Essay Title: The Cause and Effects of Computer Viruses

Abstract: From the analysis of web security, and particularly the topic of 'The Cause and Effects of Computer Viruses', it can be seen that many different types of computer viruses cause problems for computers all over the world, with varying degrees of severity.

Regardless of the degree of severity, the cause of the problems cannot be overlooked, as however minor the effect is on a user, the ability of the virus to spread and increase in overall severity is a major problem with individual and organisational web security.

Introduction: Computer viruses are a major problem for computer users. They infect a large number of computer-related systems, affecting computer security everyday, even on the web. Computer viruses are continually be created, according to Computer Research and Technology (http://www.crt.net.au/index.htm) at a rate of 15 new viruses per day (see Herald Sun search in Part A), and they are spreading and infecting millions of computers at alarming rates.

Viruses are transferred between computer systems using various methods. The effects of the viruses vary depending on the area the virus was created to affect, and depending on the severity of the virus.

Since the discovery of viruses many computer security companies have formed (e.g. Norton Anti-Virus) and are attempting to identify specific viruses so that they can protect computer systems worldwide.

The area of transmission this essay will be focusing on relates to the transmission of viruses using the web. As the web allows for the sharing of data between computers and networks, it is an ideal method for virus transmission.

This essay will focus mainly on the causes and effects that arise from computer viruses that are transferred using the web, using information gathered from various sites on the web.

Body: Computer viruses transmitted using the web affect web security and can cause web-reliant companies to lose millions of dollars.

The causes of viruses must be looked at, so that the effect on web security can be seen. The majority of web related viruses arise from downloading data from the web, and receiving e-mails. Certain e-mail accounts are more prone to sending viruses than others. According to Computer Research & Technology (http://www.crt.net.au/index.htm) 'Analysis has shown that a greater percentage of viruses come from 'free' mail accounts than from general private domains. The average number of viruses contained within one popular, free mail system soared to one in 500'. This shows that a major cause of computer viruses affecting the security on the web is the free e-mail accounts provided by certain web-sites, as the users of these free accounts are greater prone to receiving and forwarding infected files, thus reducing the security on the web

Web transmitted viruses can be as simple as receiving an e-mail with an attachment and opening the attachment. The virus that was received from the attachment, once belonged to another computer, and will attach itself to files on the host computer and replicate according to the virus's definitions. From this it can be seen how viruses are transferred and therefore cause computer security problems. This is further emphasised by Brain (http://www.howstuffworks.com/index.htm), who states 'A person might download an infected game from a bulletin board and run it. A virus like this is a small piece of code embedded in a larger, legitimate program. Any virus is designed to run first when the legitimate program gets executed. The virus loads itself into memory and looks around to see if it can find any other programs on the disk. If it can find one, it modifies it to add the virus's code to the unsuspecting program. Then the virus launches the "real program." The user really has no way to know that the virus ever ran'. From Brain's comments it can be seen that the cause of the virus can be from receiving something simple from the web.

Another form of computer virus is a hoax. Hoaxes do not actually replicate when you execute programs like the above virus. Hoaxes basically inform the user of some disturbing and untrue information that the user inevitably forwards to other friends and colleagues. According to Computer Research & Technology (http://www.crt.net.au/index.htm) 'a virus hoax is an e-mail that is intended to scare people about a non-existent virus threat. Users often forward these alerts thinking they are doing a service to their fellow workers, but this causes lost productivity, panic and lost time. This increased traffic can soon become a massive problem in e-mail systems and cause unnecessary fear and panic'. This further emphasises how another type of virus is caused, and how it affects web security.

The effects of viruses must also be looked at so that the effects on web security can be fully realised. Viruses cost organisations thousands of dollars. According to Computer Research and Technology (http://www.crt.net.au/index.htm) 'the financial cost of virus infection, measured in cost per incident, has declined to $2,454 in 2000 from $8,100 in 1996, according to the ICSA study. The study also reports that complete recovery from an infection takes an average of 45.6 hours and 9.4 person-days of work. Often the cost is much more: one respondent to the study reported a cost of $150,000 for a single incident. The ICSA study indicates that the reported costs of virus infection would be much higher if related costs such as loss of business and lower productivity were taken into consideration' (also see Herald Sun search in Part A). This further emphasises the effect viruses have on web security, as the cost of a virus can be very expensive.

The severity of computer viruses varies according to the type of virus. As can be seen above, a hoax usually does not affect any files on a computer, but it can cause a loss in productivity. Therefore the severity of a hoax depends on the amount of productivity lost.

According to Brain (How Stuff Works - http://www.howstuffworks.com/index.htm) 'most viruses have some sort of destructive attack phase where they do some damage. Some sort of trigger will activate the attack phase, and the virus will then "do something" -- anything from printing a silly message on the screen to erasing all of your data'. It can be seen from this statement that the severity of the virus ultimately depends on the attack phase, and the effect of the silly message or lost data on the user.

Viruses also can adjust filenames on your computer and they can attack virus scanners, according to Computer Research and Technology, which will inevitably affect the security of the users' computer on the web.

Conclusion: From the above analysis of the causes, transmission and effects of computer viruses it can be seen that poor web security can result in large amounts of damage to the user.

On the other hand it can also be seen that poor web security can result from viruses that are received simply by opening e-mail attachments, or by downloading information from the web.

However the virus is received the overall conclusion is that viruses are easily transmitted and the result of obtaining a virus can be loss of time, money, or just sher frustration with computer performance for the user.

References: This assignment was completed using the work created by authors employed by the companies that maintain the web-sites listed under resources in this web-site.