



Report

General Information

Analysis Start Time	2016-12-27 00:24:02
Analysis End Time	2016-12-27 00:26:35
File MD5	FBB1697176295E070B55C331EFCD7EAB
File Size	163.25 KB
File Name	obfuscated.apk
Package Name	com.manager.appinstaller
Version Code	1
Version Name	1.0
Min SDK	6
Target SDK	N/A
Max SDK	N/A
Pcap File	 (/file_download?md5=FBB1697176295E070B55C331EFCD7EAB&type=pcap)
Logcat File	 (/file_download?md5=FBB1697176295E070B55C331EFCD7EAB&type=logcat)



Risk Score



Risky Behaviors

Connects to the Internet
Encrypt or Decrypt data
Exist unused permissions
Gets packages installed on the device
Gets the unique device ID, IMEI for GSM and MEID for ESN or ESN for CDMA phones
Utilizes Java reflection

Malware Detected by VirusTotal

(<https://www.virustotal.com/en/file/cc0773e1ff1a65026162c233cd44e91b85c548b027a234e2278a9d05da5081cd/an>)

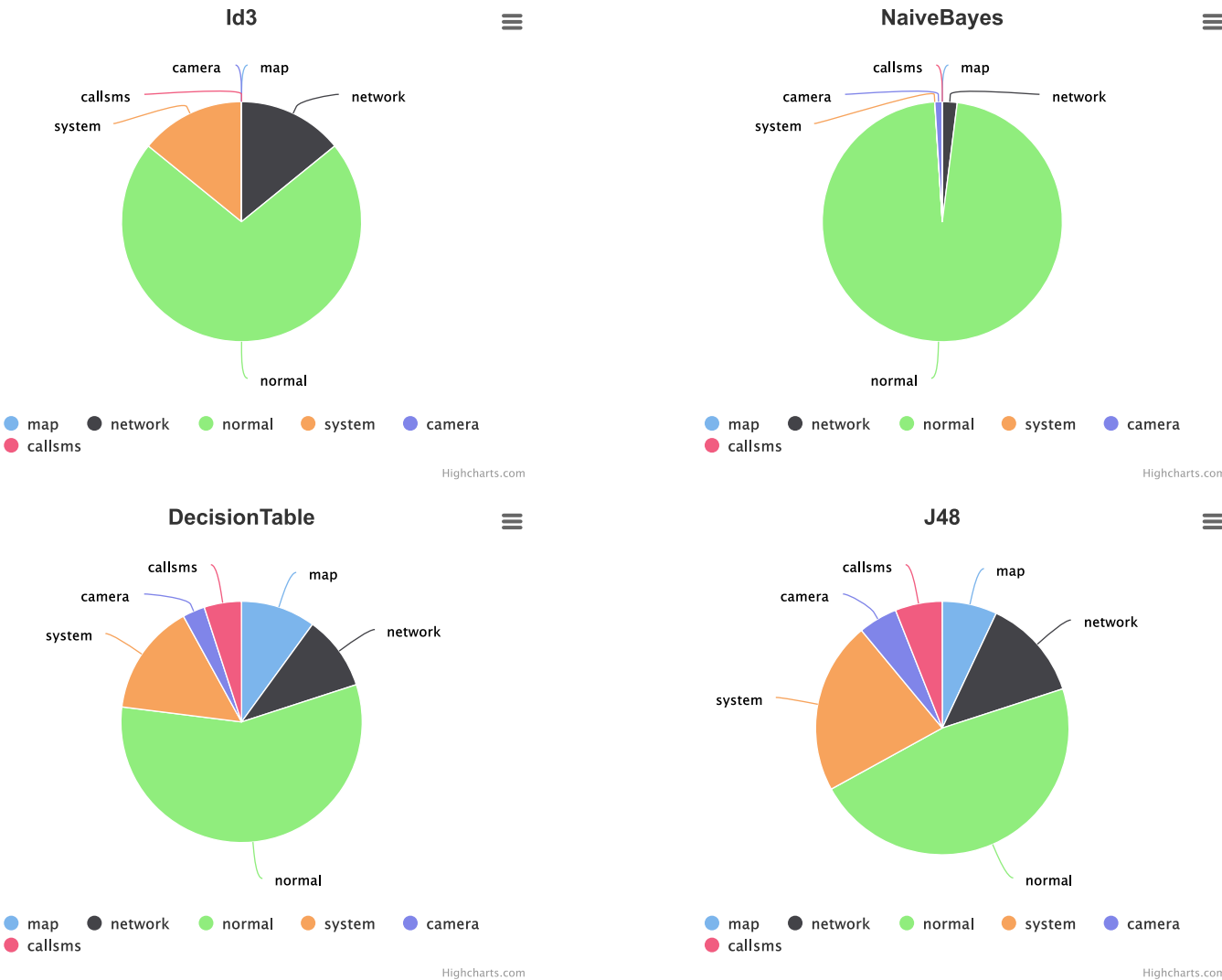
AVG	Android/R1.DET.5A9DFAADCAEE
Ad-Aware	Android.Trojan.DDLight.C
BitDefender	Android.Trojan.DDLight.C
ESET-NOD32	a variant of Android/Lightdd.D
F-Secure	Trojan:Android/DroidDream.D
Fortinet	Android/DrdLight.B!tr

Kaspersky	HEUR:Trojan-Downloader.AndroidOS.DorDrae.a
McAfee	☑
Qihoo-360	Trojan.Android.Gen
Symantec	☑

Certificate

Content	Owner: CN=Shield4J, OU=Shield4J, O=Shield4J, L=Madrid, ST=Spain, C=ES Issuer: CN=Shield4J, OU=Shield4J, O=Shield4J, L=Madrid, ST=Spain, C=ES Serial number: 525d3abd Valid from: Tue Oct 15 20:53:17 CST 2013 until: Tue Oct 22 20:53:17 CST 2013 Certificate fingerprints: MD5: 23:41:A0:6E:C8:61:3A:77:90:2B:F4:5D:A0:0E:8C:1D SHA1: 06:80:89:B9:ED:18:01:EC:35:31:9E:88:B1:4F:92:9D:77:05:80:37 SHA256: 32:B2:E8:32:0D:11:B0:72:42:19:3C:AA:65:67:26:8B:7D:44:09:89:70:D1:CF:D5:E7:F6:74:AD:E0:FA:D7:99 Signature algorithm name: SHA1withRSA Version: 3
Sha1	068089B9ED1801EC35319E88B14F929D77058037

Classification



Code Features

Code Feature	Used
--------------	------

Code Feature	Used
Native Code	✖
Dynamic Loader	✔
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.
android.permission.READ_PHONE_STATE	dangerous	<div><div></div></div>	✖	✖	✔	Allows read only access to phone state. targetSdkVersion is 4 or higher.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	<div><div></div></div>	✖	✖	✖	Allows an application to write to external storage. { android.content.Context#getExternalCacheDir}.

Activities

Name	Main Activity	Exposed
com.google.ads.AdActivity	✖	✖
com.manager.appinstaller.main <ul style="list-style-type: none">android.intent.action.MAIN	✔	✔

Services

Name	Exposed
com.manager.appinstaller.use.AppUseService	✖

Broadcast Receivers

Name	Dynamically Registered	Exposed
com.google.ads.e	✔	?
com.manager.appinstaller.use.Receiver <ul style="list-style-type: none">android.intent.action.PHONE_STATE	✖	✔
u\$b	✔	?

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/)

IP Distribution

Urls

Country	Url	IP
N/A	http://market.android.com/details	N/A
N/A	http://clk	N/A
N/A	http://sites.google.com/site/gson/gson-user-guide#toc-serializing-and-deserializing-gener	N/A
N/A	http://googleads.g.doubleclick.net	N/A
N/A	http://a.admob.com/f0?	N/A
N/A	http://www.googleadservices.com/pagead/aclk	N/A
N/A	http://www.gstatic.com/afma/sdk-core-v	N/A
N/A	http://googleads.g.doubleclick.net/aclk	N/A
N/A	http://c.admob.com	N/A

Sensitive Files

N/A

Native Codes

N/A

Dynamic Loaders

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

Crypto Operation

N/A

Network Operations

N/A

Socket Connections

N/A

File Operations

Operation	File Path	Data
read	/dev/urandom	=v5\x10_F\xef\xbf\xbdW\xef\xbf\xbd\xef\xbf\xbd\x06\xcf\x91\xef\xbf\xbd'\xef\xbf\xbdw\xef\xbf\xbd
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbd? \xef\xbf\xbd]\xef\xbf\xbdl\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdU\xef\xbf\xbd\x02z[\xef\xbf\xbd\xef\xbf\xbd>\xef\xbf\xbdSD\xef\xbf\xbd\xef\xbf\xbd\x04\xef\xbf\xbd[\xef\xbf\xbd1\xef\xbf\xbd\xef\xbf\xbd\x15\xef\xbf\xbd{\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdh'\xef\xbf\xbd\x12\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd;\xef\xbf\xbd\xef\xbf\xbd\x0a\xef\xbf\xbdN\xef\xbf\xbd\xef\xbf\xbd%4O\xef\xbf\xbd
write	/data/data/com.manager.appinstaller/cache/	sE\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdWW\xda\xad\xef\xbf\xbd&]\xef\xbf\xbd\xef\xbf\xbd0B\x07\xef\xbf\xbd\xef\xbf\xbd^\xd2\xa8TW\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd5\xef\xbf\xbd\x7f\x1bO\xef\xbf\xbd\xef\xbf\xbd=\xef\xbf\xbd\x1e\xef\xbf\xbd\xef\xbf\xbd(\xef\xbf\xbd)\x0aGX7\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x0c\xef\xbf\xbd\xef\xbf\xbd\x18\x08\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd_S
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbd(\xef\xbf\xbd\xef\xbf\xbd=\xef\xbf\xbdv\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd<\x1f\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x0cix\x09\xef\xbf\xbdY@ bj\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdnp\xdb\xabi\xef\xbf\xbdB\x18\xef\xbf\xbd\x7f\xef\xbf\xbd&\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdFc[\x06\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x12\xef\xbf\xbd\xef\xbf\xbd\x0aM\xef\xbf\xbd\xef\xbf\xbd
write	/data/data/com.manager.appinstaller/cache/	\x03c\xef\xbf\xbd4\xd1\xa1\xef\xbf\xbd\x13>\xef\xbf\xbdm\xef\xbf\xbd\x1d!\x16;\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdK\xef\xbf\xbd\xef\xbf\xbd8@\xef\xbf\xbd\xef\xbf\xbdP\x0f\xef\xbf\xbdCg\xef\xbf\xbd\xef\xbf\xbdE\xef\xbf\xbd\xcb\x8\xef\xbf\xbd3[~\xef\xbf\xbd\x0aD\xef\xbf\xbd\xef\xbf\xbd\x1d\x04L\xef\xbf\xbd\xef\xbf\xbdqm\xef\xbf\xbd4/H\xef\xbf\xbd
write	/data/data/com.manager.appinstaller/cache/	4\xef\xbf\xbdh\xef\xbf\xbd6\x0b\xef\xbf\xbdH\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdulQwc\x0f=]\x14C\x7f\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd4m\x02h4\xef\xbf\xbd<\xef\xbf\xbdY'\xef\xbf\xbd\xef\xbf\xbd\xde\x1b8\xef\xbf\xbd[\xef\xbf\xbd6\x19w\xef\xbf\xbd\x01JBj\xef\xbf\xbd\x0a\xef\xbf\xbd\xef\xbf\xbd? \xef\xbf\xbd \xef\xbf\xbdK
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbd-0\xef\xbf\xbdEPR\xef\xbf\xbdOy\xef\xbf\xbd\xef\xbf\xbdN\xef\xbf\xbd\xef\xbf\xbdZi"\xef\xbf\xbd\xef\xbf\xbdS\xef\xbf\xbd\xdd\xadK'\xef\xbf\xbdk=\xef\xbf\xbd):\xef\xbf\xbd,\x0e0\xef\xbf\xbd\x1cGj)\xef\xbf\xbd:\xef\xbf\xbd,m\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd?)a\xef\xbf\xbd\xef\xbf\xbd\x0d\x1c8\x98\xef\xbf\xbd\x02:\xef\xbf\xbd-\xef\xbf\xbd\x1a
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbd\x1c8\x9e\xef\xbf\xbd\xef\xbf\xbd\x1eRM6\xef\xbf\xbd\xef\xbf\xbd@s\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd0\xef\xbf\xbdj\xef\xbf\xbdP\x0b\xef\xbf\xbd\x1cU\xef\xbf\xbd\x11m\xef\xbf\xbd\x1c2\xbdIF_gVj)\xef\xbf\xbd\xef\xbf\xbd\x1b\xef\xbf\xbd\xef\xbf\xbd'\xef\xbf\xbdA\x04\xef\xbf\xbd>\x6>\x12~\xef\xbf\xbd,\xef\xbf\xbdLBSv=
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd3\xc4\x90\xef\xbf\xbdg\x0c)\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd1\xef\xbf\xbdK\x1f\xef\xbf\xbd\xef\xbf\xbd\x1f\xef\xbf\xbd(\xef\xbf\xbd\$1\xef\xbf\xbdv\xef\xbf\xbdP\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdR\xef\xbf\xbdO\xef\xbf\xbdW\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x18J\xef\xbf\xbdm\xef\xbf\xbd\xef\xbf\xbd-\x05\x1c\x16j]\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x105\xef\xbf\xbd\xef\xbf\xbd

Operation	File Path	Data
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbd\x0a\xef\xbf\xbd-\xef\xbf\xbd\xcb\x8d\xef\xbf\xbd\x7f\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd%\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd(0\xef\xbf\xbdyK\xef\xbf\xbd,N\xef\xbf\xbdrb@\xef\xbf\xbd\xef\xbf\xbd\x c4\x84\xef\xbf\xbd\xef\xbf\xbd=bO66{\xef\xbf\xbd\xef\xbf\xbdG,P\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x 14mq\xef\xbf\xbdH\xef\xbf\xbd\
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdvR\x15\x1c7\xef\xbf\xbd \xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd#\xef\xbf\xbd\xef\xbf\xbd4\x15k<h\xef\xbf\xbd\xef\xbf\x bd\x0d\xef\xbf\xbd\$\x18\xef\xbf\xbd? \xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\x bd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x9c\x9c\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x12)S- \xef\xbf\xbdQ\xef\xbf\xbd0QJ]\xef\xbf\xbd
write	/data/data/com.manager.appinstaller/cache/	\xdf\x9b\xef\xbf\xbdA'\xef\xbf\xbdnp\x1e&\xef\xbf\xbd\xef\xbf\xbd@\x\xef\xbf\xbdM\xef\xbf\xbdTP\xef\x bf\xbd\x0c\x5\x94\x02\xdc\xbfW\xef\xbf\xbd\xef\xbf\xbd1\x1duT\xef\xbf\xbdK\xef\xbf\xbd\xef\xbf\xbd @\xef\xbf\xbd=oXJ6\xef\xbf\xbd^,,f\xef\xbf\xbd\xef\xbf\xbd=\xef\xbf\xbd4n\xef\xbf\xbd>5a1\xef\xbf\x bdH0
write	/data/data/com.manager.appinstaller/cache/	{0}It;\xef\xbf\xbdM-\xef\xbf\xbd\xef\xbf\xbd\x17\xcc\xbb0\xef\xbf\xbd- o_\x07Y\xef\xbf\xbd\xef\xbf\xbdAK\xef\xbf\xbd~@)\xef\xbf\xbd(\xef\xbf\xbd\xef\xbf\xbd*\A\xef\xbf\xbd\x ef\xbf\xbd\x0b\xef\xbf\xbd\xef\xbf\xbdQW\xef\xbf\xbdnt\x0a\ \xef\xbf\xbd\xef\xbf\xbd\x16\xef\xbf\xbd\xef \xfbf\xbd.\xef\xbf\xbd\x12\xef\xbf\xbd\:\xef\xbf\xbd\x5\x80\xef\xbf\xbd\x3\x8c\xef\xbf\xbdlu
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbd\ \xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x10\xef\xbf\xbd\xef\xbf\xbd(C0e\ xef\xbf\xbd\xef\xbf\xbd \x07\xef\xbf\xbd\x0dmD\ xef\xbf\xbd\xef\xbf\xbdW\ xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x131\x00\ xef\x bf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdEP8\x18\x1e\ xc2\ xac\ xef\xbf\xbd\xef\xbf\xbdK2\x1b\ xef\xbf \xbd\x7e\x82\x89\x0b\x0b\x17\ xef\xbf\xbd\xef\xbf\xbd.c\ xef\xbf\xbd\xef\xbf\xbdP\ xef\xbf\xbd1
write	/data/data/com.manager.appinstaller/cache/	\x05\x17W\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x1\x7fxde\xab\ xef\xbf\xbd\xef\xbf \xbd[dq\ xef\xbf\xbd\xef\xbf\xbd)\ xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd9j!Y\ xef\xbf \xbd\xef\xbf\xbdz\ xef\xbf\xbd\x06\x7\x90\ xef\xbf\xbd\xef\xbf\xbd\ x0f\ xef\xbf\xbdjc)\x07\ xef\xbf\xbd\ xef \xbd\xbdY8P\xdd\x85zs\ xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x18\ xef\xbf\xbd\xef\xbf\xbd\x02
write	/data/data/com.manager.appinstaller/cache/	\xd4\xb4y6\xef\xbf\xbdM\xef\xbf\xbd\zyl\x03\xef\xbf\xbd&\ xef\xbf\xbd\xef\xbf\xbdRd\ xef\xbf\xbd\xef\xbf \xbdE-\ xef\xbf\xbd\x\$mi%\ xef\xbf\xbd\x1eCf\ xef\xbf\xbd\xef\xbf\xbd(\ xef\xbf\xbd4T\ xef\xbf\xbd\xef\xbf \xbd\xef\xbf\xbdK-G\x04\ xef\xbf\xbd\ xef\xbf\xbdK:\x09#a2\ xef\xbf\xbd#o\x08DT\x06\ xef\xbf\xbdW,
write	/data/data/com.manager.appinstaller/cache/	\3jmy\ xef\xbf\xbdQ\ xef\xbf\xbd\x19\x0f\ xef\xbf\xbdA\ xef\xbf\xbd\xef\xbf\xbd\x150\ xef\xbf\xbd\x7f2E\ ef \xbf\xbd;\x1d\ xef\xbf\xbd\x0b\ xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdD\ xef\xbf \xbd\ x0c\ xef\xbf\xbdH\ xef\xbf\xbd\x1b\x0a\ xef\xbf\xbd\xef\xbf\xbd\x0c\ o\x03\ xef\xbf\xbdD\ xef\xbf\xbd L\x15H\ xef\xbf\xbdw3h~\ xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x19\ xef\xbf\xbdz\ xef\xbf\xbd\xef\xbf\xbd" M\ xef\xbf\xbdv\ xdb\ xba\x0f\ xef\xbf\xbd\x00r\ xef\xbf\xbd
write	/data/data/com.manager.appinstaller/cache/	\3jmy\ xef\xbf\xbdQ\ xef\xbf\xbd\x19\x0f\ xef\xbf\xbdA\ xef\xbf\xbd\xef\xbf\xbd\x150\ xef\xbf\xbd\x7f2E\ ef \xbf\xbd;\x1d\ xef\xbf\xbd\x0b\ xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdD\ xef\xbf \xbd\ x0c\ xef\xbf\xbdH\ xef\xbf\xbd\x1b\x0a\ xef\xbf\xbd\xef\xbf\xbd\x0c\ o\x03\ xef\xbf\xbdD\ xef\xbf\xbd L\x15H\ xef\xbf\xbdw3h~\ xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x19\ xef\xbf\xbdz\ xef\xbf\xbd\xef\xbf\xbd" M\ xef\xbf\xbdv\ xdb\ xba\x0f\ xef\xbf\xbd\x00r\ xef\xbf\xbd
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbd_\x1aN\x19\ xef\xbf\xbd0G\x100\x074\ xef\xbf\xbdm\ xef\xbf\xbd<96@<\ xef\xbf\xbd\xef\xbf\xbd\xcf\xaa\ ef \xbf\xbd\ xef\xbf\xbdK\ Xf\x09\ xef\xbf\xbd\xef\xbf\xbd\x0a\ xef\xbf\xbd\ xef\xbf\xbdj\ ;br\x04\ xab\x03\ xef\xbf \xbd\x15a\ xef\xbf\xbd\x0b\ xc2\ x82A\ xef\xbf\xbd\xef\xbf\xbdp+\ xef\xbf\xbdj\ x02<\ xef\xbf\xbd\xef\xbf\x bd
write	/data/data/com.manager.appinstaller/cache/	w\ xef\xbf\xbd\xef\xbf\xbd*\ xef\xbf\xbd\xef\xbf\xbd.\ xef\xbf\xbd\xef\xbf\xbd# [\ xef\xbf\xbd\xef\xbf\xbd8U\ xef\xbf\xbd)0\ xef\xbf\xbd\x1d5\x93\ xef\xbf\xbdT\ xef\xbf\xbd\xef\xbf\xbdG\ x ef\xbf\xbdq^!\x17\x04\ xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd^*\ xef\xbf\xbd\xcb\ xbe\ xef\xbf\xbd\xef\xbf\xbd\ xef\xbf\xbdn\ xef\xbf\xbd*&aK\x1c\ xef\xbf\xbd\ xef\xbf\xbd\ xef\xbf\xbd\ xef\xbf\xbd\ xef\xbf\xbd\x1f\ xef\xbf \xbd
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x1bA\x01,J\x08\ xef\xbf\xbd\xef\xbf\xbdj\ s\ xef\xbf\xbd\x1a\ xef\xbf\x bd\ xef\xbf\xbdj\ xef\xbf\xbd<\ xef\xbf\xbdX\ xef\xbf\xbd\xef\xbf\xbd&\ xef\xbf\xbd\xef\xbf\xbd? m\ xef\xbf\xbdK\ xef\xbf\xbdJ\x19F\ xef\xbf\xbd\x03\ xef\xbf\xbd\xef\xbf\xbd\x15N\ xef\xbf\xbd\ xef\xbf\xbd \x15N\ xef\xbf\xbd\ xef\xbf\xbd\x1x02w~\ xef\xbf\xbd\ xef\xbf\xbd\ xef\xbf\xbdq\x2\x8b\x18\ xef\xbf \xbd\x11\x12
write	/data/data/com.manager.appinstaller/cache/	~\ xef\xbf\xbd.\ xef\xbf\xbd\xef\xbf\xbd2\ xef\xbf\xbd\xef\xbf\xbd_\ xef\xbf\xbd\xef\xbf\xbd/Zi\x1c\ xef\xbf\x bd\$E\ xef\xbf\xbd\x9\x1b1%\ xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x0b\ xef\xbf\xbd\x15I=\ xef\xbf\xbd\x0f\ xef\xbf\xbd\xef\xbf\xbd:\ xef\xbf\xbdm*\x1e\ xef\xbf\xbdW\ xef\xbf\xbd\ xef\xbf\xbd\ xef\xbf\xbd\ x0f\ x2G \ xef\xbf\xbd\ xef\xbf\xbd6\ xef\xbf\xbd<\ xcd\ xa6Nz\ xef\xbf\xbd\ xef\xbf\xbd#\ xef\xbf\xbd\ xef\xbf\xbd

Operation	File Path	Data
write	/data/data/com.manager.appinstaller/cache/	\xcb\xbf\xef\xbf\xbd\x1b\xef\xbf\xbd\xef\xbf\xbd\x08\xef\xbf\xbd5? \xef\xbf\xbdP\xef\xbf\xbdQ\xef\xbf\xbdK\xef\xbf\xbd\xef\xbf\xbdY\xef\xbf\xbd\xc3\xae#\xef\xbf\xbd\x0d PNI\x02ICHy-cV\x10\xef\xbf\xbd^\x0f\xef\xbf\xbd\x15\x0d\xef\xbf\xbd\xef\xbf\xbdZ\xef\xbf\xbd] \xef\xbf\xbd\xef\xbf\xbd_\x00\xef\xbf\xbd\xef\xbf\xbd!\xef\xbf\xbd\xef\xbf\xbd>H\xef\xbf\xbdv\x0d
write	/data/data/com.manager.appinstaller/cache/	}\xef\xbf\xbdO\xef\xbf\xbd\xef\xbf\xbd\x1aV\x019\x0c\xef\xbf\xbdJ\xef\xbf\xbd\xcf\x93\xef\xbf\xbd\xef xbf\xbd\xef\xbf\xbdv\x15\xef\xbf\xbd\x1f_\x0f\xef\xbf\xbd\x0d\xef\xbf\xbdF? \xef\xbf\xbdTn\xef\xbf\xbdh\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd%4 4z!\x17\xef\xbf\xbdB9\x010\xef\xbf\xbd#\xef\xbf\xbd\xef\xbf\xbd7Of
write	/data/data/com.manager.appinstaller/cache/	D\xef\xbf\xbd\x06\x19\xef\xbf\xbd@z\x0cL\x12\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf \xbd:\x0f\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdK\x03H\x1e\xef\xbf\xbd\xef\xbf\xbd\x1e5\xef\xbf\x bd2o\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x16p\xef\xbf\xbd\xef\xbf\xbd\x01s1\xdb\xa9\xef\xbf\xbd)M\x1 2\xef\xbf\xbdm\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x0f\xef\xbf\xbd\xef\xbf\xbdn
write	/data/data/com.manager.appinstaller/cache/	e \x1c;\xef\xbf\xbd6\xef\xbf\xbd[\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd83eh\xef\xbf\xbd\xef\xbf\xbd\xef\xbf xbd"\x0c\xef\xbf\xbd*a+7\xef\xbf\xbd\xcc\xa3\x179YxU\xef\xbf\xbd0\xef\xbf\xbd\xef\xbf\xbd\xcf\x99O u\xef\xbf\xbd'\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd3n\$M\xef\xbf\xbd\x1b\xef\xbf\xbd~\xef\x b\xbd\xef\xbf\xbd!\x1b\x1e
write	/data/data/com.manager.appinstaller/cache/	j\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdh\x00\xef\xbf\xbd%\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd \x07\xef\xbf\xbd\x07\xef\xbf\xbd\xef\xbf\xbd\x09\x94;\x01\xef\xbf\xbd\x0cE3\x18\xef\xbf\xbdrl_'a\xef xbf\xbd0\xef\xbf\xbdMdl\xef\xbf\xbdj\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x14\x 16\x02\xef\xbf\xbd\xef\xbf\xbdO\xef\xbf\xbd9\x1c\xde\x89(
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbd:\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd}\xe8\x83\x9f\xef\xbf\xbd\xef\xbf\xbd'\xef\xbf\xbdm\x d6\x7\xef\xbf\xbd\x08\x85P\xef\xbf\xbd\xef\xbf\xbd\x00- \xc6\x8c4\x14\xdd\x90\x04\xef\xbf\xbd\xef\xbf\xbd\x04\xef\xbf\xbd\x11eZ\x11\xef\xbf\xbdC,\xef\xbf\x dK\xef\xbf\xbd\xef\xbf\xbdU@\x0c\xef\xbf\xbd0\xef\xbf\xbd\x1be\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x ef\xbf\xbdHV
write	/data/data/com.manager.appinstaller/cache/	@\xef\xbf\xbd\xef\xbf\xbd\x07Clij\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x0c\xef\xbf\xbd\xef bf\xbd\xef\xbf\xbd\x05\x96\xef\xbf\xbd'jaR\x1b\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xce\xbf xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xda\xa9hG\xef\xbf\xbdn\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf xbd\x1c\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x0b\xef\xbf\xbd\xef\xbf\xbd<\xef\xbf\xbd\xef\xbf\xbd~\xef xbf\xbd%_ayNt
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbd[\xef\xbf\xbd\x1f\xef\xbf\xbd\x7f\xef\xbf\xbdW\x13\xef\xbf\xbd\x05\x8b\xef\xbf\xbd)ao\xef bf\xbd\xef\xbf\xbd\x01\xef\xbf\xbd\xef\xbf\xbd\xdc\x8e\xef\xbf\xbdY\xef\xbf\xbdjDqY_\xef\xbf\xbd\x0d1\ xbc\xef\xbf\xbd\xef\xbf\xbd\x1aj\xef\xbf\xbd\xef\xbf\xbdK\xef\xbf\xbd\x1fTRRny\x17rf\x01bEk\xef\xbf xbd\x19\xef\xbf\xbd6[\xef\xbf\xbd.
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbd;\x13E\x11}\xef\xbf\xbd\xef\xbf\xbdX\xef\xbf\xbd'\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdV\xef xbf\xbd\xef\xbf\xbdip\xef\xbf\xbd\xef\xbf\xbd4a\x0d0\x84\x0e%M\xef\xbf\xbd\xef\xbf\xbd\x1f\xef\xbf\xbd t\xef\xbf\xbd\x05\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdR\xef\xbf\xbd.\xef\xbf\xbd\xef\xbf\xbd 14:\xef\xbf\xbd\xef\xbf\xbd\x12\xef\xbf\xbd\x03a\xef\xbf\xbd\xef\xbf\xbd\x05y\xef\xbf\xbd\xef\xbf\xbd
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbd\xca\x90\xef\xbf\xbd\xef\xbf\xbd\x0a7y9a\xef\xbf\xbd\xef\xbf\xbdQ\xef\xbf\xbd\xef\xbf\xbd S+\x0a\xef\xbf\xbd\xef\xbf\xbd\x7fDax\xef\xbf\xbd3V\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x ef\xbf\xbd \xef\xbf\xbd\x09\xef\xbf\xbd\xef\xbf\xbdj\x16\xef\xbf\xbd\x0d7\x966\xda\x89+O\xef\xbf\xbd\xef\xbf\xbd d:\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdD\xef\xbf\xbdN\xef\xbf\xbd*_
write	/data/data/com.manager.appinstaller/cache/	PK\x03\x04\x14\x00\x08\x08\x08\x00\xef\xbf\xbdX\xef\xbf\xbd\x00\x00\x00\x00\x00\x00\x00\x00\x00 x00\x00\x00\x0b\x00\x04\x00classes.dex\xef\xbf\xbd\xef\xbf\xbd\x00\x00\xef\xbf\xbd[\x0bt[G\xef\xbf\x bd\xef\xbf\xbdG\x0f\xef\xbf\xbdt- \xef\xbf\xbd\xef\xbf\xbd\x13;\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdV\x1eN\xef\xbf\xbd\$\xef\xbf\xbd,\xef bf\xbdR\xef\xbf\xbd4\xef\xbf\xbd\xef\xbf\xbdY\xef\xbf\xbdv\x17tm%\xef\xbf\xbd\x0c\x8b6,\xef\xbf\xbd\ x01\xef\xbf\xbd\x0dP
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdzk\xef\xbf\xbd\xdf\x90\xef\xbf\xbd\xef\xbf\xbd9=#d<F\xef\xbf\xbdq\ xef\xbf\xbd\xef\xbf\xbdN'a\xef\xbf\xbd[\xef\xbf\xbd[\xef\xbf\xbd\x05\xef\xbf\xbdW=q\xdf\x823\x13_zv\x c7\xaf5f\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdL\x16\xef\xbf\xbd\x08\xa1\x0c3/W\x16v'\xef\xbf\xbd;^
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbd\xef\xbf\xbd\x03_\x1c0\xef\xbf\xbdC%\xef\xbf\xbd\xef\xbf\xbd_d\xef\xbf\xbd0Z\xef\xbf\xbd \xef\xbf\xbd%\xef\xbf\xbd'\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x08\x16=w\xef\xbf\xbd\x0b\ xef\xbf\xbd\xef\xbf\xbdY\xc6\xb8\xef\xbf\xbd\xef\xbf\xbdma9jS[\xef\xbf\xbd>\xef\xbf\xbdQ1+\x1f\xef\x b\xbd\x1cs\xef\xbf\xbd\x03\xef\xbf\xbd\xef\xbf\xbdS

Operation	File Path	Data
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbd\xXg^\x1c\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd(m\xef\xbf\xbd\x16\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdquO\xef\xbf\xbd\x8\xa9' \xef\xbf\xbd\xef\xbf\xbdA\xef\xbf\xbd\x0/\x0\xef\xbf\xbd\xef\xbf\xbdO\xef\xbf\xbd\xef\xbf\xbd, \xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd1("\x1e\x00\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd^\x1f\xef\xbf\xbd\xef\xbf\xbd\x0e2
write	/data/data/com.manager.appinstaller/cache/	Afp\x07\xef\xbf\xbd\xef\xbf\xbd\xc9\xb9 \xd0\x950ni\xef\xbf\xbd\x6\xa5\xef\xbf\xbd\x09\xef\xbf\xbd\xef\xbf\xbd!\xef\xbf\xbd!\xef\xbf\xbd\xd7\xbf\xef\xbf\xbdR\xef\xbf\xbd\xef\xbf\xbd\x14.\x1av\xef\xbf\xbd"Vu\xef\xbf\xbd\x09@\x1fr\x16r\xef\xbf\xbd\x1b\x18\xef\xbf\xbd\xef\xbf\xbdiz\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdj \x11[\xef\xbf\xbd
write	/data/data/com.manager.appinstaller/cache/	\x1f\xef\xbf\xbd\rj8\xef\xbf\xbdT/Yw\xef\xbf\xbdN0\xef\xbf\xbd\xef\xbf\xbd.\xef\xbf\xbd\xef\xbf\xbd\x18\xef\xbf\xbdN\xef\xbf\xbd&\xef\xbf\xbd\x02\x0cp\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdHpN\x1a_\xc6\x8b\xef\xbf\xbdP\xef\xbf\xbd\xef\xbf\xbdY\xdc\x9f\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x08e\x06\xef\xbf\xbdv22A@\xcb\xa6R\xef\xbf\xbd(2
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbdB\xef\xbf\xbd\x0\x93wVB\x06\xef\xbf\xbd\xef\xbf\xbd\x7fU.\xef\xbf\xbd^KF\xef\xbf\xbd\xef\xbf\xbd\x04\xef\xbf\xbdC:\xef\xbf\xbd7t>&\xef\xbf\xbd>Y7G\xef\xbf\xbd,;\xef\xbf\xbd\xef\xbf\xbd\x0f%\x1f\xef\xbf\xbdX\xef\xbf\xbd\xef\xbf\xbd7j\xef\xbf\xbdY\x1fxd5\x80.\xef\xbf\xbd72/q
write	/data/data/com.manager.appinstaller/cache/	M+\xef\xbf\xbdn\xd2xad\xef\xbf\xbdS\xd6\xb5w\xef\xbf\xbd\xef\xbf\xbd6\xf3\x8a\x8f\xa6\xef\xbf\xbd4W\xef\xbf\xbdFfa\xef\xbf\xbd\xef\xbf\xbdh\x1b8\x0eao'\xef\xbf\xbd+/\x1P\xef\xbf\xbd\xef\xbf\xbdj \xef\xbf\xbd\x0dx\xef\xbf\xbdD\xef\xbf\xbd<\xef\xbf\xbd\xef\xbf\xbd\x1d\xef\xbf\xbd\xef\xbf\xbdF@
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbdp\xef\xbf\xbd\x10T\xef\xbf\xbdz\xef\xbf\xbd9v\xef\xbf\xbd\xef\xbf\xbdM\xef\xbf\xbdg:\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x0e\xef\xbf\xbd2J\xef\xbf\xbd\xef\xbf\xbd\x05\xef\xbf\xbd.\x16\xef\xbf\xbd6?\x1P\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdY\xef\xbf\xbd\xdf\xa0B\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdV\xef\xbf\xbd\x11C\x7f\xef\xbf\xbd\x0a\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdH\x12
write	/data/data/com.manager.appinstaller/cache/	\x05G\xef\xbf\xbd\xef\xbf\xbdU\xef\xbf\xbd\xef\xbf\xbd5\xef\xbf\xbd\x19+\xef\xbf\xbd\xef\xbf\xbd\x03\xef\xbf\xbd\x11\xef\xbf\xbd"\xef\xbf\xbd5\xef\xbf\xbd\x17\xde\xacF\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd91[\xef\xbf\xbd\xef\xbf\xbdY\xef\xbf\xbd\xe5\xa3\xab\xef\xbf\xbd"\xef\xbf\xbdFW\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdj \xef\xbf\xbdy0'\x1d=\xef\xbf\xbd\x15\xef\xbf\xbdP\xef\xbf\xbd\xef\xbf\xbdN\x0d
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbd\x14\xef\xbf\xbd\x10\xef\xbf\xbd.\xef\xbf\xbd\xef\xbf\xbd\x1fx00\xef\xbf\xbd\x0d{k\x1d\xef\xbf\xbd\xef\xbf\xbd:\xef\xbf\xbdj E\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd"\xdf\xa0\xef\xbf\xbd\xef\xbf\xbdJ\xef\xbf\xbd\xef\xbf\xbd\x11\xef\xbf\xbdv\xef\xbf\xbd@(\x16KJ)\xef\xbf\xbd9hD\xef\xbf\xbdm\xef\xbf\xbdD\xef\xbf\xbd\x06\xef\xbf\xbd\xdb\xb3A\xef\xbf\xbd#\xef\xbf\xbd\x0a
write	/data/data/com.manager.appinstaller/cache/	w\xef\xbf\xbd"\x02N5\xef\xbf\xbdA^\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd[v\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd_\x07\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdV%\xef\xbf\xbd\xef\xbf\xbd\x15\xef\xbf\xbd\xcd\xbd4\xef\xbf\xbdT\xef\xbf\xbd\x0d\xef\xbf\xbd:\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd8\x1a\x14
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbd\xef\xbf\xbd4\x12l>\xef\xbf\xbd@Zy,*[K\xef\xbf\xbd\xef\xbf\xbd1)\xef\xbf\xbd>x\xef\xbf\xbdCkD\x00\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x05\xa2\xef\xbf\xbdN,\xef\xbf\xbd\xef\xbf\xbd\x03\x7f\xef\xbf\xbdX\xef\xbf\xbd8k@\xef\xbf\xbd\xef\xbf\xbd\x0e\xef\xbf\xbd\xc3\x87\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdCt
write	/data/data/com.manager.appinstaller/cache/	\x05\x01\x0e\x04\x11Zp\xef\xbf\xbd@\xef\xbf\xbd\xef\xbf\xbd5\xef\xbf\xbdS\x0\xef\xbf\xbd\xef\xbf\xbd\x00\xef\xbf\xbd-\x09F\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd;\x08\x1fx0b\xef\xbf\xbd\xcc\x8fO\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd~\xef\xbf\xbd\xe8\x96\x90\x03\xef\xbf\xbd=\x07}a\xef\xbf\xbd\xef\xbf\xbd+, \xd5\xa3G\xef\xbf\xbd\x12\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbd\xef\xbf\xbdR\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdH\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x0bS\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdn?\x1b@\xef\xbf\xbdX\xef\xbf\xbd8qz\xef\xbf\xbd\xef\xbf\xbd~st\xef\xbf\xbd\x06\xef\xbf\xbd[\xef\xbf\xbd\xef\xbf\xbd\x0b\x1a\xef\xbf\xbd&\xdb\x88\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdQW1"Z\x09\x98\xef\xbf\xbd
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbdv\xef\xbf\xbd\x7f\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdO\x1eV\x0e\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x11M\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x1d\xef\xbf\xbd\$[m[\xef\xbf\xbd\x18\x1fx16\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x19\xef\xbf\xbd\xef\xbf\xbdq\xef\xbf\xbdFS\xef\xbf\xbdh\x00\xef\xbf\xbd\xef\xbf\xbdhj\xef\xbf\xbd\xcc\x92y\xef\xbf\xbdpIn\x02\xef\xbf\xbd\xcd\x88

http://sanddroid.xjtu.edu.cn/report?apk_md5=FBB1697176295E070B55C331EFC7EAB

Operation	File Path	Data
write	/data/data/com.manager.appinstaller/cache/	\x0a\xef\xbf\xbd\x06\xef\xbf\xbd\xef\xbf\xbdg\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd0Vw)\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x18\xef\xbf\xbd[B\xc2\xb8\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x11\xef\xbf\xbd\x0c6\xb3%\x16\xef\xbf\xbd\xef\xbf\xbd\x06\xdd\xa8\xef\xbf\xbdBZ\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x059\xef\xbf\xbd2\C!?\xef\xbf\xbd\xef\xbf\xbdca4
write	/data/data/com.manager.appinstaller/cache/	K\x0e\xef\xbf\xbd\xef\xbf\xbd\x1f+\x18\x0a^\xef\xbf\xbd\xef\xbf\xbd\xce\x8c\x10\x14\xef\xbf\xbd\xef\xbf\xbd\x18\xef\xbf\xbd3;#\xef\xbf\xbdF\xef\xbf\xbd,yShF\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x03e\x05/\x01\xd9\x88\xef\xbf\xbd\xef\xbf\xbd\x0c7\x91\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x09\x05\xbf\xef\xbf\xbd\x14
write	/data/data/com.manager.appinstaller/cache/	E\x0b\xef\xbf\xbd\x07\x8b\xef\xbf\xbd4\x12\x03\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdJ\xef\xbf\xbd7\xef\xbf\xbdT\x10q\xef\xbf\xbd\x17\xef\xbf\xbd+\xef\xbf\xbd\xe6\xbe\x96\xef\xbf\xbd6\xef\xbf\xbd>\xce\x8b\x0c\xef\xbf\xbd\xef\xbf\xbd\x0c\x0a\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd;\xcel\xb7\xef\xbf\xbd\xef\xbf\xbd\xbd\x07\xef\xbf\xbd\x10\xef\xbf\xbd\x18\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x06\x93\xef\xbf\xbd
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbd\$\xef\xbf\xbdM\xef\xbf\xbd\x0cU\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdJ\xef\xbf\xbd\x0e5\xef\xbf\xbd\x0c\x1a\xef\xbf\xbd\xef\xbf\xbd\x04D\x0d\x81\x1b\x09\x13@\xef\xbf\xbd6\xef\xbf\xbd4\xef\xbf\xbd\xef\xbf\xbdp\xef\xbf\xbdB\xef\xbf\xbd9\x12[U\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd^\xef\xbf\xbd;\xef\xbf\xbdV\x15\xef\xbf\xbd\x12\xef\xbf\xbd
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdH'\x7f\xef\xbf\xbd\x14\xef\xbf\xbd\xef\xbf\xbdH\xef\xbf\xbd\x1f\xef\xbf\xbd\xef\xbf\xbdV@h\xef\xbf\xbd9(\xef\xbf\xbd{\xef\xbf\xbd1\x12\x0f\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd*\x05\xef\xbf\xbd\x05\xef\xbf\xbd S\xef\xbf\xbdQNn\xef\xbf\xbd\xcf\xa2\xef\xbf\xbdZ\x13\xd7\xbd\xef\xbf\xbd\xef\xbf\xbd\x19\xef\xbf\xbd\x14\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd
write	/data/data/com.manager.appinstaller/cache/	"\xef\xbf\xbd\xef\xbf\xbd\b\x00\xc5\x89\xef\xbf\xbd\x0a\x023(y\xef\xbf\xbd\xef\xbf\xbd=E\xef\xbf\xbd\x19\xef\xbf\xbd>\x15\x1aZ\x12\xef\xbf\xbd\xef\xbf\xbdOX\x17\x13\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd<\xef\xbf\xbd\x13\xef\xbf\xbd"w\xef\xbf\xbd"\xef\xbf\xbd\xef\xbf\xbd\x19\xef\xbf\xbd\x15\xef\xbf\xbdR>b\xef\xbf\xbd\xef\xbf\xbdh\x15\x07\x0a_8\$\xef\xbf\xbdG
write	/data/data/com.manager.appinstaller/cache/	f\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdG\xef\xbf\xbd\x18\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x06\x97\xef\xbf\xbd;\xef\xbf\xbd4\x02\x80\xa8\xb6\xef\xbf\xbd,\xef\xbf\xbd\x12s\xef\xbf\xbdc\xef\xbf\xbd\$\xef\xbf\xbdm\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdhJ\xef\xbf\xbd\x19;\xef\xbf\xbd\xef\xbf\xbd\xbd \x06\x1d\xef\xbf\xbd\xef\xbf\xbdLo\x1c\xef\xbf\xbd\x0d\xef\xbf\xbd\x03\xef\xbf\xbd~\xef\xbf\xbd4
write	/data/data/com.manager.appinstaller/cache/	2\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdDNg\x07\x11mMj\x0an\xef\xbf\xbd\x1c\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x03^Q)%eqA9\x03'\xef\xbf\xbd\x07\xb8\x0d\xef\xbf\xbd\x07\xa0DH\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdg8\x1c\xef\xbf\xbdv&\xef\xbf\xbd\x06\xef\xbf\xbd\x06q\xef\xbf\xbd\xef\xbf\xbdH\xef\xbf\xbd0\xef\xbf\xbd\x16
write	/data/data/com.manager.appinstaller/cache/	e\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd%\xef\xbf\xbd\x13'\xef\xbf\xbd\x0a\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdI\xef\xbf\xbd\x19\xef\xbf\xbdp\x0a+r\xef\xbf\xbdh\xc8\xbe!\x11\x01\xd5\x90i\xef\xbf\xbd<g\x10\x15\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd"\xef\xbf\xbd\x15\x10\xc4\x95d\x16\xef\xbf\xbd\x0fx\xef\xbf\xbd!! Pw\x0fO\xef\xbf\xbd
write	/data/data/com.manager.appinstaller/cache/	JBn\x1f\xef\xbf\xbd5? 1;\xcd\x96\xef\xbf\xbd\x0a0a\x09!\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd1\xef\xbf\xbdW\xef\xbf\xbd\x1a9I\x13\x02\xef\xbf\xbd? \xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd(\x1f\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xbd\xef\xbf\xbdZ\xef\xbf\xbd\xef\xbf\xbdXT.\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdW\xef\xbf\xbd\xef\xbf\xbd9<
write	/data/data/com.manager.appinstaller/cache/	j>L\x0c\x14sJ\x01&D\xef\xbf\xbd\xef\xbf\xbdE\xef\xbf\xbd\x02\xef\xbf\xbd\x10'\xef\xbf\xbdB6\xef\xbf\xbd\xe4\x9e\xb9Gr\x1f\xef\xbf\xbd\xef\xbf\xbd^\x07\xef\xbf\xbd\x02\x01\xef\xbf\xbd\x18\x03\x0aK\xef\xbf\xbd\xef\xbf\xbd.\xef\xbf\xbd\x05\xa3J\xef\xbf\xbd1.)Q\xcc\x81\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdp\xef\xbf\xbd
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbd\xef\xbf\xbdA\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdW\xef\xbf\xbd\xef\xbf\xbdZ\x1e\x1dh(\x09\xef\xbf\xbd.\x7f\xef\xbf\xbd4\xef\xbf\xbdC\xef\xbf\xbdWJ\xef\xbf\xbdU\xef\xbf\xbd\x1e*? r\xef\xbf\xbd\xef\xbf\xbd>rZ\xef\xbf\xbd\xef\xbf\xbd#\xef\xbf\xbdJ\xef\xbf\xbd\xef\xbf\xbd\x02\x02\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd<<\xef\xbf\xbdS\x0c\x10_\xef\xbf\xbd\xef\xbf\xbd
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbd\xef\xbf\xbdU@\xef\xbf\xbd\xef\xbf\xbd%\xef\xbf\xbd\xef\xbf\xbdF\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x10\x1c6W\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x0fu\xef\xbf\xbdJ\xef\xbf\xbd2\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x02e\x07\x9b\x11\xef\xbf\xbd\x09\xca\x9f\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdK\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x14;\xbd\xb0\xef\xbf\xbd\xef\xbf\xbd(vFw\xef\xbf\xbd0

11/28

Operation	File Path	Data
write	/data/data/com.manager.appinstaller/cache/	2\xef\xbf\xbd\xdc\xbd\xef\xbf\xbdF)~\xef\xbf\xbd-~Lw\x1e\xef\xbf\xbd\x16;;\xef\xbf\xbd\xef\xbf\xbd4\xef\xbf\xbd\xef\xbf\xbd2\xef\xbf\xbd\x16\xef\xbf\xbdO\xef\xbf\xbd6\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd9f\xef\xbf\xbd)\xef\xbf\xbd\xd5\x89\x1d\xef\xbf\xbd\x14\xd1\xbf\x07\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdW8\xef\xbf\xbd\x1e&s
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbdj)\xef\xbf\xbd\xef\xbf\xbdj)\xef\xbf\xbd\xef\xbf\xbdxc3\xa4\xef\xbf\xbd\x1aub\xef\xbf\xbd\xef\xbf\xbd\$\xef\xbf\xbd\xdc\x0fb\x01\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdD\xef\xbf\xbdw\xef\xbf\xbd\x01\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdA`/\x05\x0d[\xef\xbf\xbd&\xef\xbf\xbd\x14\xef\xbf\xbd5\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdMw\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x05
write	/data/data/com.manager.appinstaller/cache/	\xef\xbf\xbd\xef\xbf\xbd1\x07l\xef\xbf\xbdY\x1eQ\xef\xbf\xbd\xef\xbf\xbdNR\xef\xbf\xbd\xef\xbf\xbdjs"k7p\x1cw\xef\xbf\xbd\x1c\xef\xbf\xbdw\xef\xbf\xbdndmP\x01oN\x11\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x1e\xef\xbf\xbd\x19\x1d\xef\xbf\xbd/[\xef\xbf\xbdw\x1b-\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdV\xef\xbf\xbd:\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd
write	/data/data/com.manager.appinstaller/cache/	IG\x14\xef\xbf\xbd\x1c\xef\xbf\xbd\x1\x8b? \xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdY\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdq\xef\xbf\xbdZ\xef\xbf\xbd\x1\x88\xef\xbf\xbd\x03#\xef\xbf\xbdD\xef\xbf\xbd\x1pKC\xef\xbf\xbd0\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd{\xef\xbf\xbdW\xef\xbf\xbd_F_\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdSiJ
write	/data/data/com.manager.appinstaller/cache/	jd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x15\xef\xbf\xbd4\xef\xbf\xbd\xef\xbf\xbdC&\xdc\x82j)\xef\xbf\xbdAJCb\xef\xbf\xbd\xef\xbf\xbd@\xef\xbf\xbd)b\xef\xbf\xbd\x11l\x00\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x19\x7fE\xef\xbf\xbdG\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdh\x00Q\x1d\x1xba\xef\xbf\xbd\x04\x1a8i\xef\xbf\xbd\xef\xbf\xbdA\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\x10\x05\xe5\x88\x81
write	/data/data/com.manager.appinstaller/cache/)\xef\xbf\xbd\x01\xef\xbf\xbd\x15\x7f\xef\xbf\xbdqY\x09\xef\xbf\xbdN\xef\xbf\xbd\xef\xbf\xbd\x0b\xef\xbf\xbdj)\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdMbJ\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\$\xef\xbf\xbd\xef\xbf\xbd6\xef\xbf\xbdj)\x16\xec\x86\x9cHd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdK\x17\xef\xbf\xbd\xef\xbf\xbd\x1e\xef\xbf\xbd>(\. \xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd

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: Landroid/content/pm/PackageManager;->getInstalledPackages**
 - Description: Gets packages installed on the device
 - Caller Code: Lcom/manager/appinstaller/use/d;->i(Landroid/content/Context;)Ljava/util/List;
 - Threat Level:
 - Path Index: 20
- **API: Landroid/content/pm/PackageManager;->getInstalledPackages**
 - Description: Gets packages installed on the device
 - Caller Code: Lcom/manager/appinstaller/use/d;->q(Landroid/content/Context; Ljava/lang/String;)Z
 - Threat Level:
 - Path Index: 22
- **API: Landroid/telephony/TelephonyManager;->getDeviceId**
 - Description: Gets the unique device ID, IMEI for GSM and MEID for ESN or ESN for CDMA phones
 - Caller Code: Lcom/manager/appinstaller/use/d;->g(Landroid/content/Context;)Ljava/lang/String;
 - Threat Level:
 - Path Index: 30
- **API: Landroid/telephony/TelephonyManager;->getDeviceId**
 - Description: Gets the unique device ID, IMEI for GSM and MEID for ESN or ESN for CDMA phones
 - Caller Code: Lcom/manager/appinstaller/use/d;->g(Landroid/content/Context;)Ljava/lang/String;
 - Threat Level:
 - Path Index: 52
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/a;->b(Landroid/content/Context;)Ljava/util/List;
 - Threat Level:
 - Path Index: 752
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/a;->b(Landroid/content/Context;)Ljava/util/List;
 - Threat Level:
 - Path Index: 976
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->d(Ljava/lang/Object;)V
 - Threat Level:
 - Path Index: 166
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->d(Ljava/lang/Object;)V
 - Threat Level:
 - Path Index: 252
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->d(Ljava/lang/Object;)V
 - Threat Level:
 - Path Index: 592
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->d(Ljava/lang/Object;)V
 - Threat Level:
 - Path Index: 736














- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 850
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 942
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 1140
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 1256
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 1322
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 1388
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 1454
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 1534
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 1616
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->e(l)Ljava/lang/Object;
 - Threat Level: 
 - Path Index: 140
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->e(l)Ljava/lang/Object;
 - Threat Level: 
 - Path Index: 186
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level: 
 - Path Index: 212
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level: 
 - Path Index: 236
- **API:Ljava/lang/reflect/Method;->invoke**














- Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level: 
 - Path Index: 392
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level: 
 - Path Index: 946
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level: 
 - Path Index: 994
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level: 
 - Path Index: 1258
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level: 
 - Path Index: 1498
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level: 
 - Path Index: 1586
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level: 
 - Path Index: 1750
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level: 
 - Path Index: 1876
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level: 
 - Path Index: 1970
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/a/b;->a()V
 - Threat Level: 
 - Path Index: 126
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/google/ads/g\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 166
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/google/ads/g\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 252
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/google/ads/g\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 592
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection

- Caller Code: Lcom/google/ads/g\$a;->d(Ljava/lang/Object;)V
- Threat Level:
- Path Index: 736
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/google/ads/g\$a;->d(Ljava/lang/Object;)V
- Threat Level:
- Path Index: 850
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/google/ads/g\$a;->d(Ljava/lang/Object;)V
- Threat Level:
- Path Index: 942
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/google/ads/g\$a;->d(Ljava/lang/Object;)V
- Threat Level:
- Path Index: 1140
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/google/ads/g\$a;->d(Ljava/lang/Object;)V
- Threat Level:
- Path Index: 1256
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/google/ads/g\$a;->d(Ljava/lang/Object;)V
- Threat Level:
- Path Index: 1322
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/google/ads/g\$a;->d(Ljava/lang/Object;)V
- Threat Level:
- Path Index: 1388
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/google/ads/g\$a;->d(Ljava/lang/Object;)V
- Threat Level:
- Path Index: 1454
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/google/ads/g\$a;->d(Ljava/lang/Object;)V
- Threat Level:
- Path Index: 1534
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/google/ads/g\$a;->d(Ljava/lang/Object;)V
- Threat Level:
- Path Index: 1616
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/google/ads/g\$a;->e(l)Ljava/lang/Object;
- Threat Level:
- Path Index: 140
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/google/ads/g\$a;->e(l)Ljava/lang/Object;
- Threat Level:
- Path Index: 186
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/google/ads/g\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level:
- Path Index: 212
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/google/ads/g\$a;->b(Ljava/lang/String;)Ljava/lang/Class;











- Threat Level:
- Path Index: 236
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/google/ads/g\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level:
 - Path Index: 392
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/google/ads/g\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level:
 - Path Index: 946
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/google/ads/g\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level:
 - Path Index: 994
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/google/ads/g\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level:
 - Path Index: 1258
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/google/ads/g\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level:
 - Path Index: 1498
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/google/ads/g\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level:
 - Path Index: 1586
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/google/ads/g\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level:
 - Path Index: 1750
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/google/ads/g\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level:
 - Path Index: 1876
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/google/ads/g\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level:
 - Path Index: 1970
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/google/ads/g;->a()V
 - Threat Level:
 - Path Index: 126
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/a\$a;->d(Ljava/lang/Object;)V
 - Threat Level:
 - Path Index: 166
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/a\$a;->d(Ljava/lang/Object;)V
 - Threat Level:
 - Path Index: 252
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/a\$a;->d(Ljava/lang/Object;)V
 - Threat Level:





- Path Index: 592
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/a\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 736
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/a\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 850
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/a\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 942
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/a\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 1140
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/a\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 1256
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/a\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 1322
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/a\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 1388
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/a\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 1454
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/a\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 1534
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/a\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 1616
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/a\$a;->e(I)Ljava/lang/Object;
 - Threat Level: 
 - Path Index: 140
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/a\$a;->e(I)Ljava/lang/Object;
 - Threat Level: 
 - Path Index: 186
- **API:Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/a\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level: 
 - Path Index: 212














- **API:Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/a\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level: 
- Path Index: 236
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/a\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level: 
- Path Index: 392
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/a\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level: 
- Path Index: 946
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/a\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level: 
- Path Index: 994
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/a\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level: 
- Path Index: 1258
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/a\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level: 
- Path Index: 1498
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/a\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level: 
- Path Index: 1586
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/a\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level: 
- Path Index: 1750
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/a\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level: 
- Path Index: 1876
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/a\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level: 
- Path Index: 1970
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/a;->a()V
- Threat Level: 
- Path Index: 126
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/a/i\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 166
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/a/i\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 252
- **API: Ljava/lang/reflect/Method;->invoke**














- Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/use/a/i/\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 592
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/use/a/i/\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 736
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/use/a/i/\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 850
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/use/a/i/\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 942
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/use/a/i/\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 1140
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/use/a/i/\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 1256
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/use/a/i/\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 1322
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/use/a/i/\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 1388
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/use/a/i/\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 1454
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/use/a/i/\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 1534
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/use/a/i/\$a;->d(Ljava/lang/Object;)V
 - Threat Level: 
 - Path Index: 1616
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/use/a/i/\$a;->e()Ljava/lang/Object;
 - Threat Level: 
 - Path Index: 140
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lcom/manager/appinstaller/use/a/i/\$a;->e()Ljava/lang/Object;
 - Threat Level: 
 - Path Index: 186
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection

- Caller Code: Lcom/manager/appinstaller/use/a/i/\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level:
- Path Index: 212
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/a/i/\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level:
- Path Index: 236
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/a/i/\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level:
- Path Index: 392
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/a/i/\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level:
- Path Index: 946
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/a/i/\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level:
- Path Index: 994
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/a/i/\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level:
- Path Index: 1258
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/a/i/\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level:
- Path Index: 1498
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/a/i/\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level:
- Path Index: 1586
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/a/i/\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level:
- Path Index: 1750
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/a/i/\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level:
- Path Index: 1876
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/a/i/\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level:
- Path Index: 1970
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/a/i/->a()V
- Threat Level:
- Path Index: 126
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e/\$a;->d(Ljava/lang/Object;)V
- Threat Level:
- Path Index: 166
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e/\$a;->d(Ljava/lang/Object;)V

- Threat Level: 
- Path Index: 252
- **API:Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 592
- **API:Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 736
- **API:Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 850
- **API:Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 942
- **API:Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 1140
- **API:Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 1256
- **API:Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 1322
- **API:Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 1388
- **API:Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 1454
- **API:Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 1534
- **API:Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 1616
- **API:Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e\$a;->e()Ljava/lang/Object;
- Threat Level: 
- Path Index: 140
- **API:Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e\$a;->e()Ljava/lang/Object;
- Threat Level: 

- Path Index: 186
- **API:Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level: 
- Path Index: 212
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level: 
- Path Index: 236
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level: 
- Path Index: 392
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level: 
- Path Index: 946
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level: 
- Path Index: 994
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level: 
- Path Index: 1258
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level: 
- Path Index: 1498
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level: 
- Path Index: 1586
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level: 
- Path Index: 1750
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level: 
- Path Index: 1876
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
- Threat Level: 
- Path Index: 1970
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/manager/appinstaller/use/e;->a()V
- Threat Level: 
- Path Index: 126
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lw\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 166

- **API:Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lw\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 252
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lw\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 592
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lw\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 736
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lw\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 850
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lw\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 942
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lw\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 1140
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lw\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 1256
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lw\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 1322
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lw\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 1388
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lw\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 1454
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lw\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 1534
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lw\$a;->d(Ljava/lang/Object;)V
- Threat Level: 
- Path Index: 1616
- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lw\$a;->e(I)Ljava/lang/Object;
- Threat Level: 
- Path Index: 140
- **API: Ljava/lang/reflect/Method;->invoke**

- Description: Utilizes Java reflection
 - Caller Code: Lw\$a;->e()Ljava/lang/Object;
 - Threat Level: 
 - Path Index: 186
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lw\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level: 
 - Path Index: 212
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lw\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level: 
 - Path Index: 236
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lw\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level: 
 - Path Index: 392
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lw\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level: 
 - Path Index: 946
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lw\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level: 
 - Path Index: 994
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lw\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level: 
 - Path Index: 1258
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lw\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level: 
 - Path Index: 1498
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lw\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level: 
 - Path Index: 1586
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lw\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level: 
 - Path Index: 1750
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lw\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level: 
 - Path Index: 1876
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lw\$a;->b(Ljava/lang/String;)Ljava/lang/Class;
 - Threat Level: 
 - Path Index: 1970
- **API: Ljava/lang/reflect/Method;->invoke**
 - Description: Utilizes Java reflection
 - Caller Code: Lw;->a()V
 - Threat Level: 
 - Path Index: 126
- **API: Ljava/net/URL;->openConnection**
 - Description: Connects to the Internet

- Caller Code: Lb;->a([Ljava/lang/String;)Ljava/lang/Void;
- Threat Level:
- Path Index: 38
- **API: Ljava/net/URL;->openConnection**
- Description: Connects to the Internet
- Caller Code: Lcom/google/ads/e;->onReceive(Landroid/content/Context; Landroid/content/Intent;)V
- Threat Level:
- Path Index: 188
- **API: Ljava/net/URL;->openConnection**
- Description: Connects to the Internet
- Caller Code: Lcom/manager/appinstaller/use/a/d;->f()Ljava/net/URLConnection;
- Threat Level:
- Path Index: 140
- **API: Ljava/net/URL;->openConnection**
- Description: Connects to the Internet
- Caller Code: Lcom/manager/appinstaller/use/a/d;->f()Ljava/net/URLConnection;
- Threat Level:
- Path Index: 198
- **API: Ljava/net/URL;->openConnection**
- Description: Connects to the Internet
- Caller Code: Lh\$a;->a([Ljava/lang/String;)Ljava/lang/Void;
- Threat Level:
- Path Index: 620
- **API: Ljava/net/URL;->openConnection**
- Description: Connects to the Internet
- Caller Code: Lx;->a([Ljava/lang/String;)Ljava/lang/Void;
- Threat Level:
- Path Index: 42
- **API: Ljavax/crypto/Cipher;->doFinal**
- Description: Encrypt or Decrypt data
- Caller Code: Lcom/manager/appinstaller/use/c;->a([B Ljava/lang/String;)[B
- Threat Level:
- Path Index: 112
- **API: Ljavax/crypto/Cipher;->doFinal**
- Description: Encrypt or Decrypt data
- Caller Code: Lcom/manager/appinstaller/use/c;->d([B)[B
- Threat Level:
- Path Index: 112
- **API: Ljavax/crypto/Cipher;->doFinal**
- Description: Encrypt or Decrypt data
- Caller Code: Lu;->b(Ljava/lang/String;)Ljava/lang/String;
- Threat Level:
- Path Index: 84

Permission Usage

- **Permission Name: android.permission.ACCESS_NETWORK_STATE**
- Used Type: Api
- Caller Code: Lcom/manager/appinstaller/use/d;->r(Landroid/content/Context;)Z
- Callee Code: Landroid/net/ConnectivityManager;->getActiveNetworkInfo()Landroid/net/NetworkInfo;
- Path Index: 26
- **Permission Name: android.permission.ACCESS_NETWORK_STATE**
- Used Type: Api
- Caller Code: Lu;->c(Landroid/content/Context;)Ljava/lang/String;
- Callee Code: Landroid/net/ConnectivityManager;->getActiveNetworkInfo()Landroid/net/NetworkInfo;
- Path Index: 26
- **Permission Name: android.permission.INTERNET**
- Used Type: Api
- Caller Code: Lb;->a([Ljava/lang/String;)Ljava/lang/Void;
- Callee Code: Ljava/net/URL;->openConnection()Ljava/net/URLConnection;
- Path Index: 38
- **Permission Name: android.permission.INTERNET**
- Used Type: Api
- Caller Code: Lcom/google/ads/e;->onReceive(Landroid/content/Context; Landroid/content/Intent;)V
- Callee Code: Ljava/net/URL;->openConnection()Ljava/net/URLConnection;
- Path Index: 188

- **Permission Name: android.permission.INTERNET**
 - Used Type: Api
 - Caller Code: Lcom/manager/appinstaller/use/a/d;->f()Ljava/net/URLConnection;
 - Callee Code: Ljava/net/URL;->openConnection()Ljava/net/URLConnection;
 - Path Index: 140
- **Permission Name: android.permission.INTERNET**
 - Used Type: Api
 - Caller Code: Lcom/manager/appinstaller/use/a/d;->f()Ljava/net/URLConnection;
 - Callee Code: Ljava/net/URL;->openConnection(Ljava/net/Proxy;)Ljava/net/URLConnection;
 - Path Index: 198
- **Permission Name: android.permission.INTERNET**
 - Used Type: Api
 - Caller Code: Lh\$a;->a([Ljava/lang/String;)Ljava/lang/Void;
 - Callee Code: Ljava/net/URL;->openConnection()Ljava/net/URLConnection;
 - Path Index: 620
- **Permission Name: android.permission.INTERNET**
 - Used Type: Api
 - Caller Code: Lx;->a([Ljava/lang/String;)Ljava/lang/Void;
 - Callee Code: Ljava/net/URL;->openConnection()Ljava/net/URLConnection;
 - Path Index: 42
- **Permission Name: android.permission.INTERNET**
 - Used Type: Api
 - Caller Code: Lb;->a([Ljava/lang/String;)Ljava/lang/Void;
 - Callee Code: Ljava/net/URLConnection;->connect()V
 - Path Index: 82
- **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.READ_PHONE_STATE**
 - Used Type: Api
 - Caller Code: Lcom/manager/appinstaller/use/d;->g(Landroid/content/Context;)Ljava/lang/String;
 - Callee Code: Landroid/telephony/TelephonyManager;->getDeviceId()Ljava/lang/String;
 - Path Index: 30
- **Permission Name: android.permission.READ_PHONE_STATE**
 - Used Type: Api
 - Caller Code: Lcom/manager/appinstaller/use/d;->g(Landroid/content/Context;)Ljava/lang/String;
 - Callee Code: Landroid/telephony/TelephonyManager;->getDeviceId()Ljava/lang/String;
 - Path Index: 52
- **Permission Name: android.permission.READ_PHONE_STATE**
 - Used Type: Api
 - Caller Code: Lcom/manager/appinstaller/use/d;->h(Landroid/content/Context;)Ljava/lang/String;
 - Callee Code: Landroid/telephony/TelephonyManager;->getSubscriberId()Ljava/lang/String;
 - Path Index: 30
- **Permission Name: android.permission.READ_PHONE_STATE**
 - Used Type: Api
 - Caller Code: Lcom/manager/appinstaller/use/d;->h(Landroid/content/Context;)Ljava/lang/String;
 - Callee Code: Landroid/telephony/TelephonyManager;->getSubscriberId()Ljava/lang/String;
 - Path Index: 52
- **Permission Name: android.permission.READ_PHONE_STATE**
 - Used Type: Intent Action
 - Callee Code: android.intent.action.PHONE_STATE
- **Permission Name: android.permission.READ_PHONE_STATE**
 - Used Type: Intent Action
 - Callee Code: android.intent.action.PHONE_STATE

Log Message

Tag	Message
-----	---------



May Log Message

Tag	Message	Caller Code	Path Index
leeeeeeeeeeeeeeeeeee ength	13	Lcom/manager/appinstaller/use/a/d;->b(Ljava/net/URLConnection;)[B	316
processTransaction result	9	Lcom/manager/appinstaller/use/a/g;->e(I Landroid/content/ContentValues; Landroid/os/Handler;)	342

ScreenShots

