La informática forense

Por Ing. Vladimir Fernández Figueredo, Jefe de Grupo de Operaciones, Filial Datos, Dirección Territorial Cienfuegos, ETECSA
vfernandez@enet.cu

Introducción

Hasta que el 22 de noviembre de 1988, Robert T. Morris, un estudiante de la Universidad de Cornell (Ithaca, NY), protagonizó el primer gran incidente de seguridad —uno de sus programas se convirtió en el famoso *worm* o gusano de Internet, que provocó que miles de ordenadores conectados a la Internet quedaran inutilizados durante varios días, se calcula que un 10 % de los ordenadores de los Estados Unidos estuvieron bloqueados simultáneamente y sufrieron pérdidas estimadas en varios millones de dólares— muy pocas personas tomaban en serio el tema de la seguridad en redes de computadores de propósito general.

En la medida que crece y se diversifica el uso de infraestructuras tecnológicas, se incrementan también los riesgos de que las computadoras, dispositivos y sistemas informáticos, conectados o no a Internet, sean vulnerables a ataques o incidentes que ponen en peligro la integridad, disponibilidad y autenticidad de los datos que se procesan, almacenan o transfieren [1]. Y más allá de los datos, el daño a dichas infraestructuras es latente.

Con el incremento del número de incidentes de seguridad, es cada vez más frecuente el análisis de las acciones realizadas por los atacantes en los equipos: por un lado, para conocer y aprender el modo en que operan, averiguar el alcance del mismo y, llegado el momento, tomar las medidas oportunas para denunciar el ataque a las autoridades competentes; por otro, para llevar a cabo la actualización o recuperación parcial o completa del equipo atacado, pues al conocer el daño es posible intentar recuperarlo, con el fin de asegurar la continuidad del sistema. Cada vez es más costoso parar un servicio para efectuar la reinstalación de los sistemas informáticos y aplicaciones. De ahí, que se recomienda evaluar profundamente las implicaciones que ha tenido el problema de seguridad mediante las herramientas de análisis forense.

En este trabajo se analiza el concepto de delitos informáticos, el estado del arte de la informática forense, y se abordan sus definiciones, objetivos y usos. Se explica brevemente el concepto de evidencia digital y se muestran algunos de los programas y herramientas usadas por los especialistas forenses.

Desarrollo

Los delitos informáticos

Según documento de la ONU en el Undécimo Congreso de las Naciones Unidas sobre prevención del delito, la delincuencia informática es difícil de comprender o conceptualizar plenamente. A menudo, se la considera una conducta proscrita por la legislación, que implica la utilización de tecnologías digitales en la comisión del delito; se dirige a las tecnologías propias de la computación y las comunicaciones; e incluye la utilización incidental de computadoras en la comisión de otros delitos [2].

Algunas definiciones son:

Delitos informáticos: son todos aquellos en los cuales el sujeto activo lesiona un bien jurídico, que puede o no estar protegido por la legislación vigente y que puede ser de diverso tipo, a través de la utilización indebida de medios informáticos.

Delitos electrónicos o informáticos electrónicos: son una especie del género de los delitos informáticos en los cuales el autor produce un daño o intromisión no autorizada en equipos electrónicos ajenos, y que, por regla general, no se encuentran legislados.

Delitos cibernéticos: son ilícitos en que se tiene a las computadoras como instrumento, medio o como fin.

Entre los principales delitos e incidentes de seguridad que afectan hoy a las tecnologías de la computación y las comunicaciones y que causan cuantiosas pérdidas, pueden mencionarse:

- Los virus informáticos de alcance mundial que causan considerables perjuicios a las redes comerciales y de consumidores.
- Los ataques a servidores con el objetivo de sabotearlos DDoS—*Distributed Denial of Service Attack* / Ataques Distribuidos de Denegación de Servicio—.
- El vandalismo electrónico y la falsificación profesional.

- El robo o fraude, por ejemplo, ataques de piratería contra bancos o sistemas financieros y fraude mediante transferencias electrónicas de fondos.
- La "pesca" (*phishing*) consistente en el envío masivo de mensajes electrónicos con falsos remitentes para que los usuarios proporcionen sus claves de acceso y contraseñas de sus cuentas.
- El envío o ingreso subrepticio de archivos espías o *Keyloggers*.
- El uso de Troyanos/*Backdoors* para el control remoto de los sistemas o la sustracción de información.
- El uso de archivos BOT del IRC para el control remoto de sistemas y sustracción de información.
- La inundación de mensajes de propaganda supuestamente de origen conocido (*spam*).
- La difusión de material ilícito y nocivo o contrario a los principios éticos y políticos de un país.

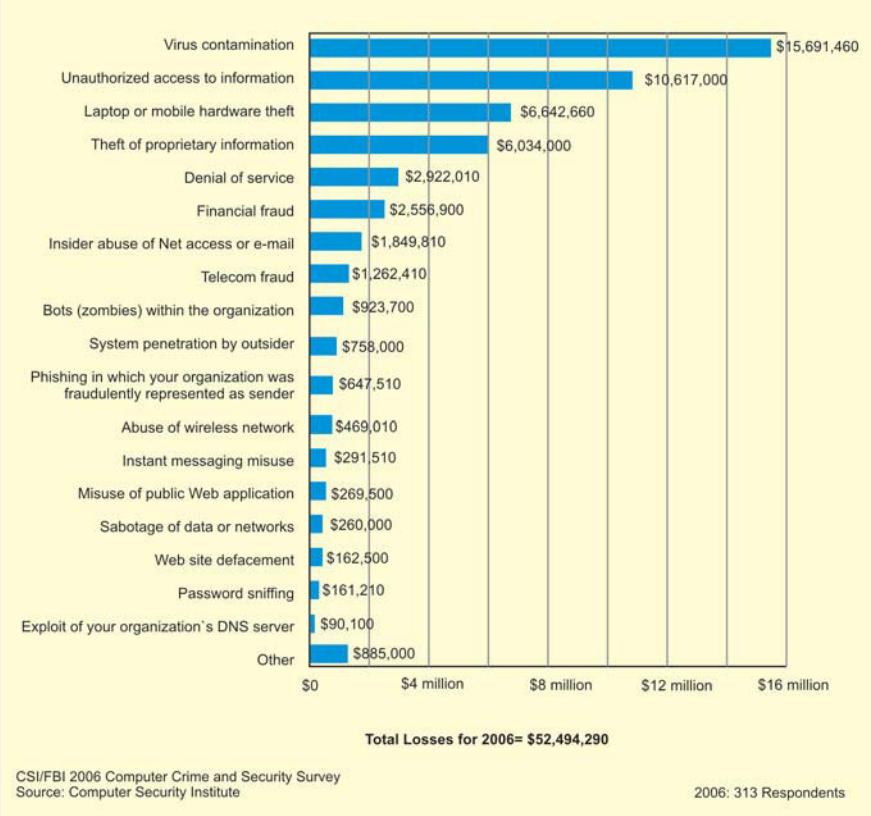

Figura 1 Pérdidas por tipo de delito según *survey* CSI/FBI en el 2006

La figura 1 muestra las pérdidas estimadas por tipos de delitos durante el año 2006 según el *survey* realizado por el Computer Security Institute (CSI) y el Buró Federal de Investigacines (FBI) a 313 entidades estadounidenses que fueron capaces de estimar estos valores.

Los mecanismos de seguridad

Para contrarrestar los efectos de los ataques que se incrementan progresivamente en cantidad y formas, existen varios mecanismos de seguridad. Típicamente, los mecanismos de seguridad que se emplean en sistemas informáticos y en redes de propósito general pueden dividirse en 3 grandes grupos: prevención, detección y recuperación.

Los **mecanismos de prevención** son aquellos que aumentan la seguridad del sistema durante su funcionamiento normal, para prevenir la ocurrencia de violaciones de la seguridad. Por **mecanismos de detección** se conocen los que se utilizan para detectar violaciones de la seguridad o intentos de violación. Y finalmente, los **mecanismos de recuperación** son aquellos que se aplican, cuando se ha detectado una violación del sistema, para retornarlo a su estado de funcionamiento correcto; ejemplos de estos mecanismos son la utilización de copias de seguridad, el uso de herramientas para la recuperación de datos borrados y contenidos en el propio sistema.

Dentro de este último grupo de mecanismos de seguridad se encuentra un subgrupo denominado **mecanismos de análisis forense**, cuyo objetivo no es simplemente retornar al sistema a su modo de trabajo normal, sino averiguar el alcance de la violación, las actividades de un intruso en el sistema, y la puerta utilizada para entrar; de esta forma se previenen ataques posteriores y se detectan ataques a otros sistemas de la red.

Sin lugar a dudas, una de las cosas más difíciles de hacer después de una intrusión en un sistema informático es la obtención de pruebas que tengan valor legal en el ámbito jurídico y que permitan denunciar y demostrar el origen y la identidad del atacante. En muchos casos, las evidencias dejadas en el equipo son la única defensa posible contra estos ataques, sin embargo, el atacante habrá borrado parte de las huellas dejadas por las acciones realizadas.

Unido a esto, se encuentra la dificultad intrínseca del proceso de búsqueda de pruebas. Además, la actuación de los administradores de sistemas informáticos, en muchos casos, resulta precipitada: en su afán por retornar el sistema a su modo de funcionamiento normal reinstalan parte o la totalidad del software, eliminando cualquier tipo de evidencia que todavía pudiera permanecer en el equipo. Hasta hace muy poco

tiempo, el análisis forense de sistemas informáticos tenía más de arte que de ciencia, no obstante, cada día van surgiendo nuevas herramientas que ayudan a automatizar el proceso de recolección y el análisis de datos.

Análisis forense

Existen múltiples definiciones sobre el tema forense en informática. Una primera revisión sugiere diferentes términos para aproximarse a este tema, dentro de los cuales se tienen: Computación Forense, Forensia Digital, Forensia en Redes, entre otros. Cada uno de estos términos trata, de manera particular o general, temas que son de interés para las ciencias forenses aplicadas en medios informáticos. Es importante destacar, que al ser esta especialidad técnica un recurso importante para las ciencias forenses modernas, asumen dentro de sus procedimientos las tareas asociadas con la evidencia, como son: identificación, preservación, extracción, análisis, interpretación, documentación y presentación de las pruebas en el contexto de la situación bajo inspección.

Primeramente, la Computación Forense puede interpretarse de dos maneras [3]:

1-Como una disciplina de las ciencias forenses que, considerando las tareas 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.

2-Como la disciplina científica y especializada que, al entender los elementos propios de las tecnologías de los equipos de computación, ofrece un análisis de la información residente en dichos equipos.

La informática forense tiene 3 objetivos básicos:

- La compensación de los daños causados por los delatores o intrusos.
- La persecución y el procesamiento judicial de los delatores.
- La creación y aplicación de medidas para prevenir casos similares [4].

Estos objetivos son logrados de varias formas, entre ellas, la principal es la recolección de evidencia.

La evidencia digital

De acuerdo con el documento "Guidelines for the Management of IT Evidence" [5], la evidencia digital es: "cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático". En este sentido, la evidencia digital, es un término utilizado de manera amplia para describir "cualquier registro generado por o almacenado en un sistema informático que puede ser utilizado como evidencia en un proceso legal".

La evidencia digital es la materia prima para los investigadores donde la tecnología informática es parte fundamental del proceso. Sin embargo, y considerando el ambiente tan cambiante y dinámico de las infraestructuras de computación y comunicaciones, es preciso detallar las características de dicha evidencia en este entorno. La evidencia digital posee, entre otros, los siguientes elementos que la hacen un constante desafío para aquellos que la identifican y analizan: es volátil, anónima, duplicable, alterable, modificable y eliminable.

Estas características advierten sobre la exigente labor que se requiere por parte de los especialistas en temas de informática forense, tanto en procedimientos, como en técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la evidencia en la escena de un incidente.

El proceso de recolección y manejo de la evidencia digital puede resultar complejo, puesto que en muchos casos resulta imposible parar algún servicio para examinar el o los dispositivos afectados, por lo tanto, una vez que se detecta un ataque, deben tomarse algunas medidas por parte de los administradores, con el objetivo de evitar que aumenten los efectos negativos del ataque, lo que en alguna medida puede atentar contra el trabajo posterior de los especialistas forenses al comprometer la integridad de la evidencia, entonces resulta necesario que los administradores cuenten con los conocimientos suficientes para actuar ante tales eventos sin afectar el análisis posterior.

Esterilidad de los medios informáticos de trabajo

La evidencia digital es única, cuando se compara con otras formas de evidencia documental. A diferencia de la documentación impresa, la evidencia computacional es frágil y una copia de un documento almacenado en un archivo es idéntica al original. Otro aspecto único de la evidencia computacional es el potencial de realizar copias no autorizadas de archivos, sin dejar rastro de que se realizó. Esta situación crea problemas concernientes a la investigación del robo de secretos comerciales, como listas de clientes, material de investigación, fórmulas y software propietario.

Verificación de las copias en medios informáticos

Las copias efectuadas en los medios previamente esterilizados, deben ser idénticas al original del cual fueron tomadas. La verificación de estas debe estar asistida por métodos y procedimientos matemáticos que establezcan que la información traspasada a la copia es completa. Para esto, se sugiere utilizar algoritmos y técnicas de control basadas en firmas digitales que puedan comprobar que la información inicialmente tomada corresponde a la que se ubica en el medio de copia.

Manejo y recolección de evidencia digital

La IOCE —*International Organization on Computer Evidence*— define los siguientes puntos como los principios para el manejo y la recolección de evidencia computacional [6]:

- Sobre recolectar evidencia digital, las acciones tomadas no deben cambiar por ningún motivo esta evidencia.
- Cuando es necesario que una persona tenga acceso a evidencia digital original, esa persona debe ser un forense profesional.
- Toda la actividad referente a la recolección, el acceso, almacenamiento o a la transferencia de la evidencia digital, debe ser documentada completamente, preservada y disponible para la revisión.
- Un individuo es responsable de todas las acciones tomadas respecto a la evidencia digital mientras que esté en su posesión.
- Cualquier agencia que sea responsable de recolectar, tener acceso, almacenar o transferir evidencia digital es responsable de cumplir con estos principios.

Herramientas de análisis forense

Las herramientas informáticas son la base esencial de los análisis de las evidencias digitales en los medios informáticos. Sin embargo, es preciso comentar que requieren de una formalidad adicional que permita validar tanto la confiabilidad de los resultados de la aplicación de las mismas, como la formación y el conocimiento del investigador que las utiliza. Estos dos elementos hacen del uso de las herramientas una reflexión constante y cuestionamiento por parte de la comunidad científica y práctica de la informática forense en el mundo.

Dentro de las herramientas frecuentemente utilizadas en procedimientos forenses en informática se detallan algunas que son aplicaciones que tratan de cubrir todo el proceso en la investigación forense en informática, las cuales pueden clasificarse en cuatro grupos principales.

Herramientas para la recolección de evidencia

Existe una gran cantidad de herramientas para recuperar evidencia. El uso de herramientas sofisticadas es necesario debido a:

- La gran cantidad de datos que pueden estar almacenados en una computadora.
- La variedad de formatos de archivos, los cuales pueden variar enormemente, aún dentro del contexto de un mismo sistema operativo.
- La necesidad de recopilar la información de una manera exacta, y que permita verificar que la copia es exacta.
- Limitaciones de tiempo para analizar toda la información.
- Facilidad para borrar archivos de computadoras.
- Mecanismos de encriptación o de contraseñas.

Algunas de las herramientas más usadas son:

ENCASE Disponible en: http://www.guidancesoftware.com/

EnCase es un ejemplo de herramientas de este tipo. Desarrollada por Guidance Software Inc., permite asistir al especialista forense durante el análisis de un crimen digital. Es el software líder en el mercado, el producto más difundido y de mayor uso en el campo del análisis forense.

Algunas de las características más importantes de EnCase son:

- Copiado comprimido de discos fuente.
- Búsqueda y análisis de múltiples partes de archivos adquiridos.
- Diferente capacidad de almacenamiento.
- Varios campos de ordenamiento, incluyendo estampillas de tiempo.
- Búsqueda automática y análisis de archivos de tipo Zip y *attachments* de *e-mail*.
- Análisis electrónico del rastro de intervención.
- Soporte de múltiples sistemas de archivo.
- Integración de reportes.

Otras herramientas son:

FORENSIC TOOLKIT. Disponible en:http://ww.accessdata.com/Product04_Overview.htm.

WINHEX. Disponible en: http://www.x-ways.net/winhex/index-e.html.

Herramientas para el monitoreo o control de computadoras

Algunas veces se necesita información sobre el uso de las computadoras, por lo tanto, existen herramientas que monitorean el uso de estas para poder recolectar información. Algunos programas simples como *key loggers* o recolectores de pulsaciones del teclado, que guardan información sobre las teclas que son presionadas, hasta otros que guardan imágenes de la pantalla que ve el usuario de la computadora, o hasta casos donde la máquina es controlada remotamente.

Herramientas de marcado de documentos

Un aspecto interesante es el de marcado de documentos, en los casos de robo de información, es posible, mediante el uso de herramientas, marcar software para poder detectarlo fácilmente. El foco de la seguridad está centrado en la prevención de ataques, algunos sitios que manejan información confidencial o sensitiva, tienen mecanismos para validar el ingreso; pero, debido a que no existe nada como un sitio 100 % seguro, debe estar preparado para incidentes.

Herramientas de hardware

Debido a que el proceso de recolección de evidencia debe ser preciso y no debe modificar la información, se han diseñado varias herramientas como las de DIBS que están disponibles en: http://www.dibsusa.com/products/products.asp.

Mobile Forensic Workstation —para la recolección detallada y el análisis de datos *in situ*—.

Rapid Action Imaging Device (RAID) —para el copiado rápido de discos duros—.

Aircapture WLAN 1 —para la captura, el almacenamiento y análisis de comunicaciones inalámbricas—.

Para mayor información de otras herramientas forenses en informática se sugiere revisar el enlace: http://www.e-evidence.info/vendors.html.

La informática forense en Cuba

En nuestro país al igual que en muchos otros países, el rol de peritos informáticos es asumido por ingenieros y licenciados en informática, ingenieros en telecomunicaciones y electrónicos, fundados exclusivamente en su formación académica. En una gran parte de las entidades con medios de cómputo y redes de computadoras, no se toma muy en serio esta actividad y en muchos casos los incidentes de seguridad no son analizados ni reportados.

A nivel central la Oficina de Seguridad para las Redes Informáticas OSRI, adscrita al Ministerio de la Informática y las Comunicaciones —http://www.mic.gov.cu/hticentity.aspx— es la entidad rectora y con mayor desarrollo en la actividad informática forense; entre sus objetivos está llevar a cabo la prevención, evaluación, aviso, investigación y respuesta a las acciones, tanto internas como externas, que afecten el funcionamiento adecuado de las tecnologías de la información del país.

Conclusiones

Los delitos informáticos van en ascenso en cuanto a la cantidad y variedad, los atacantes están cada vez más especializados y aparecen delitos más lucrativos para los delincuentes informáticos, por lo tanto resulta primordial tener en cuenta los mecanismos de seguridad para protegerse, principalmente los de respuesta a incidentes juegan un papel importante y dentro de estos, el análisis forense, debido a que resulta necesario no sólo determinar la procedencia del ataque para juzgar el atacante, sino también averiguar el alcance de la violación y la vía de entrada para prevenir otros ataques.

Referencias bibliográficas

[1] "Código de prácticas para *digital forensics*", (metodología). 1er Flash Mob sobre *Digital Forensics* 2003, Barcelona. Disponible en: http://cp4df.sourceforge.net/flashmob03/doc/03-Metodologia-rev3.pdf. (Consulta: febrero/2007).

[2] Delitos Informáticos. Presentación en el Undécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Bangkok, Tailandia, 2005. Disponible en: http://www.unodc.org. (Consulta: febrero/2007).

[3] J Cano, Jeimy. "Introducción a la informática forense". (2006). Disponible en: http://www.acis.org.co/fileadmin/Revista_96/dos.pdf. (Consulta: febrero/2007).

[4] Boas, Marco Villas. *Manual de Informática Forense*. Brasil: Del Rey, 1994.

[5] Guidelines for the Management of IT Evidence (Standard). Disponible en: http://www.standards.com.au. (Consulta: febrero/2007).

[6] López, Oscar. "Informática Forense: generalidades, aspectos técnicos y herramientas". Disponible en: http://www.criminalistaenred.com.ar/Informatica_F.html. (Consulta: febrero/2007).