Construction of Index System Based on Advanced Persistent Threat

Jia Lin[1], Rong Jiang[2], Yu-Lu Qi[3], Shu-Qiang Yang[4], Ai-Ping Li[5]

[1]*School of Computer National University of Defense Technology, Changsha, China*
[2]*School of Computer National University of Defense Technology, Changsha, China*
[3]*School of Computer National University of Defense Technology, Changsha, China*
[4]*School of Computer National University of Defense Technology, Changsha, China*
[5]*School of Computer National University of Defense Technology, Changsha, China*
1e-mail: linjia15@nudt.edu.cn

Abstract: With the proliferation of advanced persistent threat (APT), APT attack effect evaluation is playing an increasingly important role in cyberspace. As one of the hot issues of network security, the evaluation to its attack effect can quantify the harm caused by APT. Then according to the evaluation results, we can derive specific measures to the network attack. At present, a lot of work has done in the network attack effect evaluation index system. However, a significant barrier to the development of APT attack effect evaluation is that the existing index system is either from the point of view of the network security situation, or for a single attack weapons to customize. In this paper, an evaluation index system is proposed through analysing the features of APT. Through this index system, we can not only quantify APT attack effect, but also visually observe the APT ability from various angles. Then, we use the analytic hierarchy process (AHP) to model the evaluation process and calculate the weight of each indicator. Finally, the Ukrainian Power Outages is taken as an example to validate the proposed index system. The experimental results verify the effectiveness of the index system.

1. Introduction

With the rapid development of computer technology, the role of computer networks is more and more important. However, with the expansion of network size and the development of related technologies, the forms and means of cyber security threats are constantly changing. Network security has become a bottleneck restricting the development of social informatization.

Advanced Persistent Threat (APT) is one of the hot topics in the field of network security. APT means using of advanced means of attack on specific targets for long-term continuous attack on the form of network attacks. Almost all means of the network attacks can be applied to APT, so the defense of APT is still a difficult problem in the field of network security.

The assessment of the effectiveness of network attacks can be achieved on the quantification of network attacks, and giving reasonable recommendations according to the results. So as to achieve the purpose of active defense. Therefore, we establish an APT evaluation index system, and model the assessment based on the index system.

The remainder of this paper is organized as follows. In section 2, we briefly review relate works. In section 3, we propose an APT attack evaluation system and model it based on AHP. Then, in section 4 we take the Ukrainian Power Outages as an example to validated the validity of the model. Finally, we draw our conclusion in section 5.

2. Related Works

The construction of the evaluation index system of network attack is one of the hotspots of safety research at home and abroad. A lot of work has been done in index system at home and abroad.

Wang Juan et al. put forward 25 indicators from the perspective of the network situation [1]; Duan Bin et al. put forward a hierarchical worm hazard assessment index system from the perspective of the features of worms [2]. Wang Zhiping constructs a multi-level and multi-dimensional network security index system from 4 perspectives: basic operation dimension, fragile dimension, threat dimension and risk dimension [3]. Han Lansheng et al. proposed a set of three-level hazard evaluation index system for all computer virus [4]. Ai Peng puts forward a set of three-level network evaluation index system for all types of network attacks from the perspective of whether the systems, networks and services are normal or not [5].

The above research work, either from the perspective of the network situation, or only consider a single means of attack. Therefore, we propose an evaluation index system of APT from the perspective of composite attack.

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (http://creativecommons.org/licenses/by/4.0/).

3. Construction of Index System

In this section, we introduce APT and present the index system based on its features firstly. Then, we introduce the process of data normalization and index weight calculation.

3.1 About APT

For the definition of APT, there is no uniform standard. Generally, APT refers to the use of advanced means of attack on specific targets for long-term continuous attack on the from of network attacks. Its essence is a specific target for the precise attack. The term APT was originally originated in the 2005-2006, where network security engineers working with the Air Force described some of the security incidents. Some scholars believe that only those involving foreign organizations, directed against specific targets for long-term and deliberate attack is called APT. After the exposure of Google's Aurora operations in 2009, APT gradually spred in the media. Since then, all the delicate and persistent attacks are called APT. In recent years, security incidents related to APT are increasing. Fig. 1[6] shows the number of APT in recent years.

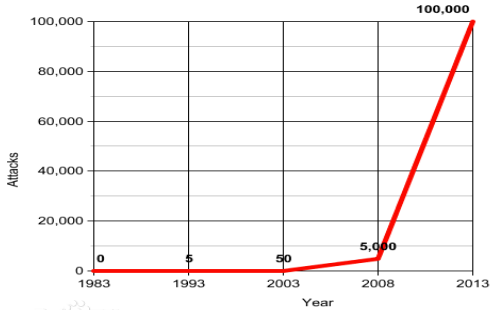

Figure 1. Number of APT

The concept of APT has 3 meanings:

Advanced: Attackers have the ability to evade detection, gain and maintain access to well-pretected networks and sensitive information systems. They usually have sufficient resources to attack.

Persistent: It is difficult to completely curbed APT and clear from the network system.

Threat: APT has both the ability and the intention to attack.

3.2 Evaluation Index System of APT

According to the definition of APT and its inherent features, we propose a complete index system, as shown in table I

Table1. Evaluation Index System of APT

U000 Attack Effect Evaluation of APT	U100 Persistent	U110 Attack Duration	/
		U120 Attack Frequency	/
	U200 Hiding Ability	U210 Static Hiding Ability	/
		U220 Dynamic Hiding Ability	U221 Load Hiding Ability
			U222 Run Hiding Ability
		U230 Communication Hiding Ability	U231 Communicti on Mode Hiding Ability
			U232 Communicati on Content Hiding Ability
	U300 Diffusibility	U310 Scale of Diffusion	U311 Number of Affected Machines
			U312 Highest Authority of the Affected Machines
		U320 Diffusion Ability	U321 Number of Infected Platforms
			U322 Dependency on User Behavior
			U323 Camouflage
			U324 Exploit Ability
	U400 Intractable	U410 Copy Ability	U411 Number of Static Copies
			U412 Number of Dynamic Copies
		U420 Recover Ability	U421 Static Recovery Capability
			U422 Dynamic Recovery Capability
		U430 Update Ability	/
	U500 Harmfulnes s	U510 Cause Paralysis Class	U511 Ability of Destruction
			U512 Duration of Destruction
		U520 Information Theft Class	U521 Value of Stealing Information

Description:

Persistent: Including not only the total duration of the attack, but also the attack frequency.

Hiding Ability: The probability of being detected and the clearance of the activity traces is complete or not.

Diffusibility: Including horizontal diffusion (scope of influence), vertical diffusion(rights) and methods of dissemination.

Intractable: Backup, complexity of clean and so on.

Harmfulness: Most of APT can be divided into paralysis class and information theft class by attack effect.

All indicators can be divided into consumption indicators and gain-type indicators. For gain-type indicators, the greater the index value is, the greater the valuation is; consumption indicators are the opposite. So set the consumption indicator value negative.

3.3 Calculation

In the evaluation of attack effectiveness, the calculation mainly includes data normalization and index weight calculation.

3.31 Data Normalization

Normalization, also known as quantification. Raw data often have different dimensions. Therefore, the raw data need to be normalized to eliminate the difference in dimensions. We divide the index into quantitative indicators and qualitative indicators. The normalization methods of qualitative indicators and quantitative indicators are not the same. Since data normalization is not the main work of this study, we briefly introduce the normalization of these two types of data.

3.32 Normalization of Quantitative Indicators

Quantitative indicators are assessment indicators that can be accurate quantitative definition, accurate measurement. Quantitative indicators are usually integer or floating-point values.

For the normalization of quantitative indicators, we use a linear normalization method. The normalized formula is:

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}}. \qquad (1)$$

In this formula, X is the value of the current indicator. X_{norm} is the value after normalization. X_{max} and X_{min} are respectively the maximum and minimum values of a certain range.

3.33 Normalization of Qualitative Indicators

Qualitative indicators refer to indicators that can not be directly analyzed and evaluated directly through data, and the objective of the evaluation is analyzed and analyzed to reflect the evaluation results.

In general, qualitative indicators can be classified into Boolean types and level types. For Boolean types, we can convert "True" to 1 and "False" to 0. For level types, the normalization is shown in table II.

Table2. Normalization of Qualitative Indicators

Disappointing	Acceptable	Moderate	Good	Outstanding
0.1	0.3	0.5	0.7	0.9

3.34 Weight Calculation

We use AHP to calculate the index weight. AHP is a systematic analysis method proposed by A.L. Saaty[7], an American operational scientist. There are already a lot of work done using AHP for weight calculation. Due to space constraints, we don't elaborate on AHP. Only describes the calculation of the weights of the indicators under U400.

The scale of the judgment matrix is shown in table III.

Table3. Scale of Judgment Matrix

Scaling	Meaning
1	Representing two factors compared to the same importance
3	Indicating that one factor is slightly more important than the other
5	Indicating that one factor is obviously more important than the other
7	Indicating that one factor is strongly more important than the other
9	Indicating that one factor is extremely more important than the other
2,4,6,8	The median of the two adjacent judgments
Reciprocal	Indicator i and j compared to determine a_{ij}, then j and i compared to determine $a_{ij} = 1/a_{ij}$

According to table III, we construct the judgment matrix A as follows:

$$A = \begin{bmatrix} 1 & 1/3 & 5 \\ 3 & 1 & 9 \\ 1/5 & 1/9 & 1 \end{bmatrix}. \qquad (2)$$

The eigenvalue of A is 3.0291 and the eigenvector is $[0.3662,\ 0.9265,\ 0.0868]^T$.

The average random consistency indicators are shown in table 4.

Table4.Average Random Comsistency Index

n	***1***	***2***	***3***	***4***	***5***	***6***
RI	0	0	0.52	0.89	1.12	1.24

Consistency index of A:

$$CI = \frac{\lambda_{max} - n}{n-1} = 0.01455 \qquad (3)$$

Consistency ratio of A:

$$\mathrm{CR} = \frac{CI}{RI} = 0.02798. \quad (4)$$

Since CR < 0.1, it is acceptable to judge the consistency of the matrix.

The index weight of U410, U420, U430 is:

$$0.265 : 0.672 : 0.063. \quad (5)$$

The weights of other indicators are calculated by similar methods. The final indicator weights are shown in table 5

Table5. Index Weight

Index	*U100*	*U200*	*U300*	*U400*	*U500*	*U110*
Weigh t	0.225	0.135	0.21	0.175	0.255	0.5
Index	*U120*	*U210*	*U220*	*U230*	*U221*	*U222*
Weigh t	0.5	0.231	0.692	0.077	0.5	0.5
Index	*U231*	*U232*	*U310*	*U320*	*U311*	*U312*
Weigh t	0.7	0.3	0.7	0.3	0.4	0.6
Index	*U321*	*U322*	*U323*	*U324*	*U410*	*U420*
Weigh t	0.192	0.258	0.233	0.317	0.265	0.672
Index	*U430*	*U411*	*U412*	*U421*	*U422*	*U510*
Weigh t	0.063	0.5	0.5	0.5	0.5	*1*
Index	*U520*	*U511*	*U512*	*U521*		
Weigh t	0	0.6	0.4	1		

4 Experiment

In order to verify the validity of the proposed index system, we take the Ukrainian Power Outages as an example to experiment it.

December 23, 2015, the Ukrainian electricity sector suffered malicious code attacks. At least 3 zones were attacked and led to hours of power outages around 15 p.m. local time.

According to the Antiy's analysis report about Ukrainian Power Outages[8], we can see that this attack was initiated by the SandWorm, caused a large area of power outages, lasted 3 to 6 hours. It mainly uses BlackEnergy and KillDisk to achieve the purpose of attack.

Firstly, BlackEnergy encrypts itself and its installation package is named the same as the system process. So BlackEnergy's static hidden ability is strong. Secondly, BlackEnergy runtime injects the process into Svchost.exe to hide itself. Finally, BlackEnergy's update ability is weak.

For KillDisk, its features include:

1. Overwrite MBR and partial sectors.
2. Clean up the system log.
3. Process traversal and clean up the process.
4. File erase.
5. End process.
6. Shutdown operation.

Through its function, KillDisk is very destructive, but the difficulty of removal is low.

Due to the high concealment of APT itself, some data cannot be obtained, such as the Attack Duration and the Number of Affected Machines. As the Ukrainian Power Outages is a paralysis attack, the total duration of the attack is less than the average APT event. Other unknown data are also available.

In summary, the index values of the Ukrainian Power Outages are shown in table 6

Tablr6 Index Value of the Ukrainian Power Outages

Index	*U110*	*U120*	*U210*	*U221*	*U222*	*U231*
Value	0.3	0.1	0.9	0.9	0.9	0.1
Index	*U232*	*U311*	*U312*	*U321*	*U322*	*U323*
Value	0.1	0.5	0.7	0.3	-0.7	0.9
Index	*U324*	*U411*	*U412*	*U421*	*U422*	*U430*
Value	0.1	0.1	0.1	0.1	0.1	0.3
Index	*U511*	*U512*	*U521*			
Value	0.9	0.7	X			

Therefore, the evaluation of the Ukrainian Power Outages is:

Persistent:

$$\mathrm{U100} = 0.5 \cdot 0.3 + 0.5 \cdot 0.1 = 0.2. \quad (6)$$

Hiding Ability:

$$\mathrm{U200} = 0.231 \cdot 0.9 + 0.692 \cdot (0.5 \cdot 0.9 + 0.5 \cdot 0.9) + 0.077 \cdot (0.7 \cdot 0.1 + 0.3 \cdot 0.1) = 0.8384. \quad (7)$$

Diffusibility:

$$\mathrm{U300} = 0.7 \cdot (0.4 \cdot 0.5 + 0.6 \cdot 0.7) + 0.3 \cdot (0.192 \cdot 0.3 - 0.258 \cdot 0.7 + 0.233 \cdot 0.9 + 0.317 \cdot 0.1) = 0.4695. \quad (8)$$

Intractable:

$$\mathrm{U400} = 0.265 \cdot (0.5 \cdot 0.1 + 0.5 \cdot 0.1) + 0.672 \cdot (0.5 \cdot 0.1 + 0.5 \cdot 0.1) + 0.063 \cdot 0.3 = 0.1126. \quad (9)$$

Harmfulness:

$$\mathrm{U500} = 1 \cdot (0.4 \cdot 0.9 + 0.6 \cdot 0.7) + 0 \cdot 1 \cdot X = 0.78. \quad (10)$$

Attack Effect Assessment of APT:

$$\mathrm{U000} = 0.225 \cdot 0.2 + 0.135 \cdot 0.8384 + 0.21 \cdot 0.4695 + 0.175 \cdot 0.1126 + 0.255 \cdot 0.78 = 0.4677. \quad (11)$$

The evaluation results are shown in Fig. 2.

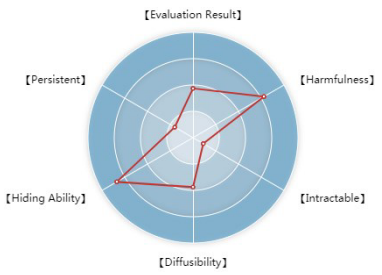

Figure 2. Evaluation Result of the Ukrainian Power Outages

Through the analysis of the Ukrainian Power Outages, we can see that there was no warning before the attack occurred. During the attack, the new 0day vulnerability was not used and the attack time was short. After the attack occurred, MBR and some sectors are overwritten, the system log is cleared and the controlled host cannot boot. Attack deals one-time damage to a controlled host, but the intransigence of malicious code is poor.

The above analysis and calculation results are basically the same, the Ukrainian Power Outages has a high degree of concealment and harm. But the continuity and intractability are poor. Its diffusion is moderate. Its comprehensive attack effect is moderate.

5 Conclusion

In this paper, a set of APT evaluation index system is proposed by analyzing the features of APT. And then use AHP to calculate the weight of this index system. Finally, the validity of the index system is verified by experiments. The experiment results show that it cannot only calculate the quantitative results of APT, but also see the ability of APT in five dimensions.

Acknowledgment

This work is supported by National Key Research and Development Program (No.2016YFB0800804).

References

[1] W. Juan, Z. Fengli, F. Chong and C. Lisha, “Study on index system in network situation awareness,” Computer Applications, vol. 27, no. 8, pp. 1907–1909, 2007

[2] D. Bin, H. Weihong, and L. Aiping, “Research on quantitative assessment model for internet worm threat,” Netinfo Security, no. 6, pp. 41–47, 2016.

[3] W. Zhiping, “Research of Network Security Situation Evaluation Based On Index System,” National University of Science Technology, 2010.

[4] H. Lansheng, Z. Cong, Z. Mengsong and L. Qiwen, “Fuzzy Evaluation Model fro Harms of Computer Virus,” Journal of Chinese Mini-Micro Computer System, vol. 31, no. 7, pp. 1297–1301, 2010.

[5] A. Peng, “Research and Implementation of Evaluation Technology of Network Attack Effect,” National University of Science Technology, 2015.

[6] https://baike.baidu.com/pic/APT%E6%94%BB%E5%87%BB/5030382/0/dc54564e9258d10979684498d258ccbf6c814d15?fr=lemma&ct=single#aid=0&pic=dc54564e9258d10979684498d258ccbf6c814d15.

[7] T. L. Saaty, “how to make a decision: The analytic hierarchy process,” European Journal of Operational Research, vol. 48, no. 1, pp. 9–26, 1990.

[8] “A Comprehensive Analysis Report on Ukraine Power Grid Outage,” http://www.antiy.com/response/A Comprehensive Analysis Report on Ukraine Power Grid Outage/A Comprehensive Analysis Report on Ukraine Power Grid Outage.html, 2016.