Se ha observado una nueva campaña que aprovecha un kit de explotación abusando de una falla de Internet Explorer parcheada por Microsoft el año pasado para entregar el troyano RedLine Stealer.

> *«Cuando se ejecuta, RedLine Stealer realiza un reconocimiento contra el sistema de destino (incluido el nombre de usuario, el hardware, los navegadores instalados, software antivirus) y luego filtra los datos (incluidas las contraseñas, tarjetas de crédito guardadas, las billeteras criptográficas, los inicios de sesión de VPN) a un servidor de mando y control remoto»,* dijo Bitdefender.

La mayoría de las infecciones se localizan en Brasil y Alemania, seguidos están Estados Unidos, Egipto, Canadá, China, Polonia, entre otros.

Los kits de explotación o los paquetes de explotación son herramientas integrales que contienen una colección de vulnerabilidades diseñadas para aprovechar las vulnerabilidades del software de uso común al escanear los sistemas infectados en busca de distintos tipos de fallas, e implementar malware adicional.

El principal método de infección utilizado por los hackers para distribuir kits de explotación, en este caso el kit de explotación RIG, es por medio de sitios web comprometidos que, al ser visitados, sueltan el código de explotación para finalmente enviar la carga útil de RedLine Stealer para llevar a cabo ataques de seguimiento.

La vulnerabilidad en cuestión es CVE-2021-26411 (puntuación CVSS: 8.8), una vulnerabilidad de corrupción de memoria que afecta a Internet Explorer y que ha sido armada previamente por atacantes vinculados a Corea del Norte. Microsoft lo abordó como parte de sus actualizaciones de Patch Tuesday para marzo de 2021.

> *«La muestra de RedLine Stealer entregada por RIG EK viene empaquetada en múltiples capas de encriptación para evitar la detección»,* dijo la compañía de

> seguridad.

RedLine Stealer, un malware que roba información que se vende en foros clandestinos, cuenta con funciones para filtrar contraseñas, cookies y datos de tarjetas de crédito guardados en los navegadores, así como billeteras criptográficas, registros de chat, credenciales de inicio de sesión de VPN y texto de archivos según los comandos recibidos de un servidor remoto.

Está lejos de ser la única campaña que implica la distribución de RedLine Stealer. En febrero de 2022, HP detalló un ataque de ingeniería social utilizando instaladores de actualización de Windows 11 falsos para engañar a los usuarios de Windows 10 para que descarguen y ejecuten el malware.