ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
CENTRO DE INVESTIGACIÓN CIENTÍFICA Y TECNOLÓGICA

Investigación Forense: Estudio para determinar los métodos usados en la Intrusión del caso del Banco JBR

Diego Donoso [(1)]; Daniel Quiñonez [(2)]
Facultad de Ingeniería en Electricidad y Computación
Escuela Superior Politécnica del Litoral
Campus Gustavo Galindo Velasco, Km. 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil-Ecuador
djdonoso@espol.edu.ec[(1)]; dquinone@espol.edu.ec[(2)]
Febrero del 2012 – Febrero del 2013
Guayaquil-Ecuador

Director de Tesis Ing. Karina Astudillo, mail karina.astudillo@elixircorp.biz

Resumen

El presente trabajo tiene como objetivo dilucidar si la institución bancaria JBR sufrió un ataque de intrusión informática. Para reconstruir la escena de los hechos analizaremos todo tipo de archivos o registros que nos sirvan para descubrir los rastros que el posible atacante pudo haber dejado. Como pista principal se encontró un archivo update.exe de 0 bytes de longitud en la carpeta raíz de uno de los servidores del Banco JBR, gracias a esto comenzó la investigación realizando la captura de datos en vivo, seguida de la obtención de imágenes forenses, finalizando con el apagado del sistema para evitar que el evento continúe. El análisis empieza con la interpretación de los datos capturados en vivo, es decir, conexiones, puertos procesos, sesiones abiertas; cualquier información que permita determinar si hubo un ataque. Seguido del análisis de sesiones capturadas con la herramienta tcpdump y terminamos con la interpretación de la información en la imagen forense, que con la ayuda de la herramienta Autopsy se pude recrear una línea de tiempo de la actividad en los archivos y así concluir si existió un ataque y si el mismo tuvo éxito.

Palabras Claves: *Análisis, Autopsy, tcpdump, Forense, Captura de datos en vivo*

Abstract

This papers aims to discover if JBR Bank suffered a hacking attack. To reconstruct the crime scene we will analyze every kind of files or logs that help us to discover or trace tracks that the alleged attacker may have left to run their attack. A file called update.exe with 0 bytes in length was found in the root folder of one of the JBR Bank's servers, thanks to this an investigation was started executing a Live Response Process, followed by obtaining a forensic image and ending with the system shutdown to prevent the event continues. The analysis begins by interpreting the information captured with the Live Response Process, ie the connections, ports, processes, open session, any information that could led to determine if there was indeed an attack. Followed with the analysis of captured sessions with tcpdump and ending with the interpretation of the information in the forensic image, that with the help of the tool Autopsy we could recreate a timeline of activity on the files and thus concluded if there was an attack and if that was the case if it did succeeded.

Keywords: *Analysis, Autppsy, tcpdump, Forensics, Live Response Process*

1. Introducción

Cada día automatizamos más los procesos cotidianos gracias al avance tecnológico y así mismo los procesos ilegales también son facilitados. Este hecho ha creado la necesidad de que las autoridades deban especializarse y capacitarse en nuevas áreas en donde las tecnologías de Información y Comunicación se conviertan en herramientas necesarias en auxilio de la Justicia y la persecución de delito y delincuente.

La informática forense está adquiriendo una gran importancia dentro del área de la información electrónica, esto debido al aumento del valor de la información y/o al uso que se le da a ésta, al desarrollo de nuevos espacios donde es usada (por Ej. El Internet), y al extenso uso de computadores por parte de las compañías de negocios tradicionales (por Ej. bancos). Es por esto que cuando se ejecuta un cybercrimen, muchas veces la información queda almacenada en forma digital. Sin embargo, existe un gran problema, debido a que los computadores guardan la información de forma tal que no puede ser recolectada o usada como prueba utilizando medios comunes, se deben utilizar mecanismos diferentes a los tradicionales. Es de aquí que surge el estudio de la computación forense como una ciencia relativamente nueva.

Resaltando su carácter científico, tiene sus fundamentos en las leyes de la física, de la electricidad y el magnetismo. Es gracias a fenómenos electromagnéticos que la información se puede almacenar, leer e incluso recuperar cuando se creía eliminada.

La informática forense, aplicando procedimientos estrictos y rigurosos puede ayudar a resolver grandes crímenes apoyándose en el método científico, aplicado a la recolección, análisis y validación de todo tipo de pruebas digitales.

2. Metodología

Para realizar este análisis tenemos que separar la información en dos tipos para facilitar nuestra investigación

2.1 Análisis de la Información Volátil

Los datos volátiles de un ordenador víctima suele contener información importante que nos ayuda a determinar el "quién", "cómo", y, posiblemente, "por qué" del incidente.

Para responder estas preguntas, entre los datos volátiles recopilados podemos adquirir esta información:

- La Fecha y Hora del sistema
- Las conexiones actuales de red
- Puertos TCP/UDP abiertos
- Cuales aplicaciones ejecutables están abriendo puertos TCP/UDP
- Tabla de nombres de NetBIOS en el caché
- Sesiones de Usuarios abiertas
- La tabla de enrutamiento interna
- Procesos que se están ejecutando
- Servicios en ejecución
- Tareas programadas
- Archivos abiertos
- Proceso de volcados de memoria

2.2 Análisis de la Información No Volátil

La Información no volátil la podríamos conseguir analizando mediante el uso de una duplicación de imagen forense, pero este procedimiento puede ser complicado ciertas veces. La información no volátil que se puede conseguir antes de la duplicación forense es la siguiente:

- Versión del Sistema y el Nivel del Parche
- Sistema de archivos de hora y marca de fecha
- Registro de datos
- La política de auditoría
- Un historial de los inicios de sesión
- Registro de eventos del sistema
- Cuentas de usuario
- Registros de IIS
- Archivos sospechosos

2.3 Análisis de la Imagen Forense

Para completar nuestra investigación debemos indagar en el sistema de archivos de la víctima y tratar de recuperar cualquier archivo sospechoso, pero nuestra experiencia nos ha enseñado que el atacante siempre borra los archivos más relevantes a la investigación.
Para llevar a cabo este análisis primero debemos reducir nuestro conjunto de datos, así podremos analizar los datos eficientemente. Además realizaremos una búsqueda de caracteres para poder identificar archivos relevantes o fragmentos de estos.

3. Desarrollo del proyecto

La Institución bancaria JBR se comunicó con nuestros consultores en Investigación Forense el día 1 de Octubre del 2003 solicitando nuestra ayuda, ellos habían sufrido un ataque el cual gracias al Equipo de Respuesta a Incidentes del Banco ya había sido detectado. Ellos logran capturar toda la información volátil al momento del ataque mediante el uso de distintos métodos y herramientas forenses que serán

explicados más adelante en este capítulo.

Se cree que el atacante logró instalar herramientas para su beneficio por medio de una puerta trasera anteriormente abierta por el mismo sujeto. Nuestro equipo de consultores analizará toda la evidencia que nos facilitó el banco para comprobar si esta suposición es cierta.

Aunque el Equipo de Respuesta a Incidentes del Banco hizo un excelente trabajo capturando toda la información volátil posible, solo eso no bastaría para identificar de forma eficaz al atacante por esto también se realizó una duplicación forense del equipo afectado utilizando las herramientas respectivas para mantener la cadena de custodia intacta y de esta manera realizar una investigación transparente y confiable.

3.1 Análisis de la Información Volátil y No Volátil

El objetivo principal de este análisis era identificar si hubo o no hubo un incidente. Con la información volátil y no volátil durante la captura de datos en vivo nos indica que una intrusión no autorizada sí ocurrió.

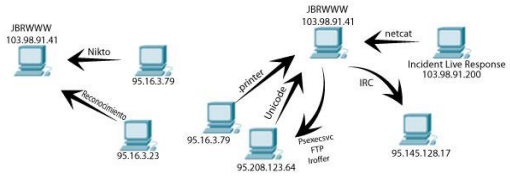

Figura1: Conexiones de Red durante la Intrusión a las 9:08 de 01/Oct/03

A pesar de que no teníamos los registros de los eventos de seguridad de Windows, los registros de IIS indicaron que JBRWWW fue escaneado con una herramienta conocida como Nikto a las 6:51:17PM el 23 de Septiembre del 2003, desde la dirección IP 95.16.3.79. Aproximadamente unos 18 segundos antes del escaneo, una página Web por defecto de IIS fue accedida desde la dirección IP 95.16.3.23. Es común antes y después de un ataque revisar el estado del sitio web para acceder a tal página. Esto puede indicar que el atacante tenía acceso o control del sistema en 95.16.3.73 o quizás estaba trabajando con alguien más quien lo hizo.

Luego el 1 de Octubre del 2003 un atacante desde la dirección IP 95.208.123.64, posiblemente trabajando en conjunto con 95.16.3.79, inició un ataque exitoso Unicode después de haber fallado con el desbordamiento de búfer del ".printer".

Aunque los detalles no han sido determinados, parece que los atacantes fueron capaces de ejecutar comandos en JBRWWW a través del ataque Unicode IIS y se estableció una sesión FTP de regreso en los sistemas. Además fueron capaces de instalar netcat e iroffer en el directorio C:\WINNT\system32\os2\dll. Esta figura nos mostrará una secuencia general de las actividades basadas en la información anteriormente analizada.

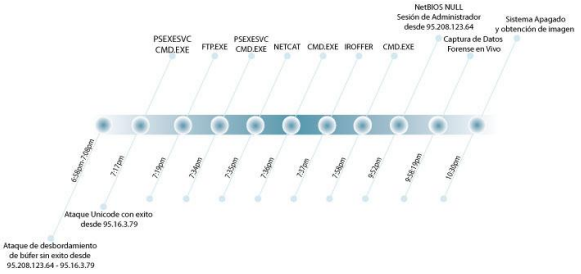

Figura 2: Línea de tiempo del ataque el 01/Oct/03

3.

Pudimos observar como el atacante concentró su actividad en contra del Web Server 103.98.91.41 y no atacó ninguna otra máquina del Banco JBR. El atacante ejecutó su reconocimiento desde la dirección IP 95.16.3.23 y ataques desde las direcciones IP 95.208.123.64 y 95.16.3.79. Aseguramos que el atacante usó PsExec para ganar acceso interactivo al sistema y lo usó para transferir un programa llamado iroffer.exe. Vemos que iroffer.exe fue usado para acceder a un servidor IRC en la dirección IP 95.145.128.17.

Toda la evidencia basada en red fue derivada de archivos Libpcap creados con Tcpdump. A pesar de que algunas organizaciones coleccionan información de esta manera algunas otras no lo hacen, aun así se pudo recrear la información estadística, de alerta y de sesión de los dos archivos Libpcap iniciales; existen otros métodos para capturar esta información sin necesidad de coleccionar todo el tráfico en crudo.

3.3 Análisis de la Imagen Forense

Para completar nuestra investigación debemos indagar en el sistema de archivos de la víctima y tratar de recuperar cualquier archivo sospechoso, pero nuestra experiencia nos ha enseñado que el atacante siempre borra los archivos más relevantes a la investigación.
Para llevar a cabo este análisis primero debemos reducir nuestro conjunto de datos, así podremos analizar los datos eficientemente. Además realizaremos una búsqueda de caracteres para poder identificar archivos relevantes o fragmentos de estos.

Anteriormente habíamos determinado que el directorio C:\winnt\system32\os2\dll contenía herramientas que el atacante había depositado, tales como iroffer.exe. Empezaremos analizando este directorio con la herramienta Authopsy del Sleuth Kit y ver si encontramos algún archivo de interés.

En esta figura encontramos varias rarezas que han sido

marcadas de color rojo por el programa Autopsy.

Primero tenemos unos archivos con el inodo de número cero, los cuales somos incapaces de poder recuperar. Los otros archivos tienen bloques de datos que han sido reasignados, el archivo mybot.xdcc.tmp y el archivo mybot.xdcc.txt poseen el mismo inodo que el archivo mybot.xdcc.bkup, el cual es 8123-128-1.

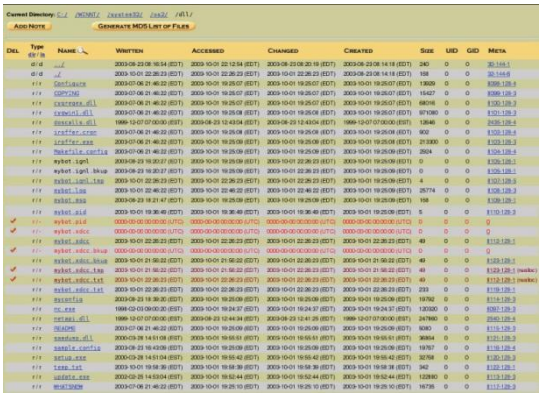

Figura 3: Archivos borrados en el directorio C:\winnt\system32\os2\dll

Solo con esto no podemos obtener mucha información relevante ya que la mayoría de atacantes sobrescribe sobre sus huellas, por ende procederemos a adquirir los metadatos de todos los archivos que existen en la evidencia ya sean borrados o lógicos; con los metadatos podremos realizar una línea de tiempo de la actividad en los archivos y así podremos reducir nuestro rango a investigar. Para esto utilizaremos las facilidades que nos brinda Autopsy y procederemos a examinar los archivos que fueron creados aproximadamente a las 7:25 PM del 01/10/2003, que fue el momento en que se creó la mayoría de archivos del directorio C:\winnt\system32\os2\dll.

En esta imagen observaremos que primero fue creado psexecsvc.exe en el sistema aproximadamente a las 6:58PM. Este es el servicio que es creado cuando un usuario remoto ejecuta PsExec, una herramienta a control remoto.

Asumimos que alguien usó PsExec, el cual requiere ser validado como Administrador en la máquina víctima. Luego, vemos que nc.exe fue creado en la máquina aproximadamente a las7:24PM, este archivo pertenece a la herramienta netcat. A las 7:25PM Iroffer fue transferido a la máquina. A las 7:48 y 7:52, update.exe fue transferido a JBRWWW. Luego después de las 10:00PM varios componentes de Iroffer fueron creados.

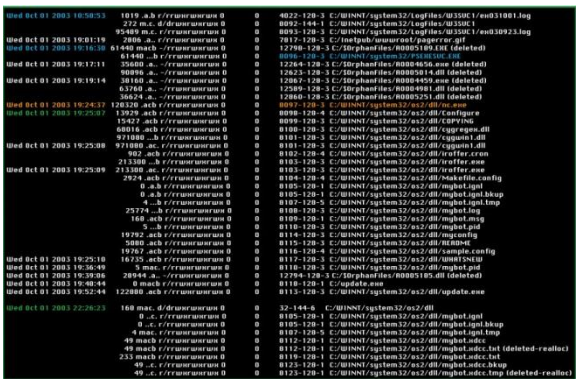

Figura 4: Archivos creados durante el 1 de Octubre del 2003

Como podemos ver alguien usó PsExec para ganar acceso a JBRWWW, posiblemente adivinando las contraseñas, después varias herramientas fueron transferidas a la máquina por el atacante y por último Iroffer fue ejecutado tras una hora de su transferencia.
Por último procederemos a realizar una búsqueda de caracteres con la opción que nos brinda Autopsy; primero usamos la opción extraer caracteres y luego podremos realizar la búsqueda de palabras claves, como sabemos nuestro atacante dejó una herramienta llamada IROffer en el servidor, veremos si podemos averiguar algo con esto:

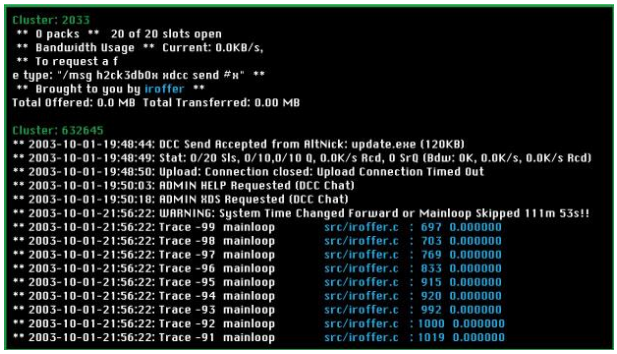

Figura 5: Búsqueda de caracteres (iroffer)

La siguiente búsqueda relevante que haremos es la del archivo encontrado en el directorio C:\update.exe veremos si podemos encontrar alguna relación con otros archivos sospechosos:

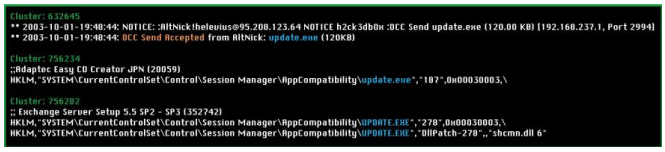

Figura 6: Búsqueda de caracteres (update.exe)

Hemos presentado las salidas más relevantes en las figuras 59-60 y en esta última podemos apreciar que update.exe pudo haber sido localizado en nuestro sistema por el protocolo DCC. El protocolo DCC por lo general es asociado con la herramienta IRC, el cual es una herramienta muy común que los atacantes usan para controlar computadoras remotamente.

Además podemos continuar este rastro generando el informe del clúster 632645 y nos mostrará una relación con un archivo lógico llamado c:/winnt/system32/os2/dll/mybot.log, el cual parece ser un archivo de registros para las herramientas del atacante. Sin más información podemos suponer que este registro pertenece al robot IRC llamado IROffer.

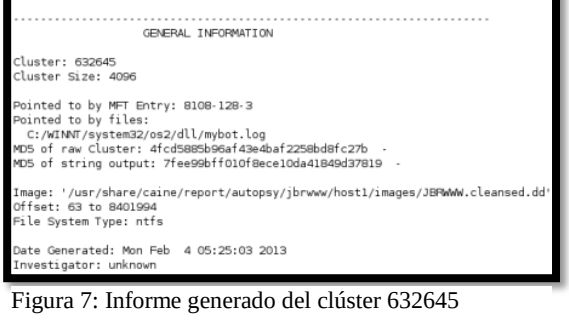

Figura 7: Informe generado del clúster 632645

Tras examinar el archivo mybot.log encontramos una cabecera el nombre de iroffer y más adelante en este mismo archivo veremos el intento de la transmisión del archivo update.exe.

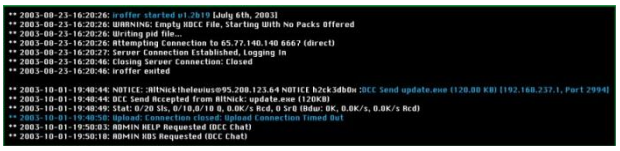

Figura 8: Partes relevantes del archivo mybot.log

Este archivo nos muestra que el archivo update.exe no pudo ser transmitido con éxito hacia la máquina víctima. El atacante intentó subir el archivo, pero falló dejándonos un archivo con longitud cero, como vemos en el directorio raíz de la máquina victima JBRWWW.

4. Conclusiones

Tras haber analizado varias evidencias hemos confirmado la presencia de un atacante gracias al registro de las conexiones que nos brinda la herramienta netstat, pudimos localizar conexiones desde la IP 95.28.123.64 el cual tenía varios puertos abiertos para herramientas como Psexec, IROffer, IRC

La revisión de los registros IIS nos demuestran que hubo un ataque anteriormente, el día 9 de Septiembre del 2003 hubo un ataque de reconocimiento desde la dirección 95.16.3.79 con la herramienta online Nikto.

El día 1 de Octubre del 2003, un ataque Unicode y Double Decode fueron ejecutados a nuestra victima desde las direcciones IP 95.208.123.64 y 95.16.3.79 logrando darle privilegios al atacante de ejecutar la línea de comandos cmd.exe bajo el usuario IUSR_JBRWWW. Esto le permitió establecer una sesión FTP, además pudo instalar netcat e iroffer en el directorio C:\WINNT\system32\os2\dll.

Tras analizar los archivos de la actividad de red capturados con snort pudimos confirmar que hubo un escaneo de vulnerabilidades con la herramienta Nmap. La revisión de los registros de alertas de Argus nos muestra varios ataques de reconocimiento al server desde la IP 95.16.3.79, pero además una conexión de nuestro server a la IP 95.145.128.17, el cual asumimos que pertenece a un servidor IRC.

En las sesiones capturadas por tcpflow encontramos un sesión IRC con el Nick h2ck3db0x donde al atacante intenta transferir archivos a través del protocolo DCC, pero sin éxito por algún error de configuración entre el cliente y servidor.

Al analizar la línea de tiempo de actividad en los archivos creada por Autopsy pudimos asegurar que luego del ataque de desbordamiento de búfer el atacante logró ejecutar psexec con un usuario Administrador, el cual pudo ser obtenido por ataque de fuerza bruta. Esto le permitió instalar netcat e iroffer y con este pudo conectarse al servidor IRC y tener visión de los archivos en JBRWWW.

Gracias a la búsqueda de caracteres con palabras claves sospechosas pudimos confirmar el intento de transmisión de update.exe a través del protocolo DCC, el cual no tuvo éxito dejándonos un archivo de longitud cero.

Por último podemos concluir que un ataque bien planeado tuvo éxito, éste logró tener acceso solo al Web Server en la dirección IP 103.98.91.41, pudo haber tenido más control en el sistema, pero fue detectado a tiempo sin causar grandes pérdidas.

Al ser una institución bancaria se pudo haber comprometido mucha información valiosa, pero gracias a que el ataque fue detenido a tiempo el atacante no pudo conseguir nada, por lo que la institución bancaria no debería presentar un informe a sus clientes finales.

5. Recomendaciones

Una de las primeras cosas que pudimos notar en nuestra investigación fue la falta de políticas de auditoría, esto nos hizo perder mucha información valiosa para nuestra investigación que nos pudo haber facilitado el trabajo, por lo que se recomienda configurar estas políticas para poder mantener un registro de inicios de sesión.

Se recomienda también mantener actualizado todo el sistema para evitar que los intrusos aprovechen exploits conocidos y tomar control del sistema como se lo hizo en este caso.

Aunque en este caso el ataque pudo ser neutralizado por un usuario, no está de más decir que mantener informados a los usuarios sobre cómo aplicar las políticas de seguridad y mantener sus contraseñas privadas como es debido evitará que ocurran incidentes parecidos en el futuro.

Los administradores del sistema deben mantenerse siempre informados sobre las nuevas amenazas que aparecen día a día para poder defenderse de la mejor manera posible contra estos atacantes.

Al instalar actualizaciones o programas de cualquier tipo asegurarse que solo sean de una fuente confiable, así el sistema se mantendrá limpio y en un funcionamiento óptimo. Asegurarse de descargar y ejecutar archivos de los cuales sabemos su procedencia.

Al momento de instalar scripts en el sitio Web asegurarse de que no contengan errores, esto lo logramos relizando una búsquedade los scripts en sitios

como milw0rm.com para ver que estos no contengan errores.

Hacer una copia de seguridad del sitio. Mantener los archivos en otro PC, USB o Disco Duro Externo.

6. Referencias

[1] Cano Martines, J. J., Mosquera González, J. A., & Certain Jaramillo, A. F. (Abril de 2005). Obtenido de Evidencia Digital: contexto, situación e implicaciones nacionales: http://derecho.uniandes.edu.co/derecho1/export/derecho/descargas/texto/NasTecnologias6.pdf

[2] Brezinski, D., & Killalea, T. (2002). Obtenido de RFC 3227: Guidelines for Evidence Collection and Archiving. Network Working Group. February: http://www.rfceditor.org/rfc/rfc3227.txt

[3] CASEY, E. (2004). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.

[4] Dawson, K., & Kirch, O. (2002). Guía de Administración de Redes con Linux. Obtenido de http://linux.casa.cult.cu/docs/garl2/x-087-2-iface.netstat.html

[5] Galarza, M. D. (2010). Obtenido de Informáticos, Equipo de Investigación de Incidentes y Delitos: WWW.EIIDI.COM

[6] Lima, M. d. (2007). Obtenido de http://www.monografias.com/trabajos17/delitos-informaticos/delitos-informaticos.shtml

[7] López Delgado, M. (s.f.). Análisis Forense Digital. Obtenido de http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

[8] Martines Jeimy, J. C. (Junio de 2006). Revista ACIS. Obtenido de Introducción a la informática forense: http://www.acis.org.co/fileadmin/Revista_96/dos.pdf