La vulnerabilidad de día cero de Google Chrome, explotada activamente pero ya corregida, que se dio a conocer a inicios de julio, fue armada por una compañía israelí de spyware y utilizada en ataques dirigidos a periodistas en el Medio Oriente.

La compañía checa de ciberseguridad Avast, vinculó la explotación a Candiru (también conocido como Saito Tech), que tiene un historial de aprovechar vulnerabilidades previamente desconocidas para implementar un malware de Windows denominado Devils Tongue, un implante modular con capacidades similares a Pegasus.

Candiru, junto con NSO Group, Computer Security Initiative Consultancy PTE. LTD. y Positive Technologies, fueron agregados a la lista de entidades por el Departamento de Comercio de Estados Unidos en noviembre de 2021 por participar en *«actividades cibernéticas maliciosas».*

> *«Específicamente, una gran parte de los ataques tuvo lugar en Líbano, donde los periodistas se encontraban entre los objetivos. Creemos que los ataques fueron altamente dirigidos»*, dijo el investigador de seguridad Jan Vojtesek.

La vulnerabilidad se rastrea como CVE-2022-2294, y se refiere a una corrupción de memoria en le componente WebRTC del navegador Google Chrome, que podría conducir a la ejecución de shellcode. Google la abordó el 4 de julio de 2022. Desde entonces, Apple y Microsoft solucionaron el mismo problema en los navegadores Safari y Edge.

Los hallazgos alertan sobre múltiples campañas de ataque montadas por el proveedor israelí de hacking, que se dice que regresó con un conjunto de herramientas renovado en marzo de 2022 para apuntar a usuarios en el Líbano, Turquía, Yemen y Palestina a través de ataques de abrevadero usando exploits de día cero para Google Chrome.

La secuencia de infección detectada en el Líbano comenzó cuando los atacantes comprometieron un sitio web utilizado por los empleados de una agencia de noticias para inyectar código JavaScript malicioso desde un dominio controlado por un atacante que es

responsable de redirigir a las víctimas potenciales a un servidor de explotación.

Por medio de esta técnica de abrevadero, se crea un perfil del navegador de la víctima, que consta de unos 50 puntos de datos, incluyendo detalles como el idioma, zona horaria, información de la pantalla, tipo de dispositivo, los complementos del navegador, la referencia y la memoria del dispositivo, entre otros.

Avast evaluó que se recopiló la información para garantizar que el exploit se entregara solo a los objetivos previstos. Si los hackers consideran valiosos los datos recopilados, el exploit de día cero se entrega a la máquina de la víctima por medio de un canal encriptado.

El exploit, a su vez, abusa del desbordamiento del búfer del montón en WebRTC para lograr la ejecución del shellcode. Se cree que la falla de día cero se encadenó con un exploit de escape de sandbox (que nunca se recuperó) para obtener un punto de apoyo inicial, usándolo para soltar la carga útil de Devils Tongue.

Aunque el malware sofisticado es capaz de grabar la cámara web y el micrófono de la víctima, el registro de teclas, la filtración de mensajes, el historial de navegación, las contraseñas, las ubicaciones y mucho más, también se ha observado que intenta escalar sus privilegios mediante la instalación de un controlador de kernel firmado vulnerable («HW.sys«) que contiene un tercer exploit de día cero.

A inicios de enero, ESET explicó cómo los controladores de kernel firmados vulnerables, un enfoque llamado Bring Your Own Vulnerable Driver (BYOVD), pueden convertirse en puertas de enlace no protegidas para que los atacantes obtengan acceso arraigado a las máquinas con Windows.

La divulgación se produce una semana después de que Proofpoint revelara que los grupos de hacking de estados nacionales alineados con China, Irán, Corea del Norte y Turquía, han estado atacando a periodistas para realizar espionaje y propagar malware desde principios de 2021.