



## Social Media Malware Problems +1

*Eddy Willems*  
[Eddy.Willems@gdata.de](mailto:Eddy.Willems@gdata.de)

Go safe. Go safer. G Data.

## Agenda



- Introduction
- Some History
- Social Networks
- The Survey
- The Future



Go safe. Go safer. G Data.

## Introduction



- Involved in the industry since 1989
- Worked as consultant for several CERT-organisations and commercial enterprises like Westcon (NOXS) and Kaspersky Lab
- Security Evangelist at G Data
- Co-founder and Director Security Industry Relationships of EICAR
- Press officer at AMTSO



Go safe. Go safer. G Data.

## Introduction



- Established 1985 in Germany (Bochum): over 25 years old
- Privately owned
- Security-Pioneer: first antivirus solution in 1987 ... Atari
- Security solutions for end users and companies based on dual engine, cloud security, etc
- Available worldwide in more than 90 countries

Go safe. Go safer. G Data.



TIME

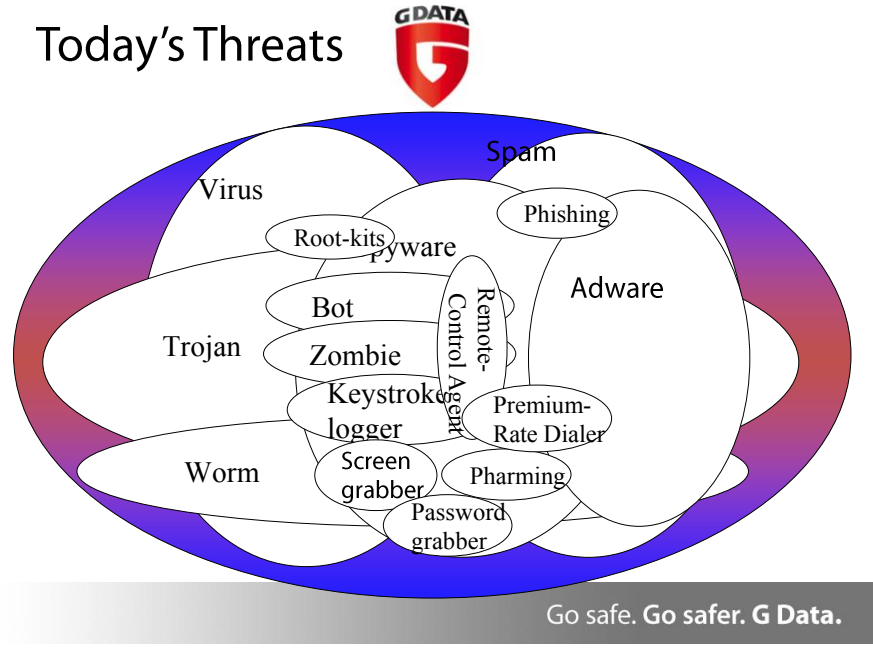
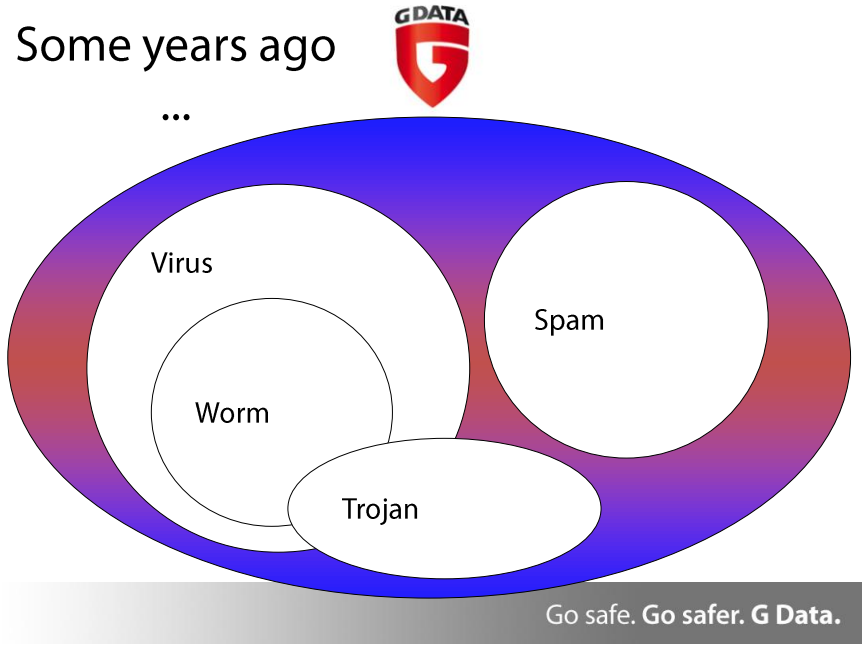
Go safe. Go safer. G Data.



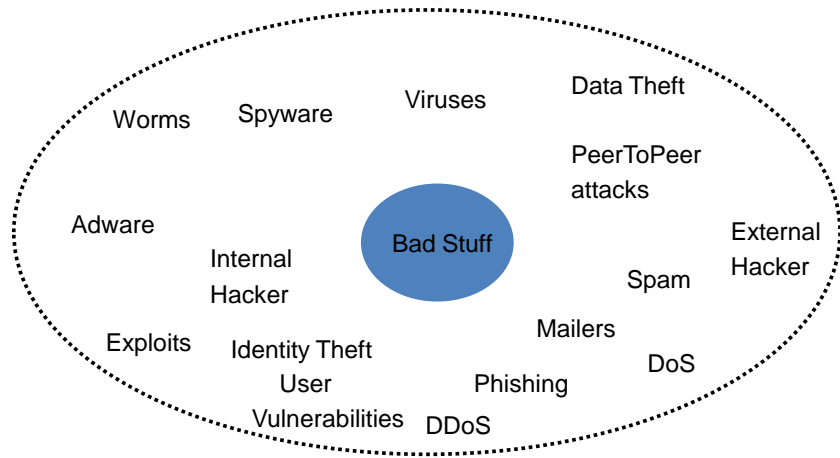
Some History: The old days !



Go safe. Go safer. G Data.



## What are the real threats ?

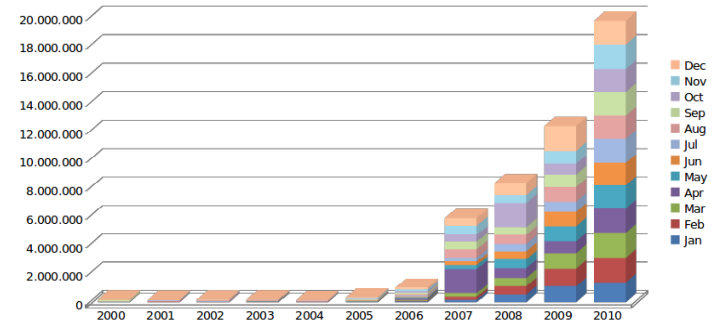


Go safe. Go safer. G Data.

## The Number Game ?



New unique samples added to AV-Test's malware repository (2000-2010)



New threats per day 60.000 ... Signatures are lower (malware also)

Counting every threat or just families of threats ...

Go safe. Go safer. G Data.

Social networks?



PHP tag CSS movies combination  
 Web 2..... XML mobility  
 AJAX Social Networks  
 socialize friends flexibility  
 blog

Go safe. Go safer. G Data.

The Good



- Working together, Socialize, Friends
- Fast, News, Gossip, Applications, Games
- Question: Who's on Facebook, Twitter? Who is using it over here?



Go safe. Go safer. G Data.

# The Bad: Twitter



twitter

Name or location search Home Find & Follow Settings Help Sign out

o\_o michelle1

Follow

Check out my new website  
[http://\[redacted\].m/g...](http://[redacted].m/g...)

2 days ago from web

RSS Older >

© 2008 Twitter About Us Contact Blog Status Downloads API Help Jobs TOS Privacy

GO SAFE. GO SAFER. G DATA.

# The Bad: Youtube



YouTube Broadcast Yourself™ Worldwide | English (0) Account | QuickList (0) | Help | Sign Out

Home Videos Channels Community Search Upload

CLICK HERE FORN PORN ==>

Rate: ☆☆☆☆☆ 0 ratings Views: 1,962

Share Favorite Playlists Flag

Send Video MySpace Facebook more share options

GO SAFE. GO SAFER. G DATA.

# The Bad: Facebook



Posts by Everyone

My total facebook views are: 5714  
Find out your total profile views @ <http://bit.ly/e1JCS8>  
4 seconds ago via Real Friends V4.5

My total facebook views are: 12035  
Find out your total profile views <http://bit.ly/g6lecf>  
7 seconds ago via Read The Words

My total facebook views are: 862  
Find out your total profile views <http://bit.ly/g6lecf>  
14 seconds ago via Read The Words

My total facebook views are: 1245  
Find out your total profile views <http://bit.ly/g6lecf>  
a few seconds ago via The FreshMen

My total facebook views are: 25406  
Find out your total profile views <http://bit.ly/g6lecf>  
a few seconds ago via Read The Words

**Request for Permission**

Pro Check+ is requesting permission to do the following:

- Access my basic information**  
Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've shared with everyone.
- Post to my Wall**  
Pro Check+ may post status messages, notes, photos, and videos to my Wall
- Access my data any time**  
Pro Check+ may access my data when I'm not using the application

Report App

Logged in as (Not You?)

Go safe. Go safer. G Data.

# The Bad: LinkedIn



**Jessica Alba naked**  
Jessica Alba naked at Company Net  
Albany, New York Area

**Current** • Jessica Alba naked at Company Net

**Industry** Aviation & Aerospace

**Websites**

- Jessica Alba naked PART 1
- Jessica Alba naked PART 2
- Jessica Alba naked PART 3

**Jessica Alba naked's Experience**

**Jessica Alba naked**  
**Company Net**  
(Privately Held; 11-50 employees; Aviation & Aerospace industry)  
Currently holds this position

**Additional Information**

Jessica Alba naked's Websites:

- Jessica Alba naked PART 1
- Jessica Alba naked PART 2
- Jessica Alba naked PART 3

Go safer. G Data.

## Vulnerabilities/ Problems



- Technology problem
  - Zero-day vulnerabilities
  - Lack of patches
  - Unlicensed software
- Human behaviour
  - Social engineering
  - Curiosity, naivety
  - Trust in friends
  - Lack of awareness

Go safe. Go safer. G Data.

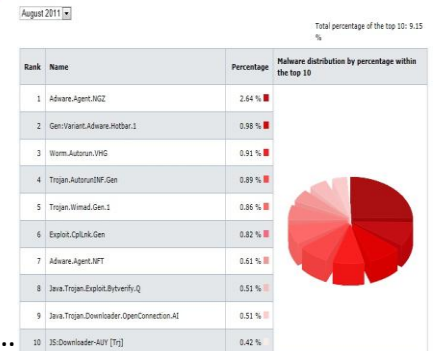
## Technology problems



Critical vulnerabilities:

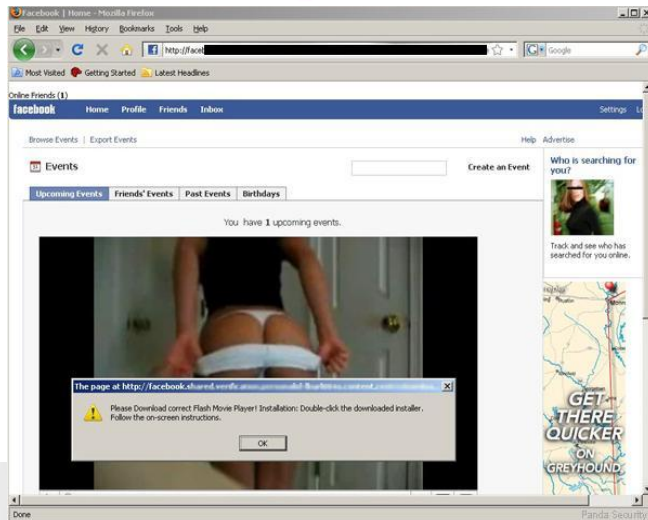
It is NOT only the OS like  
Windows

It is pdf's, flash, Java, etc ...



Go safe. Go safer. G Data.

## Human vulnerabilities

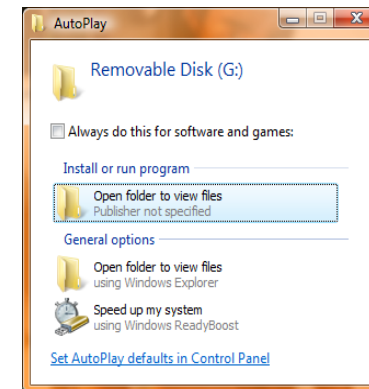


Data.

## Human problems

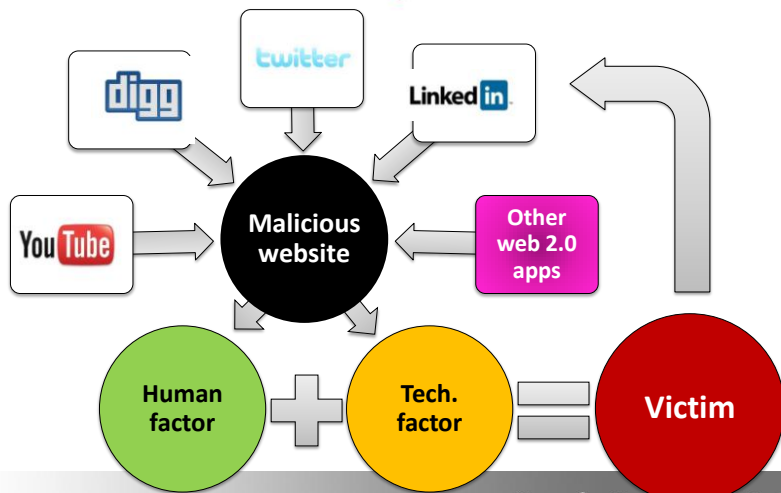


### Example: Humans and Kido/Conficker



Go safe. Go safer. G Data.

How does a web 2.0 attack work?



Go safe. Go safer. G Data.

Social networks and success rate



- Social Network attacks – very similar to how email worms used to spread
- Success rate of infection:
  - Rate factor 1 when spreading through email
  - 10 times higher when spreading through social networks
- Problems with social networks are not limited to malware
- Risk of personal information leakage which can be misused

Go safe. Go safer. G Data.

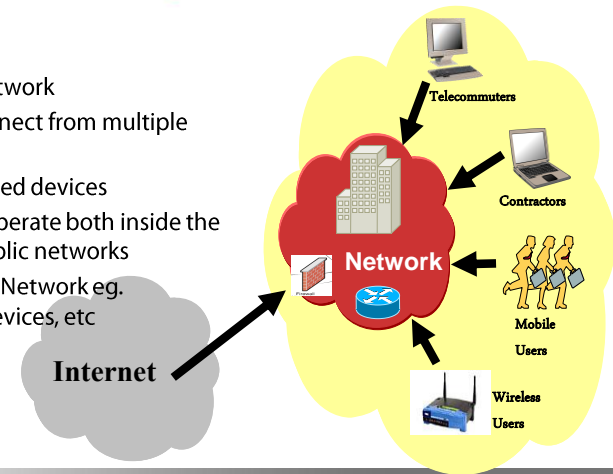
## Social networks and privacy



## Today's Networks Lack Boundaries



- Internal/External network
- Individual Users connect from multiple locations
- Managed/Unmanaged devices
- Individual devices operate both inside the network, and on public networks
- New Devices on the Network eg. Netbooks, Mobile devices, etc



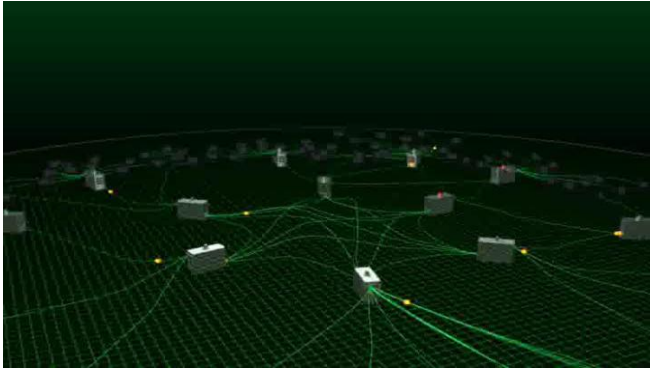
Go safe. Go safer. G Data.

Social Media  
... Clouds



Go safe. Go safer. G Data.

Botnets



Go safe. Go safer. G Data.

## Botnets



Botnet used for:

- DDoS's
- Spam, gathering data for Spam
- Phishing
- Stealing private data
- Ransoming
- Botnet renting
- Click fraud, BH SEO poisoning, etc

Go safe. Go safer. G Data.

## CyberCrime



- Profitability ✓
- Easy to do  
(technically and morally) ✓
- Low risk business ✓
- New services that are  
profitable to attack ✓



Go safe. Go safer. G Data.



# That's what we say?

Go safe. Go safer. G Data.

## The survey and other related problems



- **G Data** worked together with **SSI** a global provider of sampling solutions with an international staff of 400 people representing 50 countries and 36 languages with 6 million research respondents in 72 countries
- Our research was done online in 11 countries: Austria, Belgium, France, Germany, Italy, Netherlands, Russia, Spain, Switzerland, UK, USA
- Around **16.000 respondents** in 2011
- **Survey questions**= Brainstorm result of some brilliant minds inside G Data

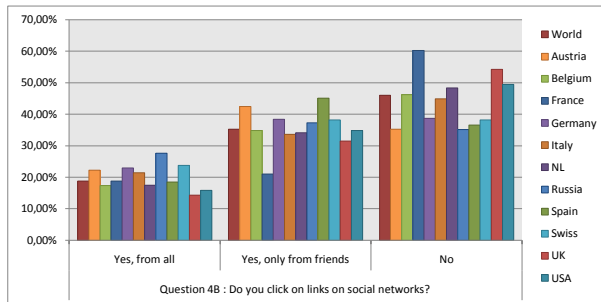


Go safe. Go safer. G Data.



One of the questions:

Do you click on links on social networks?

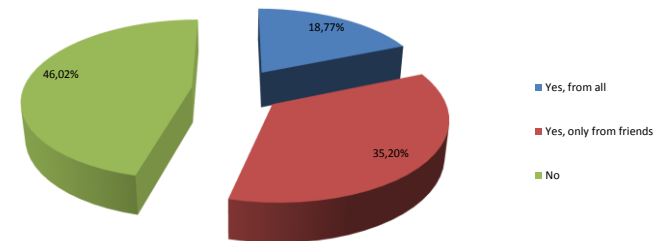


Survey results copyrighted by G Data

Go safe. Go safer. G Data.



Do you click on links on social networks?

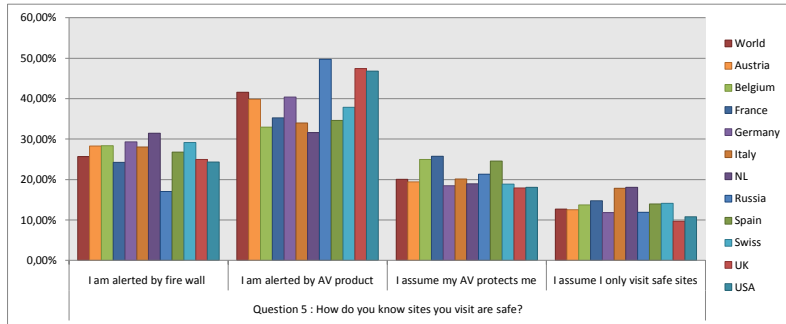


Go safe. Go safer. G Data.



Another question:

How do you know sites you visit are safe?

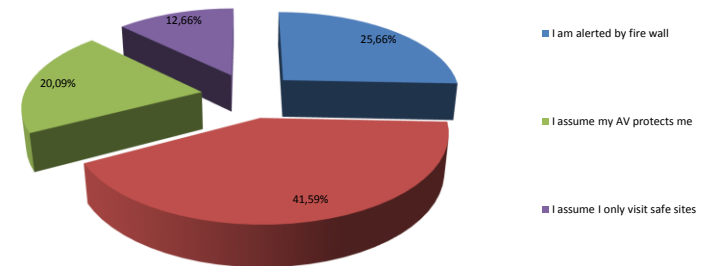


Survey results copyrighted by G Data

Go safe. Go safer. G Data.



How do you know sites you visit are safe?

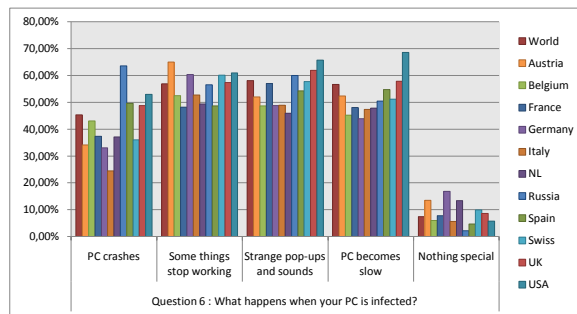


Go safe. Go safer. G Data.



The last question:

What happens when your PC is infected?

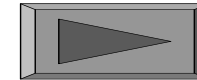


Survey results copyrighted by G Data

Go safe. Go safer. G Data.



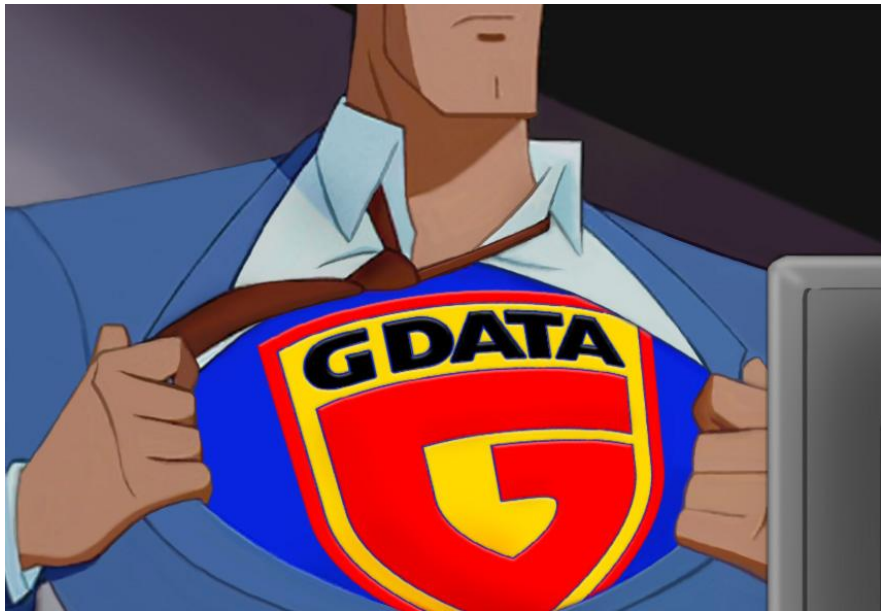
# THE FUTURE



- Continued human behaviour attacks and social media attacks
- More programs and apps related malware => mobile malware
  - 64Bit Malware (eg. TLD4 rootkit), Java/pdf based malware
- More targeted attacks driven by hacktivism (visible), cyberespionage or cybersabotage

→ The real problems will stay under the radar of the public ...

Go safe. Go safer. G Data.



Go safe. Go safer. G Data.



**Thank you!**

[Eddy.Willems@gdata.de](mailto:Eddy.Willems@gdata.de)

*Find me at G Data, Twitter, Youtube, etc ...*

Go safe. Go safer. G Data.