International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Ethical Hacking: Numerous Approaches to Spyware Detection and Prevention

Vijaya Bhaskar Reddy Muvva

Department of Information Technology, University of Technology and Applied Sciences-Shinas, Shinas, Oman
E-mail: *bhaskarj921[at]gmail.com*

Abstract: ***Network security is one of the most important parts of computer networking, irrespective ofif the network is limited to a home environment with a one connection to the internet or multiple connections with thousands of users. The connected systems in the network are exposed to various malicious programs such as Viruses, Worms, Trojan horses, Spyware, Adware and Zero-day attacks. Among these a new malicious program gained propulsion known as Spyware. This paper discusses various approaches used by hacker in installing spyware and throws light on how the users can prevent remote attacks and data monitoring by spyware attacks. This paper also exhibits the implementation of the same in Personnel computer.***

Keywords: Spyware; Adware; Detection; Prevention; Ethical Hacking; Malicious code

1. Introduction

Ethical hacking refers to identifying the vulnerabilities of computer and information systems by duplicating actions of malicious hackers. It deals with different types of attacks such as scanning networks, system hacking, malware threats, sniffing, social engineering, denial of services and session hijacking. Among these types of attacks, May users are not aware of spyware attacks. User may be cautious of virus attacks where as spyware attacks may be done without the knowledge of the user. So, there is a need to be cognizant to these kinds of attacks. This paper presents rudimentary things about the function of spyware and its prevention and removal from the systems to safeguard important data confidentiality and integrity. Spyware is defined as: "Software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumers consent, or that influences some control over a computer without the consumer's knowledge [1]. The spyware attack has Positive and negative type of consequences to users [2]. Spyware threat has emerged as most complex and sophisticated threat over the past few years. The problem caused by spyware is now even getting more severe [3]. Since users are usually unaware such programs exist on their machine, over time as performance continually degrades users may mistakenly believe their machines are outdated and in need of replacement. A spyware application is typically difficult to remove once it has been installed on a computer system and it can seriously degrade system performance and compromise the privacy of the user [4].

The objective of this paper is:

- How the hacker install spyware software in the user computer and how it works.
- How to detect spyware in computer.
- How to prevent spyware attacks in computer.
- Real time implementation of spyware attack using SpyAgent software.

2. How the hacker installins spyware software in the user computer and how it works

Spyware does not spread in the same way like viruses. Virus attacked systems generally do not permit to transmit or copy the software to other computers. Most spyware is installed without knowledge of user or by using other tactics which are deceptive in nature.

The following approaches are some of the ways by which spyware can be installed:

- The most common method of installation is to attach or bundle the software with a useful application that user wishes to install.
- Another way is because of vulnerabilities in the web browser itself. For example, Internet explorer also serves as a point of attachment for spyware in the form of Browser Helper Objects, which modify the behavior to add toolbars or to redirect traffic.
- In certain cases with the visit of some websites spyware may activate the installation without any notice to the user.
- Keyloggers is software that works as spyware. It is used basically for commercial or private applications which allow keyboard strokes to be captured and sometimes makes it possibleto collect screen captures from the computers.

The above points illustrate different types of behaviors observed in the most of the spyware programs. Research studies have categorized a number of spyware programs into different groups as shown in below figure.

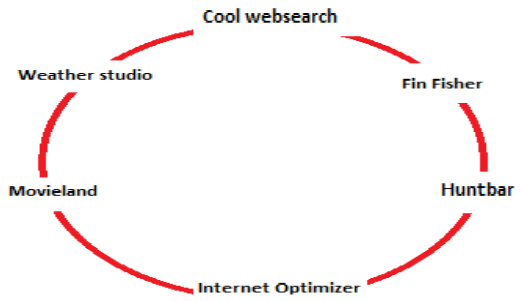

Figure 1: Spyware programs into different groups.

When multiple computers are attached by spyware two methods are used to uniquely identify a computer. The first method is to generate a globally unique identifier (GUID) and second is to install a cookie on the users' machine. GUID contain information unique to the machines hardware, such as serial numbers. Cookies are files that contain data which programs use. Spyware would typically create a cookie that stores computer specifications, installation version, etc. This unique information provides the key for the entry in the users databases [5].

3. How to detect spyware in computer

There are many spyware detection methods, some of the popular and effective detection methods are discussed below.

a) Signature-Based Detection

Signature based methods maintain a database consisting of unique strings or specific features called signatures. For detection it extracts specific features binaries and compares it with existing database. This method is not good enough to detect new and previously unseen spyware executables [6].

b) Data mining based detection

This application allows us to detect whether a particular executable is spyware or not prior to their installation [7].

c) Identifying suspicious behavior

- Slow network speed.
- Sluggishness in system like frequent computer crashes.
- Receiving suspicious text messages.
- Ever present pop-up advertisements.
- Changes inuser PC settings and inability to change these settings
- Changes in web browsers like return of deleted tool bars.

4. Methods of Removal / Prevention

There are many spyware prevention and removal methods, when practiced user can make sure that, the system is free from entry of such spyware.

- One of the simple method is to read the End User License Agreement (EULA) of all software downloaded off the internet, or software downloaded free of charge or payable.
- Another method is to refrain from browsing certain types of sites which are prone to containing spyware.
- Another method of protection is to install a spyware removal tool. These software's scan users hard drive for known spyware programs, and remove them from the systems.
- According to PC security news, the top rated programs are: Webroot Spy Sweeper, PC Tools Spyware Doctor, Computer Associates Pest Patrol, and Panicware Anti-spyware [8].

Apart from these there is some common prevention methods are listed below:

1) Installing real-time anti-spyware protection.
2) Cautiousness while web surfing.
3) Lookout for pop-ups.
4) Checking and keeping operating system updates.
5) Apply patches to software installed on your computer.
6) Checking browser settings frequently.
7) Antivirus-Total internet security.
8) Enabling firewall.

5. Real time Implmentation of spyware program attack using SpyAgent software

In this paper the presenter uses SpyAgent software to implement spyware program.
The following steps are executed during the installation and implementation of SpyAgent.

Figure 2: Downloading PC monitoring software

Figure 3: Installing SpyAgent

Figure 4: Selecting what configuration options you want to spy

Figure 5: Stat Monitoring

Figure 6: Monitoring started

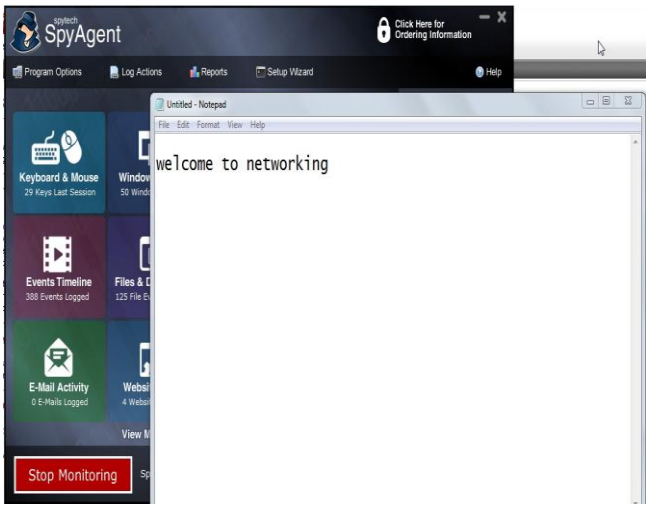

Figure 7: Open notepad and type some text

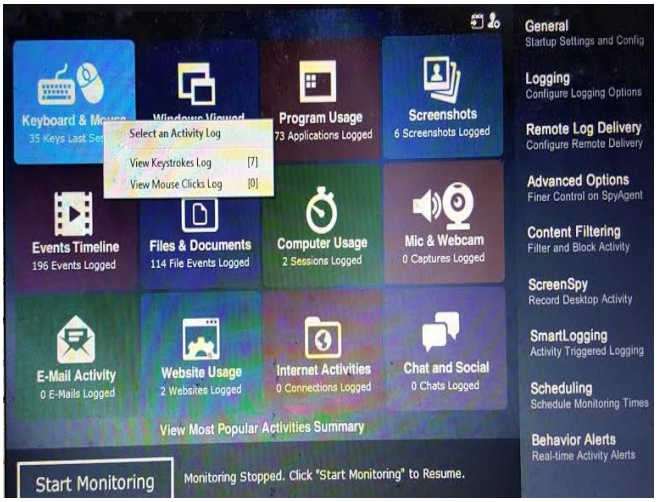

Figure 8: Stop monitoring and click on view Keystroke Log event

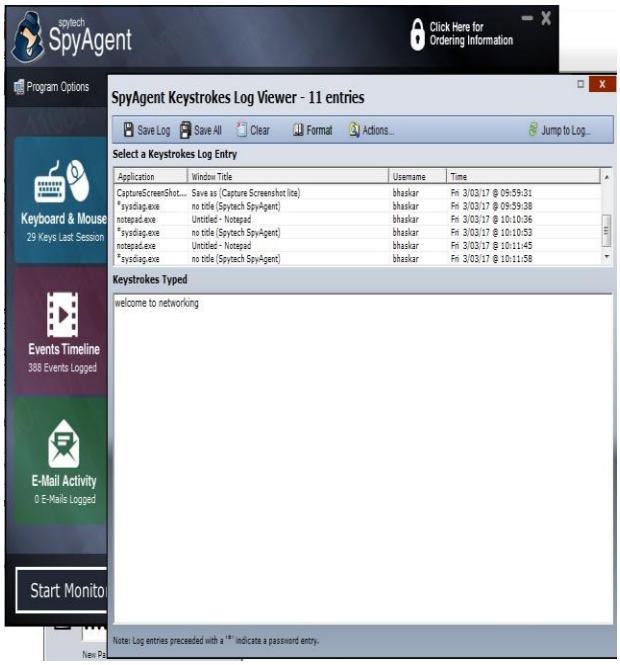

Figure 9: Shows the Keyboard event what the user typed

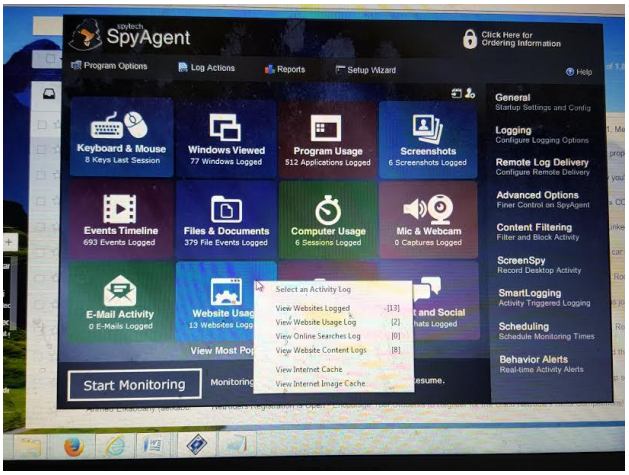

Figure 10: Shows Website Usage Event

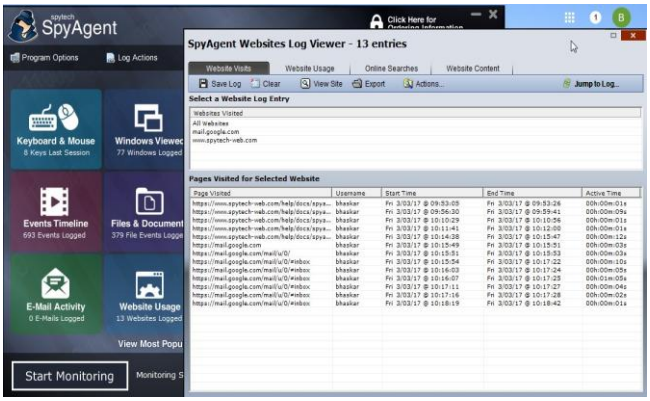

Figure 11: Shows the websites visited by the user

6. Reports

The following are the reports generated by SpyAgent.

Figure 12: Report for user Keystroke activities

Figure 13: Report generated for user websites visited

7. Conclusion

In Ethical Hacking stealing the data though ethically appreciated, but it should not be misused. In case of misuses the attacker may face legal consequences as it breaches the integrity, confidentiality and data protection of the users. As such spyware attacks indulge in unlawful and illegal ways the users must be apprehensive about such attacks. Thispaper tries tocreate such awareness among users.

References

[1] Federal Trade Commision Staff Report, http://www.ftc.gov
[2] M. Warkentin, X. Luo, and G.F. Templetion, “A Framework for Spyware Assesment,” Communications of the ACM, vol. 48, No.8, pp. 79-84, Auguest2005.
[3] M. Saqib and M. Papadaki, “Comparing Anti-Spyware Products-A Different Approach”, Advances in Networks, computing and communications 6, IEEE, 2011, pp 294-301.
[4] N. Lavesson, M. Boldt, P. Davidson and A. Jacobsson, “Learning to detect spyware using end user Licence Agreements”, Spring-Verlag, London, 2009.
[5] Computer Spyware, http://imps.mcmaster.ca/courses/SE-4C03-07/wiki/mcclafpj/ComputerSpyware.html
[6] G. Mththew and E. Zadok, “Data Mining methods for Detection of New Malicious Executables”, IEEE, 2001.
[7] K. Pandey, M. Naik, J. Qamar and M. Patil, “Spyware Detection using Data Mining”, International Journal of Engineering and Techniques, vol 1, Issue 2,pp.5-8, March 2015.