BOLETÍN DE CIBERSEGURIDAD

MARZO 2026 - GUATEMALA

BOLETÍN DE CIBERSEGURIDAD, MARZO DE 2026

En esta época de descanso, aumentan los viajes, el uso de redes Wi-Fi públicas en destinos turísticos y las transacciones en línea para reservas de hoteles y restaurantes, lo que también incrementa los riesgos cibernéticos. Es fundamental reforzar la cultura de seguridad manteniendo prácticas responsables que protejan nuestros datos personales, institucionales y familiares, garantizando que el verano se disfrute con tranquilidad y protección digital en esta Semana Santa.

FUENTE: SUBDIRECCIÓN DE EQUIPO DE RESPUESTA A INCIDENTES CIBERNÉTICOS.

ALERTA DE HARDWARE: GOOGLE CONFIRMA FALLO DE SEGURIDAD EN PROCESADORES QUALCOMM PARA ANDROID

Google ha emitido una advertencia oficial sobre la vulnerabilidad CVE-2026-21385, localizada en un componente crítico de los procesadores Qualcomm utilizados en millones de dispositivos Android. Este fallo de seguridad permite a un atacante local obtener privilegios elevados, lo que en lenguaje sencillo significa que una aplicación maliciosa podría saltarse todas las restricciones de seguridad del sistema operativo y acceder a zonas prohibidas de la memoria del teléfono. Aunque Google ya ha incluido la corrección en su boletín de seguridad de abril de 2026, la protección real de los usuarios depende de que los fabricantes (como Samsung, Xiaomi o Motorola) adapten y envíen esta actualización a sus modelos específicos lo antes posible.

FUENTE: THE HACKER NEWS

ALERTA CRÍTICA: ATACANTES VULNERAN DISPOSITIVOS FORTIGATE PARA SECUESTRAR REDES CORPORATIVAS

La Municipalidad de Guatemala ha detectado una red de estafas digitales que utiliza mensajes de texto y redes sociales para enviar notificaciones falsas de multas de tránsito. Los delincuentes imitan portales oficiales de EMETRA para robar datos bancarios bajo presión y falsas urgencias.

¿Cómo opera el fraude?

1. Mensaje de Alarma: Recibes un aviso de "multa vencida" con recargos elevados.
2. Enlace Engañoso: Incluyen un link a una página web que copia logos y colores oficiales, pero cuya dirección (URL) tiene letras alteradas.
3. Robo de Datos: Solicitan pagos pequeños o información de tarjetas para clonar tus cuentas.

Recomendaciones Oficiales:

1. EMETRA NO envía mensajes solicitando pagos inmediatos ni enlaces externos.
2. Verifica manualmente: Si tienes dudas, ingresa directamente al portal oficial de la Municipalidad o acude a una alcaldía auxiliar.
3. Desconfía de la urgencia: No compartas datos financieros en sitios que recibas por SMS o redes sociales.

FUENTE: LA HORA.GT

ALERTA CRÍTICA: ATACANTES VULNERAN DISPOSITIVOS FORTIGATE PARA SECUESTRAR REDES CORPORATIVAS

El equipo de respuesta a incidentes de Fortinet (PSIRT) y agencias de ciberseguridad globales han confirmado la explotación activa de múltiples vulnerabilidades críticas en dispositivos FortiGate (incluyendo CVE-2026-24858 y fallos de día cero relacionados con SSO). Los atacantes están utilizando estas fallos para saltarse la autenticación administrativa y obtener acceso completo a la configuración del firewall. Una vez dentro, extraen el archivo de configuración, el cual contiene datos sensibles de la topología de la red y, crucialmente, las credenciales encriptadas de cuentas de servicio (como LDAP/Active Directory). Mediante técnicas de descifrado, los criminales obtienen estas claves y las utilizan para realizar un movimiento lateral profundo dentro de la red interna de la organización, creando estaciones de trabajo falsas y comprometiendo servidores críticos sin ser detectados por los sistemas de seguridad tradicionales.

FUENTE: THE HACKER NEWS

LA NUEVA AMENAZA: HIVE0163 USA IA PARA CREAR MALWARE "FANTASMA" Y SECUESTRAR REDES CORPORATIVAS

El grupo de ransomware Hive0163 ha perfeccionado sus tácticas mediante el uso del malware Slopoly, el cual está asistido por inteligencia artificial para garantizar un acceso persistente y sigiloso. A diferencia del malware tradicional, Slopoly utiliza algoritmos de IA para reescribir su propio código sobre la marcha y adaptar sus técnicas de evasión cada vez que se ejecuta.
Esto significa que cada instancia del virus es única, lo que lo hace prácticamente indetectable para los antivirus basados en firmas y los sistemas EDR tradicionales. Una vez que Slopoly se instala silenciosamente, Hive0163 tiene el control total de la red para robar datos, descifrar credenciales y, finalmente, desplegar el ransomware que paraliza la operación de la empresa, cobrando rescates millonarios.

FUENTE: THE HACKER NEWS

GUÍA DE CIBERSEGURIDAD: PARA ESTA SEMANA SANTA 2026

Reserva Segura:
Evita ofertas "relámpago" en redes sociales que exigen depósitos inmediatos por WhatsApp; los estafadores suplantan hoteles y agencias reales para robar anticipos. Verifica siempre el dominio del sitio web y utiliza plataformas de pago reconocidas antes de confirmar tu estadía.
Conexiones en el Descanso:
No realices transferencias bancarias ni accedas a correos corporativos usando el Wi-Fi abierto de hoteles o restaurantes, ya que estas redes pueden ser interceptadas para capturar contraseñas. Prefiere el uso de tus datos móviles o una VPN para cifrar tu navegación mientras estás fuera.
Privacidad y "Oversharing": Evita publicar fotos o ubicaciones en tiempo real que confirmen que tu casa está vacía; los delincuentes monitorean redes sociales para identificar objetivos de robo residencial. Lo más seguro es compartir tus momentos de descanso una vez hayas regresado a casa.

FUENTE: SUBDIRECCIÓN DE EQUIPO DE RESPUESTA A INCIDENTES CIBERNÉTICOS.