Mes: Diciembre 2025

Resumen mensual

Malware

ToddyCat usa nuevo malware para vulnerar Outlook y Microsoft 365

Resumen: Nuevas herramientas usadas por el actor de amenaza ToddyCat han sido reveladas recientemente por investigadores, con nuevas capacidades que permiten el robo información de correos electrónicos, cookies y credenciales almacenadas en navegadores, y tokens de acceso utilizados por aplicaciones de Microsoft 365.

¿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://bitlifemedia.com/2025/11/el-grupo-toddycat-usa-nuevo-malware-para-vulnerar-outlook-y-microsoft-365/

Sturnus: el troyano bancario para Android que espía chats y toma el control

Resumen: Investigadores han descubierto un nuevo programa malicioso de Android llamado Sturnus, diseñado para ser capaz de leer conversaciones en aplicaciones cifradas como WhatsApp, Telegram o Signal sin necesidad de romper su criptografía. Usando permisos de accesibilidad, el troyano es capaz de acceder a la información de las aplicaciones, pudiendo leer también pulsaciones de teclas y realizar acceso remoto.

¿Cómo protegerse?

- ✅ Evita instalar aplicaciones desde sitios web no verificados.
- ✅ 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://tabletzona.es/sturnus-el-troyano-bancario-para-android-que-espia-chats-y-toma-el-control/

SmartTube, la alternativa de YouTube en la TV, distribuyó 'malware' de forma accidental en sus últimas versiones

Resumen: La aplicación de televisión SmartTube, que ofrece una alternativa a YouTube para ver videos, ha distribuido durante el último mes varias versiones infectadas con un programa malicioso. El responsable del proyecto ha comunicado que el equipo que usa para crear los archivos APK había sido comprometido, y que su firma digital había sido expuesta, recomendando a los usuarios de la aplicación que descarguen versiones nuevas para evitar posibles ataques.

¿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.europapress.es/portaltic/ciberseguridad/noticia-alternativa-youtube-tv-smarttube-distribuyo-malware-forma-accidental-ultimas-versiones-20251201160259.html

Phishing

Nueva estafa de phishing ClickFix usando la imagen de Google Meet

Resumen: Una nueva variante de ataque de phishing de tipo ClickFix se está propagando mediante correos electrónicos fraudulentos, bajo la inofensiva apariencia de una invitación a Google Meet. Al acceder a la página maliciosa, aparece un mensaje indicando de varias acciones que el invitado debe realizar para solucionar un error. Sin embargo, en su lugar, la ejecución de estos comandos lleva al compromiso del usuario.

¿Cómo protegerse?

- ✅ No ejecutes combinaciones de teclas o comandos solicitados por páginas web.
- ✅ No accedas a enlaces provenientes de orígenes desconocidos.
- ✅ Comprueba la autenticidad de las páginas web a las que accedas.

Link: https://www.redeszone.net/noticias/seguridad/cuidado-google-meet-estafa-tecnica-robar/

"Vota por mi hijo": la nueva estafa de la que advierte la Policía Nacional

Resumen: La Policía Nacional alerta de una nueva estafa mediante comunicaciones de WhatsApp, donde las victimas reciben mensajes de contactos conocidos, como amigos y familiares. En estos mensajes se solicita ayuda con una votación para que el hijo del remitente gane un concurso. El enlace redirige a una web que solicita un número de contacto, así como un código de 6 dígitos. Esa clave de seis cifras es, en realidad, el código de verificación de WhatsApp. Al proporcionarlo, los estafadores toman el control total de su cuenta, suplantan su identidad y propagan el engaño automáticamente entre todos sus contactos.

¿Cómo protegerse?

- ✅ Activa autenticación de doble factor en tus cuentas y no compartas los códigos 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://www.lasexta.com/tecnologia-tecnoxplora/internet/vota-hijo-asi-nueva-estafa-que-advierte-policia-nacional_20251118691c598c360d0840bce694bf.html

Una 'fábrica de estafas' envía dos millones de SMS al día para robar datos bancarios en España

Resumen: La Guardia Civil de Alicante ha desmantelado una operación en España con una gran infraestructura que se usaba para el envío masivo de mensajes y llamadas fraudulentas. Los atacantes suplantaban la identidad de la Policía Nacional o el Banco de España para presionar a sus víctimas y solicitarles información personal y bancaria. Los investigadores indican que previamente estudiaban los perfiles de las potenciales víctimas y las comunicaciones iban dirigidas hacia colectivos concretos.

¿Cómo protegerse?

- ✅ Evita acceder a enlaces sospechosos recibidos por SMS.
- ✅ No realices transacciones bancarias sin verificar la legitimidad de su origen.
- ✅ Nunca des datos personales o bancarios por teléfono ni en páginas no verificadas.

Link: https://www.abc.es/espana/comunidad-valenciana/fabrica-estafas-envia-dos-millones-sms-dia-20251128113906-vi.html

Brechas de seguridad

Iberia sufre una brecha de seguridad que afecta a datos personales de sus clientes

Resumen: Uno de los proveedores externos de la aerolínea Iberia ha sufrido un incidente de seguridad, obligando a la empresa a notificar la posible filtración de datos personales de varios de sus usuarios. Entre estos datos se podrían incluir nombres, apellidos, direcciones de correo electrónico o teléfonos. La compañía indica que datos bancarios o contraseñas de acceso no se encuentran entre los datos filtrados.

¿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://noticiasciudadanas.com/iberia-brecha-seguridad-datos-clientes/

La Policía Nacional detiene a un ciberdelincuente por sustraer y vender unos 64 millones de datos personales privados

Resumen: La Policía Nacional ha detenido en Igualada (Barcelona) a un joven de 19 años acusado de robar y vender millones de datos personales de nueve empresas. El sospechoso habría obtenido información como DNI, direcciones, teléfonos e incluso datos bancarios. Según los agentes, el perpetrador vendía estos datos posteriormente en foros clandestinos usando varias cuentas y seudónimos. La investigación comenzó en junio y permitió localizarlo tras rastrear su actividad en la red.

¿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.policia.es/_es/comunicacion_prensa_detalle.php?ID=16737

La empresa española de RR.HH. Marlex sufre una brecha de seguridad durante un ataque de ransomware

Resumen: La empresa de gestión de talento Marlex ha sido víctima de un ciberataque llevado a cabo por el grupo de ransomware Rhysida. Los actores de amenaza avisan a la empresa de la filtración inminente de la información obtenida durante el ataque si no reciben el pago que solicitan, que alcanza aproximadamente 1 millón de euros. Aunque se desconoce la información exfiltrada, podría implicar que afecte potencialmente a decenas miles de personas involucradas con la empresa.

¿Cómo protegerse?

✅ Limita la información personal que puedas dar a 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/marlex-rrhh-ataque-ransomware.html

CVEs

Actualizaciones de seguridad de Microsoft de diciembre de 2025

Resumen: Microsoft ha publicado sus actualizaciones de seguridad correspondientes a diciembre de 2025, corrigiendo 57 vulnerabilidades que afectan a Windows, Microsoft Office, Azure y otros productos de la compañía. Entre los fallos solucionados se incluyen varias vulnerabilidades críticas que permiten elevación de privilegios y ejecución remota de código, una de ellas explotada activamente.
Gravedad: 🔥 Alta (8.8/10) – 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/incibe-cert/alerta-temprana/avisos/actualizaciones-de-seguridad-de-microsoft-de-diciembre-de-2025

Múltiples vulnerabilidades en productos de VMware

Resumen: Fortinet ha corregido múltiples vulnerabilidades críticas que permitían a un atacante no autenticado eludir la autenticación del inicio de sesión SSO (Single Sign-On) mediante mensajes manipulados. Estos problemas afectaban a versiones de FortiOS, FortiWeb, FortiProxy y FortiSwitchManager siempre que la función SSO estuviera habilitada.
Gravedad: 🔥 Crítica (9.8/10) – Riesgo para los usuarios que tengan su red gestionada con productos de Fortinet.
Ejemplo real: Usuarios que utilicen productos de Fortinet.

✅ **Solución:** Actualizar de manera urgente a las últimas versiones o desactivar temporalmente la función SSO para mitigar los riesgos de posible explotación.

Link: https://www.incibe.es/incibe-cert/alerta-temprana/avisos/omision-de-autenticacion-en-el-inicio-de-sesion-sso-en-productos-de-fortinet

Actualización de seguridad de Android de diciembre de 2025

Resumen: Google ha publicado su boletín mensual de actualizaciones para dispositivos Android, solucionando múltiples vulnerabilidades en funcionalidades del sistema operativo, así como varios errores críticos en el kernel. Estas vulnerabilidades de ser explotadas podrían potencialmente permitir a atacantes realizar una denegación remota de servicio o escalada de privilegios.
Gravedad: 🔥 Crítica (10/10) – 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/multiples-vulnerabilidades-en-el-kernel-de-android