**Mirai Botnet Attack**

It all starts with the dark side of the internet which introduced new kind of Crime called **Cybercrime** Among the malware (malicious software) botnet is a most **widespread** and **serious threat**. Several large institutions, government organizations, almost every social networking websites Facebook, Twitter, Instagram etc, e-commerce website Amazon, Flipkart etc, in short, every firm associated with internet became the victim of this malware. The **funniest part** about this kind of malicious software is that it is freely available in the market for the lease. It can be used in DDoS attacks (Smurf attack), Phishing, Extortion etc.

**How it Works:**

Either you write code to build software or use it from the available (Leaked) botnet like ZEUS Botnet(king of all botnet), Mirai botnet, BASHLITE etc. then find the vulnerable system where you can install this software through some means like social engineering (e.g Phishing) soon that system becomes a part of bot army. Those who control it called as the botmaster which communicates its bot army using command and control channel.

**Botnet Communication:**

At first, those who want to be botmaster finds the target system (here target system means finding the vulnerable system), then use popular social engineering techniques like phishing, click fraud etc to install small (Kbs) executable file into it. A small patch has been included in the code which made it not visible even with all the running background process. A naive user won’t even come to know that his/her system became the part of a bot army. After infection, bot looks for the channel through which it can communicate with its master. Mostly Channel (command and Control channel) uses the existing protocol to request for the command and receive updates from the master, so that if anyone tries to look at the traffic behavior then it will be quite difficult to figure it out.

Botmaster used to write scripts to run an executable file on different OS.

**For Windows:** Batch Program

**For Linux:** BASH Program

Following are the major things can be performed on bots:

1. **Web-Injection:**  
   Botmaster can inject snippet of code to any secured website which bot used to visit.
2. **Web-filters:**  
   Here on using a special symbol like:”!” for bypass specific domain,”@” for the screenshot are used.
3. **Web-fakes:**  
   Redirection of the webpage can be done here.
4. **DnsMAP:**  
   Assign any IP to any domain which master wants to route of the bot family.

**Types of Botnet: Based on Channel:**

1. **Internet Relay Chat (IRC) Botnet:**

Internet Relay Chat (IRC) acts as the C&C Channel.Bots receive commands from a centralized IRC server. A command is in the form of a normal chat message.  
**Limitation:** Entire botnet can be collapsed by simply shutting down the IRC Server.

1. **Peer-to-Peer (P2P) Botnet:**

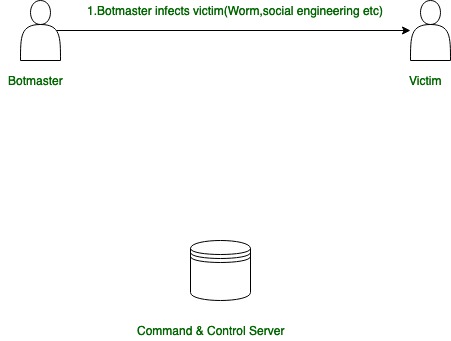
Formed using the P2P protocols and decentralized network of nodes.  
Very difficult to shut down due to its decentralized structure. Each P2P bot can act both as the client and the server. The bots frequently communicate with each other and send “keep alive” messages.  
**Limitation:**Has a higher latency for data transmission.

1. **Hyper Text Transfer Protocol (HTTP) Botnet:**

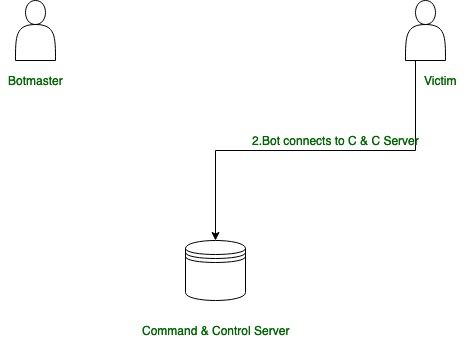
Centralized structure, using HTTP protocol to hide their activities.Bots use specific URL or IP address to connect to the C&C Server, at regular intervals. Unlike IRC bots, HTTP bots periodically visit C&C server to get updates or new commands.

**Botnet Lifecycle** can be understood using the following stages:

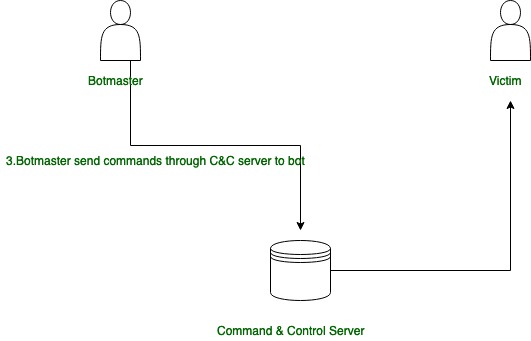
Stage-1:



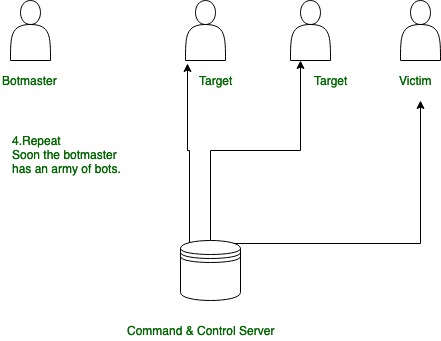
Stage-2:



Stage-3:



Stage-4:



This is a brief introduction of the botnet.

The Mirai botnet is a [malware](https://www.radware.com/security/ddos-knowledge-center/ddospedia/malware/) designed to [hijack Internet of Things (IoT) devices](https://www.radware.com/security/ddos-experts-insider/losing-sleep-c-suite/iot-internet-of-things-threats/) and turn them into remotely controlled “bots” capable of launching powerful volumetric distributed denial of service [(DDoS)](https://www.radware.com/cyberpedia/ddospedia/ddos-meaning-what-is-ddos-attack/) attacks.

The Mirai botnet was first seen in August 2016 and has since been used to launch large DDoS attacks on websites, networks and other digital infrastructure. Mirai was published as a source code by “Anna-senpai” to a public and easily accessible forum. The malicious code allows an attacker to gain control of vulnerable IoT devices such as webcams, DVRs, IP cameras, and routers. In early 2017, Krebs publicly named Josiah White and Paras Jha as the likely creators of Mirai botnet.

Security researchers estimate that there are millions of vulnerable IoT devices actively taking part in these coordinated attacks. Mirai can also infect all devices connected to the same network, making it possible to create a large botnet capable of launching devastating attacks.

## How botnets work?

Botnets are networks of computers or other internet-enabled devices that have been infected with malicious software. Each device in the botnet is referred to as a “bot” and can be used by an attacker to carry out various malicious activities such as sending spam emails or launching DDoS attacks. Botnets are created when attackers use automated tools like worms or phishing emails to spread malicious software across multiple devices. Once a device is infected with the malicious code, it becomes part of the botnet and can be used by the attacker for their own purposes.

## How does Mirai work?

The Mirai botnet works by scanning for vulnerable IoT devices that have open ports or default usernames and passwords. Once it finds these vulnerable devices, it uses exploits to gain access and infects them with its malicious code. The infected device then joins the Mirai botnet which allows the attacker to send commands from a central server which is known as a “command & control” server (C&C). This C&C server can then be used to launch large-scale DDoS attacks on websites, networks and other digital infrastructure by using all of the bots in the Mirai Botnet at once.

## Mirai botnet analysis and detection

The best way to protect against Mirai Botnet attacks is by ensuring that your IoT devices are secure at all times. This means regularly updating firmware on any connected device, changing default passwords, disabling remote access if not needed, keeping your network firewall up-to-date, regularly monitoring for suspicious activity and avoiding public Wi-Fi networks whenever possible. It's also important to note that many IoT manufacturers now offer security solutions specifically designed for their products, so it's worth researching what type of protection your connected devices offer before purchasing them. Finally, if you suspect your device has already been compromised by a Mirai attack, you should immediately disconnect it from your home network until you can confirm its safety.

Radware [DDoS protection](https://www.radware.com/solutions/ddos-protection/) and [application delivery solutions](https://www.radware.com/solutions/application-delivery-and-protection/) mitigate network and application DDoS attacks by using approaches that block attacks without impacting legitimate traffic. By using machine-learning and behavioral-based algorithms to understand what constitutes legitimate behavior profiles, Radware can automatically block malicious attacks. This increases protection accuracy while minimizing false positives.