Un malware complejo nunca antes visto apunta a routers de nivel empresarial para espiar de forma encubierta a las víctimas en América Latina, Europa y América del Norte, al menos desde julio de 2022.

Se descubrió que la campaña, denominada Hiatus por Lumen Black Lotus Labs, implementa dos binarios maliciosos, un troyano de acceso remoto denominado Hiatus RAT y una variante de tcpdump que hace posible la captura de paquetes en el dispositivo de destino.

> *«Una vez que un sistema objetivo está infectado, HiatusRAT permite que el actor de amenazas interactúa de forma remota con el sistema y utiliza una funcionalidad preconstruida para convertir la máquina comprometida en un proxy encubierto para el actor de amenazas»,* dijo la compañía en un comunicado.

> *«El binario de captura de paquetes permite al actor monitorear el tráfico del router en los puertos asociados con las comunicaciones de transferencia de archivos y correo electrónico».*

El grupo de amenazas destaca principalmente los modelos del router DrayTek Vigor al final de su vida útil (EoL) 2960 y 3900, con aproximadamente 100 dispositivos expuestos a Internet comprometidos a mediados de febrero de 2023. Algunas de las industrias verticales afectadas incluyen productos farmacéuticos, servicios de TI/consultoría, empresas y gobierno municipal, entre otros.

De forma curiosa, esto representa solo una pequeña fracción de los 4100 routers DrayTek 2960 y 3900 a los que se puede acceder públicamente a través de Internet, lo que plantea la posibilidad de que *«el actor de la amenaza esté manteniendo intencionalmente una huella mínima para limitar su exposición».*

Debido a que los dispositivos afectados son routers de gran ancho de banda que pueden

admitir simultáneamente cientos de conexiones VPN, se sospecha que el objetivo es espiar a los objetivos y establecer una red proxy sigilosa.

> *«Estos dispositivos generalmente viven fuera del perímetro de seguridad tradicional, lo que significa que generalmente no se monitorean ni actualizan. Esto ayuda al actor a establecer y mantener la persistencia a largo plazo sin ser detectado»,* dijo Mark Dehus, director de inteligencia de amenazas de Lumen Black Lotus Labs.

Se desconoce el vector de acceso inicial exacto usado en los ataques, pero una violación exitosa es seguida por la implementación de un script bash que descarga y ejecuta HiatusRAT y un binario de captura de paquetes.

HiausRAT tiene muchas funciones y puede recopilar información del router, ejecutar procesos y comunicarse con un servidor remoto para obtener archivos o ejecutar comandos arbitrarios. También es capaz de transmitir tráfico de comando y control (C2) por medio del router.

El uso de routers comprometidos como infraestructura de proxy es probablemente un intento de ofuscar las operaciones de C2, dijeron los investigadores.

Los hallazgos llegan más de seis meses después de que Lumen Black Lotus Labs también arrojara luz sobre una campaña de malware no relacionada centrada en el router que usaba un nuevo troyano llamado ZuoRAT.

> *«El descubrimiento de Hiatus confirma que los atacantes continúan buscando la explotación del router. Estas campañas demuestran la necesidad de proteger el ecosistema de routers, y los routers deben monitorearse, reiniciarse y actualizarse regularmente, mientras que los dispositivos al final de su vida útil deben*

> *reemplazarse»,* dijo Dehus.