BOLETÍN DE ALERTA

Boletín Nro.: 2015-03
Fecha de publicación: 27/03/2015
Tema: Campaña de Malware a través de falsa aplicación de Whatsapp Call

Descripción:
Desde ayer está disponible la funcionalidad de llamadas desde la aplicación de Whatsapp en la región, para ciertos dispositivos y operadoras, principalmente Android.Para poder acceder a la funcionalidad, se debe tener la aplicación WhatsApp actualizada al menos a la versión v2.11.561 (la última versión disponible es v2.12.14.).

Para activarla, alguien que ya tiene la función de llamadas de voz WhatsApp habilitado debe llamarle. Una vez que contesta la llamada, aparecerán tres pestañas en la parte superior de la interfaz de WhatsApp: llamadas, chats y contactos; con lo cual las llamadas de voz se habrán activado.
Sin embargo, esta funcionalidad no funcionará todavía para todos los dispositivos. La funcionalidad no se encuentra todavía disponible para iOS, según lo anunció la compañía en la Conferencia F8 de Desarrolladores de Facebook.

La nueva funcionalidad ha sido anunciada ya hace varios meses y ha estado en fase de prueba en diversos países.

Esta situación ha generado expectativas que han sido aprovechadas por delincuentes para impulsar campañas de distribución de malware utilizando falsos anuncios o invitaciones para obtener la funcionalidad de Whatsapp Call.

El día de ayer se han viralizado numerosos mensajes que circulan en Whatsapp que invitan a ingresar a un enlace, reenviar la invitación a una cierta cantidad de contactos y luego instalar una aplicación maliciosa.

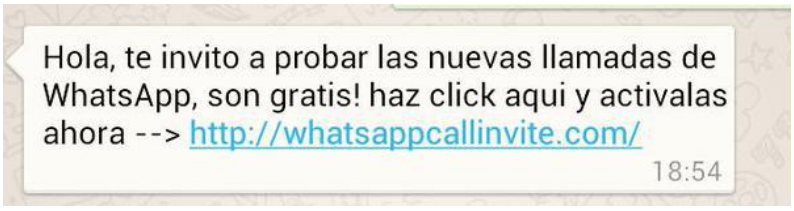


Fig. 1: Ejemplo de un mensaje malicioso

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

Los enlaces dirigen a diversas aplicaciones maliciosas y/o indeseadas, entre ellas: SpeedyPhone, BadaBeeSMS, etc.
Algunos de los enlaces maliciosos observados son:

- whatsappcallinvite.com
- whatsappsite.com
- whatsappcallmzzhost.com

Impacto:
Las aplicaciones maliciosas pueden robar datos sensibles tales como credenciales bancarias, información de contactos, registros de llamadas, fotos, contraseñas, entre otras cosas.

Algunas de las aplicaciones pueden corromper el dispositivo, pudiendo dejarlo inservible.

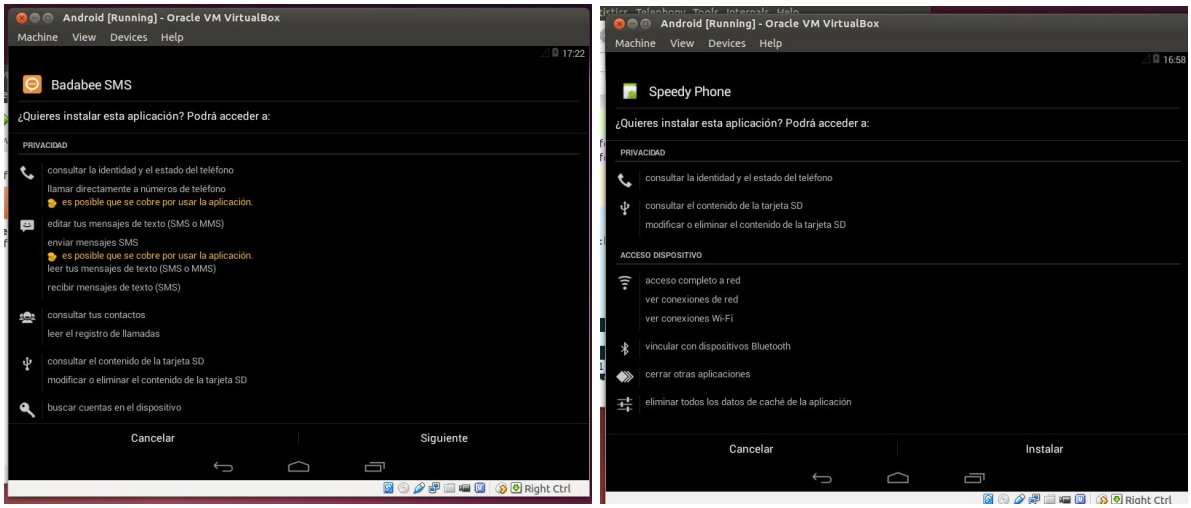


Fig. 2: Ejemplo de los permisos solicitados por las aplicaciones

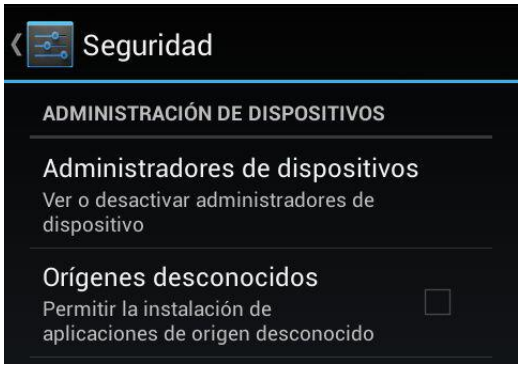
Mitigación:
Se recomienda no ingresar en enlaces no solicitados o dudosos.

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 no permitir que una aplicación maliciosa pueda ser instalada en nuestro móvil.

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

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



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.

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