Architecture of the Honeypot System for Studying Targeted Attacks

Vitaly V. Polyakov, Sergei A. Lapin
Altai State University, Barnaul, Russia

Abstract – Among the threats to information systems of state institutions, enterprises and financial organizations of particular importance are those originating from organized criminal groups that specialize in obtaining unauthorized access to the computer information protected by law. Criminal groups often possess a material base including financial, technical, human and other resources that allow to perform targeted attacks on information resources as secretly as possible. The principal features of such targeted attacks are the use of software created or modified specifically for use in illegal purposes with respect to specific organizations. Due to these circumstances, the detection of such attacks is quite difficult, and their prevention is even more complicated. In this regard, the task of identifying and analyzing such threats is very relevant. One effective way to solve it is to implement the Honeypot system, which allows to research the strategy and tactics of the attackers. In the present article, there is proposed the original architecture of the Honeypot system designed to study targeted attacks on information systems of criminogenic objects. The architectural design includes such basic elements as the functional component, the registrar of events occurring in the system and the protector.

The key features of the proposed Honeypot system are considered, and the functional purpose of its main components is described. The proposed system can find its application in providing information security of institutions, organizations and enterprises, it can be used in the development of information security systems.

Index Terms – Honeypot system, target attacks, computer information.

I. INTRODUCTION

Building an information security system for modern enterprises is implementation process for set of measures countering all possible threats, especially unauthorized remote access to automated workplaces via specialized malicious software. Such software can be used by organized groups of individuals to steal money, remove, copy, modify or restrict access to computer information protected by law, for example, which is a commercial, banking, medical or other type of secret.

Especially threatening are the groups aiming at obtaining unauthorized access to the information system of specific enterprises, or group of enterprises combined with the same type of activity [1, 2]. Such enterprises include financial organizations, industrial, energy systems, etc. Using malicious software written or modified specifically for specific organizations is one of the features of such actions. Revealing those attacks is quite difficult, and their prevention is even more complicated. Therefore, the task of revealing and analyzing those threats is quite topical. Using specific Honeypot system is one of the ways of solving such problems [3]. The Honeypot research system began to be actively used in the 2000s [4-5]. Currently, it includes many varieties of freely marketed software worldwide. In technical terms, the Honeypot system presents a special computer program installed on a separate server or virtual system (site, user page, etc.), that is, a virtual automatic workstation (AWS), to which a relatively simple unauthorized access is presented to potential attackers by means of previously prepared vulnerabilities.

II. FORMULATION OF THE PROBLEM

The purpose of this article is to describe the new architecture of the research system Honeypot, designed specifically to study targeted attacks on information resources of state institutions, enterprises, financial organizations. In order to achieve this goal, the following tasks are solved in the article: formulating requirements for the system, defining the main parts that make up its architecture, and describing their basic functional capabilities.

III. ARCHITECTURE AND FUNCTIONING OF THE HONEYPOT SYSTEM

Using Honeypot system proposed in this article helps the researcher to solve such tasks facing him:

- Identifying previously unknown problems in the information security system of organizations. In the course of their activities, attackers often use original techniques that not only circumvent the existing restrictions imposed by information security tools, but also implement them in such a way as to reduce the likelihood of revealing their unauthorized activity in the system. In such cases, the Honeypot system allows to deeply explore such original techniques, while determining the circumstances that facilitate the implementation of unauthorized access to the system. For example, security flaws may include errors in the definition of rules for access control, the availability of redundant user capabilities when working on the network (for example, the ability to connect to non-standard port numbers), errors in determining the rules for the operation of intrusion detection systems, and so on.

- analyzing step-by-step intruder’s actions within the information system of the enterprise in particular situations.
• identifying targets pursued by intruders and potential targets of encroachment. When analyzing the actions carried out by an intruder inside the system, the researcher can draw certain conclusions about the internal data of the enterprise that the intruder tries to access (financial resources, confidential information, etc.).
• detecting previously unknown malicious software used by intruders. When conducting targeted attacks on information systems, intruders can use narrowly targeted, previously unknown malicious software. Providing a higher level of protection of information systems is associated with the timely detection of such software, as well as by studying its capabilities and key signs of availability in the system.
• collecting various information about the intruder’s infrastructure (server, address, etc.).

The above listed tasks can be solved more effectively by using the unique Honeypot system architecture proposed in this article, including elements as follows:
• several interrelated automated workstations for users (AWS), that can be executed both on individual computers and in the virtual systems form. Regardless of the way which they are executed, each one of such separate workstations will be called an instance of the Honeypot system.
• the entry point to the system, which is a special instance of the Honeypot system.
• the collector for occurred events.

In general, the Honeypot system presents the implementation of the enterprise network. At the same time, not a single instance of Honeypot should have access to any enterprise workstation, i.e. the Honeypot system and the enterprise network should be isolated from each other in order to avoid access to protected objects for the intruders while researching their activities. Each available Honeypot instance must have its own functional purpose in the enterprise architecture. However, the requirements for their implementation remain the same. The proposed architecture meets the following requirements:
• every instance of the Honeypot system has its own, strictly defined function within the system. For example, it could be a server of various kinds, an automated workplace for the user, etc. Together, all instances of the Honeypot system should look like a network or a fragment of an enterprise network.
• every instance of the Honeypot system provides logging for all performed actions. Each attack by an intruder, including the malicious software actions, should be recorded for further analysis by the researcher.
• every instance of the Honeypot system ensures the safe storage of the events that occurred in the system. The information about the actions carried out by intruders should be preserved and well protected from unauthorized access;
• every instance of the Honeypot system is designed in such a way as to hide its true functional purpose. Using Honeypot systems is associated with creating conditions that allow varying the ability to gain access to the system for intruders. This mechanism allows to better adapt to the specific situations and needs of the researcher. In general, the results of the researcher's activity will be the higher, the more original actions are performed by the attacker.
• Honeypot system has a number of distinctive features from the normal modes of operation of the operating system, according to which an attacker can identify and terminate his activity [7]. In order to prevent the identification of such signs by Honeypot, a module is used, which allows to hide the signs of the Honeypot work - the protector. Its main purpose is the hidden functioning of all the modules described above, which provide information collection, Honeypot's own processes, as well as a number of other features that are not inherent in the process of the system under which Honeypot is masked, such as specific elements of the file system, system information, etc.

Thus, the listed requirements form the following components of the Honeypot instance of the system, defining its architectural execution:
• functional component.
• registrar of events occurring in the system.
• protector.

After the intruder has access to the described system, a direct study of his actions begins. Conditionally, such actions can be divided into the following groups:
• usage of only a single instance of the Honeypot system.
• usage of the Honeypot system instance as a gateway for further illegal actions against other information systems.
• usage of the Honeypot system instance to commit unlawful actions in regard with the workstation's LAN of the enterprise.

The intruder can make network connections, install and run malicious software, create new files, change / replace / delete existing files on the system, etc. Therefore, it is important to monitor the behavior of such software in the system [8-10], so an instance of the Honeypot system must include tools that allow to:
• monitor network activity. Their main task is to obtain a complete copy of the transmitted data, as well as to collect information on emerging network connections, such as IP addresses, port numbers, domain names, etc.
• track events in the file system.
• monitor the activity of emerging and existing processes in the system, since an intruder can use malicious software and, consequently, generate new processes in the operating system, so the occurring events of this kind need their logging. Such tools should ensure collection of the following data: time of process start / stop, process ID, data on interaction with other processes, etc.

The architecture of a single instance of the Honeypot system is shown in figure 1.
An important aspect of operation of the Honeypot system is that the intruder needs to be somehow given the access to the system without arousing his suspicion. A module called the system entry point, representing a special instance of the Honeypot system, is responsible for solving this problem. The system entry point must fulfill all the requirements described above and have the abovementioned components for the system instances. Along with this, it has an additional component that allows an intruder to gain access to its operating system. Various methods can be used for such task. One them can be usage of special e-mail addresses having domain name of the enterprise. Also it is possible to pass registration on any specialized network resources that correspond with specifics of the enterprise, using the data of e-mail addresses, or make them public via any other way. Intruders who target information systems can use such addresses to send out letters containing malicious software, and gain access to the system upon its launching [1, 11]. The entry point is checking all received e-mails and, in case of finding attachments to them, tries opening them.

Safe storage and systematization for further and deeper analysis should be ensured for the information gathered during the research. In this article, each instance of the Honeypot system, upon occurrence of an event, secretly sends information about it to a special server that is part of the system - a storage device for the events occurred. Such server should store received information about the events that occurred at the Honeypot system instances. Analyzing actions of the intruder, the researcher, facilitated with this server, should have opportunity to restore the history of the events and study received copies of malicious software. The work of the entire proposed system can be described as follows. The researcher creates special e-mail addresses under domain name of the organization. After that, those addresses are made public any way in the public domain, on thematic forums, conferences, etc.

This is done to attract attention of intruders who commit illegal activities aimed at gaining access to confidential information of organizations. After that, the Honeypot system instance, herein called the entry point, expects correspondence incoming to the abovementioned e-mail addresses. When an e-mail containing attachment arrives, its contents are launched. Was such content a malware, certain events in the operating system would be logged by the event recorder and would be immediately sent to the event storage

device, another component of the considered Honeypot system. Further, all activity of malicious software in the system along with actions of the intruders, including those aimed at gaining access to other instances of the Honeypot system, will be supplied to the researcher for their study.

A laboratory testing of the proposed architecture of the Honeypot research system was carried out, which showed its reliability and effectiveness.

IV. SUMMARY AND CONCLUSIONS

The architecture of the Honeypot system designed to study targeted attacks on the information system of organizations was proposed in this article. Possibilities of the Honeypot system were defined, its main components and their functional purpose were described. The proposed architecture can find its application in information security systems of institutions, organizations and enterprises, it can be used to develop new information security systems.

The reported study was funded by RFBR according to the research project № 16-33-01160-OGN.

REFERENCES

Polyakov Vitaly Viktorovich, PhD, Associate Professor.
In 2009, at the Dissertational Council at the Omsk Academy of the Ministry of the Interior of the Russian Federation, he defended his thesis on the topic: "Features of investigation of unauthorized remote access to computer information".
In 2013, he won the All-Russian Grant Competition of the President of the Russian Federation for state support of young Russian scientists. A scientific research on topic of: "Legal problems of crime prevention in the sphere of computer information" was successfully carried out within the framework of the grant. In 2016 he won the All-Russian competition of grants held by the Russian Humanitarian Scientific Foundation, with the project: "Criminalistic features of crimes in the field of computer information" (2015-2018).
At present time he conducts classes in the academic disciplines: "Criminalistics", author's special courses for undergraduates: "Criminalistic characteristics of computer crimes", "Investigation of computer crimes", "Prevention of computer crimes."

Lapin Sergei Aleksandrovich, postgraduate student of the Altai State University.
In 2013 he graduated from the magistracy in the direction of "information security". In 2013 he became the executor of the grant from the President of the Russian Federation for the state support of young Russian scientists. A scientific research on topic of: "Legal problems of crime prevention in the field of computer information" was conducted within the framework of the grant. In 2016 he became the executor of the grant of the Russian Humanitarian Scientific Foundation, on the topic of: "Criminalistic features of crimes in the sphere of computer information" (2015-2018).
Since 2014, he has been engaged in practical activities in the field of information security, working in DrWeb, Group-IB, and Kaspersky Lab as a virus analyst, a specialist in computer criminalistics and an expert in responding to incidents of information security.