Sources of Threats

- **Malware**
- **People** – hackers/crackers, thieves, former employees, business competition, laziness, …
- **Nature/Environmental Threats** – flood, fire, extreme temperatures, humidity, lightning, dust, earthquake, …

Malware

- Portmanteau of the words **malicious software**
- Any executable code, which can infiltrate a computer system with a malicious intent.
- Types of malware
    - Ransomware
    - Trojan horses
    - Worms
    - Viruses
    - Rootkits
    - Spyware/Crimeware
    - Adware

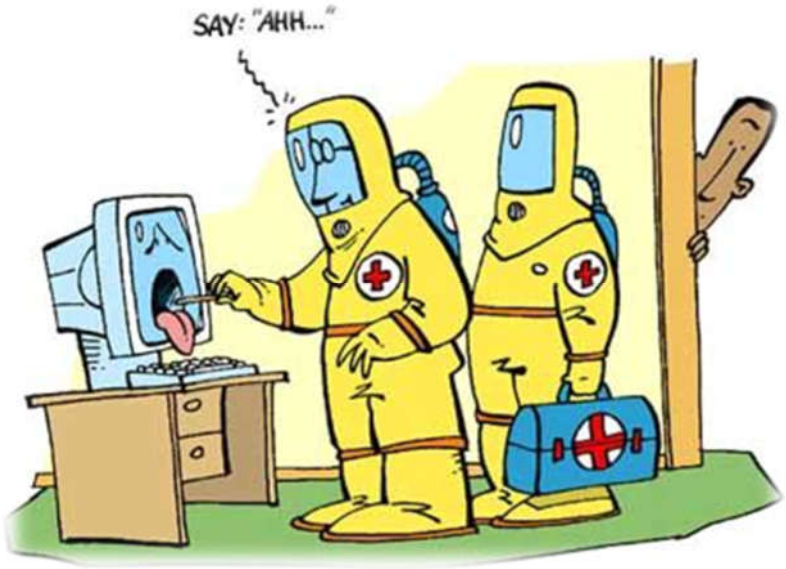

Figure 1: Infected Computer (source: http://junibob.com/Quickstart/ImageLib/Computer_Virus.png)

Ransomware

Ransomware is a type of malware that prevents or limits users from accessing their system:

- by locking the system's screen, or
- by locking the users' files

unless a ransom is paid.

More modern ransomware types – **crypto-ransomware** – encrypt certain file types (typically documents, pictures, music, videos) on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key. Since in most cases is used the asymmetric encryption, for most victims the only viable way is to pay the ransom.

For older kinds of ransomware are available tools, which may decrypt the encrypted data or regain access to the locked system; however, in newer versions the ransom is often the only way. It is not guaranteed, though – sometimes the hackers-programmers make a mistake in the ransomware code, which encrypts them incorrectly. The result is an irreversible data loss.

*The only reliable way of prevention is a **backup**, which is kept separately from the infected computer/smartphone.*

Trojan Horse

- It is a malicious program, which disguises as a harmless/useful application

- Non-self-replicable malware – it ***does not infect*** the system ***automatically***; the system can be infected
    - by installation of software, which pretends to be useful (cracks, rogue antispyware);
    - from an infected website (using ActiveX or Flash);
    - using exploits, i.e. flaws in the software;
    - from email attachments.

Figure 2: Malware (source: TechTips.com)

- Possible actions:
    - It may open **backdoor** – hidden access for the Trojan creator, usually with the administrator privileges – it provides the attacker the complete control of the system.
    - Install ransomware or other malware
    - Steal personal data/passwords
    - Turns a computer to a **zombie** – a part of the **botnet** = a network of devices ready to attack other systems
- The name is derived from the Trojan horse mentioned in the Homer's Iliad.

Worm

- A self-replicating malware (like the viruses), which is spread over the network or infecting mass-storage devices (flash disks, external HDD).
- The worm does not infect an existing file in the computer – it creates new executable containing the worm only (therefore the best way how to treat that infection is to delete such as files).
- Worms can misuse the system exploiting the system vulnerabilities – the best prevention are updates for the operating system and all installed programs.
- Actions – like viruses.

Virus

- Like worms – it is self-replicating software
- Unlike the worms: they put their code into existing files/other zones, which may contain executable code (boot sector, firmware …)
- True viruses are quite rare these days
- **Categories**
    - ***boot virus*** – it infects the code stored in the master boot sector of a disk – this code is executed when operating system starts from such as disk;
    - ***file virus*** – a virus infects existing executable files in the computer system embedding its code to the original file; it has several subtypes

- ***macrovirus*** – infects documents (usually made in Microsoft Office programs), which can contain macros (simple routines, which automate some tasks in documents);
- ***autorun viruses*** – they misuse automated start of programs from storage devices (mainly flash disks); if the root folder of such as disk contains an *autorun.inf* file, it automatically tries to start the program defined in the *autorun.inf*;

- Actions
  - File system damage/encryption
  - Botnet client installation
  - Backdoor/installation of other malware

Rootkit

- Sophisticated type of malware, which deceives the computer system by modification of its core elements, so they can completely control the system and hide its presence – no program running in the compromised system can detect it; the best way of detection is to scan the system from a clean, trustworthy environment (live CD/DVD/flash disk, another computer system).
- Actions
  - Backdoor
  - Monitoring of the user action
  - Botnet
  - Spam distribution

Spyware/Crimeware

1. Any kind of software, which is designed to monitor user's activities and collect sensitive/valuable information without his/her knowledge.
2. System is infected
   - using system vulnerabilities
   - by deception of the user (e.g. it can be a part of a program and user agrees with its installation; sometimes it is claimed in the EULA – End-user License Agreement – however who reads EULA?)
3. Actions

- Activation of the keylogger (it collects information about the keys pressed in programs) – sometimes combined with the screenshots and web cam monitoring (*be careful – the keylogger can be also a device; e.g. inserted between the keyboard connector and the USB/PS2 port of a computer – such as devices is virtually invisible for software scanners*);
- Monitoring of the user's web pages and emails;
- Deactivation of antimalware/security software (antivirus, antispyware, firewall)

Adware

Software, which automatically displays advertisements on the system/in a program. Some of them are legal (e.g. unregistered software, trials), some are combined with spyware and force the user to interact with the ads.

Prevention

- regular **backup** of data and partitions
- regular installation of **updates** (for both OS and applications);
- regular **scan** of the system by a reliable antivirus/antimalware software;
- anti-spam module for email clients;
- **firewall** – it controls network connections and filters all unexpected/undesirable attempts to break into the system from the network or attempts to communicate with the network without the user's acknowledgement;
- **self-education** in the computer security

Detection and Removal

- antivirus
  - detection only (mostly trial versions or online scanners),
  - detection and removal,
  - detection, removal and resident protection
  - examples: Eset Smart Security/NOD32, Avira Antivir, Norton Internet Security, Avast!, AVG, Microsoft Security Essentials…
- antispyware
  - Windows Defender, Spyware Doctor, Lavasoft Adaware, SpywareBlaster, Spybot Search&Destroy
- other security related software (e.g. keylogger detectors, rootkit detection kits, …)
- Threat – **rogue antivirus/antimalware** – they pretend being useful security software; in fact they just cause fake alerts, system crashes or even install real malware on the system (examples: MS Antivirus, Green Antivirus, SystemDoctor …)

Computer Scan

1. There is already an antivirus tool installed
   a. Update it to the last version
   b. Choose the targets – at least once per month perform scan of the whole system (memory + disks)
   c. In Windows Vista/7 is recommended to perform the scan with Administrator privileges.
   d. If an active virus/worm/Trojan is found in the memory, you should clean the system in the offline mode – active malware can re-infect the computer almost instantly
      i. Safe mode
      ii. LiveCD/LiveDVD/LiveFlash operating system with an antivirus – almost all paid versions of antivirus tools are able to create such as medium
      iii. Dismantle the hard disk(s) from the infected computer and clean in another one (mind the priveleges – rights for some folders must be taken over to get in).
   e. Actions: virus – heal/clean, delete if necessary; other types of malware - delete
2. There is no antivirus tool
   a. Install a new one (if the computer is infected by an aggressive type of malware, the installation might fail), like
      i. Avira Antivir (scanner + cleaning + resident shield)
      ii. MS Security Essentials (scanner + cleaning + resident shield)

iii. MWAV (scanner only)
iv. Eset Online Scanner
v. Trial version of tools mentioned above
vi. Scan form a LiveCD or at another computer system

b. Perform the steps like in the step 1.

Antivirus (AV) Tools

- **Scanner** = checks selected targets and looks for signatures of malicious code in the files/memory; it can use also heuristic analysis – it is used for unknown types malware; instead of specific signatures it tries to identify some common features of malware
- **Real-time protection** = a part of the AV, which is permanently running while the OS is working; it monitors opened files, flash disks, downloaded files…
- **Firewall** = an optional part, sometimes an independent program – it monitors network communication and blocks unauthorized attempts to connect to/from the system.
- **Antispam** = another optional part – it is designed to scan incoming emails and to remove spam.
- **Rescue media builder** = an optional part, which can build and burn bootable CD/DVD or create bootable flash disk with the core part of the antivirus.

Backup

Data backup

- **Only data files:**
  - To a cloud storage (+ reliability, availability; - limited capacity and speed, if a related account is hacked, the hacker has access to all important data)
  - To a local storage
    - NAS, external HDD – relatively reliable, large and fast; there is a chance of failure; data can be encrypted by the ransomware
    - Optical media (CD,DVD, BD) – relatively durable and not vulnerable to ransomware; slow and low capacity, cheap media are not reliable
- **Partitions**:
  - Data + software – the whole system can be recovered to a previous state (e.g. before an infection)
  - Requires large storage devices (NAS, external hard-disk drives)
  - Tools: built-in OS tools – Windows Backup; dedicated tools: Macrium Reflect, Acronis True Image