Falsa extensión de ChatGPT instala malware que roba cookies de Facebook

El equipo de investigación de ESET, compañía líder en detección proactiva de amenazas, identificó que los cibercriminales están creando sitios falsos utilizando el nombre de ChatGPT como señuelo para infectar con malware.

Si bien muchas de estas páginas suelen estar activas durante un corto período de tiempo, recientemente se descubrió una que llamó la atención. Se trata de un sitio que incluye el nombre de ChatGPT en la URL y que ofrece una herramienta basada en el código de este popular chatbot para fines de marketing y publicidad.

Las cookies son pequeños archivos que contienen información que permiten autenticar y mantener una sesión abierta en un dispositivo.

Esto significa que, gracias a las cookies, la persona evita tener que colocar manualmente sus credenciales cada vez que quiere acceder a su cuenta. Si un atacante tiene acceso a las cookies de Facebook en un equipo, pueden utilizarlas para realizar acciones en nombre del usuario sin su consentimiento y obtener acceso no autorizado.

En este caso el objetivo es que la víctima descargue una aplicación maliciosa que se instala como una extensión para Google Chrome y permite al atacante acceder a las cookies del navegador, dándole la posibilidad de realizar distintos tipos de acciones.

La persona que descarga e instala esta falsa herramienta del sitio, que ya fue dado de baja, sin darse cuenta instalará código malicioso que corre como una extensión para el navegador.

Con información de El Impulso