Malware por medio de WhatsApp

INTRODUCCIÓN

WhatsApp es una aplicación que permite comunicarnos diariamente con familiares, amigos, compañeros de trabajo e incluso para contactar empresas. La aplicación se ha vuelto bastante popular alrededor del mundo dada la facilidad para compartir una gran variedad de información como fotos, videos, enlaces, archivos, etc., por medio de mensajes que son recibidos al instante en los dispositivos móviles.

Es común recibir una gran cantidad mensajes al día, incluso de quienes no están en la lista de contactos, dando a los atacantes una excelente oportunidad de usar estos mismos mensajes para compartir malware, infectar dispositivos y tener acceso a la información de los mismos.

METODOS DE ATAQUE

Phishing: es un ataque que persiste y es aún más eficaz su distribución por medio de esta red social. Consiste en mensajes que contienen enlaces a sitios externos que suplantan la identidad de alguna entidad o sitio de confianza, en los que se solicita ingresar credenciales para validar la cuenta, desbloquearla, actualizar la versión de la aplicación, o incluso reclamar un regalo. Dado que en WhatsApp al enviar un enlace a una página web muestra una imagen miniatura con el contenido del sitio, en primera instancia se podría observar que el sitio es legítimo ya que se parece mucho al original dando la confianza al destinario de ingresar al enlace recibido. Sin embargo, es un claro intento de robar nuestras credenciales de acceso una vez que ingresemos al sitio falso o de redirigirnos a la descarga de malware.

Imágenes Gif: Recibir imágenes gif mediante mensajes es una de las cosas que más llaman la atención revisar al recibir un mensaje, es por eso que no pasa por desapercibido tampoco para los atacantes y pueden incluir en los ellos malware que se instala en el teléfono después de abrir dicha imagen o GIF, dando acceso al dispositivo para grabar vídeo o audio, debido a una vulnerabilidad detectada en ciertas versiones de WhatsApp para Android el pasado octubre del 2019.

Videos: Igualmente, en noviembre del 2019, la compañía perteneciente Facebook reportó que se había encontrado una vulnerabilidad que permitía incluir código malicioso en archivos de video MP4. En este caso se veían afectados tanto usuario Android y iOS.

Archivos: Mediante archivos PDF, Word o Excel maliciosos que pueden obtener datos personales, credenciales de acceso de cuentas bancarias y números de PIN.

VERIFICACIÓN

Validar que la versión de WhatsApp que se tenga instalada sea 2.19.274 o superior en el caso de Android y para iOS 2.19.100 o superior de acuerdo al anuncio de seguridad publicado por la misma aplicación.

La principal recomendación es mantener actualizada la aplicación y descargarla desde sitios seguros como Play Store para dispositivos Android o App Store para dispositivos iOS y en la página oficial de la aplicación.

Para validar que versión de WhatsApp está instalada:

- Abrir WhatsApp
- Tocar el icono de los **tres puntos**.
- Seleccionar **Ajustes**
- Ir a **Ayuda**
- Seleccionar **Info. de la aplicación**
- Se mostrará la versión instalada

La forma segura de actualizar la aplicación, sin descargar otra actualización falsa que haya sido subida por algún atacante, es la siguiente:

PLAY STORE	APP STORE
• Ingresar a Play Store • Ir a Mis Apps y juegos • Revisar el apartado de Actualizaciones • Buscar en la lista de Actualizaciones disponibles para WhatsApp • Seleccionar en la columna a la derecha la opción Actualizar.	• Abrir App Store • Tocar Hoy en la parte inferior de la pantalla. • Tocar ícono de perfil en la parte superior de la pantalla. • Desplazarse hacia abajo para ver las actualizaciones pendientes y las notas de la versión. • Tocar Actualizar junto a una app para que solo se actualice esa app, o toca Actualizar todas.

RECOMENDACIÓN

WhatsApp en su página oficial nos da recomendaciones para no caer en estos ataques y poner especial atención a los mensajes que reciben con las siguientes características:

- El mensaje tiene faltas de ortografía o errores gramaticales.
- Se pide que abras un enlace.
- El remitente dice que representa a WhatsApp.
- Se solicita que compartas información personal (p. ej. números de tarjetas de crédito o de cuentas bancarias, fecha de nacimiento, contraseñas, etc.).
- Se pide que reenvíes el mensaje.
- El mensaje dice que podrás evitar una penalización, como el bloqueo de tu cuenta, si lo reenvías.
- El mensaje te promete un regalo de WhatsApp o de otra persona.
- El mensaje dice que, si abres un enlace, se activará una función nueva.
- Se indica que debes pagar por el uso de WhatsApp (WhatsApp es una aplicación gratuita).

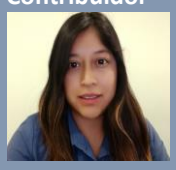
No se debe abrir ningún mensaje con estas características de un remitente desconocido, una vez recibido, lo más seguro es borrar el mensaje y no abrir ningún enlace ni enviar información personal.

Igualmente instalar un antivirus nos protegerá de aplicaciones maliciosas y de actividades que realicen las mismas en nuestros dispositivos.

FUENTE DE REFERENCIA

- https://faq.whatsapp.com/en/general/28030005?lang=es
- https://www.facebook.com/security/advisories/cve-2019-11931
- https://faq.whatsapp.com/21197244/?lang=es

Contribuidor



Nayely Morales Perales: Ingeniera en Computación. Egresada de la Facultad de Ingeniería de la UNAM (México). Interesada en informática forense, respuesta a incidentes, así como en la prevención de incidentes de seguridad.

LinkedIn: mx.linkedin.com/in/nayely-morales-perales-1454a247

Recursos LCW

LinkedIn	https://www.linkedin.com/company/cysecbywomen/
Facebook	https://www.facebook.com/CySecByWomen/
Twitter	@cysecbywomen