Revista Digital Universitaria
10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

ARTICULO

EL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES Y SUS FUTUROS RIESGO

Israel Becerril Sierra
Especialista de seguridad informática en sistemas Unix
UNAM-CERT

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

Resumen

En este artículo se tratan temas relacionados con el análisis forense aplicado a dispositivos móviles. Se describen los objetivos a seguir en dicho estudio, se plantea la búsqueda de información almacenada en ellos bajo un escenario en el que se ha cometido un delito o violado una política. Como consecuencia, surge la necesidad de reflexionar sobre las carencias que tienen las leyes para poder definir un dispositivo móvil como evidencia en un caso legal; finalmente, se predicen las estrategias que los intrusos estarán usando para vulnerar un dispositivo móvil y afectar a sus usuarios, además de hacer énfasis en la evolución que tendrán los virus y gusanos para infectar dispositivos móviles que puedan ser usados con fines maliciosos.

Palabras Clave: Dispositivos móviles, Forense en celulares, Botphones, espionaje, evidencia digital, derecho informático.

INICIO

Casi todos usamos un celular

Los teléfonos celulares, así como todos los dispositivos móviles, son aparatos que en la actualidad utiliza la mayoría de la gente. Al igual que las computadoras, estos artefactos han dejado de ser un lujo, pues se han convertido en una necesidad. Además de cumplir con la función básica de un celular (realizar y recibir llamadas telefónicas), la mayoría de ellos cuentan con funciones especiales, entre las que encontramos el envío de mensajes de texto cortos (SMS), mensajes de texto multimedia (MMS), mensajes instantáneos (IM), correos electrónicos, navegar en Internet y administrar información personal (PIM) con ayuda de ciertas aplicaciones, entre otras.

La mayoría de los celulares permiten a los usuarios la instalación de ciertas aplicaciones, así como el almacenamiento de información personal y confidencial, ésto sin importar el sistema operativo, la forma en la que se sincroniza la información o cómo se conectan con los equipos de cómputo. Los celulares son parte de la tecnología que nos rodea hoy en día, debido a esto su mejora y actualización es constante.

Cuando un celular es involucrado en un crimen o en un incidente, los analistas forenses requieren de herramientas que permitan obtener una apropiada y rápida recuperación de la información almacenada en el dispositivo. La información obtenida, después de ser analizada, servirá para redactar un reporte detallado de las actividades realizadas, incluyendo fechas, con la finalidad de buscar evidencias que revelen la causa y forma en la que se llevó acabo un delito o se violó una política, en algunos casos esta información puede obtenerse, aun cuando haya sido borrada.

Análisis forense en celulares

En este trabajo normalmente se involucran la identificación, preservación (no modificar la evidencia), obtención, documentación y análisis de información. En el análisis forense clásico se siguen ciertas metodologías y procedimientos bien definidos. Muchas de estas metodologías pueden ser adaptadas al análisis forense en celulares. Tales consisten generalmente en los siguientes pasos:

- Preparar una copia de la evidencia digital (sin tener que arriesgar la integridad de la evidencia).
- Examinar la copia obtenida con la finalidad de recuperar la información.
- Analizar la información recuperada.
- Crear un reporte describiendo los datos recuperados en todo el procedimiento de análisis.

Las herramientas de análisis forense intentan facilitar el trabajo en cada uno de estos pasos, enfocados a crear un reporte final de calidad y veraz.

Este tipo de trabajo en celulares es un tema relativamente nuevo, surge a raíz del análisis forense en equipos de cómputo, enfocado a servidores de trabajo y red. Un dispositivo móvil es capaz de almacenar información digital en una memoria interna o externa, en una pequeña tarjeta que traen todos los celulares (SIM) o enviarla a otro dispositivo haciendo uso de Internet. Toda información digital puede convertirse en evidencia que revele detalles de actividades realizadas en el dispositivo móvil; dichas actividades deben investigarse contestando las mismas preguntas en las que se basa el análisis forense clásico: ¿qué se hizo?, ¿cómo se hizo? y ¿en qué orden se hizo? Las discrepancias entre el análisis forense a celulares y el análisis forense clásico existen debido a varios factores, entre los que se incluyen:

- El diseño orientado a la facilidad de transporte (por ejemplo el tamaño y las pilas que requieren de una interfaz y hardware especial).
- El sistema de archivos almacenado en una memoria volátil contra memorias no volátiles.

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

- El comportamiento de hibernación, la suspensión de procesos cuando se apaga y se vuelve a activar.
- La diversidad de sistemas operativos embebidos.
- Ciclos cortos de producción para introducir nuevos dispositivos.

La mayoría de los dispositivos móviles ofrecen excelentes sistemas operativos básicos con capacidades competentes entre ellos. Sin embargo, la diversidad de familias existentes en el mercado difieren en áreas como tecnología del hardware, características avanzadas, incluso en el aspecto físico.

En un caso práctico de un dispositivo móvil con tecnología GSM, puede trabajarse en dos escenarios: el primero inicia con la tarjeta SIM instalada en el celular y el segundo parte simplemente de una tarjeta SIM, sin necesidad de conocer el modelo y fabricante del dispositivo móvil donde fue instalada la tarjeta SIM.

Un dispositivo móvil como parte de un delito

El tema de la extorsión telefónica se ha incrementado por la facilidad con la que se puede adquirir un celular, sin necesidad de que el usuario proporcione datos de identificación personal. Cada vez que una persona mal intencionada tenga acceso a un celular que no necesariamente le pertenezca, puede utilizar la información encontrada para hacer una extorsión telefónica. La forma más común de operar de los extorsionadores telefónicos se basa en hacer llamadas al azar, y en las subsecuentes que el extorsionador realice, sólo necesitará cambiar los dos últimos dígitos. Si la llamada es contestada, el extorsionador exige grandes cantidades de dinero a cambio de la libertad de un familiar presuntamente secuestrado. En este tipo de casos un analista forense, utilizando las herramientas correctas, podría obtener las últimas llamadas realizadas y contestadas, los últimos mensajes de texto enviados y recibidos, los últimos mensajes de texto multimedia, los mensajes instantáneos, correos electrónicos e incluso información personal, sin olvidar los archivos de imágenes que podrían ayudar a describir acciones delictivas. El analista, al encontrar todos los eventos registrados en el dispositivo móvil, tendrá elementos suficientes para asegurar que se ha realizado un acto delictivo y culpar o exonerar al dueño del dispositivo.
Por diversos que sean los dispositivos móviles, tecnológicamente puede ser fácil encontrar evidencias digitales, esta misma diversidad acarrea consigo una desventaja al momento de crear leyes internacionales que puedan aplicarse en cualquier país en el que se esté haciendo mal uso del dispositivo móvil. La velocidad con la que cambia la tecnología en los dispositivos móviles es mayor comparada con la velocidad en que cambian las leyes de un país, pudiendo significar un problema si se considera que un intruso puede diseñar una estrategia de ataque, usando un dispositivo móvil desde un país donde no existan leyes que consideren la evidencia digital como parte de un delito.

Futuras amenazas

De acuerdo con la actual evolución tecnológica de los dispositivos móviles existen nuevas bondades que los asemejan cada vez más a una computadora, del tamaño de un celular o un asistente personal digital (PDA), por lo que estos dispositivos presentan la capacidad de funcionar como una cámara digital que obtiene imágenes y video de alta calidad, un reproductor de música con capacidad de almacenar hasta 250 canciones (en el peor de los casos), una agenda personal con capacidad de conectarse a Internet, de forma inalámbrica, para consultar correo electrónico o cualquier sitio Web, un sistema de posicionamiento global que ayude a localizar la ubicación física de quien porta el dispositivo, así como la ruta más corta para llegar a un destino, finalmente, un teléfono que pueda llevarse a casi cualquier parte del mundo, con la confianza de que el dispositivo hará lo necesario para negociar la renta de señal y realizar una llamada o videollamada, todo ésto en un mismo dispositivo de tamaño atractivo.

Para que los nuevos dispositivos móviles puedan ser aprovechados al máximo, la mayoría de los proveedores de servicios de Internet y telefonía están instalando y ajustando su infraestructura para que el intercambio de información sea más rápido y accesible en casi cualquier parte del mundo. Con estos avances en la tecnología, los analistas forenses predicen que a corto plazo, los vectores de ataques estarán enfocados a apoderarse de los dispositivos móviles conectados a Internet. Los intrusos aprovecharán el ancho de banda para infectar a los dispositivos móviles con algún virus o gusano. Una vez infectados, los intrusos programarán instrucciones que reporten las actividades de las víctimas, para lo cual recibirán imágenes o videos en tiempo real que detallen el lugar donde se encuentre las víctimas, las personas que lo acompañan, la forma como viste la víctima e incluso quiénes la rodean. El intruso estará recibiendo de forma automatizada una serie de imágenes y videos en un servidor central, desde el cual podrá enviar órdenes para aumentar o disminuir la frecuencia a la que el dispositivo móvil mandará archivos multimedia. En el ataque también pueden incluirse conversaciones privadas obtenidas gracias al dispositivo móvil que la víctima porte en la bolsa del pantalón, en la camisa o atado a la cintura.
Esta nueva forma de espionaje puede ser nombrada como "Botphones", haciendo alusión al término "bot", utilizado para nombrar un equipo de cómputo comprometido que puede ser controlado remotamente tanto de forma centralizada como descentralizada.

Siguiendo la misma línea de los "Botphones", otro vector de ataque puede estar basado en las conexiones de salida que realiza un dispositivo móvil. Con esto podemos pensar en una negación de servicio provocado por miles de dispositivos móviles comprometidos, que intenten hacer conexiones a un servidor al mismo tiempo, hasta lograr impactar la disponibilidad de un servicio.

Este y otros ataques forman parte de los problemas que estaremos sufriendo como sociedad. Mientras no existan leyes que respalden a las víctimas, tendremos que ir inventando nuevas formas para evitar caer en manos de los intrusos y no hacer de la tecnología un instrumento que los intrusos usen para beneficiarse.

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

Conclusiones

Los dispositivos móviles comenzaron siendo un lujo en el que el color, marca, modelo y dimensiones, daban estatus social. A medida que pasó el tiempo, se convirtieron en una necesidad, pues son un medio de comunicación al alcance de casi cualquier bolsillo. Los sociólogos comentan que un dispositivo móvil es parte de la vida de una persona, tanto que al momento de adquirirlo y con la gran variedad existente en el mercado, la mayoría de las personas eligen un dispositivo móvil pensando más en su aspecto físico que en las características internas; no obstante, aseguran que esto va cambiando, pues la tecnología ha sabido combinar el potencial interno con las características físicas. Esto hace que el número de dispositivos móviles con capacidad de conectarse a Internet se incremente de forma considerable.

El reto de la tecnología no sólo será innovar sobre dispositivos móviles que sean de dimensiones pequeñas para que sea fácil portarlos, o crear dispositivos con materiales que alarguen su vida útil, sino también deberá innovarse para crear dispositivos móviles que brinden seguridad a sus usuarios, ésto es: que puedan almacenar información sin la incertidumbre de que cualquier persona en alguna parte del mundo -y sin conocimiento del usuario -, pueda acceder, crear o modificar dicha información.

En muchos países se ha invertido más en tener acceso a la tecnología que en leyes que ayuden a regular su uso. Esta crisis ha provocado que los intrusos diseñen sus ataques desde países en donde una demanda no procedería. En la medida en la que un país no tome en cuenta la importancia del derecho informático, los intrusos seguirán viendo como blanco de ataque los dispositivos móviles, incrementando la amenaza a la que están expuestos los usuarios.

Los “Botphones” son un concepto utilizado para describir nuevas formas de infectar a un dispositivo móvil. Un “Botphone” es un dispositivo móvil comprometido por un intruso para monitorear las actividades de sus víctimas, ya sea obteniendo grabaciones de conversaciones, capturando imágenes o video, hasta haciendo uso de su infraestructura para atacar a otros usuarios. Cada vez que un “Botphone” se conecta a Internet, enviará una alerta al intruso para indicar que está disponible y a la espera de cualquier orden sin que se percate el usuario.

Bibliografía

AYERS Rick, Cilleros Nicolas, Daniellou Ronan, Jansen Wayne. Cell Phone Forensic Tools: An Overview and Analysis, National Institute of Standard and Technology (NISTIR) 7387, extraído de www.http://csrc.nist.gov/publications/nistir/nistir-7387.pdf, 2007

AYERS Rick & Jansen Wayne. Guidelines on Cell Phone Forensics. Extraido de National Institute of Standard and Technology de www.http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf. ,2007

BEJTLICH Richard, Jones Keith, Rose Curtis W. Mobiledevice Forensics: Real Digital Forensics: Computer Security and Incident Response, Pearson Education, USA., 2005.

DELAITRE Aurelien & Jansen Wayne. Reference Material for Assessing Forensic SIM Tools, nternational Carnahan Conference on Security Technology. Octubre. 2007 en www.http://csrc.nist.gov/groups/SNS/mobile_security/documents/mobile_forensics/Referenc e%20Mat-final-a.pdf. , 2007

SALES Jane. Symbian OS Internals: Real-time Kernel Programming, Wiley, USA, 2006.

SUÁREZ Gutiérrez, Carlos. Celulares y privacidad en ENTER@TE. Año 6 Núm. 6 2007. http://www.enterate.unam.mx/Articulos/2007/junio/art4.html.

GFI. Targeted cyber attacks. http://www.gfi.com/whitepapers/cyber-attacks.pdf

Wikipedia, Botnet, http://es.wikipedia.org/wiki/Botnet

Wikipedia, Bot, http://es.wikipedia.org/wiki/Bot