BOLETÍN DE CIBERSEGURIDAD

MES DE FEBRERO 2026

BOLETÍN DE CIBERSEGURIDAD, FEBRERO 2026

"Así como nos unimos para celebrar la amistad y el cariño en este mes de febrero, es vital reconocer que nuestro entorno digital también requiere ese mismo cuidado y atención para proteger a quienes más valoramos.

En este mes, frente al aumento de intercambios digitales, regalos sorpresa y transacciones en línea, los riesgos cibernéticos como el phishing emocional se vuelven más presentes. Reforzar nuestra cultura de seguridad no es solo una tarea técnica, es un acto de cuidado que protege nuestros datos personales y los de nuestra red de contactos y seres queridos. Al igual que procuramos el bienestar de nuestros afectos en el Día del Cariño, debemos garantizar que nuestra huella digital sea segura, permitiéndonos compartir y conectar con la tranquilidad y la protección que nuestro entorno digital merece.

FUENTE: SUBDIRECCIÓN DE EQUIPO DE RESPUESTA A INCIDENTES CIBERNÉTICOS.

ALERTA DE MICROSOFT: EL COMANDO "NSLOOKUP" ESTÁ SIENDO UTILIZADO PARA OCULTAR NUEVOS VIRUS

Microsoft ha detectado una sofisticada campaña de malware denominada "ClickFix", que utiliza ingeniería social para engañar a los usuarios. Los atacantes muestran errores falsos en páginas web y piden a las personas que copien y peguen un comando técnico en sus computadoras para "solucionarlos". Al hacerlo, se activa la herramienta legítima de Windows nslookup, que descarga un troyano de forma fragmentada y silenciosa para evadir a los antivirus tradicionales. Una vez instalado, los criminales obtienen acceso total al equipo para robar contraseñas e información sensible. La recomendación principal es jamás ejecutar comandos dictados por sitios web externos.

FUENTE: MICROSOFT.COM

¡ACTUALIZA YA! GOOGLE PARCHA LA PRIMERA VULNERABILIDAD CRÍTICA DE CHROME DEL 2026

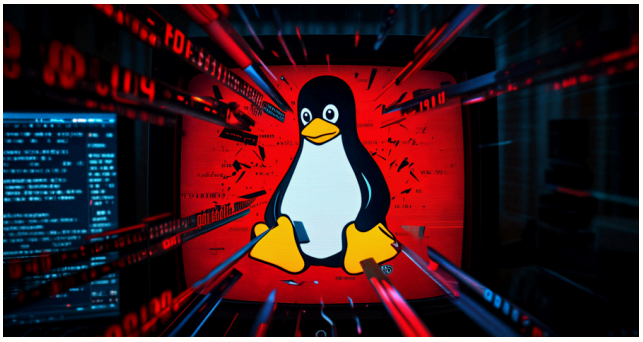
Google ha lanzado una actualización de emergencia para corregir la vulnerabilidad CVE-2026-2441, un fallo de "día cero" de alta severidad que ya está siendo explotado activamente en internet. El problema radica en un error de memoria (tipo use-after-free) dentro del motor de procesamiento de fuentes CSS del navegador.

Según los reportes técnicos de Microsoft Threat Intelligence y CISA, un atacante puede tomar el control total de la sesión del usuario simplemente logrando que este visite una página web maliciosa diseñada específicamente para activar el fallo. Debido al riesgo inminente de ejecución de código remoto, Google recomienda a todos los usuarios verificar que su navegador esté actualizado a la versión 145.0.7632.75 o superior para cerrar esta puerta de entrada a posibles virus y troyanos.

FUENTE: THE HACKER NEWS

ALERTA SSHSTALKER: LA BOTNET QUE REVIVE VIEJOS FALLOS PARA SECUESTRAR SERVIDORES LINUX

Investigadores de seguridad han descubierto una nueva botnet denominada "SSHStalker", la cual se especializa en atacar servidores Linux mediante ataques de fuerza bruta por el protocolo SSH. Una vez que logra entrar, utiliza exploits de kernel antiguos (fallos de seguridad de años pasados que muchos administradores no han parchado) para obtener permisos de administrador (root). Lo más curioso de esta amenaza es que utiliza el protocolo IRC, una tecnología de chat de los años 80, como centro de mando y control (C2) para recibir órdenes de los atacantes. Una vez que el sistema está bajo su mando, SSHStalker lo utiliza para realizar ataques de denegación de servicio (DDoS) o minería de criptomonedas, aprovechando la potencia del servidor infectado.



FUENTE: THE HACKER NEWS

ALERTA DE ESPIONAJE: ZERODAYRAT, EL NUEVO SOFTWARE QUE CONVIERTE TU CELULAR EN UN MICRÓFONO ABIERTO

Investigadores de seguridad de iVerify han alertado sobre la aparición de ZeroDayRAT, una plataforma de "Malware como Servicio" (MaaS) diseñada para comprometer dispositivos Android e iOS. A diferencia de otros virus, este kit permite vigilancia en tiempo real: los atacantes pueden activar de forma remota la cámara (frontal o trasera) y el micrófono, ver la pantalla en vivo y rastrear la ubicación GPS exacta del usuario. Además de espiar la vida privada, ZeroDayRAT incluye módulos de robo financiero diseñados para vaciar carteras de criptomonedas y capturar credenciales bancarias mediante la superposición de pantallas falsas. Se propaga principalmente a través de mensajes de texto (Smishing) con enlaces que parecen actualizaciones legítimas o aplicaciones de "regalo".

FUENTE: SECURITYWEEK.COM

TRES FLECHAZOS DE SABIDURÍA PARA NO MORIR DE VIRUS

- Duda de ofertas sospechosas: No hagas clic en enlaces de sorteos o premios "sorpresa" por redes sociales o WhatsApp; suelen ser estafas para robar tus datos.
- Evita descargas peligrosas: Nunca abras archivos adjuntos ni instales apps que prometan "tarjetas de regalo", ya que pueden contener virus.
- Cuida tu información personal: En apps de citas, no compartas datos financieros, dirección exacta ni contenido íntimo bajo ninguna circunstancia, sin importar qué tan seguro creas estar.

FUENTE: SUBDIRECCIÓN DE EQUIPO DE RESPUESTA A INCIDENTES CIBERNÉTICOS.