RSAConference2016
Abu Dhabi | 15–16 November | Emirates Palace

SESSION ID: CCT-W04

Android Malware Pattern Recognition for Fraud and Attribution

Nikos Tsouroulas
Head of Cybersecurity
Telefonica 11Paths
nikolaos.tsouroulas@telefonica.com

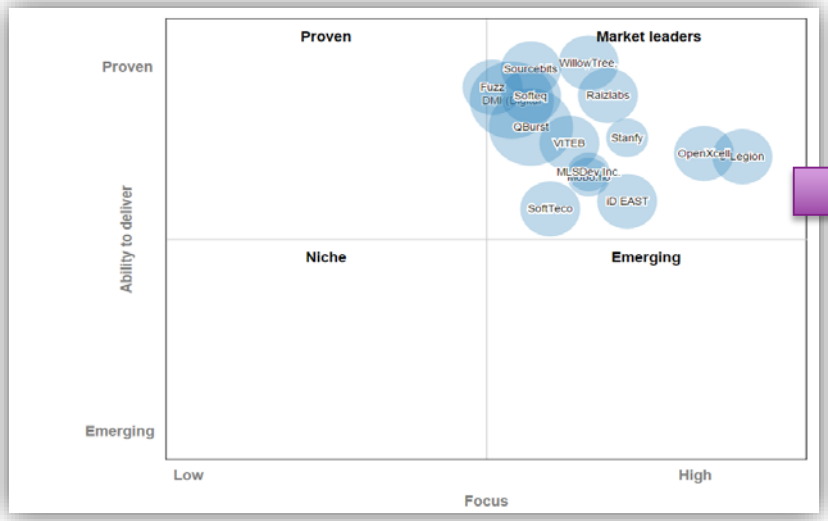
Ahmed Alketbi
Senior Manager Security Solutions Marketing
Etisalat

Index

- Introducing Mobile App Singularities
- Case Study 1: Who is behind FOBUS aka “PODEC”?
- Case Study 2: SHUABANG. How we discovered one of the most ingenious ways of fooling Google Play.
- Conclusions

Some thoughts…

"83 % of the top 400 Mobile android Apps come from few unique developers"



Android App Developers, Leaders Matrix

The same applies for malware

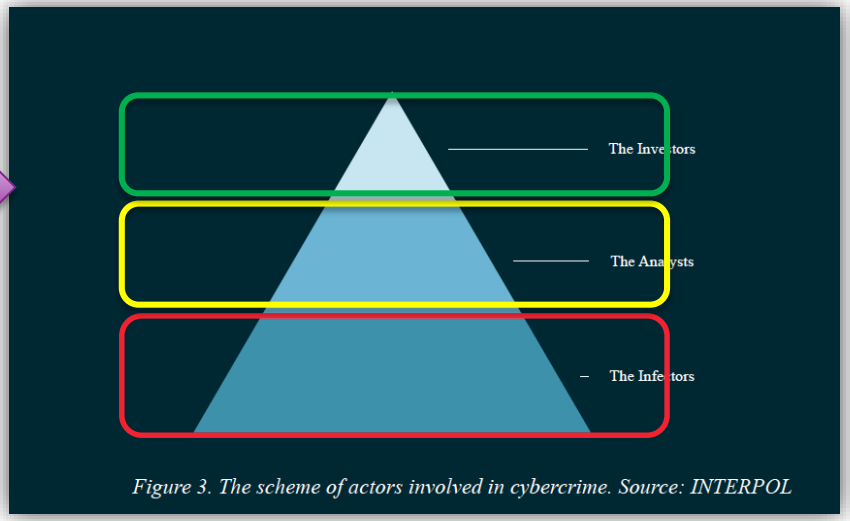


Figure 3. The scheme of actors involved in cybercrime. Source: INTERPOL

etisalat
Eleven Paths

Some thoughts…

The entire ecosystem is potentially insecure even by using "trusted" markets

Malware slips through, it is impossible to review in all the de

"TRUST" is not a security control

Cyber criminals find ways to trick the controls (i.e. Gremlin aps)

etisalat Eleven Paths

Android Malware is coming…

New Research Finds Mobile Malware Infections Overhyped in US

Research Conducted on 50% of US Mobile Traffic Finds You are 1.3 Times More Likely To Get Struck By Lightning Than Have Mobile Malware Communicating on Your Device

Investigación sobre el 50% de los móviles estadounidenses concluye que tienes 1.3 más posibilidades de ser alcanzado por un rayo que de tener malware en tu dispositivo de comunicación

TAG Malware , Operating System , Richard Stallman , iOS , Android , Windows

Malware, All Malware: How Free Software Advocate Richard Stallman Sees Windows, Android And iOS

By **Sumit Passary**, Tech Times | May 27, 7:39 AM

Richard Stallman, a free software activist, says that iOS, Android and Windows are malware. Stallman believes that

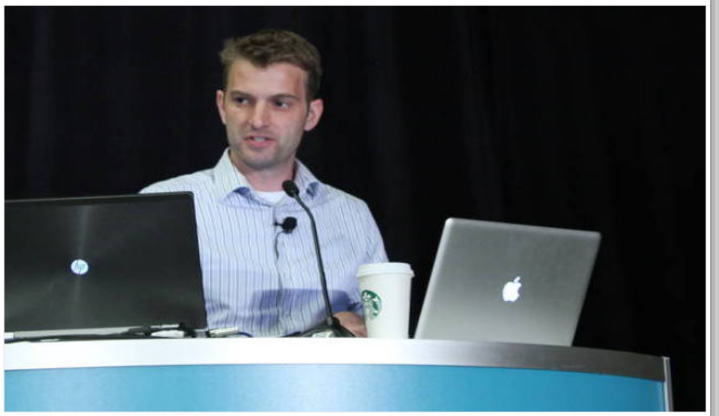
Richard Stallman, a computer programmer and free software activist, brands famous operating systems such as iOS, Windows and Android as malware.

In an opinion piece in The Guardian, Stallman suggests that nearly all operating systems, whether desktop operating system or mobile operating system, can be considered malware. Stallman argues that any software that is not distributed free of cost is malware.

Stallman, who founded the Free Software Foundation, also made it clear in the opinion piece that he is not talking about any type of

Google guru: Android doesn't have malware, it has Potentially Harmful Applications™ instead

And who installs five AV apps on their mobes?



Language ... Adrian Ludwig at RSA 2015

21 Apr 2015 at 23:14, Darren Pauli 311 47 29

RSA 2015 Malware doesn't exist on Android, Google says, but Potentially Harmful Applications™ do.

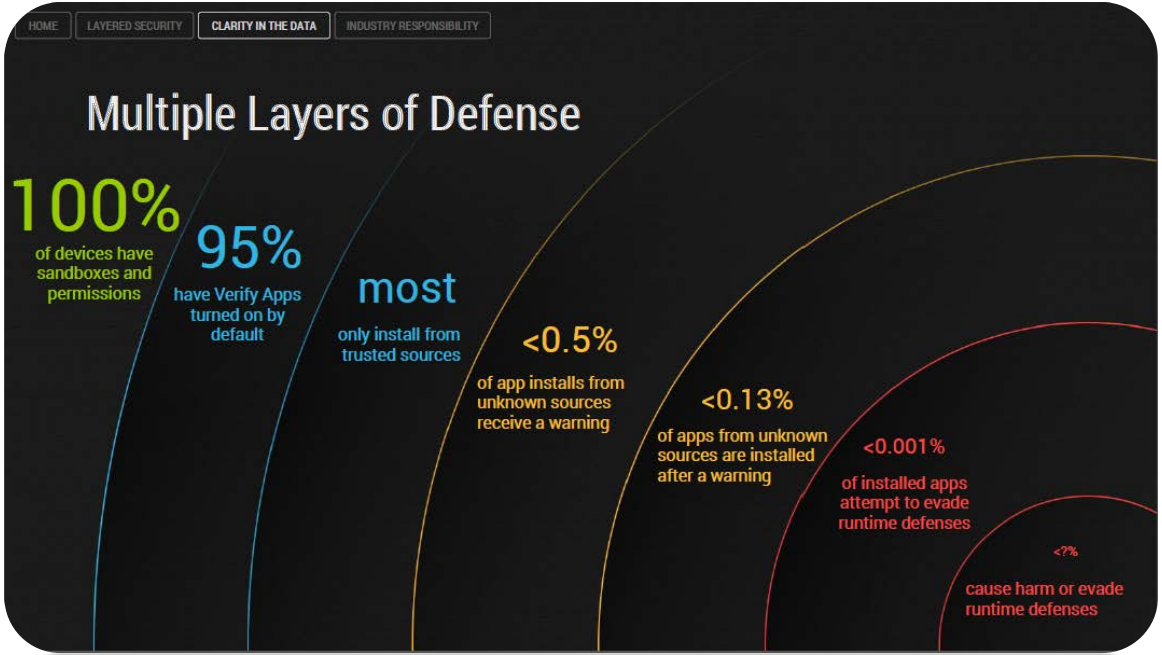
etisalat Eleven Paths

Is Google Play (un)safe?

Android and Google Play, they do indeed have great security measures and are getting better.

But what if… malware (ok, PHA) do not need to break them?

- Adware
- RATs
- Trojans
- mRansomware
- …

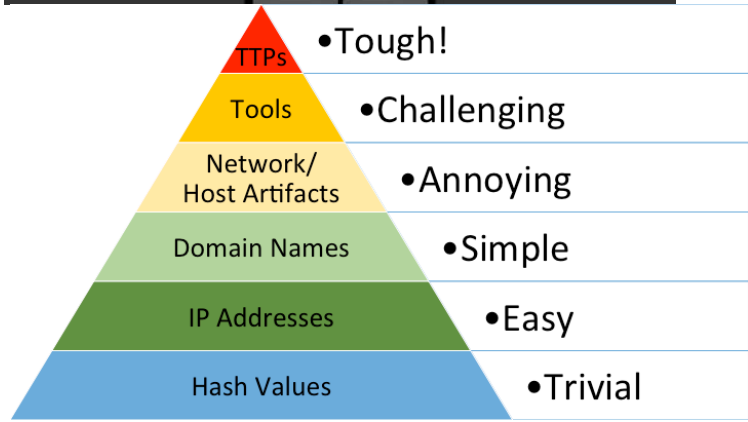


…all with a significant install rate. At least enough to keep production… why would attackers invest time in creating them otherwise?

etisalat
Eleven Paths

Big Data, intelligence & malware

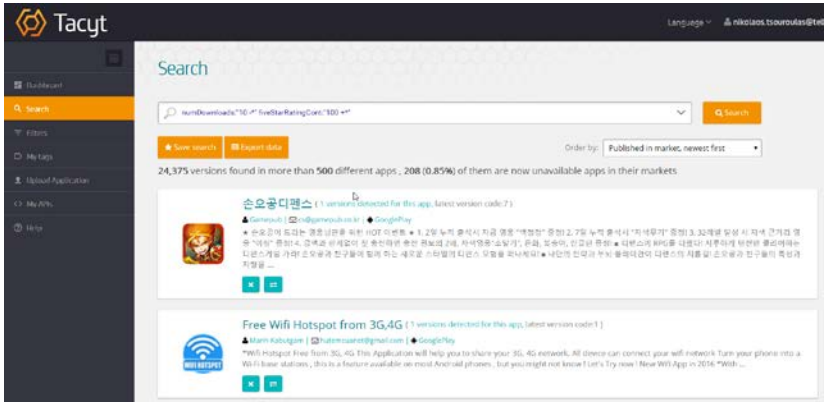
- With almost **1.5M apps** in each Google Play and App Store, with 2-3k new apps every day, traditional approaches are condemned to always be one step behind the attackers.
- Modern Cybersecurity is about leveraging Big Data Analytics & Intelligence to become **proactive**.
- Can we apply similar techniques in order **to change the pace in mobile app security?**



etisalat
Eleven Paths

App Singularities for mobile malware detection and analysis

- Creating malware **professionally is very demanding.**
- Attackers repeat patterns and make mistakes like any other SW developers, thus introducing **Singularities**.
- Having tools to easily crawl for such Singularities at the **moment of submission and at scale** greatly enhances **detection and attribution** capabilities.



Apps with more votes than downloads

etisalat
Eleven Paths

Attribution: Who is behind FOBUS aka "PODEC"?

CASE Study 1

Knowing the enemy

Fobus (aka “podec”) is a very hard to uninstall malware. It spies on the phone and is able to make calls, steal data, etc. And it is incredibly hard to remove.

We started the analysis with a sample, shown in blog of Avast.

Fobus, the sneaky little thief that could

Go to comments Leave a comment

One small Android application shows lots of determination and persistence. Too bad it’s evil.

Mobile malware, Fobus, acts like this famous little engine. “I think I can, I think I can!”

Top 20 malicious mobile programs

Please note that, starting from this quarterly report, we are publishing the ranking of *malicious* programs, which does not include potentially dangerous or unwanted programs such as RiskTool or adware.

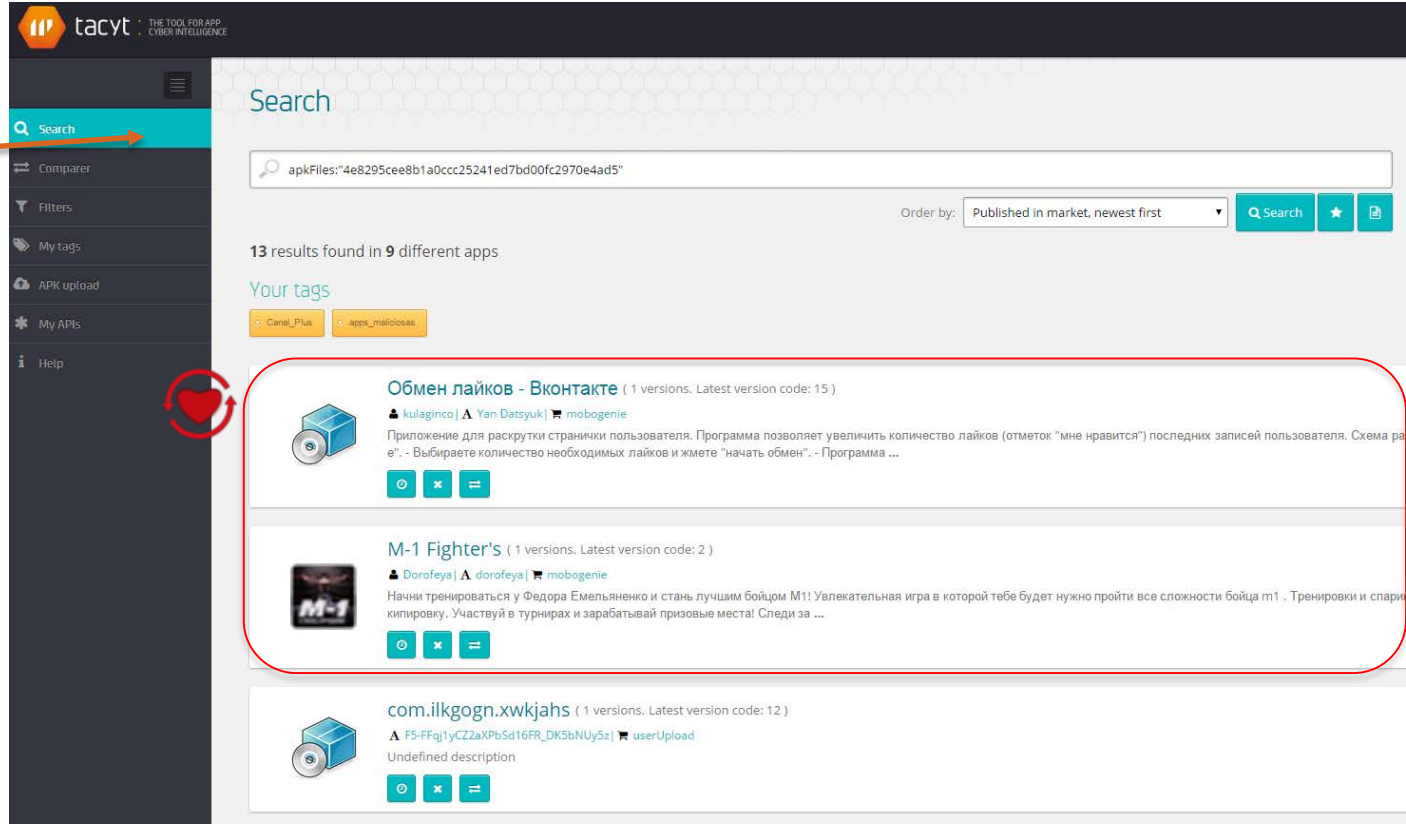
	Name	% of attacks *
1	DangerousObject.Multi.Generic	17.5%
2	Trojan-SMS.AndroidOS.Podec.a	9.7%
3	Trojan-SMS.AndroidOS.Opfake.a	8.0%
4	Backdoor.AndroidOS.Obad.f	7.3%
5	Trojan-Downloader.AndroidOS.Leech.a	7.2%
6	Exploit.AndroidOS.Lotoor.be	5.7%
7	Trojan-Spy.AndroidOS.Agent.el	5.5%
8	Trojan.AndroidOS.Ztorg.a	3.1%
9	Trojan.AndroidOS.Rootnik.a	3.0%
10	Trojan-Dropper.AndroidOS.Gorpo.a	2.9%
11	Trojan.AndroidOS.Fadeb.a	2.7%
12	Trojan-SMS.AndroidOS.Gudex.e	2.5%
13	Trojan-SMS.AndroidOS.Stealer.a	2.5%
14	Exploit.AndroidOS.Lotoor.a	2.1%
15	Trojan-SMS.AndroidOS.Opfake.bo	1.6%
16	Trojan.AndroidOS.Ztorg.b	1.6%
17	Trojan.AndroidOS.Mobtes.b	1.6%
18	Trojan-SMS.AndroidOS.FakeInst.fz	1.6%
19	Trojan.AndroidOS.Ztorg.pac	1.5%
20	Trojan-SMS.AndroidOS.FakeInst.hb	1.4%

* Percentage of users attacked by the malware in question, relative to all users attacked

etisalat Eleven Paths

Narrowing the scope - reusing files

Files inside the original APK are reused among malicious apps: x.app & notification.png seems to be very uncommon.



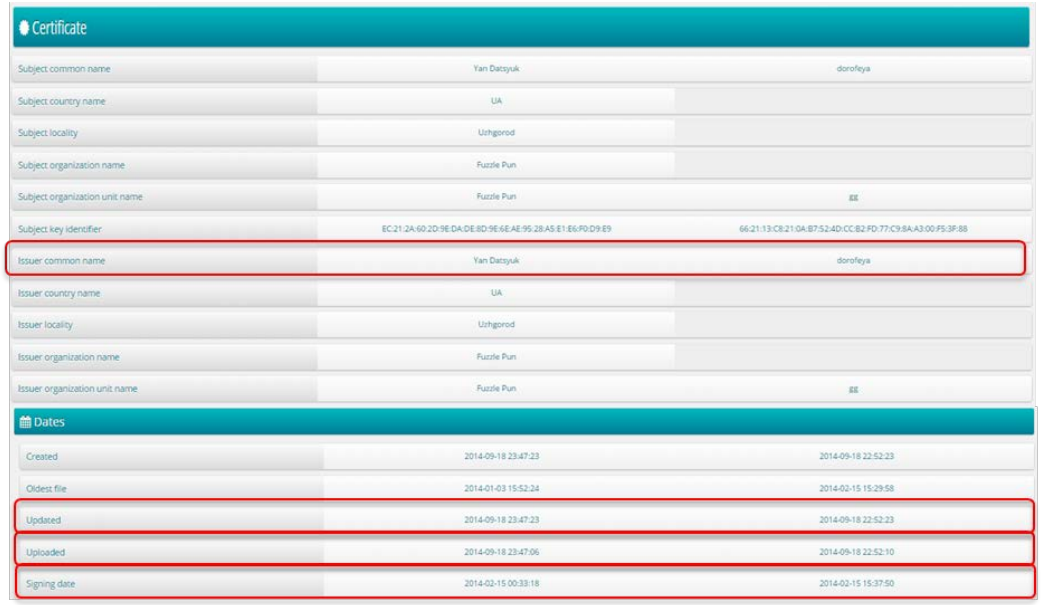
Narrowing the scope - Analyzing permissions

Comparing both apps, they have a lot of permissions (basically full control of the device) and exactly the same.

Permissions		
com.android.launcher.permission.INSTALL_SHORTCUT	✓	✓
android.permission.SEND_SMS	✓	✓
android.permission.PROCESS_OUTGOING_CALLS	✓	✓
android.permission.WRITE_EXTERNAL_STORAGE	✓	✓
android.permission.WRITE_CALL_LOG	✓	✓
android.permission.WRITE_SMS	✓	✓
android.permission.ACCESS_WIFI_STATE	✓	✓
android.permission.ACCESS_COARSE_LOCATION	✓	✓
android.permission.RECEIVE_SMS	✓	✓
android.permission.CALL_PHONE	✓	✓
android.permission.READ_CONTACTS	✓	✓
android.permission.WRITE_CONTACTS	✓	✓
android.permission.READ_PHONE_STATE	✓	✓
android.permission.READ_SMS	✓	✓
android.permission.RECEIVE_BOOT_COMPLETED	✓	✓
android.permission.INTERNET	✓	✓
android.permission.WRITE_SETTINGS	✓	✓
android.permission.ACCESS_FINE_LOCATION	✓	✓

etisalat
Eleven Paths

Narrowing the scope - Dates & digital certificate



Certificate

Subject common name	Yan Datsyuk	dorofeya
Subject country name	UA	
Subject locality	Uzhgorod	
Subject organization name	Fuzzle Pun	
Subject organization unit name	Fuzzle Pun	
Subject key identifier	EC:21:2A:60:2D:9E:DA:DE:8D:9E:6E:AE:95:28:A5:E1:E6:F0:D9:E9	66:21:13:C8:21:0A:B7:52:4D:CC:B2:FD:77:C9:8A:A3:00:F5:3F:88
Issuer common name	Yan Datsyuk	dorofeya
Issuer country name	UA	
Issuer locality	Uzhgorod	
Issuer organization name	Fuzzle Pun	
Issuer organization unit name	Fuzzle Pun	

Dates

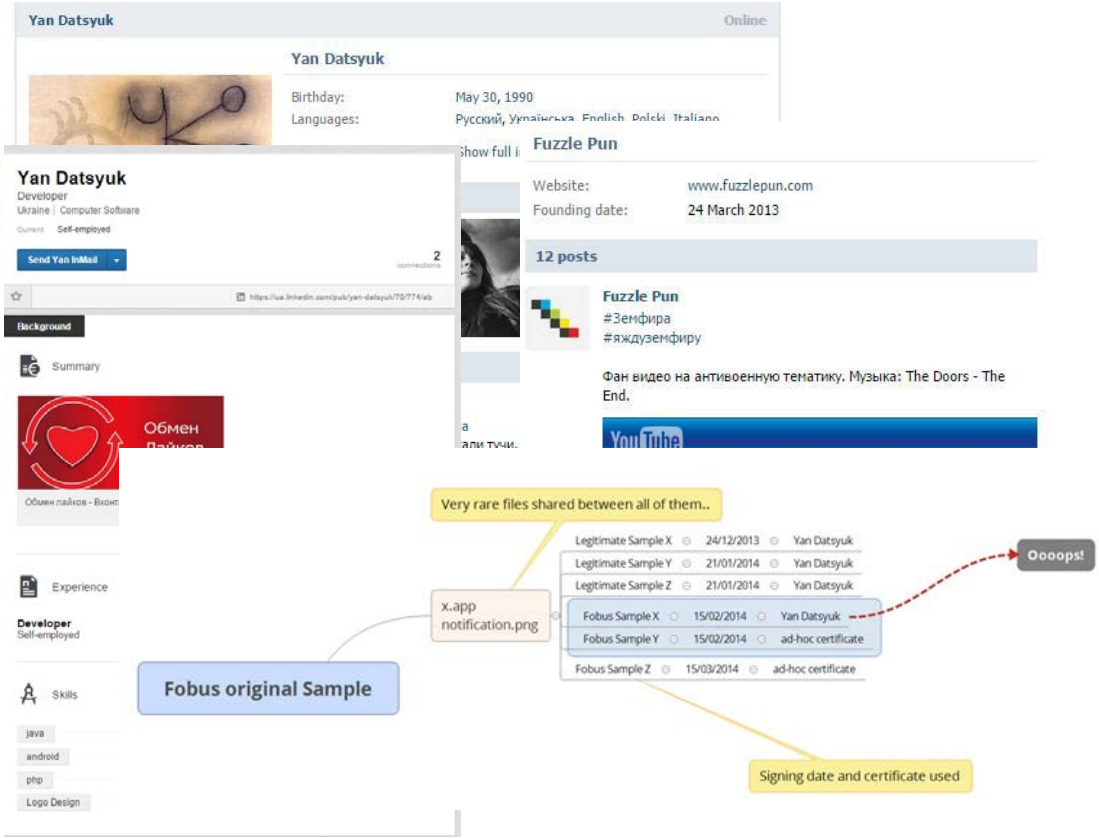
Created	2014-09-18 23:47:23	2014-09-18 22:52:23
Oldest file	2014-01-03 15:52:24	2014-02-15 15:29:58
Updated	2014-09-18 23:47:23	2014-09-18 22:52:23
Uploaded	2014-09-18 23:47:06	2014-09-18 22:52:10
Signing date	2014-02-15 00:33:18	2014-02-15 15:37:50

- Same update, uploaded and signing dates ➔ **Singularity**
- Different developers and digital certificates
- We already have a name ‘Yan Datsuk’ and a company ‘Fuzzle Pun’
- Both apps are in Russian
- A deeper analysis confirms that both apps are Fobus.

etisalat
Eleven Paths

HUMINT – Profiling the bad guy

- Location
- Company profile (VK)
- Personal profile (VK, Facebook, Google+)
- Professional profile (LinkedIn)
- HackerOne profile
- Email
- Relationship between company & developer



etisalat
Eleven Paths

SHUABANG: How we discovered one of the most ingenious ways of fooling Google Play

CASE 2

Black ASO {App Store Optimization}

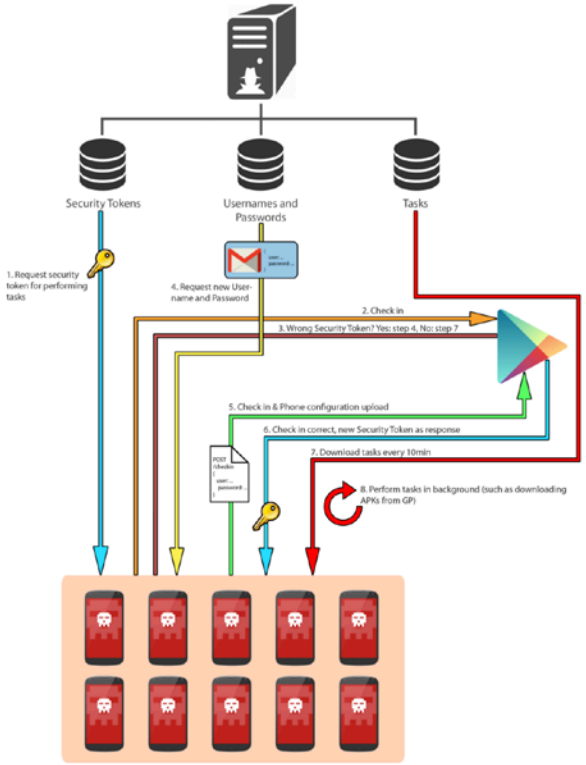
- Black App Store Optimization
  - Positioning apps in markets
    - Spam
    - Download rate
    - Reviews
- Goal
  - Build up an automated infrastructure
  - Infrastructure for sale to third parties
  - To extend the botnet

etisalat
Eleven Paths

What is Shuabang?

- Shuabang is a technique, quite common in China. It is the BlackHat App Store Optimization.
- There are companies that charge you to “rise up” your app in stores, voting them, or adding fake downloads.
- To get that in Google Play, they need registered users in Google Play, that means, basically, Gmail accounts (users and passwords) associated with a telephone (a real deviceID). How to get them?
  - You can buy them.
  - You can create them.
  - You can steal them.
  - Or you can **create your own botnet…**

Botnet scheme



1. The attacker recovers a Google Security Token and links it to a fake Google user account and a specific device.
2. From the malware app the Google check-in process is done using that token
3. If the token is valid, the attacker provides a user name and a password to the malware app
4. From the malware app on the device, credentials and device config are uploaded.
5. If the credentials are valid, Google Play returns a new Security token as a response.
6. With this new token, the malware app is able to execute several tasks and actions, ordered by the attacker in the background

etisalat
Eleven Paths

We found something that looked very suspicious…

- We were looking for **Wallpapers that connected to PHP sites (title:*wallpaper* links:*.php permissionName:*ACCOUNT* permissionName:*BOOT*)**. That simple. And we found this…

ACCOUNT

ID	用户名	密码	创建时间	设备表识	地区	操作
10661	stcloudbv29@gmail.com	*******	2014-11-06,23:32:10	7005fa5fca[redacted]	巴西	修改 删除
10662	amandacq92@gmail.com	*******	2014-10-29,18:26:43	bf81f80f7d[redacted]	巴西	修改 删除
10663	besscwb6@gmail.com	*******	2014-11-06,23:37:14	d3b9d21d7[redacted]	巴西	修改 删除
10664	isaacpd70@gmail.com	*******	2014-10-29,18:34:31	e83ed7c05[redacted]	巴西	修改 删除
10665	nilslvb@gmail.com	*******	2014-11-06,23:42:50	389fb6783[redacted]	巴西	修改

User Accounts

User	From Host
dujiadui	%
jiankongbao	60.195.252.106
jiankongbao	60.195.252.108
root	%
root	localhost.localdomain
root	127.0.0.1
root	::1

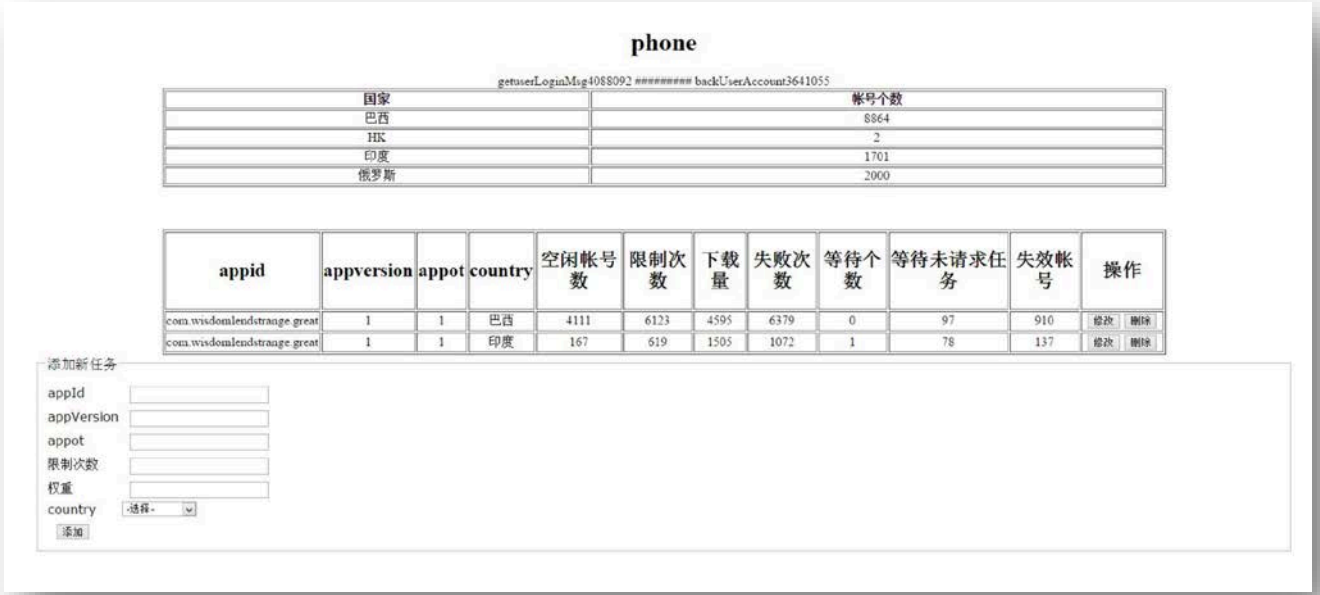
etisalat Eleven Paths

Stolen users

```
361. ----------------------------------------------------------
362. Program:          Firefox
363. Url/Host:         https://login.facebook.com
364. Login:            confusedmime@gmail.com
365. Password:         pleasefuckoff
366. Computer:         ZARDOZ
367. Date:             2011-10-16 12:51:54
368. Ip:                        71.35.156.85
369. ----------------------------------------------------------
370. Program:          Firefox
371. Url/Host:         https://www.google.com
372. Login:            confusedmime
373. Password:         pleasefuckoff
374. Computer:         ZARDOZ
375. Date:             2011-10-16 12:51:55
376. Ip:                        71.35.156.85
377. ----------------------------------------------------------
378. Program:          Firefox
379. Url/Host:         https://addons.mozilla.org
380. Login:            confusedmime@gmail.com
381. Password:         ion15
382. Computer:         ZARDOZ
383. Date:             2011-10-16 12:51:55
384. Ip:                        71.35.156.85
385. ----------
```

etisalat
Eleven Paths

Shuaban Botnet: Control Panel



phone

getuserLoginMsg4088092 ######## backUserAccount3641055

国家	帐号个数
巴西	8864
HK	2
印度	1701
俄罗斯	2000

appid	appversion	appot	country	空闲帐号数	限制次数	下载量	失败次数	等待个数	等待未请求任务	失效帐号	操作
com.wisdomlendstrange.great	1	1	巴西	4111	6123	4595	6379	0	97	910	修改 删除
com.wisdomlendstrange.great	1	1	印度	167	619	1505	1072	1	78	137	修改 删除

添加新任务

appId
appVersion
appot
限制次数
权重
country -选择-
添加

etisalat
Eleven Paths

And this is what it was…

SHA256:	34e9927358bcb56c3ce0ef09fd71bdd48cfc22b9491565dc77df0e8b7bc93c99
Nombre:	com.businessprisonice.eletricscreen.apk
Detecciones:	0 / 48
Fecha de análisis:	2014-10-30 11:00:35 UTC (hace 4 meses, 1 semana)

Análisis | Información adicional | Comentarios 0 | Votos

Antivirus	Resultado	Actualización
AVG	✔	20141030
Ad-Aware	✔	20141030
AegisLab	✔	20141030

Singularity, Let's find more apps like this

- These applications had several points in common that could be used as the developer's "fingerprint".
  - The apps were created with Java version 1.8.0_05 (Oracle Corporation).
  - The certificates, although different, were valid for 271 years.
  - **certificateSubjectCommonName** is normally formed by a combination of several words.
  - Images were also useful to find similar applications. For example, if a search was made for similar images, a different developer may be found: **yu jinhui**.
- And finally we found this in common:

http://apptools.myappblog.net/selfpush/selfpush/gameframe/www/test/getcontent.php (links:*myappblog*)
The number of different developers took a huge bump.

shengzls, feng wenjie, tong ronghai, shui hongli, yan dongba, tang xiaocan, wan lichun, jie libao, wen xiaojian, yuan junrong, wen xiaojian...

Finally it got baptized…

SHA256:	227bd4004a2bb5b9431645e5284c3f5c4d5f35fb863c359f00c94bb0f74f8900
Nombre:	227bd4004a2bb5b9431645e5284c3f5c4d5f35fb863c359f00c94bb0f74f8900
Detecciones:	3 / 56
Fecha de análisis:	2014-12-11 10:39:45 UTC (hace 2 meses, 3 semanas)

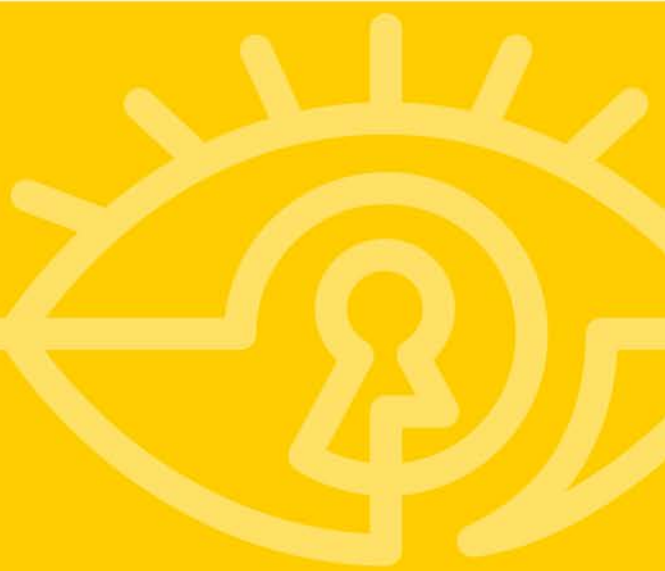
Análisis | Detalles | Información adicional | Comentarios 0 | Votos | Información de comportamiento

Antivirus	Resultado	Actualizaci
ESET-NOD32	a variant of Android/Glooken.A	20141211
Ikarus	Trojan.AndroidOS.ShuaBang	20141211
Kaspersky	not-a-virus:HEUR:RiskTool.AndroidOS.Bauts.a	20141211

Shuabang Botnet: Facts

- Stolen 12.567 Google accounts
- Expert understanding of internals (unpublished) of the device registration system with.
- 100 malicious apps available in Google Play
- Permissions apparently harmless
- Complex tasking system managed effectively
- Fraud-per-click managed in a smart way
- Resources usage without using Google original account in the infected device
- Building up a development framework

etisalat
Eleven Paths



Conclusions

How high where those groups in the food chain?

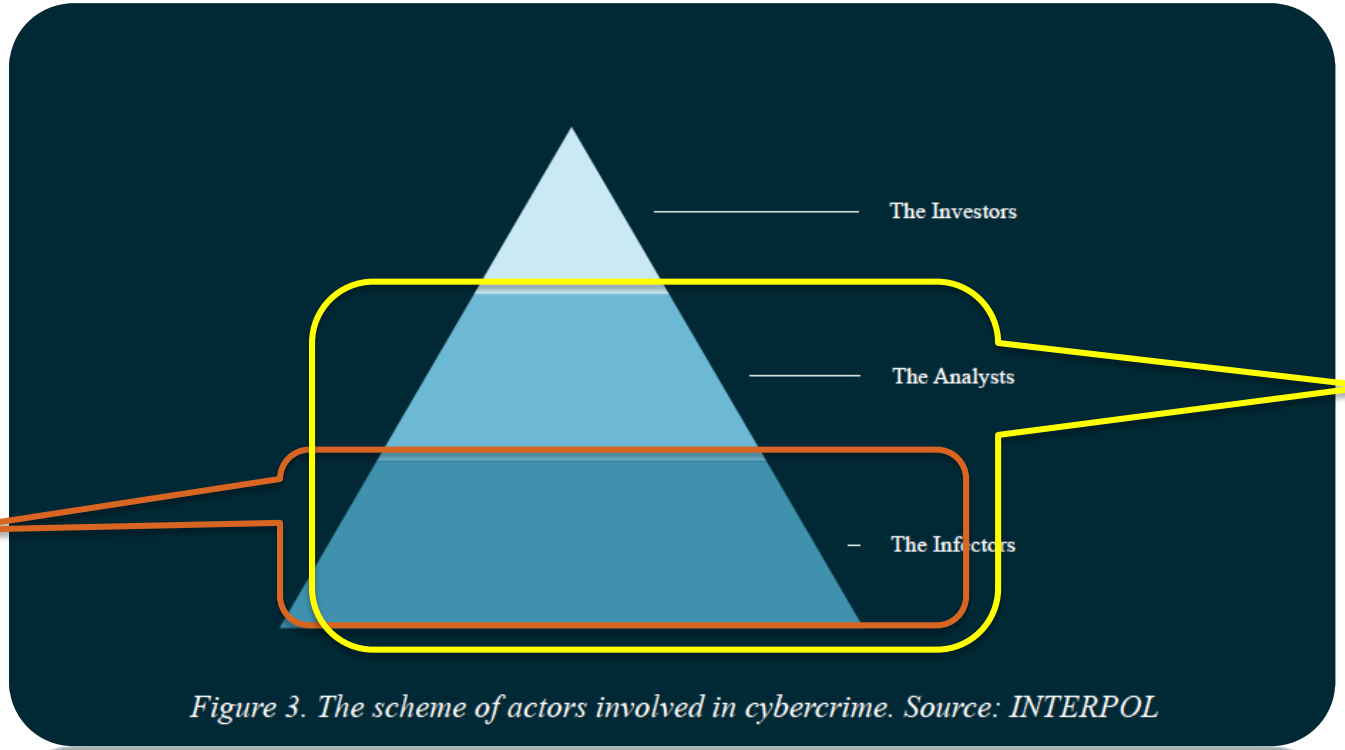


Figure 3. The scheme of actors involved in cybercrime. Source: INTERPOL

Yan Datsyuk
- Fobus-

Shuabang

What should we do about all this?

Mobile apps are pervasive in our digital world. They represent a **huge opportunity for criminal activity and they are already being exploited by criminal organizations**.

Official ecosystems to distribute apps have helped to increase security but have been demonstrated to **not be totally failsafe**.

Don't use unofficial stores unless you know what you are doing.

Do not implicitly trust mobile apps. Depending on your security requirements **the risk by not be acceptable.**

Apply adequate policies through MDM solutions.

Consider anti-malware solutions.

Monitor your own apps.

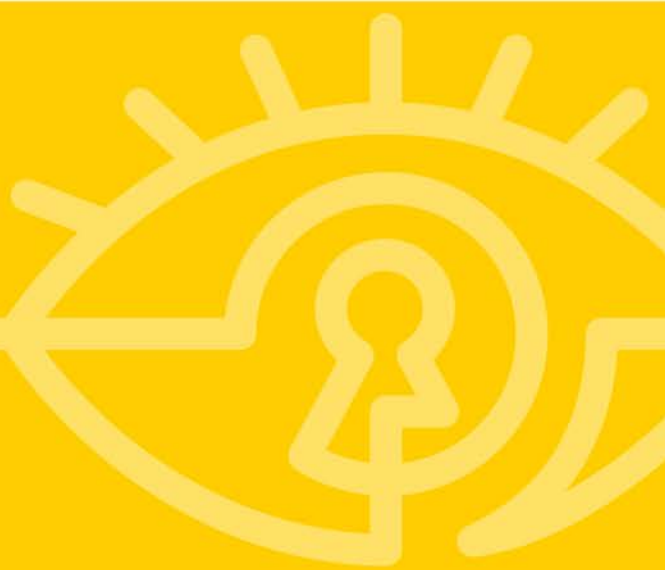
Educate your employees.

Employ both traditional signature-based techniques and complement with Big-Data Analytics

Leverage singularities to hunt down malware as soon as they appear on the app store. We don't have to wait for them to be installed and do harm

Combine this with OSINT source to hunt-down the authors, contact the appropriate LEA

etisalat
Eleven Paths



Thank you