[Forense] Análisis forense de Whatsapp

Directorios

Whatsapp almacena sus datos en varios directiorios como el almacenamiento externo:

- /android/media/com.whatsapp/whatsapp
- /WhatsApp
- /sdcard/WhatsApp/

Almacenamiento interno (Root Necesario):

- /data/data/com.whatsapp/
- /data/app/com.whatsapp-d.apk

Archivos

Artefacto	**Ubicación**	**Archivo**
Clave de cifrado	/data/data/com.whatsapp/files	key
BBDD Contactos	/data/data/com.whatsapp/databases	wa.db
BBDD chats	/data/data/com.whatsapp/databases	msgstore.db
Backups BBDD chats (AES 256)	/mnt/sdcard/Whatsapp/Databaeses	msgstore.db.cryptxx

Chats Cifrados

Se encuentran en una cota privadas, mientras que sus backups están en zona pública. Dependiendo de la versión de whatsapp puede ir cifrado con un algoritmo u otro. Pueden ser extraidos mediante el uso de adb pull

Clave de Cifrado

La clave de cifrado se almacena en el archivo key localizado en el almacenamiento interno, por lo que se necesita acceso root para poder acceder a ella. De todas formas existe un método para extraerla sin ser root mediante el downgrade de la APK:

1. Se borra la APK de Whatsapp
2. Se instala una versión antigua con vulnerabilidades
3. Se accede al contenido del fichero key
4. Se vuelve a instalar la versión original de whatsapp