Seguridad Digital

Transcribed on August 4, 2025 at 2:02 PM by Minutes AI

Speaker 1 (00:06)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema de la protección de ejecución de código y la firma digital del software y las aplicaciones.

Hablaremos de diferentes herramientas que tenemos disponibles como puede ser Sitchake, como puede ser Cross Explorer o como puede ser el propio administrador de tareas.

Una vez que tenemos el sistema operativo configurado y tenemos la seguridad implementada en los diferentes aspectos del propio sistema operativo, tenemos que pensar en la seguridad de las aplicaciones, es decir, tenemos que evitar que se ejecuten aplicaciones maliciosas en el dispositivo o que cuando nos descargamos un determinado archivo o una determinada aplicación, asegurarnos que esa aplicación no contenga software malicioso o piezas de malware que puedan utilizarse para controlar el dispositivo.

¿Cómo podemos saber si un programa que descargamos de Internet contiene malware o qué herramientas tenemos disponibles en el propio sistema operativo para prevenir la ejecución de malware o para minimizar el impacto de la ejecución de aplicaciones maliciosas?

Un buen acercamiento es publicar el hash asociado a un determinado archivo o aplicación.

Es decir, tendremos una aplicación o tendremos un archivo que tendrá una firma criptográfica y esa firma criptográfica va a estar publicada junto con el archivo.

Cuando nosotros nos descargamos el archivo podemos verificar esa firma criptográfica y si coincide nos vamos a encontrar con que ese software o esa aplicación no ha sido modificado.

Esto normalmente es una medida de seguridad excelente, aunque también es verdad que ha habido casos donde los atacantes han podido acceder al sitio web y no solo han modificado el archivo sino que también han modificado el hash.

De esta manera tendríamos el hash o la firma de un archivo malicioso.

Windows PowerShell utiliza el comando getfieldhash para verificar la firma de un archivo.

Es una de las maneras que tenemos simplemente con un comando que tenemos en el propio sistema operativo en la consola de Windows PowerShell con el que nosotros podemos verificar el hash o la firma de un determinado archivo.

Una de las mejores garantías de saber que estamos ejecutando software legítimo es que el fabricante firme ese software.

Un certificado digital nos va a dar garantías de que realmente un producto, una determinada aplicación pertenece a ese autor y va a dificultar en gran medida modificar el software y añadirle malware a ese software.

Algunas herramientas que nosotros podemos utilizar nos van a permitir verificar ese certificado digital para comprobar que ese certificado digital es correcto y que ese certificado digital realmente pertenece al fabricante de ese software.

Algunas de estas herramientas las tenemos integradas dentro del propio sistema operativo, es decir, dentro del administrador de tareas, por ejemplo, podemos verificar el certificado digital asociado a la ISO o a la librería o al elemento que lanza un determinado proceso.

Después también tenemos otras herramientas que podemos descargar de forma gratuita, por ejemplo, como las herramientas de Sysinternals, que nos van a permitir verificar los certificados digitales asociados, por ejemplo, al fabricante de un determinado ejecutable o de una determinada línea.

La suite de herramientas de Sysinternal está disponible para su descarga en la URL que tenéis en la diapositiva.

Dentro de la suite de herramientas vamos a tener una específica para comprobar las firmas digitales.

Esta herramienta se llama SIP Check y tiene la sintaxis que veis en la diapositiva.

Tenemos otras herramientas dentro de la suite de Sysinternals como por ejemplo Process Explorer, que también nos permite verificar las firmas digitales asociadas a un determinado ejecutable.

Realmente lo que hace es que verifica las firmas digitales de la librería o de la imagen que lanzó ese proceso.

Entonces, una de las cosas que podemos hacer es verificar esa firma digital y además Process Explorer nos va a permitir no sólo eso, sino que también enviar esa muestra a VirusTotal.

VirusTotal es una página web, un servicio web en el que nosotros podemos enviar cualquier tipo de archivo, lo va a analizar con una serie de motores antimalware y después nos va a dar el resultado de cuántos de esos motores antimalware detectan ese archivo como malicioso.

Pues desde Process Explorer nosotros directamente podemos enviar ese archivo a virustotal para que se analice.

Estamos en la máquina virtual, nos vamos al navegador, nos vamos al navegador, nos vamos a la página de Sysinternal.

En la página de Sysinternal, que es un proyecto que está integrado dentro de las herramientas que tenemos disponibles en el sitio oficial de Microsoft, Sysinternal, están creadas en 1996 por Marrusinovic, que es actualmente el director del proyecto de Microsoft Azure y están disponibles para su descarga gratuita.

En la página tenemos información sobre las diferentes actualizaciones que se van haciendo en todas las herramientas, es decir, que es un proyecto vivo, es un proyecto donde las herramientas se siguen manteniendo actualizadas y tendríamos aquí la posibilidad de ir a la parte de descargas, donde vamos a tener diferentes modelos de descargas para que se adapten a nuestras necesidades.

Podemos descargar específicamente una determinada herramienta o podemos descargar todas las suites de herramientas y tenerlas disponibles para su uso.

Las herramientas The Sysinternal tienen que tener una serie de condiciones adicionales.

Tienen que ser herramientas que tengan muy poco impacto en el sistema, que no requieran privilegios de administración para su utilización, aunque es verdad que hay herramientas que si se ejecutan como administrador tenemos más información del sistema que si se ejecutan sin privilegios, no necesitan ser instaladas y dejan muy poco rastro en el sistema.

Podemos ejecutar las herramientas desde la propia web o podemos ejecutar las herramientas desde un lápiz extraíble.

De tal manera que podemos llegar con una serie de herramientas que sabemos que un malware lo ha modificado y que vamos a utilizar para analizar un determinado equipo.

Una de las cosas que son habituales dentro del procedimiento de un software malicioso es modificar las herramientas de aná infecto un equipo y después infecto aquellos procesos que pueden ser detectados a través del visor de eventos del administrador de tareas para que sea más difícil localizar las acciones de ese software malicioso.

Cuando nosotros llegamos con unas herramientas de Sysinternal que tenemos en un dispositivo extraíble, sabemos que esas herramientas son legítimas y que no han sido modificadas, con lo cual nos van a dar una lectura correcta de lo que está sucediendo en el dispositivo.

Otro elemento que es interesante conocer es VirusTotal.

VirusTotal es un servicio que tenemos disponible en la red y este servicio nos permite enviar cualquier tipo de archivo y lo va a analizar con una serie de motores antimal y después nos va a dar un resultado de cuál de esos motores o cuántos de esos motores han detectado que ese archivo puede ser malicioso o puede tener software camuflado o puede tener algún tipo de mar.

Si nos vamos al administrador de tareas, dentro del administrador de tareas yo puedo ir a la parte de Detalles y voy a tener los diferentes procesos.

Puedo seleccionar cualquiera de estos procesos y si me voy a la parte de Propiedades del proceso, dentro de la parte de propiedades del proceso, voy a tener información relacionada con ese proceso.

Si me voy a la parte de detalles, en la parte de detalles voy a tener las firmas asociadas a ese determinado proceso, voy a saber el nombre del producto y el copyright relacionado con ese determinado producto, con ese determinado proceso.

Sin embargo, si nosotros queremos hacer un análisis más exhaustivo, podemos descargarnos las herramientas de Sysinternal y luego dentro de las herramientas de Sysinternal podemos ejecutar Process Explorer.

Vamos a ejecutarlo como administrador.

Una vez que tenemos Process Explorer abierto, podemos seleccionar cualquier proceso, nos vamos a este determinado proceso, nos vamos a la parte de propiedades y dentro de la parte de propiedades nosotros podemos verificar la firma digital asociada a ese determinado proceso.

Después nos aparecería aquí en la parte de columnas, si tenemos habilitadas esas columnas, pues esa verificación del certificado digital que firma aquella DLL o que firma aquella ISO o aquel ejecutable que ha lanzado este proceso.

Entonces tendríamos aquí información sobre el pad del elemento que ha lanzado el proceso, tendríamos aquí la línea de comandos con las que se ha lanzado ese proceso, que también es un dato muy interesante, y luego tendríamos aquí la posibilidad de verificar que ese determinado proceso tiene una firma digital o válida.

Como podéis ver, Process Explorer es como un administrador de tareas con esteroides, es mucho más potente, tiene funcionalidades mucho más interesantes que el administrador de tareas.

Desde aquí también podríamos enviar a VirusTotal el hash relacionado con el ejecutable que lanzó ese proceso y entonces verificaría con una serie de motores antivirus, en este caso con 76 motores antimalware, va a detectar y va a analizar ese hash y va a ver si pertenece alguno de sus componentes a un malware o se detecta algún tipo de software malicioso.

Entonces nosotros desde aquí podríamos enviarlo y podríamos obtener ese análisis relacionado con el análisis de ese determinado hash o relacionado con el análisis de ese determinado archivo.

Normalmente cuando nosotros enviamos el proceso la primera vez a virustotal, lo que suele hacer es enviar el hash del archivo y verificar en una base de datos si ese hash ya ha sido analizado y si ese hash pues contiene algún malware o algún tipo de actividad sospechosa.

Si nosotros volvemos a reenviar el archivo, lo que hace es realmente enviar ese archivo a virustotal para hacer un análisis más exhaustivo del archivo.

Nosotros También tenemos la posibilidad de directamente cualquiera de los procesos que se están ejecutando, simplemente desde aquí indicar que lo chequeé con VirusTotal, entonces directamente nosotros lo lanzaríamos desde ahí con botón derecho y nos aparecería aquí ese elemento.

Incluso dentro de las opciones nosotros tenemos la posibilidad de verificar todas las imágenes o tenemos la posibilidad de verificar todos los procesos que actualmente están detectados en Process Explorer y chequearlos con virustoto.

Para finalizar, recordar que tenemos varias herramientas que nos van a permitir verificar el origen de un software y de esta manera dificultar la ejecución de software malicioso en el dispositivo.

Recordar también que tenemos la suite de herramientas de SysInternal que nos ofrece un amplio número de herramientas con diferentes propósitos con la posibilidad de verificar las firmas digitales asociadas a programas y aplicaciones.

Llegamos al final de la sesión, os esperamos en el siguiente vídeo.