Project

Source

Issues

Wikis

Downloads

androguard - DatabaseAndroidMalwares.wiki

Export to GitHub

Open Source database of android malware

This database is open source and anybody can send comments in order to add new links to analysis articles, to apply modifications on signatures or to add new signatures (it's is done on our free time, of course our free time is limited, so if you want to help, you are welcome !).

email: androguard (at) t0t0 (dot) fr

Submit malware

You can also send us samples in order to add them to the database, and moreover sometimes we request samples to analyze and add them in the database.

Submit information

You can send us more information about a malware, and sometimes we request information (INFORMATION) on a specific malware because we don't have found anything on internet.

Malware name

We used common names for malware, so if you have know others names for a malware, please contact us.

Malware detection

You can test if an application contains a malware in the androguard example database, or add/remove new signatures. So for few malwares, we created a signature to detect them. **For now, we use similarity distance and clustering to search a signature in an application. For more information go to this page.**

This database is an example of how it's possible to use androguard in order to detect parts of your application in another one.

If you are interesting about android malwares, it's possible to download few of them on the website of contagiodump or contagiominidump

On this page, you will find information about android malwares. Firstly, you will have links of different analysis of each malware, and some requests. Next you can find which techniques have been used to add the sample in androguard database, but it's more interesting to check directly the signature. Of course, by using the similarity distance, we can detect variants of each malware.

How to use it

You can download the database and the configuration in the mercurial repository or directly with these links : * database * config

And you can check a repository with androsign.py :

```
desnos@t0t0:~/androguard$ ./androsign.py -d
apks/malwares/moghava/ -b signatures/dbandroguard -c signatures/dbconfig
d9b21e6a6ff59e26dfc8c350f90fe53558ac623df72ff0eec4f03210c12257fa : ----> Moghava
94bb6ade1ef31c6c96b98c7d8fad1abbc794292730f4363ea3cd9204fc5c9dfd : ----> Moghava
```

or a simple file :

```
desnos@t0t0:~/androguard$ ./androsign.py -i
apks/malwares/moghava/d9b21e6a6ff59e26dfc8c350f90fe53558ac623df72ff0eec4f03210c12257fa -b
signatures/dbandroguard -c signatures/dbconfig
d9b21e6a6ff59e26dfc8c350f90fe53558ac623df72ff0eec4f03210c12257fa : ----> Moghava
desnos@t0t0:~/androguard$ ./androsign.py -i apks/com.rovio.angrybirdsseasons-1.apk -b
signatures/dbandroguard -c signatures/dbconfig com.rovio.angrybirdsseasons-1.apk : ----> None
```

It's possible to check if your application is detecting in our database during a classing RE session.

Supported Android Malware

basebridge

- http://www.fortiguard.com/encyclopedia/virus/android_basebridge.a!tr.html
- http://www.symantec.com/security_response/writeup.jsp?docid=2011-060915-4938-99&tabid=2
- SIGNATURE
- SIGNATURE
- SIGNATURE

basebridgeincluded

- http://www.fortiguard.com/encyclopedia/virus/android_basebridge.b!tr.html
- SIGNATURE

crusewind (crusewin)

- http://blog.trendmicro.com/android-malware-acts-as-an-sms-relay/
- http://www.symantec.com/security_response/writeup.jsp?docid=2011-070301-5702-99&tabid=2
- http://www.fortiguard.com/av/VID2837880
- SIGNATURE

dogowar

- http://www.symantec.com/connect/blogs/animal-rights-protesters-use-mobile-means-their-message
- SIGNATURE

droiddream (rootcager)

- http://blog.mylookout.com/droiddream/
- http://about-threats.trendmicro.com/Malware.aspx?language=us&name=ANDROIDOS_DORDRAE.N
- http://www.symantec.com/security_response/writeup.jsp?docid=2011-022303-3344-99&tabid=2
- http://androguard.blogspot.com/2011/03/droiddream.html
- http://androguard.blogspot.com/2011/03/droiddream-part-2.html
- SIGNATURE

droiddreamincluded (INFORMATION)

- SIGNATURE

droiddreamlight

- http://droidsecurity.appspot.com/securitycenter/securitypost_20110601.html
- http://www.avgmobilation.com/securitycenter/securitypost_20110601.html
- SIGNATURE

droidkungfu (fokonge, gongfu)

- http://www.cs.ncsu.edu/faculty/jiang/DroidKungFu/
- http://blog.fortinet.com/clarifying-android-droidkungfu-variants/
- http://www.fortiguard.com/encyclopedia/virus/android_droidkungfu.b!tr.html
- http://www.isolatedthreat.com/2011/08/android-analysis-droid-kung-fu.html
- http://www.f-secure.com/weblog/archives/00002177.html
- http://nakedsecurity.sophos.com/2012/04/12/android-malware-angry-birds-space-game/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+nakedsecurity+%28Naked+Security+-+Sophos%29&utm_content=Google+Reader
- http://blog.fortiguard.com/tag/droidkungfu/
- SIGNATURE

droidkungfu2

- http://www.cs.ncsu.edu/faculty/jiang/DroidKungFu2/
- SIGNATURE

droidkungfu3

- http://www.csc.ncsu.edu/faculty/jiang/DroidKungFu3/
- SIGNATURE

droiddeluxe

- http://www.csc.ncsu.edu/faculty/jiang/DroidDeluxe/
- https://www.kindsight.net/sites/default/files/Kindsight_Malware_Analysis-Android-Trojan-DroidDeluxe-final.pdf
- SIGNATURE

ewalls

- http://www.symantec.com/security_response/writeup.jsp?docid=2010-073014-0854-99
- SIGNATURE

- SIGNATURE

fakeinstaller (boxer)

- http://www.droidsecurity.com/securitycenter/secuirtypost_20111110.html#tabs-2
- http://blog.trendmicro.com/rogue-instagram-and-angry-birds-space-for-android-spotted/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Anti-MalwareBlog+%28Trend+Micro+Malware+Blog%29
- SIGNATURE

finfisher

- http://citizenlab.org/2012/08/the-smartphone-who-loved-me-finfisher-goes-mobile/

foncy

- http://www.securelist.com/en/blog/208193261/SMS_Trojans_all_around_the_world
- http://code.google.com/p/androguard/wiki/AndroidMalwareAnalysis#Foncy
- SIGNATURE

geinimi

- http://blog.mylookout.com/2011/01/geinimi-trojan-technical-analysis/
- http://www.fortiguard.com/av/VID2374726
- http://www.symantec.com/security_response/writeup.jsp?docid=2011-010111-5403-99&tabid=-9
- SIGNATURE

gingermaster

- http://www.cs.ncsu.edu/faculty/jiang/GingerMaster/
- http://www.avgmobilation.com/securitycenter/securitypost_20110825.html#tabs-2
- http://droidsecurity.appspot.com/securitycenter/securitypost_20110825.html#tabs-2
- SIGNATURE

ggtracker

- http://www.symantec.com/security_response/writeup.jsp?docid=2011-062208-5013-99&tabid=2

- http://blog.mylookout.com/blog/2011/06/20/security-alert-android-trojan-ggtracker-charges-victims-premium-rate-sms-messages/ggtracker-teardown_lookout-mobile-security/
- SIGNATURE

golddream (spygold)

- http://www.cs.ncsu.edu/faculty/jiang/GoldDream/
- http://www.symantec.com/security_response/writeup.jsp?docid=2011-070608-4139-99&tabid=2
- SIGNATURE

hipposms

- http://www.csc.ncsu.edu/faculty/jiang/HippoSMS/
- SIGNATURE
- SIGNATURE

hongtoutou

- http://blog.mylookout.com/2011/02/security-alert-hongtoutou-new-android-trojan-found-in-china/
- http://blog.aegislab.com/index.php?articleId=75&blogId=1&op=ViewArticle
- http://www.fortiguard.com/av/VID2494321
- http://www.antiy.net/en/alert/analysis_report_on_android_trojan_hongtoutou.html
- SIGNATURE

lena (dkfbootkit)

- http://blog.mylookout.com/2011/10/security-alert-legacy-makes-a-another-appearance-on-android-market-meet-legacy-native-lena/
- http://blog.mylookout.com/wp-content/uploads/2011/10/LeNa-Legacy-Native-Teardown_Lookout-Mobile-Security1.pdf
- http://research.nq.com/?p=391
- http://blog.mylookout.com/blog/2012/04/03/security-alert-new-variants-of-legacy-native-lena-identified/
- SIGNATURE (detected with droidkungfu2 signature)

Logastrod

- http://www.f-secure.com/weblog/archives/00002280.html
- SIGNATURE

lovetrap (cosha)

- http://www.symantec.com/security_response/writeup.jsp?docid=2011-072806-2905-99
- SIGNATURE

moghava

- http://www.symantec.com/connect/blogs/androidmoghava-recipe-mayhem
- http://forensics.spreitzenbarth.de/2012/03/02/detailed-analysis-of-android-moghava/
- SIGNATURE

nickibot

- http://www.csc.ncsu.edu/faculty/jiang/NickiBot/
- http://blog.spiderlabs.com/2011/10/nickispyc-an-analysis.html
- SIGNATURE

nickyspy

- http://www.avgmobilation.com/securitycenter/securitypost_20110804.htm#tabs-2
- http://www.kompyuteran.com/2011/08/trojan-disguised-as-google-plus-app-attacks-android-phones/
- SIGNATURE

ozotshielder (kmin)

- http://www.symantec.com/security_response/writeup.jsp?docid=2011-091505-3230-99
- SIGNATURE
- SIGNATURE
- SIGNATURE

plankton (tonclank)

- http://www.csc.ncsu.edu/faculty/jiang/Plankton/
- SIGNATURE
- SIGNATURE
- SIGNATURE

pjapps

- http://www.symantec.com/connect/blogs/android-threats-getting-steamy
- http://blog.webroot.com/2012/02/17/an-evolution-of-android-malware-my-how-youve-grown-pjapps-part-1/
- SIGNATURE
- SIGNATURE
- SIGNATURE

roguesppush (autospsubscribe)

- http://www.cs.ncsu.edu/faculty/jiang/RogueSPPush/
- http://www.f-secure.com/v-descs/trojan_android_autospsubscribe_a.shtml
- SIGNATURE

smshider

- http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=527859#none
- http://blog.mylookout.com/2011/06/security-alert-malware-found-targeting-custom-roms-jsmshider/
- SIGNATURE

sndapps

- http://www.csc.ncsu.edu/faculty/jiang/SndApps/
- http://www.f-secure.com/weblog/archives/00002202.html
- SIGNATURE

spitmo (zitmo)

- http://www.f-secure.com/weblog/archives/00002236.html
- http://forensics.spreitzenbarth.de/2011/12/06/detailed-analysis-of-android-spitmo/
- http://www.fortiguard.com/av/VID3373196
- http://blog.fortinet.com/zitmo-hits-android/
- http://www.securelist.com/en/blog/208193029/ZeuS_in_the_Mobile_for_Android
- http://cert.lexsi.com/weblog/index.php/2011/07/12/416-zeus-in-the-mobile-android (FR)
- http://www.kindsight.net/sites/default/files/android_trojan_zitmo_final_pdf_17585.pdf
- http://www.trusteer.com/blog/song-remains-same-man-mobile-attacks-single-out-android

- http://www.securelist.com/en/blog/208193760/New_ZitMo_for_Android_and_Blackberry
- SIGNATURE
- SIGNATURE

walkinwat

- http://www.symantec.com/security_response/writeup.jsp?docid=2011-033008-4831-99
- SIGNATURE

yzhcsms (uxipp, wukong)

- http://www.csc.ncsu.edu/faculty/jiang/YZHCSMS/
- SIGNATURE
- SIGNATURE

zsone

- http://blog.mylookout.com/2011/05/security-alert-zsone-trojan-found-in-android-market/
- SIGNATURE

Pending Android Malware

adboo

- http://www.f-secure.com/weblog/archives/00002298.html

adop

- http://nakedsecurity.sophos.com/2012/04/26/dirty-tricks-android-apps/

adsms

- http://www.symantec.com/security_response/writeup.jsp?docid=2011-051313-4039-99&tabid=2

anserverbot

- http://www.csc.ncsu.edu/faculty/jiang/AnserverBot/

- http://www.csc.ncsu.edu/faculty/jiang/pubs/AnserverBot_Analysis.pdf

antares(Antammi) (INFORMATION)

arspam

- http://androidcommunity.com/android-arspam-is-the-latest-malware-threat-says-symantec-20111230/

battery doctor (fakedoc)

- http://www.pcworld.com/article/241967/sleazy_ads_on_android_devices_push_bogus_battery_upgrade_warnings.html
- http://blog.soleranetworks.com/2011/10/16/snoopy-android-adware-poses-as-power-saving-patch/
- http://www.fortiguard.com/av/VID3304615

beanbot

- http://www.csc.ncsu.edu/faculty/jiang/BeanBot/

bgserv

- http://www.symantec.com/security_response/writeup.jsp?docid=2011-022303-3344-99&tabid=2
- http://about-threats.trendmicro.com/Malware.aspx?language=us&name=AndroidOS_BGSERV.A

bowad (malex) (INFORMATION)

caldx

- http://research.nq.com/?p=469

cawitt (twikabot)

- http://www.mobiantivirus.org/Android/styled-79/index.html

ci4

- http://blog.mylookout.com/blog/2012/06/22/security-alert-ci4-sms-bot/
- http://www.hotforsecurity.com/blog/android-sms-bot-uses-twitter-to-hide-cc-server-2602.html

counterclank

- http://vrt-blog.snort.org/2012/01/androidcounterclank-malware-or-adware.html
- http://www.symantec.com/security_response/writeup.jsp?docid=2012-012709-4046-99&tabid=2
- http://blog.mylookout.com/blog/2012/01/27/lookout%E2%80%99s-take-on-the-%E2%80%98apperhand%E2%80%99-sdk-aka-android-counterclank/

ddspy

- http://research.nq.com/?p=496

dougaleaker (dougalek)

- http://www.symantec.com/security_response/writeup.jsp?docid=2012-041601-3400-99
- http://www.symantec.com/connect/blogs/movie-malware-steals-personal-information-japanese-android-users
- http://mcaf.ee/yndzs

droidcoupon (SAMPLE REQUEST)

- http://labs.netqin.com/us/?p=112

droidlive

- http://www.csc.ncsu.edu/faculty/jiang/DroidLive/

droidkungfu.E/C

- http://www.f-secure.com/weblog/archives/00002258.html
- http://www.f-secure.com/weblog/archives/00002259.html

droidkungfusapp

- http://www.csc.ncsu.edu/faculty/jiang/DroidKungFuSapp/
- http://research.netqin.com/?p=232

droisnake

- http://about-threats.trendmicro.com/Malware.aspx?language=us&name=AndroidOS_DROIsnake.a

dropdialer

- http://www.symantec.com/connect/blogs/androiddropdialer-identified-google-play
- http://www.f-secure.com/weblog/archives/00002398.html

fakeangry (Anzhu)

- http://www.malwarecity.com/blog/from-china-with-love-new-android-backdoor-spreading-through-hacked-apps-1261.html
- http://news.drweb.fr/show/?i=589&c=5

fakeinst (smstado, fakebrows)

- http://about-threats.trendmicro.com/Malware.aspx?language=fr&name=ANDROIDOS_FAKEBROWS.A
- http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=366740#none
- http://www.f-secure.com/weblog/archives/00002278.html

fakelottery (steek)

- http://blogs.avg.com/news-threats/rays-bad-you-phone-answer/

fakeneflic

- http://www.symantec.com/connect/blogs/will-your-next-tv-manual-ask-you-run-scan-instead-adjusting-antenna
- http://blog.mylookout.com/2011/10/security-alert-fake-netflix-app-aids-phishing/

fakenotify

- http://www.f-secure.com/weblog/archives/00002278.html
- http://www.f-secure.com/weblog/archives/00002291.html
- http://www.f-secure.com/weblog/archives/00002299.html
- http://blog.trendmicro.com/malicious-mobile-apps-found-hosted-in-german-ip-address/

fakesecsuit

- http://www.securelist.com/en/blog/208193604/Android_Security_Suite_Premium_New_ZitMo

fakesmsreg

- http://www.f-secure.com/weblog/archives/00002305.html
- http://forensics.spreitzenbarth.de/2012/02/03/detailed-analysis-of-android-fakeregsms-b/

faketimer (oneclickfraud)

- http://unixfreaxjp.blogspot.com/2012/02/ocjp-010.html
- http://translate.google.fr/translate?hl=fr&sl=ja&tl=en&u=http%3A%2F%2Funixfreaxjp.blogspot.com%2F2012%2F02%2Focjp-010.html
- http://www.symantec.com/connect/blogs/scam-proves-privacy-concerns-mobile-devices-0

faketoken

- http://blogs.mcafee.com/mcafee-labs/android-malware-pairs-man-in-the-middle-with-remote-controlled-banking-trojan
- http://forensics.spreitzenbarth.de/2012/03/16/detailed-analysis-of-android-faketoken/

fakeupdates (gapp)

- http://www.antiy.com/cn/security/2012/trojan_android_gapp.html
- http://translate.google.com/translate?hl=fr&sl=zh-CN&tl=en&u=http%3A%2F%2Fwww.antiy.com%2Fcn%2Fsecurity%2F2012%2Ftrojan_android_gapp.html
- https://blogs.mcafee.com/mcafee-labs/google-code-projects-host-android-malware

fakerun (fakeapp)

- http://blog.trendmicro.com/fake-version-of-temple-run-unearthed-in-the-wild/
- http://blog.trendmicro.com/fan-apps-now-spreading-on-the-android-market/

feebs (INFORMATION)

findandcall

- http://www.securelist.com/en/blog/208193641/Find_and_Call_Leak_and_Spam

fjcon

- http://www.csc.ncsu.edu/faculty/jiang/Fjcon/
- http://research.netqin.com/?p=258

foncy.b

- http://www.securelist.com/en/blog/208193332/IRC_bot_for_Android
- http://blog.spiderlabs.com/2012/01/android-irc-bot-this-aint-your-grannys-android-malware-or-maybe-it-is.html
- http://stratsec.blogspot.com/2012/01/butterfly-effect-of-boundary-check.html

gamblersms

- http://www.cs.ncsu.edu/faculty/jiang/GamblerSMS/

gamex (muldrop)

- http://blog.mylookout.com/blog/2012/04/27/security-alert-gamex-trojans-hides-in-root-required-apps-tricking-users-into-downloads/
- http://news.drweb.fr/show/?i=637&c=5

gappusin

- http://www.symantec.com/security_response/writeup.jsp?docid=2012-022007-2013-99&tabid=2

gappll

- http://research.nq.com/?p=443

gomanag

- http://blog.webroot.com/2012/02/29/an-evolution-of-android-malware-when-stealing-data-isnt-enough-meet-gomanag-part-2/

ggsearch

- http://blog.mylookout.com/blog/2012/08/09/lookout-ggsearch-update/

gonein60

- http://www.malwarecity.com/blog/all-data-stored-on-your-smartphone-gone-in-60-seconds-1156.html
- http://www.droidsecurity.com/securitycenter/securitypost_20110927.html#tabs-2
- http://www.symantec.com/security_response/writeup.jsp?docid=2011-093001-2649-99&tabid=2

jee (geofeebot)

- http://blogs.avg.com/news-threats/mobile-threat-update-careful-bite/
- http://research.nq.com/?p=340

- http://research.nq.com/?p=479

jifake

- http://blog.fortinet.com/qr-code-and-mobile-malware-it-happened/
- http://www.securelist.com/en/blog/208193145/Its_time_for_malicious_QR_codes

luckycat

- http://stratsec.blogspot.fr/2012/08/lucky-cat-is-threat_3.html

mania

- http://www.securelist.com/en/blog/208193532/Foncy_is_dead_Long_live_Mania
- http://blog.fortiguard.com/tracking-androidfoncy/

meswatcherbox

- http://www.symantec.com/security_response/writeup.jsp?docid=2011-111612-2736-99

mobiletx

- http://www.f-secure.com/weblog/archives/00002233.html

mobinauten (SmsHowU, smsspy)

- http://threatcenter.smobilesystems.com/?p=1936
- http://www.fortiguard.com/av/VID2129667

notcompatible

- http://blog.mylookout.com/blog/2012/05/02/security-alert-hacked-websites-serve-suspicious-android-apps-noncompatible/
- http://www.symantec.com/connect/blogs/website-injection-campaign-used-conjunction-android-trojan
- https://blogs.mcafee.com/mcafee-labs/androidnotcompatible-looks-like-piece-of-pc-botnet

nyearleaker

- http://www.symantec.com/security_response/writeup.jsp?docid=2012-010514-0844-99

opfake (all)

- http://www.f-secure.com/weblog/archives/00002260.html
- http://stratsec.blogspot.com/2012/02/conventional-malware-techniques-spread.html
- http://www.f-secure.com/weblog/archives/00002306.html
- http://blogs.avg.com/news-threats/avg-mobile-threat-update-week-3/
- http://blogs.avg.com/news-threats/fake-mobile-update-week-4/
- http://www.symantec.com/connect/blogs/revamped-fake-android-market-sms-fraud
- http://nakedsecurity.sophos.com/2012/02/24/android-malware-facebook/?utm_source=twitter&utm_medium=gcluley&utm_campaign=naked%2Bsecurity
- http://blog.mylookout.com/blog/2012/02/24/social-malware-malware-distributed-through-facebook/
- http://www.symantec.com/connect/blogs/attempts-spread-mobile-malware-tweets
- http://blog.trendmicro.com/fake-google-play-site-leads-to-rogue-apk-app/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Anti-MalwareBlog+%28Trend+Micro+Malware+Blog%29&utm_content=Google+Reader
- http://blog.aegislab.com/index.php?op=ViewArticle&articleId=166&blogId=1
- http://totaldefense.com/blogs/security-advisor/2012/02/27/Android-Social-Engineering-Threats-in-the-Spotlight.aspx
- http://www.symantec.com/connect/blogs/thieves-temple-androidopfake-makes-another-run
- http://about-threats.trendmicro.com/Malware.aspx?language=us&name=ANDROIDOS_FAKE.DQ
- http://www.symantec.com/connect/blogs/malware-charges-fee-free-apps-google-play

opspys

- http://research.nq.com/?p=464

pdaspy

- http://blog.trendmicro.com/17-bad-mobile-apps-still-up-700000-downloads-so-far/?

pirates (INFORMATION)

premiumtext (rufraud)

- http://www.symantec.com/security_response/writeup.jsp?docid=2011-080213-5308-99
- http://nakedsecurity.sophos.com/2012/05/24/angry-birds-malware-fine/

pushbot (SAMPLE REQUEST)

- http://www.csc.ncsu.edu/faculty/jiang/PushBot/

qicsomos

- http://www.symantec.com/connect/blogs/day-after-year-mobile-malware
- http://forensics.spreitzenbarth.de/2012/01/17/detailes-analysis-of-android-qicsomos/

quickpay

- http://blog.webroot.com/2012/05/03/you-want-to-pay-for-what/

rufailed (rufraud)

- http://www.f-secure.com/weblog/archives/00002289.html
- http://blog.aegislab.com/index.php?op=ViewArticle&articleId=155&blogId=1
- http://blog.aegislab.com/index.php?op=ViewArticle&articleId=154&blogId=1

roguelemon

- http://www.csc.ncsu.edu/faculty/jiang/RogueLemon/

rootsmart

- http://www.cs.ncsu.edu/faculty/jiang/RootSmart/
- http://resources.infosecinstitute.com/rootsmart-android-malware/
- http://www.symantec.com/connect/blogs/androidbmaster-million-dollar-mobile-botnet
- http://forensics.spreitzenbarth.de/2012/02/12/detailed-analysis-of-android-bmaster/
- http://resources.infosecinstitute.com/rootsmart-android-malware/
- http://blog.aegislab.com/index.php?op=ViewArticle&articleId=160&blogId=1

scarlet (INFORMATION)

scavir

- http://www.securelist.com/en/blog/208193306/Android_malware_new_traps_for_users

smsreplicator

- http://www.talkandroid.com/19466-sms-replicator-for-android-will-secretly-forward-texts/

smssend/fakeplayer

- http://www.kaspersky.com/about/news/virus/2010/First_SMS_Trojan_detected_for_smartphones_running_Android

smsspy

- http://blog.trendmicro.com/beta-version-of-spytool-app-for-android-steals-sms-messages/

smszombie

- http://blog.trustgo.com/SMSZombie/

spacem (denofow)

- http://blog.mylookout.com/2011/06/the-world-isn%e2%80%99t-ending%e2%80%94but-a-%e2%80%9crapture%e2%80%9d-themed-trojan-plagues-android-phones/

steek (ANDROIDOS_FAKECLICK.ER)

- http://www.symantec.com/connect/blogs/more-fraudware-headaches-android-marketplace
- http://blog.trendmicro.com/trending-scams-seen-in-the-android-market/
- http://www.fortiguard.com/av/VID3458224

spy32 (INFORMATION)

SW.Qieting.A (INFORMATION)

SW.Securephone (INFORMATION)

tapsnake

- http://www.symantec.com/security_response/writeup.jsp?docid=2010-081214-2657-99

tgloader (stiniter)

- http://research.nq.com/?p=364
- http://nakedsecurity.sophos.com/2012/03/29/trojan-android-games-send-expensive-smss/
- http://www.symantec.com/security_response/writeup.jsp?docid=2012-030903-5228-99
- http://www.fortiguard.com/av/VID3677621

tigerbot (spyera)

- http://research.nq.com/?p=402
- http://blog.mylookout.com/blog/2012/04/16/lookout%E2%80%99s-take-on-spyera-aka-tigerbot/
- http://blog.trendmicro.com/?p=41932

vdloader

- http://research.nq.com/?p=542
- http://www.symantec.com/connect/blogs/new-android-malware-spotted-third-party-app-markets

vidro

- http://www.securelist.com/en/blog/208193729/Vidro_How_deep_and_mobile_is_the_rabbit_hole

updtbot

- http://research.nq.com/?p=410

updtkiller

- http://research.nq.com/?p=454

uranico

- http://www.symantec.com/connect/blogs/fortune-teller-app-ripping-personal-data-also-appeared-google-play

voicecharger

- http://blogs.avg.com/news-threats/voice-changer-voice-charger/

zeahache

- http://www.symantec.com/security_response/writeup.jsp?docid=2011-032309-5042-99

zsone.a

- http://www.f-secure.com/weblog/archives/00002373.html

Potentially Unwanted Program

diydos

- https://blogs.mcafee.com/mcafee-labs/unwanted-apps-in-google-play-pose-as-fake-av

igirl

- http://news.drweb.fr/show/?i=597&c=5

LOIC

- https://blogs.mcafee.com/mcafee-labs/android-diy-dos-app-boosts-hacktivism-in-south-america

---

Pending ARM binaries

Foncy

- http://www.securelist.com/en/blog/208193332/IRC_bot_for_Android
- http://blog.spiderlabs.com/2012/01/android-irc-bot-this-aint-your-grannys-android-malware-or-maybe-it-is.html
- http://stratsec.blogspot.com/2012/01/butterfly-effect-of-boundary-check.html

---

Pending ARM exploits

rageagainstthecage

exploid

gingerbreak

- http://www.trustgo.com/footer/blog.php#On_the_Verge

Pending APK exploits

z4root

univerandroot

superuser

Techniques

Reflection

- http://www.dataprotectioncenter.com/antivirus/f-secure/trojanandroidfakenotify-gets-updated/
- http://totaldefense.com/blogs/2012/03/12/Android-Malware-adopts-reflections.aspx