Una nueva campaña de malware incipiente que incorpora dispositivos Android a una botnet con el objetivo principal de realizar ataques distribuidos de denegación de servicio (DDoS) ha sido detectada.

Llamada Matryosh por investigadores de Netlab, de Qihoo 360, la amenaza se ha encontrado reutilizando el marco de la botnet Mirai y se propaga por medio de las interfaces expuestas de Android Debug Bridge (ADB) para infectar dispositivos Android y atraparlos en su red.

ADB es una herramienta de línea de comandos que forma parte del SDK de Android que maneja las comunicaciones y permite a los desarrolladores instalar y depurar aplicaciones en dispositivos Android.

Aunque esta opción está desactivada de forma predeterminada en la mayoría de los teléfonos inteligentes y tabletas Android, algunos proveedores se envían con esta función habilitada, lo que permite a los atacantes no autenticados conectarse remotamente a través del puerto 5555 TCP y abrir los dispositivos directamente para su explotación.

En julio de 2018, se utilizaron puertos ADB abiertos para difundir múltiples variantes de botnet de Satori, incluido Fbot, y un año después, se descubrió un nuevo malware de botnet de minería de criptomonedas, que hizo avances utilizando la misma interfaz para apuntar a usuarios de dispositivos Android en Corea, Taiwán, Hong Kong y China.

Pero lo que destaca de Matryosh es que utiliza Tor para enmascarar su actividad maliciosa y canalizar los comandos de un servidor controlado por un atacante a través de la red.

> *«El proceso de obtención de C2 está anidado en capas, como muñecos de anidación rusos»*, dijeron los investigadores de Netlab.

Para esto, Matryosh primero descifra el nombre de host remoto y usa la solicitud DNS TXT, un tipo de registro de recursos, para obtener TOR C2 y TOR Proxy. Luego, establece una conexión con el proxy TOR, y se comunica con el servidor TOR C2 a través del proxy, y espera más instrucciones del servidor.

Los investigadores de Netlab dijeron que el formato de comando de la botnet emergente y su uso de TOR C2 son muy similares a los de la botnet LeetHozer desarrollada por el grupo Moobot.

> *«Basándonos en estas consideraciones, especulamos que Matryosh es el nuevo trabajo de este grupo de padres»*, dijeron los investigadores.