ALERTA

Amenazas Botnet Mirai

COLCERT AL-1207-036

La botnet Mirai, conocida por ataques DDoS masivos en el pasado, está resurgiendo como una amenaza significativa, aprovechando vulnerabilidades web conocidas para atacar más de 1.200 sitios. La sofisticación aumentada a través de la inteligencia artificial (IA) y el aprendizaje automático (ML) en los ataques DDoS presenta un desafío adicional para las organizaciones.

La combinación de estos factores crea una doble amenaza que exige atención y medidas preventivas.

TLP:CLEAR

BotNet Mirai

”Ataques DDoS Potenciados por IA”

Características clave de Mirai:

- Amenaza persistente
- Explota de vulnerabilidades Conocidas
- Tiene vectores de ataque
- Propagación eficiente
- Mecanismos de evasion
- Amenaza IA/ML
- Malware polimórfico

Aspectos a tener en cuenta:

- Ataques DDoS a gran escala que pueden interrumpir sitios web y servicios.
- Robo de datos y pérdida de información confidencial.
- Daños a la reputación y pérdida de ingresos.

Para protegerse contra esta amenaza:

Actualizar y parchear software, fortalecer contraseñas, segmentar redes, implementar soluciones de seguridad, monitorear la actividad de la red y capacitar a los empleados en prácticas de seguridad cibernética.

Revisión de las últimas versiones disponibles de seguridad sobre la ameanza e implementación de medidas de mitigación y contención.

NIVEL DE RIESGO

ALTO

FUENTES:

https://www.imperva.com/blog/how-to-identify-a-mirai-style-ddos-attack/
https://www.msn.com/en-gb/money/technology/a-new-botnet-is-spreading-mirai-across-the-world-with-thousands-of-devices-affected/ar-AA1kqcTc?ocid=msedgntp&pc=LCTS&cvid=44150312094240ddb39131fe998f320a&ei=69

COLCERT