Deteccion, prevencion y proteccion.

# 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 a 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 cambiaría 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 críticas 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 las 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

Detención basada en firmas es una técnica muy fácil de implementar y gracias a la utilización de hashes criptográficos es muy eficaz a la hora de encontrar amenazas conocidas por lo que su tasa de falsos positivos es bajísima.

Las desventajas mas significantes de la detección basado en firmas son causadas debido a la base de datos. La base de datos juega un papel crucial en el sistema, por lo que tiene que estar siendo actualizada continuamente para que se puede detectar nuevos malware generados lo cual lo convierte en un sistema vulnerable a zero-day malware. Otra gran desventaja es que entre mas grande sea la base de datos más carga habrá sobre la CPU del sistema por lo que es difícil encontrar un equilibrio entre rapidez del sistema y eficacia de la bade de datos. Esta técnica de detención tampoco es capaz de combatir malware que muta su código en cada infección como polymorphic y metamorphic malware.

## Detección basada en comportamiento

La detención basada en comportamiento evita el uso de las firmas criptográficas. Se analiza un archivo para determinar si es un posible malware centrándonos mucho mas en que hace el archivo al ejecutarlo envés del contenido del mismo. Este tipo de mecanismo permite detectar malware que muta ya que siempre usaran los recursos y servicios del sistema de manera similar. Un detector basado en comportamiento esta dividido en tres bloques. El primer bloque recoge información dinámica/estática del ejecutable. El segundo bloque convierte la información obtenida en representaciones intermedias la cual el tercer bloque utilizara para determinar si el archivo analizado es considerado como malware.

## Ventajas y desventajas

La principal ventaja de este método es que es capaz de detectar malware que el método por firmas no es capaz como malware desconocido y variaciones de polymorphic malware. Las desventajas mas significativas son la tasa alta de falsos positivos y la cantidad de tiempo durante el escaneo de archivos.

### Heurísticas

Detención de malware utilizando usando heurística fue creado para superar las desventajas encontradas en la detención por firmas o comportamiento. Los métodos usados son procesamiento de datos y técnicas de aprendizaje automáticas para aprender el comportamiento de un ejecutable. Las características en uso por la detección usando heurística se pueden dividir generalmente en cinco bloques.

1. Llama a sistema API

Casi todos los programas usan llamadas API para enviar sus solicitudes al sistema operativo, las secuencias de llamadas API es una de las maneras mas acertadas que refleja el comportamiento de un pedazo de código como malware. Hofmeyr fue de los primeros que considero las secuencias de llamadas a sistema API como características de malware[3] por lo cual se desarrollo detención basada en llamadas a sistema. Distancia de haming que es el mínimo numero de sustituciones que se tiene que cambiar en una cadena para que sea idéntica a otra, fue utilizado para comparar las secuencias de llamadas API y poder clasificarlo como malware.

1. Código Operacional

Código operacional es la subdivisión de lenguaje de instrucciones de máquina que identifica la operación a realizar. Un programa esta definido por una serie de instrucciones de ensamblador. Bilar mostro la habilidad de utilizar código operacional como características en la detención de malware, analizo y demostró la alta fiabilidad para detectar amenazas de un ejecutable [4]. Hay varios tipos de detención de malware basados en código operacional por ejemplo un enfoque centrado en detectar variantes de malware ofuscado. Normalmente el procedimiento es descomponer el ejecutable en instrucciones de ensamblador y calcular la relevancia de estas instrucciones basándose en la técnica de frecuencia-peso de termino se realiza un vector que representa las características del ejecutable para poder ser estudiado como posible amenaza. Tambien es posible detectar malware desconocido y metamorphic basado en graficas de medición de similitud para poder llevar a cabo esta técnica de detención basada en código operacional se extrae código operacional de archivos benignos y malwares y se cuenta el numero de código operacional

1. N-Grams
2. Grafica de flujo de control
3. Caracteristica h­­­ibrida

Signatures vs behaving

<https://www.cyberdefensemagazine.com/advanced-malware-detection/>

Heuristics pasivos/activos

<https://www.welivesecurity.com/la-es/2010/02/16/tipos-heuristica/>

<https://support.eset.com/en/kb127-what-are-heuristics>

<https://www.welivesecurity.com/la-es/2013/03/18/heuristica-antivirus-deteccion-proactiva-amenazas/>

Detencion en general

https://scholarworks.sjsu.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=1329&context=etd\_projects

Detencion por comportamiento

[file:///C:/Users/user/Downloads/Asurveyonheuristicmalwaredetectiontechniques.pdf](file:///C:\Users\user\Downloads\Asurveyonheuristicmalwaredetectiontechniques.pdf)

1-G. Jacob, H. Debar, and E. Filiol, “Behavioral detection of malware: from a survey towards an established taxonomy,” Journal in Computer Virology, pp. 251–266, 2008 (COMPONENTES DE DETECION POR COMPORTAMIENTO)

[2]D. Bilar, “OpCodes as predictor for malware,” International Journal of Electronic Security and Digital Forensics, vol. 1, no. 2, p. 156, 2007.

[3] S. Hofmeyr, S. Forrest, and A. Somayaji, “Intrusion detection using sequences of system calls.” Journal of Computer Security, pp. 151–180, 1998.