MALWARE: Threats and Attacks

Part 1-D: How to protect from Malware attacks, Antivirus Techniques

Presented by:
Evanthia Stefani & Eudoxia Sianou
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

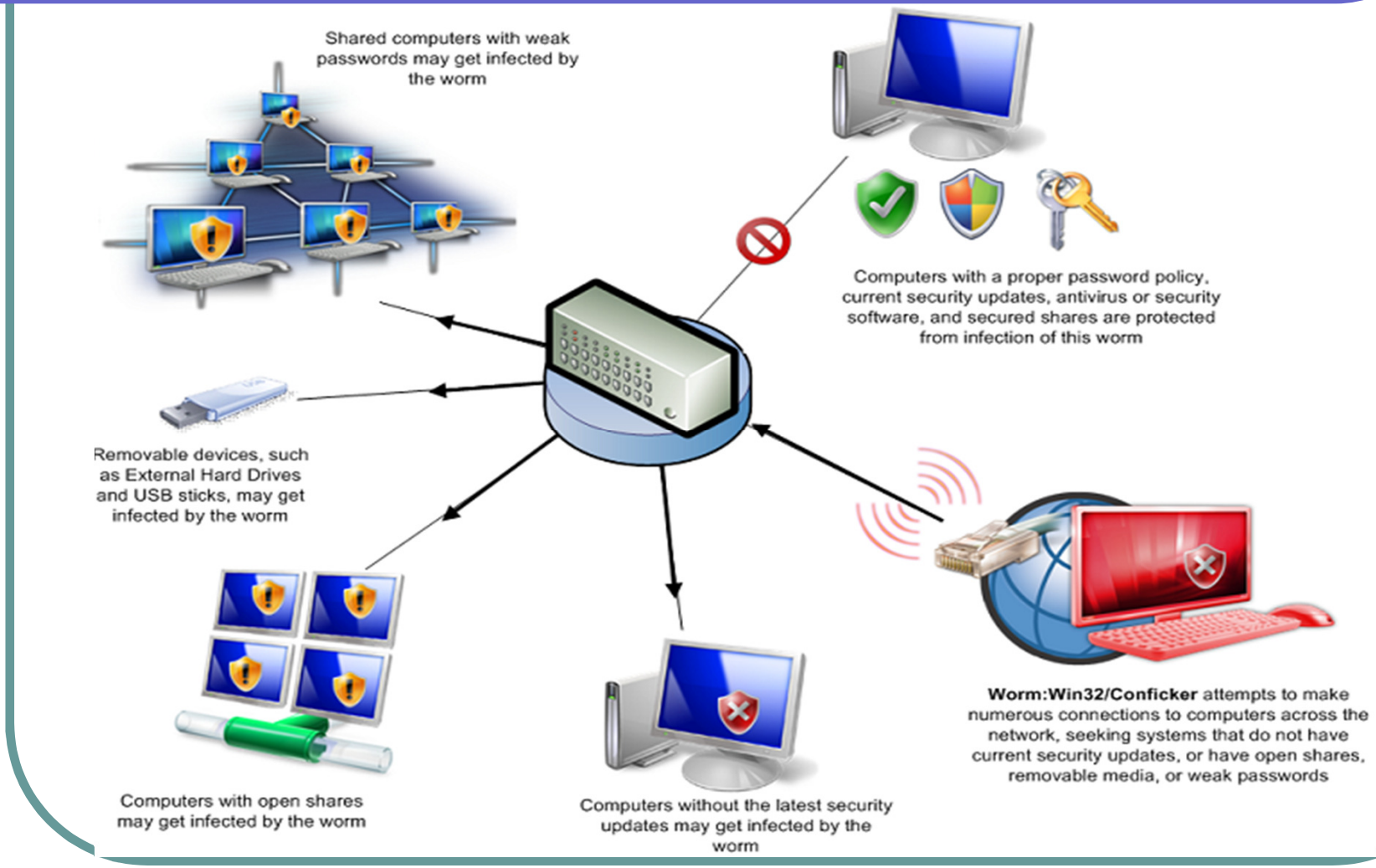
TECHNOLOGICAL EDUCATIONAL INSTITUTION
OF WESTERN MACEDONIA

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

Outline

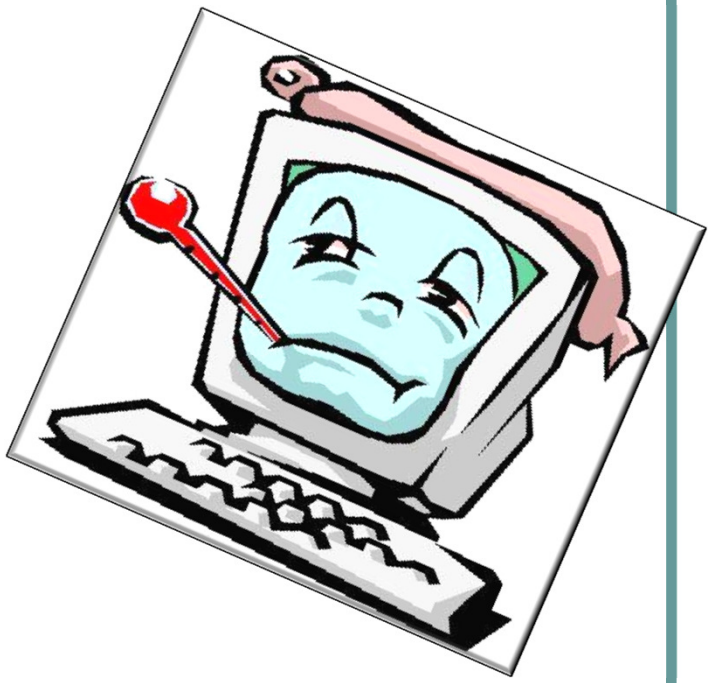
- Malware threats and attacks
- Antivirus
- How an Antivirus program works
- Antivirus detection techniques
- Stealth Viruses
- Macro Viruses
- Honey pot
- Cloud antivirus

Malware threats and attacks



Antivirus Aproaches

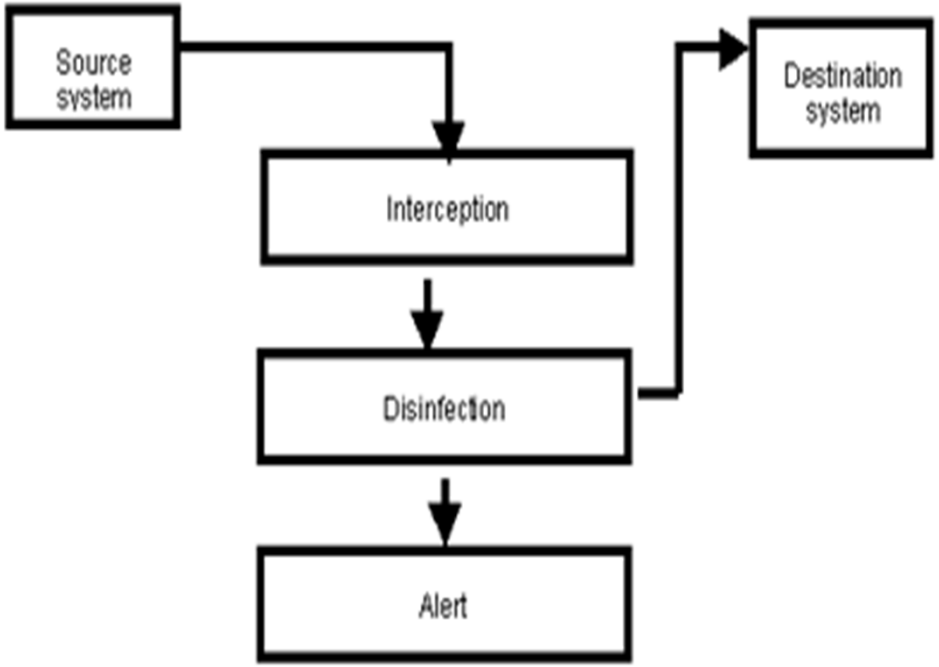
- **Detection** – determine that it has occurred and locate the virus
- **Idetification** – identify the specific virus
- **Removal** – remove all traces and restore the infected program to its original state.



Generations of Antivirus software

- **1st Simple scanners** (record of program lengths)
- **2nd Heuristic scanners** (integrity checking with checksums)
- **3rd Activity traps** (memory resident, detect infected actions)
- **4th Full-featured protection** (suite of antivirus techniques, access control capability)

How an Antivirus Program Works



Detection : Detecting whether or not, some code is a virus or not.

Identification: The process may be distinct from detection, or identification may occur as a side effect of the detection method being used.

Disinfection: Disinfection is the process of removing detected viruses; this is sometimes called *cleaning.*

Antivirus methods

- **Signature based detection** is the most common method. To identify viruses and other malware, antivirus software compares the contents of a file to a dictionary of virus signatures. Because viruses can embed themselves in existing files, the entire file is searched, not just as a whole, but also in pieces.
- **Heuristic-based detection**, like malicious activity detection, can be used to identify unknown viruses.
- **Generic detection,** refers to the detection and removal of multiple threats using a single virus detection.

Antivirus tasks

- The tasks for an antivirus software that lie beyond detection are verification, quarantine, and disinfection.
  - **Verification**
  - **Quarantine**
  - **Disinfection**

Antivirus - Verification

- Verification is performed for two reasons:
  - Reduce false positives
  - Positively identify the virus
- Transformation of the virus for more information.
- Comparing the found virus to a known copy of the virus.
- Using a virus-specific signature, for detection methods that aren't signature-based to begin with.
- Checksumming and comparing.
- Calling special-purpose code to do the verification.

Antivirus - Quarantine

- Quarantine is the isolation of the infected file.
- It’s a temporary measure .
  - Until the user decides how to handle the file.
  - Until an anti-virus update that can deal with the virus is available .
- Copies the infected file into a "quarantine“ directory.
  - The file permissions may be easily changed by a user.
- One solution is to encrypt quarantined file.
- Another solution is to render the files in the quarantine directory invisible.

Antivirus - Disinfection

- Virus-specific or Virus-behavior-specific.
- Using the virus' code:
  - Stealth viruses supply the uninfected contents of a file.
  - *Generic disinfection* methods
    - Anti-virus system stepped through the viral code.
    - Emulation of the infected code.
    - Disinfection code runs *inside* the emulator along with the infected code.
    - Deleting the infected file.
- Restore infected files from backups.

Antivirus Detection Techniques #1

- **Scanning:** Scanners can be classified based on when they are invoked.
  - On demand
  - On access
    - Pros: Gives precise identification of any viruses that are found.
    - Cons: Requires an up-to-date database of virus signatures for scanning to be effective.

Antivirus Detection Techniques #2

- **Static heuristics:** Static heuristics can find known or unknown viruses by looking for pieces of code that are general virus-like," instead of scanning for specific virus signatures.
  - Pros: Static heuristic analysis detects both known and unknown viruses.
  - Cons: False positives are a major problem.

Antivirus Detection Techniques #3

- **Integrity checkers:** With the exception of companion viruses, viruses operate by changing files. An integrity checker exploits this behavior to find viruses, by watching for unauthorized changes to files.
  - Pros: Integrity checkers boast high operating speeds and low resource requirements.
  - Cons: Detection only occurs after a virus has infected the computer.

Antivirus Detection Techniques #4

- **Behavior blockers:** A *behavior blocker* is anti-virus software which monitors a running program's behavior in real time.
  - Pros: Known and unknown viruses are detected.
  - Cons: While a behavior blocker knows which executable is the problem.

Antivirus Detection Techniques #5

- **Emulation:** anti-virus techniques using *emulation* let the code being analyzed run in an emulated environment.
  - Pros: Any viruses found are running in a safe environment.
  - Cons: Emulation is slow.

Stealth Viruses

- Anti-Stealth Techniques
  - Detect and disable the stealth mechanism.
  - Bypass the usual mechanisms to call the operating system in favor of unconvertible ones.

Macro Viruses

- Macro Virus Detection
  - Delete all macros in the infected document, including any unfortunate, legitimate user macros.
  - Delete macros know to be associated with the virus found.
  - For macro viruses detected using heuristics, remove the macros found to contain the offending behavior.
  - Emulator-based detection can track the macros seen to be used by the macro virus and delete them.

Honey pot #1

- A **Honey pot** acts as a deception tool for luring the attacker and logging its activities.
- Looks vulnerable.
- Appears to be a legitimate and a real machine.
- The concept is to learn from the intruder's action.
- Honey pots against worms:
  - As standalone defense
  - In conjuncture

Honey pot #2

- Honey pot with signature based detection.
  - The signature-based approaches have the advantage over the anomaly-based systems in that they are simple and able to operate online in real time. Combining honey pots with signature based detection gives the advantages of both.
- Honey pot with anomaly based detection.
  - It incorporates the advantages of both honey pots as well as anomaly based.

Honey pot #3

- Give the Honey Pot an attractive name.
  - The Honey Pot should not normally be accessed by anyone.
- How do we track the intruders without them knowing it?
  - Multiple logging or layers.
  - Logs can only be trusted of their integrity can be guaranteed.
  - Create logs on a safe system.
  - Network sniffer.

Honey pot #4

- Advantages:
  - Small data sets of high value
  - New tools and tactics
  - Minimal resources
  - Information
  - Simplicity
- Disadvantages:
  - Limited
  - Risk

Cloud antivirus

- Runs on the cloud.
- Scans all your files.
- The data are analyzed by the servers.
- Users must be connected to the internet.
  - But what happens if the user is not connected to the internet?

Cloud antivirus

- Improving System Load with a Lightweight Agent.
  - Cloud anti-virus employs agent software on the protected endpoint that is much lighter than the installed components of traditional anti-virus tools.
- Endpoint to Cloud Connectivity.
  - If the endpoint is not connected to the Internet, its ability to protect the user is limited because it cannot query the anti-virus cloud.
- Data Analysis in the Cloud.
  - The processing of the data collected by agents on protected end-points is analyzed by the servers of the anti-virus service provider.
- Behavior Monitoring and Blocking.
  - Cloud anti-virus is usually combined with other malware detection techniques, which are found in traditional anti-virus products.

Summary

- Malware threats and attacks
- Antivirus
- How an Antivirus program works
- Antivirus detection techniques
- Stealth Viruses
- Macro Viruses
- Honey pot
- Cloud antivirus

References #1

- John Aycock, *"Computer Viruses and Malware", Advances in Information Security,* Volume 22, pp 97-108
- William Stallings, *Network Security Essentials: Applications and Standards (4th Edition),* Prentice Hall, 2011, pp 305-373
- Lenny Zeltser, “What is Cloud Anti-Virus and How Does It Work?” http://blog.zeltser.com/post/1256199682/what-is-cloud-anti-virus
- “What Is Cloud Antivirus – Review Of Panda Cloud Antivirus Software”, Addictivetips http://www.addictivetips.com/windows-tips/what-is-cloud-antivirus-review-of-panda-cloud-antivirus-software-screenshots/

References #2

- Pragya Jain & Anjali Sardana: *A Hybrid Honeyfarm Based Technique For Defense Against Worm Attacks,* Department of Electronics & Computer Engineering, Indian Institute of Technology Roorkee, Roorkee, Uttarakhand, INDIA, Part 4, pp.1084 - 1089
- Lance Spitzner, Honeypots, Definitions and Value of Honeypots, http://www.trackinghackers.com/papers/honeypots.html
- William W. Martin, *CISSP, Honey Pots and Honey Nets - Security through deception,* SANS, May 25, 2001

Questions?

Thank you!

Obrigado!

Eyxaristo poly!

Bedankt!

Teşekkürler!

Ačiū!

Danke!