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 de Zaragoza Zaragoza, Spain

3rd June, 2012

Ethical Hacking and Cyber Security Cardiff, United Kingdom

- 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)



- 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



Outline

Background

- What is a malware?
- Types of malware
- But... from where?

Objectives of malwareMalware goals

Malware Market

Spreading mechanisms

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?



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





Malware taxonomy

• Virus

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



Malware taxonomy

• Virus

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



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...





Malware taxonomy

• Virus

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

Θ...

• Ask the Greeks...

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





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





Types of malware

Definitions (II): types of malware (2)

- . . .
- 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...





Types of malware

Definitions (II): types of malware (2)

- **O**
- 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...



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!





Background But...from where?

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

Software malware threats



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



Background But... from where?

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

Infection of web malware threats



(monthly report of Kaspersky¹, April 2012)

Zaragoza ¹Collects data from computers having installed Kaspersky softwa¹⁵⁴² products.

3rd June, 2012 8 / 20

From where is it coming?: Some statistics (III) Top 10 countries of risk of infection



(monthly report of Kaspersky², April 2012)

²Collects data from computers having installed Kaspersky software products.

R.J. Rodríguez

Avoiding to be infected by malware

3rd June, 2012 9 / 20

Universidad Zaragoza Background But...from where?

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

Infected sites hosting malware



(monthly report of Kaspersky³, April 2012)

³Collects data from computers having installed Kaspersky software products.

3rd June, 2012 10 / 20

Universidad Zaragoza

Outline

Background

- What is a malware?
- Types of malware
- But... from where?

Objectives of malware
Malware goals
Malware Market

Spreading mechanisms

Preventing mechanisms



Main malware goals

Botnets

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





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)





3rd June, 2012 12 / 20

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. Blocke used stores encrypted. Brooke used satisfies a logat an access to year system and files. Invy attempt to restore the drives using other way will Plass resember Your 110. 77 . with fis help your signeen passaced will be generated.Kater passwords.



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)

• 0.S.





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.





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.

<section-header><section-header> Definition Control</section-header></section-header>	<section-header><section-header> But and the second seco</section-header></section-header>	<section-header><section-header><text><text><text><text><text></text></text></text></text></text></section-header></section-header>	<section-header><section-header><text><text><text><text><text><text></text></text></text></text></text></text></section-header></section-header>	<section-header><section-header><section-header><text><text><text><text><text></text></text></text></text></text></section-header></section-header></section-header>	<section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>	<section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>	<section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>	<section-header><section-header><text><text><text><text><text><text></text></text></text></text></text></text></section-header></section-header>	<section-header><section-header><text><text><text><text><text><text></text></text></text></text></text></text></section-header></section-header>	<section-header><section-header> Definition Control</section-header></section-header>		
<text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text>	<text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text>	<text><text><text><text><text><text><text></text></text></text></text></text></text></text>	<text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text>	<text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text>	<text><text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text></text>	<text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text>	<text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text>	<text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text>	<text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text>	<text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text>		<text></text>
<text></text>	<text><text></text></text>	<text><text><text><text><text><text><text></text></text></text></text></text></text></text>	<text><text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text></text>	<text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text>	<image/> <section-header><section-header><section-header><section-header><section-header><text><text><text></text></text></text></section-header></section-header></section-header></section-header></section-header>	<image/> <section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>	<image/> <section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>	<text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text>	<text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text>	<text></text>		<section-header></section-header>
<text><text><text><text><text><text></text></text></text></text></text></text>	<text><text><text><text><text><text></text></text></text></text></text></text>	<text><text><text><text><text><text><text></text></text></text></text></text></text></text>	<text><text><text><text><text><text><text></text></text></text></text></text></text></text>	<text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text>	<text><text><text><text><text><text><text></text></text></text></text></text></text></text>	<text><text><text><text><text><text></text></text></text></text></text></text>	<text><text><text><text><text><text></text></text></text></text></text></text>	<text><text><text><text><text><text><text></text></text></text></text></text></text></text>	<text><text><text><text><text><text><text></text></text></text></text></text></text></text>	<text><text><text><text><text><text></text></text></text></text></text></text>		<text></text>
<text><text><text><text><text></text></text></text></text></text>	<text><text><text><text><text><text></text></text></text></text></text></text>	<text><text><text><text><text></text></text></text></text></text>	<text><text><text><text><text></text></text></text></text></text>	<text><section-header><section-header><section-header></section-header></section-header></section-header></text>	<text><section-header><section-header><section-header><section-header><section-header><text><text><text><text></text></text></text></text></section-header></section-header></section-header></section-header></section-header></text>	<page-header><section-header><section-header><section-header><section-header><section-header><section-header><text></text></section-header></section-header></section-header></section-header></section-header></section-header></page-header>	<page-header><section-header><section-header><section-header><section-header><section-header><section-header><text></text></section-header></section-header></section-header></section-header></section-header></section-header></page-header>	<text><section-header><section-header><section-header></section-header></section-header></section-header></text>	<text><section-header><section-header><section-header></section-header></section-header></section-header></text>	<text><text><text><text><text></text></text></text></text></text>	<text><section-header></section-header></text>	
<section-header><section-header><text><text></text></text></section-header></section-header>	<section-header><section-header><text><text></text></text></section-header></section-header>	<text><text><text><text><text></text></text></text></text></text>	<text><text><text><text><text></text></text></text></text></text>	<text><text><text><text><text></text></text></text></text></text>	<section-header><section-header><section-header><section-header><text><text></text></text></section-header></section-header></section-header></section-header>	<section-header><section-header><section-header><section-header><text><text><text></text></text></text></section-header></section-header></section-header></section-header>	<section-header><section-header><section-header><section-header><text><text><text></text></text></text></section-header></section-header></section-header></section-header>	<text><text><text><text><text></text></text></text></text></text>	<text><text><text><text><text></text></text></text></text></text>	<section-header><section-header><text><text></text></text></section-header></section-header>	<section-header><section-header><section-header></section-header></section-header></section-header>	<text><text></text></text>
<text><text><text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text></text></text></text>	<text><text><text></text></text></text>	<text><text><text></text></text></text>	<text><text><text></text></text></text>	<text><text><text></text></text></text>	<text><text><text></text></text></text>	<text><text><text></text></text></text>	And and an an and an an an and an	
	<text><text></text></text>	<text><text><text></text></text></text>	<text><text><text></text></text></text>	<section-header><text><text><text><text><text><text></text></text></text></text></text></text></section-header>	<text><text><text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<section-header><text><text><text><text></text></text></text></text></section-header>	<section-header><text><text><text><text></text></text></text></text></section-header>		International	 An and a stand a
<text><text><text></text></text></text>	<text><text><text></text></text></text>	<text><text><text></text></text></text>	<text><text><text></text></text></text>	<text><text><text></text></text></text>	<text><text><text></text></text></text>	<text><text><text></text></text></text>	<text><text><text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text></text></text></text>		And the stand is a loss of the stand is loss of the stand is a loss of the stand is a loss
		<text><text><text></text></text></text>	<text><text><text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text></text></text></text>	<text><text><text></text></text></text>		 And an analysis of the state of	 And an experimental structure of the structu
					<text><text></text></text>	and an an and an an and an	and an an and an an and an					The second secon
 A standard stan	Statistical St							An example of the strength o	An example of the strength o	 A standard stan	And the second	
And the Additional state of th	And the Additional Control of the Additional	The second secon	And the Address and the Addres	And the Advancement of the Advan	And the Address and the Addres	And the Address and the Addres	And the Address and the Addres	And the Additional and the Addit	And the Additional and the Addit	And the Additional state of th	And the second s	And and a set of a se
And a fully cardinal factor an	and an effect of the second se	And effect the And effect of	And effect and the strength of	Start (Start)	And of operating in the Department of the De	And of operating the operat	And of operating the operat	And region to the Normality of the Norma	And region to the Normality of the Norma	And a fully cardinal factor an	hadra diport a tradi di fogola tradi di fogola di alta di a	Refer of popo a track do Psychical and, por normatica integration and psychical and, por normatica integration and psychical and provide autor of polarity and psychical an
and an of the original constraints of the original constra	any or four management of the strength of the	ung more services and services	ung more menung me menung menung menu	ung no series and seri	the off off off off off off off off off of	the other structure str	the other structure str	due de construction de la construction de la construcción de la con	due de construction de la construction de la construcción de la con	and an of the original constraints of the original constra	Alle pur den en tentes a relation entralise entre de la sel publica de la sel p	ande, ser four instance insegnosebelo groups de anal procession de manuel procession de anal procession de manuel procession de de la de rite, répresentation (2) les de arts, procession de de la de la de la desta de la desta la de la de rite, répresentation (2) les de la de rite, procession de la desta de la desta la de la de rite, répresentation de la desta de la
And the set of section of the set of section of the set of section of the set	And the set of the set	Bernard Be	Bernard Be	Berger and State and S	The provide structure of the control	Bergersteinen einen	Bergersteinen einen	An end and a many and	An end and a many and	And the set of section of the set of section of the set of section of the set	The second secon	the product of the state o
and an of the gradema part of the second part of	ne et et je operante en en et en	Net of the start is grant and the start is	Needers a genorize and the set of	And the set of the set	na statu kuje na poslavani pos	And the top of the second	And the top of the second	And the transformation of the second seco	And the transformation of the second seco	and an of the gradema part of the second part of	Version a la granditaria de producto de los segundarias de persona de la segundaria de l	Puedes adquire to papadeced wice signer ter reder receives a parameter reder rear (anter severe Nankarga y Newsyord). Convex, Calman de Telefono, Teleco, Operano, Calman de Telefono, Teleco, Operano, Teleco, Operano, Calman de Telefono, Teleco, Operano, Calman de Telefono, Calman de Te
Australia and Aust	Apartalization of the second s	Aparticipation of the second s	Approximation of the second se	Annual Annua	horsenantitude subsche Statute auf der Statute subsche Statute	horsenegitis General Salanda partene fana (General partene fana) (General Constanting), entre fana (General	horsenegitis General Salanda partene fana (General partene fana) (General Constanting), entre fana (General	An	An	Australia and Aust	en electrice deposition de position en la contraction de la contra	Internet to private a series, some information of the series of the seri
												an electric depositioner policy and an electric sector and a sector of the sector and the sector of the sector and the sector of
											14	
												16
												r mail
												Incl
											16	
adeuteriar para de la 2000, y Cara Margar de Televis	atender sing, kenne de State, y daer herene et de State, y daer herene et de State.	adevide to be of the second and the second adevide to be of the second adevide to be o	advertes sig, kezus de led 2000, y Cara Receipte de Telefores	advertes sig, terres de led 2000, y Cara Arange de Telderes.	advanta sing, increase to load 30.000, if Gene Records of Montes.	advanta site and a site of	advanta site and a site of	advector sing, tence de fed 30.000, y Cara Recorgin de Telefores.	advector sing, tence de fed 30.000, y Cara Recorgin de Telefores.	adeuteriar para de la 2000, y Cara Margar de Televis	adjustication potential and another and a feet the feet of 00,000, y Caroli Recorger de Telefonica	A DESCRIPTION OF A DESC
and a light of the set	and a part of the second	consisting provide a first case of a set of a se	Instead papers a new setting based and and another in the setting of the setting	Linters & games a size, units black a size analysis of existing descalable accurate analysis on existing descalable accurate analysis encision of existing descalable accurate analysis encision	Linters to particular and a statistical and a	Linters & particular to the data data and part of the second balance of the data and the data and the second balance of the data and the	Linters & particular to the data data and part of the second balance of the data and the data and the second balance of the data and the	neres la paro en uno, cuel dade anza antegra en enter trans depusidade suburationes enter en enter de facilitary o transporter transporter de de Care de Belleria, Terra, Care de enter trans depusidade suburationes enter ente enter enter	neres la paro en uno, cuel dade anza antegra en enter trans depusidade suburationes enter en enter de facilitary o transporter transporter de de Care de Belleria, Terra, Care de enter trans depusidade suburationes enter ente enter enter	and a light of the set	Ferture is general an arror, used datasia and your another of the standard y ferenerand. Conversion Convere	Textures to general an array, used Machanian an object an array of the second and a second machanian and the second macha
Instead by provide a starting provided and in the starter rate of	neers to provide a start or providence training and extension dependences and the start of the extension dependences and the start of the extension dependences and the start of the start	network by portion and register of the state	nexes by porce and rules deal and relief of the second deal and rules of t	nexes by powers and under advantation of the second s	Inter to pool on a new cost to be to an a statistication of the st	Here is pool on any case takes and a set	Here is pool on any case takes and a set	needs special en en construit stad and antigen et en en e	needs special en en construit stad and antigen et en en e	Instead by provide a starting provided and in the starter rate of	The set of	Puedes adjant to payoficial ender signature redex. epar (where ender a "becknarge y "becknarge y "becknarge y "becknarge"). Extend to particular and an anti-anti-anti-anti-anti-anti-anti-anti-
And is the y department and (). These is an approximation of the second and a second and a instance is provided in the second and a second and a instance is approximation of the second and a second and a instance is approximately and a second and a second and a instance is approximately and a second and a second and a instance is approximately and a second and a second and a instance is approximately and a second and a second and a instance is approximately and a second and a second and a instance is approximately and a second and a second and a instance is approximately and a second and a second and a instance is approximately and a second and a second and a instance is approximately and a second and a second and a instance is approximately and a second and a second and a instance is approximately and a second and a second and a instance is approximately and a second and a second and a instance is approximately and a second and a second and a instance is approximately a second and a second and a second and a instance is approximately and a second an	Alta de dr. y receiming alta (d). Testes la productión de la regularization de receiminaria de la productión de la regularization de Testes la regular	Althe de ref. y (Apriles plane 3) The de ref. y (April April 2) The de ref. y (April 2) The de	Althe de ref. y (Applein plane 3) The de ref. y (Applein plane 3)	Althe de ref. (reference here of a constraint	Alta de fair, prépais pais 01 marce la service de la serv	Althe de risk (y delam bale 3)	Althe de risk (y delam bale 3)	Mark de Krig (Appendisken) Hand de Krig (Appendisken) Ha	Mark de Krig (Appendisken) Hand de Krig (Appendisken) Ha	And is the y department and (). These is an approximation of the second and a second and a instance is provided in the second and a second and a instance is approximation of the second and a second and a instance is approximately and a second and a second and a instance is approximately and a second and a second and a instance is approximately and a second and a second and a instance is approximately and a second and a second and a instance is approximately and a second and a second and a instance is approximately and a second and a second and a instance is approximately and a second and a second and a instance is approximately and a second and a second and a instance is approximately and a second and a second and a instance is approximately and a second and a second and a instance is approximately and a second and a second and a instance is approximately and a second and a second and a instance is approximately and a second and a second and a instance is approximately a second and a second and a second and a instance is approximately and a second an	defails de titre, y dequais public (2). Media da traite, y dequais public (2). Media da traite public de t	Soft as do vitra, y deguisin puters (9). Provide adaptar to populational environ signatures index: repart (ander service): Manual Adaptar to populational and an international index and the service i
revenues and a production of the solution	Production of provide view or logicly strategies and the strategies of the strate	une single and the single sin	uno dia base o paraditar o se confejo francas. Instru se para o para di a se confejo francas. Instru se para o para di a se confejo francas. Instru se confeso francas. Instru se conf	uno dia bana in a suati no se single internationali di anti a suato di anti a	Development of such are stated in the state of the sta	un seide saute in de saute in de saute internet de la saute internet de	un seide saute in de saute in de saute internet de la saute internet de	The state of the state is the state of t	The state of the state is the state of t	revenues and a production of the solution	Demokracian de la consequer para la consequere para la consequer para la consequer para la consequer p	somewhat put and the stand there index (sign), Venuexaas admin de virz, y depende plan (P) works als produced with a stand to be virze, stand to be virze.
Big the intervention of the data part of the data par	Bit physics in the operation of the distance of the distan	Bergericht werden eine Bergerichtwerden eine Bergericht werden eine Bergericht werden e	 ¹ Operating the state strain and the strain and	 	 Benefit and a strategies of the str	Berganic Consequence Propagation (Consequence Propagation) (Conseq	Berganic Consequence Propagation (Consequence Propagation) (Conseq	in the provide structure of the structu	in the provide structure of the structu	Big the intervention of the data part of the data par	indepartor to score usegne to evaluation of the score use of the score of the score use of the score us	and you is consistent and in a billion of a second
Bug the form that an analysis of the product o	ulty of the offset state strategy could be particular to the strategy of the s	the unit of the end	In the other based on the state of the other based on the other bas	In the other works and integration that the other works and the	But of the other strategies and the other s	• Our production of the pro	• Our production of the pro	It up the output to the product of the product o	It up the output to the product of the product o	Bug the form that an analysis of the product o	High year for status at logic scale (a second	unity or for entranses at long-sector process and or for a for entranses at long-sector process and or for a for a for entranses and or for a
The process of the	The process of the second s	The process of the second s	The provide the structure of the stru	the off of the strength of the	they decide the set of the set	the drive of the sector of	the drive of the sector of	the net of the strength of the	the net of the strength of the	The process of the	the second	the second
when drags strates in Synchroniz (Section 2014) and the strates strate	when drags strates the "Specification" in the strates of the strat	And a digar strate drawbards the distribution of the distribution	And a digar strate drawbard to the strate drawbard strategies and the	And a diga transformed in the second	In the other state is the other is the ot	Interface of the Antonic of the A	Interface of the Antonic of the A	And a right strate is hypothesis of the strate is the stra	And a right strate is hypothesis of the strate is the stra	when drags strates in Synchroniz (Section 2014) and the strates strate	Indear Agos za krali de Typelandi mar y nor versata caracteriza fa na sa krali de sa kraljevice na sa mar y nor versata caracteriza fa na sa kraljevice na sa mar y nor versata caracteriza fa na sa kraljevice na sa Portuga caracteriza fa na sa kraljevice na sa Na sa kraljevice na sa kralje	Index of goal think of Postland, and y the or status dispropriation of the status of
what rugs of the state of the s	And region that A hydroxies in the second se	Start digs track in by during the start of the start o	State diggs state high state and stat State and state	State digst transfer that hybrid is a state of the sta	And effects of the Althought of the A	And effects in the National State of the	And effects in the National State of the	And a right of the start of the	And a right of the start of the	what rugs of the state of the s	Martin drog and set have been been been been been been been be	https://google.com/google/inter-inter
the of sector and the other se	the of each of the other than the ot	And for an or and a constant of the second o			and after proton is hybridized. With the second	and after proton to how has a second and	and after proton to how has a second and			the of sector and the	And and page 1 to the dis Physichel Marine Marine Marine Marine Marine	Note: Control (status)
And a fuge to the design of th	And a fuge tests in the second s	Mart Fuge 1 store & Drawlen Image: Store S	And regis the A Pointer and regis the A Point	And regin the A Product And regin the A Produ	And regions that is a fixed with the second	And regions the of Nychine in the Section of	And regions the of Nychine in the Section of	And regin the drawned Image: State S	And regin the drawned Image: State S	And a fuge to the design of th	And the days is took of hypothesis and thypothesis and the days is took of hypothesis	Instant drage a native in Repetition And and a provide in any and any and any and any any and any
And the second secon	A set of the set o	And the second		A standard and a stand A standard and a standar		Martine Martine State Stat	Martine Martine State Stat	And the second sector of th	And the second sector of th	And the second secon		Alter and a second secon
Detroit of the sector of th	Interventional and the second and	And the Additional and the Addit	And the Address and the Addres	And the Address and the Addres	And the Andread Andrea	And the Automatical Control of the Automatical C	And the Automational Control of the Automation o	International and the second secon	International and the second secon	Detroit of the sector of th	And the second s	And the field of the state of t
And the Additional state of th	And the Additional Control of the Additional	The second secon	And the Address and the Addres	And the Advancement of the Advan	And the Address and the Addres	And the Address and all the Address and a sector of the Ad	And the Address and all the Address and a sector of the Ad	And the Additional and the Addit	And the Additional and the Addit	And the Additional state of th	And the second s	And and a set of a se
And the figure the sharehold and the sharehold a	And the grant of the structure of the st	And the second s	And the second s	And the Analysis of the Analys	And the Analysis of the Analys	An entropy of the strategy of	An entropy of the strategy of	And the Advances of the Advanc	And the Advances of the Advanc	And the figure the sharehold and the sharehold a	And etchy and	And and gave a start due balance and an an an and an an and an an and an an and an an and an an an an an an and an and an and an
And a second	And the second secon	And the second s	And the second s	And the standing of the standi	And the second s	And the second s	And the second s	And the standing of the standi	And the standing of the standi	And a second		And the set of the set
And region and a development of the second o	And a group of a gr	And a special provide the special provide t	And a second	And the standing of the sta		<text><text></text></text>	<text><text></text></text>	And registrational and regist	And registrational and regist	And region and a development of the second o	Statistics and the statistic and the statisti	And the second s
And the standing of the stand	And the second	And the standing of the standi	And the standing of the standi	And the standing of the standi	And the standing of the standi	And the standing of the standi	And the standing of the standi	And the standing of the standi	And the standing of the standi	And the standing of the stand	And the second and th	And the second s
Standard Stand Standard Standard S	And the standard sta	and a set of the set		and an				and a set of the set	and a set of the set	Standard Stand Standard Standard S	And the second	An en
 A standard stan								An example of the strength o	An example of the strength o	 A standard stan	And the second	
	And the second											Note that the second s
And and a work of the formation of the f	An array water and a straight of the straighto									And and a work of the formation of the f	And each of any of a constraint of a constrain	And an
	And and a way way way way way way way way way w										And and the ansate of the ansa	And a the structure struct
All and the answer of the answ	And and a way way way way way way way way way w	All arts variable and variable	All arts variables and the second variables an					All and the answer an	All and the answer an	All and the answer of the answ	And and a way and a many and a ma	And an the university of the second s
				And the formation of th		And the second of the second o	And the second of the second o				And a data sector and a data s	And the first operation of the second
	And the second s					And the second of the second o	And the second of the second o				And a data sector and a data s	And the first operation of the second
								Standard Control Co	Standard Control Co		And each operation of the second operation operation of the second operation opera	And the first of t
		And the second of the second o	And the second of the second o		An and a set of the s	An and a standard	An and a standard	Set of the set of t	Set of the set of t		the market of the sector of t	Statistical Control
					<text><text><text><text></text></text></text></text>			Martine State S	Martine State S		and an and a set of	and eine an
		And an and a set of the set of			<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>				Between the structure of the structur	 A standard and a standa
				<text><text><text></text></text></text>							And and a state of	 Beneficial de la construcción de la co
			<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>		And and a start of	And and a start of	<text><text><text></text></text></text>	<text><text><text></text></text></text>		And and a stand a s	 Beneficial State State
		<text><text><text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>		And and a start	And and a start	<text><text><text></text></text></text>	<text><text><text></text></text></text>		And the stand	Berger and State Stat
			<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text></text></text></text>	<text><text><text><text></text></text></text></text>		And and a stand a s	and print and
	 And the stand st	<text><text><text></text></text></text>	<text><text><text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>		 Between statutes and statutes a	 Between the structure of the structure of
An off of the strategies and		<text><text><text></text></text></text>	<text><text><text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	An off of the strategies and	 And and an and an and an and an and and a	And the state of the state
An off of the strategies and		<text><text><text></text></text></text>	<text><text><text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	An off of the strategies and	 And and an and an and an and an and and a	And the state of the state
An off of the strategies and		<text><text><text></text></text></text>	<text><text><text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	An off of the strategies o	 And and an and an and an and an and and a	And the state of the state
				<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>		And and a standard	and the descent of the strength of the stren
			<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>		<text><text><text></text></text></text>	<text><text><text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>		And the stand build b	Berger A. Start Sta
			<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	And and a start	And and a start	And and a start	<text><text><text></text></text></text>	<text><text><text></text></text></text>		And the stand	Berger and State Stat
			<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	And and a construction of the second of t	And and a start of	And and a start of	<text><text><text></text></text></text>	<text><text><text></text></text></text>		And and a stand a s	 Beneficial de la construcción de la co
				<text><text><text></text></text></text>							And and a state of	 Beneficial de la construcción de la co
						and an an and an an an and an	and an an and an an an and an					The second secon
		And an and a set of the set of			<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>				Between the structure of the structur	 A standard and a standa
					<text><text><text><text></text></text></text></text>			Martine State S	Martine State S		and an and a set of	and eine an
		And the second of the second o			<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>				Set and the set of	 Barting and an an and an and an an and an an and an an an an an and an an
		And the second of the second o			<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>	<text><text><text><text></text></text></text></text>				Set and the set of	 Barrier and an an and an and an an and an an and an an an an an and an an
				An example of the second secon		Barter Standbart Standb	Barter Standbart Standb	An example of the second secon	An example of the second secon			The second secon
				An example of the second secon		Barter Standbart Standb	Barter Standbart Standb	An example of the second secon	An example of the second secon			The second secon
				An example of the second secon	<text><text><text></text></text></text>	<text><text></text></text>	<text><text></text></text>					The second secon
		And an and a set of the set of th			<text><text><text><text></text></text></text></text>	<text><text><text></text></text></text>	<text><text><text></text></text></text>				Set and a set	 Barting and an an and an and an an and an an and an an an an an and an an
				An example of the second secon	<text><text><text></text></text></text>	<text><text></text></text>	<text><text></text></text>					The second secon
		And the set of the set			<text><text><text><text></text></text></text></text>	<text><text><text></text></text></text>	<text><text><text></text></text></text>				Set and a set	 Barting and an an and an and an an and an an and an an an an an and an an
		And the set of the set			<text><text><text><text></text></text></text></text>	<text><text><text></text></text></text>	<text><text><text></text></text></text>				Set and a set	 Barting and an an and an and an an and an an and an an an an an and an an
					<text><text><text><text></text></text></text></text>			An and a set of the se	An and a set of the se		and an and a set of	and an early a set of a set o
		And the second of the second o	And the sector of the sector o	And and a set of a	An and a set of the	And an and a set of a set o	And an and a set of a set o	Statistics and sta	Statistics and sta		the market of the sector of t	Statistical Control
		And the second of the second o	And the second s	An example of the sector of th	And an and an	And the second of the second o	And the second of the second o	Standard Standar Standard Standard S	Standard Standar Standard Standard S		the market of t	Martine Carlos Carlo
		And the second of the second o	And the second s	An example of the sector of th	And an and an	And the second of the second o	And the second of the second o	Standard Standar Standard Standard S	Standard Standar Standard Standard S		the market of t	Martine Carlos Carlo
		And the stand an	And end the under a second the u	And end the unit of the unit o							And and the second and a second	And have a set of the
		An and a set of the se	And the sector of the sector o	And the sector of the sector o	An and a set of the	And an and a set of a set o	And an and a set of a set o	Statistics and sta	Statistics and sta		the market of the sector of t	Statistical Control
		And the second of the second o	And the sector of the sector o	And the sector of the sector o	An and a set of the	And an and a set of a set o	And an and a set of a set o	Statistics and sta	Statistics and sta		the market of the sector of t	Statistical Control
					<text><text><text><text></text></text></text></text>			An and a set of the se	An and a set of the se		and an and a set of	and an and an and and and and and and an
					<text><text><text><text></text></text></text></text>			An and a set of the se	An and a set of the se		and an and a set of	and an and an and and and and and and an
		An example of the second secon		An example of the second secon	<text><text><text><text></text></text></text></text>	An and a set of the se	An and a set of the se				and an and a set of	and an early a constraint on the first on t
		And the sector of the sector o			<text><text><text></text></text></text>	<text><text><text></text></text></text>	<text><text><text></text></text></text>				and an and a set of a	Construction of the second of the secon
				And the set of the set	<text><text><text></text></text></text>							 Beneficial de la construction de la co
								The section of the	The section of the		The second se	The second se
								The section of the	The section of the		The second se	The second se
								The section of the	The section of the		The second se	The second se
				And the set of the set	<text><text><text></text></text></text>	<text><text><text></text></text></text>	<text><text><text></text></text></text>					 Bergersen and Bergersen and Ber
		And the set of the set			<text><text><text></text></text></text>	<text><text><text></text></text></text>	<text><text><text></text></text></text>				and an and a set of a	Construction of the second of the secon
		And the sector of the sector o			<text><text><text></text></text></text>	<text><text><text></text></text></text>	<text><text><text></text></text></text>				and the set of the set	Status de la de
		And the second of the second o	And the sector of the sector o	And the sector of the sector o	And and a set of the set of th	And and a set of a	And and a set of a				and an example of the second	Starting and the sta
											Alte sich verschaften sich voll. Marie sich verschaften	And and the adversarial set of the set of th
And entry and en	And entry and en	And and the other set of the other set o	And and the answer an	And and the answer an		And and the answer of the answ	And and the answer of the answ	And and the analysis of the an	And and the analysis of the an	And entry and en	And and ender share and ender	And and the adversarial of the a
	And the second secon											And the second secon
The second se	Bernard B									The second se		And the second
And a set of the set	and a set of the set	and an and a standing of the	and an	and an	<text></text>	<text></text>	<text></text>	and an	and an	And a set of the set	And a set of the set	
And the standard s	And the standing of the stand	And the standing of the stand	And the standing of the stand	And a stand	And the standing of the standi			Statistical and the st	Statistical and the st	And the standard s	And the second and th	And the second s
And region and a final definition of the second definition of the secon	And region and the Product and the	And a straight of the strai	And a start of the start of	And a start of the start of	And the second s	And the standard and	And the standard and	And registry and the standing of the standi	And registry and the standing of the standi	And region and a final definition of the second definition of the secon	And the second s	And a series of the second sec
And region and a final definition of the second definition of the secon	And region and the Product and the	And a straight of the strai	And a start of the start of	And a start of the start of	And the standing of the sta	And the standard and	And the standard and	And registry and the standing of the standi	And registry and the standing of the standi	And region and a final definition of the second definition of the secon	Statistics and sta	And the second s
And region the Andread Constraints of the Andre	And the standing of the stand	and a sector of the sector o	And the second s	And the standing of the sta		And the second of the second o	And the second of the second o	And endowed and the strength of the strengt	And endowed and the strength of the strengt	And region the Andread Constraints of the Andre	And an and a straight of the straight of th	And a base of the second seco
And the second	And the standing of the stand	And the standing of the stand	And the standing of the stand	Statistical and the st	And the standing of the standi	<text></text>	<text></text>	Statistical and the st	Statistical and the st	And the second	And a second and a	And the second s
And the second	And the standing of the stand	And the standing of the stand	And the second	And the standing of the stand	And the standing of the standi	<text><text></text></text>	<text><text></text></text>	And the standing of the stand	And the standing of the stand	And the second	And a second and a	And the second s
And region to a short whether the short whether	And the standing of the standi	And region to a subject of the subj	And region the Monthead Strategies and the Monthead Strate	And endowed and the strength of the strengt	And an experimental strategy of the strateg	And region the analysis of the	And region the analysis of the	And endowed and the strength of the strengt	And endowed and the strength of the strengt	And region to a short whether the short whether	And a second and a	And the second s
And the second	And the standing of the stand	and a set of the set	And the second s	And the standing of the sta	And an expension of the second	And the second of the second o	And the second of the second o	And endowed and the strength of the strengt	And endowed and the strength of the strengt	And the second	And an and a straight of the straight of th	And a base of the second seco
And the second	And the standing of the stand	and a sector of the sector o	And the second s	And the standing of the sta		And the second of the second o	And the second of the second o	And endowed and the strength of the strengt	And endowed and the strength of the strengt	And the second	And an and a straight of the straight of th	And a base of the second seco
And the second	And the standing of the stand	and a set of the set	And the second s	And the standing of the sta	And the second s	And the second of the second o	And the second of the second o	And endowed and the strength of the strengt	And endowed and the strength of the strengt	And the second	And an and a straight of the straight of th	And a base of the second seco
And region to a short whether the short whether	And the standing of the standi	And a set of the set	And the second s	And a start of the start of		And an and a strategies of the	And an and a strategies of the	And endowed and the strength of the strengt	And endowed and the strength of the strengt	And region to a short whether the short whether	And a second sec	And the second
And region to a short whether the short whether	And the standing of the standi	And region to a subject of the subj	And region the Monthead Strategies and the Monthead Strate	And endowed and the strength of the strengt	And an experimental strategy of the strateg	And region the analysis of the	And region the analysis of the	And endowed and the strength of the strengt	And endowed and the strength of the strengt	And region to a short whether the short whether	And a second and a	And the second s
And region a standard devices of the standard device	And region to a field of the field of t	And a construction of the	And a specific provide the	And a start of the start of	And the second s			And a start of the start of	And a start of the start of	And region a standard devices of the standard device	Statistics and sta	And a set of the set o
And region to a strategies of the strategies of	And region to a strategies of the strategies of	And registion to according to the second	The second se		And the second secon	<text><text></text></text>	<text><text></text></text>			And region to a strategies of the strategies of	And the second s	And the second and th
And any constraint of the second of the s	And the second seco	The second se	The second se	The second se	And the second s	And a figure a solution of the	And a figure a solution of the	The second se	The second se	And any constraint of the second of the s	And the second secon	And a figure start in the start and a star
And a set of the se	And a set of the se	And the second s	And the second s	And an appropriate the standard of the stan	And the second s	And the second s	And the second s	And an appropriate the standard of the stan	And an appropriate the standard of the stan	And a set of the se	Statistical and the sta	And registry and the formation of the second secon
And the second secon	And the American Strategy and the America	And the second s	And the second s	And the second s	And the second secon	And the second s	And the second s	And the second s	And the second s	And the second secon		And and a set of a first set of a first set of a
And the factor of the factor o	And the factor and th	And the fragmentational of the second of the	And the Advance of	And the Andrewski and the Andr	And the Advances of the Adv	And the Alexandramical	And the Alexandramical	And the Andrewski and the Andr	And the Andrewski and the Andr	And the factor of the factor o	And the second secon	And Andread Andre
And the factor of the factor o	And the factor and th	And the second secon	And the second secon	And the second secon	Note: A set of the	Note: A set of the	Note: A set of the	And the Andrewski and the Andr	And the Andrewski and the Andr	And the factor of the factor o	And the second secon	And and you say the Argonization and the Argonizati
And the second secon	And the second secon	And the second s	And the second of the second o	And the second of the second o	And the second s	And the second secon	And the second secon	And the second s	And the second s	And the second secon		And and a set of a formation of the set of t
And the second secon	And the American Strategy and the America	And the second s	And the second s	And the second s	And the second secon	And the second s	And the second secon	And the second s	And the second s	And the second secon		And and a set of a first set of a first set of a
And experimentation of a state of the sta	And a second	And a strategy of the strat	And the standing of the sta	And a standard and	And the second s	And regard the strength of the	And regard the strength of the	And a standard and	And a standard and	And experimentation of a state	Statistical and the sta	And an and a set of the set of t
And a set of the se	And the second s	And the second secon	And the second secon	And the second secon	And the second s	And the second s	And the second s	And the second secon	And the second secon	And a set of the se	Statistical and the sta	And registry and the formation of the second secon
And region and a final definition of the second definition of the secon	And region and a final definition of the second definition of the secon	And a construction of the construction of t	And registry and the strength of the streng	The second se	And the second secon	And the standing of the sta	And the standing of the sta	The second se	The second se	And region and a final definition of the second definition of the secon	And the second and th	And a construction of the
And experimentation of a state	And a second	And the second s	And the standing of the sta	And the second secon	And the second secon	And the second secon	And the second secon	And a standard and	And a standard and	And experimentation of a state	And the second secon	And the second
And the second secon	And the second secon	And the second s	And the second of the second o	And the second of the second o	And the second s	And the second secon	And the second secon	And the second s	And the second s	And the second secon		And and a set of a formation of the set of t
And the second secon	And the second secon	And the second s	And the second of the second o	And the second of the second o	And the second s	And the second secon	And the second secon	And the second s	And the second s	And the second secon		And and a set of a formation of the set of t
And the second secon	And the second secon	And the second s	And the second of the second o	And the second of the second o	And the second secon	And the second secon	And the second secon	And the second s	And the second s	And the second secon	And the second secon	And and a set of a se
And experimentation of a state	And the second secon	And a set of the se	And the standing of the sta		And the second secon	And the second of the second o	And the second of the second o	And the standing of the sta	And the standing of the sta	And experimentation of a state of the sta	And the second secon	And the second s
And region to a the Andread Control of the A	And region and the Product and and the Andread Control of the Andrea	And a construction of the construction of t	And end of the standard s	<text><text></text></text>	And the second secon	<text><text></text></text>	<text><text></text></text>	<text><text></text></text>	<text><text></text></text>	And region and a final definition of the second definition of the secon	And the second and th	And a construction of the

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)





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 (C20	:)	
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	No.	
Other	7.3 %	168 million \$
Total:	7.3 %	168 million \$



(taken from http://www.securityaffairs.com/)

Malware Market (II)

An incipient well-profit market: economic damages



Outline

Background

- What is a malware?
- Types of malware
- But... from where?

Objectives of malwareMalware goals

Malware Market

Spreading mechanisms

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?

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



Spreading mechanisms

How the hell did it comes here?

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



Spreading mechanisms

How the hell did it comes here?

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



Spreading mechanisms

How the hell did it comes here?

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



Outline

Background

- What is a malware?
- Types of malware
- But... from where?

Objectives of malwareMalware goals

Malware Market

Spreading mechanisms

Preventing mechanisms



Preventing mechanisms



Some useful preventing techniques

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



Some useful preventing techniques

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



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 \rightarrow "Force Quit" ... (MacOS)
 - \$ps | aux (MacOS & Linux)

3rd June, 2012 18 / 20



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 \rightarrow "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?



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 \rightarrow "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





R.J. Rodríguez

Avoiding to be infected by malware

3rd June, 2012 19 / 20

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 de Zaragoza Zaragoza, Spain

3rd June, 2012

Ethical Hacking and Cyber Security Cardiff, United Kingdom