Deloitte.

Deloitte Hungary
Bronz Medalist
Global Cyberlympics 2012

Cyber security
Where does the world go?

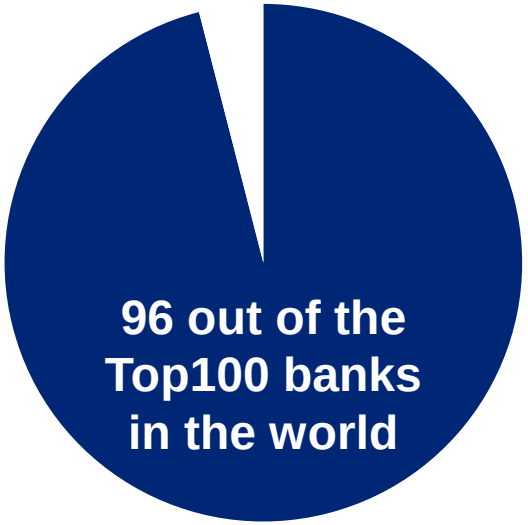
20ht November 2013

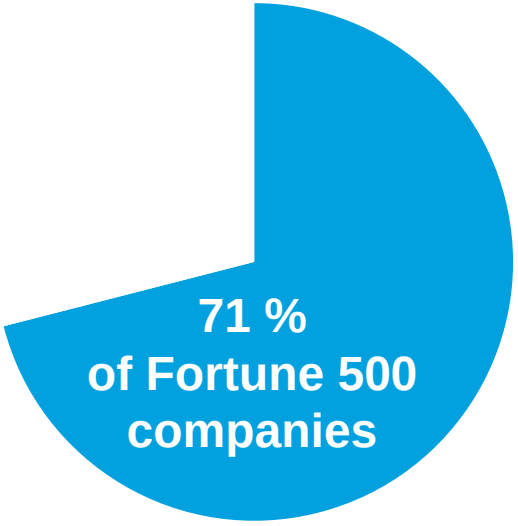
Some history

Early days	Since we started using computers and store data electronically, there are **people** who **attempt override controls in order to access these data with malicious purposes.**
60`s	Computer crime was mostly related to **physical damages**, though **some programs** were developed that formed some similarities with early days of viruses.
70`s	**First** program really considered as **virus was Creeper**, running on TENEX – PDP-10. Traditional computer crime mostly focused on **unauthorized manipulation of data.**
80`s	**Personel computers** started their widespread and so did the **copyright breaches and other computer crimes.** **Remote access** to computers got a different approach to crime, i.e. a crime could be committed from a remote location.
90`s	**Computer crimes diversified and so did the attack methods:** DoS, automated scanners, key loggers, password crackers, www attacks etc.
21th century	**WANs, wireless technologies, mobile technologies etc.** However, several `old` methods still remain in a new and modern format.

An `old system`

In 2013…





use this:

A while ago when life was simple

1998

- Vulnerabilties, vulnerabilities, vulnerabilities
- Infrastructure security was a big driver
- Dshield, packetstormsecurity
- Classic network-based pentests (later called infrastructure pentest)
- War-dialing

1999 - 2002

- Web-app testing
- Improving the security of your site by breaking into it
- Lack of knowledge around secure app development
- Levin the hacker
- Infrastructure security was still not much in focus – almost sure that xspy worked
- In 2000 / OSSTMM and pentesting is getting a bit more known
- Tools like nmap, superscanner, nessus were the most popular
- Metasploit
- john-the-ripper

2003 - 2004

- WiFi – aircrack, kismet – war-driving
- OWASP established
- Threat modeling, threat agents
- SDLC

Not so long time ago when life became not that simple

2005 - 2008	• More distuingished pentest phases – internal/external – infrastructure/app • Physcial site control • Phishing – social engineering • Demand for binary app testing (mainly legacy apps) • DoS attack in Baltics
2009 - 2011	• SCADA testing (2010 stuxnet) • Testing the human factor became more popular / awareness • Still breaking in via lack of proper input control
2012 - 2013	• APT and related testing • Mobile apps • DDoS • Still breaking in through weak apps and insecure infrastructure, though the latter became less frequent

Cyber

Cyber attack

under certain conditions is considered in some states as an act of war

Cyber war – Cyber terrorism – Electronic warfare

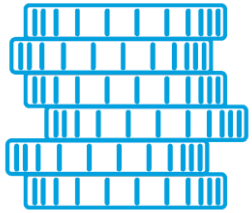
Cyber crime – E-crime

Botnets, Phishing, E-scams,
Identity theft

Source: militarypictures.info

What is the size of the problem?

20 %



20% of all information technology costs is spent on cyber security.

Office of Management and Budget - USA

100bn $

Annual cyber security costs are around USD 100 billion.

Center for Strategic and International Studies

165bn $

By 2013 the market of cyber security solutions will increase to USD 165 billion.

Strategic Defense Intelligence

Avoid `Cyber Pearl Harbor`

What is the size of the problem?

Cost of cybercrime

Type of crime	Estimated cost	% of GDP	Source
Global, in USD			
Piracy	**1-16 billion**	**0.008-0.02**	**IMB**
Drug trafficking	**600 billion**	**5**	**UNODC**
Global cybercrime	**300-1000 billion**	**0.4-1.4**	**Many sources**
Only USA, in USD			
Car related crime	**99-168 billion**	**0.7-1.2**	**CDC, AAA**
Theft	**70-280 billion**	**0.5-2**	**NRF**
US cybercrime	**24-120 billion**	**0.2-0.8**	**Many sources**

IMB=International Maritime Bureau
UNODC= United Nations Office on Drugs and Crime
CDC= Center for Disease Control and Prevention
AAA=American Automobile Association
NRF= National Retail Federation

Source: Center for Strategic and International Studies and McAfee - Aviation week

Cyber attacks

Direct attack against companies:
- DDoS
- Industrial espionage
- APT - e.g. RAT

Organized crime:
- Techinal
- Legal
- ML

Attacks from the `client` side:
- Online fraud
  - web
  - mobile

Internal threats:
- Data leakage
- Sabotage

Custom malware
zero days
social engineering

Long lasting cyber stories

The Citibank case

Владимир Левин (Vladimir Levin) attacked Citibank Cash Manager system in 1994.
He later was cought by the police and got arrested. According to the case documents, he managed to steal 10.4m USD and transferred this money to accounts in Finnland, USA, Israel, Netherlands.

In 2005 a completly different story came up, when ArkanoiD published the full story to provider.ru.

Long lasting cyber stories

Carberp

Carberp is one of the most well-known botnet:

- Running exploits
- Making codes persistent
- Making c&c to operate
- Plugin for data theft
- Other tools

Carberp was about USD 40,000 to purchase, then anyone could subscribe to it for a monthly subscription fee (USD 2-10k).

This July, the source code `leaked` as well as the botnet generating tool.

Long lasting cyber stories

Zeus

- **Original Zeus start-kit** — **4,000 USD**
- **Windows7/Vista compatibility modul** — **2,000 USD**
- **Back-connect modul** — **1,500 USD**
  The criminal may reconnect to the victim`s computer and may perform e.g. a bank transaction.
- **Firefox form grabbing** — **2,000 USD**
  Able to thief data in cells, e.g. account names, passwords
- **FTP client saved auth. data collecting modul** — **2,000 USD**
- **VNC modul (not supported in the future)** — **1,0000 USD**

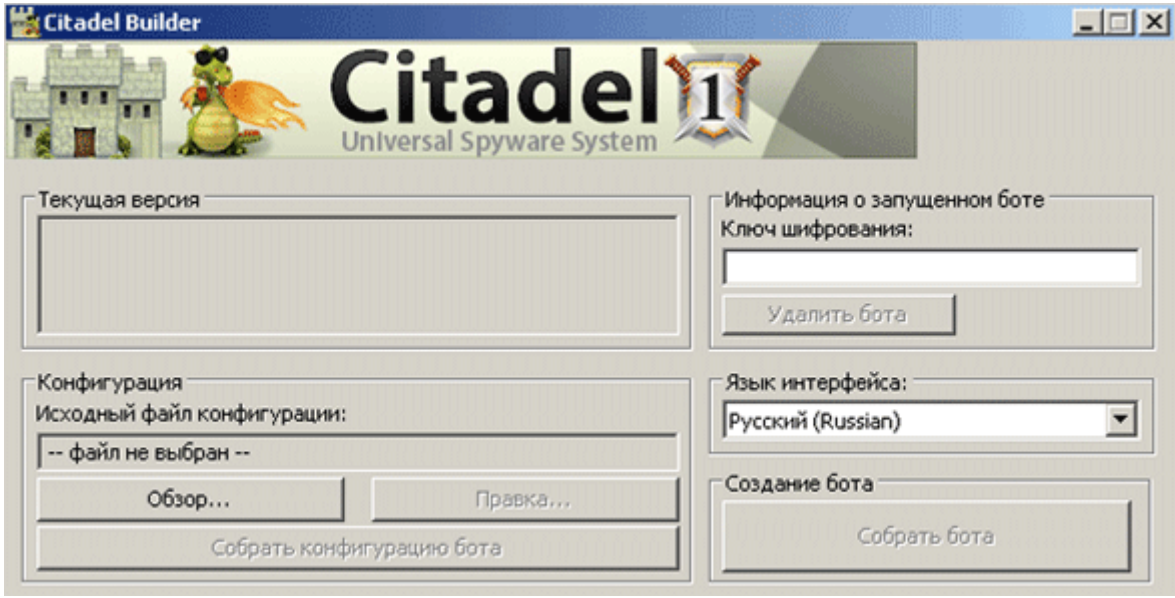
However, SpyEye only costs USD 500.

(Plus, the new Firefox injection modul is additional USD 1,000)

Long lasting cyber stories

Citadel

- Started as a Zeus v2 trojan (January 2012), but its `features` and its `service` exceeded all previous `solutions`.
- The first malware with fully comprehensive client service (Fraud as a Service).
- Their sales model has changed recently, the goals are:
  - Less but `trusted` clients
  - Less sales



Long lasting cyber stories

Eurograbber

- A trojan variant of Zeus
  (built on Zeus, SpyEye and Carberp trojans)
- Since August 2012
- In 2012, it caused more than EUR 36 million for banks and bank`s clients
- More than 30,000 corporate and private bank accounts were
- Very sophisticated way of attack

Long lasting cyber stories

TeamSpy

- Spear phishing / Social engineering
- Trojan and malware
- Interaction
- Persistent connection

The TeamSpy case

- 20th March, 2013 / Kaspersky report on TeamSpy
- Covert cross-nation, cyber surveillance data theft and monitoring operation
- Contains Cyrillic language
- Default character set cp1251
- c&c domain names refer to Belarusian and Ukrainian words
- Some c&c domains registered in 2004(!!)
- First known report of runtime patched Teamviewer in May 2012
- Potentially active since 2004, but from 2008 definite

Long lasting cyber stories

The Euronet case

Reuters - Payment processor Euronet Worldwide Inc said a "small portion" of its European business was the target of a criminal security breach late last year, sending its shares down as much 6 percent. It affected Euronet's processing business, which is around 5% of their total revenue.

Euronet Chief Executive Michael Brown:

"*When we heard the first little inklings of this, we jumped in, figured it out, got third parties involved who are real experts at this, and closed the breach... between our discovery and our shutdown, it wasn't a long period of time.*"

About the delay in disclosing the incident, Mr. Brown said it was not a severe breach.

"*Maybe the reason a lot of people didn't make a big deal about it, is just because the severity wasn't as bad as some other people have seen... We had a limited amount of bad activity and we've been free and clear for over a month.*".

A hack attack` s effect on the stock exchange

AP Twitter feed hack

Long lasting cyber stories

Ransomware – the security threat yet-again

- The first ransomware appeared in 1989: named AIDS or PC Cyborg
- The author (Joseph Popp) requested USD 189 from his targets to unlock their computers from the unsolicited encryption. He made several mistakes – among others a technical mistakes well.
- The victims of CryptLocker are not so lucky. The virus appeared in 2013.

- **The `hardest` part is always the money…**
- A money laundering network was submerged in the summer of 2013. The investigation showed that USD 6 billion was laundered by the network and they had about 1 million clients.

Mobile security

Top 10 mobile threats

1. The mobile device attack surface is narrow but deep
2. Mobile malware is going to grow up
3. An application store is not a security model
4. You will lose devices, you will lose data
5. Who owns the device? Who owns the data?
6. Channel security is complex
7. Mobile device security solutions are immature
8. IT has less control in a mobile world
9. Exercising tight control has its downside
10. Lack of a formal strategy invites chaos

What can you do?

- **Prepare for the `worst`**
  The question is not if you are going to be attacked but when?
- **Knowledge**

  A high-caliber attack can be only `warded off` with high-caliber tools. You need to have deep knowledge about the used techniques, rather in less areas but with high expertise. Practice and research is crucial for professional development.