Avoiding to be infected by malware

We are not alone. . . : watch your back!

Ricardo J. Rodríguez

rjrodriguez@unizar.es

tw: @RicardoJRdez – http://www.ricardojrodriguez.es

Universidad Zaragoza

Universidad de Zaragoza

Zaragoza, Spain

3^{rd} June, 2012

Ethical Hacking and Cyber Security

Cardiff, United Kingdom

$whoami

- CLS member since the beginning (2000)
- PhD candidate of University of Zaragoza

Research areas

- Performance in complex software systems
- Secure Software Enginnering (SSE)
- Fault-Tolerant systems (model & design)

Universidad Zaragoza

$whoami

- CLS member since the beginning (2000)
- PhD candidate of University of Zaragoza

Research areas

- Performance in complex software systems
- Secure Software Enginnering (SSE)
- Fault-Tolerant systems (model & design)
- Malware analysis

Universidad Zaragoza

Outline

Universidad Zaragoza

Definitions (I): what is a malware?

Malicious software

Its main goal

- Specially designed for harming your computer

FAQs

- What can it perform to my computer?
- How did it get in?
- How can I prevent from any of these?

Universidad Zaragoza

Definitions (II): types of malware (1)

Malware taxonomy

- Virus
  - Files
  - Self-replicating. Get the vaccine!

Universidad Zaragoza
1542

Definitions (II): types of malware (1)

Malware taxonomy

- Virus
  - Files
  - Self-replicating. Get the vaccine!
- Worm
  - Network
  - *Spreads the love* by itself

Universidad Zaragoza
1542

Definitions (II): types of malware (1)

Malware taxonomy

- Virus
  - Files
  - Self-replicating. Get the vaccine!
- Worm
  - Network
  - *Spreads the love* by itself
- Backdoor
  - Please, CLOSE the door AFTER entering!

Universidad Zaragoza
1542

Definitions (II): types of malware (1)

Malware taxonomy

- Virus
  - Files
  - Self-replicating. Get the vaccine!
- Worm
  - Network
  - *Spreads the love* by itself
- Backdoor
  - Please, CLOSE the door AFTER entering!
- Trojan
  - Ask the Greeks...

Universidad Zaragoza
1542

Definitions (II): types of malware (1)

Malware taxonomy

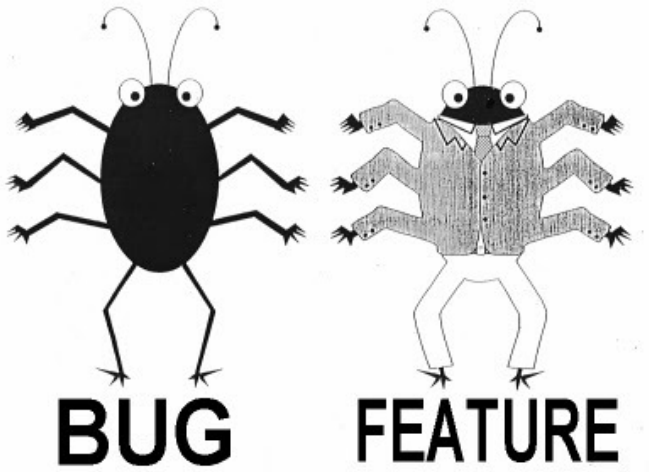
- Virus
  - Files
  - Self-replicating. Get the vaccine!
- Worm
  - Network
  - *Spreads the love* by itself
- Backdoor
  - Please, CLOSE the door AFTER entering!
- Trojan
  - Ask the Greeks...
- ...

Universidad Zaragoza

Definitions (II): types of malware (2)

Malware taxonomy

- ...
- Exploit
  - Authorised access through system vulnerabilities

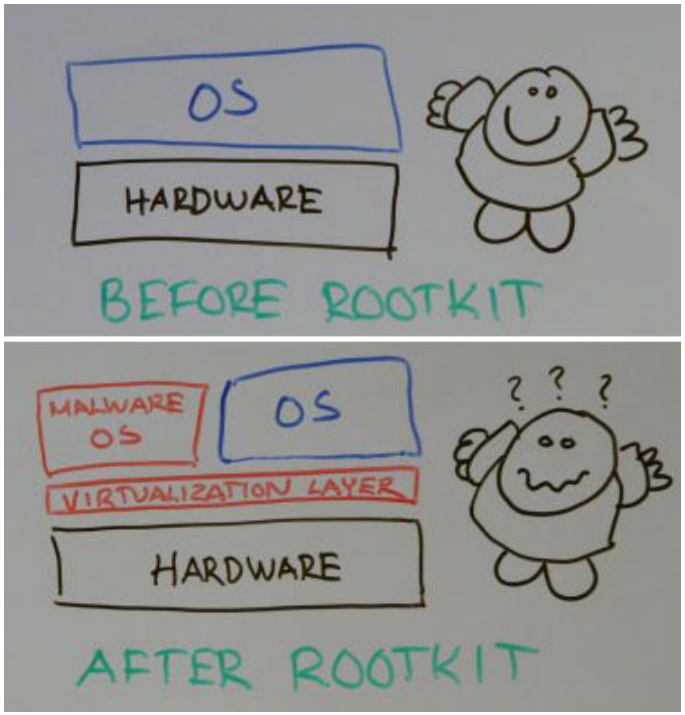


Universidad Zaragoza
1542

Definitions (II): types of malware (2)

Malware taxonomy

- ...
- Exploit
  - Authorised access through system vulnerabilities
- Rootkit
  - As Anonymous, they are there but you don't realise that...



Universidad Zaragoza
1542

Definitions (II): types of malware (2)

Malware taxonomy

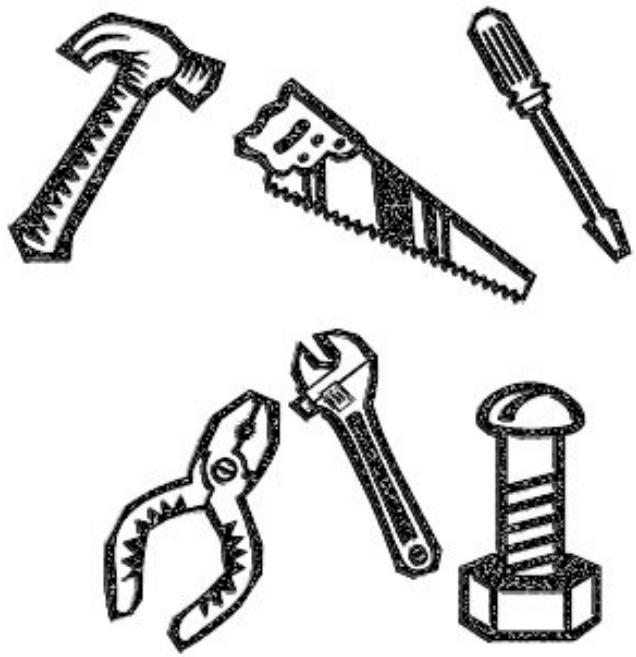
- ...
- Exploit
  - Authorised access through system vulnerabilities
- Rootkit
  - As Anonymous, they are there but you don't realise that...
- Spyware
  - As reading Facebook's timeline, but more user-focused...

Universidad Zaragoza
1542

Definitions (II): types of malware (2)

Malware taxonomy

- ...
- Exploit
  - Authorised access through system vulnerabilities
- Rootkit
  - As Anonymous, they are there but you don't realise that...
- Spyware
  - As reading Facebook's timeline, but more user-focused...
- Hack tools
  - System tools allow other actions...

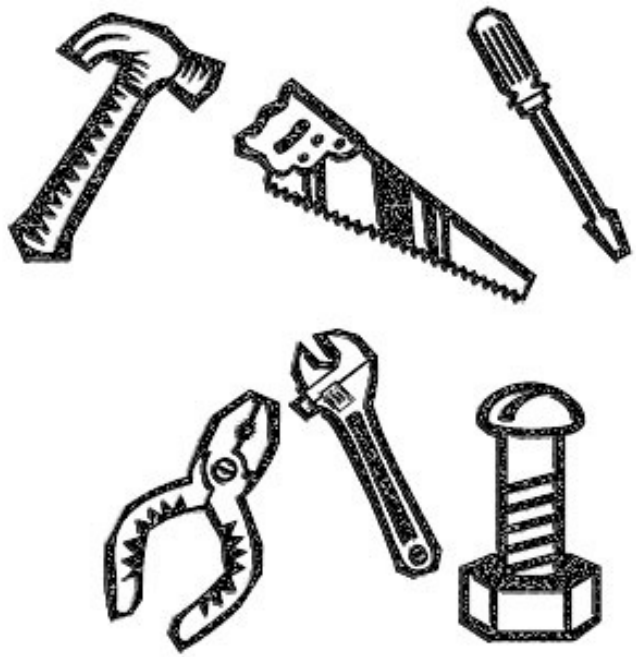


Universidad Zaragoza
1542

Definitions (II): types of malware (2)

Malware taxonomy

- ...
- Exploit
  - Authorised access through system vulnerabilities
- Rootkit
  - As Anonymous, they are there but you don't realise that...
- Spyware
  - As reading Facebook's timeline, but more user-focused...
- Hack tools
  - System tools allow other actions...

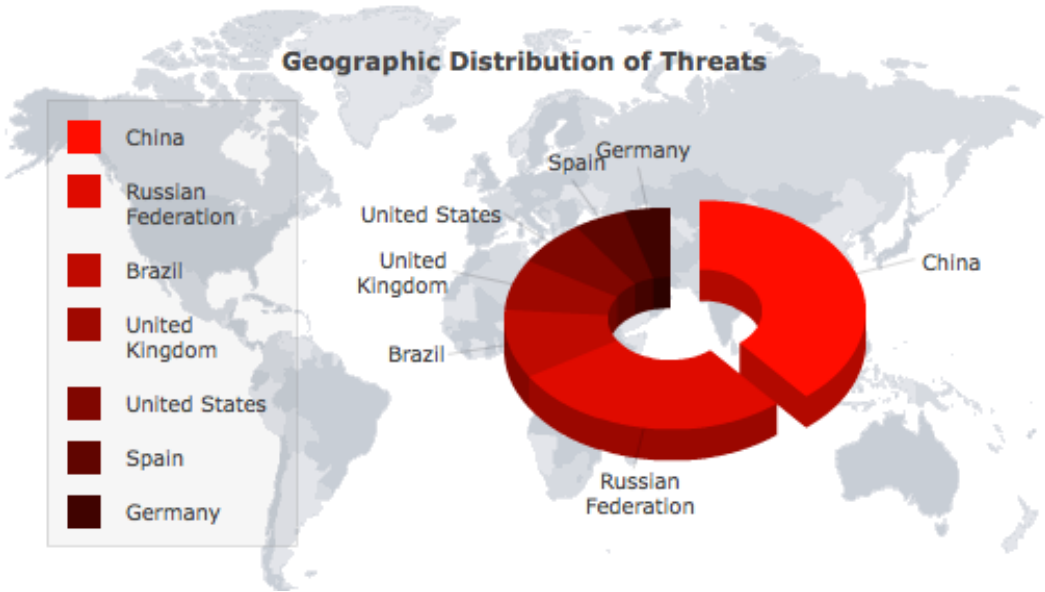


Non-orthogonal taxonomy!

Universidad Zaragoza 1542

From where is it coming?: Some statistics (I)

Software malware threats

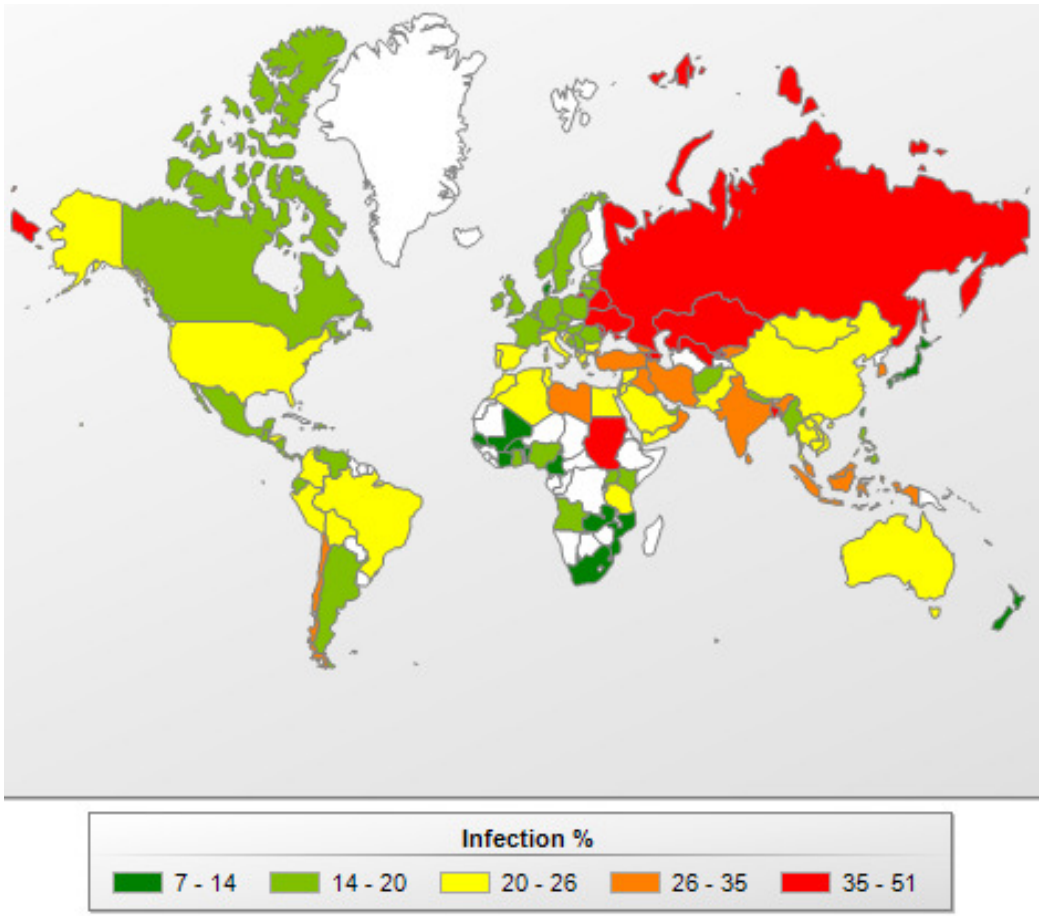


(report of `http://www.threatexpert.com/`, end of May 2012)

Universidad Zaragoza
1542

From where is it coming?: Some statistics (II)

Infection of web malware threats



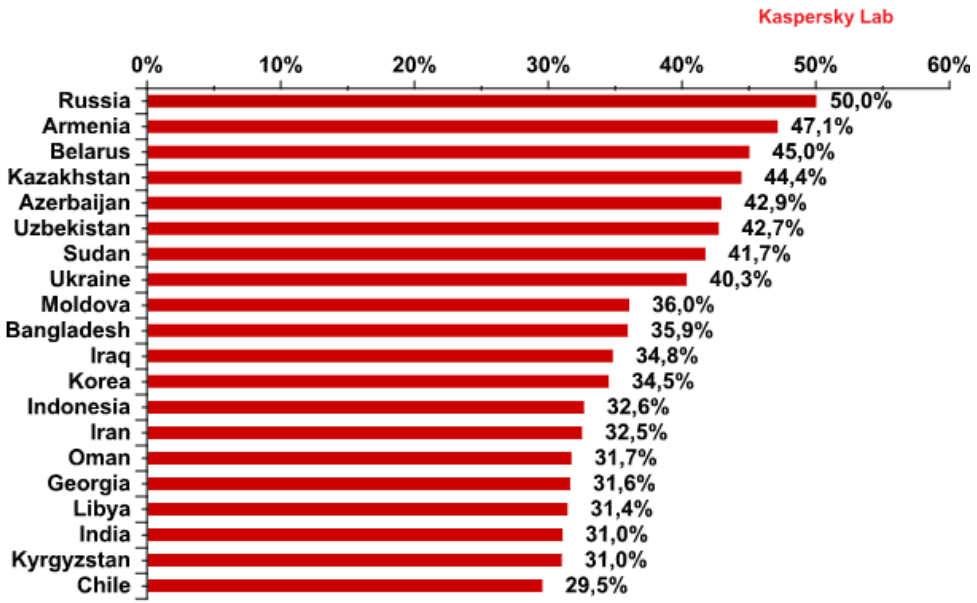
(monthly report of Kaspersky[1], April 2012)

Universidad Zaragoza 1542

[1] Collects data from computers having installed Kaspersky software products.

From where is it coming?: Some statistics (III)

Top 10 countries of risk of infection



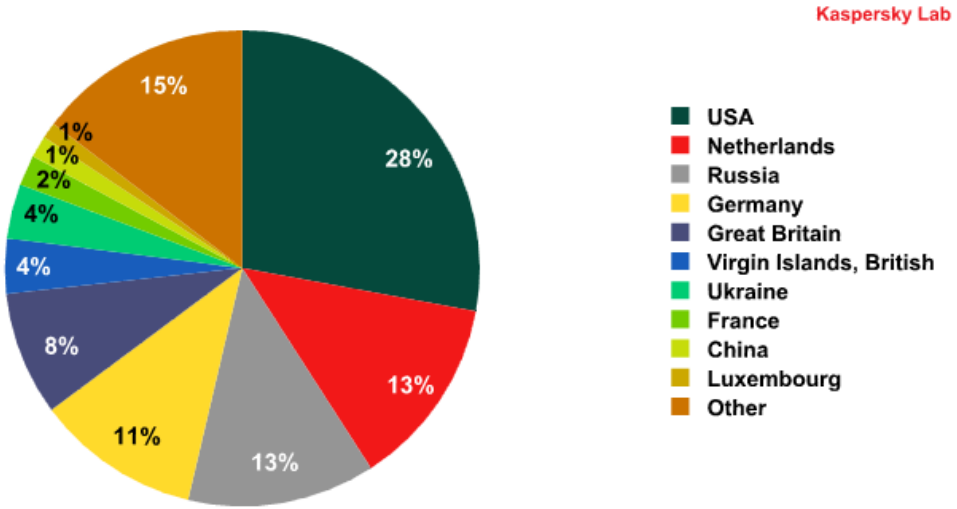
(monthly report of Kaspersky[2], April 2012)

Universidad Zaragoza 1542

[2] Collects data from computers having installed Kaspersky software products.

From where is it coming?: Some statistics (IV)

Infected sites hosting malware



(monthly report of Kaspersky[3], April 2012)

[3] Collects data from computers having installed Kaspersky software products.

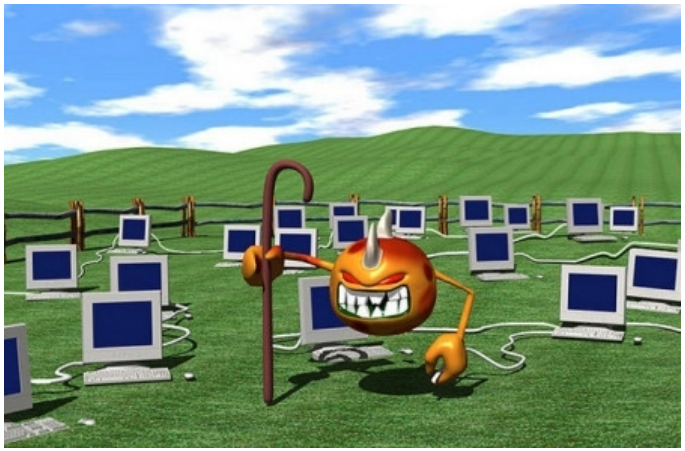
Outline

Universidad Zaragoza

What do they intend?

Main malware goals

- Botnets
  - The Lord is my Shepherd
  - E.g.: DDoS, spam...



Universidad Zaragoza
1542

What do they intend?

Main malware goals

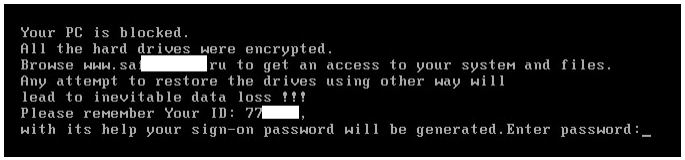
- Botnets
  - The Lord is my Shepherd
  - E.g.: DDoS, spam...
- Information retrieval
  - User-content data (files)
  - Privacy data (keyloggers)
  - Pictures (by using webcam)

Universidad Zaragoza
1542

What do they intend?

Main malware goals

- Botnets
  - The Lord is my Shepherd
  - E.g.: DDoS, spam...
- Information retrieval
  - User-content data (files)
  - Privacy data (keyloggers)
  - Pictures (by using webcam)
- Computer-napping (ransomware)
  - MBR (Master Boot Record)

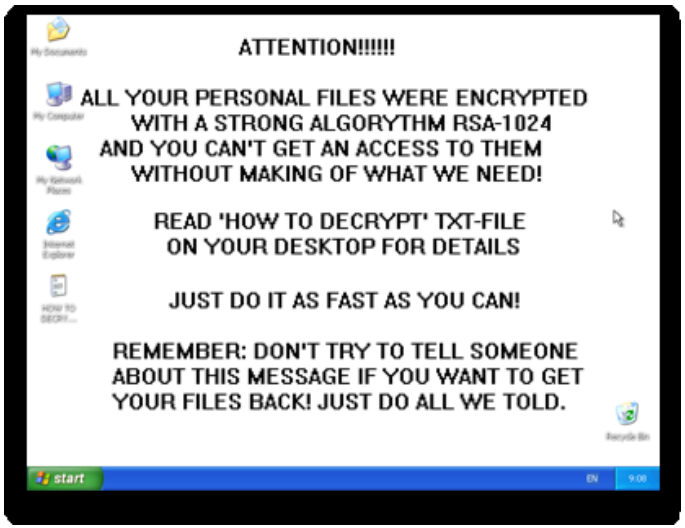


Universidad Zaragoza
1542

What do they intend?

Main malware goals

- Botnets
  - The Lord is my Shepherd
  - E.g.: DDoS, spam...
- Information retrieval
  - User-content data (files)
  - Privacy data (keyloggers)
  - Pictures (by using webcam)
- Computer-napping (ransomware)
  - MBR (Master Boot Record)
  - O.S.

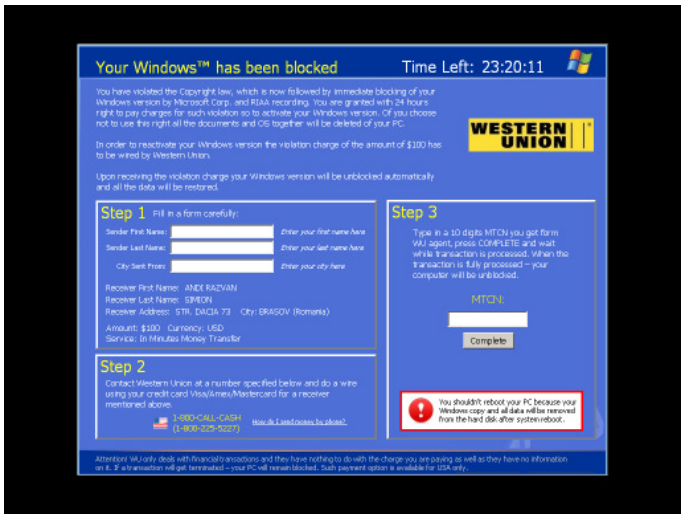


Universidad Zaragoza
1542

What do they intend?

Main malware goals

- Botnets
  - The Lord is my Shepherd
  - E.g.: DDoS, spam...
- Information retrieval
  - User-content data (files)
  - Privacy data (keyloggers)
  - Pictures (by using webcam)
- Computer-napping (ransomware)
  - MBR (Master Boot Record)
  - O.S.



Universidad Zaragoza
1542

What do they intend?

Main malware goals

- Botnets
  - The Lord is my Shepherd
  - E.g.: DDoS, spam...
- Information retrieval
  - User-content data (files)
  - Privacy data (keyloggers)
  - Pictures (by using webcam)
- Computer-napping (ransomware)
  - MBR (Master Boot Record)
  - O.S.

Universidad Zaragoza
1542

What do they intend?

Main malware goals

- Botnets
  - The Lord is my Shepherd
  - E.g.: DDoS, spam...
- Information retrieval
  - User-content data (files)
  - Privacy data (keyloggers)
  - Pictures (by using webcam)
- Computer-napping (ransomware)
  - MBR (Master Boot Record)
  - O.S.
- Fraud (explicitly)
  - Extra hits on ads (adware)
  - Porn diallers (modem connections)
  - Premium numbers callings, SMS (mobile phones)

Universidad Zaragoza
1542

Malware Market (I)

An incipient well-profit market: 2011 benefits estimation

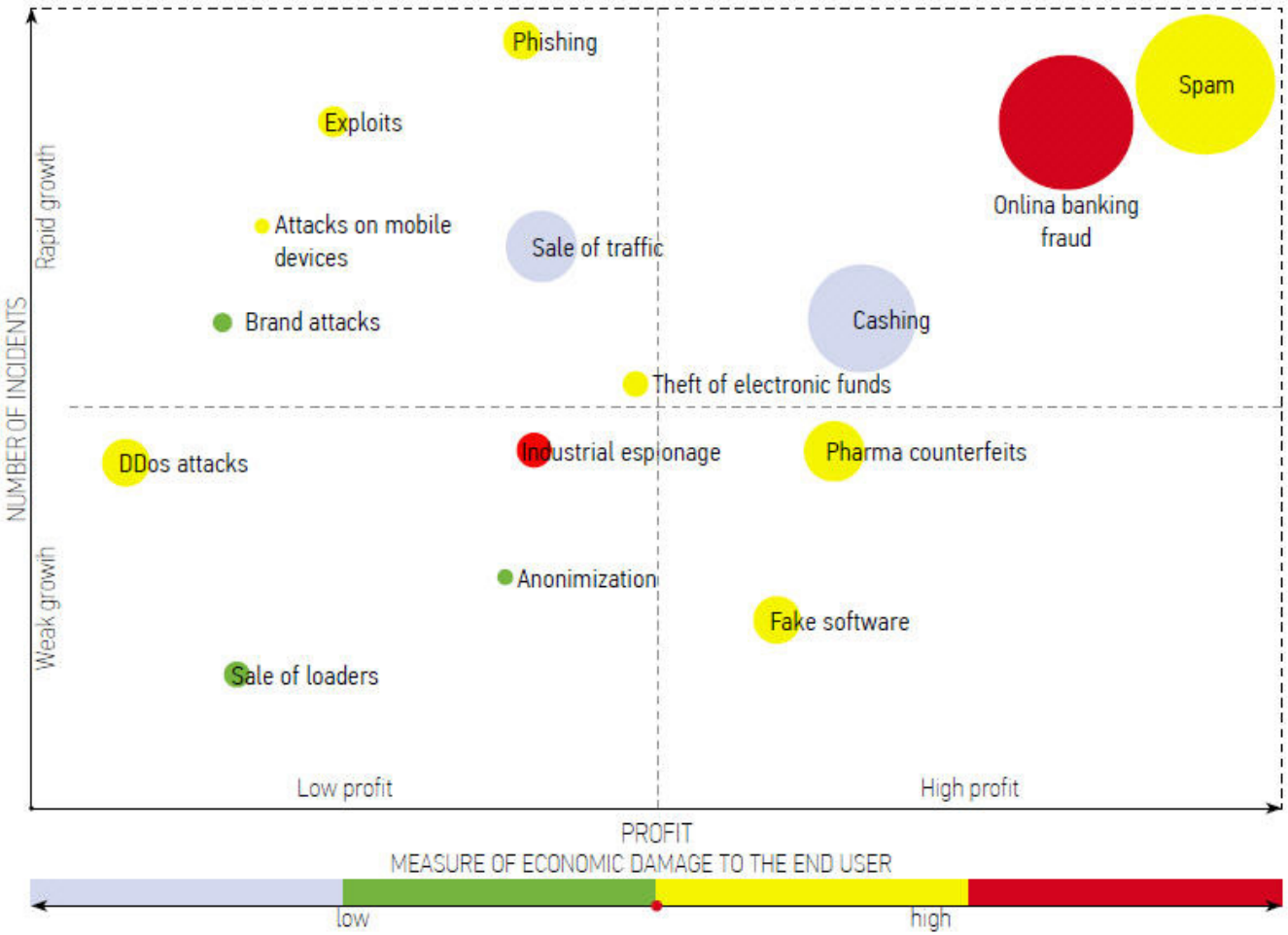
TREND	TOTAL MARKET SHARE	AMOUNT
ONLINE FRAUD		
Online banking fraud	21.3 %	490 million $
Cashing	16 %	367 million $
Phishing	2.4 %	55 million $
Theft of electronic funds	1.3 %	30 million $
Total:	41 %	942 million $
SPAM		
Spam	24 %	553 million $
Pharma and counterfeits	6.2 %	142 million $
Fake software	5.9 %	135 million $
Total:	36.1 %	830 million $
INTERNAL MARKET (C2C)		
Sale of traffic	6.6 %	153 million $
Sale of exploits	1.8 %	41 million $
Sale of loaders	1.2 %	27 million $
Anonymization	0.4 %	9 million $
Total:	10 %	230 million $
DDOS ATTACKS		
DDoS attacks	5.6 %	130 million $
Total:	5.6 %	130 million $
OTHER		
Other	7.3 %	168 million $
Total:	7.3 %	168 million $

(taken from `http://www.securityaffairs.co/`)

Universidad Zaragoza

Malware Market (II)

An incipient well-profit market: economic damages



(taken from `http://www.securityaffairs.co/`)

Outline

Universidad Zaragoza
1542

Spreading mechanisms

How the hell did it comes here?

- File sharing
  - Diskettes? :)
  - USB
  - Internet software...

Universidad Zaragoza

Spreading mechanisms

How the hell did it comes here?

- File sharing
  - Diskettes? :)
  - USB
  - Internet software...
- E-mail

Spreading mechanisms

How the hell did it comes here?

- File sharing
  - Diskettes? :)
  - USB
  - Internet software...
- E-mail
- P2P networks

Universidad Zaragoza

Spreading mechanisms

How the hell did it comes here?

- File sharing
  - Diskettes? :)
  - USB
  - Internet software...
- E-mail
- P2P networks
- IRC (Internet Relay Chat)

Universidad Zaragoza

Spreading mechanisms

How the hell did it comes here?

- File sharing
  - Diskettes? :)
  - USB
  - Internet software...
- E-mail
- P2P networks
- IRC (Internet Relay Chat)
- Bluetooth (mobile phones)

Universidad Zaragoza

Spreading mechanisms

How the hell did it comes here?

- File sharing
  - Diskettes? :)
  - USB
  - Internet software...
- E-mail
- P2P networks
- IRC (Internet Relay Chat)
- Bluetooth (mobile phones)
- Android market (mobile phones)

Universidad Zaragoza

Outline

Universidad Zaragoza

Preventing mechanisms

Some useful preventing techniques

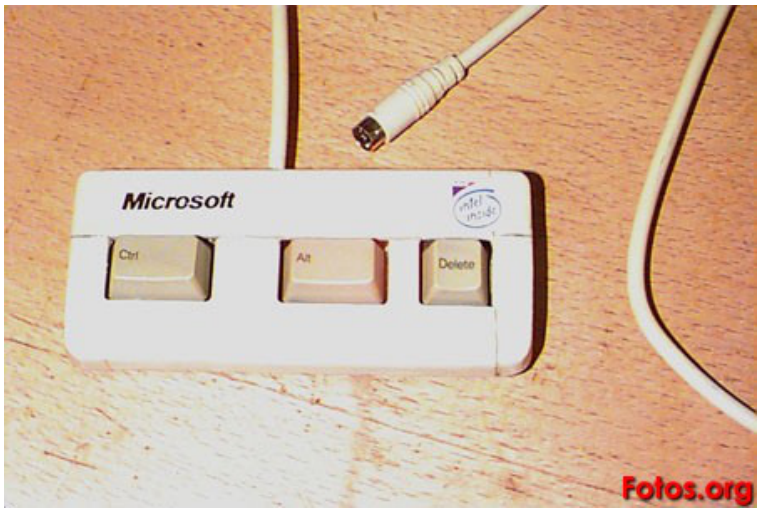
- Install some AV & anti-spyware
  - A trustworthy AV...

Preventing mechanisms

Some useful preventing techniques

- Install some AV & anti-spyware
  - A trustworthy AV...
- Avoid certain websites
  - Careful with the ads!

Preventing mechanisms



Some useful preventing techniques

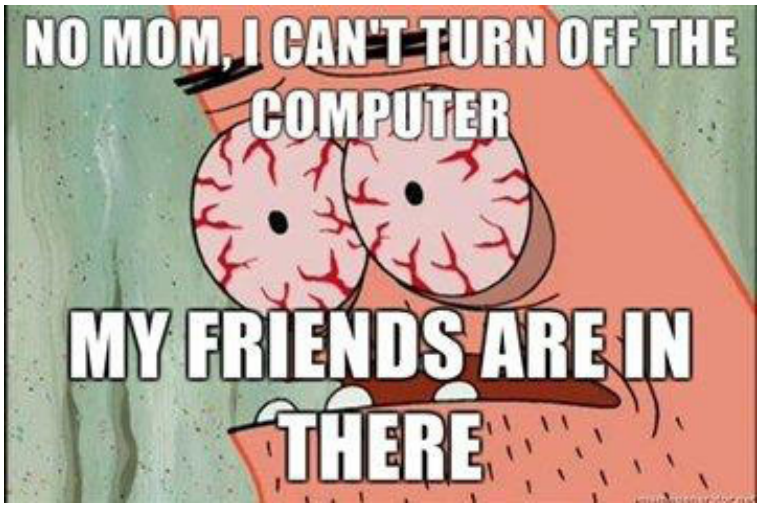
- Install some AV & anti-spyware
  - A trustworthy AV...
- Avoid certain websites
  - Careful with the ads!
- Look active processes
  - Ctrl + Alt + Del (Windows)
  - Apple → "Force Quit"... (MacOS)
  - $ps | aux (MacOS & Linux)

Preventing mechanisms

Some useful preventing techniques

- Install some AV & anti-spyware
  - A trustworthy AV...
- Avoid certain websites
  - Careful with the ads!
- Look active processes
  - Ctrl + Alt + Del (Windows)
  - Apple → "Force Quit"... (MacOS)
  - $ps | aux (MacOS & Linux)
- Don't trust spam mails!
  - Photos of your friend (who?)
  - Are you really a Nigeria's lord?
  - Won the lottery without any ticket?

Preventing mechanisms



Some useful preventing techniques

- Install some AV & anti-spyware
  - A trustworthy AV...
- Avoid certain websites
  - Careful with the ads!
- Look active processes
  - Ctrl + Alt + Del (Windows)
  - Apple → "Force Quit"... (MacOS)
  - $ps | aux (MacOS & Linux)
- Don't trust spam mails!
  - Photos of your friend (who?)
  - Are you really a Nigeria's lord?
  - Won the lottery without any ticket?
- Ask your computer-geek friend

The End

شُكراً!

Avoiding to be infected by malware

We are not alone. . . : watch your back!

Ricardo J. Rodríguez

rjrodriguez@unizar.es

tw: @RicardoJRdez – http://www.ricardojrodriguez.es

Universidad Zaragoza

Universidad de Zaragoza

Zaragoza, Spain

3^{rd} June, 2012

Ethical Hacking and Cyber Security

Cardiff, United Kingdom