegador web; en su lugar, utiliza un gestor de contraseñas seguro.
✅ Activa el doble factor de autenticación en todas las cuentas de usuario.
✅ Usa un antivirus y mantén tu dispositivo actualizado.

Link: https://www.genbeta.com/seguridad/espana-destaca-ciberseguridad-no-para-bien-cada-mes-experimentamos-unos-72-ataques-malware-dispositivo-nordvpn

Phishing

La Guardia Civil detiene a 15 personas acusadas de estafar 1,6 millones de euros por Internet a víctimas de toda España

Resumen: La Guardia Civil ha detenido a una red criminal que habría estafado a múltiples víctimas en España mediante SMS y llamadas fraudulentas. Este ciberataque contra individuos y empresas empleaba identidades robadas para solicitar el pago a sus víctimas. Los agentes creen que la trama afectó a múltiples provincias en España y se estima que habrían robado casi 1,6 millones de euros.

¿Cómo protegerse?

✅ Si recibes un mensaje o una llamada sospechosa, verifica su autenticidad llamando directamente al teléfono oficial, incluso si parece provenir de un contacto de confianza.
✅ Verifica el remitente: Los bancos y empresas nunca piden datos a sus clientes.
✅ Nunca des datos personales o bancarios por teléfono ni en páginas no verificadas.

Link: https://www.rtve.es/noticias/20250713/guardia-civil-detiene-a-15-personas-acusadas-estafar-16-millones-euros-por-internet-a-victimas-toda-espana/16662567.shtml

Un ataque de phishing está robando cuentas de Microsoft

Resumen: Un grupo de ciberdelincuentes está suplantando la página de inicio de sesión de Microsoft para robar credenciales. Los atacantes realizan el envío de enlaces mediante correo electrónico que camuflan las páginas fraudulentas para simular ser seguras y de apariencia legítima. En esta campaña los investigadores han reportado que los correos suelen tener enlaces para abrir un supuesto buzón de voz o un documento compartido, tras el que solicitan las credenciales en la página maliciosa.

¿Cómo protegerse?

✅ Mantén actualizados tus dispositivos y evita hacer clic en enlaces sospechosos.
✅ Nunca des datos personales o bancarios por teléfono ni en páginas no verificadas.
✅ Si recibes un mensaje sospechoso, verifica su autenticidad contactando con el remitente o la empresa a través de sus canales oficiales, incluso si el mensaje parece legítimo.

Link: https://www.20minutos.es/tecnologia/ciberseguridad/ataque-phishing-robando-cuentas-microsoft-conseguir-contrasenas_6234282_0.html

DHL no está avisando por correo de que un paquete ha sido devuelto y que se cobrará una tarifa de envío

Resumen: Se ha detectado una nueva campaña que suplanta a la empresa de transporte DHL mediante el envío de correos electrónicos fraudulentos informando de la devolución de un paquete. Los estafadores engañan a la víctima para que realice un pago mediante una dirección URL fraudulenta prometiéndole así poder recuperarlo.

¿Cómo protegerse?

✅ No descargues archivos ni hagas clic en enlaces o adjuntos sospechosos.
✅ No compartas datos personales en las redes sociales ni realices pagos en páginas web no verificadas.
✅ Si dudas del remitente, contacta con él únicamente a través de los canales oficiales.

Link: https://www.incibe.es/ciudadania/avisos/dhl-no-esta-avisando-por-correo-de-que-un-paquete-ha-sido-devuelto-y-que-se

Brechas de seguridad

Google confirma haber sido víctima de una filtración de datos

Resumen: Google ha confirmado una filtración de datos por el abuso de una aplicación de terceros que permitió a los atacantes el acceso remoto. Mediante una suplantación telefónica (vishing) los cibercriminales lograron acceso a uno de sus sistemas que almacenaba datos de pequeñas y medianas empresas. Según Google el acceso fue breve y la brecha está contenida, además la información extraída fue limitada y se trataba de datos en su mayoría básicos y de dominio público.

¿Cómo protegerse?

✅ Revisa que la autenticación multifactor (MFA) esté activada en todas tus cuentas.
✅ Actualiza las contraseñas de forma periódica y utiliza un gestor de contraseñas para facilitar su gestión y almacenamiento seguro.
✅ Revisa de forma periódica la actividad de tus cuentas de correo electrónico, plataformas digitales y entidades bancarias para detectar accesos no autorizados.

Link: https://diariocompostela.elidealgallego.com/articulo/innovacion/google-confirma-filtracion-datos-provocada-ataque-ingenieria-social-sobre-salesforce-ejecutado-grupo-shinyhunters-5391074

Las empresas Betfair y Louis Vuitton sufren ciberataques

Resumen: Dos grandes empresas de los sectores de apuestas y moda de lujo han sido víctimas de ciberataques que comprometieron datos sensibles de sus clientes en varios países europeos. Se trata de Betfair y Louis Vuitton, que recientemente han sufrido brechas de seguridad. Estos no son los únicos casos, ya que otras compañías de los mismos sectores también han sido objeto de ciberataques recientemente.

¿Cómo protegerse?

✅ Actualiza las contraseñas de forma periódica y utiliza un gestor de contraseñas para facilitar su gestión y almacenamiento seguro.
✅ Revisa que la autenticación multifactor (MFA) esté activada en todas tus cuentas.
✅ Revisa de forma periódica la actividad de tus cuentas de correo electrónico, plataformas digitales y entidades bancarias para detectar accesos no autorizados.

Link: https://bitlifemedia.com/2025/07/betfair-louis-vuitton-ciberataques/

Millones de DNI españoles filtrados y vendidos en la dark web

Resumen: Investigadores han reportado el posible robo de datos de millones de DNI españoles que se estarían vendiendo en la dark web. En las evidencias proporcionadas por el ciberdelincuente, se ven imágenes que incluyen el nombre, foto, dirección, firma, fecha de nacimiento e incluso la identidad de los progenitores. Sin embargo, las autoridades oficiales no han confirmado esta posible brecha de seguridad.

¿Cómo protegerse?

✅ Actualiza las contraseñas de forma periódica y utiliza un gestor de contraseñas para facilitar su gestión y almacenamiento seguro.
✅ Revisa que la autenticación multifactor (MFA) esté activada en todas tus cuentas.
✅ Revisa de forma periódica la actividad de tus cuentas de correo electrónico, plataformas digitales y entidades bancarias para detectar accesos no autorizados.

Link: https://www.hardwarepremium.com/noticias/23960/dni-espanoles-dark-web-venta/

CVEs

Actualizaciones de seguridad de Android de agosto de 2025

Resumen: Google ha publicado un conjunto de actualizaciones de seguridad para solucionar un total de 6 vulnerabilidades (con CVE asignado), clasificadas 2 como críticas y 4 como altas. Estas vulnerabilidades podrían permitir la ejecución remota en combinación con otros errores y sin necesidad de privilegios de ejecución adicionales.
Gravedad: 🔥 Crítica – Afecta a una gran cantidad de usuarios y empresas.
Ejemplo real: Usuarios que utilizan dispositivos Android.

✅ **Solución:** Asegurarse que el software de los dispositivos Android está actualizado a la última versión.

Link: https://www.incibe.es/incibe-cert/alerta-temprana/avisos/boletin-de-seguridad-de-android-agosto-de-2025

Vulnerabilidad 0day en WinRAR

Resumen: La firma de seguridad ESET ha publicado una nueva vulnerabilidad descubierta en WinRAR. Se tarta de la segunda vulnerabilidad reportada recientemente con una alta criticidad que permite la ejecución de código mediante la creación de archivos comprimidos maliciosos. La vulnerabilidad está siendo explotada activamente y diversos atacantes la han incluido ya como parte de su modus operandi.
Gravedad: 🔥 Alta (8.4/10) – Riesgo para usuarios que utilizan el software WinRAR.
Ejemplo real: Usuarios que tienen el software WinRAR en sus sistemas.

✅ **Solución:** Actualizar WinRAR para corregir las vulnerabilidades identificadas.

Link: https://www.muycomputer.com/2025/08/11/si-usas-winrar-debes-actualizar-de-inmediato/

Ejecución remota de código en SharePoint Server de Microsoft

Resumen: Microsoft ha publicado actualizaciones de seguridad sobre una vulnerabilidad crítica que podría permitir el acceso a los atacantes mediante la ejecución remota de código. Esta vulnerabilidad está siendo activamente explotada y ya se conocen algunas víctimas, aunque cabe destacar que no afecta a sus soluciones en la nube.
Gravedad: 🔥 Crítica (9.8/10) – Riesgo para usuarios de SharePoint on-premise.
Ejemplo real: Entornos que cuenten con SharePoint Server (entornos on-premise).

✅ **Solución:** Actualizar los servidores de SharePoint a las últimas versiones disponibles.

Link: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos/ejecucion-remota-de-codigo-en-sharepoint-server-de-microsoft