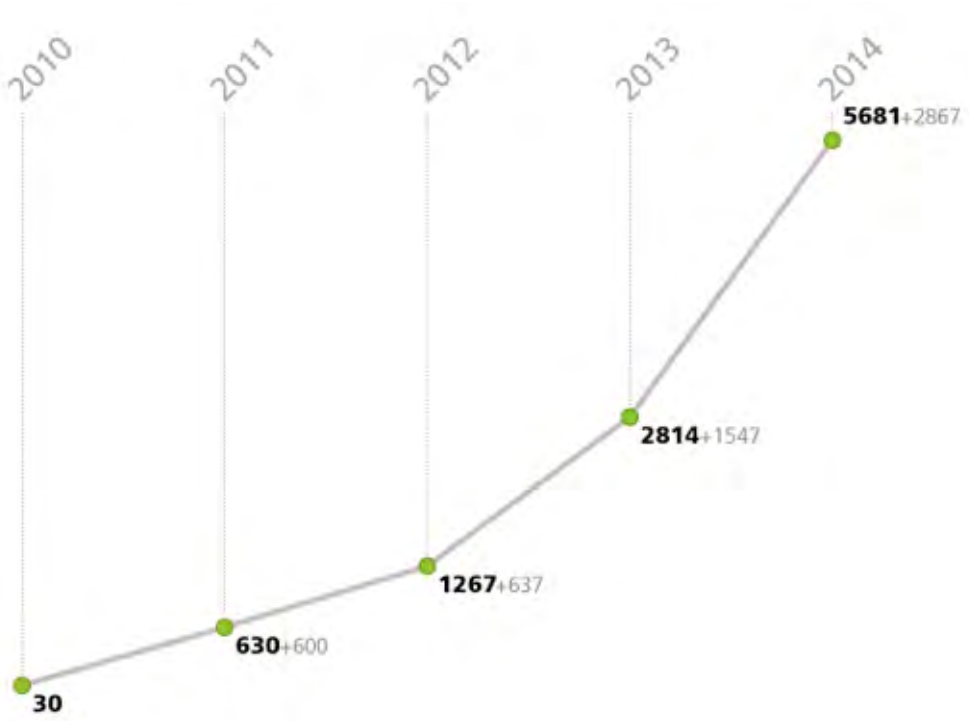
Robos a través de móviles

Android es el sistema más usado entre los usuarios de dispositivos móviles y el segundo más usado después de Windows para los creadores de virus. Los primeros programas malintencionados para Android aparecieron en el año 2010.

La mayor parte de los programas malintencionados se crean para infectar los dispositivos móviles bajo la administración de Android – por causa de la "amplia" difusión de este SO y su código abierto, así como la posibilidad de instalar aplicaciones obtenidas de cualquier fuente.

Este gráfico demuestra el crecimiento del número de entradas de programas malintencionados para el SO Android en la base de virus Dr.Web



¡Crecimiento del número de entradas en el año 2014 — 102%!

¡A partir del año 2010, el número de entradas aumentó 189 veces!

Al día de 1 de abril del año 2015 el número de firmas añadidas a la base Dr.Web para detectar los programas malintencionados para Android alcanzó casi 9 mil.

Es decir, solo en los tres primeros meses del año 2015 la base aumentó más de un 50%!

Asimismo, hay que entender que usando una sola firma, Dr.Web puede determinar mucho más de un programa malintencionado.

La mayoría de los programas malintencionados para Android se crean para ROBAR.

Los dispositivos móviles tienen amplia funcionalidad, y los creadores de los troyanos para Android roban todo lo que se puede robar desde un dispositivo móvil:

- Dinero — desde una cuenta móvil, sistemas de pagos en línea y tarjetas bancarias
- Nombres de usuario y contraseñas — para sistemas de banca en línea y de pagos electrónicos, cuentas en las redes sociales etc.
- SMS
- Llamadas
- Mensajes de correo electrónico
- Fotos — usando las mismas, se puede chantajear a la víctima o hacerle un daño moral al publicar las fotos en Internet
- Grabaciones de conversaciones del titular del dispositivo móvil — incluso si el mismo no las realizó, un troyano puede hacer en vez de él
- Direcciones de la libreta de contactos
- Coordenadas del dispositivo — es decir, la ubicación del titular del mismo y los datos sobre su movimiento
- Cualquier tipo de información técnica sobre el dispositivo (identificadores IMEI/IMSI/SID, número del dispositivo móvil, versión del SO, versión del sistema SDK, modelo del dispositivo, los datos sobre el fabricante del dispositivo)

¡En muchos casos los usuarios mismos descargan e instalan en dispositivos móviles los programas malintencionados!

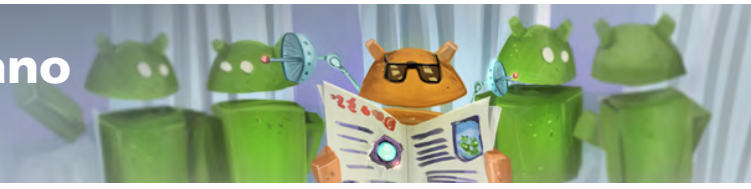
Así, por ejemplo, Android.Plankton, capaz de recabar y transmitir la información sobre un dispositivo infectado, fue descargado manualmente por los usuarios 150 000 veces (!) desde el sitio web oficial de Android Market (nombre antiguo de Google Play), antes de ser eliminado por la administración del portal.

Según las estadísticas de Dr.Web para Android, un 50% de nuestros usuarios tienen activada en su dispositivo una opción de instalación de aplicaciones desde fuentes desconocidas (es decir, no desde el ecosistema Google Play). Quiere decir que los usuarios mismos pueden instalar las aplicaciones malintencionadas descargadas de un foro o desde otro sitio web sospechoso.

Los métodos de la ingeniería social les permiten a los ciberdelincuentes difundir ampliamente los troyanos entre usuarios. Por ejemplo, más de **30 mil** de titulares de dispositivos Android de Corea del Sur descargaron el troyano bancario **Android.SmsBot.75.origin al intentar saber qué fue de un «mensaje de correo».**

La mayoría de los usuarios están convencidos de que siempre notarán la acción de un troyano en el dispositivo móvil.

Un buen troyano es un troyano que no notan los usuarios.



Los creadores de virus ya lo saben hace mucho.

La acción de los troyanos que funcionan con más éxito y se dedican a robar, en la mayoría de los casos puede ser descubierta solo al haberlo robado todo.

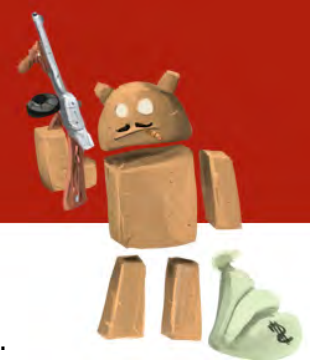
- Por ejemplo, un troyano-dialer Android.Dialer.7.origin, para disminuir la probabilidad de detección de su actividad no deseada por el usuario, desactiva el altavoz del móvil por el periodo de la «conversación por móvil» iniciada por el mismo, y para ocultar completamente la actividad malintencionada, elimina del registro del sistema, así como del listado de llamadas realizadas toda la información que le pueda comprometer.
- Los troyanos que roban dinero desde la cuenta de un dispositivo móvil por medio de suscribir al usuario a cualquier servicio de pago, también se

ocultan con mucho éxito en el dispositivo de la víctima. Normalmente un servicio de pago envía un SMS de confirmación en caso de finalizar una operación correctamente — los troyanos ocultan estos SMS, para que el usuario no lo note antes de lo debido. Algunos programas malintencionados pueden enviar automáticamente los SMS con un código de confirmación para la autorización en los servicios de pago — estos mensajes también se interceptan y se roban con mucha frecuencia.

- Muchos troyanos "avanzados" se difunden como programas legales, y, una vez iniciados, eliminan su ícono y luego funcionan sin que el usuario lo note.
- Existen troyanos que los malintencionados meten dentro del sistema operativo o incorporan en las imágenes de firmware difundidas. Estos "partisanos" tienen permisos avanzados y son capaces de realizar una amplia gama de acciones no deseadas sin que alguien lo note.
- Para no ser detectados por los programas antivirus, algunos troyanos tienen una función para afrontar el software de protección similar: pueden bloquear los antivirus y hasta eliminarlos completamente desde un dispositivo.

Troyanos bankers

Son familias de troyanos Android creados para robar los medios desde tarjetas bancarias y desde sistemas de pagos en línea.



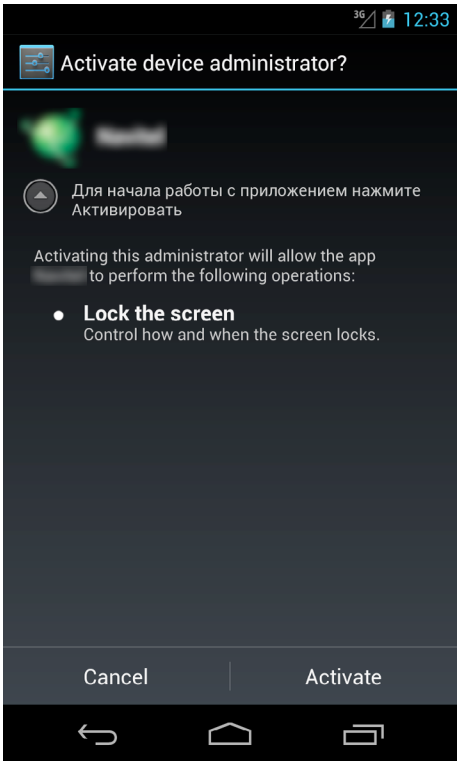
La banca móvil realmente es cómoda. Muchos bancos ofrecen a sus usuarios las versiones Android de aplicaciones para la banca en línea. Las mismas se usan no solamente para operaciones personales, sino también para los pagos corporativos. Normalmente los directivos más importantes de la empresa que tengas acceso a la cuenta usan esta posibilidad.

El robo del dinero de usuarios es el vector más impor–tante de ataques de los creadores de virus.

Android.BankBot.33.origin

Es capaz de:

- Obtener la información sobre el saldo actual de la cuenta bancaria y el listado de tarjetas bancarias conectadas al móvil del usuario;
- Robar los datos de autenticación de la cuenta de banca en línea por medio de descargar en el navegador del dispositivo infectado de un sitio web malintencionado que imita el aspecto de un verdadero portal de Internet, donde se le ofrece a la víctima que introduzca su información confidencial para entrar;
- realizar operaciones ilegales con el dinero de las víctimas, transfiriéndolo a la cuenta que pertenece a los malintencionados.



La víctima puede no enterarse del robo durante un rato,porque Android.BankBot.33.origin es capaz de interceptar y bloquear las notificaciones por SMS sobre las operaciones realizadas.

Los usuarios MISMOS instalan este troyano (¡para realizarlo, en la configuración del sistema debe estar permitida la instalación de programas de fuentes de terceros!)

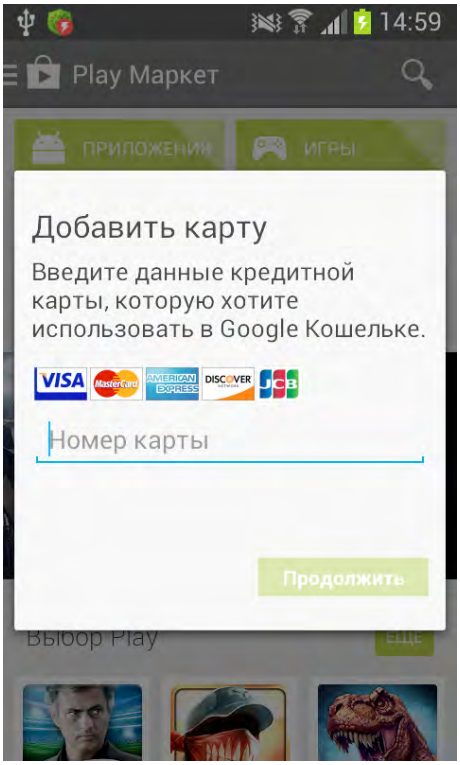
De enero a abril de 2015, este programa troyano fue detectado en dispositivos de usuarios del Antivirus Dr.Web para Android 62 840 veces, es decir, un 0,37% del número total de amenazas detectadas en este periodo.

Android.SpyEye.1

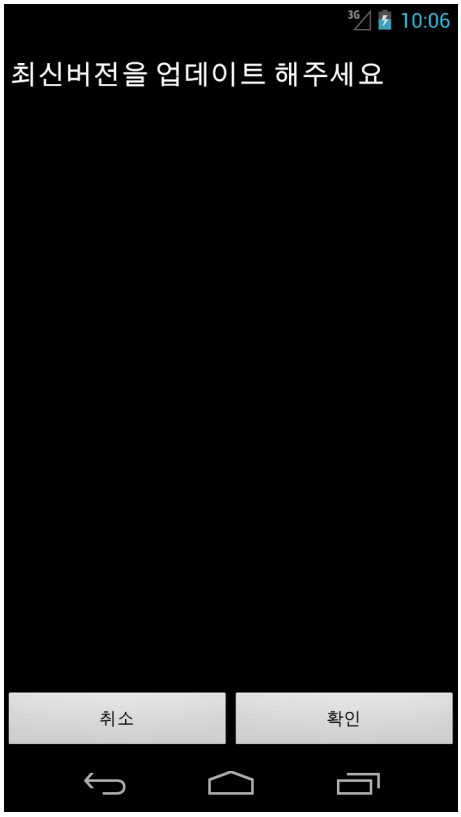
Si un usuario del equipo de escritorio o del portátil visita un sitio web bancario la dirección de la cual está en el archivo de configuración del troyano bancario que infectó su equipo, en la página web consultada se inyecta un texto ajeno o un formulario web para introducir los datos de acceso a la cuenta. La víctima sin enterarse de nada abre en el navegador la página web del banco donde tiene abierta la cuenta y ve un mensaje diciendo que el banco empezó a usar las nuevas medidas de seguridad, sin cumplir con las cuales el usuario no podrá obtener acceso al sistema «Banca-Cliente», así como la propuesta de descargar en el móvil la actualización del cliente móvil que contiene un programa troyano. Este programa es capaz de interceptar y reenviar a los malintencionados las contraseñas válidas solo una vez enviadas por SMS, necesarias para acceder al sistema «Banca-Cliente».

Android.BankBot.21.origin

Para obtener los requisitos bancarios de la tarjeta bancaria usada y robar dinero, Android.Bank-Bot.21.origin comprueba si está activa la ventana de la aplicación Google Play en el dispositivo móvil y, si es así, imita el formulario estándar de conexión de la tarjeta a la cuenta del usuario. La información introducida por la víctima se transmite al servidor de los malintencionados. Luego se roba el dinero usando las tecnologías.



Android.BankBot.29.origin



El troyano intenta obtener los derechos del administrador del dispositivo móvil— «oculta» del usuario la solicitud del sistema correspondiente usando su propia ventana de diálogo, y, como resultado, la víctima potencial con alta probabilidad puede proporcionarle a la aplicación malintencionada los permisos necesarios. Luego se roba el dinero usando las tecnologías.

Robo de SMS entrantes

Vd. dirá: no es nada grave si se roba un SMS. Pero todo depende de la causa por la que a su móvil fue enviado un SMS robado por los malintencionados.

¿Qué SMS entrantes, la pérdida de los cuales puede causar daños financieros, roban los troyanos?

- SMS que confirman o solicitan permiso para conectarse a servicios Premium o del contenido de móviles. Se roban para que la víctima no se entere de la suscripción a estos servicios mucho rato y no haga nada para bloquear la actividad del troyano.
- SMS con mensajes de sistemas Banca-Cliente que contienen los códigos de comprobación mTAN.

Los SMS robados se reenvían al servidor que administra el troyano y pertenece a los malintencionados. Esta funcionalidad existe en los troyanos de varias familias.

Pérdida de dinero por medio de envío de SMS entrantes

Por ejemplo, los troyanos de la familia Android. SmsSend sacan el dinero de la cuenta móvil a favor de los delincuentes por medio de enviar SMS caros desde el móvil de la víctima.

Según las estadísticas obtenidas usando Dr.Web para Android, el número de detecciones de los troyanos de la familia Android.SmsSend fue 20 223 854 en el año 2014.

Los troyanos de la familia **Android.SmsBot** también pueden enviar, interceptar y borrar los SMS.

Según las estadísticas obtenidas usando Dr.Web para Android, el número de detecciones de los troyanos de la familia Android.SmsBot fue 5 985 063 en el año 2014.

Robo del dinero por medio de llamar a los números premium

Los dialers es una familia de troyanos Android que llaman a los números Premium sin que el dueño del móvil lo sepa. Este modo de «ganar dinero» también lo usan mucho los creadores de virus.

Según las estadísticas obtenidas usando Dr.Web para Android, el número de detecciones de los troyanos de la familia Android.Dialer fue 177 397 en el año 2014.

Robo de direcciones de contactos

Aunque el problema parece ser muy poco grave, también es un negocio. Se puede vender cualquier contacto activo, y hay varias categorías de clientes para comprarlo.

1. Spammers. La actividad de los spammers es un negocio que funciona con éxito. Y no son solo envíos de spam de publicidad que no dañan mucho.

El envнo masivo de los SMS que contienen un enlace para descargar el programa malintencionado llega a ser un mйtodo cada vez mбs usado de difusiyn de las amenazas Android de hoy.

Por ejemplo, Android.Wormle.1.origin puede difundirse usando los SMS entre todos los conocidos del dueño del dispositivo. Hasta finales de noviembre del año,Android.Wormle.1.origin infectó más de 15 000 dispositivos móviles de Android de ciudadanos de unos 30 países.

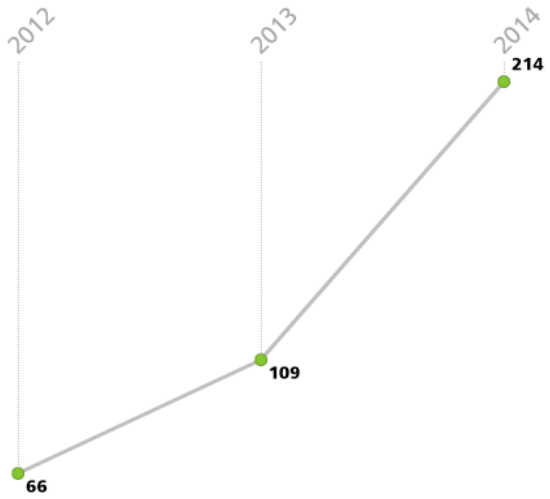
2. Phishers. Recaban los contactos para enviar los mensajes de phishing con supuestos enlaces a los sitios web de bancos o sistemas de pago. Si Vd. va a este sitio web, un phisher puede obtener sus datos de autenticación para entrar en el sistema de banca en línea o los datos de la tarjeta bancaria. Asimismo, Vd. mismo se le proporcionará estos datos, al haber introducido los datos necesarios en el formulario ofrecido por el phisher, pensando que es el sitio web del banco.

3. Organizadores de ataques DDoS — necesitan los contactos de los dueños de dispositivos móviles que pueden ser infectados y usados para organizar los ataques DDoS, por ejemplo, para un competidor no deseado de un cliente.

4. Espías (servicios especiales, competidores). Cualquier contacto sirve para un espía o un chantajista. Además, la gente que le está vigilando puede leer su correo, grabar sus conversaciones, descargar sus fotos al servidor remoto.

Por ejemplo, Android.Spy.130.origin transmite a los malintencionados la información sobre la mensajería SMS, las llamadas realizadas, las coordenadas GPS actuales, y asimismo es capaz de llamar al número requerido sin que nadie lo note, convirtiendo el Smartphone o la tableta infectada en un dispositivo de escucha.

Gráfico de crecimiento del número de entradas de troyanos de la familia Android. Spy en la base de virus Dr.Web



Vd. usa activamente los servicios

- Google Play
- Google Play Music
- Gmail
- WhatsApp
- Viber
- Instagram
- Skype
- «VKontakte»
- «Odnoklassniki»
- Facebook
- Twitter...?

A los malhechores les servirán los datos que Vd. almacena allí — ¡para la venta o el chantaje!

Dr.Web para Android protege contra el robo a través de móviles

Componentes de protección de Dr.Web para Android

Antivirus
Protegerá contra los troyanos y otros programas malintencionados

Antirrobo
Ayudará a encontrar un dispo
sitivo móvil en caso de pérdida o del robo del mismo y en caso necesario borrar la información confidencial del mismo de forma remota

Antispam
Protegerá contra las llamadas y mensajes SMS no deseados

Filtro URL de la nube
Restringirá el acceso a los recursos de Internet no deseados sin distinción del estado de las bases de virus en su Dr.Web para Android

Firewall
Controlará la actividad de las aplicaciones en la red

Auditor de seguridad
Realizará el diagnóstico, detectará los problemas de seguridad y ofrecerá soluciones para resolverlos

Enlaces útiles

Proyecto informativo «Robos a través de móviles»