Cognitive approach for social engineering

How to force smart people to do dumb things.

Enrico Frumento**,**
CEFRIEL, Politecnico di Milano (IT)
Claudio Lucchiari, Gabriella Pravettoni, Mario Andrea Valori,
IRIDe (Interdisciplinary Research and Intervention on Decision),
Center Università di Milano (IT)

www.cefriel.it

AIM AND MAIN CONTRIBUTION OF THIS PAPER

- Understand the importance of Cognitive Sciences for the study of Social Engineering
- Perform a real and controlled phishing vulnerability assessment with real business users
- Address countermeasures

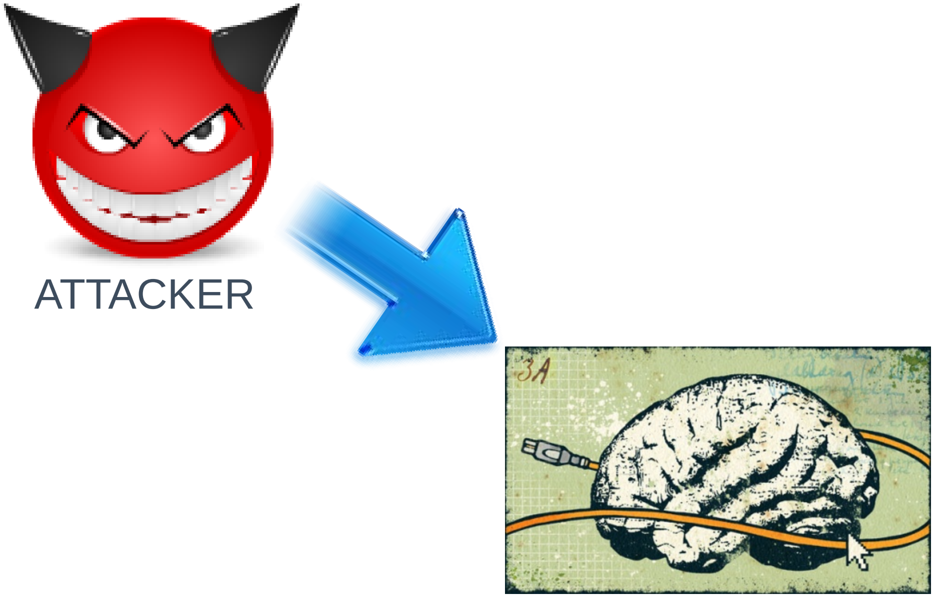
STRUCTURE OF THE PRESENTATION

- How psychology contributes to security
  - malware 2.0
  - Memetics what else?
- Our view of Social Engineering
  - Social engineering 2.0
  - Cognitive approach
- An early study: Mobile World and SMSishing
  - Results
  - So far..
  - What's to come..

STRUCTURE OF THE PRESENTATION

- How psychology contributes to security
  - malware 2.0
  - Memetics what else?
- Our view of Social Engineering
  - Social engineering 2.0
  - Cognitive approach
- An early study: Mobile World and SMSishing
  - Results
  - So far..
  - What’s to come..

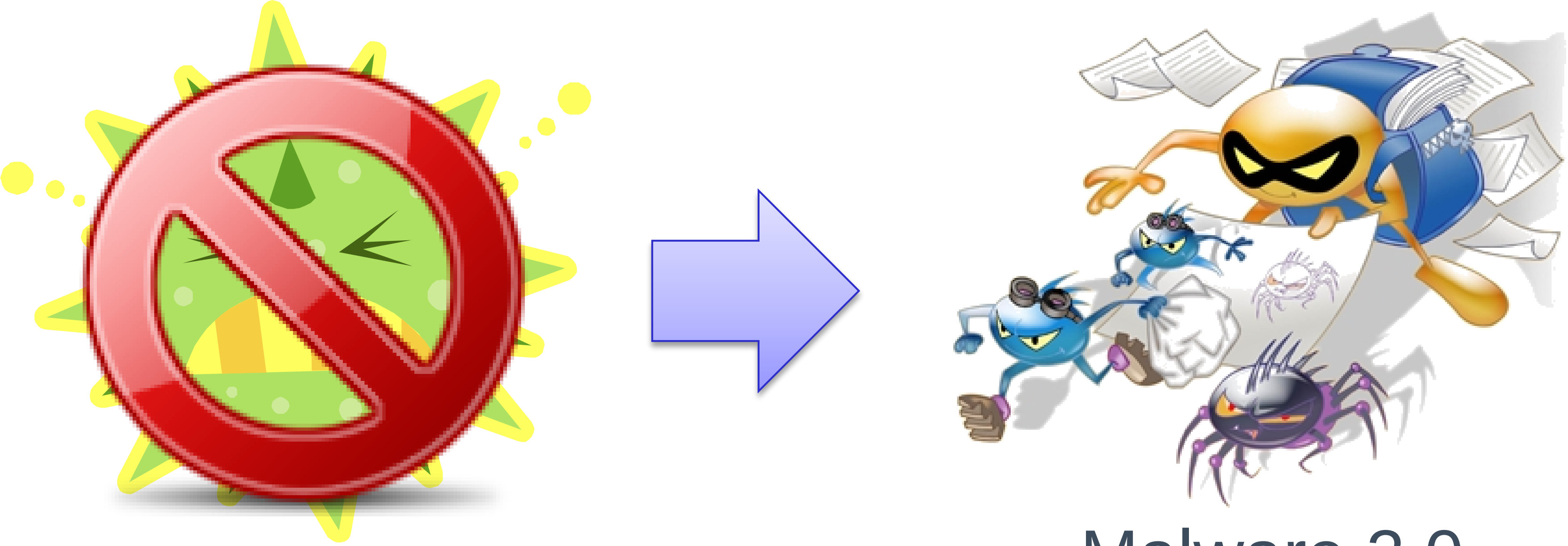
HOW PSYCHOLOGY CONTRIBUTES TO SECURITY


ATTACKER

- Which psychological models are really used (if any) by attackers of an informatics system to fool its users?
- How extensively is psychological modeling used?

Social Engineering: Memetics, Cognitive Sciences

WHERE ARE VIRUS ANYWAY?



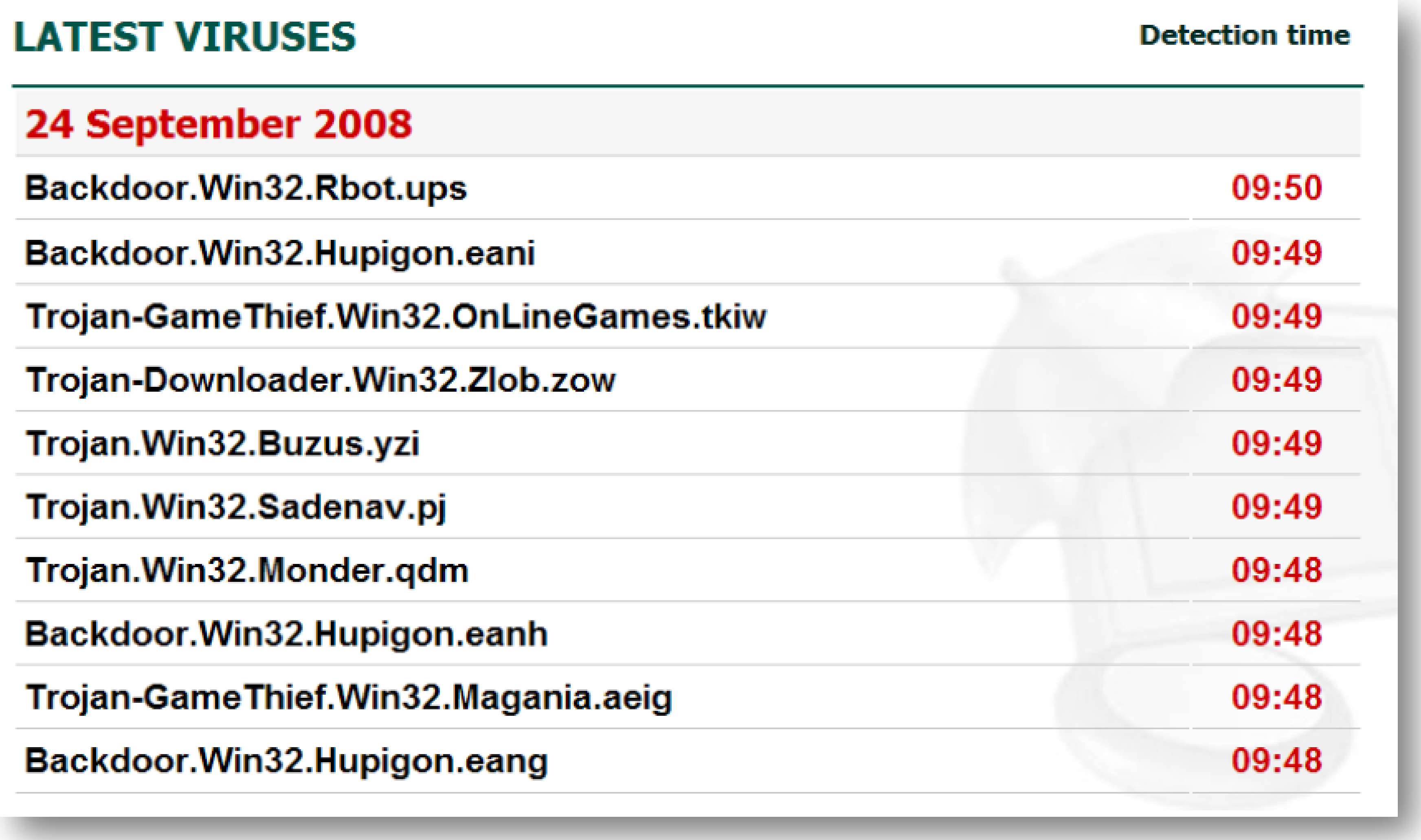
Malware 2.0

MALWARE 2.0

- The Malware 2.0 model is characterized as follows:
  - the absence of a single command and control center for networks of infected computers
  - the active use of methods to combat the analysis of malicious code and attempts to gain control over a botnet
  - short-lived mass mailings of malicious code
  - **Effective use of Social Engineering**
  - the use of a range of methods to spread malicious programs and a gradual move away from the use of methods (e.g. email) which attract attention
  - using a range of modules (rather than a single one) in order to deliver a range of malicious payloads
  - Malware as-a-service

Source: Kaspersky Labs

TROJANS, TROJANS AND AGAIN TROJANS..



LATEST VIRUSES	Detection time
24 September 2008	
Backdoor.Win32.Rbot.ups	09:50
Backdoor.Win32.Hupigon.eani	09:49
Trojan-GameThief.Win32.OnLineGames.tkiw	09:49
Trojan-Downloader.Win32.Zlob.zow	09:49
Trojan.Win32.Buzus.yzi	09:49
Trojan.Win32.Sadenav.pj	09:49
Trojan.Win32.Monder.qdm	09:48
Backdoor.Win32.Hupigon.eanh	09:48
Trojan-GameThief.Win32.Magania.aeig	09:48
Backdoor.Win32.Hupigon.eang	09:48

Source: Kaspersky Labs

ANOTHER WAY TO VIEW THIS TREND.

MALWARE & PUP UNIQUE FAMILIES FROM 1997 TO 2007

..AND THIS TREND FROM 2008 TO 2009 IS EVEN WORST..

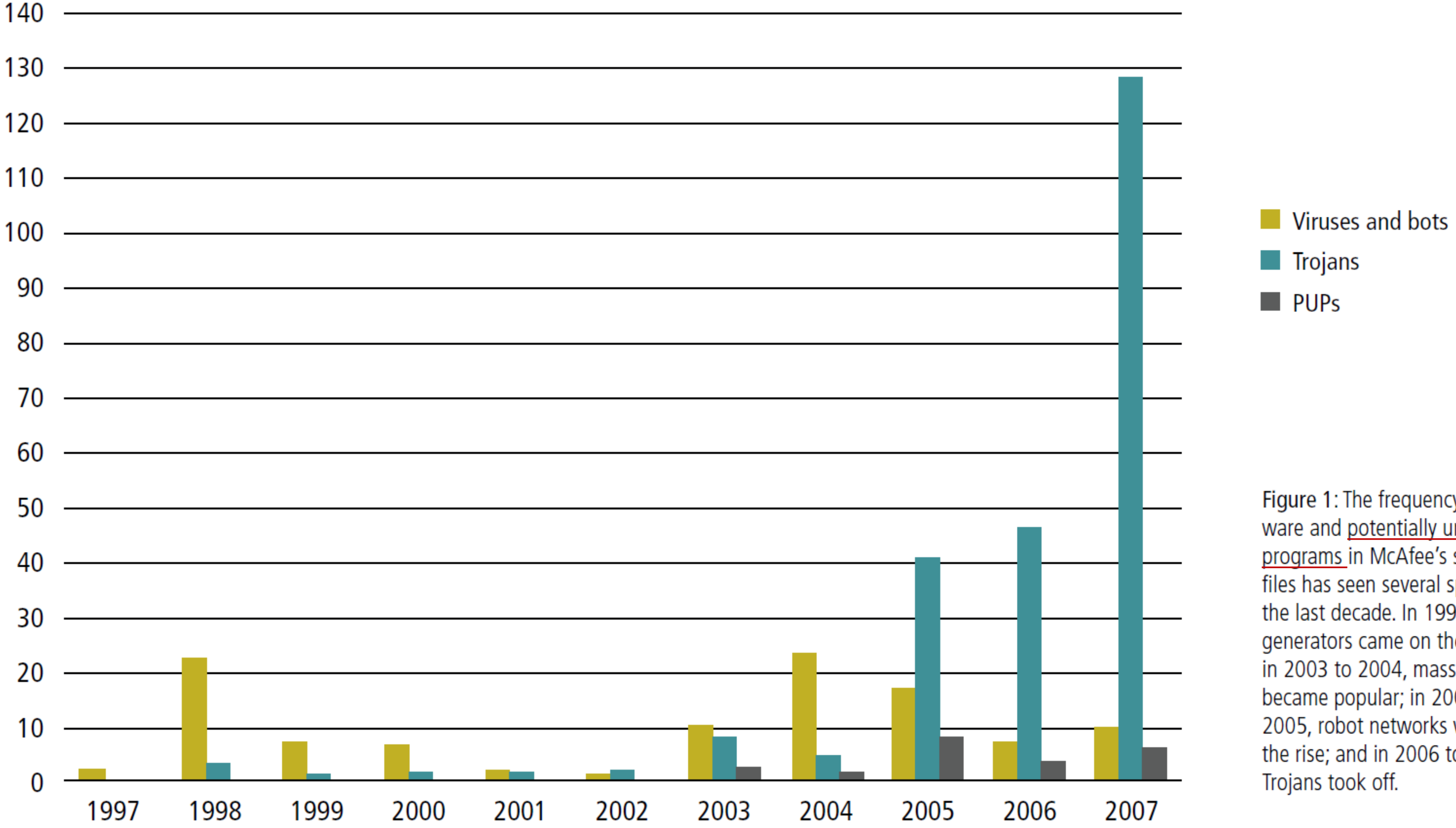


Figure 1: The frequency of malware and potentially unwanted programs in McAfee's signature files has seen several spikes in the last decade. In 1998, virus generators came on the scene; in 2003 to 2004, mass mailers became popular; in 2004 to 2005, robot networks were on the rise; and in 2006 to 2007 Trojans took off.

Source: McAfee Journal

WHY THIS UNDISPUTED DOMAIN OF TROJANS?

- Trojans are not (usually) able to infect the machine on their own, the user must be convinced to follow the hook and perform an attack task (click on a link or execute an attachment).

- User (or victim) must be convinced to do an action
  - The hook must be good enough
  - The message must be convincing

- **The cognitive models of any person could be (ab)used.**

- Social Engineering is the science needed to do this important task:
  - The dawn of Social Engineering 2.0
    - SPAM and modern phishing (eg. Spear Phishing)
    - Strong contextualization of hooks (eg. Using social networks or linked-data)

Take advantage of common weaknesses

- People don’t understand the technology
  - Online Viewer Exploits
- People caught off guard
  - Phishing
  - Snail mail phishing
- People trust other people
  - Hijack domain: typosquatting
- People trust the system
  - Hacking RFID, telefonia
- People in a hurry
  - ATM scam
- People get careless
  - Social engineering, easier than it sounds…

Source: Forgotten, sorry! But was taken from a two years ago conference

The essential change with modern malware is that the human element could be exploited **even for automated attacks**

How can we model and handle the human problem?

Which approaches have been tried so far?

AN EARLY APPROACH: MEMETICS

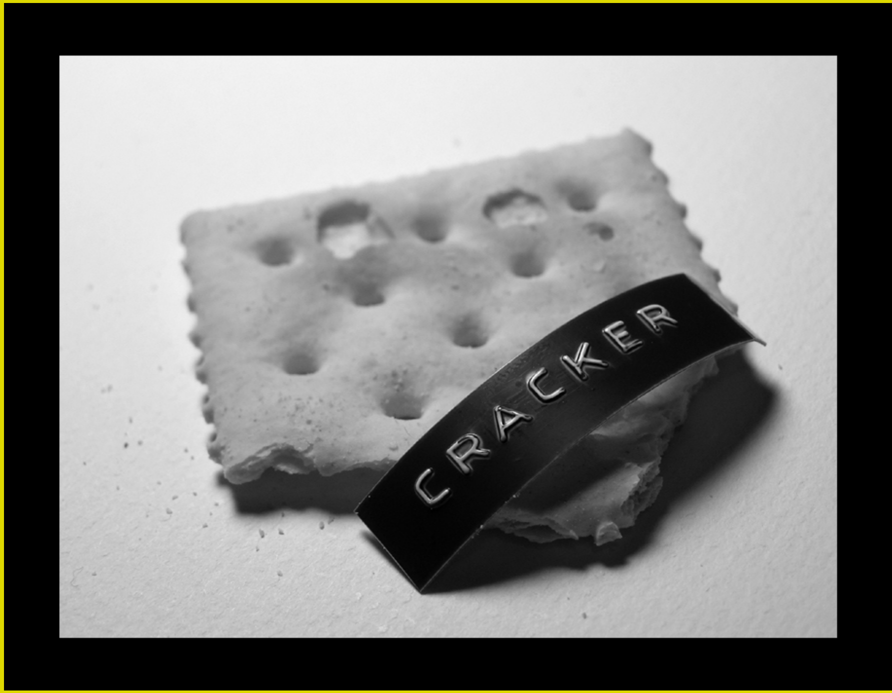
- **Memetics is a science that studies how memes (ideas) spread and evolves**.
- "Meme" is an abbreviation of "mimeme" a greek word that means «imitation», it is the cultural equivalent of gene for biologists.
- It do exists a powerful analogy between the transmission and evolution of memes and the transmission and evolution of genes.
- The memetics is a «science» that applies the Darwinian evolution law (Universal Darwinism) to ideas transmission and evolution.
- This idea is really useful to model Social Engineering attacks:
  - Virus of the mind, R. Brodie
  - Why Phishing Works, J.D. Tygar
  - "Whatever Happened to the Unlikely Lads? A Hoaxing Mmetamorphosis", D. Harley, R. Abrams, Virus Bulletin Conference, Sept 2009

BUT..

Memetics is still not widely accepted by psychologists and cognitive scientists

- *“Darwinizing Culture: The Status of Memetics as a Science” R. Aunger*
- *“The Meme Machine”, S. Blackmore*

- Memetics is handy and easy to understand
- Cognitive Science is a better methodological approach



ANOTHER APPROACH: CYBERSKEPTICISM

- **«Cybersketicism: The Mind’s Firewall”**
  - It is taught to US Army
  - Quite effective way of thinking
  - Good for your own mind shaping process
  - Needs a previously well performed motivation phase
  - Almost a technique (a mental framework) rather than a theory

Practicing cyberskepticism. (US Army)

STRUCTURE OF THE PRESENTATION

- How psychology contributes to security
  - malware 2.0
  - Memetics what else?
- Our approach to Social Engineering
  - Social engineering 2.0
  - Cognitive approach
- An early study: Mobile World and SMSishing
  - Results
  - So far..
  - What’s to come..

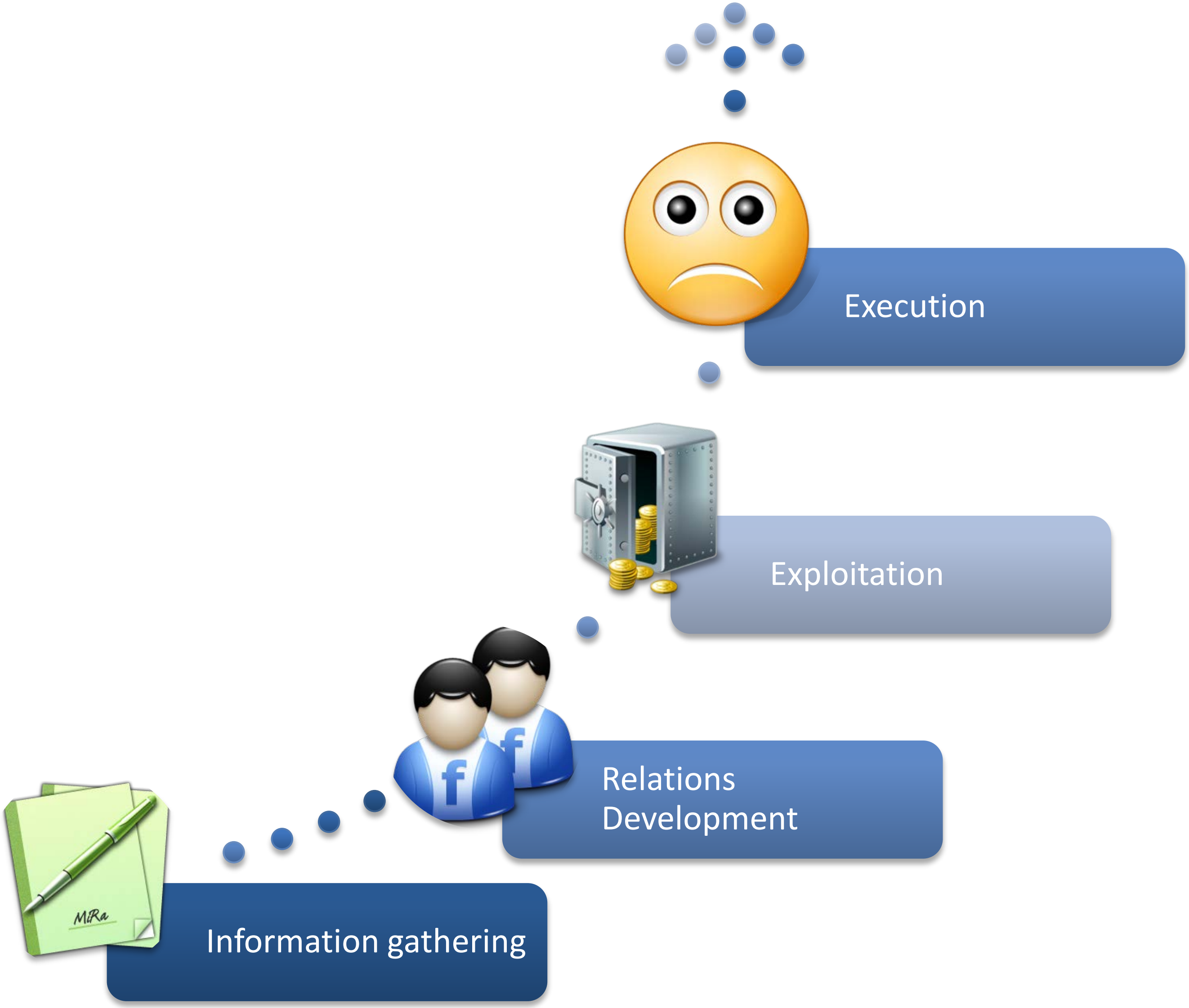
STATUS OF DETECTED ATTACKS

- "Complex" attacks, or innovative evolution of attacks techniques are seldom observed
  - Spear phishing, smishing, complex social attack are techniques rarely detected at the moment
  - All the recent reports state that this is going to change soon

- It's the right moment to study them and develop countermeasures!

INTO MODERN SOCIAL ENGINEERING

PHASES OF AN ATTACK



Information gathering

Relations Development

Exploitation

Execution

INTO MODERN SOCIAL ENGINEERING

WHAT MAKES SE 2.0 DIFFERENT FROM SE 1.0

Malware Ecosystem 2.0

- SE is a fundamental part of the malware 2.0 spread policies and tactics

Automatic Social Engineering Attacks (ASE)

- Automation of SE attacks is now possible thanks to mining and gathering spiders on Social Networks and Automatic Sentiment Analysis tools (semantic analysis of data)

Chat-bot

- Chat-bot are already used since years with IM systems, but social engineering attacks give them a second youth. For example for ASE attacks to create relations into mass social engineering attacks.

Predominance of Mail attack vector

- Predominance of mail above all the other attack vectors (presence, phone, fax,…). The advantage is that less “personal” talent is required and more victims are available and automation is easy

Abuse of linked-data

- Several Public Bodies (Web of Data vs Web of Documents) is rapidly moving toward the free and shared widespread diffusion of data. This is happening thanks to semantics and the Linked-Data. These information if abused are an huge source for social engineering attacks (for the information gathering phase);

Psychology (ab)use of personality profiling and cognitive models

- Professional and less pioneering use of memetics and, most of all, of psychological models of the attack victims

Economic Drivers

- Like Malware before, Social Engineering is out of its romantic phase and is now a professional tool for cybercrime

STRUCTURE OF THE PRESENTATION

- How psychology contributes to security
  - malware 2.0
  - Memetics what else?
- Our view of Social Engineering
  - Social engineering 2.0
  - Cognitive approach
- An early study: Mobile World and SMSishing
  - Results
  - So far..
  - What’s to come..

OUR WORK

- To perform this study we used a pure cognitive approach to our phishing attacks
  - To further stress this, the attacks has been created by a cognitive science student and not by a technical skilled attacker.

- The study targeted about 5000 employees of four different corporations
  - SMSishing
  - Phishing

- Complete results will be published. This is a preview of only those about SMSishing

WHY DO WE STARTED WITH MOBILE TERMINALS?

- **WIDESPREAD**

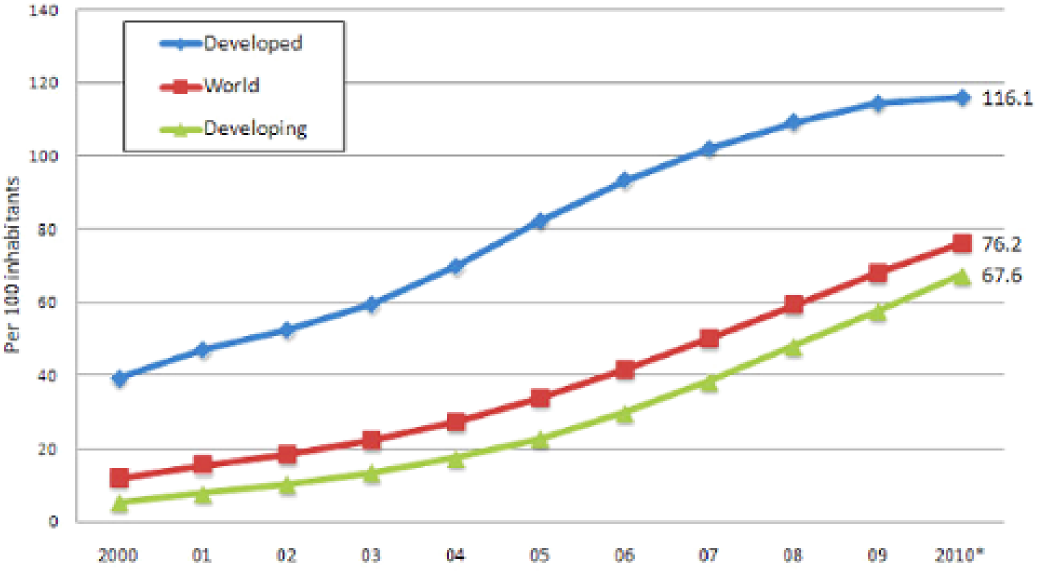
  Currently mobile phone are the most common communication devices in the world

  Sources: Akamai, The State of the Internet, 1st Quarter, 2010 Report

  5 billion SIM active - Ericsson Observatory, July 2010

- **CROSSCULTURAL**

  Phones in the last 10 years has had the largest circulation in both developed and developing countries.



- **CONNECTED**

  This year the number of internet connections from mobile devices exceeds fixed connections

  Source: ITU (International Telecommunication Union)

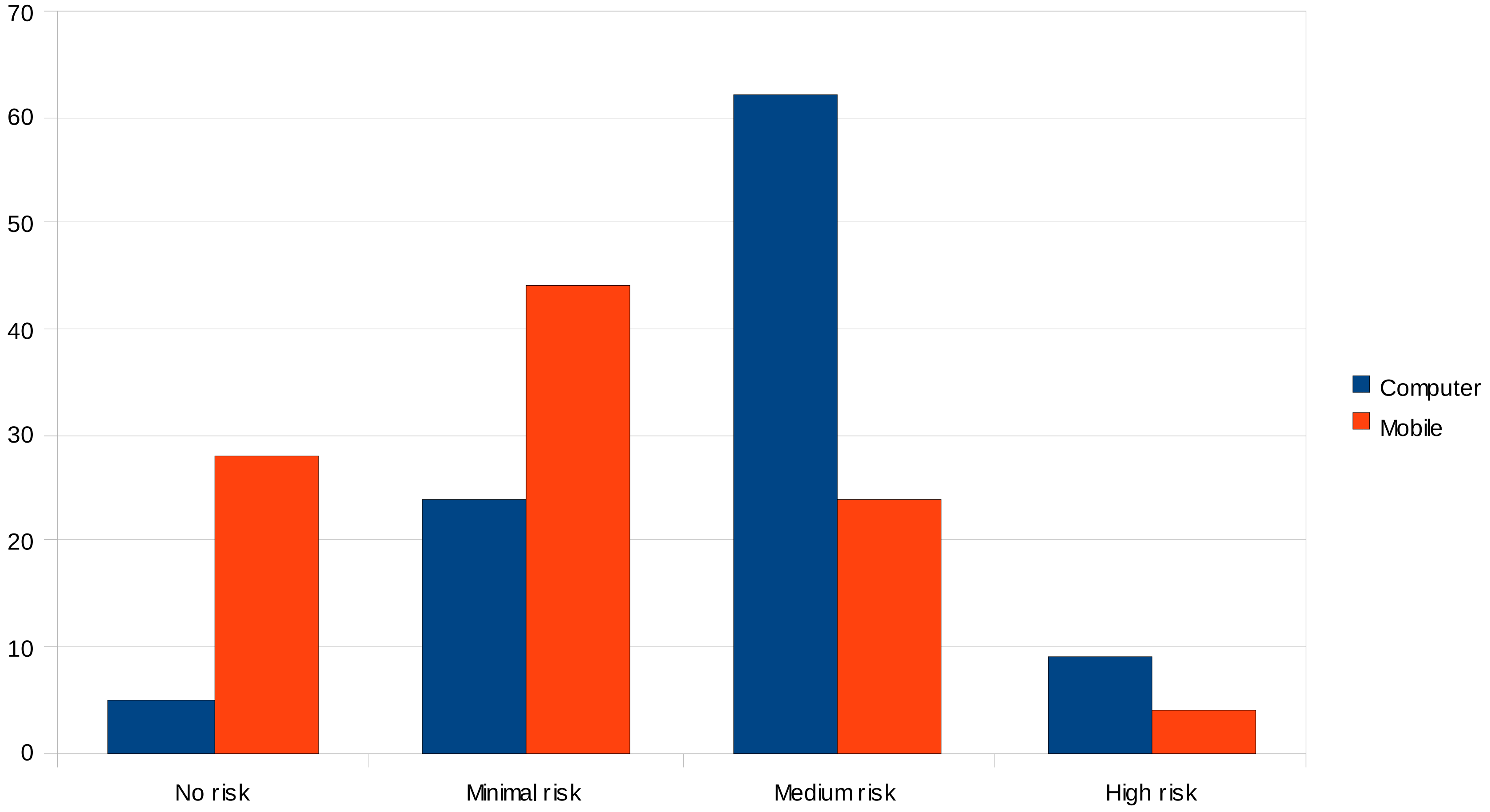
WHY MOBILE TERMINALS ARE SO IMPORTANT?

- By the cognitive point of view the advantage are:
  - Utility
  - Easy of use
  - Lack of required resources

- By the functional point of view the evolution has been:
  - Device to make only calls
  - Device occasionally connected
  - Devices permanently connected

WHICH IS THE MOST IMPORTANT COGNITIVE PROBLEM?

- The perception of safety a comparison between computers and mobile phones (results of our own survey | 400 answers)



METHOD AND TEST

- We needed a benchmark
  - On the same population we performed 3 similar tests on PCs and mobile terminals
- Test 1: Slightly contextualized mail
  - a company new SOS password service
- Test 2: Quite generic spam
  - special discounts for company’s employees
- Test 3: very slightly contextualized spam on SMS
  - request to upgrade the terminal

FIRST TEST: RUN ON PC/LAPTOP

!!! please don't reply [automatic mail] !! !

Dear user,

You've recently joined the company and have been issued a Corporate Intranet Login and a fist Corporate Intranet Password that you generated. A web interface, SOSPassword, is at your disposal to give you more autonomy when managing your passwords:

http://ITservices.$corporation/sospassword@123.456.789.0

SOSPassword enables you to change and synchronize on line the password.

For an easiest synchronization, the password expire after 120 days.

ADVANTAGE:

You won't have to call the helpdesk when you have forgotten your passwords or when they have expired, you can manage the change yourself in SOSPassword.

FOR YOUR FIRST USE OF SOSPASSWORD:

Log into SOSPassword with your Corporate Intranet Login and Corporate Intranet Password (only at first use) and create your 5 individual questions/responses

[e.g. Your Favorite book, your maiden name, Your dog's name, etc]. These questions will then be used to authenticate you for future connections to SOSPassword.

TIPS:

- Add the URL to your favorite:
http://ITservices.$corporation/sospassword@123.456.789.0
- Read the FAQ and Download the available User Guide.

We thank you for your cooperation.

(C) 2010 CEFRIEL & Università Statale Milano

SECOND TEST: RUN ON PC/LAPTOP

Dear Colleagues,

As many of you already know our company has been engaged in a campaign

aimed at providing benefits to their employees in the form of rebates and discounts for goods and services provided by Ns. partners.

As I'm sure you already know a few weeks ago, the Apple computer company known around the world, unveiled its flagship long-awaited, the famous iPad.

Under a business agreement signed by us with some vendors, all Ns. Employees will have the opportunity to enjoy a discount of 40% of the cost of this jewel of technology.

Many security systems include a request to retrieve your password, these questions usually standardized, tend to deal with specific difficult for an outsider to discover what colors and favorite foods, first name or names of relatives and the like. Providing this information increases the chances of an attacker to access other systems.

To take advantage of this and other great offers you only need to register in the database of our official supplier, through this link:

http://$openservices/$corporation/offers

necessarily using the corporate email.

Is invited to make such entry is absolutely free and without any obligation to buy.

Regards

Office of Human Resources - $corporation

NB: subscribe to the service indicated in this message requires more than a personal ID (must mail the company) the choice of a password. For security reasons you can not use the same password as that used for access to their corporate account.

THIRD TEST: RUN ON MOBILE

!!! please don't reply [automatic SMS] ! ! !

Dear user, for enforcing IT mobile defenses, your terminal must be upgraded. A new tool from IT internal service is available in the Intranet IT section.

For upgrade, please use this link:

http://ITservices.$corporation/securitypatch@123.456.789.0

We thank you for your cooperation.

IT Security Services - $corporation

WHICH PSYCHOLOGICAL EFFECTS WE USED..

- **These tests were built stressing two basic behaviors**

- **Assumption of truth (truth-bias)**: People are used to evaluate facts using an heuristic process (non Bayesian thinking) which is largely incomplete. Initial facts are integrated with assumptions «a priori» in a not analytic process.

- **Stereotypical Thinking**: people's judgment is often done comparing events against their own model. The most common is the thief's stereotype. An updated version is the **phishing mail stereotype** (e.g. syntax errors and semantic inconsistencies in the text).

Founding studies come from psychology, cognitive science and marketing techniques

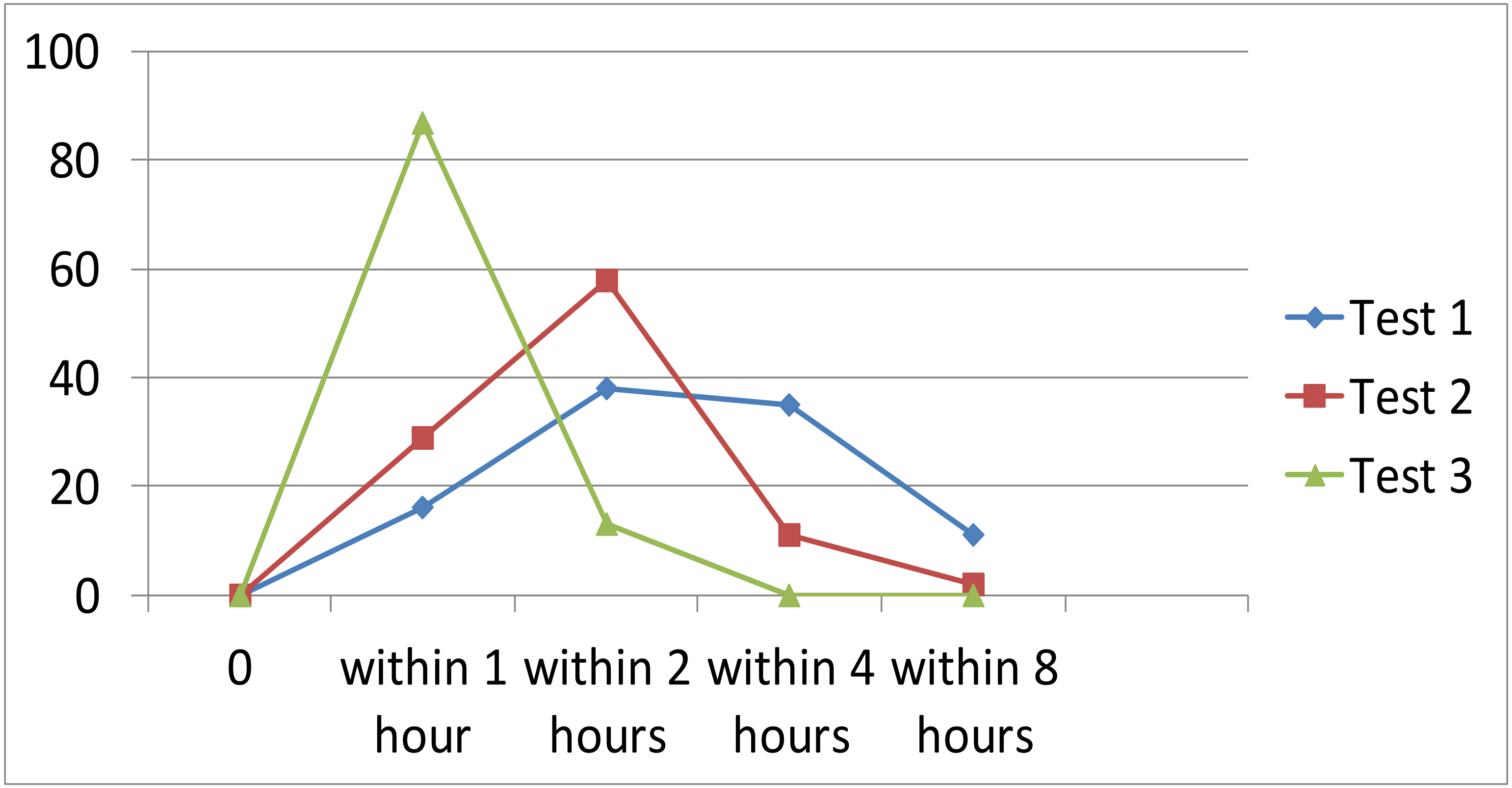
GLOBAL RESULT OF THE EARLY TESTS

	# failure	% failure
First test	531/4936	10.67%
Second test	280/4936	5.67%
Third test	168/820	20.49%

Population tested against SMSishing

- **Gender**: 551 male | 269 female
- **Age**: 12 under 30 | 370 over 30 and under 50 | 438 over 50
- **IT skills**: 716 low | 104 high
- **Work organization**: 307 alone | 167 team | 346 group
- **Trainings**: 105 humanities | 290 scientific | 242 technical | 80 language | 103 other

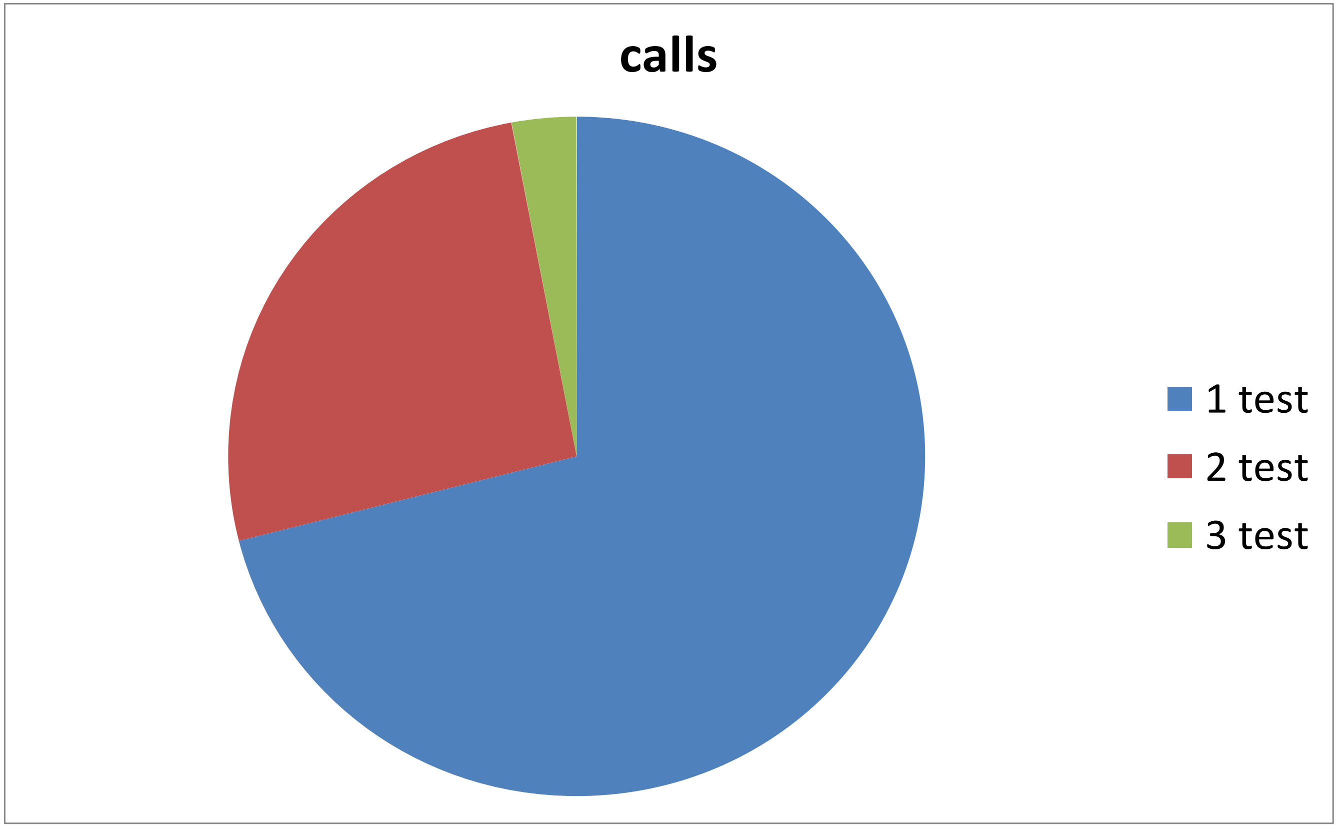
- Graphical comparison between the reaction times



- SMSishing is “faster” than phishing

SOME STATISTIC: CALLS TO IT CENTER

- Graphical comparison between callbacks to IT Center



- SMSishing originated far less doubts

QUESTIONS: WHAT MATTERS A LOT?

- Question 1: Does team working matter?

	% failure (general)	% failure (team-working)
First test	10.67%	9.77%
Second test	5.67%	4.92%
Third test	20.49%	19.76%

- Answer: The phone belongs to the private sphere (the team does not work).
- Question 2: Does linguistic competencies matter?

	% failure (general)	% failure (linguistic background)
First test	10.67%	7.53%
Second test	5.67%	3.35%
Third test	20.49%	21.25%

- Answer: The phone carries too few data (linguistic expert don't have advantages)

QUESTIONS: DOES TRAINING WORK?

- Question 3: Does classical training works with mobile users?

	% failure (general)	% failure (post training)
First test	10.67%	4.41%
Second test	5.67%	2.11%
Third test	20.49%	16.94%

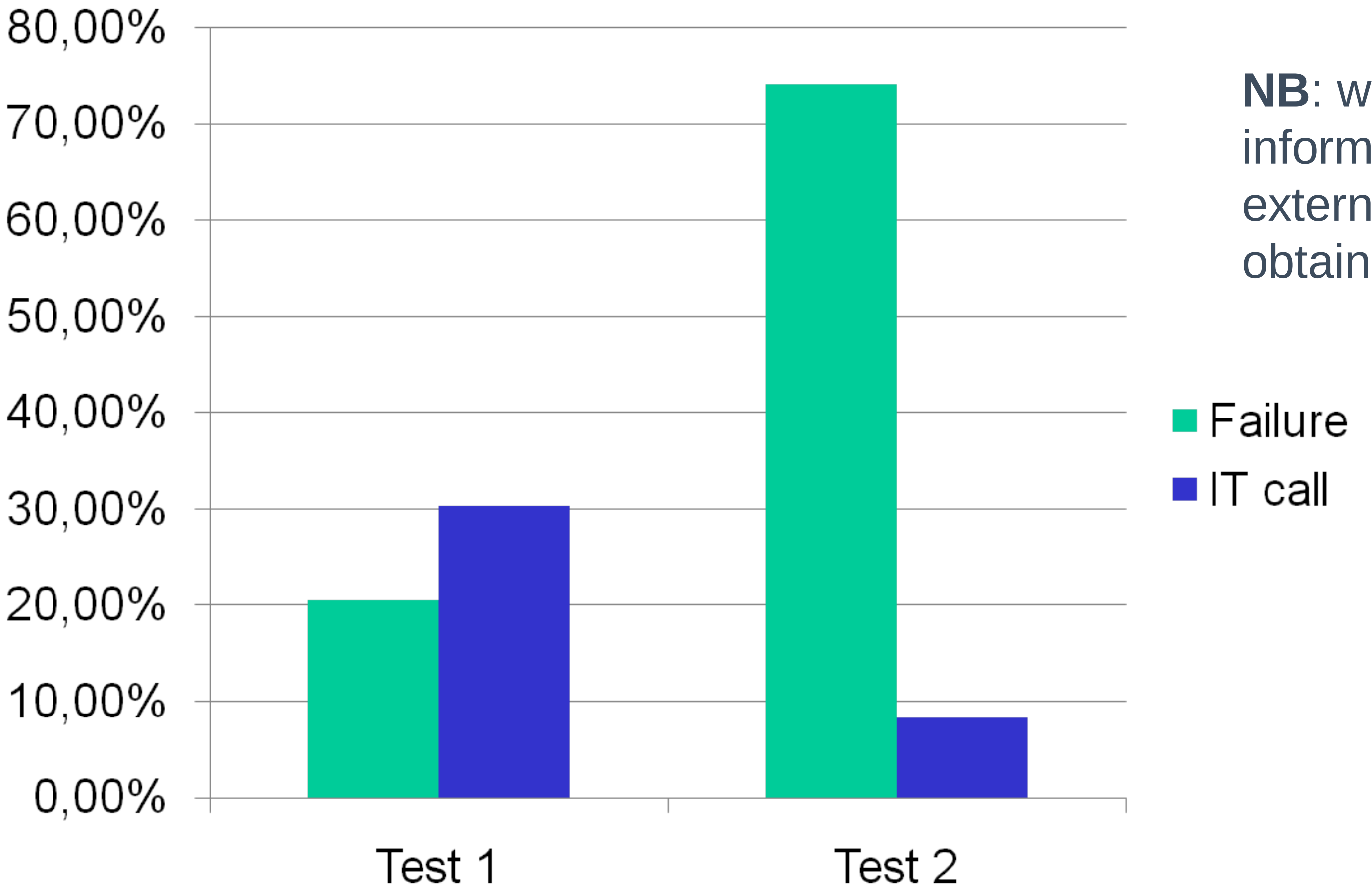
- Answer: Training performed poorly for mobile terminals
- Question 4: How long training results last?

	% failure (general)	% failure (3 months later)
First test	10.67%	5.83%
Second test	5.67%	3.09%
Third test	20.49%	17.27%

- Answer: differences reside in the cognitive processes, the training despite performing poorly lasts longer

QUESTION: WHICH IS THE PERFECT ATTACK?

- Fourth test: a contextualized SMSishing message
  - Test1: an SMS using a contextualized hook but non standard look
  - Test2: An MMS using also the Corporate's look and logo



NB: we only used information that any external attacker might obtain

WHAT’S TO COME: COUNTERMEASURES

- Technical approach (block the terminals)
  - Pros: easy to implement
  - Cons: professional users don’t want blocked terminals, easily circumvented on most mobile platforms
- Cognitive approach (understanding the complexity of the terminal interactions)
  - A wikinomics strategy proposal: a company guided collaborative peer-to-peer strategy for learning best practices
  - Early results on a pilot test dropped failures from 20.49% to a promising 13.98%
- Try new learning procedures starting from the Neurocognitive Sciences
  - Exploit beneficial effects of stress on learning processes
  - “Multisensory” learning
  - Using error theories developed for other sectors like for Medical Error Prevention

- Thanks for your attention-

M-For-Mature
By: Alex Miller
Little White Lies
Oh yeah, baby. Work it. Work it good.
You know what Daddy likes...
Huh? What's this?
"Download all the hardcore action you can handle. Click here."
This sounds legitimate.
Click!
This is the worst Trojan/Malware infection I've ever seen. What were you doing on this thing?
Solitaire. I was...I was playing solitaire.