Introducción a la virología móvil, parte II

10.10.2006 |LINK http://www.viruslist.com/sp/analysis?pubid=199595296

Alexander Gostev
Analista de virus en jefe, Kaspersky Lab

Introducción a la virología móvil, parte II

Epidemias

En esta parte, trataremos de establecer cual es el estado de la propagación de los virus móviles en el mundo moderno. Con bastante frecuencia los usuarios y los periodistas les reprochan a las compañías antivirus que éstas, de forma artificial, hacen escenas de histeria y exageran el peligro de los virus. Según ellos, Cabir tiene pocas posibilidades de propagarse, ya que para ejecutarlo el usuario tiene que pulsar tres veces el botón de confirmación (recepción, ejecución e instalación). Por su parte, ComWar no puede ser tan difundido, porque el sistema MMS no es muy popular y son pocos los que lo usan (se supone que es el 2% del total de los usuarios de teléfonos móviles). Estos incrédulos no quieren ni escuchar sobre el peligro de infección que conllevan los troyanos-vándalos como Skuller, porque según suponen, hay que descargarlos desde Internet, copiarlos al teléfono y ejecutarlos.

Sí, desde el punto de vista teórico, estos argumentos son bastante lógicos y convincentes. Pero el mundo de los virus para ordenador y para dispositivos móviles, al igual que las personas que los usan, constantemente refutan las tesis expuestas. La probabilidad de que un usuario acepte y ejecute Cabir es la misma que la de que un usuario acepte y ejecute un archivo recibido por correo electrónico, enviado quién sabe porqué y para qué. ?Y es que los ejecutan! Recuerde todas las epidemias de proporciones gigantescas de gusanos de correo ocurridas en años recientes: Mydoom, Netsky, Sober. Las compañías antivirus no se cansaban de repetir: "No ejecuten archivos recibidos por correo antes de analizarlos con un antivirus". Pero esto no servía de nada: la curiosidad humana y el incumplimiento de las reglas de seguridad más elementales siempre eran más fuertes.

Cabir

Las compañías antivirus recibieron a Cabir en junio de 2004. Pasado sólo un mes, se supo que en las Filipinas ya se habían registrado casos de infección causados por Cabir. Fue algo sorprendente. En aquel entonces creíamos que Cabir era un "gusano de colección" y que nunca saldría de los límites de las colecciones de las compañías antivirus. En la práctica, Cabir no sólo cayó en las manos de las compañías antivirus, sino también en las de los autores de virus. El gusano logró evadirse y empezó su marcha triunfal por el mundo.

Nuestra compañía hace tiempo que colabora con la compañía finlandesa F-Secure, que fue una de las primeras en prestar atención al problema de los virus móviles y ahora realiza investigaciones en este campo, dedicándole una significante parte de sus publicaciones. F-Secure empezó sin demora a elaborar una lista de países, dónde se habían registrado casos de infección por Cabir. En menos de un año, hacia el verano de 2005, en la lista ya habían 20 países. Nosotros también llevamos una estadística similar y ahora en esta lista también se mencionan nuestros datos. Además, recibíamos confirmaciones sobre casos de infección de diferentes países mencionados en la lista. Así, podemos considerar que la lista refleja el estado real de las cosas y merece completa confianza.

Hace cerca de un año, perdimos la cuenta y dejamos de aumentar países a la lista. Es evidente, que la cuenta ya se lleva por decenas y entre los países afectados por Cabir no sólo están los que cuentan con un elevado grado de informatización.

1.	Filipinas
2.	Singapur
3.	Emiratos Árabes Unidos

4.	China
5.	India
6.	Finlandia
7.	Vietnam
8.	Turquía
9.	Rusia
10.	Gran Bretaña
11.	Italia
12.	EEUU
13.	Japón
14.	Hong Kong
15.	Francia
16.	Sudáfrica
17.	Países bajos
18.	Egipto
19.	Luxemburgo
20.	Grecia
21.	Ucrania
22.	Nueva Zelandia
23.	Suiza
24.	Alemania

Lista de países donde se detectó a Cabir, según los datos conjuntos de F-Secure y Kaspersky Lab, septiembre de 2005.

Pondré varios ejemplos reales de infección con Cabir. El noveno país en la lista es Rusia. El caso ocurrió en enero de 2005. Para ese entonces, ya contábamos con la información de que Cabir estaba atacando a los portadores de teléfonos móviles en el metros de Moscú. La información procedente de la vecina Ucrania era análoga. Allá, Cabir había aparecido en Kiev y Jarkov. Sin embargo, no podemos confirmar estos casos, ya que no vimos ningún teléfono infectado y ningún usuario ucraniano solicitó ayuda a Kaspersky Lab para eliminar a Cabir. En enero esta "laguna" fue cubierta. Una empleada de una compañía que se encontraba en el mismo edificio que Kaspersky Lab, solicitó ayuda a nuestro servicio de asistencia técnica, quejándose que desde hacía varios días su teléfono había empezado a "comportarse de una forma rara" y que todo había empezado después de haber aceptado un archivo en el metro. Cuando revisamos el teléfono en nuestro laboratorio antivirus, nuestras sospechas se confirmaron: era Cabir.a.

Más tarde, durante el transcurso de todo 2005, en muchas ocasiones tuvimos la oportunidad de ver teléfonos infectados. Además, cerca de 10 empleados de nuestra compañía fueron atacados por Cabir cuando sus teléfonos recibieron solicitudes de aceptar un archivo llamado caribe.sis. El último caso parecido lo detectamos en febrero de 2006.

Es probable que el caso más ilustrativo, masivo y famoso de epidemia local causada por Cabir haya sido el incidente ocurrido en Helsinki en agosto de 2005. Entonces transcurría el décimo Campeonato Mundial de atletismo ligero. La oficina central de F-Secure se encuentra en Helsinki y ellos fueron los primeros en enterarse de que en el estadio donde se llevaba a cabo el campeonato se habían registrado casos de infección con Cabir. Cuando en un pequeño espacio se concentran decenas de miles de personas de todo el mundo, un sólo teléfono infectado basta para que el gusano empiece a propagarse con rapidez. En la cancha del estadio se batían records deportivos, mientras en las tribunas Cabir establecía el record de velocidad de propagación. Por suerte, los empleados de F-Secure actuaron con celeridad: en la zona de Customer Service Center del estadio se estableció un lugar especial, adónde podía llegar cualquiera que sospechase que su teléfono estuviera infectado. Allá, se verificaba el teléfono y se lo "limpiaba" del

virus. Si no se hubiese podido poner freno a la epidemia, los espectadores se habrían ido cada uno a su país, llevando consigo teléfonos infectados y aumentando la cantidad de países invadidos por el gusano.

Este es un ejemplo clarísimo de las condiciones más favorables para la propagación de los gusanos Bluetooth:

- una gran multitud
- un espacio reducido

también son zonas de riesgo los cafés, teatros, cines, aeropuertos, estaciones, metro, estadios, etc.

Los gusanos Bluetooth tienen las siguientes peculiaridades de propagación:

- el radio de infección está limitado por el radio de acción de la conexión Bluetooth (de 10 a 20 metros)
- los gusanos Bluetooth no pueden infectar a una víctima previamente establecida, por ejemplo, usando una lista o un número de teléfono. La infección ocurre de forma espontánea: si un objeto vulnerable se encuentra en el radio de acción de la infección, se intentará contagiarlo.

ComWar

El segundo virus móvil detectado circulando en el mundo real es ComWar. A diferencia de Cabir, que primero cayó en las manos de las compañías antivirus y sólo después fue detectado en libertad, ComWar fue detectado después de causar víctimas en varios países, las cuales enviaron los archivos sospechosos para su análisis a los laboratorios antivirus. Nosotros "tuvimos el gusto" de ver por primera vez a ComWar en marzo de 2005, sin embargo la investigación del incidente reveló que en diversos foros de usuarios de teléfonos móviles (p.ej. en Holanda y Serbia) se lo había mencionado ya en enero del mismo año. Así, podemos constatar sin temor a equivocarnos, que ComWar estuvo por lo menos dos meses propagándose por el mundo sin que las empresas antivirus tuvieran noticias de él. Esto demuestra que la interacción entre los usuarios y las compañías antivirus todavía está poco desarrollada en lo que respecta a la esfera de los dispositivos móviles. Si bien en los ordenadores personales cualquier acción sospechosa genera inmediata desconfianza en el usuario (piensa que es un virus) y lo mueve a comunicarse con las compañías antivirus, para que suceda lo mismo con los usuarios de teléfonos inteligentes todavía se necesitará mucho tiempo.

F-Secure, como en el caso de Cabir, de inmediato empezó a hacer una lista de los países dónde se había detectado a ComWar. Y nosotros también cotejamos sus datos con los nuestros. La última versión de esta lista tiene fecha de septiembre de 2005.

1.	Irlanda
2.	India
3.	Omán
4.	Italia
5.	Filipinas
6.	Finlandia
7.	Grecia
8.	Sudáfrica
9.	Malasia
10.	Austria
11.	Brunei
12.	Alemania
13.	EEUU
14.	Canadá

15.	Gran Bretaña
16.	Rumania
17.	Polonia
18.	Rusia
19.	Países Bajos
20.	Egipto
21.	Ucrania
22.	Serbia

Lista de países donde se detectó a Cabir, según los datos conjuntos de F-Secure y Kaspersky Lab, septiembre de 2005.

Es digno de mencionar que ambas listas tienen casi el mismo número de países (23 países en la de Cabir y 22 den la de ComWar). ComWar apareció ocho meses después que Cabir, pero su método de propagación por MMS, que puede enviarse a cualquier distancia, le permitió ponerse a la par de Cabir en poco tiempo. En la actualidad, es probable que la cantidad de países dónde se han registrado casos de infección con ComWar sea mayor que la de Cabir.

No obstante, debemos hacer una importante aclaración: en la lista se enumeran los países dónde se registró por lo menos un incidente con estos gusanos. La lista no permite sacar conclusiones sobre las dimensiones de la propagación del gusano en un país en particular. sólo se puede hacer conjeturas, partiendo de indicios indirectos.

Por suerte, el problema de los gusanos que se difunden por MMS preocupa no sólo a las compañías antivirus, sino también a los proveedores de telefonía móvil. Éstos se han empezado a preocuparse por la defensa de sus usuarios contra los MMS infectados y alguno (en Rusia) han implementado en sus redes nuestras soluciones antivirus, que son muy parecidas a las que se usan para el análisis antivirus de los mensajes de correo electrónico tradicional.

Desde ese momento obtuvimos acceso a las estadísticas con cifras concretas y a la dinámica de desarrollo. Resulta que en el tráfico MMS, además de los programas maliciosos para móviles, también están presentes los gusanos tradicionales para ordenador. Este fenómeno está se debe a que se los envía a direcciones de correo electrónico que también pueden ser direcciones de MMS. Pero ahora nos interesan sólo los gusanos móviles.

Es la primera vez que publicamos parte de esta información al público en general. Recibimos estos datos como resultado del análisis de la totalidad del tráfico MMS de uno de los proveedores de telefonía móvil en Rusia. De conformidad con el acuerdo pactado con el proveedor, no divulgaremos la cantidad total de los MMS analizados.

Nombre del programa malicioso	**Cantidad de MMS infectados**
Worm.SymbOS.ComWar.a	4733
Worm.SymbOS.ComWar.c	450
Trojan-SMS.J2ME.RedBrowser.b	1
estadística del 11-17 de junio de 2006.	
Nombre del programa malicioso	**Cantidad de MMS infectados/cambios respecto al periodo anterior**
Worm.SymbOS.ComWar.a	5498 (+765)
Worm.SymbOS.ComWar.c	854 (+404)
Trojan-SMS.J2ME.RedBrowser.b	1
estadística del 18-24 de junio de 2006.	
Nombre del programa malicioso	**Cantidad de MMS infectados/cambios respecto al periodo anterior**

Worm.SymbOS.ComWar.a	4564 (-934)
Worm.SymbOS.ComWar.c	756 (-98)

estadística del 25 de junio – 1 julio de 2006.

Nombre del programa malicioso	Cantidad de MMS infectados/cambios respecto al periodo anterior
Worm.SymbOS.ComWar.a	4837 (+273)
Worm.SymbOS.ComWar.c	698 (-58)
Worm.SymbOS.ComWar.d	6 (+6)

estadística del 1-7 de julio de 2006.

Preste atención a la presencia de ComWar.d en la estadística. Esta variante fue creada en un país de habla hispana y por eso causa sorpresa verla en el tráfico MMS ruso. Además, se detectó por primera vez a ComWar.d en marzo de 2006. después de sólo 4 meses llegó a Rusia.

No puedo dejar de mencionar un divertido caso de infección por ComWar, registrado por un empleado de nuestra compañía. En junio de 2006, Kaspersky Lab estaba realizando una conferencia de partners. La sede era Grecia. Al terminar la conferencia, algunos de nuestros empleados partieron en un crucero en yate por el mar Egeo. Un día, el capitán y dueño del yate se acercó a nuestros empleados y se quejó de que su smartphone Nokia recibía muchos extraños mensajes sobre MMS que no habían sido recibidos por el destinatario, a pesar de que él no había enviado ningún MMS. En ese mismo instante, nuestros empleados descargaron de Internet la versión beta de nuestro antivirus KAV Mobile y con su ayuda lograron determinar la causa del extraño comportamiento del teléfono: estaba infectado por ComWar. El mismo hecho de que el gusano se haya estado propagando desde un yate que navegaba en el mar (en la zona de cobertura) es bastante curioso.

Además de Cabir y ComWar, definimos como virus "en libertad" a ciertas variantes de Skuller, Drever, Appdisabler, Cardtrap, PbStealer, RedBrowser, Doombot, Flexispy y el gusano StealWar. Muchos de ellos se publicaron en los sitios web dedicados a los usuarios de teléfonos Symbian, presentándose como juegos y aplicaciones útiles. Una parte de los troyanos móviles se encuentra en las redes P2P. El truco preferido de los autores de virus móviles es hacer pasar a sus criaturas por nuevas versiones de programas antivirus para teléfonos móviles.

La "patria" de los virus

Cuando se habla de los virus para ordenador, es difícil evitar la pregunta en que países se crea la mayor parte En los medios de información occidentales, existe el estereotipo de la "amenaza rusa". Pero esto es sólo un mito, que cae por su propio peso al analizarlo con la debida atención. Se ha arrestado a los autores de los virus que causaron epidemias en los años recientes, y es fácil establecer el país de los que todavía están en libertad:

- gusanos Sasser y NetSky (Alemania)
- gusano Zafi (Hungría)
- gusano Bozori (Turquía-Marruecos)
- puertas traseras Abobot y Codbot (países Bajos)
- gusano Slammer (Asia Oriental)
- gusano Sober (Alemania)

sólo el gusano Bagle ha sido creado por los rusos y al parecer estamos ante una banda internacional de delincuentes.

Conforme a nuestras observaciones, en la actualidad el líder en esta equívoca competencia es China, seguida a pocos pasos por Brasil. Un significante porcentaje de los virus modernos se crea en Turquía. Los países de la ex URSS en conjunto producen una cantidad de virus comparable a la de Turquía.

En lo que toca a los virus móviles, resulta que el cuadro es bastante similar. El país de origen de los virus de las 31 familias puede ser establecido con un elevado grado de certeza.

Como recordamos, el francés Vallez creó a Cabir. después de caer en las manos de la comunidad informática clandestina, sus modificaciones empezaron a aparecer como los setas después de la lluvia. Los habitantes de los países del sur y este de Asia fueron los más activos en la creación de nuevas variantes: Filipinas, Indonesia, Malasia y China. Cuando el brasileño Velasco se dedicaba a la creación del virus Lasco, al mismo tiempo creó varias modificaciones de Cabir.

La ex URSS aportó a la virología móvil cuatro programas maliciosos. Pero la verdad es que tres de ellos eran "de concepto" y fueron los primeros en su género. La primera puerta trasera para WinCE, que recibió el nombre de Brador, fue creada por un programador de Ucrania, conocido bajo el seudónimo de BrokenSword. El gusano ComWar, que ya hemos analizado con detalle en este artículo, sin lugar a dudas fue creado en Rusia. Las pruebas son los textos dentro del gusano y la información que tenemos sobre la persona que se esconde bajo el seudónimo e10d0r. El tercero es el troyano RedBrowser, de autor desconocido. No obstante, los textos dentro del troyano y los números de teléfono adónde se envían los SMS no dejan dudas acerca de su procedencia rusa.

En lo que se refiere a Locknut, detectado por la compañía antivirus neozelandesa SimWorks, se establecieron sulas "huellas rusas" basándose en que los textos contenían obscenidades en ruso y los nombres de los archivos también estaban en ruso.

Como ya hemos mencionado, una serie de variantes de ComWar contiene textos en castellano. Esto podría servir para suponer que el autor es de Espada, pero no contamos con datos que confirmen la presencia de ComWar en este país (lo que podría ser una prueba indirecta).

A Turquía le pertenecen varias modificaciones de Skuller, Cardtrap, como también del primer troyano de la familia Arifat del que tenemos noticias.

Pero la mayor cantidad de virus móviles se ha creado en China, y quizás, en Corea del Sur. No hemos llegado a ninguna conclusión determinada, ya que estamos ante una situación muy específica. El problema es que la aplastante mayoría de troyanos móviles del último año fue detectada y enviada a las compañías antivirus precisamente desde Corea del Sur. Sin embargo, la investigación de una serie de incidentes estableció los siguientes hechos: los troyanos se almacenaban en los servidores coreanos que habían sido hackeados desde China. En China se crearon virus como: PbSteales, StealWar y algunas variantes de casi todas las familias troyanas.

Y no podemos dejar de mencionar la gran actividad demostrada por uno de los autores de virus de Malasia. A su "pluma" pertenece una gran parte de los Skuller, y quizás también sea el autor del primero de ellos.

¿Que demuestran todos estos hechos? Que el mundo de los virus móviles se desarrolla según las mismas leyes que los programas maliciosos para ordenadores. Tanto los uno como los otros se crean en los mismos países.

Problemas de los sistemas operativos

El factor más importante del desarrollo de los programas maliciosos para dispositivos móviles son las vulnerabilidades de software y de los sistemas operativos móviles. En el mundo de los ordenadores personales, casi todas las grandes epidemias virales de los años recientes se debieron a la presencia de vulnerabilidades en el sistema operativo Windows. Y es que los delincuentes sólo tienen dos formas de penetrar en un sistema: usando el factor humano (la ingeniería social) y los errores del software (vulnerabilidades). Estos mismos vectores de ataque se pueden aplicar a los dispositivos móviles.

Hay que tener en cuenta, como mínimo, tres fuentes importantes de vulnerabilidades:

- el sistema operativo Windows CE
- el sistema operativo Symbian
- los protocolos de comunicación inalámbrica (Bluetooth, WiFi, puertos infrarrojos)

Windows CE es un sistema de extrema vulnerabilidad, desde el punto de vista de su seguridad. No establece ningún tipo de limitaciones para las aplicaciones y procesos que pueden ser ejecutados. Un programa puede obtener acceso ilimitado a todas las funciones del sistema operativo: recepción y envío de archivos, funciones de los servicios del teléfono y de multimedia, etc.

Es muy fácil crear programas para Windows CE. Es un sistema de programación muy abierto, que permite usar no solo los idiomas de bajo nivel (p.e. ASM para ARM), sino también medios de programación tan poderosos como .NET.

A pesar de que en este momento conocemos sólo cuatro familias de virus para Windows CE, no hay que subestimar el potencial de este SO, desde el punto de vista de la creación de virus. Los virus móviles actuales corresponden a los tipos más peligrosos de programas maliciosos: virus clásico, gusano postal, puerta trasera y gusano capaz de copiarse al ordenador al conectarse el teléfono. La popularidad de las plataformas basadas en Windows CE está creciendo a pasos gigantescos, y en los próximos años pueden llegar a ocupar el primer lugar, desplazando a Symbian.

En estas condiciones, vemos que está creciendo el interés hacia esta plataforma por parte de los autores de virus y de los investigadores. Ya hablamos dicho que en la conferencia DefCon de agosto Collin Mulliner presentó una ponencia sobre el descubrimiento de vulnerabilidades en el procesamiento de MMS en Windows CE 4.2x. Actualmente, Microsoft y sus partners están llevando a cabo la corrección de este error, pero incluso después de la publicación del parche, será necesario notificar a todos los usuarios de los dispositivos vulnerables de la necesidad de "actualizar" sus teléfonos inteligentes y PADs.

No hay que olvidar que esta es sólo una de las serias vulnerabilidades de Windows CE descubiertas en los meses recientes. Existe la posibilidad de organizar ataques DoS por medio de las vulnerabilidades de ActiveSync y MMS/SMS.

Un peligro aparte son las potenciales vulnerabilidades de Internet Explorer para Windows CE y los programas de conversión de los formatos de los archivos. No tenemos la menor duda de que estas vulnerabilidades existen. La cuestión es quién será el primero en descubrirlas: los autores de virus o los investigadores honrados, como Collin Mulliner o Tim Hurman (Éste último descubrió la vulnerabilidad "Bluetooth stack remote code execution", cuya información se ha convertido en un verdadero secreto).

El primer virus para Windows CE –Duts- usaba una de las vulnerabilidades en el API de archivos, que todavía Microsoft todavía no conocía (de día cero).

En resumen: Windows CE ganará popularidad día tras día. El ritmo de aparición de programas maliciosos para esta plataforma pronto se acercará al de los programas maliciosos para Symbian. El principal medio de funcionamiento de los virus será .NET. Una significante parte de los virus utilizará las vulnerabilidades de WinCE.

El sistema operativo integrado más popular de la actualidad es Symbian. Aquí, la situación de las vulnerabilidades no es tan amenazante como en Windows CE. Pero esta sensación de seguridad es aparente. La arquitectura de Symbian Series 60 tiene una serie de serios errores, es decir, peculiaridades que nosotros consideramos vulnerabilidades. Ya hemos dicho que Symbian permite reemplazar cualquiera de las aplicaciones del sistema sin el consentimiento del usuario, y si surge algún problema con un formato de archivo desconocido, el sistema se vuelve inestable y puede causar el reinicio del teléfono. además, los niveles de seguridad de las aplicaciones son muy parecidos a los de Windows CE. En palabras más simples, no hay ningún sistema de seguridad. Si un programa logra penetrar al sistema, obtiene el poder absoluto sobre todas las funciones. Por fortuna, hasta hoy no se han descubierto vulnerabilidades en el procesamiento de las conexiones Bluetooth y MMS en esta plataforma. Es fácil imaginar qué podría haber sucedido si Cabir o ComWar hubiesen tenido la posibilidad de penetrar al sistema y ejecutarse automáticamente.

Symbian es un sistema más restringido que Windows CE. Para crear programas serios se necesita un DDK que cuesta varias decenas de miles de dólares. Pero, a juzgar por la cantidad de programas troyanos existentes, las vulnerabilidades presentes en la arquitectura del sistema operativo permiten a los autores de virus contentarse con los medios que están a la disposición del público en general.

Se ha conformado una situación bastante paradójica: Symbian es más popular que WinCE, pero se conocen menos vulnerabilidades para la primera. En nuestra opinión, esto tiene sólo una explicación: los esfuerzos de los investigadores todavía no se han concentrado en Symbian en la misma medida que en los productos de Microsoft. Con todo, basta una rápida mirada y un par de simplísimos experimentos para demostrar que los errores de Symbian se encuentran con mucha frecuencia. Para confirmar estas palabras, les expondré la descripción de uno de ellos, que puede considerarse desconocido por el momento. Esta información nos fue enviada por uno de nuestros usuarios, la verificamos y logramos reproducirla en nuestro laboratorio.

Esta vulnerabilidad afecta a los teléfonos que funcionan con Symbian Series 6.x. La comprobamos en los teléfonos Siemens SX-1 y Nokia 3650.

Basta crear un archivo con el nombre "INFO .wmlc", dónde después de INFO y hasta el punto haya 67 espacios. El contenido del archivo puede ser cualquiera (de más de 2 bites). Si se envía este archivo a otro dispositivo vía Bluetooth o puerto infrarrojo (o enviado por MMS, puesto en un sitio web (no lo hemos comprobado)), al abrirlo el destinatario recibirá el siguiente mensaje de error «App. closed AppArcServerThread USER 8». Luego, el teléfono empieza a funcionar de forma más lenta y pueden fallar varias aplicaciones, para terminar reiniciando el teléfono.

Estamos ante una vulnerabilidad clásica del tipo DoS. La extensión "wmlc" está relacionada con el navegador de Internet preestablecido, el cual, al toparse con un nombre de archivo extraño, causa un error en el componente responsable de la ejecución del navegador. Como no hemos realizado un análisis detallado de la vulnerabilidad, es posible que además del error mencionado, permita ejecutar un código arbitrario en el sistema.

La presente puede considerarse una notificación oficial a la compañía Symbian sobre la existencia de la vulnerabilidad.

La compañía Symbian, la comunidad de fabricantes de smartphones con este sistema operativo y los programadores ya han notado la existencia de virus para este sistema operativo y están haciendo todos los esfuerzos para que la siguiente versión de Symbian está protegida al máximo contra todo tipo de programas maliciosos. Hace poco se anunció que están diseñando una arquitectura de protección de las aplicaciones parecida en su estructura a la tecnología TrustinComputer, que se integra a algunos procesadores para PC. Se planea crear una especie de "región de memoria protegida", adónde tendrán acceso sólo los programas de confianza. En principio, esta manera de abordar el asunto puede resolver el problema de los troyanos-vándalos primitivos como Skuller, pero no resolverá todos los problemas con las vulnerabilidades en el sistema operativo y sus aplicaciones. además, no hay que olvidar una ley más de la existencia de los virus: "Un virus puede hacer en un sistema todo lo que puede hacer el usuario". Esto significa que los gusanos que se envían a sí mismos por Bluetooth y MMS se convertirán en realidad en el futuro.

En este artículo no nos hemos detenido en los detalles de las vulnerabilidades intrínsecas de los protocolos inalámbricos Bluetooth y WiFi. Remitimos a todos los interesados en este aspecto del problema a los materiales de grupos como Trifinite o Pentest. Ya hemos publicado los resultados de algunas de nuestras investigaciones en este campo. Señalamos que, a pesar de que existe cierta cantidad de vulnerabilidades en los protocolos inalámbricos para dispositivos móviles, los autores de virus todavía no los han empezado a usar en sus creaciones. No obstante, no tenemos la menor duda de que esto sucederá en un futuro inmediato.

Fuente:

- Kaspersky Lab