Conciencia Tecnológica No. 32, Julio-Diciembre 2006

Virus Telefónicos

Nota de divulgación

L.I. Gloria Leticia Betts Gómez (1), Cristopher Castillo Bernal (2)
(1) Miembro del Cuerpo Académico de Sistemas Distribuidos del Instituto Tecnológico de Aguascalientes,
(2) Alumno de la carrera de Informática del Instituto Tecnológico de Aguascalientes.
Departamento de Sistemas y Computación del Instituto Tecnológico de Aguascalientes, Av. A. López Mateos No. 1801, Fracc, Bonagens, Aguascalientes, Ags., C.P. 20256 Tel (449) 9105002, Fax (449) 9700423
gbetts@ita.mx, dashermx@hotmail.com

Resumen

Desde junio del 2004, y para algunos analistas desde el 2000, se registran virus en los dispositivos móviles, pero de acuerdo con los expertos, aún no se trata de una situación de alarma, aunque no está de más seguir algunas precauciones. Según dice F-Secure, firma europea de antivirus, la mayoría de éstos se han detectado en Europa, sobre todo en la plataforma GSM. De los virus telefónicos más conocidos se pueden mencionar los llamados Cabir, Skulls y CommWarrior. Empresas como Trend Micro ya están buscando cómo solucionar esta problemática, sacando al mercado antivirus que permitan eliminar estas amenazas.

Palabras clave

Virus telefónico, plataforma GSM, teléfono celular, Bluetooth, Mensajes Multimedia.

Introducción

La humanidad y el avance tecnológico ha ido de la mano en los últimos tiempos, ya que el ser humano ha visto la necesidad de ir desarrollando una serie de artefactos que permitan llevar una vida más cómoda en todos los sentidos. Lo anterior también ha acarreado una serie de problemáticas que el ser humano moderno tiene que enfrentar. En el área computacional ha habido un gran avance en muchos aspectos, pero esto también ha permitido que un grupo de gentes desarrolle una serie de barreras que hagan que este avance no sea tan placentero. A penas hace algunos años se había visto truncado el avance cómodo en el área anteriormente comentada, con el surgimiento de los virus informáticos, que son una serie de códigos maliciosos que tienen como finalidad el dañar algún elemento (ya sea programa, sistema operativo, aplicación, etc.) de un sistema computacional y que, en algunas ocasiones también permiten que las personas creadoras de estos virus tengan un beneficio económico con el ya conocido robo de identidad, que viene a ser la obtención ilegal de información de un equipo computacional. En últimas fechas ha salido a la luz una nueva amenaza que apenas comienza a darse a conocer alrededor del mundo: *los virus telefónicos*. Debido al gran boom que ha tenido el área de telefonía móvil en todo el mundo, y que ya ha llegado a nuestro país, algunas gentes ya comienzan a aprovecharlo de manera negativa con la creación de los virus ya anteriormente mencionados.

Cabir y skulls: Los primeros virus telefónicos conocidos

En el año de 2004 surgió el primer código maligno enfocado a la telefonía celular llamado *Cabir*. Dicho código era capaz de poder saltar de un teléfono celular a otro mediante la tecnología de red inalámbrica conocida como Bluetooth. Dicho virus realizaba la infección a celulares cuyo sistema operativo era Symbian. La forma de operar del virus era que al momento de que se ejecutaba algún fichero infectado dentro de la pantalla del teléfono celular se mostraba una leyenda que decía “Caribe”, y enseguida realizaba una serie de modificaciones en el sistema operativo para que se activara cada vez que se encendiera el teléfono. Después de hacer lo anteriormente mencionado, el virus Cabir comenzaba a buscar otras víctimas. Para ello se necesitaba que el nuevo teléfono infectado tuviera la ya mencionada conexión vía Bluetooth, mediante la cual detectaban otros teléfonos con el sistema operativo Symbian, a los que enviaba un archivo e infectaba. Al parecer, el virus fue desarrollado por un grupo rusos expertos en seguridad conocido como “29 ª”, que estaban más preocupados por poder traspasar la seguridad en nuevas tecnologías, que en hacer algún daño. Se detectó además que el Cabir se extendió a 16 países en aproximadamente 6 meses.

Otro de los primeros virus telefónicos es el llamado *Skulls* (calaveras en inglés). Este virus también surgió en el año 2004, pero a diferencia del antes mencionado Cabir, no tenía la capacidad de distribuirse mediante redes inalámbricas o similares. Dicho virus era descargado directamente por los mismos usuarios de teléfonos celulares que poseían el sistema operativo Symbian, con la finalidad de cambiar la apariencia

visual de la pantalla de su teléfono (era distribuido en Internet como un skin). En efecto, el virus Skulls cumplía su cometido, pero con el inconveniente de que realizaba un cambio muy drástico, ya que todos los íconos mostrados en la pantalla del celular eran cambiados por unas calaveras. Pero eso no era lo peor, dicho cambio evitaba que se pudiera acceder a aplicaciones habituales del dispositivo, como agenda, mensajes, cámara, tonos, etc, provocando que el teléfono celular ya no se pudiera utilizar como habitualmente se hacía. Sólo se dejaba libre el acceso a la función de envío y recepción de llamadas, siendo las demás funciones inaccesibles. F-Secure, la compañía antivirus que detectó dicho virus, recomendaba a todos los afectados que no apagaran su celular, pues esto dificultaría la desinstalación del virus. Ésta se podía llevar a cabo por medio de programas para la gestión de archivos que debían estar instalados en el teléfono antes de que este resultara infectado. Si no era el caso, la única solución era devolver el teléfono al estado en que éste se encontraba al salir de la fábrica. Cualquier modificación realizada posteriormente por su propietario se perdía.

Cabe hacer mención que un virus telefónico se comenzó a diseminar en Japón desde el 2003, un año antes de los mencionados anteriormente, pero este no tuvo una gran difusión ya que fue controlado de manera inmediata e incluso no se tiene registrado con algún nombre en específico.

Commwarrior: Virus con nueva forma de distribución

En la actualidad se están buscando nuevas vías de distribución de virus telefónicos, ya que la primera, que fue mediante red inalámbrica Bluetooth, no tuvo el éxito esperado, debido a que esta tecnología tiene un radio de acción muy corto además de que el destinatario tiene que configurar de manera manual su teléfono para poder recibir datos. Por ello se ha detectado el desarrollo de un nuevo tipo de virus que se distribuye mediante la mensajería multimedia (MMS). Este nuevo tipo de virus se llama *CommWarrior*.

La tecnología MMS consiste en una extensión del estándar SMS (Short Message Service) desarrollada por el 3GPP (Third Generation Partnership Project) que permite a los usuarios intercambiar mensajes multimedia entre teléfonos celulares o en general, entre dos dispositivos preparados para su uso. En un mensaje MMS puede incluirse audio, vídeo o imágenes estáticas, y es recibido por el destinatario de forma casi instantánea, al igual que un SMS. Para expandirse, CommWarrior escanea la libreta de direcciones del teléfono y se autoenvía de forma periódica a contactos seleccionados de forma aleatoria, en un mensaje en el que se incluye como fichero adjunto, animando al usuario a instalarlo como aplicación. Paralelamente, y al igual que su homólogo Cabir, CommWarrior intenta infectar a los dispositivos compatibles con el sistema operativo Symbian que se encuentren en las proximidades a través del protocolo Bluetooth.

CommWarrior presenta dos características que lo pueden llegar a hacer muy peligroso: por una parte es capaz de infectar a cualquier teléfono celular en cualquier rincón del mundo, con lo que detener una posible infección masiva puede ser muy difícil y, por otra parte, al trabajar silenciosamente en segundo plano, puede provocar un gasto económico importante al enviar mensajes MMS sin que el usuario se dé cuenta. Un defecto que se le puede adjudicar a este virus es el hecho de que todavía le da el poder al usuario final o destinatario de elegir el ejecutarse o no, pudiendo así no infectarse con sólo denegar su instalación.

Timofónica: conexión entre Internet y telefonía móvil

En el año de 2005, surgió un virus troyano llamado “Timofónica”, cuya finalidad era la de criticar las políticas y acciones de una compañía de telefonía celular española. Si bien este virus, escrito en VBS actuaba de forma muy similar a LoveLetter, su acción consistía en autoenviar copias suyas por medio de correo electrónico a todas las cuentas almacenadas en la libreta de direcciones del usuario e instalar un caballo de Troya que, al siguiente arranque, borraba los datos de la CMOS y formateaba el disco duro, de tal manera que no se pueden recuperar los datos perdidos por medio de ninguna aplicación específica. Pero la acción más «curiosa» de este virus, y la más destacable, era su capacidad de enviar mensajes cortos mediante SMS (*Short Message System*), el conocido protocolo empleado por millones de teléfonos móviles para mandar y recibir texto, en el que pueden viajar desde noticias hasta breves avisos o divertidos dibujos basados en ASCII.

Valiéndose de lo que en la Red es conocido como técnicas de «spamming», el i-worm de origen español explotaba la facilidad de los clientes de la compañía española de telefonía móvil GSM, de recibir correo electrónico en sus terminales por medio de una pasarela, correo.movistar.net, que lleva ya más de un año funcionando.

Mediante ésta resulta posible, anteponiendo el número de abonado como nombre de usuario, enviar e-mails a abonados de la compañía telefónica, de tal manera que la persona cuyo teléfono sea por ejemplo 609609609 podrá recibir en su móvil todos los mensajes que se envíen a la dirección 609609609@correo.movistar.net.

De esta forma, y por cada destinatario encontrado en la libreta de direcciones del usuario afectado, «Timofónica» genera un número de teléfono al azar, al que antepone uno de los prefijos de los abonados de la compañía celular (696, 609, 619, 629, 630, 639, 646, 649), y le envía un SMS por medio de la pasarela e-mail.

Es importante recalcar que se trata tan sólo de un simple mensaje de texto que ni siquiera porta consigo ficheros adjuntos, de modo que aquellos abonados que lo reciben no corren peligro alguno y podrán borrarlo sin problemas de ninguna índole. Es decir, hay que dejar bien claro que no se trata de un virus que atacará a los móviles como en algunos medios así se describió, sino simplemente un gusano que aprovechaba una característica de la pasarela sms-mail de la compañía celular española para enviar mensajes SMS a números de móvil aleatorios. Mensajes que en ningún caso causaban ningún daño al terminal y eran fácilmente eliminables.

Trend Micro Mobile Security: De los primeros antivirus enfocados a la telefonía celular

A finales del año 2004 TrendLabs, el centro global de investigación antivirus de Trend Micro, sacó al mercado uno de los primeros antivirus enfocados a teléfonos celulares y dispositivos móviles como PDA's, etc. Dicho antivirus recibe el nombre de Trend Micro Mobile Security. Entre las funciones de este nuevo antivirus para teléfonos celulares y computadoras de mano están las siguientes:

* Rastreo de virus en tiempo real, así como funciones de rastreo manual iniciado por el usuario.
* Anti spam para mensajes SMS, que incluye listas de remitentes bloqueados y de remitentes permitidos, así como bloqueo de remitentes sin número de identificación.
* Actualización instantánea de patrones de virus, a través de comunicaciones GPRS o mediante la sincronización de los patrones de virus previamente descargados a la PC.

Este antivirus es compatible con teléfonos celulares que utilicen el sistema operativo Symbian V.7.0 en adelante y Microsoft Windows Mobile 2003.

Conclusiones

Al parecer el desarrollo del mundo de los virus telefónicos apenas comienza, ya que ésta área podría tener un futuro muy prometedor, ya que la telefonía móvil es una de las ramas que ha tenido y tendrá muchos más avances lo que a su vez tendrá como consecuencia una mayor vulnerabilidad en los dispositivos.

Todo esto ha derivado de lo que antes era una simple necesidad de comunicación bipartita vía voz y que ahora se ha convertido en algo mucho más complicado como la utilización de voz, texto, audio, video, gráficos, juegos y más en un mismo dispositivo.

Actualmente los teléfonos que han sido infectados no han tenido una afectación muy grande, pero ya se comenta que se puede llegar a estar trabajando en este momento en virus mas dañinos que afecten de manera definitiva el uso de un teléfono celular.

Tendremos que estar listos para poder enfrentar una seria problemática que a lo mejor en estos momentos vemos un poco distante, pero que en un futuro no muy lejano, podremos llegar a ver como algo cotidiano y que llegará a repercutir en nuestra tranquilidad tanto emocional como económica.

Referencias

[1] Boletines Universidad Autónoma de México http://biblioteca.dgsca.unam.mx/cu/productos/boletines/index.html

[2] Belt Ibérica S.A. Analistas de Prevención http://www.belt.es/articulos/index.asp

[3] Hispasec http://www.hispasec.com/directorio/laboratorio/artículos/Comparativa2001/introduccion/12.html