



Deceiving Permissions - Rules for Android Malware Detection

Vanja Svajcer
Principal Researcher, SophosLabs

Session ID: MBS - 210

Session Classification: Advanced

RSACONFERENCE
EUROPE 2012

Deceiving Permissions

- Overview and stats
- Finding detection rules
 - Process
 - Tools
 - Results



Android malware ecosystem

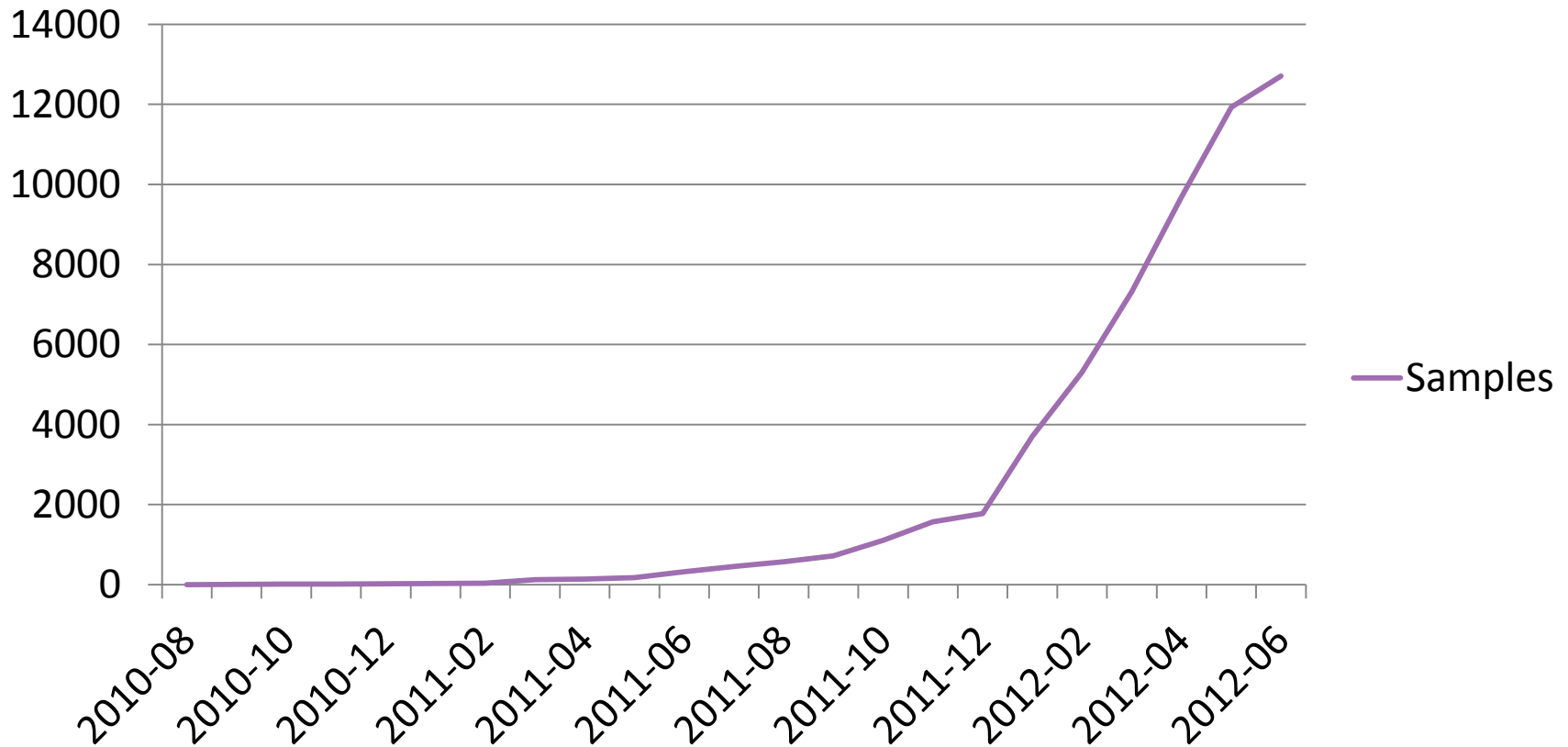


- Information stealers (Andr/SMSRep)
- SMS senders (Andr/AdSMS)
- Phishing (fake mobile banking software)
- Privilege escalation exploits (DroidDream)
- Zeus for Android (Zitmo)

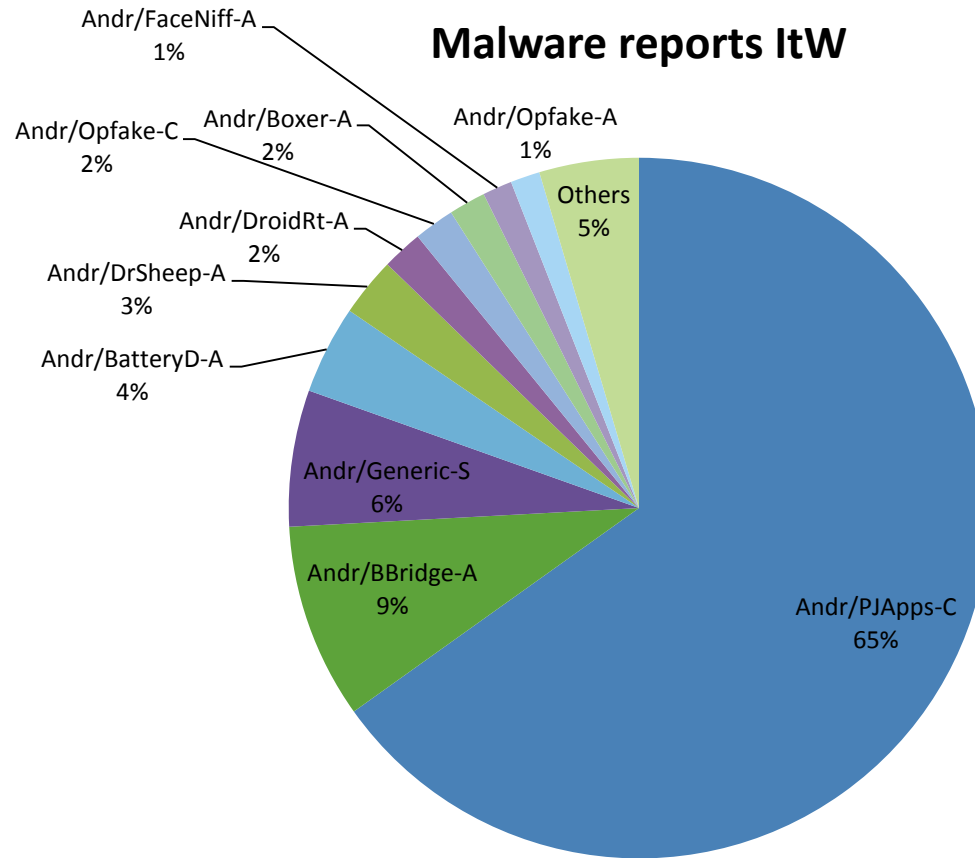


Android Malware

Discovered samples

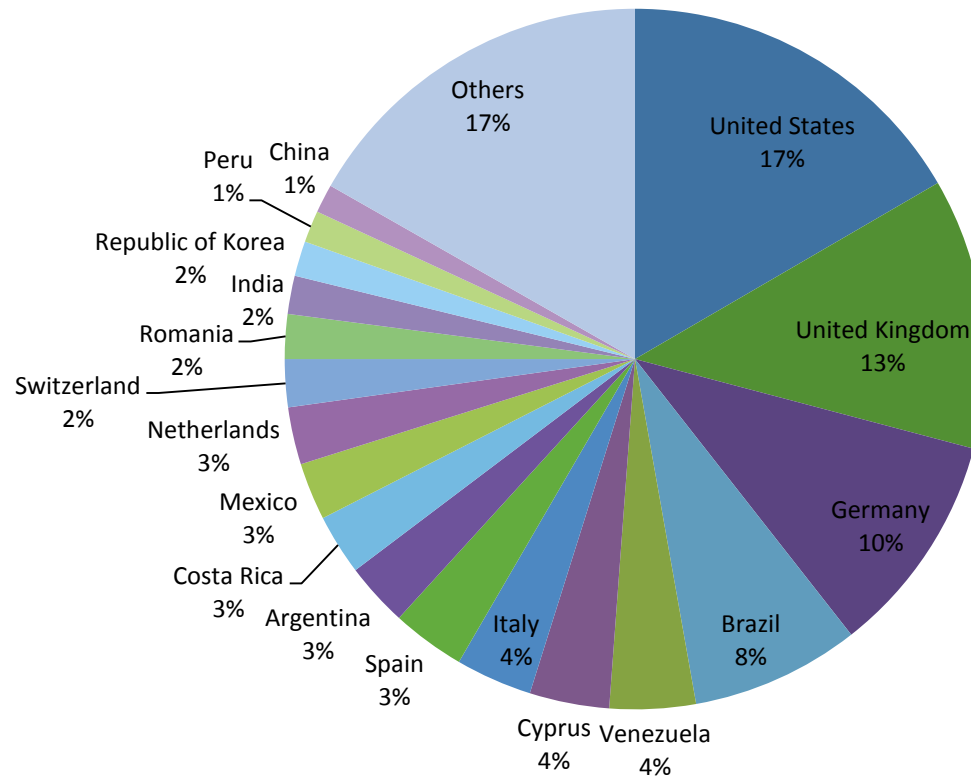


Android malware ItW

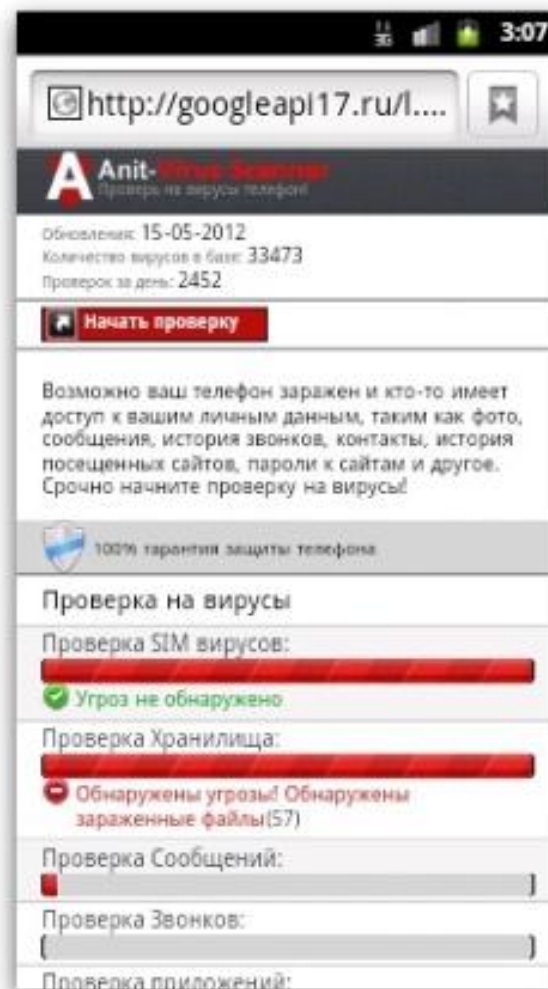
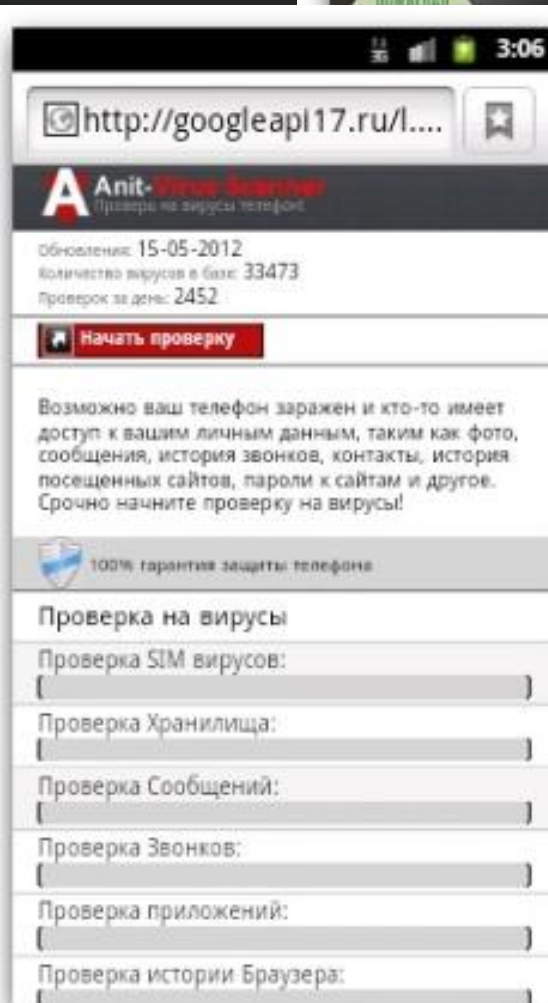
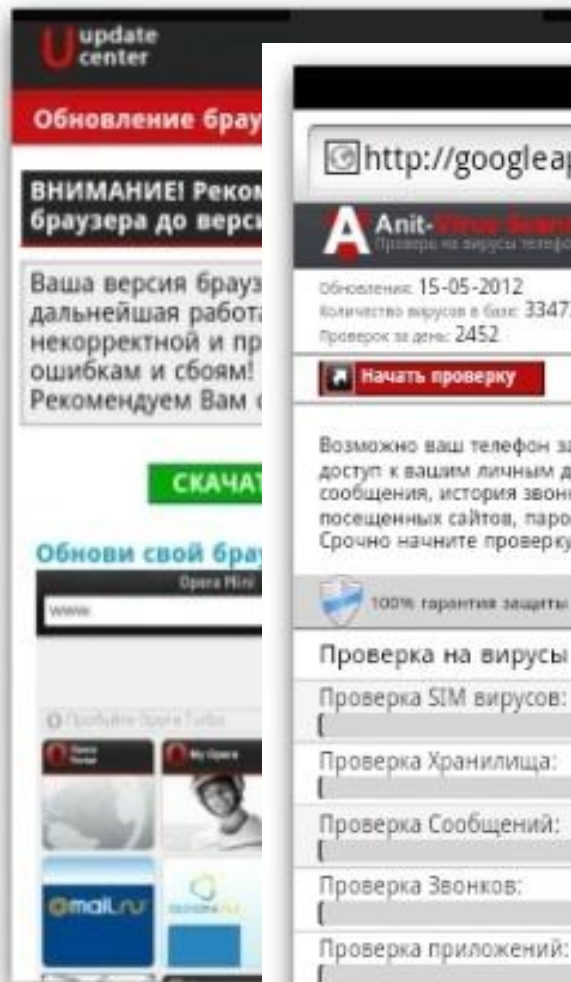


Android malware ItW

Android malware reports per country



Andr/Boxer family



Android

ельное приложение для
между пользователями со
ую вы можете делать
к ним фильтры, и
не, так и в социальные
более 30 млн

е количество
ку, будь то спорт, мода,
ушки и парни, достаточно
вив перед этим символ #.
графии, ставить лайки и

и погружайтесь в

м для

Andr/Boxer family

Witness



Andr/Boxer family

Witness



Android content detection



- APK = JAR = ZIP
- Signing mandatory
 - Self-certified certificates norm
- Classes.dex (Dalvik)
- AndroidManifest.xml
- Native ELF files
 - .so (shared objects)
 - command line



Classes.dex

Hex Workshop - [classes.dex]

File Edit Disk Options Tools Window Help

16 10 B S L Q F D

~ << >> << >> ^ | & % / * - + < > A↑ a↓ aA

| Offset | Hex | Assembly |
|----------|---|------------------|
| 00000000 | 6465 780A 3033 3500 3633 0D50 2B7A F94E | dex.035.63.P+z.N |
| 00000010 | B191 5D26 4075 5C2A 7CB9 0AF2 B854 CC40 | ..j&@u* ...T.@ |
| 00000020 | 5037 0100 7000 0000 7856 3412 0000 0000 | P7..p...xV4.... |
| 00000030 | 0000 0000 8036 0100 AB04 0000 7000 0000 |6.....p... |
| 00000040 | B600 0000 1C13 0000 D500 0000 F415 0000 | |
| 00000050 | D200 0000 F01F 0000 F001 0000 8026 0000 |&.. |
| 00000060 | 2700 0000 0036 0000 70FC 0000 E03A 0000 | '....6..p..... |
| 00000070 | B5D9 0000 E403 0100 BBD5 0000 06FA 0000 | |
| 00000080 | 71D0 0000 A6FA 0000 9CFA 0000 93FA 0000 | q..... |
| 00000090 | 75D0 0000 C1FB 0000 A0FB 0000 200B 0100 | u..... |
| 000000A0 | 04E9 0000 FDE8 0000 AEED 0000 A7ED 0000 |x... |
| 000000B0 | 4CFE 0000 B5EF 0000 99EF 0000 78EF 0000 | L..... |
| 000000C0 | 95D3 0000 43F4 0000 4DE9 0000 80D3 0000 |C...M..... |
| 000000D0 | 87F3 0000 27F4 0000 37F4 0000 1FF4 0000 |'...7..... |
| 000000E0 | 4A0A 0100 6BE9 0000 94D0 0000 20CD 0000 | J...k..... |
| 000000F0 | A5CD 0000 FBCD 0000 6ECF 0000 84D3 0000 |n..... |
| 00000100 | 22DB 0000 36D4 0000 A5DC 0000 83D5 0000 | "...6..... |
| 00000110 | BED5 0000 5FD6 0000 BBD6 0000 2DD7 0000 |-..... |
| 00000120 | 6ED7 0000 DAD7 0000 B8DC 0000 59D8 0000 | n.....Y... |
| 00000130 | F3DC 0000 6CD9 0000 51E8 0000 6204 0100 |1...Q...b... |
| 00000140 | F9FD 0000 5EF5 0000 BDE7 0000 47F5 0000 |^.....G... |
| 00000150 | 5CF6 0000 7DE3 0000 6EE3 0000 700E 0100 | \...}...n...p... |

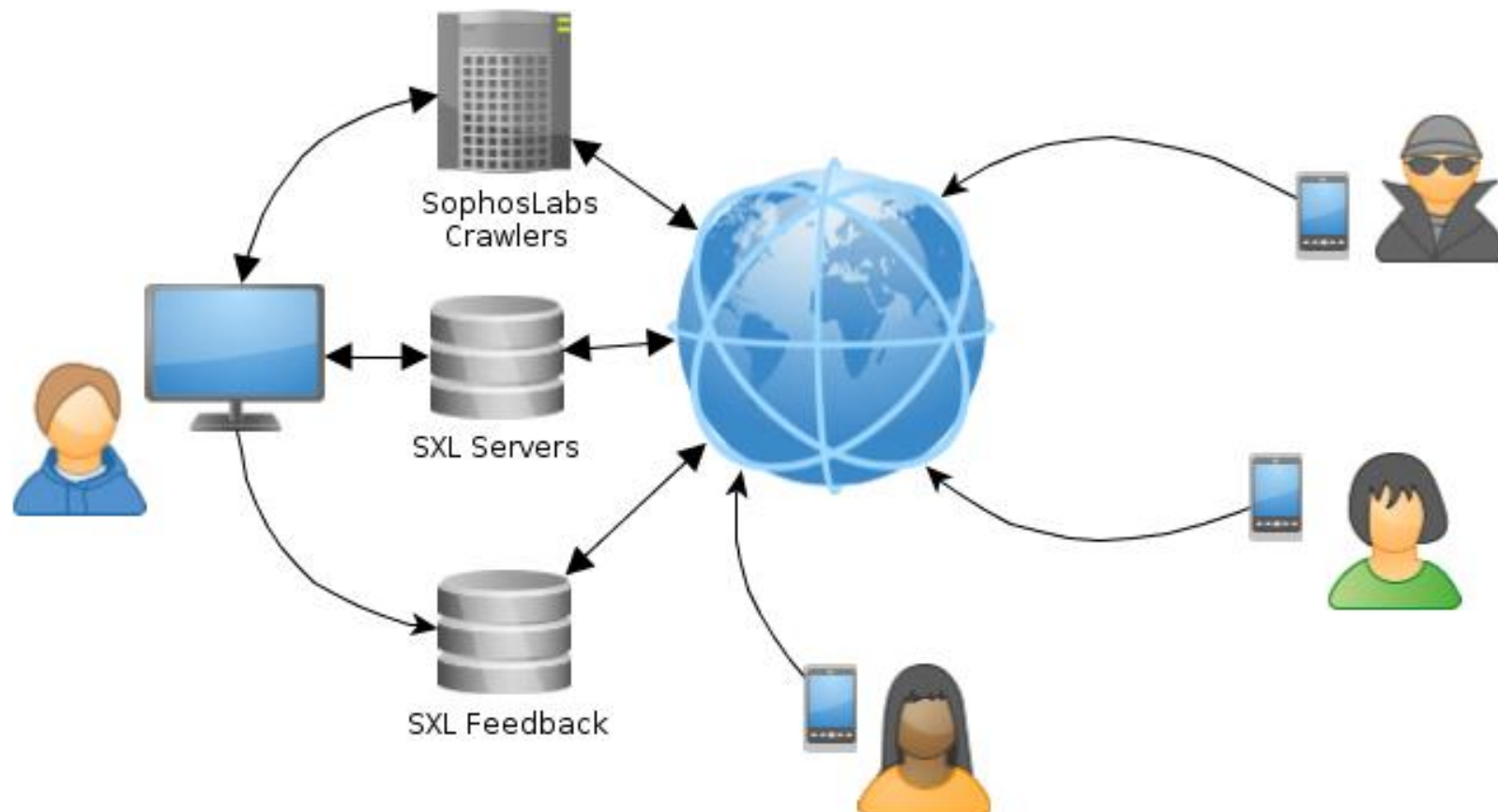
classes.dex

offset: 0 [0x00000000]

Find Results

| Address | Length |
|----------------------|-----------|
| 8BIT Signed Byte | 100 |
| 8BIT Unsigned Byte | 100 |
| 16BIT Signed Short | 25956 |
| 16BIT Unsigned Short | 25956 |
| 32BIT Signed Long | 175662436 |
| 32BIT Unsigned Long | 175662436 |

Mobile Security - ecosystem



Finding rules



- Cloud lookups
 - Package name
 - Permissions bitmap
 - Certificate information
- Test set 7k APK files



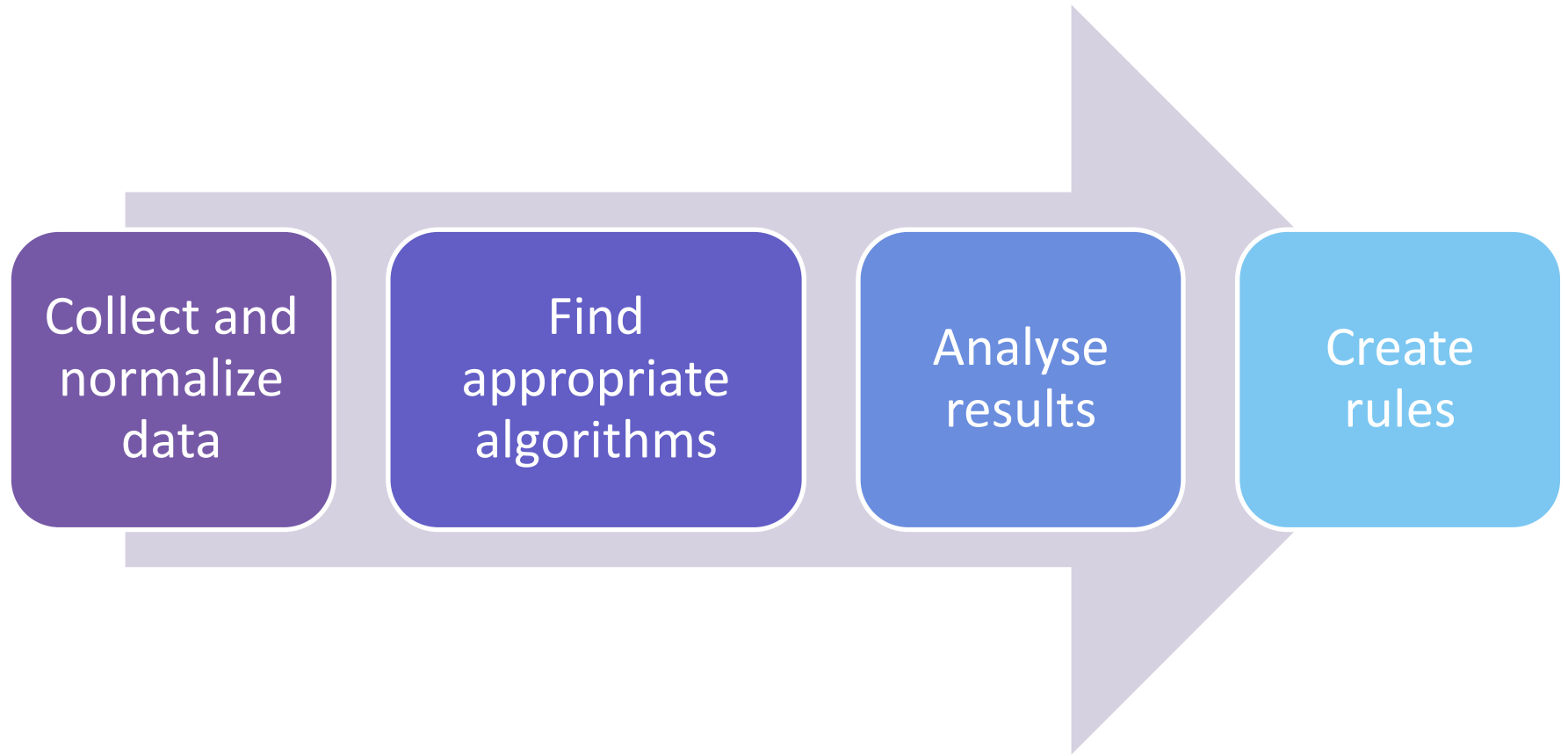
Mining for attributes



- Data mining
 - Classification
 - Clustering
 - Attribute evaluation (125 attributes)
 - Find attribute combinations for suspicious APK detections
 - WEKA toolkit



Data mining process



Data extraction



- Tools
 - Apktool (decode Android manifest)
 - Aapt (permissions)
 - Keytool (certificate information)
 - Dexdump (class names)
 - Perl (for creating ARFF or C4.5 file format)



Classification and clustering



- Classification
 - Decision trees
 - Multilayer perceptron (neural network)
 - PART
 - k-NN
 - Voting
- Clustering
 - k-Means (finding k is a bit tricky)
 - EM



Decision rule example



android.permission.SEND_SMS = true AND
android.permission.AUTHENTICATE_ACCOUNTS = false AND
android.permission.USE_CREDENTIALS = false AND
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS = false AND
android.permission.CHANGE_WIFI_STATE = false AND
android.permission.BLUETOOTH_ADMIN = false AND
android.permission.RECORD_AUDIO = false AND
android.permission.DEVICE_POWER = false AND
android.permission.CHANGE_NETWORK_STATE = false AND
android.permission.CHANGE_CONFIGURATION = true: malware (974.0)



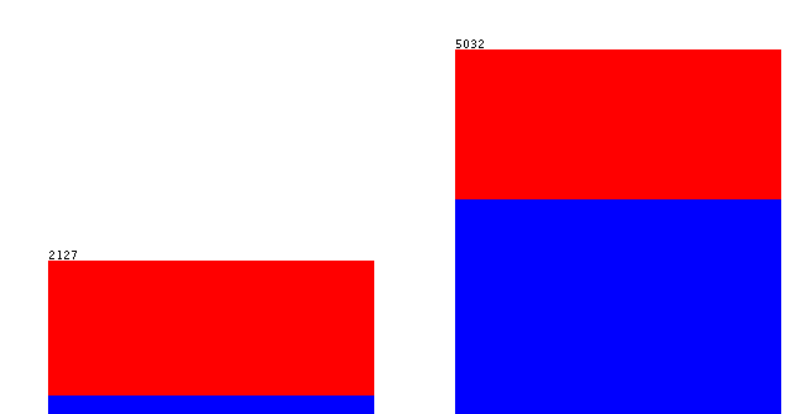
Attributes



- Attribute evaluation
 - Single
 - Combination



Receive_boot_completed

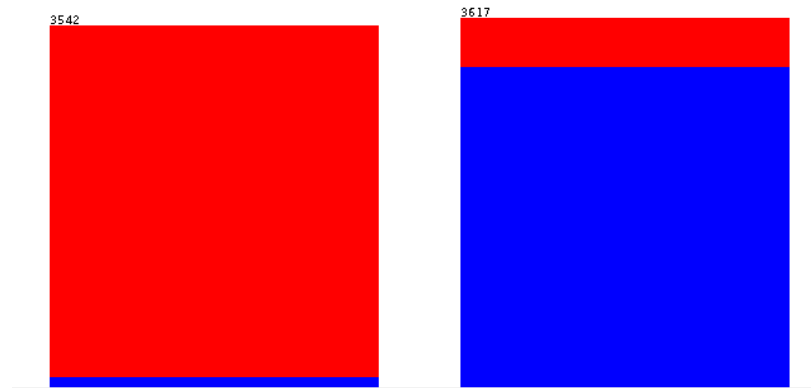


True

False



Send_sms

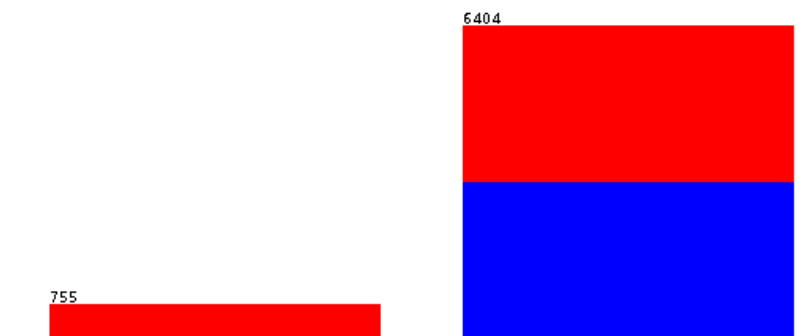


True

False



Install_packages

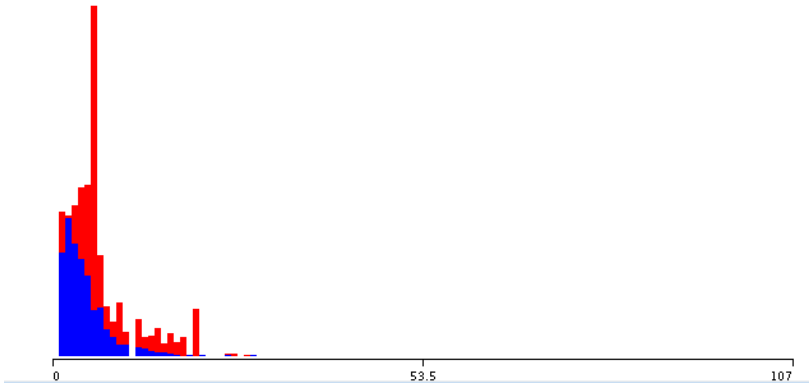


True

False



Number of permissions



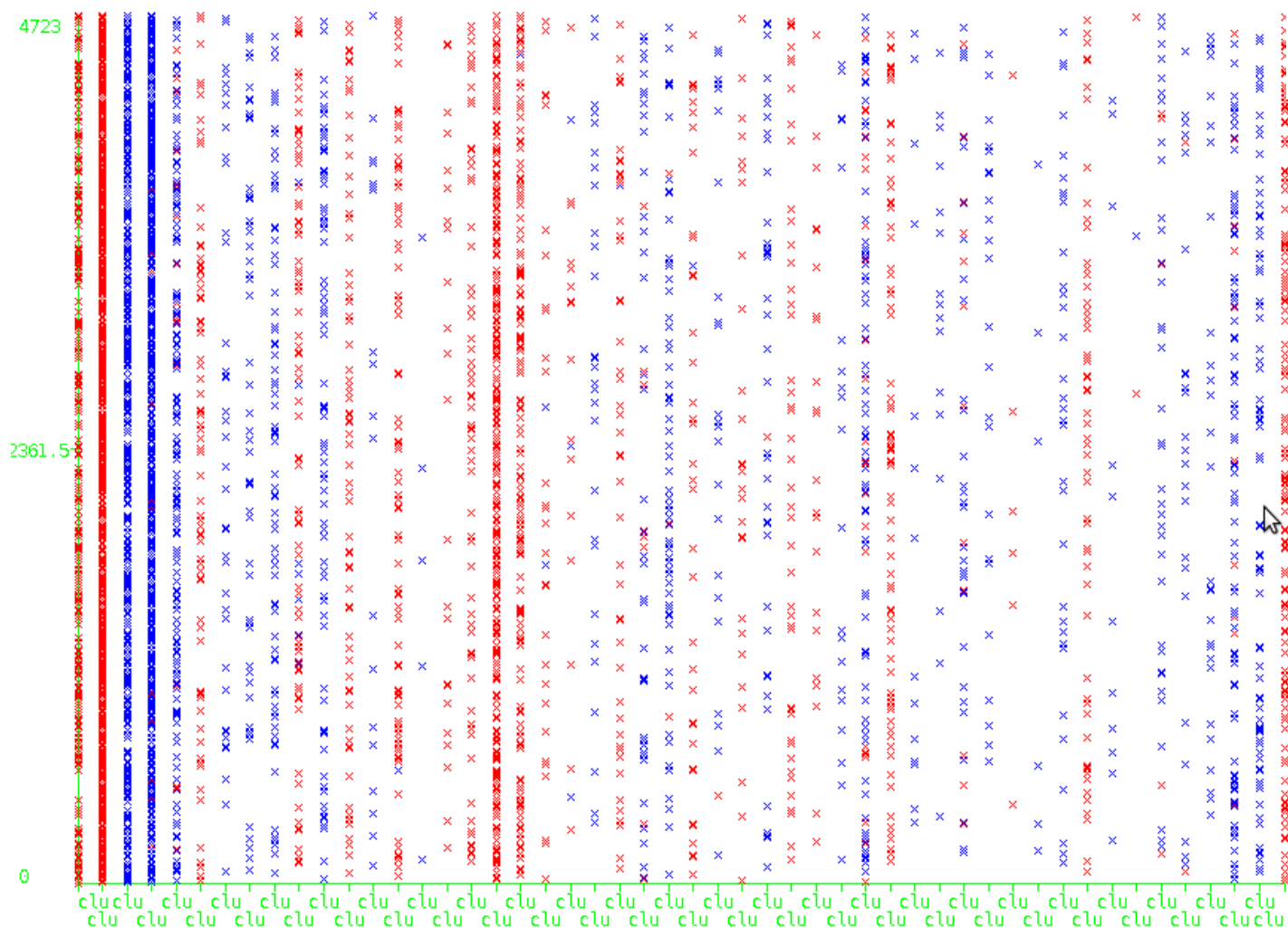
Top attributes - IG



0.61300345 android.permission.SEND_SMS
0.26650618 permission number
0.25418388 android.permission.RECEIVE_SMS
0.20317289 android.permission.CHANGE_CONFIGURATION
0.14376634 android.permission.RECEIVE_BOOT_COMPLETED
0.13039788 android.permission.READ_PHONE_STATE
0.11595942 android.permission.READ_SMS
0.08563974 android.permission.INSTALL_PACKAGES
0.0616352 android.permission.RECEIVE_WAP_PUSH
0.05807259 android.permission.WRITE_SMS
0.05672391 android.permission.ACCESS_NETWORK_STATE
0.04802936 com.android.browser.permission.READ_HISTORY_BOOKMARKS



Cluster assignments



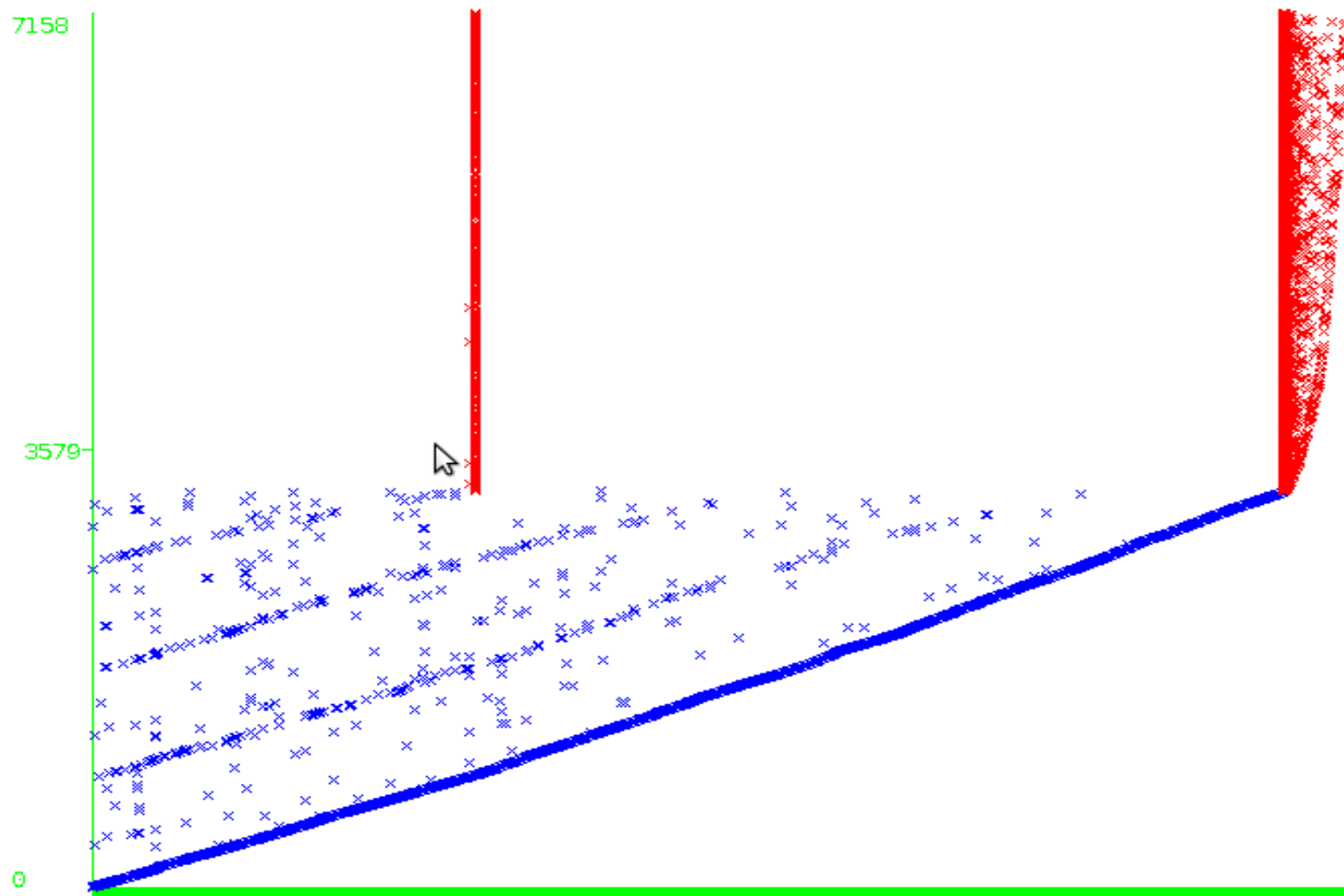
Andr/Boxer-A cluster



```
Cluster : cluster60
certificate : c67f8fc63e25c1f2d3d3623210d126bc96afee69
package : ru-2emskdev-2eandrinst
android.permission.CHANGE_CONFIGURATION : true
android.permission.INTERNET : true
android.permission.READ_PHONE_STATE : true
android.permission.RECEIVE_BOOT_COMPLETED : true
android.permission.RECEIVE_SMS : true
android.permission.SEND_SMS : true
permnum : 6.0
class : malware
```



APK certificate clusters



Top certificates

| CertsSha1 | Count | Detected | Possible Certificate names |
|--|-------|----------|---|
| 38918a453d07199354f8b19af05ec6562ced5788 | 6036 | 0 | ["com.android","com.google"] |
| 24bb24c05e47e0aefa68a58a766179d9b613a600 | 4354 | 0 | ["com.google"] |
| 0eb79878d3551cbe6ecf0e711e688951b44d7337 | 4312 | 0 | ["android.tts","app.batterymonitor","app.batterymonitor2","com.android","com.broadcom"] |
| 61ed377e85d386a8dfee6b864bd85b0faa5af81 | 3754 | 1995 | ["au.com","biz.mtoy","chaire1.mm","cmp.netsentry","cn.jingling"] |
| 9ca5170f381919dfe0446fcdab18b19a143b3163 | 3574 | 0 | ["android.tts","com.android","com.broadcom","com.cisco","com.google"] |
| 5cb0136d4f218b1d7a489024972f8aa4720f5e67 | 1966 | 1966 | ["com.depositmobi","com.soft","com.software","com.some","net.install"] |
| c67f8fc63e25c1f2d3d3623210d126bc96afee69 | 1487 | 1487 | ["com.android","com.bratolubzet","com.maestrodeoid","com.manufacturatinkov","com.satismangrooup"] |
| c3169c61b106efa253f56dfe542392f7bd80ee2d | 1476 | 0 | ["com.android","com.arcsoft","com.samsung","com.sec","com.smls"] |
| 66da9177253113474f6b3043b89e0667902cf115 | 1451 | 0 | ["com.rovio"] |
| b599462d81daaeb2081e6129e75a54ef0aedbf03 | 1439 | 0 | ["com.android","com.hu1","com.samsung","com.sec"] |
| 9741a0f330dc2e8619b76a2597f308c37dbe30a2 | 1350 | 0 | ["com.android","com.arcsoft","com.lifevibes","com.samsung","com.sec"] |
| 184ab55237bb822a4175b62155ff209b822b785e | 1193 | 1193 | ["ahv7teix.ohshooc8","aichoor9.cai6ood0","aig0.ohdu","android.app","cai7real.mah5lure"] |
| 8a3c4b262d721acd49a4bf97d5213199c86fa2b9 | 1163 | 0 | ["com.facebook"] |
| 330df1d4f77968c397ff53d444089bb46dc330f1 | 1111 | 0 | ["com.android","com.sonyericsson","com.svox"] |
| 69726e79fdb776e41111cb4b99e3b6a9d1abec3c | 1033 | 0 | ["com.android","com.htc","com.rosedata","com.sdgtl","com.svox"] |
| d5ca82cbddd3985279b074ea53ba9a30688935be | 972 | 0 | ["com.adobe"] |
| 59a3683b5b6101178204a75b90fea6098229c844 | 910 | 0 | ["com.android","com.htc"] |
| ba141746d704b96ed4dbc24d02d44bb2a3908512 | 906 | 0 | ["com.android","com.hu1","com.samsung","com.sec","om.samsung"] |
| 5f206863fd884ee45873b7688828880d221301 | 893 | 0 | ["com.glu"] |
| 80d0156e14efa9b2be949acc1791720cc58cb6e3 | 870 | 0 | ["android.tts","com.android","com.aricent","com.google","com.sonyericsson"] |



Conclulsion



- Android malware numbers exponentially increasing
- Increased complexity (obfuscation, polymorphism)
- Single permissions and combinations are (not) good alone
- Certificate reputation significant
- More attributes to be added in future research

