Investigadores del equipo de seguridad Netlab de Qihoo 360 publicaron los detalles de una nueva botnet en evolución llamada Abcbot, que se ha observado en la naturaleza con funciones de propagación similares a gusanos para infectar sistemas Linux y lanzar ataques distribuidos de denegación de servicio (DDoS) contra objetivos.

Aunque la primera versión de la botnet se remonta a julio de 2021, las nuevas variantes observadas tan recientemente como el 30 de octubre, fueron equipadas con actualizaciones adicionales para atacar servidores web Linux con contraseñas débiles y son susceptibles a vulnerabilidades de N días, incluida una implementación personalizada de funcionalidad DDoS, lo que indica que el malware se encuentra en continuo desarrollo.

Los hallazgos de Netlab también se basan en un informe de Trend Micro a inicios del mes pasado, que publicitó los ataques dirigidos a Huawei Cloud con malware de minería de criptomonedas y cryptojacking. Las intrusiones también fueron notables por el hecho de que los scripts de shell maliciosos deshabilitaron específicamente un proceso diseñado para monitorear y escanear los servidores en busca de problemas de seguridad, así como restablecer las contraseñas de los usuarios al servicio de nube elástica.

Según la compañía china de seguridad, estos scripts de shell se están utilizando para difundir Abcbot. Hasta ahora, se han observado un total de seis versiones de la botnet.

Una vez instalado en un host comprometido, el malware desencadena la ejecución de una serie de pasos que dan como resultado que el dispositivo infectado se reutilice como servidor web, además de enviar la información del sistema a un servidor de comando y control (C2), propagándose el malware a nuevos dispositivos mediante la búsqueda de puertos abiertos y la actualización automática a medida que sus operadores ponen a disposición nuevas funciones.

> *«Lo interesante es que la muestra del 21 de octubre, utiliza el ATK Rootkit de código abierto para implementar la función DDoS, un mecanismo que requiere que Abcbot descargue el código fuente, compile y cargue el módulo rootkit antes realizando un ataque DDoS»,* dijeron los investigadores.

«Este proceso requiere demasiados pasos, y cualquier paso que sea defectuoso dará como resultado la falla de la función DDoS», agregaron. Esto llevó al adversario a reemplazar el componente estándar con un módulo de ataque personalizado en una versión posterior lanzada el 30 de octubre, que abandona por completo el rootkit ATK.

Los hallazgos se producen poco más de una semana después de que el equipo de seguridad de Netlab revelara los detalles de una botnet «Pink» que se cree que infectó a más de 1.6 millones de dispositivos ubicados principalmente en China, con el objetivo de lanzar ataques DDoS e insertar anuncios en sitios web HTTP visitados por usuarios desprevenidos.

> *«El proceso de actualización en estos seis meses no es tanto una actualización continua de funciones como una compensación entre diferentes tecnologías. Abcbot está pasando lentamente de la infancia a la madurez. No consideramos que esta etapa sea la forma final, obviamente hay muchas áreas de mejora o características por desarrollar en esta etapa»,* dijeron los desarrolladores.