УДК 00 – 004.056

Jurakulov Sh.B.
assistant professor
TUIT Karshi branch
Uzbekistan, Karshi
Sharifov Ya.X.
assistant professor
TUIT Karshi branch
Uzbekistan, Karshi

EMULATION OF NETWORK ACTIVITY FOR MALWARE ANALYSIS IN AN ISOLATED ENVIRONMENT

Annotation

As part of the study, the principles of a secure runtime environment and detection of malicious software in an isolated environment were studied. Attention was paid to the problem of unavailability of network services when analyzing malicious software in an isolated environment. As a result of the work, the existing network activity emulation systems, their advantages and disadvantages were considered. An algorithm for the functioning of the network activity emulation technique was developed, and basic modules were created, including HTTP/HTTPS, DNS, SMTP, FTP, SMB, recording network traffic and configuring rules. The technical details of the development of a technique for emulating network activity were presented. Samples of malicious software were used to demonstrate the capabilities of the system. In general, the development of a network activity emulation technique for malware analysis in an isolated environment has improved the efficiency and accuracy of malware analysis in a controlled security environment.

Keywords*: information security, network activity emulation, isolated environment, virtualization, malicious software.*

Introduction

The issues of analyzing malicious activity are becoming more relevant due to the inefficiency of signature methods. One of the ways to detect malicious activity is to track requests to external network services. Thus, in the process of automatic analysis of malicious code in an isolated environment, situations often arise when malicious software requires the availability of certain services on the Internet. However, simply preventing any access to the Internet is in many cases impossible, since malware often requires access to run and demonstrate its activity. If services are not available, the malware does not execute code blocks and thus limits the analyzed area of behavior. In order to make the analysis as complete as possible, it is necessary to emulate inaccessible services between the isolated environment and the network.

Network activity emulation is an important tool for malware analysis. It allows you not only to emulate inaccessible services, but also to recreate the network conditions in which malicious software operates. This is especially important when analyzing the spread of such types of malware that actively use the network for their work. Using the network activity emulation technique allows you to conduct research in a controlled environment and obtain more accurate and reliable results.

Features of the work of the VPO, which depends on the availability of network services for the execution of malicious code. One of the key goals of malware analysis is to identify their functionality, which may be aimed at damaging the system or a specific organization. However, in some cases, the execution of malware tasks may depend on the availability of network services. This section provides an overview of services that may be critical to the operation of common malware families, and how their unavailability may affect threat analysis and protection.

The work of malware, which depends on the availability of network services to execute malicious code, is closely related to the C2 system, since these programs can use network services to receive commands from intruders and transfer data. If the availability of network services for executing malicious code is limited, this may affect the ability of attackers to manage malware and receive information from it.

Command and Control

The Management and Control Infrastructure, also known as the C2 system, or Command and Control, is a tool for remote management and control of malicious software. Through C2, attackers can control hacked computers with an autonomous VPO, collect information and carry out various types of computer attacks. Malware is usually installed on the target computer by exploiting vulnerabilities or social engineering and communicates with the C2 system to receive instructions, download additional malicious data, and transfer stolen data. Limiting the availability of network services for executing malicious code can block the ability of attackers to manage malware and receive information from it, therefore, the work of such malware is closely related to the C2 system.

The "Cobalt Strike" malware family

"Cobalt Strike" is a complex for conducting attacks, which allows you to deliver a payload to the attacked computer and control it. Interaction with the Cobalt Strike server part takes place by creating hidden channels using DNS, HTTP, HTTPS protocols to prevent the detection of this network interaction. The payload can execute the following commands:

- get information about the system (OS, hardware, list of processes, computer name);
- get information about the network environment;
- execute a shell command.

Download and run the executable file.

To perform these tasks, Cobalt Strike uses a C2 server that provides communication between the attacker and infected devices. Therefore, a working network infrastructure is needed to use Cobalt Strike.

Conclusions

As a result of the research, a technique for emulating network activity was developed to analyze malicious software in an isolated environment. The main problem associated with the unavailability of network services when analyzing malicious software in an isolated environment has been identified and studied. The existing network activity emulation systems were analyzed, and based on this, a mathematical formulation of the problem of network activity emulation in an isolated environment for malware analysis was developed. An algorithm for the functioning of the network activity emulation technique was also developed, as well as the main modules were designed, including HTTP/HTTPS, DNS, SMTP, FTP, SMB, recording network traffic and configuring rules. In the technological part, the technical details of the development of a technique for emulating network activity using the Python programming language, which provides an extensive set of libraries for working with network protocols, were presented. In addition, the technological aspects of all modules of the emulation system were considered, their functionality, implementation features and interaction were described. Samples of malicious software were used to demonstrate the capabilities of the system. In general, the development of a technique for emulating network activity in an isolated environment has made it possible to increase the efficiency and accuracy of malware analysis in an isolated environment.

Literature

1. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под ред. Зегжда Д.П. и др. М.: Горячая линия, 2021. 560 с.

2. Барабанов А.В., Гришин М.И., Кубарев А.В. Моделирование угроз безопасности информации, связанных с функционированием скрытых в вредоносных компьютерных программ//Вопросы кибербезопасности. 2014.

№ 4 (7). С. 41–48.

3. Ермаков А.О., Кавешников М.Б., Клянчина Е.В. Вредоносное программное обеспечение APT-групп и его характеристики//Вопросы кибербезопасности. 2017. № S2 (20). С. 24–29.

4. Жуковский Е.В., Зегжда Д.П. Анализ вредоносного по, обладающего механизмами опасного триггерного поведения//Защита информации. Инсайд. 2019. № 3 (87). С. 60–63.

5. Марков А.С., Фадин А.А. Организационно-технические проблемы защиты от целевых вредоносных программ типа Stuxnet//Вопросы кибербезопасности. 2013. № 1 (1). С. 28–36.

6. Мирзабаев А.Н., Самонов А.В. Метод обеспечения устойчивости вычислительного процесса в условиях воздействия вредоносных программ//Вопросы кибербезопасности. 2022. № 2 (48). С. 63–71.

7. Шкирдов Д.А., Сагатов Е.С., Сухов А.М., Дмитренко П.С. Выявление сетевых угроз на основе данных с серверов-ловушек//Защита информации. Инсайд. 2020. № 3 (93). С. 48–56.

8. Thorsten Holz. Improving Dynamic Malware Analysis by Emulating the Internet. [Электронный ресурс]. URL: www.researchgate.net/publication/221540604_TrumanBox_Improving_Dynamic_Malware _Analysis_by_Emulating_the_Internet.

9. Зулькарнаев Р.Ф. Изоляция и АСУ ТП//Защита информации. Инсайд. 2019. № 6 (90). С. 34-38.

10. Петренко С.А., Петренко А.А., Костюков А.Д. (2021). Киберустойчивость цифровых экосистем//Защита информации. Инсайд. № 4(100). С. 17-23.