MALWARE Y DISPOSITIVOS MÓVILES

El teléfono móvil es uno de los dispositivos electrónicos de mayor uso actualmente. Los terminales que, en un principio, estaban destinados a mantener a dos personas comunicadas mediante voz, han añadido paulatinamente más y más funcionalidades extra. Tal es la cantidad de posibilidades y funciones que ofrece un teléfono móvil hoy en día que se ha acuñado un nuevo término para denominar a estos dispositivos: *smartphones* o teléfonos inteligentes.

Recientemente han aparecido otros *gadgets*[1] tecnológicos que ofrecen (en un tamaño algo mayor) las mismas posibilidades que los últimos teléfonos móviles, pero sin la posibilidad de realizar llamadas, por ahora. Se sitúan entre el teléfono móvil y los *netbooks*[2] y se les ha llamado *tablets* o tabletas electrónicas.

Los *smartphones* y *tablets* han incorporado la complejidad del ordenador de uso personal, con las ventajas que esto conlleva. Sin embargo, este avance ha tenido como consecuencia efectos colaterales menos deseables, como son los problemas de seguridad y la creación de malware específico. La aparición de este tipo de código malicioso, entre otros factores, ha sido propiciada por la gran cantidad de datos personales y de valor que se almacenan en los teléfonos y *tablets,* constituyendo un valioso botín para los atacantes.

I ¿Qué objetivo interesa en un dispositivo móvil?

Una de las principales razones por las que los creadores de malware han decidido ampliar su rango de acción a los dispositivos móviles, es la gran cantidad de información de valor almacenada en ellos y el hecho de que, cada vez con mayor frecuencia, se realicen operaciones de navegación a través de ellos.

Veamos cuáles son los principales objetivos que se encuentran en el punto de mira de los creadores de software malicioso para dispositivos móviles.

Nombres de usuarios y contraseñas

Actualmente, el acceso a la mayoría de funcionalidades en la red requiere de un usuario y una contraseña. Estos sitios suelen poseer información personal que no está disponible públicamente, sino que pertenece exclusivamente al usuario (correos, datos personales, información confidencial, etc.). La obtención de ambos valores (identificador del usuario y

[1] Dispositivo con un propósito y función específicos, generalmente de pequeñas proporciones, práctico e innovador. Suelen tener un diseño más ingenioso que el de la tecnología corriente.

[2] Ordenador portátil de reducidas dimensiones.

su contraseña) permitiría suplantar la identidad de la persona a la que le han sido sustraído los datos. También permitiría a un atacante obtener acceso a otros datos de índole personal.

Respecto a las contraseñas utilizadas para la banca online, no es un dato que se suela almacenar como tal en un dispositivo móvil, pero últimamente algunas entidades bancarias han comenzado a enviar SMS con contraseñas temporales (habitualmente de un solo uso) para el acceso a ciertos servicios. Ante esta medida de seguridad, troyanos como el conocido Zeus han hecho su aparición en diversas plataformas, entre ellas Blackberry, donde intercepta los SMS con las claves enviadas por la entidad bancaria[3].

Otras formas en las que podrían ser utilizadas unas credenciales robadas no afectan de forma tan directa al usuario atacado. A veces, quienes están detrás del robo de las credenciales, simplemente desean hacer llegar publicidad personalizada o utilizar la cuenta para realizar engaños más creíbles, por ejemplo enviando desde esa cuenta mensajes a todos los contactos con enlaces a sitios web maliciosos.

Actualmente, en los *smartphones* y *tablets* se puede llegar a almacenar la misma cantidad de contraseñas que en un ordenador de sobremesa. En concreto, es común guardar las credenciales de servicios de redes sociales (Facebook, Tuenti, Twitter, etc.) o de comunicación instantánea (WhatsApp, Skype, Messenger, etc.).

Datos de formularios

Otros puntos desde donde se podrían obtener datos personales de interés son todos los formularios de las webs a las que se suele acceder desde estos dispositivos. Los formularios más deseados por los atacantes son los relativos a compras online, en los que se introducen los datos cuya obtención puede traducirse rápidamente en beneficios económicos, como son los referentes a tarjetas de crédito.

El aumento de la utilización de la banca online a través de dispositivos móviles, gracias a que desde las mismas entidades se facilita el acceso adaptando sus webs o desarrollando aplicaciones para gestionarlo, es otro de los principales factores que está atrayendo el diseño de malware para estas plataformas.

Datos y documentos privados

Aparte de los datos personales específicos, también tiene gran interés la obtención de documentos que sólo se encuentran disponibles en ciertos círculos cerrados. En este sentido podría incluirse el espionaje industrial y el robo de documentos de ámbito

[3] ZeuS Mitmo: Man-in-the-mobile: http://securityblog.s21sec.com/2010/09/zeus-mitmo-man-in-mobile-i.html

personal. Concretamente, el atacante que busque este tipo de información se centrará principalmente en fotografías, correos electrónicos y mensajes SMS o MMS.

La comodidad y facilidad que propicia la utilización de tabletas electrónicas para la lectura de todo tipo de documentos de texto o visualización de imágenes, diagramas, etc., también propicia el almacenamiento de estos archivos en el aparato. Debido a la movilidad y funcionalidad que proporcionan, han resultado ser muy populares en entornos empresariales.

Ya se han conocido casos de personajes famosos que han sido víctimas de estos ataques, a los que les fueron sustraídos datos personales, fotos comprometidas o información relevante. En algunos casos se puede llegar a pedir un rescate por estos datos.

Mensajes premium

No siempre el objetivo del malware es generar un beneficio gracias a la obtención de datos o contraseñas que más tarde puedan ser utilizadas. Existe una vía más rápida de lucrarse gracias a la infección de un dispositivo móvil, y su único requerimiento es que éste posea la capacidad de enviar mensajes de texto. Existe malware para móviles inteligentes que se encarga de dar las órdenes pertinentes al teléfono para enviar mensajes a números premium[4]. Los mensajes enviados inadvertidamente por el teléfono al número (que es propiedad del atacante o se encuentran asociados), generan una comisión de la que obtiene un beneficio directo.

Un caso de este popular malware que afecta concretamente a dispositivos Android es la familia Android.Pjapps. Los usuarios suelen percatarse del problema cuando reciben mensajes SMS no solicitados, por los que se les cobra una cantidad, o cuando reciben una factura que no corresponde con la realidad de uso.

Otra variedad de ataque similar consiste en instar al usuario a realizar una llamada o a enviar un mensaje a este tipo de teléfonos. La principal vía para realizar este ataque suele ser a través de SMS en el que se promete un premio o recompensa por el envío de mensajes. Este caso no implica infección, sino ingeniería social.

Secuestro del dispositivo

Los terminales permiten, a través de diferentes métodos, bloquear el sistema para que no pueda ser utilizado si no se conoce un código en concreto. También es posible deshabilitar las llamadas o no permitir el acceso a los datos almacenados mediante el cifrado.

[4] Números de tarificación especial que ofrecen servicios de notificación y envío de SMS a un precio superior al habitual.

Existe malware para móviles que bloquea el acceso a los datos o a ciertas funcionalidades, pidiendo un rescate para recuperar el estado original del dispositivo. Son técnicas ya utilizadas con éxito en los ordenadores de sobremesa. Este tipo de malware es conocido como "*ransomware*".

II Otros objetivos del malware

Además del robo de información y la búsqueda de ganancias económicas, existen otras posibles motivaciones para los ataques e infecciones de dispositivos móviles.

Demostración de capacidad

Aunque la gran mayoría del malware que actualmente se crea y se encuentra en circulación tiene como objetivo la búsqueda de un beneficio económico (directo o indirecto), todavía es posible encontrar código malicioso que se centra principalmente en la demostración de poder del creador. Inicialmente, este tipo de malware se realiza con el fin de poner a prueba los conocimientos y destreza de quien lo genera.

Este fue el origen de las primeras muestras de malware que hicieron su aparición hace unos 30 años, cuyo único objetivo era la búsqueda de la fama y la demostración las habilidades de los creadores antes el resto de la comunidad. En un entorno relativamente inexplorado, como es todavía el de los *smartphones*, aún es habitual encontrar pruebas de concepto y experimentos. En algunos casos estos experimentos se utilizan para desarrollar en el futuro código más efectivo.

Botnets

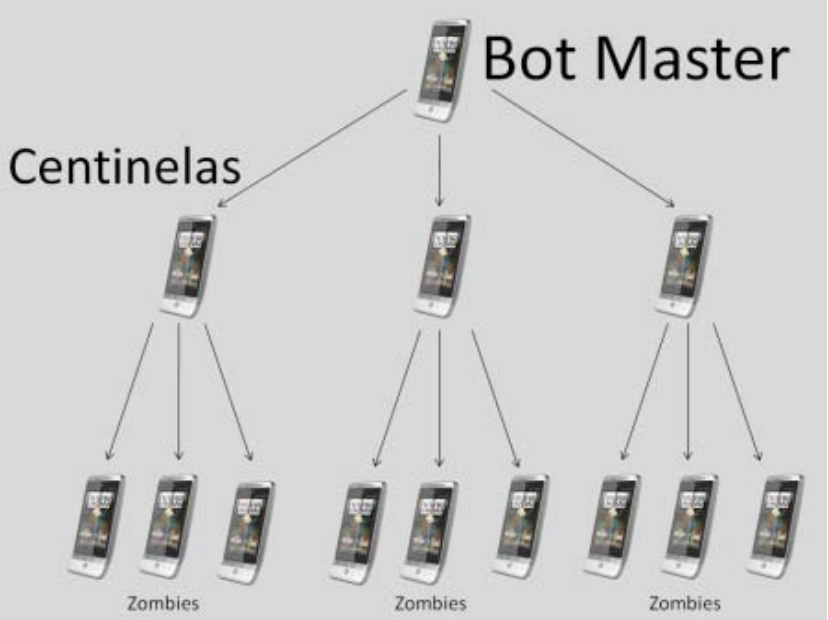
Las llamadas botnets son redes formadas por un gran número de equipos infectados, también conocidos como *zombis*. Estos dispositivos se encuentran controlados por un programa malicioso, que permite que puedan ser manejados de forma remota por una máquina central, encargada de monitorizar a todo el conjunto y de darles las órdenes para las que estén programados. También se utilizan como granja de sistemas que permite obtener mayor potencia de cómputo y así poder enviar correo basura o realizar ataques de denegación de servicio (bloqueo) de páginas web por saturación.

Las botnets son habituales en el mundo de los sistemas de sobremesa y actualmente están comenzando a despuntar entre los teléfonos inteligentes.

Uno de los ejemplos más sonados de este tipo de infección en dispositivos móviles es el del troyano conocido como Geimini. Este troyano se instala a través de aplicaciones legítimas a las que se les añadía el código malicioso de este troyano. Entre sus funcionalidades se encuentran desde el envío de información sobre el hardware (tipo CPU, marca, etc.) y datos como número de teléfono, datos de la red, IMEI, etc. hasta

poder recibir órdenes de servidores orientados al control de la red de dispositivos infectados.

Ilustración 1: Estructura jerárquica de botnets



Fuente: Eset.com

III Formas de infección

En este apartado se destacan algunos de los puntos de infección comúnmente utilizados por los atacantes en la actualidad.

Redes sociales

Una de las formas más usadas para obtener datos personales o comprometer una cuenta es a través de falsas funcionalidades añadidas a una red social. Habitualmente las redes sociales ofrecen juegos y aplicaciones adicionales. Los atacantes suelen crear aplicaciones falsas que incitan al usuario a su instalación y por tanto, llevan a la infección del teléfono o dispositivo móvil.

Otra variante de este tipo de ataques son los sitios web externos a las redes sociales que ofrecen supuestas funcionalidades extra. Los principales engaños y trampas utilizadas para atraer al público suelen ser aplicaciones que aseguran permitir conocer qué personas visitan un perfil o quién ha bloqueado una cuenta en los sistemas de mensajería. Este tipo de aplicaciones no existen y no cumplen realmente la función que prometen.

Dichos sitios fraudulentos suelen requerir la introducción de los datos personales necesarios para acceder a la cuenta. Así, estas aplicaciones, además de no cumplir su función, infectarán el sistema y obtendrán datos personales.

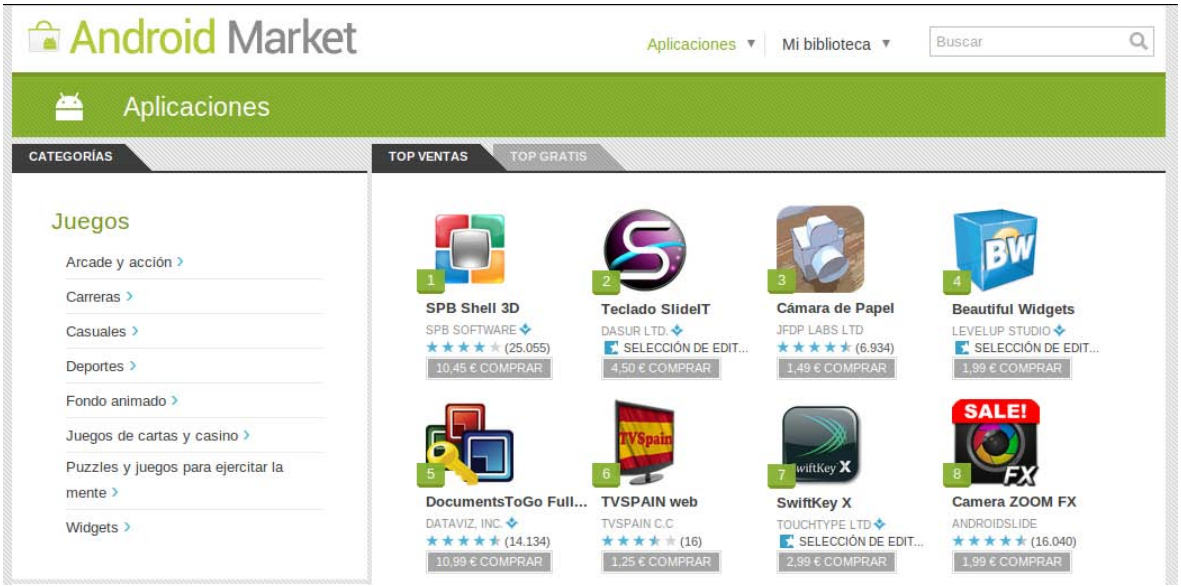
Correo electrónico

El correo es uno de los medios tradicionales de infección en dispositivos electrónicos y esto se ha trasladado a los terminales móviles. Al igual que en el caso de los sistemas de sobremesa, los atacantes envían al correo programas camuflados, incitando al usuario a que los ejecute en su terminal. Con esto consiguen infectar el sistema, haciendo creer al usuario que ha instalado una aplicación.

Tiendas de aplicaciones

Actualmente las principales plataformas de terminales poseen una tienda oficial de aplicaciones, también conocidas como *stores* o *markets*. En ellas se pueden encontrar gran cantidad de programas clasificados según su categoría, con valoraciones y comentarios de los usuarios que enriquecen la experiencia con el dispositivo.

Ilustración 2: Ejemplo de tienda de aplicaciones



Fuente: Android Market

Cada tienda virtual sigue su propia política para controlar las aplicaciones que se ponen a disposición del público, siendo algunas más restrictivas que otras. Esto quiere decir que las aplicaciones son sometidas a controles más o menos rigurosos para detectar malware o comportamientos sospechosos en ellas antes de que puedan ser descargadas por el público. Aun con estos controles, se han dado casos en los que las tiendas oficiales han

alojado aplicaciones infectadas. El usuario deberá tomar las máximas precauciones a la hora de instalar cualquier software, aunque provenga de una tienda oficial.

Actualmente existen dos modelos de políticas diferentes en cuanto a la supervisión de las aplicaciones en estas tiendas. El primero es el de las tiendas que poseen una política de control de las aplicaciones que requiere que todas sean revisadas por la propia empresa. En el otro extremo, se encuentra el modelo de tienda en el que cualquier desarrollador puede poner a disposición de la comunidad una aplicación creada por él mismo, sin que esto implique una supervisión previa y rigurosa de dichas aplicaciones. Este segundo modelo suele cubrir su déficit de supervisión oficial mediante la colaboración de algunos usuarios, que comprueban extraoficialmente algunas aplicaciones reportando los posibles problemas que encuentran.

También es posible encontrar "tiendas alternativas" que ofrecen aplicaciones para estos dispositivos sin estar vinculadas a las empresas y marcas que desarrollan los sistemas operativos. En este caso las aplicaciones no necesariamente han de pasar por un control o supervisión de seguridad.

Por otro lado, existe una gran cantidad de aplicaciones disponibles en Internet Pueden encontrarse tanto en páginas web dedicadas exclusivamente a ello como en foros sobre diversos temas entre los que se pueden incluir este tipo de aplicaciones. En estos casos no existe ningún aval de supervisión o control oficial.

Tanto en el caso de tiendas con un nivel de control elevado, como en las tiendas que no cuentan con ningún tipo de control se puede encontrar alguna aplicación con fines maliciosos.

Redes locales (WiFi)

Actualmente, la gran mayoría de los dispositivos móviles inteligentes posee la capacidad de conectarse a Internet. Esto suele hacerse mediante una conexión directa de datos (GPRS o 3G) a través de las redes de un operador móvil o mediante la conexión a una red de área local que proporciona acceso a Internet (Wi-Fi).

En este último tipo de redes, un dispositivo que se encuentre infectado podría iniciar una búsqueda de otros objetivos en la misma red local, con la intención de infectarlos.

Ilustración 3: Visor de redes Wi-Fi disponibles

Fuente: esferaiphone.com

Otro peligro al que se enfrentan los dispositivos móviles que se conectan a redes Wi-Fi es la fiabilidad de la conexión. Una red Wi-Fi no protegida puede permitir a atacantes conectados a la misma red la obtención del tráfico no cifrado generado por el dispositivo (los datos que circulan por la red).

Bluetooth

Otra tecnología ampliamente extendida es la conocida como *bluetooth*. Se trata de un protocolo, orientado principalmente al intercambio de datos entre dos dispositivos, muy popular antes de que se extendiera el uso de Wi-Fi e Internet en los terminales móviles.

Un móvil infectado podría iniciar una búsqueda de otros dispositivos con el sistema *bluetooth* activado. Si la nueva víctima acepta la conexión, el infectado podría enviar el código que se ejecutaría en el dispositivo. Algunas empresas también utilizan este método para enviar publicidad no solicitada a través de *bluetooth* a los aparatos que lo tienen activo en un radio de acción de unos 100 metros. Un malware aparecido en 2006 llamado *Commwarrior*, destinado esta vez a Symbian, aprovechaba, entre otras, las comunicaciones *bluetooth* como medio de propagación.

Vulnerabilidades

Los *smartphones* utilizan software complejo y por tanto, no están exentos de contener vulnerabilidades. Estos fallos en los programas permitirían a los atacantes ejecutar código en el sistema, por ejemplo con solo visitar una página web si el programa vulnerable es el navegador.

Las vulnerabilidades explotadas a través de páginas web cargan un contenido especialmente preparado para que ocurra el fallo y se aproveche la vulnerabilidad al ser procesado. Este tipo de vulnerabilidades pueden tener diferentes repercusiones, desde hacer que el programa o el dispositivo entero deje de funcionar, hasta que el navegador pueda ejecutar código y tomar el control del aparato.

Uno de los ejemplos más conocidos y ampliamente utilizados, en principio no destinado a la infección, es el método utilizado para "liberar" (eliminar las limitaciones establecidas por su fabricante) los dispositivos que utilizan el sistema operativo iOS, entre otros. Lo que permite realizar esta liberación es precisamente aprovechar diferentes vulnerabilidades del software original.

IV Protección

Al igual que en el campo de los sistemas de sobremesa, se deben seguir cuatro normas básicas que sirven para proteger cualquier dispositivo informático:

- **Mantener el dispositivo actualizado** con las últimas versiones del sistema operativo y del software instalado.
- **Hacer uso de diferentes perfiles de usuario** cuando sea posible. Se debe usar aquel que tenga los privilegios mínimos necesarios para la utilización el sistema en lugar de un perfil de administrador con todos los permisos.
- **No instalar software de repositorios no oficiales** o de dudosa procedencia.
- **Instalar un sistema antimalware** en caso de que exista.

Otros consejos orientados a la protección frente a diversas formas de engaño y vectores de entrada de malware podrían ser:

- Establecer una contraseña tanto para el encendido como para el desbloqueo del terminal. También es necesario modificar todas las claves que estén establecidas por defecto para personalizarlas. Así se evitarían casos como el de ciertos modelos de dispositivos liberados, en los que todos comparten una misma contraseña por defecto.

- Al conectarse a una red Wi-Fi ajena, evitar el envío de datos personales y el uso de la banca online.

- Comprobar el origen y la confianza de cualquier tipo de contenido (ejecutables, documentos...) que vaya a ser descargado, instalado o abierto con cualquier programa. En caso de tratarse de software, comprobar que las aplicaciones se encuentren firmadas por su fabricante original.

- No aceptar ni hacer caso de mensajes de correo electrónico, SMS, MMS, etc. de origen desconocido y comprobar la autenticidad de con los mensajes provenientes de contactos de confianza pero cuyo contenido se salga de la normalidad. No visitar desde el dispositivo los enlaces a páginas que sean propuestos a través de mensajes, correo, mensajería instantánea, etc.

- Configurar el navegador y gestor de correo para que el contenido de los correos electrónicos no sea cargado por defecto, ni se visualice en modo HTML. Deshabilitar la carga de contenido externo a la hora de la previsualización y lectura de correos electrónicos.

Ilustración 4: Opciones de visualización del correo electrónico

Fuente: INTECO

- No aceptar conexiones ni transferencias no solicitadas o de origen desconocido vía *bluetooth* o infrarrojos.

- Mantener todos los datos sensibles protegidos frente a accesos no permitidos mediante el cifrado.
- Realizar periódicamente una copia de seguridad del sistema y todos sus datos para poder recuperarlos en caso de pérdida o avería del dispositivo.
- Conservar el código IMEI del teléfono móvil para que, en caso de pérdida o robo del terminal, éste pueda ser bloqueado.


www.facebook.com/ObservaINTECO


www.twitter.com/ObservaINTECO

www.inteco.es/blog/Seguridad/Observatorio/BlogSeguridad

www.youtube.com/ObservaINTECO


www.scribd.com/ObservaINTECO


www.slideshare.net/ObservaINTECO


observatorio@inteco.es