Se encontró una nueva variante de la botnet Mirai, que aprovecha varias vulnerabilidades de seguridad para propagarse a dispositivos Linux e IoT.

Observada durante la segunda mitad de 2022, la nueva versión ha sido denominada V3G4 por Unit 42 de Palo Alto Networks, que identificó tres campañas distintas probablemente realizadas por el mismo atacante.

> *«Una vez que los dispositivos vulnerables se vean comprometidos, los atacantes los controlarán por completo y se convertirán en parte de la botnet. El actor de amenazas tiene la capacidad de utilizar esos dispositivos para realizar más ataques, como ataques distribuidos de denegación de servicio (DDoS)»,* dijeron los investigadores de Unit42.

Los ataques se centran principalmente en servidores expuestos y dispositivos de red que ejecutan Linux, y el adversario usa hasta 13 vulnerabilidades que podrían conducir a la ejecución remota de código (RCE).

Algunas de las vulnerabilidades más notables se relacionaron con fallas críticas en Atlassian Confluence Server and Data Center, rouers Dray Tek Vigor, Airspan AirSpot y cámaras IP Geutebruck, entre otros. La vulnerabilidad más antigua de la lista es CVE-2012-4869, un error RCE en FreePBX.

Después de un compromiso exitoso, la carga útil de la botnet se recupera de un servidor remoto usando las utilidades wget y cURL.

La botnet, además de verificar si ya se está ejecutando en la máquina infectada, también toma medidas para eliminar otras botnets de la competencia, como Mozi, Okami y Yakuza.

V3G4 incluye además un conjunto de credenciales de inicio de sesión débiles o

predeterminadas que usa para realizar ataques de fuerza bruta a través de Telnet/SSH y propagarse a otras máquinas.

También establece contacto con un servidor de comando y control para esperar comandos para lanzar ataques DDoS contra objetivos a través de los protocolos UDP, TCP y HTTP.

> *«Las vulnerabilidades mencionadas anteriormente tienen menos complejidad de ataque que las variantes observadas antes, pero mantienen un impacto de seguridad crítico que puede conducir a la ejecución remota de código»,* dijeron los investigadores.

Para evitar este tipo de ataques, se recomienda que los usuarios apliquen los parches y actualizaciones necesarios a medida que sean aplicables, y aseguren los dispositivos con contraseñas seguras.