# Mobile Implants

In March 7-th 1876, an outstanding american scientist inventor Alexander Bell received a patent for the invention of the phone. Apart from  him, a lot of other engineers also worked on the idea of voice transmission at a distance. Inventions developed rapidly. Telephone communication capabilities are growing steadily. The progress has advanced so far that nowadays using telephone communication we have the opportunity to stay in touch anywhere in the world in 24/7 mode.

Almost everyone has a mobile phone. It is a complex technical device that can handle multiple tasks and greatly facilitates our lives.With the development of the mobiles phones, a malware has also improved.There are companies that provide the necessary malware components as well as training operators of these systems.

Any modern mobile device has at least a microphone and speaker, access to the Internet as well as a camera and GPS navigation.Some devices also have a front camera for video calls.All these things the attackers successfully use to collect information about the owner of the device.

Mobile implants:The name "implant" was not invented by security experts. This name was given by the hackers.Let's look at an example of a malware program: BackdoorAndroidOS.Kresok (md5 39be87178c84d4afd07a80323a1d4b91) for Android from FlexiSpy.

For example, we can see how to activate remotely the microphone for sound recording.

```
                .byte 0x24 # $
aLcomVvtCapture:.string "Lcom/vvt/capture/audio/AudioCapture;",0
                                        # DATA XREF: METHODS:_def_AudioCapture__clinit_@V↑i
                                        # METHODS:_def_AudioCapture__init_@VLLLL↑i ...
                                        # String #10205 (0x27dd)
```

It is not a problem for them to know the location of the victim using the GPS locator function. The attackers get access to the phonebook  and also to the files stored on the victim's device. They have the ability to read SMS messages and view the call history.

## Encryption and mobile implants

Not so long ago, in mobile messengers, the use of point-to-point encryption began.Such a cryptographic protocol provides for encryption of messages on the sender's device and decryption of messages on the recipient's device.This protocol is a fairly reliable solution the transmission of information.Was the method "point to point" encryption a solution of all problems of confidence? Unfortunately, no.Attackers gain an access to the messages before they are encrypted and sent.

The screenshots below show the example how hackers gaining an access to some popular messengers.

The screenshot shows how the implant tries to access the messages in the telegram.

```
                .byte 0x36 # 6
asc_3B7DB8:     .string "Lcom/vvt/capture/telegram/internal/MessagesController;",0
                                        # DATA XREF: METHODS:_def_MessagesController__init_@V↑i
                                        # String #10683 (0x29bb)
                .byte 0x36 # 6
asc_3B7DF0:     .string "Lcom/vvt/capture/telegram/internal/NativeByteBuffer$1;",0
                                        # DATA XREF: METHODS:_def_NativeByteBuffer$1__init_@V↑i
                                        # METHODS:_def_NativeByteBuffer$1_initialValue@L↑i ...
                                        # String #10684 (0x29bc)
```

The following screenshot shows how the implant accesses messages in WeChat.

```
                .byte    8
aMicromsg:      .string "MicroMsg",0    # DATA XREF: WeChatCapturingHelper__clinit_@V+42↑r
                                        # WeChatCapturingHelper_getAllPossibleMsgFolderPaths@L+2A↑r ...
                                        # String #14541 (0x38cd)
```

Attackers are also interested in the applications WhatssApp,Viber and etc.

Voice communication through messengers has long become very popular.Attackers are interested in the victim's talks through popular means of communication such as Line, Skype.Below are a short code in which there is a trespass interception of the Voip calls E-mail is also interesting for attackers.

The screenshot shows the code that provides access to calls via Skype.

```
                .byte 0x2E # .
aLcomVvtVoip_22:.string "Lcom/vvt/voipcapture/skype/SkypeVoipCapture$1;",0 # String #12742 (0x31c6)
                .byte 0x37 # 7
aLcomVvtVoip_23:.string "Lcom/vvt/voipcapture/skype/SkypeVoipCapture$CopyResult;",0
                                        # DATA XREF: METHODS:_def_SkypeVoipCapture$CopyResult__init_@VLTi
                                        # METHODS:_def_SkypeVoipCapture$CopyResult__init_@VLLTi
                                        # String #12743 (0x31c7)
                .byte 0x2C # ,
aLcomVvtVoip_24:.string "Lcom/vvt/voipcapture/skype/SkypeVoipCapture;",0
                                        # DATA XREF: METHODS:_def_SkypeVoipCapture__clinit_@VTi
                                        # METHODS:_def_SkypeVoipCapture__init_@VLLLLTi ...
                                        # String #12744 (0x31c8)
```

The Line Messenger is very popular today.The Implant intercepts calls made through it.

```
                .string ";",0           # String #12737 (0x31c1)
                .byte 0x2A # *
aLcomVvtVoip_18:.string "Lcom/vvt/voipcapture/line/LineVoipCapture;",0
                                        # DATA XREF: METHODS:_def_LineVoipCapture__clinit_@VTi
                                        # METHODS:_def_LineVoipCapture__init_@VLLLLTi ...
                                        # String #12738 (0x31c2)
```

E-mail is also interesting for attackers.The screenshot shows the code that receives the data of the client Gmail.

```
                .string ";",0           # String #11678 (0x2d9e)
                .byte 0x3A # :
aLcomVvtData_13:.string "Lcom/vvt/database/monitor/gmail/GmailDatabaseObserverData;",0
                                        # DATA XREF: METHODS:_def_GmailDatabaseObserverData__init_@VTi
                                        # METHODS:_def_GmailDatabaseObserverData_getDatabasePackagePath@LTi ...
                                        # String #11679 (0x2d9f)
                .byte 0x2B # +
aLcomVvtData_14:.string "Lcom/vvt/database/monitor/gmail/GmailUtils;",0
                                        # DATA XREF: METHODS:_def_GmailUtils__init_@VTi
                                        # METHODS:_def_GmailUtils_getDatabaseFilePath@LLTi
                                        # String #11680 (0x2da0)
```

In fact, it is not important what messenger you use. Rather, it is important how much the attacker is interested in you.

There are several tips that will help you avoid infection with mobile implants.

1.You need to install really good antivirus software.
2.Do not charge the electronic device from the computer.
3.If you often maintain confidential correspondence, use only those messengers that do not save the message archive and metadata and also use point-to-point encryption.
4.If possible, try to use different messengers to communicate

Please do not forget: safety first!

Dmitriy Melikov Independent researcher
https://twitter.com/DmitriyMelikov
melikov.dima.dm@protonmail.com

Germany 2017