*Grenze International Journal of Engineering and Technology, Jan Issue*

# Analysing the Effectiveness of Intrusion Detection Systems against the Mirai Botnet: A Comparative Study

Binu P K[1], Barun Kumar[2] and Rishav Sethia[3]
[1-3]Department of Computer Science and Application, Amrita School of Computing, Amrita Vishwa Vidyapeetham Amritapuri, India
Email: binu@am.amrita.edu, amscp2csc21023@am.students.amrita.edu, amscp2csc21046@am.students.amrita.edu

***Abstract*—The rise of the Internet of Things (IoT) has led to an increased risk of cyber attacks on IoT devices, including botnet attacks. Botnets are networks of compromised devices that can be controlled remotely by cybercriminals to carry out malicious activities, such as distributed denial of service (DDoS) attacks. The Mirai botnet is one of the most notorious botnets that have caused significant damage to IoT devices worldwide. To protect IoT devices from such attacks, intrusion detection systems (IDSs) are used to detect and mitigate attacks.**

**However, the effectiveness of IDSs against botnet attacks is still a subject of debate, as botnets are becoming more sophisticated and difficult to detect. To address this issue, this research paper aims to analyse and compare the effectiveness of three widely used IDSs, namely Snort, Zeek, and Suricata, against the Mirai botnet. The study involves simulating Mirai botnet attacks in a controlled environment and evaluating the performance of each IDS in terms of detection and mitigation capabilities.**

**The findings of this research can help organisations to select and implement effective IDSs to mitigate the impact of botnet attacks on IoT devices. By understanding the strengths and weaknesses of different IDSs, organisations can improve the security of their IoT devices and reduce the risk of cyber attacks. Overall, this research paper contributes to the existing literature on IDSs and their effectiveness against botnet attacks, highlighting the importance of selecting and implementing effective IDSs to protect IoT devices from cyber threats.**

***Index Terms*— Malware, Mirai, IDS, Snort, Zeek, Suricata, Network Security.**

## I. INTRODUCTION

The Internet of Things (IoT) has revolutionised the way we live and work, with a wide range of devices now connected to the internet. However, this also means that these devices are vulnerable to cyber attacks, which can have significant consequences for both individuals and organisations. One of the most significant threats to IoT devices is botnet attacks, which involve a network of compromised devices controlled remotely by cybercriminals to carry out malicious activities. The Mirai botnet is one of the most notorious botnets that have caused significant damage to IoT devices worldwide. In 2016, the Mirai botnet was responsible for a series of DDoS attacks that disrupted internet services in the United States and Europe. The Mirai botnet targets IoT devices that have weak or default credentials, such as routers, cameras, and DVRs, and infects them with malware to form a network of compromised devices.

To protect IoT devices from such attacks, intrusion detection systems (IDSs) are used to detect and mitigate attacks. IDSs monitor network traffic and analyse it for signs of malicious activity, such as unusual network

*Grenze ID: 01.GIJET.10.1.517*

traffic patterns, known attack signatures, and anomalous behaviour. IDSs can be classified into two categories: signature-based IDSs and anomaly-based IDSs. Signature-based IDSs use known attack signatures to de- tect attacks, while anomaly-based IDSs use machine learning techniques to identify anomalous behaviour. The effectiveness of intrusion detection systems (IDSs) in countering botnet attacks is being questioned due to the growing complexity of botnets, which makes them harder to detect. Therefore, this research paper aims to assess and compare the efficiency of three commonly used IDSs, namely Snort, Zeek, and Suricata, in detecting and mitigating Mirai botnet attacks. The study involves simulating Mirai botnet attacks in a controlled setting and analysing the performance of each IDS in terms of detection and mitigation abilities.

The structure of the paper is as follows: Section II provides a brief background, introducing the key terms and concepts related to the research topic. Section III presents a literature review focused on papers specifically addressing the Mirai botnet. This review delves into existing research on botnet attacks, examining the current state of knowledge and identi- fying any research gaps specific to the Mirai botnet. Section IV describes the methodology, detailing the experimental setup and data collection process employed in this study. Section V presents the results, including a comparative analysis of the effectiveness of different approaches in countering the Mirai botnet. Section VI discusses the implications of the findings and provides practical recommendations for organisations to enhance their security against Mirai botnet attacks. Finally, Section VII concludes the paper, summarising the key findings, emphasising their significance, and suggesting future research directions in the field of botnet attacks.

## II. Background

The increasing prevalence of Internet of Things (IoT) devices and their interconnectivity has brought about significant advancements in various domains, ranging from smart homes to industrial automation. However, this rapid expansion of IoT networks has also introduced critical security challenges. One notable threat that has emerged in recent years is the Mirai botnet, a sophisticated malware targeting vulnerable IoT devices.

### *A. Mirai Botnet and the Rise of IoT Devices:*

In 2016, the Mirai botnet gained notoriety from a white hat malware research group, MalwareMustDie [1]. Mirai specifically targeted devices with default or weak credentials, compromising them through brute-force attacks and incor- porating them into a massive botnet capable of launching devastating assaults. The rapid rise of the Mirai botnet can be attributed to the proliferation of IoT devices, which increased exponentially due to the growing popularity and adoption of IoT technologies. The prevalence of weaker security in IoT devices compared to traditional computing devices provided an ample breeding ground for malware like Mirai.

Notably, Mirai was responsible for high-profile attacks, such as the unprecedented 623 Gbps DDoS[2] attack on the Krebs on Security blog and the disruptive DDoS attacks[3] on the Dyn DNS provider, impacting major websites like Amazon, Github, Netflix, PayPal, Reddit, and Twitter. These incidents highlighted the urgency for improved security measures in IoT devices and emphasised the need for robust intrusion detection systems (IDSs) to detect and mitigate botnet threats. The Mirai botnet's rapid growth and significant attacks underscored the risks associated with vulnerable IoT devices and emphasised the importance of strengthening security practices within the IoT ecosystem.

To understand the severity of the Mirai threat, it is crucial to delve into how the Mirai malware operates and communicates. Mirai primarily targets IoT devices, such as routers, cameras, and DVRs, which often have weak security configurations. The malware exploits known vulnerabilities in these devices, typically related to default or easily guessable credentials.

Once a device is infected with Mirai, it establishes commu- nication with a command and control (C&C) server, which serves as the central coordinating point for the botnet. The infected device becomes a bot, and its control is handed over to the botnet operator. Mirai uses custom binary protocols designed specifically for botnet control.

Through the C&C server, the botnet operator can issue com- mands to the infected devices, instructing them to carry out malicious activities. These activities often involve launching large-scale DDoS attacks against targeted websites or services. Mirai utilises the collective computing power of the infected devices to generate massive amounts of traffic, overwhelming the targeted servers and causing disruptions.

Mirai is also capable of conducting reconnaissance, scanning for vulnerable devices to infect and expand its botnet. It utilises techniques such as brute-force attacks to guess default or weak credentials, and it actively seeks out devices with specific vulnerabilities that it can exploit. Fig 1 shows the graphical representation of the communication between the bot, C&C server, Loader and Report Server.

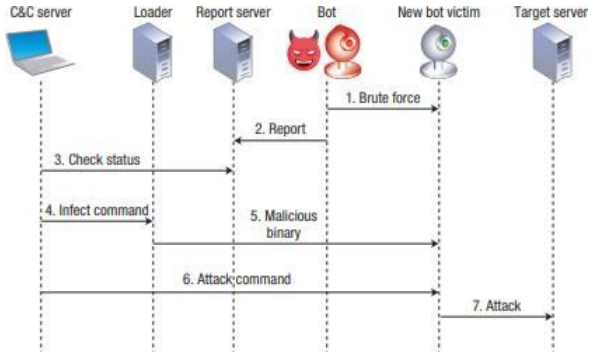


Fig. 1. Mirai Botnet communication and Operation

*B. Intrusion Detection Systems (IDSs) in IoT Networks*

Intrusion Detection Systems (IDSs) play a vital role in monitoring and safeguarding networked systems. They are designed to detect and respond to unauthorised activities and potential security breaches. However, the dynamic nature of IoT devices and the evolving sophistication of malware pose unique challenges for traditional IDSs.

Unlike traditional computing systems, IoT devices exhibit diverse functionalities, communication protocols, and resource limitations. These factors make it challenging to deploy and manage IDSs effectively within IoT environments. Further- more, the sheer volume and heterogeneity of IoT devices make it difficult to develop universal detection mechanisms that can accurately identify and mitigate emerging threats, such as the Mirai botnet.

Consequently, there is a pressing need to analyse the effectiveness of IDSs against the Mirai botnet specifically. Understanding the strengths and limitations of different detec- tion mechanisms and methodologies is crucial to developing robust security measures for IoT networks. By conducting a comparative study, we can evaluate the performance of various IDSs and explore strategies to enhance their effectiveness in countering the Mirai botnet.

In conclusion, the rise of IoT devices and the emergence of the Mirai botnet have significantly impacted the security land- scape. This research paper aims to address the effectiveness of intrusion detection systems in mitigating the threats posed by the Mirai botnet through a comprehensive comparative study. By understanding the vulnerabilities exploited by Mirai and evaluating different IDSs, this research aims to contribute to the development of proactive measures that enhance the security of IoT ecosystems and protect against similar IoT-based threats.

## III. Related Works

Several studies have been conducted to evaluate the Mirai botnet and its attack. In ”DDoS in the IoT: Mirai and Other Botnets,” [4] the authors analyse the Mirai botnet and its variants, and highlight the risks posed by IoT devices. They identify five main reasons why IoT devices are particularly advantageous for creating botnets: constant and unobtrusive operation, feeble protection, poor maintenance, considerable attack traffic, and noninteractive or minimally interactive user interfaces. The authors argue that device vendors should assume responsibility for distributing products with weak security, including default credentials and remote access capabilities. In ”A Practical Analysis on Mirai Botnet Traffic,”

[5] the authors demonstrate the practical functioning of the Mirai botnet based on an isolated hardware testbed. They show the traffic patterns for infection from other hosts, as well as communication with the CnC. The analysis is based on the fingerprints of the traffic patterns to perform detection based on the Mirai traffic signature in real-time. The authors suggest that more general patterns could be learned and applied for detecting other malware and variations of the Mirai source code.In ”The Evolution of Bashlite and Mirai IoT Botnets,”

[6] the authors study the behaviour of the Bashlite and Mirai IoT botnets using data collected by honeypots deployed across Brazil. They show that these botnets and their operators have evolved significantly, with botnet infrastructure becom- ing more resilient and easier to manage, and the software integrating more effective attacks. The authors also provide indications that botnet operators are becoming more proficient at managing and exploiting the capabilities of their botnets, including choosing effective application-layer attacks for each target, automating management, and coordinating attacks.The paper ’Understanding the Mirai Botnet’ [7] presents a retrospective analysis of the Mirai botnet, focusing on answering four research questions: how Mirai emerged and spread, the types of compromised devices and their vulnerabilities, the evolution and competition among

Mirai variants, and the targets and characteristics of Mirai's DDoS attacks. The study combines multiple measurement perspectives and leverages data from various sources to provide a comprehensive dataset covering a seven-month period. The paper reveals that Mirai emerged from the Qbot botnet, targeted vulnerable DVRs and IP cameras, and saw the creation of multiple variants and copycats after its source code was leaked. It also exam- ines Mirai's attack vectors, duration, intensity, and frequency against various targets. The insights from this paper enhance our understanding of the Mirai botnet, its behavior, and its implications for IoT security, offering valuable information for the development of effective countermeasures and inter- ventions against future botnet attacks.

The "Malware Detection and Mitigation Techniques: Lessons Learned from Mirai DDOS Attack" [8] discusses the use of Free and Open Source Software (FOSS) to identify, classify, and remove malware from compromised systems. The focus is on the Mirai botnet, a malware that affected the availability of banking systems and utilized compromised IoT devices for DDoS attacks. The article emphasizes the difficulties in collecting and analyzing malware samples, and highlights the importance of automation in handling these issues. The authors propose using FOSS tools such as ClamAV and Yara to detect and classify malware, and suggest the use of honeypots for monitoring and detecting malicious activity. The article con- cludes that FOSS tools provide a cost-effective and versatile approach to mitigating malware attacks.

The research paper "IoT based Mirai Vulnerability Scanner Prototype"[13] investigates the Mirai malware, drawing paral- lels between its impact on IoT network-enabled devices and the pervasive nature of Covid-19. The paper delves into the underlying concepts, evolutionary aspects, and propagation methods of Mirai. Additionally, it introduces a vulnerability scanner designed to assist home users and network adminis- trators in identifying potential entry points for Mirai within their networks. By simulating attacks akin to those executed by Mirai, the scanner aims to pinpoint vulnerabilities and provide users with actionable recommendations to safeguard their networks against this malware. The ultimate objective of the scanner is to gain insights into the breakpoints and vulnerabilities present in user networks.

The research paper titled "Botnet Detection using Machine Learning" [14] presents a comparative study of supervised and unsupervised machine learning algorithms for detecting botnets in network flow data. Highlighting the significance of internet security and data breach prevention, the paper explores the use of algorithms such as SVM, Random Forest, KNN, K-Means, PCA, and RNN. The study aims to identify and eliminate botnets promptly, contributing valuable insights for network security professionals and researchers in combating this growing threat.

The research paper "Development of Intrusion Detection Sys- tem Using Deep Learning for Classifying Attacks in Power Systems"[15] investigates the application of machine learning algorithms, particularly deep neural networks (DNN), for detecting and classifying cyberattacks in smart power grids. By utilizing a standard power system dataset and comparing various ML models, the study demonstrates that the Random Forest model achieves the highest accuracy in identifying attacks. The findings highlight the potential of DNN, along with other ML algorithms, in developing effective intrusion detection systems for securing power grid infrastructure.

The research paper "An Integrated Approach to Network Intrusion Detection and Prevention"[16] explores the imple- mentation of machine learning algorithms, specifically K- Nearest Neighbor (KNN) and Support Vector Machine (SVM), in an Intrusion Detection System (IDS) to enhance real-time anomaly detection. The paper also introduces a novel method for preventing Denial-of-Service (DoS) attacks by blocking malicious IP addresses in routers. This integrated approach contributes to strengthening the security of computer networks in the face of evolving threats.

The research paper "A compendium on network and host- based intrusion detection systems"[17] offers a comprehensive exploration of deep learning and neural network models in the context of Intrusion Detection Systems (IDS). It provides a detailed analysis of methodologies and showcases the potential of deep learning techniques in enhancing intrusion detection capabilities. The paper serves as an extensive resource for understanding the application of these advanced techniques in IDS.

The research paper "Network Intrusion Detection System Using Stacking and Boosting Ensemble Methods"[18] explores the implementation of anomaly-based network intrusion detection using stacking and boosting ensemble methods. The study aims to develop an efficient intrusion detection system with high accuracy and detection rate while minimizing false alarms. Evaluations are conducted on the NSL-Knowledge Discovery Dataset, showcasing the importance of network security in an interconnected environment.

The papers reviewed provide a detailed understanding of the Mirai malware and botnet, and demonstrate the importance of implementing effective security practices to mitigate this threat. Through our analysis, we have identified various pat- terns in the Mirai botnet traffic and the evolution of its behaviour, as well as the increased proficiency of botnet opera- tors in managing and exploiting their capabilities.The findings has helped us to

analyse the effectiveness and performance of different IDS in detecting and mitigating the threat posed by the Mirai botnet.

## IV. Methodology

The purpose of this study was to analyse the effectiveness of intrusion detection systems (IDS) against the Mirai botnet. To achieve this goal, we utilised VMWare virtualization software on a computer with an AMD 4600H processor and 16 GB of RAM to simulate a network environment infected by the Mirai botnet.

We used four virtual machines (VMs) to set up the network environment. The first VM was the router, which acted as the gateway between two subnets. The bot VM was on one subnet, while the loader and CNC VMs were on another. The router had 4 logical processors and 1 GB of RAM allocated to it, while the CNC had 2 logical processors and 1 GB of RAM. The loader had 2 logical processors and 1 GB of RAM allocated to it, and the bot had 1 logical processor and 1 GB of RAM allocated to it To simulate the mirai botnet we have used the released source code of Mirai [9].

We chose Arch Linux as the operating system for the bot VM because it is minimal and can run on devices with fewer resources. The CNC VM acted as the command and control centre, while the loader VM loaded and executed the Mirai malware into the bot VM. The bot VM was infected by the Mirai malware to simulate a botnet.

To analyse the effectiveness of IDS against the Mirai botnet, we installed three IDS systems (Snort [10], Zeek [11], and Suricata [12]) on the router VM. The IDS systems were configured to detect and alert us to any malicious activity on the network. We then measured the effectiveness of each IDS system by analysing the number of alerts generated, their accuracy, and the resources they consumed.

We chose Snort, Zeek, and Suricata for this study because they are widely used and have proven to be effective against various types of network attacks. Snort is a signature-based IDS that uses rules to detect known threats. Zeek (formerly known as Bro) is a network security monitoring tool that generates high-level protocol analysis. Suricata is a network IDS that combines signature-based detection with anomaly- based detection.

We conducted our experiments by running the Mirai botnet in the network environment and measuring the effectiveness of the IDS systems. We then analysed the results and compared the performance of each IDS system. Our evaluation criteria included the number of alerts generated, their accuracy, and the resources consumed.

In summary, this study utilised VMWare virtualization soft- ware and four VMs to simulate a network environment in- fected by the Mirai botnet. We installed three IDS systems (Snort, Zeek, and Suricata) on the router VM and measured their effectiveness against the Mirai botnet. By doing so, we aimed to provide insights into the strengths and weaknesses of IDS systems in detecting and mitigating botnet attacks.

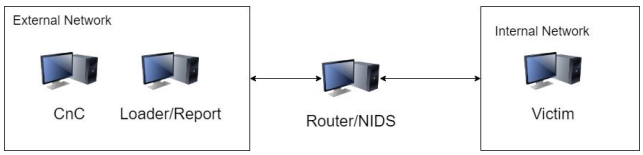


Fig. 2. Network Architecture

## V. Results

Based on the results of our comparative study analysing the effectiveness of intrusion detection systems (IDSs) against the Mirai botnet, we observed notable differences in the performance of the evaluated systems.

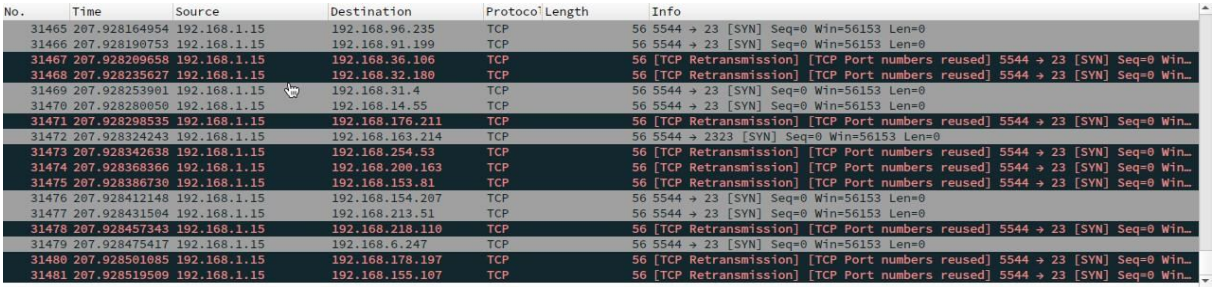


Fig. 3. Traffic of a device affected by Mirai

Fig. 3 illustrates the traffic generated by a device infected with the Mirai malware. The infected device continuously sends SYN packets to port 23 (telnet) in order to determine if the port is open, targeting random IP addresses within the specified IP range.

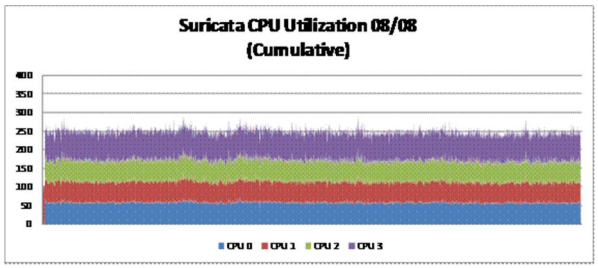


Fig. 4. Suricata CPU usage

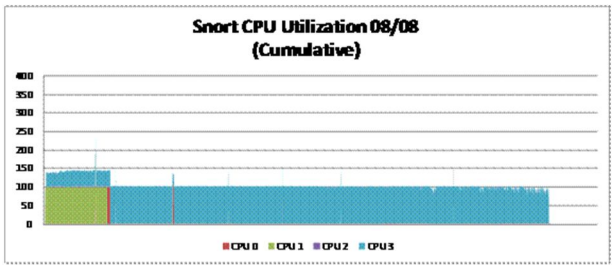


Fig. 5. Snort CPU Usage

The CPU usage of Snort and Suricata is visually depicted in Figures 4 and 5, respectively. These figures provide valuable insights into the computational resource utilization of these in- trusion detection systems, shedding light on their performance and efficiency in terms of CPU utilization. The comparison of CPU usage between Snort and Suricata helps to evaluate and understand the resource requirements and potential impact on system performance when employing these intrusion detection systems. In contrast, both Suricata and Zeek, out of the box, did not exhibit similar detection capabilities for Mirai botnet activity. They did not produce any specific alerts or indications of suspicious patterns associated with the botnet. This highlights the importance of customization and rule development in these systems to enhance their ability to detect and mitigate Mirai botnet attacks effectively.

These findings underscore the necessity of configuring and fine-tuning IDSs to optimise their detection capabilities for specific threats like the Mirai botnet. While Snort demon- strated initial capabilities in detecting network anomalies re- lated to Mirai botnet scanning through SYN packets, further analysis and customization may be required to enhance the out-of-the-box performance of Suricata and Zeek.

Overall, our study highlights the importance of understanding the strengths and limitations of different IDSs and emphasises the need for organisations to carefully tailor and refine their chosen IDSs to effectively detect and mitigate sophisticated botnet attacks like Mirai. Further research and customization efforts are warranted to enhance the out-of-the-box perfor- mance of Suricata and Zeek in detecting Mirai-specific threats arising from the scanning behaviour of the malware, which involves sending SYN packets to random addresses within the network range.

| Features | NIDS | | |
|---|---|---|---|
| | *Snort* | *Suricata* | *Zeek* |
| Lightweight | Yes | No | No |
| Multi-threaded | No | Yes | No |
| Open-source | Yes | Yes | Yes |
| Default Rules | Yes | No | No |
| User Friendly | Yes | No | Yes |

## VI. Implications and Recommendations

The findings of this study have several implications for organisations seeking to protect their IoT devices from botnet attacks. Firstly, the study reveals that Snort emerged as the most effective IDS in this research. Its effectiveness, combined with its lightweight nature, makes it an ideal choice for deployment on low-resource IoT devices such as Raspberry Pi. Furthermore, Snort's long-standing presence in the field has contributed to its maturity and the existence of a large open-source community supporting its development.

Secondly, Suricata, another IDS examined in the study, stood out for its user-friendly interface and ease of use. This aspect makes Suricata an attractive option for organisations looking for simplicity in implementing an effective IDS solution.

Lastly, Zeek was identified as a valuable tool for network monitoring and traffic analysis. While not directly related to IDS functionality, its inclusion in the study highlights its potential for assisting organisations in detecting and mitigating botnet attacks through comprehensive network analysis.

In conclusion, this study underscores the importance of carefully selecting an IDS solution based on factors such as effectiveness, resource requirements, user-friendliness, and community support. Snort's effectiveness and suitability for low-resource IoT devices, Suricata's user-friendly interface, and Zeek's network monitoring capabilities are all valuable considerations for organisations aiming to enhance their IoT device security against botnet attacks.

## VII. Conclusion

According to the study's findings, the performance of out- of-the-box NIDS (Network Intrusion Detection System) was found to be unsatisfactory, except for Snort's ability to de- tect unreachable ICMP packets due to community rules. To enhance detection capabilities and improve security against botnet attacks, organisations are advised to obtain rules subscriptions for both Snort and Suricata.

Alternatively, organisations can opt to create custom rules specifically tailored to their unique needs. By developing rules from scratch, organisations gain the flexibility to define detection criteria that align with their network environment and potential threats. This approach enables a more targeted and precise detection of botnet attacks. Regardless of the chosen approach, it is crucial for organisations to invest in effective rule management. This includes keeping rules up to date through regular updates and maintenance. By ensuring the NIDS remains equipped with the latest rules, organisations can enhance its effectiveness in detecting evolving botnet attacks, providing vital protection for their IoT devices and network infrastructure.

In addition to strengthening the NIDS, organisations should prioritise the improvement of IoT device security by imple- menting essential measures. This includes changing default passwords to unique and strong credentials, applying security patches promptly to address known vulnerabilities, and regularly updating firmware to benefit from security enhancements and bug fixes. These actions collectively contribute to mitigating the risk of botnet attacks and bolstering the overall cybersecurity posture of organisations and their IoT devices.

## References


[1] MalwareMustDie, https://blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html.

[2] ArsTechnica,https://arstechnica.com/information-technology/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever.

[3] The Guardian, https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

[4] C. Kolias, G. Kambourakis, A. Stavrou and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," in Computer, vol. 50, no. 7, pp. 80-84, 2017, doi: 10.1109/MC.2017.201.

[5] G. Gallopeni, B. Rodrigues, M. Franco and B. Stiller, "A Practical Analysis on Mirai Botnet Traffic," 2020 IFIP Networking Conference (Networking), Paris, France, 2020, pp. 667-668.

[6] A. Marzano et al., "The Evolution of Bashlite and Mirai IoT Botnets," 2018 IEEE Symposium on Computers and Communications (ISCC), Natal, Brazil, 2018, pp. 00813-00818, doi: 10.1109/ISCC.2018.8538636.

[7] Manos Antonakakis, Tim April, Michael Bailey, Matthew Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou. 2017. Understanding the mirai botnet. In Proceedings of the 26th USENIX Conference on Security Symposium (SEC'17). USENIX Association, USA, 1093–1110.

[8] Jaramillo, Luis Eduardo Suástegui. "Malware Detection and Mitigation Techniques: Lessons Learned from Mirai DDOS Attack." Journal of Information Systems Engineering \& Management (2018): n. pag.

[9] Mirai released Source Code https://github.com/jgamblin/Mirai-Source-Code.

[10] Snort, https://www.snort.org/.

[11] Zeek, https://zeek.org/.

[12] Suricata, https://suricata.io/.

[13] S. Vysakh and P. K. Binu, "IoT based Mirai Vulnerability Scanner Prototype," 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2020, pp. 97-101, doi: 10.1109/ICSSIT48917.2020.9214099.

[14] K. B. Aswathi, S. Jayadev, N. Krishna, R. Krishnan and G. Sarath, "Botnet Detection using Machine Learning," 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2021, pp. 1-7, doi: 10.1109/ICCCNT51525.2021.9579508.

[15] Ankitdeshpandey and R. Karthi, "Development of Intrusion Detection System Using Deep Learning for Classifying Attacks in Power Systems ", in Soft Computing: Theories and Applications, Singapore, 2020.

[16] B. Bhanu Prakash, Kaki Yeswanth, M. Sai Srinivas, Balaji S., Y. Chandra Sekhar, and Aswathy K. Nair, "An Integrated Approach to Network Intrusion Detection and Prevention", in Inventive Communication and Computational Technologies, Singapore, 2020.

[17] Kumaran U., "R. Vigneswaran, Poornachandran, P., and Dr. Soman K. P., "A Compendium on Network and Host based

Intrusion Detection Systems", in Lecture Notes in Electrical Engineering, 2020.
[18] V. Sidharth and C. R. Kavitha, "Network Intrusion Detection System Using Stacking and Boosting Ensemble Methods," 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2021, pp. 357-363, doi: 10.1109/ICIRCA51532.2021.9545022.