El malware SmokeLoader se está empleando para transportar un nuevo tipo de malware denominado Whiffy Recon, el cual se encarga de efectuar un rastreo de redes Wi-Fi en máquinas con Windows que han sido comprometidas.

> *«Esta nueva cepa de malware tiene una única operación. Cada 60 segundos, triangula la ubicación de los sistemas infectados al explorar los puntos de acceso Wi-Fi cercanos como un punto de datos para la API de geolocalización de Google. La ubicación proporcionada por la API de Geolocalización de Google se envía de regreso al atacante»,* afirmó el equipo de la Unidad de Contraamenazas de Secureworks (CTU, por sus siglas en inglés) en un comunicado.

SmokeLoader, tal como sugiere su nombre, es un malware de carga cuyo único propósito es introducir cargas adicionales en un anfitrión. Desde 2014, este malware ha estado disponible para actores de amenazas con base en Rusia. Tradicionalmente, se distribuye a través de correos electrónicos de phishing.

Whiffy Recon funciona revisando si el servicio de Configuración Automática de WLAN (WLANSVC) está presente en el sistema infectado y se autoanula si el nombre del servicio no existe. Vale la pena señalar que el escáner no verifica si está en funcionamiento.

La persistencia se logra mediante un acceso directo que se agrega a la carpeta de Inicio de Windows.

> *«Lo que resulta inquietante en nuestro descubrimiento de Whiffy Recon es que no está claro cuál es la motivación detrás de su funcionamiento»,* comentó Don Smith, Vicepresidente de Inteligencia de Amenazas de Secureworks CTU.

> *«¿Quién o qué está interesado en conocer la ubicación real de un dispositivo*

> *infectado? La regularidad del escaneo cada 60 segundos es inusual, ¿por qué actualizarse cada minuto? Con este tipo de datos, un actor de amenazas podría construir una imagen de la geolocalización de un dispositivo, vinculando lo digital con lo físico».*

El malware también está configurado para registrarse en un servidor de comando y control (C2) remoto al enviar un *«botID»* generado al azar en una solicitud POST HTTP, tras lo cual, el servidor responde con un mensaje de éxito y un identificador único secreto que se guarda posteriormente en un archivo llamado *«%APPDATA%\Roaming\wlan\str-12.bin».*

La segunda fase del ataque implica rastrear puntos de acceso Wi-Fi mediante la API de WLAN de Windows cada 60 segundos. Los resultados de este rastreo se envían a la API de Geolocalización de Google para determinar la ubicación del sistema y, finalmente, transmitir esa información al servidor C2 en forma de una cadena JSON.

> *«Este tipo de actividad/capacidad rara vez es utilizada por actores delictivos. Como capacidad autónoma, carece de la habilidad de monetizarse rápidamente. Las incógnitas aquí son preocupantes y la realidad es que podría utilizarse para respaldar cualquier número de motivaciones maliciosas»*, añadió Smith.