

Report

General Information

Analysis Start Time	2017-01-06 02:06:54
Analysis End Time	2017-01-06 02:07:53
File MD5	4B351CBE7CE4401980D9217313A9D107
File Size	114.38 KB
File Name	1483634283_chome.apk
Package Name	gherter.werwqerew.vbxcvbx
Version Code	1
Version Name	49.50
Min SDK	10
Target SDK	22
Max SDK	N/A
Pcap File	 (/file_download?md5=4B351CBE7CE4401980D9217313A9D107&type=pcap)
Logcat File	 (/file_download?md5=4B351CBE7CE4401980D9217313A9D107&type=logcat)

Risk Score




Risky Behaviors

Exist unused permissions
Loads and links the dynamic library
Loads code dynamically
Utilizes Java reflection

Malware Detected by VirusTotal

(<https://www.virustotal.com/en/file/f1d2a0b923281690e5c5c464f9bcaabf9db4ae23894d9777d231d60152745fc9/analysis/1483634283-chome.apk>)

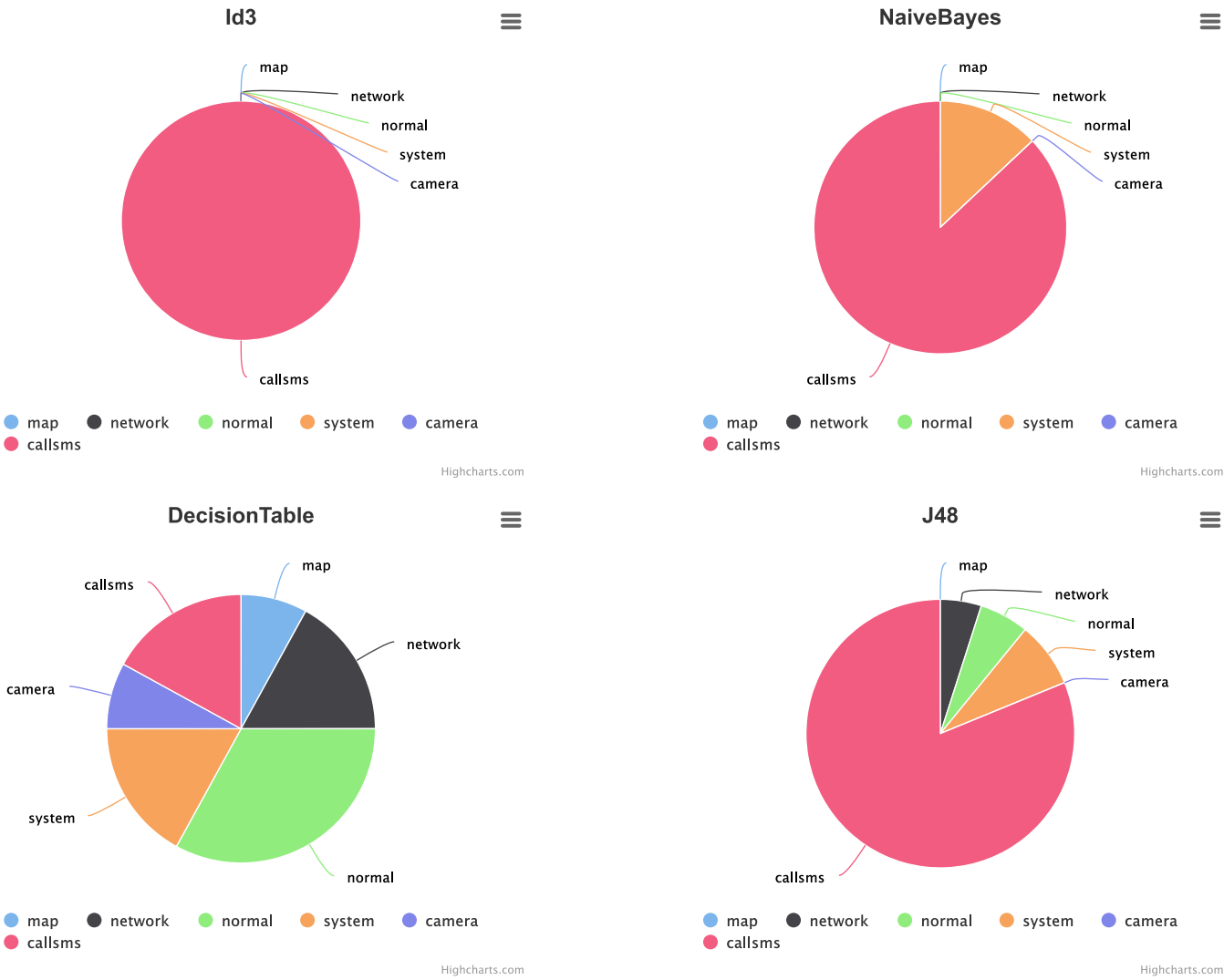
AVG	Android/G2P.EO.1D1629AF43F2
Ad-Aware	Android.Trojan.FakeInst.TP
BitDefender	Android.Trojan.FakeInst.TP
ESET-NOD32	a variant of Android/TrojanDropper.Agent.YM
F-Secure	Trojan:Android/Marcher.N
Fortinet	Android/Generic.AP.50DE8ltr
Kaspersky	HEUR:Trojan-Spy.AndroidOS.SmForw.gr
McAfee	

Qihoo-360	Trojan.Android.Gen
Symantec	✔

Certificate

Content	Owner: CN=xlskzrsme, OU=ginsgueznc, O=bcziwnzeg, L=kctcbpxhvw, ST=wsdfjhgbi, C=US Issuer: CN=xlskzrsme, OU=ginsgueznc, O=bcziwnzeg, L=kctcbpxhvw, ST=wsdfjhgbi, C=US Serial number: 168a21bc Valid from: Thu Jan 05 13:55:54 CST 2017 until: Sat Jul 13 13:55:54 CST 2126 Certificate fingerprints: MD5: DA:76:C7:7A:7F:67:72:79:E5:6B:7A:95:9C:51:0B:42 SHA1: 74:12:58:1A:FF:9C:55:8D:76:94:5A:20:C9:BF:FA:C2:F7:7A:22:4E SHA256: FE:17:4A:11:56:FE:89:1E:4F:F1:25:AF:D8:28:04:A2:DA:C4:83:22:87:D6:91:8A:82:27:FC:37:CB:5C:C7:D5 Signature algorithm name: SHA256withRSA Version: 3 Extensions: #1: ObjectId: 2.5.29.14 Criticality=false SubjectKeyIdentifier [ KeyIdentifier [ 0000: FC 76 3A 3A C9 D7 03 14 C7 AD 06 16 D9 96 01 1F .v::..... 0010: F5 FB FF 72 ...r ] ]
Sha1	7412581AFF9C558D76945A20C9BFFAC2F77A224E

Classification



Code Features

Code Feature	Used
Native Code	✔

Code Feature	Used
Dynamic Loader	✓
Java Reflection	✓
Crypto	✗

## Permissions

Permission Name	Protection Level	Threat Level	Customized	Duplicated	Used	Description
android.permission.ACCESS_NETWORK_STATE	normal		✗	✗	✗	Allows applications to access information about networks
android.permission.ACCESS_WIFI_STATE	normal		✗	✗	✗	Allows applications to access information about Wi-Fi networks
android.permission.BROADCAST_SMS	signature		✗	✗	✗	Allows an application to broadcast an SMS receipt notification. Not for use by third-party applications.
android.permission.CALL_PHONE	dangerous		✗	✗	✗	Allows an application to initiate a phone call without going through being placed.
android.permission.CHANGE_NETWORK_STATE	normal		✗	✗	✗	Allows applications to change network connectivity state
android.permission.CHANGE_WIFI_STATE	dangerous		✗	✗	✗	Allows applications to change Wi-Fi connectivity state
android.permission.DISABLE_KEYGUARD	dangerous		✗	✗	✗	Group of permissions that are related to the screenlock. Allows applications to disable the keyguard
android.permission.EXPAND_STATUS_BAR	normal		✗	✗	✗	Used for permissions that change the status bar Allows an application to expand or collapse the status bar.
android.permission.GET_ACCOUNTS	normal		✗	✗	✗	Permissions for direct access to the accounts managed by the Account Manager. Allows access to the list of accounts in the Accounts Service
android.permission.GET_TASKS	dangerous		✗	✗	✗	Group of permissions that are related to the other applications running apps, or killing background processes. Allows an application to get information about the currently or recently running tasks.
android.permission.INTERNET	dangerous		✗	✗	✗	Used for permissions that provide access to networking services. The or other related network operations. Allows applications to open network sockets.
android.permission.MODIFY_PHONE_STATE	signature system		✗	✗	✗	Allows modification of the telephony state - power on, mmi, etc. Not for use by third-party applications.
android.permission.PACKAGE_USAGE_STATS	signature system		✗	✗	✗	Allows an application to collect component usage statistics
android.permission.READ_CONTACTS	dangerous		✗	✗	✗	Used for permissions that provide access to the user's social connections, expressed as two distinct permissions). Allows an application to read the user's contacts data.
android.permission.READ_EXTERNAL_STORAGE	normal		✗	✗	✗	Group of permissions that are related to SD card access. Allows an application to read from external storage. targetSdkVersion is 4 or higher.

Permission Name	Protection Level	Threat Level	Customized	Duplicated	Used	Description
android.permission.READ_PHONE_STATE	dangerous		✗	✗	✗	Allows read only access to phone state. targetSdkVersion is 4 or higher.
android.permission.READ_SMS	dangerous		✗	✗	✓	Allows an application to read SMS messages.
android.permission.RECEIVE_BOOT_COMPLETED	normal		✗	✗	✓	Allows an application to receive the to the user.
android.permission.RECEIVE_SMS	dangerous		✗	✗	✓	Allows an application to monitor incoming SMS messages, to record or perform processing on them.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal		✗	✗	✗	N/A
android.permission.RESTART_PACKAGES	normal		✗	✗	✗	The { android.app.ActivityManager#restartPackage} API is no longer supported.
android.permission.SEND_SMS	dangerous		✗	✗	✗	Used for permissions that allow an application to send messages receiving or reading an MMS. Allows an application to send SMS messages.
android.permission.STOP_APP_SWITCHES	signature system		✗	✗	✗	Allows an application to tell the activity manager to temporarily
android.permission.SYSTEM_ALERT_WINDOW	dangerous		✗	✗	✗	Group of permissions that allow manipulation of how another application displays UI to the user. Allows an application to open windows using the type system-level interaction with the user.
android.permission.SYSTEM_OVERLAY_WINDOW	normal		✗	✗	✗	N/A
android.permission.WAKE_LOCK	normal		✗	✗	✗	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming
android.permission.WRITE_EXTERNAL_STORAGE	dangerous		✗	✗	✗	Allows an application to write to external storage. { android.content.Context#getExternalCacheDir}.
android.permission.WRITE_SETTINGS	normal		✗	✗	✓	Allows an application to read or write the system settings.
android.permission.WRITE_SMS	dangerous		✗	✗	✗	Allows an application to write SMS messages.

## Activities

Name	Main Activity	Exposed
com.oidufsd.oidfpas.MyActivity • android.intent.action.MAIN	✓	✓
com.oidufsd.oidfpas.MyWebActivity • android.intent.action.VIEW	✗	✓

## Services

Name	Exposed
com.oidufsdf.oidfpas.MainService <ul style="list-style-type: none"><li>com.android.action.start.msg.service</li></ul>	✖

## Broadcast Receivers

Name	Dynamically Registered	Exposed
com.oidufsdf.oidfpas.BootReceiver <ul style="list-style-type: none"><li>android.intent.action.BOOT_COMPLETED</li><li>android.intent.action.USER_PRESENT</li><li>android.provider.Telephony.SMS_RECEIVED</li></ul>	✖	✔
com.oidufsdf.oidfpas.MyAdmReceiver <ul style="list-style-type: none"><li>android.app.action.DEVICE_ADMIN_ENABLED</li></ul>	✖	✖
com.oidufsdf.oidfpas.ShutdownReceiver <ul style="list-style-type: none"><li>android.intent.action.ACTION_SHUTDOWN</li></ul>	✖	✔

## Content Providers

N/A
-----

## Features

N/A
-----

## Libraries

N/A
-----

## Advertisement Modules

N/A
-----

## Urls

N/A
-----

## Sensitive Files

N/A
-----

## Native Codes

Lib Name	Caller Code	Path Index
cocos2d	Lcom/API;->()V	4

## Dynamic Loaders

N/A
-----

## Crypto Operation

N/A

Network Operations

N/A

Socket Connections

N/A

File Operations

N/A

DNS Query

N/A

HTTP Data

N/A

Files Recovered From Http

N/A

Execute Shells

N/A

Started Services

N/A

May Send SMS

N/A

Send SMS

N/A

Block SMS

N/A

Phone Call

N/A

Data Leakage

N/A

Sensitive APIs

- **API: Ldalvik/system/DexClassLoader;->loadClass**
  - Description: Loads code dynamically
  - Caller Code: Lcom/oidufsd/oidfpas/MainService;->initPlugin(Lcom/PluginBase;)Lcom/PluginBase;
  - Threat Level:
  - Path Index: 90
- **API: Ljava/lang/System;->load**
  - Description: Loads and links the dynamic library
  - Caller Code: Lcom/API;->()V
  - Threat Level:
  - Path Index: 4
- **API: Ljava/lang/System;->loadLibrary**
  - Description: Loads and links the dynamic library
  - Caller Code: Lcom/API;->()V
  - Threat Level:
  - Path Index: 4
- **API: Ljava/lang/reflect/Method;->invoke**
  - Description: Utilizes Java reflection
  - Caller Code: Lcom/oidufsd/oidfpas/MyActivity;->a(Landroid/content/Context; Landroid/content/ComponentName;)Landroid/content/Intent;
  - Threat Level:
  - Path Index: 78

### Permission Usage

- **Permission Name: android.permission.READ\_SMS**
  - Used Type: Content Provider
  - Callee Code: -
- **Permission Name: android.permission.RECEIVE\_BOOT\_COMPLETED**
  - Used Type: Intent Action
  - Callee Code: android.intent.action.BOOT\_COMPLETED
- **Permission Name: android.permission.RECEIVE\_SMS**
  - Used Type: Intent Action
  - Callee Code: android.provider.Telephony.SMS\_RECEIVED
- **Permission Name: android.permission.WRITE\_SETTINGS**
  - Used Type: Content Provider
  - Callee Code:
- **Permission Name: android.permission.WRITE\_SETTINGS**
  - Used Type: Content Provider
  - Callee Code: /

### Log Message

N/A

### May Log Message

N/A

### ScreenShots

