International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

A Proposal for Worm Malware Detection by Using Association Rules

Karim Hashim Al-Saedi[1], Osama Mohammed Qasim[2]

Abstract: ***Many attacks of malware occur in these days especially worms. Worms can replicate itself inside the network and spread through each device connected to the network. To prevent these attacks we need a strong Intrusion Detection System to defy this kind of threats. In this proposal, we proposed a method to detect the worms, to be able to prevent the attacks and ensure our network safety. The function of the method is to aggregate the data packets that comes from the outside, and then analyze it. The method will extract the exact feature from a data set and check it if the packet weather it was a threat or a benign depending on rules stored in the database by using one of the data mining technique namely Association Rules. When detect occur awarning will be sounded and it will be stored as a threat, the control unit will arrange the alerts of the malware. We used the Association Rules technique because this technique can extract the wanted features for the malware and classify it as tables and give us the last result of detection. This technique help to reduce the amount of worm malware threats and make the system more accurate in detection.***

Keywords: Worm, Malware Detection, Association Rules

1. Introduction

Network Security is one of the Computer Science sections, which means protecting the data stored in the computers linked together through a network. In these days network knowledge has been developed and became common in the world, the attackers of networks are growing, and the threats of those attackers has been evolved[1]. Network Security is one of the most important cases for foundations such as universities ,general and particular projects ,these foundations provides a very important functions on processes and nation safety [2].

Online services turned out progressively common for the customers in the last decades. Network users are able to communicate in business, information casting and participate knowledge. So as to decrease expanses, these services are cooperative by Information Technology (IT) associations and Internet Service Providers (ISPs)[3].

This may put the network at risk and cause malware. Malware is a software could be installed in our computers, smartphones and in any device connected to the network, and it damages these devices by trying to get gateway to the personal data and important information of our devices or by showing unwelcomed announcements (Adware) [4].

In electronic devices like computers and smart phones there are numerous amount of malicious software (malware) types that spreads through the world and it is multiplying rapidly, malware is increasing about 400K/day to 1M/day [5]. Kaspersky Labs found unprecedented types of mobile malware in 2015, and it was 884,774 types. This means three times more than they discovered in 2014, which it were 295,539 types [6].

Malware considered as the most serious impendences for the people who uses the network, which threats confidentiality and safety of their data. Great forms of malware expanded through the network, lurking in packages. Each day new forms of malware are discovered, so there must be a technique to prevent these attacks [7]. The malware makers and programmers have many choices to make a decision about safeguarding the code from the anti-malware programs [8].

One of the malware threats is worm, worm can spread in the network fast by replicating itself [9][10]. Network worm is a dangerous problem that the world faces nowadays specially individuals and facilities. Despite of the ability of the detection techniques, still its comprehensive effect is difficultly determined. Also its unknown how many devices connected to a network will end up with this kind of threat [11].

There are many types of worms: Cross-Site Scripting (XXS) and Java Script, this worms threaten the public websites (social networks) like Facebook, Twitter, LinkedIn, etc. [12][13]. Second there is the wormhole, this attack happens in wireless networks, a connection between two or more devices like Ad-Hoc networks[14]. And there is the Polymorphic worm, this worm is one of the most dangerous worms, because it is hard to detect, in each case it make changes of its aspect [15]. These attacks of worms need techniques to detect and prevent.

This gives rise to detection techniques. Detection techniques are the most important safeguard for the networkand have major benefits for network security. Presently the malware deterrence is the antivirus programs, they are the first defense line that rise against malware. Mostly the functionsused to detect a threat is Behavioral-based tool, Signature-based and Heuristic methods[16][17]. The popular one is Signature-based, it includes finding malware from the network packets that has a doubtful data [18].

Keeping the secrecy, impartiality and availability in a genuine operating system (OS) is a very hard task, because of the huge amount of the system objectives and the difficulties of interactions between themmake protecting all topics of the system expend time and prone for errors. The main difficulties of network security is the weakness for knowing the importance of its system objects that involves security, which facing huge amount of system objects in a true operating systems [19].

2. Related Works

The impulsive decent of malware action packet depends on a method of tracing system to detect the malware. Xiaoyan Sun, et al. calculated the present decent theory of malware action specification. By decreasing the involvement of the malware packet decent, the system builds a graph to detect and mine the malware [20].

Xiao, et al.in 2013 used API (Application Programming Interface) system to expose unknown threats of malware. The algorithm they utilized for mining association rules to expose these threats was OOA (Object-Oriented Associate Mining. With multiple tests the amended algorithm confirmed the proposed system is influential and can be used for detecting the anonymous and different malware threats [21].

Malware tries to hide the dynamic signatures, Chun-I Fan, et al. used hooking methods to track these signatures. By using the techniques of data mining,they contrasted the different actions between malicious software and non-malicious software to detect and identify the threat of malware. The test results proved that the detection ratio was 95% with 80 attributes. This method increased the detection and decreased the complexity [22].

James B. Fraley, et al. they detected the polymorphic malware threat by employing the techniques of data mining and feature extraction methods. The results of their study was 0.0030 low false positive rates, while high true positive was 0.9978 for anonymous files with size about (4k) [23].

A modern study used by Tobias Wuchner, et al. for detecting malware graph by using frequency-based graph mining methods for extracting features form many graph malicious software. This increased the efficiency of the detection by more than 600% [24].

3. Problem Statement

The Intrusion Detection System detects a big number of malware threats. These threats are stored in the data set, so for the IDS it is difficult to detect and analyze new threats. When these attacks happens the detection system will not consider it as threat and it will pass as non-malicious data. Once this data enter the network and pass the IDS, it begin to does its malicious work and threatens the network security. It is highly necessary to make a smart detection system which capable of analyzing and detecting new types of threats by employing data mining techniques.

4. Research Objectives

In this research, we will present a system that detects as possible new attacks that threatens the network. In order to achieve that the objectives of the system as follows:

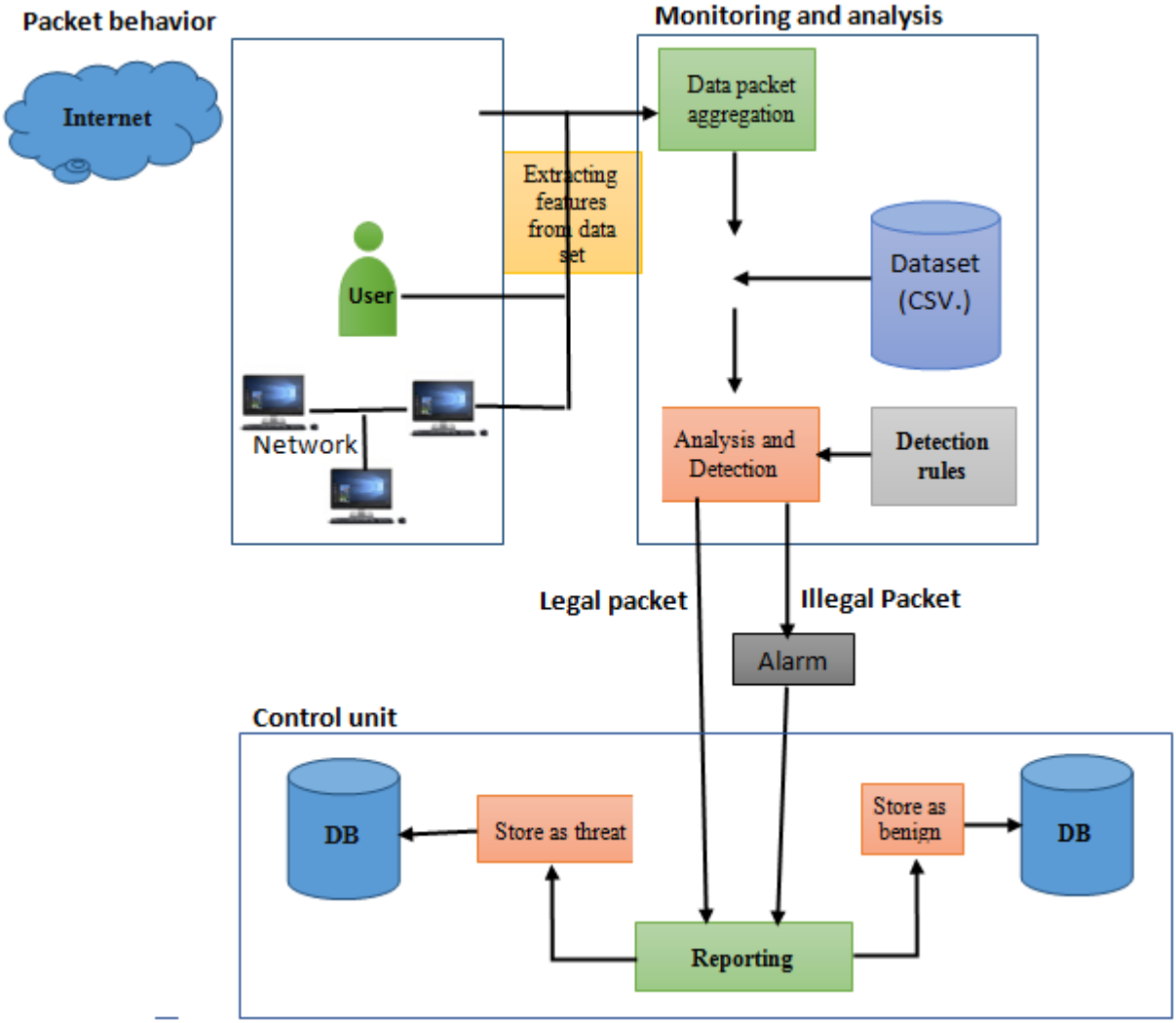
- To detect worm malware by using Association Rules technique.
- To extract the exact characteristics from the data set of malware worm alerts by using classification technique.
- To build a data mart for storing the new types of threats when the attack occur.

5. Paper Motivations

- The need for network security became a high priority, because of huge using of the network in these days.
- Too many attacks that threaten the network specially the new attacks that is hard for the IDS to detect.
- Today the world is dealing with a numerous amount of data, which make the use of data mining techniques is the best choice to employ it in the IDS.

6. Proposed Method

Our proposed method for IDS to detect worm summarizes in the Fig 1 below it contains three phases: Packet behavior, Monitoring and Analysis and Control unit, each phase has multiple processes:



When a packet sent to the network, it could come from cloud internet, a single user or from a network.

Many different types of data packets will enter the network; the system will aggregate it all and then analyze it by extracting the features from the data set. The system will detect the malware according to the detection rules. When the detection happens, the method willgenerate warning, deal with the detected data, and consider it as a threat and the rest will consider as benign data.

Each of the threat data and the benign data will be stored in a separate database (one for threats and the other for the benign). In each step, the system will make a report for the current state, store it in the database, and send it to the control unit.

7. Expected Results and Conclusions

The expected result of this proposal is to make an IDS system that capable of detecting and analyzing the new attacks of worm malware by using the Association Rules technique. In this proposal, we propose a system decreases the threats, has more accuracy, able to detect a new attack, increase the network security efficiency and then store in the database to make the system learn the new attacks.

References

[1] A. . Fallis, "Neural Network Model," *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2013.
[2] M. S. Kacar and K. Oztoprak, "Network Security Scoring," *2017 IEEE 11th Int. Conf. Semant. Comput.*, pp. 477–481, 2017.
[3] H. Li, P. W. C. Prasad, A. Alsadoon, L. Pham, and A. Elchouemi, "An improvement of Backbone Network security using DMVPN over an EZVPN structure," pp. 14–16, 2016.
[4] A. Juan *et al.*, "Native Malware Detection in Smartphones with Android OS Using Static Analysis , Feature Selection and Ensemble Classifiers," pp. 67–74, 2016.
[5] J. R. Upchurch, "Malware Provenance : Detecting Code Reuse in Malicious Software," pp. 101–109, 2016.
[6] M. Ping, B. Alsulami, and S. Mancoridis, "On the Effectiveness of Application Characteristics in the Automatic Classification of Malware on Smartphones," pp. 75–82, 2016.
[7] E. Bocchi *et al.*, "MAGMA network behavior classifier for malware traffic," *Comput. Networks*, vol. 0, pp. 1–15, 2016.
[8] L. Jones, A. Sellers, and M. Carlisle, "CARDINAL : Similarity Analysis to Defeat Malware Compiler Variations," 2015.
[9] M. A. Ahmad, S. Woodhead, and D. Gan, "Early

Containment of Fast Network Worm Malware," pp. 195–201, 2016.
[10] L. Xue and Z. Hu, "Research of Worm Intrusion Detection Algorithm Based on Statistical Classification Technology," *2015 8th Int. Symp. Comput. Intell. Des.*, pp. 413–416, 2015.
[11] M. Martens, H. Asghari, M. van Eeten, and P. Van Mieghem, "A time-dependent SIS-model for long-term computer worm evolution," *2016 IEEE Conf. Commun. Netw. Secur.*, pp. 207–215, 2016.
[12] P. Chaudhary, "Cross-Site Scripting (XSS) Worms in Online Social Network (OSN): Taxonomy and Defensive Mechanisms," pp. 2131–2136, 2016.
[13] S. Gupta and B. B. Gupta, "Alleviating the proliferation of JavaScript worms from online social network in cloud platforms," *2016 7th Int. Conf. Inf. Commun. Syst. ICICS 2016*, pp. 246–251, 2016.
[14] D. Goyal, "To Detect Or Preventing Worm Hole In MANET."
[15] A. Mondal, "Automated signature generation for polymorphic worms using Substrings extraction and Principal Component Analysis," 2015.
[16] Z. Bazrafshan, H. Hashemi, S. M. H. Fard, and A. Hamzeh, "A survey on heuristic malware detection techniques," *IKT 2013 - 2013 5th Conf. Inf. Knowl. Technol.*, pp. 113–120, 2013.
[17] Y. Ye, T. Li, Q. Jiang, and Y. Wang, "CIMDS: Adapting postprocessing techniques of associative classification for malware detection," *IEEE Trans. Syst. Man Cybern. Part C Appl. Rev.*, vol. 40, no. 3, pp. 298–307, 2010.
[18] C. J. Fung, D. Y. Lam, and R. Boutaba, "RevMatch : An Efficient and Robust Decision Model for Collaborative Malware Detection," no. Cmd.
[19] W. Mao, Z. Cai, D. Towsley, Q. Feng, and X. Guan, "Security importance assessment for system objects and malware detection," *Comput. Secur.*, 2017.
[20] X. Sun, Q. Huang, Y. Zhu, and N. Guo, "Mining distinguishing patterns based on malware traces," *Proc. - 2010 3rd IEEE Int. Conf. Comput. Sci. Inf. Technol. ICCSIT 2010*, vol. 2, pp. 677–681, 2010.
[21] X. Xiao, D. Yuxin, Z. Yibin, T. Ke, and D. A. I. Wei, "Proceedings of the 2013 International Conference on Machine Learning and Cybernetics, Tianjin, 14-17 July, 2013 MALWARE DETECTION BASED ON OBJECTIVE-ORIENTED ASSOCIATION MINING," pp. 14–17, 2013.
[22] C.-I. Fan, H.-W. Hsiao, C.-H. Chou, and Y.-F. Tseng, "Malware Detection Systems Based on API Log Data Mining," *2015 IEEE 39th Annu. Comput. Softw. Appl. Conf.*, vol. 3, pp. 255–260, 2015.
[23] J. B. Fraley and M. Figueroa, "Polymorphic malware detection using topological feature extraction with data mining," *SoutheastCon 2016*, pp. 1–7, 2016.
[24] O. Paper, "Leveraging Compression-based Graph Mining for Behaviorbased Malware Detection," vol. XX, no. c, pp. 1–14, 2014.