Un troyano de acceso remoto nunca antes visto, denominado ZuoRAT, ha estado seleccionando routers de oficinas pequeñas y oficinas domésticas (SOHO) como parte de una campaña sofisticada dirigida a las redes de América del Norte y Europa.

El malware *«otorga al actor la capacidad de pivotar en la red local y obtener acceso a sistemas adicionales en la LAN secuestrando las comunicaciones de la red para mantener un punto de apoyo no detectado»,* dijeron los investigadores de Lumen Black Lotus.

Al parecer, la operación que apuntó a los routers de ASUS, Cisco, Draytek y Netgear, comenzó a inicios de 2020 durante los meses iniciales de la pandemia de COVID-19, permaneciendo efectivamente bajo el radar por más de dos años.

> *«Los consumidores y los empleados remotos usan rutinariamente routers SOHO, pero estos dispositivos rara vez son monitoreados o parcheados, lo que los convierte en uno de los puntos más débiles de perímetro de una red»,* dijo el equipo de inteligencia de amenazas de la compañía.

El acceso inicial a los enrutadores se obtiene al escanear en busca de fallas conocidas sin parches, para cargar la herramienta de acceso remoto, usándola para obtener acceso a la red y soltar un cargador de shellcode de próxima etapa, que se utiliza para entregar Cobalt Strike y backdoors personalizadas como CBeacon y GoBeacon, que son capaces de ejecutar comandos arbitrarios.

Además de permitir el reconocimiento en profundidad de las redes de destino, la recopilación de tráfico y el secuestro de comunicaciones de red, el malware se ha descrito como una versión muy modificada de la botnet Mirai, cuyo código fuente se filtró en octubre de 2016.

> *«ZuoRAT es un archivo MIPS compilado para routers SOHO que puede enumerar un host y una LAN interna, capturar paquetes que se transmiten por medio del dispositivo infectado y realizar ataques de persona en el medio (secuestro de DNS y HTTPS basado en reglas predefinidas)»,* dijeron los investigadores.

También se incluye una función para recolectar conexiones TCP por medio de los puertos 21 y 8443, que están asociados con FTP y navegación web, lo que podría permitir al adversario controlar la ac
actividad de Internet de los usuarios detrás del router comprometido.

Otras capacidades de ZuoRAT permiten a los atacantes monitorear el tráfico DNS y HTTPS con el objetivo de secuestrar las solicitudes y redirigir a las víctimas a dominios maliciosos utilizando reglas preestablecidas que se generan y almacenan en directorios temporales en un intento de resistir el análisis forense.

Ese no es el único paso que toman los hackers para ocultar sus actividades, ya que los ataques se basan en una infraestructura C2 ofuscada de varias etapas que implica utilizar un servidor privado virtual para eliminar el exploit RAT inicial y aprovechar los routers comprometidos como servidores proxy C2.

Para evitar aún más la detección, se detectó que el servidor de prueba aloja contenido aparentemente inocuo, en un caso imitando un sitio web llamado «muhsinlar.net», un portal de propaganda creado para el Partido Islámico de Turkestán (TIP), un equipo extremista uigur originario de China.

Se desconoce la identidad del colectivo adversario detrás de la campaña, aunque un análisis de los artefactos reveló posibles referencias a la provincia china de Xiancheng y el uso de yuque y Tencent de Alibaba para comando y control (C2).

La naturaleza elaborada y evasiva de la operación junto con las tácticas utilizadas en los ataques para permanecer encubierto apuntan hacia una posible actividad del estado-nación,

dijo Black Lotus Labs.

> *«Las capacidades demostradas en esta campaña: obtener acceso a dispositivo SOHO de diferentes marcas y modelos, recopilar información de host y LAN para informar la orientación, el muestreo y el secuestro de comunicaciones de red para obtener un acceso potencialmente persistente a dispositivos en tierra y robar intencionalmente la infraestructura C2 aprovechando múltiples etapas de comunicaciones en silos de router a router, esto apunta a un actor altamente sofisticado»*, agregaron los investigadores.