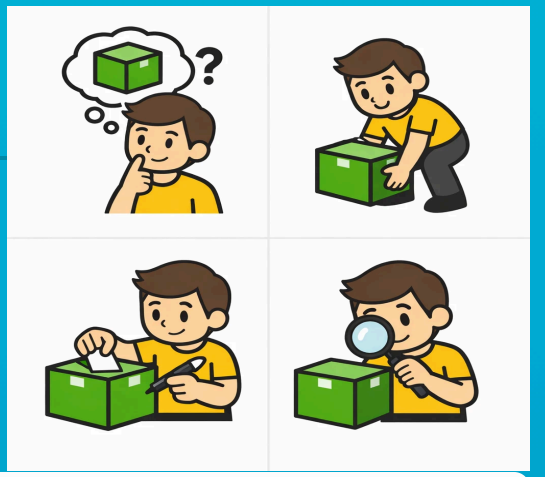
Análisis de evidencias



El análisis de las evidencias obtenidas en la recolección es el siguiente paso. Consiste en clasificarlas para realizar un estudio sobre ellas, lo que permitirá conocer si los datos que contienen son o no pertinentes para la investigación.

Otra tarea esencial que incluye el análisis, cuando se encuentra dentro de una investigación para un proceso judicial, es validar cada evidencia registrada para confirmar que se pueden presentar como elemento probatorio ante un tribunal. Es decir, se comprobarán aspectos como la línea temporal y los códigos hash.

Análisis de evidencias 2

Al igual que ya pasaba en la recolección de evidencias, durante la fase de análisis se deben documentar todos los aspectos que intervienen en ella, como el entorno, la tecnología, las herramientas, los procedimientos y los recursos que se utilicen y el personal implicado, además de especificar toda la línea temporal.

La norma UNE 71506:2013, sobre procesos de análisis forense dentro del ciclo de gestión de evidencias informáticas, establece una metodología para la preservación, adquisición, documentación, análisis y presentación de las evidencias informáticas. Algunos de los procesos y técnicas que se establecen para esta fase son:

Análisis de evidencias 3

- Identificación de los usuarios junto a los privilegios y permisos de estos dentro de los sistemas, así como las fechas de último acceso y las acciones realizadas.
- Recuperación de archivos específicos y correos electrónicos, incluso aquellos que han sido borrados.
- Consulta de la navegación por internet para obtener el historial, las cookies y la caché del navegador.
- Estudio de las particiones y el sistema de archivos.
- Análisis de la memoria RAM.
- Identificación de las conexiones de red y tarjetas instaladas y su dirección MAC, los protocolos usados y las direcciones IP.
- Revisión en las impresoras de la cola de trabajo.
- Estudio de los registros del sistema operativo y de los logs de otras aplicaciones como por ejemplo de los sistemas IDS/IPS.

Análisis de evidencias 4

- Revisión de colas de impresión y registros del sistema operativo.
- Estudio de logs de aplicaciones y sistemas IDS/IPS.
- Recuperación de datos borrados y análisis forense de particiones.

El resultado del análisis con las conclusiones alcanzadas se deberá documentar y presentar formalmente junto con las evidencias originales.

Metodologías

Existen diversas metodologías para realizar el trabajo de la fase de análisis de una investigación forense que dependen en gran medida de las herramientas que se utilicen, así como de las capacidades y experiencia de los analistas.
A la hora de analizar las evidencias se utilizan diferentes herramientas, según la naturaleza de la propia prueba o según el tipo de información que se quiere extraer de ella. Es por esto por lo que se encuentran herramientas tales como:

Metodologías 1

- **Análisis de correos electrónicos:** se revisan datos de correo electrónico, incluidos metadatos, archivos adjuntos y contenido. Por ejemplo, Aid4Mail.
- **Análisis de archivos sospechosos:** se utilizan para analizar archivos individuales que a menudo pueden estar infectados o ser parte del malware, o haber sido modificados por uno. Por ejemplo, una sandbox.
- **Análisis de archivos eliminados:** estas herramientas permiten recuperar archivos eliminados. Para entornos Linux existe, por ejemplo, Extundelete.
- **Análisis de internet:** analizan la información contenida en los navegadores, así como todos los datos or archivos relacionados con internet almacenados en el sistema. Por ejemplo, Magnet IEF.
- **Análisis de dispositivos móviles:** estas herramientas están especialmente diseñadas para analizar datos en dispositivos móviles, incluidos registros de llamadas, mensajes de texto, datos de aplicaciones y del propio sistema. Por ejemplo, CelleBrite Physical Analyser.

Metodologías 2

- **Análisis de red:** las herramientas forenses de red capturan el tráfico de la red y buscan comportamientos sospechosos, como accesos no autorizados. Entre estas herramientas la más conocida es Wireshark.
- **Análisis de registros:** estas herramientas utilizan como fuente archivos de registro, principalmente de dispositivos de red (routers, firewalls, entre otros), herramientas de seguridad (IDS, EDR, etc.) y de equipos finales (servidores, PC, etc.), que se examinan para extraer información valiosa relacionada con el incidente, como actividades inusuales de usuarios o alteraciones en el sistema. Por ejemplo, Logdissect.
- **Análisis de memoria:** herramientas que realizan análisis de datos volátiles en el volcado de memoria. Esta es una de las herramientas esenciales para los analistas forenses ya que la memoria puede ser una fuente de información crítica en una investigación. Por ejemplo, Volatility.

IoC

A partir del análisis de las evidencias recogidas en un sistema comprometido en un incidente de ciberseguridad es posible identificar elementos tales como ficheros, entradas de registro, procesos o servicios que indican que ese dispositivo ha sufrido una brecha de seguridad. Esos elementos o características propias de un ataque son lo que se conoce como indicadores de compromiso (IOC, Indicators of Compromise).

Hay muchos tipos de indicadores de compromiso, como, por ejemplo:

- **Nombres de archivos y procesos:** algunos malware crean archivos y ejecutan procesos en el sistema que los identifican. ¿Quién no ha mirado en el administrador de tareas de Windows qué procesos se están ejecutando cuando el sistema hace cosas sospechosas?
- **Direcciones de IP:** direcciones IP que han sido identificadas como origen o destino de ataques, por ejemplo de servidores C&C (comando y control).
- **Cambios en el registro de Windows** que pueden almacenar la configuración de software malicioso.
- **Nombres de dominio:** son nombres de dominio que se han asociado a actividades maliciosas como, por ejemplo, correos electrónicos de phishing.
- **Hashes de archivos maliciosos:** los haches de ficheros maliciosos pueden detectarse aun cuando se ha querido enmascarar el archivo con otro nombre.
- **En general,** cualesquiera cambios en los comportamientos habituales de los sistemas (tráfico de red inusual, aumento de fallos de login, incrementos en los accesos a disco o memoria, etc.) pueden ser indicadores de que algo no va bien, lo que puede ser un ataque o una simple eventualidad por unos hechos concretos.

IoC

La empresa de seguridad ESET dispone de un repositorio en GitHub con IOC correspondientes a diferentes campanas de malware que han analizado y que se pueden consultar en **github.com/eset/malware-ioc**

Los IOC son utilizados por los equipos de respuesta a incidentes para identificar, detectar, contener, mitigar y eliminar malware, intrusiones u otras actividades maliciosas en los sistemas, antes de que se propaguen o causen mayores daños. Ademós, sirven como evidencia forense ya que prueban que se ha producido un ciberataque.

A partir de los IOC incluso es posible descubrir más detalles sobre el ataque, así como las técnicas y tócticas utilizadas o quién es el autor del ataque. Esto no quiere decir que los IOC sean la solución a todos los problemas, ya que para conocer un IOC antes algún sistema ha debido ser víctima del ataque y se debe haber encontrado el indicador de compromiso, lo que no es una tarea fócil, pues en muchas ocasiones los atacantes se afanan por esconderlos.

Sandbox

Una herramienta muy útil cuando no se dispone de entornos específicos para el análisis forense de evidencias, algunas de las cuales podrían poner en riesgo los sistemas que se usan para analizarlas, es el sandbox o entorno de pruebas. Consiste en una máquina virtual aislada en la que se puede ejecutar software potencialmente malicioso sin afectar a los recursos reales del sistema. La ventaja de esta herramienta es que, al ser un espacio aislado y controlado, se pueden probar aplicaciones, abrir archivos, acceder a URL, entre otras tareas, para ver cómo se comportan; y si finalmente el comportamiento es dañino no afectará a nada fuera de ese entorno de pruebas. El entorno de pruebas tiene su propia red, lo cual no tiene acceso a los recursos del sistema real. Con este recurso, los investigadores pueden probar un malware y obtener algunos datos muy útiles, como los siguientes:

Sandbox 2

Con este recurso, los investigadores pueden probar un malware y obtener algunos datos muy útiles, como los siguientes:

- Si se autorreplica.
- Si intenta contactar con un servidor de comando y control.
- Si descarga archivos de otra ubicación.
- Si cifra información.
- Si crea variables en el registro del sistema.
- Si se conecta con alguna aplicación.

Sandbox 2 (continuación)

En definitiva, habrá que vigilar los efectos del malware sobre el sistema, lo que incluye las modificaciones del sistema de archivos, la comunicación de red y las llamadas al sistema. Todas estas averiguaciones serían indicadores de compromiso del malware que se está analizando. Incluso, podría ser que se tratase de un exploit de día cero, y que esos indicadores fueran aún desconocidos. Esa información será esencial para identificar o comprender cómo funciona el malware, y saber cómo contenerlo, mitigarlo y eliminarlo, y así ayudar a actualizar las políticas de seguridad de la organización. Pero los sandbox no son siempre invencibles, ya que existe malware diseñado para reconocer cuándo se encuentra en un entorno de pruebas y en ese caso puede actuar de diferentes maneras:

Sandbox 3

- Alterar su comportamiento para pasar desapercibido y evitar ser detectado o dar pistas sobre cómo vencerlo.
- Permanecer latente hasta que se encuentre en un entorno real.
- Explotar vulnerabilidades propias del entorno de pruebas.

Sandbox 4

Los entornos de pruebas deben estar bien diseñados, preparados, protegidos y actualizados para este tipo de malware. Un uso habitual del sandbox es utilizarlo como zona de cuarentena o prueba para los correos electrónicos sospechosos y sus archivos adjuntos. Una vez que los filtros de correo han marcado una serie de correos como posible amenaza, es decir, lo que se suele redirigir a la carpeta Spam o Correo no deseado, se llevan al sandbox para examinar sus archivos adjuntos o sus enlaces URL con seguridad. Un entorno de pruebas puede incluir componentes hardware, por ejemplo, puede tener su propio router y conexión a internet. De esta manera se haría prácticamente imposible para un software malicioso acceder a la red del sistema real.