CC7178NI Cyber Security Management
Cyber Security and Risk management on IoT Devices

Assessment Weightage & Type

50% Individual Coursework

Year

2023/2024 Spring

Student Name: Manish Gurung

London Met ID: 17030839

College ID: NP01MS7S240020

Assignment Due Date: 6th May 2024

Assignment Submission Date: 6th May2024

Word Count: 3461

I confirm that I understand that my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Abstract

The proliferation of IoT devices has brought a new age of connectivity, transformed industries and increased efficiency. However, this development has also brought with it several security issues, from IoT architectural flaws to cyberattacks aimed at networked systems. Cyber-attacks targeting IoT devices have escalated in the last three years. The rise in average weekly IoT cyber-attacks per sector highlights the growing threat. Through an analysis of Mirai Botnet's large-scale DDoS attacks and Stuxnet Worm's infiltration of critical infrastructure, this report highlights the urgent need for robust cybersecurity measures. The crucial role of mitigation strategies, stakeholder collaboration, and cybersecurity resilience in navigating the dynamic threat landscape is highlighted with key findings.

Table of Contents

Table of Figures

1 Introduction

Figure 1: Internet of Things (IoT) (Intuz, 2023)

Internet of Things (IoT) refers to the network of physical devices, appliances and other physical objects which are embedded with sensors, software and network connectivity which then allows them to collect and share data (IBM, n.d.). The arrival of IoT has brought a new era of connectivity which has permanently revolutionized how devices interact, communicate, and operate. It has spread over many domains which include smart homes, healthcare, transportation, and many industries. This interconnected network of physical devices, sensors, actuators, and other smart objects enhances efficiency and results in enrichment of user experiences. Although this proliferation of digital technology in the form of IoT devices has greatly revolutionized how everything operates, it also brings an increase in cyber threats such as data breaches and malware attacks. Due to the interconnected networks, diverse endpoints and cloud-based services, usage of IoT devices leads to the 'attack surface' being amplified which makes it challenging to maintain security. This is because numerous of these devices lack strong security features and can be exploited easily.

1.1 Problem Definition

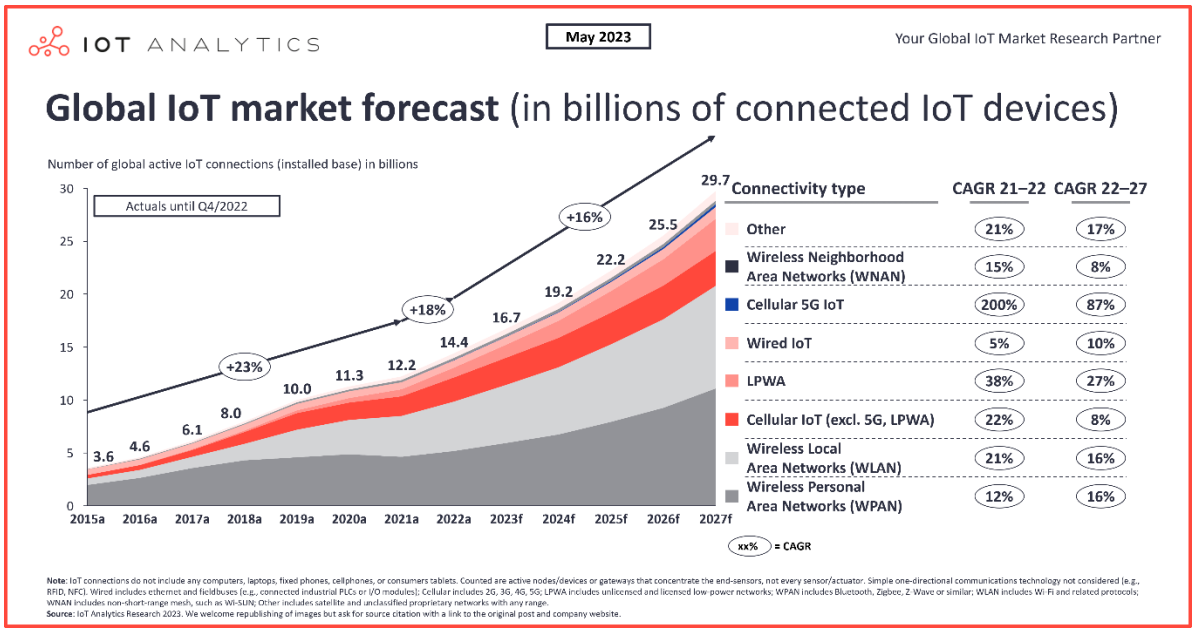

Figure 2: Global IoT Market Forecast (IoT Analytics, 2023)

The rapid proliferation of IoT devices has brought a multitude of security concerns which stem from the complexities and vulnerabilities present in an interconnected system. Unlike traditional computing devices, IoT devices have a resource-constrained environment. They have limited power, memory, and energy resources as well. Consequently, these devices lack robust security mechanisms which are present in conventional computing systems which makes them prone to cyber-attacks.

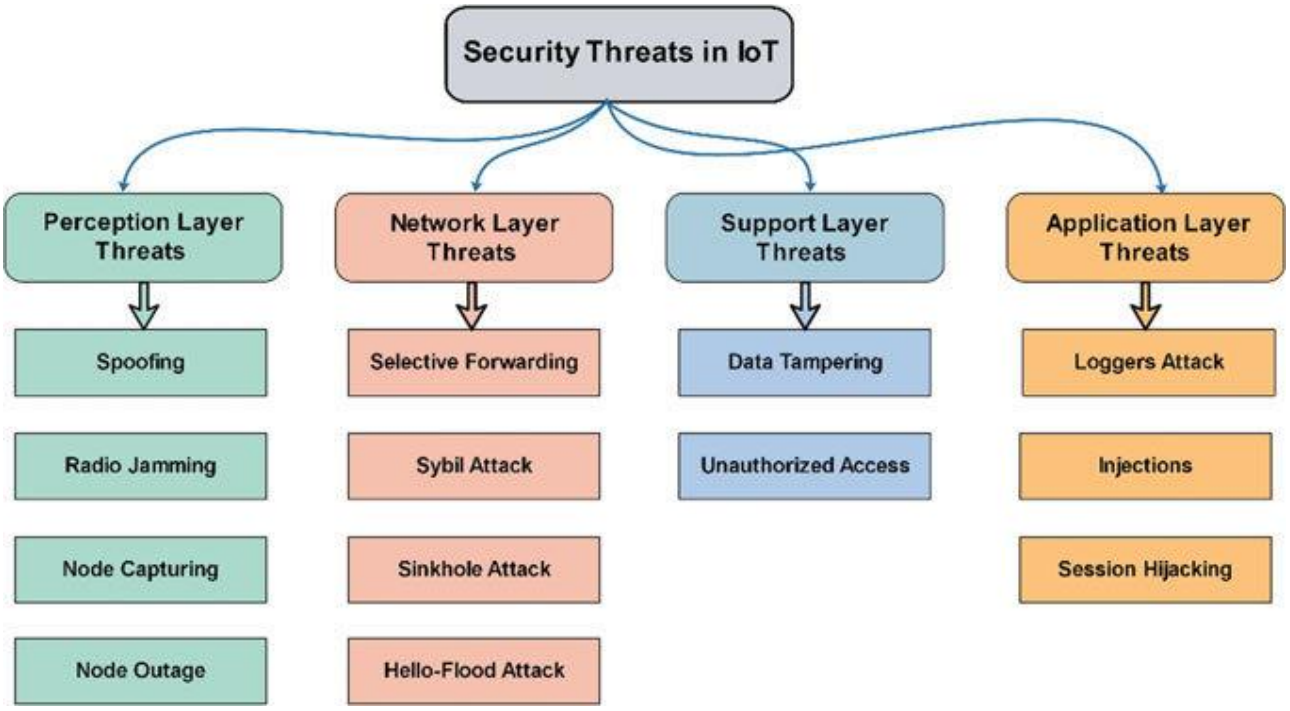

Figure 3: Security threats in IoT (Hany F. Atlam, 2019)

As shown above, security threats in IoT devices can span over multiple layers of the IoT architecture which includes the perception, network, support, and application layers. In the perception layer, threats such as physical tampering, sensor spoofing, and side-channel attacks compromise device integrity and data accuracy. The network layer risks things like man-in-the-middle attacks, denial-of-service attacks, and rogue devices that threaten data confidentiality, availability, and authenticity. The support layer faces challenges like weak authentication, data leakage, and insider threats, impacting the security of backend infrastructure and cloud platforms. Finally, in the application layer, vulnerable interfaces, malicious firmware, and lack of security updates pose risks to user privacy and device security.

1.2 Current Scenario

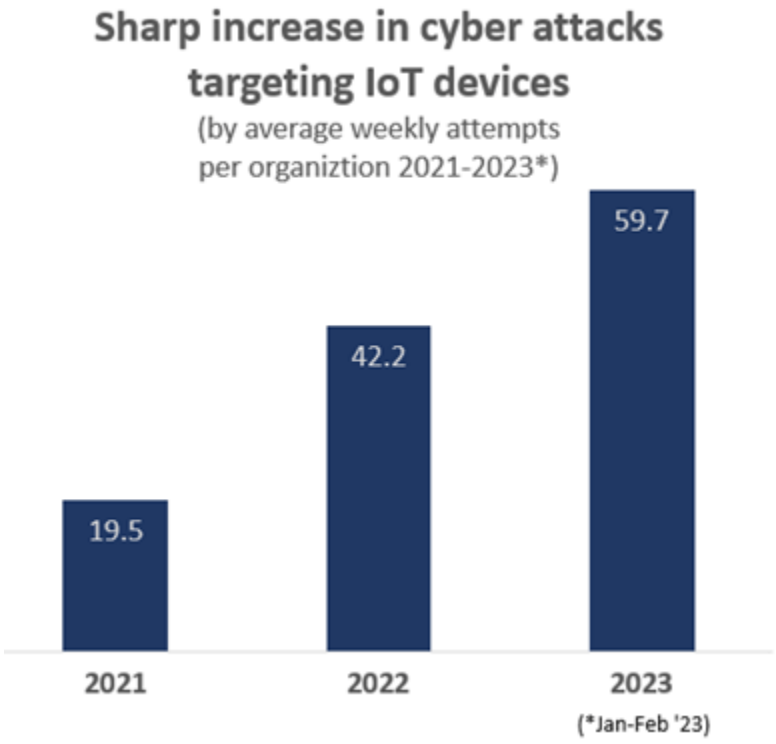

Figure 4: Cyber Attacks Targeting IoT devices (Check Point, 2023)

As shown in the above figure, there has been a trend of escalation with cyber attacks that target IoT devices within the last three years. From 2021 to 2023, the number of cyber attacks targeting IoT devices has risen to an extreme, rising from 19.5 attacks in 2021 to 59.7 attacks in 2023. This data shows the vulnerability of IoT ecosystems and the need for enhanced security measures for proper protection of interconnected devices.

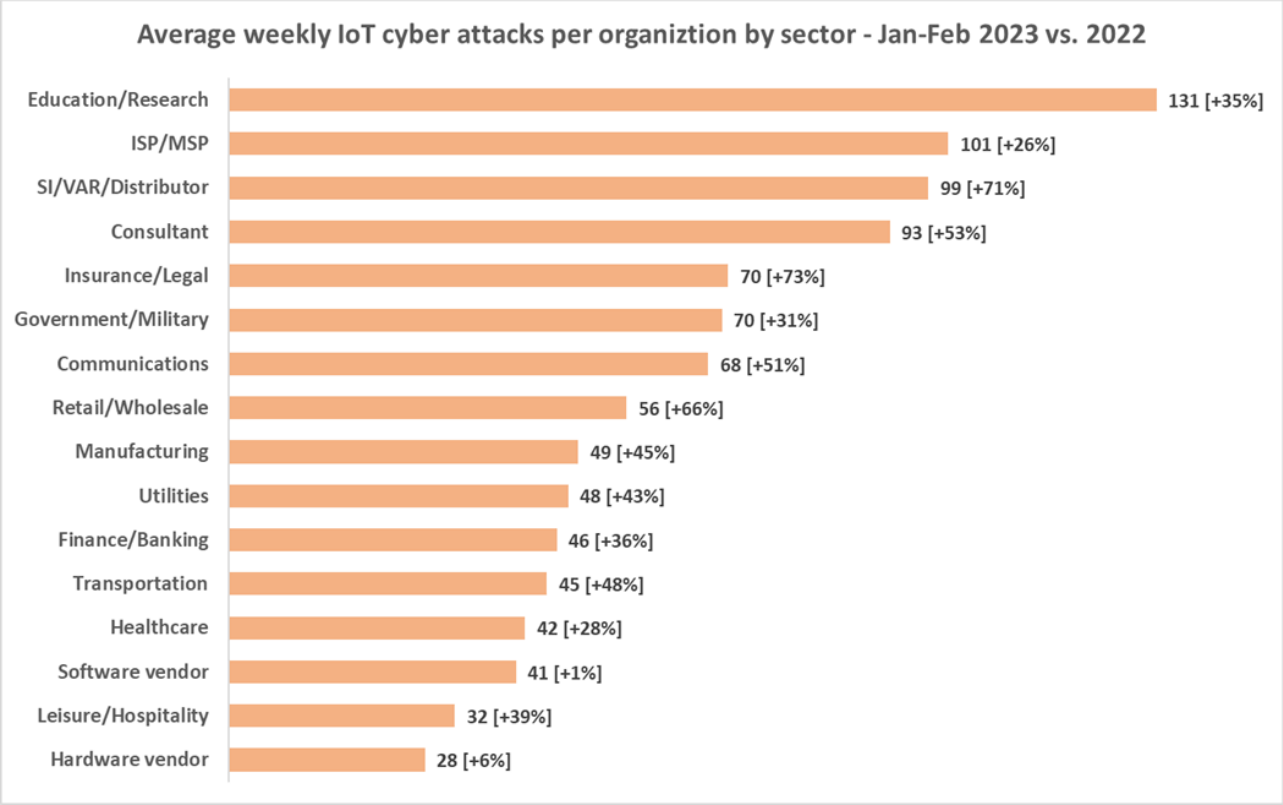

Figure 5: Average Weekly IoT Cyber Attacks per sector (Check Point, 2023)

The figure above illustrates the rise in average weekly IoT cyber attacks per organization across various sectors, which highlights the increasing threat faced by organizations worldwide. Each sector is experiencing a substantial increase in cyber attacks as compared to the previous year, ranging from education, research, healthcare to finance/banking and transportation. With such a significant increase, the vulnerabilities present in IoT security need to be addressed.

As usage of IoT devices continues to increase, organizations must invest in advanced security solutions to resist cyber threats. They must conduct regular security assessments and continuous monitoring to strengthen their defenses against increasing threats. Failure to address these cyber risks could result in severe consequences such as data breaches, operational disruptions, and reputational damage as well.

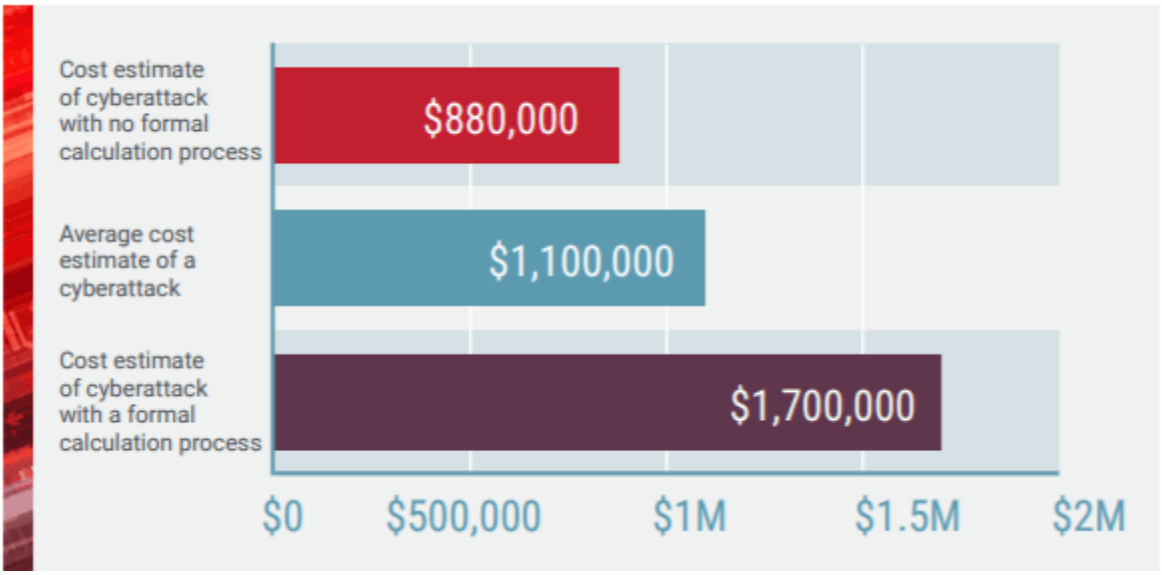

Figure 6: Cost of Cyberattacks (Radware, 2019)

It is crucial to recognize the substantial financial costs that occur due to cyberattacks. With the attempts of cyberattacks rapidly increasing, the financial costs over the past few years have been amounting to an alarming number. As shown in the above figure, the average cost estimate of a cyberattack amounts to $1,100,000 while the cost estimate of a cyberattack with a formal calculation process amounts to $1,700,000. This data shows concerns regarding the increasing cyberattacks and the critical importance of effective cybersecurity measures needed.

The findings from a recent survey and analysis released by KeyFactor and Vanson Bourne showcased the current state of IoT security and revealed the financial toll from cyberattacks. According to the report, 89% of organizations operating and utilizing IoT and connected products have fallen victim to cyber-attacks, with an average cost of $250,000 per incident (Vanson Bourne, 2019). This data shows the urgency in implementing robust cybersecurity measures to lessen the financial risks which occur due to the vulnerabilities of IoT.

2 Literature Review

The increased usage of IoT devices has brought a lot convenience and efficiency to multiple industries. However, this has also introduced significant cybersecurity challenges as well. In the new age of IoT, there are millions or even billions of connected devices which are susceptible to cyberattacks. These cyberattacks take various forms and target mostly all the vulnerabilities that are present in an IoT device and structure.

2.1 Cybersecurity in IoT Architecture

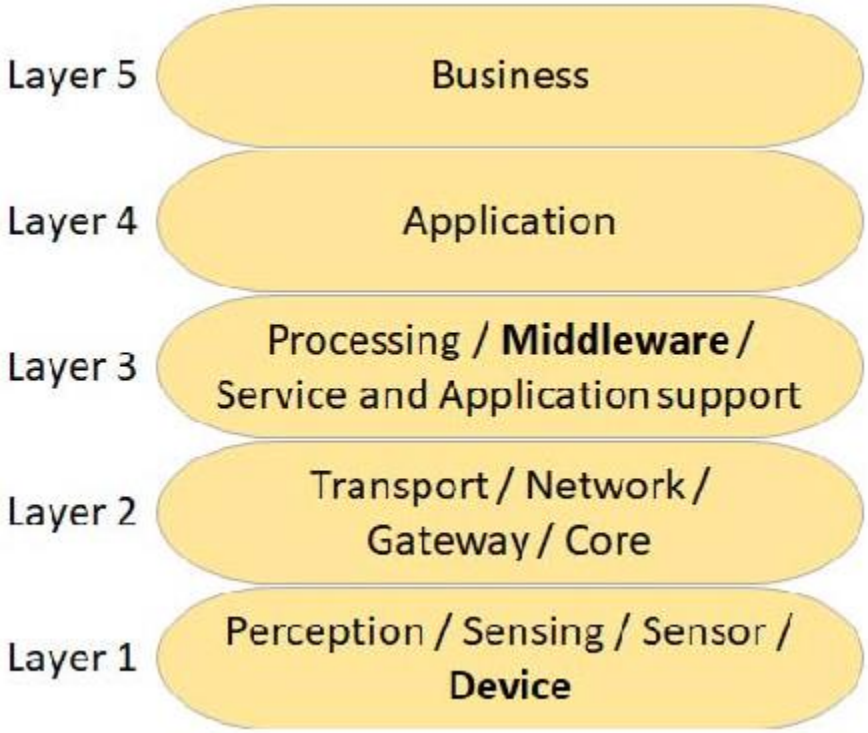

Figure 7: Layers of IoT Architecture (Wunck & Baumann, 2017)

Perception Layer

At the forefront of IoT architecture lies the perception layer which consists of sensors and actuators. These components gather data from the environment and also interact with it directly. Due to this reason, they become a prime target for various cyber-attacks. The security of the perception layer needs to be ensured to make sure that the data collected is accurate.

Network Layer

The network layer is often known as the backbone of an IoT system which facilitates communication between devices and backend systems. The network layer is vulnerable to cyber-attacks such as man-in-the-middle attacks and denial-of-service attacks. Robust network security protocols need to be implemented to protect against such mentioned cyber threats.

Processing Layer

In the processing layer, the data collected from the sensors is first analysed and then processed to give some meaningful insights. The processing layer is very susceptible to security risks such as unauthorized access and data manipulation. Implementation of encryption and access control mechanisms is needed to reduce these risks and ensure integrity of data processing operations within organizations.

Application Layer

In the application layer, user interfaces, APIs and applications that interact with IoT devices are present. Insecure interfaces and malicious firmware are some of the risks that have an effect on the security of an IoT system. Secure software development practices need to be implemented and regular updates of firmware should be done to increase the security of the application layer

Service Management Layer

The management and orchestration of IoT services and resources belongs to the service management layer. Weak authentication mechanisms and inadequate access controls in this layer can lead to unauthorized access and data breaches. Strengthening authentication mechanisms and implementing strong access control policies are important to protect IoT resources.

2.2 Applications of IoT Devices

Essentially, IoT devices are the devices which are connected to a network so the applications of IoT devices could be endless. Almost any object can be equipped with the appropriate technology that can be able to help in data transmission from IoT devices and their connected networks.

- **Healthcare Applications** – IoT is reshaping healthcare with IoT sensors such as the AliveCor heat monitor which enables remote patient monitoring, helping in early disease detection and other parameter tracking. Sensors collect vital information such as temperature, heart rate and glucose levels which improves medical devices and leads to better health outcomes. (Baker, et al., 2017)

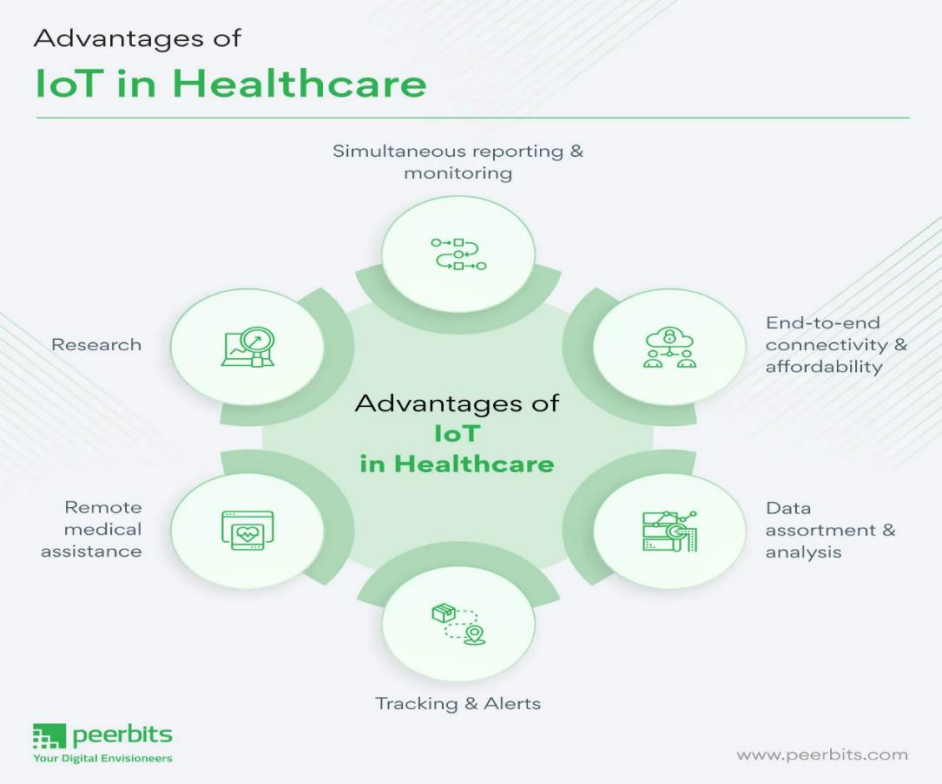

Figure 8: Advantages of IoT in Healthcare (Pisuwala, 2023)

- **Agricultural Applications** – IoT technology can play a vital role in reducing agricultural waste and in enhancing supply chains. Automation through wireless sensor networks can improve some processes, such as irrigation, maximizing crop yields. Real-time monitoring enables for better responses to soil conditions and optimising water usage. These IoT devices can provide better insights to help in decision making for agricultural purposes.
- **Smart Cities –** IoT technology in smart cities enables efficient urban management, including real-time traffic monitoring and smart waste management with IoT-enabled containers. Additionally, IoT devices predict air quality for environmental monitoring.

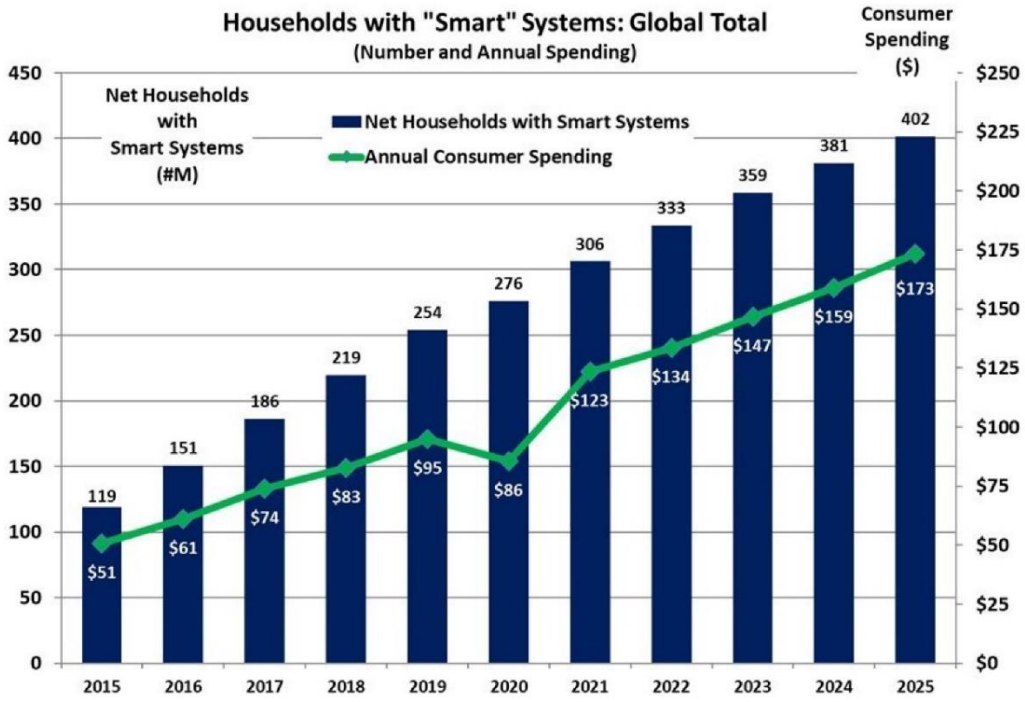

Figure 9: Households with Smart Systems: Global Total (Businesswire, 2021)

- **Smart Home Applications –** IoT sensors can manage home conditions, appliances and access by focusing on home automation. These devices provide assistance and convenience by remote control which can be extremely beneficial for elderly in particular. . The smart home market is growing rapidly, driven by the popularity of devices like Amazon and Google speakers, with a projected market value of USD 155 billion by 2023. (Businesswire, 2021)

2.3 Challenges

2.3.1 Security of IoT devices

Although the widespread use of IoT devices brings a lot of convenience, it also raises significant security concerns. Devices like mobile phones, medical sensors, and security systems are increasingly vulnerable to cyberattacks, such as the Mirai malware, which converts devices into botnets for Distributed Denial of Service (DDoS) attacks. Such poorly protected IoT devices with open designs get targeted by the attackers most commonly. Since IoT devices often collect sensitive data, these data transmissions can be intercepted by third parties who intend to conduct harm or use these data for foul purposes. The entire network of IoT devices used could be disrupted by attackers, which could lead to devastating effects.

2.3.2 Authentication and Password Security

One of the main security issues faced by IoT devices is lack of security regarding authentication and passwords. Having weak passwords makes devices vulnerable to cyberattacks as they can be easily cracked by the hackers/attackers. There is a high need for stronger authentication methods for such devices. Complex passwords and multi-authentication can help verify user identities before providing access. Implementing robust authentication measures is essential to safeguard IoT devices from unauthorized access as well as cyber threats.

2.3.3 Interoperability Challenges

Interoperability is a key challenge in the smooth operation of IoT devices, as they often operate on different infrastructures and protocols. International organizations like IEEE and the Internet Engineering Task Force develop standards to improve compatibility. Protocols such as Bluetooth and ZigBee establish rules for communication, addressing interoperability concerns. Initiatives like the BiG IoT project aim to create a common API for IoT devices to communicate effectively. Standardization efforts are crucial for ensuring seamless interaction between diverse IoT devices, facilitating their integration, and enhancing the overall functionality of IoT systems. (Chataut, et al., 2023)

3 Critical Analysis

3.1 Case Study: Mirai Botnet

3.1.1 Background

The Mirai botnet is a malware which was designed to hijack IoT devices and then convert them into ‘bots’ which would be controlled remotely, while being able to launch powerful distributed denial of service (DDoS) attacks. (Radware, n.d.) It infects smart devices which run on ARC processors which turns them into a network of remotely controlled bots. ‘Botnet’ is the network of bots which is most used to launch DDoS attacks. (Cloudfare, 2024)

Mirai Botnet was created by three young men named Paras Jha, Dalton Norman, and Josiah White. Mirai was initially created as part of a Minecraft scam for the purpose of knocking rival Minecraft servers offline using DDoS attacks. The Mirai botnet then expanded and spread to infect thousands of IoT devices and then conducted full, large-scale attacks. (Malwarebytes, 2023)

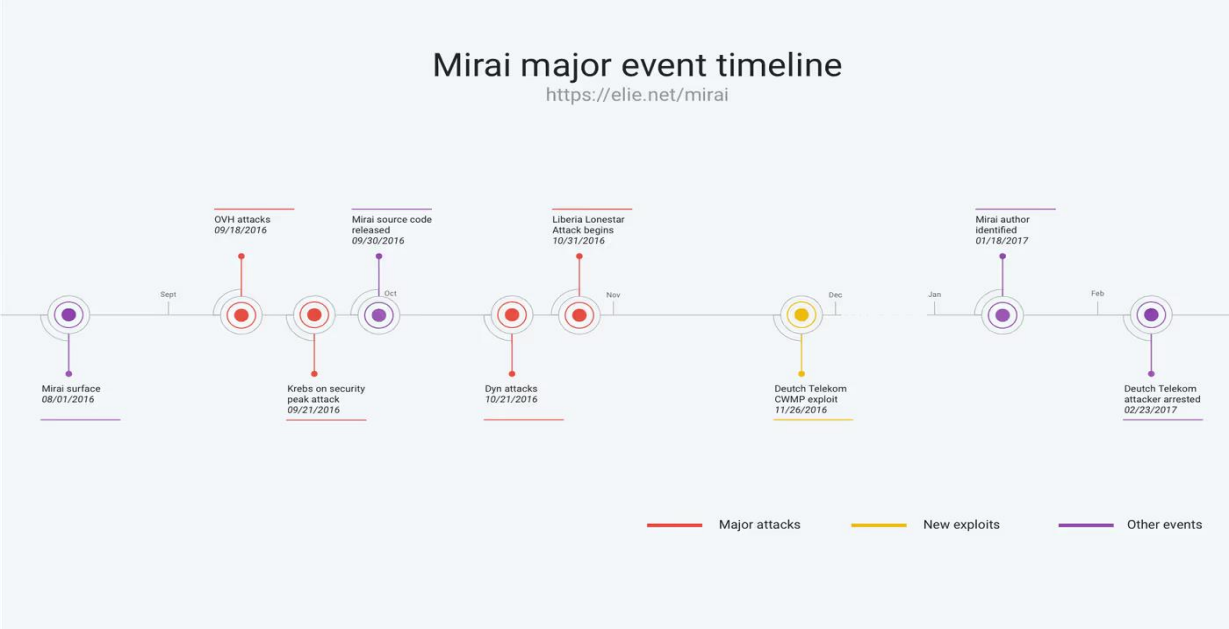

Figure 10: Mirai major event timeline. (Bursztein, 2017)

3.1.2 Issue Identification

In September 2016, Mirai launched its first large-scale attack against a French technology company known as OVH. The main reason why OVH was the main target was due to the fact that OVH hosts roughly 18 million applications. The attack, which peaked at 1Tbps which also demonstrated the power of the botnet. It is estimated that around 145,000 devices were used within the assault on the technology company. After that, the second largest attack peaked around 400 Gbps. (CIS, 2024)

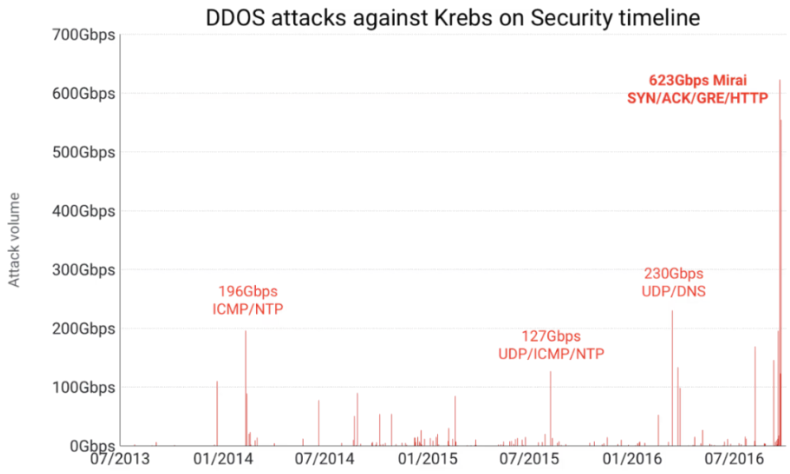

Figure 11: DDoS attacks against Krebs on Security timeline (Bursztein, 2017)

Subsequently, the next target of the Mirai Botnet was, Krebs on Security, which was created by Brain Krebs. He was a journalist in the line of investigative journalism into cyber-related crimes which was mainly the reason why Krebs on Security was attacked next as it was seen as a potential threat. In late September 2016, Krebs on Security was flooded with over 600GB of data. (CIS, 2024). On September 30th 2016, Mirai was published as a source code by "Anna-senpai" to a public and easily accessible forum. This action led to the proliferation of copycat hackers running their own Mirai botnets, making it extremely difficult to understand the motives behind attacks more challenging. The ambiguity of the Mirai attacks posed significant difficulties for cybersecurity experts in effectively countering the threat.

3.1.3 Mitigation

To mitigate the risks posed by such attacks, some practices are present, which are recommended by the Center for Internet Security (CIS) and Cybersecurity and Infrastructure Security Agency (CISA). Such mitigations which are to be followed are: -

- **Network Segmentation** – It is critical to ensure that all IoT devices are on a separate network from such systems which are critical. This way the potential impact of botnet infections can be limited and unauthorized access to sensitive data and resources can be minimized as well.
- **Regular Updates** – Infections can be reduced when IoT devices are up to date. Make sure to update IoT devices with the latest firmware to ensure a lesser chance of attacks and infections.
- **Anti-Virus Software –** Anti-Virus software provides protection for your computer and other devices against most viruses that your devices come to face. It is crucial to use anti-virus software and make sure to keep it up to date.
- **Password Policies and Authentication** – Enforcing strong password policies and using multifactor authentication can significantly enhance the security of IoT devices. This reduces the risk of attacks as well as unauthorized attacks. Complex passwords and regular password changes should be made, which are always important to enhance security.
- **Anti-Malware Tools/System** – Anti-Malware tools and systems should be placed to help in detecting and preventing botnet infections as well as other suspicious activities on IoT networks. Monitoring network traffic is vital to early threat detection and also in preparing for a response which minimizes the impact of such attacks.

3.1.4 Summary

The Mirai botnet poses a serious threat to cybersecurity because it may organize large-scale DDoS attacks and disrupt critical services by taking advantage of the weaknesses of IoT devices. The evolution of the Mirai and its variants highlight the complexity of lowering the risks of IoT botnet threats. To defend against such threats, organizations need to be following strict security policies and benchmarks, implementing network segmentation, maintaining regular updates, and strengthening authentication mechanisms. By adopting such an approach and taking all the necessary steps, organizations can mitigate the risks which are posed by Mirai Botnet and other malicious attacks.

3.2 Case Study: Stuxnet Worm

3.2.1 Background

Stuxnet is a computer worm which was originally aimed at Iran's nuclear facilities. However, since then it has mutated and spread to many other industrial and energy producing facilities (Trellex, 2023). It is quite commonly known now that Stuxnet was created by the intelligence agencies of the United States and Israel, however, it was first identified by the infosec community in 2010. It is presumed that Stuxnet's development began around 2005. It was created as a tool to derail or delay. It was believed that if Iran were on the verge of developing atomic weapons, then this could ultimately lead to a regional war starting. (Fruhlinger, 2022)

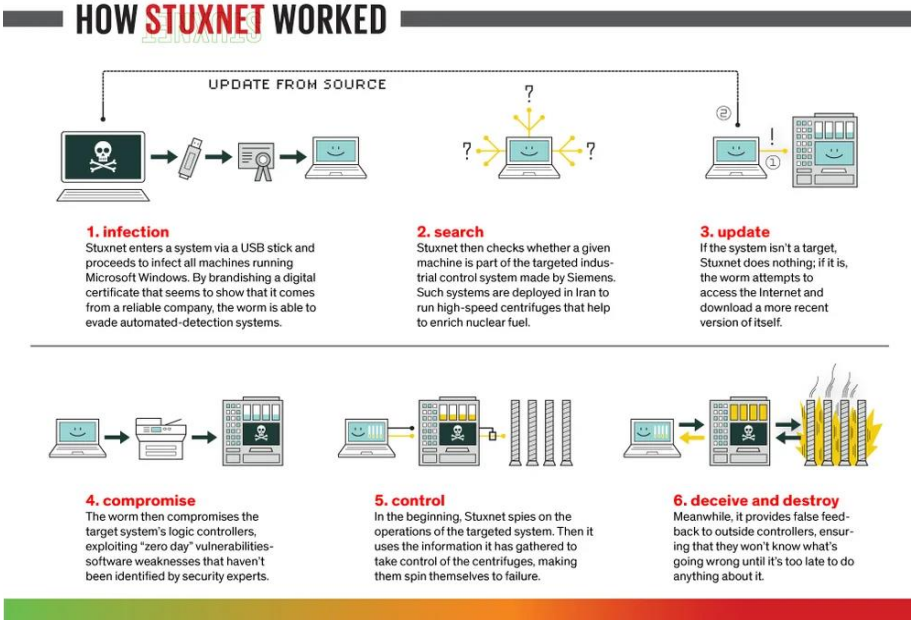

Figure 12: How Stuxnet worked (L-Dopa, 2024)

Stuxnet infects the system through the means of USB sticks, targeting machines that run Microsoft Windows. It then displays a fake digital certificate that appears trustworthy. Stuxnet checks if a system is part of the Iranian nuclear enrichment program, and if not, it remains inactive. If it's a target, Stuxnet accesses the internet to download updates, compromises system logic controls, spies on operations, and takes control of centrifuges, causing system failures.

3.2.2 Issue Identification

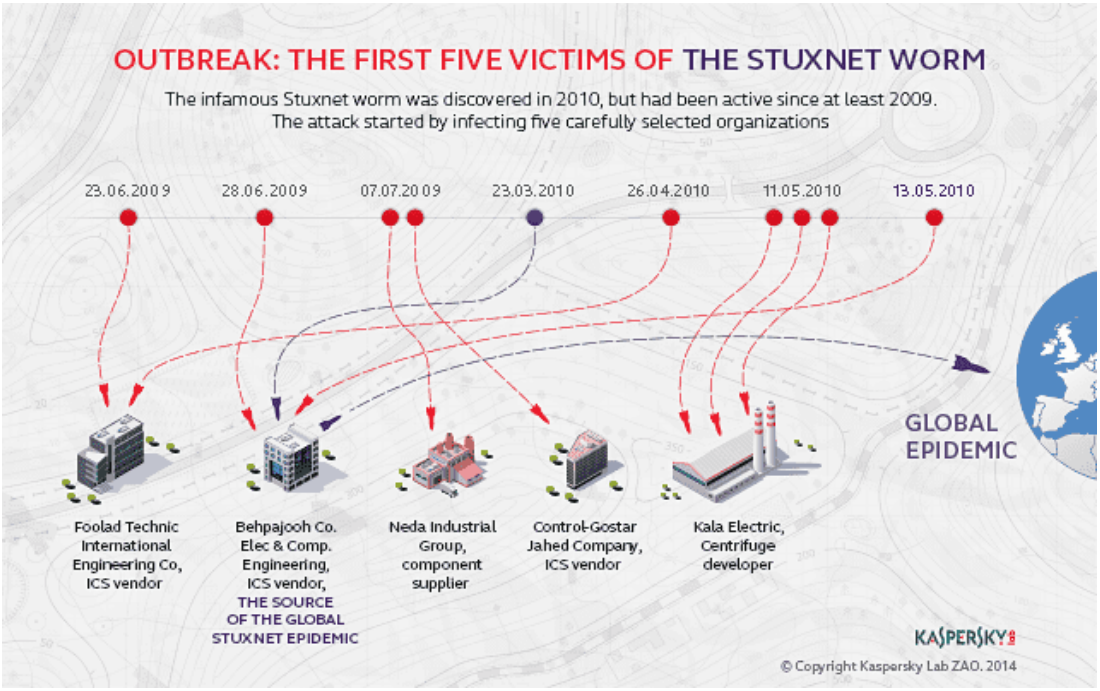

Figure 13: First Five Victims of Stuxnet (Kaspersky, 2014)

Stuxnet Worm was first discovered in 2010 however, it was found to be active since at least 2009. As shown in the above figure, the initial phases of the Stuxnet worm consisted of five attacks on organizations working in the ICS area in Iran, developing ICS or supplying materials and parts. On 23rd June 2009, Foolad Technic International Engineering received the first attack of the Stuxnet worm. Shortly after on 28th June 2009, Behpajooh Co. Elec & Comp. Engineers were the second victim, just five days later. Multiple attacks followed the same organizations.

The fifth organization that was attacked, namely Kala Electric, was surprising as it produces uranium enrichment centrifuges. With this information it can be believed that the main target of the Stuxnet was this kind of equipment.

Over fifteen Iranian facilities are said to have been attacked and infiltrated by the Stuxnet worm with its initiation coming from a random worker's USB drive. Although specific details have not been released regarding the effects of these attacks, it can be estimated that the Stuxnet worm destroyed 984 uranium enriching centrifuges. This led to 30% decrease in enrichment efficiency by estimation. (Holloway, 2015)

3.2.3 Mitigation

Several Mitigation Measures have been recommended to reduce the risk of infection as well as minimize the impact of Stuxnet on systems: -

- **Microsoft Security Patches** – Applying Microsoft security patches such as MS08-067 and MS10-046b can be helpful to address the known vulnerabilities that are exploited by Stuxnet worm. This can help prevent Stuxnet from exploiting the system if in case of infiltration.
- **Vendor Recommendations** – Following Vendor recommendations for system upgrades and patch applications will ensure better compatibility as well as provide better effect.
- **Restrictive Policies –** Establishing internal policies to restrict or disable USB drives is a vital role in prevention of Stuxnet. As USB drives are a common vector for the propagation of Stuxnet malware, restricting and disabling USB drives can help prevent the infiltration of the malware.
- **Cleanup Procedures & Consultation** - Owners of infected systems, especially those running Siemens software, should carefully analyze and seek guidance from Siemens Customer Support. Collaboration with ICS-CERT can provide additional analysis and support for mitigating Stuxnet infections.
- **Collaboration** – Collaboration with Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) can be beneficial for additional analysis and support for mitigating Stuxnet infections.

3.2.4 Summary

In conclusion, Stuxnet is an important event in the history of cyberwarfare, showing the possibility that nation-states may utilize malware as a means of surveillance and attack against vital infrastructure. It takes a multifaceted strategy, including patch management, network segmentation, and security awareness training, to reduce the risks posed by Stuxnet and related threats. However, to prevent such attacks, governments, industry stakeholders, and cybersecurity professionals must continue to collaborate and practice caution due to the ever-evolving nature of cyber threats.

4 Conclusion

In conclusion, the study of IoT security through two major case studies—the Mirai Botnet and the Stuxnet Worm, shows the vital role that cybersecurity plays in a society growing more interconnected. Undoubtedly, the spread of IoT devices has benefited many different industries, transforming business, increasing productivity, and enhancing user experiences. But these developments also bring with them a variety of security issues that need to be resolved to protect against malicious attacks.

Unchecked vulnerabilities in IoT devices can have disastrous consequences, as demonstrated by the Mirai Botnet case study. Through a series of large-scale DDoS attacks, Mirai demonstrated the potential for widespread disruption and highlighted the urgent need for robust security measures. The Stuxnet Worm case study highlights the possibility of highly skilled cyberattacks aimed at critical systems, demonstrating the constantly changing nature of cyberthreats and their possible consequences for national security.

From the two case studies, a lot of key takeaways can be seen. Firstly, the interconnected nature of IoT ecosystems leads to the attack surface being amplified, making cybersecurity measures a topmost priority for organizations. Secondly, mitigation strategies such as network segmentation, regular updates and strong authentication protocols are a must for reducing the risk of exploitation and minimizing the impact of cyber-attacks. Also, collaboration and information sharing between key industry stakeholders, government and cybersecurity professionals is crucial to stay prepared for any emerging threats. This way risk management strategies can be formed through which organizations can mitigate the risks that are associated.

The findings emphasize the significance of investing in cybersecurity resilience to effectively defend against the numerous challenges that are constantly presented with an ever-changing threat landscape. The potential of IoT technologies is limitless and as they continue to develop, it is of vital importance to prioritize security to safeguard against malicious actors and ensure the safety and reliability of interconnected systems.

5 References

Baker, S., Xiang, W. & Atkinson, I., 2017. *Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities,* s.l.: IEEE.

Bursztein, E., 2017. *Inside Mirai the infamous IoT Botnet: A Retrospective Analysis.* [Online]
Available at: https://elie.net/blog/security/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/
[Accessed 26 March 2024].

Businesswire, 2021. *Strategy Analytics: Global Smart Home Market Roaring Back in 2021.* [Online]
Available at: https://www.businesswire.com/news/home/20210706005692/en/Strategy-Analytics-Global-Smart-Home-Market-Roaring-Back-in-2021
[Accessed 29 March 2024].

Chataut, R., Phoummalayvane, A. & Akl, R., 2023. *Unleashing the Power of IoT: A Comprehensive Review of IoT Applications and Future Prospects in Healthcare, Agriculture, Smart Homes, Smart Cities, and Industry 4.0,* s.l.: s.n.

Check Point, 2023. *Check Point.* [Online]
Available at: https://blog.checkpoint.com/security/the-tipping-point-exploring-the-surge-in-iot-cyberattacks-plaguing-the-education-sector/
[Accessed 11 March 2024].

CIS, 2024. *The Mirai Botnet – Threats and Mitigations.* [Online]
Available at: https://www.cisecurity.org/insights/blog/the-mirai-botnet-threats-and-mitigations
[Accessed 27 March 2024].

Cloudfare, 2024. *What is the Mirai Botnet?.* [Online]
Available at: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/
[Accessed 25 March 2024].

Fruhlinger, J., 2022. *Stuxnet explained: The first known cyberweapon.* [Online]
Available at: https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html
[Accessed 26 March 2024].

Hany F. Atlam, A. A. M. O. A. A. A. A. B. W., 2019. Principles of Internet of Things (IoT). In: *Principles of Internet of Things (IoT) Ecosystem: Paradigm.* s.l.:s.n.

Holloway, M., 2015. *Stuxnet Worm Attack on Iranian Nuclear Facilities,* s.l.: Standford University.

IBM, n.d. *What is the Internet of Things (IoT)?.* [Online]
Available at: https://www.ibm.com/topics/internet-of-things
[Accessed 8 03 2024].

Intuz, 2023. *IoT Device Management: Importance, Challenges, Solutions.* [Online]
Available at: https://www.intuz.com/guide-on-iot-device-management
[Accessed 8 March 2024].

IoT Analytics, 2023. *State of IoT 2023.* [Online]
Available at: https://iot-analytics.com/number-connected-iot-devices/
[Accessed 10 March 2024].

Kaspersky, 2014. *Stuxnet Patient Zero: First Victims of the Infamous Worm Revealed.* [Online]
Available at: https://www.kaspersky.com/about/press-releases/2014_stuxnet-patient-zero-first-victims-of-the-infamous-worm-revealed
[Accessed 27 March 2024].

L-Dopa, 2024. *IEEE Spectrum.* [Online]
Available at: https://spectrum.ieee.org/the-real-story-of-stuxnet
[Accessed 25 March 2024].

Malwarebytes, 2023. *What was the Mirai Botnet.* [Online]
Available at: https://www.malwarebytes.com/what-was-the-mirai-botnet
[Accessed 26 March 2024].

Pisuwala, U., 2023. *Internet of Things in Healthcare: Applications, Benefits, and Challenges.* [Online]
Available at: https://www.peerbits.com/blog/internet-of-things-healthcare-applications-benefits-and-challenges.html
[Accessed 30 March 2024].

Radware, 2019. *ThreatPost,* s.l.: s.n.

Radware, n.d. *The Story of Mirai Botnet.* [Online]
Available at: https://www.radware.com/security/ddos-knowledge-center/ddospedia/mirai/
[Accessed 25 March 2024].

Trellex, 2023. *What is Stuxnet?.* [Online]
Available at: https://www.trellix.com/security-awareness/ransomware/what-is-stuxnet/
[Accessed 25 March 2024].

Vanson Bourne, 2019. *Digital Trust in a Connected World: Navigating the State of IoT Security,* s.l.: KeyFactor.

Wunck, C. & Baumann, S., 2017. *Towards a process reference model for the information value chain in IoT applications,* Munich: IEEE.