Una botnet recientemente descubierta capaz de organizar ataques distribuidos de denegación de servicio (DDoS), se dirigió a los dispositivos EdgeMarc de Ribbon Communications (antes Edgewater Networks) sin parches, pertenecientes al proveedor de servicios de telecomunicaciones AT&T mediante la explotación de una vulnerabilidad de cuatro años en los dispositivos red.

La división de seguridad de red Netlab de la compañía china Qihoo 360, que detectó la botnet por primera vez el 27 de octubre de 2021, la llamó EwDoor y dijo que observó 5700 direcciones IP comprometidas ubicadas en Estados Unidos durante un breve período de tres horas.

> *«Hasta ahora, en nuestra opinión, EwDoor se ha sometido a tres versiones de actualizaciones, y sus funciones principales se pueden resumir en dos categorías principales de ataques DDoS y puerta trasera. Teniendo en cuenta que los dispositivos atacados están relacionados con la comunicación telefónica, suponemos que su objetivo principal son los ataques DDoS y la recopilación de información confidencial, como registros de llamadas»*, dijeron los investigadores.

Al propagarse por medio de una falla en los dispositivos EdgeMarc, EwDoor admite una variedad de características, incluyendo la capacidad de auto actualizarse, descargar archivos, obtener un shell inverso en la máquina comprometida y ejecutar cargas útiles arbitrarias.

La vulnerabilidad en cuestión es CVE-2017-6079, con puntuación CVSS de 9.8, una falla de inyección de comando que afecta a los controladores de borde de sesión que podrían ser armados para ejecutar comandos maliciosos.

Además de recopilar información sobre el sistema afectado, EwDoor también establece

comunicaciones con un servidor de comando y control remoto (C2), ya sea directa o indirectamente utilizando BitTorrent Trackers para obtener la dirección IP del servidor C2, a la espera de más comandos emitidos por los atacantes.

> *«Identificamos previamente este problema, tomamos medidas para mitigarlo y seguimos investigando, no tenemos evidencia de que se haya accedido a los datos de los clientes»,* dijo AT&T.