Online Malicious Attacks and Defending Techniques and Approaches- A Survey

M. Narmatha
Assistant Professor, Department of Computer Science, Sri Jayendra Saraswathy Maha Vidhyalaya College of arts and science, Coimbatore, Tamil Nadu, India.

Shri Hari Aravind.K
M.Phil Scholar, Department of Computer Science, Sri Jayendra Saraswathy Maha Vidhyalaya College of arts and science, Coimbatore, Tamil Nadu, India.

Abstract – Internet security is the major part of current network scenario, there are several types of security threats threatens the internet transactions. Data stealing, data corruptions, intrusion activities are day to day increasing due to the distributed nature. Even though there are several techniques and approaches are proposed, still some new issues grow tremendously every day. So knowing the definitions, behaviors and its possible counter measures are important to create a new authentication and prevention schemes. This paper surveys various types of online attacks and its possible counter measures. And the possible techniques to detect online malicious attacks with its pros and cons are discussed.

Index Terms – Honeypot, Online Attacks, Cyber Attacks, Virus, Episode Mining, Intrusion.

1. INTRODUCTION

Information Technology revolution had a great impact on the online applications. It is always considered as a major challenge to most applications. To ensure the security of the online/web information is extremely important. There are several attacks threatens the current online applications. The main aim of information security domain is to protect, detect and thwart data from corruption, modification, tampering and access [1]. This paper surveys different types of attacks, and its countermeasures. This also discusses various techniques and tools to handle such attacks.

A. Online attacks:

Online data security threats are relentlessly inventive. There are several security threats threatens the current internet application and users. Using new ways of annoying activities, the attacker can steal and harm the data [2]. This type of threat is an event that can take advantage of vulnerability and cause a negative impact on the system. The dangerous and potential threats in such scenario should be identified and prevented earlier, and the related vulnerabilities should be predicted to minimize the risk of the security hazard. The types of online attacks are discussed below.

1.1 Virus Threats:

Virus threats are the malicious programs, which can access the computer and its resources without the permission or knowledge of the user. This can alter the way a computer operates and performs many malicious activities. These types of viruses replicate and execute it to damage the system faster. It can be identified by several types such as memory targeted virus, email viruses, boot sector virus and encrypted macro viruses. When the virus affects a system, the following behaviors are generally used to detect [3].

Behaviors:

- This type of security violations may delete files or changing random data on the computer disk.
- This may slow down the system and reduces the performance.
- some viruses do less harmful things such as playing music or creating messages or animation on the system screen

Countermeasures:

- Obtaining certification from vendors that products are virus-free;
- With the use of updated virus scanning tools can reduce the virus and it can delete virus contained programs;
- Formulation of information security policies and training can reduce the problems of viruses.

1.2 Spyware Threats :

Spyware is software which installed in the system without the user knowledge. It is considered as a serious computer security threat [19]. This has been generated with a set of programs that will monitor the online activities or system and its installs programs without the user approval for profit or to capture personal information [4]. Generally this type of programs

comes from a malicious websites, and this is included in the genuine software's.

Behaviors:

There are several behaviors can be detected after a system affected by the spyware threat.

- The affected system has several and numerous infections if that is affected by the spyware.
- Users frequently notice unwanted behavior and the program ruins the performance of the system.
- A spyware infestation can create significant unwanted CPU activity, disk usage, and network traffic.
- It creates stability issues, such as OS booting failure applications freezing, and data crashes. It interrupts the network and makes the internet connectivity.

To secure the system form the above attacks several antivirus, anti-spyware and anti-spam related software's are introduced.

Countermeasures:

- With the use of firewalls, the spyware can be blocked.
- Anti-spyware software's can be used to protect.
- These types of anti-virus software's are rules-based or based on downloaded definition files that identify currently active spyware programs.

1.3 Phishing Threats

Phishing threats are a form of Internet fraud, and this makes the user to disclose all their confidential information's. This data will be used to do some illegal process. This type of threats can be performed to steal sensitive financial and personal information's through message and email format [5]. Some of the most common attacks include:

- Bonk – An attack on the Microsoft TCP/IP stack that can crash the attacked computer.
- RDS_Shell – A method of exploiting the Remote Data Services component of the Microsoft Data Access Components that lets a remote attacker run commands with system privileges.
- Win Nuke – An exploit that can use NetBIOS to crash older Windows computers.

Behaviors:

- Phishing attack contained data may include bad grammar, misspellings, and/or generic greetings.
- This may include maliciously crafted attachments with varying file extension or links to a malicious website
- This may appear to be from a position of authority or legitimate company. Ie the employer name of the company etc.,
- This usually asks the user to update or validate information or click on a link
- Threatens extreme consequence or promises reward
- Appears to direct you to a web site that looks real

Countermeasures:

The following countermeasures can be taken to guard against phishing and anti- phishing:

- Avoiding or Deleting suspicious e-mails can avoid
- Reporting any potential incidents to the server may reduce the severity.
- Digital signatures can avoid phishing.
- Configure Intrusion Detection Systems (IDS) to block malicious domains / IP addresses
- Ensure anti-virus software and definitions are up to date.

1.4 Back doors:

These types of attacks are also called as trap door attack; this is a set of code written in the specific applications or the operating systems. This type of programs grants the users to access the programs without security restrictions. Back/trap doors become a problem when the programmer forgets to remove a back door after debugging, Because, the programmers are used the triggers for fast debugging [6].

Behaviors:

The followings are the basic behaviours arises due to the back doors.

- The back door can either recognise some special sequence of input, or is triggered by being run from a certain user ID which is then granted special access rights accordingly.
- Further, an attacker can create a back door for his future access after gaining access to an account.

Countermeasures:

- Obtain certification from vendors that the products contain no undocumented back doors and accept systems only from trusted sources;

- Put in place stringent system development and change control procedures such that systems can normally be put into production use only after thorough testing to confirm that no back doors have been included in the systems;
- Regular integrity checks on programs used in production to ensure that the programs have not been altered.

1.5 Brute force:

Brute force attack is a technique to capture encrypted messages, and then use software to break the code and gain access to messages, user IDs, or passwords. If the attacker gains access to a user ID that has sufficient privileges, the user can create a back door for future access, even if the password of the user ID is subsequently changed[7]. A computer program or ready-made software is commonly used for implementing brute force attack to crack the passwords.

Behaviors:

- This type of attack can access or block the user account.
- May disconnect the access of the application

Countermeasures:

- Deploying strong encryption technology and effective key management practices to protect confidentiality of messages, user IDs and passwords;
- Enforce sound password policies (e.g., mandating minimum length of passwords, or periodic changes in passwords);
- Perform penetration testing to identify vulnerability to unauthorized interception and assess the strength of encryption;
- Provide adequate education to customers on security precautions (particularly on setting passwords).
- honey pot mechanism
- CAPTCHA (Completely Automated Public Turing test) mechanism can avoid brute force attacks [8]

1.6 Eavesdropping Attacks:

Eavesdropping is a cyber-attack that focuses on capturing small packets from the network transmitted by other computers and reading the data content in search of any type of information. This type of network attack is generally one of the most effective attacks [9]. This can be performed when the encryption services are least preferred. This is performed by the Un-authorized user to interrupt the application.

Behaviors:

- Detecting that an unknown data is leaked to others.
- Unusual hardware changes, sounds are the indication of eavesdropping.

Countermeasure:

- Standard encryption `techniques such as AES 128 bit or RC4 stream cipher can reduce the harm due to this attack.
- Single sign-on protocol can be included with SSL
- Strong authentication protocol; like Kerberos can be used.
- Continuous supervision/observation of all service personnel allowed into the area for repairs or to make alterations.

1.7 Replay Attacks:

This is similar to the playback attack, and it's a part of masquerade attack. An attacker copies the message, data, user credentials or key information transmitted between two hosts and then uses it for a nefarious purpose [10]

Behaviors:

Delay in data transmission and gives delayed response.

Countermeasure:

- OTP can be applied to avoid this type of attack.
- Cookie timeout settings can protect users from replay attacks.

1.8 Keylogger Attack:

It captures the keystrokes of the user for stealing their password. This is usually performed with the help of software's, which captures and stores the content in a place without the user permissions. Several banking applications are using the following countermeasure to thwart the keylog attacks [11].

- OTP (one-time password)
- Virtual keyboard can control this type of key logging and stealing attacks.

Summary:

The most of the important and valuable information's are affected by the above types of attacks. From the above analysis, possible enhancements and techniques can be established to handle different types of online malicious attacks. For the above, different types of countermeasures are generate. The popular and the proposed research techniques are discussed below.

2. TECHNIQUES AND METHODS

i. Honeypot system:

Honeypot mechanism is a popular security mechanism, which detects, deflects and selects optimal countermeasures at the time of vulnerabilities and security violations. These types of systems are continuously monitors and isolate the attacker system if any vulnerability detected [12, 18]. The honey pot systems are segregated into two types based on its deployment. The first type is production honeypots and research honeypots. Form the above two, production honeypots are easy to deploy, and this is low interactive honeypot. This type of honeypot system will give less information than another research honeypot system. The research honeypot techniques are tough to deploy, this type of system will collect information's from different sources and performs the deployment with the ability to detect new types of intrusions.

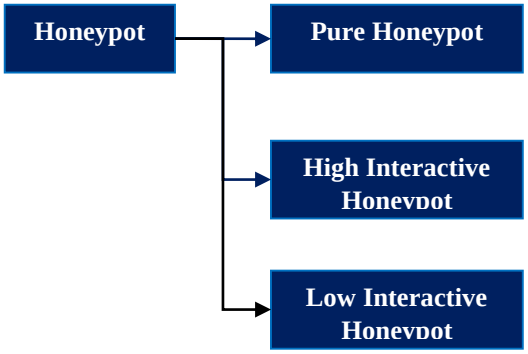

Fig 1.0 Types of Honeypot

The fig 1.0 shows the basic types of honeypot techniques. The Honeypot are considered as weapons against different online attacks. Two or more counteract on a network form a honeynet. Typically, a honeynet is used for monitoring a larger and more varied network. This can be used when the network size is huge and not sufficient for one system. Honeynets and honeypot techniques are usually implemented as parts of larger network intrusion detection systems.

ii. Problem of Honeypot in Online attack Detection:

Honeypots are effective for online attack detection and deflection. However, events and logs collected by a honeypot can rapidly build up an enormous amount of data. This huge dataset will be unable to handle by the network administrator. So, effective techniques and tools should be used to handle such huge events. The followings are the research works, which handles the above issues in honeypot techniques.

Mannila, Heikki, Hannu et al. [13], considered the problem of recognizing frequent intrusion events and its sequences. It finds the maximum frequent episodes from the set of events. An episode is defined to be a collection of events that occur within time intervals of a given size in a given partial order. From the episodes, the rules are created and those rules will be applied to predict the behavior of the sequence. In this paper, the author defines the episodes on partial orders. The authors used alarm flow and inverse structures to recognize the anomalies. They produced an algorithm for finding all episodes from a given class of episodes that are frequent enough. The preliminary results are quite encouraging, but the algorithm implementation is not well suitable for large network logs.

In paper [14], authors Pawar et al, proposed new and advanced intrusion detection system to speed up the attack data detection and prevention process by applying data inference detection process. This paper created an ID for a small internet and LANs. But this is not suitable for large scale online attack detection processes. Later several authors proposed different data mining techniques [15] [16] to handle the above log handling issues in honeypot. Such algorithms are frequent pattern mining algorithms, n-gram analysis process and rule mining algorithms. The authors [17] extended the existing n-grams concept to determine whether a program was normal. In this paper, the ID logs are identified by two set of categories, one is normal sequence and other one is anomaly conditions, this can be detected by its various episode logs and that will be matched with the rule. But the n-gram techniques are used when the repetitive episodes are mined; this is unsuccessful when the terms are dissimilar.

3. CONCLUSION

With the use of honeypot and different types of security approaches, several online and malicious attacks are detected earlier and that will be treated before it affects the application. In the current scenario, cyber/online attacks are a common and spreads well easily, and several techniques were implemented with several common and few uncommon rules to detect and thwart such attacks. Due to the numerous size of intrusion logs, the prediction and decision making process are tough and complicate. In this scenario effective tools and techniques should be identified and that should be used for further intrusion and online attack analysis. Otherwise any type honeypot detection and prediction process is become ineffective. This paper discusses numerous attacks in the online scenario, several traditional tools and algorithms used to handle the attacks with its counter measure. However, the techniques almost concentrated on general detection and analysis process, where the online applications and data security needs additional concentration and work to improve the following problem. The first problem is discovering appropriate techniques to prevent such attacks and selecting optimal countermeasure after speedy evaluation of attacks from the huge intrusion log.

REFERENCES

[1] Liang, Yingbin, and H. Vincent Poor. "Information theoretic security."*Foundations and Trends in Communications and Information Theory* 5.4–5 (2009): 355-580.
[2] Canali, Davide, and Davide Balzarotti. "Behind the scenes of online attacks: an analysis of exploitation behaviors on the web." *20th Annual Network & Distributed System Security Symposium (NDSS 2013)*. 2013.
[3] Bascle, Jeff P., et al. "System and method for reducing the vulnerability of a computer network to virus threats." U.S. Patent No. 7,571,483. 4 Aug. 2009.
[4] Kirda, Engin, et al. "Behavior-based Spyware Detection." *Usenix Security*. Vol. 6. 2006.
[5] Ramzan, Zulfikar. "Phishing attacks and countermeasures." *Handbook of Information and Communication Security*. Springer Berlin Heidelberg, 2010. 433-448.
[6] Dai, Shuaifu, et al. "A framework to eliminate backdoors from response-computable authentication." *2012 IEEE Symposium on Security and Privacy*. IEEE, 2012.
[7] Cho, Jung-Sik, Sang-Soo Yeo, and Sung Kwon Kim. "Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value." *Computer Communications* 34.3 (2011): 391-397.
[8] Von Ahn, Luis, et al. "CAPTCHA: Using hard AI problems for security."*International Conference on the Theory and Applications of Cryptographic Techniques*. Springer Berlin Heidelberg, 2003.
[9] Li, Xu, et al. "Securing smart grid: cyber attacks, countermeasures, and challenges." *IEEE Communications Magazine* 50.8 (2012): 38-45.
[10] Syverson, Paul. "A taxonomy of replay attacks [cryptographic protocols]."*Computer Security Foundations Workshop VII, 1994. CSFW 7. Proceedings*. IEEE, 1994.
[11] Jesudoss, A., and N. Subramaniam. "A Survey on Authentication Attacks and Countermeasures in a Distributed Environment." *Indian Journal of Computer Science and Engineering (IJCSE)* 5.2 (2014): 71-77.
[12] Tang, Yong, et al. "Honeypot technique and its applications: A survey."*MINIMICRO SYSTEMS-SHENYANG-* 28.8 (2007): 1345.
[13] Mannila, Heikki, Hannu Toivonen, and A. Inkeri Verkamo. "Discovering frequent episodes in sequences Extended abstract." *1st Conference on Knowledge Discovery and Data Mining*. 1995.
[14] Pawar, A. B., D. N. Kyatanavar, and M. A. Jawale. "Design of Advanced Intrusion Detection System." (2013).
[15] Lin Shukuan, Qiao Jianzhong, Wang Ya. Frequent episode mining within the latest time windows over event streams. Appl. Intell. 2014;40(1):13–28.
[16] Hwang K, Cai M, Chen Y, Qin M. Hybrid intrusion detection with weighted signature generation over anomalous internet episodes. IEEE Trans Dependable Secure Comput 2007;4(1):41–55.
[17] Lee W, Stolfo SJ, Mok KW. Adaptive intrusion detection: a data mining approach. Artif Intell Rev 2000;14(6):533–67.
[18] Baykara M, Das R. A survey on potential applications of honeypot technology in intrusion detection systems. International Journal of Computer Networks and Applications. 2015; 2(5):203–211.
[19] Joe, M. Milton, and B. Ramakrishnan. "Review of vehicular ad hoc network communication models including WVANET (Web VANET) model and WVANET future research directions." *Wireless networks* (2015): 22 (7), PP: 2369-2386..