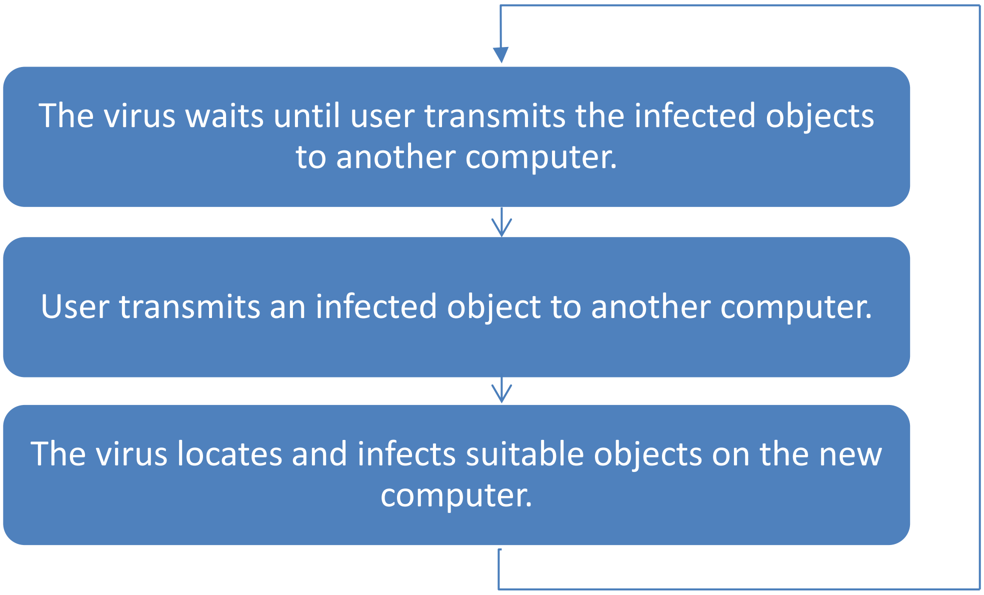
COMPUTER INFILTRATIONS

The term infiltration covers a wide range of computer programs that have one thing in common. Once released, they replicate in a way that cannot be controlled by their author. This can easily lead to worldwide epidemics where millions of computers may become infected.

Viruses

A virus is a computer program that spreads or replicates by copying itself. There are many known techniques that can be used by a virus, and viruses appear on many platforms. By definition, a virus infects other programs with copies of itself. It has the ability to clone itself, so that it can multiply, constantly seeking new host environments. Some viruses contain routines that damage the computer system on which it runs. This so called payload routine may also display graphics, play sounds or music etc. This has led to a situation where viruses are assumed to cause deliberate damage, even if there are many viruses that don't. The term virus has become a synonym for malicious software, which is incorrect from a technical point of view.
The process of spreading a virus includes both technical features in the virus itself and the behaviour of the computer user. Most viruses are by nature parasitic. This means that they work by attaching themselves to a carrier object. This object may be a file or some other entity that is likely to be transmitted to another computer. The virus is linked to the host object in such a way that it activates when the host object is used. Once activate, the virus looks for other suitable carrier objects and attaches itself to them. Here is the typical lifecycle of a computer virus:

Figure 6.1 A typical lifecycle of a computer virus


The virus waits until user transmits the infected objects to another computer.

User transmits an infected object to another computer.

The virus locates and infects suitable objects on the new computer.

From this we can draw the conclusion that a virus does not appear as an object in itself. A virus always resides hidden in some useful object.

Types of Viruses

Viruses can become destructive as soon as they enter a system, or they can be programmed to lie dormant until activated by a trigger. This trigger may be a predetermined date or time. The well-known Michelangelo virus, for example, has a trigger set for Michelangelo's birthday (March 6). There are several different types of viruses that can infect PC systems.

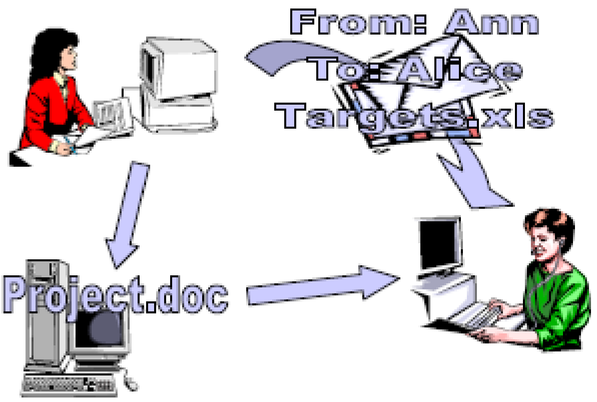
Boot sector viruses

A boot sector virus infects the boot sector of floppy disks or hard drives. The boot sector is a small program that initialises the operating system. By placing its virus code in the boot sector, a virus is guaranteed to be executed. It can load itself into the memory immediately and it is able to run whenever the computer is on, infecting the entire system. Boot sector infectors are spread through infected bootable floppy disks (or other removal media) and can damage the entire computer system from the moment the computer is switched on.

Document or macro viruses

Document or macro viruses are written in a macro language. Such languages are usually included in advanced applications such as word processing and spreadsheet programs. The vast majority of known macro viruses replicate using the MS Office program suite, mainly MS Word and MS Excel, but some viruses targeting other applications are known as well. Macro viruses differ from earlier boot sector and file viruses in many ways. Most differences are beneficial to macro viruses and enable them to spread much faster than any other kind of virus seen thus far. The most important difference is that macro viruses infect data files rather than program files.

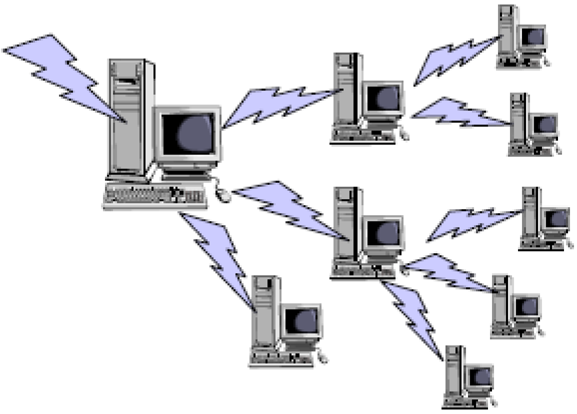
Figure 1 A document or macro virus spreads when documents are exchanged, regardless of the media used



Worms

A worm is by definition similar to a virus but more independent. Worms are constructed to infiltrate legitimate data processing programs and alter or destroy the data. A computer worm is a self-replicating computer program that penetrates an operating system with the intent of spreading malicious code. Worms utilize networks to send copies of the original code to other computers, causing harm by consuming bandwidth or possibly deleting files or sending documents via email. Worms can also install backdoors on computers. Worms are often confused with computer viruses, the difference lies in how they spread. Computer worms self-replicate and spread across networks, exploiting vulnerabilities, automatically, that is, they don't need a cybercriminal's guidance, nor do they need to latch onto another computer program.

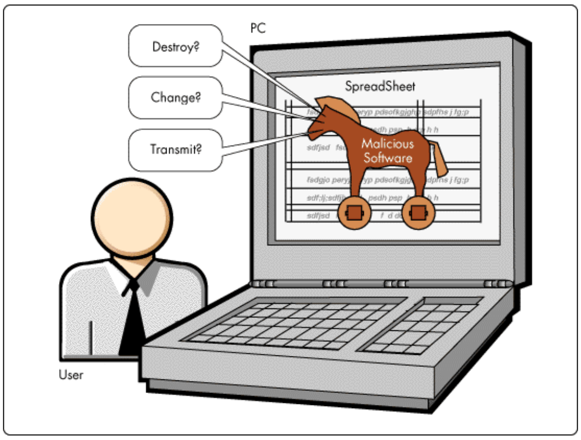
Figure 2 A pure worm locates and infects other machines on the same network without user interventions



Trojan horses

The name Trojan horse is borrowed from Greek mythology. In the computer world the term refers to a program that contains hidden malicious functions. The program may look like something funny or useful such as a game or utility, but harms the system when executed. Many Trojans contain activation criteria that enable the Trojan to work for a while. The user is convinced that the program is safe and useful, and forwards it to other users before the malicious code strikes. Trojans lack a replication routine and thus are not viruses by definition. A Trojan is spread to other computers only through deliberate transfer by the users.

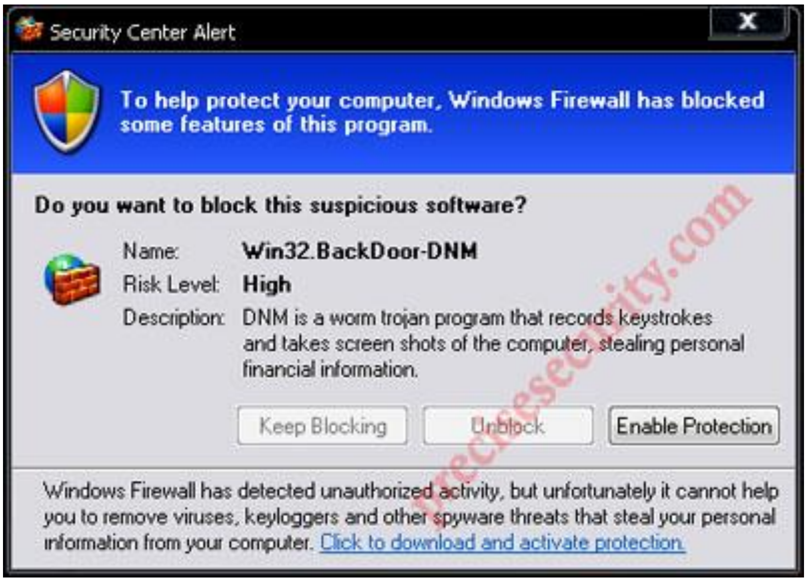
Figure 3 Trojan horse



Backdoor Trojans

Backdoor Trojans are a special kind of Trojan that grants unauthorized access to computer systems. This type of Trojan is rather common and can pose a significant threat to business users. The server module of a backdoor Trojan is often hidden in a useful program such as a game or a utility. There are several tools that allow hackers to attach backdoor Trojans to virtually any computer program. The modified program still works normally, but installs the spying tool in the target computer in addition to its normal functionality.

Figure 4 Backdoor Trojan



To help protect your computer, Windows Firewall has blocked some features of this program.

Do you want to block this suspicious software?

Name: Win32.BackDoor-DNM
Risk Level: High
Description: DNM is a worm trojan program that records keystrokes and takes screen shots of the computer, stealing personal financial information.

Windows Firewall has detected unauthorized activity, but unfortunately it cannot help you to remove viruses, keyloggers and other spyware threats that steal your personal information from your computer. Click to download and activate protection.

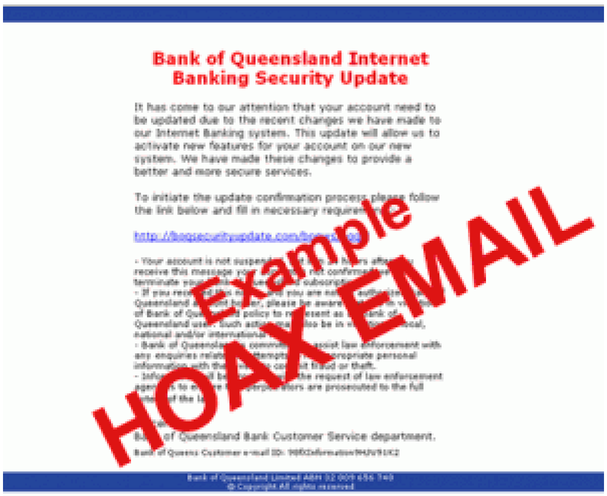
Jokes

A joke program does something funny or tasteless, but does not harm the computer environment. The effect may be music or sounds, video or animations, interactive functions etc. Some jokes may disturb the computer’s user interface and be rather annoying, but the effect is temporary and no permanent damage is done. If permanent damage is done, then the program is by definition a Trojan rather than a joke.

Hoaxes

A hoax is a chain letter that is usually circulated as an email message. These chain letters may have any content and are actually not related to computer viruses in any way. However, the problem is well known to vendors of anti-virus software because many hoaxes warn about a non-existing computer virus. A trained security expert can usually tell a hoax from a real virus warning. Many hoaxes describe viruses with functionalities that usually disclose the real nature of the message. The source is often not a reliable security expert and the message contains the famous sentence “Forward this warning to all your friends immediately”.

Figure 5 Hoax virus



Bank of Queensland Internet Banking Security Update

It has come to our attention that your account need to be updated due to the recent changes we have made to our Internet Banking system. This update will allow us to activate new features for your account on our new system. We have made these changes to provide a better and more secure services.

To initiate the update confirmation process please follow the link below and fill in necessary requirements.

http://boqsecurityupdate.com/[illegible]

- Your account is not suspended [illegible] hours after [illegible] receive this message your [illegible] not confirmed [illegible] terminate your [illegible] subscription [illegible]
- If you rece[illegible] you are not [illegible] authorised [illegible] Queensland [illegible] holder, please be aware [illegible] of Bank of Qu[illegible] policy to re[illegible]present as [illegible] Bank of Queensland user. Such action [illegible] also be in [illegible] local, national and/or international [illegible]
- Bank of Queensland [illegible] committed [illegible] assist law enforcement with any enquiries relat[illegible] attempts [illegible] appropriate personal information with th[illegible] commit fraud or theft.
- Info[illegible] b[illegible] the request of law enforcement agen[illegible] to e[illegible] perpetrators are prosecuted to the full [illegible] of the l[illegible]

[illegible]

B[illegible] of Queensland Bank Customer Service department.

Bank of Queens Customer e-mail ID: [illegible]

Bank of Queensland Limited ABN 32 009 656 740
© Copyright All rights reserved

Virus authors and impact on IT systems

A common belief is that viruses are written by teenage boys. This is true in part, but the situation is changing as new virus writing techniques enter the scene. Writing a working virus is not too difficult, but writing a successful virus is not an easy task. The motives of most virus writers remain unknown. There are however some motives that can be identified by examining virus samples or talking to known or anonymous virus authors.

- ✓ **Challenge and curiosity** – there are no courses or good books about how to write viruses. Many programmers want to see if they can do it, and do not necessarily realize that the virus may cause significant damage.
- ✓ **Fame and power** – even if the author remains anonymous, it probably gives a kick to read about the virus in headlines. The virus, and possibly the damage it has caused makes other people work and react in some way.
- ✓ **Protest and anarchy** – a virus is quite a powerful way to cause intentional damage. There have been cases where a virus is intended to harm a school's network.
- ✓ **Proof of concept** – someone may for example want to prove that a certain replication technique works. This type of virus may also appear on new platforms or applications capable of hosting viruses.
- ✓ **Political motives** – a virus may be used to spread a political message. This may, for example, be protests against totalitarian governments, multinational corporations etc. Organized political parties do not use viruses.

The damage caused by viruses can be divided into two categories: intentional damage and unintentional damage. Intentional damage, or harmless effects, is caused explicitly by the payload routine. Unintentional damage may be caused as a side effect when the virus replicates.

Harmless effects

These effects are always produced by the payload routine, but they are not malicious. The effect may be a picture, animations or video, music or sounds, interactive functions, political messages etc. These effects usually give you an idea about the virus author’s way of thinking, age or nationality. These effects may be funny or annoying and may distract or disturb the user, but they do not cause any permanent damage.

Compatibility problems

Individuals make viruses and worms and they do not have resources to test their creations on a wide range of computer systems. Nor do they develop the viruses according to quality control systems and guidelines. This makes it likely that they cause compatibility problems when run on systems that differ from the one on which they were developed. These problems can occur as error messages, crashes, inability to access certain functions etc. These problems are grouped as unintentional damage.

Compromising system integrity

Intentional damage is often caused by erasure or modification of data. Erasing files is perhaps the most obvious way to cause damage. Erasing files, however, is a clumsy way and modern, well maintained, systems can usually recover from backups. Modifying data is a much more sophisticated strategy. Small changes are made to the system now and then. The backup routine stores partially corrupted data until the virus is detected. Restoring the data is hard or impossible as several generations of backups are compromised. The last correct backups may be too old and it may even be hard to tell which backups are or are not valid.

Granting unauthorized access

Viruses may plant backdoors in the system, or steal passwords. These functions can later be used by hackers to access the system. Damage caused by such hacking activities is hard to predict. Unauthorized usage of the system may, for example, continue unnoticed for a long time.

Disclosure of confidential data

Viruses and worms have access to the same communication methods as the user, and even use them to replicate. A payload routine may easily locate documents that match certain criteria and send them to anyone on the Internet. Some email worms also cause disclosure of data as a part of replication. The worms that replicate when attached to a document, such as Melissa, send this document to recipients to whom the user had no intention of sending the document.

Computer resource usage

Viruses and worms can disturb computer systems by spending resources, either intentionally or unintentionally. Some viruses contain payloads that deliberately eat system resources, but resource consumption is probably unintentional in most cases. Unintentional resource consumption may be caused by errors in the virus or the replication. Code Red is an example of this. Searching for new hosts to spread to requires both network traffic and CPU resources. This load was obvious in the slower response time from the infected web servers or even in the total inability to serve users.

Human resource usage

Cleaning virus infections means extra work for the IT support staff. This damage, and the downtime for the user, may result in great expense unless the viruses are stopped properly using anti-virus software.

PR aspects

The attitude towards viruses is negative. The problem is well known and all business users know the severity. Sending a virus to a customer or business partner is not good for the company's image. This may be especially dangerous if the incident makes it to the headlines. This is not at all impossible, especially if the virus was included in a mass-produced software product.

Computer protection

Protecting your computer from viruses and other threats isn't difficult, but you have to be diligent. Here are some tips for computer protection:

- ✓ ***Install an antivirus program***. Installing an antivirus program and keeping it up-to-date can help defend your computer against viruses. Antivirus programs scan for viruses trying to get into your email, operating system, or files. New viruses can appear daily, so check the antivirus manufacturer's website frequently for updates. Some antivirus programs are sold with annual subscriptions that can be renewed as needed, but many are also available for free.
- ✓ ***Don't open email message from unfamiliar senders, or email attachments that you don't recognize.*** Many viruses are attached to email messages and will spread as soon as you open the email attachment. It's best not to open any attachment unless it is something you are expecting.
- ✓ ***Use a pop-up blocker with your browse.*** Pop-up windows are small browser windows that appear on top of the website you're viewing. Although most are created by advertisers, they can also contain malicious or unsafe code. A pop-up blocker can prevent some or all of these windows from appearing.
- ✓ ***Use a firewall.*** Windows Firewall or any other firewall program can help alert you to suspicious activity if a virus or worm attempts to connect to your computer. It can also block viruses, worms, and hackers from attempting to download potentially harmful programs to your computer.
- ✓ ***Use your browser's privacy settings.*** Being aware of how websites might use your private information is important to help prevent targeted advertising, fraud, and identity theft.
- ✓ ***Turn on User Account Control (UAC).*** When changes are going to be made to your computer that require administrator-level permission, UAC notifies you and gives you the opportunity to approve the change. UAC can help keep viruses from making unwanted changes.

✓ ***Clear your Internet cache and your browsing history.*** Most browsers store information about the websites you visit, and information that websites might ask you to provide (such as your name and address). While it can be helpful to have these details stored on your computer, there are times when you might want to delete some or all of them, for example when you're using a public computer and don't want to leave personal information behind.

Control questions

1) What is computer virus?
2) Explain worms, trojans and hoaxes?
3) Explain some impacts of viruses on computers.