ALERTA

Campaña de Malware:CAPTCHA. Distribución de Lumma Stealer

COLCERT AL-2709-050

Una nueva y sofisticada campaña de **malware** está utilizando páginas web falsas de CAPTCHA para distribuir el peligroso **troyano bancario Lumma Stealer**.Los atacantes emplean dos tácticas principales para engañar a las víctimas.

ELEMENTOS DE INTELIGENCIA DISPONIBLES

Descargas de Software Pirateado: Al buscar versiones gratuitas o crackeadas de juegos populares, los usuarios son redirigidos a sitios web falsos que simulan un CAPTCHA.

Phishing de GitHub: Los atacantes envían correos electrónicos falsos que parecen provenir de GitHub, alertando a los usuarios sobre una supuesta vulnerabilidad de seguridad y dirigiéndolos a las mismas páginas falsas de CAPTCHA.

ANÁLISIS

Engaño del CAPTCHA: Una vez en la página falsa, se pide al usuario que complete un CAPTCHA; sin embargo, al hacer clic en "No soy un robot", se copia un script malicioso en el portapapeles del usuario.
Ejecución del Script: Los atacantes instruyen a las víctimas para ejecutar el script, lo que desencadena la descarga e instalación del **malware Lumma Stealer**.
Instalación del Malware: El script descargado, se encuentra altamente resguardado para evadir la detección y se instala en la carpeta Temp del Sistema.

IMPACTO PARA COLOMBIA Y LA REGIÓN

La campaña de malware que utiliza engaños de CAPTCHA para distribuir Lumma Stealer tiene un impacto considerable en América Latina, aumentando el riesgo de robo de datos personales y financieros. Esto podría afectar la confianza del consumidor en el comercio electrónico y los servicios bancarios en línea.

NIVEL DE RIESGO

MEDIO

FUENTES:

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/behind-the-captcha-a-clever-gateway-of-malware/
https://www.infosecurity-magazine.com/news/malicious-ads-infostealer-league/
https://www.infosecurity-magazine.com/news/lumma-new-anti-sandbox-method/

COLCERT