Integrated approach to the detection of distributed network attacks

Shangytbayeva Gulmira [1, a *], Beysembekova Roza[2, b]

[1,2]Kazakh National Technical University named after K.I.Satpayev

Satpayev st 22, Almaty, Kazakhstan

agul_janet@mail.ru, broza@mail.ru

Keywords: information security, attacks, threats, network attacks

Abstract. The article discusses an integrated approach to the detection of distributed network attacks and attacks of malicious behavior and attacks of abnormal activity in distributed networks.

Introduction

Computer viruses are currently one of the most dangerous threats to information security of automated information systems. Computer viruses are currently one of the most significant threats to information security, as evidenced by numerous data on the annual financial losses as a result of the effects of virus attacks.

To minimize the risk of information security in corporate information networks are now being used develop and implement systems to detect network attacks. They are a specialized or software and hardware, which provide active audit and security management (forecasting, detection, prevention, control, respond to security threats in real time) in corporate networks. Solution to the problem of developing an effective information protection from network attacks requires the development of new methods, capable of withstanding distributed network attacks of various origins and more adequately reflect the complex dynamics of random processes attacks. Requires the development of methods to detect distributed network attacks using modern methods of decision support based on the theory of intelligent systems, allows us to go in solving protection products and information technology systems of the principle of "detection and elimination of" the principle of "forecasting and warning in real time ".

Shortcomings of existing approaches

Currently, many companies to effectively protect automated information systems from malicious software is sufficient to establish antivirus products on all workstations and servers that automatically provide the desired level of security. Unfortunately, experience shows that such an approach does not fully solve the problem of protection against malicious code. This is due to the following main reasons:

• the vast majority of antivirus tools based on the signature method detection of malicious software that does not allow them to detect new viruses whose signatures are not available in their databases;

• In some cases, organizations are no regulatory guidance documents governing the work of antivirus protection equipment. This can lead to possible violations of the rules of operation - namely, failure to update signature databases, disabling anti-virus components, run the program with unverified information carriers, etc.;

• antivirus protection does not allow to identify and eliminate vulnerabilities based on which computer viruses can penetrate in automated information systems of enterprises;

• antivirus software does not have features that enable to eliminate the consequences of virus attacks.

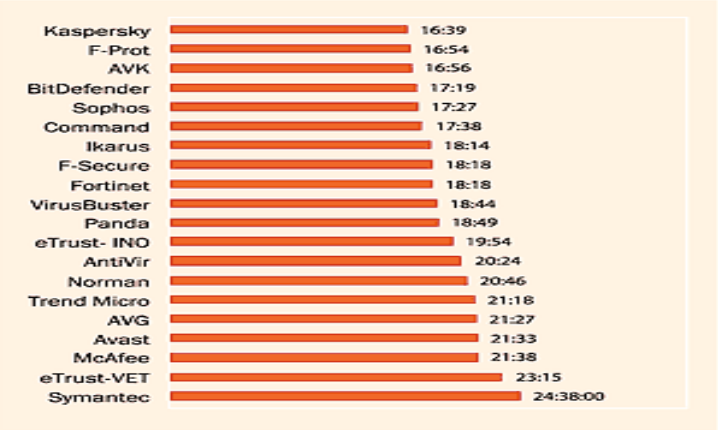

Figure 1. Antiviral Laboratories, responsive to emerging viruses differently

Another common approach to protecting against malicious code is the use of automated information systems, antivirus protection is only one producer, which are installed on the servers, workstations and network gateways. The disadvantage of this method is the high level of dependence on products of this manufacturer. This means that if, for whatever reason, will not operate a scan engine or the vendor (manufacturer software) is not able to timely update its database, under threat of a virus outbreak would be the entire infrastructure of the company. The urgency of the problem stems from the fact that the Antiviral Laboratories, responsive to emerging viruses differently (Figure 1). The difference in reaction time of up to eight hours, during which the automated information system could potentially be successfully attacked by hackers. It is also necessary to note the difference in time of response of companies to a particular virus, the manufacturer, which is now the first to respond to the emergence of the virus, Class A, tomorrow may release the latest virus signature for type B.

Next, consider what way should build protection system. It is indisputable that only a comprehensive approach to protecting against viruses and to detect distribution network attacks avoids the above drawbacks.

Detection of malicious attacks conduct

Accepted provide two basic kinds of Intrusion Detection System: Work First is to find evidence of previously known attacks; The second comprises a program to detect anomalies in the functioning of the system.

If the detection of attack requires an understanding of the expected behavior of the controlled offender information, the technology - the technology of detecting malicious behavior. Work abuse detection systems based on the compilation of patterns or "signatures" attacks. Safety systems of this type are effective for the known attack patterns, however, in case of a new unknown attacks or stroke attack deviations from a template, there are serious problems. Therefore it is necessary to maintain a large database of every attack and its variations, and continuously replenish the base templates. Also it is important to determine the sample size parameters controlled by the detection of network attacks based on malicious behavior. A small number or incorrectly selected parameters may lead to the fact that a model describing the behavior of entities in the system based on this method will be incomplete, and many attacks cannot be detected. On the other hand, too large a number of monitoring parameters carried method will cause a decrease productivity controlled unit due to increased demands for resources consumed.

Detection of attack abnormal activity

Intrusion Detection Technology Based on the methods of detecting abnormal (suspicious) activity, in contrast to the discussed above, is more flexible and can detect unknown attacks. Anomaly detection systems based on the assumption that all the actions the attacker certainly something different from the behavior of the average user.

Detect attacks caused by abnormal activity, based on a comparison of current values of the parameters of activity with the values that are currently considered normal. As these parameters may be, for example, quantitative use of system resources, the intensity of requests to resources or system service. Under the current values of the parameters generally understood activity average computed over a short time interval (from several minutes to several hours), immediately preceding the moment in question. The normal mean values of these parameters are calculated over a sufficiently long period of time (days to months).

This technology is based on the conclusion that the anomalous behavior of the subject (system software, user), manifested as a deviation from normal behavior. An example of anomalous behavior can serve a large number of compounds in a short period of time, high CPU load and network load ratio. However, the anomalous behavior is not always attack. For example, the attack is not receiving a large number of responses to a query about the activity of the stations from the network management system.

Work systems to detect anomalous activity is preceded by a period of accumulation of information when building the concept of normal system activity, process or user. It becomes a benchmark for evaluating subsequent data. Therefore, when setting up and operation of this category are faced with two problems:

– building a profile of the subject (difficult to formalize and time-consuming task that requires more work);

– the definition of the boundary values of the characteristics of the behavior of the subject in order to reduce the probability of occurrence of one of the above two extreme cases.

This technology requires constant log of all actions controlled entity required to detect abnormal activity, which significantly reduces the performance of the protected host. Such systems a lot of CPU require large amounts of space to store the collected data and, in principle, applicable to systems that are critical to the speed, operating in real time. Another drawback of the existing systems to detect anomalous activity is that they are based on assumptions about the fixed network processes and mutual independence of private metrics that are never fulfilled in practice. This predetermines the use of such systems the method of stationary statistics, which are not suitable for short-term forecasting, which makes responding to security threats in real time. Rather rarely update the database parameters of normal behavior allows offenders to adapt their behavior to the requirements of the detection of abnormal activity, which treats it as a result of a legitimate user. Ignoring the mutual dependence of private metrics leads to inadequate response of the system, resulting in a large number of false positives.

Multi-agent systems detect abnormal network activity

Taking into account the current and future trends in the development of information technology systems, as well as objective disadvantages described above two approaches to the detection of network attacks can be concluded on the need to offset the efforts to develop and implement an integrated concept of building security systems based on distributed computing systems, using mechanisms protection based on the active audit. The components of such systems should be specialized by type of tasks, interact with each other to exchange information and consistent decision-making, to adapt to the reconfiguration of the hardware and software network traffic changes, new types of attacks. Among the possible technologies to implement this approach as the most promising technology is considered intelligent multi-agent systems.

The main provisions of the proposed approach are as follows. Components of system information protection (protection agents) are intelligent stand-alone programs that implement certain security features in order to ensure the required security class. They allow you to implement a comprehensive security mechanisms built on top of network software, operating systems and applications, increasing the security of the system to the required level. It is assumed that the agents distributed over the hosts of the protected network, specialized on the types of tasks and interact with each other to exchange information and consistent decision-making. It is important to emphasize that there is no explicit "control center" of

the family of agents - depending on the current situation may lead to become any of the agents specializing in management tasks. If necessary, agents can be cloned and stop functioning. Depending on the situation (type and number of attacks on a computer network, the availability of computing resources to perform security functions) may be generated by multiple instances of each class of agents. They adapt to the reconfiguration of the network traffic changes and new types of attacks, using the experience.

The proposed approach is based on the technology of intelligent multi-agent systems will be used in Intrusion Detection System following new approaches, significantly increases the efficiency of the system of protection of distributed network attacks:

- Mobility, the system is built on mobile agents, that allows you to make the system flexible, easily reconfigurable, vitality;
- The activity, the system not only captures the facts of remote network attacks, but also conducts active measures against a remote attacker;
- Self-organization, the use of simplified structure and principles of human immune system, allows us to solve the problem of recovering the system as a result of failures of self-control to detect their own mistakes;
- Specialization in the types of tasks;
- Adaptation to the reconfiguration of the hardware and software network traffic changes, new types of attacks;
- Implementation support making the most rational solution to block the distribution in time and space of a network attack.

Implementation of the process of forecasting and detection of distributed network attacks is the main content of specific functions of the multi-agent Intrusion Detection System.

Conclusion

Detection of network attacks on the resources of information technology systems are very complex process that is associated with the collection of a large amount of information about the operation of information technology systems, data analysis, and revealing the fact of attacks. For effective forecasting and detection of attacks requires integrated application of different signature methods and methods of detecting anomalous network activity.

Since solution problem improve the effectiveness of information security in corporate networks in the use of adaptive methods, that allow real-time to carry out time-dependent processes characterizing network attacks, then, it is necessary to consider the approach, which combines the method of multi-agent systems with methods adequate to detect signs of attacks based on statistical methods of probability theory, fuzzy probabilistic and statistical methods, methods of the theory of intelligent systems, as well as methods of artificial neural network. These methods should allow a wide range of conditions of corporate networks and information technology systems adequate to real-time detection of non-stationary random dynamic processes of abnormal activity and malicious behavior on network systems and information technology systems at low probability of false alarm and missing network attacks.

References

[1] The DDoS That Almost Broke the Internet, 2013.

[2] CloudFlare blog, Deep Inside a DNS Amplification DDoS Attack, 2013.

[3] Global Upgrade Makes Internet More Secure, 2010.

[4] Peng Liu Denial of Service Attacks, University Park, 2004.

[5] J. Reynolds, R. Braden Request for Comments (RFC), 2004.

[6] W. Eddy TCP SYN Flooding Attacks and Common Mitigations, 2007.