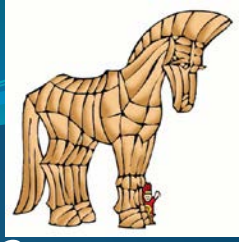
Computer infiltrations

Computer infiltration

- Computer infiltration means unauthorized entering program code into computer system in order to perform undesired (often concealed) activities.
- Currently, there are about 80,000 types of infiltration (according to AEC) with 500 to 800 new types appearing every month.
- The problem is that classification is not unified and types are difficult to differentiate from mutations of the type.
- Based on behavior and program code construction we can differentiate the bellow types of infiltration.

Trojan horse



Usually an interesting or somehow useful program which, in addition to the useful code, contains a code performing undesired activities characterized as follow:

- does not replicate its code and is not able to spread,
- harmful activities involve eavesdropping (Internet activity monitoring, password monitoring) as well as destruction (erasing data, disc formatting, erasing a random hard drive sector etc.)
- harmful activities are launched by a pre-defined impulse unknown to the user (number of launches of a program, system date etc.)

In the past two years Trojans have been spread as part of other infiltrations (worms). Based on handling activities Trojans can be classified as:

- **Spyware/Adware** – program performing concealed monitoring of Internet sites visited and consequently launching aimed advertising based on client profile.
- **Key logger** (password thief) – monitoring output codes of keyboard router and providing remote access to sensitive data (access password, code key, PIN etc.).

- **Backdoor** - Of all trojans, backdoor trojans pose the greatest danger to users' PCs because they give their authors remote control over infected computers. They are downloaded, installed, and run silently, without the user's consent or knowledge. Upon installation, backdoor trojans can be instructed to send, receive, execute and delete files, gather and transfer confidential data from the computer, log all activity on the computer, and perform other harmful activities.
- **RAT** - Remote Access Tool. A program that enables a hacker to remotely access and control other people's computers. A RAT can serve a variety of malicious purposes, including hijacking and transferring private information, downloading files, running programs, and tampering with system settings.

Worms

Independent program (set of programs) requiring no host code with the following features:

- active worm is able to replicated and spread its functional copies without human assistance to other computer systems via Internet – using known weak point in applications and OS (e-mail, IRC, WWW etc.),
- launched automatically upon OS system start (infects Registry and *.ini files),
- destructive activities range is very wide, often involving eavesdropping for sensitive data via Internet,
- very common.

Viruses

Dependent program code connected to a host executable unit, which is a desired part of a computer system (program, script, command file, macro, OS installer etc.). Launching this executable unit also executes virus code with the following features:

- infects other available executable unit by inserting its replication (mutation) to this unit,
- able to spread to other computer systems,
- performs destructive activities (optional feature).

Hoaxes

Fake alarm e-mails using “social engineering” (fraud, lie, moral blackmail) to send the message to all available addresses. They have the following features:

- reporting shocking news (e.g. on a “new” infiltration), or appeal to humanitarian considerations (helping the seriously ill, helping in connection with an actual humanitarian crisis etc.),
- referring to reputable IT companies (IBM, Microsoft, etc.), giving trustworthy reference ,
- require instant action, i.e. sending to all potentially affected people,
- sent consciously by people who the addresses knows.

SPAM

- Is an unsolicited mail message offering goods or services often with immoral content. It is sent via infiltrated systems connected to the Internet (BOT) with a fake heading making it difficult to track the actual sender and to block the respective SMTP communication. E-mail addresses are gathered, e.g. as part of a prior infiltration of an intermediary system by a worm or from public databases (ICQ).

- The motive is “cheap” marketing, as laws in many countries restrict unsolicited electronic advertising.

Phishing, Pharming

- Phishing is based on fake e-mail messages using “social engineering” and technological tricks (redirecting URL links, keylogger infiltration) to convince the user to disclose personal data and sensitive banking details (access password to Internet banking, bank account data, credit card data, etc.).
  Pharming is a similar type of attack redirecting the user to fake Internet banking sites, typically by compromising DNS.

Potentially unsafe applications

- There are many legitimate programs which serve to simplify the administration of networked computers. However, in the wrong hands, they may be misused for malicious purposes.
- “Potentially unsafe applications” is the classification used for commercial, legitimate software. This classification includes programs such as remote access tools, password-cracking applications, and key loggers (a program recording each keystroke a user types).

Potentially unwanted applications

Potentially unwanted applications are not necessarily intended to be malicious, but may affect the performance of your computer in a negative way. Such applications usually require consent for installation. If they are present on your computer, your system behaves differently (compared to the state before their installation). The most significant changes are:

- new windows you haven't seen previously are opened,
- activation and running of hidden processes,
- increased usage of system resources,
- changes in search results,
- application communicates with remote servers.

How Did My PC Get Infected with Infiltration?

The following are the most likely reasons why your computer got infected with Infiltration:

- Your operating system and Web browser's security settings are too lax.
- You are not following safe Internet surfing and PC practices.

- **Downloading and Installing Freeware or Shareware** – small charge or free software applications may come bundled with spyware, adware, or programs like Infiltration. Sometimes adware is attached to free software to enable the developers to cover the overhead involved in created the software. Spyware frequently piggybacks on free software into your computer to damage it and steal valuable private information.

- **Using Peer-to-Peer Software** - The use of peer-to-peer (P2P) programs or other applications using a shared network exposes your system to the risk of unwittingly downloading infected files, including malicious programs like Infiltration.
- **Visiting Questionable Web Sites** - When you visit sites with dubious or objectionable content, trojans-including Infiltration-, spyware, and adware, may well be automatically downloaded and installed onto your computer.

Detecting Infiltration

The following symptoms signal that your computer is very likely to be infected with infiltration:

- **PC is working very slowly**
  Infiltration can seriously slow down your computer. If your PC takes a lot longer than normal to restart or your Internet connection is extremely slow, your computer may well be infected with Infiltration.
- **New desktop shortcuts have appeared or the home page has changed**
  Infiltration can tamper with your Internet settings or redirect your default home page to unwanted web sites. Infiltration may even add new shortcuts to your PC desktop.

- **Annoying popups keep appearing on your PC**
  Infiltration may swamp your computer with pestering popup ads, even when you're not connected to the Internet, while secretly tracking your browsing habits and gathering your personal information.

- **E-mails that you didn't write are being sent from your mailbox**
  Infiltration may gain complete control of your mailbox to generate and send e-mail with virus attachments, e-mail hoaxes, spam, and other types of unsolicited e-mail to other people.

Antivirus Software

- Antivirus software is designed to detect, prevent, and remove malicious software, aka malware. The classification of malware includes viruses, worms, trojans, as well as (depending on the scanner) some forms of potentially unwanted programs (such as adware and spyware).

Free Versus Fee

- Antivirus software is sold or distributed in many forms, from standalone antivirus scanners to complete Internet security suites that bundle antivirus with a firewall, privacy controls, and other adjunct security protection. Some vendors, such as Microsoft, AVG, Avast, and AntiVir offer free antivirus software for home use (sometimes extending it for small home office – aka SOHO – use as well).

- Periodically, debates will ensue as to whether free antivirus is as capable as paid antivirus. A long term analysis of AV-Test.org antivirus software testing suggests that paid products tend to demonstrate higher levels of prevention and removal than do free antivirus software. On the flip side, free antivirus software tends to be less feature-rich, thereby consuming fewer system resources which suggests it may run better on older computers or computers with limited system capacity.

- Whether you opt for free or fee-based antivirus is a personal decision that should be based on your financial capabilities and the needs of your computer. What you should always avoid, however, are pop-ups and advertisements that promise a free antivirus scan. These ads are scareware - bogus products that make erroneous claims that your computer is infected in order to trick you into buying a fake antivirus scanner.

Most famous antivirus softwares

- avast!
  AVG
  AVIRA
  BitDefender
  eScan
  ESET
  F-Secure
- G DATA
  K7
  Kaspersky
  McAfee
  Microsoft
  Panda
  PC Tools
- Qihoo - 360
  Sophos
  Symantec
  Trend Micro
  TrustPort
  Webroot

Top 10 Alerts

- MyWebSearch
- KillAV
- ShopperReports
- Zugo
- OnLineGames
- Softomate
- SearchPage
- Static IP Route
- Search Settings
- Alot

Computer Safety Tips

1) Use antivirus software and keep it up-to-date.
2) Install security patches.
3) Use a firewall.
4) Secure your browser.
5) Take control of your email.
6) Treat IM suspiciously.
7) Avoid P2P and distributed filesharing.
8) Keep abreast of Internet scams.
9) Don't fall victim to virus hoaxes.

Something about hackers

- Thanks to the media, the word "hacker" has gotten a bad reputation. The word summons up thoughts of malicious computer users finding new ways to harass people, defraud corporations, steal information and maybe even destroy the economy or start a war by infiltrating military computer systems. While there's no denying that there are hackers out there with bad intentions, they make up only a small percentage of the hacker community.

Something about hackers

- The term computer hacker first showed up in the mid-1960s. A hacker was a programmer -- someone who hacked out computer code. Hackers were visionaries who could see new ways to use computers, creating programs that no one else could conceive. They were the pioneers of the computer industry, building everything from small applications to operating systems. In this sense, people like Bill Gates, Steve Jobs and Steve Wozniak were all hackers -- they saw the potential of what computers could do and created ways to achieve that potential.

Something about hackers

- A unifying trait among these hackers was a strong sense of curiosity, sometimes bordering on obsession. These hackers prided themselves on not only their ability to create new programs, but also to learn how other programs and systems worked. When a program had a **bug** -- a section of bad code that prevented the program from working properly -- hackers would often create and distribute small sections of code called **patches** to fix the problem. Some managed to land a job that leveraged their skills, getting paid for what they'd happily do for free.

Something about hackers

- As computers evolved, computer engineers began to network individual machines together into a system. Soon, the term hacker had a new meaning -- a person using computers to explore a network to which he or she didn't belong. Usually hackers didn't have any malicious intent. They just wanted to know how computer networks worked and saw any barrier between them and that knowledge as a challenge.

Something about hackers

- In fact, that's still the case today. While there are plenty of stories about malicious hackers sabotaging computer systems, infiltrating networks and spreading computer viruses, most hackers are just curious -- they want to know all the intricacies of the computer world. Some use their knowledge to help corporations and governments construct better security measures. Others might use their skills for more unethical endeavors.

Thank you for your attention!