INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

COMMON TYPES OF MALICIOUS ATTACKS FOR WEB USERS

DEEPTI V. PATANGE[1], DR. P. K. BUTEY[2]

1. Department of Computer Science, Arts, Science & Commerce College, Chikhaldara, Dist. Amravati.
2. H.O.D. Department of Computer Sci, Kamla Nehru College, Nagpur

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract: In my previous research paper we use a clustering based model to anticipate crime trends. The data mining techniques are used to analyze the web data. Cyber-crime and internet security have become one of the major concerns in the modern age. There had been an enormous increase in the cyber-crime in the recent past all over the world. With this rapid growth in cyber-attacks one of the main enrolment was malicious attacks on web. By these attacks no one has been saved. The researchers all over the world are continuously pursuing the ways and methods to curb and try to reduce the internet crime. In this paper we study the common types of malicious attacks and their behavior/effects on web users.

Keywords: Web Users, Common Malicious Attacks, Clustering, Behavior/ Effects, Cyber Crime.

Corresponding Author: MS. DEEPTI V. PATANGE

Access Online On:

www.ijpret.com

How to Cite This Article:

Deepti V. Patange, IJPRET, 2016; Volume 4 (9): 740-746

PAPER-QR CODE

INTRODUCTION

'Malware' is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransom ware, spyware, adware, scare ware and other malicious programs [1]. In computer and computer **networks** an **attack** is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset [2].

Internet crime is a strong branch of cybercrime. Identity theft, Internet scams and cyber stalking are the primary types of Internet crime. Because Internet crimes usually engage people from various geographic areas, finding and penalizing guilty participants is complicated. Some of the very common internet crimes types are as listed below.

- **Cyberbullying And Harassment**
- **Hate Crimes, Racism, Hate Websites**
- **Internet Bomb Threats**
- **Password Trafficking**
- **Identity Theft And Fraud**
- **Email Phishing**
- **Domain Name Hijacking**

I. RELATED WORK

A. Cyber Attacks

Users can be silently infected just by visiting a web site with attacks known as drive-by downloads or social engineering attacks where misleading applications can attempt to trick users into installing fake antivirus solutions or fake video players.

Lin and Zarri [3][4] presented a method for information retrieval and append based on event ontology closer the goal of semantic web.

B. Focus

The focus of this research paper is on the effect of these attacks on web users and tries to find the reasons for performing such things by hackers.

III. METHODOLOGY

In this section we will discuss about the methodology for the research.

A. Data Collection

B. Preprocessing

C. Clustering

VI. OBJECTIVES OF THE RESEARCH

1. To study the effects/behavior of malicious attacks on web for crime relations.
2. Analytical study of Clustering for Pattern Discovery, to find crime patterns of malicious attacks on web.

V. RESEARCH METHODOLOGY

The proposed project was implemented in these stages online banking system.

A. Procuring Data Set

The dataset of Cyber Crime Attacks for the current research work was downloaded from the website www. NSL. cs.ulb .ca/ nsl/ kdd.

B. Cleaning Data Set

By doing cleaning data set, 13 attributes which were reduced to only 4 attributes and 50000 instances or records became the final cleaned dataset for the data mining procedures.

C. Processing Data Set

The data pre-processing and data mining was performed using the world famous Weka Data Mining tool which is open source software under the GNU General public license.

VI. PREFORMING ANALYSIS ON DATA SET

There are two methods used in the current study for generating results as below

K-Means Algorithm

The K-means [5] algorithm is an evolutionary algorithm observations into K groups, where K is provided as an input parameter. It then assigns each observation to clusters based upon the observation proximity to the mean of the cluster. The cluster's mean is then recomputed and the process begins again. Convergence may be defined differently depending upon the implementation [6].

The k-means cluster is simplest unsupervised and easiest way of clustering [7].

VII. RESULTS AND ANALYSIS

The dataset was preprocessed using Weka tool and statistical output was produced with respect to Minimum, Maximum value, Mean and the Standard Deviation.

The frequency of the attacks based on the network protocol was generated using visualization method in the Weka tool. The type of attacks was represented using different colors in fig 1.

The most common types of the malicious attacks that are sent by the attackers were depicted in these results and

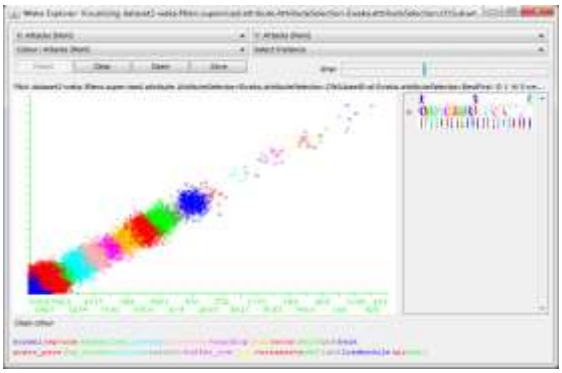

Fig.1

these common attacks on the web are explained as below.

NEPTUNE: A SYN Flood is a denial of service attack to which every TCP/IP implementation is vulnerable. Each half-open TCP connection made to a machine causes the 'tcpd' server to add a record to stores information and all pending connections is of finite size. The attackers system can simply continue sending IP-spoofed packets requesting new connections faster than the victim system which can cases, the system may exhaust memory, crash, or be rendered otherwise inoperative [8].

WAREZCLIENT: Warezclient attack can be launched by any legal user during an FTP connection after warezmaster attack has been executed and users download the illegal “warez” software that was posted earlier through a successful warezmaster attack. But these downloading files from hidden directories on the FTP server [9].

WAREZMASTER: Warezmaster exploits a system bug associated with a file transfer protocol (FTP) server. Normally, guest users are never allowed write permissions on an FTP server. Hence they can never upload files on the server. The attacker then creates a hidden directory and uploads “warez” (copies of illegal software) onto the server [10].

IPSWEEP: An Ipsweep attack is a surveillance sweep to determine which hosts are listening on a network. This information is useful to an attacker in staging attacks and searching for vulnerable machines.

TEARDROP: Teardrop is a program that sends IP fragments to a machine connected to the Internet or a network. Teardrop exploits an overlapping IP fragment bug [11] present in Windows machines. This attack has not been shown to cause any significant damage to systems, and a simple reboot is the preferred remedy and if there is unsaved data in open applications then data was lost [12][13].

NMAP: Nmap is a general-purpose tool for performing network scans. Nmap supports many different types of port scans options include SYN, FIN and ACK scanning with both TCP and UDP, as well as ICMP (Ping) scanning [14]. SATAURN: system crackers, potential intruders, or simply random people on the Internet could run the program against hosts that they have no authorization to do so against [15].

SMURF: In the "smurf" attack, attackers use ICMP echo request packets directed to IP broadcast addresses from remote locations to create a denial-of-service attack. There are three parties in these attacks: the attacker, the intermediary, and the victim [16]. The smurf attack is effective because the attacker is able to use broadcast addresses to amplify. In smurf attack, the attacker sends a stream of ICMP 'ECHO' requests to the broadcast address of many subnets, resulting in a large, continuous stream of 'ECHO' replies that flood the victim.

POD: Ping of Death (PoD) is a type of Denial of Service (DoS) attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command [17].

BACK: In this denial of service attack against the Apache web server, an attacker submits requests with URL's containing many front slashes. As the server tries to process these requests it will slow down and becomes unable to process other requests [18].

FTP_WRITE: The Ftp-write attack is a Remote to Local User attack that takes advantage of a common anonymous ftp mis-configuration. The anonymous ftp root directory and its subdirectories should not be owned by the ftp account or be in the same group as the ftp account [19].

BUFFER_OVERFLOW: The most common is the buffer overflow attack. Buffer overflows occur when a program copies too much data into a static buffer without checking to make sure that the data will fit. By carefully manipulating the data that overflows onto the stack, an attacker can cause arbitrary commands to be executed by the operating system [20].

IMAP: The IMAP attack exploits a buffer overflow in the IMAP server of Redhat Linux 4.2 that allows remote attackers to execute arbitrary instructions with root privileges [21].

PHF: The Phf attack abuses a badly written CGI script to execute commands with the privilege level of the http server function escape_shell_cmd() to prevent exploitation of shell-based library calls may be vulnerable to attack. [22].

LAND: The Land attack is a denial of service attack that is effective against some older TCP/IP implementations. The Land attack occurs when an attacker sends a spoofed SYN packet in which the source address is the same as the destination address [23].

PERL: The Perl attack is a User to Root attack that exploits a bug in some Perl implementations. [24].

LOADMODULE: The Loadmodule attack is a User to Root attack against SunOS 4.1 systems that use the xnews window system to load two dynamically loadable kernel drivers into the currently running system and to create special devices in the /dev directory to use those modules.

VIII. CONCLUSION

Always we have attempted to visit a known malicious web site, domain or IP address. Visiting this web site could potentially put you at risk to becoming infected. Users can be silently infected just by visiting a web site with attacks known as drive-by downloads or social engineering attacks where misleading applications can attempt to trick users into installing fake antivirus solutions or fake video players. An effective web crime detection system should be able to discover both the known and new attacks as soon as possible. From fig. 1 maximum attacks were performed by Neptune attack. This attack could pose a serious security threat. This protection prevents access to potentially malicious domains, websites or IP addresses that are known to be associated with malware, viruses, misleading applications such as fake antivirus or fake codecs.

REFERENCES:

1. Malware - Wikipedia, the free encyclopedia en.wikipedia.org/ wiki/ Malware
2. www. pcworld.com/ article/ 210891 / malware.html
3. H. F. Lin and J. M. Liang Event based ontology design for retrieving digital achieves on human religious self-help consulting. Proc. Of 2005 *IEEE International Conference on e-technology, e-Commerce and e-Service*, 2005 pp. 453-475.
4. G. P. Zarri. Semantic web and Knowledge Representation, Proc. Of the 13th International Workshop on Database and Expert System Applications (DEXA'02), 2002, pp. 1529-4188.
5. Teknomo, Kardi, "K-means Clustering Tutorials".
6. http:// databases. about.com/ od/ datamining/ a/kmeans.htm.

7. Sheilini Jindal , "*A Proportional Analysis On The Illustrious Practices For The Extraction And Discovery Of Hidden Patterns - Data And Web Mining*", International Journal of Enterprise Computing and Business Systems (Online)http://www.ijecbs.com, Vol. 1 Issue 1, January 2011.
8. http://www.cert.org/ftp/cert advisories/ CA-96.21.tcp syn flooding, 19 September, 1996.
9. Maheshkumar Sabhnani, Gursel Serpen, KDD Feature Set Complaint Heuristic Rules for R2L Attack Detection.
10. http:// www. cert.org/ ftp / cert_advisories/ CA- 97.28, Teardrop _Land, 16 December, 1997.
11. Number Distributed Denial of Service Attacks , The Internet Protocol Journal, Volume 7.
12. http:// www. cisco.com/ web /about/ ac123/ ac147/ archived_issues/ ipj_7-4/ dos_attacks.html
13. http:// www3. physnet. uni-hamburg. de/ physnet/ security/ vulnerability/ teardrop.html
14. NMAP Homepage. http:// www. insecure.org/ nmap/index.html. 1998.
15. http:// www. porcupine.org/ satan/ demo/ docs/dangers.html
16. http:// www. cert. org/ ftp/ cert _advisories/ CA-98.01.smurf, 5 January , 1998.
17. https:// www. incapsula. com/ ddos/attack-glossary/ ping-of-death.html.
18. http:// www. rootshell. com/ archive-j457nxiqi3gq59dv/199801/beck.tar.gz.html., 1 January, 1998.
19. http:// www. cert. org/ ftp/ cert_advisories/CA-93%3a10. anonymous. FTP.activity., 14 July , 1993.
20. Anonymous. Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network, Sams.net , 201 West 103rd Street, Indianapolis, IN, 46290, Chapter 15, pp. 359-362, 1997.
21. http:// www. cert. org/ ftp/ cert _advisories/ CA-97.09.imap_pop., 7 April, 1997.
22. http:// www. cert. org/ ftp/ cert _advisories/ CA-96.06.cgi_example_code., 20 March, 1996.
23. http:// www. cert. org/ ftp/ cert _advisories/ CA-97.28.Teardrop_Land., 16 December , 1997.
24. http:// www. cert. org/ ftp/ cert _advisories/CA-96.12.suidperl_vul., 26 June , 1996.