Virus para móviles

Diagnosis del problema

El verano pasado saltaba la noticia. Durante la celebración de los Mundiales de Atletismo 2005 en el estadio olímpico de Helsinki cientos de teléfonos móviles fueron infectados por un virus llamado *Cabir* a través de la conexión inalámbrica de corto alcance (*Bluetooth*). Pocos meses después, apareció otro nuevo virus – *Commwarrior* – capaz de replicarse no solo a través de Bluetooth sino también a través de mensajes de texto con imágenes y sonido (MMS) y enviarse a las direcciones y números de la agenda de sus víctimas. Por primera vez, los virus para teléfonos móviles se convertían en algo mucho más real y más cercano de lo que se creía.

El Instituto Nacional de Tecnologías de la Comunicación (INTECO), con sede en la capital leonesa, informaba recientemente, a través de la web de su Centro de Alerta Temprana Antivirus, sobre la detección de la aparición de un nuevo gusano de correo electrónico, Eliles.A, que no sólo se propaga a otros ordenadores sino que también lo hace a través de mensajes de texto (SMS) a teléfonos móviles. Dichos mensajes incluyen un link que descarga en el móvil un archivo malicioso llamado “Antivirus.sis” que puede afectar al sistema operativo de determinados modelos de teléfonos móviles.

Dadas las capacidades de extensibilidad y flexibilidad que se van observando en los sistemas software para plataformas móviles, el peligro de virus, gusanos y caballos de Troya está comenzando a aparecer en los terminales de telefonía móvil.

Los métodos de infección utilizados por los virus son (ordenados según su incidencia):

1. Las conexiones inalámbricas *Bluetooth*
2. El envío de mensajes multimedia
3. Las descargas de aplicaciones que no son lo que dicen ser
4. El intercambio de tarjetas de memoria.

Echando la vista atrás, fue en 2000 cuando se informó de la existencia del primer software malicioso capaz de funcionar sobre ciertos tipos de agendas electrónicas y teléfonos móviles. En los últimos meses está apareciendo toda una lista de virus, gusanos y troyanos que afectan a diversos sistemas operativos específicos de dispositivos móviles y agendas electrónicas, lo que puede constituir el principio de las nuevas tendencias en código malicioso.

Hasta el momento, afortunadamente no se han producido en España casos de suficiente importancia – ni por el número de infecciones ni por la gravedad de los daños causados – que puedan ser comparables con los casos más importantes en el ámbito de los ordenadores, pudiendo considerarse incluso anecdóticos los ataques de virus móviles en nuestro país. El motivo principal de ello es que aún existen pocos virus y únicamente afectan a ciertos modelos de teléfono que incluyen sistemas operativos avanzados.

En cualquier caso, si bien hasta el momento no ha habido epidemias masivas ni casos muy graves, no debemos bajar la guardia.

Potenciales amenazas

No cabe duda de que la llegada de las tecnologías móviles e inalámbricas y su constante evolución ha revolucionado en los últimos años la forma en la que nos comunicamos y trabajamos. La proliferación de dispositivos y aplicaciones móviles ha traído consigo el incremento, constatado, de la productividad y eficiencia de las empresas, erigiéndose como una de las herramientas tecnológicas fundamentales para la mejora de la productividad corporativa. Sin embargo, una de las principales barreras que encuentran las empresas en el uso de estas tecnologías, es la seguridad de los datos.

Los servicios móviles que ya están disponibles o que lo estarán en un futuro cercano deberían estar soportados por sistemas que limiten al máximo las posibilidades de intrusión, propagación y robo de datos para uso fraudulento.

Históricamente no ha tenido mucha utilidad explotar las vulnerabilidades de la telefonía móvil debido al reducido número de usuarios y a la rigidez del software necesario para su funcionamiento. Las conexiones a Internet desde teléfonos móviles hasta hace poco tiempo eran limitadas, lentas y apenas existían aplicaciones que las utilizaran. Así, el desarrollo de software para teléfonos móviles prácticamente ha estado centrado en la generación de juegos y aplicaciones multimedia.

Además, la integración vertical de los operadores en la cadena de valor del mercado de la telefonía móvil –que impide el libre acceso a las redes – dotaba de mayor seguridad a sus plataformas. Los sistemas operativos instalados en dispositivos móviles generalmente son propietarios, por lo que casi hay tantos sistemas operativos como fabricantes de terminales.

La evolución hacia tecnologías de tercera generación está haciendo mucho más atractivo este campo y se prevé un aumento de los riesgos de seguridad de la telefonía móvil. Asimismo, la competencia entre operadores fabricantes y proveedores de servicios, ha desencadenado el lanzamiento de nuevos servicios de datos cada vez a precios menores con el objeto de ampliar y fidelizar a un mayor número de clientes. En consecuencia el

número masivo de servicios con una tarifa reducida ha hecho aumentar la demanda. Así pues, con la aparición de la tecnología 3G y los servicios de datos en tarifa plana de las operadoras, aumentan las facilidades para los usuarios para conectarse a Internet desde el dispositivo móvil, con lo que consecuentemente estarán más expuestos a ser infectados por un virus informático.

La difusión masiva de los virus en la telefonía y dispositivos móviles está hoy día limitada gracias a la ausencia de un sistema operativo estándar que permita la existencia de una plataforma homogénea de manera independiente a las peculiaridades intrínsecas del hardware de cada fabricante. Si bien la implantación de sistemas operativos estándares tendrá como efecto positivo el crecimiento del desarrollo de aplicaciones derivado del aumento del mercado potencial de usuarios, también es cierto que tendrá como consecuencia una detección más rápida de sus vulnerabilidades y que los programas maliciosos puedan afectar a un rango mayor de terminales.

Finalmente, el crecimiento de la capacidad de almacenamiento de datos en los dispositivos móviles, la sincronización de datos con el ordenador de nuestras oficinas o nuestras casas, la integración del correo electrónico y el desarrollo de aplicaciones empresariales y personales que nos permitan guardar datos y realizar operaciones que normalmente realizaríamos con un PC, necesariamente resultan muy atrayentes para los hackers.

Los atacantes, conscientes de todas estas circunstancias, están intentando sacar provecho de esta situación. De este modo, los riesgos se han multiplicado:

- A mayor número de servicios, surgen más posibilidades de encontrar vulnerabilidades explotables para intrusión, propagación y robo.

- A mayor número de clientes de servicios de pago, mayor es la probabilidad de capturar las claves de acceso y operación de usuarios incautos o confiados.

- A mayor cantidad de dispositivos móviles, mayor es el volumen de conexiones y, por tanto, mayor será la propagación de cada amenaza.

- A una más alta velocidad de transferencia, mayor será la rapidez de difusión de los virus y menores las capacidades de detección y bloqueo.

Los analistas del sector coinciden en señalar que este será un nuevo campo de lucha contra los hackers, que pueden utilizar los virus como arma para controlar los aparatos infectados y utilizarlos para su propio beneficio. El robo de datos personales o la utilización de “puertas traseras” (*backdoors*) por las que introducir publicidad – por desgracia tan conocidos por cualquier internauta – no tardarán en llegar a los dispositivos

móviles. Ahora se pueden descargar e instalar en ellos programas, y aunque la elección depende en último caso de los usuarios, la posibilidad de infección existe, pues éstos pueden ser engañados.

Así pues, una vez los dispositivos móviles se han convertido en terminales capaces conectarse a redes de datos, las medidas de seguridad de la información deben de ser similares a las que se toman respecto a los ordenadores personales. Incluso mayores, pues para usuarios de dispositivos móviles existe un riesgo añadido: la posibilidad de su pérdida o robo del terminal, por lo que la encriptación y el aislamiento de los datos personales dentro del dispositivo se hace imprescindible.

Solución al problema: recomendaciones de INTECO

Afortunadamente, en los mercados móviles e inalámbricos no sólo compiten los fabricantes de terminales y los operadores de telefonía; también los fabricantes de sistemas de seguridad compiten por ofrecer cada vez mejores soluciones y, por el momento, son capaces de evolucionar al tiempo que lo hacen los nuevos servicios.

Paralelamente, para no repetir los errores cometidos por la industria de los ordenadores, los fabricantes de dispositivos y operadores de telefonía deberán invertir y centrarse en la seguridad de las redes inalámbricas y en la seguridad de los dispositivos móviles, como la mejor defensa contra los ataques.

Del mismo modo, también los usuarios deben poner su granito de arena y deben continuar mejorando su cultura de seguridad, pasando a contemplarla como una medida de ahorro de tiempo y de dinero.

Así pues, es factible protegerse contra virus, gusanos, troyanos y otros códigos maliciosos en telefonía móvil y dispositivos similares siguiendo una serie de buenas prácticas. Por ello, desde INTECO ofrecemos las **siguientes recomendaciones con objeto de ayudar a los usuarios** a proteger sus dispositivos y seguir confiando en las tecnologías móviles:

- Actualice el software y sistema operativo de su sistema móvil e instale un antivirus (si su dispositivo móvil se lo permite).

- Si su dispositivo móvil está equipado con infrarrojos, no permita la recepción de datos de fuentes que no conoce o de las que desconfía.

- Si tiene *bluetooth* en su sistema móvil, téngalo desactivado por defecto cuando no necesite hacer uso de esta tecnología, y actívelo solo cuando vaya a usarlo. Tenga su sistema móvil siempre protegido con una contraseña –y recuerde cambiar la que

aparece por defecto en su dispositivo – para evitar que entren con facilidad desde otro sistema.

- Desconfíe de los mensajes recibidos de sitios no solicitados o remitentes desconocidos. Algunos contienen textos invitándole a instalar actualizaciones de seguridad que finalmente son códigos maliciosos; asegúrese de que provienen de una fuente fiable.

- Tenga especial atención si le envían algún enlace a una web para descargarse un vídeo, sonido o foto, ya que pueden contener código malicioso.

- Lea todos los acuerdos de usuario del software que se instale, para evitar el asentimiento a software del estilo "*spyware*", esto es, aplicaciones ajenas al terminal, cuya finalidad es capturar los datos y claves de usuario y del propio dispositivo.

- Si tiene un dispositivo móvil de última generación (3G), no instale aplicaciones que reciba por medio de un mensaje multimedia no solicitado (ni siquiera cuando provenga de fuentes conocidas o amigos) sin antes asegurarse de que son inocuas o que han sido revisadas por su sistema antivirus.

- Evite especialmente programas informáticos distribuidos ilegalmente ya que suponen una fuente mucho más probable de infección vírica.

Para dar solución a este nuevo fenómeno, INTECO ha constituido un grupo de trabajo – donde están presentes fabricantes y operadores – que liderará las acciones de seguridad de información en plataformas móviles.

Adicionalmente, INTECO ofrece gratuitamente a los usuarios, a través de su Centro de Alerta Temprana Antivirus, (www.alerta-antivirus.es), un servicio que permite obtener información detallada y permanentemente actualizada, y pone a su disposición gratuitamente las mejores herramientas para combatir los distintos tipos de virus informáticos y eliminar sus perjudiciales efectos. En este sentido, la base de datos del CATA recoge las principales amenazas para dispositivos móviles, recomendaciones para su prevención y protección, así como soluciones en caso de infección.