IoT Vigilant

Hackathon Cybercamp

Málaga 2018

Equipo

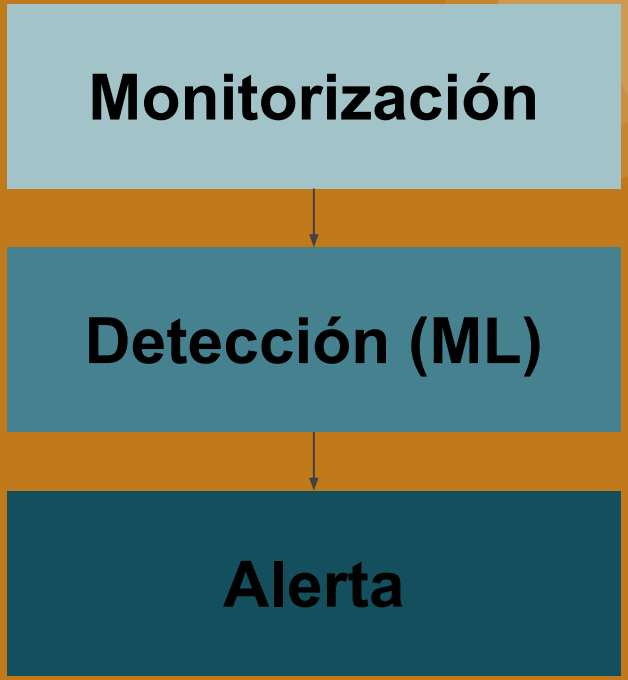
Victor Hugo García

Carlos Polop

Guillermo Barrenechea

David Ramírez

Detección de amenazas IoT basado en anomalías



Ámbito y contexto/Motivación*

- El número de dispositivos IoT crece de manera exponencial.
- Cada vez más, estos dispositivos son el objetivo de ataques
  - Farming de BotNets para DDoS
  - Intrusiones más sutiles
- Queremos detectar estos ataques y **prepararnos para los nuevos**

Ámbito y contexto/Motivación*

- Tradicionalmente, la detección de intrusiones se ha realizado a través de **firmas.**
- Esto funciona especialmente bien contra sistemas con un comportamiento complejo y difícil de acotar:
  - Hosts, servidores, etc.
- Los IoT son dispositivos **simples** y eso los hace mucho más **predecibles**

Motivación

- **Problema**: No existen soluciones IDS gratuitas orientadas hacia la detección de malware en IoT. Por ejemplo, algunas de los proyectos más conocidos son:
  - Snort: Reglas predefinidas
  - Suricata: Reglas predefinidas
- **Requisito**: Necesitamos un sistema capaz de detectar amenazas en condiciones predecibles.
  - ¡Este es el reto perfecto para usar Machine Learning!

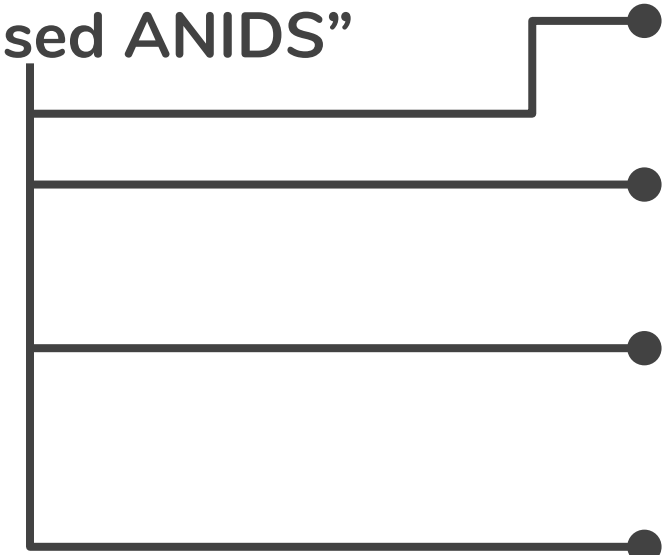
Estado del arte

- Soluciones existentes
  - IoT Security - ElevenPaths (Privativo)
  - ZingBox IoT (Privativo)
  - Hogzilla (Open source)
    - Algunas limitaciones

- **Nuestro proyecto: IoT Vigilant**
  - Open source ANIDS
  - Algoritmo de detección mejorado:
    - Basado en técnicas de Machine Learning no supervisado avanzadas.
  - Despliegue sencillo

Solución

“Unsupervised ANIDS”



- **IDS:** Intrusion Detection System
- **Network:** en contraposición a “host”
- **Anomaly-Based**: Detección de comportamientos anómalos
- **Unsupervised**: No requiere conocimiento previo o entrenamiento

Aspectos relevantes

- Utilizamos un framework completo de herramientas **Open-Source**:
  - Grafana
  - Elasticsearch
  - scapy
  - Scikit-learn
  - ...
- La idea sobre la que está basado el sistema permite agregar **múltiples instancias para aumentar la efectividad** del algoritmo.

Target

- Este proyecto está orientado para su uso en redes empresariales o de gran tamaño en las que existan multitud de dispositivos IoT

- El proyecto busca ser capaz de combinarse con las soluciones basadas en firmas para lograr una **defensa homogénea**.

- No obstante, se enfoca de tal manera que cualquiera pueda desplegarse su propia instancia en local y defender su casa o PYME.

Planteamiento del desarrollo

- Comenzamos desde cero
- Research: Búsqueda del algoritmo de ML más adecuado.
- Desarrollo e integración de los diferentes módulos

Funcionalidades

- Detección y alerta de comportamiento asociado a **intrusiones**:
  - Dispositivos siendo atacados
    - Escaneos de puertos
    - Ataques de denegación de servicio
    - ...
  - Dispositivos usándose para atacar
    - Conectados a botnets o usándose como spammers
    - Exfiltración de datos via red (Túneles DNS, etc.)
    - ...
- De manera indirecta, obtenemos **visibilidad** sobre la red:
  - Dispositivos nuevos, desaparecidos, actualizándose

Gracias

Y al turrón!