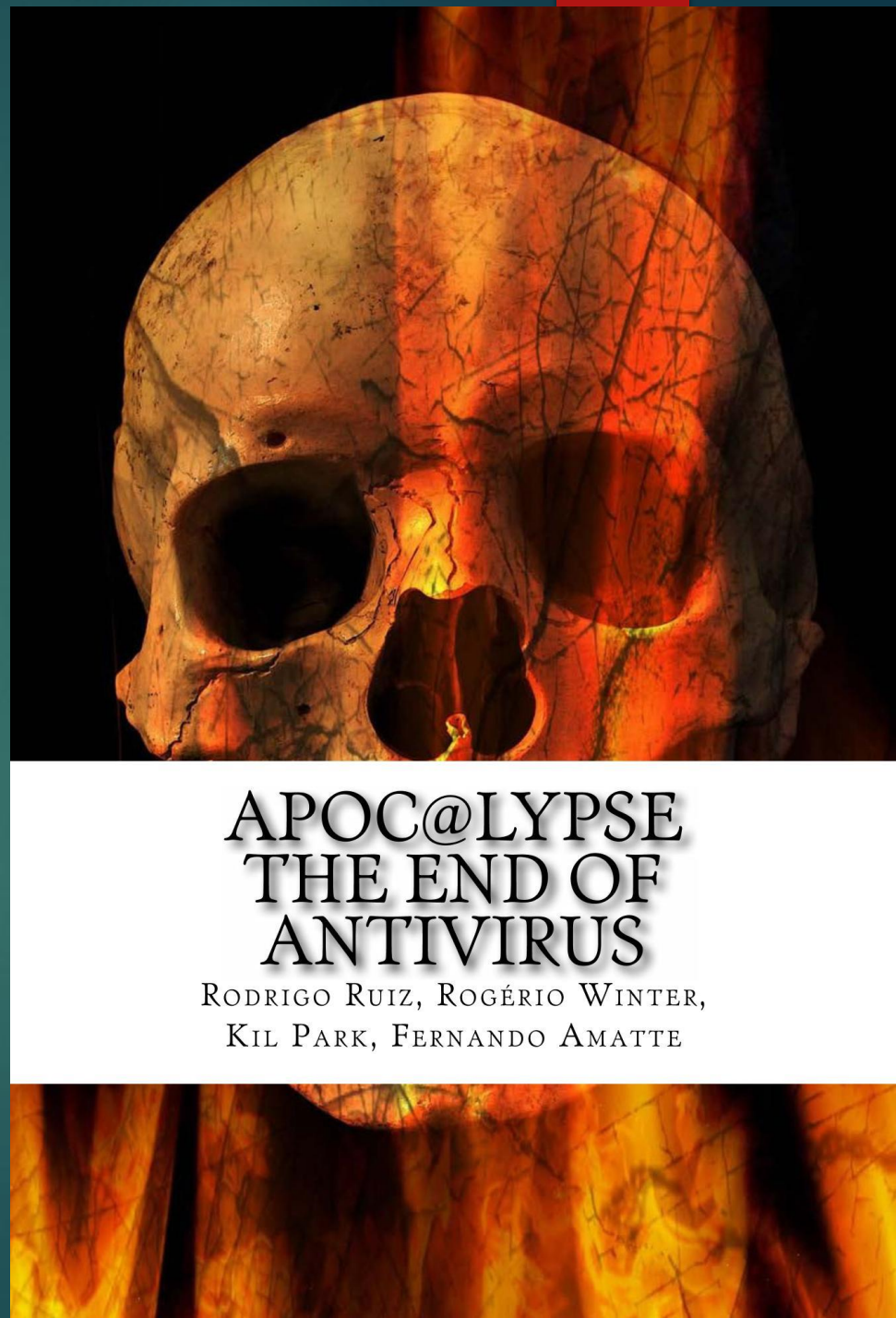
Do you believe in your protect system?

ROGERIO WINTER

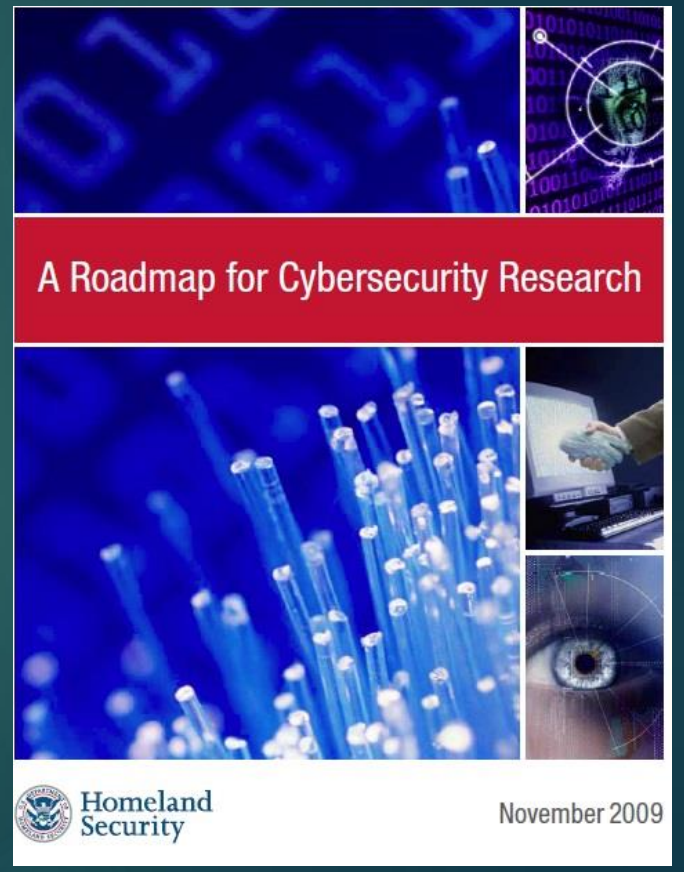


Agenda

- Introduction of theme
- What **IS NOT** Apoc@lypse Technique?
- What **IS** Apoc@lypse Technique?
- Conclusions and Questions
- Prize Book

Hard Problems

1. Scalable trustworthy systems (including system architectures and requisite development methodology)
2. Enterprise-level metrics (including measures of overall system trustworthiness)
3. System evaluation life cycle (including approaches for sufficient assurance)
4. Combatting insider threats
5. Combatting malware and botnets
6. Global-scale identity management
7. Survivability of time-critical systems
8. Situational understanding and attack attribution
9. Provenance (relating to information, systems, and hardware)
10. Privacy-aware security
11. Usable security



Think about it

- Are you sure that your systems are protected?
- Do we really test our protections properly?
- How are we testing our systems?
- **Are concepts in computer science consolidated or are they eventually reviewed and questioned?**

Microsoft patches critical bug that affects every Windows version since 95

- a serious flaw that existed for almost:
- **19 YEARS**
- November 12, 2014

Brazil Method of anti-malware test

- Brazil Method anti-malware test and the implications for cyber defense XVI Symposium of Operational Applications in Areas of Defense (SIGE) - Aeronautics Institute of Technology (Brazil),2014.
- Antonio Montes Filho, **Rogério Winter , Rodrigo Ruiz, Fernando Pompeo Amatte** , José Geremonte Garcia, Bruna Stefani de Oliveira Martins

Anti-malware –detection rate

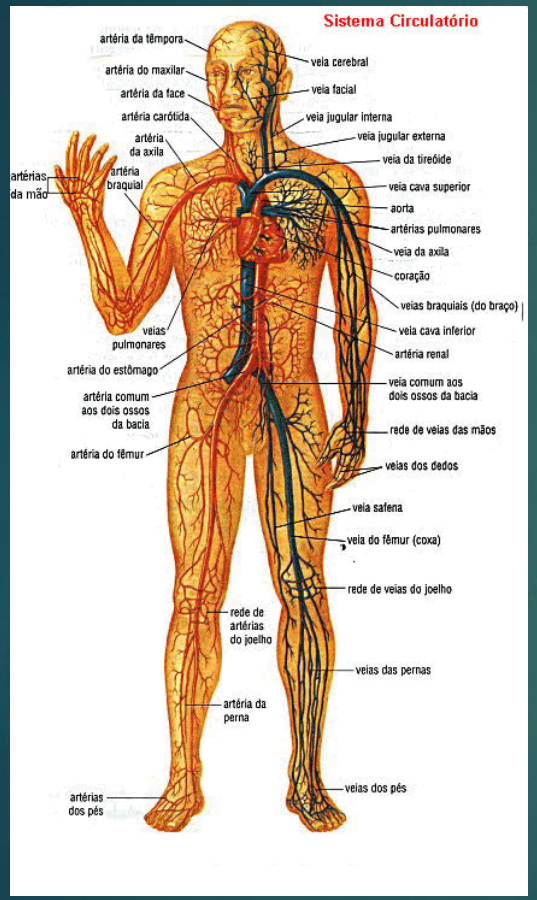
What **is not** Apoc@lypse Technique?

- The Apoc@lypse Technique is not a malware

What is the Apoc@lypse?

- A cyber autoimmune disease
- What is a autoimmune disease?
- What is a cyber autoimmune disease?
- Proof-of-concept

Human immune system X Cyber immune system

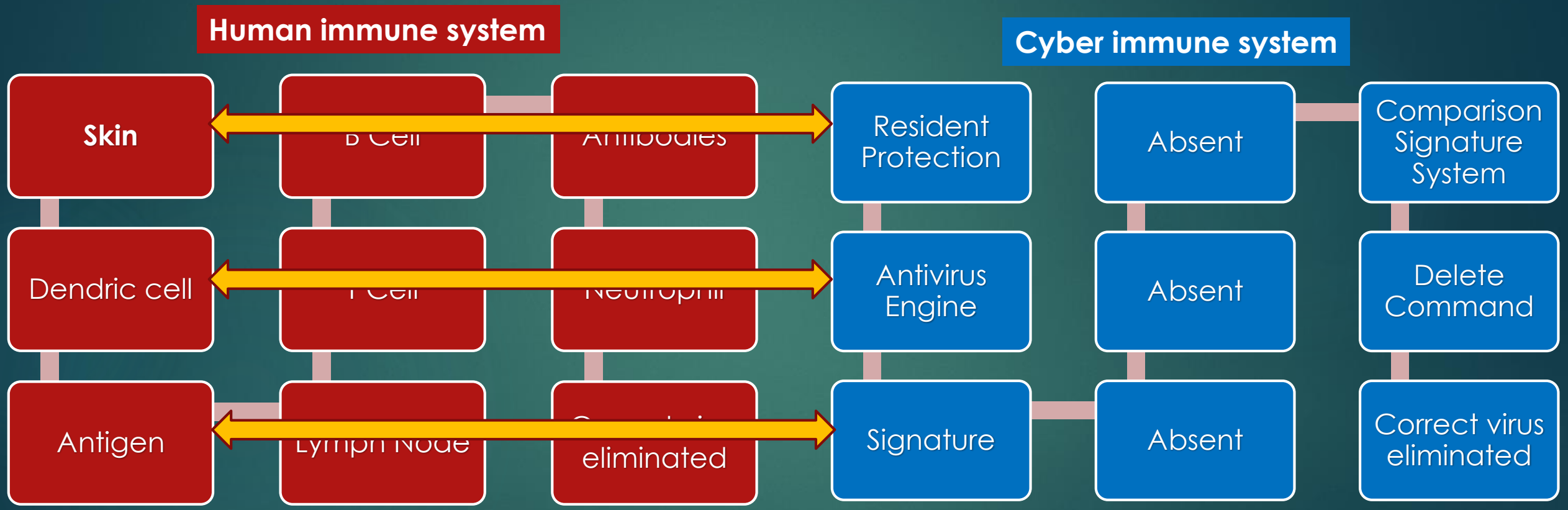


X

What is Autoimmune Disease ?

Autoimmune disease is a disease in which a person's immune system wrongly attacks its own healthy cells and tissues

Human X Cyber Body



What is the Apoc@lypse?

- Apoc@lypse technique is a proof-of-concept of **Autoimmune Cyber Disease**
- Bioinspired technique
- The technique shows a misconception of signature appoach

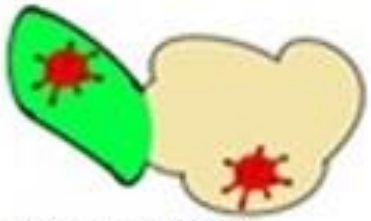
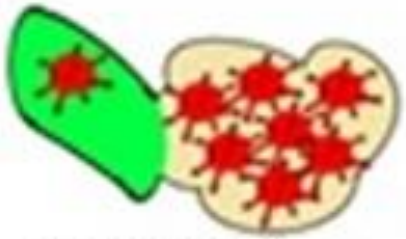
Events and action

Element/action	Biological	Cyber Equivalence	Antivirus action	Antivirus Attitude
	Virus	Malware	REMOVE FILE	RIGHT
	Harmless bacterium	Commands in BAT file	NO THREATS FOUND	RIGHT
	Bacterium infected to transport DNA of virus	Commands in BAT file that is transporting malicious code	NO THREATS FOUND	WRONG

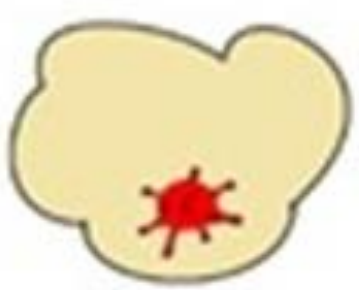
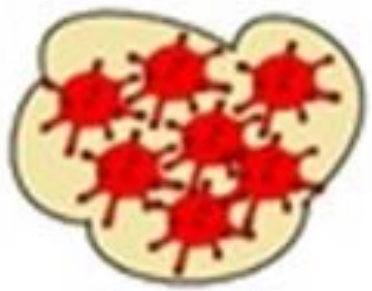
Events and action

Element/action	Biological	Cyber Equivalence	Antivirus action	Antivirus Attitude
	host	Any benign program used for transport of the bacterium BAT	NO THREATS FOUND	RIGHT
	Infected host	Infected program that transport the bacteria which was contaminated with DNA of virus	NO THREATS FOUND	WRONG
	Healthy cell	Any user file, software, or operating system	NO THREATS FOUND	RIGHT

Events and action

Element/action	Biological	Cyber Equivalence	Antivirus action	Antivirus Attitude
 PROCESS OF INFECTION	Bacterium transmitting the DNA	Commands in BAT file	NO THREATS FOUND	WRONG
 PROCESS OF INFECTION	Bacterium transmitting the DNA of the virus for the cell in invasive way	Commands in BAT file	NO THREATS FOUND	WRONG

Events and action

Element/action	Biological	Cyber Equivalence	Antivirus action	Antivirus Attitude
	Cell infected with the virus in a noninvasive way	Any user file, programs, or operating system file	REMOVE FILE	WRONG
	Cell infected with the virus in invasive way	Any user file, or operating system file	REMOVE FILE	RIGHT

How does the miracle occur?

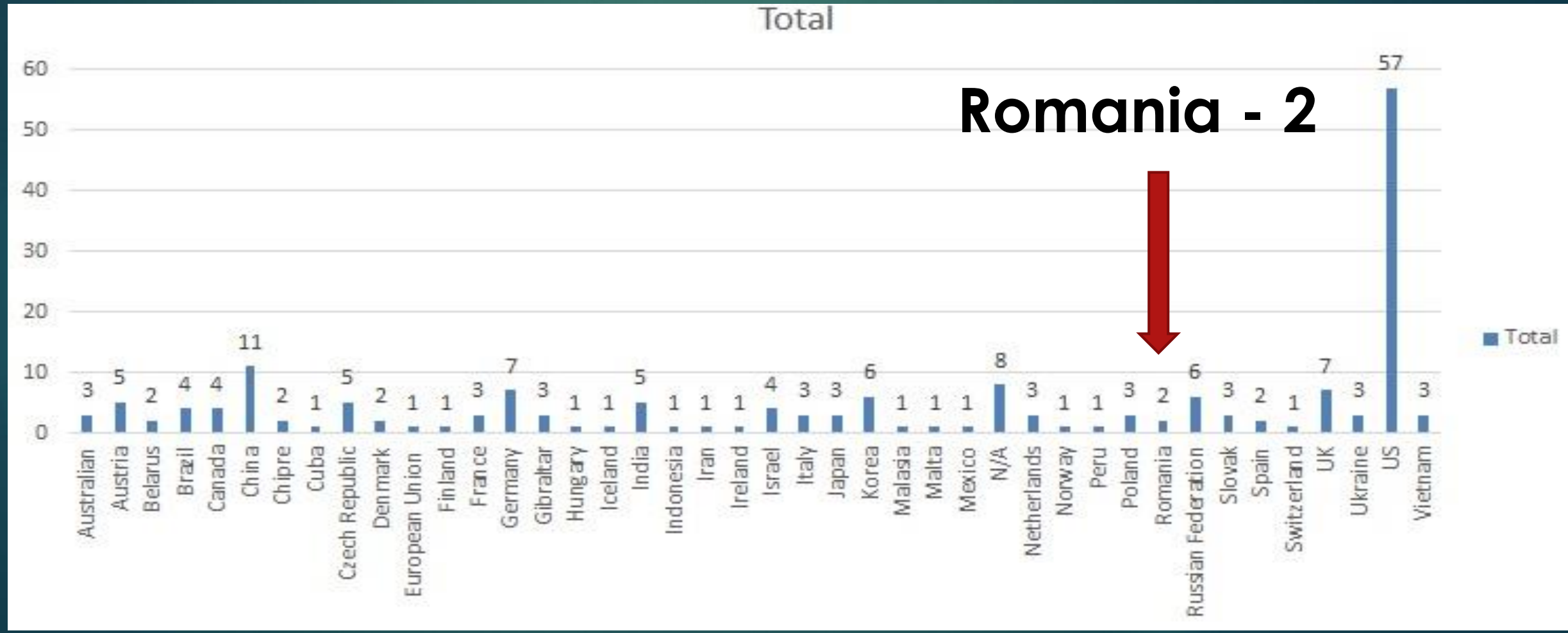
- The bacterium will guarantee a camouflage and protection of the virus
- We can use any part of the malicious DNA
- DNA virus selected - some antivirus will be affected and others not
- But….There is a special DNA that affects all

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Proof of concept of Apoc@lypse

- We can demonstrate that is possible to take control of anti-malware system and to command operating system destruction
- The Apocalypse Technique is effective in Windows, Linux, Android, UNIX and Mac
- We tested 150 anti-malware system existing in the international market

Geographical distribution



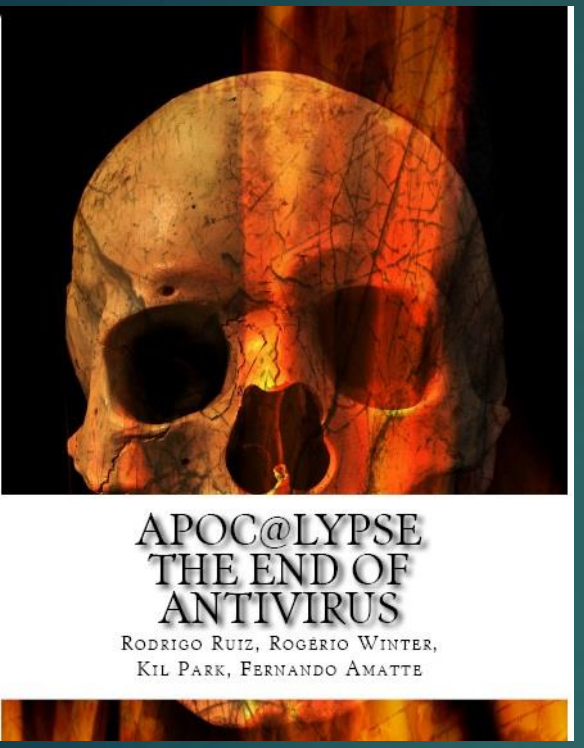
How apoc@lypse will affect:

- People?
- Companies?
- Government?
- signatures and hashes to identify and distinguishes the appearance, and not the attitude of software
- Even the heuristic concept carries with the detection of several indicators of a signature or stereotype of a threat

What will you do?

- You will either use it or not

Conclusion



Learn more about Apoc@lypse

- https://www.createspace.com/5603067
- http://www.amazon.com
- https://www.facebook.com/apocalypseantivirus

Please, feel free to contact me:

- Email: rogwinter@gmail.com
- Skype: rog.winter
- Twitter:@rogwinter
- Linkedin

Questions?

Prize book

Apoc@lypse: the end antivirus