Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1213

(09/2017)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad en el ciberespacio – Ciberseguridad

Capacidades de seguridad necesarias para luchar contra las redes robot en teléfonos inteligentes

Recomendación UIT-T X.1213

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	**X.1200–X.1229**
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistema de transporte inteligente (ITS)	X.1370–X.1379
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1213

Capacidades de seguridad necesarias para luchar contra las redes robot en teléfonos inteligentes

Resumen

En la Recomendación UIT-T X.1213 se analizan el origen y las amenazas de seguridad que pueden plantear las redes robot en teléfonos móviles y se exponen las capacidades de seguridad necesarias para luchar contra ellas.

Estudios de organizaciones de todo el mundo muestran que el rápido desarrollo de los dispositivos de Internet móvil y la extendida utilización de teléfonos inteligentes han hecho que las redes robot, que anteriormente afectaban casi únicamente a las redes informáticas, estén extendiéndose rápidamente por los teléfonos móviles. En la actualidad, las diferencias de condiciones y ecosistemas entre países y regiones hacen que haya diversos niveles de restricción a la propagación de redes robot en teléfonos inteligentes. En los informes analíticos de diversas empresas de seguridad y organizaciones de investigación se constatan notables diferencias en los datos estadísticos sobre la gravedad de la propagación de redes robot en teléfonos inteligentes. La amenaza que suponen las redes robot en teléfonos inteligentes está aumentando a gran velocidad en algunas regiones y podría expandirse a nivel mundial, transformando un problema regional en un grave problema mundial.

En comparación con los ordenadores personales y los servidores, los teléfonos inteligentes tienen menos potencia de procesamiento, espacio de almacenamiento y duración de batería. Sin embargo, para los usuarios las redes robot en teléfonos inteligentes podrían tener repercusiones negativas más graves por los siguientes motivos: 1) en los teléfonos inteligentes se suele almacenar información de identificación personal (IIP) muy importante y 2) los ataques a los teléfonos inteligentes o la infraestructura del operador puede degradar severamente la percepción del usuario dada la prevalencia de los teléfonos inteligentes y la dependencia de los usuarios en los mismos.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1213	2017-09-06	17	11.1002/1000/13261

Palabras clave

Información de identificación personal (IIP), instrucción y control (C&C), red robot, software maligno, teléfono inteligente.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1213

Capacidades de seguridad necesarias para luchar contra las redes robot en teléfonos inteligentes

1 Alcance

El objetivo de esta Recomendación es determinar las capacidades de seguridad necesarias para luchar contra las redes robot en teléfonos inteligentes mediante el estudio de los retos que plantean esas redes robot, las amenazas específicas que suponen y los requisitos que imponen en las redes de operador y en los teléfonos inteligentes mismos. Esta Recomendación se centra en el análisis de las amenazas y la enumeración de requisitos. La meta es salvaguardar las infraestructuras de los operadores y los teléfonos inteligentes, garantizar los servicios de los operadores así como su calidad y mejorar la experiencia del usuario. Las soluciones técnicas detalladas, así como otro tipo de terminales inteligentes, como las tabletas, quedan fuera del alcance de esta Recomendación.

2 Referencias

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

En esta Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 bot [b-UIT-T X-Sup.8]: Programa informático automatizado que se emplea para realizar determinadas tareas con fines malignos. Es sinónimo de robot.

3.1.2 botmaster [b-UIT-T X-Sup.8]: Persona responsable del control y el mantenimiento de una red robot (botnet).

3.1.3 red robot (botnet) [b-UIT-T X-Sup.8]: Robots (bots) de software maligno controlados a distancia que se ejecutan autónoma o automáticamente en los ordenadores infectados en conjunción con un servidor de instrucción y control que pertenece al botmaster.

3.1.4 información de identificación personal (IIP) [b-UIT-T X.1252]: Toda información a) que identifica a una persona y que puede utilizarse para identificar, contactar o localizar a la misma; b) que puede utilizarse para obtener información de identificación o de contacto sobre una determinada persona; c) que puede relacionarse directa o directamente con una persona.

3.2 Términos definidos en esta Recomendación

Ninguno.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

2FA Autentificación por dos factores *(two factor authentication)*

2G Telecomunicaciones móviles de segunda generación *(second generation of mobile telecommunication)*

3G Telecomunicaciones móviles de tercera generación *(third generation of mobile telecommunication)*

4G	Telecomunicaciones móviles de cuarta generación *(fourth generation of mobile telecommunication)*
API	Interfaz de programación de aplicación *(application programming interface)*
C&C	Instrucción y control *(command and control)*
CPU	Unidad central de procesamiento *(central processing unit)*
DDoS	Denegación de servicio distribuida *(distributed denial of service)*
DNS	Sistema de nombres de dominio *(domain name system)*
GPS	Sistema de posicionamiento global *(global positioning system)*
HTTP	Protocolo de transferencia de hipertexto *(hyper text transfer protocol)*
IDS	Sistema de detección de intrusiones *(intrusion detection system)*
IIP	Información de identificación personal
IoT	Internet de las cosas *(internet of things)*
IP	Protocolo Internet *(internet protocol)*
IPS	Sistema de prevención de intrusiones *(intrusion prevention system)*
MITM	Intermediario *(man-in-the-middle)*
MMS	Servicio de mensajería multimedios *(multimedia messaging service)*
NFC	Comunicaciones en el campo cercano *(near field communication)*
OTP	Contraseña de utilización única *(one-time passcode)*
P2P	Par a par *(peer-to-peer)*
PC	Ordenador personal *(personal computer)*
PNG	Gráfico de redes portátiles *(portable network graphic)*
QoS	Calidad de servicio *(quality of service)*
QRcode	Código de respuesta rápida *(quick response code)*
SIM	Módulo de identidad del abonado *(subscriber identity module)*
SMS	Servicio de mensajes breves *(short message service)*
USB	Bus serie universal *(universal serial bus)*
WiFi	Fidelidad inalámbrica *(wireless fidelity)*

5 Convenios

Ninguno.

6 Antecedentes

El rápido desarrollo de los dispositivos de Internet móvil ha hecho que los terminales móviles sean cada vez más inteligentes y posean capacidades de funcionamiento superiores. En esta Recomendación, por teléfono inteligente se entiende el tipo de teléfono móvil que posee las siguientes características:

– sistema operativo independiente;

– capacidad de ampliar continuamente las funciones y capacidades del teléfono mediante la instalación de aplicaciones de terceros;

– capacidad de acceso a la red inalámbrica, incluida la capacidad de acceder a Internet móvil mediante una red de comunicaciones de operador móvil.

En los últimos años el número de usuarios de teléfonos inteligentes ha seguido creciendo a un ritmo acelerado. Si bien los teléfonos móviles aportan comodidad a la vida cotidiana, las amenazas de seguridad que suponen crecen en la misma proporción.

6.1 Resumen de las consideraciones de seguridad

Habida cuenta de que el número de usuarios de teléfonos inteligentes crece rápidamente, es necesario suprimir efectivamente las redes robot en teléfonos inteligentes y controlarlas para evitar que se conviertan en un importante factor de influencia en la estabilidad social y en una amenaza a la seguridad pública.

En lo que atañe a los operadores móviles, las redes robot a gran escala podrían menoscabar gravemente la utilización efectiva de las redes de los operadores y reducir la calidad del servicio (QoS) ofrecido a los usuarios, causando la insatisfacción de estos últimos y la pérdida de abonados. En cuanto a los usuarios, cuyos teléfonos inteligentes estén pirateados y controlados por botnets, las pérdidas potenciales son importantes, pues con frecuencia almacenan gran parte de su información de identificación personal (IIP), como listas de contactos e información de pagos en línea, en los teléfonos inteligentes.

Por consiguiente, la lucha contra las redes robot en teléfonos inteligentes es necesaria ahora y de cara al futuro. Los operadores deben aumentar su seguridad en este sentido para acabar con el rápido crecimiento de redes robot, reducir las pérdidas en términos de abonados, limitar las quejas de los usuarios, etc.

6.2 Evolución de las amenazas de redes robot en los teléfonos inteligentes

Los primeros virus en teléfonos inteligentes aparecieron en 2004 siendo *Cabir* el primer gusano basado en teléfonos inteligentes descubierto. En 2009, el software maligno (malware) *iKee.B* ya poseía las características de una red robot o botnet y podría asumir el control de los iPhones infectados y enviar la IIP del usuario a su botmaster. En 2011 se descubrió una botnet móvil representantiva, *Android.Geinimi*, que podía ocultar métodos de comunicación, disponía de abundantes módulos de ataque y se consideraba altamente dañina.

La generalización de la utilización de los teléfonos inteligentes se ha acompañado de un extraordinario crecimiento del malware para teléfonos inteligentes, que utiliza principalmente ciertas funciones de los teléfonos inteligentes como medio de propagación. Una vez descargado e instalado en el teléfono móvil, el malware mostrará con frecuencia y en secreto anuncios que inducirán un mayor tráfico de teléfonos móviles, impondrán tasas, etc., lo que redundará en pérdidas para los usuarios. Además, es posible que los usuarios de teléfonos inteligentes se enfrenten a otros problemas, como el redireccionamiento a sitios web de peska, la infección del teléfono con virus o caballos de Troya, la divulgación o el robo de su lista de contactos y/o agenda de direcciones, o el robo de cuentas y contraseñas. De todos estos delitos, el más frecuente es la divulgación de IIP, cuentas personales y contraseñas.

En los últimos años el malware de teléfonos móviles ha experimentado un crecimiento exponencial. El malware es la principal causa de propagación de virus botnet, pues un número cada vez mayor de malware utiliza métodos o funciones de puerta trasera controlada a distancia, que son la característica distintiva de los robots en teléfonos inteligentes. El objetivo principal de los botmasters es obtener beneficios del robo de IIP y de la imposición de tasas indebidas. En la actualidad, los malware más comunes conllevan el robo de IIP, la imposición de tasas indebidas, comportamientos malignos, el deterioro del funcionamiento y la propagación maligna.

6.3 Protección para teléfonos inteligentes

Los principales problemas de seguridad a que se enfrentan los usuarios de teléfonos inteligentes son el acoso telefónico, el spam por servicio de mensajes breves (SMS), etc., resultantes de la navegación web, la descarga de ficheros, los pagos móviles, etc. Estas amenazas se contrarrestan normalmente con el software de seguridad instalado en los teléfonos inteligentes.

Las dos principales funciones del software de seguridad de los teléfonos móviles son la gestión del teléfono y la protección de seguridad. La función de gestión del teléfono incluye la limpieza de la memoria, la ampliación del tiempo de espera, la gestión del programa de reinicio automático, la gestión de SMS, la gestión de números de teléfono, etc. El objetivo de la función de gestión del teléfono es que el teléfono inteligente funcione sin interrupciones y aumente la eficiencia de utilización del dispositivo. La función de protección de seguridad comprende, sobre todo, la supervisión del tráfico de datos, el bloqueo del acoso telefónico, el escaneado periódico, la eliminación periódica de virus, etc. El objetivo de la función de protección de seguridad es proteger al teléfono inteligente contra las amenazas a la seguridad.

La instalación de un software de seguridad puede contribuir a la protección de los teléfonos inteligentes contra ciertas botnets y malware en el lado del terminal de usuario, pero, como las habilidades de los atacantes de teléfonos inteligentes aumentan y sus métodos de ataque se diversifican, los teléfonos inteligentes seguirán afrontando amenazas a su seguridad. Además de aumentar la protección de seguridad en el lado terminal, los operadores deben también ofrecer más protección de seguridad en el lado red. La coordinación y cooperación de ambos extremos aumentará notablemente la capacidad de los teléfonos inteligentes para soportar ataques de botnets.

7 Características de las redes robot en teléfonos inteligentes

Las botnets en teléfonos inteligentes explotan las características de los teléfonos inteligentes y las redes móviles utilizando Internet para difundir los malware a gran escala. Mediante el análisis de las características de los teléfonos inteligentes y las redes móviles, así como del objetivo de los ataques de los botmaster, pueden resumirse las características de las botnets en teléfonos inteligentes y reconocer las posibles amenazas a la seguridad.

7.1 Información de identificación personal en robots

Las botnets en teléfonos inteligentes están compuestas de un gran número de bots basados en teléfonos inteligentes. A diferencia de lo que ocurre con los ordenadores personales (PC) tradicionales, la mayoría de la IIP y la información privada en los teléfonos inteligentes está almacenada de manera centralizada, lo que hace que las botnets en teléfonos inteligentes supongan una amenaza mucho mayor para los usuarios de esos teléfonos, pues pueden perder una enorme cantidad de datos.

Entre las funciones integradas en los teléfonos inteligentes se cuentan la gestión de la información personal, los calendarios y agendas, el diario, la definición de tareas, las aplicaciones multimedios, la navegación web, etc. la abundancia de información personal almacenada en las aplicaciones de teléfonos inteligentes convierte a este tipo de teléfonos en el objetivo principal de los atacantes. Además, con el sistema de posicionamiento global (GPS) del teléfono se puede adquirir información sobre la ubicación del usuario, que es otro tipo de IIP. Una vez en posesión de los atacantes, éstos pueden divulgar la IIP del usuario.

7.2 Diversos medios de propagación

En primer lugar, las botnets en teléfonos inteligentes pueden expandirse mediante aplicaciones infectadas que los usuarios suelen encontrar y descargar desde tiendas de aplicaciones o foros de telefonía móvil que no exigen una autentificación segura.

En segundo lugar, las botnets en teléfonos móviles pueden transmitirse por Bluetooth, fidelidad inalámbrica (WiFi), bus serie universal (USB) y demás interfaces periféricas de los teléfonos inteligentes.

En tercer lugar, las botnets en teléfonos móviles pueden transmitirse por el protocolo de transferencia de hipertexto (HTTP), el SMS, el servicio de mensajería multimedios (MMS), el código de respuesta rápida (QRcode), etc.

La diversidad de medios de propagación hace que la transmisión de botnets en teléfonos inteligentes sea relativamente fácil, lo que, en consecuencia, impone mayores requisitos de protección de seguridad.

7.3 Apertura

Los sistemas operativos móviles abiertos ofrecen a los teléfonos inteligentes un gran número de opciones en términos de programas de aplicación, pero al mismo tiempo estos programas también exponen a los teléfonos inteligentes a un mayor número de amenazas y piratas. La apertura permite a los piratas a incorporar virus o caballos de Troya en aplicaciones ampliadas, lo que facilita la propagación de las botnets en teléfonos inteligentes.

Los teléfonos inteligentes tienen múltiples tipos de interfaces periféricas, entre las que se cuentan Bluetooth, las comunicaciones en el campo cercano (NFC) y los USB. Los atacantes pueden utilizar cualquiera de estas conexiones por interfaz periférica. Además, los teléfonos inteligentes suelen soportar el acceso a redes móviles de segunda, tercera o cuarta generación (2G, 3G o 4G) y el acceso WiFi, mediante el cual los usuarios pueden acceder a Internet. Estas funciones tienen un valor comercial y de aplicación evidente, pero también ofrecen a los atacantes muchas vías para llevar a cabo sus acciones.

7.4 Infección dirigida

Las redes robot en teléfonos inteligentes suelen estar dirigidas a ciertos tipos de objetivos, infectándolos mediante copia directa o engañando a los usuarios para que descarguen malware o caballos de Troya. Los atacantes pueden también centrarse en los teléfonos inteligentes que utilizan el mismo sistema operativo para desencadenar la infección. Con este método aumenta drásticamente la eficacia del ataque al tiempo que disminuye su coste.

7.5 Ocultación

Las redes robot en teléfonos inteligentes son cada vez más complejas. Algunas son capaces de ocultar su ataque borrando todo rastro de instalación tras lograr infectar el teléfono inteligente en cuestión. Algunas redes robot pueden borrar sus rastros de conexión a la red y al buzón de salida tras haber enviado la IIP del usuario a través de un acceso a Internet. Otras pueden incluso encargar servicios personalizados a proveedores de servicio específicos y bloquear automáticamente los mensajes de verificación de los operadores móviles.

Algunos malware y caballos de Troya, que roban IIP o imponen tasas indebidas, no lanzan sus ataques inmediatamente después de su instalación, sino que los lanzan de acuerdo con un horario definido por el malware o en los tiempos de reposo de los teléfonos inteligentes infectados.

Hoy en día un número cada vez mayor de malware dispone de puertas traseras controladas a distancia como función básica, que es una de las características distintivas de los robots de teléfonos inteligentes.

Muchas redes robot se propagan a través de programas malignos incorporados en aplicaciones móviles populares. Cuando un usuario descarga e instala aplicaciones desde las tiendas de aplicaciones o foros de telefonía móvil sin mecanismos de autentificación segura, se activan los programas malignos ocultos en las aplicaciones.

7.6 Intereses comerciales

A diferencia de la mayoría de los malware tradicionales, cuyo objetivo es el sabotaje, el objetivo de las redes robot en teléfonos inteligentes suele ser obtener beneficios. Por ejemplo, se benefician de robar la IIP del usuario o de imponer tasas indebidas, creando así una industria oscura de fraude por Internet. Los beneficios comerciales llevan a los atacantes a invertir más recursos en el desarrollo de redes robot en teléfonos inteligentes y a fomentar el desarrollo de la industria del fraude por Internet. Esto significa que las redes robot en teléfonos inteligentes supondrán más amenazas de seguridad para los usuarios y será cada vez más difícil protegerlos contra ellas.

7.7 Cambio constante de conexión a la red

La gran movilidad de los teléfonos inteligentes hace que la conexión a la red cambie continuamente, lo que induce a la cada vez mayor diversidad de las redes robot en teléfonos inteligentes. Los teléfonos inteligentes pueden itinerar, no sólo entre redes que utilizan la misma tecnología de interconexión, sino entre redes que utilizan distintas tecnologías, por ejemplo, de una red 3G a un punto de acceso WiFi público. Por tanto, los robots en teléfonos inteligentes pueden tener que cambiar su canal de comunicación con el servidor de instrucción y control (C&C) con más frecuencia que los robot en PC, lo que hace aún más compleja la detección de las redes robot en teléfonos inteligentes mediante la identificación de sus canales de comunicación.

8 Amenazas de seguridad

8.1 Divulgación de información de identificación personal

– Información de la tarjeta módulo de identidad del abonado (SIM):

  Una vez infectado el teléfono inteligente con un robot, el botmaster puede robar la información de la tarjeta telefónica del usuario, incluida su información de registro, los parámetros de configuración del hardware, etc. Los botmaster pueden obtener más beneficios financieros si venden o divulgan esa IIP. Más preocupante todavía es que los botmaster pueden lanzar ataques más peligrosos en los teléfonos inteligentes con la misma configuración analizando sus vulnerabilidades.

– Almacenamiento en el teléfono:

  Los botmaster de las redes robot en teléfonos inteligentes pueden utilizar la nube para controlar a distancia todos sus robots. De este modo, el botmaster puede robar a partir del robot la IIP del usuario, incluidos su número de teléfono, lista de contactos, registro de llamadas, correos electrónicos, información de ubicación, fotos y vídeos, etc. El botmaster puede dar al robot la instrucción de telecargar esa información en servidores distantes.

– Cuentas bancarias y contraseñas:

  Cuando un usuario realiza un pago utilizando su teléfono inteligente, los atacantes pueden adquirir el control pleno del teléfono gracias a sus vulnerabilidades y proceder al robo de las cuentas bancarias y contraseñas del usuario. Además, pueden interceptar el código de verificación SMS y realizar transferencias de dinero indebidas, al tiempo que suprimen todo rastro del ataque. De este modo los atacantes pueden robar dinero fácilmente sin que el usuario del teléfono se dé cuenta.

– Cuentas de aplicación y contraseñas:

  Utilizando el mismo método los atacantes pueden robar las cuentas y contraseñas de los usuarios para las aplicaciones y utilizar esa información para cometer otros fraudes y generar los correspondientes beneficios.

8.2 Imposición de tasas indebidas

– Descarga automática o supresión de software:

Cuando un teléfono inteligente está controlado por un robot, recibe instrucciones desde un servidor C&C y el botmaster puede hacer que el teléfono haga prácticamente cualquier cosa. Siguiendo las instrucciones del botmaster, el teléfono inteligente puede automáticamente descargar aplicaciones innecesarias o desinstalar determinadas aplicaciones, lo que aumentará los gastos por consumo de tráfico de datos y causará pérdidas financieras al usuario.

– Spam por SMS:

Determinados malware pueden hacer que los teléfonos inteligentes envíen SMS utilizando la lista de contactos del teléfono. Primero, el atacante engaña al usuario para que descargue e instale el malware y, a continuación, el teléfono infectado entrará automáticamente en contacto con el servidor C&C para recibir instrucciones. Una vez recibidas las instrucciones para el envío de SMS basura, el teléfono empezará a enviar los mensajes a la lista de contactos del teléfono, lo que reducirá la calidad de funcionamiento e inducirá al cobro de tasas indebidas en concepto de acceso a Internet y mensajería SMS. Si se eleva la frecuencia del spam por SMS, es posible que se degraden los canales móviles, lo que supondrá una reducción de la calidad de funcionamiento del teléfono e incluso su indisponibilidad. Además, si el teléfono infectado pertenece a una empresa o una institución pública, la reputación de esta última podrá verse afectada, pues es posible que la lista de contactos almacenada en el teléfono contenga los números de importantes socios comerciales o gubernamentales. Si un teléfono infectado envía SMS basura con frecuencia, es posible que el receptor ponga el número en lista negra, lo que puede tener consecuencias financieras impredecibles y puede menoscabar las relaciones comerciales.

8.3 Comportamientos malignos

– Ataques de denegación de servicio distribuida (DDoS):

En paralelo a la generalización de la utilización de teléfonos inteligentes y el rápido crecimiento de las aplicaciones de Internet móvil, los botmasters pueden lanzar ataques DDoS, si el número de robots controlados es muy grande. Los botmasters pueden controlar un gran número de teléfonos infectados y pueden lanzar ataques simultáneos a un sitio web concreto, lo que llevará al fallo de los servidores web. Concretamente, si los teléfonos inteligentes infectados pertenecen a ciertas empresas o instituciones públicas, su reputación podrá verse considerablemente menoscabada, pues es probable que las listas de contactos de esos teléfonos contengan los números de importantes socios comerciales o contactos gubernamentales. Una vez detectado un ataque DDoS, la víctima responderá bloqueando los números de teléfono atacantes, lo que puede tener consecuencias financieras impredecibles y puede menoscabar las relaciones comerciales.

– Publicidad engañosa maligna:

Es posible transformar un teléfono inteligente infectado en un receptor de publicidad basura. Los usuarios pueden recibir diversos anuncios y cada clic generará ingresos para la red robot. De este modo, los botmasters obtendrán ingentes beneficios generados por tasas de publicidad fraudulentas. Sin embargo, los clic no proceden del usuario del teléfono, sino del robot maligno instalado en el teléfono.

– Acceso no autorizado a redes de empresa:

Las redes robot en teléfonos inteligentes pueden permitir a los atacantes obtener acceso a redes de empresa seguras a través de dispositivos de red infectados. Un dispositivo infectado puede analizar la vulnerabilidad del anfitrión en la red de empresa e informar de ello al botmaster. Los atacantes pueden, además, explotar esa vulnerabilidad y atacar a los anfitriones de la red de empresa y robar información confidencial.

8.4 Degradación de la calidad de funcionamiento

Los botmasters pueden degradar la calidad de funcionamiento de los teléfonos inteligentes de la siguiente manera:

– Puede haber componentes de virus disimulados en imágenes de gráfico de redes portátiles (PNG), que en realidad son códigos automatizados. Tras la infección, el virus se cargará automáticamente al encender el teléfono inteligente y se ejecutará constantemente de manera oculta, lo que causará una grave degradación de la calidad de funcionamiento del sistema operativo.

– La conexión frecuente a servidores troyanos en busca de instrucciones causará daños persistentes en el teléfono.

– La descarga automática y oculta de aplicaciones basura conllevará un consumo de batería y una importante degradación de la calidad de funcionamiento en un corto periodo de tiempo.

– Los botmasters pueden enviar continuamente SMS basura a los teléfonos inteligentes infectados impidiendo así su funcionamiento y agotando la batería.

8.5 Transmisión maligna

Algunos malware pueden descargar aplicaciones en un teléfono inteligente infectado, de manera oculta, sin permiso del usuario, y posteriormente lanzar mensajes fraudulentos que inducen al usuario a tocar la pantalla, dando así pie a la instalación del malware. Una vez instalada la aplicación, ésta accederá a un sitio web concreto de manera soterrada para elevar su clasificación de descargas e inducir a más usuarios a descargar la aplicación maligna. De este modo se amplía exponencialmente la botnet y los atacantes obtienen mayores beneficios.

8.6 Pérdida de credibilidad

Los teléfonos inteligentes infectados con redes robot pueden utilizarse para enviar correos electrónicos basura o participar en ataques DDoS, comportamientos que no sólo eleven los costes de la red y el consumo de la batería, sino que también pueden causar la pérdida de credibilidad del usuario. Por ejemplo, cuando un teléfono infectado con una botnet envíe masivamente mensajes o correos-e basura a los contactos almacenados en él, el emisor (propietario del teléfono inteligente) perderá credibilidad. Concretamente, si el teléfono pertenece a una empresa o institución pública, las pérdidas pueden ser mucho mayores, pues la lista de contactos almacenada en el teléfono probablemente contendrá los números de importantes socios comerciales o gubernamentales.

9 Capacidades de seguridad necesarias

9.1 Capacidades de seguridad de red necesarias

9.1.1 Supervisión del tráfico de red

Los operadores deben ofrecer la capacidad de supervisar el tráfico Internet del teléfono inteligente. Pueden establecer un mecanismo de supervisión del tráfico o elaborar una tabla con todos los usuarios y analizar inteligentemente el tráfico Internet de un teléfono inteligente. Cuando se detecte tráfico anormal, los operadores podrán enviar inmediatamente una alarma o comunicar la información pertinente al usuario y, de ser necesario, interceptar el tráfico sospechoso.

9.1.2 Detección de código maligno móvil

Los dispositivos de protección de seguridad de la red de un operador deben detectar y analizar el código maligno en sus aplicaciones. De detectarse código maligno en una aplicación, el operador podrá enviar inmediatamente una alarma o comunicar la información pertinente a los usuarios que descargan o utilizan la aplicación.

9.1.3 Transmisión encriptada de información sensible

La red de un operador debe soportar la transmisión encriptada de la información enviada por los teléfonos inteligentes. Cuando los usuarios activen esa función, los dispositivos de red del operador deberán garantizar la integridad y confidencialidad de la información transmitida, incluidas las listas de contactos, la información de ubicación, las cuentas y contraseñas, etc.

9.1.4 Red cebo

Las redes de operador deben crear un sistema informático que sirva de cebo y propicie el acceso de botnets y programas malignos al teléfono inteligente. Una vez detectadas las botnets, se obtendrá su información de control y los operadores podrán recurrir a la observación y el rastreo para saber cómo proteger mejor los teléfonos inteligentes.

9.1.5 Protección contra ataques DDoS

– Los dispositivos de protección de seguridad y los servidores del sistema de nombres de dominio (DNS) de la red de un operador deben responder a una política de seguridad que impida a los anfitriones de las botnets conectarse a sus controladores.

– Los cortafuegos, sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS) y demás dispositivos de seguridad de la red de un operador deberán poder ofrecer configuraciones de seguridad que bloqueen los ataques de tráfico.

– Los dispositivos de red y de seguridad de la red de un operador deben responder a políticas de bloqueo del tráfico DDoS que bloqueen el tráfico DDoS del servidor objetivo en otros dominios.

9.1.6 Detección de botnets

Los dispositivos de protección de seguridad de la red de un operador deben poder detectar la mutación de las botnets y recopilar y compartir la totalidad de las direcciones de protocolo Internet (IP), para lo que se ha de crear una base de datos de direcciones IP de controladores y anfitriones de botnets para realizar filtrados de tráfico maligno, analizar las acciones de los robots, crear mecanismos para determinar la fiabilidad de las direcciones IP y métodos de protección de otro tipo.

9.1.7 Detección y eliminación de SMS basura

Una red de operador debe disponer de mecanismos para detectar y suprimir SMS basura. Cuando se observa que un terminal móvil recibe una gran cantidad de mensajes basura, debe facilitarse oportunamente el bloqueo del spam para evitar el colapso causado por la recepción masiva de mensajes basura. Durante la detección, los operadores deberán informar a los usuarios a fin de que estos últimos puedan tomar las medidas necesarias para resolver el problema.

9.1.8 Lista negra y lista blanca

Los dispositivos de protección de seguridad de una red de operador deben tener la capacidad de añadir malware, códigos malignos y sitios web malignos en sus listas negras. Si los controladores de las botnets solicitan a sus anfitriones controlados que se conecten a un sitio web maligno o que descarguen un malware, que figure en la lista negra, los dispositivos de seguridad deben poder bloquear esa conexión a tiempo.

Del mismo modo, los dispositivos de seguridad de una red de operador deben poder establecer una lista blanca. Bajo determinadas condiciones se permitirá al usuario conectarse a sitios web fiables y descargar aplicaciones fiables que figuren en la lista blanca.

9.1.9 Capacidad de cooperación

Para mejorar la integridad y credibilidad del software de seguridad, los operadores deben poder cooperar con los proveedores de productos de seguridad para teléfonos inteligentes. Gracias a esa cooperación podrá ofrecerse protección de seguridad contra botnets tanto desde el lado red como desde el lado terminal móvil.

Además, los operadores también deben cooperar con los entes gubernamentales y administrativos. Si un teléfono inteligente se convierte en robot, los operadores deberán informar al propietario a través de los canales administrativos. Por otra parte, para poner fin a las redes robot en teléfonos inteligentes y a sus actividades malignas, los operadores deben cooperar con los entes gubernamentales y administrativos a fin de definir la legislación al respecto y los procedimientos correspondientes.

9.1.10 Garantía de identidad

Si el teléfono de un usuario (en particular, un grupo de usuarios) queda infectado y empieza a enviar masivamente mensajes basura, etc., es posible que el usuario pierda la confianza de los receptores de los mensajes basura. Si el teléfono inteligente pertenece a una empresa o institución pública, las pérdidas pueden ser mucho mayores, pues probablemente su lista de contactos contenga los números de importantes socios comerciales o instituciones gubernamentales.

Para no perder esa confianza, los operadores deben tener la capacidad de garantizar la identidad del usuario del teléfono inteligente (en particular cuando se trata de grupos de usuarios) en caso de que se detecte un funcionamiento anormal, como el envío masivo de mensajes. Por ejemplo, un operador debe poder detectar el envío masivo de mensajes por un usuario y, de acuerdo con las políticas definidas, informarlo por mensajería o suspender temporalmente esa función y pedir la confirmación del usuario antes de volver a activarla.

9.2 Capacidades de seguridad de los teléfonos inteligentes necesarias

9.2.1 Almacenamiento encriptado de la información de identificación personal

Los teléfonos inteligentes deben soportar el almacenamiento encriptado de la lista de contactos, los mensajes SMS, las fotografías, los registros de llamadas y demás IIP. En los teléfonos inteligentes, la IIP debe almacenarse utilizando métodos de encriptación.

9.2.2 Acceso encriptado a la información de identificación personal

Los teléfonos inteligentes deben ofrecer un mecanismo de acceso encriptado a las listas de contactos, mensajes SMS, fotografías, registros de llamadas y demás IIP. Los usuarios de teléfonos inteligentes deben poder configurar contraseñas, huellas digitales o demás restricciones para acceder a determinados tipos de información personal (como fotografías o SMS concreto).

9.2.3 Utilización de software de seguridad

Los usuarios de teléfonos inteligentes deben instalar en sus teléfonos software de protección de seguridad, que los ayudará a detectar y eliminar las posibles amenazas o vulnerabilidades y tomará las medidas de protección necesarias en caso de ataque. Si el teléfono inteligente carece de software de protección, debería poder recordar al usuario que debe instalarlo. Si el software está instalado, el teléfono debe poder instar al usuario a inspeccionar periódicamente el sistema y actualizar el software de seguridad.

9.2.4 Alerta a la vinculación de cuentas bancarias

Si un usuario opta por guardar números de cuenta o contraseñas cuando utiliza funciones de pago móvil, el teléfono inteligente debe advertirle de que no está recomendado guardar números de cuenta o contraseñas en el teléfono.

9.2.5 Supervisión del tráfico Internet en los teléfonos inteligentes

El software de protección de seguridad de los teléfonos inteligentes debe poder analizar inteligentemente la utilización del tráfico Internet de un usuario, cuando se detecte tráfico anormal en un breve periodo de tiempo, debe poder bloquear el tráfico sospechoso lo antes posible e instar al usuario a cerrar la conexión o dejar de navegar por sitios web sospechosos.

9.2.6 Eliminación de código maligno móvil

Una vez detectado el código maligno en aplicaciones o malware, el teléfono inteligente debe poder informar al usuario para que decida si ha de suprimir el software y comunicar la información a las autoridades pertinentes.

9.2.7 Utilización segura de WiFi

Para proteger la IIP de un usuario, como los números de cuenta y las contraseñas, y prevenir ataques por intermediario (MITM) cuando se esté utilizado WiFi, los teléfonos inteligentes deben ofrecer medidas para garantizar la utilización segura del WiFi. Por ejemplo, cuando un usuario activa una conexión WiFi, el teléfono inteligente debe poder activar automáticamente la función de transmisión encriptada y desactivarla cuando cese la conexión WiFi.

9.2.8 Mecanismos de verificación de terceros

Cuando un usuario de teléfono móvil esté utilizando el pago móvil o cualquier otra aplicación que exija una identificación de cuenta, el teléfono debe soportar, para realizar el pago, la verificación de terceros, como el reconocimiento vocal o la utilización de un código de verificación de imagen.

9.2.9 Supervisión del consumo y la calidad de funcionamiento

Un teléfono inteligente debe poder supervisar la calidad de funcionamiento de su unidad central de procesamiento (CPU) y el consumo de batería. Cuando la calidad de funcionamiento de la CPU o el consumo de batería son anormales, se debe generar una notificación de alerta para informar al usuario.

Apéndice I

Conexión de malware a redes robot

(Este Apéndice no forma parte integrante de la presente Recomendación.)

I.1 Introducción

Este apéndice se basa en el estudio de investigaciones existentes y no es fruto de una investigación original. Los datos e informes analíticos proceden de organizaciones de consultoría chinas y del resto del mundo, así como de empresas de software antivirus. Se parte de la base de que las conclusiones alcanzadas por estas empresas y compañías se basan en la recopilación de una amplia cantidad de datos y en análisis de macrodatos.

Cada país tiene su cultura, costumbres, leyes, reglamentos y decretos de aplicación reglamentaria que dan como resultado distintos ecosistemas y entornos para la propagación de virus y malware de teléfonos inteligentes. Por motivos evidentes, las empresas de software antivirus, por ejemplo, pueden tender a sobreestimar el número de ataques detectados basándose en definiciones amplias y en perspectivas analíticas favorables. Por consiguiente, es posible que los informes de distintas empresas y organizaciones arrojen cifras estadísticas dispares. Sin embargo, las conclusiones básicas y las tendencias suelen ser idénticas para todos.

Por otra parte, 1) gran parte, si no la totalidad, del malware detectado posee características y capacidades que las redes robot podrían fácilmente utilizar; 2) los estudios sobre tendencias de malware y la experiencia con los teléfonos inteligentes sugiere que la amenaza de redes robot en teléfonos inteligentes está cerca; 3) hoy en día, a causa de la globalización, algunos problemas regionales de malware y redes robot pueden extrapolarse a otras regiones y convertirse en grandes problemas en el futuro, por lo que es necesario estar preparado.

I.2 Antecedentes

El rápido crecimiento de los teléfonos inteligentes es, quizá, uno de los grandes éxitos de nuestro tiempo. En China, por ejemplo, el número total de usuarios de teléfonos móviles ha superado los 1 300 millones, de los cuales más de 680 millones utilizan teléfonos inteligentes y están conectados a la red.

Los teléfonos inteligentes actuales están diseñados con el menor número de fallos posible, por lo que sufren pocas infecciones por virus. De hecho, el diseño de estos teléfonos hace que sólo una pequeña parte de los productos de teléfonos inteligentes sean susceptibles de infección. Sin embargo, aunque la posibilidad de infección es escasa, un teléfono infectado puede causar pérdidas insoportables e irreversibles al usuario cuya IIP fundamental, como números de cuentas bancarias, contraseñas, dirección de residencia y fotografías familiares, puede estar almacenada en el teléfono inteligente.

La creciente popularidad de los teléfonos inteligentes hace que el desarrollo de virus y malware esté más dirigido a los teléfonos que a los PC, pues los primeros son ahora el principal objetivo de los ataques de piratería. Además, la mayoría de ciberdelitos cuyo objetivo son los teléfonos inteligentes no están motivados por intereses personales o por la curiosidad, sino por la obtención de beneficios financieros mediante la petición de recompensas y el fraude financiero. Detrás de estos ciberdelitos está la industria oscura del fraude por Internet, cuyas posibilidades de cambiar en el futuro son escasas. Además, la Internet de las cosas (IoT) conecta a los terminales inteligentes entre ellos a fin de transmitir y compartir eficazmente datos e información. Una reciente investigación de Gartner [b-Gartner] predice que en 2015 habrá más de 4 900 millones de dispositivos con conexión a la IoT en el entorno doméstico inteligente, y que llegarán a los 25 mil millones en 2020. Sin embargo, esto supone una amenaza aún mayor para la IIP de los usuarios, pues un único fallo/laguna/fuga en el flujo

de datos, o la fragmentación de la recopilación de información de los enlaces IoT, puede llevar a la divulgación de la IIP de los usuarios y plantear nuevos problemas para la seguridad móvil.

Por consiguiente, los usuarios de teléfonos inteligentes suelen prestar más atención a la seguridad móvil, sobre todo cuando se trata de proteger su IIP. De acuerdo con la empresa mundial de analítica *mSecurity* [b-mSecurity], las inversiones en seguridad móvil alcanzaron los 11 mil millones USD en 2014 y crecerán a un ritmo global del 20% durante los próximos 6 años [b-GNSM].

I.3 Entorno macroscópico en China

Hay datos concretos que demuestran la tendencia al crecimiento exponencial del malware móvil.

En China, por ejemplo, los teléfonos inteligentes han ganado rápidamente popularidad en los últimos años. De acuerdo con los estudios realizados por *Qihoo 360*, una de las mayores empresas de software de seguridad de las redes y la información de China, el número de usuarios de telefonía móvil ha pasado de 1 000 millones en 2012 a 1 300 millones en 2015; y durante ese mismo periodo el número de usuarios de teléfonos inteligentes ha pasado de 270 millones a 680 millones.

Durante ese tiempo han surgido numerosos problemas de seguridad. En 2012 se encontraron muestras de 175 000 nuevos malware móviles y se infectaron 71 millones de teléfonos inteligentes. En 2015 se encontraron 18,7 millones de muestras de nuevos malware móviles y 370 millones de teléfonos resultaron infectados. A causa de la fuga de IIP con conexiones WiFi gratuitas y la generación de tráfico adicional a causa de códigos malignos, los usuarios se han visto forzados a adquirir seguros para pérdidas imprevistas de pagos móviles, acoso telefónico, fuga de IIP a partir de teléfonos de segunda mano, fuga de IIP a causa del software de redes sociales y todo tipo de spam. Para que un teléfono inteligente funcione en un entorno sano y seguro, es fundamental contar con protección contra los virus y malware, con supervisión del tráfico, protección de IIP, supervisión de la velocidad de red y supervisión de la seguridad WiFi. Los estudios muestran que las empresas de software de seguridad móvil deben cooperar estrechamente con los fabricantes de teléfonos para lograr una mejor protección y seguridad de los teléfonos inteligentes.

I.4 Problemas del iPhone

El iPhone de Apple ejerce un mayor control sobre el software instalado por los usuarios que otras plataformas, como Android. Apple dice tener una mayor seguridad [b-AppleSecurity] porque está motivada para ello y adopta medidas para diseñar ese ecosistema de software. Apple ha ido creando progresivamente un modelo donde el hardware y los sistemas operativos están integrados y, por lo general, los usuarios adquieren el software en la tienda de software oficial de la marca.

Sin embargo, se ha constatado que el número de malware diseñado para infectar dispositivos con iOS va en aumento [b-AppleThreat]. Los últimos estudios demuestran que la percepción general de seguridad del iPhone se ve menoscabada con el rápido crecimiento de usuarios de iPhone y de aplicaciones para iPhone.

XcodeGhost (detectado por Symantec como OSX.Codgost en ordenadores Mac OS X y como IOS.Codgost en dispositivos iOS) es una versión modificada del entorno de desarrollo Xcode y se considera como malware. Configura las aplicaciones para obtener información sobre los dispositivos y telecarga esa información en servidores C&C. Además, las aplicaciones troyanas pueden recibir instrucciones de los servidores C&C para lanzar ataques de peska. Un gran número de aplicaciones creadas con XcodeGhost lograron evitar las propias verificaciones de seguridad de Apple y se pusieron a la venta en la tienda de aplicaciones oficial, demostrando que el proceso de selección no garantiza la ausencia de malware en la tienda de aplicaciones de la marca. En noviembre de 2015 se descubrió una nueva variante de XcodeGhost en versiones no oficiales de Xcode 7, que permitía crear aplicaciones para iOS 9.

Los estudios muestran que prácticamente la mitad de los usuarios de iPhone ya no considera que su teléfono es absolutamente seguro. Casi el 33% de los teléfonos inteligentes ha sufrido infecciones; en el caso de los iPhone se trata del 23,9%.

En la actualidad y contrariamente a los teléfonos Android, los teléfonos de Apple controlan mejor la ejecución de aplicaciones/códigos gracias a un mecanismo de clave de permiso del creador. Una vez detectadas estas aplicaciones/códigos malignas en sus dispositivos, Apple puede impedirles funcionar en todos los dispositivos rechazando simplemente la clave de firma del creador.

Aunque se trata de una plataforma de software que no es de código abierto, iOS sigue teniendo sus puntos débiles, a saber, el acoso telefónico y la peska. Por este motivo, en junio de 2016, en el marco de la Apple Worldwide Developers Conference (WWDC), celebrada en San Francisco, Apple presentó públicamente su interfaz de programación de aplicación Ident-A-Call, que reduce notablemente las posibilidades de que los usuarios de iPhone reciban acoso telefónico y ataques de peska y demuestra que la seguridad móvil se está convirtiendo en un problema muy serio. Ha dejado de ser un problema meramente técnico para convertirse en un problema social.

I.5 Ejemplos y algunas tendencias del nuevo malware

I.5.1 Ejemplo 1

Los software de redes sociales y de pagos móviles se están convirtiendo en los nuevos objetivos de los virus y el malware, sobre todo porque están estrechamente relacionados y porque están adquiriendo una importancia cada vez mayor en la vida cotidiana.

Un malware denominado "*a.privacy.BankSteal.a*" adopta la apariencia de una aplicación de software de redes sociales muy famosa con un logo muy conocido, lo que dificulta que los usuarios puedan distinguir entre el malware y el software legítimo. Una vez infectado el teléfono inteligente, el malware induce al usuario a introducir su IIP, como números de tarjetas bancarias, contraseñas, nombres de usuario, números de tarjetas de identidad y números de teléfono, y a continuación se ejecuta en segundo plano interceptando los SMS del usuario. El malware envía la información a los piratas por correo electrónico, poniendo en serio peligro la IIP del usuario y la seguridad de los bienes del usuario.

I.5.2 Ejemplo 2

En 2015 se observó en todas las regiones del mundo un incremento en la utilización de teléfonos inteligentes para la utilización de servicios de banca en línea. Hoy en día muchas instituciones ofrecen una aplicación Android que utiliza la autentificación de dos factores (2FA), lo que ha acelerado la aparición de malware móvil [b-FinancialThreat].

El método de ataque más común es la intercepción de mensajes de texto que forman parte del proceso 2FA y su reenvío al servidor C&C del malware para su utilización por el atacante. Como suele ocurrir con el malware Android, la aplicación solicita permiso para recibir, escribir y enviar mensajes de texto, así como otro tipo de permisos, durante la fase de instalación.

En un sistema 2FA típico, el segundo factor, generalmente una contraseña de único uso (OTP) generada, se envía al número móvil registrado del usuario por SMS. Para aumentar la seguridad de la entrega de la OTP, algunas organizaciones financieras han empezado a enviar las OTP por llamada de voz, en lugar de SMS. En el último trimestre de 2015 se encontró una nueva variante de *Android.Bankosy*, que es un malware Android que roba información y es capaz de engañar a los sistemas 2FA que utilizan las llamadas de voz. El servidor C&C del malware puede dar al teléfono infectado la instrucción de reenviar todas las llamadas utilizando un código de servicio especial.

Otro tipo de ataque que ha ganado popularidad son las aplicaciones bancarias falsas independientes, que pueden resultar muy convincentes para los usuarios, por ejemplo, utilizando aplicaciones de testigo 2FA legítimas. Lo más peligroso de este tipo de aplicación maligna es que pide al usuario su nombre de usuario y contraseña durante la fase de instalación, obteniendo así toda la información

necesaria para llevar a cabo el fraude. Es posible así acceder a cuentas bancarias sin utilizar un ordenador infectado. En otros casos, los atacantes sustituyen el software de banca móvil legítimo ya instalado con su propio software maligno. Hay otro malware Android denominado *Android.Fakelogin* que utiliza técnicas de ingeniería social flexibles para robar los datos de identificación bancaria de una amplia gama de usuarios. En lugar de adoptar la apariencia de una aplicación concreta, *Android.Fakelogin* identifica la aplicación bancaria que se ejecuta en el dispositivo del usuario y la recubre con una página de entrada falsa y personalizada en la interfaz del usuario. Para ello accede a la lógica en la nube residente en un servidor C&C distante para determinar qué página de peska mostrar exactamente. Si el usuario intenta conectarse a través de la página fraudulenta, sus credenciales se enviarán directamente al servidor C&C del atacante. Aunque el malware se ataca a aplicaciones legítimas disponibles en Google Play, las aplicaciones que descargan *Fakelogin* no están disponibles en Google Play.

I.5.3 Ejemplo 3

Una de las muchas tendencias del nuevo malware es que es cada vez más maligno y descarado a la hora de hacer chantaje a los usuarios de teléfonos inteligentes. Por ejemplo, desde 2014 hay más malware dirigido hacia usuarios concretos mediante ataques par a par (P2P).

Hay un malware denominado "*a.rogue.SimpleLocker.a"* que obliga al teléfono del usuario a ejecutar el malware como principal prioridad y bloquea frecuentemente la pantalla del teléfono. Se exige al usuario del teléfono inteligente que pague una recompensa por el desbloqueo de la pantalla o no podrá ejecutar ninguna otra aplicación en el teléfono. En segundo plano, el malware está conectado a Internet y puede desbloquear a distancia la pantalla una vez abonada la recompensa. El malware ya no se esconde, es abiertamente maligno y descarado convirtiéndose en prioritario para chantajear a los usuarios. Cuantos más teléfonos infectados, mayores beneficios para los piratas.

I.6 Conclusión

En paralelo al rápido desarrollo de la Internet móvil, los teléfonos inteligentes son cada vez más inteligentes y su calidad de funcionamiento es mayor. La rápida adopción de los teléfonos inteligentes es quizá uno de los grandes logros de nuestro tiempo y los estudios demuestran que las redes robot informáticas están logrando rápidamente adaptarse al entorno de los teléfonos móviles. La velocidad a la que van apareciendo virus y malware es tan impresionante como el aumento de la utilización de este tipo de teléfonos, por lo que es necesario ahora y de cara al futuro trabajar para luchar contra las redes robot en teléfonos inteligentes.

Bibliografía

[b-UIT-T X.1205] Recomendación UIT-T X.1205 (2008), *Aspectos generales de la ciberseguridad.*

[b-UIT-T X.1252] Recomendación UIT-T X.1252 (2010), *Términos y definiciones sobre gestión de identidad de referencia*.

[b-UIT-T X.1546] Recomendación UIT-T X.1546 (2014), *Malware attribute enumeration and characterization*.

[b-UIT-T X-Sup.8] Suplemento 8 a la Serie X de Recomendaciones UIT-T (2010), *ITU-T X.1205 – Supplement on best practices against botnet threats*.

[b-AppleSecurity] Página web: *Apple Claims Better Security with iOS 9, Gets Hacked before Its Release*, 13 de septiembre de 2015, <https://lifars.com/2015/09/hacker-cracks-ios-9-with-a-jailbreak-before-its-public-release/>

[b-AppleThreat] O'Brien, Dick (2016), *The Apple threat landscape*, Symantec Security Response, Version 1.02, 11 de febrero de 2016.

[b-FinancialThreat] Candid, West (2015), *Financial threats*, Symantec Security Response, Version 1.0, 22 de marzo de 2016.

[b-Gartner] Gartner Press Release, 11 de noviembre <http://www.gartner.com/newsroom/id/2905717>

[b-GNSM] *Global Network Security Market 2015-019*.

[b-mSecurity] Mobile Security (mSecurity) Market Forecast 2014-2024.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2018