2017 9th International Conference on Measuring Technology and Mechatronics Automation

Study on Network Information Security Based on Big Data

Wang Jia

Hebi Polytechnic College
403475627@qq.com

***Abstract*—Nowadays, APT attacks bring extreme threat and challenge to the network information security. Based on analysis of big data technique, the paper presents an APT security protective framework, which integrates deep and three-dimensional defense strategies, besides, the big data are used to explore and analyze possible APT attacks as well as threat positioning and tracks.**

Keywords- APT, Big data, Network security framework

I. INTRODUCTION

Currently, the network system faces more and more serious security challenges, within the numerous challenges, a new network attack characterized of organization, special target and long persistence becomes wild increasingly, which is internationally called APT (Advanced Persistent Threat) attack, besides, before an attack, the APT attackers generally make preparations for a long time which may be months or years, and it makes it difficult to determine the APT attack time, therefore, during the APT attack protection, the attack detection is the premise and base for security protection and reinforcement, which is the most difficult for the APT attack protection. Yet, typical cases show that APT attacks have strong capabilities of concealment and targets, and most of traditional testing tools are helpless for the APT attacks. For this purpose, the paper creates a comprehensive system security protection framework and presents a big data-based system security testing framework to detect the APT attacks layer by layer through multiple security techniques.

II. SYSTEM SECURITY FRAMEWORK NEED BASED ON BIG DATA ANALYSIS

(1) In order to meet challenges of diverse APT attacks, it needs to create a multi-dimensional cooperative defense system to prevent from the APT attacks in different angles. (2) In order to tackle the higher concealment of APT attacks, it needs to well detect abnormal behaviors as stealing files transmitted via cryptograph with abnormal flows. (3) In order to tackle the long term APT concealment, it needs to monitor the states of all layers of the client virtual machine for a long time.

III. SYSTEM SECURITY FRAMEWORK DESIGN BASED ON THE BIG DATA ANALYSIS

The APT attacks aiming at the network information systems adopt a variety of technical means, with higher pertinence and long persistence. In view of the potential counter measures by attackers, it needs to create a deep, three-dimensional defense system against the APT attacks. The system should be capable of intelligent detection and deep correlation analysis, and execute targeted security protection and active defense. Based on the points given above, the author proposes a security framework to prevent from the APT attacks through a network information system consisting of system security testing, system security protection and active defense, refer to figure 1 for details. figure 1 shows, in case of any network access, the integrated intrusion detection gateway may identify and block some attacks. At the same time, the network security system will collect all kinds of network events from attackers, gateways and intranets, extract the event features and perform deep data correlation analysis to discover the APT attacks that are not recognized by the integrated intrusion detection gateway. Then, the defense system, based on correlation analysis results, will prevent from the APT attack process in the intranets through the system security protection. Finally, the defense system will adopt the object-based active defense technology to counter so as to prevent from the APT attacks basically.

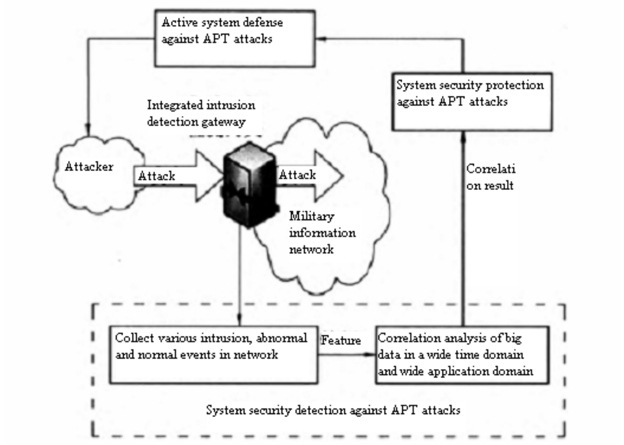
Active system defense against APT attacks
System security protection against APT attacks
Integrated intrusion detection gateway
Attacker
Attack
Attack
Military information network
Correlati on result
Collect various intrusion, abnormal and normal events in network
Feature
Correlation analysis of big data in a wide time domain and wide application domain
System security detection against APT attacks

Fig 1 Security Framework of Network Information System Against APT Attacks

A. *System Security Testing Against the APT Attacks*

The system security detection against the APT attacks shall include three processes as integrated intrusion detection, traceability, network event collection and big data deep correlation analysis. First of all, the integrated intrusion detection of the system, through the introduction of the core server bypass deception mechanism (such as Honeynet or Honeypot technology) will take the initiative to deceive any possible potential attack, the virtual Honeypot is an intelligence gathering system of the defender, the deployment of non-business purpose of security resources are made to lure attackers to attack so as to capture and evidence the attacks and understand the attack tools and

2157-1481/17 $31.00 © 2017 IEEE
DOI 10.1109/ICMTMA.2017.104

methods. After discovering the attacks, the source will be traced, which will be realized mainly through data traceability, data mining and so on. Finally, considering the information that the defense system collects have typical characteristics of big data such as huge data volume, quick data update, multiple data type and low data value density, the big data analysis is used to conduct correlation analysis on the network event information and access executer information in a wide time domain and wide application domain so as to identify the attack behaviors that the military information system intrusion detection gateway fails to detect.

B. System security protection against the APT attacks

The security needs of resources shall be classified according to the security level of the confidential data, and construct trusted virtual domain according to the user's confidentiality level, and the high-level resources can be safely isolated. At the same time, the important data shall be encrypted and stored, and the cryptograph access is implemented to restrict the penetration of APT attacks from outside to inside. In addition, it needs to ensure the data security in the dynamic state, and provide a safe migration of virtual machines and keep the security strategies consistent during the migration.

C. Active system defense against the APT attacks

First of all, it needs to consider the APT attacks overall and form an ability of quickly screening a large amount of information in the network and discover weak signals that can be captured in the complex and secret network attacks, and establish a counterintelligence system that can implement APT attack detection. Second, the defense system shall list an attack list, and select appropriate attack objects to counter and interfere the object with higher protection level after it is ripe. Finally, the above active defense process may work on the wrong objects, but in order to maintain the high level security of network information system, it still needs to implement interference and counter. The active defense strategy can effectively disrupt the attacker's attack plan and restrict the attacker's attack ability as to better defend the APT attacks.

IV. Key Technique Analysis Of Network Security Protective Framework

A. Big Data Analysis

The APT attack defense cannot be separated from the big data analysis technique, whether the log data generated by the network system itself or the log information generated by the platform, both can use the big data analysis technique for data reanalysis, the data statistics, data mining, correlation analysis, trend analysis and so on can be used to discover the traces of APT attacks in the recorded historic data so as to make up the deficiency of traditional security protection. No doubt, the big data analysis technique requires a powerful data collection platform and powerful data analysis capabilities, and it shall be combined with a wide range of unified monitoring and fast automatic response system so as to overcome the difficulties in survey and analysis caused by the information isolated islands.

B. Attack tracing technique

Multi-layer attack analysis of network information security system include system call analysis, attack analysis of key kernel structure, file and process analysis, and network flow analysis, etc. It needs to create a uniform multilayer attack description model, and conduct multiple correlation analysis as per relevant rules according to the massive log information of multilayer attack model so as to identify possible attacks in the system and provide reliable basis for tracing the track. The data traceability technique has been widely studied in the field of database. At present, there are two main challenges for data traceability: (1) How to process heterogeneous data sources, such as columnar database, document database, Key /Value system and XML database. It is important to ensure the data mining system to effectively process different data sources. (2) How to deal process massive data. With the time going and the application of Internet and the Internet of Things, the data grow exponentially, in order to process the big data efficiently, the data mining algorithms must be highly efficient and elastic.

V. Conclusion

The frequent APT attacks have brought huge challenges to the cyberspace security, and the attack layer by layer differs from traditional Trojan and viruses, and its hidden attack ability makes it hard for the traditional defense technologies to protect the important information assets effectively. Fortunately, some defense technologies have been developed to deal with APT attacks. Yet, most of the defense products only focus on some aspects of the APT attack chain for protection. Therefore, it is necessary to form an APT attack chain-based defense system architecture covering all aspects of APT attacks, and achieve the complete defense of APT attacks through the combination of management and technical means.

REFRENCE

[1] Ma Y T, He K Q, Li B, et al. Empirical study on the characteristics of complex networks in networked software [J]. Journal of Software, 2011, 22(3): 381-407. (in Chinese)

[2] Fang J Q, Wang X F, Zheng Z G. Research of dynamical complexity of nonlinear networks [J]. Complex Systems and Complexity Science, 2010, 7(2-3): 5-9.

[3] He C W, Zhang L J, Zhang H. An approach to aspect-oriented software evolution based on metadata and reflection [J]. Acta Electronica Sinica, 2011, 39(8):1771−1777. (in Chinese)

[4] Sureka A. Learning to classify bug reports into components [J]. Objects, Models, Components, Patterns, 2012, 73(4): 288-303.

[5] Zhang H Y. On the distribution of software faults [J]. IEEE Transactions on Software Engineering, 2008, 34(2):301-302.

[6] Chen P, Han H，Shen X B. Detecting integer bugs based on static and dynamic program analysis [J]. Acta Electronica Sinica, 2010, 38(8):1741-1747. (in Chinese)