Mes: Febrero 2026

Resumen mensual

Malware

OpenClaw abre la puerta a un arsenal de malware para robar contraseñas

Resumen: OpenClaw, también conocido como MoltClaw o ClawdBot, es un programa de IA para equipos personales que ha ganado una gran popularidad recientemente debido a su utilidad como asistente personal. Sin embargo, apenas unos días después de su salida al público ya han aparecido múltiples complementos fraudulentos que realizan actividades maliciosas, buscando robar información de sus usuarios.

¿Cómo protegerse?

- ✅ Limita el acceso de tecnologías instaladas a tu información personal.
- ✅ Evita guardar contraseñas en el dispositivo, usa un gestor de contraseñas.
- ✅ Usa un antivirus y mantén tus dispositivos actualizados.

Link: https://computerhoy.20minutos.es/ciberseguridad/fiebre-por-clawdbot-ahora-openclaw-abre-puerta-un-arsenal-malware-robacontrasenas_6929111_0.html

Regresa el troyano Grandoreiro con una campaña que suplanta a Endesa y distribuye malware bancario

Resumen: Grandoreiro, un programa malicioso usado anteriormente en ataques de ingeniería social ha resurgido en una nueva campaña de phishing donde los atacantes suplantan a Endesa. A través de mensajes que alertan de un supuesto error en datos personales o de pago, se adjunta un archivo que, al abrirse, descarga e instala el troyano en el equipo de la víctima, recopilando datos financieros en segundo plano.

¿Cómo protegerse?

- ✅ No abras enlaces o archivos recibidos de fuentes desconocidas.
- ✅ Instala un antivirus con análisis en tiempo real en tu ordenador.
- ✅ Usa autenticación multifactor (2FA) para evitar accesos a tus cuentas.

Link: https://www.ultimahora.es/noticias/tecnologia-videojuegos/2026/02/13/2569809/regresa-troyano-grandoreiro-una-campana-suplanta-endesa-distribuye-malware-bancario.html

El malware de robo de información LummaStealer vuelve a operar a gran escala tras su desmantelamiento

Resumen: Tras su caída durante una operación internacional que consiguió desmantelar su infraestructura operativa, han vuelto a detectarse casos del programa malicioso LummaStealer, dedicado al robo de información. Esto sugiere el regreso del actor de amenaza, lo que supondría un riesgo para la actividad empresarial.

¿Cómo protegerse?

- ✅ Evita guardar información sensible en tu navegador para impedir su extracción.
- ✅ No descargues aplicaciones desde fuentes no oficiales.
- ✅ No concedas accesos innecesarios a tus datos ni a las funciones del dispositivo.

Link: https://www.infobae.com/america/agencias/2026/02/12/lummastealer-resurge-tras-su-desmantelamiento-el-malware-de-robo-de-informacion-vuelve-a-operar-a-gran-escala/

Phishing

La Guardia Civil alerta de una campaña de 'phishing' con notificaciones falsas de Hacienda

Resumen: La Guardia Civil y el Instituto Nacional de Ciberseguridad (INCIBE) advierten de una campaña masiva de suplantación de identidad. Su objetivo es incitar a las víctimas a clicar en un correo que suplanta la apariencia de la Agencia Tributaria para obtener credenciales de acceso, lo que les permitiría acceder a datos sensibles como los encontrados en la declaración de la Renta de los ciudadanos afectados.

¿Cómo protegerse?

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

Link: https://www.abc.es/tecnologia/guardia-civil-alerta-campana-phishing-notificaciones-falsas-20260204120919-nt.html

Piden varios años de cárcel para seis acusados de estafar 343.608 euros a una empresa usando phishing

Resumen: Seis detenidos acusados de haber realizado un ataque de phishing, se enfrentan a hasta 5 años de cárcel tras estafar miles de euros. Los fondos sustraídos por los atacantes fueron enviados a una entidad bancaria en Rumanía después de pasar por varias cuentas, dificultando su trazabilidad. La investigación permitió identificar como destino final una cuenta de una empresa ubicada en Pontevedra, aparentemente dedicada a obras y servicios, pero sin ninguna actividad real.

¿Cómo protegerse?

- ✅ Confirma por múltiples vías la autenticidad de actividades de carácter financiero.
- ✅ Evita acceder a enlaces sospechosos recibidos mediante comunicaciones.
- ✅ Si dudas del remitente, contacta con él mediante otros canales.

Link: https://www.infobae.com/espana/agencias/2026/02/01/piden-5-anos-de-carcel-para-cinco-acusados-de-estafar-343608-euros-a-una-empresa-usando-el-metodo-phishing/

Phishing en Huesca provoca que 5 personas pierdan hasta 71 mil euros

Resumen: La Policía Nacional avisa de un fraude activo en el que, mediante el uso de técnicas de suplantación, se ha conseguido estafar a 5 personas una cantidad que se aproxima a 71 mil euros. Mediante el uso de mensajes SMS fraudulentos, una técnica conocida como “smishing”, los atacantes se hacen pasar por bancos y añaden enlaces que llevan a páginas web bajo su control. Al introducir sus credenciales en estas webs, las victimas dan acceso a sus cuentas bancarias sin ser conscientes de ello.

¿Cómo protegerse?

- ✅ Usa siempre enlaces oficiales para acceder a páginas web importantes.
- ✅ No confíes en comunicaciones provenientes de SMS, especialmente de bancos.
- ✅ Nunca des datos personales o bancarios por teléfono ni a través de páginas web no verificadas.

Link: https://www.larazon.es/aragon/nueva-estafa-phishing-huesca-provoca-que-5-personas-pierdan-71-mil-euros-b30m_202602156991df801817b41eb6498250.html

Brechas de seguridad

Los 'hackers' que atacaron la red del Ayuntamiento de Beniel filtran datos sensibles

Resumen: El Ayuntamiento de Beniel, un municipio de Murcia, ha sufrido un ciberataque recientemente, donde los atacantes consiguieron obtener información sensible que podría afectar a los habitantes del municipio. En la información exfiltrada se incluyen datos como nombre y apellidos, documento de identificación, domicilio, correo electrónico, teléfono, imagen, número de la Seguridad Social y tarjeta sanitaria entre muchos otros.

¿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.laverdad.es/murcia/otros-municipios/ayuntamiento-beniel-sufre-filtracion-datos-parte-hackers-20260201155837-nt_amp.html

Nike investiga una filtración masiva de datos compartida por los 'hackers' de World Leaks

Resumen: La empresa Nike ha informado sobre un posible ataque de ciberseguridad tras la supuesta filtración de 1,4 terabytes de datos atribuida al grupo de actores de amenaza WorldLeaks. Los atacantes no han revelado el tipo de información exfiltrada y han iniciado una cuenta atrás, amenazando con su publicación si no se cumple el pago exigido a la compañía.

¿Cómo protegerse?

✅ Verifica el origen de las comunicaciones que recibas: aunque incluyan información legítima, pueden proceder de ciberdelincuentes.
✅ No compartas información personal innecesaria al registrarte en servicios.
✅ Usa autenticación multifactor para evitar el robo de tus cuentas.

Link: https://www.lavanguardia.com/economia/20260128/11451647/nike-investiga-filtracion-masiva-datos-compartida-hackers-world-leaks.html

Flickr sufre una brecha de datos a través de un proveedor de email

Resumen: La compañía Flickr ha avisado de un incidente de seguridad que afectaría a varios usuarios de su plataforma. El suceso está relacionado con uno de sus proveedores de correo electrónico y habría expuesto datos como nombres, correos, direcciones IP, o ubicación, entre otros. Flickr ha confirmado que contraseñas o datos de pago no se habrían visto comprometidos durante el ataque.

¿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/flickr-sufre-brecha-datos-proveedor-email.html

CVEs

Actualizaciones de seguridad de Microsoft de febrero de 2026

Resumen: Microsoft ha liberado un paquete de actualizaciones para dar soporte a múltiples productos de la compañía, solucionando varias vulnerabilidades para Microsoft Windows, Office y Azure. De las 59 vulnerabilidades reportadas, 2 han sido calificadas como críticas, 43 como altas, 13 como medias y 1 como baja.
Gravedad: 🔥 Crítica (9.8/10) – 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-febrero-de-2026

Actualizaciones de seguridad de febrero de 2026 en productos de SAP

Resumen: SAP ha liberado un conjunto de actualizaciones para corregir vulnerabilidades presentes en varios de sus productos, incluyendo S4/HANA y NetWeaver. Algunas de las vulnerabilidades solucionadas con estos parches podrían permitir a un atacante ejecutar sentencias SQL arbitrarias y realizar llamadas a funciones remotas entre otras.
Gravedad: 🔥 Crítica (9.9/10) – Riesgo para usuarios que usen productos de SAP.
Ejemplo real: Usuarios que utilicen S4/HANA o NetWeaver.

✅ **Solución:** Actualizar de manera urgente el software a su última versión para evitar la explotación de estas vulnerabilidades.

Link: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos/actualizaciones-de-seguridad-de-febrero-de-2026-en-productos-de-sap

Vulnerabilidad de emisión de autenticación en telnetd

Resumen: Se ha descubierto un fallo crítico en la aplicación telnetd, usada comúnmente durante años en entornos corporativos con máquinas Linux. La vulnerabilidad, identificada como CVE-2026-24061, permitiría a potenciales atacantes acceder a servidores telnet evadiendo el proceso de autenticación y adquiriendo privilegios de root, lo que les daría control total sobre la máquina.
Gravedad: 🔥 Crítica (9.8/10) – Riesgo para usuarios que utilizan el servicio de telnet.
Ejemplo real: Empresas con servidores Linux con servicio telnetd desplegado.

✅ **Solución:** Actualizar la aplicación telnetd a la última versión.

Link:https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos/omision-de-autenticacion-en-telnetd