Entelgy
GO FOR IT

NIRYARA

Beneficios:
- ***Detección*** *de amenazas*
- ***Análisis*** *automatizado de malware*
- ***Automatización*** *de tareas*

El objeto del proyecto **Niryara** consiste en el desarrollo de una herramienta de detección y análisis automatizado de malware no basado en firmas. La herramienta permite automatizar las tareas previamente realizadas de forma manual por los analistas. Facilita su trabajo y les permite centrarse en el análisis de la información aportada por esta herramienta.

Los objetivos de I+D son:

- **Análisis estático** de malware de forma automatizada. Análisis de la muestra sin necesidad de su ejecución.
- **Análisis dinámico** de malware de forma automatizada y mediante el uso de multi-sandbox. Para el análisis dinámico es necesario el uso de diferentes sandboxes (entornos virtuales controlados con simulación por ejemplo de conexión a internet), tantos como SO se quieran simular.
- Creación de un **motor de generación de IOCs** (Indicadores de Compromiso o Artefactos, en la terminología de gestión de incidencias) en base al análisis de las muestras. Permite el bloqueo en FWs e IDS/IPS de las muestras.
- Sistema de **etiquetado** para la clasificación y compartición de una forma intuitiva y sencilla de las muestras y sus análisis.
- Ofrecer **mecanismos para evitar el ocultamiento** del malware y las técnicas anti-análisis.

Los objetivos del proyecto son:

- Aportar nuevos enfoques a la detección de malware no contemplados actualmente.
- Permitir un análisis en profundidad de las muestras detectadas.
- Automatizar el trabajo a realizar.
- Simplificar la usabilidad de la solución ofrecida.

NIRYARA (IDI - 20150344)

CDTI Centro para el Desarrollo Tecnológico Industrial

GOBIERNO DE ESPAÑA MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD

UNIÓN EUROPEA FONDO EUROPEO DE DESARROLLO REGIONAL "Una manera de hacer Europa"