International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 5 | ISSN : 2456-3307

IOT Malware : An Analysis of IOT Device Hijacking

M. Shobana*[1], Dr.S.Rathi[2]
*[1]Research Scholar, *1Department of Computer Science and Engineering, Government College of Technology, Coimbatore, India
[2]Senior Assistant Professor, 2Department of Computer Science and Engineering,Government College of Technology, Coimbatore, India

ABSTRACT

The tremendous improvement in the network technology flourishes all the fields which includes defense, medical, industries etc beyond the human imagination. This improvement leads to the birth of IoT (Internet of Things), that is it connects all types of devices in the lake of Internet. Increase in the usage of Internet gradually increases the threat of security widely among the applications that are based on IoT. The starting point for this security threat is the IoT device which is vulnerable to the hacker's attack. This paper explores various types of IoT malware and spots the vulnerables points in the IoT environment.

Keywords : Internet of things; Malware; IoT Devices; PDoS; DDoS.

I. INTRODUCTION

The INTERNET OF THINGS (IOT) has been foreseen to be the core technology which would make smart cities and smart homes feasible in the future. The IoT is envisaged to be made of several heterogeneous devices with unique identifiers. While many existing devices, such as networked computers or mobile phones, have some form of unique identities and are also connected to the Internet, the focus of IoT is in the configuration, control, and networking via the Internet of Devices or "Things" that are customarily not associated with the Internet.[1]

The IoT emerges as a dream of a future Internet where any question having processing and sensorial abilities can speak with different gadgets utilizing Internet communication protocols, with regards to detecting applications. A large number of such applications are required to utilize a lot of detecting and actuating gadgets, and in outcome its cost will be a critical element. Then again, cost confinements manage limitations regarding the assets accessible in sensing phase, for example, memory and computational power, while the unattended work of numerous gadgets will likewise require the utilization of batteries for energy storage. In general, such components inspire the outline and appropriation of communication and security mechanism improved for compelled detecting stages, fit for giving its functionalities productively and dependably. As the Internet communication framework develops to incorporate detecting objects, proper components will be required to secure interchanges with such gadgets, with regards to future IoT applications, in territories as differing as medical, smart grid, home robotization and smart city. After various research commitments in the current past focusing on low-energy remote detecting applications and correspondence secluded from the outside world, a move towards its joining with the Internet is taking place.[2]

IoT being a generally new idea, the security challenges included have not been tended to properly at the plan level for these objects. Utilizing powerful security hones, particularly confirmation and key administration plans to ensure anonymity and protection, is required [3].

II. IoT SECURITY THREATS

As the IoT matures, so will the security threats. Inevitably, attackers will resort to vulnerabilities that will wreak unavoidable, persistent, and largescale havoc[4]. The followings are the vulnerable points to the hackers in the IoT environment:

A. Insecure wireless connections
B. Incompatibility in Internet and IoT application domains
C. Hardware diversity
D. IoT devices
E. Data reside in the cloud
F. Identifying every “thing”

III. IoT MALWARES

Malware, or malicious software, is a kind of software used to distract computer or mobile operations, gather sensitive information, gain access to private computer systems, or display unwanted things. The malware which is specially designed to compromise IoT devices (home routers ,CCTV Cameras, printers)is referred to as IoT malware. The real time scanning performed by antivirus software is a great overhead in IoT devices. They have founded many botnets and worms which is expert in affecting the insecure IoT devices. Chaitanya Aggarwal et al proposed a technique to resolve the IoT malware using software defined network and edge computing[5]. In this paper, Nine most vulnerable malwares have been analyzed evolved from the year 2013 to 2017.Out of nine malwares, seven of them are IoT botnets and the remaining two are IoT Worm.

IV. IoT BOTNETS

The behavior of the IoT botnet is close enough to the normal botnet, the dissimilarity is, this botnet is mainly designed to target IoT devices. A botnet is a robot network of compromised machines, or bots, that run malicious software under the command and control of a botmaster. Botnets have a wide range of detestable purposes including email spam delivery, distributed denial-of-service (DDoS) attacks, password cracking, key logging, and crypto currency mining.[6]

A. Bricker bot

Bricker bot founded by Radware is a kind of botnet which is equipped for influencing IoT gadgets, for example, a set top box,routers and so on. That is any gadget which is associated with the Internet. Bricker bot is intended to build up lasting Denial of Services Radware's honeypot, recorded 1,895 PDoS endeavors performed from a few areas around the globe. Its sole reason for existing was to bargain IoT gadgets and degenerate their storage.

Bricker bot utilizes the assault procedure, Telnet brute force – which is utilized by Mirai botnet. Bricker bot for the most part focused on the IoT gadget which depends on Busy box-linux. BusyBox consolidates minor forms of numerous basic UNIX utilities into a single little executable. It gives substitutions to the vast majority of the utilities more often discover in GNU fileutils, shellutils, and so on[7].

1) BrickerBot.1:

Bricker bot.1 got found on March 20 ,2017[8]. BrickerBot.1 infected 1,895 gadgets in the initial four days of its operation and its exist period is from 20th to 25th March 2017 . According to the researchers the attacks of this malware has been stopped. These gadgets additionally have SSH revealed through an older version of Dropbear SSH server. The greater

part of these gadgets were additionally distinguished as universality system gadgets running outdated firmware. Some of these gadgets are get to connects with beam directivity [9].

2) BrickerBot.2

Radware's honeypot recorded endeavors from a moment, fundamentally the same as bot prefer BrickerBot.1 which began Permanent Denial of Service endeavors on a similar date – both bots were found short of what one hour separated –with bring down power yet more exhaustive and its location(s) disguised by TOR egress nodes.It has release near 12 assaults for every day.It targets Linux-based gadgets which could possibly run BusyBox and which uncover a Telnet benefit ensured as a matter of course or hard-coded passwords[10].

3) BrickerBot.3:

BrickerBot.3 showed up on April 20,2017.It has propelled 1,295 assaults within just 15 hours. It utilized a changed attack script that additional few commands intended to all the more totally sudden stunning exhibition its objectives. BrickerBot.3 assaulted about 1,400 gadgets in 24 hours [11].

4) BrickerBot.4:

In the vicinity of 5:22pm and 8:44pm GMT a similar honeypot additionally distinguished yet another, very sequence of commands. The assault was just endeavored from a single device which was situated on the Clearnet and upon examination additionally had an obsolete variant of the Dropbear SSH server (SSH-2.0-dropbear_2014.63). This isolated bot performed 90 assaults and was not seen again in the vicinity of 8:44pm and midnight[12].

B. Leet

Leet founded by Imperva Incapsula is a botnet found on December 21,2016.It assaults the imperva network with an enormous record of 650Gbps utilizing DdoS(Distributed denial of services) attack.With the assistance of some defenseless IoT gadgets, this botnet enters the imperva network effectively. Hacker Programmers actualized the IP ridiculing procedures so it is difficult to find the vulnerable gadget in the system[13].

The attack came in two waves. The first wave kept going around 20 minutes and crested at 400 Gbps. This bombed in its motivation. "The offender regrouped and came back for a second round," reports Imperva. In the second wave enough botnet to produce a 650 Gbps DDoS surge of more than 150 million packets for every second (Mpps).Mirai payloads are created from random strings, while the payloads in this assault were organized from the substance of system records. Just 0.01% of all packets produced from leet indicated similarity from mirai assault. This present assault's activity was created by two diverse SYN payloads: Regular ones, and unusually huge SYN packets extending from 799 to 936 bytes in size. The previous was utilized to accomplish high Mpps(million bundles every second) packet rates, while the last was utilized to scale up the attack's ability to go 650 Gbps.[14]

C. Mirai:

Mirai botnet was founded by MalwareMustDie On September 30, 2016 the Mirai botnet code was distributed online in the hacking group discussion "Hackforums". The source code for the botnet was then openly discharged on the English-language hacking group Hackforums on September 30 by a client utilizing the screen name Anna-senpai. Creators of the botnet code regularly do this when their code is by and large broadly utilized or is utilized as a part of a prominent assault. Distributing the code ensures that law implementation won't have the capacity to recognize the maker of the botnet exclusively by finding a duplicate of the source code on a system. The arrival of the code made it conceivable to look at precisely how the Mirai botnet functions and brought on an expansion

in assaults credited to the Mirai botnet and subsidiaries[15]

Mirai is a type of malware pecularily designed to capture Internet of Things devices to attack and keeps them into a botnet-a gathering of computing devices that can be halfway controlled. From that point this IoT armed force can be utilized to mount distributed denial of service (DDoS) attacks in which a firehouse of garbage movement surges an objective server with pernicious activity. It distinguishes a portion of the command and control framework related with the botnet, including various snarky domains with the .cx domain. The domains are prefixed with "network" or "report" in light of their roles in the botnet[16].

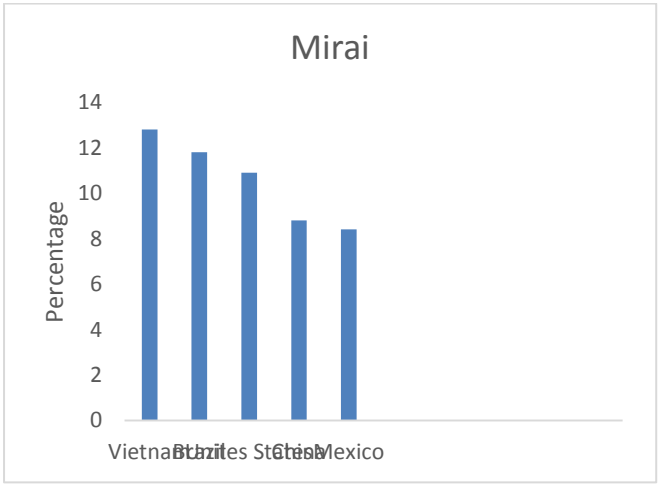

Figure 1: Countries infected by Mirai

D. *Amnesia:*

Amnesia was founded by PaloAlto Networks. On 22nd march 2016,the assault about the amnesia cames into the light. It is also called as Tsunami and it was established by reseachers who worked at palo alto systems. Amnesia botnet is extraordinarily intended to influence DVR(digital video recorder).This botnet is likewise tends to influence gadgets which depends on LINUX OS and it is made by China-based TVT Digital. It is distinguished that about identical items from more than 70 worldwide vendors. Analysts expresses that the defect is affecting around 227,000 gadgets everywhere throughout the planet including the accompanying countries, for example, Taiwan, the United States, Israel, Turkey, and India.

Amnesia is said to be the primary malware which influences the malware analysis sandbox itself.It is equipped for ruling every one of the gadgets once it is associated with internet.This botnet ready to erase all the document which get enter on the Linux based servers. Amnesia communicates with its C2 server utilizing the IRC protocol. CCTVSCANNER and CCTVPROCS are the commands utilized by amnesia which are utilized for checking and exploiting the RCE vulnerability in TVT Digital DVRs. In the wake of accepting the commands, Amnesia will right off the basic HTTP request to the IP address included with the order, checking whether the objective is a vulnerable DVR gadget[17].

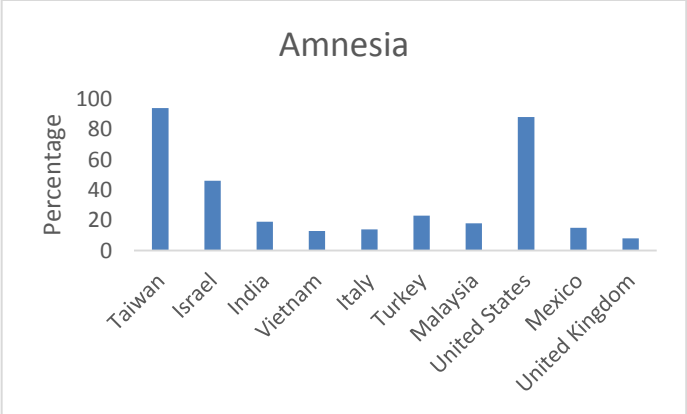

Figure 2: Countries infected by Amnesia

E. ***Remaiten:***

Remaiten was founded by ESET. Remaiten consolidates the elements of two malwares specifically kaiten and gafgyt with peculiar spreading mechanism. A noticeable feature of Linux/Gafgyt is telnet checking. At the point when educated to perform telnet checking, it tries to interface with arbitrary IP addresses reachable from the Internet on port 23. If the connection succeeds, it will attempt to figure out the login information from an implanted list of username/password combination. If it

successfully sign in, it telecasts a shell command to download bot executables for numerous models and tries to run them. This is a straightforward though boisterous method for contaminating new victims, as it is likely one of the binaries will execute on the running architecture.

Linux/Remaiten enhances this spreading mechanism via conveying downloader executables for CPU designs that are generally utilized as a part of embedded Linux gadgets, for example, ARM and MIPS. In the wake of signing on through the telnet provoke of the victim device, it tries to decide the new victim device's platform and exchange just the proper downloader. This downloader's work is to ask for the architecture-appropriate Linux/Remaiten bot binary from the bot's C&C server. This binary is then executed on the new victim device, making another bot for the malicious operators to utilize[18].

Once executed, the bot keeps runs in the background and changes its procedure name to look authentic, with two version utilizing "- bash" for that (to be specific Remaiten 2.0 and 2.1), and the third (version 2.2) utilizing "- sh." After that, utilizing the create_daemon funcion, the bot makes a document named ".kpid" in one of the predefined daemon catalogs and composes its PID to a record. Remaiten version 2.2 incorporates a wget/tftp command to download a shell script that downloads the bot binaries, including records that targets platforms, for example, PowerPC and SuperH. This demonstrates awful performers are prepared for any circumstance, as they went into the inconvenience of compiling their malware for these architectures[19].

F. *Bashlite*

Bashlite was founded by *Level 3 Communications.*Bashlite is a kind of malware that infects Linux devices and utilize these devices to dispatch DDoS assaults. The malware is otherwise called Gafgyt, Torlus, Lizkebab and some others [20] [21]. It was made by a software engineer working under the pseudonym "Sinden"[22]. The malware comprises of server and client code. The server code is intended to keep running on at least one Command and Control (C&C) servers. With those servers, the botnet proprietor can control the group of bots running the client code. The two communicate with each other with a custom protocol propelled by IRC.If an IP-address has an open Telnet port, the malware will attempt to login to the gadget utilizing a list of predefined username/password combination.

1) Version 1(ELF BASHLITE.A):

It was first seen in September 2014[23]. This variant does not do much harm once successfully logged into a device: It checks whether the device runs a BusyBox shell [24]. If this is the case it executes a command to echo the string "gayfgt" B.

2) Version 2(ELF BASHLITE.SMB):

A later variation (ELF BASHLITE.SMB [25]), recognized in October 2014, is more harmful[25]. It initially downloads two scripts from a remote server. Those scripts are intended to increase full access to the system by mishandling the ShellShock exploit [26] [27]. One of the shell scripts downloads the malware for an extensive variety of models utilizing wget and executes them all.

As the malware is self-recreating, the hacker needs at least one compromised device to begin with. This is accomplished by utilizing a Perl Telnet bot to infect the main gadgets [28].The "flooder" some portion of the malware consolidates four DDoS assaults and a commented (not active)e-mail function. The DDoS attacks are UDP, TCP, Junk and Hold floods. The new variant highlights some additional control elements and one new attack "GETFLOOD", which dispatches a HTTP GET surge DDoS on the objective [29].

G. Wifatch

Wifatch malware was founded by Symantec software company and showed up on the time of November 2014. It is likewise called as Zollard and Reincarna. It influences a large number of IoT gadgets which incorporates routers, cameras. It for the most part focuses on the gadgets which holds weak user name and password by introducing telnet protocols on the gadget. When it infects a gadget, Wifatch checks it for known malware and handicaps Telnet to keep others out.While a threat like Wifatch can be utilized for an extensive variety of malicious activities, including distributed denial-of-service attacks and DNS poisoning, the way that it wasn't utilized for anything malicious has persuaded that its administrators are "IoT vigilantes" whose objective is to secure defenseless gadgets. Be that as it may, the engineers of Wifatch claim to have made the malware to learn, to comprehend, and for clients' security without uncovering their own personality. The Wifatch botnet utilizes a peer-to-peer (P2P) architecture to prevent takeovers and every one of the orders sent to the bots are marked with a private ECDSA key[30].

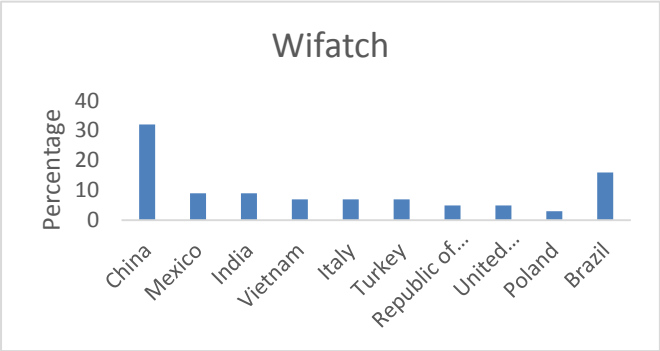

Figure 3: Countries infected by Wifatch

V. IOT WORM

A PC worm is a self-imitating PC program that enters operating system with the goal of spreading malicious code. Worms use systems to send duplicates of the first code to different PCs, bringing about damage by expending transfer speed or conceivably erasing records or sending reports by means of email. Worms also can install backdoors on computers.

A. Hajime

Hajime is a Japanese word and its meaning is "starting" This malware is first found on October 5,2016 by Rapidity networks. Hajime utilizes Bit Torrent's UTP for direct peer to peer communication. The Hajime is a worm and it has a lifecycle comprises of three phases, they are reconnaissance and infection phase, downloader stub and DHT downloader A Hajime injection starts when a hub as of now in the Hajime network, scanning random IPv4 addresses on public in general Internet discovers a gadget which acknowledges connection on TCP port23, the assigned port for the Telnet benefit. The assaulting Hajime hub endeavors a few client name and secret key blends from its hardcoded list of credentials and, after being allowed section, inspects the objective framework and starts its infection in stages. The main stage is a little, fleeting file exchange program which interfaces back to the attacking hub and duplicates down a considerably bigger download program. The download program–the second stage–joins a shared decentralized system and recovers its arrangement and a checking program. The examining program looks general society web for more helpless frameworks to contaminate, therefore proceeding with the life cycle.The Hajime worm appears to be the work of a white hat hacker attempting to wrestle control of IoT devices from Mirai and other malicious threats[31].

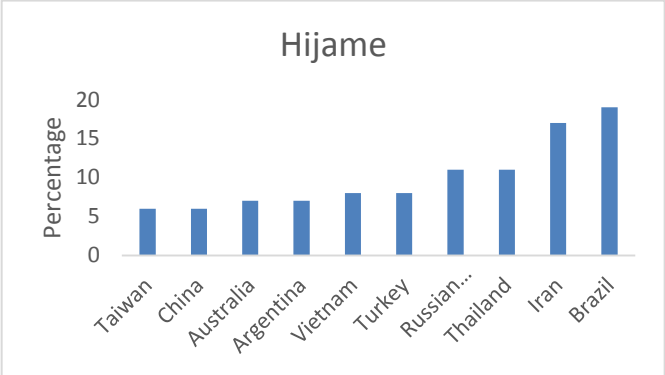

Figure 4: Countries infected by Hijame

B. Darlloz

Symantec confirmed the finding of the first IoT malware, Linux.Darlloz, which brings up the malware issue for IoT security [32].Darlloz is a sort of worm and it was found on 26,November,2013.The worm targets PCs running Intel x86 architecures. That, as well as spotlights on devices running the ARM, MIPS and PowerPC designs, which are typically found on routers and set-top boxes. The fundamental motivation of this worm is to mine cryptocurrencies in the compromised IoT devices. The worm introduces "cpuminer," which is an open-source mining program. It then starts digging for Mincoins or Dogecoins, two spinoff cryptocurrencies from Bitcoin. Bitcoins can't be mined proficiently any more by PCs, yet Mincoins and Dogecoins can. Dogecoin is a decentralized, distributed computerized cash that empowers client to effectively send cash on the web. Both mincoins and dogecoins can be considered as Internet currency[33].Linux.Darlloz, at first seemed, by all accounts, to be not strange. It uses an old weakness in scripting language PHP to access a PC; endeavors to increase regulatory benefits by attempting a progression of normally utilized usernames and passwords and spreads itself via looking for different PCs. The worm leaves a secondary passage on the infected PC, enabling the attacker to issue orders to it. this worm does is sweep for occasions of another Linux worm, known as Linux.Aidra. In the event that it finds any documents related with this threat, it endeavors to erase them. The worm likewise endeavors to hinder the correspondences port utilized by Linux.Aidra. There is no charitable thought process behind evacuation of the other worm[34].

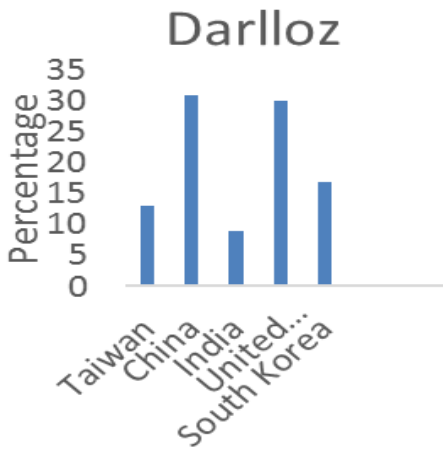

Figure 5:Countries infected by Darlloz

TABLE I. COMPARISON OF THE DIFFERENT MALWARE CHARACTERISTICS

Malware Name	Targeted IoT Devices	Targeted Architecture	Number of IoT Devices	Attack	Communication Protocol	Language used
BrickerBot	Devices using BusyBox such as webcams, toys,smart bulbs etc.	Linux	2 000,000	Permanent denial-of-attack (PDoS)	Transmission Control Protocol(TCP)	Linux Commands
Leet	All internet connected Devices	Linux,Unix	400,000	Distributed denial-of-service attacks (DDoS)	Transmission Control Protocol(TCP)	C
Hajime	DVRs,webcams, and routers	Not limited to any Specific	300,000	Brute-force attack	P2P(Peer-to-Peer)	C

		Architecture				

Malware Name	Targeted IoT Devices	Targeted Architecture	Number of IoT Devices	Attack	Communication Protocol	Language used
Mirai	CCTV camera	Linux,Windows	300,000	Distributed denial-of-service attacks (DDoS)	HTTP(Hypertext Transfer Protocol)	C
Amnesia	DVR	Linux	227,000	virtual machine evasion techniques	IRC(Internet Relay Chat)	Delphi
Remaiten	Routers	Linux	100,000	Distributed denial-of-service attacks (DDoS)	IRC(Internet Relay Chat)	Shell Commands
Bashlite	web-connected video cameras and DVRs	Linux,X86,ARM, MIPS	1000,000	Distributed denial-of-service attacks (DDoS)	IRC(Internet Relay Chat)	C
Wifatch	Home routers	Linux,ARM,MIPS,SH4, PowerPC and X86	13,000 Appx.	Distributed denial-of-service attacks (DDoS)	Transmission Control Protocol(TCP)	Perl
Darlloz	Routers,Set top boxes	Linux	Greater than 31,000	Coin Mining	HTTP	PHP

VI. DISCUSSION

The table 1 shows that the behavior and range of vulnerability of each malware. Fig 1,2,3,4,5 shows the percentage of each country which is infected by the corresponding IoT malwares.From this analysis, some points can be concluded to take certain steps regarding the privacy issues involved around the IoT devices. First of all, the most attractive IoT devices for hackers is home routers, Set top boxes and CCTV cameras. These devices act as a slave to the attacker. Most of the malware targeted Linux based tiny devices. Specifically, it is clear that most of the system which is running busybox are likely to be targeted easily. The size and power of the botnet are the main parameters to measure the influence of the malware towards the targeted device. Here the size of the botnet can be calculated based on the number of the IoT got infected by that particular botnet. Based on this survey, some architectures namely X86, ARM and MIPS are repeatedly targeted by many malware like Bashlite, Wifatch, Remaiten, Darlloz and Mirai. Some malware like Hajime is capable to inject all kinds of architecture based IoT devices. It

releases various kinds of version according to the IoT device. Since most of the IoT devices is based on the linux system, hackers are equipping their malware to affect that particular operating system. Recently most of the botnet is using Transmission control protocol as its communication protocol to transmit its command. This technique makes use of accessing the port 23 which is in IoT device. In most of the IoT device, port 23 keeps open and it acts as a most vulnerable point to the botnet.

VII. CONCLUSION

In this paper, nine of the IoT malware has been analyzed in terms of its degree of vulnerability. For the past two years, most of the hackers concentrate on infecting the IoT devices because of its insecure design. Another reason behind this is, the user who is handling this simple device may be unaware of the hacking. While many users ensure that their computers are secure from attack, users may not realize that their IoT devices need to be protected too. Researchers have to concentrate on the security framework for the IoT devices which should be taken care of dynamic change of username and password. Rather than using signature based detection, implementation of behavior based detection can handle a new kind of malware.

VIII. REFERENCES

[1]. Bagha and V. Madisetti, Internet of Things—A Hands on Approach, India: Universities Press, 2015.

[2]. Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva ,Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues, IEEE communication surveys & tutorials,2015.

[3]. Sravani challa, mohammad wazid,ashok kumar das,Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications,IEEE Access 2017

[4]. Constantinos Kolias and Angelos Stavrou ,Securely Making “Things” Right,Computer,2015

[5]. Chaitanya Aggarwal , Kingshuk Srivastava Securing IOT Devices Using SDN and Edge Computing, International Conference on Next Generation Computing Technologies (NGCT-2016),2016

[6]. Pierluigi Paganini." Brickerbot botnet, the thingbot that permanently destroys IoT Devices " Internet: http://securityaffairs.co/wordpress/57839/malware/brickerbot-botnet-iot.html,April 8,2017.

[7]. “BrickerBot Permanent Denial-of-Service attack Update-A”.Internet: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-102-01A, April 12,2017.

[8]. Dan Goodin “BrickerBot, the permanent denial-of-service botnet is back with a vengeance”.Internet:https://arstechnica.com/security/2017/04/brickerbot-the-permanent-denial-of-service-botnet-is-back-with-a-vengeance/,April 25,2017.

[9]. Internet: BusyBox: A Swiss Army Knife for Linux

[10]. “BrickerBot PDoS Attack: Back With A Vengeance”.Internet:https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-back-with-vengeance/ ,April 21,2017.

[11]. Kevin Townsend,” Massive Attack from New "Leet Botnet" Reaches 650 Gbps”.Internet: http://www.securityweek.com/massive-attack-new-leet-botnet-reaches-650-gbps, December 28, 2016.

[12]. Tara Seals,”Leet IoT Botnet Bursts on the Scene with Massive DDoS Attack”.Internet: https://www.infosecuritymagazine.com/news/leet-iot-botnet-bursts-on-the-scene/, Jan 3, 2017.

[13]. Motivating a Market or Regulatory Solution to IoT Insecurity with the Mirai Botnet Code

[14]. Lily Hay Newman,” The Botnet That Broke the Internet Isn’t Going Away”.Internet: https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/, Sep 12,2016.

[15]. Greg Masters,” Amnesia botnet targeting DVRs, Palo Alto report ”.Internet: https://www.scmagazine.com/amnesia-botnet-

targeting-dvrs-palo-alto-report/article/649070/, April 6,2017.

[16]. Claud Xiao, Cong Zheng and Yanhui Jia," New IoT/Linux Malware Targets DVRs, Forms Botnet".Internet:http://researchcenter.paloaltonetworks.com/2017/04/unit42-new-iotlinux-malware-targets-dvrs-forms-botnet/, April 6,2017.

[17]. Matthew Bing "The Lizard Brain of LizardStresser".Internet: https://www.arbornetworks.com/blog/asert/lizard-brain-lizardstresser/, June 29, 2016.

[18]. Michal Malik and Marc-Etienne M.Léveillé,"Meet Remaiten – a Linux bot on steroids targeting routers and potentially other IoT devices".Internet: https://www.welivesecurity.com/2016/03/30/meet-remaiten-a-linux-bot-on-steroids-targeting-routers-and-potentially-other-iot-devices/, Mar 30 2016

[19]. SecurityWeek News ,"New Remaiten Malware Builds Botnet of Linux-BasedRouters".Internet: http://www.securityweek.com/new-remaiten-malware-builds-botnet-linux-based-routers, March 30, 2016.

[20]. "BASHLITE".Internet: https://en.wikipedia.org/wiki/BASHLITE.

[21]. "Level-3,The Art of transformation".Internet: http://blog.level3.com/ security/attack-of-things/.

[22]. Internet: http://x.malwaremustdie.org/stat/ sinden.html.

[23]. "ELF_BASHLITE.A".Internet: http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/elf_bashlite.a.,Sep 26,2014.

[24]. Pierluigi Paganini "A new BASHLITE variant infects devices running BusyBox"Internet: http://securityaffairs.co/ wordpress/30225/cyber-crime/bashlite-exploits-shellshock.html, November 16, 2014.

[25]. Internet:http://www.trendmicro.com/vinfo/us/threatencyclopedia/malware/ELF_BASHLITE. SMB.

[26]. Eduard Kovacs , "BASHLITE Malware Uses ShellShock to Hijack Devices Running BusyBox".Internet: http://www.securityweek.com/bashlite-malware-uses-shellshock-hijack-devices-running-busybox, November 14, 2014.

[27]. Internet: https://en.wikipedia.org/wiki/Shellshock_(software_bug).

[28]. "MMD-0052-2016 - Overview of "SkidDDoS" ELF++ IRC Botnet".Internet: http://blog.malwaremustdie.org/2016/02/mmd-0052-2016-skidddos-elf-distribution.html, Feb 7 2016.

[29]. Internet: http://www.it-administrator.de/themen/sicherheit/fachartikel/204048.html.

[30]. Eduard Kovacs," Developers of Mysterious Wifatch Malware Come Forward".Internet: http://www.securityweek.com/developers-mysterious-wifatch-malware-come-forward, October 07, 2015.

[31]. Sam Edwards Ioannis Profetis ,Hajime: Analysis of a decentralized internet worm for IoT devices,2016.

[32]. Zhi-Kai Zhang , Michael Cheng Yi Cho , Chia-Wei Wang ,IoT Security: Ongoing Challenges and Research Opportunities.

[33]. Kaoru Hayashi," IoT Worm Used to Mine Cryptocurrency".Internet: https://www.symantec.com/connect/blogs/iot-worm-used-mine-cryptocurrency, Mar 19, 2014.

[34]. Bruce Sterling," Spime Watch: Linux.Darlloz, the Internet-of-Things worm".Internet: https://www.wired.com/2014/01/spime-watch-linux-darlloz-internet-things-worm/,Jan 29,2014.