Safety of information systems

Lecturer: Roman Danel

Software Threat

- **Viruses -** a type of malicious software program ("malware") that, when executed, replicates by reproducing itself (copying its own source code) or infecting other computer programs by modifying them:
    - stealth,
    - boot,
    - polymorphic – virus changes its structure not to be find by searching virus patterns
    - macro virus – usually connected with Office SW, based on VBA
- **Trojan Horses** - any malicious computer program which is used to hack into a computer by misleading users of its true intent. The term is derived from the Ancient Greek story of the wooden horse that was used to help Greek troops invade the city of Troy by stealth. A , computer virus that is disguised as a normal software, and in fact carries out malicious operations without the user's awareness
- **Worms** - a standalone malware computer program that replicates itself in order to spread to other computers. The worms used for propagation mechanism based on an error in the operating system, database or a web or mail client.
- **Backdoors** - s a method, often secret, of bypassing normal authentication in a product, computer system, cryptosystem or algorithm etc.
- Lost function from development time
- **Phishing** - a way of attempting to acquire sensitive information such as usernames, passwords and credit card details using social engineering
- **Hoax** - deliberately fabricated falsehood made to masquerade as truth
- **Spyware** - is software that aims to gather information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge
- **Botnet** - is a number of Internet-connected computers communicating with other similar machines in which components located on networked computers communicate and coordinate their actions by command and control (C&C) or by passing messages to one another (C&C might be built into the botnet as P2P). Botnets have been used many times to send spam email or participate in distributed denial-of-service attacks.

- **Keylogger** – records the press of keyboards keys
- **Dialers** – attempts to dial telephone lines at other locations
- **Dropper** - s a program (malware component) that has been designed to "install" some sort of malware (virus, backdoor, etc.) to a target system
- **Downloader**
- **Rootkit** - software that enables continued privileged access to a computer while actively hiding its presence from administrators

Spoofing is a term used in Internet security for identity falsification. Spoofing refers to the falsification of reports (e.g. phishing), falsifying websites (pharming) or falsifying intermediary in the communication between two parties (so-called Man In The Middle). The aim of spoofing is to elicit confidential information from the user.

Pharming (based on the word farming) is a term for a fraudulent attack designed to elicit confidential information from users via controlled websites. Pharming is a more insidious form of phishing, because the attacker does not attack directly to the user and does not create fake websites, but masters (redirects) the actual web page of the institution (such as banks pages). In technical terms, this is an attack on the DNS server.

Defence against pharming is mainly on the website operators, security of the DNS server, use a certificate or verification SMS. There are also pharming attacks launched on the local computers and devices (so-called local pharming). Most important, as in the case of Phishing, is a caution of the user.

Hoax is a label for an alarm or false message or information usually designed to trigger chain propagation, thus extending the alarm information to the greatest number of people. Hoaxes can be deceptive, alarming or it can just be a joke.

Zombie computer is a computer connected to the Internet that has been compromised by a hacker, computer virus or Trojan horse program and can be used to perform malicious tasks of one sort or another under remote direction. Botnets of zombie computers are often used to spread e-mail spam and launch denial-of-service attacks (DOS attacks). Most owners of "zombie" computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to fictional zombies. A coordinated DDoS attack by multiple botnet machines also resembles a "zombie horde attack", as depicted in fictional zombie films.

Email harvesting is the process of obtaining lists of email addresses using various methods. Typically these are then used for bulk email or spam.

Spambot is a computer program designed to assist in the sending of spam.

Attacker Types

- Hacker
    - Beginner -> recognition, self-realization
    - Advanced -> overcome intellectual challenges, the ideal of free access to information ...

- Virus creator - "betrayed idealists", "unappreciated experts" ...
- Insider threat - retaliation against an employer, a sense of injustice, ...
- Information warrior - patriotic themes - destabilization of enemy sources
- Thief - pursuit of profit finance, BC Fishing
- Political activist - fanatic idealist ...

Errors that attackers employ:

- **Programming errors** - occur when some state of programs are unhandled, poor memory allocation calculations, inadequate checking of user input and so on.

- **Design errors** - arising from the erroneous judgment of the program designer. They are often difficult to remove. WiFi networks encryption by WEP is a good example. It is still widely used on all network cards and WiFi access points, in spite of the fact that soon after its introduction a very simple way of breaking it was published.

- **Configuration errors** - caused by error or ignorance on the side of the user or administrator who configured the program or the device. Many of the devices and programs are set for total ease of use from the manufacturers and these settings can sometimes be hazardous. An example may be a typical access point on WiFi network - where the vast majority come with encryption turned off, so after switching to WiFi networks (and thus to the local network, where the access point is connected) anyone can join.

- **Physical violation** - a large part of the security arrangements can be bypassed if the attacker has physical access to the device or computer. For example, the hard drive may be removed from your computer and its contents read of edited even though the hacker cannot log on to the computer itself.

- **Operator errors** - just accidentally running a malicious program when the user is logged in with administrator privileges may infect your computer, regardless of how good a firewall protects you against Internet attacks

Aims of attackers:

- Theft of data and information
- Identity theft
- Destruction of Data
- Destabilization of system
- Blocking certain sites or resources

Antispyware

Antispyware is security software designed to protect data from attacks or risks caused by Spyware. Antispyware is used to find and remove spyware, which is usually searched based on a database or analysis of suspicious behavior.

Malware is a summary term for all malicious software. It is such software, which was created with the intent to break into the computer system or damage it. The term malware was created from words malicious and software.