Or what is considered as an evidence cannot indeed be

OPERATIONAL EXPLOITATION AND CORRUPTION OF ANDROID BASED SYSTEMS

Eric FILIOL, Valentin HAMON, Dorian LARGET & Thibaut SCHERRER

ASIA'S FOREMOST INFORMATION SECURITY CONFERENCE
GROUND ZERO SUMMIT 2013
NOVEMBER 7-10, 2013 | THE ASHOK, NEW DELHI

AGENDA

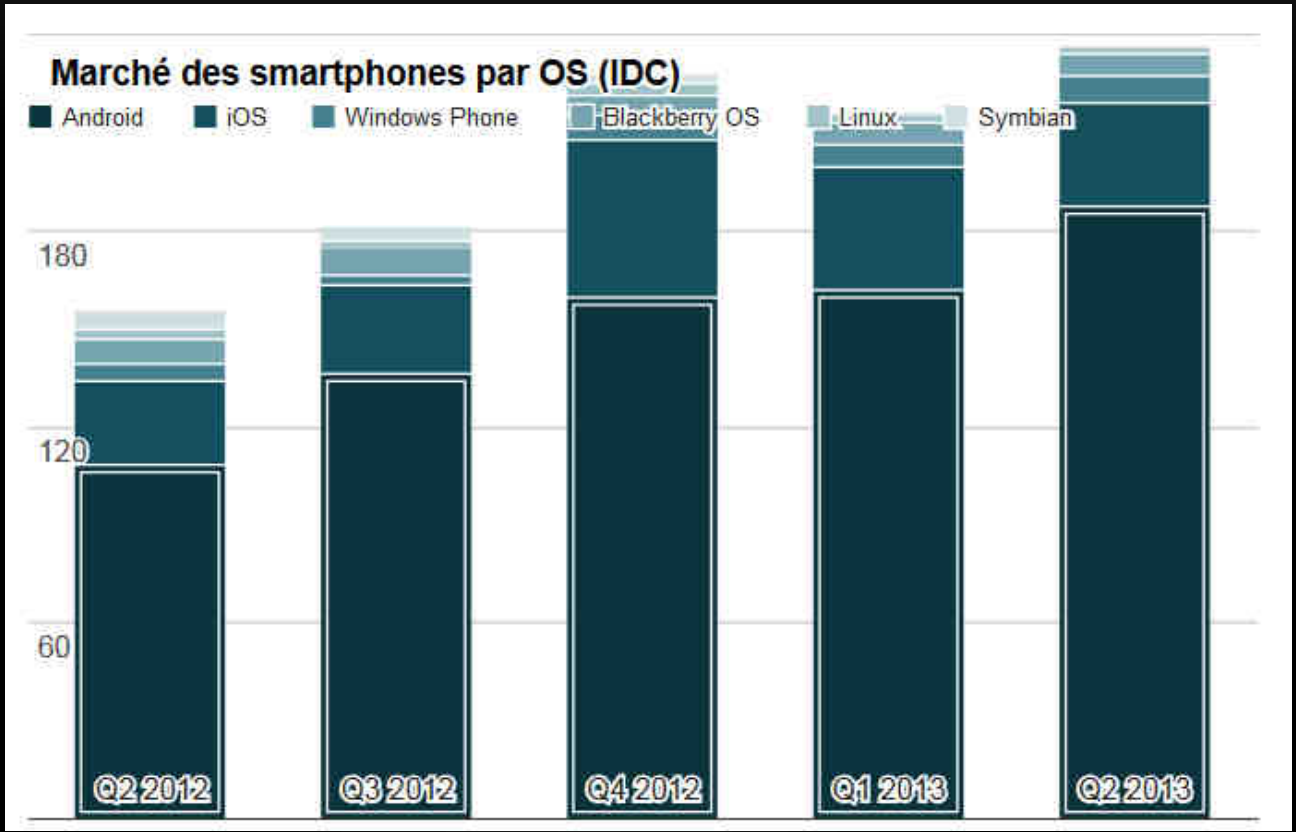
- Android
- Data
- Patching
- Injection device
- DAVFI

WHO ARE WE?

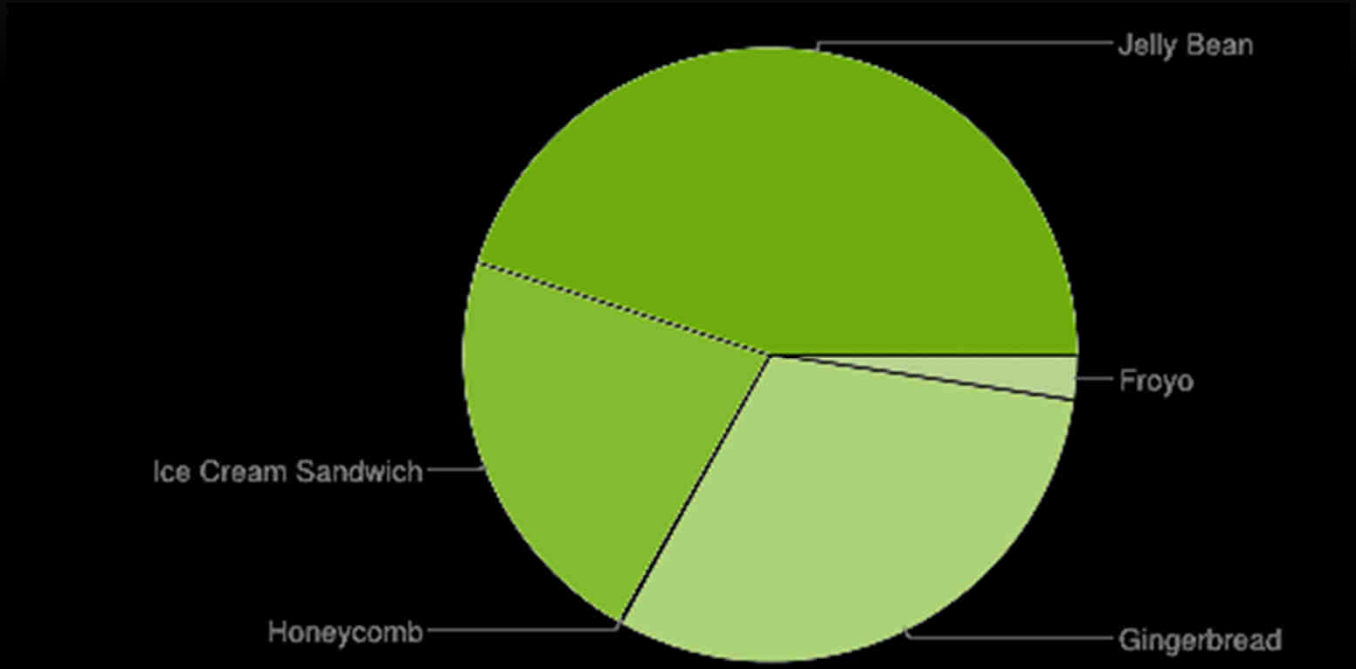
- Operational Cryptology Lab at ESIEA

- Academic but operational research lab
  - From theory to pure hacking
  - The attackers's vision and mind as scientific approach.
- Suppported by the French DoD and Industry

WHY ANDROID?


Marché des smartphones par OS (IDC)
Android
iOS
Windows Phone
Blackberry OS
Linux
Symbian
180
120
60
Q2 2012
Q3 2012
Q4 2012
Q1 2013
Q2 2013

ANDROID VERSIONS



MOBILITY SECURITY ISSUES

- Mobile devices are nowadays the entrypoint of our whole life
  - Whoever controls our mobile devices actually controls our life
- We all let our mobile device unattended for a few minutes at least (when you sleep, take a shower, in your pocket…)
- Our attacks work with all Android-based mobile devices (smartphones, tablets…)
- Due to the lack of time, we show here only a very few attacks/demos
  - We have designed/tested hundreds of them

DATA STORED ON THE DEVICE

OBJECTIVES

- Know witch data malwares, hackers and root applications could find on my smartphone
  - Analyse Android data

  - Analyse Applications data

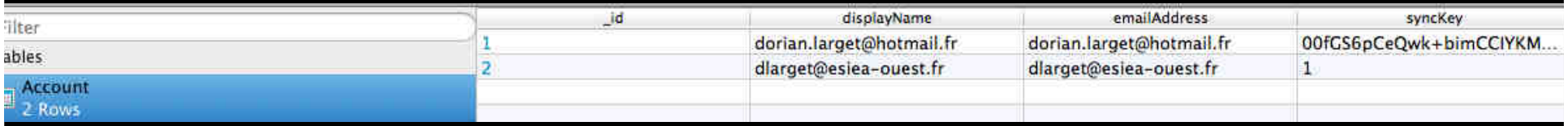
DATA : ANDROID

DATA : ANDROID (1/5)

- Contacts
  - Name
  - Numbers
  - Emails adresses
- SMS
  - Number
  - Texts

DATA : ANDROID (2/5)

- Data/data/com.android.email/databases/EmailProvider.db
  - Every accounts



_id	displayName	emailAddress	syncKey
1	dorian.larget@hotmail.fr	dorian.larget@hotmail.fr	00fGS6pCeQwk+bimCCIYKM...
2	dlarget@esiea-ouest.fr	dlarget@esiea-ouest.fr	1

DATA : ANDROID (3/5)

- Data/data/com.android.email/databases/EmailProvider.db

  All emails in Plaintext

snippet	protocolSearchInfo
Si cet e-mail ne s'affiche pas...	NULL
M. Dorian Larget, Nous vous...	NULL
INSCRIPTION COMMANDE EN...	NULL

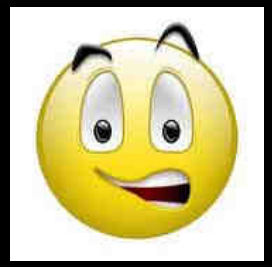
fromList	toList
[redacted]	dorian.large[redacted]
contact.[redacted]	dorian.large[redacted]
laboitea[redacted]	dorian.large[redacted]

DATA : ANDROID (4/5)

- Data/data/com.android.email/databases/EmailProvider.db

  Password in Plaintext in 4.1.2

  Password encrypted in 4.2.2



address	port	flags	login	password
dub-m.hotmail.com	443	5	dorian.larget@hotmail.fr	H[redacted]
m.hotmail.com	443	5	dorian.larget@hotmail.fr	H[redacted]
lalo.esiea-ouest.fr	443	5	etd-l\dlarget	H[redacted]
lalo.esiea-ouest.fr	443	5	etd-l\dlarget	H[redacted]

DATA : ANDROID (5/5)

- Data/misc/wifi/wpa_supplicant

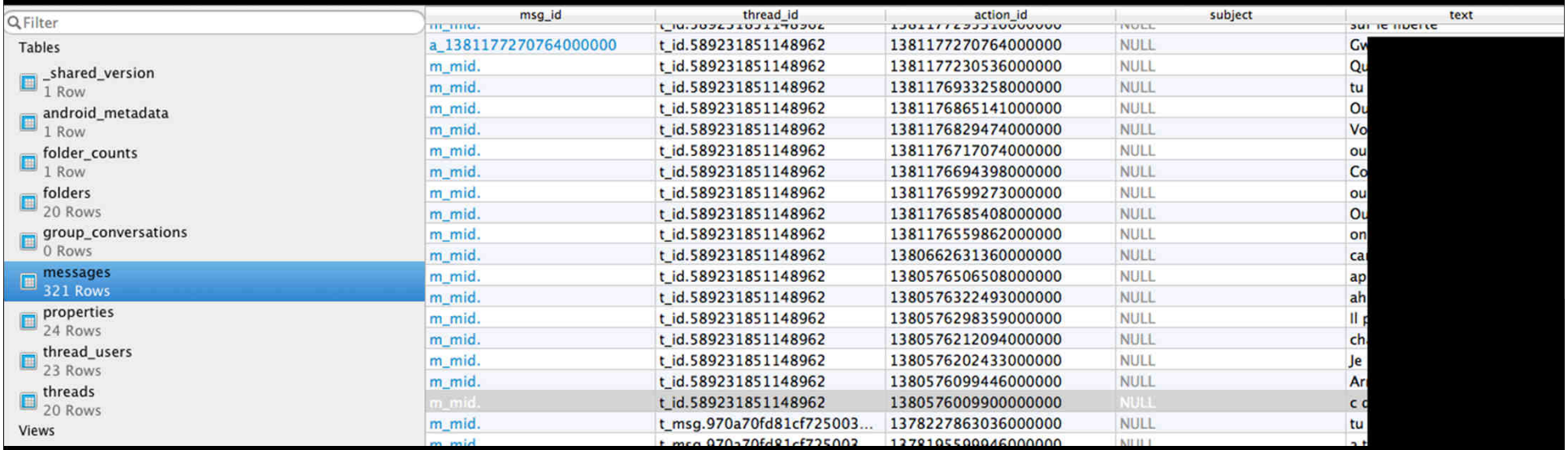
```
ctrl_interface=wlan0
update_config=1
device_name=m0xx
manufacturer=samsung
model_name=GT-I9300
model_number=GT-I9300
serial_number=4df1564f71515f71
device_type=10-0050F204-5
config_methods=physical_display virtual_push_button keypad
p2p_listen_reg_class=81
p2p_listen_channel=1
p2p_oper_reg_class=115
p2p_oper_channel=48

network={
        ssid="Intel-CP-THIBAUT-PC"
        psk="b[redacted]
        key_mgmt=WPA-PSK
        priority=1
}
```

APPLICATION DATA : FACEBOOK

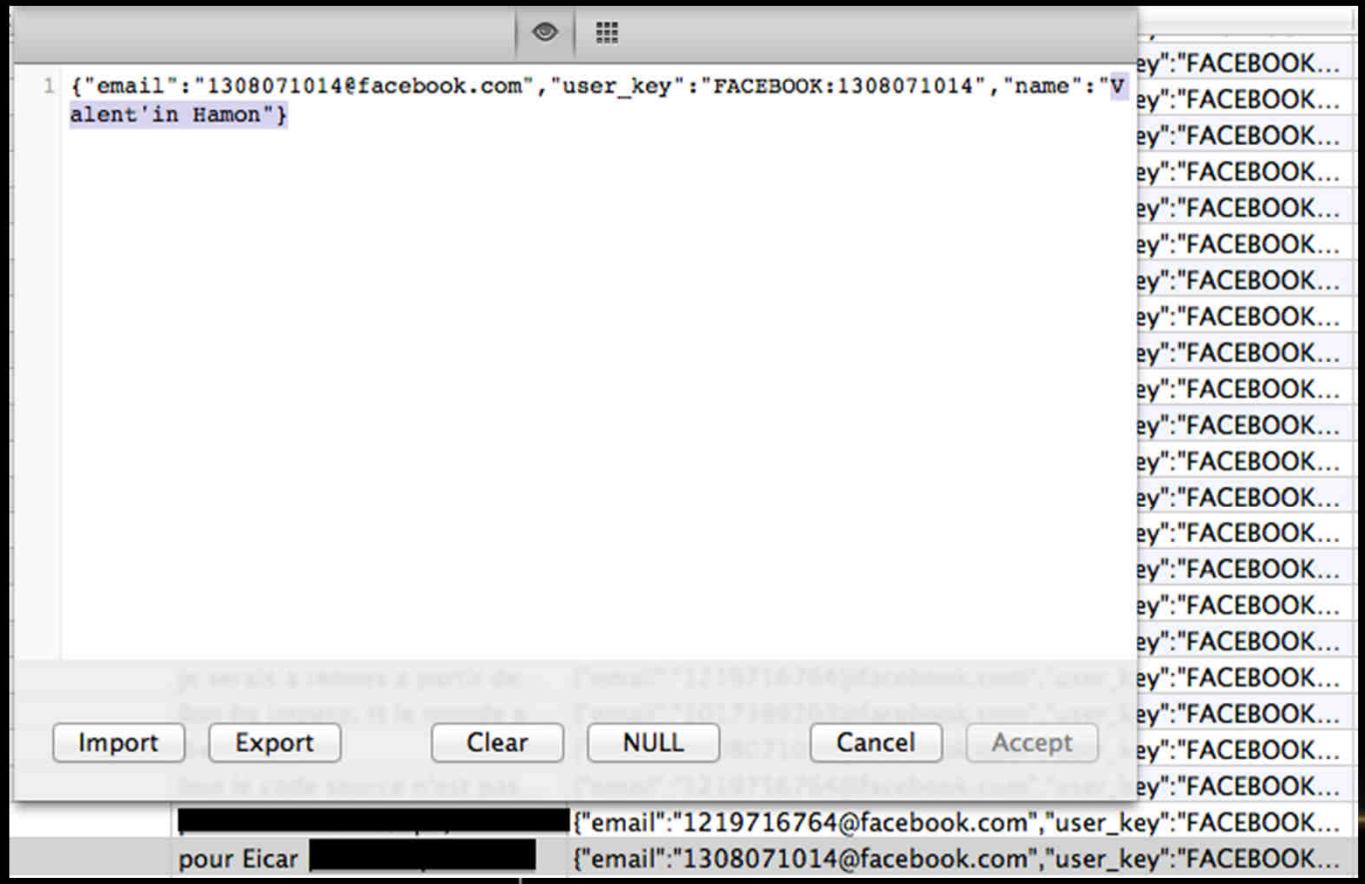
APPLICATION DATA : FACEBOOK (1/8)

- Data/data/com.facebook.katana/databases/threads_db2
  - Every Facebook Messages



APPLICATION DATA : FACEBOOK (2/8)

- Data/data/com.facebook.katana/databases/threads_db2



Username
Profil Id

APPLICATION DATA : FACEBOOK (3/8)

- Data/data/com.facebook.katana/databases/threads_db2

GPS position
Source of Messages

coordinates	offline_threading_id	source
NULL	NULL	chat
NULL	NULL	web
{"latitude":47.2254583,"longi...	5765889882682101680	mobile
NULL	5765889862695779476	mobile

APPLICATION DATA : FACEBOOK (4/8)

- Data/data/com.facebook.katana/databases/threads_db2

Every Facebook Contacts
Name
Emails etc…

user_key	first_name	last_name	name
FACEBOOK:100003702991682	Emmanuelle	[redacted]	Emmanuelle [redacted]
FACEBOOK:100002382279989	Audrey	[redacted]	Audrey [redacted]
FACEBOOK:1453213882	Emilie	[redacted]	Emilie [redacted]

APPLICATION DATA : FACEBOOK (5/8)

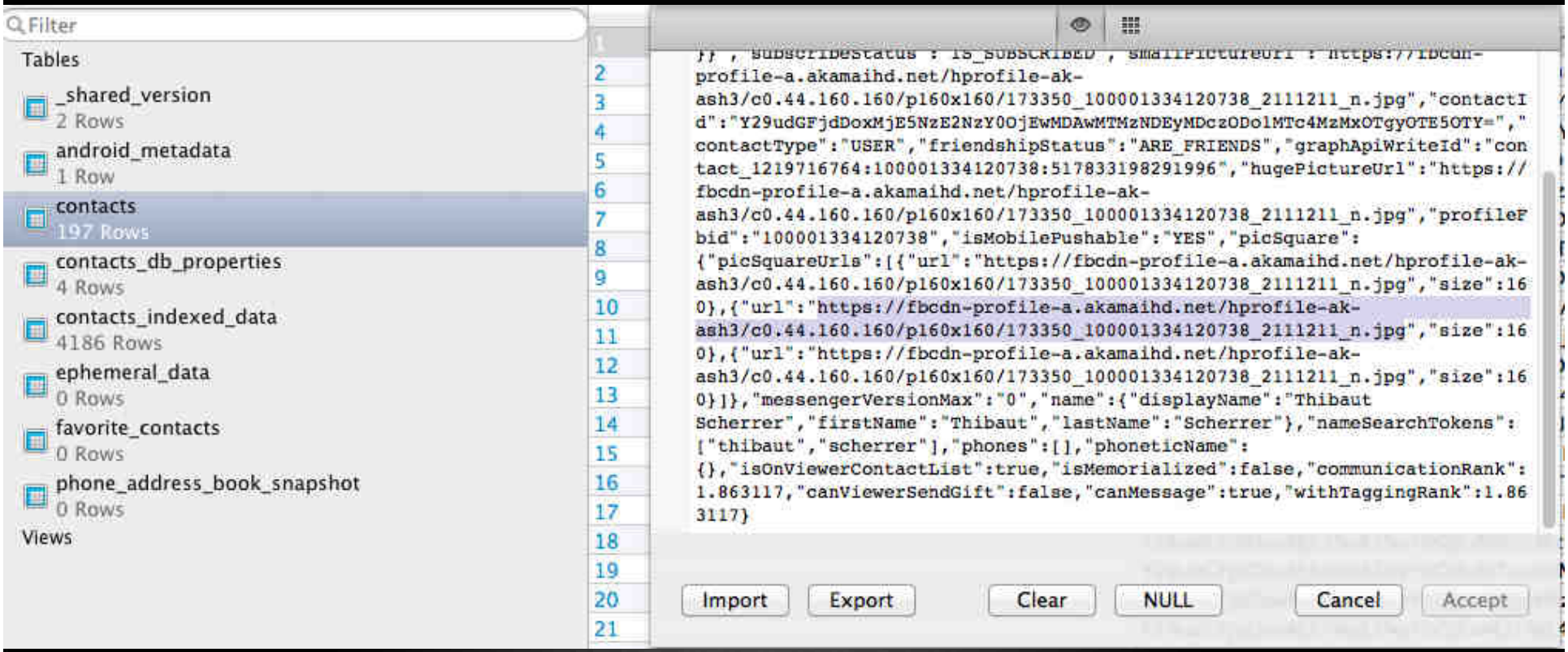
- Data/data/com.facebook.katana/databases/pref_db

Our Username

key	type	value
/fb_android/uvm/active_session_info	1	{"username":"dorian.la[redacted]...

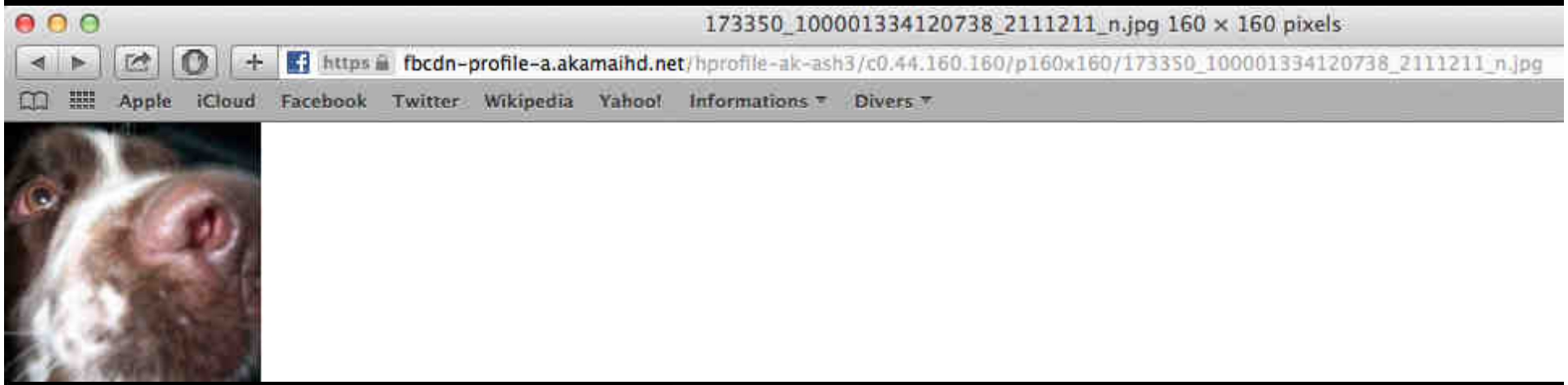
APPLICATION DATA : FACEBOOK (6/8)

- Data/data/com.facebook.katana/databases/contacts_db2



APPLICATION DATA : FACEBOOK (7/8)

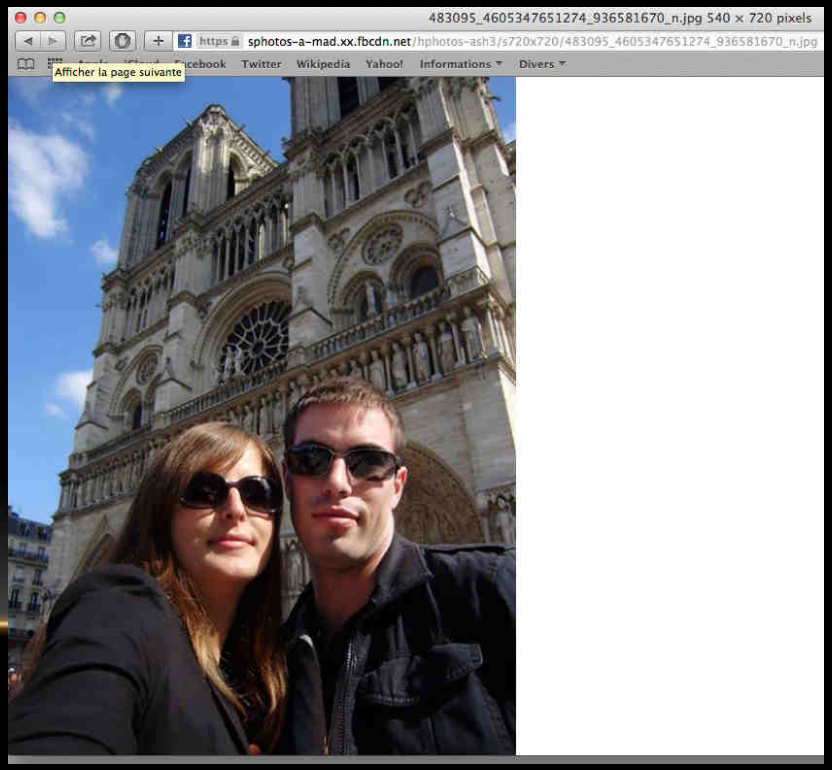
- Fbcdn-profile-a.akamaihd.net/hprofile-a3-ash3/…….



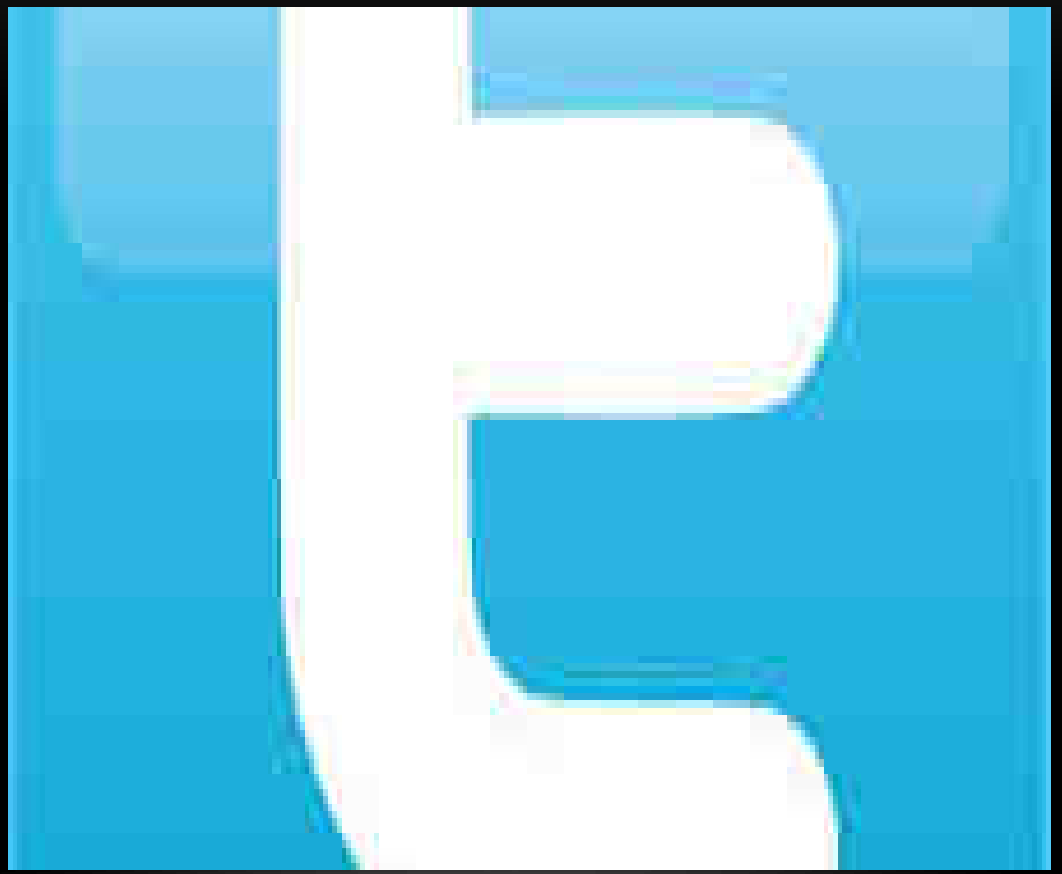
APPLICATION DATA : FACEBOOK (8/8)

- 1 month ago….
- https://sphotos-a-mad.xx.fbcdn.net/hphotos-ash3/s720x720/483095_4605347651274_936581670_n.jpg

NEVER PUBLIC!!!!!!!



APPLICATION DATA : TWITTER



APPLICATION DATA : TWITTER (1/3)

- Data/data/com.twitter.android/databases/819875234-5.db

user_id	username	name	description	web_url
819875234	DLarget	dorian larget	Student-Researcher	NULL
[redacted]				
769489166	HamonV	Hamon Valentin	I.T. Security Student Researcher	NULL

APPLICATION DATA : TWITTER (2/3)

- Data/data/com.twitter.android/databases/819875234-5.db

Soon at ground zero summit un New Delhi !	Twitter for Android	http://twitter.com/d...
[News]. Nexus 5 vs iPhone 5s http://t.co/ruq...	Google	http://www.google.c...
Operational exploitation and corruption of A...	web	NULL

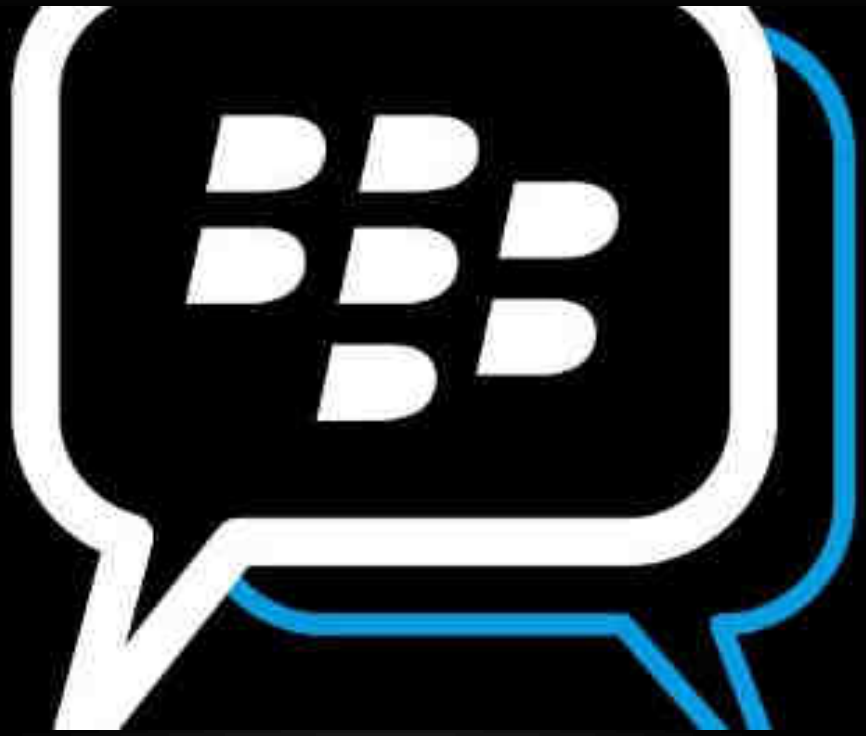
HamonV	Hamon Valentin	https://pbs.twimg.c...
JournalDuGeek	Le Journal du Geek	https://pbs.twimg.c...
HamonV	Hamon Valentin	https://pbs.twimg.c

APPLICATION DATA : TWITTER (3/3)

- Data/data/com.twitter.android/databases/819875234-5.db

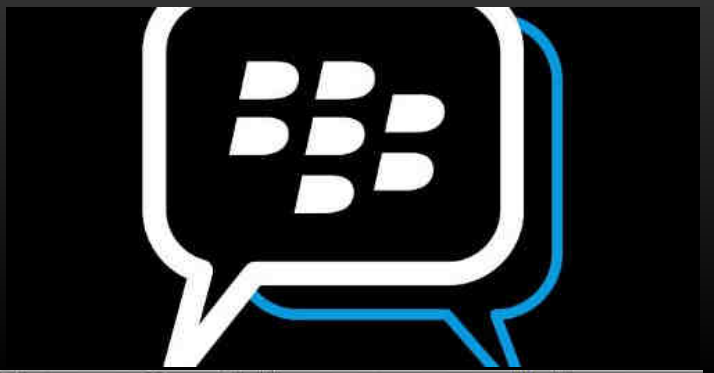
username	name	description	web_url
g0summit	GroundZero Summit	G0S is a largest collaborative...	http://t.co/F3AU22blaJ
DLarget	dorian larget	Student-Researcher	NULL
O			
Je			
C			
g			
ac			
D			
D			
D			
D			
D			
D			

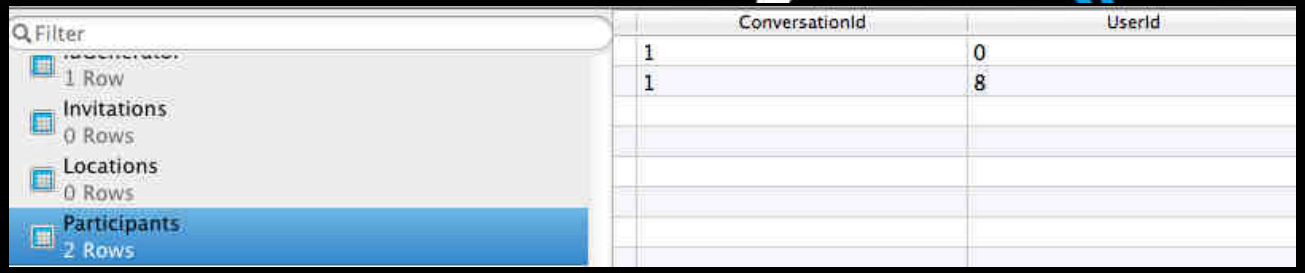
APPLICATION DATA : BBM



APPLICATION DATA : BBM

- Data/data/com.bbm/files/bbmcore/master.db





UserId	DisplayName
0	dorianlarget-34[redacted]
3	
4	
5	
6	
7	
8	Valentin Hamon

Timestamp	Content
1383578377	Hi dorian
1383578406	Hi. Test for ground zero summit

APPLICATION DATA : SKYPE

APPLICATION DATA : SKYPE

- Data/data/com.skype.raider/files/accountName/main.db

city	phone_home	phone_office	phone_mobile	emails
laval	NULL	NULL	NULL	dorian.large[redacted]

Filter

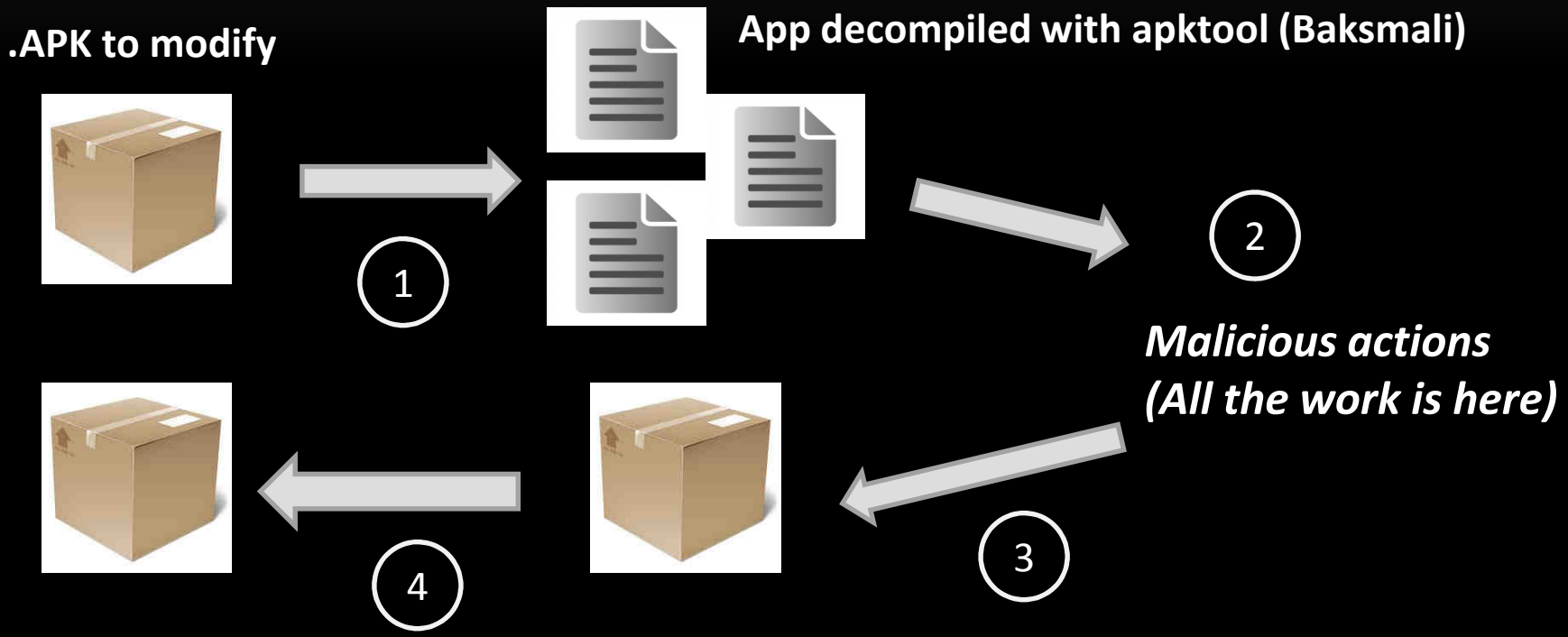
Tables

Accounts
1 Row

type	skypename	pstnnumber	fullname	birthday
NULL	dorianlarget	NULL	dor[redacted]	19901[redacted]

APPLICATION PATCHING

ANDROID APP PATCHING : PRINCIPLE (1/2)



https://code.google.com/p/smali/
https://code.google.com/p/android-apktool/

ANDROID APP PATCHING : PRINCIPLE (2/2)

An Android smartphone contains many applications in such folders:

/system/app : **system** apps (phone, camera, systemui,…)

or

/data/app : **normal** apps

or

/mnt/asec : **encrypted** apps (paid apps)

All these applications can be patched !!!

NB: We can easily steal any encrypted apps !!!!

ANDROID APP PATCHING : POSSIBILITIES

Malicious actions :
What we can do?

Principally, we can :
- **Modify**
- **Add**
- **Remove**

For example: remove Antiviruses features, add malicious listeners, modify algorithms, replace URLs…

https://code.google.com/p/smali/
https://code.google.com/p/android-apktool/

ANDROID APP PATCHING : SMALI (1/2)

Smali language:

Similar to bytecode but easier to read and modify.
Automatically generated from DEX files*
=> known and fixed indentation => easy to patch.

```
.method private doAddOp(ILandroid/support/v4/app/Fragment;Ljava/lang/String;I)V
    .locals 4
    .parameter "containerViewId"
    .parameter "fragment"
    .parameter "tag"
    .parameter "opcmd"

    .prologue
    .line 394
    iget-object v1, p0, Landroid/support/v4/app/BackStackRecord;->mManager:Landroid/support/v4/app/FragmentManagerImpl;

    iput-object v1, p2, Landroid/support/v4/app/Fragment;->mFragmentManager:Landroid/support/v4/app/FragmentManagerImpl;

    .line 396
    if-eqz p3, :cond_1
```

Writing a big malicious code in smali directly is not « trivial »!

*Compiled Android application code files.
https://code.google.com/p/smali/

ANDROID APP PATCHING : SMALI (2/2)

TIPS

We don't want to code a complete malicious code directly in smali, so :

How to generate a smali code easily?

1 – Coding and Testing code in Java with an IDE (eclipse)
2 – Building an APK with this IDE
3 – Dissamble with apktool
4 – Extract our smali files
5 – Search/replace package names (with regular expressions).

Smali

ANDROID APP PATCHING : PRATICAL EXAMPLE (1/6)

Context:

Physical attack**

↓

Root access on phone (by pushing a superuser binary in /system/bin)

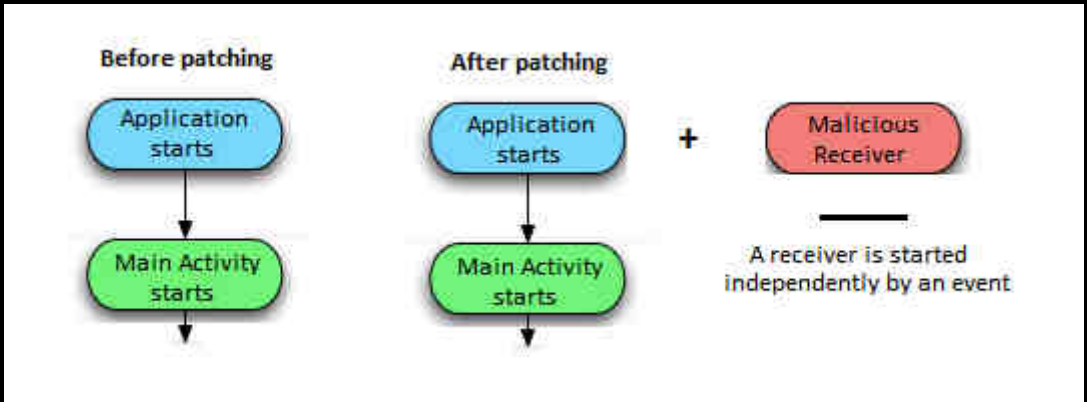
↓

Patch of *com.android.camera*
(SYSTEM APP)

**** : Full details in the next section of this presentation by Thibaut Scherrer**

ANDROID APP PATCHING : PRATICAL EXAMPLE (2/6)

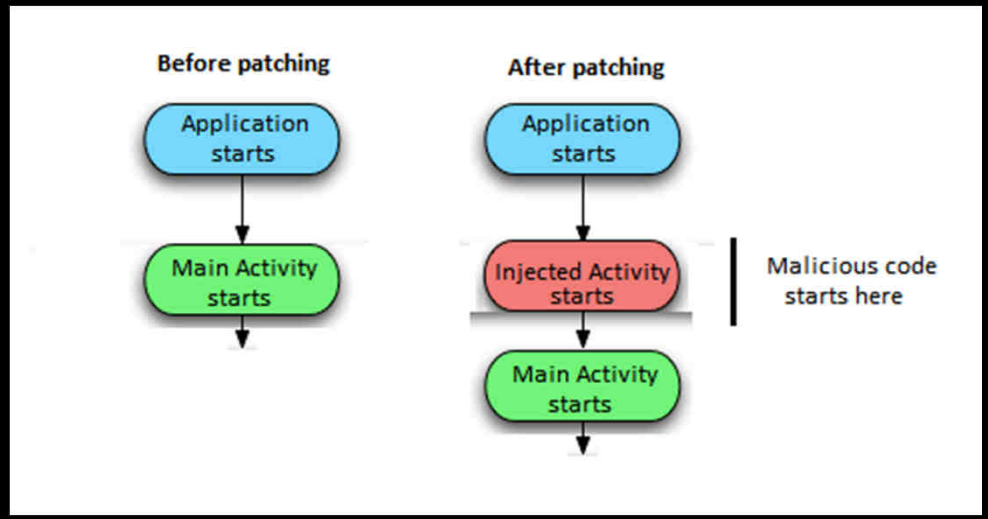
Injection of a malicious receiver:



Inject a malicious SMSReceiver + BootReceiver ?

ANDROID APP PATCHING : PRATICAL EXAMPLE (3/6)

Man in the middle attack:



ANDROID APP PATCHING : PRATICAL EXAMPLE (4/6)

Injection of a malicious SMS trojan with these features:

- SMS Hooking
- Remote Shell controlled by SMSes
- Remote Phone Calls

Demo presented after by Thibaut Scherrer.

ANDROID APP PATCHING : PRATICAL EXAMPLE (5/6)

Advantages of this attack:

- Camera still works the same.
- Camera can be disabled, but who will disable it? Nobody.
- AVs cannot scan it without root access… Tell me how they can do it?
- Because we got root access, remote shell gives us full possibilities.
- Victims cannot see anything (very steathly).

ANDROID APP PATCHING : PRATICAL EXAMPLE (6/6)

How to do it?

1 – We modify the Android Manifest file => silently add *all permissions for Camera !*
2 - We write the java code of a Trojan SMSReceiver.
3 - We add SMSReceiver.smali to the Camera smali files.
4 - We add the receiver declaration in the Android Manifest file.

```
<receiver android:name="com.android.camera.SMSReceiver" android:exported="true" >
<intent-filter android:priority="999">
<action android:name="android.provi .Telephony.SMS_RECEIVED" >
</action>
</intent-filter>
</receiver>
```

We set high priority for SMS Hooking

THE ATTACK

OPERATIONAL(S) POINT OF VIEW

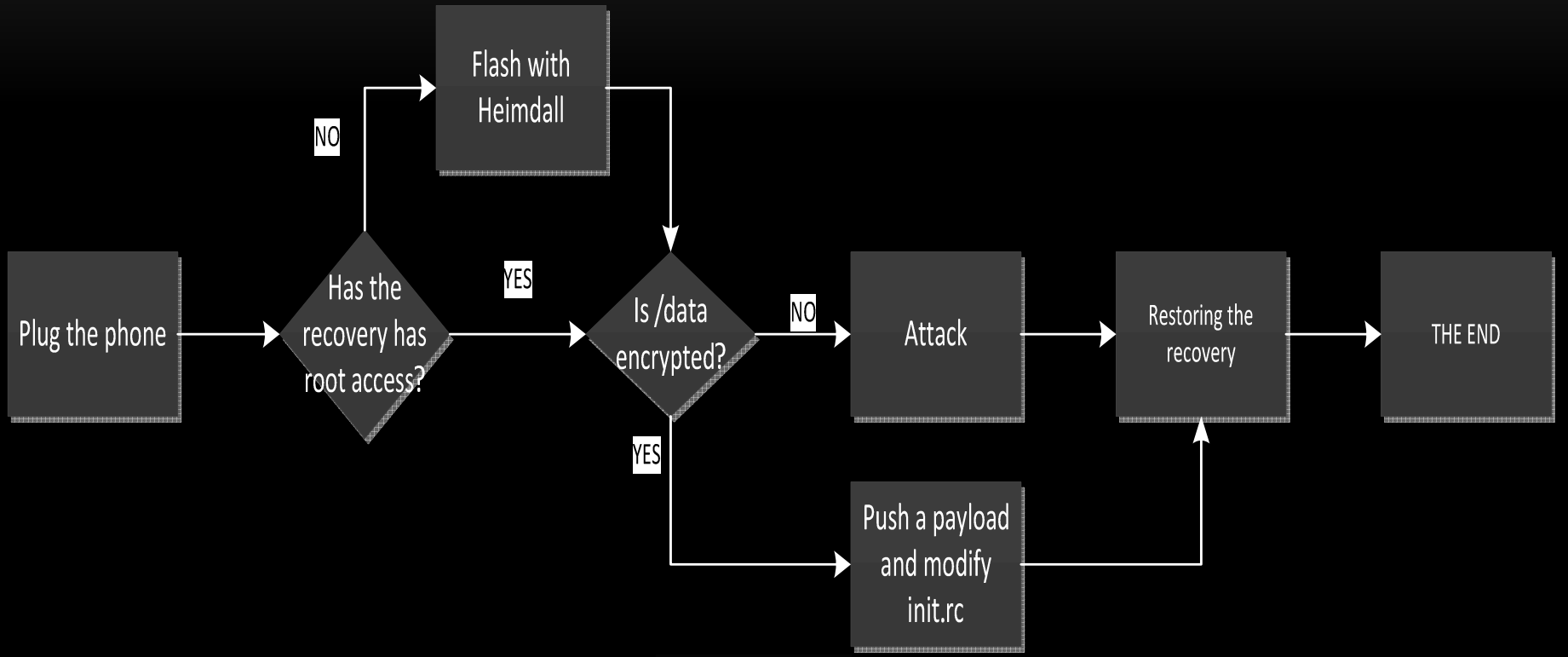
- Steal or inject new pieces of data
  - Steal emails or password…
  - Inject “fake evidence”
- Corrupt the system and inject new vulnerabilities
  - System apps patching

PERFORMING THE ATTACK: TOOLS

- Android tool
  - Recovery mode => gaining root access
  - Android Debug Bridge (adb) => shell to the phone
- Download mode
  - Heimdall => flashing the Recovery mode (for Samsung devices)

Does not need USB DEBUGGING at all !

PERFORMING THE ATTACK: AUTOMATION



PERFORMING THE ATTACK: DEVICE (1/5)

Attack

Stealth way?

PERFORMING THE ATTACK: DEVICE (2/5)

Attack

PERFORMING THE ATTACK: DEVICE (3/5)

Features we want :

- Small device.
- Mobility.
- Running Linux.

PERFORMING THE ATTACK: DEVICE (4/5)

≈70$

+

≈50$

PERFORMING THE ATTACK: DEVICE (5/5)

iMito MX2

- HDMI Dongle used to run Android on a TV
- Based on a dual core ARM chipset
- Able to run an OS from micro SD card

Embedded Ubuntu : project from www.slatedroid.com

PERFORMING THE ATTACK

DEMO

Injection of fake SMS + patch the Camera.apk

WHICH DEVICES CAN BE ATTACKED?

- Every smartphone with a custom recovery (because of root access)
- Every smartphone whose bootloader is not locked

WHICH DEVICES CAN BE ATTACKED?

Fasboot vs Download mode

- Mode used to flash the device
- Samsung: Download mode
- All other Android devices: Fastboot mode

Fastboot provides an oem lock/unlock functionality

Fasboot oem unlock => wipe data / factory reset

DAVFI

WHAT IS DAVFI?

- DAVFI is a R&D program supported by the French government's Fund for a Digital Society (FSN) which was established as part the French government's economic stimulus program (Network Security and Resilience Project).
- **The idea behind DAVFI is to enable France and Europe to become fully independent in the area of antivirus software.**
- DAVFI will deliver a reliable, controlled and high performance antiVirus Software that can be integrated into a complete offer designed to Institutions, Critical Infrastructure Operators (CIO), companies and individuals.
- To ensure trust in the software, its analysis engine will be **open source and free**.

DAVFI RATIONALES

- DAVFI considers a totally different security model that is not driven by a commercial model (protect rather than “make them pay model”)
- With a different security model,
  - it is possible to proactively protect (more powerful than simply “detect”)
  - The (formal, technical) proof of security can be provided
- The French Government projects imposes a endless R&D and service support for the user

DAVFI CONSORTIUM

Nov'IT company :	Project leader, operating company delivering innovative security services
ESIEA :	School of higher education, Operational Cryptology and Virology Lab (C+V)°
Qosmos company :	Network Intelligence solutions editor
Teclib company :	Expert in development, integration of inventory tools and IT management
DCNS Research :	World leader in the field of Naval Defense (warships, combat systems…)

Official website: http://www.davfi.fr/index_en.html

DAVFI ANDROID

- Full antiviral exploitation system d'exploitation
  - OS & AV are a single application.
  - The OS develops an actual immune system with additional security features/applications.
- Hardened, sanitized & clean up Cyanogen-based (demonstrator) & AOSP Android sources.
- The system operates close to the hardware.
- Low-level file system encryption.
- Full code execution control by cryptographic certification
- System self-protection features.
- Smartphones, tablets, desktop, laptop (Android compatible).

SECURITY ARCHITECTURE

DAVFI Market :
Applications certification and AV Server

APPLICATIONS CERTIFICATION AND AV SERVER

- Any Android application is analysed and certified before being made available on the DAVFI Market.
- Advanced behaviour-based AV analysis allowing the processing of hundreds apps per day.
- Cryptographic certification.
- No application can be executed on the device if it does not come from the DAVFI Market.
- The AV function is deported upstream on the server.
- The user is then free to download any apps from the DAVFI market or from his company dedicated
- The DAVFI market is an infrastructure that can specifically modified according to the business and company's needs.
- 500 applications available by now.
- Any app developper can submit his apps for DAVFI certification/labelling.

ADDITIONAL SECURITY FUNCTIONS

- SMS polymorphic encryption with *SMS Perseus*
  - Point to point and ad-hoc connexion (no central serveur)
  - Reduced detectability (low entropy profile)
  - Provable high security
- Point to point VoIP encryption.
- Remote system protection (theft and loss management) by double key and threshold scheme.
- Low-level self-protection against physical access –based attacks like the ones presented before.
  - 100 % provable if fastboot (all devices except Samsung devices)
  - 90 % provable for Samsung

DAVFI ANDROID SECURITY

- Solution tested successfully against all known attacks
- Security proof against
  - Known and unknown malware (including 0-day)
  - Physical access-based attacks.
- Technical research available soon (march 2014)
- Call to the internationa hacker community to limitless analysis.
- ROM should be available around the end of november (stay tuned up to the www.davfi.fr/index_en.html)

Q&A

eric.filiol@esiea-ouest.fr
dlarget@esiea-ouest.fr
vhamon@esiea-ouest.fr
tscherrer@esiea-ouest.fr