

# 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<sup>rd</sup> 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 Engineering (SSE)
- Fault-Tolerant systems (model & design)



# \$whoami

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

## Research areas

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



# Outline

- 1 Background
  - What is a malware?
  - Types of malware
  - But... from where?
- 2 Objectives of malware
  - Malware goals
  - Malware Market
- 3 Spreading mechanisms
- 4 Preventing mechanisms



# 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?



# Definitions (II): types of malware (1)

## Malware taxonomy

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

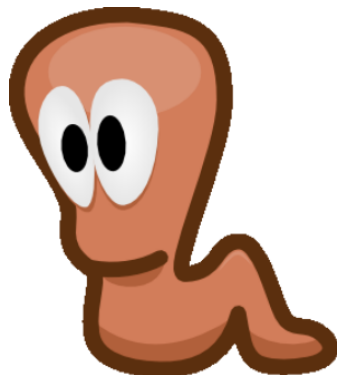


Universidad  
Zaragoza

# Definitions (II): types of malware (1)

## Malware taxonomy

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



Universidad  
Zaragoza

# 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!





# 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...



# Definitions (II): types of malware (1)

## Malware taxonomy

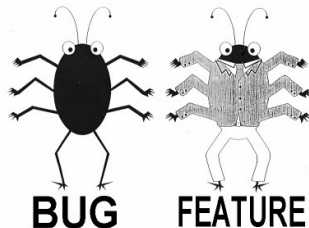
- **Virus**
  - Files
  - Self-replicating. Get the vaccine!
- **Worm**
  - Network
  - *Spreads the love* by itself
- **Backdoor**
  - Please, CLOSE the door AFTER entering!
- **Trojan**
  - Ask the Greeks. . .
- . . .



# Definitions (II): types of malware (2)

## Malware taxonomy

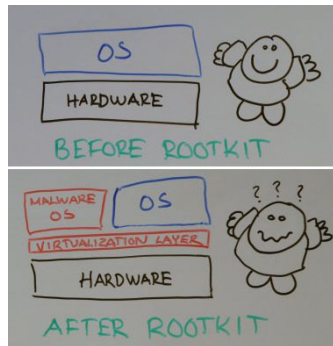
- ...
- **Exploit**
  - Authorised access through system vulnerabilities



# Definitions (II): types of malware (2)

## Malware taxonomy

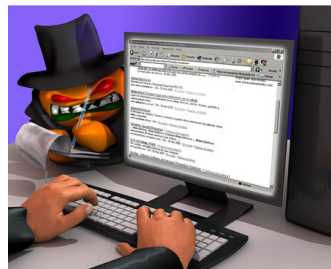
- ...
- **Exploit**
  - Authorised access through system vulnerabilities
- **Rootkit**
  - As Anonymous, they are there but you don't realise that...



# 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...



Graphic Design by Panda Software



Universidad  
Zaragoza

# 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...



# 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...



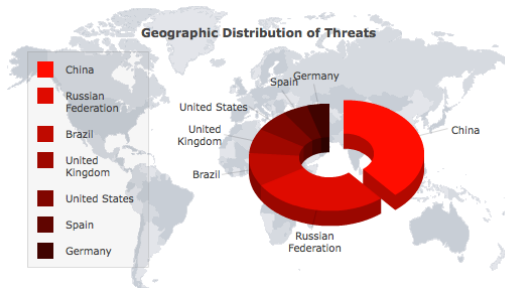
**Non-orthogonal taxonomy!**



Universidad  
Zaragoza

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

## Software malware threats



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

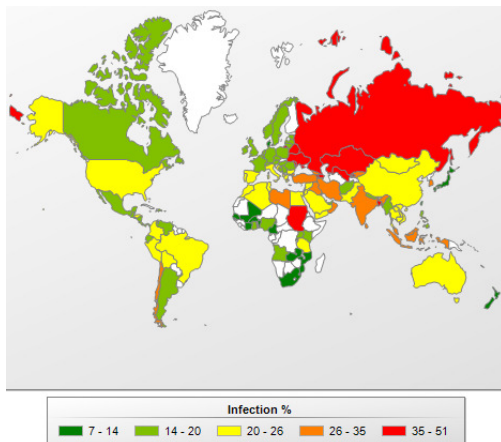


**Universidad**  
Zaragoza



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

Infection of web malware threats



(monthly report of Kaspersky<sup>1</sup>, April 2012)

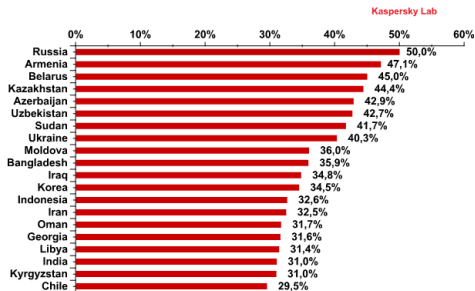


Universidad  
Zaragoza

<sup>1</sup>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<sup>2</sup>, April 2012)

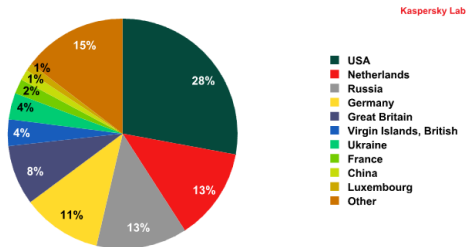


Universidad  
Zaragoza

<sup>2</sup>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<sup>3</sup>, April 2012)



Universidad  
Zaragoza

<sup>3</sup>Collects data from computers having installed Kaspersky software products.

# Outline

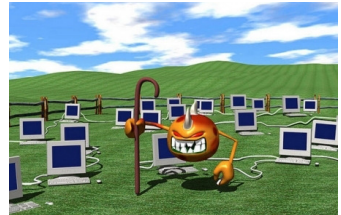
- 1 Background
  - What is a malware?
  - Types of malware
  - But... from where?
- 2 Objectives of malware
  - Malware goals
  - Malware Market
- 3 Spreading mechanisms
- 4 Preventing mechanisms



# What do they intend?

## Main malware goals

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



Universidad  
Zaragoza

# 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

# 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)

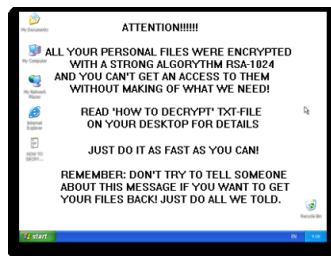
```
Your PC is blocked.  
All the hard drives were encrypted.  
Browse www.sah.com to get an access to your system and files.  
Any attempt to restore the drives using other way will  
lead to inevitable data loss !!!  
Please remember Your ID: 79  
with its help your sign-on password will be generated. Enter password: _
```



# 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.

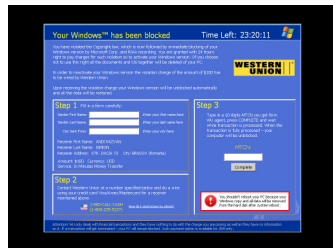




# What do they intend?

## 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.



# 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.

The image shows a ransomware payment page in Spanish, titled 'Atención!' (Attention!). The page is from the Brigada de Investigación Tecnológica (BITE) of the Spanish National Police. It contains several sections with instructions for paying the ransom:

- Para quitar el bloqueo del ordenador, usted debe pagar una multa de 100 euros.** (To remove the computer lock, you must pay a fine of 100 euros.)
- Unidad Estatal Anti-Fraudes de Pagos:**
  - 1) Realizar el pago a través de Ukash: Para ello, por favor introduce a código de identificación de transacción para cada transacción realizada en la tienda de pago y, posteriormente, pide el QR (o código) de tu tarjeta de crédito. A continuación, escanea el código QR y responde de inmediato.
  - 2) Realizar el pago a través de Paysafecard: Para ello, por favor introduce a código de identificación de transacción para cada transacción realizada en la tienda de pago y, posteriormente, pide el QR (o código) de tu tarjeta de crédito. A continuación, escanea el código QR y responde de inmediato.
- ¿kash? ¿Dónde conseguir Ukash?**
  - Comer.es: Comprar - a partir de ahora está disponible Ukash en todos los lugares de Comer.
  - Calvo y Sainza: Calvo y Sainza - a partir de ahora Ukash está disponible en todos los lugares de Calvo y Sainza.
  - Cinecine: Cinecine - ahora, Ukash está disponible en los 160.000 locales de Cinecine.
  - Expresopago: Expresopago - Compra tu Ukash online a través de tu Internet Bank o visitando tu tienda de crédito.
  - Monederos: Monederos - Compra tu Ukash en Monederos.
  - MundoRecepcion: MundoRecepcion - Compra tu Ukash en MundoRecepcion.
- ¿Paysafecard? ¿Dónde conseguir Paysafecard?**
  - Para ello, por favor introduce el código de identificación de transacción para cada transacción realizada en la tienda de pago y, posteriormente, pide el QR (o código) de tu tarjeta de crédito. A continuación, escanea el código QR y responde de inmediato.



Universidad  
Zaragoza

# 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

# Malware Market (I)

An incipient well-profit market: 2011 benefits estimation

TREND	TOTAL MARKET SHARE	AMOUNT
<b>ONLINE FRAUD</b>		
Online banking fraud	21.3%	490 million \$
Cashing	16%	367 million \$
Phishing	2.4%	55 million \$
Theft of electronic funds	1.3%	30 million \$
<b>Total:</b>	<b>41%</b>	<b>942 million \$</b>
<b>SPAM</b>		
Spam	24%	553 million \$
Pharma and counterfeits	6.2%	142 million \$
Fake software	5.9%	135 million \$
<b>Total:</b>	<b>36.1%</b>	<b>830 million \$</b>
<b>INTERNAL MARKET (C2C)</b>		
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 \$
<b>Total:</b>	<b>10%</b>	<b>230 million \$</b>
<b>DDOS ATTACKS</b>		
DDoS attacks	5.6%	130 million \$
<b>Total:</b>	<b>5.6%</b>	<b>130 million \$</b>
<b>OTHER</b>		
Other	7.3%	168 million \$
<b>Total:</b>	<b>7.3%</b>	<b>168 million \$</b>

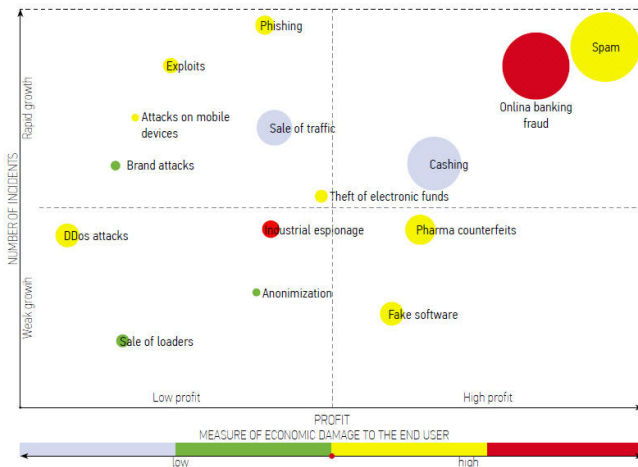


Universidad  
Zaragoza

(taken from <http://www.securityaffairs.co/>)

# Malware Market (II)

An incipient well-profit market: economic damages



(taken from <http://www.securityaffairs.co/>)



iversidad  
Zaragoza

# Outline

- 1 Background
  - What is a malware?
  - Types of malware
  - But... from where?
- 2 Objectives of malware
  - Malware goals
  - Malware Market
- 3 Spreading mechanisms
- 4 Preventing mechanisms



# Spreading mechanisms

How the hell did it comes here?

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



# 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**



# Spreading mechanisms

How the hell did it comes here?

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



# 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)



# 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)



# Outline

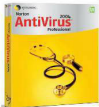
- 1 Background
  - What is a malware?
  - Types of malware
  - But... from where?
- 2 Objectives of malware
  - Malware goals
  - Malware Market
- 3 Spreading mechanisms
- 4 Preventing mechanisms



# 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)



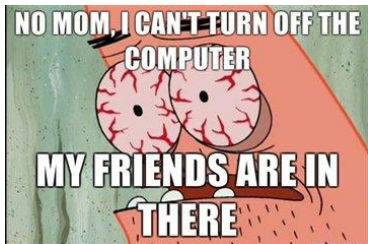
# Preventing mechanisms



## 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!



**Universidad**  
Zaragoza

# 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<sup>rd</sup> June, 2012

**Ethical Hacking and Cyber Security**  
Cardiff, United Kingdom