MALWARE: Threats and Attacks

Part 1-A: Anatomy of Malware

Presented by:

Eleni Vasalou & Periklis Brentakis
Senior undergraduate students
Dept. of Informatics & Comp. Technology
T.E.I. of Western Macedonia, Greece

Reviewed by:

Spyridon Nikolaou, MSc
Lecturer,
Dept. of Informatics & Comp. Technology
T.E.I. of Western Macedonia, Greece

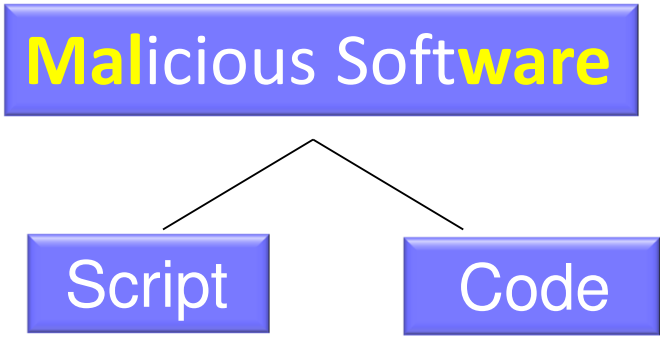
ERASMUS INTENSIVE PROGRAMME
The Information Warfare, Cyber Warfare and Open Sources Intelligence: An Interdisciplinary Approach
16 - 29/4/2012
Yasar University, Izmir, Turkey

Outline

- What is Malware
- Virus Analysis
- Worms
- Trapdoor / Backdoor
- Spyware
- Malware's Lifetime Phases
- Boot Sector Viruses
- Types of Malware
- Standard Criteria
- Trojan Horses
- Botnets / Zombies
- Adware
- Malware attachments
- Conclusions

What is Malware

- Contains harmful bugs
- Disguised as genuine software
- Not easily detectable
- Hackers use drive-by malware to spread



- Exists in order to harm our computers
- Behaves in unexpected ways
- Can do anything any other program can
- Predictability of a 2-years-old child
- Runs under the users authority
- It can do exactly what the user can do

Types of Malware

- Virus
- Worm
- Trojan Horses
- Logic Bomb
- Backdoor (Trapdoor)
- Mobile Code
- Exploits
- Downloaders
- Virus generator Kit
- Auto-rooter
- Flooders
- Keyloggers
- Rootkit
- Zombie, botnet
- Spyware
- Adware

Virus Analysis #1

- A virus can replicate itself
- Viruses are insidious
- Infection usually spreads at a geometric rate

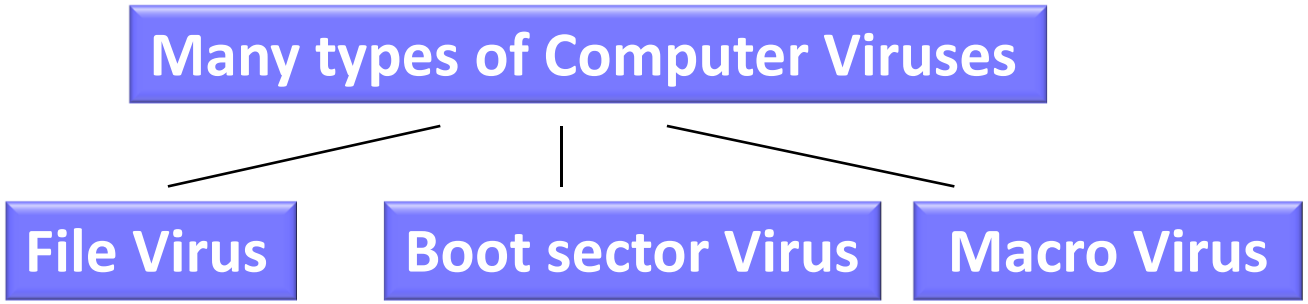
Malicious Software

- Transient Program
- Resident Program

- Transient – They need a host to exist (Viruses, Logic Bombs, Trapdoors)
- Resident – They can exist on their own (Worms , Zombie)

Virus Analysis #2

- Virus is an executable program
- Able to replicate itself
- Can be introduced along with any software program
- It can attach itself to or sometimes replace an existing program
- Contains infructions to initiate some sort of event



Standard Criteria for making viruses

- It is hard to detect.
- It is not easily destroyed or deactivated.
- It spreads infection widely.
- It can reinfect its home program or other programs.
- It is easy to create.
- It is machine independent and operating system independent.

Worms

Spreads copies of itself through network

Works as a standalone program

Always cause at least some harm to the network

Are skilled enough to do serious damage such as:

- Destroying crucial files
- Slowing a system
- Forcing critical programs to stop

Common types of Worms

1. E-mail Worms
2. Instant Messaging Worms
3. Internet Worms
4. IRC Worms

Trojan Horses

- Looks like a useful file or software
- Designed to give full control of infected PC to another PC
- Takes its name from Greek Mythology

They can

- Make copies
- Steal information
- Harm their host computer system

- Comprised more than 80% of all computer malware detected in the world!
- Designed to provide some form of remote access
- Significantly advanced in their complexity, methods and payload

Backdoors / Trapdoors

They ‘ve been used in legal for many years

Insert during code development

Attackers use backdoors that they detect as part of an exploit

A backdoor is a security risk

They become threats if they are used for getting access to not-restricted information

Botnets / Zombies

Takes control of another computer through network

Most common use is Denial-of-Service attack (DoS)

Logic Bombs

Detonates when a specified condition occurs

Spyware

Similar to Adware but with malicious intent

May be installed on purpose from the computer owner

Monitor the activity of the user while on internet

Spyware can:

- Interfere with computer operations
- change settings
- bring up different home pages
- cause loss of internet service
- Interfere with the functioning of other installed programs

Classified as privacy-invasive software

Adware

Shows advertisements (invasive or non-invasive)

Downloading them without knowing about it

Often piggybacks on other program downloads that you want

Examples of freeware containing adware:

- Advanced search engines
- Instant news and weather updates
- Computer games
- Peer-to-peer(P2P) file sharing programs
- Fun mouse pointers, desktop themes and backgrounds
- Emoticons and smiles used in E-mail
- Applications that say they will improve the efficiency of your computer

Typical lifetime Phases of Malware

1) Dormant Phase

2) Propagation Phase

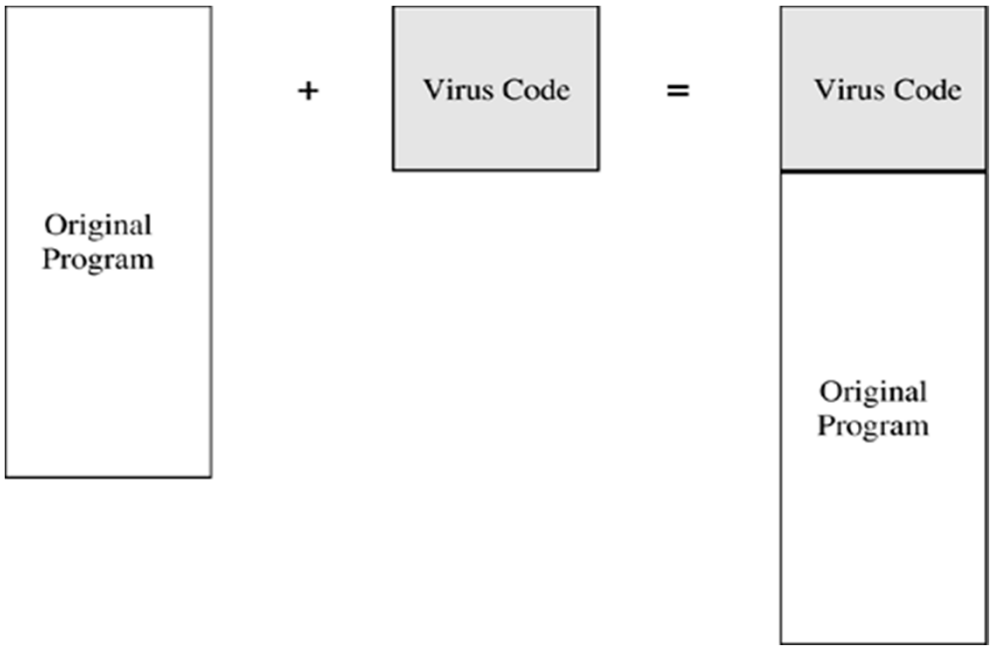
3) Triggering Phase

4) Execution Phase

How a virus can attach itself #1

Appends to a Program

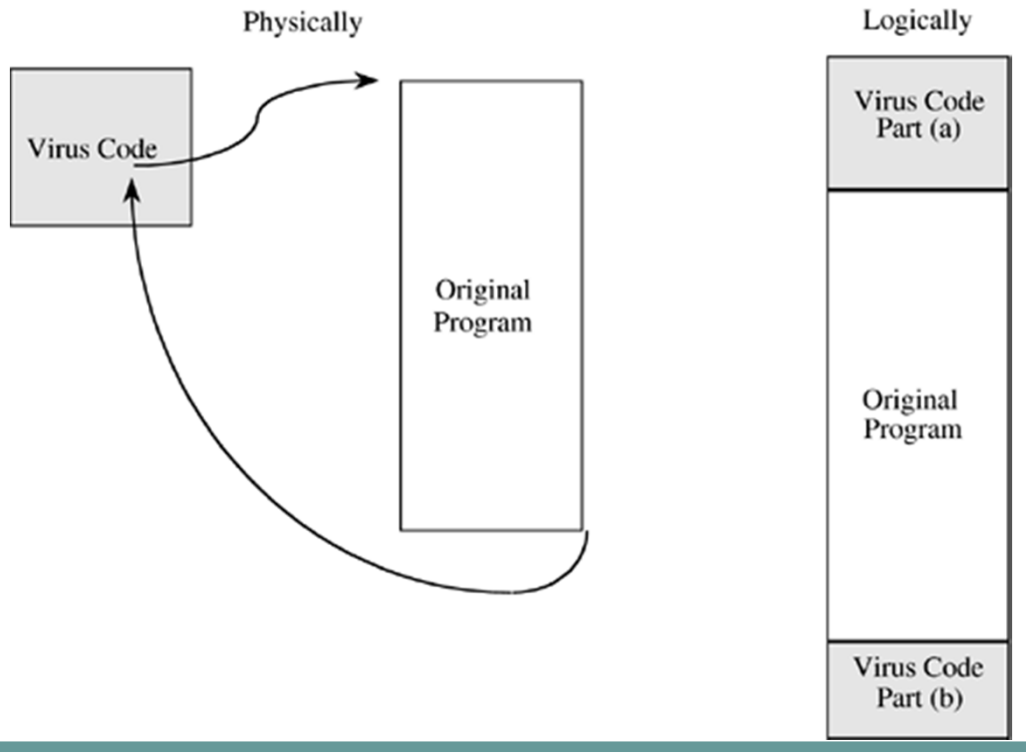
- It Stacks on a program and pretend being a part of it



How a virus can attach itself #2

Surrounds a Program

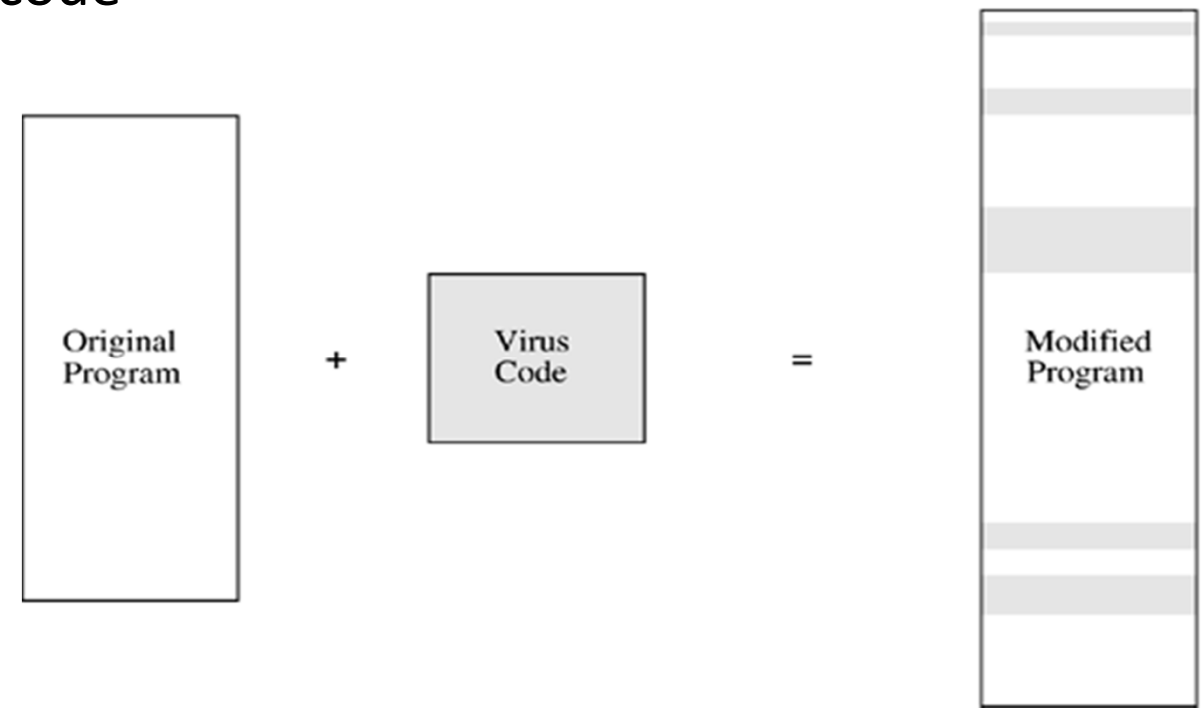
- It separates in two and stacks at the beginning and at the end of the program



How a virus can attach itself #3

Integration and Replacement

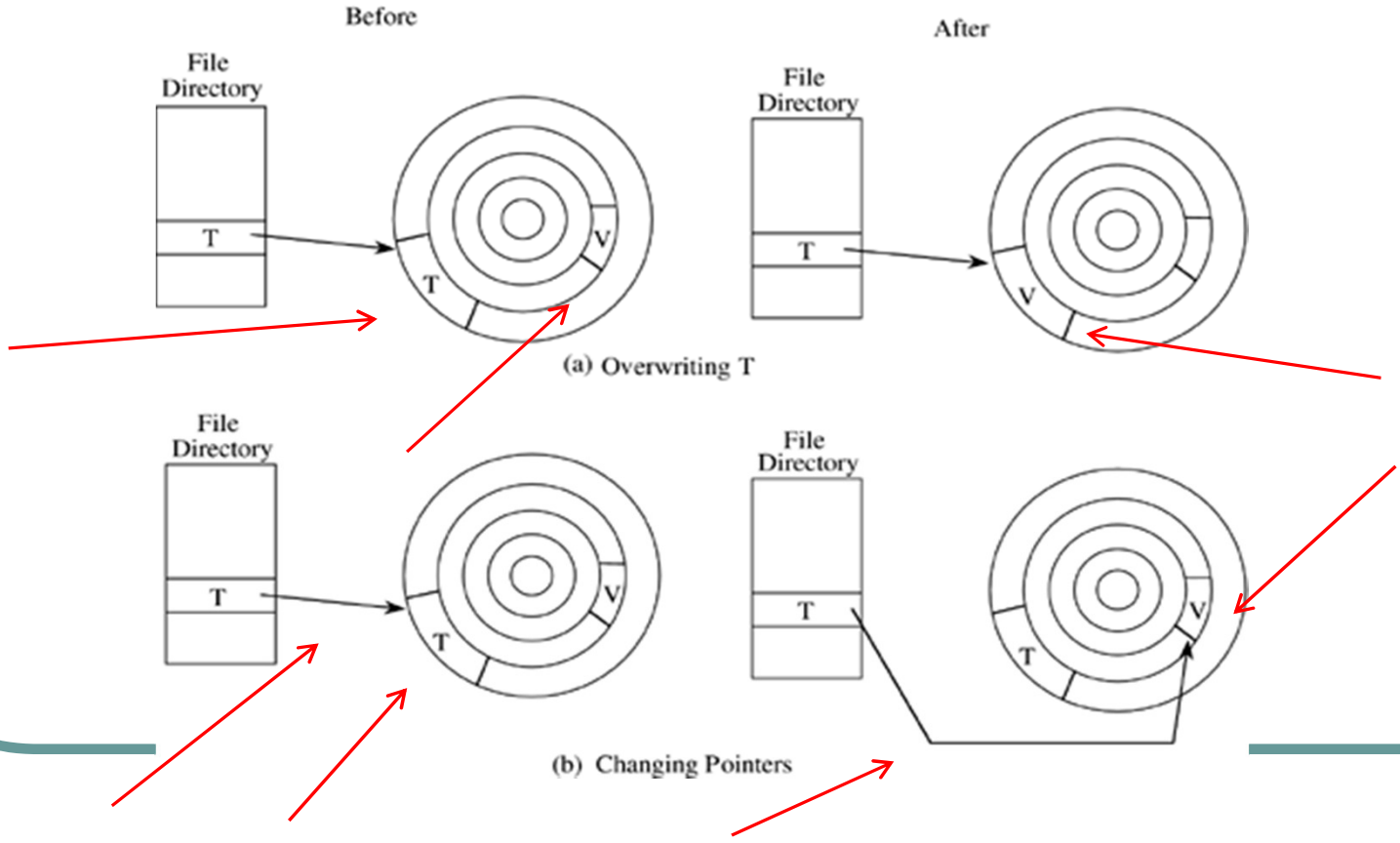
- It modifies the code of the program and getting mixed with its code



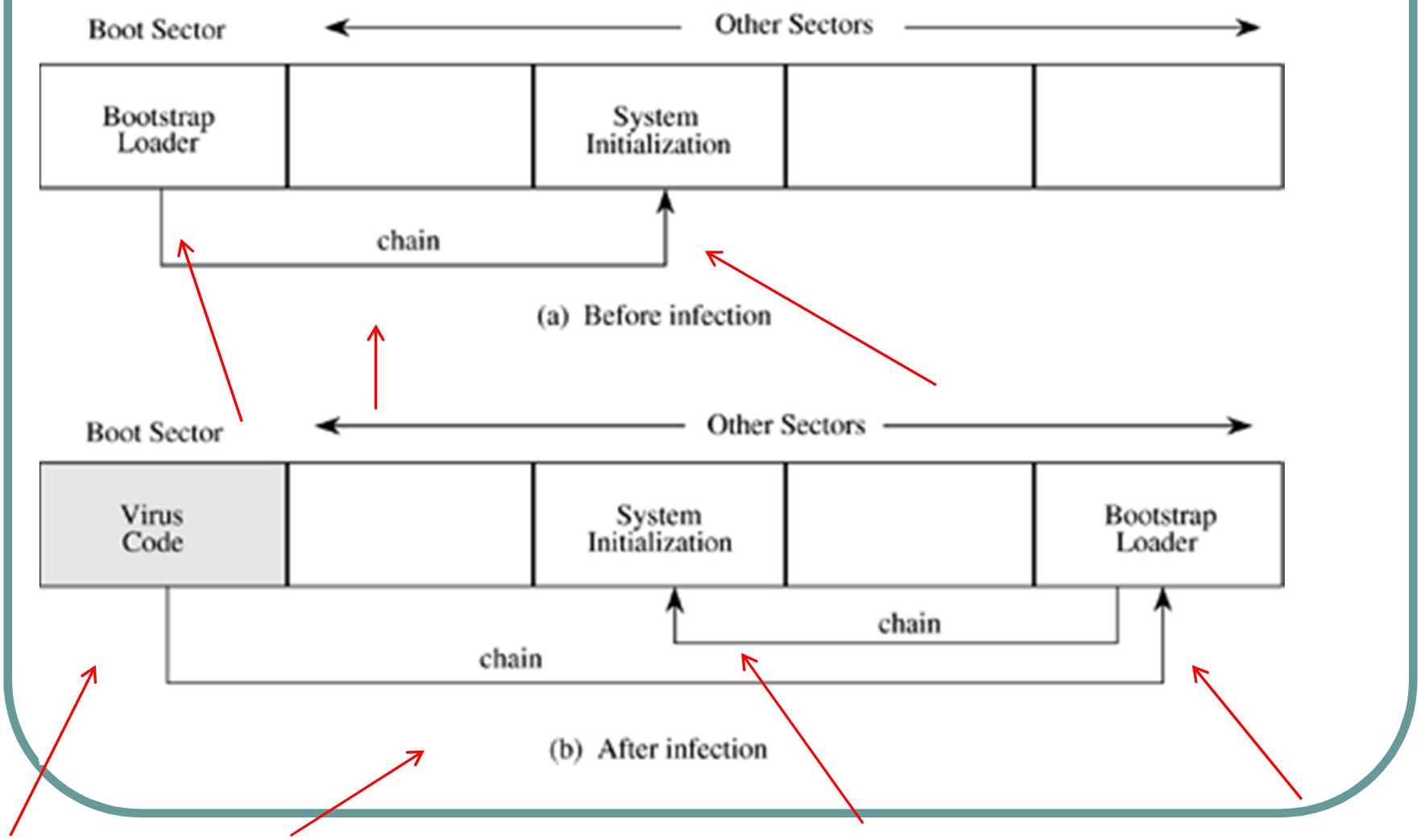
How a virus gains control

1) Renames itself as the target's program name

2) Changes the pointers in the table name



Boot Sector Viruses



Conclusions

Many ways of a virus to affect our computer → Hard to avoid being affected

We lack of protection in many parts:

1. Installation progress
2. Network Use
3. Boot sector

Its necessary to discover new ways of protection more capable and successful than today's

There is a high amount of people that work on Malicious Software and we could resemble them as "drug-addict's" which means that, with the passion that they work on it, it will keep developing in really fast tempo.

References

- Charles P. Pfleeger, Shari Lawrence Pfleeger, Security in Computing, 4th Edition, Prentice Hall, 2008, pp 111-144
- William Stallings, Network Security Essentials: Applications and Standards (4th Edition), Prentice Hall, 2011, pp 305-373
- Tech FAQ, "*Trojan Virus*", http://www.tech-faq.com/trojan-virus.html
- Tech FAQ, "*Computer Worms*", http://www.tech-faq.com/computer-worm.html
- Hong Kong University of Sciencce & Technology, "*What is Computer Virus?*", http://www.ust.hk/itsc/antivirus/general/whatis.html
- Hong Kong University of Sciencce & Technology, "*Types of Viruses*", http://www.ust.hk/itsc/antivirus/general/types.html
- Spam Laws, "*What is adware (Other Than Annoying)?*", http://www.spamlaws.com/what-is-adware.html
- Search Security, "*Back Door*", http://searchsecurity.techtarget.com/definition/back-door
- What Is My IP Address, "*What is Spyware?",* http://whatismyipaddress.com/spyware

MALWARE: Threats and Attacks

Part 1-B: Anatomy of Web Malware

Presented by:

Theodosios Okalidis
Senior undergraduate student
Dept. of Informatics & Comp. Technology
T.E.I. of Western Macedonia, Greece

Reviewed by:

Spyridon Nikolaou, MSc
Lecturer,
Dept. of Informatics & Comp. Technology
T.E.I. of Western Macedonia, Greece

ERASMUS INTENSIVE PROGRAMME
The Information Warfare, Cyber Warfare and Open Sources Intelligence: An Interdisciplinary Approach
16 - 29/4/2012
Yasar University, Izmir, Turkey

Outline

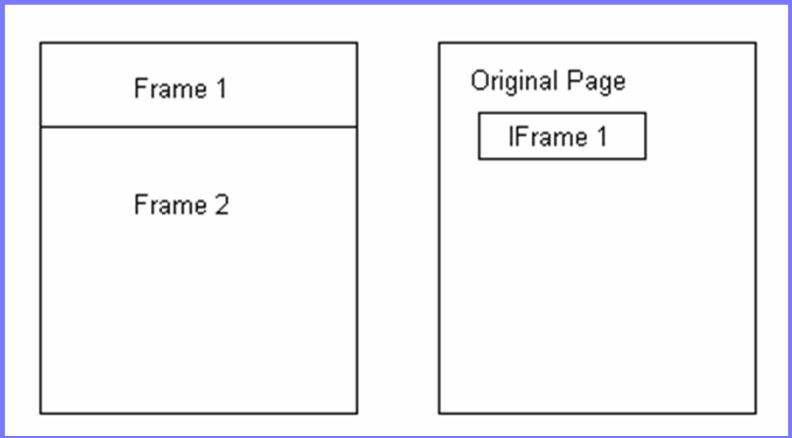
- Web malware and attacks
- Common Web malware-installation tactics
- Web server infections
- Preventing Web server infections
- Conclusion

Introduction to Web Malware

- Distribution through web browsers
- Not easily spread over the network
- Attackers compromise websites to distribute malware
- Attackers increase their profits

Web Malware Attacks

- The attacker must find a way to connect with the victim (e.g. social networks, instant messaging, loaded HTML code)
- The attacker must install malware on the victim's computer



Side-by-side illustration of traditional Frames versus Inline Frames

Common Web Malware-Installation Tactics

- Browser/Plug-in Exploits (“Drive-by” download)
  - Exploit vulnerabilities
- Social Engineering
  - Exploit natural human tendency to trust

Social engineering technique where attackers use a fake software update to trick users into installing malware

Web Server Infections

IFrame Distribution Tools

- Attackers:
  - use valid credentials to log on and make changes
  - use FTP service to capture legitimate credentials
  - purchase credentials from black markets
  - modify the server to distribute their IFrame
- In 2009 a command-and-control server contained credentials for 88,000 FTP servers

SQL Injection

- Vulnerability in Web applications
- Validation error
- Attackers:
  - infect thousands of Web servers
- In 2009, an attacker infected more than 125,000 Web pages

HTML Viruses

- Attaching to other files
- Inject into legitimate executable files and Web files
- Extensions:
  - htm -html -asp
  - aspx -php -jsp

Malvertising

Advertising firm outsources the job of finding ads

Vulnerability Exploitation

- Software vulnerabilities:
  - Operating system
  - Web server software
  - Web development platform (i.e. PHP, ASP)

- Result ⟶ unpatched systems

Preventing Web Server Infections

- Securing the Platform
- Secure Web Application Development Techniques
- Web Application Firewalls (WAFs)

Conclusion

- Defend against Web malware:
  - Secure Web server and application
  - Detect compromises early
  - Disinfect malicious content
  - Remain aware of the latest threats
- Defend a Web server
  - Secure administration and programming practices
  - Provide additional protection using a WAF

References

- Charles P. Pfleeger, Shari Lawrence Pfleeger, Security in Computing, 4th Edition, Prentice Hall, 2008, pp 111-144
- Verisign, An iDefense Focused Intelligence Report, The iDefense Intelligence Operations Team, January 2010, http://www.verisign.com/trust-seal/resources/whitepaper-web-malware.pdf

MALWARE: Threats and Attacks

Part 1-C: Stuxnet Worm

Presented by:

Sotirios Glykas
Senior undergraduate student
Dept. of Informatics & Comp. Technology
T.E.I. of Western Macedonia, Greece

Reviewed by:

Spyridon Nikolaou, MSc
Lecturer,
Dept. of Informatics & Comp. Technology
T.E.I. of Western Macedonia, Greece

ERASMUS INTENSIVE PROGRAMME
The Information Warfare, Cyber Warfare and Open Sources Intelligence: An Interdisciplinary Approach
16 - 29/4/2012
Yasar University, Izmir, Turkey

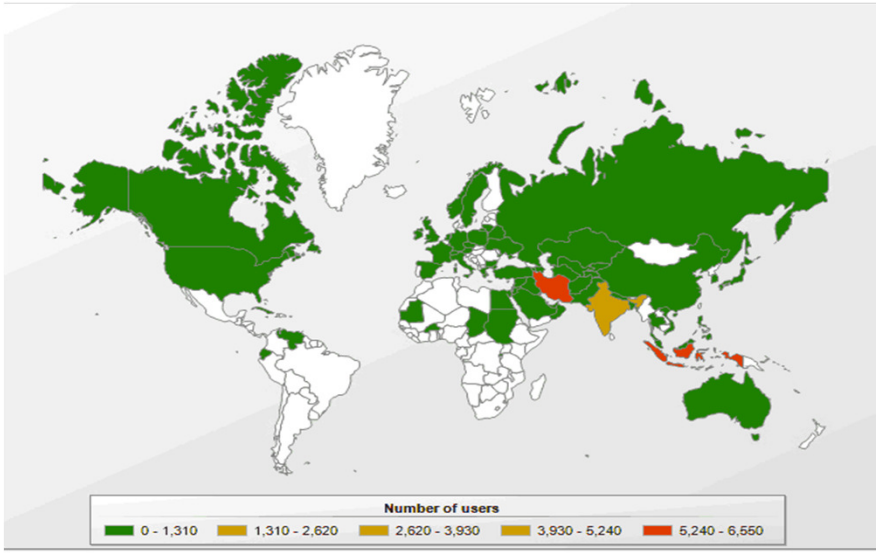
What is Stuxnet?

- Stuxnet achieved many things in the malicious code realm
- First to exploit 4 0-day vulnerabilities
- Compromised 2 digital certificates
- Injected code into industrial control systems and hid the code from operators.

Aspect	Stuxnet	Common malware
Targeting	Extremely selective	Indiscriminate
Type of target	Industrial control systems	Computers
Size	500 Kbytes	Less than 1 Mbyte
Probable initial infection vector	Removable flash drive	Internet and other networks
Exploits	Four zero-days	Possibly one zero-day

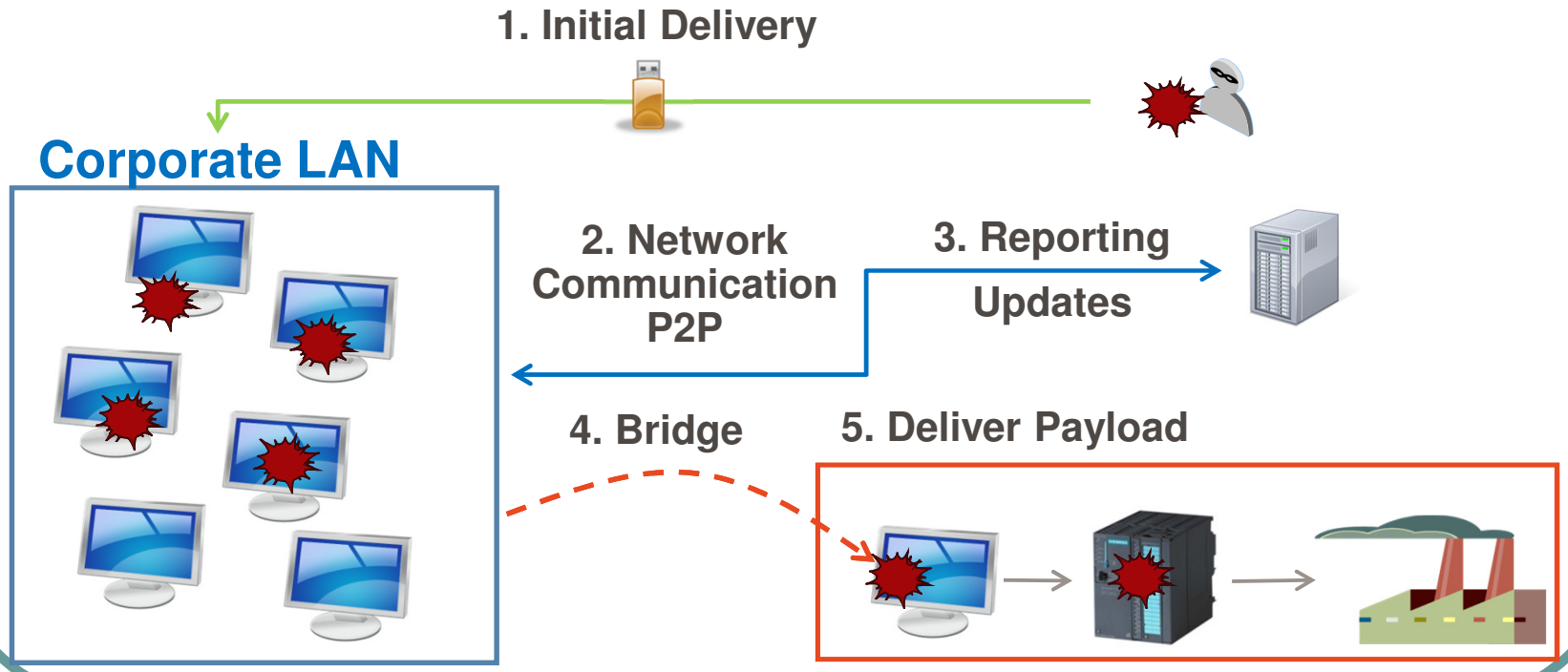
Stuxnet Purpose

- Infection criteria
  - Initial infection by removable flash drive
  - Windows rootkit prevents discovery
  - Stuxnet allows only 3 infections for 21 days
  - Spreads through Network Shares to other PCs
  - Seeks servers running Siemens WinCC for SQL injection
- The most likely target
- About the creators



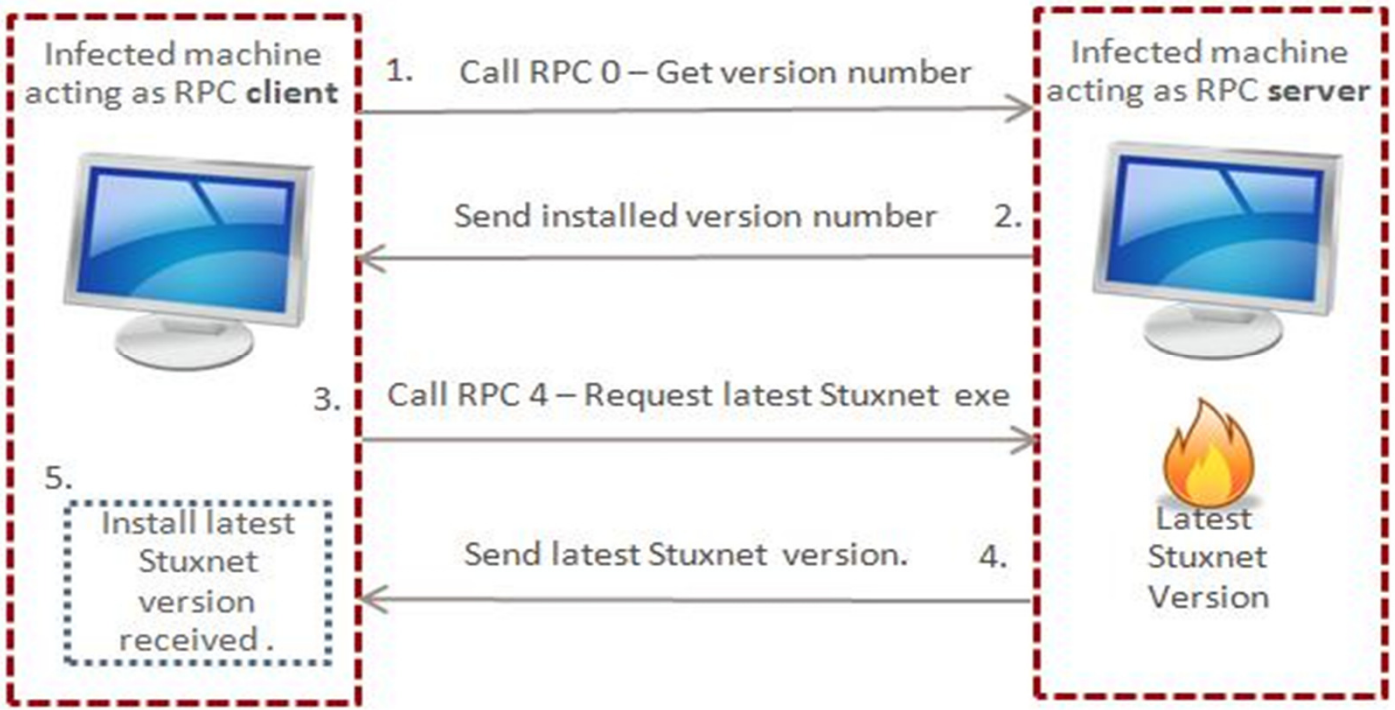
Propagation

- A trust trick
- How could it propagate so well?



Propagation Methods

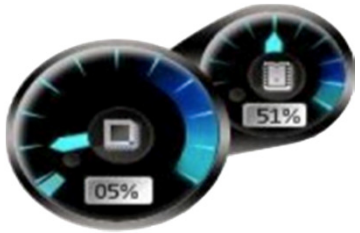
- .LNK propagation
- LAN propagation
- Windows task scheduler
- Siemens' mistake

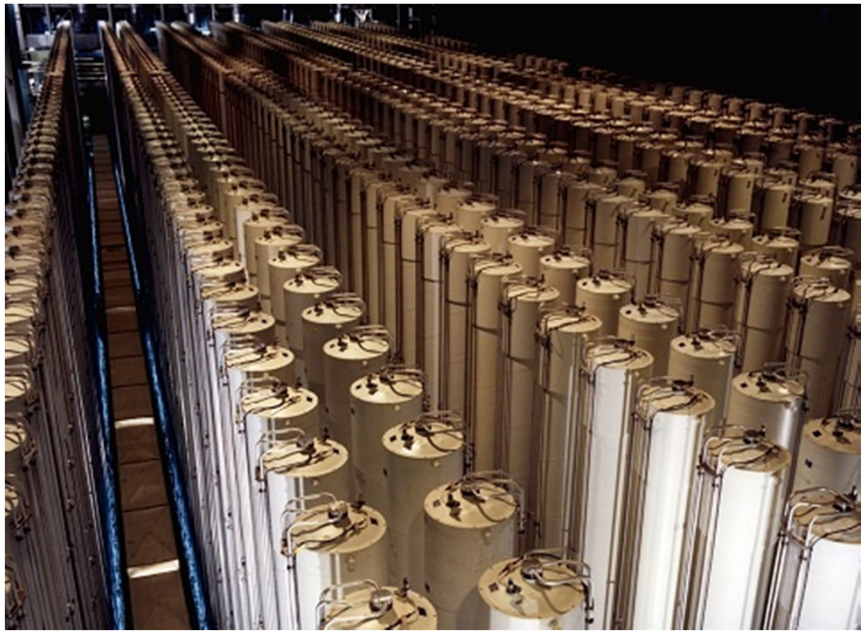


Detection Evasion

- Code injection in:
  - Active processes
  - New processes
- .dll Trick

CPU Frequency change





Windows PC → controls → Nuclear Centrifuges

Stuxnet Updates

- Check if infected!
- If yes, which version?
  - Older version
  - Newer version

Conclusion

- Trust and protection.
- What it changed?
- What could happen?
- Fear?

References

Matrosov A., Rodionov E., Harley D., Malcho J., **Stuxnet under the microscope,** Version 1.31 by ESET:
http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf

Falliere N., O'Murchu L., **W32.Stuxnet Dossier,** Feb 2011, Version 1.4 by Symantec:
http://www.symantec.com/content/en/us/enterprise/media/security_responce/whitepapers/w32_stuxnet_dossier.pdf

Constantine, L., **Crossing the Line: Terrorism in Cyberspace and Targets in Real-Space,** 2011 International Conference on Cyberworlds, Pages: 1 - 4

Karnouskos, S., **Stuxnet Worm Impact on Industrial Cyber-Physical System Security,** IECON 2011 - 37th Annual Conference on IEEE Industrial Electronics Society, 2011 , Pages: 4490 - 4494

Miyachi, T.; Narita, H.; Yamada, H.; Furuta, H., **Myth and reality on control system security revealed by Stuxnet**, Proceedings of 2011 SICE Annual Conference,
Pages: 1537 - 1540

Questions?

Thank you!

Obrigado!

Eyxaristo poly!

Bedankt!

Teşekkürler!

Ačiū!

Danke!