Mes: Agosto 2026

Resumen mensual

Malware

800 paquetes maliciosos de npm roban información mediante un RAT

Resumen: Investigadores identificaron cerca de 800 paquetes maliciosos publicados en npm como parte de una campaña de cadena de suministro. Los paquetes descargaban un malware capaz de funcionar en Windows, Linux y macOS e incluían capacidades de acceso remoto y robo de información. La campaña demuestra el creciente riesgo asociado al uso de dependencias de terceros en entornos de desarrollo.

¿Cómo protegerse?

- ✅ Auditar periódicamente las dependencias de software.
- ✅ Utilizar herramientas de Software Composition Analysis (SCA).
- ✅ Limitar la instalación de paquetes no verificados.

Link: https://thehackernews.com/2026/08/nearly-800-malicious-npm-packages.html

WindRelay para Android convierte móviles en repetidores NFC

Resumen: Una nueva familia de malware para Android llamada WindRelay convierte los teléfonos infectados en intermediarios NFC para realizar fraude con pagos contactless. La amenaza trabaja junto al conocido RAT SpyNote y permite retransmitir datos de tarjetas bancarias en tiempo real. Los ataques comienzan mediante campañas de ingeniería social y falsas verificaciones bancarias.

¿Cómo protegerse?

- ✅ Evitar instalar APKs fuera de tiendas oficiales.
- ✅ Revisar permisos de accesibilidad concedidos a aplicaciones.
- ✅ Utilizar soluciones de seguridad móvil corporativas.

Link: https://thehackernews.com/2026/08/windrelay-android-malware-turns-victims.html

Gusano ligado a Keyv compromete cientos de paquetes npm

Resumen: Un gusano asociado a paquetes comprometidos del ecosistema Keyv logró propagarse a cientos de paquetes npm. El malware robaba credenciales de repositorios, servicios cloud, registros npm y entornos CI/CD. Los investigadores recomiendan considerar comprometidas las credenciales de cualquier sistema afectado.

¿Cómo protegerse?

- ✅ Rotar credenciales potencialmente expuestas.
- ✅ Revisar pipelines CI/CD para detectar actividad anómala.
- ✅ Implementar firmas y validación de paquetes.

Link: https://thehackernews.com/2026/08/keyv-linked-npm-worm-poisons-hundreds.html

Phishing

Phishing AitM en Microsoft 365 secuestra cuentas para robar correos financieros

Resumen: Una campaña masiva de phishing dirigida a Microsoft 365 utiliza técnicas Adversary-in-the-Middle (AitM) para capturar credenciales y códigos MFA. Los atacantes emplean servicios legítimos como Google, Google Meet y Amazon S3 para ocultar la infraestructura de ataque. El objetivo principal es el acceso a cuentas relacionadas con nóminas y áreas financieras

¿Cómo protegerse?

- ✅ Implantar autenticación resistente al phishing (FIDO2).
- ✅ Supervisar accesos desde ubicaciones y dispositivos inusuales.
- ✅ Formar a los usuarios sobre ataques AitM.

Link: https://thehackernews.com/2026/08/microsoft-365-aitm-phishing-hijacks.html

UNC6671 usa vishing para robar datos SaaS a través de móviles personales

Resumen: El grupo UNC6671 está utilizando campañas de vishing haciéndose pasar por personal de soporte técnico corporativo. Los atacantes contactan a empleados en sus teléfonos personales y los redirigen a portales falsos para capturar credenciales y sesiones. Posteriormente exfiltran datos de Microsoft 365, Okta y otras plataformas SaaS.

¿Cómo protegerse?

- ✅ Verificar cualquier solicitud de soporte mediante canales oficiales.
- ✅ No introducir credenciales tras recibir llamadas no solicitadas.
- ✅ Aplicar MFA y monitorización de accesos a SaaS.

Link: https://thehackernews.com/2026/08/unc6671-vishing-attacks-target-personal.html

Campañas Evilginx continúan burlando la MFA en Microsoft 365

Resumen: Diversas campañas basadas en Evilginx siguen permitiendo el secuestro de sesiones de Microsoft 365 mediante técnicas AitM. Los atacantes capturan tokens válidos de autenticación y mantienen acceso persistente a las cuentas comprometidas. Las organizaciones siguen siendo objetivo prioritario.

¿Cómo protegerse?

- ✅ Adoptar autenticación basada en claves FIDO2.
- ✅ Revisar sesiones activas sospechosas.
- ✅ Habilitar políticas de acceso condicional.

Link: https://thehackernews.com/2026/08/microsoft-365-aitm-phishing-hijacks.html

Brechas de seguridad

Brecha en PNLD expone contactos de la policía y organismos públicos del Reino Unido

Resumen: Police National Legal Database (PNLD) confirmó una brecha que expuso información de contacto de policías, organismos gubernamentales y profesionales del sector judicial. Los datos comprometidos aparecieron publicados en la dark web. Aunque no se han reportado credenciales afectadas, la información expuesta podría utilizarse en campañas dirigidas de phishing

¿Cómo protegerse?

- ✅ Incrementar la vigilancia frente a correos dirigidos.
- ✅ Revisar accesos a portales públicos y bases de datos.
- ✅ Aplicar segmentación y controles de exposición de datos.

Link: https://thehackernews.com/2026/08/pnld-breach-exposes-uk-police-and.html

Brecha en ShipMonk expone datos de clientes de Trezor

Resumen: La empresa logística ShipMonk sufrió una brecha que expuso nombres, direcciones, teléfonos y correos electrónicos de clientes asociados a envíos de Trezor. El incidente afecta a usuarios de varios países y aumenta el riesgo de ataques dirigidos y fraudes personalizados

¿Cómo protegerse?

- ✅ Desconfiar de correos relacionados con pedidos o criptomonedas.
- ✅ Verificar cualquier solicitud de información personal.
- ✅ Activar MFA en todas las cuentas asociadas.

Link: https://thehackernews.com/2026/08/threatsday-ghostjacking-ai-attacks.html

INC Ransomware explota vulnerabilidades en SonicWall SMA1000

Resumen: El grupo INC Ransomware se ha convertido en uno de los principales actores explotando las vulnerabilidades CVE-2026-15409 y CVE-2026-15410 en dispositivos SonicWall SMA1000. Los ataques han afectado tanto a organizaciones públicas como privadas y han permitido robo de credenciales, acceso persistente y movimiento lateral en redes corporativas

¿Cómo protegerse?

- ✅ Aplicar urgentemente los parches de SonicWall.
- ✅ Rotar credenciales almacenadas en los dispositivos afectados.
- ✅ Revisar indicadores de compromiso y accesos remotos.

Link: https://thehackernews.com/2026/08/inc-ransomware-emerges-as-dominant.html

CVEs

SharePoint Weak Authentication Vulnerability (CVE-2026-55040)

Resumen: Vulnerabilidad de autenticación débil en Microsoft SharePoint que permite a atacantes remotos eludir mecanismos de seguridad y obtener acceso no autorizado a funcionalidades protegidas. Ha sido incluida por CISA entre las vulnerabilidades explotadas activamente.

Gravedad: 🔥 Crítica (9/10) – Riesgo crítico en plataformas de colaboración empresarial y gestión documental, pudiendo facilitar accesos no autorizados e información corporativa sensible.
Ejemplo real: La vulnerabilidad comenzó a ser explotada tras la publicación de un PoC público, afectando a servidores SharePoint expuestos a Internet.

✅ **Solución:** Microsoft ha publicado actualizaciones de seguridad para corregir la vulnerabilidad. Se recomienda aplicar los parches disponibles, revisar los registros de autenticación en busca de accesos anómalos y limitar la exposición de servidores SharePoint a Internet mediante segmentación de red y controles de acceso adicionales.

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

Broadcom VMware vCenter Path Traversal (CVE-2026-59310)

Resumen: Vulnerabilidad de Path Traversal que permite ejecución remota de código en VMware vCenter y que ya está siendo explotada por actores maliciosos

Gravedad: 🔥 Crítica (9/10) – Impacto muy elevado en infraestructuras virtualizadas y centros de datos corporativos, pudiendo comprometer múltiples sistemas desde la plataforma central de administración.
Ejemplo real: Investigadores han observado campañas que utilizan esta vulnerabilidad para desplegar puertas traseras, reverse shells e incluso ransomware derivado de Babuk.

✅ **Solución:** Broadcom ha publicado actualizaciones de seguridad para las versiones afectadas de VMware vCenter. Es recomendable aplicar los parches con prioridad alta, revisar indicadores de compromiso en los hosts gestionados por vCenter y reforzar el acceso administrativo mediante MFA y segmentación.

Link: https://www.vmware.com/security/advisories.html

Microsoft Internet Key Exchange (IKE) (CVE-2026-33824)

Resumen: Vulnerabilidad Double Free en el servicio Internet Key Exchange de Microsoft que permite la ejecución remota de código sin autenticación previa.

Gravedad: 🔥 Crítica (9/10) – Alto impacto en infraestructuras VPN, comunicaciones seguras y servicios de acceso remoto corporativo.
Ejemplo real: La vulnerabilidad ha sido asociada a campañas de explotación por actores avanzados que combinan automatización e intrusión manual.

✅ **Solución:** Microsoft ha corregido la vulnerabilidad mediante actualizaciones de seguridad. Se recomienda actualizar todos los sistemas afectados, revisar configuraciones IPsec/VPN expuestas a Internet y monitorizar intentos de conexión inusuales relacionados con el protocolo IKE.

Link: https://msrc.microsoft.com

Progress Kemp LoadMaster Command Injection (CVE-2026-8037)

Resumen: Vulnerabilidad de inyección de comandos que permite la ejecución remota de código sin autenticación en dispositivos Progress Kemp LoadMaster. Se han observado cientos de intentos de explotación en entornos reales.

Gravedad: 🔥 Crítica (9/10) – Impacto crítico en balanceadores de carga y componentes perimetrales expuestos a Internet.
Ejemplo real: Los sistemas de monitorización han registrado cientos de intentos de explotación procedentes de decenas de países diferentes.

✅ **Solución:** Progress recomienda actualizar inmediatamente los dispositivos afectados a versiones corregidas. Adicionalmente, conviene restringir el acceso administrativo desde Internet, revisar los registros del sistema en busca de actividad sospechosa y validar la integridad de las configuraciones críticas.

Link: https://thehackernews.com/2026/08/progress-kemp-loadmaster-flaw-hits-cisa.html

Apple macOS Screen Sharing Authentication Bypass (CVE-2026-65400)

Resumen: Vulnerabilidad de autenticación en macOS que permite el acceso al servicio Screen Sharing sin disponer de credenciales válidas. Apple confirmó la existencia de explotación activa tras la publicación de los parches.

Gravedad: 🔥 Crítica (9/10) – Alto impacto en equipos macOS corporativos con servicios de acceso remoto habilitados.
Ejemplo real: La vulnerabilidad ha sido utilizada para obtener acceso privilegiado a sistemas afectados y desplegar software de minería de criptomonedas.

✅ **Solución:** Apple ha publicado actualizaciones de seguridad para corregir el problema. Se recomienda actualizar todos los equipos afectados, deshabilitar los servicios de compartición remota que no sean necesarios y revisar accesos remotos recientes para detectar comportamientos anómalos.

Link: https://support.apple.com/security-updates