

the adventures of

alic & bob


Targeted Attacks: Mission 'Smartphones'

Speaker : Denis Maslennikov

Job Title : Senior Malware Analyst

Company Name : Kaspersky Lab

Agenda

- **Targeted attacks on smartphones**
 - **What** are they?
- **Target: smartphone. Why?**
 - **Consumerization** and threats
- **How targeted attack could proceed**
 - **Details** on possible scenarios
- **How to suppress targeted attacks?**



Targeted attacks on smartphones

- **Targeted attack on smartphone**

An attack on a smartphone which aims to steal corporate data stored on a device

Targeted attacks on smartphones

- **Targeted attack on smartphone**

An attack on a smartphone which aims to steal corporate data stored on a device

- **Small F.A.Q.**

- **Can targeted attacks be real?**
 - We'll discuss this later



Targeted attacks on smartphones

- **Targeted attack on smartphone**

An attack on a smartphone which aims to steal corporate data stored on a device

- **Small F.A.Q.**

- **Can targeted attacks be real?**
 - We'll discuss this later
- **Have they taken place already?**
 - It is **possible** that they have taken place



Target: smartphone

Why?

Target: smartphone. Why?

Mobile Devices Sales to End Users by Device Category Smartphones (Thousands of Units)

	2009	2010	2011	2012
Asia/Pacific	37 579,0	50 793,3	69 238,2	94 896,4
Eastern Europe	6 969,0	9 104,5	13 244,7	20 365,3
Japan	17 426,7	18 369,0	19 976,4	25 636,9
Latin America	7 251,7	10 453,5	18 626,9	29 003,3
Middle East and Africa	12 005,3	15 338,6	22 744,8	35 264,1
North America	45 601,8	66 695,3	89 861,2	104 698,4
Western Europe	45 540,7	79 373,1	139 580,6	174 321,3
Total	172 374,2	250 127,2	373 272,9	484 185,7

Gartner, Forecast: Mobile Devices, Worldwide, 2003-2014, 1Q10 Update

Target: smartphone. Why?

- Your **device** contains a lot of ‘interesting’ things

- outgoing **SMS** messages to your **friends**

- **work emails**

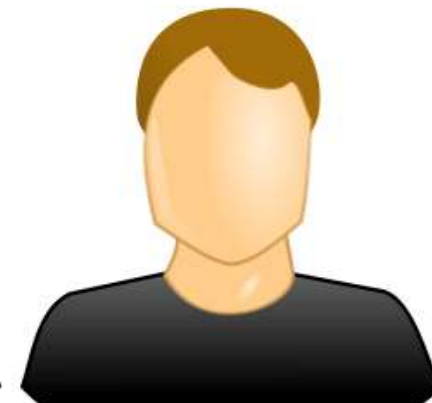
- **business contacts**

- trip **calendar**

- vacation **photos**

- **GPS** coordinates

- So, your **device is you!**

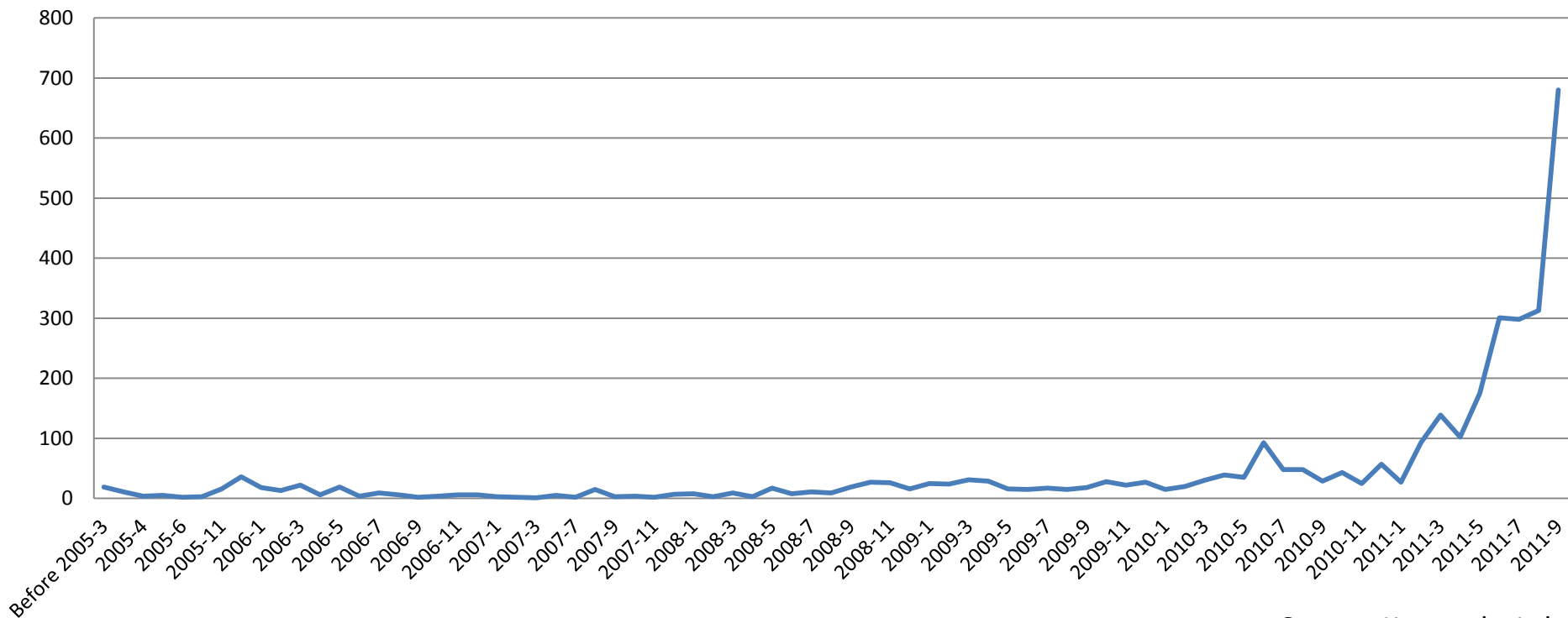


Target: smartphone. Why?

- **Mobile malware:**

- Almost **100% growth** of threats in 2011 over 2004-2010

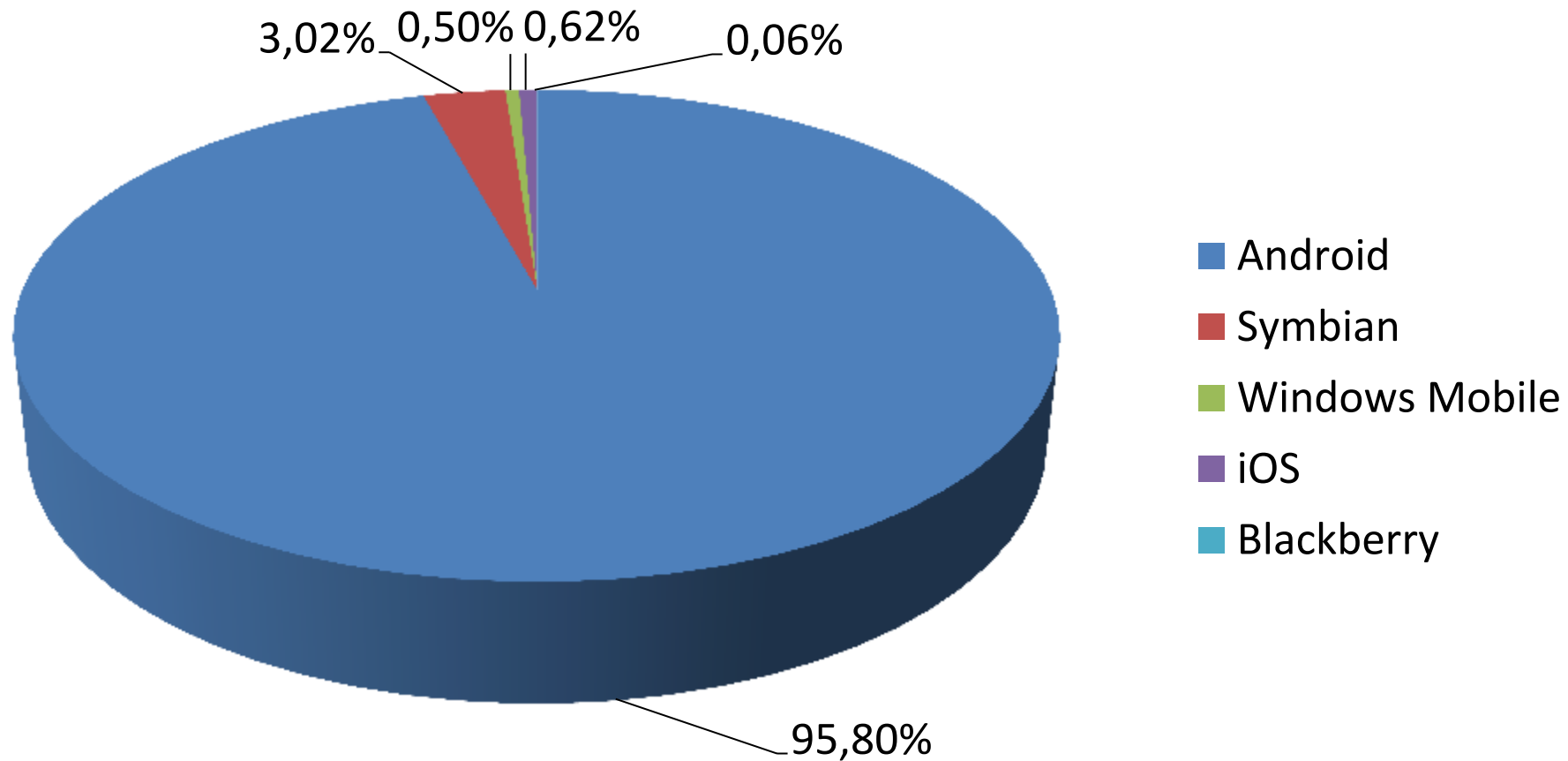
Number of modifications



Source: Kaspersky Lab

Target: smartphone. Why?

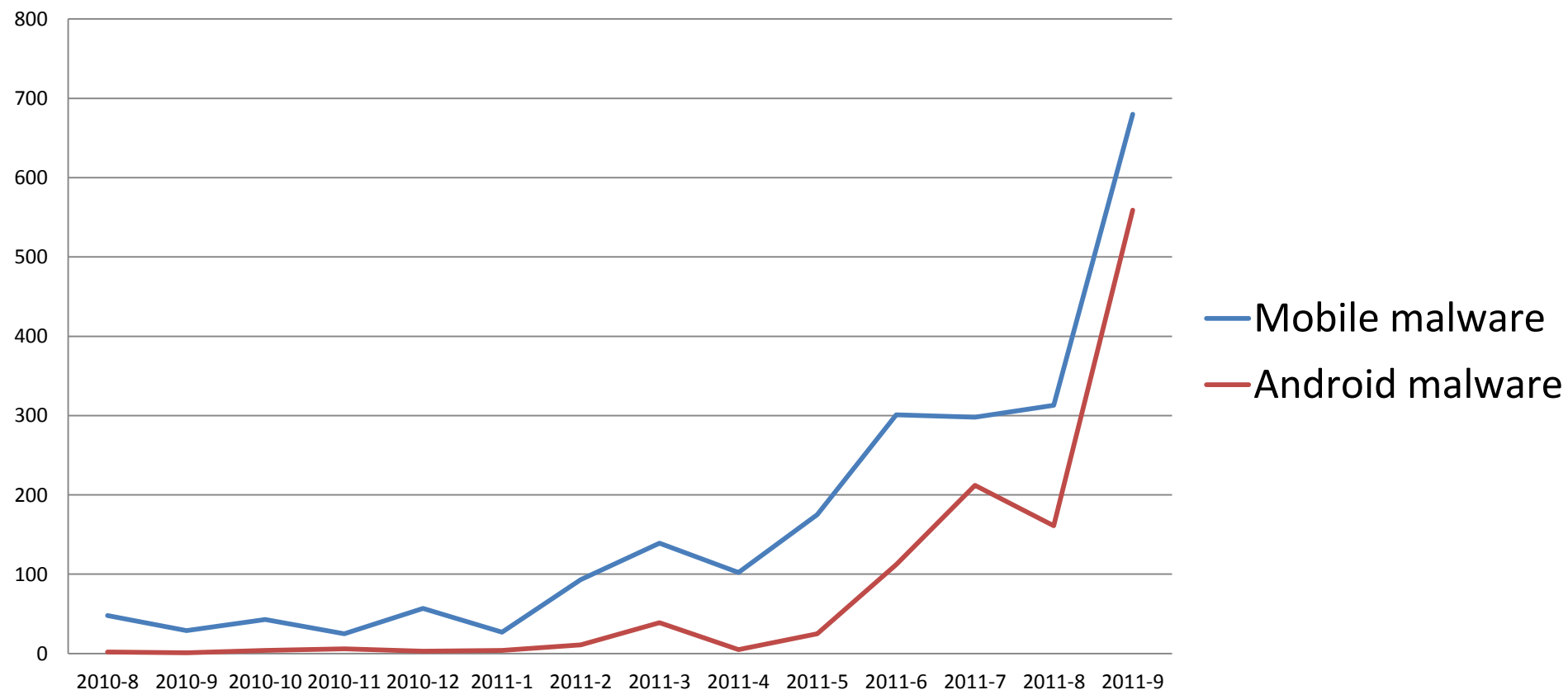
Malware for smartphones, 2011



Source: Kaspersky Lab

Target: smartphone. Why?

Android modifications vs. Mobile malware modifications



Source: Kaspersky Lab

How targeted attack could proceed

Details on possible scenario

Profiling the target: step 1

- **Profiling the target**
 - Trying to find the **most vulnerable**



Profiling the target: step 1

- **Profiling the target**
 - Trying to find the **most vulnerable**
 - **Social networks, again**



2nd

Recruiter and HR Business Partner, PSO 
San Francisco Bay Area | Staffing and Recruiting

Current

- **Recruiting Lead, PSO** at 
- **HR Business Partner, PSO** at 

Past

- Recruiter, PSO Leadership at 
- Recruiter at 
- Senior Consultant, IT Solutions at 

[see all...](#)

Education

- University of Oxford

Recommendations

2 people have recommended

Connections

425 connections

Public Profile

<http://www.linkedin.com/pub/>



Profiling the target: step 2

- Retrieving a phone number
 - It's even easier than email!

Press contacts for media

These contacts are for media enquiries only.

Anyone is welcome to [subscribe to our press releases by email](#)

For general enquiries (questions, school projects) look through [questions](#), or contact our [supporter services](#).

Media Contacts

For general media requests, please contact our duty press officer

[Redacted]

Email: [Redacted]

EU focused media requests [Redacted]

[Redacted]

Phone: +32 [Redacted]
Mobile: +32 [Redacted]

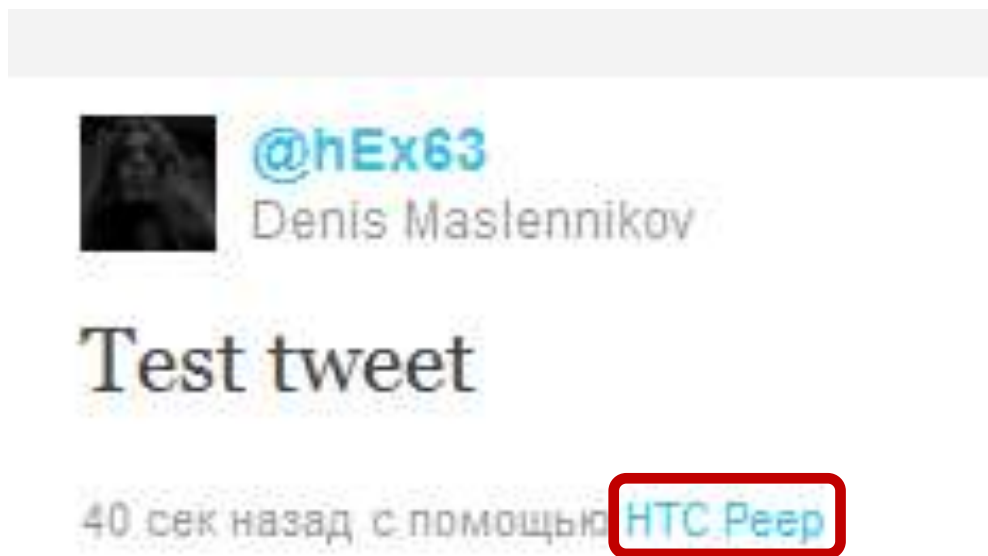
Profiling the target: step 3

- **Retrieving a device model**
 - It's also rather easy!



Profiling the target: step 3

- **Retrieving a device model**
 - It's also rather easy!



Sniffing: illustration 😊



Sniffing

- Using **public Wi-Fi on corporate device?**
 - **Not a good idea at all!**

- Using public Wi-Fi on corporate device?
 - Not a good idea at all!

BBC Mobile News Sport Weather Travel TV

NEWS TECHNOLOGY

Home UK Africa Asia-Pac Europe Latin America Mid-East South Asia US & Canada Business Health

17 May 2011 | Last updated at 10:34 GMT | 2,637 | Share | Facebook | Twitter | Email | RSS

Android handsets 'leak' personal data

More than 99% of Android phones are potentially leaking data that, if stolen, could be used to get the information they store online.

The data being leaked is typically used to get at web-based services such as Google Calendar.


The discovery was made by German security researchers looking at how Android phones handle identification information.

Google has yet to comment on the loophole uncovered by the team.

ID attack

University of Ulm researchers Bastian Konings, Jens Nickels, and Florian Schaub made their discovery while watching how Android phones handle login credentials for web-based services.

Many applications installed on Android phones interact with Google services by asking for an authentication token - essentially a digital ID card for that app. Once issued the token removes the need to keep logging in to a service for a given length of time.



Android phone owners are being urged to update their handset to avoid problems

Related Stories

- How safe is your smartphone?
- Is 'open' killing the Android?
- Apple, Google in privacy hearing

Armed with the token, criminals would be able to pose as a particular user and get at their personal information.

Even worse, found the researchers, tokens are not bound to particular phones or time of use so they can be used to impersonate a handset almost anywhere.

"[T]he adversary can gain full access to the calendar, contacts information, or private web albums of the respective Google user," **the researchers wrote in a blog post explaining their findings.**

Abuse of the loophole might mean some people lose data but other changes may be harder to spot.

"...an adversary could change the stored e-mail address of the victim's boss or business partners hoping to receive sensitive or confidential material pertaining to their business," the team speculated.

Physical access

Where is your device?

RSA CONFERENCE CHINA 2011
NOVEMBER 2-3 | CHINA WORLD HOTEL | BEIJING



Scene from...

RSA CONFERENCE CHINA 2011
NOVEMBER 2-3 | CHINA WORLD HOTEL | BEIJING



Scene from 'The Dark Knight'

RSA CONFERENCE CHINA 2011
NOVEMBER 2-3 | CHINA WORLD HOTEL | BEIJING



Real life example

- **More serious issues**

IAEA fears Iran officials have hacked UN nuclear inspectors' devices

Article

Published On Wed, 18 May 2011

George Jahn
Associated Press

VIENNA — The UN nuclear agency is investigating reports from its experts that their cellphones and laptops may have been hacked into by Iranian officials looking for confidential information

looking for confidential information

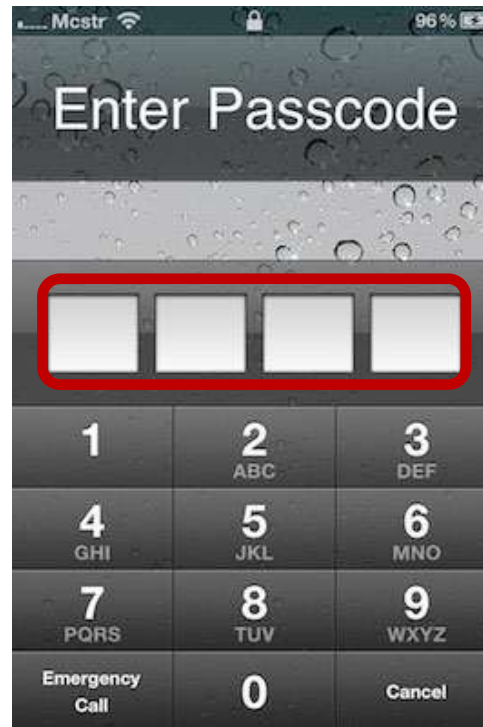
One of the diplomats said the International Atomic Energy Agency is examining “a range of events, ranging from those where it is certain something has happened to suppositions,” all in the first quarter of this year. He said the Vienna-based nuclear watchdog agency was alerted by inspectors reporting “units of electronic equipment.

while the equipment was left unattended

Two other diplomats in senior positions confirmed the essence of the report but said they had no further information. All three envoys come from member nations of the International Atomic Energy Agency and spoke on condition of anonymity because their information was privileged.

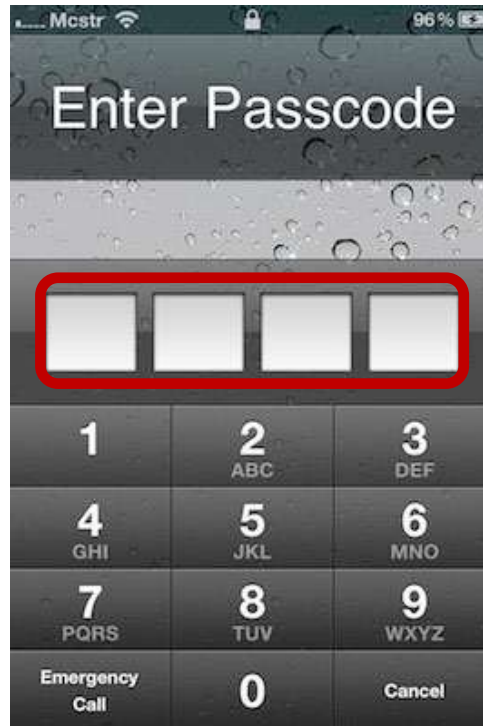
Screen lock: PIN

- **Direct physical access**
 - **Passcode?**



Screen lock: PIN

- **Direct physical access**
 - **Passcode?**



- 1234/birth year/0000/9876/etc?

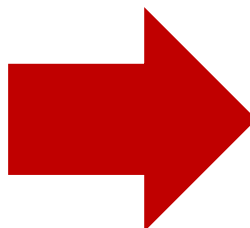
Screen lock: swipe lock

- **Direct physical access**
 - **Swipe lock?**



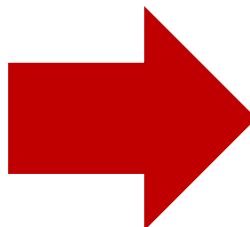
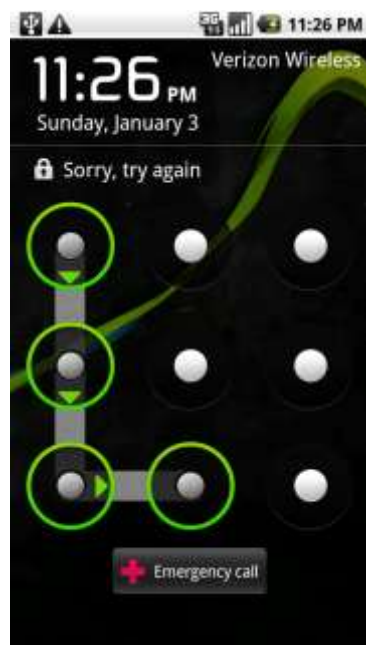
Screen lock: swipe lock

- **Direct physical access**
 - **Swipe lock?**



Screen lock: swipe lock

- Direct physical access
 - Swipe lock?



- **Complete retrieval: 68%**

Smudge Attacks on Smartphone Touch Screens; Aviv, Gibson, Mossop, Smith, University of Pennsylvania

Physical access: possible result

- **Present with pre-installed malware**
 - Classic Trojan attack



Remote attack

Unique malware

- **What functionality is necessary?**
 - **Mask itself**
 - **Read data** stored on smartphones
 - **Retrieve GPS coordinates**
 - **Where have you been and where are you now**
 - **Able to communicate with the drop-zone**
 - **Upload stolen information**



Functionality

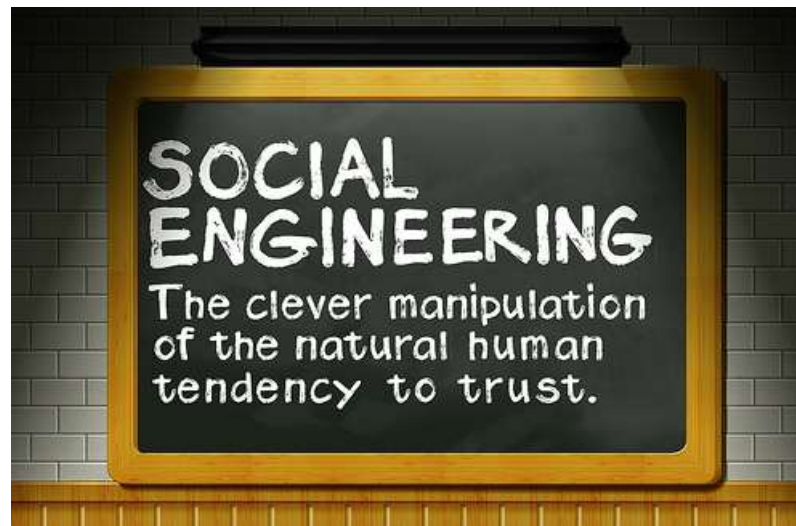
In discovered malware

- Has it been done?

Read data	<i>Monitor.AndroidOS.Flesp</i>
GPS	<i>Monitor.AndroidOS.Tapsnake</i>
Disguise	<i>Trojan-Spy.AndroidOS.Geinimi</i>
Communication	<i>Backdoor.AndroidOS.Rooter (DroidDream)</i>

Delivering the malware

- Usage of **social engineering tricks** to get the victim to **click on a link**:
 - In the **SMS spam** message
 - In the **Skype spam** message
 - In the **social network spam** message



(Un)Trusted sources

- **‘But I use only official application stores!’**
- **Malware in the Android Market**
 - **March 1, 2011**
 - Malicious apps have been **available for several days**



(Un)Trusted sources

- **‘But I use only official application stores!’**
- **Malware in the Android Market**
 - **March 1, 2011**
 - Malicious apps have been **available for several days**
 - **May 11, 2011**
 - Malicious apps have been **available for several...**



...months?

(Un)Trusted sources

- Android Market mirroring web sites
- Screenshot captured May 12
- Malware uploaded February 27
- 2,5 months before it was noticed!

The screenshot shows an Android Market listing for an application named "3D Cube horror terrible". The interface includes a header with the title, a section for screenshots (with two images: a distorted face and a Rubik's cube), a "Discussion(s)" section (with a message "No discussion found"), and a "Comments and Ratings" section. On the right side, there are details: Price (Free), Version (4.0), Downloads (100-500), Size (184.0 KB), and Category (Brain & Puzzle). A red rounded rectangle highlights the "Last update" section, which states "1781h ago" and includes a blue "Ask for Update" button. At the bottom, there are filters and a Facebook social plugin.

Price

Free

Version

4.0

Downloads

100-500
Estimate :
100

Size

184.0 KB

Category

Brain & Puzzle

Last update

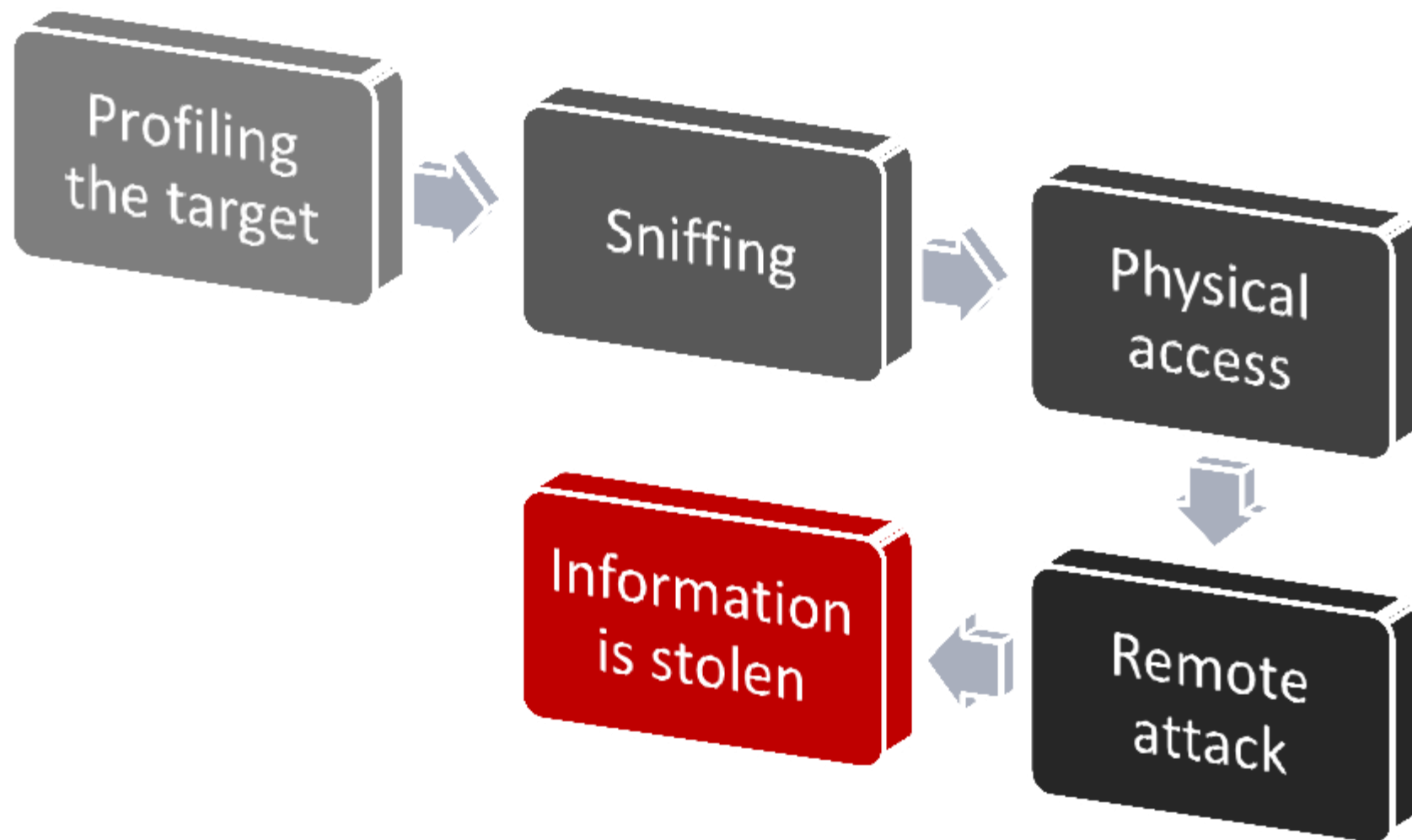
1781h ago

Ask for Update

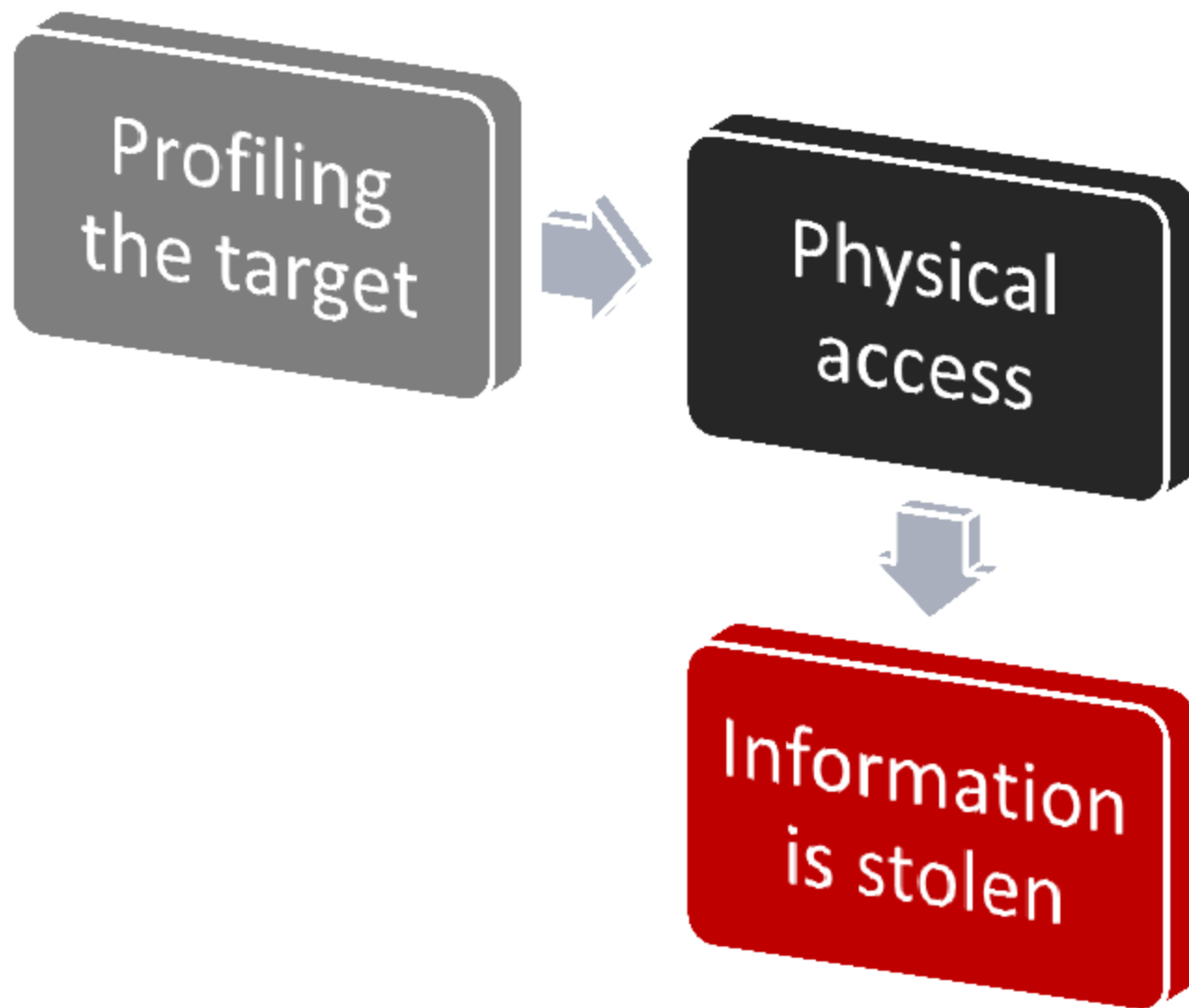
Successful targeted attack

Results

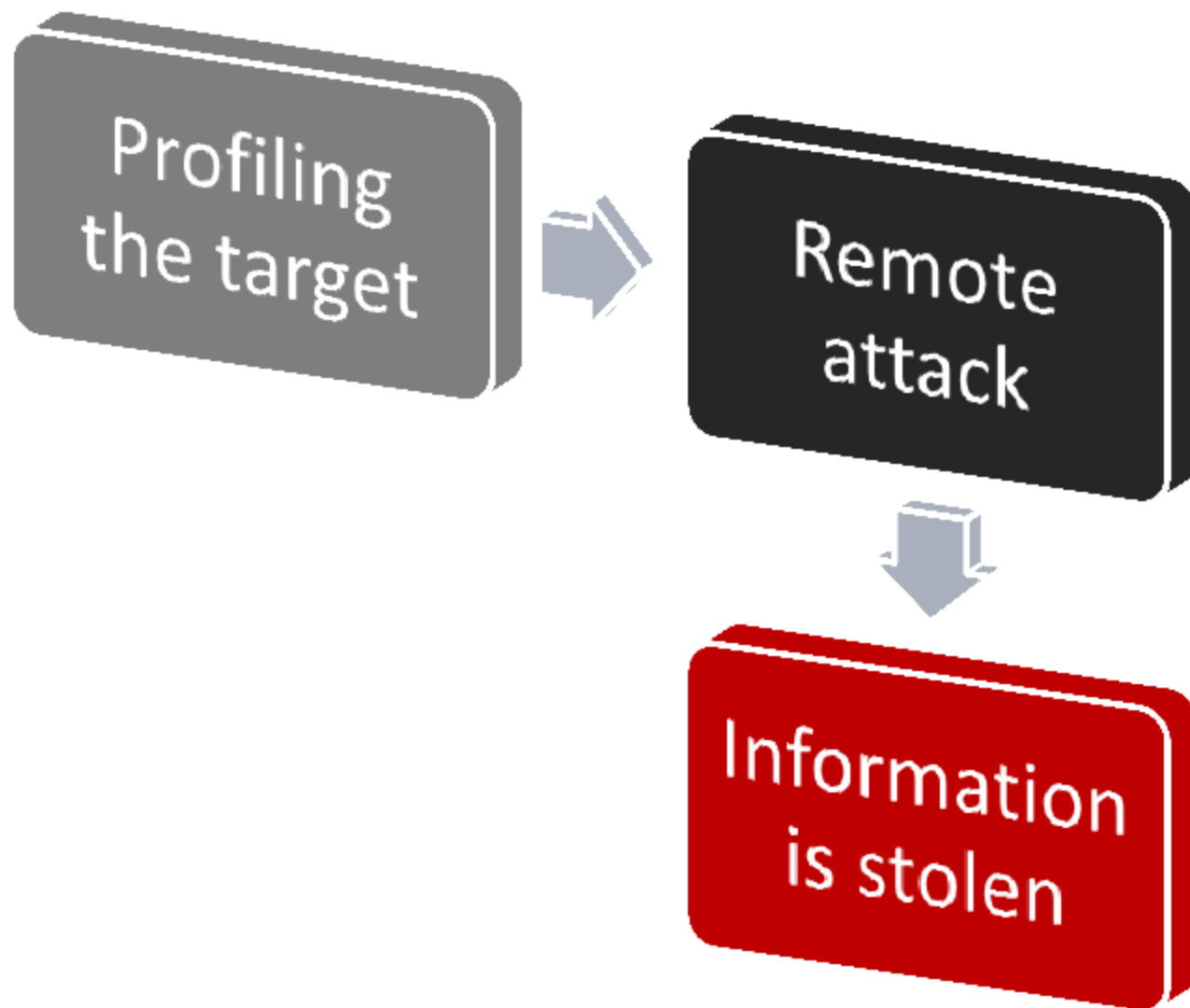
General scheme



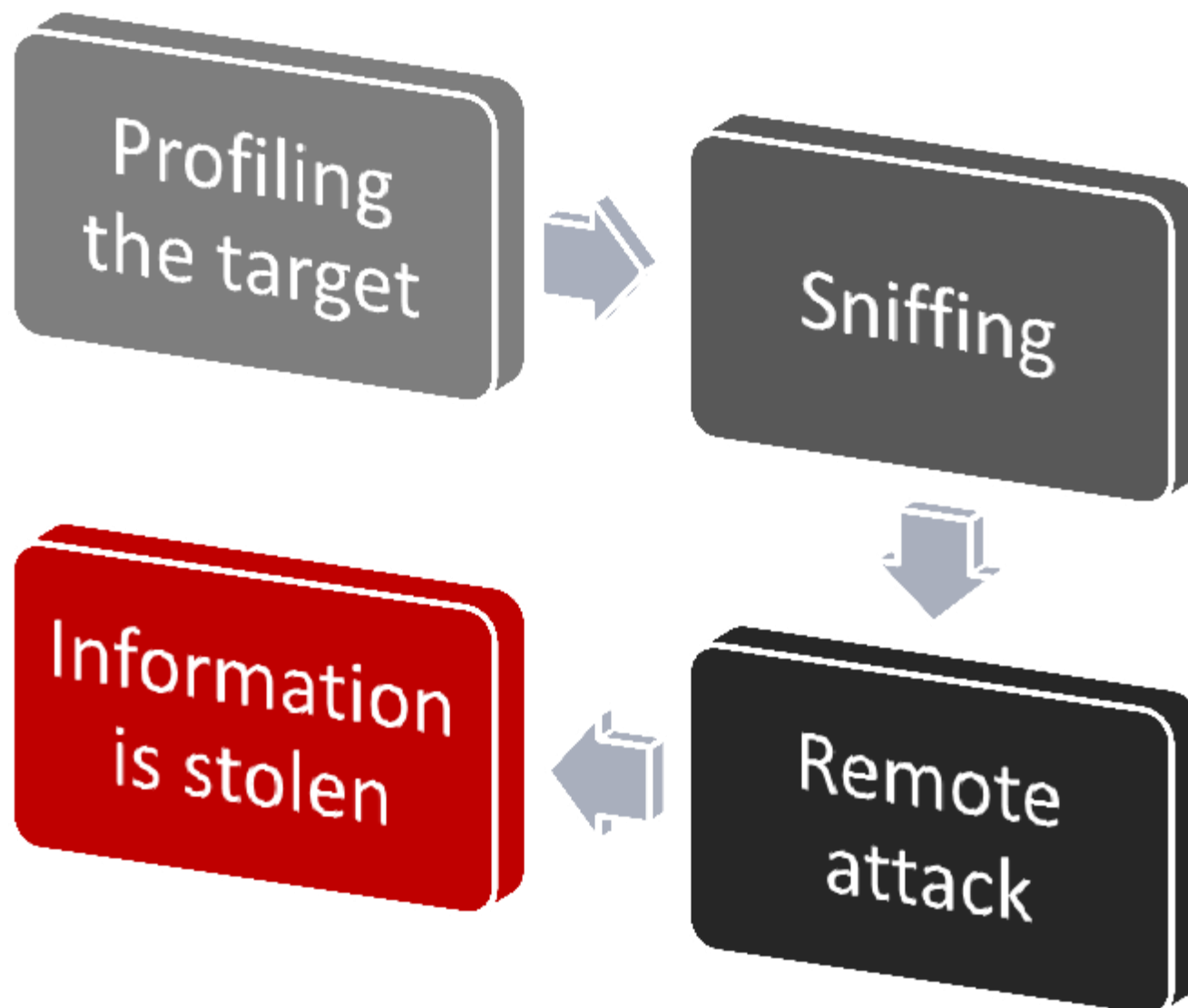
General scheme



General scheme



General scheme



Results

- **Mission accomplished**
 - Necessary information was stolen or accessed
- **What's next?**



Results

- **Mission accomplished**
 - Necessary **information was stolen or accessed**
- **What's next?**
 - **Information can be sold**
 - To competitors
 - To third party
 - **Blackmailing**
 - **Disclosure to public**
 - **Erasure or modification**



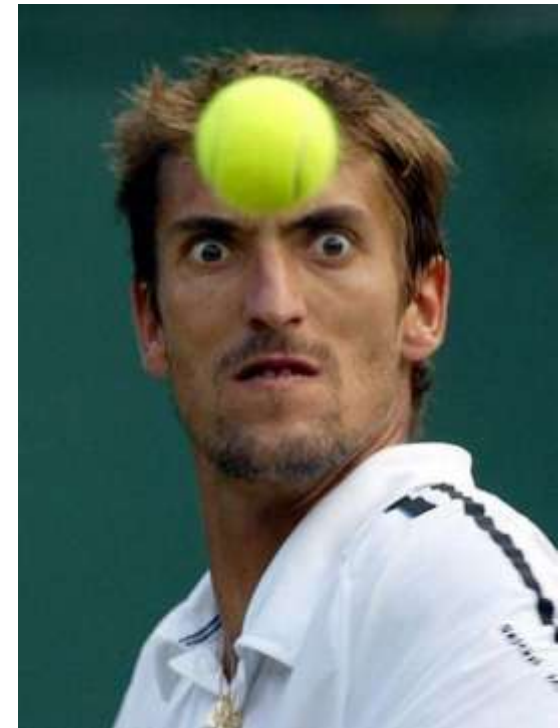
How to suppress targeted attacks

Suppressing targeted attacks

- **Don't use public or untrusted Wi-Fi networks**
 - **WPA2** encryption
 - **3G/4G** is more **secure**

Suppressing targeted attacks

- **Don't use public or untrusted Wi-Fi networks**
 - WPA2 encryption
 - 3G/4G is more **secure**
- **Physical security**
 - Always **keep an eye** on your device
 - **Always!**
 - Usage of strong **screen lock password** or **tricky swipe lock** is good idea
 - **Remote wipe software** must be **mandatory** for corporate devices



Suppressing targeted attacks

- **Making life harder for remote attacker**
 - **Update** OS and third party software **regularly**
 - **Read all permissions** carefully
 - **SMS** sending for **'media player'** is **not necessary**
 - **Ignore** all SMS (and email) **spam** messages
 - especially with **URLs**
 - **Use encryption**
 - **encode** all critical data
 - **Avoid jailbreaking or 'rooting'**



Last but not least

**Don't think that your
smartphone is safer
than your PC**

the adventures of alic & bob



Thank you!
Targeted Attacks: Mission 'Smartphones'

Speaker : Denis Maslennikov

Job Title : Senior Malware Analyst

Company Name : Kaspersky Lab