Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°146	Fecha: 23-06-2023
		Página: 4 de 7

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Falsa extensión de ChatGPT instala malware que roba cookies de sesión de Facebook		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES

Se encuentra nuevos sitos falsos que se hacen pasar por herramientas legítimas basadas en ChatGPT, con el fin que la víctima descargue e instale la aplicación maliciosa.

2. DETALLES:

El proceso de instalación de la aplicación maliciosa incluye la descarga de un archivo con extensión .msi que, al ejecutarse GPT4_V2_1.7_Setup.rar y finalizado este proceso se abre el navegador Google Chrome que lleva al sitio oficial de ChatGPT, la víctima no se da cuenta que en su equipo instaló una extensión maliciosa que se mantiene oculta.

Luego del análisis del archivo de instalación se detecta que contiene dos archivos: .gpt4.bat y un archivo ejecutable GPT4 V2.exe. Se observa que se trata de un archivo desarrollado en C# que se encarga de que el malware siga en el equipo y de crear una carpeta de nombre dmkamcknogkgcdfhhbddcghachkejeap.

Cuando el archivo gpt4.bat dentro del MSI termina de instalarse se ejecutan varios comandos. Uno de los comandos ejecutados es el encargado de abrir una nueva ventana Google Chrome y cargar el sitio oficial https://chat.openai.com/, mientras que otro comando carga una extensión en el navegador almacenada en la carpetadmkamcknogkgcdfhhbddcghachkejeap, en su interior encontramos un archivo JavaScript denominado background.js.

Después de analizar este archivo observamos que busca en la computadora, para robarle las cookies y asi pueda acceder a todas las cookies de Facebook, esto permite a los ciberdelincuentes: acceso no autorizado a la cuenta, ataques de suplantación de identidad, acceso y recopilación de información personal, recolectar información para comercializarla.

Algunas de las medidas seguridad implementadas por Facebook, como el cifrado de datos y los mecanismos de autenticación, están diseñados para proteger las cuentas de las personas, si las cookies se ven comprometidas estas medidas de seguridad pueden ser eludidas.

3. RECOMENDACIONES:

En caso de sospechar que las cookies de Facebook han sido robadas realiza lo siguiente:

- Restablece tu contraseña de Facebook lo antes posible para evitar que el atacante acceda a tu cuenta.
- Verifica si hay actividades inusuales en tu cuenta, como publicaciones, mensajes o configuraciones modificadas.
- Activa la autenticación de dos factores en tu cuenta de Facebook para agregar una capa adicional de seguridad.
- Revisa y revoca el acceso de las aplicaciones de terceros conectadas a tu cuenta de Facebook.
- Establece una vigilancia activa para detectar cualquier comportamiento sospechoso en tu cuenta o actividad en línea.
- Utiliza alguna solución de antimalware en tus dispositivos.

Fuente de Información:	hxxps://www.welivesecurity.com/la-es/2023/06/22/extension-falsa-chatgpt-roba-cookies-facebook/