

# Análisis Dinámico

## Sandboxes

- Sandboxie: analiza el comportamiento de los procesos dentro de la máquina. Puede analizar si tienen un comportamiento identificativo del malware
- Buster Sandbox Analyzer
- Cuckoo Sandbox

## Problemas de las sandbox

- No se pueden ejecutar comandos
- No acepta paquetes command control
- No se puede controlar todo lo que hace la muestra una vez se pone a dormir
- No tiene en cuenta si la muestra puede detectar que está en máquina virtual
- Pueden faltar DLLs
- Pueden faltar claves de registro
- Puede que el sistema operativo no sea el que necesita la muestra para ejecutarse

## Monitores de procesos

- Monitoriza todos los procesos que se producen en el sistema
- Alto consumo de memoria, se recomienda filtrar y quedarnos solo con los procesos que no interesen.

## Process explorer

- Muestra información de los handle y DLLs abiertos o cargados

## RegShot

permite hacer instantánea del registro del sistema

## ApateDNS

- Monitorización de red
- controla respuestas DNS
- escucha puerto UDP 53

## netcap

- Monitoriza el trafico de la red

## Fakenet

simula una red y registra y captura las llamadas y conexiones de la muestra

## Wireshark

Análisis de tráfico a nivel muy bajo Filtros muy potentes

## Proceso

1. Arrancar Process Monitor
2. Arrancar Process explorer (Sysinternals)
3. hacer snapshot con regsot
4. Montar ApateDNS o Fakenet
5. Montar Wireshark

From:

<http://knoppia.net/> - **Knoppia**

Permanent link:

<http://knoppia.net/doku.php?id=mwr:lab2>

Last update: **2024/10/15 17:00**

