Instituto Politécnico Nacional
Centro de Investigación en Computación
Laboratorio de Ciberseguridad

Febrero del 2022

Temas de Tesis

Dr. Raúl Acosta Bermejo

1. Tema
   a. Analisis malware orientado a la identificación de IoC, IoE o IoA.
   IoC (Indicadores de Compromiso), IoE (Indicadores de Exposición), IoA (Indicadores de Ataque)
   b. Links
      i. https://www.cytomic.ai/es/threat-hunting/diferencias-entre-ioc-y-los-ioa/

2. Tema
   a. Crear una BD de IoC y realizar análisis/mineria
   b. Descripción: Las constantes actualizaciones de las bases de datos de los indicadores de compromiso es un factor clave para detectar las nuevas amenazas que estas surgiendo día tras día en la red. Uno de los grandes problemas que existen dentro del sector de la ciberseguridad es la falta de actualizaciones de los indicadores de compromiso críticos. Concentrándose generalmente en las muestras de HASH (sin importar cual se esté usando) de archivos del tipo ofimática, exe, dll, APK, JS, etc.

3. Tema
   a. Desarrollo de un IDS o IPS basados en IoCs de una BD.

4. Tema
   a. Implementar un sistema tipo YARA que funcione dinámicamente (con la memoria RAM) en el SO X (Linux).
   b. Crear un Repositorio/BD de reglas YARA.

5. Tema:
   a. Analisis de las muestras de malware de MAREA para realizar una clasificación las de tipo Web.

6. Tema
   a. Analizar un subconjutno de muestras de malware de MAREA con la finalidad de identificar la evolución de las muestras.
   b. Evolución en el tiempo, en las técnicas de ataque, etc.

7. Tema:
    a. Desarrollo de un sistema de SaaS para ofrecer un servicio de análisis automatizado de malware.
    b. Desarrollo de un Maas (Malware As A Services) es el que vende malware.

       Ransomware as a service RaaS
       Crear kits listos para usarse.
       kit de phishing, ataques DDoS, troyanos para desplegar ransomware.
       alquiler de granjas de bots
       EdA: 16Shop, Emotet,
       servicios maliciosos, Como evitar la detección? dark web

    c. Links
        i. https://protecciondatos-lopd.com/empresas/malware-as-a-service-maas/

8. Tema:
    a. Clasificación de un subconjutno de muestras de malware de MAREA usando funciones hash y un nuevo algoritmo que use la taxonomia de VirusTotal.

9. Tema:
    a. Identificación de las muestras de malware de tipo Botnet en MAREA para determinar su grado efectividad.