International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Volume 7 Issue 3, March-2018, Impact Factor: 3.578

IoT: DDoS Attacks on IoT

Parul Suneja[1], Chirag Anand[2]

[1,2]Student, Department of Computer Science and Application, MDU, Rohtak, Haryana

ABSTRACT

When Kevin Ashton of MIT had first time coined the word "Internet of Things" in 1999 even he would have not imagined at that time that it will become the "next big thing" in 21st century. But everything has changed within a decade. Internet of Things refer as interconnection of smart object, included from small coffee machine to big car, communicate with each other without human interactions also called as Device to Device communications. With this rapid development of Internet of Things in different area like smart home, smart hospital etc. it also have to face some difficulty to securing overall privacy due to heterogeneity nature. Though "Internet of thing" is future and has opened opportunities in various fields, it has lots of pitfalls also. This paper puts light on one of those attacks namely Distributed Denial of Service attack and its effect on IoT.

Keywords: Internet of things, Distributed Denial of Service, IOT Attacks, IOT security risks and vulnerability.

1. INDRODUCTION

Internet of thing is defined as the system of interrelated computing devices and digital object having the ability to transfer data over the network without requiring any direct communication between person and device. Basically Internet of Things revolves around machine-to-machine communication, RFID (Radio Frequency Identification) and built.

Every day, hundreds of physical things get connected with the Internet to share local information to cyberspace. The US National Intelligence Council (NIC) estimates that by 2025 Internet nodes may reside in most of our surrounding things food packages, furniture, paper documents, and many more.

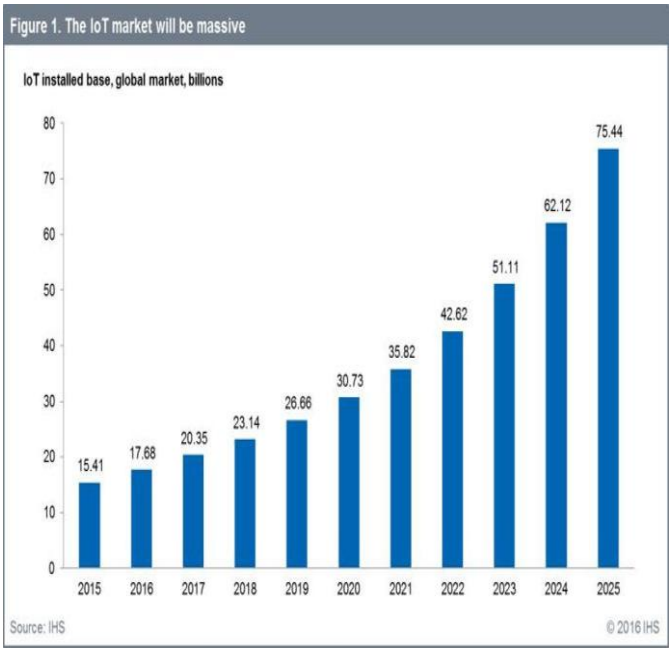

Figure 1: IoT Market will be massive

According to a report by IHS forecasts that the IoT market will grow from an installed base of 15.4 billion devices in 2015 to 30.7 billion devices in 2020 and 75.4 billion in 2025 .

However, the rapid growth of IoT also brings some new challenges in terms of security. Since billions of things are interconnected to perform personal as well as business related activities, attackers may find IoT a very attractive target of Attacks. A malicious individual can also launch attacks from the IoT environment. One very good example of these attacks is The DDos attack.

2. DOS/DDOS ATTACKS

Have you ever faced a situation like "The website is currently busy or unavailable"? It happens when a lot of people are surfing it. For example, when they announce our board results, a website often crashes. So how can you crash a website without using 100000 people? The answer lies in how you can beat a person alone? Kung fu possibly? Well, we don't need Kung fu but instead a technique called DoS (Denial Of Service). DoS attack is an attempt by malicious attacker to consuming resources or bandwidth of legitimate users. This attack is used to crash the website or make it slow. There are many programs/scripts that can send many requests to a website in one second and make it crash.

When a DoS is performed, many computers (or should I say systems) are simultaneously on the same website.

Such type of attacks when penetrated from various compromised node it called as DDoS. The most common DoS attack involves flooding of huge amount of traffic to consume network resource, bandwidth, target CPU time etc. Some of most common DoS attacks are SYN flood, DNS flood, Ping flood, UDP flood, ICMP broadcast etc.

Types of DDos Attacks:

1) Protocol Level Attack: Simply, this type of attack directly attacks the server. It tries to eat up all resources of the server or intermediate systems as Firewall/Load Balancers. It includes SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more. Actually, this attack resembles your simple kicks and punches, it means this attack works well. It is measured in Packets per second.

2) Application Layer Based Attacks: This attack is your special attack. It can finish the target in minutes if the target is vulnerable to it. It targets the software (Application layer) like windows, Open BSD, Apache etc. Its magnitude is measured in Requests per second.

3) Volume Based Attack: When everything fails (this is just an example, do not think that this is the last thing you can try) you just try attacking as fast as you can. It includes UDP floods, ICMP floods, and other spoofed-packet floods. The attack's goal is to saturate the bandwidth of the attacked site, and magnitude is measured in bits per second (Bps).

3. SECURITY RISKS AND VULNERABILITIES

When we talk about IoT, we mean all those devices that communicate and can be accessed via the internet based on their IP addresses. They include traditional office equipment like printers, copiers and video projectors, as well as the televisions in the conference room and reception areas, also devices, like the refrigerator and coffee maker in the break room. An increasing number of other equipment — such as climate control systems, motion detectors, and security and lighting systems — are also equipped with intelligence and remote access, so they can be controlled over the internet. Production systems are moving forward with IP-based machinery and industry. Last but not least, employees' personal devices — such as ubiquitous smart phones or smart watches — play a role in a company's security.

All these internet-connected devices create access points with which hackers can infiltrate a company's network and due to the wide range of devices and technologies, it is difficult to implement a cohesive security strategy. But the Krebs attack showed that it is no longer science fiction to imagine that a company could be attacked through these devices. The time has come to define policy for them and put protections in place.

Five such Security Vulnerabilities looming on the Internet of Things are:

Insecure Web Interface
To exploit this vulnerability, attacker uses weak credentials or captures plain text credentials to access web interface. The impact results in data loss, denial of service and can lead to complete device take over. An insecure web interface was exploited by hackers to compromise Asus routers in 2014 that were shipped with default admin user name and password.

Insufficient Authentication/Authorization
Exploitation of this vulnerability involves the attacker brute forcing weak passwords or poorly protected credentials to access a particular interface. The impact from this kind of attack is usually denial of service and can also lead to compromise of device. This vulnerability was exploited by ethical hackers to access the head unit of Jeep Cherokee via WiFi-connectivity. The WiFi password for Jeep Cherokee unit is generated automatically based upon the time when car

and head unit is started up. By guessing the time and using brute force techniques, the hackers were able to gain access to the head unit.

Insecure Network Services
Attackers use vulnerable network services to attack the device itself or bounce attacks off the device. Attackers can then use the compromised devices to facilitate attacks on other devices. This vulnerability was exploited by hackers that used 900 CCTV cameras globally to DoS attack a cloud platform service.

Lack of Transport Encryption
A lack of transport encryption allows 3rd parties to view data transmitted over the network. The impact of his kind of attack can lead to compromise a device or user accounts depending upon the data exposed. This weakness was exhibited by Toy Talk's server domain which was susceptible to POODLE attack. Toy Talk helps Hello Barbie doll to talk to a child by uploading the words of a child to server and provide appropriate response after processing it. Though there was no reported hack on this, such a vulnerability could easily lead to one.

Privacy Concerns
Hackers use different vectors to view and/or collect personal data which is not properly protected. The impact of this attack is collection of personal user data. This vulnerability was exemplified by the VTech hack wherein in hackers were able to steal personal data of parents as well as children using VTech's tablet.

4. PREVENTION & PRECAUTIONS:

The number of denial-of-service (DoS) or distributed-denial-of-service (DDoS) cyberattacks doubled from 3% to 6% in 2016, due to the lack of sufficient security controls of Internet-connected Internet of Things (IoT) devices. And of all IoT attacks, 60% originated from Asia, 21% from EMEA and another 19% from the Americas. The most likely reason for the high volume of attacks from Asia is that technology sourced from the region has historically been susceptible, and compromised infrastructure tends to be reused to perpetrate additional nefarious activities.
Some of the tips of precautions are:

Learn how to maintain the security of IoT devices. Consumers need to protect their IoT devices the same way they would their smart phones, tablets and home computers. Look for ways to set strong passwords, reading the manuals for instructions on how to lock down these devices.

Clean out old apps. Many of us tend to keep apps indefinitely, even if we don't use them. Check your devices periodically and delete apps you no longer use.

Own your online presence. Understand what information your devices collect and how they it is managed and stored.

Do your research. Before you purchase an IoT device, do a search to see if it has had security problems with it and if it can be easily hacked.

Change the default setting on the home router. This is worth reiterating: Strong passwords on home routers can prevent the type of DDoS that happened to Dyn.

Get aware where the risk is coming from
A company should evaluate every single device that is added to the network. It is also important to consider all network devices for penetration testing to determine what data they send on the internet. Some of this data is harmless, but it can be used as the basis for an attack when combined with other information.

Company guidelines should be updated to include the use of IoT devices.
They should, for example, define which devices are permitted on the company network and what data exchange with the network or the internet is wanted. Unwanted traffic can be prevented with the right security technology.

CONCLUSION

From the above discussion, we conclude that if 2016 was the year of the first really massive cyber attacks using IoT-enabled devices, it's pretty easy to predict that this will not be different in 2017 and beyond. It's probably a no-brainer that we can expect more security breaches and that the industry will come up with more security initiatives in regards with several aspects of the Internet of Things as it has already started to do. Regarding IoT security, Gartner said that "new threats will emerge through 2021 as hackers find new ways to attack IoT devices and protocols, so long-lived things may need updatable hardware and software to adapt during their life span."

The main problem with IoT devices is that their manufacturers have been slow to implement security. Most devices equipped with the most basic software, which often can't be updated. DDoS attacks using IoT devices can impact an organization in multiple ways.

As awareness increases, some "smarter" IoT devices can be brought up to current security standards with periodic firmware updates. Also who should be responsible for securing IoT ? Does this security — along with the protection of all the company's data and assets — fall under the CISO's domain? Defining who owns responsibility for IoT security is an important first step.

REFERENCES

[1] 7 Critical IoT Security Vulnerabilities https://www.attify.com/7criticaliotsecurityvulnerabilities/
[2] Hackers found 47 new vulnerabilities in 23 IoT devices at DEF CON http://www.csoonline.com/article/3119765/ security/hackers-found-47-new-vulnerabilities-in-23-iot-devices-at-def-con.html
[3] Issues in Internet of Things: A Survey By Prema N, Vedavathi N, Lovee Jain Department of Computer Science and Engineering, NIE Institute of Technology, Mysore, Karnataka, India http://www.ijraset.com/fileserve.php?FID=3169
[4] Internet of Things: Features, Challenges, and Vulnerabilities by Ebraheim, International Journal of Advanced Computer Science and Information Technology (IJACSIT)Vol. 4, No. 1, 2015, Page: 1-13, ISSN: 2296-1739 http://elvedit.com/journals/IJACSIT/wp-content/uploads/2015/02/internet-of-things.pdf
[5] The Security Risk within Smart Cities http://www.infosecisland.com/blogview/24951-The-Security-Risk-Within-Smart-Cities.html
[6] Smart Cities, Big Problems? The Risk of Malware in IoT-Enabled Infrastructure https://securityintelligence.com/ news/ smart-cities-big-problems-the-risk- of-malware-in-iot-enabled-infrastructure/
[7] US Army is using IoT tech and data to transform warfare https://internetofbusiness.com/us-army-iot-warfare/
[8] Roundup of Internet Of Things Forecasts And Market Estimates, 2016 https://www.forbes.com/sites/ louiscolumbus/2016/11/27/ roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#5697e882292d
[9] Study aout DDos Attacks https://www.cybrary.it/0p3n/dos-and-ddos/
[10] Imminent IoT Threats https://www.darkreading.com/endpoint/7-imminent-iot-threats/d/d-id/1327233