Instituto Tecnológico y de Estudios Superiores de Monterrey

Escuela de Ingeniería y Ciencias

Ingeniería en Ciencia de Datos y Matemáticas

Análisis Forense, Versión Ejecutiva

MA2005B.201 Aplicación de criptografía y seguridad

Óscar Antonio Banderas Álvarez A01568492

Leonardo Laureles Olmedo A01659241

Carlos Mateos Perez A01654085

Diana Paola Cadena Nito A01197399

Daniel Sánchez Villarreal A01197699

En conjunto con: IPC Services

Supervisado por

Dr. Óscar Eduardo Labrada Gómez

Dr. Alberto Francisco Martínez Herrera

Monterrey, Nuevo León. Fecha: 22 de octubre de 2022

Índice

1. Introducción

El análisis forense digital es un campo de investigación que impacta en diversos ámbitos: corporativo, investigaciones internas, criminales y de inteligencia, litigación civil y asuntos de seguridad nacional. (Cabrera, 2011). De acuerdo a la INTERPOL, este campo puede ser definido de la siguiente manera.

> "El análisis forense digital es un área de la ciberseguridad que se encarga en la detección, adquisición, tratamiento, análisis y comunicación de datos."(Interpol, 2018).

Una de las debilidades principales de la era digital es el borrado accidental, o intencional, de los datos; en el caso particular de este reporte, se está trabajando con una memoria USB a la que le fueron eliminados distintos archivos. En particular, uno de ellos es de suma importancia para la empresa en cuestión y es lo que se busca recuperar por medio de la herramienta Recuva

Al borrar un archivo de una computadora, realmente lo que se borra es el acceso directo al archivo; es decir, el sistema operativo borra la entrada del sistema de archivos. No obstante, el disco duro sigue guardando esa información hasta que se sobrescriba. Existen herramientas que facilitan este proceso pero de igual manera puede realizarse por medio de la terminal; en este caso, se trabajó con la herramienta Recuva. Este es un software que recupera archivos eliminados y trabaja con el sistema operativo Windows.

Una de las ventajas de este software es que, además de que existe una versión gratuita sin límite de cantidad de archivos a recuperar, también permite recuperarlos sin importar de qué manera fueron eliminados. Entre los tipos de archivos a recuperar se encuentran las imágenes, videos, música, archivos comprimidos e incluso e-mails de Outlook. Cabe destacar que la recuperación exitosa de la información dependerá de su estatus; Recuva lo codifica por colores: verde, naranja y rojo. Un archivo marcado como verde puede ser recuperado fácil y rápidamente; los archivos naranja de igual pueden ser recuperados pero el tiempo es más extenso. En cuanto a los archivos rojos, estos son más difíciles de recuperar y no todos los archivos son recuperados.

Retomando un poco la realización de reportes de análisis forense, la persona investigadora puede apoyarse en diversas herramientas, una de estas siendo Kaspersky Endopoint Security Cloud. Esta herramienta protege servidores de archivos y computadoras Windows, dispositivos macOS, móviles iOS y Android e incluso Microsoft Office 365. El área fuerte de esta herramienta es que puede escanear todos los dispositivos con la finalidad de encontrar amenazas. En dado caso de que se encuentre una amenaza, la herramienta es capaz de eliminarla y generar un reporte donde se incluya una visualización de los ataques para ver la causa y la ruta de estos. Esto último es de gran utilidad puesto que muchas herramientas simplemente detectan y eliminan las amenazas, pero si se requiere hacer un reporte de análisis forense, es de suma importancia contar con toda la información del ataque. (Kaspersky, S/A)

A continuación, se plantearán y desarrollaran estos dos escenarios: pérdida de información importante de una memoria USB y la infección de equipos con malware. Esto con la finalidad de recrear estos escenarios delicados para las empresas y poder ofrecer cierto marco para su prevención y tratamiento.

2. Desarrollo

2.1. Recuperación de datos

Para esta parte del reporte, se utilizó el software Recuva; se abrió la memoria USB en el ordenador, se encontraron 4 carpetas con 8 imágenes y 2 videos. Además, se creó una nueva carpeta en la computadora para que el programa deposite los archivos recuperados. Posterior a esto, se procedió a recuperar la información. Una vez recuperada la información en el programa, se despliega una pantalla donde se pueden visualizar los estados de los archivos previamente mencionados (verde, naranja y rojo). Además de este análisis sencillo, se optó por realizar un escaneo profundo para poder encontrar una mayor cantidad de archivos.

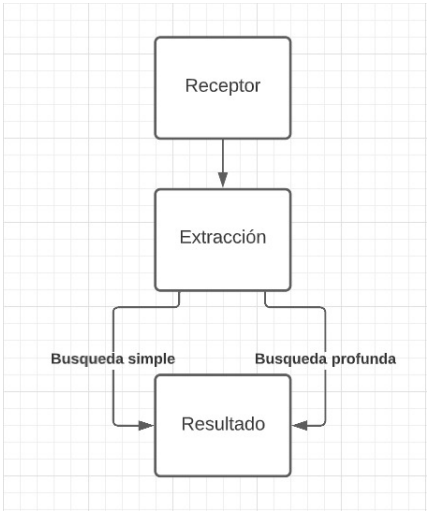

Figura 1: Diagrama de recuperación de datos

En el diagrama anterior, se observa el proceso realizado a grandes rasgos.

2.2. Análisis y detección de virus Reporte Forense

Se descargaron los virus desde la página proporcionada por la OSF y se procedió a analizar y verificar las amenazas detectadas en los dispositivos administrados. En el caso de los virus descargados, se observó que las gráficas de cadena únicamente mostraban la palabra *detected* debido a que los virus ya habían sido analizados previamente. Por esto mismo, se tomó la decisión de descargar distintos virus de la misma página para verificar si esto ocurría solamente con ese virus en particular o si era algo recurrente con los virus de esa página. Al finalizar estos procedimientos, se observó que el patrón se repetía por lo que se optó por descargar virus proveniente de otras páginas.

Para esto, se descargó primero un buscador de dark web, de donde se descargaron otros virus; para esto, primero se buscó *exe virus Windows* para encontrar un virus que pudiera ser descargado y ejecutado en la máquina virtual. Al navegar por el buscador, se ingresó a un foro llamado *BestCarding World* y descargó un archivo llamado *PlasmaHTTP.exe*. Al hacer clic en este, se descarga un archivo *.zip*, donde se encuentra una carpeta para ejecutar dentro de la máquina virtual. Antes de poder descargar el virus, la carpeta pide una contraseña; la cuál es *infected*. Una vez ejecutado el archivo, se elimina inmediatamente

de la máquina virtual al ser identificado por el programa.

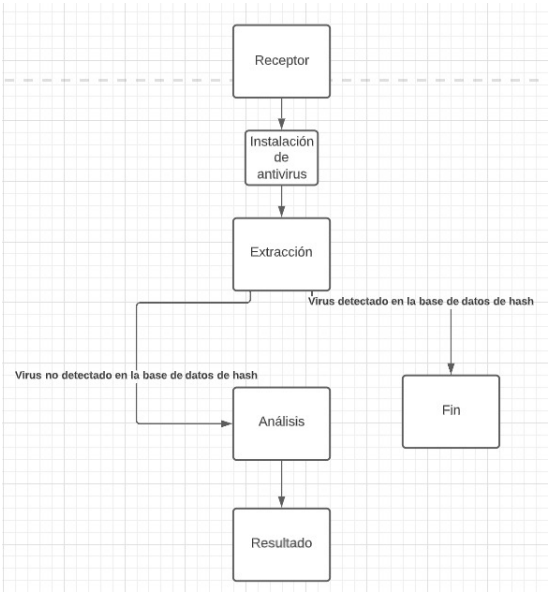

Figura 2: Diagrama de análisis y detección de virus

De igual manera, el diagrama anterior resume el procedimiento realizado en esta parte del proyecto.

3. Resultados

3.1. Recuperación de datos

Al terminar con el primer análisis, se obtuvieron 17 documentos en total; es decir, se encontraron 7 nuevos documentos nuevos lo que significa que se encontró información previamente borrada. Se observaron los estados de cada archivo (verde, naranja y rojo) así como otras columnas que dan información acerca de estos; metadatos como la dirección en donde se encuentra el archivo, fecha de la última modificación, tamaño y el estado del archivo. De estos 17 archivos, únicamente 11 se podían abrir; 6 estaban dañados y no se pudo identificar la información que contenían.

En el segundo análisis, se recuperaron un total de 12,944 archivos de los cuales 766 estaban en un estado "verde" y se pudieron rescatar todos. Del estado "amarillo", se recuperaron 26 archivos y existían dos clasificaciones para estos: *poor* y *very poor*. Los archivos en *poor* suelen ser más recuperables ya que una minoría de sus clusters han sido sobrescritos mientras que en los archivos *very poor*, la mayoría de sus clusters han sido sobrescritos (Forums, 2016). En cuanto a los archivos en un estado de "rojo", se encontraron aproximadamente 11,000 de estos.

En los archivos marcados como verdes, se encontraron únicamente imágenes como el logo de Google, el instructivo de Windows en diferentes idiomas en formato Word, algunas de las imágenes que aparecieron en el primer análisis, diversos símbolos, entre otros. En esta sección se encontraba el archivo de interés principal. La finalidad de recuperar la información de la memoria USB era recuperar un archivo con información confidencial; un archivo que fue borrado por un empleado en Alemania. Se recuperó una carpeta

con el nombre *Wichtig*, lo cuál significa *Importante*, dónde se encontró el archivo *Cosas que son muy importantes y muy confidenciales que deben de ser muy secretas.jpg*. Al recuperar la imagen y abrirla, se muestra un folder con la leyenda *Confidential*, por lo que se concluye que esa es la imagen que se estaba buscando. La recuperación de dicha información tardó 3 minutos con 10 segundos. Los archivos en estado amarillo fueron referentes a imágenes y links relacionados con otro software. La recuperación de dicha información tardó 27 minutos con 31 segundos.

Figura 3: Imagen Recuperada

3.2. Análisis y detección de virus

El proceso de revisión del equipo afectado consta de identificar el origen y desarrollo de la amenaza e indicadores de compromiso; a continuación se desglosan los descubrimientos de estos pasos.

1. **Origen de la amenaza.** La herramienta especifica los detalles del origen de la amenaza detectada, se muestra dónde empezó la amenaza, el *Process ID* que es un indicador del proceso de forma unícova. Establece si se encuentra en algún estado crítico y el nivel de integridad (que tan peligroso es el malware). De igual manera, indica desde qué usuario se ejecutó la amenaza así como la hora en la que se realizó. En la siguiente imagen, se puede apreciar esta información.

Figura 4: Gráfica de cadena y análisis de proceso

2. **Desarrollo de la amenaza.** Además de la gráfica de cadena, se puede encontrar un link con información más detallada del archivo. Este tiene como dirección a *Kaspersky Threat Intelligence Portal*, donde se observa si el archivo es una amenaza o un archivo conocido. Se cuenta con un total de 8 procesos, además de indicar si estos son críticos o no así como el nivel de seguridad que tiene. Finalmente, se muestran los parámetros de inicio y el Process ID. Los *Child Process*, son los procesos secundarios que surgen después de que algún archivo, aplicación o programa es ejecutado.

Esto es algo común ya que usualmente en los malwares se ejecutan en los *Parent Processes* y los *Child Processes* quedan en un área gris.

3. **Indicadores de compromiso.** De acuerdo con Kaspersky Endpoint Security Cloud-EDR, se detecta un archivo malicioso bloqueado, con los siguientes indicadores de compromiso mostrados en la tabla siguiente.

Ruta	**Amenaza**	**Tipo**	**Acción**	**Hora de detección**
https://anonfiles.com/rfj1Adveyf/PlasmaHTTP_zip	UDS:Dangerous ObjectMultiGeneric	Archivo	Eliminado	20/10/2022 17:29
Indicadores				
Sha-256			**MD5**	
4ea1f2ecf7eb12896f2cbf8683dae8546d2b8dc43cf7710d68ce99e127c0a966			f2b7074e1543720a9a98fda660e02688	

Cuadro 1: Indicadores

Esta herramienta nos brinda un veredicto conciso sobre el carácter peligroso/seguro del objeto ya que ofrecen información detallada sobre que tanto sospechoso es un archivo y en que aspectos, por ejemplo nos muestra que el archivo detectado es una amenaza, que tienen de malo, qué tan frecuente es la infección, a que amenazas se asemejan, que herramientas se usaron para crearlo, además de brindar información de la fecha que fue visto por primera vez así como la última, el formato y el tamaño.

4. Conclusiones

Existen distintas medidas que pueden ser llevadas a cabo por las empresas y organizaciones para mitigar o evitar la pérdida de información. A pesar de que existan medidas para recuperar sus archivos y demás, como se describió con anterioridad, esta recuperación puede tener un costo asociado. Minimizar costos es de gran relevancia para las empresas, por lo que tener las medidas necesarias para esto es de interés. Entre estas medidas de mitigación se encuentran el crear copias en la nube y tener cuidado en cuanto a dónde se conectan los dispositivos (USB).

El respaldo de la información por medio de las copias en la nube se asegura de que, en caso de algún siniestro, no se sufran pérdidas de información. Es importante que, como propietario de la información, no se confíe en su totalidad en el entorno. Una buena medida sería mantener respaldos tanto físicos como digitales; ambas tienen sus beneficios y áreas de oportunidad. Si se respalda la información únicamente por medios físicos, se corre el riesgo de que estos medios sean destruidos, haciendo imposible su recuperación. En cuanto a los respaldos digitales, se puede acceder a la información desde cualquier dispositivo electrónico con las credenciales correspondientes. Además, al estar almacenada en servidores remotos, el riesgo de que se pueda dañar, corromper o perder el disco duro físico y cualquier dato valioso es prácticamente nulo.

Otra medida de seguridad importante a tomar en consideración es el tener cuidado sobre dónde se conectan los dispositivos; en este caso, la USB. Conectarla a cualquier computadora o puerto, sin conocer el estado de estos mismos, es sumamente peligroso. Existe la posibilidad de que se coloque un malware

en el dispositivo que sea capaz de robar la información en cuestión de segundos. Se deben de tener las precauciones necesarias para evitar esto; no introducir la memoria USB a dispositivos que no hayan sido autorizados.

Es importante tener protegido cualquier dispositivo electrónico ya que no solamente se protege la vida útil del producto, sino que también se está protegiendo la información personal, como se observa en el reporte. Por lo general, el uso de malwares se da con la finalidad de robar y obtener cualquier tipo de datos; estos suelen instalarse fácil y rápidamente en el dispositivo. Por esto mismo, es de suma importancia contar con un antivirus y medidas preventivas en general. Esto protege la información así como da seguridad al usuario para navegar por el Internet. De igual manera, es importante resaltar que, aún contando con herramientas de protección, se debe hacer un uso responsable de la tecnología. Una de las herramientas recomendadas es Kaspersky ya que además de detectar y eliminar amenazas, es capaz de realizar el análisis forense que a su vez permite la interpretación de gráficas de desarrollo del ataque. Es decir, se identifica el tipo de ataque, su origen y las acciones realizadas.

Por último, es importante que al realizar un análisis forense digital, se tenga en mente qué es lo que se está buscando con dicho análisis. En este caso, se obtuvo una recuperación del archivo exitosa y se tomaron las medidas preventivas necesarias. Al realizar un escaneo profundo, la cantidad de archivos encontrados aumentó considerablemente por lo que es requerido poder discernir entre los archivos que son de interés y aquellos que sólo generan ruido. Además, se debe de realizar de la manera más controlada y limpia posible para evitar cualquier situación que desacredite el procedimiento realizado y la evidencia recuperada.

Referencias

Cabrera, G. J. (2011). Técnicas de análisis forense digital aplicadas a dispositivos y sistemas móviles. *Apuntes de Ciencia & Sociedad*, *1*(2), 6.

Forums, C. C. (2016). How is "unrecoverable" better than "poor"? https://community.ccleaner.com/topic/45573-how-is-unrecoverable-better-than-poor/

Interpol. (2018). Análisis forense digital. https://www.interpol.int/es/Como-trabajamos/Innovacion/Analisis-forense-digital

Kaspersky. (S/A). Ciberseguridad para empresas en crecimiento con recursos limitados. https://latam.kaspersky.com/small-to-medium-business-security/cloud