Dirección de Investigación Criminal e INTERPOL
Centro Cibernético Policial

BALANCE **SEMANA 14/2023**

Cyber noticias

Trabajadores de Samsung cometieron un gran error al usar ChatGPT. Los trabajadores de Samsung filtraron sin darse cuenta datos confidenciales mientras usaban **ChatGPT** para cumplir con las tareas. Al hacerlo, los trabajadores ingresaron datos, como el código fuente de un nuevo programa, notas de reuniones internas y datos relacionados con su hardware. Dado que ChatGPT retiene los datos ingresados por el usuario para capacitarse aún más, estos secretos comerciales de Samsung ahora están en manos de OpenAI. **Fuente:** Techradar.

Microsoft comparte orientación para detectar ataques de bootkit BlackLotus UEFI. Microsoft compartió una guía para ayudar a las organizaciones a verificar si los ciberdelincuentes atacaron o pusieron en peligro las máquinas con el **bootkit BlackLotus UEFI** al explotar la vulnerabilidad CVE-2022-21894. Las organizaciones y los individuos también pueden usar los consejos de Microsoft para recuperarse de un ciberataque y evitar que los actores de amenazas que usan **BlackLotus** logren persistencia y eludan la detección. **Fuente:** Bleepingcomputer.

Actualizaciones para abordar fallas de día cero en iOS, iPadOS, macOS y Safari. Apple lanzó parches de seguridad para corregir una serie de vulnerabilidades. La primera es la CVE-2023-28206, una vulnerabilidad de escritura en IOSurfaceAccelerator que permitiría a una app maliciosa ejecutar código arbitrario con privilegios de kernel. La segunda es la CVE-2023-28205, una vulnerabilidad en el motor de navegador WebKit que permitiría al ciberdelincuente engañar para que accedan a contenido web especialmente diseñado para poder ejecutar código arbitrario. **Fuente:** Welivesecurity.

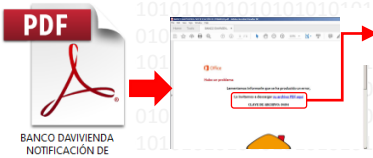
Microsoft Edge ahora puede generar imágenes con IA. Microsoft Edge se ha convertido en el primer y único navegador con un generador de imágenes de **IA** integrado, lo que permite a los usuarios crear imágenes que aún no existen, con la tecnología de los últimos modelos DALL-E de OpenAI. La función, llamada **Image Creator**, ahora está disponible en computadoras de escritorio para usuarios de **Edge** en todo el mundo.. **Fuente:** Bleepingcomputer.

Modalidad más reportada al CAI Virtual ¡ Phishing EMBARGO DAVIVIENDA!

Se identificó a través del servicio de CAI Virtual, una campaña de **phishing**, difundiendo el malware Remcos, tipo RAT (troyano de acceso remoto). Los ciberdelincuentes lo utilizan para realizar acciones en máquinas infectadas remotamente, como obtener información personal, afectar el patrimonio de las personas y/o ejecutar software malicioso. Está asociado al asunto: "EMBARGO DAVIVIENDA".

1. El correo allegado notifica un presunto incumplimiento en los pagos y obligaciones financieras, donde menciona que el supuesto departamento de CARTERAS toma la decisión de realizar un cobro jurídico.

2. Adjuntan un archivo **PDF** con un supuesto proceso jurídico de embargo bancario



3. Solicita que el destinatario dé clic en el enlace : "**su archivo PDF aquí**", el cual redireccionará a la descarga de un fichero comprimido .rar, que requiere un código de acceso que iniciará la ejecución del malware.

4. **RECOMENDACIONES**

- **EVITE** dar clic, sobre links o archivos adjuntos en correos electrónicos desconocidos y no abra archivos adjuntos.
- **VERIFIQUE** ortografía y redacción, usualmente hay errores.
- **TENGA EN CUENTA**, que ninguna entidad bancaria solicitará información de productos por correos electrónicos.
- **VERIFIQUE** que el remitente del correo corresponda a una entidad real.
- **REQUIERA** credenciales de administrador para instalar el software.
- **VERIFIQUE** los enlaces o archivos antes de ejecutarlos en un entorno de prueba (sanbox), **Ej:**Any.Run, Csirt.Ponal.
- **REALICE** copias de seguridad (**backups**) de su información de manera periódica.
- **REPORTE** el correo allegado con el CAIVirtual a través de la web: https://caivirtual.policia.gov.co

Boletín Informativo de Ciberseguridad

VULNERABILIDADES EN LA BIBLIOTECA **TPM 2.0** AMENAZAN A MILLONES DE DISPOSITIVOS IOT

ALTO

NIST
CVE-2023-1017
CVE-2023-1018

Descripción

El Modulo de Plataforma de Confianza **TPM**, que por sus siglas en ingles significa Trusted Plataform Module, es un pequeño chip instalado en la base del ordenador del equipo de computo; este criptoprocesador, es el encargado de almacenar las claves de cifrado, contraseñas, certificados digitales y la vez protege la privacidad de sus archivos sensibles.

Estado

La biblioteca de los módulos **TPM 2.0** (módulo de plataforma confiable), es afectada por la vulnerabilidad **CVE-2023-1017**, la cual corresponde a una **escritura** fuera de los límites, lo que puede provocar la alteración de datos, un bloqueo o la ejecución de código; así como la vulnerabilidad **CVE-2023-1018**, la cual se describe como una **lectura** fuera de los límites. Esto puede permitir a los ciberdelincuentes leer información confidencial de otras ubicaciones de memoria o provocar un bloqueo.

CVE-2023-1017	CVE-2023-1018
Puntuación básica:7.8 Vector de ataque (AV): local Complejidad del ataque (AC): bajo Privilegios Requeridos (PR): bajo Interacción del usuario (IU): ninguno Alcance (S): sin alterar Confidencialidad (C): alto Integridad (I): alto Disponibilidad (A): alto	Puntuación básica:5.5 Vector de ataque (AV): local Complejidad del ataque (AC): bajo Privilegios Requeridos (PR): bajo Interacción del usuario (IU): ninguno Alcance (S): sin alterar Confidencialidad (C):alto Integridad (I): ninguno Disponibilidad (A): ninguno

Recomendaciones

Aplicar las actualizaciones publicadas por **TCG** (Trusted Computing Group) y otros proveedores para abordar las vulnerabilidades presentes y reducir el riesgo.

Fuente: TrustedComputingGroup.

Actividades de gestión en seguridad digital

Incidentes gestionados a través del CAI Virtual — 4.114

170 — **Alertas y contenidos preventivos** 11 durante la semana

Muestras de malware analizadas — 223

63 — **Actividades de relacionamiento estratégico,** resaltando en la semana:

LA FM · RCN RADIO · La Cariñosa

Charlas de ciberseguridad — 32
Personas impactadas **4.353**

7.245 — **Páginas bloqueadas**
Material de abuso sexual infantil. **6.929**
Juegos ilegales de azar. **316**

Para sugerencias sobre este producto, por favor diligencie este formulario :https://bit.ly/3mz5C8d

Canales de atención y redes sociales

Página web · Twitter · Instagram · Facebook · WhatsApp