Contacto: seguridad@etb.net.co
www.etb.co

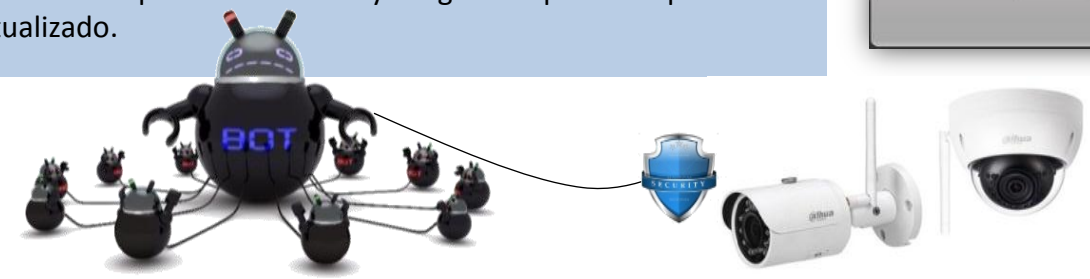
Boletín de seguridad CSIRT

Debido a la proliferación de cámaras y DVR expuestos en Internet para video vigilancia sin la debida protección; los atacantes han desarrollado nuevas técnicas para aprovechar la falta de controles de seguridad en estos dispositivos y distribuir malware para generar indisponibilidad de servicios (entre ellos aplicaciones bancarias) y, como daño colateral, afectar el servicio de Internet.

Recomendaciones de Seguridad

Para cámara o DVR público en Internet :

- Desconecte el dispositivo de su red y de Internet
- Elimine usuarios por defecto configurados en el dispositivo y cree nuevos usuarios, solamente los necesarios. Los usuarios por defecto son aquellos que el fabricante crea para configuración inicial.
- Haga uso de contraseñas robustas (mayúsculas, minúsculas, números y caracteres especiales) y evite contraseñas conocidas o fáciles de adivinar [1] (*admin:admin*, *admin:1234*, *root:root*, etc.).
- Evite la publicación en Internet de puertos innecesario (*telnet, ftp, ssh*), especialmente si no hacen uso de contraseña o si tienen configuradas contraseñas conocidas.
- Reinicie el dispositivo para confirmar que las configuraciones han sido habilitadas correctamente.
- Reconecte el dispositivo a la red. Es importante no reconectar el dispositivo antes de haberlo reseteado y cambiado la contraseña.
- Verifique las actualizaciones de software o de seguridad para los dispositivos, publicadas por su fabricante y asegúrese que su dispositivo se encuentre actualizado.



Más información:

1. https://www.cert.gov.py/application/files/1814/7801/3058/Boletin_20161031_Botnet_Mirai.pdf