IoT Security: Threat of Worms

Adryana Hutchinson

May 2022

Abstract

Growing security risks within the IoT marketplace — in particular, owing to DDoS attacks carried out by botnets — necessitate heightened countermeasures. There is no authoritative policy on IoT security due to the diverse range of protocols in both hardware and software design. Currently, researchers make use of logistic regression models to predict and curtail botnet attacks. White worms — programs that spread and secure IoT devices by utilizing infection-based tactics commonly associated with malicious botnets — warrant further study to maintain legality and ethical soundness in their implementation. From a policy standpoint, providing more secure pathways of communication between devices and disallowing insecure protocol usage would reduce the threat posed by botnets.

Introduction

As the digital landscape continues to evolve, the use of Internet of Things (IoT) devices has grown in increasing popularity. There have been several IoT innovations that intend to improve efficiency, level of service, and consumer satisfaction [4]. IoT devices are used in a variety of settings, from small toys, health care (such as pacemakers), agriculture (smart-gardening technologies), and even smart cars. Experts expect there to be over 41 billion IoT devices by 2025 [3]; by automating these processes, we are able to cut down on time and resources that can be better used in other contexts. A cost to this sudden increase in IoT usage, however, is the growing security risk within the IoT marketplace.

In September of 2020, IBM X-Force reported that the number of IoT attacks drastically rose to over 400% between October of 2019 through June of 2020 — more than the combined observed IoT attacks when compared to the previous two years [2]. Botnets like Mirai and Mozi unleash massive distributed denial-of-service (DDoS) attacks, with Mirai in particular using millions of compromised devices in 2017. Mirai and Mozi accounted for over 85% of the total observed IoT attacks detected in 2020 [2]. Statistics like these illustrate a clear need for hardened IoT infrastructure as the IoT marketplace continues to increase.

As prevalent as a security risk IoT devices impose, more than 45% of IoT interface users are unaware of the security threats IoT devices can be used to initiate, and approximately 40% of them do not perform firmware updates [4]. Consumers argue that it is not their responsibility to mitigate security risks, and it is up to device manufacturers and software developers to find solutions to security flaws [4]; this,

coupled with the fact that IoT devices are designed to use limited storage, power, and computational capabilities, presents a challenge for IoT devices in terms of security requirements.

In this research paper, I aim to analyze the present security challenges facing IoT devices; in particular, I will analyze ways to mitigate botnet attacks. I will begin by examining how and why IoT architecture often prevents hardened security measures, followed by examining the present-day security infrastructure practices. I will then discuss why a botnet's structure especially poses a large security risk to IoT devices. Next, I will present potential solutions to the growing IoT security risks relating to botnets. Finally, I will conclude with a brief overview of the proposed solutions presented in this research paper.

Section 1: Defining IoTs & Current Security

IoT devices utilize sensors in conjunction with specialized software to respond to stimuli, collect data, and communicate with other devices via the internet. The ability to communicate and exchange data over the network — typically independently — is the defining characteristic of such devices; the key is remote interaction. As such, the descriptor applies to a variety of machines. They can range from household appliances like motion-activated lights to substantial feats of engineering as self-driving vehicles [3]. IoT devices exist all around us; they bridge the gap between the physical and digital aspects of society and allow for a more interconnected world.

Due to the wide variation of IoT devices, they often differ exponentially in comparison to typical information devices, and as such, researchers suggest that solutions relating to IoT security should be different as well; this is especially poignant, as consolidated policy in IoT security practice is still lackluster [4]. Due to how particular IoT devices are designed, such as their deployment environment and mobility/complexity requirements, IoT devices suffer from a lack of cataloged security weaknesses, which is especially concerning considering the expected growth of IoT devices within the next decade [4]. Because IoT devices feature this type of diversity in application, making a unified vision of IoT security is an exceedingly difficult task [5]. The power capability, as well as the communication requirements of each IoT device often differ greatly from each other [5], necessitating that unified IoT security policy needs to be overly generalized to encompass every device. As such, in order to define generalized IoT security policy, we must pinpoint security flaws that nearly all IoT devices face, and the mechanisms used to address them. Generalized IoT system features that relate to IoT security include diversity, scalability, Quality of Service standards, cost minimization in terms of space and energy requirements, and self-management mechanisms [5]. Another important feature of an IoT system is to have it deployed in a secure, appropriate environment that protects against

communication attacks — this environment must also promote authentication and authorization standards, such as data-transfer confidentiality, data/device integrity, and guaranteed privacy protection [5].

Authentication, in particular, is incredibly important in terms of securing IoT devices and the privacy of users. This is because authenticated access control points in IoT devices, as opposed to unauthenticated control points, make common communication attacks extremely difficult to execute, especially if the attack is outside of the considered trust domain [5]. Despite this common necessity, developing an all-encompassing authentication policy to counter all possible attack scenarios would be near-impossible [5]; as previously mentioned, IoT devices are inherently dynamic, and require non-homogenized solutions.

In summary, there is no authoritative policy on IoT security due to its diverse range of protocols in both hardware and software design. Although authentication remains a high priority for all IoT devices, a generic authentication scheme will be unable to account for every variety of IoT system. In addition, due to how information centric IoT devices need to be, they are often designed with insecure connectivity with the Internet, with little to no access control policies that provide secure, authenticated network traffic. This unmoderated connectivity leaves IoT devices open to a host of communication attacks, with one of the most popular being botnet attacks. In the following section, I aim to analyze how botnets infect their hosts, their history with IoT devices, and why they are so dangerous to IoT systems in comparison to other computing technologies.

Section 2: Botnets & IoTs

As described by researchers for the European Union Agency For Cybersecurity (ENISA), "botnets are a network of connected devices infected with malware" [10]; they are controlled by a bot owner, and can perform a wide range of attacks, such as a distributed-denial-of-service (DDoS) attack. IoT botnets are similar, being a large assembly of IoT embedded technologies, such as sensors, routers, and wearable devices; like traditional botnets, malware on IoT devices gives the owner the ability to control each device in the botnet hoard [6]. Unlike traditional botnets, IoT devices operate on a much larger array of devices, with the potential of infecting hundreds of thousands of devices very quickly [6]. Infection is often done through the use of SSH and Telnet protocols — malware then tries to brute-force admin-level credentials. Once the device is infected with malware, an infected payload is sent to the device from the botnet owner [6].

IoT botnets are used for a variety of purposes. However, one of the most popular uses is to make financial gain from infected machines, such as using them to spoof sensitive information such as banking or credit card data [9]. A symptom of IoT devices always being online is the fact that an IoT botnet owner can build and deploy

massive payloads on sophisticated IoT devices [6]; routers are especially coveted by IoT botnet owners — with a large quantity of infected routers, botnet owners are able to form powerful botnets that can cause havoc on a network. This has created a lucrative market for malicious activity; cybercriminals are able to make money by "selling" DDoS attacks to clients [7]. Because of this market, botnet owners aim to take over routers from other botnet owners — as soon as a cybercriminal takes control of a pre-existing, malware-infected router, they will generally uninstall the pre-existing malware infection, only to install its own [7]. The Mirai botnet, one of the most prolific and damaging IoT botnets in recent history, was built with the sole purpose of selling DDoS attacks; its first attack, which took place on September 19th, 2016, was used to interrupt online gaming sessions by flooding French internet service provider (ISP) OVH's internet channels — the source code for Mirai was posted online afterward [7].

With the number of IoT devices continuously growing, the underground marketplace for IoT botnet attacks will continue to gain more in profit [6]. It can be said that this marketplace is responsible for the development of one of the most damaging IoT botnets in recent history. In 2016, the Mirai botnet executed record-breaking DDoS attacks on multiple Internet service providers (ISPs) [6]; Mirai had approximately 500,000 infected devices at the peak of its lifetime, and was able to perform massive DDoS attacks on companies such as Dyn (a Domain Name System (DNS) hosting provider), Amazon, Twitter and Reddit [8]. One site that was targeted by Mirai was sent 620 gigabits of traffic per second — the damage done by this attack was so massive that it caused the site's ISP to stop providing for the targeted website [7]. While Mirai is currently inactive, the growth in profit relating to IoT botnets has made creating more prolific botnets increasingly appetizing to cybercriminals. IoT botnets are one of the leading causes of recent major DDoS attacks, which has resulted in lost revenue, stolen data, and service loss [6]. The Mozi botnet, a botnet that uses some of the source code of Mirai, currently controls roughly 438,000 observed devices. Each device in the botnet is encoded to find new IoT devices to add to the botnet herd until further instructions are sent from the botnet's owner [2]. As the landscape relating to botnets continuously expands, the need to further analyze security and modern threats is increasingly warranted. In the next section, I will be detailing both current theoretical and practical ways of dealing with IoT botnets.

Section 3: Current Prevention

Attacks implemented by the Mirai botnet laid the groundwork for numerous other IoT botnets to become prominent players in IoT-related cyber-attacks. The way that the majority of Mirai-like botnets gain access to IoT devices is by using brute-force attacks on Telnet, as well as the SSH protocol; research shows that 400,000

IoT devices accept connections solely from Telnet and SSH protocols, without the need for proper authentication [8]. IoT devices that use default credentials are easily compromised when brute-force attacks are used — as such, a technique to detect botnets in the early stages of a bruteforce attack are essential [8]. One way researchers do this is by using a logistic regression model on a botnet's behavior. A logistic regression model is a statistical model that can be used to determine the probability of an event based on a set of variables called predictors — by setting these predictors to the most common botnet infection methods, researchers are able to determine when a botnet attack is happening before it infects a device [8].

A theoretical way to deal with botnet attacks on IoT devices is through the use of white worms. White worms are programs that spread and secure IoT devices by utilizing infection-based tactics commonly associated with malicious botnets; as such, they have been the subject of stigmatization and limited professional consideration [9]. The design philosophy behind white worms entails self-propagating to reach IoT devices before malicious botnets. In doing so, the program can implement any necessary security measures prior to infection. A variety of measures can be executed to strengthen security, from adjusting network ports to repairing vulnerabilities; ultimately, the white worm purports "the final aim of creating a network of safe devices by enhancing their security level" [9]. However, the existing stigma warrants efforts to maintain legality and moral soundness in their implementation.

Despite these methods, more research needs to be done in regards to preventing botnets in IoT devices. One way this could be done is by implementing an overarching policy that dictates what security procedures are required for IoT devices; as previously mentioned however, creating such policy requires generalization that may do more harm than good. In the following section, I aim to detail a potential solution that provides protection against both botnet attacks, as well as general guidelines to IoT security holistically.

Section 4: Conclusion

IoT applications are expanding across all parts of the world. Some of the major driving countries in this growth include western Europe, North America, and China [1], and while these devices continue to grow common among everyday use, imposed security measures remain lackluster. This not only harms potential business output, but it also harms the current and future consumers of IoT products. In order to improve on this trend in IoT security, I suggest a layered policy proposal that targets specific machine requirements; for example, devices that collect personal information (such as pictures, health data, etc.) should require dramatically different security requirements in comparison to devices that solely collect sensor data. The process of defining these "layers" would be governed by researchers and technical organizations, such as the Institute of Electrical and Electronics Engineers (IEEE) and ENISA.

This layered approach would mitigate the need to develop security measures that broadly encompass all IoT devices.

In regards to IoT botnets in particular, I suggest more secure pathways of communication between devices, such as requiring encrypted communication channels. Disallowing insecure protocol usage, such as Telnet, would also work to mitigate this issue. IoT device owners should be educated on the security risks of using default security settings — the development of generalized IoT antivirus software to scan for these default settings could bear fruitful results in this regard, though all-encompassing IoT antivirus software may be increasingly difficult to develop.

As we see the rise of IoT devices, increased protection measures are crucial. Further research is required in this regard — while there are potential solutions to IoT botnet concerns (and IoT security in general), wide-spread adoption has not been implemented or tested [6]. Policy regarding IoT security, as well as antivirus software specifications, should be further studied by researchers and technical experts.

References

1 V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," in IEEE Access, vol. 7, pp. 82721-82743, 2019, doi: 10.1109/ACCESS.2019.2924045. URL: https://ieeexplore.ieee.org/abstract/document/8742551

2 McMillen , Dave. "Internet of Threats: IoT Botnets Drive Surge in Network Attacks." SecurityIntelligence, 22 Apr. 2021, URL https://securityintelligence.com/posts/internet-of-threats-iot-botnets-network-attacks/

3 Ranger, Steve. "What Is the Iot? Everything You Need to Know about the Internet of Things Right Now." ZDNet, 3 Feb. 2020, URL: https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/

4 N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations,", third quarter 2019, in IEEE Communications Surveys Tutorials, vol. 21, no. 3, pp. 2702-2733, doi: 10.1109/COMST.2019.2910750. URL: https://ieeexplore.ieee.org/abstract/document/8688434

5 Jurcut, A.D., Ranaweera, P. and Xu, L, "Introduction to IoT Security. In IoT Security", (eds M. Liyanage, A. Braeken, P. Kumar and M. Ylianttila), 2020, URL: https://onlinelibrary.wiley.com/doi/10.1002/9781119527978.ch2

6 Radware, et al. "A Quick History of IOT Botnets." Radware Blog, 2 Mar. 2018, URL: https://blog.radware.com/uncategorized/2018/03/history-of-iot-botnets/

7 S. Hilt, F. Mercês, M. Rosario, and D. Sancho, "Worm War: The Botnet Battle for IoT Territory", 2020, Trend Micro, Incorporated. URL: https://documents.trendmicro.com/assets/white_papers/wp-worm-war-the-botnet-battle-for-iot-territory.pdf

8 A. O. Prokofiev, Y. S. Smirnova and V. A. Surov, "A method to detect Internet of Things botnets," 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EICon-Rus), 2018, pp. 105-108, doi: 10.1109/EIConRus.2018.8317041. URL: https://ieeexplore.ieee.org/abstract/document/8317041

9 G. Ferronato ,"IoT White Worms: Design and Application", 2020, Master's dissertation, University of Twente, Department of Electrical Engineering, Mathematics, and Computer Science. URL: http://essay.utwente.nl/83003/1/Ferronato_MA_EEMCS.pdf

10 European Union Agency for Cybersecurity (ENISA), "Botnet ENISA Threat Landscape", 2020, doi: 10.2824/552242, URL: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/