Una investigación de ciberseguridad reveló los detalles de una nueva botnet que secuestra dispositivos inteligentes conectados a Internet con el fin de realizar ciertas tareas para los hackers, principalmente ataques DDoS y minería de criptomonedas.

La botnet HEH, descubierta por Netlab, de Qihoo 360, está escrita en lenguaje Go y se desarrolló con un protocolo peer-to-peer (P2P) patentado, se propaga mediante un ataque de fuerza bruta del servicio Telnet en los puertos 23/2323 y permite ejecutar comandos de shell arbitrarios.

Los investigadores dijeron que las muestras de botnet HEH descubiertas hasta ahora admiten una gran variedad de arquitecturas de CPU, incluidas x86 (32/64), ARM (32/64), MIPS (MIPS32/MIPSIII) y PowerPC (PPC).

Aunque la botnet está en sus primeras etapas de desarrollo, cuenta con tres módulos funcionales: un módulo de propagación, un módulo de servicio HTTP local y un módulo P2P.

Inicialmente descargado y ejecutado por un script de Shell malicioso llamado «wpqnbw.txt«, el ejemplo HEH utiliza el script de Shell para descargar programas fraudulentos para todas las diferentes arquitecturas de CPU desde un sitio web («pomf.cat«), antes de terminar con procesos de servicio basados en sus números de puerto.

La segunda fase comienza con la muestra HEH iniciando un servidor HTTP que muestra la Declaración Universal de Derechos Humanos en ocho idiomas distintos, y luego inicializa un módulo P2P que realiza un seguimiento de los pares infectados y permite al atacante ejecutar comandos de shell arbitrarios, incluida la capacidad para borrar todos los datos del dispositivo comprometido activando un comando de autodestrucción.

Otros comandos hacen posible reiniciar un bot, actualizar la lista de pares y salir del bot en ejecución actual, aunque los autores de la red de bots no implementaron aún un comando de

«ataque».

> *«Después de que el bot ejecute el módulo P2P, ejecutará la tarea de fuerza bruta contra el servicio Telnet para los dos puertos 23 y 2323 de forma paralela, y luego completará su propia propagación»,* dijeron los investigadores.

En otras palabras, si el servicio Telnet se abre en el puerto 23 o 2323, intenta un ataque de fuerza bruta utilizando un diccionario de contraseñas que consta de 171 nombres de usuario y 504 contraseñas. En un robo exitoso, la víctima infectada se agrega a la botnet, magnificando así su tamaño.

> *«El mecanismo operativo de esta botnet aún no está maduro, y algunas funciones importantes como el módulo de ataque aún no se han implementado. Dicho esto, la estructura P2P nueva y en desarrollo, el soporte de arquitectura de CPU múltiple, la función de autodestrucción incorporada, hacen que esta botnet sea potencialmente peligrosa.»*, dijeron los investigadores.