International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

General Article

A Review on Internet Threats

Meenu[†*] **and Shikha**[†]

[†]Department of Computer Science, RGGCW Bhiwani, Haryana, India

Accepted 20 June 2015, Available online 25 June 2015, **Vol.5, No.3 (June 2015)**

Abstract

Personal data has never been more vulnerable to prying eyes than it is today. As Internet users are increasing day by day, security is becoming an important issue. Internet security attacks are becoming threats for the users and their private data. There are many types of internet attacks which can harm the privacy and integrity of computer. Nowadays, different internet attack types are combined such as security exploit, commonly used by malicious hackers, and computer viruses resulting in a very complex attack that, in some cases, is beyond the general scope of anti-virus or security software. In this paper, some of the major Internet privacy issues would be explored and how to combat privacy issues which concern us the most in growing Internet market.

Keywords: *Threats, phishing ,worms , denial of service , Trojans.*

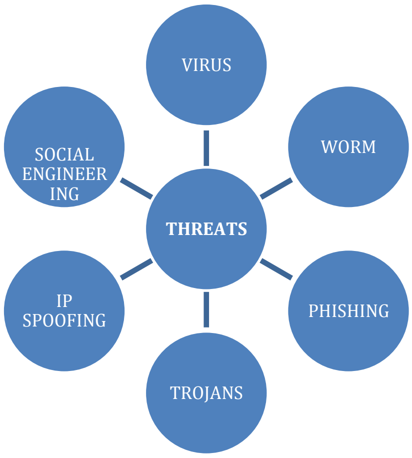
1. Introduction

Internet has witnessed an uncontrollable success over the past decade. Such successes are meant that internet is used by a number of users in their respective field according to their requirements. As a consequence of increased internet global scope, security is necessary for any internet facilitate organization. Internet security is a branch of computer security whose main aim is to protect the users from internet threats.

Internet threats are the dangerous attacks on the network, originated by the people with the special motive to steal, cause vandalism, prove themselves to be elite hackers. There are many types of internet threats which can harm the privacy and integrity of the computer. Privacy becomes the main issue for the computer users. Users should have the knowledge about the internet threats and their harms, so that they secure their private data. The following are some of the major attacks which cause threat to network, computer and individual private data.

Social Engineering

Term used among crackers and samurai (hackers who hire out for legal cracking jobs) for cracking techniques that rely on weaknesses in wetware {human beings attached to a computer) rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system's security (Castelluccio & Micheal, 2005).



Phishing

Phishing is an identity theft which forces a user to surrender private information. The number of phishing attacks is escalating and becoming more sophisticated every day and the total financial losses resulting from phishing is increasing. Phishing attacks target millions of email addresses around the world in the hope that a percentage of owners will fall victim to the trick. About 5% of fraudulent e-mail recipients do respond to e-mails or provide personal information to fake Web sites whose addresses are obtained from the emails. According to the Anti-Phishing Working Group, the number of phishing sites reached 4630 in November 2005, which is a 205% increase over November 2004. Financial Institutions, retail companies, and Internet service providers remain the frequent target (Bose, Indranil, Leung & Alvin, 2006).

*Corresponding author: **Meenu**

Worm

A worm is very similar to a virus. The key difference is that a worm attempts to propagate itself without any user‘s involvement. It typically scans other computers for vulnerabilities which it is designed to exploit. When such a machine is identified, the worm will attack that machine, copying over its files and installing itself, so that the process can continue mechanisms of attacks (J. Dubois and P. Jreije, 2006). In January, 2004 the biggest computer worm thus far- dubbed “MyDoom”- hit e-mail servers hard: 1 in 12 e-mail accounts was affected. The worm, which appeared as an innocuous error message, clogged global e-mail traffic worldwide and even forced some companies to shut down their mail servers in an attempt to stop its spread (swartz & Nikki, 2004).

Virus

Virus is a program capable of replicating with little or no user intervention and can easily destroy other programs without your permission. Viruses are no longer restricted to computers, but now infect the entire network and inform that today viruses are spread through web sites and electronic mail messages. A recent research shows that an increasing amount of malware and suspicious content is served through links from legitimate sites. Also offered are suggestions for ensuring computer security, which include not clicking on attachments from strangers, installing an extra layer of firewall protection in personal computers, and constant security scanning of systems (Sarrel & Matthew D , 2008).

The information Security Breaches survey of 1000 firms showed the number of businesses being hit by viruses or denied access to services is at an all-time high, 10% on 2002. Figures are three times those in 2000, when just 16% of UK businesses suffered attacks on their computer systems. The report found the Blaster virus responsible for a third of all infections, and over half of those in large companies (Securty-survey.gov.uk, 2004).

Trojans

Trojans take their name from the Trojan horse of Greek mythology. Computer Trojans work in the same way as worms. A game, screen saver, or cracked piece of commercial software is given to a victim (J. Dubois and P. Jreije, 2006). Computer experts are warning of an increase in targeted computer attacks worldwide. In such attacks, virus writers craft Trojan horse programs to sneak into computers and steal documents. Recently, Great Britain's central government computers were targeted by these widespread and sophisticated attacks. Central government computers have been the most popular target, but corporations and individuals are also at risk, according to a warning from the British National Infrastructure Security Coordination Center (NISCC)(Information Management Journal, 2005).

IP Spoofing

IP spoofing is a difficult problem to tackle, because it is related to the IP packet structure. IP packets can be exploited in several ways. Because attackers can hide their identity with IP spoofing, they can make several network attacks. Although there is no easy solution for the IP spoofing problem, you can apply some simple proactive and reactive methods at the nodes, and use the routers in the network to help detect a spoofed packet and trace it back to its originating source (Cisco, VOL.10).

There was a surge in IP spoofing this year. The year began with an advisory about IP spoofing, and attacks continued throughout the year. In a matter of weeks during the summer, we received more than 170 reports of IP spoofing attacks or probes, many resulting in successful break-ins. We found that several sites believed incorrectly that they were blocking such packets, and other sites had planned to block them but hadn't yet done so (CERT, 1995).

Denial-of-Service

DoS and DDoS Attacks: DoS attacks generally achieve their goal by sending large volumes of packets that occupy a significant proportion of the available bandwidth. Hence, DoS attacks are also called bandwidth attacks. The aim of a bandwidth attack is to consume critical resources in a network service. Possible target resources may include CPU capacity in a server, stack space in network protocol software, or Internet link capacity. By exhausting these critical resources, the attacker can prevent legitimate users from accessing the service (Tao, Leckie & Ramamohanarao, 2007).

2. Steps to set up privacy on internet

A. Never create easy passwords

Don't get lazy and use only one or two passwords at multiple sites just because that's easier to remember. Stay away from real words, use a combination of letters and numbers, and keep passwords at least six characters long. Don't use birth dates, names of children or pets, or simple sequences like XYZ123. Keep a record of your IDs and passwords, but not on your PC. Don't store your password to avoid entering it the next time you log on. And periodically change your passwords.

B. Never maintain a browser cache.

Browsers speed up online navigation by storing graphical and other elements of pages you visit in a cache on your hard drive. Of course, anyone with access to your PC can check where you've been and what you've seen. Regular purging is wise.

To clean out your cache in Internet Explorer 5, select Tools, Internet Options. With the General tab selected, click Delete Files in the 'Temporary Internet files' section. In Netscape 4 or higher, select Edit, Preferences. In the Category tree, double-click Advanced and then select Cache. In the Cache section, click Clear Memory Cache and OK. Then click the Clear Disk Cache button and, finally, click OK.

C. Never enable file sharing

Your PC need not be on a network to be set to allow file and printer sharing. And if it is, you've left an open door for any knowledgeable hacker to enter through in order to snoop around and perhaps do some mischief. Lock up your PC as follows: In Windows 9x, select Start, Control Panel, double-click the Network icon, and choose the Configuration tab. Click the File and Print Sharing button, and uncheck both boxes in the dialog box, if they aren't already unchecked.

D. Never preserve a history

The browser keeps a history log that identifies each Web address you visit. If you're on a public machine, you might want to purge your history periodically. To clean out your history log in IE 5, select Tools, Internet Options. In the General tab, click the Clear History button and follow the prompt. In Netscape 4 or higher, select Edit, Preferences, choose Navigator in the Category window, and click Clear History.

E. Never accept cookies from strangers

Useful cookies let Web sites recognize you on a return visit. Less-wholesome cookies follow your surfing habits and report on what you view. IE 4 and higher store cookies in the \Windows\Cookies folder. You can delete its contents by highlighting one file, then pressing Ctrl-A followed by Delete. Netscape Navigator versions 4 and higher store cookies in a file called cookies.txt. To find it, select Start, Find (or Search in Windows 2000/Me), (For) Files or Folders, and search for cookies.txt; then delete this file and its subfolders, if any.

You'll probably want to allow some cookies, so consider a cookie-management shareware program such as CookiePal or CookieCrusher.

F. Never talk to strangers without protection

You may think you're safe when you communicate with people you know, but spammers and Web sites use harvesting software to grab e-mail addresses even when you think you haven't supplied yours.

The best way to talk safely: Don't run instant-messaging software in the background. Turn it off when you aren't using it, and configure your software to hide your presence. In AOL Instant Messenger, for example, select My Aim, Edit Options, Edit Preferences, and select the Privacy tab.

Surf anonymously

If you wish to mask your ID when you surf, use one of the many anonym zing services available on the Web. Most of these Web-based services work the same: You log on to their site and go wherever you want on the Web from there. The services hide your actual IP address and substitute their own.

A. Never surf without a firewall

If you have a broadband connection such as DSL or cable, you're connected to the Internet whenever your computer's turned on. And that makes you a target for hackers in search of computers to play around in. You can stop their intrusion with a firewall--an anti-intrusion program that acts as your PC's Internet gatekeeper.

B. Never reveal information needlessly

The more personal information you supply, the less privacy you keep. Accordingly, give out the least amount of information necessary to complete any registration. Don't fill in any optional lines on profiles. Don't elect to store credit card numbers for future convenience. If a site offers to save your password for future visits, just say no.

C. Always Encrypt e-mail

Think your e-mail is private? Think again. Administrators, hackers, or anyone intent on gaining access to it can read your e-mail. For confidential correspondence, your best line of defense is encryption. Spies use it for a reason: No one but you and the intended recipient can decipher it. There are plenty of easy-to-use encryption programs available (Grimes, 2001).

3. Main cause of threats to privacy on internet

Earning a quick buck continues to be the primary driver for the spread of malicious viruses and Trojans on the Internet and will be the trend in the coming years, according to a Symantec executive. However, Ibrahim said the attacks are now more targeted. Instead of taking down whole websites, some Trojans capture user accounts particularly credit card numbers that the malware makers can use for their own purposes (Alexander Villafania , 2008).

Conclusion

Internet privacy is now becoming a major problem because the use of internet is increasing as well as the ways of attacking the networks and computers had increased with an enormous rate. The main reason behind compromising privacy is money as everyone who initiates attack on privacy wants to make some quick money. Motivation of steal, cause vandalism and proving them elite hackers are also some of the reasons behind these attacks. These attacks are dangerous for the network as well as computer which indirectly harm the individual. Identity theft is fairly common and that's why malware makers are doing targeted attacks and doing it stealthily**.** People have to be more careful when using their computers and they must use right kind of security applications**.**

References

Bose, Indranil , Leung and Alvin(2006), Phishing is here: Are we ready?, international Multi Conference International Multi Conference of Engineers & Computer Scientists 2006; 2006, p990-990.

Castelluccio, Michael (2002), Social Engineering 101, Strategic Finance; Dec2002, Vol. 84 Issue 6, p57-58.

CERT* Coordination Center 1995 Annual Report (Summary) Grimes, Brad; McCracken, Harry, Privacy Matters, PC World, May2001, Vol. 19 Issue 5, p94, 8p, 3 color. CISCO, Internet Protocol Journal, Vol10, No.4

Information security breaches survey, 2004. survey.gov.uk

J. Dubois, and P. Jreije(2006),Transaction On Engineering, Computing and Technology Volume 14 August 2006

Sarrel, Matthew D.(2008), The Rise of Blended Threats,PC Magazine; Sep2008, Vol. 27 Issue 10, p92-92.

Swartz, Nikki(2004) ,Homeland Security Offers Alerts Warning of E-mail Viruses., Information Management Journal, Mar/Apr2004, Vol. 38 Issue 2, p17-17, 3/4p.

Peng T, Leckie, Christopher1, Survey of Network Based Defense Mechanisms Countering the DoS and DDoS Problems, Kotagiri1 B (2007).

Villafania A. (2008), Money is main cause of Internet security threats—Symantec, First Posted Retrieved from: http:// newsinfo.inquirer.net/ breakingnews/ infotech/ view/ 20080925-162793/ Money- is-main-cause-of-Internet-security-threats—Symantec