Deteccion, prevencion y proteccion.

# Defensa contra Malware oculto

## Detección de Malware oculto

### Firmas

Detención basada en firmas es uno de los mecanismos contra los malware más usados debido a su sencillez, velocidad y destacable precisión a la hora de identificar malware especifico. El software de detención de malware compara con una base de datos la “firma” de los archivos ha analizar y una vez encontrada esa firma en la base de datos el archivo es identificado como malware. Hay 4 tipos de firmas: archivos completos, archivos parciales, firma borrosa, cadena de firmas.

#### Archivos completos

La idea principal es computar un “fingerprint” del archivo completo por ejemplo usando un hash criptográfico como SHA-1 y compararlos con los hashes almacenados en una base de datos, debido a las características de los hashes criptográficos es prácticamente imposible que 2 archivos completos distintos generen el mismo fingerprint por lo tanto los malwares pueden ser detectados de manera rápida y eficaz.

#### Archivos parciales

Como el nombre sugiere se computará un “fingerprint” solo de ciertas secciones del archivo. Debido al funcionamiento de las funciones hashes criptográficas el mínimo cambio en el archivo de entrada cambiaria por completo el “fingerprint” resultante lo cual impedirá compararlo exitosamente con la base de datos. En los archivos de malware hay secciones que no tienen tanta relevancia y pueden ser modificadas fácilmente por lo que se centra el análisis en las secciones criticas del funcionamiento del malware y así ser capaces de detectar variantes de malware de manera eficaz.

#### Firma borrosa

Se computará un fingerprint a base de los propiedades generales de los archivos envés de los contenidos como en los previos casos. (No muy relevante a identificar hidden malware si no va mas eficaz a worms ya que es capaz de identificar methamorphic changes)

#### Cadena de firmas

Siguiendo el mecanismo de las anteriores firmas se analizarán las posibles cadenas de caracteres y se compararan con la base de datos, este método no es muy eficaz con malware oculto ya que no suelen interactuar con el usuario pero con malware como el “Stone virus” dado que contiene una cadena diciendo “Your PC is now stoned” un archivo con esa cadena puede ser identificado como posible malware, se tendrán más características en cuenta para determinar que es malware.

#### Ventajas y desventajas

### Comportamiento

### Heurísticas

La detención basada en heurística evita el uso de las firmas. Se analiza un archivo y se valora el comportamiento con un numero de patrones para determinar si es un posible malware

#### Pasivos

se explora el archivo tratando de determinar qué es lo que el programa intentará hacer. Si se observan acciones sospechosas, éste se detecta como malicioso

#### Activos

se trata de crear un entorno seguro y ejecutar el código de forma tal que se pueda conocer cuál es el comportamiento del código. Otros nombres para la misma técnica son “sandbox”, “virtualización” o “emulación”.