



Report

General Information

Analysis Start Time	2017-01-03 18:06:29
Analysis End Time	2017-01-03 18:07:29
File MD5	3D92A7CCF7FE9A5D28ABB77A5F91DE7E
File Size	345.33 KB
File Name	vm.manager_92CF9D9E680A0975928709BC10C0627BD05AE766.apk
Package Name	vm.manager
Version Code	2
Version Name	0.1
Min SDK	8
Target SDK	N/A
Max SDK	N/A
Pcap File	 (/file_download?md5=3D92A7CCF7FE9A5D28ABB77A5F91DE7E&type=pcap)
Logcat File	 (/file_download?md5=3D92A7CCF7FE9A5D28ABB77A5F91DE7E&type=logcat)



Risk Score











Risky Behaviors

Connects to the Internet
Encrypt or Decrypt data

Malware Detected by VirusTotal

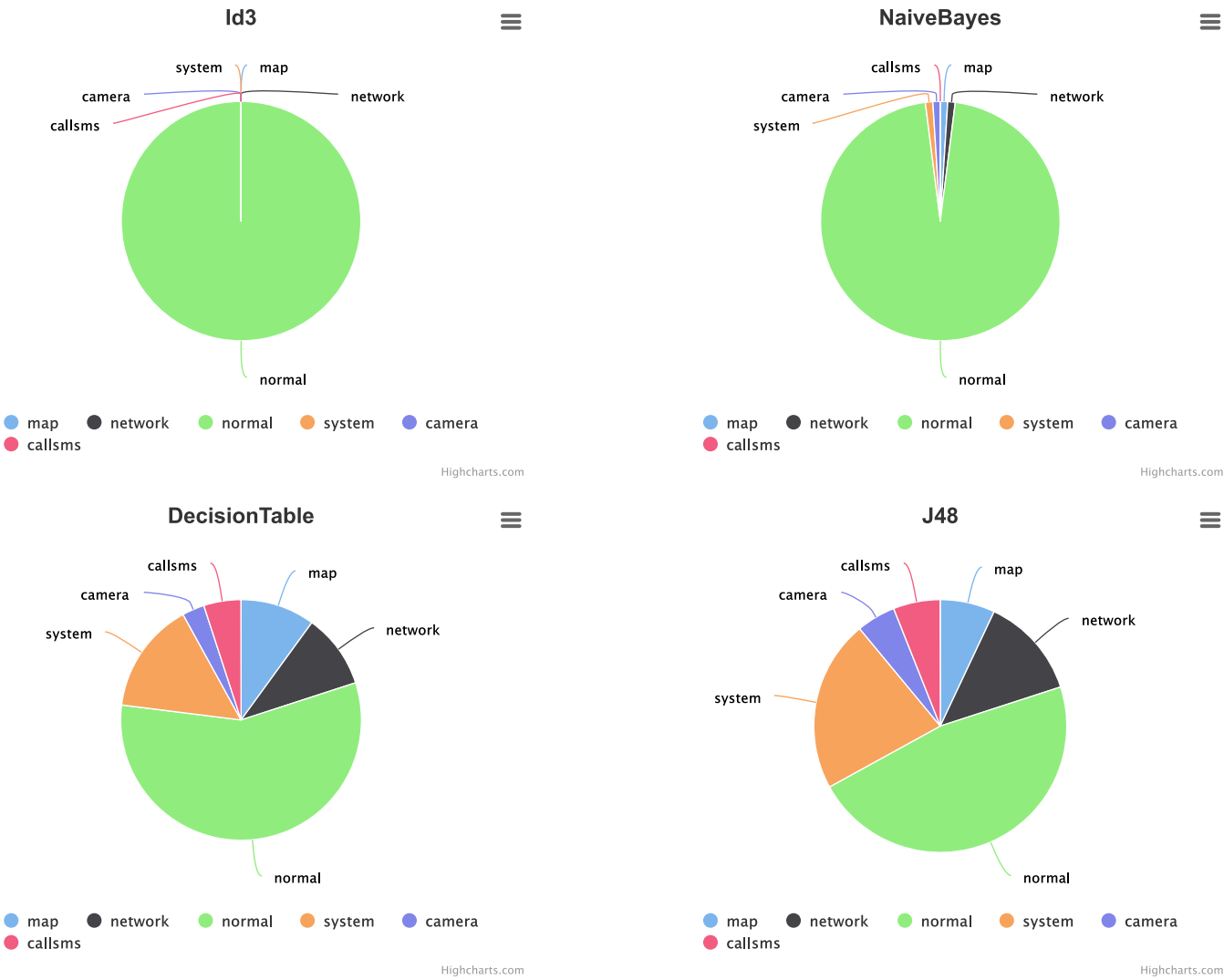
(<https://www.virustotal.com/en/file/907c11d112c85460c3b25ca6ee28cf7a57e15a2c67773051b6e3f7891942b89c/analysis/907c11d112c85460c3b25ca6ee28cf7a57e15a2c67773051b6e3f7891942b89c/>)

AVG	Android/R1.HJS.199F25DD79E9
Ad-Aware	
BitDefender	
ESET-NOD32	
F-Secure	
Fortinet	
Kaspersky	
McAfee	Artemis!3D92A7CCF7FE
Qihoo-360	
Symantec	

Certificate

Content	Owner: CN=Kabute Threepwood, OU=Kabute, O=Kabute, L=Vigo, ST=Pontevedra, C=ES Issuer: CN=Kabute Threepwood, OU=Kabute, O=Kabute, L=Vigo, ST=Pontevedra, C=ES Serial number: 4ed2c0dd Valid from: Mon Nov 28 06:59:41 CST 2011 until: Fri Apr 15 06:59:41 CST 2039 Certificate fingerprints: MD5: A0:59:DC:9D:48:96:1E:6A:0A:D7:B6:36:35:2F:EE:51 SHA1: 2F:7A:19:87:75:24:2F:E4:C0:81:AA:53:B0:D3:D5:9A:AE:B2:16:C0 SHA256: D6:6D:8D:AC:1D:45:13:B8:08:BB:F3:B1:1D:4E:6A:47:5F:B6:B8:71:A2:AD:78:9C:C8:10:C6:E9:EC:F9:87:5F Signature algorithm name: SHA1withRSA Version: 3
Sha1	2F7A198775242FE4C081AA53B0D3D59AAEB216C0

Classification



Code Features

Code Feature	Used
Native Code	✖
Dynamic Loader	✔
Code Feature	Used

Java Reflection	✓
Crypto	✓

Permissions

Permission Name	Protection Level	Threat Level	Customized	Duplicated	Used	Description
android.permission.ACCESS_NETWORK_STATE	normal	<div><div></div></div>	✗	✗	✓	Allows applications to access information about networks
android.permission.INTERNET	dangerous	<div><div></div></div>	✗	✗	✓	Used for permissions that provide access to networking services. The or other related network operations. Allows applications to open network sockets.

Activities

Name	Main Activity	Exposed
com.google.ads.AdActivity	✗	✗
vm.manager.InfoActivity	✗	✗
vm.manager.VMManagerActivity <ul style="list-style-type: none">android.intent.action.MAIN	✓	✓
vm.manager.VMManagerActivityOffline	✗	✗
vm.manager.VMManagerActivityOnline	✗	✗
vm.manager.configActivity	✗	✗

Services

N/A

Broadcast Receivers

Name	Dynamically Registered	Exposed
com.google.ads.util.AdUtil\$UserActivityReceiver	✓	?

Content Providers

N/A

Features

N/A

Libraries

N/A

Advertisement Modules

- AdMob [↗](http://www.google.com/ads/admob/) (http://www.google.com/ads/admob/)

Urls

N/A

Sensitive Files

N/A

Native Codes

N/A

Dynamic Loaders

Dex Path	Lib Path	Caller Code	Path Index
/data/app/vm.manager-1.apk	N/A	N/A	N/A

Crypto Operation

N/A

Network Operations

N/A

Socket Connections

N/A

File Operations

Operation	File Path	Data
write	/data/data/vm.manager/shared_prefs/VMManConfig.xml	<?xml version='1.0' encoding='utf-8' standalone='yes' ?>\x0a<map>\x0a<string name="currentVM">0</string>\x0a<

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: Ljava/net/URL;->openConnection**
 - Description: Connects to the Internet
 - Caller Code: Lcom/google/ads/b;->run()V
 - Threat Level:
 - Path Index: 26
- **API: Ljava/net/URL;->openConnection**
 - Description: Connects to the Internet
 - Caller Code: Lcom/google/ads/w;->run()V
 - Threat Level:
 - Path Index: 62
- **API: Ljavax/crypto/Cipher;->doFinal**
 - Description: Encrypt or Decrypt data
 - Caller Code: Lcom/google/ads/util/AdUtil;->b(Ljava/lang/String;)Ljava/lang/String;
 - Threat Level:
 - Path Index: 64

Permission Usage

- **Permission Name: android.permission.ACCESS_NETWORK_STATE**
 - Used Type: Api
 - Caller Code: Lcom/google/ads/util/AdUtil;->d(Landroid/content/Context;)Ljava/lang/String;
 - Callee Code: Landroid/net/ConnectivityManager;->getActiveNetworkInfo()Landroid/net/NetworkInfo;
 - Path Index: 16
- **Permission Name: android.permission.INTERNET**
 - Used Type: Api
 - Caller Code: Lcom/google/ads/b;->run()V
 - Callee Code: Ljava/net/URL;->openConnection()Ljava/net/URLConnection;
 - Path Index: 26
- **Permission Name: android.permission.INTERNET**
 - Used Type: Api
 - Caller Code: Lcom/google/ads/w;->run()V
 - Callee Code: Ljava/net/URL;->openConnection()Ljava/net/URLConnection;
 - Path Index: 62
- **Permission Name: android.permission.INTERNET**
 - Used Type: Api

- Caller Code: Lcom/google/ads/b;->run()V
- Callee Code: Ljava/net/URLConnection;->connect()V
- Path Index: 190
- **Permission Name: android.permission.INTERNET**
- Used Type: Api
- Caller Code: Lcom/google/ads/w;->run()V
- Callee Code: Ljava/net/URLConnection;->connect()V
- Path Index: 92
- **Permission Name: android.permission.INTERNET**
- Used Type: Content Provider
- Callee Code: l
- **Permission Name: android.permission.INTERNET**
- Used Type: Content Provider
- Callee Code: w
- **Permission Name: android.permission.INTERNET**
- Used Type: Content Provider
- Callee Code: load
- **Permission Name: android.permission.INTERNET**
- Used Type: Content Provider
- Callee Code: ad

Log Message

Tag	Message
Choreographer	Skipped 32 frames! The application may be doing too much work on its main thread.
Choreographer	Skipped 91 frames! The application may be doing too much work on its main thread.
InputEventConsistencyVerifier	KeyEvent: ACTION_UP but key was not down. in com.android.internal.policy.impl.PhoneWindow\$DecorView@410e0368 0: sent at 172928000000, KeyEvent { action=ACTION_UP, keyCode=KEYCODE_DPAD_UP, scanCode=0, metaState=0, flags=0x8, repeatCount=0, eventTime=172928, downTime=172928, deviceId=-1, source=0x101 } -- recent events -- 1: sent at 172906000000, (unhandled) KeyEvent { action=ACTION_UP, keyCode=KEYCODE_DPAD_RIGHT, scanCode=0, metaState=0, flags=0x8, repearepeatCount=0, eventTime=172906, downTime=172906, deviceId=-1, source=0x101 } 2: sent at 172901000000, (unhandled) KeyEvent { action=ACTION_DOWN, keyCode=KEYCODE_DPAD_RIGHT, scanCode=0, metaState=0, flags=0x8, repeatCount=0, eventTime=172901, downTime=172901, deviceId=-1, source=0x101 } 3: sent at 172862000000, (unhandled) KeyEvent { action=ACTION_UP, keyCode=KEYCODE_DPAD_DOWN, scanCode=0, metaState=0, flags=0x8, repeatCount=0, eventTime=172862, downTime=172862, deviceId=-1, source=0x101 } 4: sent at t at 172765000000, (unhandled) KeyEvent { action=ACTION_DOWN, keyCode=KEYCODE_DPAD_DOWN, scanCode=0, metaState=0, flags=0x8, repeatCount=0, eventTime=172765, downTime=172765, deviceId=-1, source=0x101 }
InputEventConsistencyVerifier	KeyEvent: ACTION_UP but key was not down. in android.view.ViewRootImpl@410d9ee8 0: sent at 173219000000, KeyEvent { action=ACTION_UP, keyCode=KEYCODE_DPAD_LEFT, scanCode=0, metaState=0, flags=0x8, repeatCount=0, eventTime=173219, downTime=173219, deviceId=-1, source=0x101 } -- recent events -- 1: sent at 172724000000, KeyEvent { action=ACTION_UP, keyCode=KEYCODE_MENU, scanCode=0, metaState=0, flags=0x8, repeatCount=0, eventTime=172724, downTime=172724, g24, deviceId=-1, source=0x101 } 2: sent at 172675000000, KeyEvent { action=ACTION_DOWN, keyCode=KEYCODE_MENU, scanCode=0, metaState=0, flags=0x8, repeatCount=0, eventTime=172675, downTime=172675, deviceId=-1, source=0x101 } 3: sent at 172670000000, MotionEvent { action=ACTION_UP, id[0]=0, x[0]=214.0, y[0]=350.0, toolType[0]=TOOL_TYPE_UNKNOWN, buttonState=0, metaState=0, flags=0x0, edgeFlags=0x0, pointerCount=1, historySize=0, eventTime=172670, downTime=172663, deviceId=0, source=0x1002 } 4: sent at 1 at 172663000000, MotionEvent { action=ACTION_DOWN, id[0]=0, x[0]=223.0, y[0]=345.0, toolType[0]=TOOL_TYPE_UNKNOWN, buttonState=0, metaState=0, flags=0x0, edgeFlags=0x0, pointerCount=1, historySize=0, eventTime=172663, downTime=172663, deviceId=0, source=0x1002 } 5: sent at 172627000000, KeyEvent { action=ACTION_UP, keyCode=KEYCODE_DPAD_RIGHT, scanCode=0, metaState=0, flags=0x8, repeatCount=0, eventTime=172627, downTime=172627, deviceId=-1, source=0x101 }
RESUME::	resuming

May Log Message

Tag	Message	Caller Code	Path Index
ADAPTER	1	Lvm/manager/VMMManagerActivityOffline;->updateVMList()V	244

Tag	Message	Caller Code	Path Index
ADAPTER	1	Lvm/manager/VMManagerActivityOnline;->updateVMList()V	558
CONNECT	0	Lvm/manager/VMManagerActivityOffline\$listVMTask;->doInBackground([Landroid/content/Context;)Ljava/lang/String;	108
CONNECT	0	Lvm/manager/VMManagerActivityOnline\$listVMTask;->doInBackground([Landroid/content/Context;)Ljava/lang/String;	132
EXCEPTION	2	Lvm/manager/libVirtMan;->execVMCommand(Ljava/lang/String;)Ljava/lang/String;	350
EXCEPTION	0	Lvm/manager/libVirtMan;->getVMList()Ljava/util/ArrayList;	108
RESUME::	3	Lvm/manager/VMManagerActivity;->onResume()V	112
RESUME::	3	Lvm/manager/VMManagerActivityOffline;->onResume()V	112
RESUME::	3	Lvm/manager/VMManagerActivityOnline;->onResume()V	112
SETTINGS::	4	Lvm/manager/VMManagerActivity;->onOptionsItemSelected(Landroid/view/MenuItem;)Z	140
makemachine	onCancelled()	Lvm/manager/InfoActivity\$infoVMTask;->onCancelled()V	14
makemachine	4	Lvm/manager/InfoActivity\$infoVMTask;->onPostExecute(Ljava/lang/String;)V	50
makemachine	onPreExecute()	Lvm/manager/InfoActivity\$infoVMTask;->onPreExecute()V	8
makemachine	2	Lvm/manager/InfoActivity\$infoVMTask;->onProgressUpdate([Ljava/lang/Integer;)V	54
makemachine	onCancelled()	Lvm/manager/VMManagerActivityOffline\$listVMTask;->onCancelled()V	14
makemachine	4	Lvm/manager/VMManagerActivityOffline\$listVMTask;->onPostExecute(Ljava/lang/String;)V	100
makemachine	onPreExecute()	Lvm/manager/VMManagerActivityOffline\$listVMTask;->onPreExecute()V	8
makemachine	2	Lvm/manager/VMManagerActivityOffline\$listVMTask;->onProgressUpdate([Ljava/lang/Integer;)V	54
makemachine	onCancelled()	Lvm/manager/VMManagerActivityOffline\$startVMTask;->onCancelled()V	14
makemachine	5	Lvm/manager/VMManagerActivityOffline\$startVMTask;->onPostExecute(Ljava/lang/String;)V	194
makemachine	onPreExecute()	Lvm/manager/VMManagerActivityOffline\$startVMTask;->onPreExecute()V	8
makemachine	2	Lvm/manager/VMManagerActivityOffline\$startVMTask;->onProgressUpdate([Ljava/lang/Integer;)V	54
makemachine	onCancelled()	Lvm/manager/VMManagerActivityOnline\$listVMTask;->onCancelled()V	14
makemachine	4	Lvm/manager/VMManagerActivityOnline\$listVMTask;->onPostExecute(Ljava/lang/String;)V	100
makemachine	onPreExecute()	Lvm/manager/VMManagerActivityOnline\$listVMTask;->onPreExecute()V	8
makemachine	2	Lvm/manager/VMManagerActivityOnline\$listVMTask;->onProgressUpdate([Ljava/lang/Integer;)V	54
makemachine	onCancelled()	Lvm/manager/VMManagerActivityOnline\$stopVMTask;->onCancelled()V	14
makemachine	5	Lvm/manager/VMManagerActivityOnline\$stopVMTask;->onPostExecute(Ljava/lang/String;)V	170
makemachine	onPreExecute()	Lvm/manager/VMManagerActivityOnline\$stopVMTask;->onPreExecute()V	8
makemachine	2	Lvm/manager/VMManagerActivityOnline\$stopVMTask;->onProgressUpdate([Ljava/lang/Integer;)V	54