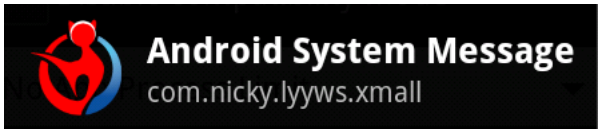
Analiza sample5.apk – Laborator 12

1. **Numele aplicatiei**

   Daca ne uitam la resursele aplicatiei, in *res/values/strings.xml,* putem vedea ca numele aplicatiei este Android System Message.

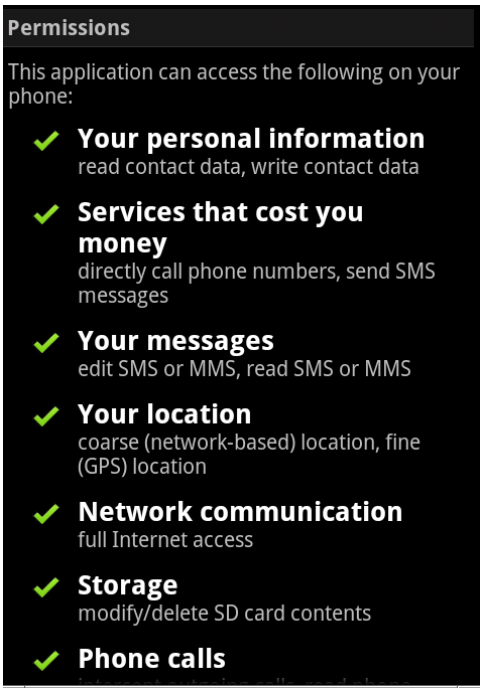
   <string name="app_name"> **Android System Message** </string>

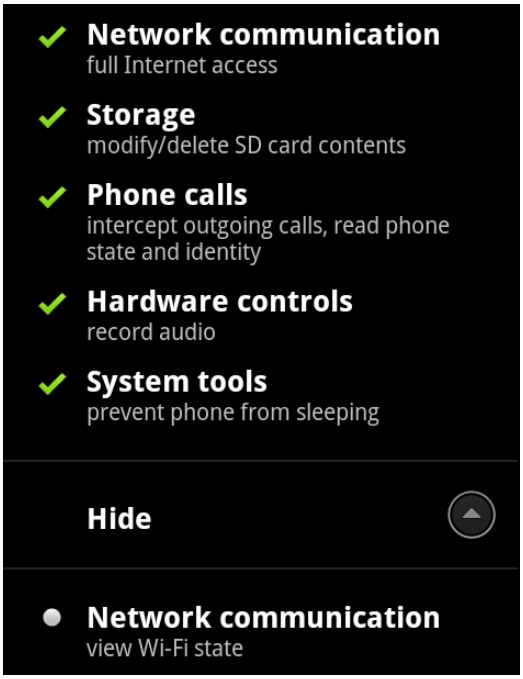


   In *AndroidManifest.xml* se poate vedea ca numele pachetului este ***com.nicky.lyyws.xmall***.

2. **Manifestul aplicatiei** (Fisierul AndroidManifest.xml):
   Aplicatia are nevoie de urmatoarele permisiuni:

   android.permission.**CALL_PHONE**->apeleaza direct numarele de telefon
   android.permission.**PROCESS_OUTGOING_CALLS**->intercepteaza apelurile facute
   android.permission.**INTERNET**->acces complet la Internet
   android.permission.ACCESS_GPS
   android.permission.**ACCESS_COARSE_LOCATION**->localizare aproximata
   android.permission.ACCESS_COARSE_UPDATES
   android.permission.**ACCESS_FINE_LOCATION->**localizare precisa cu GPS
   android.permission.**READ_PHONE_STATE**->citeste starea telefonului si identitatea
   android.permission.**READ_CONTACTS**->citirea listei de contacte
   android.permission.**WRITE_CONTACTS**->scrie datele de contact
   android.permission.ACCESS_WIFI_STATE->acces la informatii despre Wi-Fi.
   android.permission.PERMISSION_NAME
   android.permission.**SEND_SMS->** permite trimiterea de SMS-URI sau MMS-uri
   android.permission.**READ_SMS**->permite citirea de SMS-URI sau MMS-uri
   android.permission.**WRITE_SMS**-> permite editarea de SMS-URI sau MMS-uri
   android.permission.**WAKE_LOCK->**folosind PowerManager WakeLocks sa tina procesorul „treaz” sau ecranul luminos.
   android.permission.**RECORD_AUDIO->**inregistrare audio
   android.permission.WRITE_EXTERNAL_STORAGE->modificare/stergere continut card SD
   android.permission.DEVICE_POWER->inchidere/deschidere telefon





Numele aplicatiei da o impresie buna despre aplicatie, insa e vorba de un malware (trojan) care strange informatii de pe device si apoi le trimite la un server atacator remot.
Sunt cerute permisiuni care nu sunt necesare unei aplicatii de acest gen (cum se pretinde a fi). De exemplu permisiunea CALL_PHONE, RECORD_AUDIO, etc.

Analizand codul ***smali***, se poate vedea ca aplicatia poate citi ID-ul device-ului (ex. IMEI sau ESN). S-au apelat serviciile din “android.telephony.TelephonyManager.**getDeviceId**":
“com.nicky.lyyws.xmall.XM_SmsListener.smali”
"com.nicky.lyyws.xmall.GpsService.smali"
"com.nicky.lyyws.xmall.MainService.smali”
"com.nicky.lyyws.xmall.SocketService.smali"
"com.nicky.lyyws.xmall.XM_CallListener.smali"

TelephonyManager.class

```
public class TelephonyManager
{
  public static CellLocation getCellLocation(android.telephony.TelephonyManager paramTelephonyManager)
  {
    try
    {
      CellLocation localCellLocation = paramTelephonyManager.getCellLocation();
      StringBuilder localStringBuilder = new StringBuilder();
      localStringBuilder.append("Landroid/telephony/TelephonyManager;->getCellLocation(");
      localStringBuilder.append(")");
      localStringBuilder.append("Landroid/telephony/CellLocation;=");
      localStringBuilder.append(Helper.toString(localCellLocation));
      Helper.log(localStringBuilder.toString());
      return localCellLocation;
    }
    catch (Exception localException)
    {
      localException.printStackTrace();
    }
    return null;
  }

  public static String getDeviceId(android.telephony.TelephonyManager paramTelephonyManager)
  {
    try
    {
      String str = paramTelephonyManager.getDeviceId();
      StringBuilder localStringBuilder = new StringBuilder();
      localStringBuilder.append("Landroid/telephony/TelephonyManager;->getDeviceId(");
      localStringBuilder.append(")");
      localStringBuilder.append("Ljava/lang/String;=");
      localStringBuilder.append(Helper.toString(str));
      Helper.log(localStringBuilder.toString());
      return str;
```

De altfel, malware-ul poate sa inregistreze audio sau sa acceseze fisierele media, apeland din "android.media.MediaRecorder.start" serviciul:
"com.nicky.lyyws.xmall.**RecordService**.smali"

sau sa interogheze locatia telefonului (GPS):
"com.nicky.lyyws.xmall.GpsService.smali" din "android.location.LocationManager.**getLastKnownLocation**"
"com.nicky.lyyws.xmall.GpsService.smali" din "android.location.Location.**getLongitude**"
"com.nicky.lyyws.xmall.GpsService.smali" din "android.telephony.TelephonyManager.**getCellLocation**"
"com.nicky.lyyws.xmall.GpsService.smali" din "android.location.Location.**getLatitude**"

Malware-ul poate sa trimita SMS-uri:
Found invoke in "com.nicky.lyyws.xmall.MainService$1.smali" to "android.telephony.gsm.SmsManager.**sendTextMessage**"

Acest trojan poate fura credentialele utilizatorului si sa intercepteze convorbirile telefonice ale acestora in background. Poate, de asemenea, sa le memoreze intr-un director numit "shangzhou/callrecord" de pe cardul SD (se poate observa in clasa RecordService, in SocketService si in .XM_CallListener) si sa le trimita pe un server remore.

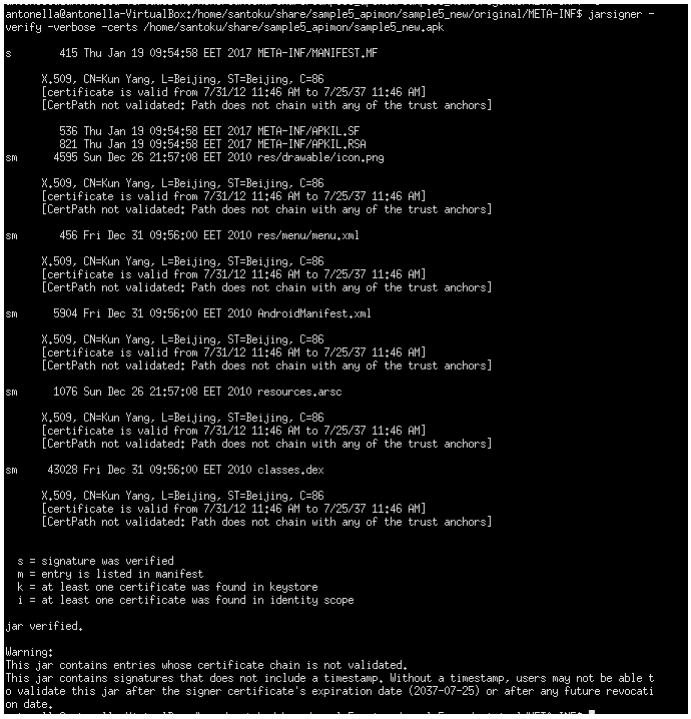
```
public class RecordService extends Service
{
  private int SleepSec = 180;
  private String callrpath = "/sdcard/shangzhou/callrecord/";
  boolean cording = false;
```

Am gasit in clasa MainService, in interiorul functiei onStart() un URL, “jin.56mo.com”.

```
    new Thread(this.sendsms).start();
if ((this.SERVER_ADDR.equals("")) || (this.SERVER_PORT == 0))
{
  localEditor.putString("Service", "jin.56mo.com");
  localEditor.putInt("Port", 2018);
  localEditor.putString("Time", "1");
  localEditor.putString("Move", "10");
  localEditor.putString("BeginTime", "00:01");
  localEditor.putString("EndTime", "23:59");
  localEditor.commit();
}
```

3. Analiza certificatului:

   Analizand certificatul apk-ului din */original/META-INF*, se poate vedea ca este criptat cu algoritmul RSA. De altfel, emitentul aplicatiei este Kun Yang, din China (Beijing) iar certificatul nu a fost validat, deci pare a nu fi de incredere.



4. BroadcastReceiver-ul BootReceiver

Conform fisieurlui AndroidManifest.xml, aplicatia “Android System Message” contine urmatoarele servicii: .MainService, .GpsService, .SocketService,

XM_SmsListener, .XM_CallListener, .XM_CallRecordService, .RecordService si **receiver-ele**: .BootReceiver (cu intent-ul android.intent.action.BOOT_COMPLETED) si .AlarmReceiver.
Trojan-ul se foloseste de receivere pentru a se active atunci cand se termina de bootat device-ul. Serviciile aplicatiei sunt declarate pentru a rula in background. Dupa bootarea dispozitivului si activarea malware-ului, se poate vedea lista de servicii la setari, in tabul *Running services.* Aceste servicii ruleaza in background fara ca utilizatorul sa observe ca ele exista.