IMPORTANCIA DE LA RECOLECCIÓN DE DATOS VOLÁTILES DENTRO DE UNA INVESTIGACIÓN FORENSE

Juan Esteban Castilla Guerra, Jonhattan Andreis Raquejo Romero
Universidad Piloto de Colombia
Bogotá D.C.
e-mail: juanesteban23@gmail.com, lseguridad@outlook.com

Resumen—En este momento donde la tecnología y las ciencias forenses ahondan en temas de alto tecnicismos y fácil manejo de la evidencia digital, podemos evidenciar en Internet el creciente desarrollo de herramientas tecnológicas de software disponibles para recuperar y analizar la información para la extracción de datos de la memoria volátil la cual puede contener muchos elementos de información importante como contraseñas, claves criptográficas, imágenes y otros datos que pueden servir de evidencia para inculpar o absolver algún grupo o persona de algún delito informático.

Abstract-In this time where technology and forensic science delve into issues of great technicalities and easy handling of digital evidence, we can see in the increasing development of Internet software technology tools available to retrieve and analyze information for data extraction volatile memory which can contain many elements of information such as passwords, cryptographic keys, images and other data that can serve as evidence to convict or acquit any group or person any computer crime.

Índice de Términos — Autorización, Datos Volátiles, Evidencia Digital, Informática Forense, Memoria RAM, Memoria Caché, Tratamiento.

I. INTRODUCCIÓN

Computación Forense (computer forensic) que entendemos por disciplina de las ciencias forenses, que considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso; o como la disciplina científica y especializada que entendiendo los elementos propios de las tecnologías de los equipos de computación ofrece un análisis de la información residente en dichos equipos [1]. Para simplificar podríamos decir que la Informática Forense busca establecer que sucedió, cuándo sucedió, como sucedió y quién estuvo involucrado; es por eso que dentro de una investigación forense la captura de la información sobre el estado actual de un equipo sospechoso antes de apagarlo es muy importante.

Existe una gran cantidad de datos volátiles que pueden perderse una vez que la computadora que se está investigando está apagada. Esta información puede ayudar a dirigir una investigación en las primeras etapas y puede ser beneficioso en otras etapas de la investigación.

En este artículo se pretender mostrar lo valioso que tiene el análisis de datos volátiles ya que con ellos podemos obtener información como:

- ✓ Contenido del portapapeles.
- ✓ Puertos de red abiertos.
- ✓ Aplicaciones y procesos en ejecución.
- ✓ Archivos temporales y de caché.
- ✓ Contenidos activos de la memoria.
- ✓ Unidades de red conectadas.

II. ¿QUÉ SON DATOS VOLÁTILES?

Los datos volátiles son aquellos que se almacenan en la memoria del sistema (por ejemplo, registros de sistema, caché, memoria RAM) y se pierden si el equipo se apaga o reinicia. La recolección de datos volátiles se centra en la recolección de datos (principalmente de la RAM) que se podrían perder si el equipo se apaga o reinicia. Los datos volátiles se deben recolectar si no se está seguro de por qué un equipo actúa anormalmente, si observa la actividad de un usuario sospechoso o si se le ha alertado de que una norma o política ha sido violada, como una alerta del firewall o del IDS (In trusion Detection System). En cualquier caso, la primera respuesta a un incidente de seguridad informática debe ser recopilar datos volátiles y analizar los resultados para determinar un próximo curso de acción.

Los datos persistentes o no volátiles residen en los discos duros del sistema u otros dispositivos de almacenamiento no volátiles (por ejemplo, dispositivos USB conectados, tarjetas de memoria, CD-ROM y otras unidades de disco duro externas) y normalmente no se pierden cuando se apaga o reinicia el equipo. En general, los datos persistentes se deben recolectar cuando se tiene claro que la evidencia relacionada con el incidente de seguridad informática reside en las áreas de almacenamiento persistente.

Para ambas estrategias de recolección, se debe evitar la contaminación del equipo sospechoso. Para la recolección de datos no volátiles, la contaminación puede ser controlada por las técnicas, herramientas y metodologías. Una de estas herramientas es dd.exe, una utilidad de imágenes gratuita desarrollada por George M. Garner Jr., que tiene la capacidad de crear una copia bit a bit del disco duro del equipo sospechoso. Si se crea el MD5 de la unidad de disco duro antes y después de usar una utilidad como DD, usted puede comparar y autenticar la copia. Para la recolección de los datos volátiles, la contaminación es más difícil de controlar debido a que las herramientas y comandos pueden cambiar las fechas y horarios de acceso a archivos, utilizar bibliotecas compartidas o archivos DLL, desencadenar la ejecución de software malicioso (malware), o en el peor de los casos forzar un reinicio del computador y perder todos los datos volátiles [2].

III. ORDEN DE LA RECOLECCIÓN DE LOS DATOS VOLÁTILES

El orden de volatilidad de la evidencia, es el orden en el cual la evidencia es más susceptible al cambio, es decir, recolectar en primer lugar los datos que tienen la mayor probabilidad de ser cambiados, modificados o perdidos [3].

IV. TIPOS DE ALMACENAMIENTO VOLÁTIL Y SU IMPORTANCIA

A. Evidencia altamente volátil

CPU (Registros Cache) y Memoria de Video. Usualmente la información en estos dispositivos es de mínima utilidad, pero debe ser capturada como parte de la imagen de memoria del sistema.

B. Evidencia medianamente volátil

RAM. Incluye información sobre los procesos en ejecución, el hecho de capturarla hace que cambie. Requiere conocimiento especializado para poder reconstruirla, pero no se requiere mucho conocimiento para hacer una búsqueda de palabras clave.

Tablas de Kernel (estado de la red y procesos en ejecución). Permiten analizar la actividad de red y los procesos que pueden ser evidencia de actividades no autorizadas.

C. Evidencia poco volátil

Medios fijos (Discos Duros). Incluye área de SWAP, colas, directorios temporales, directorios de registro – logs y otros directorios. La información recolectada en el área de SWAP y las colas permite analizar los procesos y la información de los mismos en un punto del tiempo particular. Los directorios permiten reconstruir eventos.

Medio removible (Cintas, CD-ROM). Usualmente son los dispositivos para el almacenamiento de contenidos históricos del sistema. Si existen previamente a un incidente pueden ser usadas para acortar el periodo de tiempo en el cual sucedió.

Medio impreso (Papel). Difíciles de analizar cuando son muchos. Ya que no se pueden realizar búsquedas automáticas sobre ellos [4].

V. TAREAS A REALIZAR EN EL ACCESO A LOS DISPOSITIVOS DE ALMACENAMIENTO VOLÁTIL

- ✓ Ejecutar un intérprete de comandos confiable o verificado matemáticamente.
- ✓ Registrar la fecha, hora del sistema, zona horaria. (UTC-05:00) Bogotá, Lima, Quito
- ✓ Determinar quién o quienes se encuentran con una sesión abierta, ya sea usuarios locales o remotos.
- ✓ Registrar los tiempos de creación, modificación y acceso de todos los archivos.
- ✓ Verificar y registrar todos los puertos de comunicación abiertos.
- ✓ Registrar las aplicaciones relacionadas con los puertos abiertos.
- ✓ Registrar todos los procesos activos.
- ✓ Verificar y registrar las conexiones de redes actuales y recientes.
- ✓ Registrar la fecha y hora del sistema.
- ✓ Verificar la integridad de los datos.
- ✓ Documentar todas las tareas y comandos efectuados durante la recolección.

Posteriormente, en lo posible, se debe realizar una recolección más detallada de los datos existentes en el almacenamiento volátil, efectuando las siguientes tareas:

- ✓ Examinar y extraer los registros de eventos.
- ✓ Examinar la base de datos o los módulos del núcleo del sistema operativo.
- ✓ Verificar la legitimidad de los comandos del sistema operativo.
- ✓ Examinar y extraer los archivos de claves del sistema operativo.
- ✓ Obtener y examinar los archivos de configuración relevantes del sistema operativo.
- ✓ Obtener y examinar la información contenida en la memoria RAM del sistema [5]-[6].

VI. PORQUE SON IMPORTANTES LOS DATOS VOLÁTILES

La realización del análisis forense a la memoria tiene el potencial de contribuir de manera significativa a cualquier investigación forense siempre y cuando dichos datos estén disponibles para la captura y análisis. El análisis de la memoria o análisis on-line es muy valioso porque supera algunas limitaciones del análisis forense tradicional, además de abordar los problemas que las nuevas tecnologías como el cifrado pueden causar durante el curso de un análisis en frío.

El análisis en frío está limitado de varias formas, una de ellas es que el investigador no pueda acceder a los datos cifrados a menos que pueda crackear la contraseña utilizada para cifrar los datos. Las claves y contraseñas son muy rara vez almacenadas en el disco duro. Cuando el usuario escribe sus contraseñas, o cuando los datos se descifran, las contraseñas y las claves son necesariamente cargadas y almacenadas en la memoria, el análisis de la memoria puede permitir que el analista pueda recuperarlos.

Otra limitación viene impuesta por la incapacidad del disco físico para revelar información sobre los procesos que se ejecutan en la memoria, que niega la idea al investigador de cómo las aplicaciones se estaban utilizando en el sistema en el momento del ataque.

Por otra parte, es cada vez más común que los atacantes utilicen la memoria para escribir virus, troyanos y gusanos que se encuentran sólo en la memoria y no dejan rastro en el disco físico. Y como resultado de ello, el análisis forense tradicional de los discos no revelará el código o permita a los analistas a entender cómo el ataque se está ejecutando o cómo mitigarlo [7].

Caso particular es el malware Fileless o Trojan-Spy.Win32.Lurk, explota una vulnerabilidad Java (CVE-2011-3544) como parte de una serie de ataques que han empezado a tener lugar recientemente. Llama la atención que Fileless inyecta una dll (dynamic link library) cifrada de la web directamente en la memoria del proceso javaw.exe de forma que no crea nuevos archivos en el disco duro cuando infectan los ordenadores a los que ataca. Además al ejecutarse dentro de un proceso considerado como de confianza, su detección es muy difícil para la mayoría de soluciones antivirus. Una vez que el **malware** Fileless se instala en el sistema, ataca al control de cuentas de usuarios de Windows para instalar el **troyano Lurk** y hacer que el sistema forme parte de una red ordenadores “zombie” o Botnet [8].

VII. CONCLUSIONES

Las crecientes técnicas de recolección de evidencias se han ido afinando. Los investigadores Forenses perfilan sus técnicas maximizando los recursos y las tecnologías siguen desarrollándose. En este artículo definimos la importancia del por qué la capacidad de realizar análisis forenses sobre la información volátil teniendo muy en cuenta que la memoria es un activo valioso para un analista forense.

Muchos atacantes escriben y hacen ataques desde la memoria volátil evadiendo cualquier tipo de análisis, ya que poseen el conocimiento y la experticia para hacerlo, por tanto hay que seguir ampliando el conjunto de habilidades que sean eficaces y eficientes en esta apasionante rama del análisis forense digital.

REFERENCIAS

[1] J. Cano Martínez, Computación Forense: Descubriendo los Ratros Informáticos, México D.F.: Alfaomega Grupo Editor, 2009, p. 2.

[2] K. Amari, «SANS Institute,» 2009. [En línea]. Available: : http://www.sans.org/reading_room/whitepapers/forensics/techniques-tools-recovering-analyzing-data-volatile-memory_33049. [Último acceso: Abril 2013].

[3] R. Nolan, C. O´Sullivan, J. Branson y C. Waits, «Carnegie Mellon University,» 2005. [En línea]. Available: www.cert.org/archive/pdf/FRGCF_v1.3.pdf. [Último acceso: Abril 2013].

[4] M. E. Darahuge y L. E. Arellano González, «http://xa.yimg.com/,» [En línea]. Available: http://xa.yimg.com/kq/.../Cadena+de+custodia+informatico+forense.doc. [Último acceso: Abril 2013].

[5] E. Martínez de Carvajal Hedrich, «Wikipedia,» 22 Marzo 2013. [En línea]. Available: http://es.wikipedia.org/wiki/Cómputo_forense. [Último acceso: Abril 2013].

[6] D. A. Torres, J. J. Cano y S. J. Rueda , «ACIS,» 17 Noviembre 2006. [En línea]. Available: http://www.acis.org.co/index.php?id=856. [Último acceso: Abril 2013].

[7] D. Brezinski y T. Killalea, «Internet Engineering Task Force,» [En línea]. Available: http://www.ietf.org/rfc/rfc3227. [Último acceso: Abril 2013].

[8] Maverick, «SXInformatica,» 24 Marzo 2012. [En línea]. Available: http://www.blog.sxinformatica.net/malware-que-se-instala-en-la-memoria-ram.php. [Último acceso: Abril 2013].

Perfil de los Autores

- Juan Esteban Castilla Guerra, recibió el título de Ingeniero de Sistemas de la Universidad Popular del Cesar en 2005. Actualmente cursa una Especialización en Seguridad Informática en la Universidad Piloto de Colombia. Trabaja en la Empresa Servigestión y Proyectos SAS como jefe de Sistemas. Su área de interés es la Informática Forense. e-mail: juanesteban23@gmail.com.

- Jonhattan Andreis Raquejo Romero Profesional en Ingeniería de Sistemas especialista en Seguridad Informática con conocimientos en informática forense, experiencia laboral en el manejo de técnicas del sistema de gestión COBIT e ITIL certificado en ItEssencial Hardware And Software de Cisco CCNA, CCNA Network Fundamental. e-mail: iseguridad@outlook.com