Malicious software

enisa
European Network and Information Security Agency

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the Agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details

For contacting ENISA or for general enquiries on information security awareness matters, please use the following details:

Isabella Santa, Senior Expert Awareness Raising - E-mail: awareness@enisa.europa.eu

Internet: http://www.enisa.europa.eu

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA regulation ((EC) No 460/2004). This publication does not necessarily represent the state of the art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Overview

This presentation discusses the ongoing risks associated with malicious software and highlights simple techniques that users can employ to protect themselves from malicious software.

The presentation is divided in to two sections:

- What is Malicious Software?
- How Malicious Software Can Affect You
- Types of Malicious Software
- How to Protect Yourself
- Resources

How to Use This Presentation

This presentation has been created by ENISA to raise awareness about the critical risks due to malicious software. It does so by providing easy to understand information that focuses employees’ attention on information security and allows them to recognise and respond accordingly to malicious software.

This presentation may be used by individuals, or presented in a classroom setting by instructors who are involved in their organisation’s security awareness efforts.

In conjunction with this presentation, ENISA’s has developed a reference guide for this training which provides additional notes and external references for trainers and presenters to utilize while performing security awareness training using this material.

What is Malicious Software?

What is Malicious Software?

- A hostile or intrusive program designed to insert itself on to your computer without your consent.
  - It is also called Malware from *MAL*icious soft*WARE.*
  - The amount of Malicious Software increases every year
    - Reportedly increased by 276% in 2008*
  - Malicious Software is continuously created by computer programmers from around the world

*Symantec Global Internet Security Threat Report April 2008

Types: Viruses & Worms

- Virus
  - A **virus** is a software program that can copy itself from one file to another to infect a computer.
- Worm
  - A **computer worm** is a software program that spreads from computer to computer through the network.

Types: Trojans & Backdoors

- ## Trojan horse

  A program that appears to perform a desirable function for the user but instead performs undesirable functions.

- ## Backdoors

  A hidden software program that allows someone to gain unauthorized access to a computer.

Types: Spyware & Loggers

- Spyware & Adware

  Software which collect information about what a user does on a computer. Adware will also display advertisements to the user without their consent.

- Keystroke loggers

  A piece of hardware or a software program that captures everything a users types on the keyboard.

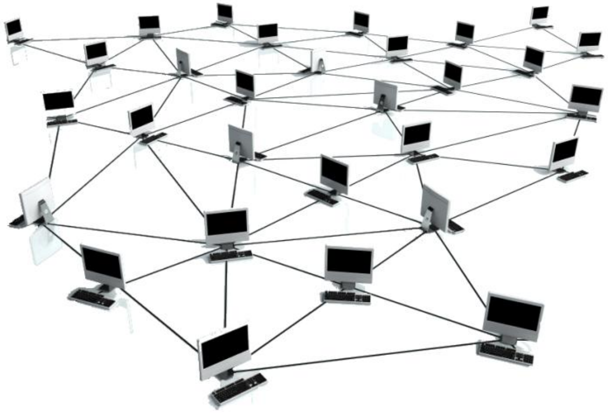
Types: Botnets & Rootkits

- **Botnets**

  Software programs that are installed without authorization on many different computers and are controlled remotely.

- **Rootkits**

  A collection of software programs that allow an attacker to do many different undesirable things and also to hide from detection.



How Does Malware Spread?

- Malware usually attacks weaknesses and vulnerabilities in other computer programs
- You can also spread Malware by:
  - Opening email attachments infected with Malware
  - Downloading infected files from the Internet
  - Sharing files that are infected with Malware
  - Visiting websites that contain Malware

How Can Malware Affect You?

Malware Affects You

- Malware Can Cause Many Problems
  - Delete your files and programs
  - Cause your computer to run slowly or become unusable
  - Record information you type including passwords
  - Access any information stored on your computer

Criminals Use Malware

- Criminals use Malware for financial gain
  - Redirect your Internet traffic for “Pay-per-Click” schemes
  - Send e-Mail SPAM
  - Attack company or government computer systems
  - Disable networks and websites

What Can Malware Steal?

- Malware is used by criminals to infect your computer and look for valuable information
  - Personal information such as bank account or payment card numbers, passwords, PINs
  - Trade secrets and intellectual property
  - Anything that is stored on your computer

How To Protect Yourself From Malware

Protect Your Computer

- Keep Your Computer and Backups Up to Date
  - Regularly apply patches from your operating system and application vendors
  - Configure your browser to block pop-up windows
  - Backup your files and programs regularly so you can recover if anything happens

Protect Your Computer

- Install a reputable anti-virus, anti-spyware, browser filter, and personal firewall product
  - Update virus definition at least once a day
  - Perform a full scan of your computer every week
  - Alert you of dangerous websites
- Beware of fake antivirus product offers

Avoid Risky Behaviour

- Avoid Unknown Files & Programs
  - Do not download programs or files that are sent to you, even if you know who sent it
  - Do not download files or programs offered over Chat or IRC
  - Do not download or install programs from pop-up windows
  - Do not open email attachments from people you do not know
  - Be careful what Internet sites you visit
  - Avoid programs and files from file sharing sites

Watch for Signs of Malware

- Regularly check the results from your anti-virus software to see if any Malware was found
- Your computer might be infected if:
  - Your computer performs slower than usual
  - Programs and files disappear, and new files and programs appear without warning
  - Your browser frequently displays pop-up windows, or you are redirected to inappropriate sites
  - Your disk drive or network connection is active when you are not using your computer

If Your Computer is Infected

- If Your Computer is Infected
  - Disconnect your computer from the network
  - Use a CD copy of Anti-Virus to scan and clean your computer
  - If you cannot remove the malicious software, take the computer to a professional who can help you

Resources

Resources

Free Online Tools & Scanners

BitDefender:	http://www.bitdefender.com/scanner/online/free.html
ESET:	http://www.eset.com/onlinescan/
F-Secure:	http://www.f-secure.com/en_IN/security/security-lab/tools-and-services/
Kaspersky:	http://www.kaspersky.com/virusscanner
McAfee:	http://home.mcafee.com/Downloads/FreeScan.aspx
Microsoft:	http://onecare.live.com/site/en-us/default.htm
Trend Micro:	http://housecall.trendmicro.com/
Symantec:	http://security.symantec.com/sscv6/WelcomePage.asp

Conclusion

Conclusion

- Malicious Software is a Constant Risk
  - There are many types of malware that can affect you.
  - Malware can steal confidential and personal information, damage files and programs, and slow your computer.
  - Install reputable anti-virus and security tools.
  - Regularly apply patches from the manufacturer of your operating system and applications.
  - Avoid common sources of malware.

European Network and Information Security Agency
P.O. Box 1309
71001 Heraklion
Greece
www.enisa.europa.eu

enisa
European Network
and Information
Security Agency