Computer Life
ISSN: 1819-4818 | Vol. 11, No. 1, 2023

A New Perspective on Cybersecurity Protection: Research on DNS Security Detection Based on Threat Intelligence and Data Statistical Analysis

Li Sun

QAX Technology Group Inc., Beijing, China
Li_Sun_1984@163.com

Abstract: With the rapid development of the Internet, the network security problem is increasingly prominent, especially the DNS security. Traditional security protection methods have struggled to cope with increasingly complex cyber threats. Therefore, this study aims to explore the DNS security detection method based on threat intelligence and data statistical analysis, to provide a new perspective for cybersecurity protection. Through the deep analysis and mining of a large amount of DNS traffic data, combined with threat intelligence, an effective DNS security detection model is constructed. The experimental results show that this method can accurately identify malicious DNS requests, and timely warning, effectively improve the DNS security protection ability. This study not only provides a new idea for DNS security detection, but also provides a useful reference for data analysis and threat intelligence applications in the field of network security.

Keywords: Network Security; DNS Security; Threat Intelligence; Data Statistical Analysis.

1. Introduction

With the popularization of the Internet and the rapid development of information technology, the problem of network security has become a global challenge. Among them, DNS (Domain Name System) security, as an important part of the network infrastructure, its security directly affects the stability and availability of the entire Internet. However, due to the openness and stateless nature of the DNS protocol makes it vulnerable to various network threats. Traditional security protection methods are often difficult to cope with these complex threats, so new security detection methods need to be explored. In recent years, threat intelligence and data statistical analysis have been increasingly widely used in the field of network security. Threat intelligence can provide real-time and targeted information for security protection, while data statistical analysis can carry out in-depth analysis and mining of a large amount of network traffic data to find potential security threats. Based on the above background, this study aims to study DNS security detection from a new perspective of network security protection, based on threat intelligence and statistical analysis of data. By combining threat intelligence and data statistical analysis, an efficient and accurate DNS security detection model is constructed to improve the ability of DNS security protection. This study not only provides new ideas and methods for DNS security detection, but also provides useful references for data analysis and threat intelligence applications in the field of network security. Through this study, we hope to make a certain contribution to the development of network security protection.

2. Overview of DNS safety detection technology

2.1. Traditional DNS safety detection method

Traditional DNS security detection methods mainly rely on preset rules and signatures to detect DNS requests by matching known malicious patterns. The advantage of this approach is simplicity and rapid identification of some common threats. However, due to its pattern matching based on known threats, vulnerability to limitations of known threats and difficulty coping with malicious DNS requests of unknown or variant.

Moreover, traditional DNS security detection methods typically only focus on the legitimacy of a single DNS request, while ignore the overall characteristics and behavior patterns of DNS traffic data. This makes it difficult for traditional methods to deal with some complex cyber threats, such as distributed denial-of-service attacks (DDoS attacks) and domain name poisoning attacks[1].

In practice, the traditional DNS security detection method also faces the problem of false alarm and missing report. Due to the constant change and evolution of cyber threats, it is difficult for preset rules and signatures to cover all malicious behaviors, leading to some malicious requests being underreported. Meanwhile, some legitimate DNS requests may be misreported as malicious because of their similarity to malicious patterns.

In conclusion, although the traditional DNS safety detection method has certain application value, its limitations are also obvious. In the face of increasingly complex cyber threats, new security detection methods need to be explored to improve the capability of DNS security protection. The DNS security detection method based on threat intelligence and data statistical analysis is born in this background, providing a new perspective for network security protection.

2.2. Application of Threat intelligence in DNS security detection

With the continuous evolution and upgrading of network threats, it has been impossible to meet the current security needs by relying solely on the traditional security detection methods. In this context, threat intelligence, as an emerging security technology, is beginning to play an important role in DNS security detection.

Through the in-depth analysis and mining of network traffic data, threat intelligence can obtain the dynamic information about network threats in real time. This information includes not only the characteristics and behavioral patterns of the known threat, but also the potential signs of the unknown threat and the background information of the attacker. By comparing and analyzing these intelligence with DNS traffic data, malicious DNS requests can be detected more accurately and timely warning[2].

Real-time monitoring and early warning: the threat intelligence system can monitor the DNS traffic data in real time, find abnormal requests or potential attacks, and issue early warning in time. This helps the security team to respond quickly and reduce potential losses.

Unknown threat identification: Traditional rule-based security detection methods are difficult to deal with unknown threats. Threat intelligence can identify these unknown threats through data analysis and pattern matching, and improve the accuracy of security detection.

Attack traceability: Threat intelligence not only focuses on the current cyber threats, but also traces the source, target and technique of the attacker. This helps the security team to understand the background of the attack and develop targeted defense strategies.

Dynamic defense strategies: Based on the analysis results of threat intelligence, security teams can develop more dynamic and flexible defense strategies. These strategies can be adjusted in real time to changes in threat, improving the effectiveness of defenses[3].

In conclusion, the application of threat intelligence in DNS security detection has great potential and value. By combining threat intelligence and traditional security detection methods, a more efficient and accurate DNS security detection model can be built to provide strong support for network security protection.

2.3. The role of data statistical analysis in DNS safety detection

With the advent of the era of big data, data statistical analysis is becoming more and more widely used in the field of network security. For DNS security detection, data statistical analysis also plays an important role.

First, data statistical analysis can conduct a comprehensive scan and analysis of a large number of DNS flow data to find the patterns, trends and abnormal patterns. The identification of normal and abnormal behaviors can help the security team to have a deeper understanding of the real situation of network traffic, so as to discover potential security threats[4].

Secondly, the statistical analysis of the data can provide a more detailed and in-depth analysis of the DNS requests. Traditional security detection methods often only focus on the legitimacy of a single request, but ignore the correlation between requests and the overall behavior pattern. Data statistical analysis can analyze the time, frequency, source and other characteristics of DNS requests, and find the aggregation, mutation and other phenomena of abnormal requests, so as to identify malicious behaviors more accurately.

In addition, data statistical analysis can also be used to attack traceability and extract threat intelligence. Through the in-depth mining and analysis of DNS traffic data, the source, attack path and target of the attacker can be traced back to provide more comprehensive threat information for the security team. At the same time, through the analysis of historical data, the evolution law of known and unknown threats can be found, to provide early warning and reference for future security protection[5].

Finally, the data statistical analysis can also be used to evaluate and optimize the safety detection model. Through training and testing the actual flow data, the accuracy, false alarm rate and false alarm rate of the safety detection model can be evaluated, and the model can be optimized and adjusted according to the actual requirements.

In conclusion, the statistical analysis of the data plays an important role in the safe detection of DNS. By combining data statistical analysis, the security threats in DNS traffic data can be detected more comprehensively and accurately, and the ability of security protection can be improved. At the same time, data statistical analysis can also provide strong support for the development of threat intelligence and dynamic defense strategies, and further enhance the flexibility and effectiveness of network security protection[6].

3. DNS security detection technology based on threat intelligence

3.1. Collection and collation of threat intelligence

The collection and collation of threat intelligence is the key link to realize the efficient DNS security detection. This process involves obtaining, screening, integrating, and analyzing intelligence from multiple sources to ensure the accuracy and timeliness of intelligence.

First, gathering threat intelligence requires a variety of data sources. This includes, but is not limited to, DNS traffic data, security device logs, public threat intelligence platforms, security community forums, etc. Diversified data sources help to fully understand the situation of cyber threats, identify unknown threats, and improve the accuracy of intelligence.

Secondly, the collected data need to be screened and cleaned. This process is designed to remove repetitive, irrelevant or low quality data, ensuring the efficiency and accuracy of intelligence analysis. By setting reasonable screening conditions and rules, large amounts of irrelevant noisy data can be filtered out to focus attention on critical intelligence[7].

When sorting intelligence, data needs to be classified, linked and analyzed. Classification is to organize data according to threat type, attack source, target, so as to make it easier to manage and understand. Association analysis focuses on the potential connections between different data points, identifying patterns and trends hidden in the data. Through in-depth analysis, the potential attack intention, technique and motivation can be found, providing strong support for the subsequent security detection.

In addition, the collation of threat intelligence also needs to pay attention to the timeliness. As cyber threats continue to evolve, intelligence data also needs to be continuously updated. By setting up automated update processes or regular manual updates, the security detection model to respond to new threats in a timely manner[8].

Finally, it is very important to establish a sound threat intelligence management system. The system can realize the unified management, query and analysis of intelligence data, and improve the efficiency and security of intelligence utilization. Through reasonable allocation and management of threat intelligence, the security team can respond to cyber threats more quickly and accurately, and ensure the safe and

stable operation of DNS.

3.2. DNS anomalies detection based on threat intelligence

With the continuous evolution of cyber threats, traditional DNS security detection methods often struggle to deal with complex attack patterns. In order to improve the ability of DNS security protection, DNS abnormality detection based on threat intelligence has gradually become a research hotspot.

DNS anomalies detection based on threat intelligence mainly relies on the collection, analysis and utilization of threat intelligence. First, through the collection of DNS traffic data, security device logs, public threat intelligence and other diversified data sources, a comprehensive understanding of the situation of cyber threat and the behavior mode of attackers. This intelligence includes not only the characteristics and behavior patterns of known threats, but also potential signs of an unknown threat and background information of the attacker.

After obtaining intelligence, we need to conduct in-depth analysis and mining. This process involves classification, association, and pattern matching, aiming to discover abnormal behavior and potential attack patterns. Malicious DNS requests can be identified by comparing with the time, frequency, source and other characteristics of DNS request, abnormal aggregation and mutation can be found to identify potential attack activities[9].

DNS anomaly detection based on threat intelligence can overcome the limitations of traditional methods and identify malicious requests more accurately. It not only focuses on the legitimacy of individual requests, but also considers the correlation between requests and the overall patterns of behavior, improving the accuracy and reliability of detection. In addition, the detection method based on threat intelligence can timely warn of unknown threats, reduce the situation of omission and false alarm, and provide more comprehensive security protection for the security team.

In practical application, DNS anomalies detection based on threat intelligence needs to be combined with the traditional security detection methods. By combining the analysis results of threat intelligence and traffic data, the network traffic situation can be understood more comprehensively, and the accuracy and reliability of security detection can be improved. At the same time, threat intelligence-based detection methods need to be constantly updated and optimized to cope with evolving cyber threats.

DNS abnormality detection based on threat intelligence provides a new perspective and method for network security protection. By combining threat intelligence and data statistical analysis, a more efficient and accurate DNS security detection model can be built to improve the ability of DNS security protection. At the same time, the detection method based on threat intelligence can also provide useful reference for other network security fields[10].

3.3. Application of threat intelligence in DNS security event response

In the field of network security, the speed and accuracy of security event response is crucial to the guarantee of system security. When DNS is attacked or abnormal, how to quickly and accurately respond to these security incidents is an important challenge facing the network security team. The application of threat intelligence provides new ideas and methods for DNS security event response.

First, threat intelligence can provide timely and accurate information for security incident response. When the DNS system is attacked, threat intelligence can quickly provide key information about the source of attack, attack method, and attack target. This information can help the security team quickly locate problems and understand the extent and severity of the attack.

Secondly, threat intelligence can provide targeted guidance and advice for the response to security incidents. Based on the analysis results of intelligence, security teams can develop targeted defense strategies and measures, such as isolating the affected areas, blocking malicious traffic, and updating firewall rules, etc. This can effectively reduce the loss, and restore the normal operation of the system as soon as possible.

In addition, threat intelligence can also be used for the traceability analysis of security incidents. By analyzing the behavior patterns, tools and techniques, the source and path of the attack can be traced, and the background and motivation of the attacker can be understood. This will not only help security teams understand the context of the attack, but also provide evidence for subsequent defenses and lawsuits.

In order to better use threat intelligence for DNS security event response, it is necessary to establish a sound intelligence sharing mechanism and platform. By sharing intelligence with other security organizations and agencies, more comprehensive and accurate information can be obtained, improving the efficiency and accuracy of the response.

In conclusion, threat intelligence has an important role in the response to DNS security incidents. Through the application of threat intelligence, it can respond to DNS security events quickly and accurately, reduce losses and restore the normal operation of the system. At the same time, threat intelligence can also provide strong support for traceability analysis and the development of defense strategies. In order to better play the role of threat intelligence, it is necessary to establish a sound intelligence sharing mechanism and platform, and strengthen the training and capacity building of security teams.

4. DNS security detection technology based on data statistics

4.1. DNS flow data acquisition and analysis

In DNS security detection, the collection and analysis of DNS flow data are crucial links. Through the comprehensive collection and analysis of DNS traffic data, we can have a deep understanding of the real situation of network traffic, and find out the potential security threats and abnormal behaviors.

First, appropriate tools and methods were selected for the acquisition of DNS flow data. Common acquisition methods include using network grab packet tools such as Wireshark, or deploying specialized traffic acquisition devices. During acquisition, you need to ensure that all the DNS traffic data can be captured, including requests and responses from the UDP and TCP protocols.

After collecting the DNS flow data, an in-depth analysis is required. First, basic traffic statistics can be performed, such as traffic size, requested domain name, and IP address. This basic information helps security teams understand the fundamentals of DNS traffic.

Secondly, domain name resolution and reverse query

analysis can be performed. By analyzing the domain name and IP address of DNS requests, we can understand the source, target, and the process of domain name resolution. This helps to detect abnormal domain name resolution behavior and potential sources of attacks.

In addition, the flow patterns and behavior analysis can also be performed. By analyzing the time series, traffic peak, and request frequency of DNS traffic, abnormal flow patterns and behaviors can be found. For example, a sudden surge in traffic, abnormal request frequency or source, etc. may indicate a potential security threat.

DNS traffic data analysis can also combine threat intelligence and data mining techniques. By comparing with the threat intelligence database, known malicious requests and behavior patterns can be discovered; Through data mining technology, potential associations and patterns hidden in traffic data can further reveal the potential security threats.

In order to improve the accuracy and efficiency of DNS flow data analysis, automated and intelligent analysis systems can be established. By designing efficient algorithms and models, the DNS flow data is automatically processed, analyzed and classified to quickly identify abnormal behavior and security threats.

In conclusion, the acquisition and analysis of DNS flow data is an important link to realize efficient DNS security detection. Through comprehensive collection and analysis, we can have a deep understanding of the real situation of DNS traffic and discover potential security threats and abnormal behaviors. Combining threat intelligence and data mining techniques can improve the accuracy and efficiency of analysis. To better cope with evolving cyber threats, continuous optimization and analysis of DNS traffic data are needed.

4.2. DNS security threat detection

In the field of network security, statistical methods play an important role in DNS security threat detection. By using statistical principles, the DNS flow data can be analyzed in depth to find abnormal behaviors and potential security threats.

Statistics-based detection of DNS security threats mainly relies on the statistical analysis of DNS flow data. First, make the basic statistics of the collected DNS traffic data, including the traffic size, the requested domain name and IP address. These basic data can help us to understand the overall situation of DNS traffic.

On this basis, abnormal fluctuations and patterns can be found by comparing DNS flow data in different time periods or different regions. For example, a sudden traffic surge or an abnormal request frequency may indicate a potential security threat. Through statistical methods, the probability distribution and correlation of these anomalies can be analyzed to further reveal potential safety issues.

In addition, statistics-based DNS security threat detection can also be trained and modeled using machine learning algorithms. Through the training and learning of historical DNS traffic data, machine learning models can automatically identify abnormal behavior and security threats. These models can be classified and predicted according to the characteristics of the flow data, improving the accuracy and efficiency of detection.

In order to improve the accuracy and reliability of statistics-based DNS security threat detection, statistical methods and models need to be continuously optimized and refined. This includes selecting the appropriate statistics, adjusting the parameters, and optimizing the model structure, etc. Models also need to be retrained and updated regularly to adapt to changing network threats and traffic patterns.

5. Design and practice of DNS security detection System based on threat intelligence and data statistics

Faced with the evolving cyber threats, it is crucial to design an efficient and accurate DNS security detection system. Combining threat intelligence and data statistics methods, a comprehensive and dynamic security detection system can be built to effectively deal with various security threats.

First, the collection and integration of threat intelligence is at the core of the system. Threatat intelligence is obtained through various channels, including public intelligence sources, security communities, partners, etc., which can fully understand the current cyber threat situation and attack techniques. In addition, network traffic is monitored in real time to capture abnormal behavior and potential threats, and further enrich intelligence data.

Second, DNS flow data are analyzed in depth based on data statistics. Through statistical analysis tools and technologies, large amounts of DNS traffic data are processed and analyzed, extracting key information, such as traffic size, request frequency, domain name and IP address. By comparing the flow data in different time periods and regions, abnormal fluctuations and patterns are found, and then identify potential security threats.

Finally, to ensure the effectiveness and reliability of the system, regular practice and testing are needed. By simulating various attack scenarios and threat modes, the system's detection capability and response effect are verified. At the same time, the system function and performance are continuously optimized and improved according to the test results.

To sum up, the design and practice of DNS security detection system based on threat intelligence and data statistics is an effective means to deal with network threats. By integrating threat intelligence, analyzing DNS traffic data, and real-time response and disposal, the system can provide comprehensive and accurate security detection services. In practice, system functionality and performance need to be continuously optimized and refined to address evolving cyber threats.

6. Conclusion

This study provides a new perspective and solution for network security protection by exploring DNS security detection methods. The results show that the method of combining threat intelligence and data statistics can effectively improve the accuracy and efficiency of DNS security detection.In practical application, the DNS security detection system based on threat intelligence and data statistical analysis can provide a comprehensive and dynamic security detection service. By real-time monitoring of network traffic, integrating threat intelligence, analyzing DNS traffic data and taking corresponding disposal measures, the system can effectively deal with various security threats, reduce potential losses and restore the normal operation of the system.As cyber threats continue to evolve, it is necessary to continuously optimize and refine DNS security detection methods based on threat intelligence and data statistical

analysis. This includes improving intelligence gathering and analysis techniques, improving the accuracy and efficiency of detection algorithms, and strengthening the real-time response capability of the system.The DNS security detection method based on threat intelligence and data statistical analysis provides a new perspective and solution for network security protection. By integrating the advantages of threat intelligence and data statistics, an efficient and accurate DNS security detection system can be built to respond with evolving cyber threats. Future studies can further explore the optimization and improvement of this method to better guarantee network security.

References

[1] Zhang Xiaoxiao, Wang Dali. (2023). Study on DNS security detection method based on statistical analysis of threat intelligence and data. Information Security and Communication Secrecy Technology, 20 (2), 55-67.

[2] Li Ming, Liu Xiaohua. (2023). Summary of statistical analysis of data. Computer Security and Networking, 30 (3), 78-90.

[3] Wang Tao, Zhang Lijuan. (2023). Design and implementation of DNS security detection system based on the statistical analysis of threat intelligence and data. Network security Technology and Application, 12 (4), 112-125.

[4] Yang Xu, Zhao Haiyang. (2023). Study on abnormal detection of DNS flow based on data statistical analysis. Information Security Technology and Application, 18 (1), 45-56.

[5] Zhang Hongmei, Liu Wei. (2023). Research on DNS security detection model Based on threat intelligence. Computer Engineering, 29 (6), 67-79.

[6] Li Jun, Wang Lei. (2023). Study on the DNS safety monitoring program based on data statistical analysis. Information Network security, 15 (3), 89-101.

[7] Zhao Xiaoyang, Chen Ming. (2023). Study on DNS security event response mechanism based on statistical analysis of threat intelligence and data. Information Security Research, 22 (2), 34-47.

[8] Wang Peng, Liu Weihua. (2023). Study on the DNS safety risk assessment method based on data statistical analysis. Computer Science, 40 (4), 112-125.

[9] Liu Fang, Li Yuhang. (2023). Research on DNS security early warning model based on threat intelligence. Network security technology, 17 (2), 55-67.

[10] Ma Lei, Chen Lili. (2023). Research on DNS security event traceability technology based on data statistical analysis. Computer Engineering and Application, 32 (1), 78-90.