Statistical Analysis of Internet Security Threats

Daniel G. James

ABSTRACT

The purpose of this paper is to analyze the statistics surrounding the most common security threats faced by Internet users. There is an estimated 1.1 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 statistical analysis will show the current percentages of incidents as they relate to different regions of the world as well as discuss the severity of each threat. Most importantly this paper will discuss measures a user can take to defend themselves against these threats and known vulnerabilities. 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. With identity theft on the rise, it is imperative to understand Internet security threats now more than ever. 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.

INTRODUCTION

There are many security threats that face computers in the world today, and we are going to look 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 there are over 1.1 billion Internet users worldwide [1]. The following table provides the statistical breakdown of world Internet usage.

Table 1 World Internet Usage and Population Statistics

World Regions	Population (2007 Est.)	Population % of World	Internet Usage, Latest Data	% Population (Penetration)	Usage % of World	Usage Growth 2000-2007
Africa	933,448,292	14.2 %	**33,334,800**	3.6 %	3.0 %	638.4% %
Asia	3,712,527,624	56.5 %	**398,709,065**	10.7 %	35.8 %	248.8% %
Europe	809,624,686	12.3 %	**314,792,225**	38.9 %	28.3%	199.5 %
Middle East	193,452,727	2.9 %	**19,424,700**	10.0 %	1.7 %	491.4%
North America	334,538,018	5.1 %	**233,188,086**	69.7 %	20.9%	115.7

						%
Latin America/Caribbean	556,606,627	8.5 %	**96,386,009**	17.3 %	8.7 %	433.4 %
Oceania / Australia	34,468,443	0.5 %	**18,439,541**	53.5 %	1.7 %	142.0 %
WORLD TOTAL	6,574,666,417	100.0 %	**1,114,274,426**	16.9 %	100.0 %	208.7 %

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 [2]. Considering this estimate of available websites, it is easy to see that the Internet is an invaluable resource to many people. 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 1.1 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. 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.

PROJECT DESCRIPTION

Email is a very useful tool that many people use daily in their personal business endeavors. According to Radicati, 651 million people around the world now use email regularly. This figure is expected to grow steadily over the next four years, reaching 850 million users by the end of 2008 [3].

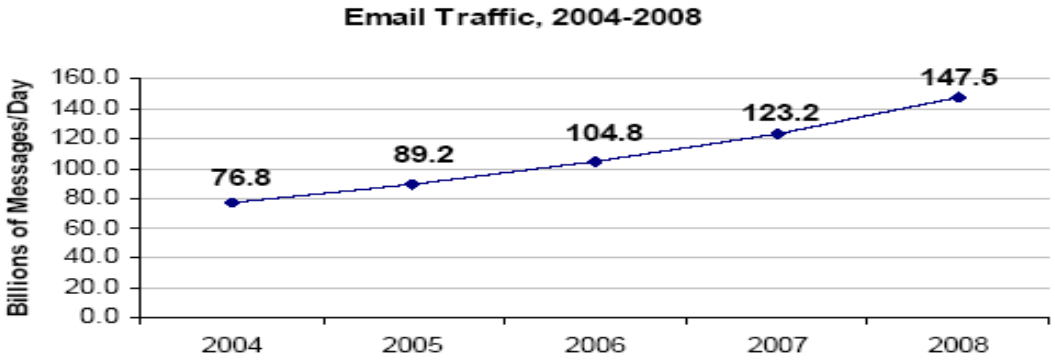

Figure 1 Internet Email Traffic Worldwide

Email is very convenient, but with that convenience comes several security risks. 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. 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, are 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 nearly $22 billion a year. A telephone-based survey of adults who use the Internet found that more than 75% receive spam daily. The average spam messages per day is 18.5, and the average time spent per day deleting them is 2.8 minutes. The loss in productivity is equivalent to $21.6 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 [3]. The best defense against spam is to use a spam filter. If you use Outlook 2003 or higher there is a built-in spam filter 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. 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.

Email users are also being targeted by a different type of spamming technique called phishing. 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 lure 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. In November 2006, 11% of fake banking websites attempted to spoof UK banking brands, while 75% of false banking sites targeted customers of US banks. The UK hosted 2% of these false banking sites, while the US hosted 63% of phishing sites globally [4]. 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 threat 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. Known computer viruses grew by 28,327 in 2004 to bring the number of old and new viruses to 112,438, according to IBM. In 2002, only 4,551 new viruses were discovered. Of 147 billion e-mails scanned by IBM for customers in 2004, 6% contained a virus. During 2002, just 0.5% of e-mail scanned had viruses [3]. 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 Trojan Infections from 2004 – mid 2006 [5]

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. There are many different antivirus vendors, and there are equally as many opinions on which one is the best to use. When selecting an antivirus product, make sure it includes an automatic update feature. 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. 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 know as spyware. 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 [6].

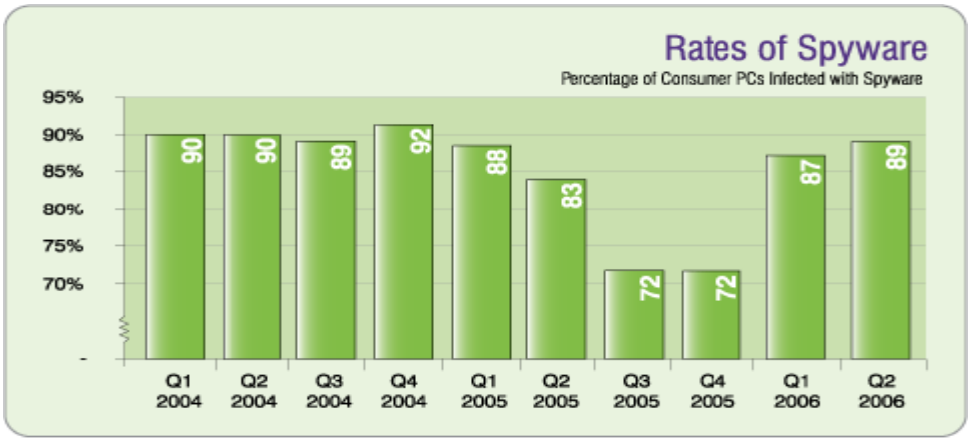

Figure 3 Spyware Infections from 2004 – mid 2006 [5]

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. The most popular method is using an Antispyware software package. These software packages work similar to Antivirus programs. Most have an automatic update feature to download the latest antispyware definitions and some will scan your PC for infections in real-time. 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 LimeWire, Kazaa, Bearshare, 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 [7]. 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.

The last Internet security threat we will discuss is the hacker. Computer hacking is something that has been glamorized by Hollywood in recent years. 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

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. 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. 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. 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. It is always important to know the risks of any activity a person chooses to pursue in life, and the Internet is no exception. 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 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.

REFERENCES

[1] *World Internet Users and Population Stats*. (2007, March 19). Internet World Stats. Retrieved March 20, 2007 from the WWW: http://www.internetworldstats.com/stats.htm

[2] *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

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

[4] *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

[5] *State of Spyware Q2 2006*. (2006, June) Webroot Software, Inc. Retrieved March 22, 2007 from the WWW: http://www.webroot.com/resources/stateofspyware/excerpt.html

[6] *Three Shocking Statistics on Spyware!*. (2007) PC Security News. Retrieved March 22, 2007 from the WWW: http://www.pcsecuritynews.com/spyware_statistics.html

[7] *Key Internet Usage Statistics*. (2006) GET-Websense. Retrieved March 23, 2007 from the WWW: http://www.3w.net/lan/internet-use-statistics.html

[8] *General Information Security Statistics*. (2004) Security Stats. Retrieved March 25, 2007 from the WWW: http://www.securitystats.com/infosec.html