Análisis de malware

$ whoami

- Sergio Apellániz
- Analista de malware en Hispasec
- Jugador de CTFs en Flaggermeister
- @sapellaniz

requirements.txt

- Windows 10 (ISO)
- Remnux (OVA)
- PEstudio
- Detect It Easy
- HXD
- Procmon
- IDA
- https://github.com/sapellaniz/taller-malware

Intro

- ¿Qué es el malware?
- ¿Qué tipos de malware existen?
- ¿En qué consiste el análisis de malware?

Fases del Análisis de Malware

- Research
- Análisis estático
  - Básico
  - Avanzado
- Análisis dinámico
  - Básico
  - Avanzado

Objetivos del taller

- Analizar una muestra de prueba
- Usar algunas de las principales herramientas
- Ver recursos online para análisis de malware
- Mostrar algunas técnicas empleadas por malware (anti-debug, anti-sandbox, ofuscación, etc)

Comenzamos!

Laboratorio

- Red Host-only
- Windows 10
  - Configuración de red
  - Herramientas
  - Carpeta compartida
  - Muestra
- Remnux
  - Configuración de red

Recursos online

- VirusTotal
- AnyRUN

Análisis estático (básico)

- Detect It Easy
- PEstudio

Análisis dinámico (básico)

- Procmon
- Inetsim

Análisis estático (avanzado)

- IDA

Algunos recursos

- https://evasions.checkpoint.com/
- https://malapi.io/
- https://abuse.ch/ (malware bazaar, feodo tracker, etc)
- https://github.com/ytisf/theZoo/tree/master/
- https://malpedia.caad.fkie.fraunhofer.de/
- https://tria.ge/
- eLearnSecurity ECMAP
- Practical Malware Analysis (ISBN 1593272901)
- Twitter

Sandbox

- https://www.virustotal.com
- https://app.any.run/
- https://www.capesandbox.com/
- https://www.joesandbox.com
- https://www.hybrid-analysis.com/