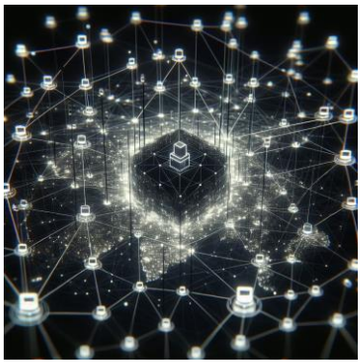
ALERTA

Botnet que compromete enrutadores y dispositivos IoT

COLCERT AL-1810-052

TLP:CLEAR



Se ha sido identificado una botnet compuesta por más de 260,000 dispositivos, que utiliza una variante del malware Mirai, para secuestrar dispositivos IoT y sumarlos a la red de Bot, desde infraestructuras en América del Norte, Europa, África y el Sudeste Asiático y lanzar ataques cibernéticos disruptivos a gran escala.

ELEMENTOS DE INTELIGENCIA DISPONIBLES

Se han identificado más de 80 subdominios (W8510.com) asociados con los servidores de comando y control (C2) del botnet, lo que proporciona indicadores de compromiso críticos para la detección y mitigación de amenazas. Las recomendaciones incluyen la aplicación regular de parches, la desactivación de servicios no utilizados, supervisión de tráfico y la implementación de segmentación de red. (Ver Apéndice A: IoC- Documento Fuente)

ANÁLISIS

Para vincular un nuevo "bot", el sistema de la botnet primero vulnera un dis positivo conectado a Internet, utilizando vulnerabilidades conocidas (Ver Apéndice B: CVE - Documento Fuente), después de vulnerado, el dispositivo ejecuta una carga útil del malware Mirai, desde un servidor remoto, posteriormente inicia el proceso para establecer conexión con el servidor de comando y control (C2), mediante TLS puerto 443, y realizar ataques de DDoS desde los dispositivos infectados y de explotación para hacer crecer la red de “bot”.

IMPACTO PARA COLOMBIA Y LA REGIÓN

Aunque las informaciones no menciona específicamente un impacto directo en la región LATAM, la naturaleza global del botnet sugiere que las organizaciones en esta región deben estar alertas y aplicar las medidas de mitigación recomendadas para proteger sus redes y dispositivos de posibles compromisos.

NIVEL DE RIESGO

MEDIO

FUENTES:

https://media.defense.gov/2024/Sep/18/2003547016/-1/-1/1/CSA-PRC-LINKED-ACTORS-BOTNET.PDF

COLCERT