SUBEX

Android Trojan-Dropper Threat Report

Date: 23/07/2021
Sanjuktasree Chatterjee

Android applications are now providing various functions in one single application. These possess some security risks to the users. Android is a very popular operating system for most users. Cybercriminals are actively targeting this platform and the applications to conduct the attack.

On 21st July 2021, we found a zero-day Android package file in our honeypot which is highly malicious. This file is a fake variant of a Chinese remote application for smart home devices which is found to be a malicious Trojan installer that can install various other malware in the system and acts as a backdoor for the device.

File Hash: `cedbb611ac8af04ef100bd2151484b5c`

Technical Analysis:

Fig: 1 shows that the sample is a Chinese application. The attacker uses the source code of a legitimate file and modifies it to create a malicious copy of it.

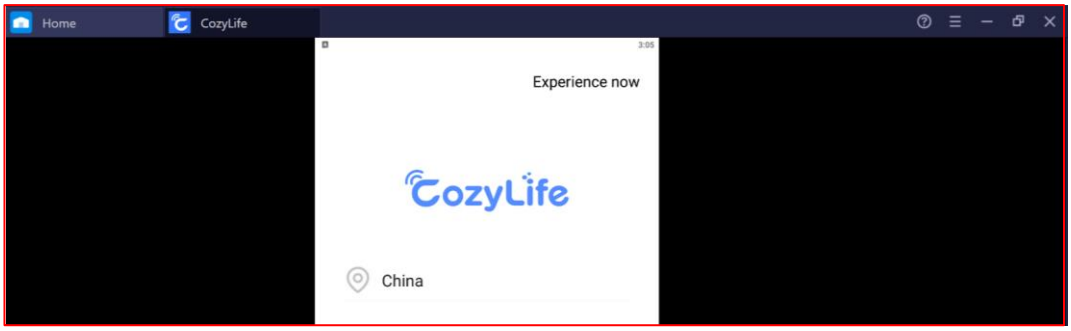


Fig: 1

In the code (Fig: 2) itself it is showing that the malware tries to open GPS to collect the location information of the device.

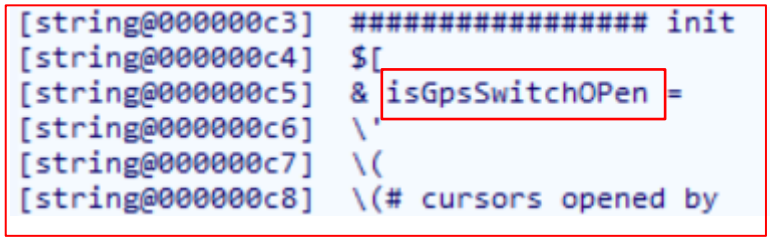


Fig: 2

There are multiple domains that has been mentioned in the code that has connections with the malicious .apk files. When it runs in the background, it accesses those domains and downloads other malware from those sites. Regex is used for multiple URLs, the malware connects with those sites to do malicious activities. The API calls like `resizeNativeKeyBoardInput`, `ShowBackHome` will check the system's internal settings and arrange it in a way that will help to download other malware. Some URLs will redirect to another web page that drops Trojan in the device.

Fig: 3

There are too many permissions given to the application which is not required for a normal remote device application. "ACCESS_COARSE_LOCATION" will check the location of the user. The Change Wi-Fi state permissions is used to create remote connections, install other apps and deliver information to the attacker's server. READ_PHONE_STATE permission helps to gather information about the device and data. "WRITE_SETTINGS" permission is used to change settings for download other malware. These seem to be malicious characteristics for this sample.

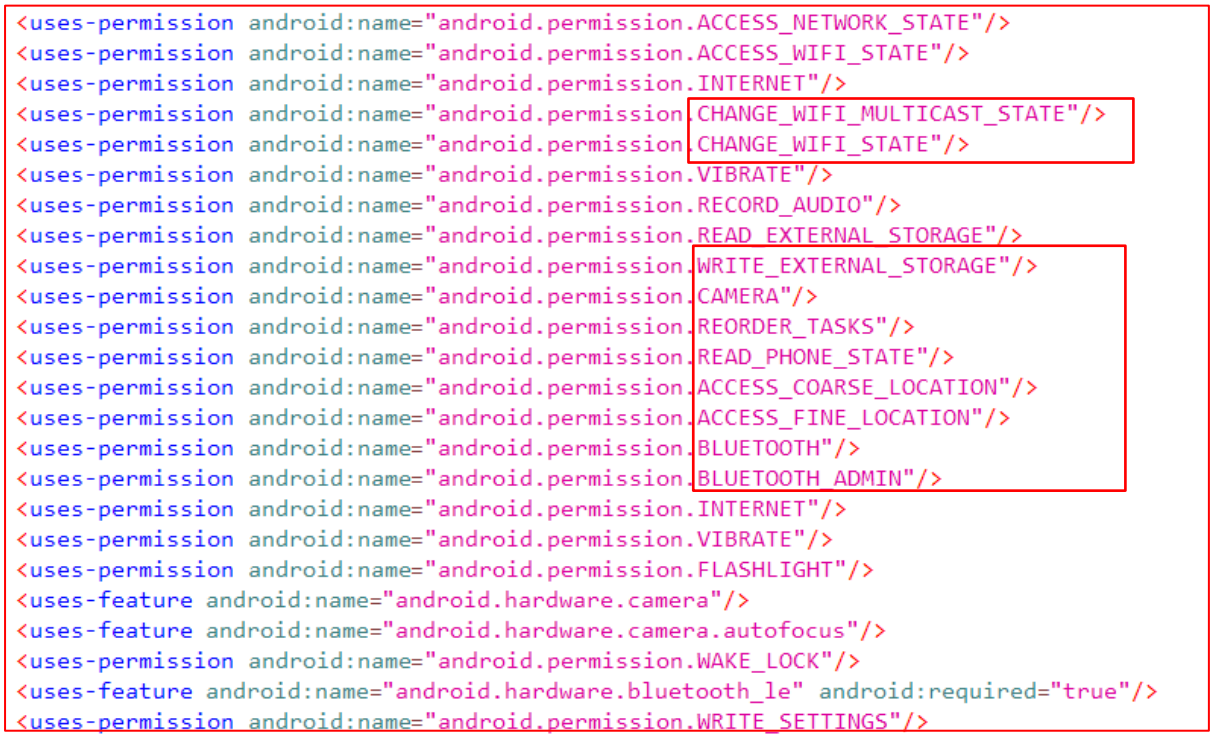


Fig: 4

In Fig: 5, the application checks for mobile device information and also storage permission to store other downloaded applications in the device.

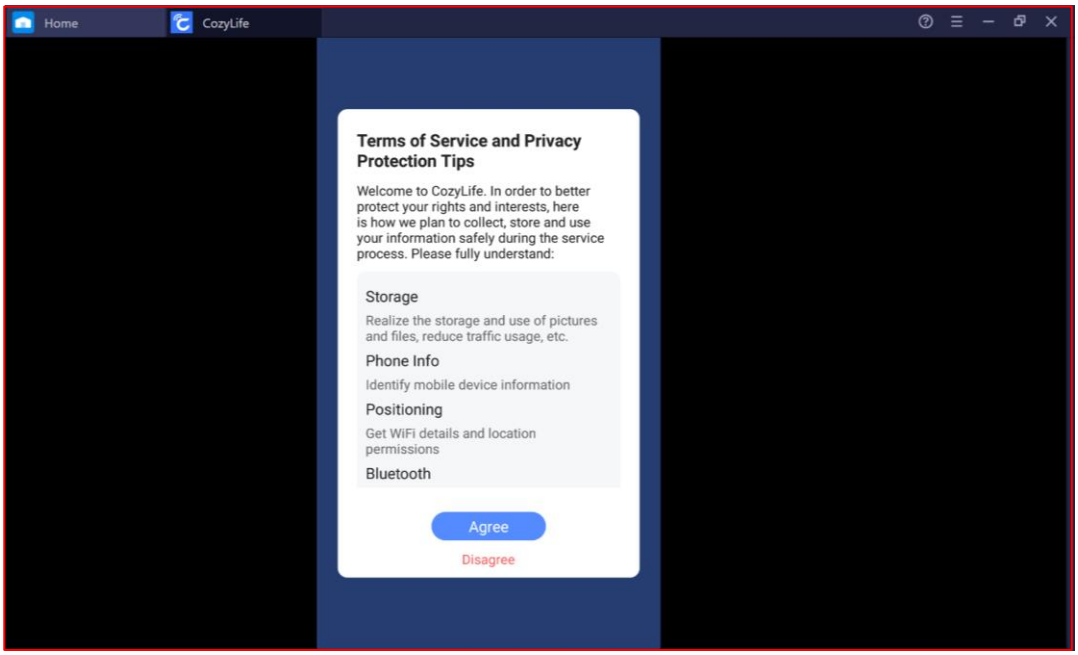


Fig: 5

The actions may be performed to communicate with these URLs in which some URLs are malicious (fig:6).

```
[string@0000c364] http://%1$s/%2$s
[string@0000c365] http://api.applink.mob.com
[string@0000c366] http://ns.adobe.com/xap/1.0/\xc0\x80
[string@0000c367] http://p.share.mob.com/tags/getTagList
[string@0000c368] http://schemas.android.com/apk/res/android
[string@0000c369] http://schemas.google.com/AddActivity
[string@0000c36a] http://schemas.google.com/BuyActivity
[string@0000c36b] httpClientConf
```

Fig: 6

The Bluetooth admin permissions are used to gather device information, IMEI number and few other device utilities which is malicious characteristics for the sample.

```
[method@00e804]:  com.alipay.mobile.aompdevice.telephonyinfo.h5plugin.H5TelephonyInfoPlugin.getImsiOperator
[method@0129a8]:  com.alipay.mobile.common.info.DeviceInfo.getOperator
[method@013162]:  com.alipay.mobile.common.logging.helper.ClientIdHelper.initClientId
[method@0141e5]:  com.alipay.mobile.common.transport.monitor.SignalStateHelper$1.run
[method@0141f7]:  com.alipay.mobile.common.transport.monitor.SignalStateHelper.b
[method@018343]:  com.alipay.mobile.nebulaappproxy.utils.TinyDeviceUtils.getIMEI
[method@01d945]:  com.amap.api.mapcore2d.gn$a.run
[method@01d969]:  com.amap.api.mapcore2d.gn.g
[method@01d96d]:  com.amap.api.mapcore2d.gn.k
[method@01d9b5]:  com.amap.api.mapcore2d.gs.a
[method@029da1]:  com.loc.dw.c
[method@029dab]:  com.loc.dw.h
[method@031ad4]:  com.ta.utdid2.android.utils.PhoneInfoUtils.getImei
[method@031ad5]:  com.ta.utdid2.android.utils.PhoneInfoUtils.getImsi
[method@031cc9]:  com.tencent.bugly.crashreport.common.info.b.b
```

Fig: 7

When the samples are used by the victim, unknowingly it starts installing other malware and hide its persistence and act as the genuine application.

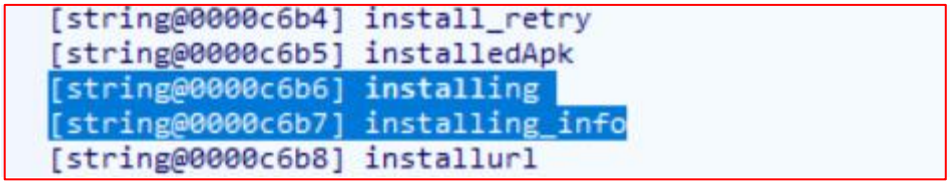
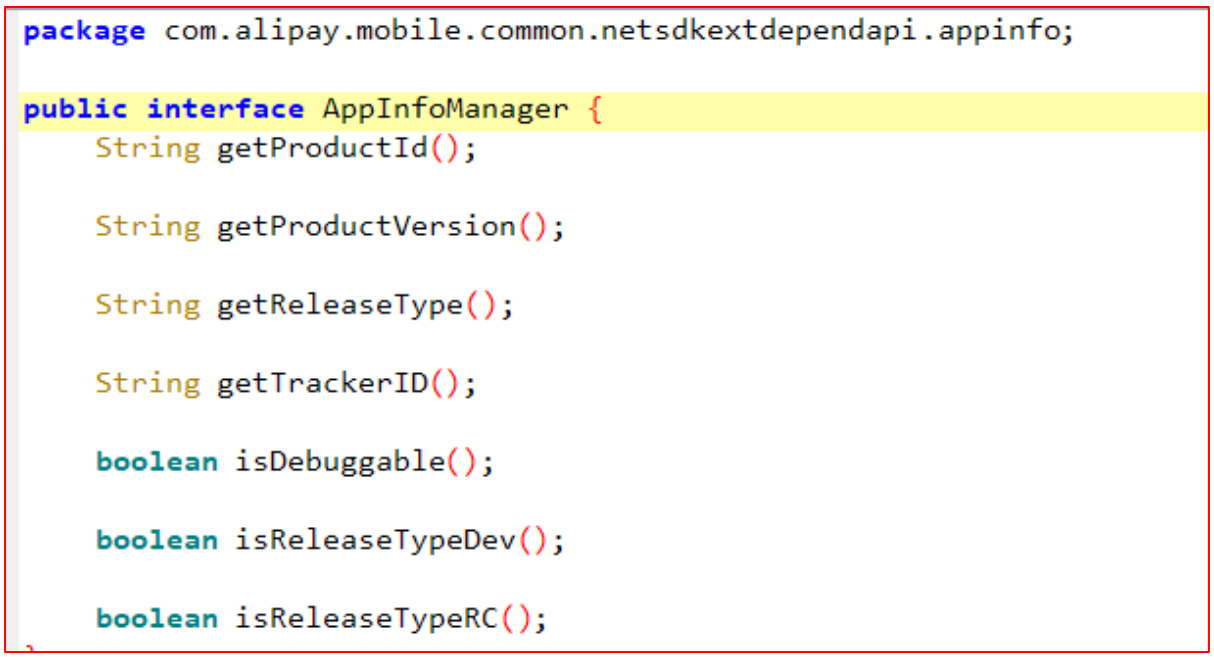


Fig: 8

The information related to anti analysis techniques (fig: 9) is present in the source code of the file.



```
package com.alipay.mobile.common.netsdkextdependapi.appinfo;

public interface AppInfoManager {
    String getProductId();

    String getProductVersion();

    String getReleaseType();

    String getTrackerID();

    boolean isDebuggable();

    boolean isReleaseTypeDev();

    boolean isReleaseTypeRC();
```

Fig: 9

The encryption mechanism is found in the source code of the file, and it is AES encrypted (Fig: 10).

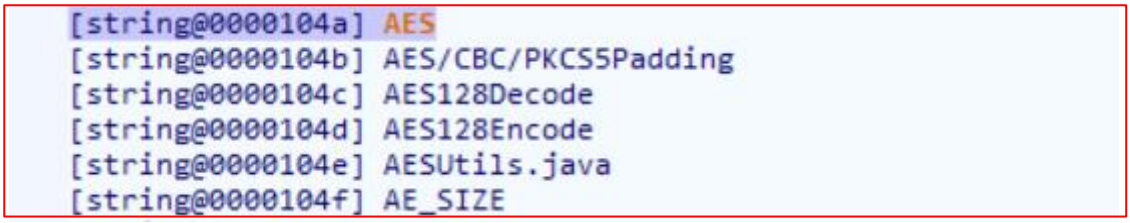


Fig: 10

The application also deletes some valuable system files and downloads history after the process has been done.

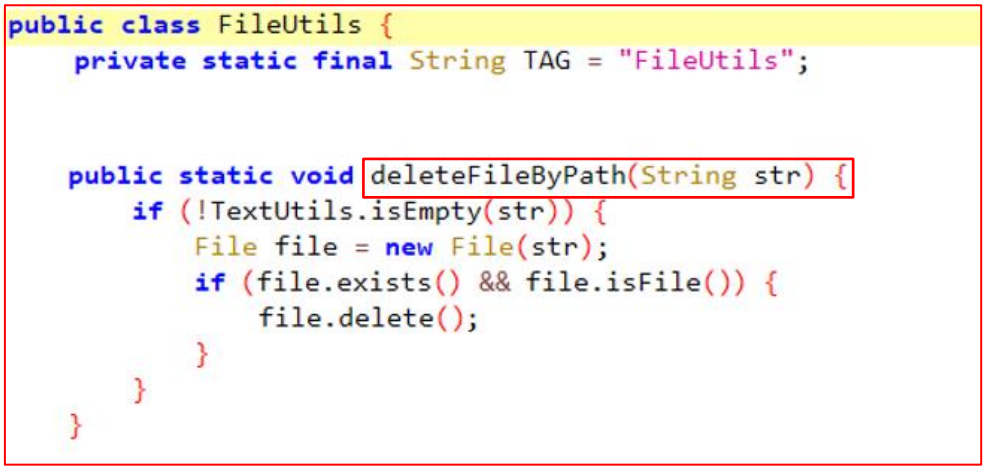


Fig: 11

IOCS:

taobao.com
http://api.applink.mob.com

MITRE Techniques:

Install Insecure or Malicious Configuration(T1478)
Masquerade as Legitimate Application(T1444)
Access Sensitive Data in Device Logs(T1413)
Deliver Malicious App via Other Means (T1476)

CVE:

CVE-2016-2569

Subex Secure Protection

Subex Secure detects the malware as "SS_Gen_Android_TrojanDropper_B"

Our Honeypot Network

This report has been prepared from the threat intelligence gathered by our honeypot network. This honeypot network is today operational in 62 cities across the world. These cities have at least one of the following attributes:

- Are landing centers for submarine cables
- Are internet traffic hotspots
- House multiple IoT projects with a high number of connected endpoints
- House multiple connected critical infrastructure projects
- Have academic and research centers focusing on IoT

- Have the potential to host multiple IoT projects across domains in the future

Over 3.5 million attacks a day is being registered across this network of individual honeypots. These attacks are studied, analyzed, categorized, and marked according to a threat rank index, a priority assessment framework that we have developed within Subex. The honeypot network includes over 4000 physical and virtual devices covering over 400 device architectures and varied connectivity mediums globally. These devices are grouped based on the sectors they belong to for purposes of understanding sectoral attacks. Thus, a layered flow of threat intelligence is made possible.