УДК 004.8:65.05:681.5 DOI: 10.31673/2786-8362.2024.025763

Жидка О.В., Дакова Л.В., к.т.н.;
Даков С.Ю., к.т.н.; **Поляшенко Д.В.**

ANALYSIS OF THE USE OF SOFTWARE HONEYPOTS IN INTERNET OF THINGS

Zhydka O.V., Dakova L.V., Dakov S.U., Poliashenko D.V. Analysis of the use of software honeypots in Internet of things. This article examines the use of software honeypots as an effective tool for protecting information in the face of modern cyber threats. A detailed analysis of various types of lures, their advantages and disadvantages, possible security threats, as well as aspects of the configuration and overall efficiency of the systems was carried out. It is important to emphasize that even with the most modern protection tools, it is impossible to ensure the absolute invulnerability of the company's data, since attackers are constantly improving their attack methods. Software honeypots offer a variety of configuration parameters − from simple software solutions to complex hardware complexes, which allows you to adapt them to specific needs and protection goals.

Lures are classified into three main groups according to the level of interaction: low, medium and high. In addition to practical applications, their role in cyber threat research plays an important role. The problem of insufficient information about potential threats is extremely relevant for security professionals, because there are often no clear answers to questions about the sources of attacks, their motives and methods. Honeypots allow not only to detect and track attacks, but also to obtain important information about the methods and tools used by attackers.

As technology advances and the number of connected devices grow, attacks are becoming more sophisticated and sophisticated. In this context, software honeypots become especially relevant, helping to reduce risks for real systems and develop more effective protection strategies. The use of honeypots is a critical component of a cyber defense strategy, providing a deep understanding of new threats and methods of their implementation. Honeypots provide critical data to improve security systems and prevent attacks. However, for maximum effect, such systems must be carefully monitored and configured to avoid potential risks and ensure their effectiveness in combating cyber threats. A balanced approach to the use of honeypots allows you to increase the level of protection and ensure greater security of information systems.

Keywords: cyber defense, cyber threat, vulnerability, honeypot, IoT

Жидка О.В., Дакова Л.В., Даков С.Ю., Поляшенко Д.В. Аналіз використання програмних приманок в Інтернеті речей. У статті розглядається використання програмних приманок як ефективного інструменту захисту інформації в умовах сучасних кіберзагроз. Проводиться детальний аналіз різних типів приманок, їхніх характеристик і функцій, переваг і недоліків, можливих загроз безпеці, а також аспектів конфігурації і загальної ефективності систем. Розглядається як програмні приманки інтегруються в загальну ієрархію інструментів захисту інформації, і оцінюється їхня привабливість і ефективність у боротьбі з сучасними загрозами та атаками. Важливо підкреслити, що навіть за наявності найсучасніших засобів захисту неможливо забезпечити абсолютну невразливість даних компанії, оскільки зловмисники постійно вдосконалюють свої методи атаки. Програмні приманки пропонують різноманітні параметри конфігурації − від простих програмних рішень до складних апаратних комплексів, що дозволяє адаптувати їх до конкретних потреб і цілей захисту. Надаються рекомендації щодо оптимального використання програмних приманок у системах IoT для покращення рівня безпеки.

Ключові слова: кіберзахист, кіберзагроза, вразливість, приманка, IoT

Introduction

In the conditions of the rapid development of the Internet of Things (IoT) and the spread of its influence on various spheres of life, there are more and more threats to information security. Given the openness and accessibility of many IoT systems, data protection is becoming a critical aspect. One of the promising methods of providing cyber protection is the use of software honeypots that allow you to distract attackers and analyze their attack methods. Software honeypots provide an opportunity to create an artificial environment that simulates a real system and serves as a trap for cybercriminals. This provides an additional layer of security that is necessary in the fight against constantly improving methods of cyber threats. This article analyzes the use of software honeypots

in IoT environments, examines their types, functions and configuration options, and evaluates their effectiveness in providing protection against modern cyber threats.

Statement of the problem. In recent years, the rapid development of the Internet of Things has raised significant concerns about the security of networked embedded devices. The number of IoT devices continues to grow, and according to current forecasts, it will exceed 50 billion in 2024. This would result in a potential economic impact of $4 trillion to $12 trillion per year. The Internet of Things is being called the next industrial revolution that will change the way businesses, governments and consumers interact with the physical world.

However, along with the benefits of digital connectivity, which makes it possible to implement ideas that previously seemed fantastic, the threat of cybercrime is also growing. Detection of threats to IoT devices using software honeypots (Honeypot) is extremely relevant in today's environment, when the number of IoT devices is growing rapidly, and the number of cyber threats is also increasing with it. This trend makes IoT devices an attractive target for hackers, as they are often poorly protected.

With this in mind, the use of honeypots becomes critical for detecting and analyzing new types of attacks. Honeypots allow researchers and cyber security professionals to observe the behavior of attackers in real time, gather valuable data about attack methods and thus develop effective countermeasures. Detecting threats using honeypots is not only relevant, but also a necessary measure to protect both individual users and entire enterprises and infrastructures from potential cyber threats. This approach helps to solve one of the key tasks of modern cyber security − reducing risks before they become critical.

Analysis of recent studies and publications. The challenges of protecting IoT systems using honeypots are being studied by many researchers and experts in the field of cyber security. However, in today's world, not many companies are willing to openly share information about the use of this protection technology in their networks. Thus, a study related to the application of software honeypots in international companies, the use of Honeypot for reputation management and detection of intrusions in IoT networks was published in the article [1]. The authors describe how Honeypot can be integrated with IoT systems to improve threat detection and device reputation management.

The authors of the article [2] consider the use of machine learning methods to detect and avoid honeypots in IoT networks. This research is important for understanding how hackers can detect honeypots and how this can be taken into account when designing effective security systems.

The study of the application of machine learning methods for the detection of Honeypot-based flows in the field of cyber security is described in [3]. However, the sheer volume of data generated by Honeypots can be overwhelming for analysts. In this context, machine learning techniques can help automate honeypot data analysis and improve the accuracy of threat detection. Performance is evaluated using real honeypot data. Based on the experimental results, the Random Forest algorithm showed better performance compared to other algorithms, with an accuracy rate of 99.20% for malware detection. The results show that machine learning can significantly improve the performance of Honeypot-based flow detection, allowing cybersecurity analysts to detect and respond to threats faster and more effectively.

These sources are valuable resources for understanding current approaches to securing IoT systems using Honeypots and demonstrate a variety of strategies and techniques that can be applied to improve security in IoT environments.

The purpose of the article is to analyze the application of software honeypots as an effective tool for ensuring information security in Internet of Things systems. The article will conduct a detailed analysis of various types of software honeypots, their characteristics and functions, as well as determine the advantages and disadvantages of their use in the context of information protection. It will consider how software honeypots are integrated into the general hierarchy of information protection tools, and evaluate their attractiveness and effectiveness in combating modern threats and attacks. The paper also aims to provide recommendations on the optimal use of software honeypots in IoT systems to improve security.

Methodology. The hypothesis of this study is that the use of Honeypot in the IoT environment is an effective way to improve the security of these devices and detect threats. Scientific articles, security reports, technical documentation on the development of Honeypot, as well as data obtained in the process of experimental deployment and testing of Honeypot in various IoT environments became the information basis of the research. Methods of literature analysis, data collection using simulations and practical experiments were used to collect and process information. The collected information was analyzed to identify the most effective approaches for deploying Honeypots in IoT networks. For this, a comparative analysis of the effectiveness of different types of Honeypot in detecting threats and their impact on the overall level of security of IoT devices was used. Indicators of system reliability and resistance to attacks were also taken into account. The main limitations of the study include the possible distortion of the results due to the limited scale of testing, the focus on specific types of IoT platforms, and the limitation of resources for conducting long tests. It should also be taken into account that some threats may have gone unnoticed due to the specifics of the selected Honeypot.

Thus, the proposed methodology makes it possible to analyze the effectiveness of using Honeypots to improve the security of IoT devices, as well as to identify possible ways to improve this approach.

Presentation of the main research material.

Honeypot technology. A honeypots is an isolated and disjointed tool that mimics a real network, attractive to attackers. This network can be seen as a fake system that looks like the real thing in order to attract the attention of attackers and become the target of their attacks, allowing them to control the interaction between them and the infected device. Honeypot collects detailed information about the actions of an attacker who interacts with the system in order to identify him. The main purpose of this technology is to identify vulnerabilities in the system and identify the tools and methods that were used to compromise it, in order to mitigate risks and prevent future attacks. In traditional IT security, honeypots are typically used to explore the dynamic threat landscape without risking critical resources [4].

An IoT Honeypot is a specialized application or system designed to attract and detect attacks on IoT devices. The goal of this application is to create a vulnerable environment that simulates real IoT devices and network services so that security researchers can observe attacker behavior, collect attack data, and improve defenses.

Honeypot adoption in IoT is being considered for several reasons: the popularity of IoT platforms, the availability of targeted attackers, and the attractiveness of IoT devices due to their low level of security.

Key features and features of IoT Honeypot:

1. Attracting Attacks − Simulates various IoT devices such as smart cameras, smart thermostats, door locks, and others. These devices look real to attackers, but they are actually traps.

2. Traffic Monitoring − Monitors inbound and outbound traffic, allowing detection of anomalies and suspicious activity such as unauthorized access attempts, port scans, or malware injection.

3. Attack analysis − collects data about attack methods, attackers' IP addresses, used exploits and other details that can help identify vulnerabilities and improve protection measures.

4. Recording and reporting − automatically generates reports on detected attacks that can be used to analyze and improve network security.

5. Integration with other security systems − IoT Honeypot can be integrated with SIEM systems (Security Information and Event Management), which allows for centralized security management and real-time incident response.

6. Customizing the environment − the ability to configure different types of devices and their parameters to reflect specific attacks that can be directed at certain IoT devices.

7. Emulation of various protocols − support for various network protocols often used by IoT devices, such as MQTT, CoAP, HTTP, and others, which allows you to more accurately simulate the behavior of real devices.

Using IoT Honeypot:

1. Threat Research − used to research new types of attacks and malware targeting IoT devices.

2. Improving security − helps identify weak points in IoT devices and develop new methods of protection.

3. Training − can be used as a training tool for cybersecurity professionals to learn how to identify and respond to threats in an IoT environment.

Classification of Honeypot tools. Today, there is a classification of Honeypot tools by the degree of interaction with the attacker, which includes the following categories: low interaction, medium interaction, high interaction.

Each of these types of honeypot provides a certain level of functionality and degree of interaction of the attacker with the system. Accordingly, the functionality of the Honeypot expands as it moves from weak to strong interactions.

Low Interaction Honeypots (LIH) are usually quite easy to install, configure, use and maintain due to their simple structure and basic functions [5]. As a rule, such Honeypot imitate only a part of the services, limiting the attacker's ability to interact with them. Honeypots detect attackers by programmatically emulating the characteristics of a specific operating system, applications, network services, or protocols while running on top of the host operating system. The main advantage of this approach is the ability to gain better control over the attacker's actions and reduce security risks, since the attacker is limited to only the emulated functions. These functions will not work in real operating conditions, but all actions of the attacker will be recorded.

On the other hand, the disadvantage of this approach is that a low-interoperability honeypot emulates only individual services or protocol steps, without reproducing the full design or functionality of such applications or protocols. This can limit the amount of data received and interaction with the attacker. Examples of such Honeypots are Dionaea, Honeyd, NetBait, Kippo and others.

The primary purpose of low-interaction honeypots is to detect scans and unauthorized connection attempts. Since such Honeypots have limited functionality, most of them are presented as software. These programs can be easily installed on the host and configured as per requirements. The task of the administrator is to monitor the alerts generated by the Honeypot, as well as to track changes in the simulated software.

Low-interaction honeypots are recommended for individual use or for small organizations. They may also be useful in improving the understanding of this technology.

Medium Interaction Honeypots (MIH) represent an intermediate option between low- and high-interaction honeypots, providing a balance between ease of use and information gathering capabilities. They give an attacker more opportunities to interact than low-interaction honeypots, but still limit the attacker's actions without giving full access to the system, as is the case with high-interaction honeypots [4].

Medium-interaction honeypots are a powerful tool for threat research and network security monitoring. They provide advanced capabilities for data collection and attack analysis while maintaining a relatively low level of risk to the system. However, they require significant effort and resources to implement, making them more suitable for organizations that have sufficient technical capabilities and experience with such systems.

High Interaction Honeypots (HIH) are mostly real systems that use standard protocol implementations. The main feature of HIH is that, being a real system, it allows full interaction with the attackers, which makes it possible to investigate their actions in real conditions. However, this approach also creates serious security issues, as malicious activities can be implemented on this system.

To minimize these risks, the implementation of HIH involves the deployment of additional monitoring and network control systems that ensure the security of the environment during the actions of attackers. This allows you to gather deep information about the methods and tools used for attacks, while maintaining control over the system and reducing risk to the larger network [6].

Table 1 lists the advantages and disadvantages of HIH, LIH, and MIH.

Table 1

Common Internet of Thing Honeypots

#	Honeypot	Advantages	Disadvantages
1	HIH	Provides a more attractive environment for interaction; deeper interaction with the attacker; collecting more data.	High labor intensity of implementation and support; higher risk of being hacked and controlled by an attacker.
2	LIH	Low labor intensity of implementation; less risk of being hacked and controlled by an attacker; high scalability; does not require a complex computing mechanism.	Limiting the data it can receive; lack of deeper interaction with the attacker.
3	MIH	Ensures balance of cost and derived value of data; higher functionality than LIH.	Higher costs than LIH.

Analysis of classic IoT honeypots. IoT honeypots inherit certain characteristics from traditional honeypots, including the ability to respond to events in real time. Although these honeypots were not originally designed specifically for IoT, they are now used as a basis for research aimed at creating IoT honeypots [7]. Table 2 lists some common IoT honeypots.

Table 2

General Internet of Things honeypots

#	Honeypot name	Level of interaction	Simulation of services
1	IoTPOT	Low	Telnet, HTTP
2	Conpot	Medium	Modbus, S7comm, SNMP
3	Honeyd	Low	FTP, SMTP, Telnet
4	Dionaea	Medium	SMB, FTP, TFTP, HTTP
5	Cowrie	Medium	SSH
6	Glastopf	Low	SSH, Telnet

IoTPOT is a specialized Honeypot designed to emulate different types of IoT devices running different architectures (e.g. ARM, MIPS). It aims to detect and analyze malware that attacks IoT devices, particularly those that target Telnet and HTTP protocols. Supports multiple architectures, capable of capturing and analyzing malicious files, possible integration with a malware analyzer.

Conpot is a Honeypot for Industrial Control Systems (ICS) that can also be used to emulate IoT devices. It emulates various industrial protocols such as Modbus, S7comm, SNMP and can be configured to emulate various IoT devices such as smart meters or other networked appliances. It is easy to configure, supports various industrial protocols, it is possible to emulate various interaction scenarios.

Honeyd is a versatile honeypot that can be configured to emulate various network devices, including IoT devices. It allows you to create virtual hosts on the network that can respond to attackers' requests, simulating the operation of real devices. Flexible in setting, supports various emulations of network devices, has wide opportunities for research.

Dionaea is a honeypot focused on detecting malware that spreads through exploits of network services such as SMB, FTP, TFTP, and HTTP. Although not exclusively IoT-specific, it can be configured to capture attacks on IoT devices.

Cowrie is a honeypot that is mostly used to emulate SSH and Telnet services. It can be configured to impersonate IoT devices, particularly those that are often vulnerable to Telnet attacks. Cowrie allows recording of attackers' sessions, including commands entered during connection.

Glastopf is a honeypot that simulates web servers that can be part of an IoT infrastructure. It is designed to capture attacks against web applications, including SQL injections and other types of malicious traffic that can be directed at the web interfaces of IoT devices.

These Honeypot help researchers understand how attackers attack IoT devices, what methods are used, and which vulnerabilities are most common, allowing for more effective defense strategies.

Conclusions

Honeypot technology provides analysts with a number of important advantages, such as collecting data on hacker activities, low system resource requirements, ease of management, and ease of use. Unlike traditional IDS systems (intrusion detection systems), which log tens or even hundreds of megabytes of information every day, Honeypot generates much smaller amounts of data. This data is 100% of the information required for analysis if the system is properly configured. This means that Honeypot is not resource-intensive and does not require frequent updates or constant technical support - just configure the system and wait.

In addition, the use of honeypots can make a strong case for investment in cybersecurity. If a company invests in IDS and other security systems, and these systems successfully protect the network from intrusions, it may appear that the money was wasted because there are no incidents. In this case, the Honeypot can show that the network is still open to attack and that the investment in security was justified.

In the conditions of the growth of cyber threats for Ukraine, especially against the background of the information war, the issue of building effective systems for the protection of information networks is becoming even more urgent. Protecting critical infrastructures with tools like Honeypots is an important step in strengthening the state's cyber security.

In addition, it is worth noting that with the development of artificial intelligence and machine learning technologies, the capabilities of Honeypots are expanding, which allows even more accurate detection of threats and more effective protection of IoT systems.

Implementation of IoT Honeypot in the network will allow to better understand the threats that can be directed at IoT devices and take timely measures to eliminate them.

List of used literature:

1. Khan, Z.A., Abbasi, U. (2020). Reputation Management Using Honeypots for Intrusion Detection in the Internet of Things. Electronics, 9, 415. DOI: http://dx.doi.org/10.3390/electronics9030415

2. M. Anwer, S. M. Khan, M. U. Farooq, W. Waseemullah, Attack Detection in IoT using Machine Learning, Eng. Technol. Appl. Sci. Res., vol. 11, no. 3, pp. 7273–7278, Jun. 2021. DOI: https://doi.org/10.48084/etasr.4202

3. Diandra Amiruddin Firmansyah, Amalia Zahra. (2023). Honeypot-Based Thread Detection using Machine Learning Techniques, International Journal of Engineering Trends and Technology, vol. 71, no. 8, pp. 243-252. Crossref, DOI: https://doi.org/10.14445/22315381/IJETT-V71I8P221

4. Opirskyy, I., Vasylyshyn, S., & Piskozub , A. (2020). Аналіз використання програмних приманок як засобу забезпечення інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(10), 88–97. DOI: https://doi.org/10.28925/2663-4023.2020.10.8897

5. Mr. Kartik Chawda ,Mr. Ankit D. Patel. (2014). Dynamic & Hybrid Honeypot Model for Scalable Network Monitoring. IEEE. URL: http://www.cse.umich.edu/techreports/cse/2004/CSE-TR-499-04.pdf

6. Lee S, Abdullah A, Jhanjhi N, Kok S. (2021). Classification of botnet attacks in IoT smart factory using Honeypot combined with machine learning. PeerJ Computer Science, 7, 350 DOI: https://doi.org/10.7717/peerj-cs.350

7. Rabhi, S., Abbes, T. & Zarai, F. (2023). IoT Routing Attacks Detection Using Machine Learning Algorithms. Wireless Pers Commun 128, 1839–1857. DOI: https://doi.org/10.1007/s11277-022-10022-7

Автори статті

Жидка Ольга – аспірант, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.
ORCID: 0009-0009-4272-9071

Дакова Лариса – кандидат технічних наук, доцент, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.
ORCID: 0000-0001-6104-8217

Даков Сергій – кандидат технічних наук, Київський національний університет імені Тараса Шевченка, Київ, Україна.
ORCID: 0000-0001-9413-3709

Поляшенко Дмитро – аспірант, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.
ORCID: 0009-0005-2347-0683

Authors of the article

Zhydka Olha – postgraduate, State University of Information and Communication Technologies, Kyiv, Ukraine.
ORCID: 0009-0009-4272-9071

Dakova Larysa – Candidate of Science (technic), Associate Professor, State University of Information and Communication Technologies, Kyiv, Ukraine.
ORCID: 0000-0001-6104-8217

Dakov Serhiy – Candidate of Science (technic), Taras Shevchenko National University of Kyiv, Ukraine.
ORCID: 0000-0001-9413-3709

Poliashenko Dmytro – postgraduate, State University of Information and Communication Technologies, Kyiv, Ukraine.
ORCID: 0009-0005-2347-0683