Mes: Octubre 2026

Resumen mensual

Malware

YuanKong: nuevo troyano Android capaz de robar PIN bancarios y contraseñas

Resumen: Investigadores han identificado YuanKong, un nuevo troyano para Android capaz de controlar dispositivos de forma remota y robar credenciales bancarias, PIN y otra información sensible. Su capacidad de ocultación lo convierte en una amenaza especialmente relevante para usuarios de banca móvil.

¿Cómo protegerse?

- ✅ Descargar aplicaciones únicamente desde tiendas oficiales.
- ✅ Revisar cuidadosamente los permisos concedidos a las aplicaciones.
- ✅ Mantener actualizado el sistema operativo y las aplicaciones instaladas.

Link: https://cybersecuritynews.com/new-yuankong-android-rat/

PoeLLM infecta más de 3K servidores para la minería de criptomonedas

Resumen: Investigadores han identificado PoeLLM, un malware que compromete servidores de inteligencia artificial y plataformas LLM para desplegar mineros de criptomonedas. PoeLLM utiliza los sistemas comprometidos para propagarse a nuevos objetivos.

¿Cómo protegerse?

- ✅ Mantener actualizados los servicios expuestos a Internet y las plataformas de IA.
- ✅ Restringir el acceso público a herramientas de administración y entornos LLM.
- ✅ Monitorizar el consumo anómalo de CPU y conexiones salientes sospechosas.

Link: https://thehackernews.com/2026/10/poellm-malware-infects-3400-servers-to.html

Potassium: la variante de Mirai que aprovecha la crisis PHP2Shell

Resumen: Los ciberdelincuentes están intentando desplegar la botnet Potassium, derivada de Mirai, aprovechando las vulnerabilidades críticas PHP2Shell. El objetivo es incorporar servidores vulnerables a una red utilizada para lanzar ataques DDoS y otras actividades maliciosas.

¿Cómo protegerse?

- ✅ Aplicar inmediatamente los parches de seguridad de PHP.
- ✅ Revisar servidores expuestos a Internet en busca de indicadores de compromiso.
- ✅ Implementar sistemas de detección y monitorización de tráfico anómalo.

Link: https://thehackernews.com/2026/10/php2shell-exploit-attempts-hit-millions.html

Phishing

Los estafadores saben tu nombre, y cuentan contigo para responder

Resumen: Se ha detectado una nueva técnica de fraude por SMS basada en mensajes extremadamente breves y personalizados que buscan provocar una respuesta espontánea de la víctima. Al conocer previamente el nombre de la persona, los delincuentes incrementan la credibilidad del mensaje y facilitan posteriores acciones de ingeniería social. La campaña se está observando con especial intensidad en Europa.

¿Cómo protegerse?

- ✅ Desconfiar de mensajes inesperados, aunque incluyan datos personales reales.
- ✅ No responder a SMS de remitentes desconocidos.
- ✅ Bloquear y reportar números sospechosos.

Link: https://www.elespanol.com/omicrono/software/20261013/ciberataque-supermercados-europeos-costo-millones-apago-neveras-congeladores/1003744417796_0.html

Microsoft alerta de campañas masivas que utilizan caracteres Unicode invisibles

Resumen: Microsoft ha detectado campañas de phishing capaces de evadir filtros de seguridad usando caracteres Unicode invisibles dentro de los correos electrónicos. Esta técnica permite ocultar palabras clave utilizadas habitualmente por los sistemas de detección. Se han distribuido millones de mensajes con temáticas financieras y corporativas.

¿Cómo protegerse?

- ✅ Utilizar soluciones avanzadas de protección de correo electrónico.
- ✅ Verificar cuidadosamente enlaces y remitentes.
- ✅ Formar a los usuarios en nuevas técnicas de phishing.

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

Suplantación de personal de soporte mediante Microsoft Teams

Resumen: Diversos grupos criminales continúan utilizando cuentas externas de Microsoft Teams para hacerse pasar por personal de soporte técnico. Los atacantes buscan convencer a los empleados para instalar herramientas de acceso remoto o revelar credenciales corporativas. Esta técnica está siendo utilizada contra organizaciones de múltiples sectores.

¿Cómo protegerse?

- ✅ Validar siempre la identidad del personal de soporte.
- ✅ Restringir las comunicaciones externas cuando sea posible.
- ✅ No instalar software a petición de contactos no verificados.

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

Brechas de seguridad

Ciberataque a supermercados europeos provoca pérdidas millonarias

Resumen: Un ataque contra grandes cadenas de supermercados de Francia, Bélgica y Países Bajos manipuló los sistemas de refrigeración industrial, provocando pérdidas económicas significativas. El incidente evidencia el creciente interés de los atacantes por infraestructuras operacionales y sistemas industriales conectados.

¿Cómo protegerse?

- ✅ Segmentar redes IT y OT.
- ✅ Limitar accesos remotos a sistemas industriales.
- ✅ Implementar monitorización específica para infraestructuras críticas.

Link: https://www.elespanol.com/omicrono/software/20261013/ciberataque-supermercados-europeos-costo-millones-apago-neveras-congeladores/1003744417796_0.html

El Colegio Oficial de Médicos de Santa Cruz de Tenerife sufre un ciberataque

Resumen: El Colegio Oficial de Médicos de Santa Cruz de Tenerife informó de un ataque que afectó a su infraestructura tecnológica y provocó el cifrado de sistemas. Aunque inicialmente se sospechó de una posible exfiltración de datos, las primeras investigaciones no encontraron evidencias de fuga de información. El incidente fue comunicado a la AEPD e INCIBE.

¿Cómo protegerse?

- ✅ Mantener copias de seguridad verificadas y desconectadas.
- ✅ Implantar sistemas de detección temprana de ransomware.
- ✅ Disponer de procedimientos de respuesta ante incidentes.

Link: https://ciberseguridad.castillalamancha.es/noticias/el-colegio-oficial-de-medicos-de-santa-cruz-de-tenerife-informa-de-un-ciberataque-su

Compromiso de claves de certificación eMudhra

Resumen: Uno de los incidentes más relevantes del mes ha sido el compromiso de claves asociadas a autoridades de certificación intermedias de eMudhra. El incidente obligó a desplegar medidas de emergencia por parte de fabricantes de navegadores y ha generado preocupación sobre la confianza en la cadena de certificación digital.

¿Cómo protegerse?

- ✅ Mantener navegadores y sistemas actualizados.
- ✅ Supervisar cambios inesperados en certificados digitales.
- ✅ Aplicar validaciones estrictas sobre infraestructuras PKI.

Link: https://en.wikipedia.org/wiki/Black_October_%28information_security%29

CVEs

CVE-2026-109618 / CVE-2026-109619 – PHP2Shell

Resumen: Dos vulnerabilidades críticas descubiertas en PHP permiten ejecución remota de código sin autenticación en servidores vulnerables. Los fallos afectan a aplicaciones ampliamente desplegadas como WordPress, Drupal y Joomla y ya están siendo explotados activamente.

Gravedad: 🔥 Crítica (10/10) – Riesgo crítico para sitios web corporativos, portales públicos y aplicaciones basadas en PHP expuestas a Internet.
Ejemplo real: Diversas organizaciones desconectaron temporalmente servicios web para actualizaciones de emergencia publicadas por el equipo de PHP.

✅ **Solución:** Actualizar inmediatamente a las versiones corregidas de PHP, verificar la existencia de indicadores de compromiso y revisar especialmente servidores que ejecuten WordPress, Drupal o Joomla expuestos a Internet.

Link: https://www.oracle.com/security-alerts/alert-cve-2026-109618.html

Google corrige 108 vulnerabilidades en Chrome, incluidas 11 críticas

Resumen: Google ha corregido 108 vulnerabilidades de seguridad en Chrome, entre ellas 11 fallos críticos que podrían permitir la ejecución de código malicioso en los equipos afectados. La actualización reduce el riesgo de compromiso de dispositivos mediante páginas web diseñadas para explotar estas vulnerabilidades.

Gravedad: 🔥 Crítica (9/10) – Alto impacto en estaciones de trabajo corporativas y usuarios que utilizan Chrome como navegador principal, pudiendo facilitar la ejecución de código y el compromiso del equipo.
Ejemplo real: Un usuario accede a una web maliciosa con una vulnerabilidad crítica para ejecutar código sin su conocimiento y tomar el control del sistema.

✅ **Solución:** Se recomienda actualizar inmediatamente Chrome a la última versión disponible, habilitar las actualizaciones automáticas del navegador y verificar que todos los equipos corporativos reciben los parches de seguridad de forma centralizada

Link: https://ciberseguridad.castillalamancha.es/noticias/google-corrige-1...-podrian-permitir-ejecucion-de-codigo

Vulnerabilidades en bibliotecas Java de código abierto detectadas por IBM y Red Hat

Resumen: La plataforma Lightwell identificó y corrigió más de 400 vulnerabilidades previamente desconocidas en bibliotecas Java. El hallazgo pone de manifiesto el creciente impacto de los riesgos asociados a la cadena de suministro de software.

Gravedad: 🔥 Alta (8.5/10) – Riesgo significativo para aplicaciones empresariales dependientes de bibliotecas de terceros y componentes open source.
Ejemplo real: Las vulnerabilidades afectaban componentes presentes en entornos productivos de numerosas organizaciones.

✅ **Solución:** Actualizar dependencias afectadas, implantar herramientas de gestión de vulnerabilidades y mantener una supervisión continua de componentes de terceros en aplicaciones corporativas.

Link: https://cybersecuritynews.com/emergency-java-update/

CVE-2026-115560 – PHP Remote Code Execution

Resumen: Investigadores alertaron de una nueva vulnerabilidad de ejecución remota de código en PHP, identificada poco después de los fallos PHP2Shell. El problema afecta al intérprete PHP y aumenta la presión sobre organizaciones que dependen de aplicaciones web basadas en esta tecnología.

Gravedad: 🔥 Crítica (9.8/10) – Alto impacto en infraestructuras web, servicios de Internet y aplicaciones empresariales desarrolladas sobre PHP.

Ejemplo real: La vulnerabilidad fue divulgada mientras numerosas organizaciones aún estaban desplegando las actualizaciones de emergencia asociadas a PHP2Shell.

✅ **Solución:** Se recomienda aplicar las actualizaciones publicadas por el proyecto PHP tan pronto como estén disponibles, mantener inventariadas todas las aplicaciones dependientes de PHP y reforzar la monitorización de los servidores web expuestos.

Link: https://thehackernews.com/2026/10/php2shell-exploit-attempts-hit-millions.html

Citrix NetScaler Zero-Day

Resumen: Citrix confirmó durante octubre la existencia de nuevas vulnerabilidades de día cero que afectan a NetScaler ADC y NetScaler Gateway, productos ampliamente utilizados para acceso remoto seguro, balanceo de carga y publicación de aplicaciones. La explotación de estos fallos puede permitir el compromiso de dispositivos perimetrales expuestos a Internet y facilitar el acceso no autorizado a infraestructuras corporativas.

Gravedad: 🔥 Crítica (9.8/10) – Impacto muy elevado en infraestructuras perimetrales, servicios VPN y plataformas de acceso remoto, pudiendo comprometer sistemas críticos de la organización

Ejemplo real: Numerosas organizaciones iniciaron revisiones urgentes de sus despliegues de NetScaler tras la divulgación de los fallos, aplicando medidas de contención y actualizaciones para evitar posibles compromisos de servicios expuestos a Internet.

✅ **Solución:** Citrix recomienda actualizar inmediatamente los dispositivos afectados a las versiones corregidas, restringir el acceso a las interfaces de administración, revisar registros en busca de actividad sospechosa y verificar la integridad de las configuraciones y credenciales almacenadas en los equipos expuestos.

Link: https://www.securityweek.com/citrix-confirms-2-netscaler-zero-days-after-admins-pulled-the-plug/