Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 073	Fecha: 25-03-2023 Página 4 de 23

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Extensión falsa de ChatGPT en el navegador Chrome está secuestrando cuentas de Facebook		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	Red, Internet, Redes Sociales, Correo Electrónico		
Código de familia	C	Código de subfamilia	C01
Clasificación temática familia	Código malicioso		

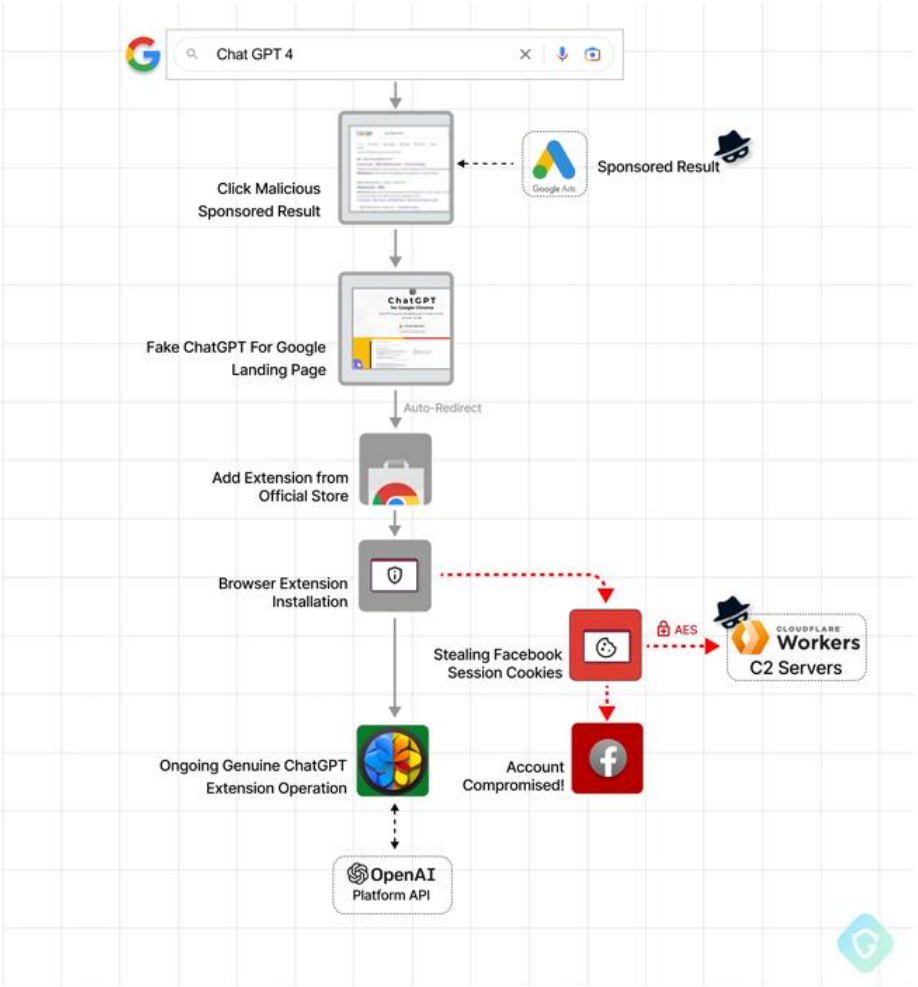
Descripción

Google intervino para eliminar una extensión falsa del navegador Chrome de la tienda web oficial que se hizo pasar por el servicio ChatGPT de OpenAI para recolectar cookies de sesión de Facebook y secuestrar las cuentas.

DETALLES:

- La extensión "ChatGPT para Google", una versión troyanizada de un complemento de navegador de código abierto legítimo, atrajo más de 9000 instalaciones desde el 14 de marzo de 2023, antes de su eliminación. Se subió originalmente a Chrome Web Store el 14 de febrero de 2023.

- Según una investigadora de Guardio Labs, la extensión se propaga a través de resultados de búsqueda de Google patrocinados maliciosos que están diseñados para redirigir a los usuarios desprevenidos que buscan "Chat GPT-4" a páginas de destino fraudulentas que apuntan al complemento falso.



- La instalación de la extensión agrega la funcionalidad prometida, es decir, mejora los motores de búsqueda con ChatGPT, pero también activa sigilosamente la capacidad de capturar cookies relacionadas con Facebook y filtrarlas a un servidor remoto de manera encriptada.

- Una vez en posesión de las cookies de la víctima, el autor de la amenaza toma el control de la cuenta de Facebook, cambia la contraseña, altera el nombre y la imagen del perfil e incluso la utiliza para difundir propaganda extremista.

- Con ello se prueba una vez más de que los ciberdelincuentes son capaces de adaptar rápidamente sus campañas para sacar provecho de la popularidad de ChatGPT para distribuir malware y organizar ataques oportunistas.

RECOMENDACIONES:

- Verificar si las extensiones para Chrome son validadas por el proveedor.
- Evite hacer clic en enlaces de mensajes de spam o en sitios web desconocidos.
- Evitar descargar aplicaciones de sitios no confiables.
- Evitar hacer clic en la URL o abrir archivos adjuntos en correos electrónicos no deseados.
- Evite revelar información personal mediante un mensaje de texto o un correo electrónico de una fuente que no sea de confianza en donde se le solicita información personal.
- Mantener actualizadas los software (Sistema operativo y antivirus) de las estaciones de trabajo.

Fuentes de información	▪ hxxps://thehackernews.com/2023/03/fake-chatgpt-chrome-browser-extension.html ▪ Análisis propio de fuentes abiertas.