Similarity and self-learning based anti-Trojan Mechanism

Yiying Zhang[1, a], Yeshen He[2], Qing Zhao[1] and Kun Liang[1]

[1]*College of Computer Science and Information Engineering, Tianjin University of Science & Technology, Tianjin, 300222, China*
[2]*CHINA GRIDCOM CO,.LTD ,Shenzhen ,Guangdong, 518031,China*

Abstract. Trojans inject systems and launch various attacks, such as eavesdropping secret information, tampering with system configuration etc., which threats to system security seriously. In this paper, a novel anti-Trojan malware mechanism was proposed based on attribute behaviour and cosine similarity. Firstly, according to the initial rules base and application behaviour, the mechanism regularized the operations of application, and then, the mechanism invoked rules to judges suspicious behaviours based on current rules base and operational impact. Once the application was considered as Trojan malware, the system would dispatch the appropriate algorithm for processing. The mechanism triggered by sensitive behaviours, and had the active prevention function and self-learning function. The analysis and experiment show the solution can detect Trojan malware effectively.

Keywords: anti-trojan mechanism; security; trojan attack; self-learning mechanism.

1 Introduction

Trojans in the computer field refers to a backdoor program, usually including server and the client. Trojans embeds the host object into the server through the camouflage and hidden, which obtain and control the user's computer or network resources, and use abnormal means to cheat the normal rights, in order to steal user information, privacy information and other data.

The National Computer Virus Emergency Response Centre (CVERC) has issued the investigation and analysis report, which indicated that Chinese computer virus infection rate was 45.07% in 2012, the proportion of spread the virus through web browser or download is 75.42%, in which the computer software such as Trojans and other malware infection event is 56.68%[1].

Trojans is embedded in the target host, so that the host user faces all kinds of threats. It caused by the user password or account theft, remote control, system (or network) efficiency drop, the browser modified and other serious consequences.

In this paper, we deeply analyzed the principle and operation mechanism about Trojans. Combining the advantages of static analysis and dynamic analysis, we propose a Trojan detection technology and methods based on behavior analysis.

[a] Corresponding author : yiyingzhang@tust.edu.cn

2 Background

Trojans usually have strongly secrecy. It started by binding the network, operation system or some applications. It induces the user to activate by means of deception and camouflage, and then provides the attacker with unauthorized computer or network resources, so that the attacker can obtain the relevant resources illegally.

2.1 Types of Trojans

With the development of operation system platform and algorithm technology, Trojans transmission and production have changed seriously. Trojans can be divided into the following types according to the behaviours and influences [7].

• System control type. Once this Trojans is able to invade system and access to part of the system permissions successfully, the control of partial functions of the system can be realized.

• Data destruction type. This Trojans targeted for the implementation of data destruction. Once the invasion is successful, it will scan and acquisition system related data resources to destroy the data.

• Information-stealing type. This Trojans generally carries out hidden attacking by scanning the system and acquiring interested data, and implement further attacks after the theft.

2.2 The properties of Trojans

At present, there are many types of Trojans, which exist in different kinds of systems. They perform different attacks according to different computer systems. Various types of Trojans have many common attributes. It mainly includes :

1) Concealment [3]

As a spy program, concealment is the most basic feature of Trojans. It usually includes two kinds of hidden ways: Communication hiding and Local hiding.

Communication hiding mainly includes communication information, network traffic, port number, communication channel, etc. Local hiding mainly includes file hiding, process hiding, Rootkit hiding, compiler hiding, encryption , etc.

2) Deceptive [6]

Trojans often disguise as an available application or attractive document, such as pictures, software, games, functional documents, etc. When users use or download, they actually download the Trojans program or the software bundled with Trojans.

3) Auto-start

Trojans must be able to auto-start on the host computer. One way is to start with the system automatically through modified the startup items such as the registry. The other way is to bind the system programs or other applications, or to replace the key file by changing the name. For example, Troy DLL will register Trojan DLL as Windows system process Svchost services in order to realize the self-starting.

4) Self-protection

In order to ensure the robustness, Trojans can set up their own protection process to achieve the self-protection. The process often includes backup, restore, process restart and so on.

2.3 Operation mechanism

Trojans belongs to Non-replicating virus, which generally uses C/S (Client/Server) mode to realize attacks. The client is deployed on a machine that implement attacks (the controlling end), which is responsible for managing and controlling the controlled side; However, the server runs on a captured computer in a hidden way (the controlled side), to receive the control command from the controlling end to implement attacks.

2.4 Trojans detection technology

Because of Trojans has variety of hiding technology and use system vulnerabilities, it is not only acquired system control permissions easily, but also escaped the routine examination from users and general tools. Trojans detection technology mainly analysed various Trojans attack mechanism and proposes detection scheme and solutions. It includes:

• Network monitoring technology, which through monitoring the port or network connection to inspect Trojans attack behaviour, including the firewall, the intrusion detection technology and so on.

• Integrity monitoring technology, which through checking the system file or directory content or attributes to compare consistent with a trusted version to find whether there is Trojan attacks;

• Signature scanning technology, which uses Trojans attribute code or attribute values (usually is binary strings) as the basis for scanning. Because the attribute code is the only identification of the Trojans, this technology for existing Trojan works well. A lot of real-time scanning tools such as 360 and Rising use this technology for virus protection, but this technology belongs to passive anti-virus that is Hysteresis [5];

• Virtual machine technology established an independent operating environment by virtualization software, which tested the running task to detect the Trojans;

• Behaviour analysis technology is a proactive defense technology. According to Trojans' own attributes and attack principles, by using heuristic methods to detecting and analysing malicious behaviour, finally it achieved Trojans monitoring.

3 Trojans detection

For Trojan attributes, this paper through the attribute code technology and behavior analysis technology, established the relevance to Trojan attributes and malicious behavior, used cosine similarity to correlation analysis. We proposed a Trojans monitoring model based on behavior analysis, and building the Trojans behavior rules library. By the similarity determination algorithm, it will comb Trojans malicious behavior, to achieve the effective detection of Trojans.

3.1 System model

Trojans detection model based on behavior analysis is mainly composed of three parts, as shown in Figure 1.

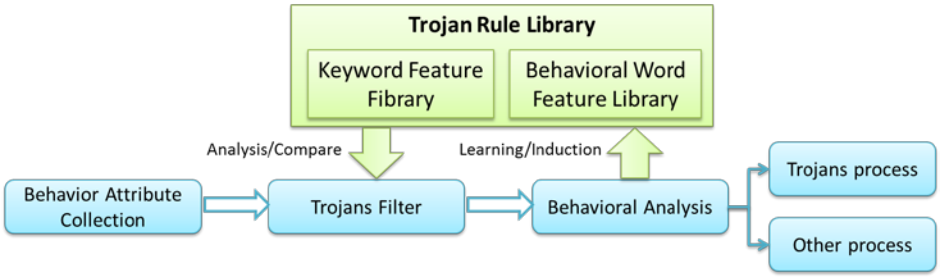

Figure 1. Trojan Detection Model

• Trojans rule library is established by known Trojans attribute code and attribute behavior. The initial Trojans rule library was used for reference and further study to add new rules.

• Behavior Attribute Collection used the data mining and statistical algorithms to catch the possible acts and establish the rules.

• Trojans Filter analysed capture process about behavioural attributes [8]. Firstly, according to the current rules library for evaluation, if there are rules matching with the rule library, it can be directly determined as a Trojans. Otherwise, according to the mining and classification algorithm for further determination to get the results related to processing.

3.2 Behaviour collection

According to the attributes of Trojans, the application process is monitored by the monitoring process to collect the process action. In particular, Trojans commonly used Hook of API process. In view of the hotspot information, we layout the monitoring points and collect the action, such as the access to the registry, the self-starting, the system key, the system authority, the important document, etc. as shown in Figure 2.

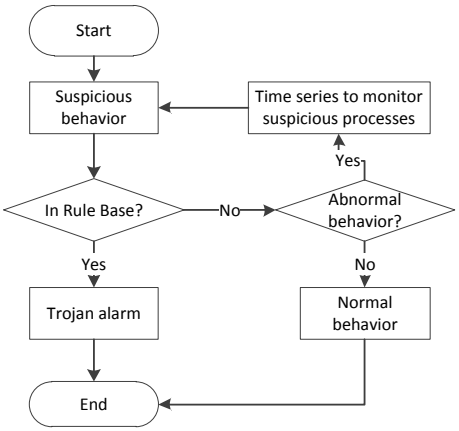

Figure 2. Trojan Detection Analysis

3.3 Behavior attributes

According to the collection for behavioral attributes, reference Trojan rule base comparative analysis [4]. Set up a series of rules for the target process behavior set is R= {r_1,r_2,…,r_n}, where r_i is the rule of a certain attribute, r_i.act for the attribute behavior; r_i.key is the feature key; r_i.weight is the characterized behavior right weight. Set Trojan rule library as D= {R_1,R_2,…,R_m}, wherein, R_i is already existing features. Set T as defined attribute behavior of reference (based on time correlation attacks, new attack is usually associated with the most recent attack, so the default value for the selected time on the latest R_i); weight i is the weight T behavior (including signature and behavior attributes); threshold is the similarity threshold, whose value is calculated as follows:

$$T.Weight = \frac{\sum_{i=1}^{|T|} T.r_i.weight}{|T|}$$
$$threshold = \sqrt{\sum_{i=1}^{|D|} .(D.R_i.weight - T.weight)^2} \quad (1)$$

Formula (2) is for the KNN (k-Nearest Neighbour algorithm) analysing function [4,5,10], by the judgment, the objectives of the review process R Meets unconventional (Trojan) attribute behaviour.

$$\mathrm{Sim}(R,T) = \frac{\sum_{i=1}^{|T|} R.weight \times weight_i}{\sqrt{(\sum_{i=1}^{|T|} R.weight^2)} \times \sqrt{(\sum_{i=1}^{|T|} weight_i^2)}} \quad (2)$$

According to formula (1), behavioral attributes and analysis algorithms is as follow:

Algorithm 1 Behavior Analysis

(1) INPUT R

(2) **FOR EACH** $\mathbf{D}_i$ IN R{ // Traversal rule base; | D | Rules library rule number ;

(3) **IF** D_i.R.act = R.r.act **or** D_i.R.key=R.r.key **THEN** // Matched

(4) {break ;}

(5) **ELSE**{

(6) **IF** (Sim(R,T)≤ threshold) //Similarity of Behavioral attributes

(7) **THEN** {

(8) R is new type of Trojan ;

(9) D=D∪{R}.

(10) } **ELSE**{

(11) R is normal Behavior ;

(12) }}}

4 Security analysis

We used the attribute code and attribute behaviour algorithm on the basis of Trojans code, and used space-time clustering, according to the time call sequence, to make the behaviour rule and normalized quantization. Based on its attributes, the similarity analysis can capture the behaviour attributes in the initial stage of the Trojans attack, established the time series, and constantly evaluated it. With the running of the system, the self-learning function will gradually improve the content in Trojans virus rule library. This makes the model self-similar, accurate, intelligent and real-time to be higher and higher.

However, according to the Uncertainty principle [11], Because of the particularity of the Trojans virus and the similarity of some application functions, the 100% accuracy can not be reached. Trojans detection problem cannot be met in polynomial time. Only through continuous training to improve the accuracy of the test analysis model. By judging algorithm can achieve higher accuracy of the monitoring and early warning.

Running test Trojans sample program on a virtual machine, This method can be used to study and detect the attribute code and attribute behaviour effectively. Especially for Trojan variant, when the attribute behaviour is normalized effectively, it can greatly improve the speed and accuracy of detection.

5 Conclusion

This paper presents a similarity determination algorithm based on data mining technology, and ensure the effect of this method from three aspects. Firstly, we established the initial rule library of Trojans according to the attribute code and behaviour. Secondly, we established a behavior attribute capture and analysis process to quantify the process attribute, and used Clustering analysis to rule of attribute behavior. Finally, Through the comparison of the rule base and the similarity comparison method, the analysis and comparison of the suspicious process is completed to determine its nature. The security analysis and experimental testing indicate that this algorithm is self-learning and active defense, It nicely balances the advantages and disadvantages of static and dynamic testing technology.

References

1. National Computer Virus Emergency Response Center. Twelfth National information network security and computer virus outbreak investigation and mobile terminal analysis report. http://www.antivirus-china.org.cn, (2013)
2. Lin C. Technology of Hacker's Attack Based on Trojan. Computer Knowledge & Technology, (2008).
3. Chen Z, Tao Y, Li G. A Method for Detecting Trojan Based on Hidden Network Traffic Analysis, Applications and Techniques in Information Security. Springer Berlin Heidelberg, 2014:65-72.
4. Wen F U, Wei B, Zhao R C, et al. Fuzzy reasoning model for analysis of program maliciousness, Journal on Communications, **31**(1):44-50, (2010).
5. Duarte L M. Behavior Model Extraction from Software, Theoretical Computer Science. IEEE, 2013:1-8.
6. Li-Jun M A. Detection Research on Behavior-based Detection of Theft-type Trojan. Journal of Guangxi University for Nationalities, (2014).
7. Liu D. Analysis on hiding technologies of Trojan horse. China Science and Technology Information,**1**(1):112~113, (2010)
8. Shi Y, Peng X, Zhang W, et al. A chaotic characteristics identification method for network security situation time series, Journal of Information & Computational Science, **9**(5):1309-1319, (2012).
9. Ji Y. The Mechanism, detection and defense of Botnet based on webpage Trojan, Network Security Technology & Application, (2013).
10. NirmalaDevi M, Appavu alias B S, Swathi U V. An amalgam KNN to predict diabetes mellitus, Proc of International Conference on Emerging Trends in Computing, Communication and Nanotechnology. 691-695(2013).
11. Hong-Jun H E, Luo L, Dong L M, et al. Formal Definition of Generalized Virus and Its Identifying Algorithm: Formal Definition of Generalized Virus and Its Identifying Algorithm, Chinese Journal of Computers, **33**(3):562-568, (2010).