POSTER: Analyzing Endpoints in the Internet of Things Malware

Jinchun Choi^{✉*}, Afsah Anwar^{✉*}, Hisham Alasmarty[✉]

Jeffrey Spaulding[†], DaeHun Nyang[‡] and Aziz Mohaisen[✉]

[✉]University of Central Florida [†]Niagara University [‡]Inha University *Equal contributors

ABSTRACT

The lack of security measures in the Internet of Things (IoT) devices and their persistent online connectivity give adversaries an opportunity to target them or abuse them as intermediary targets for volumetric attacks such as Distributed Denial-of-Service (DDoS) campaigns. In this paper, we analyze IoT malware with a focus on endpoints to understand the affinity between the dropzones and their target IP addresses, and to understand the different patterns among them. Towards this goal, we reverse-engineer 2,423 IoT malware samples to obtain IP addresses. We further augment additional information about the endpoints from Internet-wide scanners, including Shodan and Censys. We then perform a deep data-driven analysis of the dropzones and their target IP addresses and further examine the attack surface of the target device space.

CCS CONCEPTS

• Security and privacy → Mobile and wireless security.

KEYWORDS

Internet of Things, Endpoints, Malware

1 INTRODUCTION

With the number of seamlessly connected and online IoT devices soaring into 10's of billions [10], potential adversaries set such devices on target via malicious codes. Such codes or malware not only infect the devices themselves but constantly communicate with their Command and Control (C2)/dropzones around the world for future actions and updates. Forming a network, these devices have the potential to launch attacks on other targets resulting in Distributed Denial-of-Service (DDoS) attacks [9].

Reckoning that the malware sources, the C2 servers, the intermediary targets, and the victim must be connected to the Internet for the attacks to happen, studying these endpoints is important. This work attempts to understand such endpoints to decipher such patterns. Towards our goal, we extract endpoints from IoT malware binaries and perform a data-driven analysis to understand geographical affinities and their exposure to risk.

Our work is important given its insight into understanding the Indicators of Compromise (IoC), and the behavioral aspects necessary

for threat hunting. Specifically, we make the following contributions: (1) IP Centric Analysis: We investigate the target IP addresses among different dropzones. Additionally, we analyze the locations of dropzones and their target IP addresses. Moreover, we analyze the risk associated with the IP addresses through insights gained from Shodan [5]. (2) Network Centric Analysis: For the masked target endpoints, we examine the entire network and study the network devices and their exposure to risk.

2 DATASET CREATION

Our primary dataset contains a total of 2,423 IoT malware samples collected from IoTPOT [11]. We design a tool that can reverse-engineer each of the malware samples and extract the specific IP addresses from the malware code base. In total, we extract a total of 106,428 target IP addresses, resulting in 2,211 *unique target IP* addresses associated with 973 malware samples. We also find a total of 2,407 IP addresses, resulting in 877 *unique dropzone* (source of attack)/C2 IP addresses corresponding to 2,318 malware samples. Additionally, to better understand the dynamics of the extracted IP addresses, we augment the IP addresses with other details including their: country, Autonomous System Number (ASN), and location, using online DNS and IP lookup tools like the *UltraTools* [6]. Furthermore, we utilize the internet scanning services, e.g. Shodan [5], to procure the vulnerable endpoints.

3 IP CENTRIC ANALYSIS

3.1 Dropzone-Target Inter-relationship

We examine the affinity between the dropzone and the target IP addresses and find that $\approx 77\%$ of the unique target IPs receive less than 10 attacks, while at the other end of the spectrum we see that one unique target IP received 72 attacks. We also find a dropzone IP associated with one malware targeting 1,265 target IP addresses, which is significantly larger than the average (121).

Shared targets between dropzones. To inspect the shared targets between dropzone IP addresses, we group the target IP addresses by the dropzone IP addresses, and capture the common targets among the dropzones. Evidently, the results of the above analysis reflect that a large proportion of targets are being shared among dropzones. There were 2,199 cases (12.11%) with 100% overlap between dropzones. Overall, we found 6,451 cases (35.53%), with more than 80% overlap. If the target IP addresses between different dropzones are identical, it is possible that the attacker obtained the same targets through similar vulnerability analysis (e.g. Shodan) or shared the target list from underground communities.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

WiSec '19, May 15–17, 2019, Miami, FL, USA

© 2019 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-6726-4/19/05.

<https://doi.org/10.1145/3317549.3326295>

Figure 1: Attack trends between dropzones and target IPs corresponding to dropzones having over 500 target IPs. The orange circle represents dropzones, and blue, red, and green circles stand for target areas.

Table 1: Top 5 number of target and dropzone IPs by country.

Country	Dropzones	Pct.	Country	Targets	Pct.
United States	1,041	43.25	Vietnam	26,290	24.70
Netherlands	278	11.55	Brazil	20,572	19.33
France	188	7.81	China	15,799	14.84
United Kingdom	183	7.60	India	5,598	5.26
Italy	177	7.35	Pakistan	5,076	4.77

3.2 Geographical analysis

In this section, we focus on the distribution of the distances between the dropzones and their target IPs. To visualize the flow of attacks in a holistic sense, we plot circular areas whose sizes are proportional to the number of targets placed according to their *average* position (not the exact position) on a world map with geodesic lines originating from various dropzone locations. Figure 1 shows the country-level perspective of the relationship. The locations of the dropzones (depicted in orange) are spread around various countries, but, the results show a large concentration of target areas focused in Central Asia. The distribution of dropzone and target IPs by country is shown in Table 1. We notice a large distribution of dropzones from US pointing to targets in Asian countries such as Vietnam. Additionally, China and Brazil are target of attacks originating from European countries. Imperva Incapsula states that Vietnam (12.8%), Brazil (11.8%) and China (8.8%) were the countries with the most-infected devices (from the Mirai botnet) [7].

3.3 Network Penetration Analysis

This section focuses on analyzing attributes gathered from Shodan and Censys [3], namely, active ports, vulnerabilities.

Active Ports. For each dropzone and target IP address, we use information gathered from Shodan and Censys the list of active ports. We extract 5,745 active ports from 716 of 877 dropzone IPs and 1,114 active ports from 129 of 189 non-masked target IPs. Each port number is typically associated with a service, such as port 80 for HTTP traffic. While we observe common services like SSH (port 22), HTTP (port 80), and HTTPS (port 443), we point out to the usage of Network Time Protocol (NTP) on port 123. NTP is UDP-based and can be prone to “IP spoofing” for DDoS attacks [8]. This attack is also emphasized in [1], since the attacker can amplify attack packet size 1,000 larger by exploiting NTP.

Vulnerabilities. We then examine the susceptibility of the IP addresses; in particular, we determine the vulnerabilities present in the IP addresses. We gather the Common Vulnerabilities and Exposures (CVE) identifier [2]. In our analysis, the second-most common CVE among the dropzones: CVE-2014-1692. The NVD [4] reports the severity of this vulnerability as “high” since it might allow remote attackers to cause a Denial-of-Service attack through memory corruption due to uninitialized data structures from the `hash_buffer` function in OpenSSH.

4 NETWORK CENTRIC ANALYSIS

We observe the malware targeting multiple IoT devices for propagation. In this regard, malware authors often mask the endpoints on target. For such endpoints, we analyze their CIDR network. In total, we inspect 27 unique /24, 435 unique /16, and 125 unique /8 IP addresses. Towards this, we evaluate and analyze these networks to investigate their exposure to risk. In particular, we examine the devices on these networks and looked at the services being used.

The corresponding 100,793,403 active IP addresses are then clustered by their device type. Considering that open ports lead to increased security risks, we look for ports that are necessary for a device to operate uninterrupted. Taking a conservative approach, we suggest that if a port is being used by less than 10% of devices in a given device type, it should be closed to reduce its exposure to risk. Our results show the susceptibility of high-wattage IoT devices, such as heating, ventilation, and air conditioning, power distribution units, etc., can be abused by the attackers to launch large-scale coordinated attacks. Additionally, the high presence of such susceptible devices lays the foundation for attacks as demonstrated by Soltan *et al.* [12].

5 CONCLUDING REMARKS

In this paper, we analyze the $\approx 78.2\%$ of total responsive public IPv4 endpoints among dropzones and their targets as extracted from IoT malware and spread across the globe from diverse perspectives. Additionally, we augment our analysis results by leveraging the use of IoT search engines like Shodan or Censys.

Acknowledgment. Supported by NSF CNS-1809000, a collaborative seed grant from Cyber Florida, and NRF 2016K1A1A2912757.

REFERENCES

- [1] 2016. UDP Flood Attacks. <https://bit.ly/2NTNnu6>
- [2] 2018. About CVE. <https://bit.ly/1FxfOiz>
- [3] 2018. Censys Landing Page. <https://censys.io/>
- [4] 2018. National Vulnerability Database. <https://nvd.nist.gov>
- [5] 2018. Shodan Landing Page. www.shodan.io
- [6] 2018. UltraTools Free IP Tools. <https://bit.ly/2v2cLk4>
- [7] Ben Herzberg, Dima Bekerman, and Igal Zeifman. 2016. Breaking Down Mirai: An IoT DDoS Botnet Analysis. <https://bit.ly/2dQbvYo>
- [8] J. Graham-Cumming. 2014. Understanding and Mitigating NTP-based DDoS Attacks. <https://bit.ly/2ifu8pa>
- [9] C. Koliadis, G. Kambourakis, A. Stavrou, and J. Voas. 2017. DDoS in the IoT: Mirai and Other Botnets. *Computer* 50, 7 (2017), 80–84.
- [10] Peter Middleton. 2017. Forecast Analysis: Internet of Things—Endpoints, Worldwide, 2016 Update. <http://gtmr.it/2oRo4aN>
- [11] Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, and Christian Rossow. 2016. IoT POT: A Novel Honeypot for Revealing Current IoT Threats. *Journal of Information Processing* 24, 3 (2016), 522–533. <https://doi.org/10.2197/ipsjip.24.522>
- [12] Saleh Soltan, Prateek Mittal, and H. Vincent Poor. 2018. BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid. In *Proceedings of the 27th USENIX Security Symposium*. 15–32.