More ▾ Next Blog» Create Blog Sign In

contagio mobile

mobile malware mini dump

Mobile and printer friendly

NEW FILE LOCATION (instead of broken Mediafire links

TUESDAY, MARCH 20, 2018

Android Fakebank samples

Research: Symantec. Android-Fakebank

Download. Email me if you need the password

File information

#	File Name	Hash Value	File Size (on Disk)
1	191108379dccd5dc1b21c5f71f4eb5d47603fc4950255f32b1228d4b066ea512	650795A6C3301CD7FF355FA4F7EEDE8B	2625281 bytes (2.5 MiB)
2	1ef6e1a7c936d1bdc0c7fd387e071c102549e8fa0038aec2d2f4bffb7e0609c3	0693F22F405C6EFB99DACAD63CF6EE0E	4743009 bytes (4.52 MiB)
3	4aeccf56981a32461ed3cad5e197a3eedb97a8dfb916affc67ce4b9e75b67d98	37DFF309CC911A1DC16CCE4E51F9827B	5415986 bytes (5.17 MiB)
4	b9cbe8b737a6f075d4d766d828c9a0206c6fe99c6b25b37b539678114f0abffb	67E7BB573EAA1F25772809A471CDA327	4496258 bytes (4.29 MiB)

1 comments Labels: android, Fakebank Links to this post

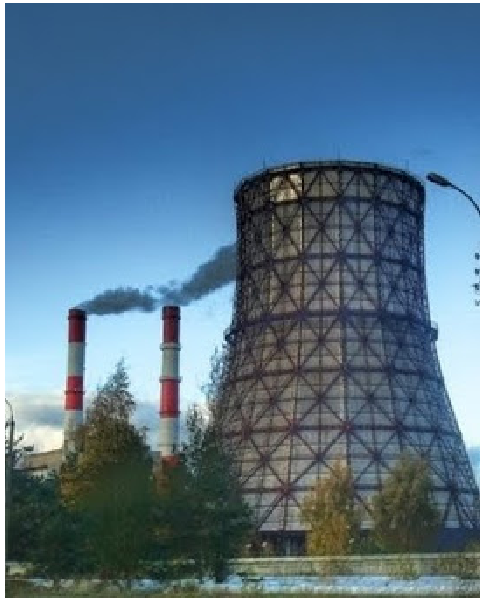
MONDAY, MARCH 19, 2018

SHARED BY

Mila

@ you can find my email address in my profile

View my complete profile



Android Tizi - Samples

2017/11/25 Research: Google. Tizi: Detecting and blocking socially engineered spyware on Android

List of SHA256 hashes
com.press.nasa.com.tanofresh
4d780a6fc18458311250d4d1edc750468fdb9b3e4c950dce5b35d4567b47d4a7

com.dailyworkout.tizi
7c6af091a7b0f04fb5b212bd3c180ddcc6abf7cd77478fd22595e5b7aa7cfd9f

com.system.update.systemupdate
7a956c754f003a219ea1d2205de3ef5bc354419985a487254b8aeb865442a55e

19032b32cc0d99e65f32a28ecffc411572bb58cc19c8cf8195339dd30011e54c
3135c6a2793b66c73aacc668f0fddcdf8afdb0749024d408f592bf715e4c68ac
b702149585354b78ee317e2cc1d89e35bf59d73e9610c6b2950899a5f1315fa5
ccf604ba0393ac28c6b5f9f8bb719de251476968589df0239c743e30e1eb2707

Download. Email me if you need the password

Read more »

0 comments Links to this post

Judy - android auto-clicking adware samples

ABOUT CONTAGIOMINIDUMP

aka "take a sample, leave a sample"
Contagio mobile mini-dump is a part of **contagiodump.blogspot.com**. Contagio mobile mini-dump offers an upload dropbox for you to share your mobile malware samples. You can also download any samples individually or in one zip. **CLICK HERE TO DOWNLOAD ALL** Note: **use infected for the password on posts before Sept. 2102 or email for the password scheme for newer samples**

BLOG ARCHIVE

- ▼ 2018 (4)
  - ▼ March (4)
    - Android Fakebank samples
    - Android Tizi - Samples
    - Judy - android auto-clicking adware samples
    - Red Drop - Android blackmailing spyware samples
- ► 2016 (14)
- ► 2015 (28)
- ► 2014 (49)
- ► 2013 (46)
- ► 2012 (56)
- ► 2011 (55)

BLOG LIST

Security Intelligence | TrendLab...

Life in Linux Kernel

Research: Checkpoint. The Judy Malware: Possibly the largest malware campaign found on Google Play

SHA256 - see 119 files below

Download. Email me if you need the password

Download part 1
Download part 2
Download part 3

Read more »

0 comments Labels: android, clickfraud, judy Links to this post

Red Drop - Android blackmailing spyware samples

Research: Wandera: RedDrop: the blackmailing mobile malware family lurking in app stores

Sha256 - see the list of 267 samples below

Malware source URLs

hxxp://sdjflsdflsdshfds.medailo.cn/mvy/32085.apk
hxxp://sdjflsdflsdshfds.ninshuohua.cn/mvy/32085.apk
hxxp://sdjflsdflsdshfds.hbzs88.cn/mvy/34021.apk
hxxp://spert.huxiawang.cn/mvy/34021.apk
hxxp://sdjflsdflsdshfds.qoshi.cn/mvy/34021.apk
hxxp://ospert.huxiawang.cn/mvy/34021.apk

contagio

AVG | Top Threats

The Official Lookout Blog

Adobe reader w old versions for Android

Rogunix.com - Mobile malware links

Xuxian Jiang @ NC State University

Kinetoo: the smartphone samurai's log

AVG Mobilation | News and Media Releases | Android Security

TAKE A SAMPLE, LEAVE A SAMPLE.

UPLOAD BOX
please upload ONLY mobile malware samples and save them in zip files with password infected. Thank you
You can also email your samples (see profile for email address)

Drag and drop files here to upload or
Select Files

MALWARE LIST

- See the categories for the malware listed on this blog.

Download. Email me if you need the password

Read more »

0 comments Labels: android, Red Drop, Spyware Links to this post

SATURDAY, JULY 9, 2016

Pokemon GO with Droidjack - Android sample

Research: Proofpoint. DroidJack Uses Side-Load...It's Super Effective! Backdoored Pokemon GO Android App Found

File Info:
MD5 d350cc8222792097317608ea95b283a8
SHA1 561ae708f234f46dbdca1d7f2a38d854d9bb60df
SHA256 15db22fd7d961f4d4bd96052024d353b3ff4bd135835d2644d94d74c925af3c4

Download. Email me if you need the password.

1 comments Labels: android, DroidJack, pokemonGo Links to this post

SUNDAY, JULY 3, 2016

- Items listed below are old and were posted on contagio before - HERE
  Android.Bgserv
  BasebridgeA
  BasebridgeB
  CollectionofJavamobilemalware
  CollectionofSymbianmalware
  DDreamLight
  Doombot_1.sis
  DroidDreamvariants
  DroidKungFu.A
  DroidKungFu.B
  Dust.exePocketPCfileinfector2004
  Fake10086
  FSCGAD_1.00.8.apk
  Geinimi.1299167838 swampy.sexpos.apk
  Holy***kingBible
  iCalendar
  ikeeBiphone
  iMatch
  JavaMobileMalwareSMSsender.zip
  jSMSHider
  MonkeyJump2.0.apk
  Mosquito.1_1.sis
  myournetpower.SuperSolo.apk
  Palm:Phage
  PJApps variants
  PMCryptic.exeWindowsCEmalware-2008
  PMSW_V1.8_.apk
  pornoplayer.apk
  RZStudio
  SMS_Replicator_Secret.apk
  SMStrojan-Tank_3d.jar
  SymbianCabir
  SymbOS_Zitmo.ACERT.SIS
  Trojan.Palm.Liberty
  Trojan.Palm.Vapor
  Trojan-SMSforAndroidFakePlayerRUapk

SEARCH THIS BLOG

Search

CATEGORIES

Overlay banker malware locker

Research: Trend Micro: Fake Bank App Ramps Up Defensive Measures
Fake Bank App Phishes Credentials, Locks Users Out

Also see: http://contagiominidump.blogspot.com/2016/07/whatsapp-sberbank-android-banker.html

Download. Email me if you need the password

File information: SHA1

Read more »

0 comments Labels: android, Banker, locker, overlay Links to this post

Marcher overlay Android trojan

Research: IBM XForce Exchange. Marcher Android Bot

Sample credit: Marc Rivero López

Download. Email me if you need the password

File information:
fafaebe042ba9c59b2c3f65f43774cdb5369f838469e133a7c26e824f6d20cc6
b8b9868a24898c8cb39d90c6d38233efabff5b0daf67bbbb54d1e3d0751dd4cb
9d76af8c314e9904906218974c6ae6eec055932aad0292de3554bf5a86371b5b
0de832302ec11bcfda465e903fcd66b2a0bcc8c2b627b43196ef76ca02899765
fd988b737500c564d143095972b20f6a0acd5a4f16a0e10fec8c4bb776469601

- Adware (1)
- airpush (1)
- Androguard (1)
- android (90)
- Android icon vulnerability (1)
- Android-steek (1)
- Android.Titan.1 (1)
- androrat (1)
- Angry Birds (1)
- anserverbot (1)
- Apkquq (1)
- appbuyer (1)
- Appinventor (1)
- APT (1)
- Armour (1)
- Arspam (1)
- Assassins Creed (1)
- AVpass (1)
- awware (1)
- Backdoor.AndroidOS.Obad.a (1)
- Backflash (1)
- Badnews (1)
- BankBot.34 (1)
- Banker (3)
- Banking (2)
- basebridge (2)
- BatteryDoctor (1)
- Beita (1)
- blackberry (2)
- bootkit (1)
- botnet (1)
- Cajino (1)
- Carberp; Android (1)
- CarrierIQ (1)

MD5s
56ED9C77571C81C208BF49FEF4422E8F
58FB8F875F3C9ACF0FD0C4EE3C0A002A
5B0EA09640C86C25DD2AEE85515B8AA7
8B9044C22485A84831B14FB8E63AD349
FBF3348F3137DD673745677FFD8E91FF

0 comments Labels: android, Marcher, overlay Links to this post

Android Triada modular trojan

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/

Read more »

0 comments Labels: android, modular, Triada Links to this post

SATURDAY, JULY 2, 2016

- Chathook (1)
- CI4 SMS Bot (1)
- clickfraud (2)
- Cloud Atlas (3)
- coinkrypt (1)
- ConnectSMS (1)
- coolreaper (1)
- Copy9 (1)
- Counterclank (2)
- Crisis (1)
- Crosate (1)
- cryptolocker (1)
- CVE-2014-3153 (1)
- CVE-2015-3636 (1)
- DDoS (1)
- deathring (1)
- Dendroid (1)
- dialer (1)
- DKFBootKit (1)
- Dougalek.A (1)
- Drive-by (1)
- DriveByDownload (1)
- droiddeluxe (1)
- DroidDreamLight (1)
- DroidJack (2)
- DroidKungFu (2)
- Droidpak (2)
- DropDialer (1)
- DSEncrypt (1)
- Enesoluty (1)
- exploit (1)
- Exprespam (1)
- Extension (1)

Android overlay malware - credentials stealer, banker

Research: Fireeye. The latest Android overlay malware spreading via sms phishing in Europe.

Download. Email me if you need the password

List of files.
MD5
035D1F3B7FB532A33DE7A8445F9FA325
036258E2C51E21C140B5838CE9BFB4F8
05131969AF2AE6CBFDDF789512F02AA2
06E74DF867E9CB5C1BAFC98165C6C248
...
Read more »

0 comments   Labels: android, overlay, sms   Links to this post

Android spyware for Viber app (Beaver Gang Counter)

Research: Sophos: “Beaver Gang Counter” malware ejected from Play Store

MD5 65065b53381ebc971160a91ef81dec99
SHA-1 433293e2689e8377c890940ed77f8fb9db24a53e
SHA-256 a707cb76e566321c08b8ba8f5c89cb0cf41125468366f5b8fdad8c6fa526deb4

Download. Email me if you need the password

https://www.virustotal.com/en/file/a707cb76e566321c08b8ba8f5c89cb0cf41125468366f5b8fdad8c6fa526deb4/analysis/

Read more »

0 comments   Labels: android, spyware., Viber   Links to this post

- fake angry (1)
- fake AV (1)
- Fake banker (1)
- Fake Installer (5)
- Fake Vertu (1)
- FakeApp.AL (1)
- FakeAV (1)
- Fakebank (2)
- Fakebanker (1)
- Fakedaum (1)
- Fakedefender (1)
- FakeGooglePlay (1)
- Fakeguard (2)
- FakeJobOffer (1)
- Fakelash (1)
- FakeLookout.A. (1)
- Fakemart (2)
- FakeNotify (1)
- Fakeplay (1)
- FakeRegSMS.B (1)
- Faketaobao (1)
- Faketimer (1)
- faketoken (1)
- Fakeupdate (1)
- Feejar (1)
- FindAndCall (1)
- FinFisher (1)
- Finspy (1)
- Fonefee (1)
- Fraud (1)
- Gamex (1)
- Gazon (1)
- Geinimi (11)
- Gepew (1)

Godless Android root exploit samples

Research: 'GODLESS' Mobile Malware Uses Multiple Exploits to Root Devices
http://documents.trendmicro.com/assets/pdf/goddless-mobile-malware-uses-multiple-exploits-to-root-devices.pdf

List of files:
MD5:
32DCA26EEE9B8BEDE8C27278A77F031B
3B1C1D476EA80BD58F3EB1BBB32C42FA
48AB87DE9DE719A08F3F70AEF4642C02
5ACEB560AC3F56956F2F4F29AD227A91
633E34627FC5068C52DF2314D0DCF735
844BA4A0564CA7FF99E5C85CAA926AD4
A5A36007625371C5C828B938796578CA
B98988B42F5E3EC92A557A1F31DF333D
BC5D697E9217FE06194E565C4E031517
F95457DC6FE0BC142D541FEA47D7CF1D
FB04E52C9C93E65F980876C767D003DC
FC27A200F241D42A46786ADEA05B0339

SHA1
44E81BE6F7242BE77582671D6A11DE7E33D19ACA
50450EA11268C09350AAB57D3DE43A4D5004B3A1
57795C32F75A02A68B9A8ACB5820EB039C083A16
5900FABBE36E71933B3C739EC62BA89AC15F5453
5D2A08D7C1F665EA3AFFA7F9607601FFAE387E8B
74A55E9EA67D5BAF90C1AD231E02F6183195E564
7809E1B6F85EE0FA7F0C2A3F1BFDC7FA668742BB
7EBDD80761813DA708BAD3325B098DAC9FA6E4F5
84C444A742B616BC95C58A85C5C483412E327C50
A3E84C4B770EF7626E71C9388A4741804DC32C15
AED8828DC00E79A468E7E28DCA923CE69F0DFB84
D57D17EB738B23023AF8A6DDAFD5CD3DE42FC705

Download. Email me if you need the password

- ggtracker (1)
- Godless (1)
- Godwon (2)
- Gone in 60 (1)
- Hacking team (2)
- HeHe (1)
- HGSpy.A (1)
- Hideicon (1)
- HijackRAT (1)
- HTML (1)
- Hummingbad (1)
- iBanking (1)
- iKee (1)
- Inception (3)
- infostealer (19)
- instagram (1)
- iOS (4)
- iphone (5)
- Jollyserv (1)
- judy (1)
- KeyRaider; iOS (1)
- Kmin (3)
- Koler (1)
- Koler.C (1)
- Korean (1)
- LeNa (2)
- LeNa.b (1)
- Lien.A (1)
- locker (5)
- Loozfon (1)
- Lotoor (4)
- Luckycat (1)
- Malapp (1)

Read more »

0 comments Labels: android, CVE-2014-3153, CVE-2015-3636, exploit, Godless Links to this post

Hummingbad - Android fraudulent ad malware campaign samples

Research: Checkpoint. From HummingBad to Worse. Hummingbad Android malware campaign.

Download. Email me if you need the password

List of files - 590 files
SHA256
005f9964b813844a6c6af354456cc7da6d23055fde896b38b04ef094acc20f09
016c6836f756c08755f4aee13d35b4bbf7310fc13a9e5715fa53f315d83d1249
01758cb79e08759d6414c9dd18ccaed4b337adf4b059165d5096dd4f5b79f673
019a0d62a989c8315ad07474027ed91665a6b18413409bd0d714c2e3bcb1558c
01b87d63826e9cf4b5c0a6e4ade6772494817f4bf9ae820b0625a54567b675b2
02308963dbc8827533d03f4274502701fb94b5190ddcbe81672f868e744a9580
02d781a16a7975e7cdd0303f85fab0490ced3e13d86af32207e229469c78ec83
031cc7ef3bf3f380e2902fb199df489d4afb56134215747b36a4da243f405001
031d2ece2d2207d522463bc2674eb6e131b3d58bc2b969d6ef3b2c2c9be5a6f0
....
open the post to see the rest
Read more »

0 comments Labels: Adware, android, awware, Hummingbad Links to this post

WhatsApp - Sberbank Android Banker

Research: ZScaler. Android Banker malware goes social

- Marcher (1)
- MMarketPay (1)
- MobiDash (1)
- modular (1)
- Moghava (1)
- MouaBad.P (1)
- Mouabad.s (1)
- mRat (1)
- Nickyspy (1)
- NotCompatible (2)
- NotCompatible.C (1)
- Oldboot (1)
- Oldboot.B (1)
- opfake (2)
- OSX (1)
- overlay (3)
- Phospy (1)
- Phosty (1)
- Pincer (1)
- PJApps (6)
- Plankton (2)
- podec (1)
- poisoncake (1)
- pokemonGo (1)
- Proxy (1)
- Qicsomos (1)
- ransomware (8)
- Red Drop (1)
- Repane (1)
- Roidsec (1)
- root exploit (6)
- Rootsmart (1)
- Russian (1)
- Samsapo.A (1)

Also see http://contagiominidump.blogspot.com/2016/07/overlay-banker-malware-locker.html

MD5
14F582EB7DBB6BF38FCE331C5D1042EA
19E36E76B58CD49025455AC23CE1461B
1B319EBE6083D273EE14154A1FD89742
21501127972BFBD1C4A89EC39E0AA084
39A5BB63F946F2AF6489456A1281B06D
835576FB19E60F6186F86706CF03AC45
86BF3FAE93B0AE555584860AB4311BB0
C237CF028E46FD07460C289C3FA46025

Sample credit: Shivang Desai and others

Download. Email me if you need the password

Read more »

0 comments Labels: android, Banker, Sberbank, Whatsup Links to this post

FRIDAY, JULY 1, 2016

Android Xiny samples Infostealer

Research: Dr. Web: Trojan targeted dozens of games on Google Play
Lookout: LevelDropper: A takedown of autorooting malware in Google Play

Sample Credit: Tim Strazzere

List of files MD5:
174C652D7595F42211B1BD8E4CD79478
20A79956BC5BF362CBD7F91FC23A7891

- Sberbank (1)
- Scipiex (1)
- SecApk (1)
- Selfmite (1)
- simhosy (1)
- Simplelocker (1)
- SimpleTemai (1)
- simplocker (1)
- Sinpon (1)
- Skullkey (1)
- sm (1)
- Smack (1)
- sms (1)
- SMS worm (1)
- SMS-trojan (20)
- SMSAgent.C (1)
- SMSbot-Google (1)
- SMSSilense (1)
- SMSzombie (1)
- SocialPath (1)
- spad (1)
- SpamSoldier (1)
- Spy App (5)
- Spy banker (1)
- Spyera (1)
- spyeye (1)
- Spyware (1)
- spyware. (1)
- Ssuci (1)
- steek (1)
- Stels (1)
- Stiniter (1)
- Sumzand (1)

66D3DF032D8C4FED2CBBF88F1293F3E6
7683D2F01BF49BED435FE7C2F171A844 (from Lookout blog)
7EBA711410F80CD405AD9FD1DC590C4A
CC881BF76890246559FC83086CFF1A73
D3F3B28C00BD903DFC270FBDF457FA1C
E75A226995CA04152B0007C96A675989

Same files in SHA1
1FACB067F3387802DE18DCC43FB9E8ABE964E479
3646C8361252876012402878B84763403928B588 (from Lookout blog)
8832D44BD531C5934A08979B1358A79C99D77C9F
8FC5DF9B9C80E4EC833DAA2A2D2B00047A6EEDE0
A49156F7F854CEE1727816D269AC5ADA5695ECA5
AC1E0BBCE00F33831735B466BF78C4487F7E2C7B
B611523D20C9B06A31207559F9E43AB1BC717327
ED1AE43A0649FB2CE6581E8FE06444FE0868AE17

Same files in SHA256
490969e1fbcb78ab7cc948a2d799fe9bc7f194930efadeb5b33f1f1118e72263
4cb55a17048352829e5d8fd02be3c334dcf92abfb8e1a697f85ef90f6dd56c3e
7f1ab172f109807c794590b14a728a15153b6644b4694c7ec431d61a8fe35ece
8e33dfacc5dc1e18d145ecdafe576c22f4dbe012e1969522e6e3f4543c51ac22
916211f649695e88dd77f7ebfef9141f25f5ad44f8f1c3052161612e8e9fa063
98e9ae7f2c0be9da1a6f2f8d472d586e7d22b1402914ea306371651d5b22b69f
b9c73175b65beb2641c85831c614ac2da9bbe6d353e3c1625785bad7e40356d4 (from Lookout blog)
db24b4e142acc6f8c81cba1a5703c6ed8b9e39817ab81a91a065e24266527f5a

Download. Email me if you need the password

0 comments   Labels: android, infostealer, Xiny   Links to this post

THURSDAY, JUNE 23, 2016

- SymbianOS (1)
- Tascudap (1)
- Tetus (1)
- TGLoader (1)
- The Interview (1)
- Tigerbot (1)
- Toll Fraud (1)
- tools (1)
- Tor (2)
- Triada (1)
- Uracto (1)
- Usbcleaver (1)
- Uten (1)
- vdloader (1)
- Viber (1)
- vmvol (1)
- waps (1)
- Whatsup (1)
- windows (2)
- wirelurker (1)
- Worm (1)
- Wroba (1)
- xbot (1)
- Xiny (1)
- xsser (1)
- YiSpecter; iphone;iOS (1)
- YZHC (1)
- Zerghelper (1)
- Zertsecurity (1)
- zitmo (3)

SUBSCRIBE TO

Posts

Hacking Team / Crisis Android samples

All Comments

Sample credits: SentinelOne, Tim Strazzere

Download. Email me if you need the password

List of files
00d430877eed07d10c1e730926dcca9f82f282af.apk
0a3ec1fd0256736aeff449a2c9b7b656a6862eaf.apk
0cbcfbebfb33fde66c282fec0248b0d99a829eab.apk
0cc2c8461c78394b186a599c2d5baad364fb41c7.apk
0e8236ddb163e7f3816cfef38b92c6e064887b3f.apk
0ef158c897f91a58aa2a13d25cd3019bc19b9954.apk
153c94a6d464497b07f1ea3511b87206a3621efd.apk

open the post to see the rest...
Read more »

0 comments Labels: android, Crisis, Hacking team Links to this post

SATURDAY, MAY 14, 2016

Android Xbot ransomware

Research : Palo Alto New Android Trojan “Xbot” Phishes Credit Cards and Bank Accounts, Encrypts Devices for Ransom by Cong Zheng, Claud Xiao and Zhi Xu

List of files

ea6d01f87f71afc7fd131f492385d164 93172b122577979ca41c3be75786fdeefa4b80a6c3df7d821dfecefca1aa6b05
79e2b3abdbf33552677660069f891b88 a22b55aaf5d35e9bbc48914b92a76de1c707aaa2a5f93f50a2885b0ca4f15f01
748a81df76ee7e691682e64867fcd48a 20bf4c9d0a84ac0f711ccf34110f526f2b216ae74c2a96de3d90e771e9de2ad4
246f497dc26d18d87f9398758ca1bcc2 f2cfbc2f836f3065d5706b9f49f55bbd9c1dae2073a606c8ee01e4bbd223f29f
7969e4ef1b2fece87b806b5dfe25a3bb 029758783d2f9d8fd368392a6b7fdf5aa76931f85d6458125b6e8e1cadcdc9b4

8e82a09c50b787b18a612addfcaedfab a94cac6df6866df41abde7d4ecf155e684207eedafc06243a21a598a4b658729
538ca97778ac886e121bc054574d7478 e905d9d4bc59104cfd3fc50c167e0d8b20e4bd40628ad01b701a515dd4311449
d5c63390f8a42e051d0ef9fbe7f08046 d082ec8619e176467ce8b8a62c2d2866d611d426dd413634f6f5f5926c451850
6a4a011115e6ab27c9941a849ec27dd2 4b5ef7c8150e764cc0782eab7ca7349c02c78fceb1036ce3064d35037913f5b6
756340895ce28c745d0d6a5409f5ca0f 33230c13dcc066e05daded0641f0af21d624119a5bb8c131ca6d2e21cd8edc1a
d846f7ac66a9a932235fb415b96fee5d dfda8e52df5ba1852d518220363f81a06f51910397627df6cdde98d15948de65
e06dd5ba1a101f855604b486d90d2651 1264c25d67d41f52102573d3c528bcddda42129df5052881f7e98b4a90f61f23
4ed28716716a7f6dc9f6ad1526512b26 7e939552f5b97a1f58c2202e1ab368f355d35137057ae04e7639fc9c4771af7e

Download. Email me if you need the password

1 comments Labels: ransomware, xbot Links to this post

TUESDAY, FEBRUARY 23, 2016

Files download information

After 7 years of Contagio existence, Google Safe Browsing services notified Mediafire (hoster of Contagio and Contagiominidump files) that "harmful" content is hosted on my Mediafire account.

It is harmful only if you harm your own pc and but not suitable for distribution or infecting unsuspecting users but I have not been able to resolve this with Google and Mediafire.

Mediafire suspended public access to Contagio account.

The file hosting will be moved.

If you need any files now, email me the posted Mediafire links (address in profile) and I will pull out the files and share via other methods.

P.S. I have not been able to resolve "yet" because it just happened today, not because they refuse to help. I don't want to affect Mediafire safety reputation and most likely will have to move out this time.

The main challenge is not to find hosting, it is not difficult and I can pay for it, but the effort move all files and fix the existing links on the Blogpost, and there are many. I planned to move out long time ago but did not have time for it. If anyone can suggest how to change all Blogspot links in bulk, I will be happy.

P.P.S. Feb. 24 - The files will be moved to a Dropbox Business account and shared from there (the Dropbox team confirmed they can host it)
The transition will take some time, so email me links to what you need.

2 comments   Links to this post

MONDAY, FEBRUARY 22, 2016

ZergHelper - Pirated iOS App Store’s Client sample

Research:
Pirated iOS App Store’s Client Successfully Evaded Apple iOS Code Review by Claud Xiao

Sample credit: Claud Xiao

File information:
“开心日常英语 (Happy Daily English) / Zerghelper

File: EnglishStudy
Size: 7925888
MD5: 00C7FF895B8707C2D63BEAD4D5ECC9F6

File: EnglishStudy-v5.0.0.ipa
Size: 21506666
MD5: 8135A3E8EF90558C70223EB00F9B19C0

File: Installer.ipa
Size: 6576644
MD5: ED9C55AC907F0FA6D8FF6693C3B14835

Download. Email me if you need the password

0 comments   Labels: Zerghelper   Links to this post

SUNDAY, OCTOBER 4, 2015

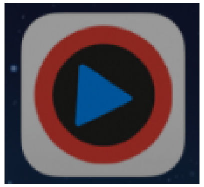
YiSpecter iOS iphone malware samples

Research: Palo Alto. Claud Xiao YiSpecter: First iOS Malware That Attacks Non-jailbroken Apple iOS Devices by Abusing Private APIs

Sample Credit: Claud Xiao

MD5
File: ADPage Size: 2570560 MD5: 8E93947DFD1B11A77A04429BD8B32CED
File: ADPage.ipa Size: 1484304 MD5: 62C6F0E3615B0771C0D189D3A7C50477
File: DaPian Size: 5978608 MD5: 3A41BB59E2946A66BBD03A8B4D51510B
File: DaPian.ipa Size: 2826575 MD5: 6E907716DC1AA6B9C490CE58AAAE0D53
File: HYQvod Size: 1984256 MD5: 35EE9556457D6170EA83C800887C1CBE
File: HYQvod.ipa Size: 2154552 MD5: 97210A234417954C7BBE87BFE685EAAE
File: HYQvod_3.3.3 Size: 3347360 MD5: 304A10D364454EE8F2E26979927C0334
File: HYQvod_3.3.3.ipa Size: 3148992 MD5: 29E147675AF38ECE406B6227F3CCD76B
File: NoIcon Size: 1426368 MD5: E6B45FAF823387BCA7524C4D0329543F
File: NoIcon.ipa Size: 581136 MD5: FBF92317CA8A7D5C243AB62624701050
File: NoIconUpdate Size: 1427040 MD5: 4460F3D29A4BCE8AA8E8FFDE4A467B70
File: NoIconUpdate.ipa Size: 590191 MD5: 0B98EE74843809493B0661C679A3C90C

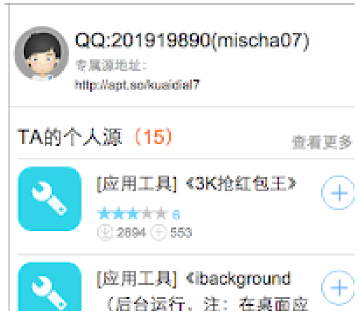
Download. Email me if you need the password (New Link)



2 comments Labels: YiSpecter; iphone;iOS Links to this post

TUESDAY, SEPTEMBER 1, 2015

KeyRaider: iOS infostealer



QQ:201919890(mischa07)
专属源地址:
http://apt.so/kuaidial7

TA的个人源（15） 查看更多

[应用工具]《3K抢红包王》
6
2894 553

[应用工具]《ibackground
（后台运行，注：在桌面应

Research: Palo Alto: KeyRaider: iOS Malware Steals Over 225,000 Apple Accounts to Create Free App Utopia

Sample Credit:Claud Xiao

02464AE6259A2C819447038578150 1B7 9	catbbs.ibackground 3.2.deb
0F710F8397EC969AF26C299A63AEDA8B	9catbbs.iappstore 4.0.deb
1DD1A8C6C213E3B51CD2463D764A9C62	9catbbs.MPPlugin 1.3.deb
3838A37A9BC7DF750FB16D12E32A2FCB	iweixin.deb
3C57E433FBBA1AC1E4DC1B84CEC038FB	repo.sunbelife.batterylife 1.4.1.deb
CAAF060572E57B6D175C3959495BCDBF	9catbbs.GamePlugin 6.1-9.deb
DDF224F63EE9C7FBA76298664A2B0B00	9catbbs.iappinbuy 1.0.deb

Download
Email me if you need the password (2015-09-03 - fixed zip file)

2 comments Labels: KeyRaider; iOS Links to this post

Home Older Posts

Subscribe to: Posts (Atom)

FOLLOW BY EMAIL

Email address... Submit

javascript:void(0)