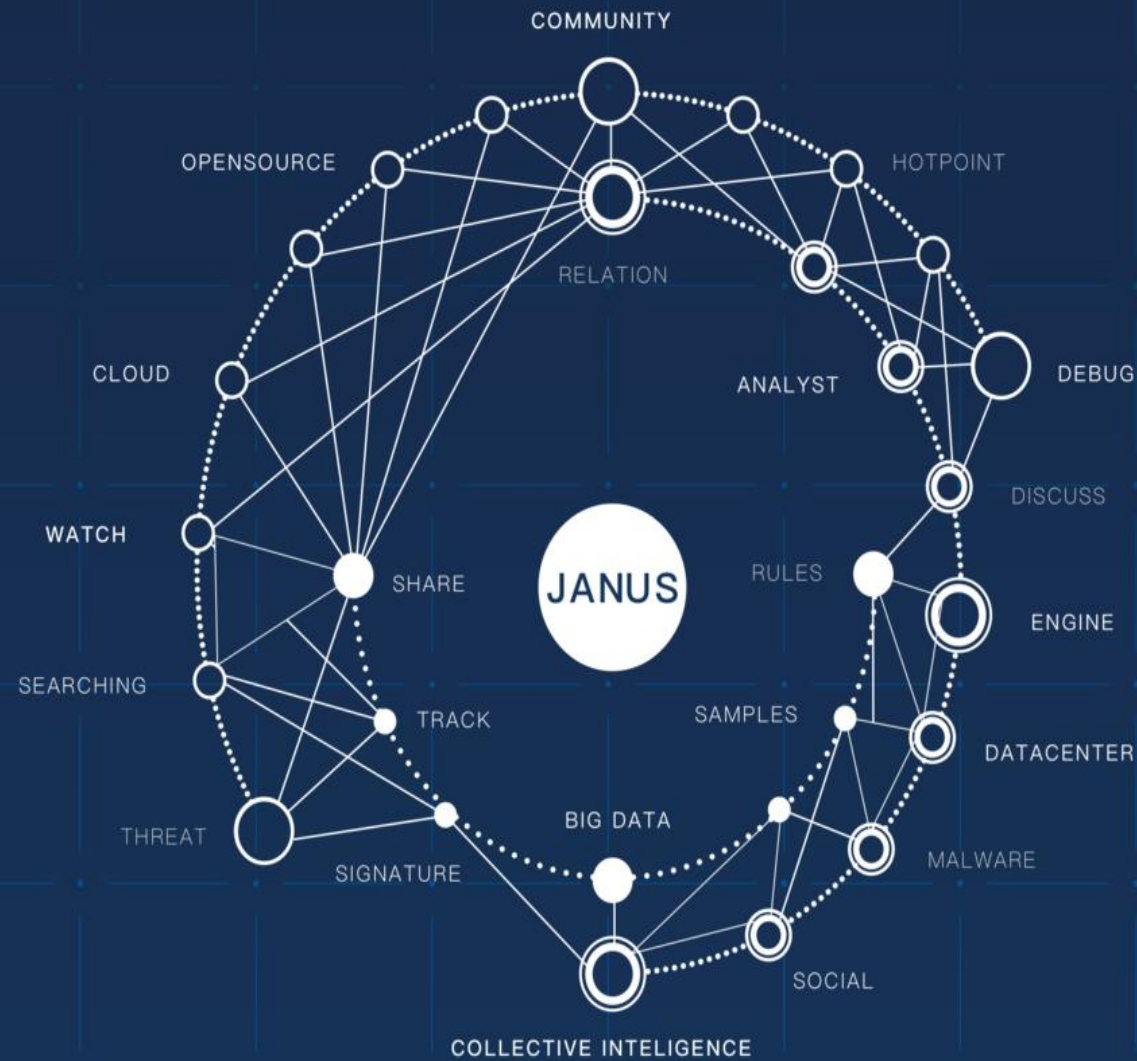


[Apply For Trial](#)



Define the rules  Rebuild the order

About us

- From PwnZen (www.pwnzen.com), a startup founded by Team Pangu.
- Janus project: www.appscan.io
- Chen Yexuan
 - Chen Yexuan is working as a Product Manager in Team Pangu. He has rich experience in web security, mobile security, cloud computing, and data mining. He was a speaker for XCon 2009.
- Tang Zhushou
 - Tang Zhushou is a member of Team Pangu. His research focuses on program analysis, theory and algorithm. He is now leading the research on software similarity detection, machine learning, and data analysis in Team Pangu. He is also an active speaker of POC, syscan360, etc.

Motivation

- We have been developing static analysis engines for Android apps since 2010
 - Data flow analysis
 - Taint Tracking
- Capable to identify suspicious or malicious behaviors, and discover potential vulnerabilities
- But, it's **slow**
- False positives and false negatives are unavoidable

Motivation

- Dilemma
 - Analyzing all Android apps on the market is impossible for us
 - Reviewing all reports is also impossible for us
- Solution
 - Scan applications on demand (with the interest of end users)
 - Leverage the users' inspection and audit to purify analysis results
 - Enable the users to define light-weight scanning rules
 - Facilitate an open community for security professionals to cultivate the sharing of samples, experiences, common issues, and advanced knowledge

Mobile Security

Detection

Customized Scan


My Rules

Community Rules

Threat Center

Trends

+ Add APK




WhatsApp Messenger
Version: 2.7.1528 Size: 4.9M
MD5: fe270dfa6e085c99fa992e32f9709113

Examination • ● ●

View Report

Trace Code




手机淘宝
Version: 3.0 Size: 954.7K
MD5: c923169e14fecf89b055efff4aab753d

Low Risk 34 Medium Risk 25 High Risk 0

View Report

Trace Code




WhatsApp
Version: 1.0 Size: 411.3K
MD5: 319f8e9a009875dbe964a29a7c0c3aa2

Low Risk 21 Medium Risk 2 High Risk 2

View Report

Trace Code




GoogleService
Version: 1.0 Size: 705.7K
MD5: 0816d7fbd9af3c950bd35929fadb544

Low Risk 29 Medium Risk 41 High Risk 8

View Report

Trace Code




Twitter
Version: 5.101.0 Size: 26.6M
MD5: bcd9f208a8c698290345fcc459f45637

Low Risk 9 Medium Risk 0 High Risk 0

View Report

Trace Code




移动积分
Version: 1.105.1 Size: 233.4K
MD5: e29f8b6174b170304c81b13cd716e421

Low Risk 12 Medium Risk 13 High Risk 2

View Report

Trace Code




WhatsApp Messenger
Version: 2.8.886 Size: 6.3M
MD5: 665e9e30303492fd5a9c0e47c58dedfc

Low Risk 52 Medium Risk 97 High Risk 14

View Report

Trace Code



The Weaver
Version: 1.0.2 Size: 8.2M
MD5: f9adf6d76d2f5041c497b9f91eac5873

Low Risk 163 Medium Risk 28 High Risk 23

View Report

Trace Code



九歌音乐(Joygor Music)
Version: 2.0.23 Size: 6.6M
MD5: 2143721d00d8eb083587904c2c65c0fe

Low Risk 384 Medium Risk 101 High Risk 24

View Report

Trace Code



小白点
Version: 1.5.0 Size: 1.8M
MD5: db9ff3bc8b36ff2de277c468e26b052f

Low Risk 17 Medium Risk 10 High Risk 1

View Report

Trace Code



笑话视频
Version: 1.0 Size: 5.3M
MD5: 5d3f33107997a4f93c9885ff9f8e9ea5

Low Risk 22 Medium Risk 27 High Risk 1

View Report

Trace Code



棒球大战僵尸 Baseball vs Zombies
Version: 3.3 Size: 23.6M
MD5: 89bb5c387876d33b09e4255780eede4a

Low Risk 22 Medium Risk 27 High Risk 1

View Report

Trace Code

On demand analysis

Project Explorer #Issues +

- AndroidManifest.xml
- src
 - android
 - baidu
 - ecjl
 - jhfdbxv
 - trpnl
 - AaTService.java
 - AndroidApp.java
 - AndroidserviceAct
 - AppManage.java
 - Audio.java
 - BackIp.java
 - BuildConfig.java
 - CRC32.java
 - Camerapic.java
 - DBOpenHelper.jav
 - DDMsm.java
 - DirTheard.java
 - ExecCmd.java
 - FileManage.java
 - FileMd5.java
 - FileTrans.java
 - FxService.java
 - GPS.java
 - GetHttp.java
 - GetMobileInfor.jav
 - GsmLocation.java
 - Heart.java
 - HttpGetFile.java
 - InstallApk.java
 - InstallApkThread.j
 - LoadPlugins.java
 - MMS.java
 - MontePI.java
 - NetWorkMonitor.j
 - ObjectToFile.java

Main Page string RecvThread.java x

```

950.         goto label_53;
951.     }
952.     lv10_SmsManager.SendTextMessage(lv11_String, null, lv3_Iterator.next(), null, null);
953.     goto label_1495;
954.     label_1902:
955.     if(!lv3_Iterator.hasNext()) {
956.         goto label_53;
957.     }
958.     lv10_SmsManager.SendTextMessage(lv11_String, null, lv3_Iterator.next(), null, null);
959.     goto label_1902;
960.     label_1633:
961.     if(lv57_int < lv35_Str
962.         lv41_1_String = lv
963.         if(lv41_1_String
964.             String lv36_String = this.f_service.f_m_app.f_m_out;
965.             if(lv36_String == null) {
966.                 goto label_1663;
967.             }
968.             new File(String.valueOf(lv36_String) + lv41_1_String + ".db").delete();
969.         }
970.         label_1663:
971.         ++lv57_int;
972.         goto label_1633;
973.     }
974.     label_53:
975.     if(lv31_String.length() > 0) {
976.         this.f_service.f_udp.SendData(String.format("offlinecmdorder\n%s\n%s", this.f_service.f_m_Imei, lv31_String));
977.     }
978.     if(lv60_int == 0) {
979.         goto label_0;
980.     }
981.     this.f_service.f_udp.SendData("backcmd\u0001" + this.f_service.f_m_Imei + "\u0001" + lv78_String);
982.     goto label_0;
983. }
984. }
  
```

Goto Declaration Ctrl+click
 Show XRef Ctrl+X
 Show Call Hierarchy
 Show Type Hierarchy

Interactive Analysis Environment

search X

RecvThread

- f_data1 : byte[]
- f_m_weixin : String
- f_service : AaTService
- f_str : String
- RecvThread(AaTService) : void
- Xor(byte[]) : String
- checkSDCard() : boolean
- delAllFile(String) : boolean
- delFolder(String) : void
- isNumeric(String) : boolean
- run() : void

RecvThread.java RecvThread.smali

Search Result Description Call Hierarchy x

sendTextMessage - ecjl/jhfdbxv/trpnl/RecvThread.java : 958
 run - ecjl/jhfdbxv/trpnl/RecvThread.java : 958

- Project Explorer
- #Issues +
- Send SMS detect (14)
 - ecjl.jhfdbxv.trpnl.DDMsm
 - ecjl.jhfdbxv.trpnl.RecvThread
 - ecjl.jhfdbxv.trpnl.RecvThread
 - ecjl.jhfdbxv.trpnl.RecvThread
 - ecjl.jhfdbxv.trpnl.RecvThread
 - ecjl.jhfdbxv.trpnl.DDMsm
 - ecjl.jhfdbxv.trpnl.DDMsm
 - ecjl.jhfdbxv.trpnl.DDMsm
 - ecjl.jhfdbxv.trpnl.DDMsm
 - ecjl.jhfdbxv.trpnl.DDMsm
 - ecjl.jhfdbxv.trpnl.RecvThread
 - ecjl.jhfdbxv.trpnl.RecvThread
 - ecjl.jhfdbxv.trpnl.RecvThread
 - ecjl.jhfdbxv.trpnl.RecvThread
 - + Service detect (1)
 - + Activity hijacking detect (2)
 - + Embedded code detect (5)
 - + SD write(test) (4)
 - + Log detect (8)
 - + SharedPreferences detect (2)
 - + Receiver expose detect (3)
 - + Over privilege detect(test) (10)
 - + Receiver explicit expose detect (1)
 - + SD read(test) (1)
 - + Permission usage detect(test) (22)
 - + Activity expose detect (1)
 - + Attack Window detect (1)
 - + Broadcast sniffing detect (3)

Main Page

string RecvThread.java x

```

950.         goto label_53;
951.     }
952.     lv10_SmsManager.SendMessage(lv11_String, null, lv3_Iterator.next(), null, null);
953.     goto label_1495;
954. label_1902:
955.     if(!lv3_Iterator.hasNext()) {
956.         goto label_53;
957.     }
958.     lv10_SmsManager.SendMessage(lv11_String, null, lv3_Iterator.next(), null, null);
959.     goto label_1902;
960. label_1633:
961.     if(lv57_int < lv35_String.length) {
962.         lv41_1_String = lv35_String[lv57_int];
963.         if(lv41_1_String != null && lv41_1_String.length() > 0 && this.f_service.f_m_app != null) {
964.             String lv36_String = this.f_service.f_m_app.f_m_out;
965.             if(lv36_String == null) {
966.                 goto label_1663;
967.             }
968.             new File(String.valueOf(lv36_String) + lv41_1_String + ".db").delete();
969.         }
970.         label_1663:
971.             ++lv57_int;
972.             goto label_1633;
973.         }
974.     label_53:
975.         if(lv31_String.length() > 0) {
976.             this.f_service.f_udp.SendData(String.format("offlineorder\n%s\n%s", this.f_service.f_m_Imei, lv31_String));
977.         }
978.         if(lv60_int == 0) {
979.             goto label_0;
980.         }
981.         this.f_service.f_udp.SendData("backcmd\u0001" + this.f_service.f_m_Imei + "\u0001" + lv78_String);
982.         goto label_0;
983.     }
984. }
    
```

RecvThread.java RecvThread.smali

search

RecvThread

- △ f_data1 : byte[]
- △ f_m_weixin : String
- △ f_service : AaTService
- △ f_str : String
- RecvThread(AaTService) : void
- Xor(byte[]) : String
- checkSDCard() : boolean
- delAllFile(String) : boolean
- delFolder(String) : void
- isNumeric(String) : boolean
- run() : void

Search Result	Description x
Description:	
There is no interaction for this SMS sending operation, risk level: HIGH.	
Principle:	
[]	
Solution:	
[Coming Soon]	

Send SMS message
without interaction,
risk HIGH

- Project Explorer
- #Issues +
- Send SMS detect (14)
- ecjl.jhfdbxv.trpnln.DDMsm
- ecjl.jhfdbxv.trpnln.RecvThread
- ecjl.jhfdbxv.trpnln.RecvThread
- ecjl.jhfdbxv.trpnln.RecvThread
- ecjl.jhfdbxv.trpnln.RecvThread
- ecjl.jhfdbxv.trpnln.DDMsm
- ecjl.jhfdbxv.trpnln.DDMsm
- ecjl.jhfdbxv.trpnln.DDMsm
- ecjl.jhfdbxv.trpnln.DDMsm
- ecjl.jhfdbxv.trpnln.DDMsm
- ecjl.jhfdbxv.trpnln.RecvThread
- ecjl.jhfdbxv.trpnln.RecvThread
- ecjl.jhfdbxv.trpnln.RecvThread
- ecjl.jhfdbxv.trpnln.RecvThread
- + Service detect (1)
- + Activity hijacking detect (2)
- + Embedded code detect (5)
- + SD write(test) (4)
- + Log detect (8)
- + SharedPreferences detect (2)
- + Receiver expose detect (3)
- + Over privilege detect(test) (10)
- + Receiver explicit expose detect (1)
- + SD read(test) (1)
- + Permission usage detect(test) (22)
- + Activity expose detect (1)
- + Attack Window detect (1)
- + Broadcast sniffing detect (3)

Main Page string RecvThread.java x

4746. move-result v12

4747.

4748. if-eqz v12, :cond_75

4749.

4750. invoke-interface {v3}, Ljava/util/Iterator;->next()Ljava/lang/Object;

4751.

4752. move-result-object v13

4753.

4754. check-cast v13, Ljava/lang/String;

4755.

4756. .line 1041

4757. .local v13, "text":Ljava/lang/String;

4758. const/4 v12, 0x0

4759.

4760. const/4 v14, 0x0

4761.

4762. const/4 v15, 0x0

4763.

4764. invoke-virtual/range {v10 .. v15}, Landroid/telephony/SmsManager;->sendTextMessage(Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;Landroid/app/PendingIntent;Landroid/app/PendingIntent;)V

4765.

4766. goto :goto_cab

4767.

4768. .line 1047

4769. .end local v13 # "text":Ljava/lang/String;

4770. .end local v15 # "list":Ljava/util/ArrayList;, "Ljava/util/ArrayList<Ljava/lang/String;>;"

4771. :cond_cbe

4772. const/16 v16, 0x0

4773.

4774. const/16 v18, 0x0

4775.

4776. const/16 v19, 0x0

4777.

4778. move-object v14, v10

4779.

4780. move-object v15, v11

4781.

4782. invoke-virtual/range {v14 .. v19}, Landroid/telephony/SmsManager;->sendTextMessage(Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;Landroid/app/PendingIntent;Landroid/app/PendingIntent;)V

RecvThread.java RecvThread.smali

Search Result	Description	Call Hierarchy
src		
ecjl		

Provide smali view to
get signature

Mobile Security

Detection

Customized Scan

My Rules

Community Rules

Threat Center

Trends

+

New Scan

Virus - NineBox_v1

Scan Range: 2 Apps: 1

2016-03-29 23:24:13

2016-03-29 23:16:39

Audit - ServerSoc...

Scan Range: 4 Apps: 3

2016-03-29 23:03:37

2016-03-29 23:02:09

Audit - ftp_crede...

Scan Range: 5 Apps: 2

2016-03-29 21:23:15

2016-03-29 21:21:17

Audit - email_cre...

Scan Range: 3 Apps: 3

2016-03-29 11:36:17

2016-03-29 11:33:55

Audit - weibo_cre...

Scan Range: 5 Apps: 3

2016-03-29 11:36:30

2016-03-29 11:33:34

New Rule

☒ My Rules☒ Collected Rulesets

[/]

Certificate Example

Private

0

Created: 2016-03-29 22:20:20 Syntax: ok

[/]

Email Example

Private

0

Created: 2016-03-29 22:19:05 Syntax: ok

[/]

Domain Example

Private

0

Created: 2016-03-29 22:17:14 Syntax: ok

[/]

IP Example

Private

0

Created: 2016-03-29 22:15:23 Syntax: ok

[/]

Audit - ServerSocketPort(WormHole_SERIES)

Public

3

Created: 2016-03-29 12:23:45 Syntax: ok

[/]


Audit - facebook_credential


Public


0

Created: 2016-03-28 23:20:13 Syntax: ok

Define your own ruleset, perform your customized scan


 Mobile Security


 Detection


 Customized Scan

[My Rules](#)

Community Rules

 Threat Center

 Trends

 Audit - ftp_credential

Create: 2016-03-28 22:21:51
Owner: demo

Rule Code

Related Apps

Comment

1

//api of ftp

2

// invoke-virtual {v4, v0, v1}, Lorg/apache/commons/net/ftp/FTPClient;->login(Ljava/lang/String;Ljava/lang/String;

3

import "janus"

4

5

rule ftp_credential

6

{

7

meta:

8

description = "This rule is used to detect ftp credential"

9

10

strings:

11

\$a = "Lorg/apache/commons/net/ftp/FTPClient;->login(Ljava/lang/String;Ljava/lang/String;)Z"

12

// \$a = "Login"

13

condition:

14

any of them

15

16

}

Edit

Write your own rule.

In this example, we can find apps use ftp protocol, which potentially leaks username and password

- Mobile Security
- Detection
- Customized Scan
- My Rules
- Community Rules
- Threat Center
- Trends



Audit - ftp_credential

Create: 2016-03-28 22:21:51
Owner: demo

0 0 0

Rule Code Related Apps Comment



儿童每日食谱-菜谱,营养,喂养,饮食,辅食,做菜,美食,早餐
Version : 1.1
Size : 12.1M
SHA1 : 5618d8f7f6564fee30a75902cf376921776ad34a
MD5 : 574d0442b9891f7f357bfa540df9d948

[View hit signature](#) 2



笑话视频
Version : 1.0
Size : 5.3M
SHA1 : 9581d87e84345f096d98200416872ef93491eaef
MD5 : 5d3f33107997a4f93c9885ff9f8e9ea5

[View hit signature](#) 1



Perfect Viewer
Version : 2.5.1.5
Size : 7.1M
SHA1 : ff7ac1c0b4161371ea5859a43aa8e3bdb4c50d93
MD5 : a860e6bb2e83421282dc98eebf33e569
\$a = Lorg/apache/commons/net/ftp/FTPClient;->login(Ljava/lang/String;Ljava/lang/String;)Z

● ————— ● This app hit the rule

[Fold](#)

Mobile SecurityDetectionCustomized Scan

My Rules

Community Rules

Threat CenterTrends

rule1

Create: 2016-03-28 21:43:44

Owner: xiaoho

1

1

Rule Code

Related Apps

Comment

```
1 rule wormHole
2 {
3   meta:
4     description = "Wormhome vulnerability found in com.qihoo.secstore con GPlay. After app launch, a
5   strings:
6     $a = "/getModel0"
7     $b = "/in" // download and install apk
8     $c = "/openPage" // Open URL
9     $d = "/openActivity" // Launch activity
10    $e = "/isAppInstalled" // Check app existance
11    $f = ".360.cn"
12    $g = ".so.com"
13    $h = ".qihoo.net"
14    $i = ".gamer.cn"
15    // 360 domains host through yunpan clod storage (anyone can upload files here)
16  condition:
17    ($a or $b or $c or $d or $e) and ($f or $g or $h or $i)
18
19
20
21 }
22
```

Edit

Domain

4

360.cn

so.com

qihoo.net

gamer.cn

Automatically
extract domain,
ip, etc. in
rule.

Mobile Security

Detection

Customized Scan

My Rules

Community Rules

Threat Center

Trends

360.cn domain

Be discovered by xiaoho at 2016-03-28 21:43:50

DNS Provider : 厦门易名科技股份有限公司

Rulesets : rule1(xiaoho)

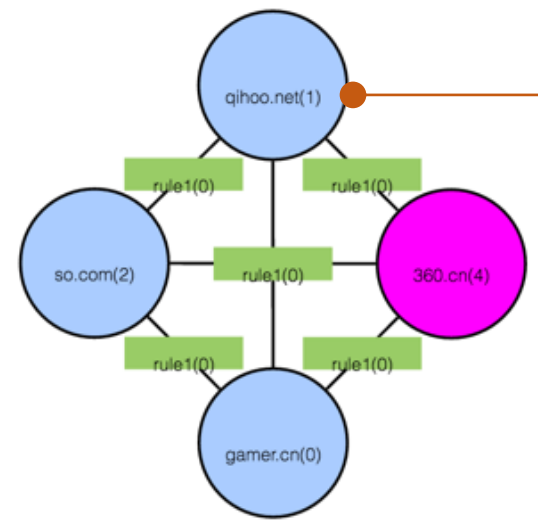
Events:

IP: 222.73.144.195 [More infos \(from virusbook \)](#)

Tags:

Related Items related Apps Comment Visual whois

Gravity Modes Reset Pause Selection Details



Relation between these domains



Mobile Security

Detection

Customized Scan

My Rules

Community Rules

Threat Center

Trends

Search Community Rules



	demo rule 5 0			
	User Name:xiaoho	Created:2016-03-29 16:43:09	Syntax:ok	
	demo rule 4 0			
	User Name:xiaoho	Created:2016-03-29 16:38:33	Syntax:ok	
	Audit - ServerSocketPort(WormHole_SERIES) 3			
	User Name:demo	Created:2016-03-29 12:23:45	Syntax:ok	
	Audit - facebook_credential 0			
	User Name:demo	Created:2016-03-28 23:20:13	Syntax:ok	
	Statistics - geinimi_statistics 0			
	User Name:demo	Created:2016-03-28 22:37:25	Syntax:ok	
	Audit - aws_credential 0			
	User Name:demo	Created:2016-03-28 22:29:21	Syntax:ok	
	Audit - weibo_credential 3			
	User Name:demo	Created:2016-03-28 22:24:44	Syntax:ok	
	Audit - email_credential 3			
	User Name:demo	Created:2016-03-28 22:22:58	Syntax:ok	
	Audit - ftp_credential 3			
	User Name:demo	Created:2016-03-28 22:21:51	Syntax:ok	
	Audit - WormHole_demo 0			
	User Name:demo	Created:2016-03-28 20:39:21	Syntax:ok	

Share rule to
community, everyone
can follow, discuss
this rule and apps hit
this rule.

- Mobile Security
- Detection
- Customized Scan
- My Rules
- Community Rules
- Threat Center
- Trends

360浏览器

Full Reports

com.qihoo.browser

Package:com.qihoo.browser

Displayed version:6.8.7beta Size:7.5M

Date added:2015-11-16 11:05:11

SHA1:931aeb81cc3fd140bc7d29e28187db7381c0fada

MD5:797ff3af86be8d103fb45b452fc6b0d6

Download

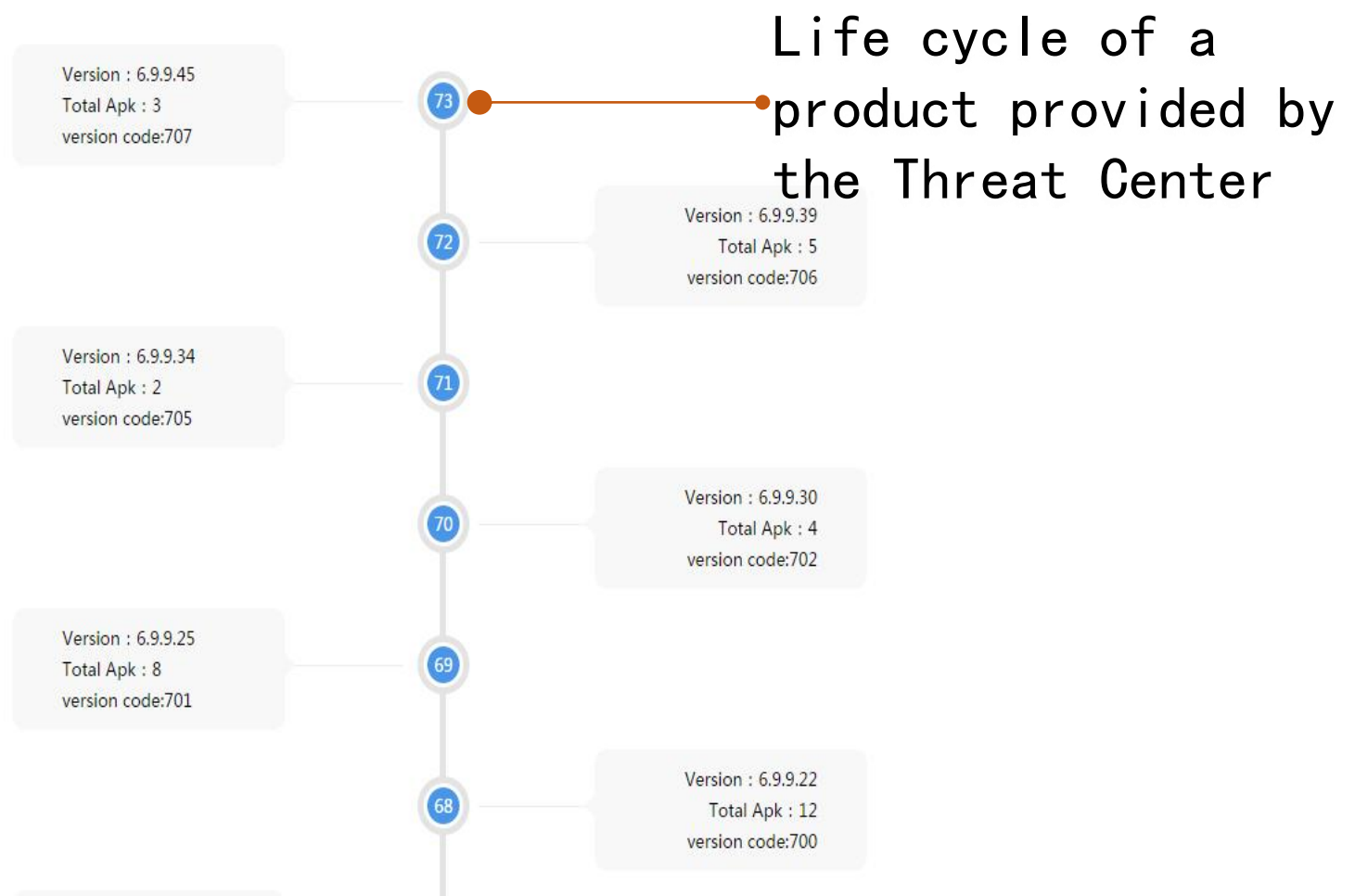
0

0

0

Life Cycle

Comments



whatsapp

App(1965)

Rules(0)

target



WhatsApp Messenger

Version:2.8.886 Size:6.3M

Package : [com.whatsapp](#)

Developer:[whatsapp inc.](#)

MD5 : 665e9e30303492fd5a9c0e47c58dedfc

SHA1 : 6bb62df6174f9e5617ae51e168d3c09f9a757c8b

Download



WhatsApp Messenger

Version:2.8.3143 Size:6.6M

Package : [com.whatsapp](#)

Developer:[whatsapp inc.](#)

MD5 : 34fc7196a19152d4969e233cfede421b

SHA1 : 9f16b7cda45207c9b37e8f072bc9fae973097feb

Download



WhatsApp Messenger

Version:2.7.1528 Size:4.9M

Package : [com.whatsapp](#)

Developer:[whatsapp inc.](#)

MD5 : fe270dfa6e085c99fa992e32f9709113

SHA1 : 6507256483b52c812dc32bc37059a92fadf4b45c

Download



WhatsApp Messenger

Version:2.7.7109 Size:4.6M

Package : [com.whatsapp](#)

Developer:[whatsapp inc.](#)

MD5 : 01a17b2b861e841d380cc2eb415f80f2

SHA1 : 5917ec4bcf6d83e960e9648392bcf095c9442687

Download

Total 8,000,000 apps

in our database,

including metadata of

static/dynamic

analysis result.

- ☒ Google App
- ☒ Baidu App
- ☒ wandoujia.com
- ☒ Tencent App
- ☒ 360.cn App
- ☒ 91.com App
- ☒ 163.com App
- ☒ Hiapk.com App
- ☒ d.cn App
- ☒ Gfan.com App
- ☒ Sogou App
- ☒ Anzhi App

Mobile Security

Detection

Customized Scan

My Rules

Community Rules

Threat Center

Trends

Tops Apps

Tops Week Tops

- 

飞信云聊版
MD5 f2e63be6c219f1415cc56431b9103858

770 872
- 

飞信云聊版
MD5 1c0b24b51871f6e35af7a8ce9f132fec

253 720
- 


プリティーリズム・シェイク - プリシェイ
MD5 e1ced0e36060f5822be242c85a60bb2a

882 666
- 


飞信云聊版
MD5 001dfda3e237b4cd95e2c2a592a48579

894 586


Trends

- 


demo rule 4
Creator xiaoho
2016-03-29 22:41:46 xiaohoShare

nice rule
- 


rule1
Creator xiaoho
2016-03-29 22:17:32 xiaohoShare

360相关
- 


搜狗浏览器
MD5 e5dce0b4ef223b8947cb40fa07225b70
2016-03-29 22:16:13 xiaohoShare

从没用过的浏览器
- 


WhatsApp Messenger
MD5 cb9a6486a655885050991080480888b7
2016-03-29 20:24:28 demoShare

test
- 


猎豹浏览器
MD5 052970e25009bcf6192d5f200b0b5014
2016-03-29 20:09:38 testShare

yoyoyo checknow
- 

飞信云聊版
MD5 001dfda3e237b4cd95e2c2a592a48579
2016-03-29 17:42:56 xiaohoShare

老唐来看看
- 

激情快播
MD5 f98ee6ad352055892ed0b9718460e434
2016-03-29 16:54:13 xiaohoShare




















老唐来看看啊
- 

系统软件深度卸载
MD5 547ec67e851f52f43bc59a7d20e5590f
2016-03-29 16:03:43 xiaohoShare

fdas

Hot rules and apps for researcher/user.

appname	手机淘宝	icon	
filename	com.taobao.model_3_c...eff4aab753d (3).apk		
md5	C923169E14FECF89B055EFFF4AAB753D	sha1	06D4B585C8DC07AB5446D27434EF805D85A8F7DA
size	0.9MB	shell	Not Found
packagename	com.taobao.model	version	3.0
issuer	CN=inn,OU=ie,O=ing,L=ot,ST=wn,C=cn		

icon1	icon2	layout	signature-packagename pair	call sequence	code sequence	drawable image
icon	apk name	package name	similarity	downloaded	debug	
	VynneMobile	com.vynne	72	downloaded	debug	
	AutumnNucleusN1	appinventor.ai_DanDraperuk.AutumnNucleusN1	51	downloaded	debug	
	Places Near By	appinventor.ai_onlineuse147.PlacesNearBy	60	downloaded	debug	
	Q-Me	com.Qme.testapp	78	downloaded	debug	
	Welcome To SansBra	com.janellebinds.selfexamapp	86	downloaded	debug	
	Touch Square	com.etermalhine.touchdirection	63	downloaded	debug	
	Predicas Cristianas	app.avxmas.predicas	61	downloaded	debug	
	해피하우스 앱 아이콘	webchurch.happyhouse	70	downloaded	debug	
	Brainfreeze Math	com.parkhapplications.brainfreezemath	64	downloaded	debug	
	Lido Taxi	ca.lidotaxi.app	74	downloaded	debug	
	GAP Summit	se.itnaskinen.android.nativevint.gapsummit2014	57	downloaded	debug	
	Climatecode	com.climatecode2	54	downloaded	debug	
	game	ru.bullyboo.game	71	downloaded	debug	
	KralFm	com.SeloSoft.kralfm	51	downloaded	debug	
	微利通券-天龍	com.megahub.prime.activity	60	downloaded	debug	
	Bloemendaal	mobownski.bloemendaal	69	downloaded	debug	
	RSS Reader	org.ccc.rss	74	downloaded	debug	
	boxfish	com.oceanbetter.boxfish	52	downloaded	debug	
	UI/RS Token	com.bon.troncommunity	61	downloaded	debug	

Eacus - MobiSec Lab



AppName: Twitter
 Package: com.twitter.android
 MD5: bcd9f208a8c698290345fcc459f45637
 SHA-1: ed6b2494a5f387c3eb56f449ac959a0c506e67a2
 Version: 5.101.0
 Signature: CN=Android Debug, O=Android, C=US
 PublicKey: Sun RSA public key, 2048 bits modulus:
 20208267221096304619078111634802311480
 74851410418041151952677755335253324678
 65478923820481701236166668830685343843
 2787258515244062754352066209959084410
 56595739500455090838031807792757832241
 2009044618463590688604425636406130057
 66513752409994512288193820894194774812
 17080836918082770053399620110116093718
 69232611923857823874088272340155417280
 21830183895567851845953633838116024319
 41248986324928552296494620859271705967
 27014398136611016791728244923650448364
 23367032978979288150227523585259260053
 08720676380296005498292706923847210249
 75887837696951496283479815328983617686
 44947057922044996877282351109288125344
 026503201
 public exponent: 65537
 sig_version: 3
 sig_serialnum: null

Summary

This task takes: **134.168s**
 Conclusion: **Coming soon**
 Link to: [Coming soon](#)

Basic Analysis

Re-pack Check: **Repacked APK**(total 12266 certifications)
 ADs Check: **AdMob**(total 72 advertisement signatures)
 Obfuscator Check: **Not Found**(total 9 signatures)
 Virus DB Check: **Not Found**(total 24 signatures)
 Embedded APK Check: **Not Found**

Plugin Analysis

FakeID Check: **Not Found**
 Root Check: **Offline**
 Smishing Check: **Offline**
 Masterkey Check: **Offline**

Advance Analysis

Behavior Check: #1 java engine takes 237 ms.
 Risk Level: **HIGH** (total 84 checkPoints and 18 rules)
 [Receiver] On receiving sms message, the app **read sms message**
 #3 c++ engine for server, build version: 2015122207 takes 1972 ms.
 Risk Level: **HIGH**
 [Service] On startup, the app **manipulate accounts**
 [Receiver] On receiving sms message, the app **read sms message**

#2 c++ engine
 128518 ms.
 Risk Level: **HIGH**
 [Service] On startup, the app **manipulate accounts**
 [Receiver] On receiving sms message, the app **read sms message**

Integrate more
function

StormDroid: A Streaminglized Machine Learning-Based System for Detecting Android Malware

Sen Chen

Dept. of Computer Science
East China Normal University
ecnuchensen@gmail.com

Minhui Xue

East China Normal University
NYU Shanghai
minhuixue@nyu.edu

Zhushou Tang

Shanghai Jiao Tong University
Pwnzen Infotech Inc.
ellison.tang@gmail.com

Lihua Xu

Dept. of Computer Science
East China Normal University

Haojin Zhu

Dept. of Computer Science
Shanghai Jiao Tong University

JANUS Beta

- Mobile Security
- Detection
- Customized Scan
- My Rules
- Community Rules
- Threat Center
- Trends

google.com domain

Be discovered by demo at 2016-03-30 02:00:26

DNS Provider : MarkMonitor, Inc.
Rulesets : Domain Example(demo)
Events:
IP: 216.58.200.110 [More infos \(from virusbook \)](#)
Tags:

Related Items related Apps Comment Visual whois

Type	Time	Rulesets	Content
ip	2016-03-30 02:00:26	Domain Example(author:demo)	82.165.37.26

Open to
community/college to
find more interesting
thing.

appscan.io