Apkscan malware analysis report
February 22, 2013

Static malware analysis

General information

File name	flash_player_installer.apk
MD5 hash	29e8db2c055574e26fd0b47859e78c0e
SHA256 hash	2076cb718edae12fa641a6b28cc53aee8d9d495518836bcc24e8e8bd1172f892
File size	301.25 KB

Android manifest (AndroidManifest.xml)

Requested permissions

ACCESS_NETWORK_STATE: Allows applications to access information about networks

CHANGE_NETWORK_STATE: Allows applications to change network connectivity state

Unknown permission: INSTALL_SHORTCUT

Unknown permission: UNINSTALL_SHORTCUT

ACCESS_NETWORK_STATE: Allows applications to access information about networks

RECEIVE_BOOT_COMPLETED: Allows an application to receive the ACTION_BOOT_COMPLETED that is broadcast after the system finishes booting.

SET_ALARM: Allows an application to broadcast an Intent to set an alarm for the user.

SYSTEM_ALERT_WINDOW: Allows an application to open windows using the type TYPE_SYSTEM_ALERT, shown on top of all other applications.

WRITE_SETTINGS: Allows an application to read or write the system settings.

WRITE_SECURE_SETTINGS: Allows an application to read or write the secure system settings.

ACCESS_WIFI_STATE: Allows applications to access information about Wi-Fi networks

UPDATE_DEVICE_STATS: Allows an application to update device statistics.

CHANGE_WIFI_STATE: Allows applications to change Wi-Fi connectivity state

WRITE_EXTERNAL_STORAGE: Allows an application to write to external storage.

INTERNET: Allows applications to open network sockets.

READ_PHONE_STATE: Allows read only access to phone state.

READ_SMS: Allows an application to read SMS messages.

SEND_SMS: Allows an application to send SMS messages.

RECEIVE_SMS: Allows an application to monitor incoming SMS messages, to record or perform processing on them.

READ_CONTACTS: Allows an application to read the user's contacts data.

DELETE_PACKAGES: Allows an application to delete packages.

GET_PACKAGE_SIZE: Allows an application to find out the space used by any package.

INSTALL_PACKAGES: Allows an application to install packages.

MANAGE_APP_TOKENS: Allows an application to manage (create, destroy, Z-order) application tokens in the window manager.

PERSISTENT_ACTIVITY: This constant was deprecated in API level 9. This functionality will be removed in the future; please do not use. Allow an application to make its activities persistent.

GET_ACCOUNTS: Allows access to the list of accounts in the Accounts Service

WAKE_LOCK: Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming

WAKE_LOCK: Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming

Services

fktjogygc.crermtcss.onjrpqg

Virus Total scan results

Avast	**Android:SMSAgent-FE [Trj]**
AVG	**Android/SMSAgent**
BitDefender	**Android.Trojan.FakeInst.CJ**
CAT-QuickHeal	**Android.Agentsms.IO1be0**

ClamAV	**Andr.Trojan.SMSsend-1**
Comodo	**UnclassifiedMalware**
DrWeb	**Android.SmsSend.336.origin**
ESET-NOD32	**Android/TrojanSMS.Agent.IO**
F-Secure	**Android.Trojan.FakeInst.CJ**
Fortinet	**Android/Agent.IO!tr**
GData	**Android.Trojan.FakeInst.CJ**
Ikarus	**AndroidOS.Trojan.SMSSend**
K7AntiVirus	**Trojan**
Kaspersky	**HEUR:Trojan-SMS.AndroidOS.Opfake.bo**
Kingsoft	**Android.Troj.Opfake.a.(kcloud)**
MicroWorld-eScan	**Android.Trojan.FakeInst.CJ**
NANO-Antivirus	**Trojan.Opfake.bfqvaq**
Sophos	**Andr/Opfake-C**
TrendMicro-HouseCall	**TROJ_GEN.RCBOHAO**

Disassembled source code

URL's

- http://docs.jquery.com/UI
- http://docs.jquery.com/UI/Accordion
- http://docs.jquery.com/UI/Accordion#theming
- http://docs.jquery.com/UI/Autocomplete
- http://docs.jquery.com/UI/Autocomplete#theming
- http://docs.jquery.com/UI/Button
- http://docs.jquery.com/UI/Button#theming
- http://docs.jquery.com/UI/Datepicker
- http://docs.jquery.com/UI/Datepicker#theming
- http://docs.jquery.com/UI/Dialog
- http://docs.jquery.com/UI/Dialog#theming
- http://docs.jquery.com/UI/Draggables
- http://docs.jquery.com/UI/Droppables
- http://docs.jquery.com/UI/Effects/
- http://docs.jquery.com/UI/Effects/Blind
- http://docs.jquery.com/UI/Effects/Bounce
- http://docs.jquery.com/UI/Effects/Clip
- http://docs.jquery.com/UI/Effects/Drop
- http://docs.jquery.com/UI/Effects/Explode
- http://docs.jquery.com/UI/Effects/Fade

- http://docs.jquery.com/UI/Effects/Fold
- http://docs.jquery.com/UI/Effects/Highlight
- http://docs.jquery.com/UI/Effects/Pulsate
- http://docs.jquery.com/UI/Effects/Scale
- http://docs.jquery.com/UI/Effects/Shake
- http://docs.jquery.com/UI/Effects/Slide
- http://docs.jquery.com/UI/Effects/Transfer
- http://docs.jquery.com/UI/Menu#theming
- http://docs.jquery.com/UI/Mouse
- http://docs.jquery.com/UI/Position
- http://docs.jquery.com/UI/Progressbar
- http://docs.jquery.com/UI/Progressbar#theming
- http://docs.jquery.com/UI/Resizable#theming
- http://docs.jquery.com/UI/Resizables
- http://docs.jquery.com/UI/Selectable#theming
- http://docs.jquery.com/UI/Selectables
- http://docs.jquery.com/UI/Slider
- http://docs.jquery.com/UI/Slider#theming
- http://docs.jquery.com/UI/Sortables
- http://docs.jquery.com/UI/Tabs
- http://docs.jquery.com/UI/Tabs#theming
- http://docs.jquery.com/UI/Theming/API
- http://docs.jquery.com/UI/Widget
- http://infomobiles.net/oferta.php
- http://infomobiles.net/oferta.php?full
- http://jquery.org/license
- http://jquerymobile.com
- http://jquerymobile.com/
- http://jqueryui.com/about
- http://jqueryui.com/themeroller/
- http://kldata2.net/

http://love.wapos.ru/imgs/tabor/foot.gif

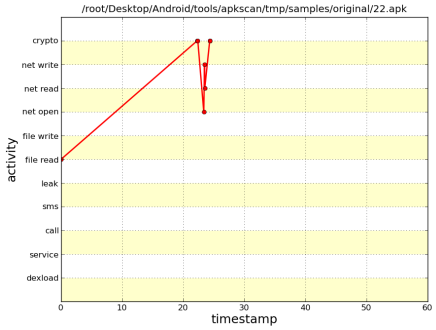
http://love.wapos.ru/imgs/tabor/h.gif

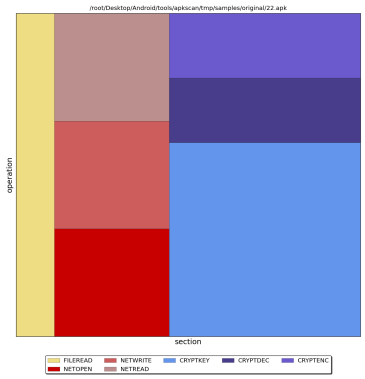
http://schemas.android.com/apk/res/android

http://sms911.ru/

http://yerc1.net/

Dynamic malware analysis





Placed phone calls

No phone calls were placed automatically.

Sent SMS messages

No text messages were placed automatically.

Cryptographic activity

Key 107, 103, 117, 116, 54, 102, 104, 110, 99, 56, 107, 114, 51, 104, 56, 55

Operation

Algorithm AES

Data

Key 107, 103, 117, 116, 54, 102, 104, 110, 99, 56, 107, 114, 51, 104, 56, 55

Operation encryption

Algorithm AES

Data board=unknown;brand=generic;device=generic;imei=357242043237517;imsi=310005123456789;session_id=1;operator=XXX;sms0=70123197112930

466272812,sms1=7834119717696546628937 2,sms2=70136197183842466286412,time=2013.02.22.09.54.44,timezone=GMT+00.00;

Key -

Operation decryption

Algorithm AES

Data 359616040020430;359616040020431;359616040020433;359616040020433;359616040020434;352085050116552

Information leakage

Network information leakage

No network information leakage detected.

SMS information leakage

No SMS information leakage detected.

File information leakage

No file information leakage detected.