IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

A Comparative Study of different Network Ports for Malware attack detection

Partha Pratim Banik
Asst. Professor, CSE & IT Dept.
Bhavan's Tripura College of Science &Technology
Anandanagar, Tripura (W), India
E-mail: banikparthapratim@gmail.com

Dr. Partha Sarathi Bhattacharjee
Website & Networking Unit
NIT Agartala
Agartala, India
E-mail:psbkls@gmail.com

Virus: Virus is one type of malware which infects computers and other files by duplicating itself. It cannot exist independently so it attaches with other filesmore precisely executable files and application and due to its replicating features,it spread across

Abstract **-Malicious software or malware is a big challenging issue in network security. Malware are regularly attacking computer systems which are connected with networks. The attacks are occurred confidential by accessing the IP addresses which are assigned to the Computers / Firewalls and the attacks are happened by different network ports. In this paper, the analysis of attack by malware are carried out with respective port numbers and emphasis on specific port security where maximum attacks are detected.**

Keywords – Malware; Ports; Virus; Spyware; IDS.

I. INTRODUCTION

Malicious software or malware poses a major security concern in this digital age as computer users, corporations, and governments witness an exponential growth in malware attacks. Current malware detection solutions accept Static and Dynamic analysis of malware signatures and behaviour patterns that are time consuming and ineffective in identifying unknown malwares. Recent malwares use polymorphic, metamorphic and other evasive techniques to change the malware behaviours quickly and to generate large number of malwares. Since new malwares are mostly variants of existing malwares, machine learning algorithms (MLAs) are being employed recently to conduct an effective malware analysis. This requires extensive feature engineering, feature learning and feature representation.
A malware gets different names such as adware, spyware, virus, worm, trojan, rootkit, backdoor, ransomware and command and control (C&C) bot, based on its purpose and behaviour. Detection and justification of malware is an evolving problem in the cyber security field.

II. TYPES OF MALWARE

Malwares exist in different forms; they are broadly categorized in the following manner. They are not mutually exclusive although many of them exist in more than one category.

files and even computers through network. System performance was degraded and denial of service attack occurs due to viruses [1].
Worms: Worms are malicious piece of code that exist independently. They have feature to multiple themself. They transmit through storage devices and emails, also consume network and computer resources which leads to performance degradation ofsystems. As they can create multiple copies of themselves, antivirus scanners can identify these codes because of multiple existences [2].
Trojan Horse: Trojan Horse behaves like a useful program but it has harmful purpose. They do not replicate themselves but it transferred in a computer by internet interaction like downloading. It steals sensitive information, observe activity of users and can delete and alter or corrupt files on the system where it resides. [3]
Rootkit: Rootkit take control of the operating system such that it can hide itself or can make a safe environment for other malwares to hide in the system. Basically, it is a masking technique to cheat antivirus so that they cannot find malwares in the system and consider them as normal applications.
Spyware: Spyware are used to steal someone personal information or keep the watch on user's activities. It is installed without the knowledge of system owner and secretly collects the information and sends it back to the creator. Even company with big names like Google also use spyware to collect the required information of their users [4].
Adware: Adware are quite irritating most of the time as it plays advertisement on user computer without its permission and interrupt its current activity. Basic purpose of the adware is to get financial benefit. It does as much harmful as other malwares.
Cookies: Cookies are in form of text file and contain information that is stored by web browser on users.

Sniffers: They are the software that observe and record the network traffic. They analyse different fields of packets and collect information for preparation of the malware attack.
Botnet: Bot is a software that allow attacker to control an infected computer .A network of infected computers controlled by hackers/attackers to do malicious activities without the knowledge of owner. They can make denial of service attacks, send spam messages, and steal information.
Keyloggers: It is kind of spyware that is used to record key strokes to steal passwords, credit card details and other important and sensitive figures. It transferred in a computer when some other malicious software is installed or any infected site is visited by user.
Spam: Junk emails are another names of spams. These identical emails are created and send to multiple recipients at the same time. It consumes a lot of bandwidth and also cause to slow down the system.
Ransomware: Now a day's Ransomware are the major threat for internet industry. Ransomware are malwares that take control of user PC by encrypting user data, stop some application and don't allow users to use your operating system until users fulfil their demands which is mostly in terms of money.

III. MALWARE DETECTION METHODS

A. Signature-based malware detection

A case strolling approach by, for instance, business antivirus is an instance of check based malware acknowledgment where the scanner looks at for a game plan of byte inside a program code to perceive and report a noxious code. The ultimate objective of the method is to perceive malware by inspecting the code in the midst of program course of action. This technique customarily covers complete program code and inside a concise time span. In any case, this technique has obstacle by neglecting the semantics of rules, which licenses malware disarray in the midst of the program's run-time [5].

B. Specification-based malware detection

It is an outstanding occasion of assurance based malware area, where a distinguishing proof count that watches out for the deficiency of case organizing was created. This count joins rule semantics to distinguish malware cases. It is used to describe the toxic practices of a malware which are development of rules addressed by components and delegate constants.

C.Behavioral-based detection

This approach performs surface checking and perceives the malware's movement. The approach produces database of a toxic lead with an unquestionable number of gatherings of malware on a target working system. It develops a two stage mapping system that creates marks at run-time from the checked structure event and API calls. The system readies a classifier using an assistance vector machines (SVMs) to perceive a toxic program from regular application lead [6].

IV. DATA MINING TECHNIQUE FOR DETECTING MALWARE

In this approach, toxic executable code or programmes are perceived. It describes a noxious executable as a program that performs work, for instance, exchanging off a structure's security, hurting a system or getting sensitive information without the customer's approval. The data mining systems perceive plans in a considerable measure of data, for instance, byte code, and use these cases to recognize future cases in practically identical data. Their framework used classifiers to recognize new malicious executables codes. Classifier is an oversee set, or area appear, made by the data mining computation that was set up to finish a given game plan of getting ready data. They created a structure that used data mining counts to plan distinctive classifiers on a course of action of harmful and kindheartedexecutable to recognize new descriptions. The copies were first statically separated to remove properties of the combined, and after that the classifiers arranged over a subset of the data.
The massive plans of activities from open sources were separated into two classes: malicious and thoughtful executables. Instance of this enlightening record is a Windows or MS-DOS mastermind executable, which is moreover applicable to various setups. Since the disease scanner was revitalized and the contaminations were obtained from open sources, it was acknowledged that the contamination scanner has a check for each malicious contamination. In this regard, the datasetis divided into two subsets: the arrangement set and the test set [6].

V. RESEARCH ISSUES & CHALLENGES [7]

There are three most important qualities that need to be measured while evaluating an Intrusion Detection System: completeness, correctness, and performance or timeliness. Evaluation is limited by the quality of the dataset. Port scan attack detection methods are very limited in the degree to which the methods can quantify their completeness, correctness and performance ortimeliness.

• Most existing attacks, especially those belonging to many-to-one or many-to-many categories, cannot be controlled at the firewall level. For example, the TCP connect(), SYN, SYN | ACK scan can be blocked at the firewall level, whereas controlling the other scanning techniques at the firewall level is an important issue which cannot be controlled by Firewall.

• The existing attack detection methods have been found to work either at packet level or flow level or both. However, our survey finds that most detection approaches use packet level information for attack detection because it gives not only the connection information but can also analyze the packet payload. However, an appropriate technique for packet analysis based on both header and payload information towards the detection of known as well as unknown attacks is still in implementation stage.
• Based on our analysis of existing methods, threshold-based methods have been found to be more effective. These threshold-based methods are highly sensitive to input parameters (thresholds) and their estimations are often found to be network scenario dependent. Therefore, development of a generic threshold-based detection mechanism across different network scenarios is a challenging issue for malware attack detection.

• With the evolving nature of networking technology and with the constant effort of attackers toward launching newer attacks, existing IDSs are inadequate for handlingknown as well as unknown attacks.

• From analysis, it is found that security practitioners have both positive and negative perceptions about port scan attack detection methods. In particular, practitioners find

itchallenging to decide where to place the attack detection module and how to best configure themfor use within an environment with multi-stage architecture.

• Due to the voluminous size of network trafficdata and the constant changing of traffic patterns as well as the presence of the noise in audit data, it is a challenging task to build normal profile of network behavior. Further research towards finding appropriate machine learning or soft computing methods is necessary to detect the unknown attack.

• Due to lack of less availability of labeled datasets for training or validation of the models, most scan detection approaches result in many false alarms, minimization of false alarm is a challenging issue for attack detection.

• Network traffic has large amount of data. It is a challenging task to update the signatures database dynamically to detect misuse detection. In this regard, various analysis were carried out by different researchers using different networking monitoring and analysing tools i.e. Wireshark, Tcpdump,bro-Ids [8][9][10].

VI. DATASET

In this experimental analysis, the dataset for the malware attack detection records are collected online. The dataset is retrieved from https://vizsec.org/ which is a list of potentially useful datasets for the VizSec research and development community.

Malware : Adware	
Port No.	**No. of hits**
0	23
53	529
67	1
80	627
123	5
443	**1339**
1900	10
3641	1
5222	9
5228	16
5351	8
5353	2
6368	1
8610	1
8612	1
12350	14
14213	1
14338	1
20999	1
32825	1
32996	1
33119	2
33142	1
33183	1
33184	1

Table 1: Adware Attack Data

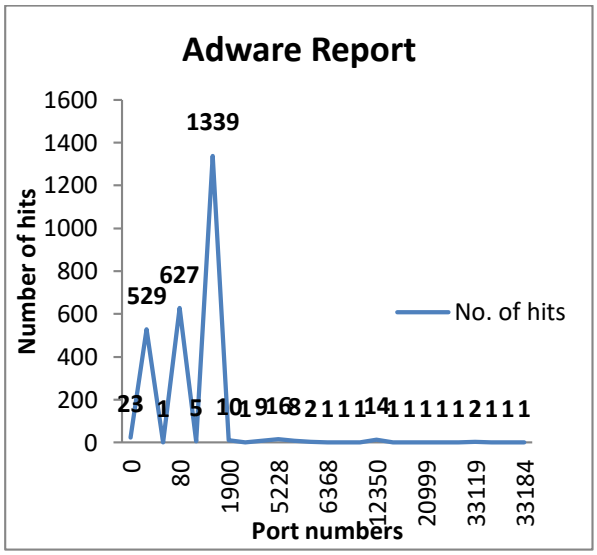

Fig 1: Adware Attack graph w.r.t ports

Malware : Beningn	
Port No.	**No. of hits**
0	4
53	41
80	12
443	**121**
1900	7
5222	4
5353	1
34259	1
36721	1
37033	1
37541	1
38005	1
40851	1
40852	1
43504	1
43954	1
44661	1
45133	1
49241	1
49398	1
50650	1
51702	1
51702	1
51791	2
52273	2
54678	1

Table 2: Beningn Attack Data

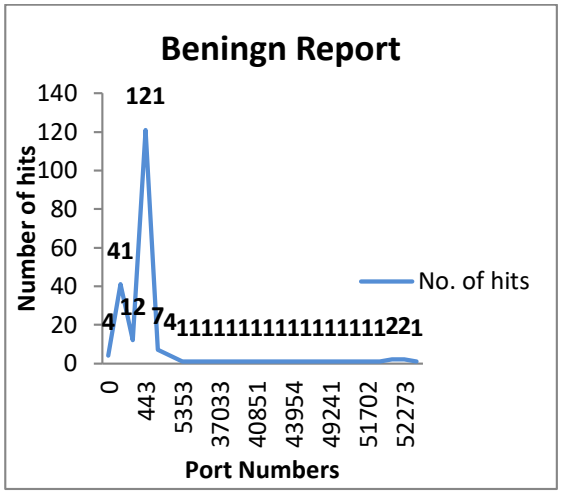

Fig 2: Beningn Attack graph w.r.t ports

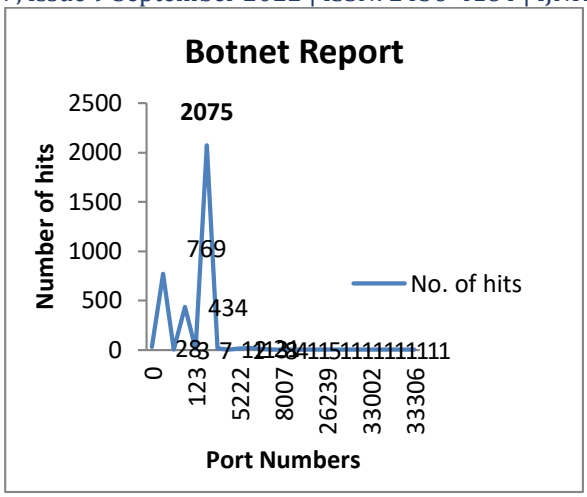

Fig 3: Botnets Attack graph w.r.t port

Malware : Botnet	
Port No.	**No. of hits**
0	28
53	769
67	3
80	434
123	7
443	**2075**
1900	12
3907	1
5222	13
5228	21
5351	8
5353	4
8007	1
8610	1
12350	5
18997	1
26239	1
27924	1
29521	1
32822	1
33002	1
33279	1
33303	1
33304	1
33306	1

Table 3: Botnet Attack Data

Malware : Premium sms	
Port No.	**No. of hits**
0	12
53	233
67	1
80	**448**
123	4
443	**341**
1900	4
5222	4
5228	6
5351	4
5353	1
8610	1
8612	1
12350	2
15323	1
19578	1
30525	1
30855	1
33149	1
33150	1
33740	1
33835	1
33921	1
34000	1
34678	2

Table 4: Premiumsms Attack Data

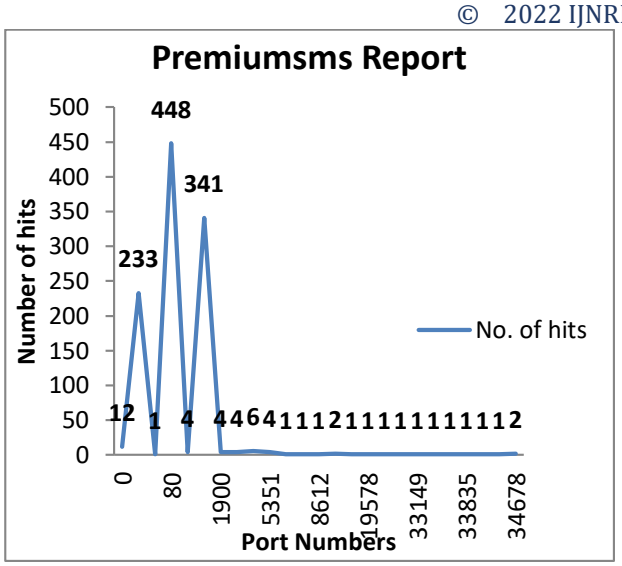

Fig 4: Premiumsms Attack graph w.r.t ports

VII. CONCLUSION

This Proposal shows different malware exposures, malware arrange plots and associated issues related to malware detection with network ports. The upsides of each malware gathering are also highlighted here. The task of lessening the dastard effects of malware can't be overemphasized here as it constitutes overall risk to the online resources and cash related activities.

From the analysis and their respective graphs, it shows that maximum hits occur for the port numbers 443and port number 80. Maximum number of hits is 1339,121 and 2075 which are occurred in port number 443 for the malwares Aadware, Beningn and Botnet. For the malware Premiumsms, maximum number of hits 448 occurs in port number 80.

As malware writer change their frameworks by including new lead and adjusting existing ones, the effort of protecting workplaces against malware defamationsshould be taken care with reasonable idea for security control while making programming. This investigation analyses some malwares for network attack detectionand the necessity of network port security to prevent the malware attacks.

REFERENCES

[1] Spafford, Eugene, "The internet worm incident." ESEC'89 pp.446-468, 1989
[2] Li, Jun and Shad Stafford, "Detecting smart, self-propagating Internet worms.", Communications and Network Security (CNS), IEEE Conference on. IEEE, 2014
[3] Idika, Nwokedi, and Aditya P. Mathur, "A survey of malware detection techniques", Purdue University,2007
[4] Yin, Heng, et al. "Panorama: capturing system-wide information flow for malware detection and analysis.", Proceedings of the 14th ACM conference on Computer and communications security.ACM, 2007
[5] H. D. Huang, T. Y. Chuang, Y. L. Tsai, C. S. Lee, "Ontology-based Intelligent System for Malware Behavioral Analysis", presented at the 2010 IEEE World Congress on Computational Intelligence (WCCI2010), 2010
[6] Zhao Hengli, Xu Ming, NingZheng, Yao Jingjing, Q. Ho, "Malignant Executables Classification Based on Behavioral Factor Analysis", introduced at the 2010 International Conference on e-Education e-Business e-Management and e-Learning, 2010

[7] Monowar H. Bhuyan, Dhruba K Bhattacharyya and JugalKalita , “Surveying Port Scans and Their Detection Methodologies”, The Computer Journal (COMPUT J), Oxford University Press, 54(10)., pp.1565-1581 , October 2011
[8]Wireshark Protocol Analyzer. Available online: http://http://www.wireshark.org/
[9] Tcpdump. Available online: http://http://www.tcpdump.org/
[10]Bro Network Security Monitor. Available online: http://www.bro-ids.org/

****