Computer infiltrations

Computer infiltration

- Computer infiltration means unauthorized entering program code into computer system in order to perform undesired (often concealed) activities.
- An Infiltration is a piece of malicious software that attempts to enter and/or damage a user’s computer.
- 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.

Viruses

- Computer virus is an infiltration that corrupts existing files on our computer.
- Viruses are named after biological viruses, because they use similar techniques to spread from one computer to another.
- Computer viruses typically attack executable files, scripts and documents.
- To replicate, a virus attaches its “body“ to the end of a target file.

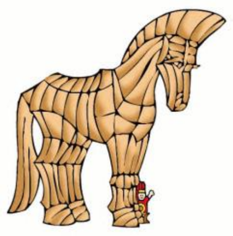
In short, this is how a computer virus works:

- After execution of the infected file, the virus activates itself (before the original application) and performs its predefined task.
- Only after that is the original application allowed to run.
- A virus cannot infect a computer unless a user, either accidentally or deliberately, runs or opens the malicious program.

Worms

- A computer worm is a program containing malicious code that attacks host computers and spreads via a network.
- The basic difference between a virus and a worm is that worms have the ability to replicate and travel by themselves; they are not dependent on host files (or boot sectors).
- Worms spread through email addresses in your contact list or exploit security vulnerabilities in network applications.
- A worm activated in a system can cause a number of inconveniences: It can delete files, degrade system performance, or even deactivate programs.
- The nature of a computer worm qualifies it as a “means of transport“ for other types of infiltrations.

Trojan horses



- Historically, computer trojan horses have been defined as a class of infiltrations that attempt to present themselves as useful programs, tricking users into letting them run.
- Their sole purpose is to infiltrate as easily as possible and accomplish their malicious goals.
- "Trojan horse" has become a very general term describing any infiltration not falling under any specific class of infiltration.

Trojan horses - subcategories

- **Downloader** – a malicious program with the ability to download other infiltrations from the Internet.
- **Dropper** – a type of trojan horse designed to drop other types of malware onto compromised computers.
- **Backdoor** – an application which communicates with remote attackers, allowing them to gain access to a system and to take control of it.
- **Keylogger** – (keystroke logger) – a program which records each keystroke that a user types and sends the information to remote attackers.

Rootkits

- Rootkits are malicious programs that grant Internet attackers unlimited access to a system while concealing their presence.
- After accessing a system (usually exploiting a system vulnerability), rootkits use functions built into the operating system to avoid detection by antivirus software: they conceal processes and files.
- For this reason it is almost impossible to detect them using ordinary testing techniques.

Adware

- Adware is a shortened term for advertising-supported software.
- Adware applications often automatically open a new pop-up window containing advertisements in an Internet browser, or change the browser's home page.
- Adware is frequently bundled with freeware programs, allowing creators of freeware programs to cover development costs of their (usually useful) applications.
- Adware itself is not dangerous, users may only be bothered by the advertisements.
- The danger lies in the fact that adware may also perform tracking functions (as spyware does).

Spyware

- This category covers all applications which send private information without user consent/awareness.
- Spyware uses tracking functions to send various statistical data such as a list of visited websites, email addresses from the user‘s contact list, or a list of recorded keystrokes.
- The authors of spyware claim that these techniques aim to find out more about users’ needs and interests and allow better-targeted advertisement.
- The problem is that there is no clear distinction between useful and malicious applications and no one can be sure that the retrieved information will not be misused.
- The data obtained by spyware applications may contain security codes, PINs, bank account numbers, etc.

Hoaxes

Mail thinks this message is Junk Mail.

From: Instant , Booster
Subject: Can you [illegible] to lose 200,[illegible] al custo
Date: [illegible] June 2008 23:33:[illegible]
To: comm[illegible] ectri[illegible]

Ca[illegible] potential [illegible] ers per year

How [illegible] you like to [illegible] 1000s of fresh,
new visitors [illegible] Your web site or affiliate web site from
Goo[illegible] ahoo, MSN and others At $0 cost to you...?

...INSTANT BOOSTER diverts 1000s of fresh,

- A hoax is misinformation that is spread across the Internet.
- Computer Virus hoaxes try to generate fear, uncertainty and doubt (FUD) in the recipients, bringing them to believe that there is an “undetectable virus“ deleting files and retrieving passwords, or performing some other harmful activity on their system.
- Some hoaxes work by asking recipients to forward messages to their contacts, perpetuating the hoax.
- If you see a message prompting you to forward it to everyone you know, it may very well be a hoax.
- Before forwarding, perform an Internet search on any message you suspect is a hoax.

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. 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.

Recognizing spam scams

- Sender address does not belong to someone on your contact list.
- You are offered a large sum of money, but you have to provide a small sum first.
- You are asked to enter, under various pretenses (data verification, Financial operations), some of your personal data – bank account numbers, usernames and passwords, etc.
- It is written in a foreign language.
- You are asked to buy a product you are not interested in.
- Some of the words are misspelled in an attempt to trick your spam filter.

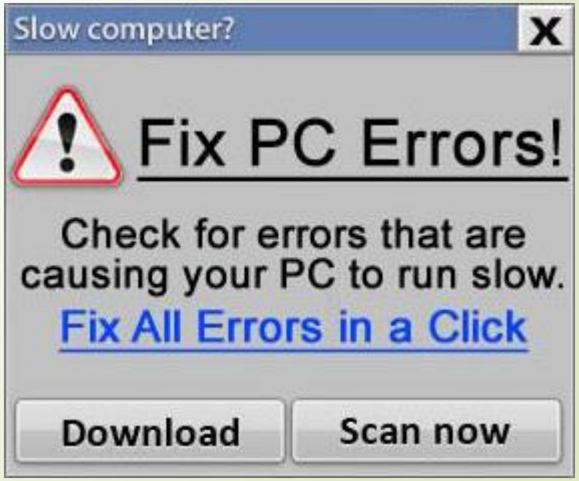
How Did My PC Get Infected with Infiltration?

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.

How to avoid malware

- Secure your computer - running antivirus and antimalware software.
- Back up your files
- Avoid suspicious links
- Identify suspicious sites



Fix PC Errors!

Check for errors that are causing your PC to run slow.

Fix All Errors in a Click

Safe online shopping

- **Shop from home** - to protect sensitive information like credit card numbers, we'll want to shop from our home Internet connection if possible.
- **Look for HTTPS** - many websites will display a lock symbol in the address bar. This is most commonly seen on the payment page of an online store. This means the website is using an HTTPS connection, which makes it safe to enter your information.
- **Research the company or seller -** anyone can set up a shop online, so it's important to research a company or seller before buying from the site. Make sure the business has a physical address and phone number you can contact if there's a problem.

Safe online shopping – cont.

- **Use secure payment methods** - credit cards are generally the safest way to pay for items online. Avoid options like direct wire transfer, bank transfers, or sending cash or checks through the mail.
- **Keep a record** - always save records of your online transactions, which should include the receipt, order number, product description, and price. You will also want to save any emails you send or receive from a seller, which may come in handy if there's a problem later on.
- **Trust your instincts!**

Understanding browser tracking

- Whenever you use the Internet, you leave a record of the websites you visit, along with each and every thing you click.
- To track this information, many websites save a small piece of data—known as a cookie—to your web browser.
- In addition to cookies, many websites can use your user accounts to track browsing activity.
- While this type of browser tracking doesn't pose a serious risk to your online security, it's important to understand how your online data is tracked and used.

Why do websites track browsing activity?

- Video sites like YouTube and Netflix collect information on the videos you watch, which helps them suggest more videos you might like.
- Online stores like Amazon and eBay keep a record of the different items you view and purchase, which helps them suggest other products you may want to buy.
- Search engines like Google keep a record of the things you search for. This can help them suggest more relevant searches, but it can also be used for advertising purposes.

How do cookies work?

- Cookies can store specific information on the websites we visit and the things we click on different sites.
- If wedon't have an account on a particular site, this information is typically saved in a cookie to our web browser.
- Cookies don't pose a serious risk to our online security—we're unlikely to acquire malware or expose sensitive financial information by using cookies.
- **How to avoid cookie tracking?**

Understanding social media privacy

- Social media sites like Facebook, Instagram, and Twitter have made it easier than ever to share things online.
- But sharing something on social media is a bit different from other types of online communication.
- Unlike email or instant messaging, which are relatively private, the things you share on social media are more public, which means they'll usually be seen by lots of other people.
- **Think before you share!**
- **Review your privacy settings!**

Detecting 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).

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

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.

Home Wi-Fi security

- Limit your signal strength so it cannot be detected beyond the boundaries of your home.
- Disable SSID (service set identifier) broadcasting so your network is not visible to other wireless users within its signal range.
- Use a strong password. You should choose a password or passphrase that's easy for you to remember but difficult for others to guess.
- Make sure your network utilizes WPA (Wi-Fi Protected Access) or WPA2.
- If you use the older WEP (Wired Equivalent Privacy) instead of WPA, make sure to maximize the encryption.

Public Wi-Fi safety tips

- Make sure you are on a legitimate network. Cybercriminals sometimes set up rogue networks with common names like Free Wi-Fi or Public Wi-Fi to get you to connect to illegitimate networks.
- Protect your computer by making sure your firewall is turned on and your antivirus software is up to date.
- Turn your Wi-Fi Connection to Network settings to a manual or non-automatic mode.
- Go to your Network or Sharing settings and disable File and Printer Sharing to prevent others on the network from accessing your files.
- Make sure you are aware of the people around you when using a hotspot.
- Do not conduct financial transactions like banking or shopping with a credit card while using public hotspots.

Creating strong passwords

- Never use personal information such as your name, birthday, user name, or email address.
- Use a longer password. Your password should be at least six characters long, although for extra security it should be even longer.
- Don't use the same password for each account.
- Try to include numbers, symbols, and both uppercase and lowercase letters.
- Avoid using words that can be found in the dictionary. For example, swimming1 would be a weak password.
- Random passwords are the strongest. If you're having trouble creating one, you can use a password generator instead.

Thank you for your attention!