International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT206637

Role of Spy-ware Analysis in the Arena of Cybersecurity

Ankita Guha[1], Adwin Manhar[2]
[1]Research Scholar, Amity University Chhattisgarh, Raipur, Chhattisgarh, India
[2]Assistant Professor, Amity University Chhattisgarh, Raipur, Chhattisgarh, India

Article Info
Volume 6, Issue 6
Page Number: 268-273
Publication Issue :
November-December-2020
Article History
Accepted : 01 Dec 2020
Published : 05 Dec 2020

ABSTRACT

This research aims to investigate the seriousness of the Cybersecurity for spyware including various types of spyware and the ways to enhance the security for reducing the spyware threats.

Keywords: Cybersecurity, Spyware, Malicious Software, Spyware Threats, Zonealarm, Secure Sockets Layer, Transport Layer Security, Pretty Good Privacy

I. INTRODUCTION

Spyware is an unwanted software that infiltrates our computing device, stealing internet usage data and other sensitive information. The first usage of the term Spyware occurred on October 16, 1995 in a Usenet post that poked fun at Microsoft's business model. Spyware at first denoted software meant for espionage purposes. During early 2000, Zone Labs founder Gregor Freund have used the term of ZoneAlarm Personal Firewall in a press release, but later in 2000, a parent using ZoneAlarm was alerted to the fact that "Reader Rabbit," one of the educational software was marketed to children by the company named Mattel toy secretively was sending back data to Mattel. Since then, "Spyware" has taken on its present sense. Spyware is used for many purposes. Usually it aims to track and sell our internet usage data, capture your credit card or bank account information, or steal our personal identity. Basically it monitors the internet activity , track the login and password information, and spying on sensitive information. Some types of Spyware can install additional software and can change the settings of our devices, so it is important to use secure passwords and keep our devices updated. There are four main types of spyware in which each uses unique techniques for tracking purposes. They are:

- ✓ Adware: In this type of spyware tracks the browser history and downloads, with the intent of predicting in which products or services you're interested in and it will try to display the same or related products to entice us to click on it or to make a purchase. And hence can slow down our system.
- ✓ Trojan: It is a kind of malicious software which disguises itself as a legitimate software. It may appear to be a Java or Flash Player update upon download, controlled by the third parties.

- ✓ Tracking cookies: It will track the users browser history, searches or any downloads for their own marketing purposes.
- ✓ System monitors: It can capture everything we do in our daily life through our system. It can also record all keystrokes, emails, websites we have visited, and programs run.

Sources for Spyware:

Spyware does not always spread in the form of a computer viruses or worm. Generally an infected system does not attempt to transmit the infections or copy the software to other computers. Instead it gets installed by itself on the system or by exploiting software vulnerabilities. It may also try to engage the users by bundling itself with its desirable software. Recently, spyware has come to include "rogue anti-spyware"programs, which masquerade as security software while actually doing damage. For example a Trojan horse, by definition, smuggles in something dangerous in guise of something desirable. The spyware distributor displays the program as in a useful purpose , for instance as a "Web accelerator" or as a helpful software agent. Therefore many users download and install the software knowingly or unknowingly which can further causes harm to the system and the user. Spyware can also be included through shareware, downloadable software as well as through music CDs. The user downloads a program (for instance, a music program or a file-trading utility) and installs it by which the additional spyware also gets installed . Although the software installed may do no harm, the bundled spyware does. In some cases, spyware authors have paid shareware authors to bundle spyware with their software, as with the Gator spyware which is now marketed by Claria. While the third way distributing spyware involves tricking users by manipulating security features designed for prevention of the unwanted installations. The Internet Explorer Web browser, by design, prevents different websites from initiating or an unwanted download. Instead a User action such as clicking on a link must normally trigger a download. Anyways the link can be proved deceptive:for instance, a pop-up ad may appear like a standard Windows dialog box , and it may contain the message such as "Would you like to optimize your Internet access?" including the Yes or No buttons and no matter which button the user presses , the download starts automatically forwarding the spyware on the user's system.

Some spyware authors infect a system by attacking security holes in the Web browser or in other software, when the user navigates to any web page which is controlled by the spyware author, the page contains code which attacks the browser and forces the download and install of the spyware. The spyware author will also have some extensive knowledge of commercially available anti-virus and firewall software, this is also known as "drive by download" . In few cases a worm or virus has also delivered a spyware. For instance, some attackers used the W32. Spybot. Worm worm to install spyware that popped up pornographic ads on the victim's system screen . They can profit even by such illegal behaviour.

Spyware in business

Recently, in the field of security, much attention has been paid to extortion programs. Nevertheless, another threat, by no means of such a high level, which gives its creators much more than ransomware, is the compromise of corporate e-mail. Today, this is currently the most profitable way to get a lot of money from a business. This is a deceptively light attack vector that uses social engineering to initiate theft. In the simplest version, the campaign to compromise business email includes the delivery of email to employees of financial departments (sometimes using fake data from other employees), who can send funds via bank transfer. Hackers usually carry out some researches in hierarchy of the

companies and its employees, for example, using profiles in social networks, and build management vertical. This may be a letter from the CEO or another top manager asking him to transfer a non-cash payment to a prospective business partner or supplier. The message should motivate the recipient to send money, which as a result will usually end up in foreign or regional bank accounts owned by cybercriminals. Since messages aimed to compromise the business email do not contain malicious or suspicious links, they can usually avoid almost all the most sophisticated threat defenses.

Despite the fact that Internet users are generally aware of spyware as a potential security threat, they do not appear to be greatly motivated to pursue or pay for commercial solutions. AOL has been featuring the free download of anti-spyware software to users at their main Web page log-in, and it appears the current market for spyware protection at the commercial level is as a value-added feature for differentiation purposes of an existing commercial Internet service. User impact: AOL users are typically seen as the “every man” of the Internet; since the ISP leads the market, it tends to the highly visible face of the market for commercial consumer Internet access services. As such, they represent the user population at the “street level. ” Prior studies of AOL users asked the customers to rate themselves on their perceived level of Internet experience, and it was found that 35% of participants classified themselves as “novices,” while 23% classified themselves as “high-end novices” [1]. Hence, basic users of Internet services demonstrate that the Internet “street” knows that spyware is a problem and would like to protect themselves but, due either to lack of perceived technical skills or perhaps lack of recognition of the severity of the computer security threat that spyware represents, they are not aggressive in their plans to take protective steps, particularly if such steps cost money. It seems as if the new AOL spyware protection service is prized as a value-added service enhancement, but not as a standalone product that can command an appreciable separate revenue stream. To the extent that service offerings such as the AOL spyware protection enhancement are valued, they seem best situated as an enhancement of current services. The greatest value to a company like AOL in offering add-on services of this nature is probably in maintaining competitive advantage, as opposed to opening new revenue sources through subscription sales. Thus, not only should AOL be offering free downloads of anti-spyware software to its users, but should continue to integrate the feature into the user interface, while at the same time work to emphasize the seriousness of actively pursuing protection against the spyware threat. Less savvy Internet users understand the threat of spyware but must be educated about the need to aggressively protect themselves against this threat. Companies providing anti-spyware software should focus on helping street-level users understand the urgency and immediacy of taking action against unwanted spyware activities and guide them in the steps to take and tools to use in protecting themselves.

Countermeasures for Spyware in Cybersecurity:

A new spyware detection technique based on reinforcement learning is proposed. It is a proactive approach for the malware detection, and allows detecting all types of spyware. The technique is based on mechanisms machine learning and is able to detect new unknown spyware. The suggested method of the spyware identification uses software behavior analysis in the computer systems. The main steps of the proposed approach are presented below: 1. Spyware sample construction. 2. Usage of the reinforcement learning algorithm, the rewards evaluation. 3. Computer systems monitoring concerning the software behavior. 4. Features selection that may indicate the presence of spyware in the computer systems. 5. Evaluation of the reward for research object. 6. Comparison of the obtained

rewards with the rewards values of the known spyware. For maximum security and privacy, make sure to adopt adequate countermeasures against it which also includes:

Network layer security: TCP/IP protocols may be secured with cryptographic methods and security protocols. These protocols include Secure Sockets Layer (SSL), succeeded by Transport Layer Security (TLS) for web traffic, Pretty Good Privacy (PGP) for email, and IPsec for the network layer security.

- ✓ Internet Protocol Security (IPsec):IPsec is designed to protect TCP/IP communication in a secure manner.
- ✓ It is a set of security extensions developed by the Internet Task Force (IETF). It provides security and authentication at the IP layer by transforming data using encryption. Two main types of transformation that form the basis of IPsec: the Authentication Header(AH) and ESP. These two protocols provide data integrity, data origin authentication, and anti-replay service. These protocols can be used alone or in combination to provide the desired set of security services for the Internet Protocol (IP) layer.
- ✓ Multi-factor authentication: MFA is a method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are). Internet resources, such as websites and email, may be secured using multi-factor authentication.
- ✓ Security token:Some online sites offer customers the ability to use a six-digit code which randomly changes every 30–60 seconds on a security token. The keys on the security token have built in mathematical computations and manipulate numbers based on the current time built into the device. This means that every thirty seconds there is only a certain array of numbers possible which would be correct to validate access to the online account. The website that the user is logging into would be made aware of that device's serial number and would know the computation and correct time built into the device to verify that the number given is indeed one of the handful of six-digit numbers that works in that given 30-60 second cycle. After 30–60 seconds the device will present a new random six-digit number which can log into the website
- ✓ Electronic mail security : It includes, Pretty Good Privacy (PGP) which provides confidentiality by encrypting messages to be transmitted or data files to be stored using an encryption algorithm such as Triple DES or CAST-128. Email messages can be protected by using cryptography in various ways, such as the following:
  1. Signing an email message to ensure its integrity and confirm the identity of its sender.
  2. Encrypting the body of an email message to ensure its confidentiality.
  3. Encrypting the communications between mail servers to protect the confidentiality of both message body and message header.

Message Authentication Code which is a cryptography method that uses a secret key to digitally sign a message. This method outputs a MAC value that can be decrypted by the receiver, using the same secret key used by the sender. The Message Authentication Code protects both a message's data integrity as well as its authenticity.

Firewalls controls access between networks. It generally consists of gateways and filters which vary

from one firewall to another. Firewalls also screen network traffic and are able to block traffic that is dangerous. Firewalls act as the intermediate server between SMTP and Hypertext Transfer Protocol (HTTP) connections. The roles of firewall in web security is to impose restrictions on incoming and outgoing Network Packets to and from private networks. Incoming or outgoing traffic must pass through the firewall; only authorized traffic is allowed to pass through it. Firewalls create checkpoints between an internal private network and the public Internet, also known as choke points (borrowed from the identical military term of a combat limiting geographical feature). Firewalls can create choke points based on IP source and TCP port number. They can also serve as the platform for IPsec. Using tunnel mode capability, firewall can be used to implement VPNs. Firewalls can also limit network exposure by hiding the internal network system and information from the public Internet. Now Internet security products include:

- ✓ Antivirus : Many types of antivirus and anti-spyware software can detect the possible presence of malware by looking for patterns in the files or memory of your computer.
- ✓ It was mainly shareware in the early years of the Internet, but now there are several free security applications available.
- ✓ Password managers: A password manager is a software application that helps a user store and organize passwords. Password managers usually store passwords encrypted, requiring the user to create a master password; a single, ideally very strong password which grants the user access to their entire password database from top to bottom.
- ✓ Security suites: So called security suites were first offered for sale in 2003 (McAfee) and contain a suite of firewalls, anti-virus, anti-spyware and more. They also offer theft protection, portable storage device safety check, private Internet browsing, cloud anti-spam, a file shredder or make security-related decisions (answering pop up windows) and several were free of charge.

II. CONCLUSION

Though there has been much debate on the subject of security enhancement for Spyware detection in systems. The suggested methods of spyware detection uses a software behaviour analysis in computer systems. The suggested method involves various sources for security which protects the spyware from further damaging or for collecting information's and harmful activities which can harm the system or the user. Therefore the Cybersecurity plays an important role in Spyware detection and providing the user with a malware ,virus and other harmful activities free system usage.

III. REFERENCES

[1]. M Mann, A Molnar, I Warren - The conversation, 2017 - dro. deakin. edu. au

[2]. D Reddy, V Rao - 2016 - aisel. aisnet. org

[3]. https://en. wikipedia. org/wiki/Spyware#References

[4]. Norton. What is spyware? And how to remove it. Available online: https://us. norton. com/internetsecurity-how-to-catch-spyware-before-it-snags-you. html (accessed on March 20, 2020).

[5]. Eset. Spyware. Available online: https://help. eset. com/glossary/en-US/spyware. html (accessed on March 20, 2020).

[6]. Avast. Spyware: Detection, Prevention, and Removal. Available online: https://www. avast. com/c-spyware (accessed on March 20, 2020)

[7]. Drozd, O. , Kharchenko, V. , Rucinski, A. , Kochanski, T. , Garbos, R. , Maevsky, D. Development of Models in Resilient Computing, Proc. of 10th IEEE International Conference on Dependable Systems, Services and Technologies, pp. 2-7 (2019).

[8]. EU Opara, AD Upadhyay… - Journal of Forensic and, 2017 - scienceinquest. com
[9]. KMEN Mallikarajunan, SR Preethi… - … on Trends in, 2019 - ieeexplore. ieee. org
[10]. RD Anderson - Tort Trial & Insurance Practice Law Journal, 2014 - JSTOR
[11]. V Lakhno, D Kasatkin, V Kozlovskyi… - International Journal of, 2019 - academia. edu
[12]. J Yin, MJ Tang, J Cao, H Wang - Knowledge-Based Systems, 2020 - Elsevier
[13]. https://us. norton. com/internetsecurity-how-to-catch-spyware-before-it-snags-you. html
[14]. RN Dreyer, GB Grindrod - US Patent 7,802,301, 2010 - Google Patents
[15]. T Stafford - ACM SIGMIS Database: the DATABASE for Advances, 2017 - dl. acm. org

Cite this article as :

Ankita Guha, Advin Manhar, "Role of Spy-ware Analysis in the Arena of Cybersecurity", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 6, pp. 268-273, November-December 2020.
Available at
doi : https://doi.org/10.32628/CSEIT206637
Journal URL : http://ijsrcseit.com/CSEIT206637