Trojan Behavior Analysis Based on FAHP Improved Algorithms

Hongliang LIU[1, 2, b], Chunguang MA[1, a], Chao LIU[2], Min YU[2]

[1]Harbin Engineering University, Harbin, 150001, China

[2]Chinese Academy of Sciences, Beijing, 100195, China

[a]email: machunguang@hrbeu.edu.cn

[b]email: liuhongliang24@163.com

Keywords: FAHP Improved Algorithms; Trojan Behavior; Behavior Modeling; Security Analysis

Abstract. In the paper, we modelling for behavior of Trojan based on fuzzy analytic hierarchy process (FAHP) improved algorithms, an efficacious analysis method which good at behavioral assessment, and has been applied in many fields of malicious code analysis. Based on the model, the harmfulness of software behavior between Trojan software and application software is analyzed quantitatively. Different by different Trojans corresponding behavior of hazardous different premise, judge the harmfulness of Trojan. Numerical analysis results demonstrate that the improved algorithms gain good effect. Compared with the results obtained by other methods, the conclusion of this paper is reliable and practical, and it has opened up a new situation for the work of judging Trojan.

Introduction

With the development and popularization of network technology, the network has entered people's lives, whether it is government agencies, secret department or individuals closely linked. However, the resulting security issues have become increasingly serious, especially the most serious dangers are Trojans, and the proportion is the highest [1, 2]. According to the National Computer Virus Emergency Treatment Center in June 2015 released the "Fourteenth National Information Network Security Situation and computer and mobile terminal virus epidemic survey analysis report" pointed out that: in 2013, the computer virus infection rate in China was 63.7%, in 2013 rose by 8.8%, in 2012 fell to the lowest point, then a continuous rise of two years up. In the newly added malware, Trojans accounted for 54.7%, followed by the back door and spyware. Therefore, the detection and analysis of Trojan horse should get more attention and research. However, at present the analysis and evaluation of the Trojan horse is relatively little, only to understand the work characteristics and the work principle of the Trojan and the degree of endanger to better prevention and control the Trojan horse [3].

Today, both domestic and foreign, in the detection and defense software of Trojan, the static feature of the contrast is still occupy a major position. Evaluate the harm of a Trojan mainly rely on the program known MD5 value to determine the harmfulness of the program [4]. Application of MD5 signature matching technology in clouds is also becoming more and more common [5]. A wide range of applications, including virtual machine detection technology, peeled to spend technology, reverse analysis, behavioral characteristics and classification methods for detecting Trojans [6]. With the improvement of computer technology, anti-Trojan technology is constantly improving, hackers continue to break all kinds of detection technology, they use the methods of anti-virtual machine, homologous variation, confusion [7], etc. Continue to break the major software for detecting Trojans. At present, there are three main research methods for the analysis of the Trojan: M. Schultz, who first proposed the naive Bayes algorithm to detect unknown malicious code, the algorithm is based on a static analysis of the program, they direct the selection program machine code, ASCII strings of the programs and analysis the PE program to obtain a reference sequence of API to be the feature vectors as the sample programs, each algorithm using this as a basis for learning and classification.[8], introduced immune algorithm into the computer system, and Forrest in the University of New Mexico,

who use the immune system to detect the abnormal changes in the program and the protected data, have a greater impact on the anti-virus and host intrusion detection research. The experimental results show that this method can easily find the Trojan infection caused by the change of the data file, and also can detect unknown Trojan. Virus Research Center at IBM, successfully neural network used to determine the boot virus, Shanghai Antiy Labs are unknown virus advocate assessment techniques, the successful use of neural network back-propagation training algorithm (BP algorithm) Construction anti-Trojan models. This technology is being gradually applied to the practical application of the sorting process Arrent-NET to capture suspicious files [9].

This article will judge the harm degree of computer Trojan program. Researching the damages to the computer and personal which caused by the Trojan program, in order to carry out more targeted detection and prevention. The chief contributions of this paper contain three aspects, first, this method breaks the traditional binary research, that is not entirely black or white, but the result is a curve, it will be more refined as a result of a variety of grades. Secondly, through the behavioral characteristics of the study program, calculate the dangers arisen, thus to solve signature analysis can't detect unknown Trojans deficiencies. Finally, we analyze some software characteristics of Trojan on the basis of the method presentation above, which show in the end of paper.

The remainder of the paper is as follows: in section II, we give a concise introduction relating the background knowledge. Section III describes our research model. Section IV analyzes the experimental results obtained from our model system. Section V gives the conclusion and aspects need to be improved in the future.

Preliminaries

Trojan behavior analysis.

Today, the detection and analysis of Trojan rely on the simple static characteristic code can't realize detection and prevention Trojan horse, but more rely on the analysis of the behavior characteristics of the Trojan horse. That is to say detection of their behavior in the application running process, analysis of whether the behavior of a Trojan horse. Although the purpose of the design of the Trojan horse is not the same, but, the running of the Trojan program has some common characteristics. According to the life cycle of Trojan horse, Trojan horse program can be divided into three stages, That is, the installation process, thread/process start process and communication process. Different stages have different behaviors, for example, the installation phase will generate the registry, open the file, the termination process, etc…In the same way, the other two stages will produce the corresponding behavior. Stages behavior are shown in table 1:

According to the specific behavior that different from normal programs behavior generated by the Trojans, and there is a certain sequence of features. By analyzing the behavior, the characteristics and harm degree of different Trojan horses can be judged.

Fuzzy analytic hierarchy process(FAHP).

Fuzzy analytic hierarchy process is applied to the theory of fuzzy mathematics to the analytic hierarchy process. It sets the fuzzy mathematics, the hierarchical organization, the weight is compared in one body, in the decision-making science occupies an important position. This paper introduces FAHP to fuzzy processing the Trojan behavior and quantitative analysis. The advantages of FAHP for AHP are reflected in the fuzzy characteristics of the matrix, to some extent it simplifies the complexity of the relative importance in the determination of the target, and the effective use of fuzzy judgment matrix to realize the decision-making from qualitative to quantitative and convenient and quick transformation, the structure of fuzzy judgment matrix can solve the consistency problem of the judgment matrix[10]. The working procedure of FAHP is to establish the hierarchy structure (As shown in Figure 2), constructing triangular fuzzy number reciprocal judgment matrix, fuzzy weight calculation of single level factor, build a possibility degree matrix, calculate the sort vector of the probability degree matrix, finally, the overall hierarchy sorting.

Table 1, factor information table of the criteria layer

Target Layer	Criterion Layer 1	Criterion Layer 2	Criterion Layer 3
Target Layer	Installation Procedure	Hidden Trojan Program (B1)	Copy Files (C1)
			Create Files (C2)
		Trojan Server Auto start Settings (B2)	Open the Registry (C3)
			Read and Write the Registry (C4)
			Close the Registry (C5)
			Open the File (C6)
			Read and Write the File (C7)
			Close the File (C8)
		Killing other Processes (B3)	Find the Specified Window (C9)
			Send VM_CLOSE to the Specified Window(C10)
			Obtain the Snapshot of all Processes (C11)
			Traverse the Snapshot and Find the Corresponding ID (C12)
			Obtain the Process Handle (C13)
			Terminate Processes (C14)
	Thread/ Process Startup Procedure	Hidden Process (B4)	Startup Service Control Dispenser (C15)
			Register Service Control Processor (C16)
			Set Service Status Information (C17)
			Open the Current Process Access Signaling and Require the Permission to Change Access (C18)
			Lookup Permissions in the Local System and Require the Permission to debug process (C19)
			Assign Access Permissions (C20)
			Activate Access Permissions (C21)
			Take a Process PID, Allocate Memory Space and Write Data in the Process (C22)
			Startup Remote Threads (C23)
			Replace the System DLL (C24)
			Intercept to View the Current Process API (C25)
			Install the Custom Transport Server Provider to the Forefront of the Service Provider Database (C26)
	Communication Procedure	Not Hidden Port (B5)	Create a Socket and Connect Clients (C27)
			Bind a Port and Set to the Listening State (C28)
			Receive Client Network Connection (C29)
		Hidden Port (B6)	Created Raw Sockets Used ICMP (C30)

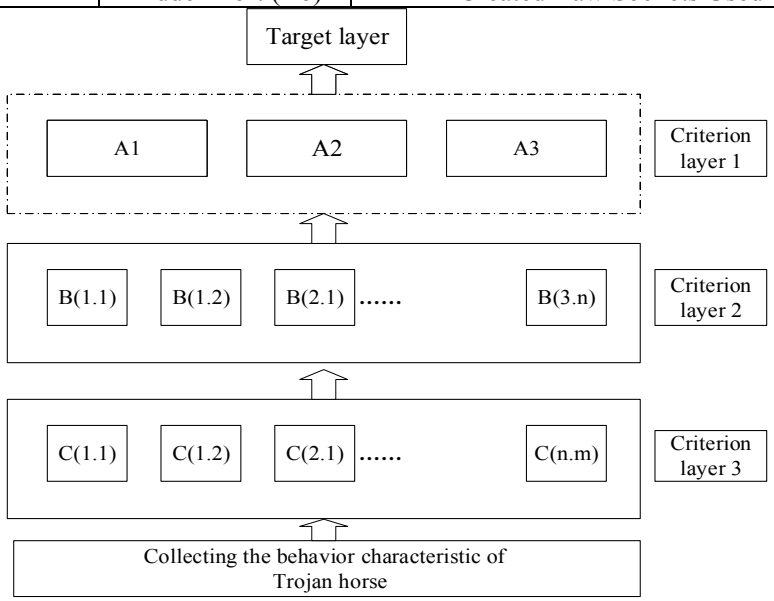

Figure2 Hierarchical structure diagram

Make the behavior characteristic of the Trojan horse program is matched with the fuzzy hierarchy structure. Target layer for Trojan program, Criterion layer 1 is the three stages of the life cycle of the Trojan program, criteria layer 2 is the factor that is contained in the implementation of the Criteria layer 1, in the same way, criterion layer 3 is the factors to realize the Criterion layer 2. According to the analysis of a large number of Trojans, sorting and classifying the behavior of the Trojan horse, to establish the information table as shown in table 1.

The model of Trojan harm evaluation

The purpose of the establishment of a hierarchical structure model is to establish the evaluation index system which based on the behavior characteristics on the basis of in-depth analysis of the practical problems, including target layer, criterion layer and index layer. Among them, the target layer is the ultimate goal for discuss the problem. The criterion layer is the criterion that affects the realization of the target. The index layer is the measure to promote the goal, this paper refers to the behavior characteristics of different Trojans. A number of factors in the same layer are belong to upper level or influenced by the upper level. At the same time, it also dominates the underlying factors or effected by the underlying factors.

Reciprocal judgment matrix. The function of the judgment matrix is a comparison that between the relative importance of the same level elements in the constraints of the upper layer. The judgment matrix is obtained by using the fuzzy DELPHI method, assuming triangular fuzzy complementary judgment matrix

$$\tilde{A} = (\tilde{a}_{ij})_{n\times n}, \quad (1)$$

in which, $\tilde{a}_{ij} = (l_{ij}, m_{ij}, \mu_{ij}), \tilde{a}_{ji} = (l_{ji}, m_{ji}, \mu_{ji}),$ (2)

and $l_{ij} + \mu_{ij} = m_{ij} + m_{ji} = \mu_{ij} + l_{ij} = 1, \mu_{ij} \geq m_{ij} \geq l_{ij}, i, j \in N$. (3)

In which, $\tilde{a}_{ij}$ means the factor i and factor j of the judgment matrix ratio of the important degree. If there are t experts to scoring, through every element of comprehensive judgment matrix can be calculated by the following formula: :

$$\tilde{a}_{ij} = \frac{1}{t} \otimes [\tilde{a}_{ij}^{(1)} \otimes \tilde{a}_{ij}^{(2)} \otimes \tilde{a}_{ij}^{(t)}], \quad (4)$$

in which, a_{ij} means the j elements of the i row of the judgment matrix, $\tilde{a}_{ij}^{(t)}$ means the t expert have given the j elements of the i row, and because of the complementary nature of the judgment matrix, so, $\tilde{a}_{ij} + \tilde{a}_{ji} = 1$. (5)

By experts scoring, the important degree of each layer factor is compared by two by two, and using the triangular fuzzy number to express it. Assume, $\tilde{a}_{ij} = (l_{ij}, m_{ij}, \mu_{ij})$ is a triangular fuzzy number, means expressed in a certain condition, degree of membership for factor χi compared with χj "… is more important than …" l_{ij}, m_{ij}, μ_{ij} mean the factors of M and N relative to the upper layer factors when comparing expert scoring the lowest, the most suitable, the highest estimate. Table 2 gives the triangular fuzzy number scale.

Table 2, the triangular fuzzy number scale.

Scale	Implication
0.9	Comparing the two factors, the former is absolutely more important than the latter
0.8	Comparing the two factors, the former is strongly more important than the latter
0.7	Comparing the two factors, the former is obviously more important than the latter
0.6	Comparing the two factors, the former is slightly more important than the latter
0.5	Comparing the two factors, the former is as important as the latter
0.1—0.4	Trans comparison, that is, if the result of comparison x_i and x_j is a_{ij}, then the result of comparison x_j and x_i is $a_{ji} = 1 - a_{ij}$

Build a possibility degree matrix.

If you want to get the weight of all the factors relative to the target layer, first of all should find out the weight of each single factor. The single hierarchy factor refers to the same hierarchy of the corresponding elements of a factor relative to the hierarchy of a factor of the relative importance of the sort, this process is called a single hierarchy ranking. Suppose that the number of factors relative to the upper layer is n, and it could be obtained by the following formula for the i factor of the triangular fuzzy number weight vector with respect to the upper layer factor.

$$\tilde{\omega}_i = \frac{\sum_{j=1}^{n} \tilde{a}_{ij}}{\sum_{i=1}^{n}\sum_{j=1}^{n} \tilde{a}_{ij}} = \frac{\left(\sum_{j=1}^{n} l_{ij}, \sum_{j=1}^{n} m_{ij}, \sum_{j=1}^{n} \mu_{ij}\right)}{\left(\sum_{i=1}^{n}\sum_{j=1}^{n} l_{ij}, \sum_{i=1}^{n}\sum_{j=1}^{n} m_{ij}, \sum_{i=1}^{n}\sum_{j=1}^{n} \mu_{ij}\right)} = \left(\frac{\sum_{j=1}^{n} l_{ij}}{\sum_{i=1}^{n}\sum_{j=1}^{n} \mu_{ij}}, \frac{\sum_{j=1}^{n} m_{ij}}{\sum_{i=1}^{n}\sum_{j=1}^{n} m_{ij}}, \frac{\sum_{j=1}^{n} \mu_{ij}}{\sum_{i=1}^{n}\sum_{j=1}^{n} l_{ij}}\right), i = 1, 2, \ldots, n$$

Because of the triangular fuzzy weights are not the fully explicit state which required for the target factor weight information, so we use a possible degree method to deal with the $\tilde{\omega}_i (i \in N)$ comparison of triangular fuzzy number $\tilde{\omega}_1$ with two by two.

Suppose $\tilde{a} = (a_l, a_m, a_n), \tilde{b} = (b_l, b_m, b_n)$, then the possibility degree of $\tilde{a} \geq \tilde{b}$ is

$$P\left(\tilde{a} \geq \tilde{b}\right) = \lambda \max\left\{1 - \max\left\{\frac{b_m - a_l}{a_m - a_l + b_n - b_l}, 0\right\}, 0\right\} + (1 - \lambda)\max\left\{1 - \max\left\{\frac{b_n - a_m}{a_n - a_m + b_n - b_m}, 0\right\}, 0\right\}, \quad (6)$$

among than $a_i, b_j, \lambda \in [0,1], i, j \in N$.

When λ>0.5, call the decision maker is risk seeking; When λ=0.5, call the decision maker is risk neutral; When λ<0.5, call the decision makers are to avoid the risk. (This paper chooses to take 0.5)

The overall hierarchy sorting.

On the probability degree of the previous step $P_{ij}(\omega_i \geq \omega_j), i, j \in N$, thereby establishing the possibility matrix $P = (P_{ij})_{n \times n}$. Then, the sort of triangular fuzzy number is converted to the sort vector of the possible degree matrix. First, transform the probability matrix into a fuzzy consistency matrix, the formula is as follows:

Suppose $r_i = \sum_{k=1}^{n} P_{ik}, i = 1, 2, 3 \ldots n$. Calculate

$$r_{ij} = \frac{r_i - r_j}{2(n-1)} + 0.5 \quad (7)$$

Thus the fuzzy judgment matrix is obtained. $R = (r_{ij})_{n \times n}$. Finally, the sorting vector of probability degree matrix is obtained by using the following formula.

$$V_i = \frac{\sum_{j=1}^{n} r_{ij} + \frac{n}{2} - 1}{n(n-1)}. \quad (8)$$

The overall sorting is the relative weight of each factor to the target layer. Calculate the lower hierarchy factor combination weight vector of the target layer.

Assume that the upper level contains the M factor, their overall ranking weights are $a_1, a_2, a_3, \ldots a_m$, and the next layer contains N factor, they are about a factor in the A layer of the hierarchical sort of weights are $b_{1j}, b_{2j}, b_{3j}, \ldots, b_{nj}$ ($b_{1j} = 0$ when there is no correlation between two factors). The weight of each factor of the B layer that for the overall layer is calculated according to the following formula $b_i = \sum_{j=1}^{m} b_{ij} a_j, i = 1, 2, 3, \ldots, n$.

Evaluation of the Trojan program.

We first construct judgment matrix which is criterion layer 1 with respect to the target layer, the results are calculated by MATLAB. Then set up the evaluation set, defined it as 5 levels (High risk, serious, dangerous, dangerous, normal). According to the weight of the front factors, and the occurrence frequency of the behavior characteristics of different schemes (frequent, occasionally, less), the results will obtained by calculation.

Evaluation and Analysis

Obtain the maximum eigenvalue λ_{max}, then calculating consistency index CR, the inspection formula of judging the consistency of the matrix is $CR = \frac{CI}{RI}$, calculate to get weight that after normalized treatment. Consistency check and correction, to determine whether passed the consistency check. This paper adopts a solution that is to continuously offer information to experts to helpfully make consistent judgments, at the same time, to help experts to improve the ability of the consistency of the logical judgment, continuously reduce the inconsistency of judgment. Specific steps are as follows:

a. Experts according to their own experience and understanding of the behavior of the program, given the initial judgment matrix P_0;

b. Using P_{1j} and $P_{(j+1}$ of the P_0, using the transfer relationship $P_{ij} = P_{ik} - P_{jk} + 0.5$ to generate P_1 and P_2.

c. If $P_0 = P_1 = P_2$, then it success. Otherwise analysis the conclusion of P_1 and P_2, point out inconsistencies, tell the expert, re validation;

d. Let the judgment matrix is P_0 which corrected by experts.

According to the expert scoring, giving the lowest intention, moderate intention, and the highest intention of different factors. According to the above method, the weight and the ranking vector of the upper layer are shown in Table 3.

Table 3, criteria layer 3 judgment matrix and weight

	Installation Procedure	Thread/ Process Startup Procedure	Communication Procedure	Weight
Installation Procedure	(0.5,0.5,0.5)	(0.5,0.7,0.8）	(0.4,0.5,0.7)	(0.25926,0.37778,0.70588)
Thread/ Process Startup Procedure	(0.2,0.3,0.5)	(0.5,0.5,0.5)	(0.3,0.4,0.6)	(0.18519,0.26667,0.44444)
Communication Procedure	(0.3,0.5,0.6)	(0.4,0.6,0.7)	(0.5,0.5,0.5)	(0.22222,0.35556,0.50000)

Through the third chapter formula calculation criterion layer 1 of the possible matrix such as table 4:

Table 4, the possible degree matrix of the criterion layer 1

Installation Procedure	Thread/ Process Startup Procedure	Communication Procedure
0.50000	0.88773	0.61917
0.11227	0.50000	0.24138
0.38038	0.75862	0.50000

In the same way, the weight of the 3 and the standard layer 2 can be obtained. By the calculation of the criteria layer, the total order is obtained, such as table 5:

Table 5, the overall hierarchy sorting

Characteristics of behavior	Weight	Characteristics of behavior	Weight
C1	0.15926	C16	0.17495
C2	0.01158	C17	0.17774
C3	0.08317	C18	0.25469
C4	0.14673	C19	0.18842
C5	0.02128	C20	0.18911
C6	0.08404	C21	0.18113
C7	0.16773	C22	0.15338
C8	0.07965	C23	0.17716
C9	0.06046	C24	0.26061
C10	0.14399	C25	0.25516

C11	0.24618	C26	0.24319
C12	0.16882	C27	0.17594
C13	0.02871	C28	0.23591
C14	0.17437	C29	0.17485
C15	0.18172	C30	0.20416

Analysis of the results of the Trojan case.

The evaluation scores and threat levels of several Trojan horses and normal programs are calculated according to the weight ratio analysis, which according to the characteristics of the Trojan horse to score, occur frequently recorded as 3 points, and occasionally recorded as 2 points, less recorded as 1 points. According to expert opinion, through the investigation of a large number of Trojans [11]. To develop a Trojan horse hazard rating table 6.

Table 6, hazard rating scale

Damage score	-2.4	2.4-4.0	4.0-6.0	6.0-8.0	8.0-14.4
Damage level	Normal	A bit dangerous	Dangerous	Serious	High-risk

According to the characteristics of the occurrence frequency and the weight of the corresponding features are calculated in Table 7 shows the results.

Table 7, examples of the evaluation of the Trojan horse

	Program	Main activity	Damage score	Damage level
Trojan program	GameThief.Win32. Magania.dlip	Steal a variety of game account information , Prevent security software, etc.	6.957	Serious
	Trojan-Downloader.Win32 . Nurech.bg	Download and run malicious software , Prevent security software, etc.	7.718	Serious
	Dropper.Win32.Delf.grq	Release Trojans, Fake windows, Theft of information, etc.	8.857	High-risk
	Banker.Win32.Delf.bz	Fake windows, Cheat information, etc.	7.629	Serious
	Mailfinder.Win32. MagPlayer.a	Collect e-mail addresses, etc.	5.984	Dangerous
	Backdoor.Assasin.20	Disguise windows, Tampering information, Theft of information, etc.	11.084	High-risk
	Trojan.Azrad	Terminate processes, Modify the registry and system services, etc.	9.032	High-risk
	Sub-Seven	Redirect the port, Modify the registry, etc.	8.937	High-risk
	Backdoor.Huigezi. ao.Installer	Intercept API, Modify the registry, Start automatically, etc.	10.132	High-risk
	byshell	Injection DLL, DLL mapping, Delete their own files, etc.	9.028	High-risk
Normal program	regedit.exe	Open the registry, Read and write the registry, Close the registry, etc.	1.482	Normal
	Lock Down 2000.exe	Monitor software processes, etc.	1.403	Normal
	koomail.exe	Open ports, Send data, etc.	1.006	Normal
	system moniter.exe	Monitor system process, etc.	0.767	Normal
	QQ.exe	Create files, Port communicate, etc.	1.424	Normal
	winrar.exe	Open files, Modify files, etc.	1.188	Normal

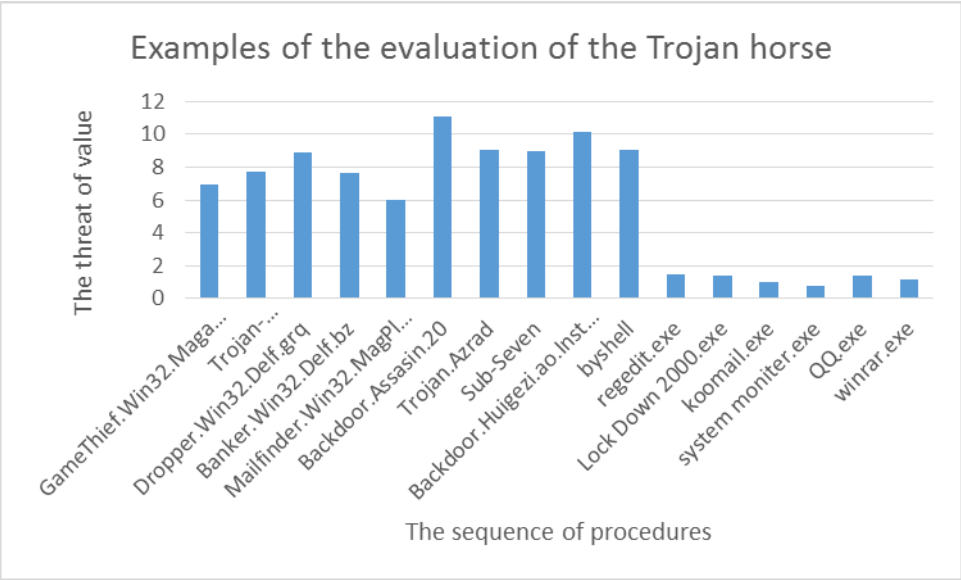

Figure 3 Analysis result of examples

The evaluation results show that the threat level of the Trojan horse, "Backdoor.Assasin.20", "Backdoor.Huigezi.ao. Installer" and other Trojan programs are at high risk. The type of Trojan hacking harm rating is serious, such as Game Thief [12]. In addition, the analysis of several normal software, the results show that the normal range. According to the lifetime of the Trojan, according to the characteristics of behavior which produced at installation procedure, thread/ process startup procedure and communication procedure. According to the fuzzy analytic hierarchy process, divide the behavior of the Trojan program into levels. For different stages of the behavior, the weights are calculated respectively. The hierarchy total sorting is calculated by the weight of overall hierarchy, the weights of all the behaviors of a Trojan horse program are obtained. Finally, judge a variety of Trojans, according to the behavior of the factors, and the ultimate hazard score for a behavior dependent or frequency calculation program, dividing the harm degree. Because of the programs above have different behavior characteristics, which has the more dangers behaviors has scores more points. At last, the results show the same results as the experts.

Summary

In the paper, we construct a FAHP model to assessment the harmfulness of software. By utilizing FAHP improved algorithms, it is easily to get the value of software behaviors. Based on above, it is conveniently to obtain the relationship between Trojan software and application software, which can provide some reference to determine whether a Trojan horse. The malicious documents behavior analysis is what we will to explore in the stage.

Acknowledgement

This work is supported by National Natural Science Foundation of China (No. 61170241, No. 61472097), Young Scholar Foundation of Institute (No. 1104005704).

References

[1] Fred Cohen. Computer Viruses-Theory and Experiments [J]. Top-Help (1984)

[2] GONG Zaiwu, LIN Yi, YAO Tianxiang. Uncertain fuzzy preference relations and their applications [M]. New York: Springer-Verlag, 2013:45-74.

[3] GONG Zaiwu, LIN Yi, YAO Tianxiang. Uncertain fuzzy preference relations and their applications [M]. New York: Springer-Verlag, 2013:45-74.

[4] Chess D. The Future of Viruses on the internet[OL].http://www.researeh.ibm.eom/antivirus/ SciPapers/Chess/Future.html

[5] Dr. Atta ur Rahman. User behaviour classification using Fuzzy Rule Based System. MIR Labs (USA), IEEE (Tunisia Section), 2013

[6] Ming Liu, Lansheng Han, Mengsong Zou, Qiwen Liu, "An Evaluating Model for Anti-virus Ability Based on AHP," 2009 International Conference on Computational Science and Engineering, August 29-August 31 2009 Vancouver, Canada, vol. 1, pp. 394-398,

[7] Atta-ur-rahman "Teacher Assessment and Profiling using Fuzzy Rule based System and Apriori Algorithm", international Journal of Computer Applications (IJCA), Vol. 65(5), pp. 22-28, March 2013

[8] D. A. Savic and W. Pedrycz. Evaluation of fuzzy linear regression made [J].Fuzzy Sets Systems, vol.39, pp.51-63. (2011)

[9] V. Chittraa, A. S. Thanamani, "Fuzzy Equivalent matrix for Discovering Pattern of Web users Navigation." international Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), vol. 2 (12), pp. 290-295. (2012)

[10] Subramanian N, Ramanathan R. A review of applications of analytic hierarchy process in operations management [J]. International Journal of Production Economics, 138 (2): 215-241. (2012)

[11] Liu D. Analysis on hiding technologies of Trojan horse. China Science and Technology Information, 2010, 1(1):112-113

[12] Kellogg, Lee, Ruttenberg, Brian; O'Connor, Alison; Howard, Michael; Pfeffer, Avi Source: Proceedings - 2014 IEEE International Conference on Big Data, IEEE Big Data 2014, p 666-674, January 7, 2015