BOLETÍN DE CIBERSEGURIDAD

CULTIVANDO UN ENTORNO DIGITAL SEGURO Y SOSTENIIBLE

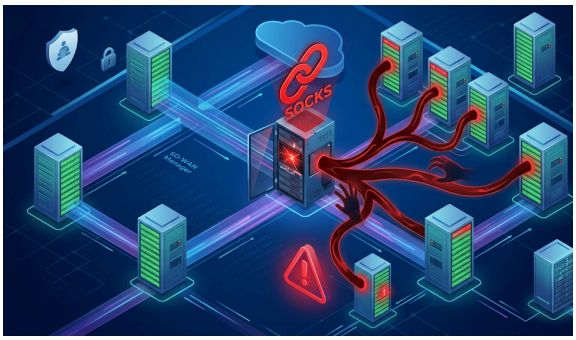
Abril 2026 | Edición Especial: Día de la Tierra

BOLETÍN DE CIBERSEGURIDAD, ABRIL DE 2026

"Así como nos unimos para proteger los recursos naturales de nuestra Guatemala en este Día de la Tierra, es vital reconocer que nuestro entorno digital también requiere un cuidado responsable y sostenible.

En este mes de abril, tras el movimiento de la temporada de verano y frente al aumento de gestiones tributarias y transacciones en línea, los riesgos cibernéticos se vuelven más presentes. Reforzar nuestra cultura de seguridad no es solo una tarea técnica, es sembrar prácticas que protejan nuestros datos personales, institucionales y familiares. Al igual que cuidamos nuestra tierra, debemos garantizar que nuestra huella digital sea segura, permitiéndonos navegar con la tranquilidad y la protección que nuestro entorno digital merece."

FUENTE: SUBDIRECCIÓN DE EQUIPO DE RESPUESTA A INCIDENTES CIBERNÉTICOS.



ALERTA CLOUD: LA BOTNET "CHAOS" EVOLUCIONA PARA CONVERTIR SERVIDORES MAL CONFIGURADOS EN TÚNELES PARA CRIMINALES

Investigadores de seguridad han detectado una nueva y agresiva variante del malware Chaos, la cual está escaneando internet en busca de instancias en la nube (AWS, Azure, Google Cloud) que tengan errores de configuración o contraseñas débiles.
Lo que hace única a esta versión de 2026 es que, además de los ataques habituales, instala automáticamente un proxy SOCKS. Esto permite a los atacantes utilizar el servidor de la víctima como un "puente" invisible para saltar hacia otros objetivos, ocultando su ubicación real y haciendo que el tráfico malicioso parezca venir de una IP corporativa legítima. Esta táctica no solo facilita el robo de datos, sino que pone a la empresa afectada en riesgo legal al ser su infraestructura la que realiza los ataques.

FUENTE: THE HACKER NEWS

¡CUIDADO CON LO QUE CLICAS! EL TROYANO MIRAX INFECTA A 220,000 USUARIOS DE ANDROID A TRAVÉS DE ANUNCIOS EN META

Expertos en ciberseguridad han detectado una campaña masiva de infección distribuida mediante anuncios maliciosos (Malvertising) en plataformas de Meta (Facebook e Instagram). El malware, denominado Mirax Android RAT, se disfraza de aplicaciones legítimas como herramientas de seguridad, optimizadores de batería o juegos populares. Una vez instalado, el troyano convierte el teléfono de la víctima en un proxy SOCKS5. Esto permite a los cibercriminales "alquilar" la conexión a internet y la dirección IP del usuario para realizar actividades ilegales (como ataques a bancos o envío de spam) de forma anónima. Hasta la fecha, se estima que más de 220,000 dispositivos han sido comprometidos, permitiendo además a los atacantes robar mensajes SMS, listas de contactos y datos bancarios.

FUENTE: THE HACKER NEWS

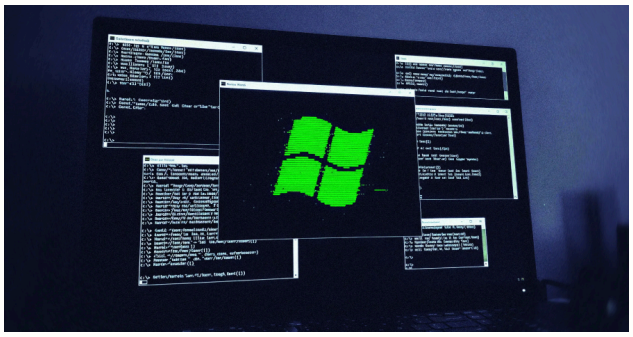
MEGA-FRAUDE GLOBAL: LA ESTAFA DE LOS "CAPTCHAS FALSOS" QUE VACÍA CARTERAS Y SECUESTRA LÍNEAS MÓVILES

Investigadores de seguridad han desmantelado una red masiva de Fraude de Bombeo de SMS (IRSF) que utiliza una técnica ingeniosa: CAPTCHAs falsos. Los atacantes han desplegado más de 120 campañas simultáneas utilizando el rastreador de tráfico Keitaro (una herramienta usada normalmente por expertos en marketing) para dirigir a las víctimas a sitios web fraudulentos.

El engaño funciona así: el usuario intenta acceder a un sitio y se le pide resolver un CAPTCHA para "verificar que es humano". Al interactuar, en realidad está activando una suscripción a servicios SMS de tarificación especial o autorizando transacciones de criptomonedas en segundo plano. Esta operación no solo roba dinero directamente de las carteras digitales, sino que genera millones de dólares en pérdidas para las empresas de telecomunicaciones al inflar artificialmente el tráfico de mensajes internacionales de alto costo.

FUENTE: THE HACKER NEWS

ALERTA DE EXPLOTACIÓN: WINDOWS SHELL CVE-2026-32202 PERMITE ROBO DE CREDENCIALES "ZERO-CLICK"

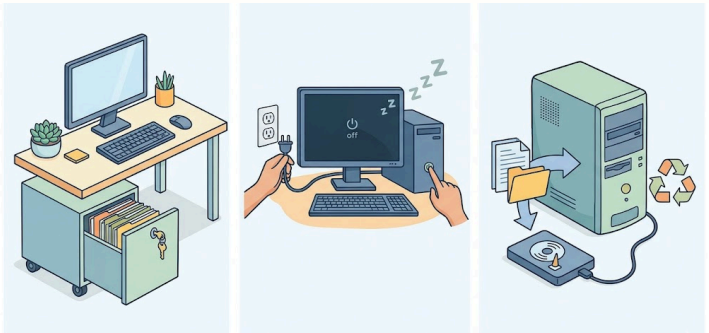


Microsoft ha confirmado que atacantes están explotando activamente la vulnerabilidad CVE-2026-32202 en el Shell de Windows. Este fallo es el resultado de un parche incompleto para una vulnerabilidad previa (CVE-2026-21510) vinculada al grupo de amenazas APT28 (Fancy Bear). El problema radica en cómo Windows Explorer procesa archivos de acceso directo (LNK) maliciosos; simplemente con que un usuario navegue a una carpeta que contenga el archivo, el sistema intenta extraer un icono, lo que fuerza una conexión SMB automática hacia un servidor del atacante. Esta conexión dispara un apretón de manos NTLM, entregando el hash Net-NTLMv2 del usuario al criminal para ataques de relevo (Relay) o descifrado fuera de línea.

FUENTE: THE HACKER NEWS

ECO-SEGURIDAD: CONSEJOS PARA CUIDAR TUS DATOS Y EL PLANETA

- No dejes post-its con contraseñas pegados al monitor ni documentos importantes sobre el escritorio al irte a comer o retirarte "Si lo dejas a la vista, lo dejas a la suerte; limpia tu mesa, asegura tu equipo."
- Apagado preventivo: Apaga y desconecta tu equipo al terminar la jornada; esto ahorra energía y cierra puertas a intrusiones cibernéticas nocturnas.
- Reciclaje seguro: Antes de desechar algun equipo antiguo pasa tus archivos importantes a un disco duro externo o a una nube limpia.



FUENTE: SUBDIRECCIÓN DE EQUIPO DE RESPUESTA A INCIDENTES CIBERNÉTICOS.