Detection and Prevention of Non-PC Botnets

Jai Puneet Singh, Akashdeep Chauhan
CIISE, Concordia University, Montréal, Québec, Canada
jaipuneet.singh@mail.concordia.ca,akashdeep.22chauhan@gmail.com

***Abstract*—Botnet attacks are serious and well established threat to the internet community. These attacks are not only restricted to PC or laptops but spreading their roots to device such as smart phones, refrigerators, and medical instruments. According to users, they are devices which are least prone to attacks. On the other hand, device that are expected to be least vulnerable have low security aspects which attracts the attackers. In this paper, we have listed the details of latest Botnet attacks and common vulnerabilities behind such attacks. We have also explained as well as suggested proved Detection ways based on their types. After an analysis of attacks and detection techniques, we have suggested recommendations which can be utilized in order to mitigate such attacks.**

Keywords: Botnets, Vulnerabilities, IoT's, Mobile.

I. Introduction

With the rise of technology and our life dependence on portable devices such as smartphones, iPads etc has increased to a great extent. It has opened a great opportunity for cyber criminals to take control of our lives. The IoT (Internet of Things) and mobile botnets have made their work quite easier [1]. As we have seen earlier the PC botnets are serious threat to the internet [2]. Mobile and IoT botnets are a similar threat which gets installed on a smartphone and it gains complete access to the device and its contents. Android software is highly vulnerable to malware as it is an open source software. The popular malware or botnet for Android devices are Droidjack [3], VikingHorde etc. It was earlier seen that mobile botnets such as DroidDream had compromised many Android devices. Similarly, Mirai botnet had compromised many IoT devices in 2016. Hence, it has also been seen botnet attacks were targeted at iPhones, Symbian devices etc. We can infer from this, that IoT and mobile botnet attack is independent of operating systems. The botnets in mobile networks are more perilous than the internet botnets as they don't need to propagate through Centralized infrastructures. It has become as most serious threats in today's era. It was found by Symantec a large number of Botnets B.Master in China infected a large number of Android phones [4]. Ar Flo et al in 2009 [5] had predicted earlier the vulnerability of mobile devices when connected to the internet. Then, it was argued that when mobile devices get connected to the internet, botnets will migrate over to the mobile networks. Mobile botnets work in a similar fashion as computer botnets as they also start their life cycle when users are fooled to run unwanted softwares [6].

In this paper, we will discuss about the non-PC botnets, their latest attacks in non-PC botnets in Section III, Section IV provides with vulnerabilities present in security infrastructure of non-PC devices. Section V gives the detection and prevention mechanism for non-PC devices. Section VI illustrates the recommendation to be adopted in order to prevent from such attacks. At last in Section VII, the paper has been concluded.

II. Current Attacks on Non-PC Devices:

Generally, There are a lot of portable devices where attackers can easily attack. It can range from the smartphones to smartTV's. Anything that is connected to the internet is vulnerable to an attack. Some of the latest attacks on non-PC devices are discussed below:

1) Mirai: It's a brute force attack that runs and scans the default username and passwords of home devices. It is a recent attack which took place in October 2016 and it had affected a large number of IoT (Internet of thing) including CCTV cameras, Digital recorder, and even digital refrigerator. The source code was later released and it was seen that attack code contained 60 combinations of common default username and passwords which were capable to corrupt 306,000 devices [7]. According to some security architect, this malware affected small western African country Liberia contrived its telecommunication network. The attack targeted Liberia's single underseas large transit Internet Cable which connects it to the rest of Africa and Europe causing single point of failure for accessing the Internet. Africa Coast to Europe (ACE) connects Europe to Africa has been deployed by Alcatel-Lucent as it provides better and high quality internet service when compared with a satellite. The capacity of this optical fiber is 5.12 Tbps and it has been shared with 23 countries [8]. This internet connectivity can easily be disrupted as the cable capacity is limited. Imperva Incapsula [**?**] is a cloud based application delivery company which has developed Mirai Scanner to check whether the devices in the network is vulnerable to Mirai attack. They have also developed the mechanism that provides security check against low volume application layer HTTP floods. They developed Mirai signatures from its source code to identify the attacks.
2) MUSE: Wei Chen et al [9] proposed MUSE which is Mobile Botnets via Multiple Push Service. Message Push services when implemented removed the dependence of direct communication between Bot and Botmaster and thus ease the deliverance of message to bots. Considering multiple push service rule, MUSE was proposed to reduce DDOS attacks, spam issues. Muse performance was able to improve controllability, scalability and robustness. Robustness in Botnet refers to the ability of network to function properly even after

some accounts have been compromised by the Attacker. On the other hand, controllability refers to ease of management of network when multiple bots are connected. Scalability depicts the ability of the network to accommodate new bots/botnets in the existing network. MUSE follows round robin algorithm for the selection of server and hybrid structure to connect the bot, botmaster and Bot Services together. Multiple push services helps in overcoming single point failure problem and also improves Robustness and scalability. It implements 10 popular push services and helps in distribution of traffic among different server and leads to improvement in the stealthiness of the network. It has been proposed by learning the weakness of earlier methodologies and it has single point of failure problem as in Punobot [10], lack of robustness in C2DM proposed by Zhao et al. [11]. They have used dynamic round robin algorithm for push service selection in order to ensure CC traffic is distributed among various servers. They used LEACH protocol [12] to dynamically select servant bots. Hence, MUSE promises for the scalability and stealthiness of Botnet attack.

3) Botnets in LTE Networks: The Long-term evolution is a high-speed wireless network which uses latest techniques of Digital signal processing for 4G telecommunication systems. It has been motivated by higher data transfer rate, high efficiency, and increased signal range. Katana et al [13] studied and designed the mobile botnet architecture which initiates a DDoS attack against a web server (HTTP server). They studied the impact of mobility of mobile devices considering random patterns of movement i.e. Asymmetric mobility model (AMM) and uniform patterns of movement i.e. Symmetric mobility model (SMM). It recommends using SMM model in LTE networks where fewer devices are infected and low CPU power consumption takes place. Evaluation of botnet model was done by using the traces of taxi cabs using Mobility models (AMM and SMM). They established a DDOS attack considering HTTP server as a victim. Server taken into consideration was hosting different sites specifically E-commerce site. Proposed model consist of 4 major parts Botmaster, C and C server, LTE network and mobile devices. Bot master is main controller in the figure 1 who handles all mobile devices. C and C server was utilised as a bridge to transfer traffic from Botmaster to multiple mobile devices. Also architecture consist of 10 hexagon LTE cells having enodeB station which further connect with 50 mobile devices. On the other hand, we have external network consisting of Web server, victim, router and C amp; C server. Mobility of the traces was first analysed using SMM model and then with AMM model. Process of attack includes scanning of vulnerable mobile devices in the network and transfers the data to Botmaster.DDOS attack is then initiated towards the victim web server.

4) SlowBot Net: Farina et al [14] had developed a new type of Botnet which is based on HTTP/HTTPS protocols and is centralized botnet for the mobile devices. The key feature of this botnet is that it uses low power consumption and resources. This is motivated by using some intelligent behavior which is provided by Test Server. It can identify the bots which cannot contribute to an attack on mobile devices and accordingly it changes the attack style. It is the further extension of the LOIC (Low Orbit Ion Cannon) famous botnet. This botnet performs the slow DoS attacks which are comparatively different from DDoS attacks. In slow DoS attacks, there is long passive waiting time also called as Wait timeout and short attack periods.

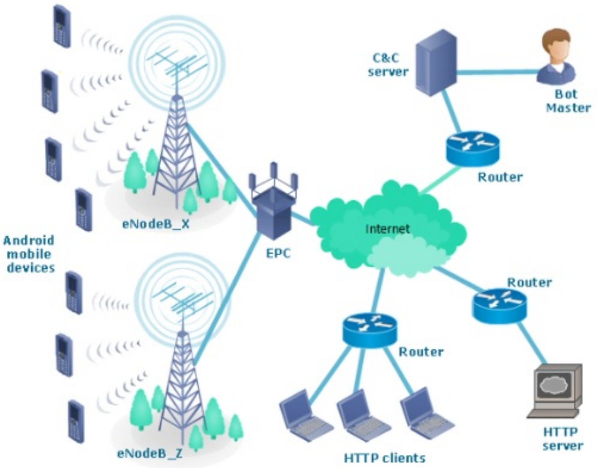

Fig. 1: Botnets in LTE network [13]

5) Social Botnet: With the rise of Online Social networks (OSN), there is a spread of social botnets. As, it is known that OSN has great digital influence (such as Marketing, recruitment, ad advertisement etc), social botnets can manipulate such influence. Hegelich et al [15] discussed the Ukrainian/Russian conflict by Twitter social bots and emphasized on Twifarm Russian botmaster for creating large fake accounts and tweets on twitter which turned the Social site into a political war. Zhang et al. [16] studied such influence and proposed social botnet on Twitter. This botnet is not blocked by Twitter as it has a policy to block the root botmaster, not the re-twitter accounts. This vulnerability is exploited and design of re-twitting tree is proposed which is a multi-objective optimization problem. It considers that at the minimum cost and time of the bot master, it can reach a large number of victim twitter users. They developed the botmaster in Java Application using OAuth protocol and open twitter API. In the end, the authors had proposed defensive mechanism for such technique which we will discuss in this paper.

6) Linux/IRCTelnet: A Linux based botnets attacking telnet ports of IoT device. It was launched one week after Mirai botnet. It affects the device operating system and adds the botnet network which is controlled by Internet Relay Chat (IRC) [8]. Malware was written in C++ and was focused on Linux based IOT devices [8]. Mirai Botnet strategy was utilized to reveal ports

of the networks by brute force approach. It was able to affect device running Linux kernel 2.6.32 and above. Also was able to launch DDOS attacks with Spoofed IPv4 and IPv6 addresses. This attack was able to affect 3400 Botnet .Malware code found was written in Italian language which give a clue of origin of attack. Also other attack such as Aidra and Kaiten were based on IRC malware [17]. kaiten attack was basically organized DDOS attacks focusing on routers and IOT devices. Improved version of this attack got name as Gafgyt. This attack used to send executable binary files along with traffic for router and devices. Process includes the search for Public IP address. After connections been maintained via IP address on successful login, binary file will execute to download bot files. Another attack based on IRC was Aidra botnet [18] which originated from Italy by a security analyst. Researchers at ATMA found attacks originating from router, TV, setup box. After analysis of the attack, it was found that it needs two servers. One was utilized to carry the executable binaries which will be injected in the devices and other to manage the bots. Bad news for attack was once the device is rebooted, connection will be diminished.

7) Other reported attacks: The first reported attack by IoT devices was by Proofpoint where they found that digital refrigerator became slave bot and started sending out spam emails. The attacker had hijacked 100,000 devices including multimedia centers, televisions, and routers etc. Cyber attacker hijacked the devices which normally sends 10 emails per day has sent 750,000 spam emails in a burst of 100,000 emails [19]. The biggest problem in IoT devices is the lack of security features as no anti-virus is installed and their availability (24/7) as opposed to PC's to prevent them from malware. Symantec, a popular antivirus company reported a new type of botnet named Linux Wifatch which attacks the router and turns them into Zombie. It's a very sophisticated piece of code written in Perl programming language and targets several different architectures. It has a file named Dahua.pm which exploits Dahua DVR CCTV system to reboot automatically [20] after one week. The routers are an interesting target for Wifatch and they perform DDoS (Distributed Denial of Service attacks) Attacks. With the rising of these IoT attacks Yin Min et al [21] proposed IoTPot which analyzes telnet based attacks on IoT devices.

III. Vulnerabilities present in security infrastructure:

In the above section, we described the various attacks that took place recently. In this section, we will discuss the vulnerabilities present in the security infrastructure that has to be secured in order to prevent from attack to take place.

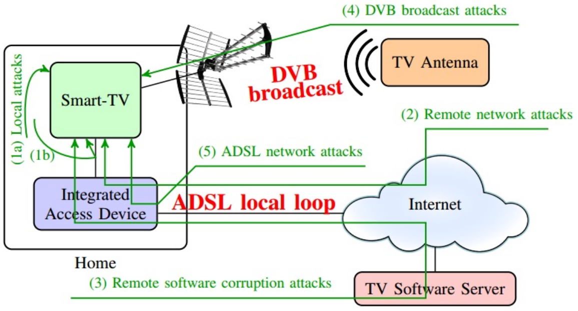

Fig. 2: Smart TV Home network vulnerabilities [23]

1) Default Passwords: Most of the IoT attacks occurred due to predictable default passwords and this benefit was taken by the attackers. This vulnerability is mitigated by using an approach proposed by Leo Linsky [22], a software engineer associated with network monitoring firm PacketSled. They have released (Do Gooder Worm) which changes the default password or weak password with a random password or with a device specific password. The idea is to patch such devices by a worm that deletes itself after changing the password. The worm also designed to shut down telnet if the devices are compromised so that malware could not be able to take edge on the compromised IoT devices.

2) Local Loop: Most of the Smart TV attacks, or other connected devices attacks occur due to local loop vulnerability in which the line is physically cut down and new ADSL and DSLAM is installed in the network [23]. The physical supports can be Copper cables, Radio Waves, fiber optics and Co-axial. The attack done indirectly using corrupted firmwares or malicious applications are most common as SmartTV has attack vector similar to personal computers. The figure 2. shows how Smart TV can be attacked in different ways from different paths. As seen from the figure, ADSL local loops can be dangerous as an attacker can gain access to Smart TV and compromise its privacy, install malicious software as well as it can carry out Distributed Denial of Service attacks.

3) UPnP protocol: This protocol is used for the event notification, discovery and control of devices. This protocol is independent of any operating system and programming languages. It is present in every network devices which helps in smooth discovery of other devices on the network. It is used for network connection, data sharing etc. Rapid 7 [24] had conducted a large number of experiments and found protocol to be vulnerable to single remote code execution flaw and other large number of vulnerabilities present in the protocol. It's recommended to push software update to remove UPnP capabilities from the device. According to the Rapid 7, over 80 million unique IP's are vulnerable to UPnP discovery from the internet access. In UPnP portable SDK, IP's are vulnerable through a single UDP packet which can execute remote code. There are 4 major CVE's assigned to the UPnP protocol. In MiniUPnP library it has been found a stack overflow vulnerability in the SOAP handler and there are DoS flaws present in

the miniUPnP SSDP parser.

4) Port 7547: The manufactures of routers Zyxel, speedport etc leave the TCP port open to outside world which is vulnerable to exploit based on TR-064 and TR-069 protocol [25]. This usually takes place on routers which uses CWMP (text based protocol). It is the one that initiates a CWMP session. These protocol are application layer protocol and used for remote management of the end users. Port 7547 is used with above protocol to provide communication between customer premises equipment and auto configurable servers. It was first identified by Reverse Engineering blog which found ERID 1000 modems to be vulnerable.
5) Netgear Equipment flaw: Recently trustwave security company has found the flaw in Netgear routers. The flaw has been found in remote management option being switched on and facing towards the internet is vulnerable to hacks. Nevertheless, Anyone who can access the Netgear routers can turn it into potential botnets [26].
6) IP Camera Vulnerability: It has been discovered that there is a vulnerability in IoT device cameras which are IP enabled by companies such as Forscam, Vstarcam etc. The weakness is present in goahead webserver used by mentioned companies [27]. It allows an attacker to craft distorted HTTP request which will disclose the conf. file with login password [28]. The security flaw is present in form of Backdoor which enables the Telnet/SSH server remotely. The vulnerability can be exploited if the web gateway of the device is exposed.
7) IPv6 vulnerability: The routing table of IPv6 has been found to be vulnerable in Livebox 3 Sagemcom SG30_sip_fr_5.15.8.1 devices and classified as critical by NIST [29]. In these devices have large default value for maximum IPv6 routing table which is usually filled within few minutes. This can cause an affected system to become unresponsive and results into DDoS attacks and thus hampering TV, internet and telephone services [30]. Recently, Cisco [31] mentioned that IPv6 ping of death vul is everyone's problem. The vulnerability is present in the IPv6 neighbor discovery which uses ICMP messages to determine link layer address of the neighbor. This is present in the CISCO and other devices which uses IOS, IOS XE, NX-OS and IOSXR software. The devices being configured with global IPv6 address and which is processing incoming traffic. Its being recommended to use Static IPv6 neighbours where its possible to avoid such vulnerability.

There are multiple approaches for C&C communication which are P2P, SMS, SMS-HTTP and hybrid structure. It has been found that mostly SMS-HTTP based are more appropriate for an attack.

IV. Detection and Prevention of Non-PC Botnets

There are many latest Detection and Prevention mechanisms for Non-PC botnets. We will be discussing some of the detection mechanism in this section and afterwards we will provide with detection analysis. Spreitzenbarth et al [36] gave the insight of Static and Dynamic botnet Analysis approaches which can be discussed as follows:

1) Static or Code based: It is a methodology used in earlier days, in which applications were downloaded with source code. The source code is analyzed for any deviation from normal coding standards. It also uses signature based techniques to verify the source code. Static analysis is vulnerable to obfuscation techniques. Malware's hide system activities by calling function outside Java Run time environment basically libraries written in C and C++.
2) Dynamic or runtime execution analysis : In this the application has to be executed in a secure sandbox and results are usually collected for further analysis. It does not inspect the source code but the source code is executed. The monitoring and logging is done for relevant operations.
   However, there are numerous approaches that have combined Static and Runtime execution analysis. Hence, we will call them hybrid approaches in this paper.

A. Static or Code based

1) Filtering Approach: The author in [37] has used static approach for detection of botnets in the android applications. The approach uses 4 filters which are MD5 filter, permissions filter, broadcast receiver filter, and background process filter to identify the botnets in an Android application. The process uses classification model for identification of botnets.
2) AndroDialysis: They have proposed Static analysis technique to find the malware on mobile devices [38]. They have exploited the inter-process communication of Android framework. It has an important feature of reusing of components across process boundaries as they form the path of access to different sensitive information. They have used Intent feature for malware detection on Android Operation system. The intent refers to the late binding messaging run-time object. The author exploits the effectiveness of Android intents i.e Implicit and Explicit to identify malicious applications. Intents are basically semantically rich features that can encode premediation of malware with the permission features.
3) Log Based Analysis: The author in [39] had used log management service available on cloud. The usage of this technique make the log analysis independent of mobile device resources. They have proposed a methodology that records the logs and sends the log file to the cloud for analysis. It has been assumed that higher the frequent interaction of bot using C&C server, higher are the chances of its detection. They have mostly targeted HTTP based botnets attacks as their higher chances of presence present in Android devices.

B. Dynamic or Runtime execution analysis

1) SmartBot: The author in [40] proposed the dynamic analysis framework which consist of three component: Dynamic Analyis, feature mining and learning. It is

S.No.	Year	Name	Architecture	Comments
1.	2011	Droiddream Light	Centralized HTTP	Download Malicious Apps, Theft of Private Data
2.	2012	Non Compatible C	P2P	Data Theft, DDoS attacks to compromise enterprise networks [32]
3.	2012	TigerBot	Centralized SMS	Capture and Upload images, Changes device settings
4.	2013	Game Over Zeus	P2P mutation of Centralized	theft of Data, Bitcoin, Skype and Banking credentials. [33]
5.	2013	Obad Botnet	Centralized HTTP	Admin rights of a device, device settings, gaining access to restricted communication channels
6.	2014	BMaster	Centralized HTTP/SMS	Revenue generation, theft of private data
7.	2014	Wroba.M	Centralized HTTP	Installation of Banking Malware [34]
8.	2014	Xsser.A	Centralized HTTP	spying and theft of private data
9.	2016	MUSE	Hybrid Structure (SMS, HTTP & bluetooth)	DDoS Attacks
10.	2016	Mirai	Centralized	DDoS Attacks may lead to Ransomware
11.	2016	Slow Botnet	Centralized HTTP/HTTPS	DDoS attacks leading to shutting of webservers advanced version of LOIC [35]

TABLE I: Time-line of Mobile botnets

the one of the method that uses dynamic observation of infected binaries. It identifies the critical features of mobile botnet applications, how they differ from normal applications. Usually, security practitioners rely on analysis tools to extract information in an automated fashion. Over here, they have conducted Dynamic analysis using the cloud based malware analysis platform Andrubis [41]. The outcome of the analysis was in form of XML files. In the second step feature mining was used to extract and observe various behavioral properties of botnet attack. This is followed by ANN back-propagation learning model for class labeling. They have also conducted a comparative analysis of the model with six different classification model (SVM, multilayer perceptron (MLP), BayesNet, simple logistic regression, Random forest, and J48). SmartBot is used to detect and analyze Android based mobile botnet applications using augmented machine learning techniques.

C. Hybrid Approaches

1) DroydSeuss [42]: It is one of the suggested public mobile Trojan trackers for the Botnets. It is based on detecting C&C channels endpoints statically and dynamically from the sample. Then the analysis of the metadata usually attached with endpoints is carried out which gives the positive signals of the presence of malware or crime. Analysis of any apk (mobile file) by the DroydSeuss involves data extraction, a ranking of endpoints and Data Mining. Data extraction lays emphasis on finding two types of C&C endpoints from selected sample which are mainly based on the web and phone number. This phase has to filter through static and dynamic data. In the case of static data, apktool is used to disassemble the APK archives. On the other hand, in the case of dynamic data archive is allowed to run in instrumented sandbox. Tracedroid was used by the authors of DroydSeuss to analyze and generate traces of endpoints. In the second phase, endpoints were prioritized and were given ranks based on levels such as suspicion, significance, and importance. The last phase comprises of relating metadata with corresponding endpoints found in the sample. To evaluate the tracker, 4293 samples of banking Trojans were taken from the virus total intelligence API and were subjected to the DroydSeuss. They were able to detect a data-stealing Trojan and an active Trojan which was affecting numerous Chinese and Korean customers. This tracker comes up with some of the limitations such as the inability of DroydSeuss to track the native code. It has a limited approach of dynamic analysis.

V. Recommendations

As we have seen innumerable threat to the IoT (Internet of Things), Mobile devices etc. We want to give the recommendations to improve the security of the iOS and Android based devices.

1) **Install Authorized Applications:** Users should practice security hygiene by not installing the applications from unauthorized origins. It has been seen by Dorazio et al [43] that jail broken iphones are more vulnerable to malware attacks. While working in closed/open network user should always disable auto run features. This feature can help the attacker to insert malicious code easily on victim workstation [44].
2) **Passwords:** It is strongly recommended that the IoT devices default password should be changed immediately after installation of the devices. IoT devices are usually connected to the Cloud and while choosing cloud providers users should ensure that they have proper security mechanism to detect the botnet attacks such as Web Application Firewall (WAF) and DDoS mitigation. Limited user interfaces is another contributing factor of security ignorance in IoT devices.
3) **Fine Grained restrictions:** Android and Iphones should allow for selectively authorizing a client software to access its device resources. Dorazio et al [43] recommends the usage of OAuth protocol in Apple and Android devices.
4) **Use Remediation tools:** It is always recommended that mobile devices should have remediation tool such as Symantec mobile security [45], McAfee Mobile Security etc. In this case, the anti-virus scanner to bypass apk

file which are controlled by mobile OS and therefore, vulnerable to botnet attacks.

5) **Browser:** It's recommended to change the browser for surfing on mobile. The browser for which most of the malware are written is on Internet explorer and Mozilla Firefox [45]. It is also worth mentioning that scripts on the mobile devices should be disabled in order to protect from the attacks.
6) **Web Filtering Service:** It's one of the best way to fight against the bots. The FaceTime, Websense and Cyveillance are the examples. These services scan the web sites which exhibits malicious activity and it block those sites from the users [46]. There is also tools like Ironport [47] and Websense which can restrict sending/receiving of emails from malware sources. The ingress and egress filtering can be used. Botnet basically initiates connection with multiple servers and then use them to extract private information which can be preventing by using the filtering approach.
7) **Implementing ACL:** In certain environments, communication between workstations from different departments are not required. Private virtual LAN and ACL (access control list) should be utilized to restrict the ability of undesired user to access the confidential information. It is recommended to implement network side ACL (Access control list) for UDP port 1900 and other specific TCP ports [24].
8) **Monitor DNS Queries:** Response of the workstation towards a DNS queries can be considered as a clue for the attack and also ones having very small TTL(Time to Live)are most prone to attacks. Monitoring the DNS queries can allow the user to restrict the attack in initial stages [44].

VI. Conclusion

In this paper, we have discussed about the latest attacks through botnets and how they can be dangerous to the Internet. We have done extensive survey of the latest attacks focusing on Botnets on non-PC devices to till date. After which we have given the insight of these attacks and what vulnerabilities allow these attacks to take place. Lastly, recommendations have been given for the users to protect their devices against these attacks. The vulnerabilities which has been seen are minor but it can cause full compromise of devices. Hence, precautions and even minor security measures should be taken seriously.

References

[1] BullGaurd, "http://www.bullguard.com/bullguard-security-center/mobile-security/mobile-threats/mobile-botnets.aspx," 2016.

[2] E. Cooke, F. Jahanian, and D. McPherson, "The zombie roundup: Understanding, detecting, and disrupting botnets." *SRUTI*, vol. 5, pp. 6–6, 2005.

[3] P. E. Chaudhry, "The looming shadow of illicit trade on the internet," *Business Horizons*, vol. 60, no. 1, pp. 77–89, 2017.

[4] Symantec, "https://www.symantec.com/connect/blogs/androidbmaster-million-dollar-mobile-botnet," 2016.

[5] A. Flo and A. Josang, "Consequences of botnets spreading to mobile devices," in *Short-Paper Proceedings of the 14th Nordic Conference on Secure IT Systems (NordSec 2009)*, 2009, pp. 37–43.

[6] C. Schiller and J. R. Binkley, *Botnets: The killer web applications*. Syngress, 2011.

[7] T. Hindu, "http://www.thehindu.com/sci-tech/technology/how-botnets-are-breaking-into-smart-homes/article16078750.ece," 2016.

[8] T. H. News, "http://thehackernews.com/2016/10/linux-irc-iot-botnet.html," 2016.

[9] W. Chen, X. Luo, C. Yin, B. Xiao, M. H. Au, and Y. Tang, "Muse: Towards robust and stealthy mobile botnets via multiple message push services," in *Australasian Conference on Information Security and Privacy*. Springer, 2016, pp. 20–39.

[10] H. Lee, T. Kang, S. Lee, J. Kim, and Y. Kim, "Punobot: Mobile botnet using push notification service in android," in *International Workshop on Information Security Applications*. Springer, 2013, pp. 124–137.

[11] S. Zhao, P. P. Lee, J. Lui, X. Guan, X. Ma, and J. Tao, "Cloud-based push-styled mobile botnets: a case study of exploiting the cloud to device messaging service," in *Proceedings of the 28th Annual Computer Security Applications Conference*. ACM, 2012, pp. 119–128.

[12] F. Xiangning and S. Yulin, "Improvement on leach protocol of wireless sensor network," in *Sensor Technologies and Applications, 2007. SensorComm 2007. International Conference on*. IEEE, 2007, pp. 260–264.

[13] A. Kitana, I. Traore, and I. Woungang, "Impact study of a mobile botnet over lte networks," *J Internet Serv Info Sec*, vol. 6, no. 2, pp. 1–22, 2016.

[14] P. Farina, E. Cambiaso, G. Papaleo, and M. Aiello, "Are mobile botnets a possible threat? the case of slowbot net," *Computers & Security*, vol. 58, pp. 268–283, 2016.

[15] S. Hegelich and D. Janetzko, "Are social bots on twitter political actors? empirical evidence from a ukrainian social botnet," in *Tenth International AAAI Conference on Web and Social Media*, 2016.

[16] J. Zhang, R. Zhang, Y. Zhang, and G. Yan, "The rise of social botnets: Attacks and countermeasures," *IEEE Transactions on Dependable and Secure Computing*, 2016.

[17] InfoSecurity, "https://www.infosecurity-magazine.com/news/kaiten-malware-returns-to-threaten/," 2017.

[18] C. N. Jersey, "https://www.cyber.nj.gov/threat-profiles/botnet-variants/aidra-botnet," 2016.

[19] C. report, "https://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/," 2014.

[20] Symantec, "https://www.symantec.com/connect/blogs/there-internet-things-vigilante-out-there," 2016.

[21] Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, "Iotpot: analysing the rise of iot compromises," *EMU*, vol. 9, p. 1, 2015.

[22] D. Reading, "http://www.darkreading.com/vulnerabilities—threats/do-gooder-worm-changes-default-passwords-in-vulnerable-iot-devices/d/d-id/1327341," 2016.

[23] Y. Bachy, F. Basse, V. Nicomette, E. Alata, M. Kaâniche, J.-C. Courrège, and P. Lukjanenko, "Smart-tv security analysis: practical experiments," in *Dependable Systems and Networks (DSN), 2015 45th Annual IEEE/IFIP International Conference on*. IEEE, 2015, pp. 497–504.

[24] H. Moore, "Security flaws in universal plug and play: Unplug. dont play," *Rapid7, Ltd*, vol. 8, 2013.

[25] A. Technica, "https://arstechnica.com/security/2016/11/notorious-iot-botnets-weaponize-new-flaw-found-in-millions-of-home-routers/," 2016.

[26] TNW, "https://thenextweb.com/gadgets/2017/01/31/netgear-vulnerability-router-bypass," 2017.

[27] NIST, "https://web.nvd.nist.gov/view/vuln/detail?vulnid=cve-2017-5674," 2017.

[28] Cybereason, "https://www.cybereason.com/cve-ip-cameras/," 2017.

[29] vuldb, "https://vuldb.com/?id.97736," 2017.

[30] NIST, "https://web.nvd.nist.gov/view/vuln/detail?vulnid=cve-2017-6552," 2017.

[31] Cisco, "https://www.theregister.co.uk/2016/06/02 /cisco_warns_of_ipv6_dos_vulnerability/," 2016.

[32] T. Strazzere, "https://blog.lookout.com/blog/2014/11/19/notcompatible/," 2014.

[33] D. Andriesse, C. Rossow, B. Stone-Gross, D. Plohmann, and H. Bos, "Highly resilient peer-to-peer botnets are here: An analysis of gameover zeus," in *Malicious and Unwanted Software:" The Americas"(MALWARE), 2013 8th International Conference on*. IEEE, 2013, pp. 116–123.

[34] R. Nigam, "A timeline of mobile botnets," *Virus Bulletin, March*, 2015.

[35] Gizmodo, "http://gizmodo.com/5877719/heres-the-tool-anonymous-is-tricking-the-internet-into-using," 2012.

[36] M. Spreitzenbarth, F. Freiling, F. Echtler, T. Schreck, and J. Hoffmann, "Mobile-sandbox: having a deeper look into android applications," in *Proceedings of the 28th Annual ACM Symposium on Applied Computing*. ACM, 2013, pp. 1808–1815.

[37] S. Anwar, J. M. Zain, Z. Inayat, R. U. Haq, A. Karim, and A. N. Jabir, "A static approach towards mobile botnet detection," in *Electronic Design (ICED), 2016 3rd International Conference on*. IEEE, 2016, pp. 563–567.

[38] A. Feizollah, N. B. Anuar, R. Salleh, G. Suarez-Tangil, and S. Furnell, "Androdialysis: Analysis of android intent effectiveness in malware detection," *Computers & Security*, vol. 65, pp. 121–134, 2017.

[39] D. A. Girei, M. A. Shah, and M. B. Shahid, "An enhanced botnet detection technique for mobile devices using log analysis," in *Automation and Computing (ICAC), 2016 22nd International Conference on*. IEEE, 2016, pp. 450–455.

[40] A. Karim, R. Salleh, and M. K. Khan, "Smartbot: A behavioral analysis framework augmented with machine learning to identify mobile botnet applications," *PloS one*, vol. 11, no. 3, p. e0150077, 2016.

[41] L. Weichselbaum, M. Neugschwandtner, M. Lindorfer, Y. Fratantonio, V. van der Veen, and C. Platzer, "Andrubis: Android malware under the magnifying glass," *Vienna University of Technology, Tech. Rep. TR-ISECLAB-0414-001*, 2014.

[42] A. Coletta, V. Van Der Veen, and F. Maggi, "Droydseuss: A mobile banking trojan tracker-short paper," *Financial Cryptography and Data Security, Lecture Notes in Computer Science (LNCS). Springer Berlin Heidelberg*, vol. 1, 2016.

[43] C. J. DOrazio, K.-K. R. Choo, and L. T. Yang, "Data exfiltration from internet of things devices: ios devices as case studies," *IEEE Internet of Things Journal*, 2016.

[44] eSecurity Planet, "http://www.esecurityplanet.com/trends/article.php/3920881/11-ways-to-combat-botnets-the-invisible-threat.htm," 2017.

[45] Symantec, "https://www.symantec.com/en/aa/mobile-device-security/," 2017.

[46] McAfee, "http://www.pcworld.com/article/137821/article.html," 2017.

[47] IronPort, "http://www.ironportstore.com/email-security.asp," 2017.