Report

General Information

Analysis Start Time	2016-12-17 23:57:28
Analysis End Time	2016-12-18 00:00:16
File MD5	3E10794A612D6A199B98D78EC449678A
File Size	624.61 KB
File Name	foto321.apk
Package Name	com.cplitdo.ygzvbnoa
Version Code	3
Version Name	1.3
Min SDK	14
Target SDK	23
Max SDK	N/A
Pcap File	(/file_download?md5=3E10794A612D6A199B98D78EC449678A&type=pcap)
Logcat File	(/file_download?md5=3E10794A612D6A199B98D78EC449678A&type=logcat)

Risk Score

100

Risky Behaviors

Exist unused permissions
Utilizes Java reflection

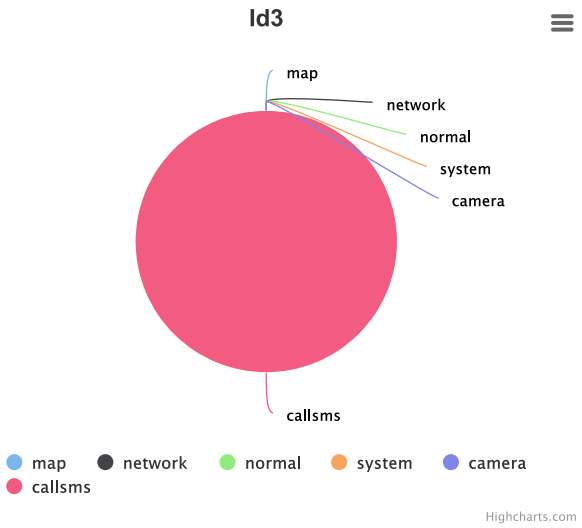
Malware Detected by VirusTotal (https://www.virustotal.com/en/file/d2ab04851db15711f509fc08069a5bcb0ca2c3f95ee4e1459c7890e205a9e1d0/ana

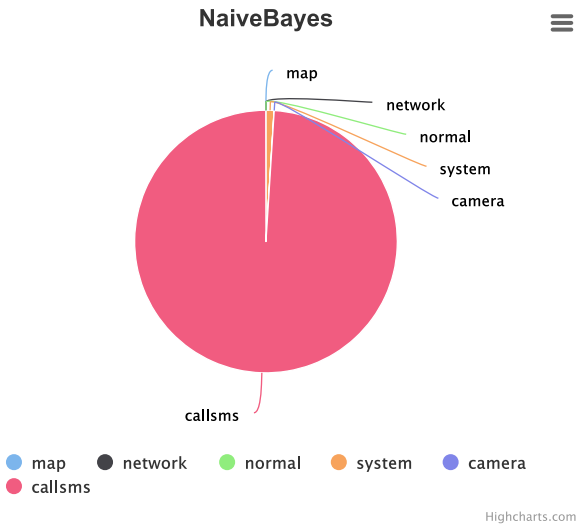
AVG	✔
Ad-Aware	✔
BitDefender	✔
ESET-NOD32	a variant of Android/TrojanDropper.Agent.APP
F-Secure	✔
Fortinet	✔
Kaspersky	✔
McAfee	✔
Qihoo-360	✔
Symantec	✔

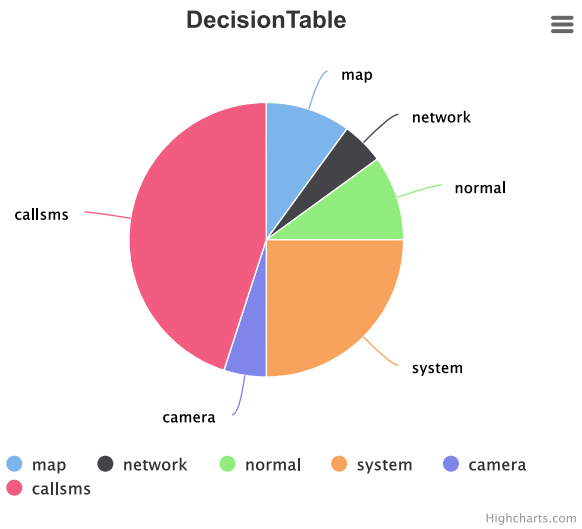
Certificate

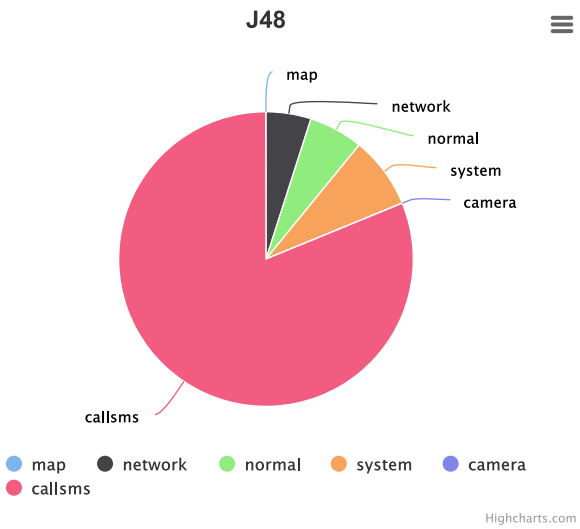
Content	Owner: CN=Uchkhd, OU=Wdyaib, O=Srwfjs, L=Vduqnqm, ST=Wzjkuwy, C=US Issuer: CN=Uchkhd, OU=Wdyaib, O=Srwfjs, L=Vduqnqm, ST=Wzjkuwy, C=US Serial number: 338ff9c2 Valid from: Sat Dec 17 02:54:55 CST 2016 until: Wed May 04 02:54:55 CST 2044 Certificate fingerprints: MD5: 09:6F:D2:34:F5:B8:15:E6:36:CE:71:A0:E4:8E:04:B0 SHA1: 3F:3C:F0:92:D5:7B:D1:E8:79:4A:AD:7D:65:64:D0:CD:D5:5C:4C:E7 SHA256: 72:08:0F:E0:E8:5C:01:51:C8:93:9A:BA:EA:05:F8:CB:54:CD:11:34:6B:1F:78:CA:52:AA:D5:71:BC:46:F1:2F Signature algorithm name: SHA256withRSA Version: 3 Extensions: #1: ObjectId: 2.5.29.14 Criticality=false SubjectKeyIdentifier [KeyIdentifier [0000: A4 D5 DA 43 AB B4 63 EF BB 5F 8E 05 47 C3 18 71 ...C..c.._..G..q 0010: A7 79 F5 7F .y..]]
Sha1	3F3CF092D57BD1E8794AAD7D6564D0CDD55C4CE7

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		✗	✗	✗	Allows applications to access information about networks
android.permission.CALL_PHONE	dangerous		✗	✗	✗	Allows an application to initiate a phone call without going through being placed.
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.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_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.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.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.VIBRATE	normal		✗	✗	✗	Allows access to the vibrator
android.permission.WAKE_LOCK	normal		✗	✗	✗	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming
android.permission.WRITE_CONTACTS	dangerous		✗	✗	✗	Allows an application to write (but not read) the user's contacts data.

Activities

Name	Main Activity	Exposed

Name	Main Activity	Exposed
com.cplitdo.ygzvbnoa.MainActivity • android.intent.action.MAIN	✔	✔
com.cplitdo.ygzvbnoa.extnvw	✘	✘
com.cplitdo.ygzvbnoa.shjldfx	✘	✘
com.cplitdo.ygzvbnoa.vmanz	✘	✘
com.cplitdo.ygzvbnoa.zmbnscs	✘	✘

Services

Name	Exposed
com.cplitdo.ygzvbnoa.bchaq	✘
com.cplitdo.ygzvbnoa.cbesdb	✘
com.cplitdo.ygzvbnoa.cnrpqnvu	✘
com.cplitdo.ygzvbnoa.faqjd	✘
com.cplitdo.ygzvbnoa.iaupk	✘
com.cplitdo.ygzvbnoa.ihlihzn	✘
com.cplitdo.ygzvbnoa.kzsditrpi	✘
com.cplitdo.ygzvbnoa.lzmgdfrfk	✘
com.cplitdo.ygzvbnoa.mnxqwswe	✘
com.cplitdo.ygzvbnoa.nahpk	✘
com.cplitdo.ygzvbnoa.psawmj	✘
com.cplitdo.ygzvbnoa.qfrbim	✘
com.cplitdo.ygzvbnoa.qjmkznob	✘
com.cplitdo.ygzvbnoa.vuxijcds	✘
com.cplitdo.ygzvbnoa.xahxushq	✘
com.cplitdo.ygzvbnoa.znuzyv	✘

Broadcast Receivers

Name	Dynamically Registered	Exposed
com.cplitdo.ygzvbnoa.rtolxqsjns • android.app.action.DEVICE_ADMIN_ENABLED	✘	✘

Name	Dynamically Registered	Exposed
com.cplitdo.ygzvbnoa.rxozkt • android.provider.Telephony.SMS_RECEIVED • android.intent.action.BOOT_COMPLETED • android.intent.action.USER_PRESENT • android.intent.action.PHONE_STATE • android.intent.action.NEW_OUTGOING_CALL	✗	✓

Content Providers

N/A

Features

N/A

Libraries

N/A

Advertisement Modules

N/A

Urls

N/A

Sensitive Files

N/A

Native Codes

N/A

Dynamic Loaders

Dex Path	Lib Path	Caller Code	Path Index
/data/app/com.cplitdo.ygzvbnoa-1.apk	N/A	N/A	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

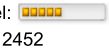
Phone Call

N/A

Data Leakage

N/A

Sensitive APIs

- **API: Ljava/lang/reflect/Method;->invoke**
- Description: Utilizes Java reflection
- Caller Code: Lcom/rcezrds/pmsalhip/d;->a(Ljava/lang/Object; Ljava/lang/Class; Ljava/lang/String; [Ljava/lang/Object;)Ljava/lang/Object;
- Threat Level: 
- Path Index: 2452

Permission Usage

- **Permission Name: android.permission.READ_PHONE_STATE**
- Used Type: Intent Action
- Callee Code: android.intent.action.PHONE_STATE

- **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

Log Message

N/A

May Log Message

N/A

ScreenShots