Analysis of Internet Security Measures Surrounding the World

Amit Kumar Jain*, Yashpal Singh,K.K Pandey, Sachin Upadhyay

Abstract The objective of this paper is to estimate the statistics surrounding the most common security threats faced by Internet users. There is an estimated of more than two billion Internet users worldwide, therefore it is important to know what security threats your computer may be vulnerable to while using the Internet. Threats discussed in this paper will include spam, phishing, computer viruses, hackers, and spyware/malware. The current percentage of Incidents as they are related to different regions of the world discusses the severity of each threat, by using suitable statistical techniques. Due to the large number of Internet users, it is probable that many of them are unaware of these threats and what they can and should be doing to protect themselves. Most importantly this paper will discuss about threats. A user can take to defend themselves against these threats and known vulnerabilities. With identity theft on the rise, it is imperative to understand Internet security threats now more than ever.

Keywords: Computer Security, Trojan horse, Spyware, etc.

1 INTRODUCTION

There are many security Measures that face computers in the world today, and we are going to see at a few of them as they relate to the Internet. Since its inception, the Internet has grown from original purpose as a military tool to a worldwide phenomenon. According to the latest statistical analysis, it is estimated that more than two billion internet users are worldwide. The following table provides the statistical breakdown of world internet usage.

The Internet is full of useful information, in fact, it is estimated that there are between 15 and 30 billion different websites in existence today. Considering this estimate of available websites, it is easy to see that the Internet is an invaluable resource to many people.

Table-1: World Internet Users and Population Statistics

World Regions	**Population (2011 Est.)**	**Internet Users Dec 31,2000**	**Internet users latest data**	**Penetration(% population)**	**Growth 2000 - 2011**	**Users% of table**
Africa	1037524058	4514400	**118609620**	11.4%	2527.4%	5.7%
Asia	3879740877	114304000	**922329554**	23.8%	706.9%	44.0%
Europe	816426346	105096093	**476213935**	58.3%	353.1%	22.7%
Middle East	216258843	3284800	**68553666**	31.7%	1987.0%	3.3%
North America	347394870	108096800	**272066000**	78.3%	151.7%	13.0%
Latin America	597283165	18068919	**215939400**	36.2%	1037.4%	10.3%
Oceania /Australia	35426995	7620480	**21293830**	60.1%	179.4%	1.0%
World Total	6930055154	360985492	**2095006005**	30.2%	480.4%	100.0%

The Internet provides many diverse and useful resources such as email, instant messaging, academic research, product research, paying bills, shopping, online banking, and the list goes on and on. For many of the Internets 2.09 billion users the Internet is not just a tool but a way of life. Businesses and people all over the world rely heavily on the Internet to perform their vital daily tasks (Table-1).

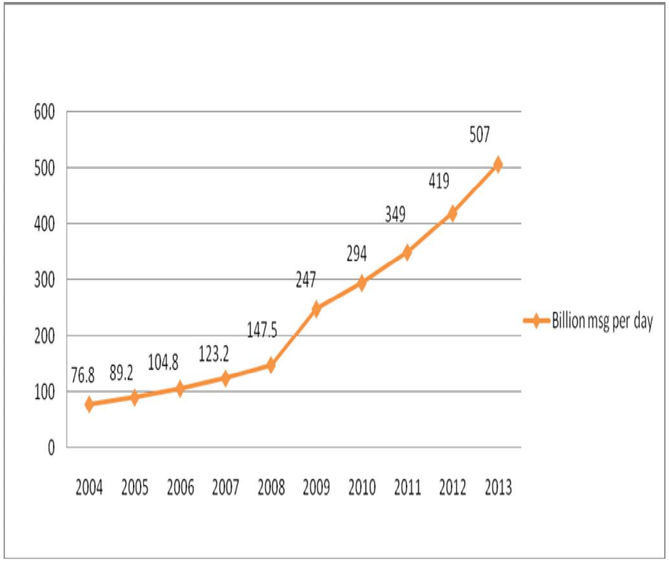
The Internet has become such an integral part of global society to the extent that the world would be hard pressed to continue forward with such great progress without it. There are so many well known advantages to using the Internet, however many users fail to take the time to research the risks involved. It is important to know the risks involved in any activity we decide to pursue in life and the Internet is no exception. The risks associated with the Internet are realized in the form of information security threats or vulnerabilities. The risks discussed in this paper include spam, phishing, Trojan viruses, hackers, and spyware/malware. This paper will also discuss some measures you, as a user, can take to help secure yourself and your computer against these Internet security threats.

Description of Project

*Author for correspondence.

Email is a very useful tool that many people use daily in their personal business endeavors. According to Radicati, 1.4 billion people around the world now use email regularly. This figures expected to grow steadily over the next two years, reaching 1.9 billion users by the end of 2013.

Figure-1: Email Traffic, 2004-2013



Internet Email Traffic Worldwide

Email is very convenient, but with that convenience comes several security risks. The most common and potentially the most harmful email security threat is not in what you send but what is sent to you. Junk email, or Internet solicitations, is a huge security risk. This type of email is widely known by the name of spam. Time wasted deleting junk e-mail costs American businesses more than $30 billion a year. Sending an email to someone is the virtual equivalent of sending someone a postcard through regular post office mail. For this reason, it is a good idea to use encryption when sending an email that contains confidential information. A Telephone-based survey of adults who use the Internet found that more than 75% receive spam daily. The average spam messages per day are 20.5, and the average time spent per day deleting them is 2.9 minutes. The loss in productivity is equivalent to $25 billion per year at average US wages, according to the National Technology Readiness Survey produced by Rockbridge Associates and the Center for Excellence in Service at Maryland's business school. 14% of spam recipients actually read messages to see what they say, and 4% of the recipients have bought

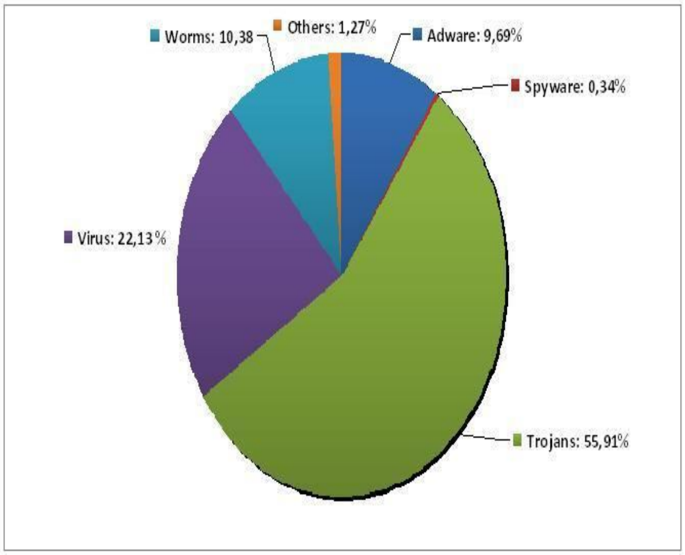
Something advertised through spam within the past year. The best defense against spam is to use a spam filter. A computer user needs to be aware of what spam is and is not so they can make informed decisions when an email arrives in their inbox. If you use Outlook 2010 or higher there is a built-in spam filters that you can configure to your personal requirements. It is also needful on a corporate or enterprise level to use a hardware spam filter to block known spam before it reaches the end users. This will save you much time and money later and is worth the investment. While it is important to defend against spam, it is nearly impossible to filter it all out. This is why user education is so important.

Email users are also being targeted by a different type of spamming technique called phishing. Phishing is a fraudulent attempt, usually made through email, to steal your personal information. The best way to protect you from phishing is to learn how to recognize a phish. A phishing email attempt will appear to many users to be a legitimate email perhaps from a reputable company or bank. However, the intent of the sender is to tempt you into giving them your personal information such as your social security number, usernames and passwords, and even your bank account or credit card numbers. This is done by sending huge amounts of spam phishing emails to many users by someone claiming for example to be your bank. The phishing email may state that your bank account information needs to be updated and will provide a hyperlink to a website that looks like your bank's website.

However, this is not your bank's website, but one created by the phisher to look just like it! You use your login information, and update your personal information and logout thinking you have updated your information, but what you have really done is given your information to a thief. The phisher will then use your personal information to steal your identity and your money. You can defend yourself against phishing attempts by being aware of procedures. A bank will never send you an email asking you for your personal information. Most of the banks correspondence will be done with post office mail or with a phone call. It is vitally important to investigate any email or link to a website you receive via email before you input any of your personal information. Microsoft's Internet Explorer 7 actually has a built in anti-phishing filter that will scan websites against a pool of known phishing sites. While this is not fool proof, it is an added defense against phishing attempts. This feature must be turned on to work, and this can be accomplished through Internet options under tools on the file menu. Again, user education and an awareness of procedure is the best defense against this type of threat or scam.

Another common Internet security measure is becoming infected with a computer virus. A computer virus can be passed many ways such as via email, floppy disk, CDRW, flash drive, network connection, or a hacker breaking into your system. There are many different computer viruses in existence today. Each one is different and their creators had different motives or functions for the virus to perform. There were over 50,000 computer viruses in 2000 and that number was then and still is growing rapidly. Sophos, in a print ad in June 2005 claims "over 103,000 viruses." And, Symantec, in April 2008 is reported to have claimed the number is over one million. Fortunately, only a small percentage of these are circulating widely. Some viruses will simply cause your data to become corrupt, while others are designed to steal your data or create a backdoor into your system via the Internet, which are called Trojan's.

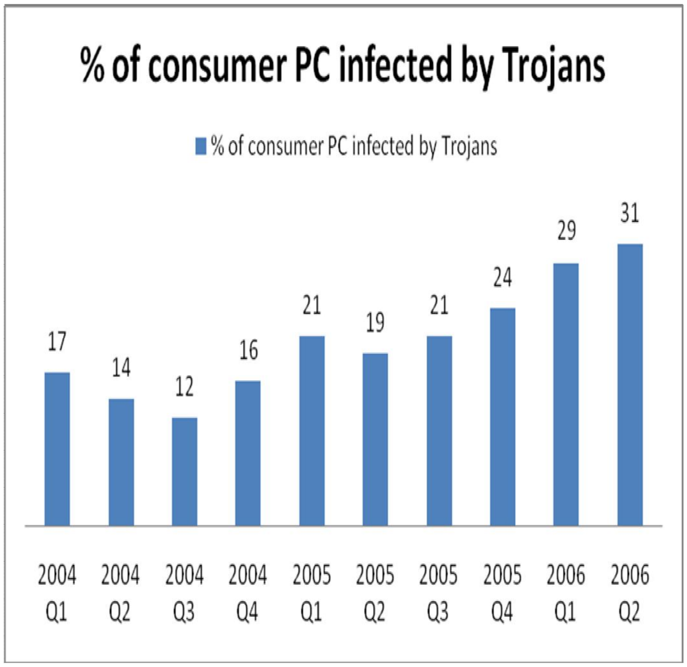
Figure-2 Annual security report 2010



Trojans still dominate the ranking of new malware that has appeared in 2010 (56 percent of all samples), followed by viruses and worms. It is interesting to note that 11.6 percent of all the malware gathered in the Collective Intelligence database is rogueware or fake antivirus software, a malware category that despite appearing only four years ago is creating much havoc among users.

Every day viruses cause a huge amount of data loss, and in turn cost individuals time and money. The best defense against computer viruses is to install an antivirus program on every computer you own. An antivirus program can only detect a virus if it knows the virus exists, and it does this via virus definitions. Since new viruses are constantly being created it is Imperative to keep your antivirus definitions up to date and by using a package with an automatic update feature will do this for you. Also, be sure the antivirus you use utilizes real-time protection, which will quickly identify the presence of a virus. There are many different antivirus vendors, and there are equally as many opinions on which one are the best to use. When selecting an antivirus product, make sure it includes an automatic update feature.

Figure-3 The infection of Trojan analyze by webroot is given below from 2004 to 2006

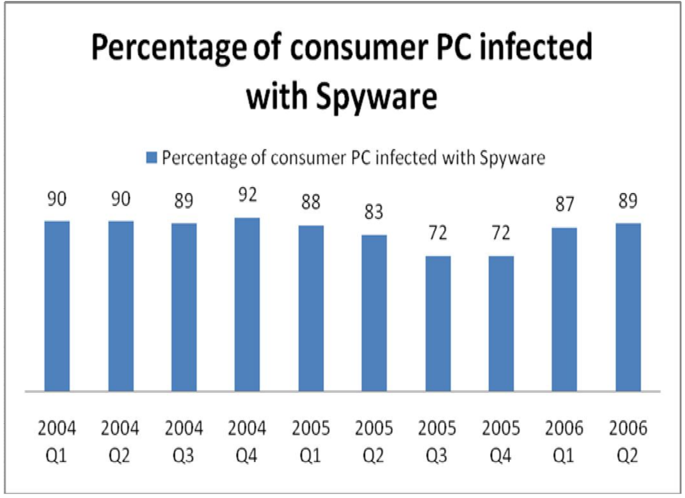


Trojan Infections from 2004 – mid 2006

It is also important that your antivirus program scans email attachments automatically for viruses. Since many viruses are transmitted via email this can be a valuable tool! First and foremost, it is important as a user to be educated and aware of potentially harmful files. Never open any files or emails if you do not know the person that sent them to you. Following this rule can save you a lot of trouble later.

Another growing security threat is something knows as spyware. Spyware is a type of malware that can be installed on computers, and which collects small pieces of information about users without their knowledge. If you notice your computer is abnormally slow all of sudden, receives many pop-up advertisements, or your homepage has been hijacked, your computer is likely infected with spyware. Here are three shocking statistics reported by PCSecurityNews.com, 8 out of 10 PC's are infected with some sort of Spyware, with an average of 24.4 spies per PC scanned, Microsoft estimates that 50% of all PC crashes are due to spyware, Dell reports that 20% of all technical support calls involve spyware.

Figure-4 The infection of Spyware analyze by webroot is given below from 2004 to 2006



Spyware Infections from 2004 – mid 2006

The presence of spyware is typically hidden from the user, and can be difficult to detect. Typically, spyware is secretly installed on the user's personal computer. Sometimes, however, spywares such as key loggers are installed by the owner of a shared, corporate, or public computer on purpose in order to secretly monitor other users. When you look at these statistics it is easy to see that spyware is a very real threat to all PC's connected to the Internet, and many users are unaware that they are victims of spyware.

There are several defenses against spyware. To help stop the spread of spyware and other malware, it is essential to be alert to suspicious activity on your computer and to learn safe computing practices. While some spyware is deployed by exploiting flaws in operating systems or applications, much of it still relies on social engineering to trick you into running or installing malware. You must exercise caution when downloading anything from public web sites, newsgroups, instant messaging sessions, or when opening email attachments, even from senders you know. Identity is often difficult to verify on the internet. Frequently, attackers and their malware impersonate associates of the target user to coax them into installing the malicious code. A common example of this is when malware infects a system and then automatically emails itself to everyone in the infected person's address book. When such an email is received, the recipient is more likely to open the contents because the sender is a familiar, trusted source.

Don't trust unknown or known high-risk sources when visiting unfamiliar web sites, you should exercise caution. This guideline should also apply to sites you expect to be high risk based on their content. Such sites include those with many popup.

Pay attention when installing applications Software installation packages sometimes take advantage of a user's tendency to not pay attention to the details and simply accept the default "checked" options. If the default options are blindly accepted and prompts are ignored, clicking next, next, next may actually be agreeing to the installation of spyware, adware, or other applications that are not desired. Reading instructions and paying attention to what is being agreed to is important to staying safe. Keep your operating system and software up to date keeping systems and applications current with security–related patches is critical. This includes patching the operating system and all installed applications, especially those related to network and internet activity like browsers, media players, email clients, and news readers. These are very common targets of attack and second only to social engineering as a means of spreading malware.

Installing trusted antivirus and antispyware tools and keeping them and their signatures current is an important part of defensive computer security. There are many packages available for purchase and some available for free to download, such as Spybot and Ad-Aware. Microsoft has even joined the fight against spyware with their free for download program called Windows Defender. One of the best defenses against spyware is to prevent infection by developing safe Internet surfing habits. In other words, stay away from questionable websites. Spyware not only comes from websites but you can also be infected by Peer to Peer file sharing. Spyware and Viruses run rampant on P2P file sharing networks such as Lime Wire, Kazaa, Bear share, Gnutella, Grokster, and eDonkey. When you connect to these and other P2P networks to share files, the chances are you do not know who you are downloading the file from or who is downloading files from you. Forty-five percent of the executable files downloaded through Kazaa contain malicious code. It is the best practice not to use these types of services as a spyware or virus infection is likely to occur on your computer.

Another Internet security threat is hacking. Computer hacking is the practice of modifying computer hardware and software to accomplish a goal outside of the creator's original purpose. People who engage in computer hacking activities are often called hackers. Since the word "hack" has long been used to describe someone who is incompetent at his/her profession, some hackers claim this term is offensive and fails to give appropriate recognition to their skills. While it remains a very interesting subject or hobby for computer techies, it is a very serious threat and should not be taken lightly. A hacker may attempt to access your computer or network for a number of reasons, which include file storage, information for identity theft, malicious intent, or even just for fun. Many computers and networks have been compromised by hackers around the world, and the users are unaware they have been hacked. The best defense against hacking is to setup a strong defense perimeter.

A good basic defense should consist of a firewall, strong passwords (at least 8 characters long utilizing both numeric, alphanumeric, and special characters), the latest software patches for your operating system and applications, and Antivirus/Antispyware software with updated definitions. PSINet Europe purposely built an unprotected server and connected it to the Internet to determine how quickly it would be compromised. Their findings were astonishing: the server was maliciously attacked 467 times in the first 24 hours, most of the attacks originated in the US or Western Europe, and after 3 weeks a total of 626 attacks were detected against the server [8]. It is easy to see from this case study project that if you have a computer connected to the Internet without proper security, it will be compromised very quickly. It is especially important for users with a broadband Internet connection to maintain security due to the nature of the "always on" Internet connection. In this case your computer is always vulnerable to attack while it is powered on unless you have the network connection disabled or unplugged.

CONCLUSION

The goal of this paper is to help those users understand the Seriousness of current Internet security threats and to show them ways to protect their personal information.After compiling and analyzing these Internet security threat statistics, the only possible conclusion is that the Internet, while very useful, is not to be taken lightly.

Due to the commercialization and ease of use of the Internet in the last decade, it is only reasonable to conclude that the Internet will grow as society becomes more reliant on it and its conveniences. Every Internet user should be aware and educated of the threats and vulnerabilities that surround the Internet and know what to do to protect themselves against these known threats. Internet users should be encouraged to stay abreast of current threats and defense mechanisms by using the Internet itself as a research tool. There are many good sources on the Internet for current and past threats and how to setup a defense against them. The irony is that you can use the Internet to learn how to make your Internet surfing more secure. It is always important to know the risks of any activity a person chooses to pursue in life, and the Internet is no exception. It also never hurts to get a knowledgeable friend or consultant to take a look at your current configuration and make suggestions on how to harden your security. In conclusion, the Internet is full of useful material but this comes at a risk. It is important to develop safe surfing habits and a strong security plan before connecting to and utilizing the Internet.

With this conclusion, it is also reasonable to conclude that new Internet security threats will likely arise in the coming months and years, and therefore will require users to become even more proactive in defending their computer systems.

REFERENCES

1- World Internet Users and Population Stats. (2011, March 31). Internet World Stats. Retrieved March 31, 2011 from the WWW: http://www.internetworldstats.com/stats.htm

2- Sara Radicati, Email Statistics Report, 2009-2013; the radicati group, inc. a technology market research firm, Palo Alto, CA.

3- The report on malware to find out Trojan.(http://press.pandasecurity.com/news/2010-annual-security-report)

4- The size of the World Wide Web. (2007, February 25). Pandia Search Engine News. Retrieved March 20, 2007 from the WWW: http://www.pandia.com/sew/383-web-size.html

5- Security Statistics. (2005) Aladdin: Securing the Global Village. Retrieved March 21, 2007.(WWW: http://www.esafe.com/home/csrt/statistics/statistics_2005.asp)

6- Some Interesting RSA Phishing Stats. (2006, November 9) ZDNet.co.uk. Retrieved March 21, 2007 from the WWW: http://community.zdnet.co.uk/blog/0,1000000567,10004498o-2000331828b,00.htm