Introduction to botnet of things

Audit Course-7 (III) Subject: Botnet OF things

Introduction

What are Botnets ?

Internet of things is talk of the town now a days but the potential threat IoT has over the cyber safety is less emphasized. The possibility for attackers with all systems interconnected with no or less security measures installed in them, makes them vulnerable to all kinds of security attacks. Botnet consists of collection of private computers interconnected together and affected by malicious software, which can be controlled as a group without the owner‘s knowledge. Botnet is robot and Network combination, the bot here is the compromised device.

A botnet is network of compromised computers called Zombie computers or Bots,under the control of a remote attacker. Botnet is a collection of devices interconnected logically. The devices include range of handheld, household and other smart devices that are connected via internet.

Terminologies

Terminology	Meaning
A botnet's originator	Known as a "bot herder" or "bot master" controls the botnet remotely.
Command-and-Control (C&C)	Controls the botnet remotely.
Covert channel	Type of computer security attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy.
Internet Relay Chat (IRC)	It is an application layer protocol that facilitates communication in the form of text
Zombie computer	It is a computer connected to the Internet that has been compromised by a hacker, computer virus or trojan horse and can be used to perform malicious tasks.

Components

Components of Botnet

a. Command and Control Server
Often abbreviated as C&C, a command and control server is the centralized computer that issues commands to and receives information back from the bots. Command and control infrastructure frequently consists of several servers and other technical components. Most botnets use a client-server architecture, but some botnets are peer-to- peer (P2P), with the command-and control functionality embedded in the botnet.

b. Peer-to-Peer Botnet
Peer-to-peer (P2P) botnets use a decentralized network of bots for added protection against takedowns. While P2P botnets can include a C&C server, they may also operate without one and be structured randomly to further obfuscate the botnet and its purpose. While P2P botnets are less likely to be identified, the botmaster cannot easily monitor command delivery and the implementation can be complex.

c. Botmaster
Alternatively called a botnet controller or bot herder, the botmaster is the botnet‘s operator. This individual remotely controls the botnet, issuing commands to the C&C server, or to individual bots within the network. A botmaster‘s name and location are heavily obfuscated to prevent identification and prosecution by law enforcement.

d. Bot
An Internet-connected individual device within the botnet is called a bot. A bot is most often a computer, but a smart phone, tablet, or Internet of Things device can also be part of a botnet. A bot receives operational instructions from a command and control server, directly from the botmaster, or sometimes from other bots within the network.

e. Zombie
Another name for a bot. Because the bot is controlled by an outside computing device or person, it is likened to a fictional zombie‘.

f. Botnet Attack
A botmaster develops a botnet by distributing bot malware to infect PCs or other devices. He may also rent an existing botnet from another criminal. The newly harvested bots or —zombiesǁ report in to the botnet‘s command and control (C&C).The C&C now controls these bots and issues instructions for the bot to distribute executable malware files, as well as the email templates and potential victim address lists. The infected zombie bots receive the orders, each sending email messages carrying the malware payload to thousands of potential victims.

Types

Phishing
Most botnets rely on spam and phishing tactics to infect more devices and grow the botnet in size. In phishing and other forms of social engineering attacks, the botnet will send emails, post comments, and create messages on social media platforms imitating people and/or organizations that are known and trusted by the target victim.

Distributed Denial of Service (DDoS)
The idea behind using botnets for DDoS attacks is to overwhelm a target server with a massive number of requests (from the zombie devices) to crash, or at least slow down, the server significantly. DDoS is one of the most common ways botnets are utilized in criminal attacks, and often the most dangerous. Damages resulting from DDoS attacks can be severe and long-lasting, not only in terms of financial damages, but also reputational damages.

Account Takeover Attack
Bot herders can use botnets to perform various forms of Account Takeover (ATO) attacks, especially brute force (credential cracking) and credential stuffing attacks.
In a brute force attack, the zombie devices are commanded to try the different possibilities of a user password to “crack” the password. For example, if it’s a 4-digit pin, zombie device 1 will try “0000”, the second zombie device will try “0001”, and so on up to “9999” or until the right PIN has been guessed.

How to know if my system in under botnet attack ?

1. Is your computer or internet connection running slower than normal?
2. Did your computer start behaving erratically? Does it crash frequently? Do you receive unexplained error messages?
3. Did the fan kick into overdrive when your computer is idle?
4. Did you notice unusual internet activity (like high network usage)?
5. Does your browser close frequently and unexpectedly?
6. Did your computer take a long time to start or shut down or didn‘t shut down properly?

Protective Measures

Updating your operating system is a good malware preventative measure.

Beware of phishing emails and avoid email attachments from suspicious sources.

Refrain from clicking on suspicious links and be careful about which site you use for downloading information.

Install anti-virus, anti-spyware, and firewalls on your systems.

If you are a website owner, establish a multi-factor verification method and implement DDoS protection tools.

This will safeguard your website from botnet attacks.

Conclusion

The Botnets are one of the most sophisticated and dangerous forms of cybersecurity threats, making them a serious concern for businesses, individuals, and even governments. Although botnets and botnet attacks can be difficult to defend against, it’s not impossible. By following the tips shared above you can effectively protect your equipment from being turned into zombie devices and mitigate the risk of your system/network being affected by various forms of botnet attacks.

Group Member Details:

Name of Group Member1:Prajwal Ravindra Sable
Class-Div : A
Roll No:COMPBEA1102

Department of Computer Engineering,
D.Y. Patil College, of Engineering,
Akurdi, Pune-44.