The cyber crime ecosystem: Challenges and solutions for smart technology

Claudia-Alecsandra GABRIAN,
Babeș Bolyai University, Doctoral School of International Relations and Security Studies Cluj-Napoca, Romania
claudia.gabrian@ubbcluj.ro

Abstract
The rising of smart technology increases the appearing of new vulnerabilities, consequently turning smart devices into a soft target by cybercriminals. While rapid proliferation has brought efficiency, smart technology has also introduced significant vulnerabilities to cybercrime. This paper will review the vulnerabilities and challenges of cybercrime within the ecosystem of smart technologies from two dimensions: analytical and user-related. The scope of this paper is to highlight main risks within smart technologies while pointing solutions for making such technologies secure and resilient, because the cybercrime groups take advantage of vulnerabilities of IoT devices. As solutions, states need a secure network infrastructure and data encryption, and a real-time threat monitoring system. The current paper fills in the gaps in previous foundational works on cybersecurity ecosystems and extends the ideas into the evolving landscape of smart technologies. A comprehensive understanding of the cyber-crime ecosystem is pieced together in the paper, using mixed-methods approach: a systematic review of existing literature and examples of how cybercriminals can target smart technologies. In this paper will be presented examples of the adaptation strategies of cybercriminals who, by exploiting gaps, have managed to develop elaborate attack vectors. Proposed solutions include creating a culture of cybersecurity awareness among citizens. Results provide a foundation for researchers who might want to extend the areas where the contexts of cybercrime and emergent technologies meet. The contribution in this paper is original, framing cybercrime within an interconnected and fast-evolving smart technology landscape. This study has underlined the requirement of realizing that such challenges need to be secure in the future of smart technology and its users worldwide.

Keywords: malware, critical infrastructure, cyberattacks, cybersecurity ecosystem, resilience.

1.Introduction

The landscape of cybercrime has turned into an immensely organized and collaborative global marketplace. It includes hackers, developers, ransomware operators and money launderers, connected with each other on the internet through online forums and marketplaces mostly located on the dark web. Further, this ecosystem facilitates all sorts of services for them, examples are ransomware-as-a-service, phishing kits, stolen credentials and cryptocurrency laundering platforms to help other hackers with very limited technical skills to conduct cybercrime. The accessibility and scalability of these services have amplified the frequency and complexity of attacks. For instance, hackers can buy on dark web through ransomware as-a-service, malware code in order to attack every system they want. Also, the anonymity afforded by encryption technologies can complicate the ability of law enforcement agencies to trace the cybercriminal groups. This collaborative infrastructure makes the cybercrime ecosystem an adversary in the cybersecurity landscape.

From intelligent homes to health monitors, from industrial sensors to everyday appliances, IoT devices have increase intelligence and connectivity into life, promising not only convenience and efficiency but real-time insights as well. Autonomous vehicles, drones, smart city systems, transportation, public safety, and intelligent houses represent also all these categories for smart devices and smart technology. These categories also brought a

lot of innovation with its share of costs, because most of the smart devices are designed for functionality, often at the cost of robust security measures. Default passwords, outdated software, and the absence of security standards by the manufacturers make these devices attractive targets for cybercriminals. Moreover, the huge amount of data generated via smart devices, stored mostly in centralized cloud systems, creates further risks with regard to breaches that may reveal sensitive personal and organizational information. With the rapid growth in the adoption of smart technologies, vulnerabilities in these systems now present an important challenge to the everyone [1].

The convergence of this cybercrime ecosystem and smart technology comes with significant current and future risks. Actually, with increased deployment in IoT, it has grown the attack surface for cybercriminals exponentially. Theoretically, a single compromise of one connected device could grant an attacker access to a wide range of home or corporate systems. This is achieved by scalable attack methods helped through the overall cybercrime ecosystem, which involves botnets targeting the IoT. Cybercriminal actors can use AI to deploy tools that not only can find but immediately exploit vulnerabilities in smart devices and technologies at a rapid scale, this might include adversarial attacks. Ransomware groups more recently have started to attack smart cities infrastructure, from traffic management systems to power distribution systems and disrupting entire communities and economies.

Data privacy implications are very important in these scenarios, because cybercriminals will exploit the volumes of personal information collected by smart gadgets for identity theft, blackmail, or even sell this information within the cybercrime ecosystem. At a geopolitical scale, smart technology may be targeted for espionage or sabotage by state-sponsored actors through leveraging the vulnerabilities in smart technology as a means to destabilize adversaries. Such challenges will require multi-layered responses: stronger device security, regulatory frameworks, and international collaboration in mitigating the risks produced at the intersection of innovation and crime.

1.1.Paper scope and methodology

The research question is in which way cybercriminal actors can affect smart technologies?

This paper employs thematic analysis based on the literature review and case studies. In this article will be presented the cybercrime ecosystem and the general understanding of this landscape, revealing also the essential directions for further research. Based on the gaps revealed by the literature review, that refers to the fact that are not a lot of studies about cybercrime and smart technologies, this comprehensive article could be applied at further research stages for people who are interested in this domain.

2.Challenges in smart technology

Smart technology can introduce potential vulnerabilities that, if exploited, could affect private life, economic security, critical infrastructure operations etc. Cyber threat activity against IoT systems is increasing globally, and the interconnection between IoT systems and smart technology increases the attack surface and heightens the potential consequences of compromise. Smart technologies are particularly attractive targets for criminals and

cyber threat actors to exploit vulnerable systems to steal critical infrastructure data, proprietary information, conduct ransomware operations, or launch destructive cyberattacks. Possible effects of successful cyber-attacks include disruption of infrastructure services, heavy monetary losses and the release of personal data of citizens [2].

The automation of infrastructure operations can increase the number of remote entry points into the network. The volume of data and the complexity of the automated operations can reduce visibility into system operations and inhibit the ability to respond in real time to incidents. Integrating AI with complex digital systems could introduce new unmitigated attack vectors and additional vulnerable network components. Dependence on an AI system, or other complex systems, can reduce overall transparency into the operations of networked devices because these systems make and execute operational decisions based on algorithms rather than human judgment [2].

The endless increase in the number of smart devices started to seamlessly bridge the physical and digital worlds. IoT is a broad concept and captures the idea of internet-enabled devices that seamlessly connect. The devices which normally count when talking about IoT are all types of smart devices which enable smart homes, factories, and cities: smart TVs, smartwatches, cars, refrigerators, medical devices, sensors, transferring information from the real to the digital world, etc. In other words, virtually all devices capable of connecting to the internet or other devices over a network [3].

The interdependency of IoT systems and thus the large number of elements involved in deploying such a system introduces added security challenges. As such, IoT security brings together network security, wireless security, and mobile system security together. IoT devices have weak security software, particularly compared with more mature devices like smartphones and laptops, and offer adversaries new attack vectors. Smartphones often act as the remote controllers for all manner of smart devices. IoT devices can be used as an easy access point into the network to perform a lateral attack to infect other devices such as mobile phones, laptops, or other systems within the network and to get full access to the activities, information, and data of the target [3].

IoT is closely related to the concept of cyber-physical systems, which describe systems that seamlessly integrate digital capabilities and physical devices and/or systems. Several smart devices communicate with one another, and an infection can spread so easily through the network of infected devices. This contrasts strongly with the IoT devices and the interconnectivity that have grown to be complex, raising the attack surface for the modern criminal remarkably. Such strong integration of physical and digital worlds allows cybercriminals to use network or device access to execute attacks with a large scale of success [3].

The IoT is a fast-growing industry regarding networked devices and new applications created within multiple industries. The IoT represents a solution that keeps individuals and objects continuously and universally connected using any network or service. A smart network is the equivalent of a digital nervous system, it connects devices for information

interchange and, by extension, increases automation in everything [4]. According to Dell, the International Data Corporation estimates that, by 2025, the number of Internet of Things devices in operation will be as high as 41.6 billion. These devices may generate data up to a tune of 79.4 zettabytes [5].

Critical security obstacles and vulnerabilities stand in the way of seeing IoT fully accepted into society in the future. They have a centralized structure, thus comprising several vulnerable points which can be attacked. An example linked with the Internet of Things has to do with weak authentications that are easily identified by their passwords. IoT devices with vulnerabilities unpatched have more adverse effects on users, the cybercriminals can steal their data, because these devices contain sensitive information that is very valuable for them.

Ensuring security among IoT devices may be quite difficult since there are very many devices connected, but security is considered one of the major needs for almost all the IoT applications. Smart applications are affecting people's privacy even though it was meant to raise their standard of living and to protect them [6].

One of the crucial topics when discussing technologies relates to their usability. Smart technologies require users to possess a high level of skills, along with sufficient ICT knowledge and abilities to handle various aspects of technology operation and effectively interact with all smart devices in a timely manner, or they need extremely user-friendly interfaces that cater to all their users' requirements and address any limitations—whether sensory, physical, skill-related, coordination deficits, or emotional and cognitive challenges [7].

Also when we talk about smart technologies development is important to understand the devices [8] as well as due to the fact that human society also requires a large number of usability specialists to manage usability, which improves the usability of technology interfaces. The complexity of developing older user-friendly interfaces stems from the variations in perception, knowledge, areas of interest, and strong and weak points of each user category. To address these differences, a unique approach to the already-classic user-centered development process is needed, namely participatory design, which involves active participation from all categories of future users. When compared to potential users who are older, digital assistive solutions are less useful. While smart technologies enhance the physical, mental, and social well-being of the elderly, they also create a vulnerability for hackers wishing to access and obtain personal device data. Smart technologies can help people live independently at home, by empowering self-management of life and improving users activities in daily living [8].

3.IoT malware

IoT malware is a malicious software designed with the purpose of targeting and infecting any device using an internet connection, it has functions in exploiting weakness in a device that is connected to the internet. An example of threat is to download applications from untrusted sources, the apps are disguised as legitimate software and when the malware is installed onto your device will compromise security and privacy. The consequences of a

malware infection in IoT may vary depending on the model of the device and the type of malware. The major scope is to steal vital information, like login details, or even spy on the activities engaged in the device [9].

Cybercriminals use AI in order to improve their technics that can lead to a major impact of their attacks, also for software development, scamming, extortions etc. AI represents an advantage for cybercriminals because they have the ability to identify vulnerabilities or more promising targets that can significantly enhances the ability to carry out more profitable attacks. The advancement of malware code can also be allowed to accelerate the process through AI, resulting in complex and more adaptive malware. The allowing of AI-powered malware to use sophisticated techniques for bypassing detection by security solutions could be capable of changing their operations depending on the target [4].

An attack surface represents the weak points or the exploitable vulnerabilities in the system which cause risks to the devices. Traditional attack surface classification includes network attack surface, human attack surface, and software attack surface. Unlike other malware, attacks by IoT malware are not oriented to a single part of the device. Beside the general classification, attack surfaces are classified into network and network device-level, service-level, firmware-level, and device-level attack surfaces [10].

In the Internet of Things mean any devices, actuators, sensors, or monitors interacting with the environment for data collection and several other purposes. Even though the device can be user-friendly, the problem with the IoT device is that security is not given importance compared to customer satisfaction. Due to these reasons, the number of attacks on IoT devices increases day by day. This attribute indicates the various IoT devices that are attacked by IoT malware. Among various IoT devices, routers are the most exploited device by different IoT malware. Malicious actors also target printers, smart TVs, video camera, gaming consoles, thermostats etc. These vulnerabilities also include some open ports present in the IP cameras that are equally vulnerable and are considered the second most highly targeted victim in IoT devices. Other devices like modems, smartphone, computers etc., are also victims of IoT malware because is not limited to any particular device, and malware may be from any category like ransomware, worm, trojan, backdoor, virus, etc [10].

4.Case study – Mirai Botnet

Cyber-attacks can affect critical infrastructure and today, hackers have more sophisticated hacking techniques that can lead to identify all the vulnerabilities of a lot of IoT-connected devices. Learning from real cases is essential, especially in understanding the impact of significant attacks and how to detect such cyberattacks quickly and remediate the threats and risks [11].

Malware known as the Mirai botnet, targets Internet of Things (IoT) devices, like routers, security cameras, and DVRs, which are usually online but lack robust security measures. The malware infiltrates these devices by searching the internet for weak or default passwords on susceptible devices, then employing brute force attacks to obtain access. A device that has contracted the Mirai virus joins a botnet, which is a collection of

compromised devices that the botnet operator can remotely manage. The Mirai botnet is made to be extremely durable and challenging to destroy. Because the malware is modular, the botnet operator can easily update and modify it to avoid detection and countermeasures. The self-replication capability of the Mirai botnet is one of its main characteristics. An infected device can automatically infect other susceptible devices with the Mirai malware when it searches the internet for them, which can spread the infection quickly and greatly. Additionally, the Mirai botnet has the ability to get around conventional security measures like intrusion detection systems and firewalls. This is because the malware conceals its existence and tries to avoid detection by using encryption and other methods [12].

When it was initially uncovered in 2016, the Mirai botnet was among the most well-known IoT-based cyberattacks ever. Initially, Mirai searched the internet for Internet of Things (IoT) devices with open ports. It then used a dictionary of pre-loaded default usernames and passwords to get access, and once infected, the devices joined the botnet. The main effect brought attention to the security flaws in IoT devices and raised awareness of the risks associated with unsecure IoT ecosystems on a global scale. There were 8.4 billion of these IoT devices in that year. The attack looked for open Telnet ports across large internet blocks and then tried to log in using 61 username/password combinations that were regularly used and never changed by the devices. Following the attack, the Mirai botnet code was made available on the dark web, allowing anyone to attempt infecting Internet of Things devices—the majority of which are still unprotected—by using it. The ability of the Mirai Botnet to launch both network-level and HTTP flood attacks, as well as the fact that, after infecting a device, it searches for additional malware on the device and removes it in order to claim the device as its own, are among its strong points. Additionally, the code of the bot contains a few Russian-language strings [13].

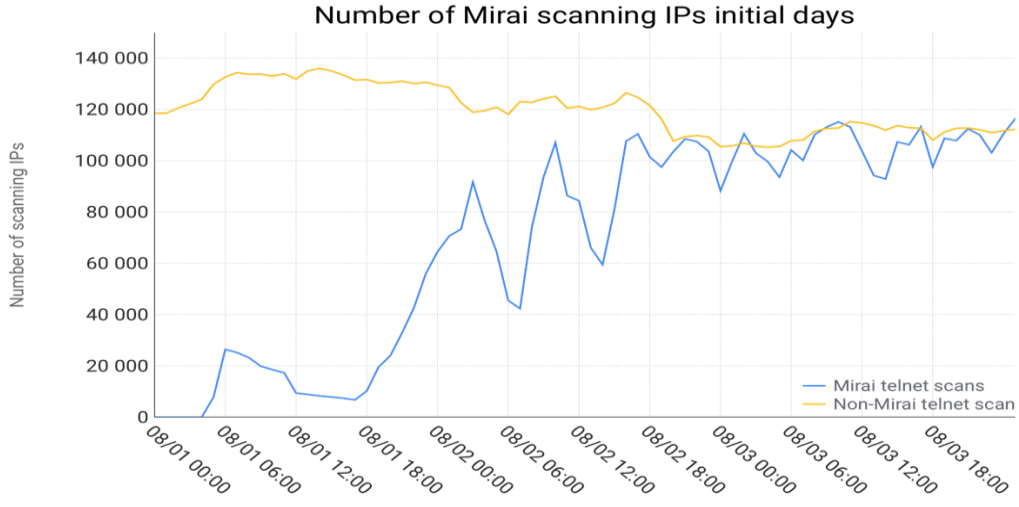

Fig. 1 Number of Mirai scanning IPs initial days
Source: Cloudflare, "Inside Mirai: The Infamous IoT Botnet – A Retrospective Analysis," 2021, [Online], Available: https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/, [Accessed: 20 December 2024].

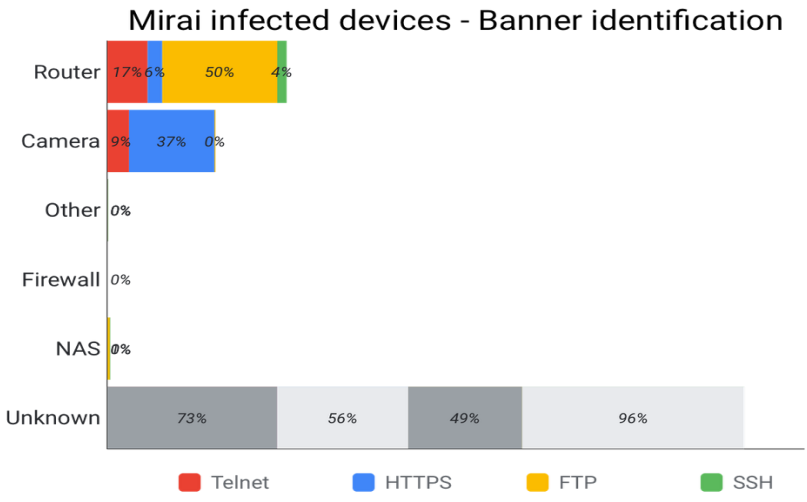

Fig. 2 Mirai infected deviced- Banner indetification
Source: Cloudflare, "Inside Mirai: The Infamous IoT Botnet – A Retrospective Analysis," 2021, [Online], Available: https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/, [Accessed: 20 December 2024].

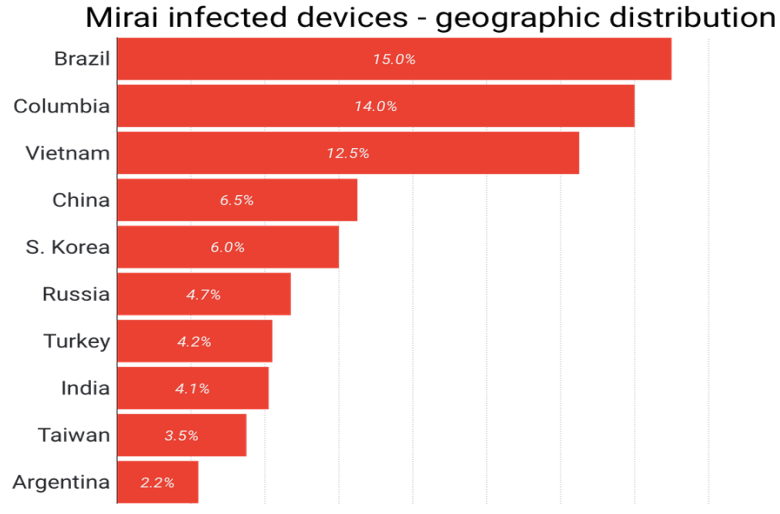

Fig. 3 Mirai infected devices – geographic distribution
Source: Cloudflare, "Inside Mirai: The Infamous IoT Botnet – A Retrospective Analysis," 2021, [Online], Available: https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/, [Accessed: 20 December 2024].

5.Solutions to mitigate cybercrime in smart technology

The rise of AI brings new challenges and great opportunities, and in order to analyze the solutions to protect smart technology is important to mention that is necessary to have an intrusion detection and prevention system. AI can definitely contribute in incident response and forensics for automated analysis of huge volumes of logs, system images, network

traffic, and user behavior to find adversarial activities. AI would reduce investigation time by the detection of patterns that may be hard to hit upon by manual observation and give an idea about techniques and tools employed by adversaries. Another possible application of AI is to correlate all the attack signatures, characteristics of malware, and patterns of attacks, tools, tactics, and procedures over time, in order to prevent smart technologies to be a target [10].

For several years, Cisco Talos has been leveraging AI in order to classify web pages, spoofing attempts, logo analysis, phishing emails based on text analytics, and binary similarities analysis. In the future, AI will extend the discipline through more automate data collection, analysis, and correlation on a large scale, enabling the detection of patterns and trends that may indicate new techniques or threat actors. AI can also be used as a predictive analytics tool, which will make the anticipation of potential cyber threats and vulnerabilities possible, based on previous data and patterns. Much of the predictive research into cybercrime is already exists, AI systems can spot common trends, patterns, or groups that may lead to a future attack by analyzing data from past attacks and adversaries. This capability further enables timely patching of vulnerabilities or implementation of additional security controls that minimize the possibility of a potential risk being exploited by an adversary [10].

In the second place, strong passwords should be a priority for everyone. Update all IoT devices with unique, complex passwords other than their respective default passwords, this would make it quite difficult for the malicious actors to get unauthorized access and deploy malware. Also, is important for everyone to be vigilant about software updates, because not all the IoT devices have an alert for an update, and it can also fail to install new updates by default. Another example is to download just the essentials apps on IoT devices, only known and trusted applications, never download apps from some anonymous websites [6].

Is important to have mitigation strategies, because take into consideration the level of risk or threat presents. By so doing, it ensures that the first vulnerabilities to be mitigated are those which are most critical hence giving maximum results. Consumer awareness refers to educate users to secure their IoT devices, because human error contributes to a quite large number of cyber incidents. This is where a continuous awareness campaign may help IoT users to avoid the potential intrusions. These strategies will reduce the ease with which attackers infiltrate in the systems and steal all the data [14].

In order to protect from a Mirai Botnet it requires a multi layered approach that includes both technical and behavioral measures. Is important to change default passwords; to update firmware; to disable remote access; use a firewall; monitor network traffic; use strong encryption; Implement network segmentation; use security software; and the most important for the users to be vigilant [12].

6.Future trends and conclusions

Emerging technologies and collaborative priorities will mark the future of cybersecurity against the emerging threats. The cybercrime is augmented by AI and has created new challenges since malicious actors increasingly use artificial intelligence in their

sophisticated, automated attacks, such as malware, phishing campaigns, ransomware etc. Is important to have systems that should be able to prevent the threats, detect them, and stop them in real time in order to keep the limit the impact of cybercriminals actors.

Smart technologies provide advantages but, at the same time, need strong protection against the risks coming from the cybercrime malicious actors. The collaboration between states is important to face transnational cybercrime, because cyberattacks do not recognize national borders. Cross-border initiatives and information-sharing frameworks may reinforce collective resilience and pave the way for timely responses against sophisticated threats. All these would have to come together in a cybersecurity framework that should be resilient, which, for the challenges of today and even future-looking vulnerabilities, securely integrates smart technologies into an ever-connected world.

With each passing day, more and more, the world and humans are getting connected while being technologically advanced; the continuous connectivity and constant availability of people, applications, and systems through mobile devices and communication networks have changed totally the way we used to live and work.

Compared to those fascinating developments in opening fast new possibilities for communications and interactions globally, everything has a flip side. Considering the increased interconnectedness of literally all devices, the consequence is a significant increase of the attack surface from the cybersecurity perspective.

The digital technologies combined with ever-changing technological ground, has formed an extremely complex and strong playground for cybercriminals. This paper explored IoT, malware, AI-based intrusion and solutions to detect and protect modern digital ecosystems against cyber-attacks.

Cybersecurity will be a key for all major undertakings in the future, while AI could be useful deploy and integrate cybersecurity solutions. The research opportunities in this area can further explore vulnerabilities, solutions and emerging attack vectors that can impact smart technologies. Also, others researchers can identify and mitigate vulnerabilities specific to another smart ecosystems that can face cybersecurity challenges to make them prime targets for disruption and exploitation by cybercriminals.

The Mirai botnet attack serves as a significant illustration of how easily exploitable vulnerabilities, particularly weak passwords, can be leveraged on a large scale. This incident underscores the necessity of implementing fundamental security measures, such as mandating strong passwords and restricting device access, to safeguard all internet-connected devices. In summary, the Mirai botnet poses a serious threat, capable of transforming your IoT devices into instruments for executing attacks. The most important prevention for the users is to remain informed, vigilant, and secure.

References

[1] A. Habib, D. Alsmadi and V. Prybutok, "Factors that determine residents' acceptance of smart city technologies," *Behaviour & Information Technology*, vol. 39(6), pp. 610-623, 2020.

[2] "Cybersecurity Best Practices for Smart Cities," *CISA*, 2023.

[3] M. Schmitt, "Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection," *Journal of Industrial Information Integration*, 2023.

[4] O. Alshamsi, "Towards Securing Smart Homes: A Systematic Literature Review of Malware Detection Techniques and Recommended Prevention Approach," *2024*.

[5] "Internet of Things and Data Placement," *DellTechnologies*.

[6] H. Sofany, "Using machine learning algorithms to enhave IoT system security," 2024.

[7] "What is IoT Malware and How Can You Secure Your Smart Home?," *Comparitech*, 2024.

[8] I. Ciobanu, "Digital divide, smart assistive technologies and ageing people," in *Smart Cities International Conference (SCIC) Proceedings*, 2024.

[9] "What is IoT Malware and How Can You Secure Your Smart Home?," *Comparitech*, 2024.

[10] Cisco Talos Blog, "The Rise of AI-powered criminals: Identifying threats and opportunities," 2023. [Online]. Available: https://blog.talosintelligence.com/the-rise-of-ai-powered-criminals/. [Accessed 24 November 2024].

[11] G. Waizel, "Using a modern honeypot model to defend smart cities and provide early detection to APT and ransomware attacks," in *Smart Cities International Conference (SCIC) Proceedings*, 2023.

[12] UMA Technology, "What Is the Mirai Botnet and How Can I Protect My Devices?," 2023. [Online]. Available: https://umatechnology.org/what-is-the-mirai-botnet-and-how-can-i-protect-my-devices/. [Accessed 22 December 2024].

[13] "The Mirai Botnet Explained: How Teen Scammers and CCTV Cameras Almost Brought Down the Internet," *CSO Online*, 2016.

[14] SentinelOne, "Mitigation Strategies to Combat Evolving Cyber Threats," 2024. [Online]. Available: https://www.sentinelone.com/cybersecurity-101/cybersecurity/mitigation-strategies/.