BOLETÍN DE ALERTA

Boletín Nro.: 2016-02
Fecha de publicación: 08/01/2016
Tema: Distribución de malware para Android a través de comentarios falsos

Descripción:
Hace un tiempo se ha observado un importante aumento de campañas de distribución de malware para Android u otro tipo de contenido malicioso a través de comentarios falsos en noticias de algunos medios digitales.
A través de perfiles falsos y/o perfiles comprometidos de Facebook, se publican comentarios, normalmente en las noticias más leídas del día de algunos medios digitales. Dichos comentarios contienen supuestas noticias llamativas y enlaces a las mismas. Por lo general, se trata de supuestos videos. Los enlaces y las supuestas noticias varían, al igual que los perfiles desde los cuales se publica.

Figura 1: Ejemplo de comentario con enlace a una noticia falsa

Al ingresar a estos enlaces por lo general se observa un cuadro que aparenta ser un video, sin embargo se trata de imágenes con enlaces a otras páginas. Al hacer click desde un equipo con sistemas operativos Windows, Linux, OS X o similar, el usuario es redirigido a diversos dominios, por lo general sitios de contenido sexual, los cuales en ocasiones pueden contener anuncios maliciosos (*malvertising*), en algunos casos se trata simplemente de un esquema de *pay-per-click* ("pago por click"), en la que los ciberdelincuentes buscan ganar dinero a través de los clicks que realiza la víctima de forma inadvertida al ingresar a uno de estos enlaces. En la mayoría de los casos el usuario no podrá ver el video deseado, ya que se trata de noticias falsas.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

Sin embargo, en los casos en los que el usuario ingresa a los enlaces de los comentarios desde un dispositivo con sistema operativo Android, será redirigido a otros dominios, los cuales terminarán descargando y/o instalando aplicaciones maliciosas en su dispositivo. En la mayoría de los casos, se comprobó que las aplicaciones maliciosas (.apk) están alojadas en dominios ajenos al Play Store de Google, las cuales son descargadas al teléfono. Los nombres de las aplicaciones varían, siendo algunas de ellas:

- GirlTube_0105_YM1.apk
- 2_1452073197162_0_11107.apk
- 20151221143517776.apk
- mb_bp_local_1_0105.apk

Sin embargo en algunos casos, redirige a aplicaciones que se encuentran en el Play Store de Google.
Si bien, todas las aplicaciones analizadas, presentaron comportamientos diferentes, todas son maliciosas.

La gran mayoría de las aplicaciones se tratan de variantes del malware conocido como **Android Porn Clicker**, una aplicación que se instala de forma inadvertida para el usuario y accede en segundo plano a numerosos enlaces, en su mayoría, sitios de contenido sexual, sin que el usuario lo perciba. Lo único que el usuario podría percibir es un considerable aumento en su consumo de ancho de banda, especialmente si utiliza la red de datos. Además, percibirá una importante disminución en la duración de su batería, debido a que el malware se ejecuta en todo momento en segundo plano, sin interrumpir la navegación.
En la mayoría de las aplicaciones además se observó que las mismas descargan adicionalmente otras aplicaciones maliciosas, sin que el usuario lo note; la mayoría de las mismas busca obtener privilegios de *root*. De esta manera la amenaza puede realizar cambios en la configuración del equipo en conjunto con el robo de información y la instalación de otros códigos maliciosos.
En algunos casos, durante las redirecciones, aparecen pop-ups con advertencias falsas tales como "Se ha detectado malware en su dispositivo", "Acelere la velocidad de su teléfono", "Repare su Android ahora", "Actualización requerida", etc. En todos los casos se trata de advertencias falsas que buscan que la víctima haga click en ellas, descargando e instalando así software malicioso en su dispositivo.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

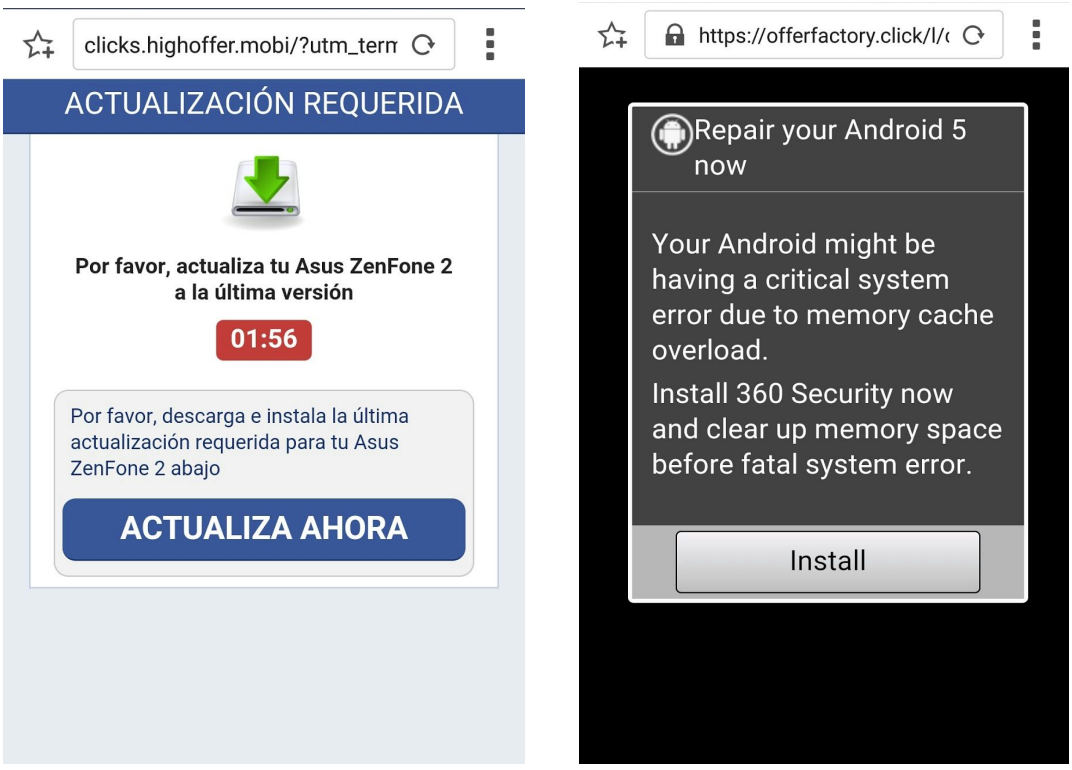


Figura 2: Alertas falsas para Android

En el caso de sistema operativo iOS, se ha observado que los enlaces redirigen a diversos sitios de contenido sexual.

En otros casos, se observó que los falsos videos redirigen a páginas web que solicitan que el usuario ingrese el número de teléfono móvil. En caso de hacerlo, la víctima queda suscripta a servicios de SMS premium. Los mensajes de estos servicios llegan de forma automática y tienen un costo que se descuenta del saldo de la víctima. Los costos pueden variar, llegando incluso a alrededor de 45.000 Gs. mensuales.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

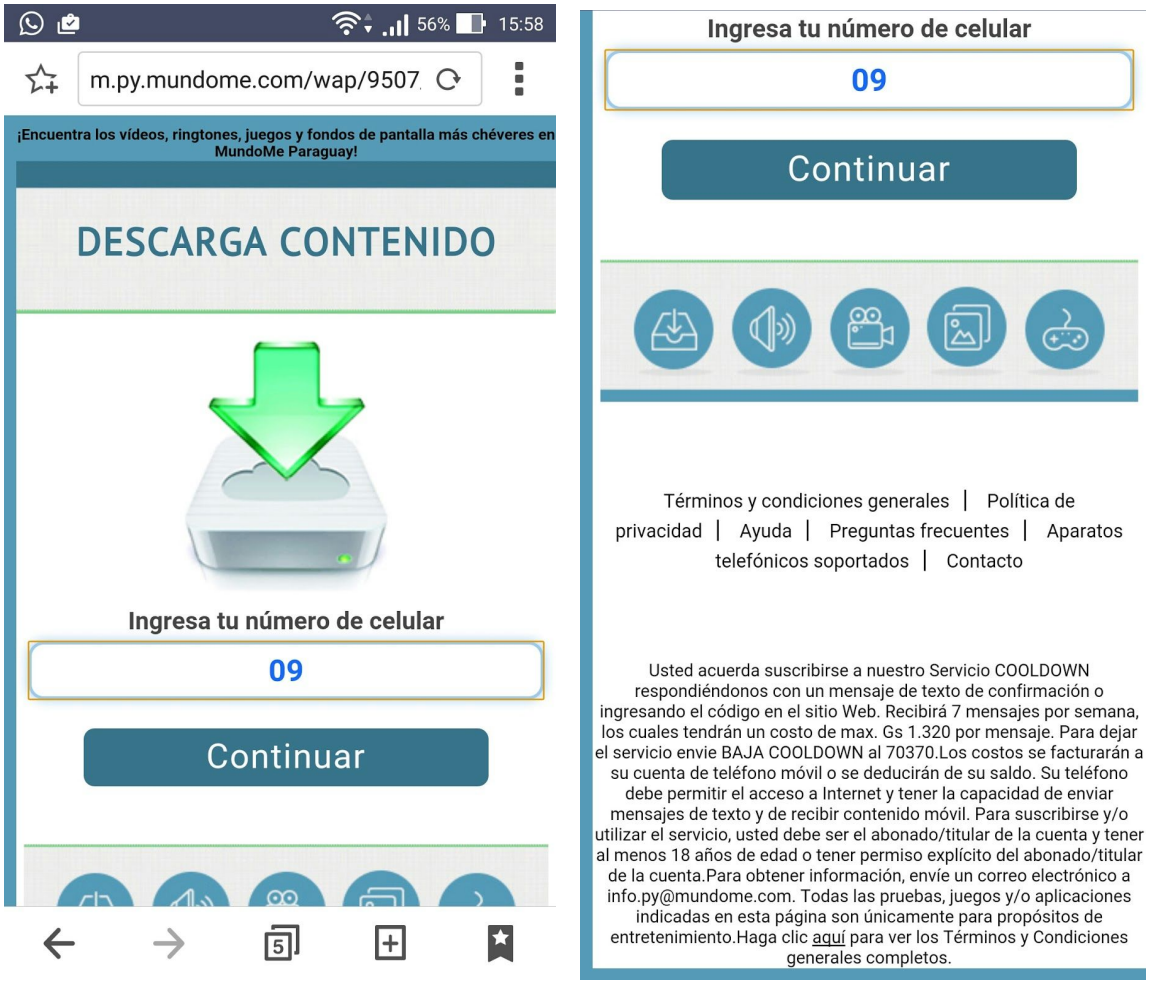


Figura 3: Página de suscripción a servicios de SMS premium

Impacto:

Al ingresar en los enlaces de los comentarios falso desde dispositivos Android, la víctima podrá quedar infectada con diferentes variantes de malware, con consecuencias diferentes para cada una de ellas. En la mayoría de los casos, podrá percibir uno o más de los siguientes síntomas:

- aumento en su consumo de ancho de banda, especialmente si utiliza la red de datos. Con esto, el saldo de navegación durará menos de lo estimado.
- disminución en la duración de la batería
- calentamiento anormal y constante del dispositivo
- lentitud, bloqueo, fallos y/o reinicio del dispositivo o de otras aplicaciones

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

Las aplicaciones maliciosas podrían robar información confidencial, tales como credenciales almacenadas en el teléfono (correo, redes sociales, bancarias, etc.) , contactos, IMEI, etc. Además, podrían instalar código malicioso adicional.

Solución:

En caso de haber ingresado a algún enlace dudoso y/o haber instalado una aplicación dudosa, se recomienda analizar el dispositivo con alguna herramienta de seguridad (*antivirus*, *antimalwar***e**, etc.) para Android. La gran mayoría de las aplicaciones maliciosas analizadas, son reconocidas como malware por la mayoría de los antivirus.

Existen diversas herramientas, gratuitas y de pago, las cuales pueden ser encontradas en las *App Stores* oficiales, algunas de las cuales son (orden alfabético):

- avast! Mobile Security & Antivirus
- AVG Antivirus
- Avira Antivirus Security
- Bitdefender Antivirus Free
- CM Security
- ESET Mobile Security
- Kaspersky
- Norton Antivirus y Seguridad
- McAfee Mobile Security
- NQ Mobile Security
- Sophos Free Antivirus and Security

Prevención:

Se recomienda no ingresar nunca en enlaces no solicitados o dudosos.

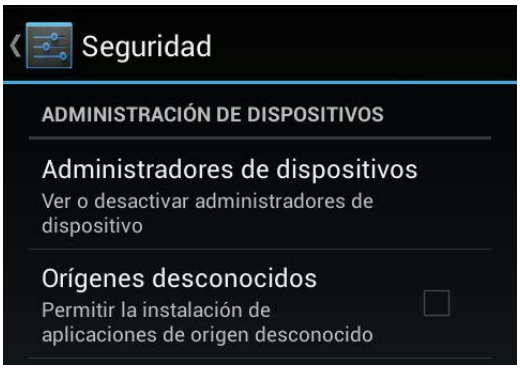
Además, no se recomienda descargar aplicaciones de fuentes que no sean los *App Stores* oficiales. Por defecto, la gran mayoría de dispositivos traen deshabilitado el permiso de instalar aplicaciones provenientes de fuentes desconocidas. Recomendamos no modificar esta configuración, de modo a prevenir que una aplicación maliciosa pueda ser instalada en nuestro móvil.

En el caso de Android, para verificar el estado de este permiso en su teléfono:

1. Ir a Ajustes > Seguridad
2. Vaya a la sección “Fuentes desconocidas”

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

3. La opción “Permitir la instalación de aplicaciones provenientes de fuentes desconocidas” debe estar desmarcada, como se observa en la imagen:



La gran mayoría de las aplicaciones maliciosas analizadas, son reconocidas como malware por la mayoría de los antivirus. Es por eso que se recomienda utilizar antivirus u otras herramientas de seguridad en los smartphones y tablets. Existen diversas herramientas, gratuitas y de pago, las cuales pueden ser encontradas en las *App Stores* oficiales.

Es importante tener en cuenta que, a la hora de descargar una herramienta de seguridad de las *App Stores*, se debe verificar que la misma provenga de una fuente oficial y de fabricantes de reconocida reputación. Ante la duda, recomendamos siempre consultar los sitios web y/o foros oficiales.

Información adicional:

http://www.welivesecurity.com/2015/07/23/porn-clicker-keeps-infecting-apps-on-google-play/
http://www.welivesecurity.com/la-es/2011/08/25/gingermaster-malware-en-android-2-3/
http://www.redeszone.net/2015/11/28/la-tematica-preferida-para-ocultar-malware-para-android-es-la-pornografia/
http://www.welivesecurity.com/la-es/infographics/malware-para-android/

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py