Se ha observado a los hackers asociados con la campaña de hacking Roaming Mantis, entregando una variante actualizada de su malware móvil patentado conocido como Wroba, con el fin de infiltrarse en los routers WiFi y realizar el secuestro del Sistema de Nombres de Dominio (DNS).

Kaspersky, que llevó a cabo un análisis del malware, dijo que la función está diseñada para apuntar a routers WiFi específicos ubicados en Corea del Sur.

Roaming Mantis, también conocido como Shaoye, es una operación de motivación financiera de larga duración que selecciona a los usuarios de smartphones Android mediante malware capaz de robar credenciales de cuentas bancarias y recopilar otros tipos de información confidencial.

Aunque se centró principalmente en la región asiática desde 2018, se detectó que el equipo de hacking expandía su rango de víctimas para incluir a Francia y Alemania por primera vez a inicios de 2022 al camuflar el malware como la aplicación del navegador web Google Chrome.

Los ataques aprovechan los mensajes de smishing como el vector de intrusión inicial de elección para entregar una URL trampa que ofrece un APK malicioso o redirige a la víctima a páginas de phishing basadas en el sistema operativo instalado en los dispositivos móviles.

De forma alterna, algunos compromisos también han aprovechado los routers de WiFi como un medio para llevar a los usuarios desprevenidos a una página de destino falsa mediante el uso de una técnica llamada secuestro de DNS, en la que las consultas de DNS se manipulan para redirigir a los objetivos a sitios falsos.

Independientemente del método usado, las intrusiones allanan el camino para la implementación de un malware denominado Wroba (también conocido como MoqHao y

XLoader) que está equipado para realizar una gran cantidad de actividades maliciosas.

La última actualización de Wroba, según la compañía rusa de seguridad cibernética, incluye una función de cambio de DNS que está diseñada para detectar ciertos routers en función de sus números de modelo y envenenar su configuración de DNS.

> *«La nueva funcionalidad de cambiador de DNS puede administrar todas las comunicaciones de los dispositivos que usan el router WiFi comprometido, como redirigir a hosts maliciosos y deshabilitar las actualizaciones de los productos de seguridad»*, dijo el investigador de Kaspersky, Suguru Ishimaru.

La idea subyacente es hacer que ls dispositivos conectados al router WiFi violado sean redirigidos a páginas web controladas por el hacker para una mayor explotación. Debido a que algunas de estas páginas entregan el malware Wroba, la cadena de ataque crea efectivamente un flujo constante de «bots» que pueden convertirse en armas para entrar en routers WiFi saludables.

Es notable que el programa de cambio de DNS se use exclusivamente en Corea del Sur. Sin embargo, el malware Wroba en sí mismo ha sido detectado atacando a víctimas en Austria, Francia, Alemania, India, Japón, Malasia, Taiwán, Turquía y Estados Unidos a través de smishing.

Wroba está lejos de ser el único malware móvil existente con funciones de secuestro de DNS. En 2016, Kaspersky desenmascaró otro troyano de Android con nombre en código Switcher que ataca el router inalámbrico a cuya red está conectado el dispositivo infectado y realiza un ataque de fuerza bruta con el objetivo de alterar las configuraciones de DNS.

> *«Los usuarios con dispositivos Android infectados que se conectan a redes WiFi gratuitas o públicas pueden propagar el malware a otros dispositivos en la red si la red WiFi a la que están conectados es vulnerable»*, dijo el investigador.