MIRAI (MALWARE)

nueva versión que realiza ataques DDoS usando los IoT de empresas

Imágenes tomadas de: https://pixabay.com, flaticon.com

¿Qué es MIRAI?

Malware de la familia de las botnets, que mediante la infección de equipos IoT (Equipos de internet de las cosas), los usa como esclavos Para la realización de ataques de denegación de servicio distribuido.

El código fuente de MIRAI es abierto, lo que ha permitido la aparición de nuevas variantes con objetivos específicos.

¿Cómo infecta los equipos?

Por medio de la realización de escaneos de equipos IoT conectados a internet, identifica aquellos que se encuentran con las credenciales de fábrica ingresando e instalándose sobre el sistema.

Según kaspersky las diferentes variantes que se encuentran distribuidas en internet, son responsables del 21% del ataque tipo bootnet que se registraron durante el año 2018.

Las nuevas adaptaciones realizadas por los delincuentes le permiten llegar a infectar equipos de nivel corporativo incorporando bajo su control nuevos dispositivos inalámbricos como paneles de publicidad, TV, cámaras de red, enrutadores, etc.

Lo anterior permite inferir un alto índice de probabilidad de que los equipos industriales IoT sean incluidos en nuevas versiones del malware.

Durante el primer trimestre de 2019, los ataque de DDoS aumentaron en un 84% al igual que la duración de los ataques en un 4,21 veces, y en los extras prolongados hasta un 487%, este aumento puede estar relacionado con una creciente demanda de esta clase de servicios y la aparición de nuevos proveedores.

¿Cómo protegerse?

- Cambiar las credenciales de fábrica de los equipos IoT (Cámaras, ruoters, swicht, pantallas etc.)

- Usar contraseñas robustas con combinaciones alfanuméricas.

- Descargar actualizaciones de aplicaciones y sistemas desde los sitios oficiales. Actualizar la base de datos su antivirus.

- No dar clic sobre urls o descargar archivos adjuntos que se encuentren en correos electrónicos de dudosa procedencia.

- Estar atento a la cantidad de trafico de red que genera cada equipo.

- Si sospecha de un equipo infectado reinícielo a su estado de fábrica y reconfigure sus credenciales de seguridad.

Ante cualquier situación contáctenos en:

@caivirtual

caivirtual@policia.gov.co

(1) 5159727.

Fuentes: securelist.lat, kaspersky.ru