Introducción a la virología móvil, parte I

29.09.2006 |

Alexander Gostev
Analista de virus en jefe, Kaspersky Lab
LINK http://www.viruslist.com/sp/analysis?pubid=199114452

Introducción

En junio de 2006 se cumplieron dos años desde que Kaspersky Lab recibió la primera muestra de virus para teléfonos celulares. Ahora ya sabemos que su autor fue el famosos grupo internacional de autores de virus 29A, para ser más exactos, uno de sus miembros llamado Vallez.

Se había abierto la caja de Pandora. Hoy en día, en las colecciones de las compañías antivirus se encuentran cientos de programas troyanos y gusanos de todas las especies que atacan a los teléfonos celulares. El pequeño riachuelo de programas perjudiciales para Symbian que existía en 2004, se ha convertido ahora en un torrente impetuoso, que amenaza con convertirse en un caudaloso río en poco tiempo. Cada semana agregamos a nuestras bases antivirus cerca de una decena de programas troyanos que tienen el prefijo "SymbOS" en su nombre.

Lo más triste es que este proceso va acompañado por epidemias reales de gusanos móviles, que están en crecimiento y cuyas verdaderas dimensiones todavía son imposibles de estimar. Hace sólo un año, supimos que se había detectado a Cabir en cierto país o ciudad. Luego, los dueños de teléfonos infectados empezaron a pedirnos ayuda y poco a poco nos convertimos en testigos de casos reales de infección. En el presente, muchos de los empleados de nuestra compañía se han tropezado con gusanos parecidos.

Es posible que la causa de semejante propagación de gusanos móviles sea el menor nivel de preparación informática de los usuarios de teléfonos celulares, si los comparamos con los usuarios de Internet. Por otra parte, incluso los usuarios experimentados consideran que los virus para dispositivos móviles son cosa del futuro o que son algo que existe, pero muy lejos.

Pero no. Los virus móviles no son un mundo paralelo. Ellos están a nuestro lado en este preciso instante y cada vez que toma usted el metro, va al cine o viaja desde un gran aeropuerto, su teléfono se encuentra bajo amenaza.

Todavía nos queda mucho camino que recorrer en la tarea de instruir a los usuarios, un camino comparable al que recorrimos en el caso de los virus informáticos comunes.

En el principio fue...

El 14 de junio de 2004 la dirección newvirus@kaspersky.com recibió una carta de un conocido coleccionista de virus informáticos, estrechamente relacionado con ciertos autores de virus, el español "VirusBuster". La carta contenía un archivo con el nombre caribe.sis. En ese momento no sabíamos ante qué fenómeno nos encontrábamos. Un rápido análisis del archivo mostró que era una aplicación para el sistema operativo Symbian y al mismo tiempo un archivo de instalación que contenía otros archivos. Como regla, los analistas de virus lidian con archivos creados para los tradicionales procesadores x86. Los archivos de caribe.sis eran aplicaciones para el procesador ARM, que se utiliza en diferentes dispositivos portátiles, incluidos los teléfonos celulares. Entonces no conocíamos las instrucciones de este procesador, pero en algunas horas los analistas lograron comprenderlas y poner en claro el objetivo de los archivos: era el primer gusano para teléfonos celulares que se enviaba a sí mismo vía Bluetooth. Nuestras conclusiones se confirmaron al día siguiente, cuando pusimos a prueba la capacidad de funcionamiento del gusano en un teléfono Nokia N-Gage, provisto del sistema operativo Symbian.

El gusano fue creado por alguien conocido por el sobrenombre de Vallez. Según nuestros datos, vive en Francia y en ese momento era parte del grupo de autores de virus 29A. Este grupo se había puesto como objetivo la creación de virus nuevos, conceptuales, para sistemas operativos y aplicaciones no estándar. Sus miembros pretendían demostrar a las compañías antivirus y a los autores de virus que existen nuevos vectores de ataque. Esta vez su objetivo era la creación de un programa malicioso para teléfonos inteligentes. El sistema de reproducción del gusano también era poco usual. Estamos acostumbrados a que los gusanos se propagan usando el correo electrónico, y era lógico esperar que Cabir se comportase de la misma manera. Sobre todo tomando en cuenta que una de las principales funciones de los teléfonos

inteligentes es la posibilidad de trabajar con Internet y con el correo electrónico. Pero el autor del gusano escogió otro método: el protocolo Bluetooth. Este fue el segundo punto clave de la idea.

El gusano usa como entorno de funcionamiento el sistema operativo Symbian, que desde entonces es el líder entre los sistemas operativos para teléfonos celulares. En gran parte este liderazgo está condicionado por el hecho de que Symbian se usa en los teléfonos inteligentes fabricados por la compañía Nokia. De facto, Symbian+Nokia es la norma para los teléfonos inteligentes y pasará aún mucho tiempo hasta que Windows Mobile pueda desplazar a Symbian de este mercado.

Así, una vez más se demostró el principio de la "ley de la aparición de virus informáticos". La aparición de programas maliciosos para determinado sistema operativo o plataforma, requiere la concurrencia de tres factores:

1. **La popularidad de la plataforma**. El sistema operativo Symbian es la plataforma más popular para los teléfonos inteligentes. La cantidad de usuarios es de varias decenas de millones en todo el mundo.

> **El autor de Cabir declara: "Symbian puede convertirse en un sistema operativo muy extendido entre los teléfonos celulares del futuro. Hoy, es el más extendido y en mi opinión, podría serlo aún más (M$ también está luchando por introducirse en este mercado)."**

2. **La presencia de medios bien documentados para el desarrollo de aplicaciones**.

> **El autor de Cabir declara: "Caribe fue escrito en c++. Symbian/Nokia nos brinda un SDK completo para el desarrollo de aplicaciones en el sistema operativo Symbian".**

3. **La presencia de vulnerabilidades o errores.** Symbian contiene varios serios errores de diseño en el sistema de trabajo con archivos y servicios. En el caso de Cabir, éstos no se utilizaron, sin embargo la mayoría de los troyanos modernos para teléfonos inteligentes los usan en su totalidad.

Cabir acaparó en un instante la atención de las compañías antivirus y de los autores de virus. Todo el mundo estaba a la espera de que el grupo 29A publicase el nuevo número de su revista electrónica. Ese era el número donde debía publicarse el código fuente del gusano. Estaba claro que su publicación provocaría la aparición de nuevas y aún más peligrosas variantes del gusano.

Siempre pasa lo mismo cuando tecnologías como esta caen en manos de los scrip-kiddies.

Pero aún sin contar con los códigos fuente, estos golfos son capaces de muchas cosas.

Tipos y familias de virus móviles existentes en el presente

En otoño de 2004 se formaron las tres principales tendencias que rigieron el desarrollo de los virus para dispositivos móviles. Una era la creación de programas troyanos que provocasen pérdidas financieras al usuario infectado. El primero de este tipo fue el troyano Mosquit.a. A pesar de que no causaba ningún daño al teléfono, con el tiempo empezaba a enviar una gran cantidad de mensajes de texto a los destinatarios listados en la libreta de direcciones. De esta manera, los autores del juego trataban de hacerle publicidad. De hecho, este fue no solo el primer troyano para teléfonos inteligentes, sino también el primer AdWare.

El troyano Skuller.a, que apareció en noviembre de 2004, fue el primero en la larga lista de miembros de esta familia de troyanos móviles. Skuller.a se caracterizó por utilizar los errores en el funcionamiento de Symbian, que permitían a cualquier aplicación guardar sus archivos reemplazando los archivos del sistema, sin ni siquiera pedir el consentimiento del usuario. El troyano cambiaba los iconos de las aplicaciones y los reemplazaba con una calavera, borrando al mismo tiempo sus archivos. Como resultado de estas acciones, después de reiniciarse, el teléfono dejaba de funcionar. El principio del "troyano-vándalo" se convirtió en uno de los más populares entre los autores de virus.

El troyano Skuller.a

Tres variantes de Cabir vieron la luz casi al mismo tiempo que Skuller.a. Estas variantes no estaban basadas en los códigos fuente del gusano original. En ese momento, Cabir ya había caído en manos de los autores de virus y algunos de ellos hicieron el truco preferido de los script-kiddies: cambiaron el nombre del archivo del gusano y cambiaron algunos textos internos por textos propios. Una de estas variantes estaba reforzada porque dentro del archivo con el gusano se había agregado a Skuller. El híbrido resultante no tenía ningún sentido: el gusano no podía reproducirse, ya que el troyano dejaba al teléfono fuera de servicio. Sin embargo, este fue el primer ejemplo de la utilización de Cabir en calidad de "portador" de otros programas maliciosos.

De esta manera, a principios de 2005, los principales tipos de virus móviles ya se habían consolidado y durante el año y medio siguiente los autores de virus les fueron fieles:

- gusanos que se propagan a través de protocolos y servicios propios de los teléfonos inteligentes;
- troyanos-vándalos que usan los errores de Symbian para instalarse en el sistema;
- troyanos orientados que provocan pérdidas financieras al usuario.

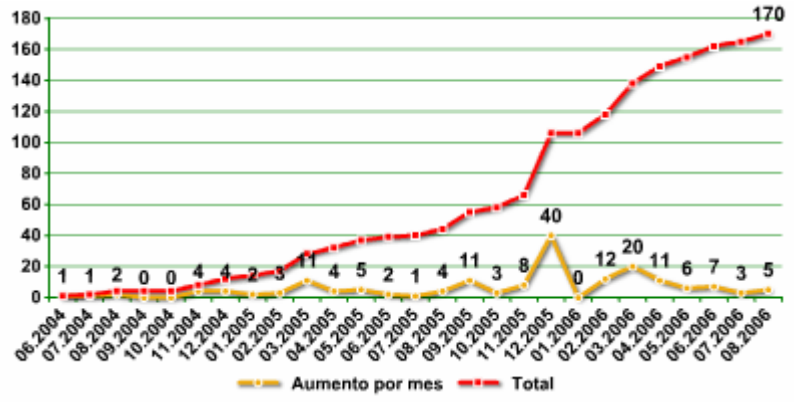
A pesar de que la cantidad de tipos principales es tan pequeña, en la práctica se han convertido en una gran diversidad de formas y tipos de virus. Actualmente, Kaspersky Lab ha determinado 31 familias de programas maliciosos para teléfonos móviles. Nuestro laboratorio mantiene una tabla, donde se pueden ver los principales rasgos característicos de estas familias.

Nombre	Fecha	Sistema operativo	Funciones	Fundamento tecnológico	Cantidad de variantes
Worm.SymbOS.Cabir	Junio de 2004	Symbian	Propagación por Bluetooth	Bluetooth	15
Virus.WinCE.Duts	Julio de 2004	Windows CE	Infección de archivos	(API de archivo)	1
Backdoor.WinCE.Brador	Agosto de 2004	Windows CE	Administración a distancia vía red	(API de red)	2
Trojan.SymbOS.Mosquit	Agosto de 2004	Symbian	Envíos masivos de SMS	SMS	1
Trojan.SymbOS.Skuller	Noviembre de 2004	Symbian	Reemplazo de iconos, reemplazo de las aplicaciones del sistema	Vulnerabilidad del sistema operativo	31
Worm.SymbOS.Lasco	Enero de 2005	Symbian	Propagación por Bluetooth, infección de	Bluetooth, Archivo (API)	1

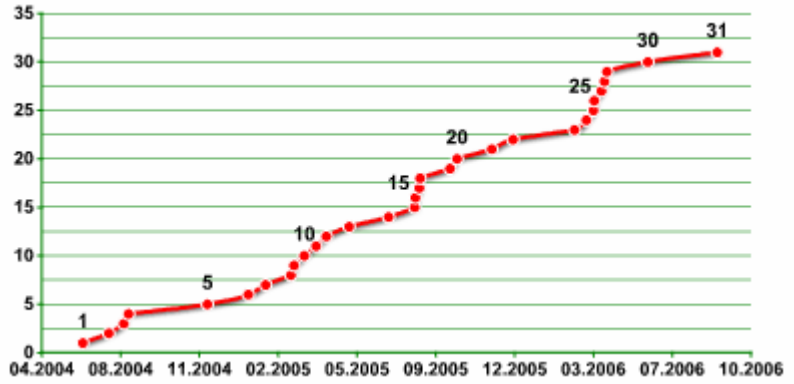
			archivos		
Trojan.SymbOS.Locknut	Febrero de 2005	Symbian	Instalación de aplicaciones corruptas	Vulnerabilidad del sistema operativo	2
Trojan.SymbOS.Dampig	Marzo de 2005	Symbian	Reemplaza las aplicaciones del sistema	Vulnerabilidad del sistema operativo	1
Worm.SymbOS.ComWar	Marzo de 2005	Symbian	Propagación por Bluetooth y MMA, infección de archivos	Bluetooth, MMS, Archivo (API)	7
Trojan.SymbOS.Drever	Marzo de 2005	Symbian	Reemplazo de aplicaciones antivirus	Vulnerabilidad del sistema operativo	4
Trojan.SymbOS.Fontal	Abril de 2005	Symbian	Reemplazo de los archivos de caracteres (fonts)	Vulnerabilidad del sistema operativo	8
Trojan.SymbOS.Hobble	Abril de 2005	Symbian	Reemplaza las aplicaciones del sistema	Vulnerabilidad del sistema operativo	1
Trojan.SymbOS.Appdisabler	Mayo de 2005	Symbian	Reemplaza las aplicaciones del sistema	Vulnerabilidad del sistema operativo	6
Trojan.SymbOS.Doombot	Junio de 2005	Symbian	Reemplazo de las aplicaciones del sistema, instalación de Comwar	Vulnerabilidad del sistema operativo	17
Trojan.SymbOS.Blankfont	Julio de 2005	Symbian	Reemplazo de los archivos de caracteres (fonts)	Vulnerabilidad del sistema operativo	1
Trojan.SymbOS.Skudoo	Agosto de 2005	Symbian	Instalación de aplicaciones corruptas, instalación de Cabir, Skuller, Doombor	Vulnerabilidad del sistema operativo	3
Trojan.SymbOS.Singlejump	Agosto de 2005	Symbian	Deshabilita las funciones del sistema, modifica los iconos	Vulnerabilidad del sistema operativo	5
Trojan.SymbOS.Bootton	Agosto de 2005	Symbian	Instalación de aplicaciones corruptas, instalación de Cabir	Vulnerabilidad del sistema operativo	2
Trojan.SymbOS.Cardtrap	Septiembre de 2005	Symbian	Eliminación de los antivirus, reemplazo de las aplicaciones del sistema, instalación de	Vulnerabilidad del sistema operativo	26

			malware para Win32 en las tarjetas de memoria		
Trojan.SymbOS.Cardblock	Octubre de 2005	Symbian	Bloqueo del funcionamiento de las tarjetas de memoria, eliminación de directorios	Vulnerabilidad del sistema operativo, API de archivo	1
Trojan.SymbOS.Pbstealer	Noviembre de 2005	Symbian	Robo de información	Bluetooth, Archivo (API)	5
Trojan-Dropper.SymbOS.Agent	Diciembre de 2005	Symbian	Instalación de otros programas maliciosos	Vulnerabilidad del sistema operativo	3
Trojan-SMS.J2ME.RedBrowser	Febrero de 2006	J2ME	Envíos masivos de SMS	Java, SMS	2
Worm.MSIL.Cxover	Marzo de 2006	Windows Mobile/ .NET	Elimina archivos y se copia a otros dispositivos	Archivo (API), Red (API)	1
Worm.SymbOS.StealWar	Marzo de 2006	Symbian	Robo de información, propagación vía BlueTooth y MMS	Bluetooth, MMS, Archivo (API)	5
Email-Worm.MSIL.Letum	Marzo de 2006	Windows Mobile/ .NET	Propagación vía correo electrónico	Correo electrónico, Archivo (API)	3
Trojan-Spy.SymbOS.Flexispy	Abril de 2006	Symbian	Robo de información	—	2
Trojan.SymbOS.Rommwar	Abril de 2006	Symbian	Reemplaza las aplicaciones del sistema	Vulnerabilidad del sistema operativo	4
Trojan.SymbOS.Arifat	Abril de 2006	Symbian	—	—	1
Trojan.SymbOS.Romride	Junio de 2006	Symbian	Reemplaza las aplicaciones del sistema	Vulnerabilidad del sistema operativo	8
Worm.SymbOS.Mobler.a	Agosto de 2006	Symbian	Eliminación de antivirus, reemplazo de aplicaciones del sistema, propagación vía tarjetas de memoria	Vulnerabilidad del sistema operativo	1
31 familias, 170 variantes					

Lista completa de las familias de virus m?viles según la clasificación de Kaspersky Lab (a 30 de agosto de 2006).



Aumento de la cantidad de variantes de virus móviles



Aumento de las familias de virus móviles

Lista completa de las familias de virus móviles según la clasificación de Kaspersky Lab (a 30 de agosto de 2006).

Si sumamos todos estos datos obtendremos la respuesta a la pregunta ¿de qué son capaces los virus móviles? Pues bien, son capaces de:

- Propagarse por Bluetooth o MMS
- Enviar mensajes de texto (SMS)
- Infectar archivos
- Permitir el acceso remoto al teléfono inteligente
- Modificar o reemplazar los iconos y aplicaciones del sistema
- Instalar caracteres y aplicaciones "falsos" o incorrectos
- Desactivar los programas antivirus
- Instalar otros programas maliciosos
- Bloquear el funcionamiento de las tarjetas de memoria
- Robar información

Es necesario reconocer que los virus móviles modernos pueden hacer casi todo lo que hacen los virus informáticos. Pero a los virus informáticos les tomó más de veinte años generar todo este espectro de comportamientos. Los virus móviles han recorrido todo este camino en sólo dos años. Sin lugar a dudas, estamos ante la esfera más dinámica y en rápido crecimiento de los programas maliciosos, y es evidente que el pico de su desarrollo está todavía muy lejos.

Fundamentos

Una de las principales diferencias entre los virus móviles y los de ordenador desde el punto de vista de la tecnología es que, aunque existen muchas familias de virus móviles, el número de programas maliciosos móviles realmente originales es reducido. Esta situación es similar a la de los virus para ordenador de finales de los años 80 del siglo pasado. Entonces existían cientos de virus, que estaban fundamentados

en varios programas maliciosos "básicos" y sus códigos fuente. Los virus Vienna, Stoned, Jerusalem fueron los tres precursores de una gran cantidad de otros virus.

Yo diría que los "precursores" de los virus móviles son los siguientes programas:

- **Cabir**
- **Comwar**
- **Skuller.gen**

Cabir

Cabir no solo generó varias nuevas variantes, cuyas únicas diferencias eran los nombres de los archivos y el contenido de su archivo de instalación sis. Sobre la base de este gusano se crearon las familias StealWar y Pbstealer, a primera vista tan independientes y poco parecidas entre sí.

Lasco

Lasco fue el primero de ellos, y además de las funciones de gusano, tenía la capacidad de infectar archivos en el teléfono. La historia de la aparición de Lasco es una excelente ilustración de las consecuencias que puede tener la publicación de códigos fuente. Un tal Marcos Velasco, brasilero que se autodenominaba experto en el campo de los virus móviles, recibió el código fuente de Cabir y se dedicó de forma abierta a escribir virus. En el transcurso de la última semana de 2004, envió a las compañías antivirus un paquete con sus variaciones sobre el tema de Cabir, muchas de la cuales eran incapaces de funcionar. Las compañías antivirus las calificaron a todas ellas como nuevas variantes de Cabir. Esta clasificación causó gran disgusto al autor, que en su intento de hacerse famoso creó una variante del gusano que era capaz de infectar los archivos sis. Así, en las bases antivirus apareció el gusano Lasco.

Por suerte la idea de infectar archivos no se hizo popular entre los autores de virus, a pesar de que Velasco publicó el código fuente de su criatura en su propia página web.

Hasta ahora no se sabe a ciencia cierta si Lasco se basó en Cabir. Marcos afirmaba que había escrito todo el código con sus propias manos, pero la cantidad de archivos, sus nombres, tamaños y principio de funcionamiento tienen mucho en común con Cabir. Usted mismo puede comparar una de las principales funciones de ambos gusanos y sacar sus propias conclusiones.

Nos referimos a la función de envío a través de Bluetooth (Cabir):

```
if(WithAddress)
{
        WithAddress = 0;
        Cancel();
        TBTSockAddr btaddr(entry().iAddr);
        TBTDevAddr devAddr;
        devAddr = btaddr.BTAddr();
        TObexBluetoothProtocolInfo obexBTProtoInfo;
        obexBTProtoInfo.iTransport.Copy(_L("RFCOMM"));
        obexBTProtoInfo.iAddr.SetBTAddr(devAddr);
        obexBTProtoInfo.iAddr.SetPort(0x00000009);
        obexClient = CObexClient::NewL(obexBTProtoInfo);
        if(obexClient)
        {
                iState = 1;
                iStatus = KRequestPending;
                Cancel();
                obexClient->Connect(iStatus);
                SetActive();
        }
}
else
{
        iState = 3;
        User::After(1000000);
```

```
}
return 0;
```
Y la la función de envío a través de Bluetooth (Cabir):
```
if ( FoundCell )
{
        FoundCell = _NOT;
        Cancel();
        TBTSockAddr addr( entry().iAddr );
        TBTDevAddr btAddress;
        btAddress = addr.BTAddr();
        TObexBluetoothProtocolInfo obexProtocolInfo;
        obexProtocolInfo.iTransport.Copy( _L( "RFCOMM" ) );
        obexProtocolInfo.iAddr.SetBTAddr( btAddress );
        obexProtocolInfo.iAddr.SetPort( 9 );
        if ( ( iClient = CObexClient::NewL( obexProtocolInfo ) ) )
        {
                iStatus = KRequestPending;
                BluetoothStatus = _BLUETOOTH_NOT_CONNECTED;
                Cancel();
                iClient->Connect( iStatus );
                SetActive();
        }
}
else
{
        BluetoothStatus = _BLUETOOTH_CONNECTED;
}
}
```

Pbstealer

Nos detendremos en uno de los "descendientes" de Cabir, el primer troyano-espía para Symbian: Pbstealer. Creado en Asia, al parecer en China, fue descubierto en uno de los servidores dedicados al juego en línea Legend of Mir. Esta forma de propagación y la notable tendencia criminal del troyano demostraron como se podían utilizar las "buenas intenciones" del autor de Cabir.

De Cabir, se utilizó la función de envío de archivos a través de Bluetooth. Sin embargo, los autores del troyano introdujeron una sola modificación, pero muy importante, al código original. El troyano encuentra la libreta de direcciones y la envía al primer dispositivo que encuentre a través de Bluetooth. De aquí viene su nombre, Pbstealer (Phonebook stealer), el ladrón de libretas de teléfonos. Hasta ahora, para robar este tipo de información, los delincuentes utilizaban diferentes vulnerabilidades en el protocolo Bluetooth, por ejemplo, BlueSnarf. Con la aparición de este troyano, las posibilidades de los delincuentes se ampliaron de forma significativa.

Y, como era de esperar, Cabir se convirtió en el "portador" preferido de otros troyanos de toda especie. Más de la mitad de los diferentes Skuller, Appdisabler, Locknut, Cardtrap y otros "vándalos" contienen a Cabir, modificado de tal manera que se envía no sólo a sí mismo, sino también el paquete completo de troyanos. Semejante comportamiento e hibridación de los programas maliciosos ha provocado grandes dificultades en su clasificación, tema que desarrollaremos más adelante.

Comwar

El segundo hito en el desarrollo de los programas maliciosos móviles fue Comwar, el primer gusano que se propagaba vía MMS. Al igual que Cabir, es capaz de enviarse a través de Blutooth, pero su principal forma de propagación es MMS. Considerando el volumen del tráfico MMS, es el más peligroso entre todos los posibles.

El radio de acción de Bluetooth es de 10 a 15 metros, y puede infectar otros dispositivos sólo dentro de estos límites. MMS no tiene fronteras y es capaz de enviarse a teléfono que se encuentran en otros países.

Al principio, el autor de Cabir había pensado en esta posibilidad, pero después la dejó de lado y optó por el Bluetooth, partiendo de premisas evidentes (por lo menos para la ideología de 29A):

"mms: Es fácil de usar a través del agente que busca la libreta de teléfonos y les envía un mensaje MMS con el gusano incluido, pero hay dos problemas:

- **No sabemos a qué tipo de teléfono estamos enviando el MMS. No sabemos si ese teléfono puede recibir mensajes MMS o si puede ejecutar el gusano.**
- **Estaríamos gastando el dinero del usuario".**

El segundo punto, muy significativo, nos permite concluir que el autor de Cabir no quería causar daños económicos a los usuarios. El autor de Comwar no tenía esta intención.

La tecnología de envíos vía MMS es la más atractiva para los autores de virus móviles, pero por el momento hemos encontrado sólo trucos basados en el gusano original, donde los "casi hackers" se limitaban a cambiar el nombre de los archivos y los textos contenidos en los archivos originales, sin cambiar las funciones de Comwar. Esto se debe a que el código fuente de Comwar no se ha hecho público y los script-kiddies no conocen el procedimiento de envío de MMS infectados.

En este momento sabemos de 7 modificaciones de este gusano, de las cuales cuatro tienen "autor".

```
CommWarrior v1.0b (c) 2005 by e10d0r
CommWarrior is freeware product. You may freely distribute it in it's original
unmodified form.
```

Comwar.b:

```
CommWarrior v1.0 (c) 2005 by e10d0r
CommWarrior is freeware product. You may freely distribute it in it's original
unmodified form.
```

Comwar.c:

```
CommWarrior Outcast: The dark side of Symbian Force.
CommWarrior v2.0-PRO. Copyright (c) 2005 by e10d0r
CommWarrior is freeware product. You may freely distribute it
in it's original unmodified form.
With best regards from Russia.
```

Comwar.d:

No contiene textos que lo diferencien. Los textos originales del MMS han sido cambiados por otros en castellano.

Comwar.e:

```
WarriorLand v1.0A (c) 2006 by Leslie
```

También tiene textos en castellano.

Comwar.f:

No contiene textos que lo diferencien. Los textos originales del MMS han sido cambiados por otros en castellano.

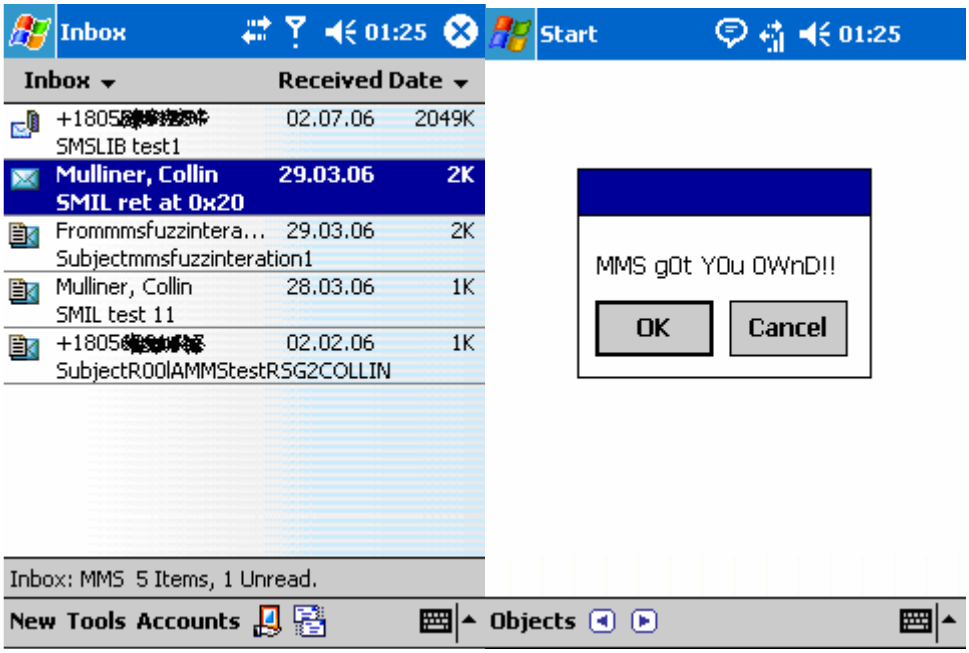
Comwar.g:

```
CommWarrior Outcast: The Dark Masters of Symbian.
The Dark Side has more power!
CommWarrior v3.0 Copyright (c) 2005-2006 by e10d0r
CommWarrior is freeware product. You may freely distribute it in it's original
unmodified form.
```

Además, en la variante .g el autor del gusano usó por primera vez la posibilidad de infectar archivos. El gusano busca en el teléfono otros archivos sis y se incrusta en ellos. De esta manera, adquiere una forma más de propagación, además de los ya tradicionales MMS y Bluetooth.

Hacemos notar que por el momento Comwar todavía no se ha convertido en "progenitor" de nuevos familias y esto está en directa relación con la no disponibilidad de su código fuente. Se lo utiliza en calidad de "portador" de otros programas troyanos, de la misma forma que Cabir. Entre todos los programas maliciosos que usan a Comwar para sus propósitos, sólo StealWar pretende convertirse en iniciador de una nueva familia. Este gusano une en su seno a Cabir, Comwar y al troyano Pbstealer. Semejante combinación es de alta peligrosidad y tiene una gran capacidad de reproducción.

Es inevitable que el principio de envíos masivos por MMS se convierta en el prevaleciente entre los otros medios de propagación de virus móviles. Sobre todo si se toma en cuenta que ya hay noticias sobre una seria vulnerabilidad en el procesamiento de MMS en el sistema operativo Windows Mobile 2003, que conduce al desbordamiento de la memoria intermedia (buffer overflow) y la ejecución de un código arbitrario. En agosto, Collin Mulliner presentó una ponencia sobre este tema en la conferencia DefCon.



Los detalles de esta vulnerabilidad estarán vedados al público hasta que Microsoft publique una actualización. Pero el peligro sigue vigente. Si se logra crear un gusano que de forma automática, sin la intervención del usuario, se ejecute al penetrar al teléfono inteligente, esto podría causar una epidemia global.

Al hablar del aporte que hizo Comwar a los virus móviles, debemos hacer notar que en su variante .c por primera vez se aplicó una tecnología que puede considerarse rootkit. El gusano pasa inadvertido en el listado de procesos y no se refleja en el listado de aplicaciones activas. Es posible que esto se deba a que el gusano camufla el tipo de su proceso como "de sistema". Por supuesto, es fácil encontrarlo si se usan otros programas que permiten visualizar los procesos activos. En la actualidad, ciertos programas maliciosos para Symbian usan un tipo similar de camuflaje.

Skuller

Como ya hemos mencionado, Skuller es la familia más numerosa de troyanos móviles: hasta el 1 de septiembre de 2006 hemos identificado 31 variantes. No es asombroso, ya que estos son los programas maliciosos más primitivos para Symbian. Cualquiera que tenga la capacidad de usar el programa de creación de archivos sis puede crear un gusano similar. Todo lo demás corre por parte de las vulnerabilidades de Symbian: la posibilidad de reemplazar cualquier archivo, incluso los del sistema, y la excesiva inestabilidad del sistema cuando se encuentra ante archivos de formato inesperado (que no son norma para una distribución dada o corruptos).

El fundamento de la mayoría de las variantes de Skuller son dos archivos. Son precisamente estos archivos los que llamamos Skuller.gen y que tienen peculiaridades que diferencian esta familia de otras similares en sus funciones (p.e. Doombot o Skudoo):

un archivo de extensión "aif" con el nombre de la aplicación a reemplazar, de un tamaño aproximado de 1601 bites. Es el archivo del icono con la calavera. Este archivo también contiene la línea de texto «↑Skulls↑Skulls»;

un archivo de extensión "app" con el nombre de la aplicación a reemplazar, de un tamaño aproximado de 4796 bites. Es una aplicación EPOC, un archivo vacío que no tiene ninguna función.

Problemas de clasificación

La clasificación es uno de los principales problemas de los virus móviles. Por clasificación entendemos la tarea de asignar a los nuevos virus una clase determinada, que refleje su tipo y conducta. Aquí surgen varias dificultades debidas a que los virus móviles tienen una gran inclinación por el cruce entre especies, es decir, la "hibridación".

La clasificación que usa Kaspersky Lab tiene una estructura clara:

Veredicto sobre la conducta. Contesta a las preguntas ¿qué es? y ¿qué hace? Ejemplos: Email-Worm, Trojan-Downloader, Trojan-Dropper.

Entorno necesario para su funcionamiento. Puede ser el nombre del sistema operativo o de una aplicación en particular. Ejemplos: Win32, MSWord, Linux, VBS.

Nombre de la familia y letra de la variante.

El último punto es el que menos problemas da. Cada programa malicioso tiene su nombre, que es propio y único. La única dificultad es la elección del nombre, pero de esto nos ocuparemos más adelante.

Pueden aparecer pequeños problemas con la definición del entorno de funcionamiento del virus móvil. En la mayoría de los casos analizamos programas para el sistema operativo Symbian y les asignamos el prefijo SymbOS. Sin embargo, cada vez con más frecuencia, el usuario requiere información más exacta: ¿funciona este virus sólo en Symbian Series 60 SE o puede también trabajar en las Series 80? ¿Quizá funcione sólo en las Series 80? ¿Y que hay de las Series 90? En lo que se refiere al sistema operativo Windows, tenemos una subdivisión similar: Win16, Win9x, Win32. Y no excluyo que en el futuro tengamos que introducir algunas cifras convencionales al prefijo SymbOS.

Pero esta es la parte más fácil del problema, que está relacionada con el segundo punto. Si volcamos nuestra vista a otra plataforma móvil, la de Windows, veremos que la situación es aún más confusa.

Tenemos muestras de virus que se escribieron para Windows CE 2003. Para ellos creamos el prefijo WinCE en nuestra clasificación. No obstante, los programas maliciosos creados para Windows Mobile 5.0 no pueden funcionar en la antigua plataforma. Y el nombre Windows CE no es del todo correcto para referirse a Windows Mobile o Pocket PC, aunque todas ellas son diferentes realizaciones de la plataforma Windows CE. Cada una de ellas utiliza su propio conjunto de componentes de Windows CE junto con su propio conjunto de peculiaridades y aplicaciones.

De esta manera, no podemos reflejar en la clasificación existente el nombre exacto de la plataforma necesaria para el funcionamiento de un virus en particular. Además, una serie de virus necesita .NET para WinCE/Windows Mobile para funcionar. A éstos les asignamos el prefijo MSIL, que no indica en absoluto que este virus sea móvil.

¿Todavía no se ha enredado? Pues espere un poco, estos no son los mayores problemas de clasificación. Estamos llegando a la parte más confusa de la clasificación: la asignación de una conducta particular a un virus. Aquí los problemas surgen en relación con la "hibridación", la aparición de programas maliciosos capaces de funcionar en diferentes plataformas móviles y los enfoques de clasificación que usan las diferentes compañías antivirus.

Analicemos unos cuantos ejemplos.

Los analistas de Kaspersky Lab con frecuencia se enfrentan a situaciones, cuando un archivo sis (que en sí es un instalador comprimido) contiene varios archivos: el gusano Cabir, el gusano ComWar, el troyano PbStealer, varios archivos Skuller.gen, varios archivos vacios (de tamaño igual a cero), que juntos son características del troyano Locknut y además instala en la tarjeta de memoria del teléfono un virus para Win32 (como lo hacen los troyanos Cardtrap).

Desde el punto de vista de la clasificación actual, deberíamos clasificar este archivo como un Trojan-Dropper. ?Pero no podemos hacerlo! El Cabir instalado enviará vía Bluetooth este archivo sis, y no a sí mismo. ¿Tendremos que clasificarlo también como gusano? Pero... ¿qué nombre le daríamos? ¿Cabir? No, no lo podemos llamar Cabir y asignarle una nueva letra de variante, porque el 90% del archivo sis no tiene nada en común con Cabir y sólo confundiríamos al usuario.

Se podría pensar en ponerle Skuller, Locknut o Cardtrap, pero ninguno de estos nombres sería exacto y correcto, porque estamos ante un "híbrido". Lo más probable es que a fin de cuentas este archivo se clasifique como troyano, y el nombre de su familia se escogerá de entre los troyanos que ya existen en nuestra colección, si hay coincidencia de signos secundarios, por ejemplo, alusión clara a un autor común.

Semejantes dificultades de clasificación son muy raras en el mundo de los virus para ordenadores, pero son muy frecuentes durante la clasificación de virus móviles.

Es posible que, a medida que se reduzcan los troyanos-vándalos primitivos, los casos como el descrito se hagan menos frecuentes y el mundo de los virus móviles, en este plano, sea más claro y estructurado.

Ejemplo número dos. Es un gusano que funciona en Win32. Al ser ejecutado en un ordenador personal, además de sus otras acciones, crea en el disco E:\ un archivo sis (como regla, los teléfonos con Symbian se conectan al ordenador como disco E:\). El archivo sis contiene varios archivos vacíos, con los que reemplaza una serie de aplicaciones del teléfono. El archivo también contiene el mismo gusano para Win32, que se copia a la tarjeta de memoria del teléfono y se complementa con el archivo autorun.inf.

Si se conecta este teléfono infectado a un ordenador, cualquier operación con la tarjeta de memoria provocará el lanzamiento del gusano, que también infectará al ordenador.

Este es un ejemplo de virus multiplataforma, que es capaz de funcionar en sistemas operativos completamente diferentes. Este gusano ya existe, y se llama Mobler. Pero...¿cómo clasificarlo?

En nuestra clasificación, se asigna a los virus multiplataforma el prefijo "Multi". ¿Worm.Multi.Mobler? Este nombre no da ningún indicio a los usuarios de que este gusano representa peligro para los teléfonos inteligentes con Symbian. A nuestro parecer, lo correcto sería dividirlo en dos componentes: clasificar el archivo Win32 como Worm.Win32.Mobler, y el archivo sis como Worm.SimbOS.Mobler. El problema es que las otras compañías antivirus no clasifican el archivo sis ni como Mobler, ni como gusano. Lo denominan Trojan.SymbOS.Cardtrap, porque, según su método de clasificación, cualquier programa malicioso que instala otros programas malicioso para Win32 en las tarjetas de memoria es un "Cardtrap". Pero éste no instala un troyano extraño. Instala su principal componente, su copia, sólo que para otro sistema operativo. Sin embargo, los estrechos marcos de las clasificaciones de las compañías antivirus les obligan a incluir en este lecho de Procrusto a todos los casos atípicos similares. A fin de cuentas, este tipo de actitud perjudica a todos, tanto a los usuarios, como a las compañías antivirus.

Si en cambio, partimos de que los métodos de propagación y la conducta en el sistema de una serie de virus móviles se diferencia cardinalmente de todo lo conocido, para reflejar estas peculiaridades es necesario crear nuevas entradas en la clasificación. Por ejemplo, sería lógico llamar a Cabir (y todos los gusanos que se propagan por Bluetooth) Bluetooth-Worm (y hacer lo mismo con el gusano Inqtana para MacOS). Los gusanos que se envían a través de MMS, los deberíamos llamar MMS-Worm. ¿Pero que haríamos entonces con los gusanos que se envían por Bluetooth y MMS? ¿Cual de los dos métodos de propagación es el "principal"? En Kaspersky Lab, podrían considerar que es MMS. Las otras compañías antivirus podrían clasificarlo como Bluetooth.

El troyano que envía mensajes SMS desde el teléfono infectado a números de pago es, a todas vistas, un Trojan-SMS. Pero el troyano que intercepta todos los SMS entrantes y salientes y los envía al delincuente...¿es un Trojan-Spy o también es un Trojan-SMS? ¿Que denominación será la más comprensible al usuario y evidenciará el peligro de infección?

Hay decenas de preguntas y ejemplos similares.

La industria antivirus tarde o temprano se enfrentará con la necesidad de crear una clasificación unificada para los virus móviles. Esta es una tarea que hay que resolver lo más pronto posible, antes de que la situación se torne crítica y empiece una confusión parecida a la de los nombres que reciben los mismos virus en diferentes compañías antivirus. La experiencia nos muestra que no fue posible crear una clasificación general (que satisfaga a todos) de virus para ordenadores. Es algo que no nos infunde gran optimismo.

Lea la continuación de este artículo en este mismo sitio la próxima semana

Fuente:

- Kaspersky Lab