Una nueva variante de la botnet de IoT, BotenaGo, ha surgido específicamente señalando los dispositivos DVR con cámara de seguridad Lilin para infectarlos con el malware Mirai.

Apodado como Lilin Scanner, por Nozomi Networks, la última versión está diseñada para explotar una vulnerabilidad de inyección de comando crítica de dos años en el firmware del DVR que fue reparada por la compañía taiwanesa en febrero de 2020.

BotenaGo, documentado por primera vez en noviembre de 2021 por AT&T Alien Labs, está escrito en Golang y presenta más de 30 exploits para vulnerabilidades conocidas en servidores web, enrutadores y otros tipos de dispositivos IoT.

Desde entonces, el código fuente de la red de bots se ha subido a GitHub, por lo que está listo para el abuso por parte de otros atacantes.

«Con solo 2891 líneas de código, BotenaGo tiene el potencial de ser el punto de partida para muchas nuevas variantes y nuevas familias de malware que utilizan su código fuente», dijeron los investigadores.

El nuevo malware BotenaGo es el último en explotar vulnerabilidades en los dispositivos Lilin DVR luego de Chalubo, Fbot y Moobot. A inicios del mes, el Laboratorio de Investigación de Seguridad de Redes de Qihoo 360 (360 Netlab) detalló una botnet DDoS de rápida expansión llamada Fodcha que se propaga por medio de varias vulnerabilidades N-Day, incluida la de Lilin y contraseñas Telnet/SSH débiles.

Un aspecto crucial que distingue a Lilin Scanner de BotenaGo es su dependencia de un programa externo para crear una lista de direcciones IP de dispositivos Lilin vulnerables, y luego explotar la falla antes mencionada para ejecutar código arbitrario de forma remota en el objetivo e implementar cargas útiles de Mirai.

Cabe mencionar que el malware no puede propagarse como un gusano y solo puede utilizarse para atacar las direcciones IP proporcionadas como entrada con los binarios de Mirai.

> *«Otro comportamiento asociado con la botnet Mirai es la exclusión de rangos de IP pertenecientes a las redes internas del Departamento de Defensa de Estados Unidos (DoD), el Servicio Postal de Estados Unidos (USPS), General Electric (GE), Hewlett-Packard (HP) y otros»,* dijeron los investigadores.

Al igual que Mirai, la aparición de Lilin Scanner apunta a la reutilización del código fuente fácilmente disponible para generar nuevas ramificaciones de malware.

> *«Sus autores eliminaron casi todos los más de 30 exploits presentes en el código fuente original de BotenaGo. Parece que esta herramienta se ha creado rápidamente utilizando el código base del malware BotenaGo»,* agregaron los investigadores.