Android Triada modular trojan

contagiominidump.blogspot.de/2016/07/android-triada-modular-trojan.html

Research: Kaspersky: Everyone sees not what they want to see
Attack on Zygote: a new twist in the evolution of mobile threats
The story of the small Trojan that could!
Checkpoint: In The Wild: Mobile Malware Implements New Features

Sample credit: Tim Strazzere

File information:

MD5 592fa585b64412e31b3da77b1e825208

SHA1 3689a276f85fd94750dc063860097fdc28ec527f

SHA256 4656aa68ad30a5cf9bcd2b63f21fba7cfa0b70533840e771bd7d6680ef44794b

Download. Email me if you need the password

https://www.virustotal.com/file/4656aa68ad30a5cf9bcd2b63f21fba7cfa0b70533840e771bd7d6680ef44794b/analysis/1457591162/

AVG Android/Deng.DSS 20160310
AVware Trojan.AndroidOS.Generic.A 20160310
Ad-Aware Android.Trojan.Triada.A 20160310
AegisLab Troj.SMS.AndroidOS.Agent.rm!c 20160310
AhnLab-V3 Android-PUP/SmsReg.ff6c 20160309
Alibaba A.L.Pay.Popr 20160310
Antiy-AVL Trojan[Backdoor:HEUR]/Android.Triada.2 20160310
Arcabit Android.Trojan.Triada.R 20160310
Avast Android:Triada-C [Trj] 20160310

Avira (no cloud) ANDROID/Triada.A.55 20160310
Baidu-International Trojan.Android.Agent.BKT 20160309
BitDefender Android.Trojan.Triada.A 20160310
CAT-QuickHeal Android.Triada.B1e19 (PUP) 20160310
Comodo UnclassifiedMalware 20160310
Cyren AndroidOS/GenBl.BCA0D997!Olympus 20160310
DrWeb Android.Rootkit.20 20160310
ESET-NOD32 a variant of Android/Spy.SmsSpy.AU 20160310
Emsisoft Android.Trojan.Triada.A (B) 20160310
F-Secure Android.Trojan.Triada.A 20160310
Fortinet Android/Agent.ANZ!tr 20160310
GData Android.Trojan.Triada.A 20160310
Ikarus HackTool.AndroidOS.RGenius 20160310
Jiangmin Backdoor.AndroidOS.cjj 20160310
K7GW Trojan (004d2c811) 20160310
Kaspersky HEUR:Backdoor.AndroidOS.Triada.b 20160310
McAfee Artemis!592FA585B644 20160310
eScan Android.Trojan.Triada.A 20160310
NANO-Antivirus Trojan.Android.Agent.dywqdy 20160310
Qihoo-360 Trojan.Android.Gen 20160310
Sophos Andr/Triada-A 20160310
Tencent Android.Trojan.Agentb.Auto 20160310
VIPRE Trojan.AndroidOS.Generic.A 20160310
Zoner Trojan.AndroidOS.SmsSpy.A 20160310

Required permissions

android.permission.CHANGE_NETWORK_STATE (*change network connectivity*)
android.permission.READ_LOGS (*read sensitive log data*)
android.permission.INTERNET (*full Internet access*)
android.permission.SEND_SMS (*send SMS messages*)
android.permission.WRITE_SMS (*edit SMS or MMS*)
android.permission.ACCESS_NETWORK_STATE (*view network status*)
android.permission.GET_TASKS (*retrieve running applications*)
android.permission.WRITE_EXTERNAL_STORAGE (*modify/delete SD card contents*)
android.permission.GET_PACKAGE_SIZE (*measure application storage space*)
android.permission.READ_EXTERNAL_STORAGE (*read from external storage*)
android.permission.RECEIVE_BOOT_COMPLETED (*automatically start at boot*)
android.permission.ACCESS_MTK_MMHW (*Unknown permission from android reference*)
com.android.alarm.permission.SET_ALARM (*set alarm in alarm clock*)
android.permission.BROADCAST_STICKY (*send sticky broadcast*)
android.permission.WRITE_SETTINGS (*modify global system settings*)
android.permission.READ_PHONE_STATE (*read phone state and identity*)
android.permission.READ_SMS (*read SMS or MMS*)

android.permission.SYSTEM_ALERT_WINDOW (*display system-level alerts*)
android.permission.KILL_BACKGROUND_PROCESSES (*kill background processes*)
android.permission.ACCESS_WIFI_STATE (*view Wi-Fi status*)
android.permission.WAKE_LOCK (*prevent phone from sleeping*)
android.permission.CHANGE_WIFI_STATE (*change Wi-Fi status*)
android.permission.RECEIVE_SMS (*receive SMS*)
android.permission.CLEAR_APP_CACHE (*delete all application cache data*)
android.permission.MOUNT_UNMOUNT_FILESYSTEMS (*mount and unmount file systems*)
android.permission.RESTART_PACKAGES (*kill background processes*)
Activities
com.good.sunsine.FlashScreen
com.good.sunsine.MainActivity
Services
com.android.system.UpdateService
Receivers
com.android.system.PopReceiver
Service-related intent filters
com.android.system.UpdateService
actions: com.android.system.UpdateService
Activity-related intent filters
com.good.sunsine.FlashScreen
actions: android.intent.action.MAIN
categories: android.intent.category.LAUNCHER
Receiver-related intent filters
com.android.system.PopReceiver
actions: android.intent.action.BOOT_COMPLETED,
android.provider.Telephony.SMS_RECEIVED, android.intent.action.PHONE_STATE,
android.intent.action.NEW_OUTGOING_CALL
categories: android.intent.category.LAUNCHER

validfrom: 06:55 AM 05/25/2015
serialnumber: 6B36CE51
Issuer
    DN: OU=98yudodaqe, CN=98eyu1982ey98eu
    CN: 98eyu1982ey98eu
    OU: 98yudodaqe
Subject
    DN: OU=98yudodaqe, CN=98eyu1982ey98eu
    CN: 98eyu1982ey98eu
    OU: 98yudodaqe
thumbprint: 41775876A2CD11B4D1B85C9D73D49B187EFFA1D2