Antiy Labs

Analysis on Android Spyware

Antiy Labs

Contents

Background

With the portable feature, intelligence terminals like mobile phone combine such privacy information as the user's current location, contacts, and the communication record in one. Based on such feature, some applications have developed the functions of tracking and information monitoring to satisfy the need to track and protect children and the old as well as to carry out business tracking. Proceeding from traditional spy requirement, some developers have designed related privacy-stealing functions to meet people's curiosity and monitoring psychology. These behaviors, hidden or practical, all have certain spy functions.

Here, based on common software behaviors on Android system, we make a summary and appreciation on widespread softwares with related functions or abilities in order to enhance our security awareness on spyware as well as to call for the use of these applications for proper purpose.

Due to the difference in national laws and regulations, the identification extent and standard on spyware varies from one to another. Therefore, related introduction in this paper does not involve the judgment on whether it is malicious or not.

Typical Case

jxAgent

jxAgent is a spyware developed by jxsoftware. When the software is installed to a mobile phone, by concealing its icon, it can initiate itself in the background to steal and send the communication record, messages and other privacy content to a specified phone number via message. At the same time, the communication between the monitored phone and the specified phone number is automatically recorded and uploaded to a specified website, which results in the leaking of privacy.

When the software is installed, once the phone is restarted or receives a message, the software will start its background service to receive the message command from the remote server and execute the corresponded privacy operations.

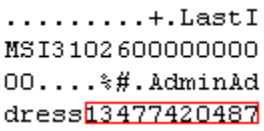
The Setting of Master Phone Number

Set the mater phone number as 13477420487(testing number) and the message sent to the infected phone as 0#.

10-02 00:51:5...	E	52	@Antiy_...	@Antiy_Dynamic_Log@SMSSF jxsoftware.AndroidAgent
10-02 00:51:5...	E	229	@Antiy_...	@Antiy_Dynamic_Log@SMSSEND 13477420487;;命令执行成功! 版本:1.0
10-02 00:51:5...	E	52	@Antiy_...	@Antiy_Dynamic_Log@SMSINTERCEPT Intent { act=android.provider.Telephon...

Intercepting Message and Set the Master Phone Number

When the phone receives a message with the beginning of 0# and sends a reply, the software will set the phone number as the master one and writes it into MyDB——the datebase of the software.



Storing the Master Phone Number in Database

Stealing Message

Thereafter, if there are other phone numbers sending messages to the infected phone, all these messages will be sent to the master phone number to steal the user's privacy.

10-02 00:59:1...	E	52	@Antiy_...	@Antiy_Dynamic_Log@SMSINTERCEPT Intent { act=android.provider.Telephon...
10-02 01:21:1...	E	52	@Antiy_...	@Antiy_Dynamic_Log@SMSSF jxsoftware.AndroidAgent
10-02 01:21:1...	E	229	@Antiy_...	@Antiy_Dynamic_Log@SMSSEND 13477420487;;1234<<13477420485

StealingMessage

Stealing Location Information

When the master phone number is used to send message with the content of 8# to the infected phone, the software will reply it in background and the reply will include the infected phone's CELLID of the base station, thus leaking the user location.

10-10 11:12:5...	E	165	@Antiy_...	@Antiy_Dynamic_Log@SMSSEND 13477420487;;LAC:-1 CellID:-1

Stealing Location Information

Stealing Contacts

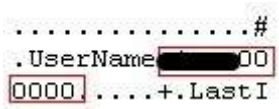
When the master phone number is used to send message with the content of 10# to the infected phone, the infected phone's reply which is sent by the software in the background will include all the contacts information in it.

10-10 11:46:1...	E	228	@Antiy_Dyn@	@Antiy_Dynamic_Log@SMSSEND 13477420487;;As A: 21111111

Stealing Contacts

Communication Recording

Send the account of 18# to the phone (testing account ***000000, already registered in www.mobilelogger.net). When the infected phone receives the command of 18#***000000, the software will record it as the master account in the database of the software.



Storing the Master Account in Database

The communication will also be recorded and sent to www.loongware.comwhich belongs to the same server with www.mobilelogger.com.

The upload link is http://www.loongware.com/ml/manager/upload.php.

The Network Package to Upload Records

The controller can enter www.mobilelogger.net with the account in which it is shown that the infected phone has uploaded the communication record.

Looking over the Stolen Privacy in the Background Server

Pdaspy

When Pdaspy is installed, the controller has to register an account to make the corresponding configuration of the software in the infected phone. When the phone is restarted, its icon will be concealed and keep running in the background to steal various privacy information of the user such as messages, contacts and location. The controller can monitor the privacy information by registering an account in related website.

The icon of the installed program:

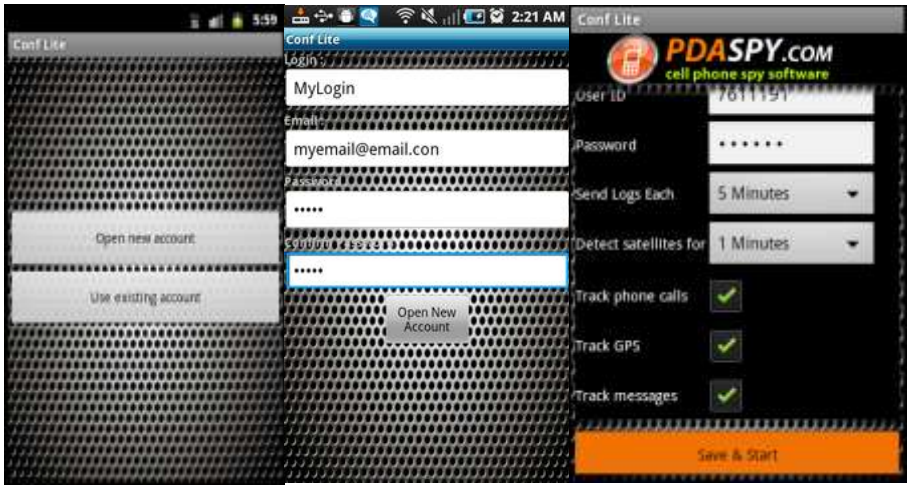
The Coin of the Virus Program

The running of the program needs a password.

```
if ((!localEditText.getText().toString().equals("passcode123")) &&
   (!localEditText.getText().toString().equals("Passcode123")) &&
   (!localEditText.getText().toString().equals("Passcode123")) &&
   (!localEditText.getText().toString().equals("passcode 123")))
```

The Interface of the Program

The interface can be entered by any one of the four passwords to create an account and set the content and cycle to monitor. The content can be the communication records, the message records, location and so on.



The Configuration Interface of the Privacy Stealing Program

The application can generate a configuration file to record information set by the user:

```
<int value="5" name="pollInterval"/>
<long value="0" name="callIndex"/>
<int value="1" name="detectSattelitesFor"/>
<boolean value="true" name="callLogging"/>
<long value="0" name="msgOutboxIndex"/>
<string name="userId">7611191</string>
<boolean value="true" name="gpsLogging"/>
<boolean value="true" name="smsLogging"/>
<long value="1" name="msgInboxIndex"/>
<string name="password">222222</string>
```

The Setting Record of the Controller

The user mailbox will receive an email:

The Controller Mailbox Receiving Email from the Background Server

If the client is logged in according to the email, the presentation of various information can be seen. The testing message has also been uploaded to the server.

Looking over the Stolen Information in the Background Server

Classification and Summary

Name	Control Channel	Threats	Description
52loc	Web	High	No icon after being installed. The software initiates its service when the user makes a calling, changes the time, sets new time zone, restarts the system, changes the phone state, installs or uninstalls a package and keeps getting the user's GPS

			information and uploads the location to a specified server to leak the user's privacy.
Xwodi	Web	High	No interface at all. Icon disguises as flash. It may record communication, invoke the camera to photograph, steal location information and upload the information to a specified server.
jxAgent	SMS	High	This spyware disguises its icon after being installed and initiates itself in the background to steal the communication records, messages and uploads the information to a specified phone number by message. Meanwhile, the communication between the monitored phone and the specified phone number can be automatically recorded and uploaded to a specified website to leak the user privacy.
Pdaspy	Web	High	This spyware can upload messages, the communication records, the GPS information to a specified server to leak the user's privacy.
Zbot	SMS	High	Disguise as mobile security software and receive remote control command to initiate or stop itself. It can pick up the account number from messages and cooperate with Zeus to steal the user's account information.
MobiStealth	Web	High	This monitor software conceals its icon after being installed. It can monitor messages and other operations and upload the information to the background server. The information can be looked over by logging in the management platform of the server.
Cheatact	SMS	High	This spyware disguises as a browser. By collocating a phone number when it runs in the first time, all messages will be sent to the number. Afterwards the configuration interface will not reveal itself and runs in the background to leak the user's privacy.
Fakeview	Web	High	This spyware has no icon after being installed and disguises as an image viewer. It can upload messages and the communication records to a remote server. The monitor can look over the user's privacy by logging in the remote server.
Gambler	Web	High	No icon after being installed. The configuration interface will pop up after the phone restarts. Afterwards, it can send the messages, the communication records and the location

			information to a specified email address to leak the user's privacy.
wdspy	SMS or Web	High	This spyware has no icon after being installed and initiates itself after the phone starts. It can monitor messages and take remote control by message commands. It has the functions of location tracking, communication recording, message-looking and contacts-looking. The information can be uploaded to the server to leak the user's privacy.
Inspector	Web	High	The software has no icon after being installed and disguises as a google map. It can initiate itself after the phone starts to monitor the phone state and upload the user's privacy. The software has the following functions: communication recording, message transmitting, information uploading, environment recording, location tracking, mandatory alarm and card-changing prompt.
Lurker	SMS	High	The software has no icon after being installed. Any other phone can send a command to take remote control of it. It can steal messages, the communication records, contacts, GPS location and other privacy.
Mobilespy	Web	High	The software has no icon after installed. It can initiate itself after the phone restarts. It can monitor the communication records, messages, the web-browsing records, image bank and other information. It can track the user's location by GPS and upload the information to a specified website.
Smstracker	Web	High	The software has no icon after installed. It will invoke the register interface after the phone restarts in the first time and collect the phone's hardware information. In addition, when the sdk version of the phone is lower than 9, the register interface can also be invoked by dialing ##070476 to realize multiple-account bonding. Afterwards, privacy information like short messages, multimedia messages, the communication records, the browser, the GPS-recorded information will be uploaded to a remote server. The monitor can look over the information by logging the account. The function of upgrading and tracking by paying fee can monitor the GPS location and the multimedia messages.
Nickispy	SMS or	High	This spyware has no icon after installed. It can

	Web		initiate itself after the phone starts. It can take remote control by message commands. It has the functions of communication recording, environment recording, message-looking and contacts-looking and sends these records by email to leak the user's privacy.
anfospy	SMS	High	The software has no icon after being installed. When the phone receives a message with "anforen" as beginning, it can initiate the background service and set the phone number as the master one. Afterwards, it sends the user's location in messages to leak the user's privacy.
babyjc	SMS	High	This spyware has no icon after being installed and disguises as a system program. It can initiate itself after the phone starts and upload the communication records, GPS location, messages, monitor inbox, delete the specified messages and get malicious commands by messages to leak the user's privacy.
UnfairWare	Web	High	This spyware initiates itself by force after the phone starts. It can monitor the communication records, messages and upload the information to the remote server to leak the user's privacy.
spitmo	Web	High	The software is PC-derived. When the computer is infected, there is a pop-up to set up APK and dial 325000. Then the program automatically stops dialing and pops up 251340 with the form of Toast. When the infected PC visits an online bank page, the message received will be uploaded to the server in the form of HTTP.
spybubble	Web	High	This spyware has no icon after installed. It can initiate itself and upload the communication records, messages, the web-browsing records and other privacy information to the specified server.
SpyHasb	Web	High	This spyware can conceal its icon after registering and get the user messages, contacts, location and other privacy information.
Spyoo	Web	High	This spyware can collect the GPS location, the communication records, the message records, the website bookmarks and other privacy information.
spytrack	Web	High	This spyware is used to monitor and upload the user's location to spysat. The monitor looks over the information by a specified account.

Ssmsp	Web	High	The software has an icon after being installed. It initiates itself after the phone starts. It can monitor the inbox, read the messages and upload to the remote server.
guggespy	Web	Middle	This spyware can be used after being registered. An artificial configuration can be made to change the icon and move the program to the system file folder. The software disguises as the system program to collect and send the user's messages and the communication records to a specified mailbox. The flooding of the software may cause severe leak of the user privacy.
GPSSpy	Web	Middle	GPSspy is a set of spyware including the main control client--GPS Spy Plus and the controlled client--GPS Spy Tracker. When the controlled client is set up, the location-changing information will be sent to the remote server.
SmsWatcher	SMS	Middle	The software, by setting a message-transmitting list, can transmit all the messages and contacts (not including those from the numbers in the message-transmitting list and the white list) to a specified number. When the software is upgraded to the professional version, it can conceal its icon.
phonespy	SMS	Middle	A number can be set up in the interface. The privacy information will be sent to the number.
SmForw	SMS	Middle	The software can monitor messages and send them to a specified number.
SmsSpy	Web	Middle	This application disguises as a normal tax calculator and uploads messages. It can stop its process and make it difficult for user to find its behavior.
Unispy	SMS	Middle	This spyware can monitor messages and receive message commands from control client to make callings to a specified phone number.
KidLogger	Web	Middle	This monitor software is designed for parents and has no icon. By dialing *123456# in local, the configuration interface will pop up. It can upload POWER OFF & ON records, the communication records, the flight model information, the inbox contents, the clipboard contents, WiFi and GSM connecting state, USB and SD state, the running programs, the Activity information, the website visiting records, the keyboard records and other privacy information.

LifeMon	Web	Middle	This software is a classical spyware designed by Lifemonitor and has no icon after being installed. It can steal and upload location information, messages and other privacy information. By dialing 222, the configuration interface can be invoked.
LMaxi	SMS	Middle	This anti-thief software has no icon after being installed. The configuration interface can be invoked by dialing a specified command. The software can realize the following functions by remote message command: sound an alarm, lock the phone when the card is changed, lock the application settings, restore the factory settings, lock the applications already set in the phone, clear the data (contacts, the communication record, short messages, multimedia messages and data in the SD card), get messages, contacts, the communication records, location and other information to the specified mailbox. It can also make a call to the specified number with no user intervention.
CerbDog	Web or SMS	Low	This anti-thief software is a comprehensive and powerful one. It can control the phone through the Internet or messages. It can realize the following functions by remote control: get the location information, track, lock and open the screen, sound an alarm, get the communication records, messages, make a calling, send messages, get the recorded communication, get images, videos, capture screen, conceal the icon, restart the phone and delete the data in the phone.
TheftAware	SMS	Low	This anti-thief software, by receiving remote message commands, can upload privacy information including messages, contacts, location, and card-changing records. By remote control, it can lock the stolen phone, make the phone sound an alarm, make a calling, delete the communication records and lock other normal functions of the phone. The software can choose to uninstall the installed programs and conceal its icon.
FoCobers	SMS	Low	This is anti-thief software. It can receive remote commands in messages to delete data, send location information, and lock the screen and so on. The software is a risk to the user.

Summary

From the perspective of control channel, Android spywares mainly control through web and SMS. Some even design strict instruction format, run in the background, and disguise as other software. It is difficult for common users to identify them.

From the perspective of technology, there is no lack of elaborate software. With meticulous technique, each shows its special prowess which may do harm to the controlled user.

About Antiy Labs

Antiy Labs is an antivirus vendor which makes advanced research and technology contributions to the field. Currently, there are tens of thousands of firewalls, UTM and security devices deployed with our antivirus engine. More information is available at www.antiy.net.

Antiy Labs