Mes: Julio 2026

Resumen mensual

Malware

Un nuevo malware para macOS emplea un ID de desarrollador legítimo

Resumen: Una nueva campaña de malware para macOS está utilizando certificados legítimos de desarrollador para hacerse pasar por el componente oficial Apple Crash Reporter. El objetivo es engañar a los usuarios para que instalen una carga maliciosa capaz de robar credenciales y otra información sensible.

¿Cómo protegerse?

- ✅ Verificar siempre la procedencia de cualquier aplicación antes de instalarla.
- ✅ Mantener macOS y las soluciones EDR actualizadas.
- ✅ Restringir la ejecución de software no autorizado mediante políticas corporativas.

Link: https://www.infosecurity-magazine.com/news/macos-malware-apple-crash-reporter/

Operation ShadowRecruit: Malware disfrazado de ofertas de empleo

Resumen: La campaña ShadowRecruit utiliza falsas oportunidades laborales para distribuir malware entre buscadores de empleo.Los atacantes emplean herramientas legítimas como Google Sheets y el framework ControlR para dificultar la detección. La campaña se ha centrado principalmente en usuarios de India, aunque la metodología puede replicarse globalmente.

¿Cómo protegerse?

- ✅ Desconfiar de procesos de selección que soliciten ejecutar archivos externos.
- ✅ Analizar documentos y enlaces recibidos durante procesos de contratación.
- ✅ Utilizar soluciones antimalware con capacidades de detección de comportamiento.

Link: https://blog.elhacker.net/2026/06/paquetes-npm-de-red-hat-comprometidos.html

148 paquetes NPM convertían navegadores en una botnet DDoS

Resumen: Investigadores descubrieron 148 paquetes maliciosos publicados en NPM que se presentaban como herramientas proxy para estudiantes. Al instalarse, transformaban los navegadores de los usuarios en nodos de una botnet destinada a lanzar ataques DDoS. La campaña demuestra los riesgos existentes en la cadena de suministro de software de código abierto.

¿Cómo protegerse?

- ✅ Validar la reputación y procedencia de las dependencias de software.
- ✅ Implementar herramientas de Software Composition Analysis (SCA).
- ✅ Restringir la instalación de paquetes no aprobados en entornos corporativos.

Link: https://thehackernews.com/2026/07/148-npm-packages-disguised-as-student.html

Phishing

Lidl advierte a sus clientes sobre campañas de phishing tras una brecha de terceros

Resumen: Lidl informó de un incidente en un proveedor tecnológico externo que pudo exponer información personal de clientes. Tras el incidente, la compañía alertó sobre posibles campañas de phishing que utilizan los datos comprometidos para aumentar su credibilidad.
Los atacantes podrían enviar correos electrónicos o mensajes simulando comunicaciones legítimas de Lidl.

¿Cómo protegerse?

✅ No abrir enlaces o adjuntos recibidos de mensajes inesperados.
✅ Confirmar las comunicaciones a través de los canales oficiales de Lidl.
✅ Activar autenticación multifactor en todas las cuentas posibles.

Link: https://www.infosecurity-magazine.com/news/lidl-notifies-customers-of/

ShadowRecruit utiliza señuelos de contratación para robar información

Resumen: Los atacantes emplean ofertas laborales falsas y documentos relacionados con procesos de selección para atraer a las víctimas.Las comunicaciones aparentan provenir de reclutadores legítimos y buscan generar confianza. Una vez ejecutados los archivos proporcionados, se despliega malware destinado al robo de información.

¿Cómo protegerse?

✅ Verificar la identidad de los reclutadores y empresas contactantes.
✅ No ejecutar archivos recibidos por correo sin validación previa.
✅ Formar a empleados y candidatos sobre tácticas de ingeniería social.

Link: https://www.seqrite.com/blog/operation-shadowrecruit-a-recruitment-themed-malware-campaign-leveraging-controlr-and-google-sheets-to-target-indian-job-seekers/

La herramienta DEBULL se aprovecha del flujo de código de dispositivos de Microsoft para atacar cuentas de M365

Resumen: Investigadores detectaron una campaña de phishing que abusa del mecanismo legítimo de autenticación Device Code Flow de Microsoft 365 para secuestrar cuentas corporativas. Los atacantes utilizan señuelos relacionados con colaboración empresarial y Microsoft Teams para convencer a las víctimas de introducir códigos de autenticación legítimos. Este método permite eludir técnicas tradicionales de phishing basadas en páginas falsas de inicio de sesión.

¿Cómo protegerse?

✅ Formar a los usuarios para que nunca introduzcan códigos de autenticación recibidos por correo o mensajería sin verificar su origen.
✅ Restringir o monitorizar el uso de Device Code Flow cuando no sea necesario para la organización.
✅ Implementar monitorización avanzada sobre eventos de autenticación y actividades anómalas en Microsoft 365.

Link: https://thehackernews.com/2026/07/debull-tooling-abuses-microsoft-device.html

Brechas de seguridad

Lidl Notifies Customers of Third-Party Data Breach

Resumen: Lidl notificó una filtración de datos relacionada con un proveedor tecnológico externo.
La información afectada podría incluir datos personales de clientes en varios países europeos.
La organización recomienda extremar la precaución frente a correos y mensajes fraudulentos relacionados con la marca.

¿Cómo protegerse?

- ✅ Cambiar contraseñas asociadas a cuentas afectadas.
- ✅ Monitorizar actividades sospechosas en cuentas personales.
- ✅ Desconfiar de comunicaciones que soliciten datos personales o financieros.

Link: https://www.infosecurity-magazine.com/news/lidl-notifies-customers-of/

Finlandia emite una orden de búsqueda contra el responsable de la brecha de Vastaamo

Resumen: Las autoridades finlandesas emitieron una orden de búsqueda internacional contra el presunto responsable del ataque a Vastaamo.
La brecha expuso información extremadamente sensible de pacientes de psicoterapia.
El caso continúa siendo uno de los incidentes de privacidad más graves registrados en Europa.

¿Cómo protegerse?

- ✅ Aplicar cifrado a datos especialmente sensibles.
- ✅ Segmentar y limitar el acceso a bases de datos críticas.
- ✅ Realizar auditorías y pruebas periódicas de seguridad.

Link: https://therecord.media/finland-issues-wanted-notice-for-hacker-vastaamo-breach

Microsoft identifica nuevas rutas de ataque vinculadas a ShinyHunters en Salesforce

Resumen: Microsoft documentó varias técnicas utilizadas por actores relacionados con ShinyHunters para comprometer entornos Salesforce.
Los atacantes aprovecharon configuraciones débiles y accesos comprometidos para acceder a información empresarial sensible.
La actividad observada estuvo relacionada con operaciones de extorsión y robo masivo de datos.

¿Cómo protegerse?

- ✅ Implementar autenticación multifactor en Salesforce.
- ✅ Revisar periódicamente permisos y cuentas privilegiadas.
- ✅ Monitorizar actividades anómalas mediante SIEM y herramientas CASB.

Link: https://thehackernews.com/2026/07/microsoft-maps-year-long-shinyhunters.html

CVEs

Microsoft SharePoint Server Missing Authentication for Critical Function (CVE-2026-56164)

Resumen: Vulnerabilidad de autenticación ausente en funciones críticas de SharePoint Server.
Permite que un atacante no autenticado eleve privilegios de forma remota.
Gravedad: 🔥 Crítica (9/10) – Riesgo muy elevado en plataformas de colaboración corporativa y entornos SharePoint expuestos a red.
Ejemplo real: Un atacante podría acceder a funcionalidades administrativas expuestas sin autenticación válida y obtener privilegios elevados en la plataforma.

✅ **Solución:** Aplicar inmediatamente las actualizaciones de seguridad publicadas por Microsoft, limitar la exposición de servidores SharePoint a Internet y revisar registros de acceso en busca de actividad sospechosa.

Link: https://msrc.microsoft.com/

Microsoft Active Directory Federation Services Insufficient Granularity of Access Control (CVE-2026-56155)

Resumen: Fallo de control de acceso insuficientemente granular en Active Directory Federation Services.
Permite a un usuario autorizado escalar privilegios localmente.
Gravedad: 🔥 Muy Alta (8/10) – Alto impacto en infraestructuras de identidad y acceso corporativo.
Ejemplo real: Un usuario con acceso limitado podría aprovechar permisos incorrectamente definidos para obtener privilegios administrativos.

✅ **Solución:** Instalar los parches de seguridad correspondientes, revisar delegaciones y grupos privilegiados y aplicar el principio de mínimo privilegio.

Link: https://msrc.microsoft.com/

SonicWall SMA1000 Code Injection Vulnerability (CVE-2026-15410)

Resumen: Vulnerabilidad de inyección de código en dispositivos SonicWall SMA1000.
Permite a un administrador autenticado ejecutar comandos arbitrarios sobre el sistema operativo.
Gravedad: 🔥 Muy Alta (8/10) – Riesgo elevado en entornos de acceso remoto seguro y redes corporativas.
Ejemplo real: Una cuenta administrativa comprometida podría utilizar el fallo para ejecutar scripts maliciosos y tomar el control completo del dispositivo.

✅ **Solución:** Actualizar a la versión corregida por SonicWall, restringir el acceso administrativo e implementar MFA para administradores.

Link: https://psirt.global.sonicwall.com/

SonicWall SMA1000 Server-Side Request Forgery (SSRF) (CVE-2026-15409)

Resumen: Vulnerabilidad SSRF que permite a atacantes remotos no autenticados provocar solicitudes desde el propio dispositivo.

Puede facilitar reconocimiento interno y acceso a recursos no expuestos externamente.
Gravedad: 🔥 Alta (7/10) – Riesgo significativo en infraestructuras híbridas, cloud y entornos segmentados.
Ejemplo real: Un atacante podría utilizar el dispositivo para interactuar con servicios internos inaccesibles desde Internet.

✅ **Solución:** Aplicar los parches publicados por SonicWall, filtrar y restringir conexiones salientes y monitorizar patrones anómalos de tráfico.

Link: https://psirt.global.sonicwall.com/

Cisco IOS Cross-Site Request Forgery Vulnerability (SSRF) (CVE-2008-4128)

Resumen: Antigua vulnerabilidad CSRF presente en determinadas versiones de Cisco IOS con interfaz web habilitada.
Puede permitir la ejecución de comandos administrativos mediante solicitudes forjadas.
Gravedad: 🔥 Media (6/10) – Impacto moderado en sistemas de comunicaciones empresariales y dispositivos de red administrados mediante interfaz web.
Ejemplo real: Un administrador autenticado podría visitar una página maliciosa que enviase comandos al dispositivo de red sin su conocimiento.

✅ **Solución:** Actualizar a versiones soportadas de Cisco IOS, deshabilitar interfaces web innecesarias y restringir el acceso administrativo mediante listas de control de acceso.

Link: https://sec.cloudapps.cisco.com/security/center/#!/home