Journal of Physical Sciences, Vol. 14, 2010, 191-198
ISSN: 0972-8791, www.vidyasagar.ac.in/journal
Published on December 24, 2010

An Extensive Study on Web Security Breaches

Mr. Taslim Taher, Shahid Al Noor and Md. Zakir Hossain

Computer Science Department, Stamford University, Bangladesh
Emails: ttaslim@gmail.com, shaahid_noor@yahoo.com,
zakir267ju@yahoo.com,

Received April 8, 2010; Accepted October 12, 2010

ABSTRACT

All over the history, the sea has been the lifeblood of commerce. Today, the Web is the modern sea, carrying electronic commerce and communications around the world. Since the turn of the century, that sea has been rough, with wave after wave of viruses and hacking attacks crashing into the cyber ports. In a networked world, there are no real safe harbors. If anyone is on the network, he is available to everyone else on the network. As economies become more dependent on information and communications technology (ICT), they are becoming more vulnerable to cyber attacks. The most serious cyber security risks are those that threaten the functioning of critical information infrastructures, such as those dedicated to financial services, control systems for power, gas, drinking water, and other utilities; airport and air traffic control systems; logistics systems; and government services. The number of attacks has become now so large and their sophistication has become so great that many organizations are facing trouble determining which new threats pose the greatest risk and how resources should be allocated to ensure that the most probable and damaging attacks are dealt with first. A concentrated and collaborative research effort as well as user awareness are needed to manage this situation. Only then the harbor defenses will improve and the situation will be better. The goal of this paper is to analyze the statistics surrounding the most common security threats related to web, to help the users understand the seriousness of current web security threats and to show them ways to protect their personal information.

Keywords: Spam; phishing; computer viruses; spyware/malware; hacking

1. Introduction

Computers and computer networks have been part of the corporate landscape for decades. But it’s only in the last five years that companies have started to connect these systems and networks to the outside world – suppliers, business partners, and the Internet. Unfortunately, in the hurry to get connected and jump on the e-business bandwagon, computer security is frequently given short shrift, placing corporate assets at risk. Computer users of today's world are facing many security threats and vulnerabilities, and this paper is going to look at a few of them. According to the latest statistical analysis, it has been found that over 1.1 billion users worldwide are connected to web [1]. The web has become the most important source of useful information now-a-days. It has been found that there are between 15 and 30 billion different websites in existence today [2]. Considering this number of available websites, it is easy to realize that the web is becoming an important resource to many people. For many of the 1.1 billion users who use the Internet, is not just a tool but a way of life. Businesses and people all over the world greatly depend on the Internet to perform their vital tasks. The Internet has become such an integral part of global society to the extent that the world would not be able to progress without it. Though there are so many well known advantages of using the web, many users fail to realize the risks involved. The risks associated with the Internet are normally realized in the form of information security threats or vulnerabilities.

2. Statistics of breaches and preventions

Email is the most common useful tool that many people use daily in their personal communication, business endeavors etc. According to Radicati, 651 million people around the world are communicating with one another using email regularly. Hopefully, this figure will grow steadily over the next four years, and this number may reach 850 million by the end of 2008 [3].

The most common and potentially the most harmful email security threat may be what is sent to the user. Junk emails, or Internet solicitations, are a huge security risk. This type of email is called spam. Between July 1 and December 31, 2005, 50% of all monitored email traffic was spam. This is a decrease from the first six months of 2005. Because, 61% of all emails were identified as spam during that time. In the second half of 2004, just over 60% of emails were identified as spam [4]. American businesses loss nearly $22 billion a year by deleting junk e-mail. A telephone-based survey found that more than 75% adults receive spam daily. The number of spam messages per day is 18.5 in average, and the average wastage of time per day for deleting them is 2.8 minutes. According to the National Technology Readiness Survey produced by Rockbridge Associates and the Center for Excellence in Service at Maryland's business school, the amount of loss in productivity is near about $21.6 billion per year at average US wages. 14% users among who have received spam actually read messages to see what they say, and 4% of them have bought something advertised through spam within the past year and mostly been cheated [3]. The best defense against spam is to use a spam filter. If anyone use Outlook 2003 or higher, there is a built-in spam filter that one can configure to his personal requirements. Corporate or enterprise level users should use a hardware spam filter to block known spam before it reaches the end users. Though it is important to prevent spam, it is impossible to filter it all out. That's why user education, awareness etc, are very important. All computer users should be aware of what spam is and is not so that they can make appropriate decisions when emails arrive in their inboxes.

Email users are also being affected by a different type of spamming technique called phishing. Phishing has proved to be a dangerous enemy now-a-days, drawing the attention of security experts and computer users worldwide. A phishing email attempt is normally appeared to many users just like a legitimate email perhaps from a reputable company or bank. The phishing email may ask someone's bank account information for updating and provide a hyperlink to a website that looks like his (user's) bank’s website. However, this is not his bank’s website, but one created by the phisher to look just like it! The misfortune user uses his login information, and updates his personal information and log-outs thinking he has updated his information, but what he has really done is given his information to a thief. The phisher will then use his personal information to steal his identity and money. According to the phishing statistics of World Phishing of Avira GmbH, the five topmost phishing regions in the world are North America, Europe, Africa, Central America and the Caribbean, Oceania and their Phishing Rates are 47.92%, 37.50%, 6.25%, 4.17% and 2.08% respectively [5].

One can defend himself against phishing attempts by being aware of procedures. A bank will never send anyone an email asking him for his personal information. Most of the banks correspondence are done with post office mail or with a phone call. Microsoft’s Internet Explorer 7 actually has a built in anti-phishing filter that scans websites against a pool of known phishing sites. Though this is not fool proof, it is an added defense against phishing attempts.

Another alarming Information security threat is computer virus. Virus is a computer program that copies itself into the host computer without the user's permission. It then reproduces itself and spreads on other computers. Many different computer viruses exist today. Each one is different and is created for different motives. Known computer viruses grew by 28,327 in 2004 to bring the number of old and new viruses to 112,438, according to IBM. Only 4,551 new viruses were identified in 2002. In 2004, 6% emails contained viruses among 147 billion e-mails scanned by IBM for customers. While, just 0.5% of e-mail scanned had viruses during 2002 [3]. Some viruses simply cause one's data to become corrupt, while others are designed to steal one's data or create a back-door into his system via the Internet, which are called Trojan’s. The top 10 computer viruses of 2009 are listed in Table 1.

Installing an anti-virus program on every computer is the best defense against computer viruses. Many different anti-virus vendors are producing anti-virus programs of their own now-a-days, and there are also many opinions on which one is the best to use. When selecting an anti-virus product, one should

Table 1. Top 10 Computer Viruses of 2009 [6]

Rank	**Virus Name**
1	Win32/Conficker
2	INF/Autorun
3	Win32/PSW.OnLineGames
4	Win32/Agent
5	Win32/FlyStudio
6	INF/Conficker
7	Win32/Pacex.Gen
8	WMA/TrojanDownloader.GetCodec
9	Win32/Qhost
10	Win32/Autorun

Table 2. Top 10 Computer Anti-Viruses of 2009 [6]

Rank	**Virus Name**
1	BitDefender Antivirus
2	Kaspersky Anti-Virus
3	Webroot Antivirus
4	G DATA AntiVirus
5	AntiVirus ESET Nod32
6	ParetoLogic Anti-Virus PLUS
7	AVG Anti-Virus
8	Vipre Antivirus + Antispyware
9	F-Secure Anti-Virus
10	Trend Micro

make sure that it includes an automatic update feature. Since new viruses are constantly arriving, it is mandatory to keep one's anti-virus definitions up to date. And, using a package with an automatic

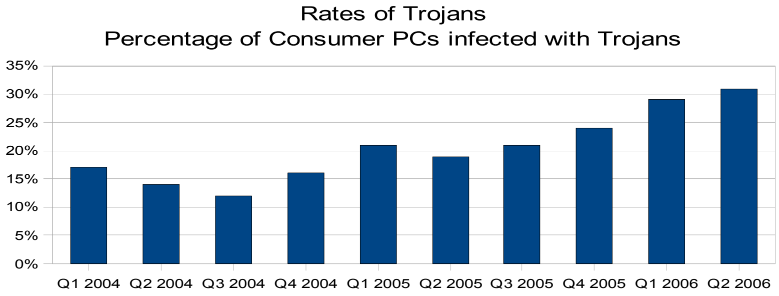

Fig.1. Trojan Infections from 2004 – mid 2006 [8]

update feature will do this for him. Also, one should make sure that the anti-virus he uses must utilize real-time protection, which will quickly identify the presence of a virus. It is also important that one's anti-virus program scans email attachments automatically for viruses.

Another growing security threat is spyware. If someone notices his computer becomes abnormally slow all of sudden, receives many pop-up advertisements, or his homepage has been hijacked, then his computer is probably infected with spyware. Three shocking statistics reported by PCSecurityNews.com are mentioned here, 8 out of 10 PC's have been attacked by some sort of Spyware, with an average of 24.4 spies per PC scanned, Microsoft estimates that 50% of all PC crashes cause of spyware, Dell reports that 20% of all technical support calls involve spyware [9]. According to Consumer Reports, State of the Net 2007, in the first half of 2007, spyware caused 850,000 U.S. Households to replace their computers. 1 out of every 11 surveyed, faced costly problem due to spyware. The economic fallout per incident was $100, causing total damage of about $1.7 billion [10]. According to Infonetics Research's Costs of Network Security Attacks: North America 2007, small and medium-sized organizations faced major problems due to spyware – representing 40% of all security downtime costs. Large U.S. organizations lose an average of 2.2% of their annual income which is more than $30 million, due to security attacks [10].

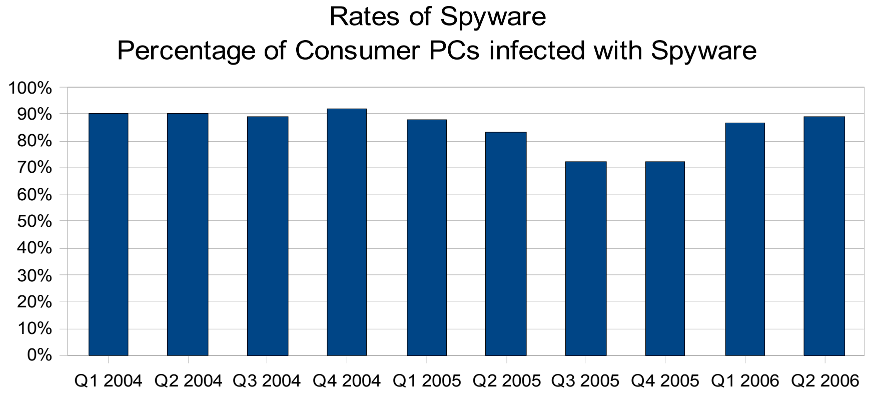

Fig. 2. Spyware Infections from 2004 – mid 2006 [8]

There remain several defenses against spyware. The most popular among them is using an Antispyware software package. The working methodology of these software packages is similar to Antivirus programs. Most of them contain an automatic update feature to download the latest antispyware definitions and some scan user's PC for infections in real-time. There are many packages which can be purchased and some are free to download, such as Spybot and Ad-Aware. Microsoft has even joined the fight against spyware with their free download-able program called Windows Defender. One of the best defenses against spyware is developing safe Internet surfing habits. In other words, questionable websites should be avoided. Though Spyware comes from websites, one can also be infected by Peer to Peer file sharing. Spyware and Viruses widely spread among P2P file sharing networks such as LimeWire, Kazaa, Bearshare, Gnutella, Grokster, and eDonkey. Forty-five percent of the executable files downloaded from Kazaa contain malicious code [11]. It is the best practice not using these types of services. Because, spyware or virus may affect one's computer in this way.

The last network security threat that will be discussed in this paper is hacking. Even Hollywood has glamorized Computer hacking in recent years. Though it is a very interesting subject or hobby for computer experts, it is a very serious threat that should not be taken lightly. A hacker may access one's computer or network for a number of reasons, which include stealing important file information, identity theft, malicious intent, or even just for fun.

Using a strong defense infrastructure is the best defense against hacking. 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 one's operating system and applications, and Antivirus/Antispyware software with updated definitions. PSINet Europe intentionally used an unprotected server and connected it to the Internet to determine how quickly it would be attacked. Their findings were surprising: the server was maliciously attacked 467 times in the first 24 hours, most of the attacks generated from the US or Western Europe. After 3 weeks, a total of 626 attacks were detected against the server [12].

3. Consequence of Legislation/Policies

Though SPAM is an international problem, it is difficult to measure the effectiveness of national or federal legislation on the volume of SPAM circulated. Several sources have expressed mixed feelings about the effectiveness of the United States CAN-SPAM act as well as about the European legislation. According to an ISOC survey, 53% of the participants believe that anti-spam legislation has little impact on SPAM circulation [4].

Message Labs provided an interesting graph which shows the number (and percentage) of SPAM email received for the period 2004-2005 while major legislations came in effect. It shows that after the CAN-SPAM introduction in January 2005, the percentage of SPAM email was reduced from 63% to 52%. Spammer operations may further shift towards overseas markets for example, Russia, China and Eastern European countries where the legislation may become difficult to enforce [4].

4. User perception on security / privacy issues

Interesting results from a survey of AOL/NCSA (2006) are listed below:

(i) Home computers not having enough core protections: 81% (Recently updated anti-virus software, firewall, and/or spyware protection)
(ii) Home computers not having current virus protection: 56%
(iii) Home computers not having properly-configured firewall: 44%
(iv) Home computers not having any spyware protection software: 38%
(v) Home computer users who have faced at least one phishing attempt via e-mail in two weeks: 23%

5. Conclusion

The web is a global network of millions of interconnected computer networks linking hundreds of millions of machines used by over a billion people. It transfers data between these machines in such a way that the computers at each end of a connection need not be aware of each other's physical location, or the technical details of the many intervening data transmission systems. With the explosion of the public Internet and e-commerce, private computers, and computer networks, if not adequately secured, are increasingly vulnerable to damaging attacks. Hackers, viruses, vindictive employees and even human error all represent clear and present dangers to networks. And all computer users, from the most casual web surfers to large enterprises, could be affected by web security breaches. However, security breaches can often be easily prevented. This paper provides the users with a general overview of the most common web security breaches and the steps they and their organizations can take to protect themselves from threats and vulnerabilities.

REFERENCES

1. World Internet Users and Population Stats. (2007, March 19). Internet World Stats. Retrieved
2. Internet World Stats March usage and population statistics 20, 2007 from the WWW: http://www.internetworldstats.com/stats.htm
3. The size of the World Wide Web. (2007, February 25). Pandia Search Engine News. Retrieved from the WWW: http://www.pandia.com/sew/383-web-size.html
4. The size of the World Wide Web. (March 20, 2007). Pandia Search Engine News 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 from the WWW: http:// www.esafe.com/ home/csrt/ statistics/statistics_2005.asp
6. Statistical Data on Network Security. Antonis GALETSAS, European

Commission, March 5, 2007.

7. Phishing statistics - World Phishing, Avira GmbH 2009 from the WWW: http://www.avira.com/en/threats/section/worldphishing/top/7/index.html
8. Top 10 Computer Viruses of 2009. sategroup, September 10, 2009 from the WWW: http://www.brighthub.com/computing/smb-security/articles /44811.aspx
9. Top 10 Computer Antiviruses of 2009 from the WWW: http://anti-virus-software-review.toptenreviews.com/
10. 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
11. Three Shocking Statistics on Spyware!. (2007) PC Security News. Retrieved March 22, 2007 from the WWW: http://www.pcsecuritynews.com/ spyware_statistics.html.
12. Spyware Statistics from the WWW: http://www.clcp.us/spyware_stats.html
13. Key Internet Usage Statistics. (2006) GET-Websense. Retrieved March 23, 2007 from the WWW: http://www.3w.net/lan/internet-use-statistics.html
14. General Information Security Statistics. (2004) Security Stats. Retrieved March 25, 2007 from the WWW: http://www.securitystats.com/infosec.html