CNCCS

Consejo Nacional Consultivo de Cyber-Seguridad

Malware en Smartphones

Sobre CNCCS:

El Consejo Nacional Consultor sobre CyberSeguridad (CNCCS) es una organización privada que cuenta con los asociados: AEDEL, Amper, Bdigital, EIIEO, Eside Deusto, Hispasec, Indra, Informática 64, Isec Auditors, Kinamik, Optenet, Panda Security, S2grupo, Secuware, TB security y S21sec. Su misión es poner a disposición de las diversas organizaciones que operan en España, gubernamentales o no, el conocimiento y experiencia de sus miembros en asuntos relacionados con la ciberseguridad nacional o global; con el fin de hacer más segura Internet y las redes de Información, a la vez que potenciar la innovación y el crecimiento económico.

ÍNDICE

1. INTRODUCCIÓN

Los dispositivos móviles han ido evolucionando hasta converger prácticamente en cuanto a funcionalidades con los ordenadores personales, hecho que se traduce en un incremento en la usabilidad de este tipo de dispositivos en cualquier ámbito. Como contrapartida, también aumentan los riesgos asociados a la vertiginosa utilización de este tipo de tecnología, concebida en muchos casos sin tener en cuenta la seguridad.

Este informe tiene como objeto exponer la problemática del malware en este tipo de dispositivos, orientado concretamente a los denominados teléfonos inteligentes (Smartphones).

Se ha optado por realizar una aproximación desde diversos puntos de vista para intentar tener una perspectiva global de este fenómeno y crear una base con la que partir para intentar predecir algunas tendencias futuras y confirmar alguna de las pasadas. De este modo, se han tenido en cuenta aspectos técnicos (peculiaridades de cada plataforma), económicos (la evolución del mercado será uno de los factores que determinen los objetivos potenciales) e históricos (desde su génesis donde los desarrollos eran principalmente pruebas de concepto o simples muestras de creatividad, hasta la actual creación de aplicaciones con fines específicamente fraudulentos).

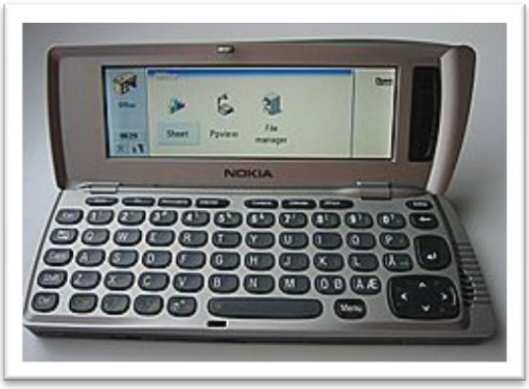
A modo de contexto, se exponen los hitos más significativos en la evolución de estos dispositivos desde su origen a finales de los años 90 hasta los nuevos modelos que están a punto de comercializarse.

2. HISTORIA

Se denomina Smartphone a los dispositivos que partiendo de la funcionalidad de un simple teléfono móvil, han evolucionado hasta estar más cerca en la actualidad de un ordenador personal portátil. Es normal hoy en día que este tipo de teléfonos dispongan de agenda, GPS, reproductor de vídeos y música, amplias opciones de conectividad y un sinfín de funcionalidades que hace unos años eran impensables para este tipo de dispositivos..

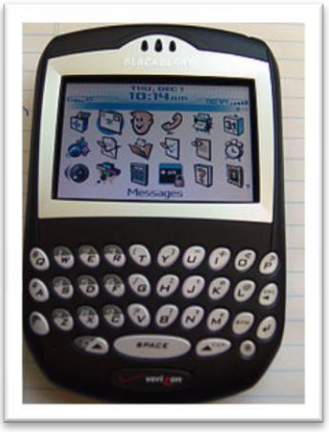
El primer dispositivo considerado como Smartphone fue creado conjuntamente por IBM con la operadora BELLSOUTH en el año 1992. Simon, nombre otorgado a este primer prototipo, fue diseñado inicialmente como una prueba de concepto para mostrar en la feria de tecnología COMDEX, comercializándose posteriormente un año más tarde. Se trata del primer dispositivo en el que se implementaron funcionalidades adicionales a las de un teléfono móvil usual del momento; incluía correo electrónico, fax, calendario, calculadora e incluso un lector de tarjetas PCMCIA.

En el año 1996 Nokia contraatacó con la salida al mercado de su modelo Nokia 9000. Básicamente era una fusión entre las funcionalidades de una PDA y las características de un teléfono inalámbrico normal. Serían otros modelos de este fabricante los primeros en incluir ciertas características indispensables hoy en día para que un dispositivo sea considerado un Smartphone, como pantalla a color e inclusión de conectividad WIFI entre otros. Cabe destacar el modelo Nokia 9210 Communicator por ser el primer dispositivo en adoptar el sistema operativo SymbianOS.



En el año 1997, Ericsson sacó a la luz su teléfono GS88, que fue el primer dispositivo catalogado expresamente como Smartphone. En modelos posteriores se incluiría pantalla táctil.

A partir del año 2000, se produce un incremento significativo en cuanto a la comercialización de distintos modelos de Smartphone. Los hitos más significativos son la salida al mercado de dispositivos con el sistema operativo Windows CE como ordenador de bolsillo y especialmente la comercialización del primer modelo de Blackberry con funcionalidades de Smartphone en el año 2002 por parte del fabricante RIM (Research in Motion), fabricante que ha llegado a cuotas de mercado importantes debido, en gran parte, a la optimización que hace de la gestión del correo electrónico.



Durante estos años, los dispositivos de los diferentes fabricantes han ido evolucionando e introduciendo nuevas características, convirtiendo la mayoría de funcionalidades que hoy conocemos, en estándares de mercado que definen lo que hoy en día entendemos como un teléfono inteligente.

En el año 2007 Apple Inc., introduce su primera generación de smartphones llamados iPhone. Estos dispositivos, que serían uno de los primeros que permitirían manipularse íntegramente desde su pantalla táctil, marcarían un punto de inflexión en este segmento de mercado. Durante estos últimos años, Apple ha sacado nuevas versiones de su iPhone con soporte 3G y descarga de aplicaciones desde su propia comunidad denominada App Store.

En el 2008 sale a la luz Android, una plataforma de código abierto específica para smartphones, basada en una modificación del kernel de Linux. Dicha plataforma se convierte en estandarte del consorcio Open Handset Alliance, creado e impulsado por Google en el año 2007 y compuesto por diversos fabricantes, desarrolladores y operadores (Intel, HTC, Dell, ARM, Motorola, entre otros) con el objetivo de desarrollar estándares abiertos para dispositivos móviles.

El primer dispositivo en utilizar la plataforma Android como base fue el HTC Dream, distribuido por T-Mobile como G1. El software implantado en dicho dispositivo incluía la integración de las aplicaciones de Google; Maps, Calendar, Gmail, y el navegador Chrome. Como novedad,

destaca el uso de aplicaciones de terceros (gratuitas y de pago) mediante la comunidad Android Market.

Otros fabricantes han seguido la línea de crear una comunidad propia para la gestión de aplicaciones externas: RIM y su BlackBerry App World, Nokia con su Ovi Store (mayo 2009), Palm y Palm App Catalog (junio 2009) o Microsoft con Windows Marketplace for Mobile (octubre 2009).

En enero de 2010, Google lanzó al mercado su dispositivo Nexus One basado en Android OS versión 2.2, distribuido en España mediante el operador Vodafone.

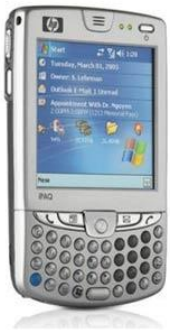
Una vez repasados algunos de los puntos más significativos en cuanto al desarrollo de esta tecnología, a continuación, se expone una visión general de las cuotas de mercado de las distintas plataformas y dispositivos más significativos, con el objetivo de entender cuáles de estos modelos son más susceptibles de convertirse en objetivo de los cibercriminales.

3. EVOLUCIÓN DEL MERCADO DE SMARTPHONES

Los Smartphone están consiguiendo un grado de penetración en el mercado muy elevado para todo tipo de usuarios, con las inevitables consecuencias que esto conlleva. Ha sido una evolución muy rápida, y tal vez siguiendo un camino diferente al esperado.

En 2006 la consultora Gartner predijo que el vencedor de la batalla comercial en el 2010 sería Windows Mobile, quitando el trono a Nokia. Nada más lejos de la realidad; Nokia, a pesar de tener un porcentaje de penetración de mercado importante, parece de capa caída y sus modelos parecen desfasados en comparación con su competencia.

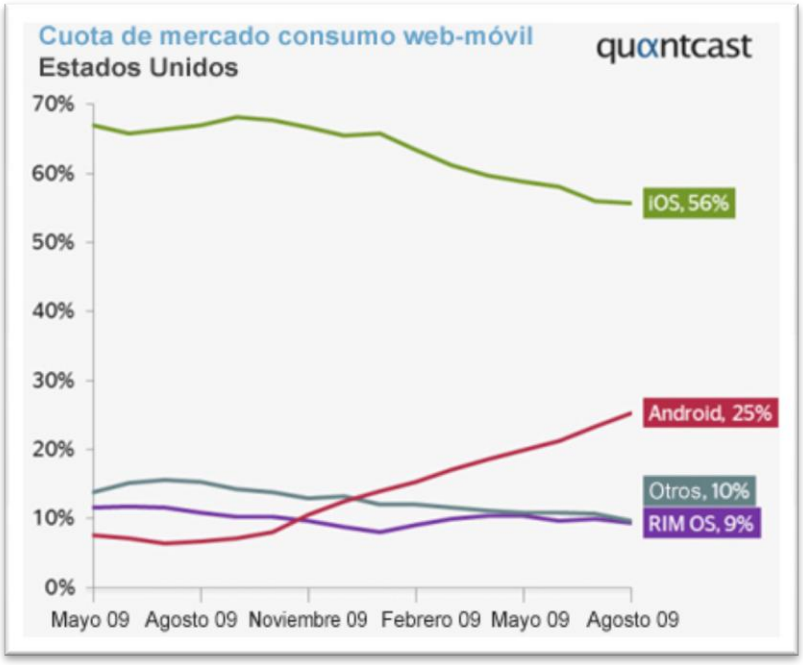
Con la llegada de iPhone a mediados de 2007 comenzó la revolución de los Smartphone, principalmente impulsada por la batalla entre iPhone y dispositivos basados en Android.



El uso de pantallas táctiles revolucionó el mercado, convenciendo a los usuarios gracias a una interfaz sencilla e intuitiva, de una superficie de visualización mucho más amplia y usable que permitía funcionalidades como navegación web y una reproducción de contenido multimedia con buena calidad.

La evolución simultánea del hardware de los dispositivos móviles, permite que en la actualidad sea habitual encontrar terminales con procesadores de 1 GHz y más de 512 MB de RAM, con complementos como GPS, bluetooth, brújula o acelerómetro, lo que ofrece a los desarrolladores un abanico de posibilidades desconocido hasta la fecha.

La generalización de la oferta de tarifas planas de datos en España por parte de las operadoras ha tenido una importancia capital en la popularización de estos dispositivos, y con ello el uso de todos los servicios asociados, desde el correo hasta la banca electrónica, desde cualquier lugar y en cualquier momento.



Fuente: Quantcast "Evolución de cuota de mercado en consumo web-móvil"

Como se puede ver en la gráfica anterior, la tendencia alcista corresponde a los terminales basados en Android, cada vez instalado por más fabricantes. iOS baja, a pesar de mantener el liderazgo, y BlackBerry pasa a tener un discreto 9%.

OS	2009	2010	2011	2014
Symbian	80.876,3	107.662,4	141.278,6	264.351,8
Cuota de mercado (%)	46,9	40,1	34,2	30,2
Android	6.798,4	47.462,1	91.937,7	259.306,4
Market Share (%)	3,9	17,7	22,2	29,6
Research In Motion	34.346,8	46.922,9	62.198,2	102.579,5
Cuota de mercado (%)	19,9	17,5	15,0	11,7
iOS	24.889,8	41.461,8	70.740,0	130.393,0
Market Share (%)	14,4	15,4	17,1	14,9
Windows Phone	15.031,1	12.686,5	21.308,8	34.490,2
Cuota de mercado (%)	8,7	4,7	5,2	3,9
Otros Sistemas Operativos	10.431,9	12.588,1	26.017,3	84.452,9
Cuota de mercado (%)	6,1	4,7	6,3	9,6
Total Mercado	**172.374,3**	**268.783,7**	**413.480,5**	**875.573,8**

De la misma manera, es importante ver qué depara el futuro, puesto que la creación de malware irá de acuerdo a esta evolución. A pesar de que todo sistema tratará de ser explotado, el que sea mayormente usado será el más atacado.

iOS y Android son los sistemas predominantes en el uso de tráfico de web, a pesar de que Symbian todavía es el sistema operativo implantado en el 40% de terminales del mercado, seguido por Android con un 17,7% y BlackBerry con un 17,5%. Gartner prevé que en 2014 Android sea la plataforma más usada, así como la existencia de un mayor número de Smartphones que de PCs en el año 2013, lo que nos da una clara idea de la importancia de la seguridad en los mismos.

4. SEGURIDAD EN DISPOSITIVOS MÓVILES

Los dispositivos móviles disponen de crecientes incentivos para ser atacados por los cibercriminales. Su uso es está generalizado y en continua expansión, contienen una vasta cantidad de información personal y confidencial, y son usados (o tienen la capacidad) para realizar prácticamente todo tipo de transacciones online.

Un aspecto interesante en lo referente a la seguridad en estos dispositivos móviles son sus canales de comunicación. En este sentido están más expuestos que los tradicionales PCs ya que las amenazas pueden venir por: SMS, Bluetooth, Wi-Fi, navegadores web, aplicaciones, y correo electrónico, hecho que puede propiciar la propagación de código malicioso orientado a este tipo de plataformas.

Se trata de dispositivos realmente personales. Precisamente es esta capacidad de personalización que disponen lo que los convierte en más peligrosos. Es común que exista un PC para toda la familia, pero también es común que cada miembro de la familia disponga de un teléfono móvil que lo llevará consigo todo el tiempo. El hecho de que todavía existan mínimas muestras de malware para móviles, la falta de concienciación por parte del usuario, y la limitación de la batería para ejecutar aplicaciones complejas como soluciones antivirus, son factores que actualmente juegan en contra del uso de los mismos.

4.1. Falsa sensación de seguridad

Físicamente los teléfonos inteligentes dan una sensación de dispositivos más personales porque los llevamos siempre encima. Tenemos un control físico total sobre ellos y esto hace pensar que son menos accesibles a intrusos. Esta falsa sensación de seguridad, junto con el uso de aplicaciones del estilo de correo electrónico, redes sociales y contenido multimedia privado, lleva a que se almacenen datos personales y confidenciales en el terminal, muchas veces de forma inadvertida para el propio usuario.

Esta sensación de seguridad conduce a que los usuarios descuiden las precauciones básicas tales como cambiar la configuración por defecto de Seguridad.

En la actualidad el número de ataques en Smartphones es pequeño en comparación a los ataques en PCs. Existen 60 millones de programas maliciosos conocidos para PC en contraposición de 600 para Smartphones, aunque se prevé un progresivo aumento en la aparición de código malicioso para estos últimos.

En este sentido el pasado 25 de septiembre S21sec hizo público el primer malware capaz de evadir un sistema de autentificación de 2 factores (PC + móvil) usado para realizar transacciones en banca electrónica y que se detalla en los puntos finales de este informe.

Múltiples factores conducirán a la aparición de nuevas amenazas. En la mayoría de los Smartphones el único mecanismo de seguridad que tienen es la simple contraseña. La seguridad y fiabilidad de las aplicaciones disponibles para instalar son factores clave en la seguridad de estos dispositivos.

En caso de robo o pérdida del dispositivo sería conveniente disponer de mecanismos de cifrado que no permitan el acceso a la información contenida. Esto es especialmente delicado en organizaciones y empresas donde la delgada línea entre las políticas de seguridad corporativas y el uso personal de estos dispositivos se ha empezado a cruzar debido a la gran acogida de estos dispositivos por el público general.

La seguridad de los Smartphones no sólo hay que verla desde el punto de vista del usuario final. Su alcance comprende desde el núcleo del sistema operativo de cada Smartphone hasta el modelo de distribución de sus aplicaciones, pasando por los entornos de desarrollo de cada plataforma.

4.2. Kits de desarrollo de aplicaciones (SDKs)

Las plataformas móviles más utilizadas (Blackberry, iPhone, y Android) proporcionan entornos de desarrollo (SDK, del inglés Software Development Kit) para la creación de las aplicaciones. Cada SDK tiene sus características propias, muchas de ellas pensadas para mejorar la seguridad, como son el cifrado, la restricción de acceso al hardware o la administración de memoria. Sin entrar en detalle, los principales entornos de desarrollo de cada plataforma son:

- **SDK de Android**: Impulsado por Google. El código para crear aplicaciones para Android es Java, por lo que las aplicaciones Android se ejecutarán sobre una máquina virtual especial, denominada Dalvik. Aunque es posible utilizar otros entornos de desarrollo, la plataforma de código libre Eclipse es la más extendida para este entorno. La característica de plataforma abierta es lo que diferencia a Android de su competencia.

- **SDK de Blackberry**: Proporcionado por RIM, el fabricante de Blackberry. El Sistema Operativo es propietario y el entorno para el desarrollo de aplicaciones es JavaME. Las aplicaciones desarrolladas necesitan ser empaquetadas para mantener la seguridad proporcionada por el sistema operativo. Las aplicaciones deben firmarse digitalmente para que puedan asociarse a una cuenta de desarrollador.

- **SDK de Nokia**: Anteriormente para desarrollar aplicaciones para esta plataforma era necesario hacerlo con el entorno de desarrollo para Symbian. Ahora Nokia ha apostado por la plataforma WRT (Web RunTime), más accesible para los desarrolladores.

- **iOS**: El iPhone necesita ser cerrado para mantener su seguridad y estabilidad. Por ello Apple proporciona su kit de herramientas de desarrollo para iOS. La última versión iOS4 ha abierto algunas restricciones en la licencia permitiendo el uso de entornos de desarrollo intermedios, abriéndose así a plataformas como Flash, Java, Silverlight o Mono.

Como prueba de concepto, en un artículo de la BBC informan de cómo se descargaron un Kit de desarrollo de aplicaciones, aprendieron conceptos básicos para programar en Java y recopilaron algunos fragmentos de código disponibles en la red. Con todo ello en pocas semanas crearon un juego que sin el conocimiento del usuario recopilaba contactos, copiaban mensajes de texto y detectaba la localización del teléfono, todo ello se enviaba a una dirección de correo pre-configurada. El juego completo consistía en 1500 líneas de código de las cuales 250 eran spyware. La aplicación se probó en un móvil, pero no se subió a ninguna tienda de aplicaciones.

Los desarrolladores tienen que ser responsables e informar de los datos a los que tendrán acceso sus aplicaciones. Pero en muchas ocasiones ni siquiera ellos conocerán toda la funcionalidad de su código al usar aplicaciones de terceras partes. Sin duda el control de las aplicaciones disponibles para estos dispositivos será clave para mantener la seguridad del usuario final.

4.3. Mercados de aplicaciones

El modelo de App store impulsado por Apple ha sido el modelo copiado por todos los demás fabricantes de móviles. Este modelo se basa en desplazar la seguridad de las aplicaciones para móviles a un punto central de distribución, en el cual cada fabricante impone sus propias normas de distribución de aplicaciones para sus dispositivos. De esta manera se intenta controlar que las aplicaciones distribuidas están libres de código malicioso.

- **App Store de Apple**: Para que una aplicación pueda estar disponible en el sitio de Apple tiene que ser aprobada por Apple. Además, los desarrolladores se deben crear una cuenta como tales y pagar una tarifa anual. Entre las comprobaciones realizadas por Apple se encuentran, entre otras: que la aplicación funcione tal y como se anuncia, y que no desestabilice al iPhone.

- **Android Market**: Por su parte, Google no veta las aplicaciones subidas al mercado de Android. Google dispone de reglas específicas, pero delega toda la responsabilidad del software que suministra en el usuario. La protección de Android contra las aplicaciones maliciosas es un modelo de seguridad basado en “capacidades”. Cada aplicación Android debe indicar al Sistema Operativo del móvil las capacidades que necesita. Al instalar una aplicación, el sistema operativo listará las capacidades que la aplicación necesita para ejecutarse, pero es responsabilidad del usuario decidir si estas capacidades son consistentes con la funcionalidad de la aplicación.

  Por su parte, Google podrá remotamente deshabilitar aplicaciones que encuentre maliciosas. Asimismo, también requiere que los desarrolladores se registren y que declaren los permisos que sus aplicaciones necesitarán para interactuar con el teléfono.

- **OVI Store de Nokia**: Propietaria, similar a Apple, pueden vetar las aplicaciones de su tienda.

- **App Store de BlackBerry**: Propietaria, similar a Apple, pueden vetar las aplicaciones de su tienda.

A modo resumen, el modelo de software de Apple, Blackberry y Nokia es cerrado en contraposición al modelo abierto de Android. Los tres primeros asumen la responsabilidad de las aplicaciones albergadas en su mercado, mientras que en Android esta responsabilidad se otorga a los propios desarrolladores. Hasta ahora, se ha demostrado que cada modelo tiene sus pros y sus contras, y que ninguno de ellos ha evitado la entrada de malware en sus dispositivos.

Para finalizar, añadiremos que la confianza en los mercados de aplicaciones como la primera frontera de Seguridad de los dispositivos es algo preocupante, lo cual subraya la necesidad de las buenas prácticas de programación y almacenamiento seguro de datos.

Cabe destacar que la diversidad de tecnologías móviles, en comparación con la dominación de plataformas Windows en PC, puede jugar en contra de una gran proliferación de código malicioso en este entorno, ya que los creadores de malware deberán escribir el código malicioso apropiado para cada plataforma.

5. MALWARE EN DISPOSITIVOS MÓVILES

El fenómeno del código malicioso destinado a Smartphones está empezando a salir de su etapa inicial en cuanto a desarrollo y madurez se refiere. Aunque en esta última década se han documentado y estudiado diversas familias de malware orientadas a este segmento, hasta ahora eran muy pocas las que generaban un beneficio económico a sus autores (principalmente mediante el envío de mensajes SMS a servicios Premium controlados por los mismos actores) y menos aún aquellas cuyo objetivo fuera explícitamente el robo de credenciales bancarias o vulnerar estas plataformas para anularlas como segundo factor de autenticación en transacciones online.

Como se irá mostrando a lo largo de este apartado, la etapa en la que se creaba código malicioso únicamente como prueba de concepto ha ido dejando paso a otros desarrollos con otro objetivo bastante menos desinteresado: realizar fraude.

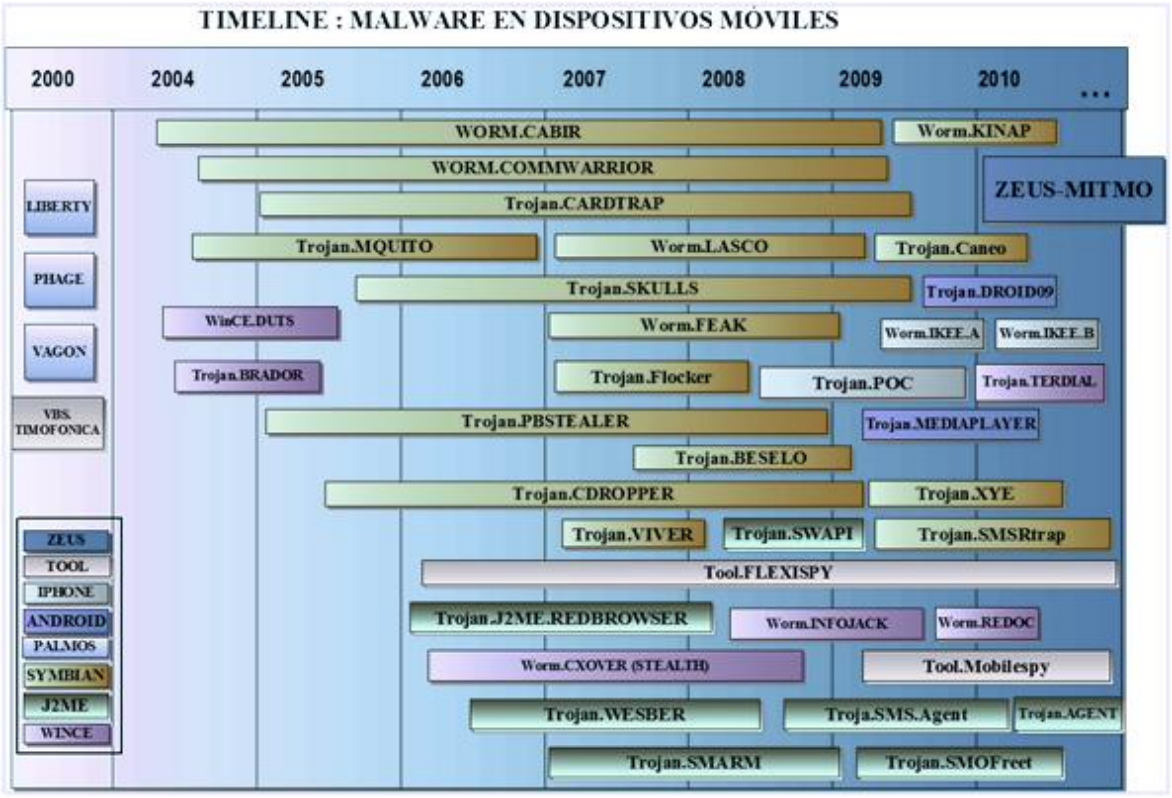
Tal y como vienen anticipando muchas de las predicciones efectuadas en los últimos años, la evolución esperada del cibercrimen pasa por extender su control hacia otro tipo de plataformas, ya sea para conseguir nuevas vías de propagación y monetización, para ser usadas como nuevos recursos de apoyo a sus infraestructuras o simplemente para vulnerar el segundo factor de autenticación mediante el uso de teléfonos móviles. Se ha comprobado recientemente (Incidente Zeus-Mitmo que se detalla posteriormente) que este hecho ha empezado a modificar el modus operandi de diferentes grupos de criminales y especialmente el de su código malicioso, el objetivo es potenciar la convergencia en una misma “infección” o “ataque”, es decir, ir un paso más allá e intentar infectar el máximo número de dispositivos de un mismo usuario.

Como punto inicial para exponer el contexto histórico, se partirá del siguiente gráfico en el que se exponen las muestras más significativas de malware desde el año 2000, incluida su categoría y el sistema operativo/plataforma al que van destinados. Se ha intentado exponer la persistencia de cada familia a lo largo del tiempo, en base a varios criterios:

- Número de incidentes documentados a lo largo de su ciclo de vida.
- Número de muestras y variantes a los largo del tiempo.
- Estadísticas de diversas firmas antivirus.
- Ciclo de vida del dispositivo al que va dirigida la muestra.
- Peculiaridades de la muestra (código obsoleto, viabilidad de infección, distribución, objetivo del desarrollo, etc.).

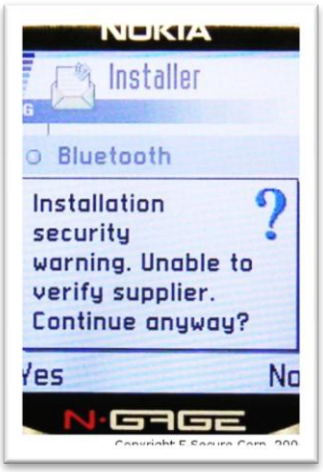
La gráfica parte desde el año 2000 en el que destacan cuatro muestras, tres de ellas destinadas a plataformas con sistema operativo PalmOS, que serían considerados los primeros virus orientados a uno de los predecesores de los Smartphones, los dispositivos PDA.

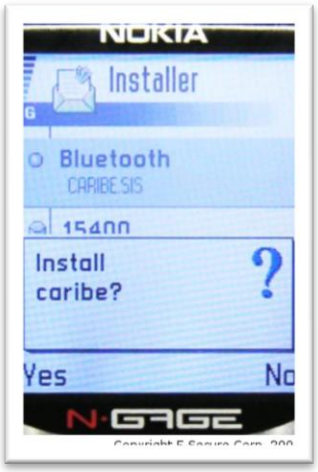
La cuarta muestra corresponde a **VBS.Timofonica**, aunque destinado a plataformas Microsoft, fue el primer virus en propagarse aprovechando el sistema de correo electrónico destinado a usuarios de un servicio móvil, enviando una copia de sí mismo no solo a los contactos encontrados en el sistema sino a los subscriptores del servicio movistar.net (mediante el cual era posible recibir el correo en el móvil), el binario enviaba mensajes a números aleatorios dentro del rango de movistar PREFIJO_MOVISTAR+número_6_cifras_aleatorio@movistar.net.



Fuente: Timeline S21sec e-crime

El primer código malicioso destinado a plataformas consideradas como Smarphones apareció el 14 de junio del año 2004, concretamente la primera muestra fue recibida por la firma de antivirus Kaspersky por parte de un coleccionista de virus llamado VirusBuster (de origen español). **Cabir**, nombre otorgado al virus, se desarrolló como prueba de concepto por parte de "Vallez", integrante del grupo de desarrollo e investigación vírica 29A, para demostrar que era posible lograr una infección en plataformas no estándar hasta el momento (en este caso destinado a plataformas SymbianOS). Utilizando el formato .sis, su característica más significativa era la propagación mediante Bluetooth.





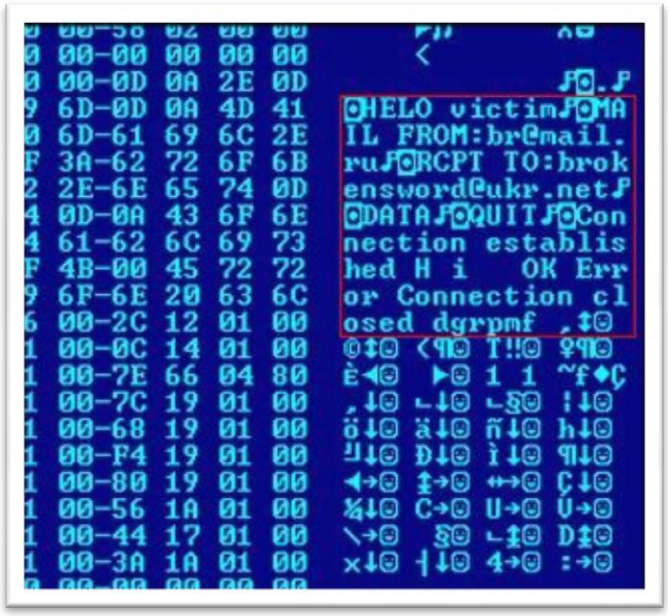
A finales de 2004, empezaron a salir distintas variante de Cabir con una carga más maliciosa que su original. Una de las mejoras implementadas en determinadas variantes era la propagación masiva en las que, a diferencia de Cabir.A, que solamente tenía la capacidad de replicarse a un dispositivo a la vez, podían hacerlo hacia cualquier teléfono descubierto vía bluetooth.

Aunque no considerada como una implementación de código malicioso per se, otra muestra de este tipo fue detectada algunos meses después de Cabir. Se denominó **Mosquito** y atacaba específicamente a plataformas Symbian. Mosquito o Mquito fue implementado como un sistema anti-copia por parte de la desarrolladora Ojum Software, que incluyó una funcionalidad "oculta" en sus juegos con la que permitía detectar la ejecución del juego en un teléfono no registrado (es decir, una copia ilegal del juego), y notificaba a los desarrolladores mediante el envío de un mensaje SMS sin que el usuario lo advirtiera (hasta ver en el detalle de la factura el envío de dichos mensajes).

Un mes más tarde a la aparición de Cabir, se hizo pública una muestra de "**Duts**" (Win.CE4.Duts.a), un binario destinado a demostrar las vulnerabilidades de dispositivos basados en Windows CE, una vez más creado por un integrante del grupo 29A. También fue desarrollado como prueba de concepto y no contenía ningún tipo de carga maliciosa, tampoco fue utilizado "in the wild" ya que la primera muestra fue enviada directamente por su creador a distintas firmas anti-virus.

Una vez infectado el dispositivo, mostraba un mensaje con la pregunta "Am i allowed to spread?" (Me permites propagarme?) En el caso de que el usuario aceptara, Dust infectaba todos los ejecutables que encontraba en su mismo directorio.

Aún en el año 2004, concretamente en el mes de agosto, destaca la aparición de **WinCE.Brador.A**. Este binario llevaba implementadas funcionalidades de "backdoor" y fue desarrollado íntegramente en ensamblador para PocketPC. Una vez infectado el dispositivo, abría el puerto 2989/TCP quedando a la escucha para comandos entrantes que permitían el control del dispositivo. Brador tiene varias características destacables como transferencia de archivos hacia/desde el dispositivo, iniciar ejecutables, mostrar mensajes al usuario, incluso enviar el contenido de carpetas al atacante remoto. Una vez infectado el dispositivo, enviaba un correo electrónico de notificación a la dirección brokensword@ukr.net (supuestamente el autor del código) conteniendo la dirección IP del sistema comprometido. El malware descrito no tenía implementada ninguna funcionalidad de propagación.

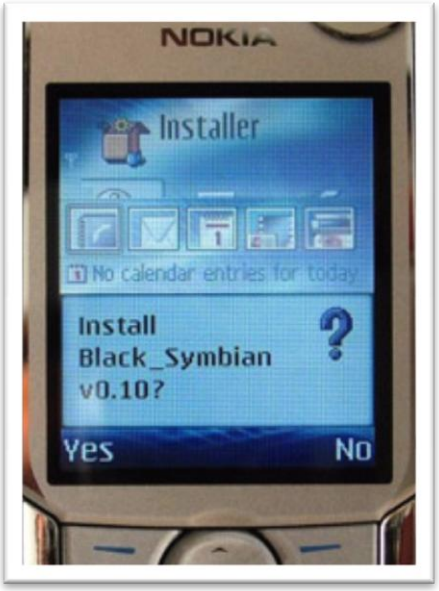


A finales de 2004, concretamente en el mes de noviembre, se descubre el código malicioso **Skulls** (Skuller.A) que se convertiría en una de las familias destinadas a dispositivos móviles con más variantes conocidas. Skull posee funcionalidades de troyano e incorpora una carga más maliciosa que sus homólogos anteriores. En este caso, sobrescribe aplicaciones legítimas por otras que están corruptas, derivando en la inutilización del sistema infectado. Una de las novedades de este código fue la utilización de una vulnerabilidad en la plataforma Symbian para escribir ficheros sin tener los privilegios adecuados. Uno de los síntomas inequívocos de la infección es el reemplazo de todos los iconos del menú con la imagen de una calavera. El método de propagación en este caso era variado, desde su envío por correo electrónico hasta redes de compartición de archivos (P2P), con el nombre de Extended-Theme-Manager. Cabe destacar que en algunas de sus variantes, Skull fue utilizado como “dropper” para instalar una variante de Cabir, seguramente para optimizar los métodos de propagación de éste último.

A partir del año 2005, y debido a la filtración del código fuente de Cabir.A, aparecieron nuevas variantes con una carga más maliciosa que su original (que simplemente tenía capacidades de “gusano” replicándose vía bluetooth) y con mejoras significativas en el modo de propagación.

Un caso a destacar es el de **Cardtrap**, que con un “payload” de funciones similares a Skulls (sobrescritura de archivos) es considerado el primer código malicioso multiplataforma, ya que no solamente tenía como objetivo plataformas basadas en SymbianOS sino que también afectaba a versiones de Windows. Debido a que copia un código malicioso destinado a la plataforma de Microsoft (concretamente una versión de Padobot), junto con un autorun.inf para provocar su ejecución al insertar la tarjeta extraíble en un ordenador. Podría considerarse a Cardtrap una de las muestras pioneras en complementar la infección de un dispositivo móvil con la de un ordenador estándar.

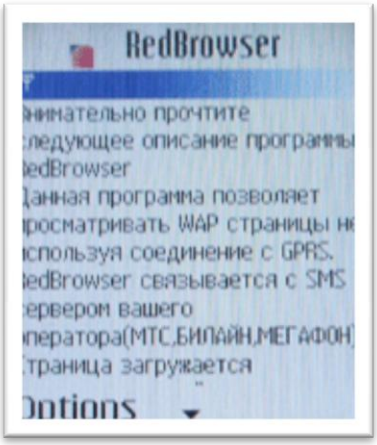
El método de propagación se llevaba a cabo mediante correo electrónico o a través de su difusión en redes P2P, utilizando el nombre Black_Symbianv0.10. Es necesario hacer mención especial a la segunda de las ocho principales variantes descubiertas de Cartrap, ya que una vez infectado y reiniciado el dispositivo por parte del usuario, dejaba inutilizado el teléfono.



A finales del año 2005, aparece en escena **Pbstealer**, teniendo el dudoso honor de convertirse en uno de los primeros binarios orientados al robo de información confidencial en dispositivos móviles. La función principal de Pbsetaler es la de copiar la lista de contactos a un archivo de texto, y su posterior envío al primer dispositivo detectado vía Bluetooh. Este código no tenía implementadas funciones de propagación.

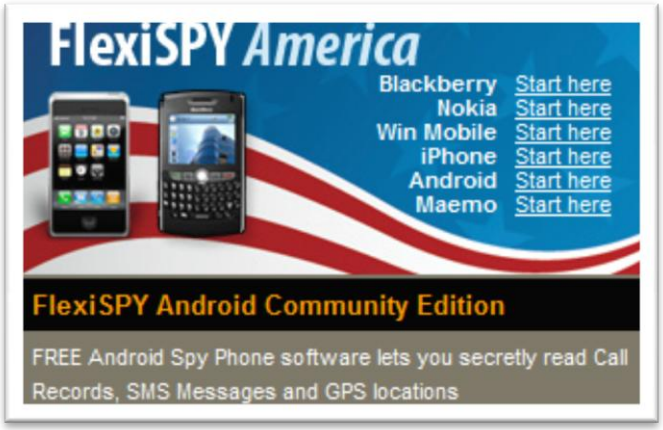
A partir del año 2006 y debido a los avances tecnológicos de los terminales, se detectan nuevos malware destinados a este tipo de dispositivos. Se empieza a tener cierta percepción de peligro y a desarrollar soluciones de monitorización destinadas a este sector.

Entre los binarios destacados de ese año, destaca **REDbrowser**, descubierto en Febrero de 2006 y cuya carga maliciosa consistía en enviar continuamente mensajes SMS a diversos servicios localizados en Rusia, con la consiguiente pérdida de saldo del dispositivo infectado. Destacar que fue la primera especie codificada íntegramente en J2ME (Java Mobile Edition v2), cosa que le permitía ejecutarse en cualquier dispositivo que soportara esta plataforma. El dispositivo solicitaba al usuario continuamente permisos para realizar el envío del mensaje SMS. REDbrowser pretendía ser un servicio para navegar por recursos accesible mediante el protocolo WAP utilizando el servicio SMS para supuestamente recibir las páginas solicitadas por el usuario.



En el mes de marzo de 2006, se descubre la primera versión del gusano **CxOver** que sería el primer código malicioso con capacidades de ocultación frente al usuario, siendo el primer tipo de código que no necesita intervención del usuario para infectar el dispositivos, programado por Dr. Julius Storm en el lenguaje MSIL (Microsoft .NET's Intermediate Language) permitía infectar sistemas operativos Windows con soporte .NET así como dispositivos móviles. El método de propagación estaba basado en el protocolo ActiveSync; cuando infectaba un ordenador, Cxover buscaba dispositivos vinculados mediante este protocolo, copiándose a todos aquellos que encontraba.

Ese mismo mes, se empieza a comercializar con Flexispy; la primera aplicación comercial legítima cuya función es la de interceptar las comunicaciones del teléfono, enviando copia de los correos y mensajes MSS a una web protegida por contraseña. En el mismo mes fue descubierto el gusano **Mobler**, cuyo método de propagación consistía en copiarse a sí mismo en cualquier dispositivo en el que tuviese permisos de escritura.



Casi un año más tarde (mayo de 2007) se descubre **Viver.A**, cuya carga maliciosa consistía en enviar continuamente mensajes SMS a un servicio Premium, cuyos beneficios obtenidos iban destinados en parte al autor del código.

Transcurrió un año sin novedades significativas en este campo, hasta enero del 2008 en el que se detecta iPhone.A, pretendiendo ser una actualización para su firmware, una vez instalado, sobrescribía algunas utilidades del sistema.

En febrero de 2008, se descubre **Infojack**, código malicioso para plataformas WINCE que roba información del dispositivo y la envía a un servidor en Internet.

En el año 2009, se detectaron nuevas variantes de código ya conocido y siguieron las novedades en cuanto a objetivos se refiere. Una de las muestras más interesantes de este periodo es el gusano **Ikee.A**, que fue el primer gusano destinado exclusivamente a plataformas iPhone. Una vez infectado el dispositivo, cambiaba el fondo de pantalla por una imagen de Rick Astley. Consiguió unas 21.000 víctimas en dos semanas.

Dos semanas más tarde de la aparición de Ikee.A, se descubrió su segunda variante, orientada esta vez a realizar fraude. **Ikee.B** o Duh (por el nombre del binario principal) incorpora nuevas funcionalidades entre las que destaca la estructura típica de aplicaciones orientadas a cometer fraude; esto es, la posibilidad de ser controlada mediante un panel de control remoto y el envío de información confidencial a su centro de control (situado en Lituania). En un momento dado de su corto ciclo de vida, el centro de control envío un comando a los dispositivos iPhone que controlaba para redirigir a los usuarios que accedían a ciertas webs de banca electrónica a un servidor réplica situado en Japón controlado por los cibercriminales, es decir, la típica infraestructura de pharming aplicada a un dispositivo móvil.

En noviembre de 2009, se descubre una aplicación maliciosa en Android Market llamada **Droid09**. Ésta pretendía ser una aplicación para la gestión de bancos online, ofreciendo al usuario un listado bastante limitado de los mismos, de los que pedía las correspondientes credenciales de acceso. Desde la percepción del usuario, no era de extrañar que una aplicación bancaria pidiese tales datos, aunque el destino de sus credenciales no fuera en absoluto legítimo. La aplicación fue borrada inmediatamente de Android Market. Otro tipo de malware detectado a finales de 2010 para esta plataforma es Android Fakeplayer, que pretendiendo ser una aplicación para reproducir vídeos, es en realidad un código malicioso destinado a enviar mensajes SMS Premium. Hasta el momento se han descubierto 3 variantes de este mismo malware.

Hasta ahora, se ha podido comprobar cómo el objetivo principal del ataque han sido las plataformas basadas en Symbian, aunque en los dos últimos dos años y teniendo en cuenta su relativamente corto ciclo de vida, las plataformas basadas en iOs (iPhone) y Android ya muestran indicadores de ser objetivos considerados por los cibercriminales. Cabe destacar también, la proliferación de malware orientado a plataformas J2ME en los últimos años.

6. ZEUS Man In The Mobile

Una vez establecidos los hitos más significativos de la última década en cuanto a código malicioso orientado a dispositivos móviles, es hora de dar paso a la actualidad. Para ello se dedica este punto de manera íntegra a exponer uno de los descubrimientos que puede marcar otro punto de inflexión en la evolución de este fenómeno: la convergencia de malware de PC y de Smartphone en un único esquema, conocido como MITMO (Man in the Mobile). Implementado como complemento en uno de los troyanos bancarios más extendidos en la actualidad, Zeus.

Aunque hasta el momento Zeus no ha sido un código malicioso orientado a Smartphones, es importante destacar que ha sido una de las primeras familias de código en tener en cuenta uno de los potenciales segundos factores de autenticación más utilizados y extendidos para conseguir el éxito en su esquema. En este caso, ha empleado una técnica para evitar el segundo factor de autenticación basado en SMS para ciertos modelos de teléfono.

Zeus es un troyano orientado principalmente al robo de credenciales bancarias. S21sec ha ido estudiando las interesantes variaciones que ha sufrido durante todo su ciclo de vida, no solo en su infraestructura sino en el modo de robar las credenciales a los usuarios infectados.

Principalmente, Zeus se basa en tres técnicas distintas para llevar a cabo su robo de información:

- **Técnica de Redirección**: Mediante esta técnica el usuario es redirigido a otro sitio web que pretende ser legítimo pero que, en realidad, es una copia del aplicativo de la entidad preparado de tal manera que todos los datos introducidos se guardan para posterior uso por parte del criminal.

- **Técnica de Captura**: Ya sea mediante la captura de las pulsaciones del teclado o mediante la captura de pantalla (dependerá de lo estipulado en su fichero de configuración).

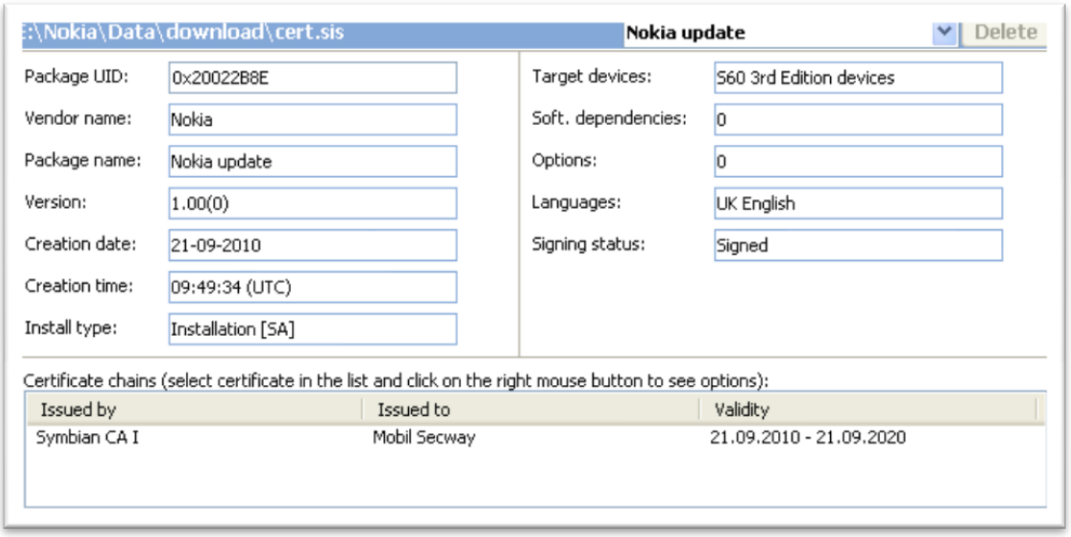
- **Técnica de Inyección**: Consistente en inyectar código HTML en el navegador del usuario infectado para solicitar datos que normalmente la entidad no pediría (en las configuraciones estudiadas, el dato solicitado suele ser el código de seguridad completo). Suele combinarse junto con la técnica descrita anteriormente.

Actualmente la técnica que más se utiliza (seguramente por su eficacia) y la que más evoluciones ha demostrado a lo largo de la historia de este código malicioso es la técnica de inyección. Una de las evoluciones más recientes ha sido la de incluir inyecciones de código de

manera que al usuario, una vez autenticado en su banca electrónica, se le pide su número de teléfono móvil y su modelo.

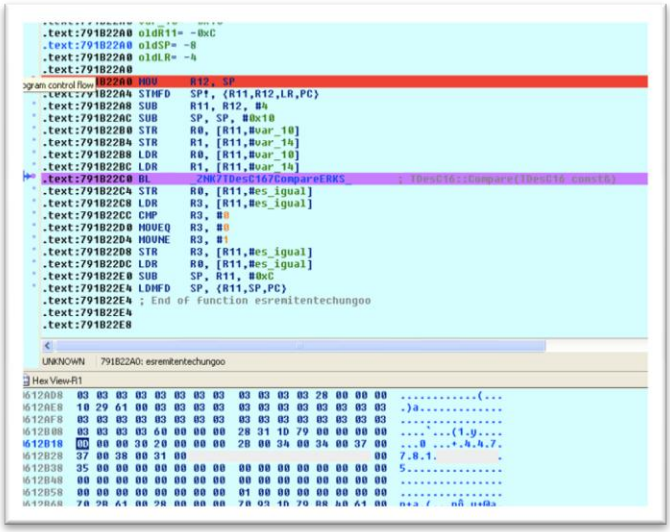
Una vez introducidos estos datos por parte del usuario infectado, éste recibe un mensaje para descargar una supuesta aplicación complementaria al sistema de banca legítima. Se ha detectado código malicioso orientado a Blackberry y a sistemas basados en Symbian. En este caso se analiza la muestra destinada a la segunda plataforma.

El archivo descargado se denomina cert.sis (MD5: b1ce81affa43bf0e51637e702d908d55) está firmado digitalmente por el proveedor MobileSecWay (relacionado con el dominio www.mobilesecway.org) del que por el momento no se tiene más información. Dentro del contenedor está la aplicación NokiaUpdate.exe (MD5: 05c97a2f749f6a2cb92e813a48e54253) que es la aplicación maliciosa en sí.



Las acciones inmediatas llevadas a cabo una vez instalada la aplicación en el dispositivo es la confirmación de su correcta ejecución mediante el envío de un mensaje SMS al teléfono +447781481725 (presumiblemente número destino controlado por el responsable de esta nueva infraestructura) con el texto "App installed ok".

A continuación monitoriza todos los mensajes SMS entrantes. En caso de que vengan del teléfono +447781481725, analiza los mensajes en busca de los comandos que debe llevar a cabo.



Las distintas órdenes que pueden ser recibidas y ejecutadas son:

- BLOCK ON: Ignorar peticiones por SMS.
- BLOCK OFF: No ignorar peticiones por SMS.
- SET ADMIN: Cambiar el número de teléfono desde el que acepta ordenes.
- ADD SENDER: Añadir contacto al que interceptar los mensajes.
- ADD SENDER ALL: Interceptar mensajes de cualquier emisor.

- REM SENDER: Borrado de un contacto.
- REM SENDER ALL: Borrado de todos los contactos.
- SET SENDER: Actualizar contacto.

Una vez ejecutadas las órdenes recibidas, el mensaje SMS original se elimina del dispositivo. Dicha interceptación ocurre antes de que los mensajes sean mostrados por pantalla en el dispositivo, de modo que el usuario no es consciente de la comunicación. La aplicación tiene implementadas funcionalidades que le permiten el reenvío de mensajes SMS, cuya finalidad es el reenvío de los TAN (Transaction Authentication Number) usados como segundo factor de autenticación en ciertas operaciones bancarias. Por lo tanto lo que consigue este esquema es evitar la autenticación de dos factores, pudiendo usar las credenciales robadas para acceder a la cuenta de la víctima y realizar el fraude mediante intercepción del SMS.

El hecho de poder recibir órdenes por SMS conduce a infecciones mucho más robustas. Con malware tradicional siempre hay un punto final central que se puede cerrar y se anula el fraude (servidor C&C, servidor de pharming, etc.). Los únicos casos en que esto no es posible es cuando se usa P2P como C&C o el troyano es un troyano tradicional de puerta trasera que escucha en un determinado puerto. En estos últimos casos el atacante tiene que seguir recibiendo la IP de la víctima de alguna forma (si es dinámica) para poder acceder a su sistema y se puede cortar el punto de recepción (cuenta de correo, servidor web, etc.). Además, con la mayoría de las redes usando algún tipo de NATing o Firewalling (incluidos los routers ADSLs domésticos), la efectividad de este tipo de ataques en ordenadores es muy inferior a lo que un día fue.

Por el contrario, el móvil puede recibir órdenes por SMS, lo cual hace que ciertos patrones de fraude no se puedan cortar de raíz acabando con un punto centralizado. En el caso del Zeus Mitmo, una vez se echó abajo el número al que se enviaban por defecto los tokens interceptados, el atacante podría haber enviado un mensaje a los móviles ya infectados para que enviaran los datos a un número nuevo. Una vez ya se tiene un móvil infectado no hay forma de evitar la intercepción de los tokens acabando con un punto central. La única forma sería que la operadora inspeccionara todos los mensajes enviados por su red y bloqueara los que siguen ciertas expresiones regulares asociadas a troyanos (^SET ADMIN: .*$, etc.). Dicho esto, hay infinitas posibilidades de camuflar los comandos con ciertas sintaxis que hagan imposible el bloqueo por colisión con patrones legítimos.

El teléfono destino de los mensajes se encuentra en Reino Unido y desactivado a fecha de hoy. Scotland Yard ha abierto investigación y está siguiendo el rastro de un segundo teléfono implicado. Parece ser que desde el verano estaban realizando pruebas, mandando SMSs con el texto “App installed ok”. En Alemania han aparecido los primeros casos de fraude con una tipología idéntica a la descrita.

Hay que tener en cuenta que la infección a partir del enlace es debida a que el usuario víctima instala el aplicativo malicioso. Este hecho se produce por la falta de percepción por parte del usuario de este tipo de amenazas, no siendo más que un *phishing* en un entorno distinto al habitual.

Las recomendaciones no pueden pasar más que por concienciar a los usuarios ante la posibilidad de este nuevo modo de fraude, así como cambiar la percepción de que la autenticación de dos factores es invulnerable. Conceptualmente es muy segura, pero según convergen los dispositivos de telefonía y ordenadores personales, esto es cada vez menos cierto. Algunas soluciones apuntan a usar otros medios de segundo nivel de autenticación, aunque en un teléfono comprometido y dependiendo del modelo, se podrían llegar a desviar incluso las llamadas de voz.

7. EL FUTURO QUE VIENE

Hay que estar preparado para futuras infecciones, los creadores de malware evolucionan continuamente sus técnicas y no cabe duda que el malware para dispositivos móviles va a seguir evolucionando:

- Móvil como medio de pago: Se están realizando grandes avances con el chip NFC (Near Field Communication). NFC es una tecnología de comunicación inalámbrica que permite transmitir datos entre dispositivos a unos 5-10 centímetros, y se puede utilizar para realizar pagos, transferir información, etc. Las ventajas de comunicación con el chip NFC radican en la velocidad de emparejamiento, el consumo, y su compatibilidad con RFID. Algunos de los últimos modelos de Nokia (como el C7) integran ya este chip, los dispositivos de Google o el futuro iPhone 6 también lo incluirá.

- Cada vez más bancos están creando aplicaciones para banca electrónica en el móvil (aplicaciones independientes del navegador, como cualquier otra aplicación de cualquier store). Es posible que el nuevo malware de móviles comience a usar técnicas más avanzadas como hooking de ciertas syscalls, para interceptar las llamadas a la API por parte de estas aplicaciones y así capturar información sensible.

- Seguimiento de individuos: Ahora que los móviles incorporan GPS sería trivial crear un programa que periódicamente consulte el GPS y mande las coordenadas a un determinado servidor web de un atacante y así poder seguir los movimientos de una determinada persona.

- Ahora que los móviles incorporan conexión a redes WiFi, se podría pensar en gusanos móviles que escanearan los sistemas de una determinada red WiFi y trataran de explotar las vulnerabilidades de estos para pasar código malicioso a otros sistemas, como ordenadores personales.

- Ataques de ingeniería social avanzados. Algunas de las muestras mencionadas anteriormente tienen la capacidad de manipular la agenda del usuario, esto puede ser muy útil para lanzar ataques de ingeniería social orientada y avanzados, cambiar la asociación entre un determinado nombre y número para hacerse pasar por otra persona o entidad, etc.

8. CONCLUSIONES

La limitada concienciación en lo referente a seguridad de los usuarios de estos dispositivos y el consecuente comportamiento pueden ser los factores de mayor riesgo para los smartphones a corto plazo. Es de gran importancia comprender que un dispositivo móvil de estas características ya no es un simple teléfono y no puede ni debe ser tratado como tal. A diferencia de las generaciones previas de móviles donde la peor amenaza podía ser una infección a través de Bluetooth, los Smartphone actuales están expuestos a los mismos peligros de Internet que la industria del PC lleva padeciendo durante años. Estos peligros son crecientes a medida que estos dispositivos son usados por la banca electrónica como segundo factor de autentificación dada la convergencia entre PCs y móviles, ya que provoca que ambos canales no sean totalmente independientes entre sí.

Muchas de las precauciones de seguridad para los Smartphones son similares a las de los PC. Se recomiendan las siguientes buenas prácticas para ayudar a proteger los dispositivos móviles:

- Habilitar medidas de acceso al dispositivo como el PIN o contraseña si está disponible.
- Configurar el Smartphone para que se bloquee automáticamente pasados unos minutos de inactividad.
- Antes de instalar una nueva aplicación revisar su reputación. Sólo instalar aplicaciones que provengan de fuentes de confianza.
- Prestar atención a los permisos solicitados por las aplicaciones y servicios a instalar.
- Mantener el software actualizado, tanto el Sistema Operativo como las aplicaciones.
- Deshabilitar características de conectividad mientras no se usen: Bluetooth, infrarrojos o Wi-fi.
- Configurar Bluetooth como oculto y con necesidad de contraseña.
- Realizar copias de seguridad periódicas.
- Cifrar la información sensible cuando sea posible.
- Utilizar software de cifrado para llamadas y SMS.
- Siempre que sea posible, no almacenar información sensible en el Smartphone, asegurándose también que no se *cachea* en local.
- Al deshacerse del Smartphone, borrar toda la información contenida en el Smartphone.
- En caso de robo o pérdida del Smartphone, informar al proveedor de servicios aportando el IMEI del dispositivo para proceder a su bloqueo.
- En determinados casos pueden utilizarse opciones de borrado remoto o automático (después de varios intentos de acceso fallidos).

- Monitorizar el uso de recursos en el Smartphone para detectar anomalías.
- Revisar facturas para detectar posibles usos fraudulentos.
- Mantener una actitud de concienciación en el correcto uso de estos dispositivos y los riesgos asociados.
- Extremar la precaución al abrir un correo, un adjunto de un SMS o hacer click en un enlace.
- Desconfiar de los archivos, enlaces o números que vengan en correos o SMS no solicitados.
- Evitar el uso de redes Wi-fi que no ofrezcan confianza.
- Tener en cuenta este tipo de dispositivos en su política de seguridad corporativa.

BIBLIOGRAFIA

- Informe S21sec e-crime Malware en Smartphones.
- Informe Gartner: http://www.gartner.com/it/page.jsp?id=1434613
- Datos estadísticos obtenidos desde www.quancast.com
- http://www.hispasec.com/laboratorio/troyano_android.pdf
- http://www.hispasec.com/laboratorio/Troyano_android_tab_snake.pdf
- http://developer.android.com/sdk/ndk/index.html
- http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf
- http://www.enisa.europa.eu/act/it/oar/smartphones-information-security-risks-opportunities-and-recommendations-for-users
- http://nakedsecurity.sophos.com/2010/12/31/geinimi-android-trojan-horse-discovered/
- http://itknowledgeexchange.techtarget.com/security-bytes/google-android-trojan-surfaces-in-china/
- http://blog.mylookout.com/_media/Geinimi_Trojan_Teardown.pdf