Mes: Septiembre 2026

Resumen mensual

Malware

CLOSEDQUORUM, el malware que utiliza IA para decidir sus ataques

Resumen: CLOSEDQUORUM es capaz de consultar varios modelos de IA para decidir automáticamente sus acciones. Puede robar credenciales, contraseñas almacenadas y datos de monederos de criptomonedas. Se trata de uno de los primeros casos documentados de malware que delega parte de sus decisiones de mando y control en servicios de IA.

¿Cómo protegerse?

- ✅ Mantener actualizadas las soluciones EDR y antivirus.
- ✅ Supervisar conexiones salientes hacia servicios de IA y Discord.
- ✅ Aplicar el principio de mínimo privilegio en los equipos.

Link: https://thehackernews.com/2026/09/windows-malware-is-built-to-let-up-to.html

CLEANGULP, el malware desplegado mediante una cadena de exploits Chrome y Windows

Resumen: Un grupo de amenazas chino fue observado explotando múltiples vulnerabilidades de día cero en Chrome y Windows para desplegar CLEANGULP. La amenaza proporciona capacidades de ejecución remota de comandos, descarga de archivos y persistencia en los sistemas comprometidos.

¿Cómo protegerse?

- ✅ Actualizar inmediatamente navegadores y sistemas Windows.
- ✅ Restringir la navegación hacia sitios no confiables.
- ✅ Monitorizar procesos y conexiones sospechosas en endpoints.

Link: https://thehackernews.com/2026/09/chinese-hackers-exploit-chrome-windows.html

KREMLIN, el malware bancario para secuestrar sesiones de los usuarios

Resumen: KREMLIN es un nuevo malware bancario que utiliza extensiones maliciosas en Google Chrome y Microsoft Edge para robar credenciales, cookies y tokens de sesión. Aunque inicialmente se ha observado en Brasil, sus técnicas podrían extenderse rápidamente a otros mercados, incluidos Europa y España.

¿Cómo protegerse?

- ✅ Revisar periódicamente las extensiones instaladas en los navegadores.
- ✅ Descargar software únicamente desde fuentes oficiales.
- ✅ Activar la autenticación multifactor en servicios bancarios y corporativos.

Link: https://csirtasobancaria.com/alertas-de-seguridad/kremlin-malware-bancario-explota-chrome-y-edge-para-secuestrar-sesiones-de-los-usuarios

Phishing

Campaña de phishing utiliza caracteres Unicode invisibles para evadir filtros

Resumen: Microsoft detectó una campaña masiva de phishing que emplea caracteres Unicode invisibles para dificultar la detección por parte de filtros de correo electrónico. Los atacantes fragmentan palabras clave financieras para evitar sistemas de seguridad tradicionales. La campaña llegó a distribuir millones de mensajes dirigidos a organizaciones y empresas.

¿Cómo protegerse?

- ✅ Implementar soluciones avanzadas de filtrado de correo.
- ✅ Revisar el contenido de mensajes sospechosos antes de interactuar.
- ✅ Formar a los usuarios sobre nuevas técnicas de evasión.

Link: https://thehackernews.com/2026/09/phishing-campaign-sends-millions-of.html

Spring Ring: ataques de vishing mediante Microsoft Teams

Resumen: La campaña Spring Ring utilizó cuentas externas de Microsoft Teams para hacerse pasar por personal de soporte técnico. Los atacantes persuadían a los usuarios para ejecutar herramientas de acceso remoto o malware. Algunas intrusiones evolucionaron hacia ataques de relay NTLM contra controladores de dominio.

¿Cómo protegerse?

- ✅ Verificar la identidad del personal de soporte antes de actuar.
- ✅ Restringir las comunicaciones externas en Teams cuando sea posible.
- ✅ Bloquear el uso de herramientas remotas no autorizadas.

Link: https://thehackernews.com/2026/09/threatsday-ceo-phishing-kits-5k-dropbox.html

Ataques de phishing orientados al robo de cuentas Microsoft mediante passkeys

Resumen: Microsoft ha alertado sobre campañas que combinan ingeniería social, SMS y sitios falsos para secuestrar cuentas protegidas mediante passkeys. Los atacantes contactan previamente a las víctimas simulando ser personal de TI y utilizan información obtenida en redes sociales para aumentar la credibilidad del engaño.

¿Cómo protegerse?

- ✅ Confirmar cualquier solicitud de soporte mediante canales oficiales.
- ✅ No seguir enlaces recibidos por SMS o mensajería instantánea.
- ✅ Aplicar políticas de acceso condicional y MFA resistente al phishing.

Link: https://cisoseries.com/cybersecurity-news-september-14-2026/

Brechas de seguridad

ShinyHunters afirma haber comprometido sistemas del FBI

Resumen: El grupo de extorsión ShinyHunters aseguró haber accedido a información de empleados actuales y antiguos del FBI. Aunque la investigación continúa, el incidente vuelve a poner de manifiesto el interés de los grupos criminales por organizaciones gubernamentales de alto perfil.

¿Cómo protegerse?

- ✅ Aplicar segmentación de redes y controles de acceso.
- ✅ Revisar continuamente privilegios administrativos.
- ✅ Monitorizar actividades sospechosas y movimientos laterales.

Link: https://www.cybersecurity-review.com/category/news-september-2026/

Brecha en Mathspace afecta a más de un millón de usuarios

Resumen: La plataforma educativa Mathspace confirmó una brecha que impactó a más de un millón de estudiantes, profesores y familiares. Los atacantes accedieron a un sistema interno de análisis y generación de informes.

¿Cómo protegerse?

- ✅ Cambiar contraseñas asociadas a servicios afectados.
- ✅ Vigilar intentos de fraude o suplantación derivados de la filtración.
- ✅ Activar MFA cuando esté disponible.

Link: https://www.bleepingcomputer.com/news/security/mathspace-discloses-data-breach-affecting-over-1-million-people/

Exposición de 220 millones de registros de viajeros en una base APIS

Resumen: Investigadores descubrieron una exposición masiva de datos en una base Advance Passenger Information System (APIS). La información incluía datos de pasajeros y tripulaciones recopilados durante años por sistemas de transporte aéreo. El incidente estuvo relacionado con múltiples errores de configuración de seguridad.

¿Cómo protegerse?

- ✅ Aplicar revisiones periódicas de configuraciones cloud.
- ✅ Limitar el acceso a bases de datos críticas.
- ✅ Implementar cifrado para la información sensible almacenada.

Link: https://www.privacyguides.org/news/2026/09/11/data-breach-roundup-sep-4-10-2026/

CVEs

Microsoft SharePoint Remote Code Execution (CVE-2026- 65660)

Resumen: Vulnerabilidad de ejecución remota de código en Microsoft SharePoint que está siendo explotada activamente. Permite a usuarios autenticados con pocos privilegios ejecutar código arbitrario sobre el servidor.

Gravedad: 🔥 Crítica (9/10) – Riesgo crítico en plataformas de colaboración empresarial y gestión documental, pudiendo facilitar la toma de control de servidores SharePoint corporativos.
Ejemplo real: CISA incorporó la vulnerabilidad a su catálogo KEV tras detectar explotación activa y el despliegue de webshells.

✅ **Solución:** Microsoft ha publicado actualizaciones de seguridad para corregir el fallo. Se recomienda aplicar inmediatamente los parches, revisar los servidores expuestos a Internet y analizar posibles indicadores de compromiso previos a la actualización.

Link: https://www.securityweek.com/microsoft-sharepoint-flaw-cve-2026-65660-now-exploited-in-attacks/

Check Point VPN Certificate Validation Bypass (CVE-2026- 85102)

Resumen: Vulnerabilidad crítica en dispositivos Check Point que permite ejecución remota de código sin autenticación durante la negociación VPN. La explotación activa comenzó pocos días después de la publicación de los parches.

Gravedad: 🔥 Crítica (9.8/10) – Alto impacto en infraestructuras VPN y accesos remotos corporativos, pudiendo comprometer completamente dispositivos perimetrales.
Ejemplo real: Se observaron accesos VPN no autorizados y actividades de reconocimiento LDAP en organizaciones afectadas.

✅ **Solución:** Check Point publicó actualizaciones el mismo día de la divulgación. Las organizaciones deben aplicar los parches de forma prioritaria, revisar conexiones VPN sospechosas y validar la integridad de las configuraciones de seguridad.

Link: https://forkast.news/the-vpn-certificate-bypass-that-was-patched-in-september-is-now-actively-exploited-federal-deadline-hits-sep-25/

Roundcube SQL Injection (CVE-2026- 48842)

Resumen: Vulnerabilidad de inyección SQL en Roundcube Webmail que permite comprometer bases de datos sin necesidad de autenticación previa. La explotación activa fue confirmada durante septiembre.

Gravedad: 🔥 Alta (8.1/10) – Elevado riesgo en plataformas de correo electrónico corporativo expuestas a Internet, con posible acceso a mensajes y credenciales.
Ejemplo real: Las autoridades canadienses confirmaron explotación activa sobre servidores Roundcube sin parchear.

✅ **Solución:** Se recomienda actualizar Roundcube, revisar la configuración del plugin afectado y analizar registros para detectar consultas o accesos anómalos.

Link: https://securityaffairs.com/199882/security/roundcube-sql-injection-cve-2026-48842-is-now-being-exploited-in-the-wild.html

Windows Update Stack Elevation of Privilege (CVE-2026- 81963)

Resumen: Vulnerabilidad de elevación de privilegios en Windows Update Stack que ya está siendo utilizada en ataques reales. Permite a un atacante local obtener privilegios SYSTEM.

Gravedad: 🔥 Alta (7.8/10) – Riesgo elevado en estaciones de trabajo y servidores Windows al facilitar la obtención de privilegios máximos sobre el sistema.
Ejemplo real: Microsoft confirmó explotación activa y la inclusión de la vulnerabilidad en el catálogo KEV de CISA.

✅ **Solución:** Las actualizaciones de septiembre de Microsoft corrigen este problema. Es recomendable desplegar los parches con prioridad alta y monitorizar intentos de escalada de privilegios en los equipos corporativos.

Link: https://www.bleepingcomputer.com/news/microsoft/microsoft-september-2026-patch-tuesday-fixes-966-flaws-2-zero-days/

Windows ALPC Elevation of Privilege (CVE-2026- 85880)

Resumen: Fallo de elevación de privilegios en Windows Advanced Local Procedure Call (ALPC) explotado activamente antes de la publicación de los parches. Permite a atacantes locales obtener privilegios SYSTEM.

Gravedad: 🔥 Alta (7.8/10) – Impacto elevado en entornos Windows corporativos al facilitar movimientos posteriores tras una primera intrusión.
Ejemplo real: Fue una de las dos vulnerabilidades de día cero corregidas durante el Patch Tuesday de septiembre.

✅ **Solución:** Microsoft ha distribuido correcciones dentro de las actualizaciones de septiembre de 2026. Se recomienda acelerar el despliegue de los parches y supervisar comportamientos sospechosos relacionados con elevación de privilegios.

Link: https://www.bleepingcomputer.com/news/microsoft/microsoft-september-2026-patch-tuesday-fixes-966-flaws-2-zero-days/