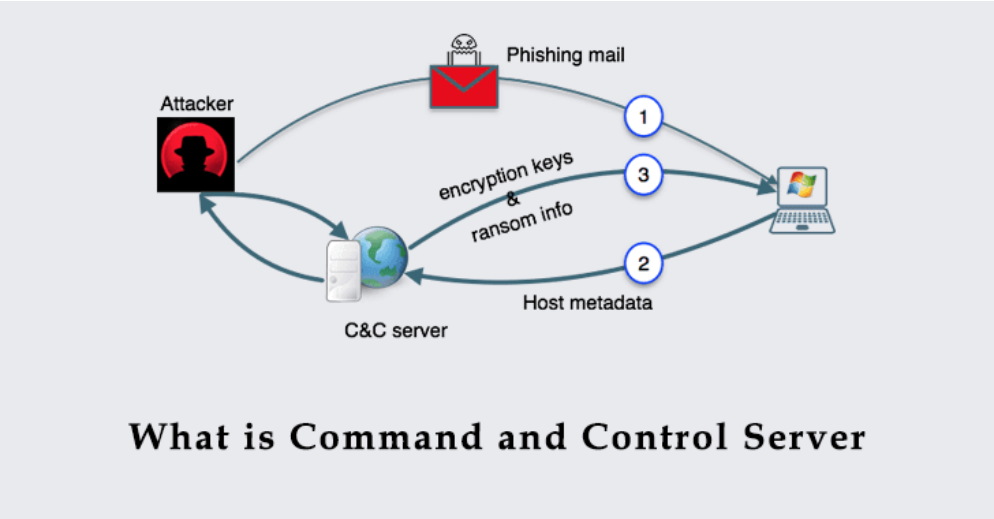
What is Command and Control (C2) Server – A Detailed Overview



Like a regular system holder, you might be wondering why is your system running slower than usual? Always you are getting random messages like pop-up, something got added as an extension in your browser and you have never used this. Your browser cannot load the page, internet connectivity is slow, and even the computer is always slow and sometimes it even gets crashes. We have no idea why all this is happening?

Well, the only answer is malware which is doing all such things. Your machine has infected in a very bad way and it can only become proper by turned into a zombie which C&C controls.

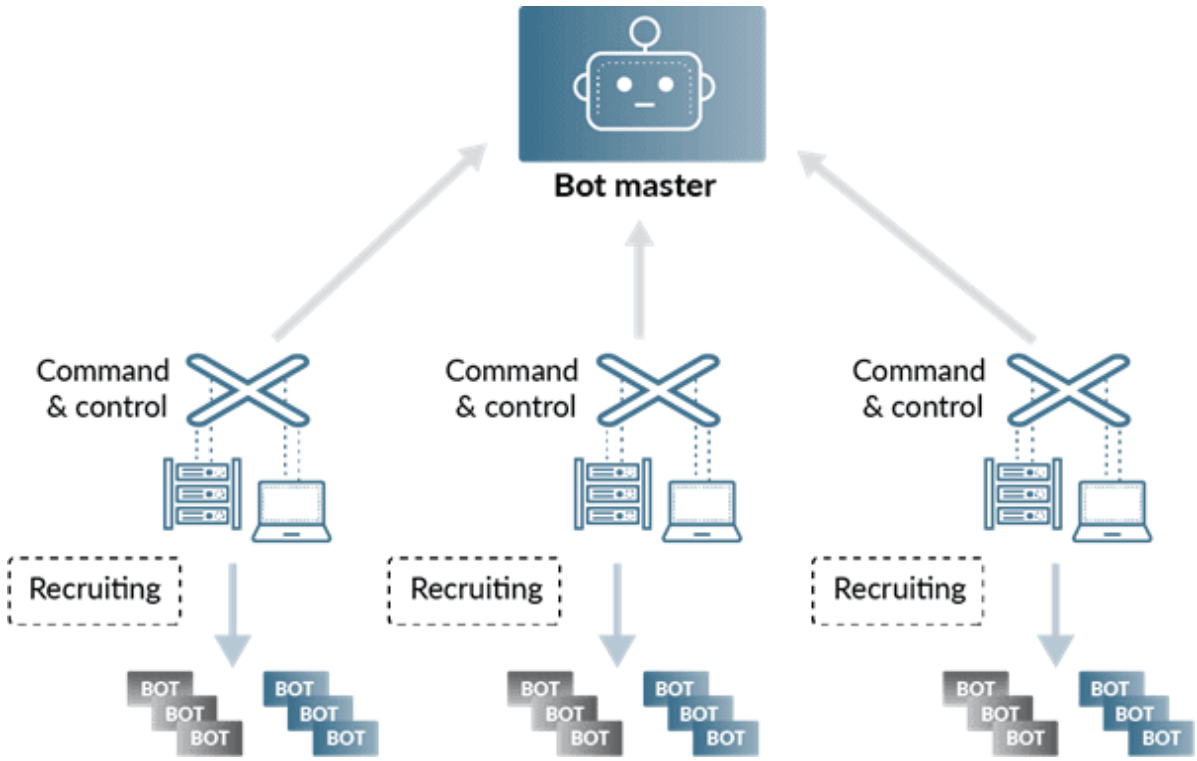
Now you might be wondering what is all about C&C? well, this full name is Command-and-control servers. The hackers mainly use this communication with a target network by using the system. These systems may be Smartphone's, Computers, loT's, etc.

We have mentioned the name called "zombie", it also calls as a botnet that is a combination of robot and network. This is a machine which infected with the Trojan horse, and it gets controlled by the C2C server. This botnet is the collection of computer sets that get used without the knowledge of their owners and send files to the other computer through the internet. The file includes spam and malware.

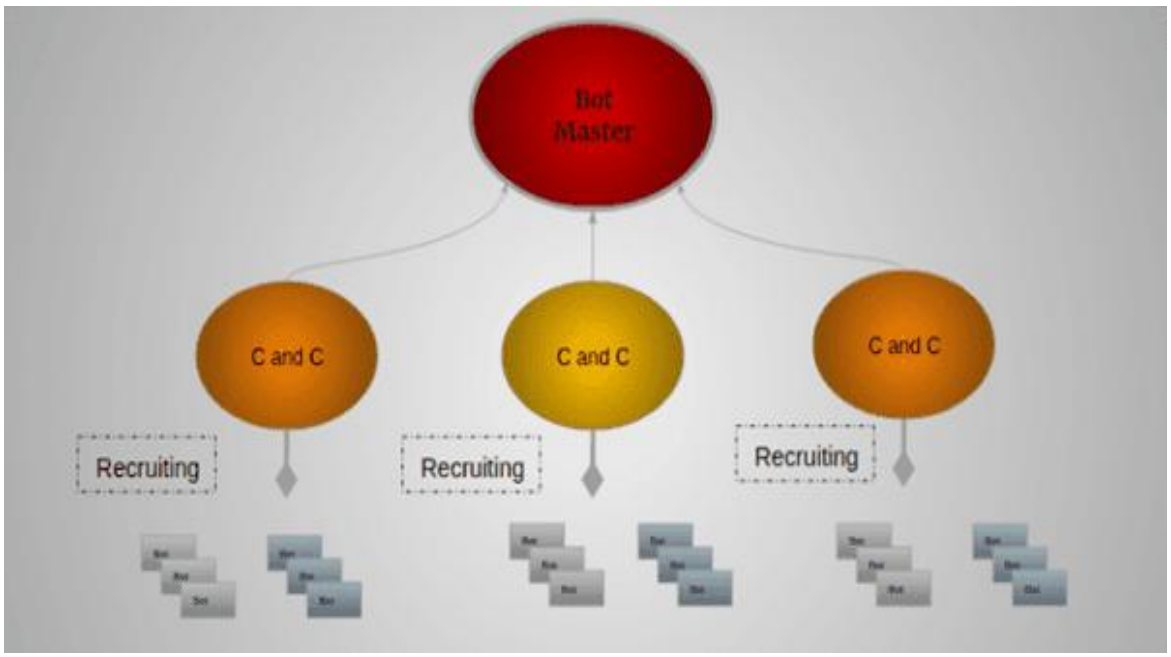
What all are hackers can do through Command and Control?

- **Data theft**: In this process, a company's data which is very sensitive, like financial documents, can be copied, and those also can be transferred to the attacker's server.
- **Shutdown**: One attacker can shut down many machines together and even make the network slow of the targeted company.
- **Reboot**: When the computer gets infected, it may suddenly shut down and reboot which will become a problem for any normal business operation.
- **Distributed denial of service (DDoS)**: It overwhelms the server and flooding them with too much internet traffic. As soon as the botnet gets established attacker will instruct every bot to send a request to the company's targeted IP address. This creates an appeal with the targeted server, and the result is traffic gets clog on the highway. It can legitimate the traffic by attacking IP addresses, and it denied access. This type of attack they do to make the website down.

This is the diagram where you can see how to stop the attacker from using DNS against you:



How does the botnet architecture look like? And how does it work?



While reading this article, you might be wondering why do we need bots and what are the uses? Let us take an example of spamming. Here sending spam is getting blacklisted because it is already set in some specific address. To overcome this issue, you need to send much spam, but for zombies to find the unique address from thousands, it is a cupcake for it. By sending more emails, attackers can make enormous money.

If you consider the fact of the C&C server and is intended to conduct DDoS then Zoobies's army keeps on sending the false request to the web server and the web server will not be able to handle the multiple request time they will do the leading attack on DDoS. After this criminals want money and they demand from the owner and after getting that they will stop such an attack.

It is effortless for a botnet to create a zombie army by installing software by stealing a password. This software mainly steal passwords from bank accounts, emails, credit card numbers, and criminals who sell passwords to make money. Zombie army only deals with all illegal activity.

Botnet Architecture Types

There are two types of architecture which include centralized and decentralized or peer-to-peer. These are discussing below:

Centralized

1. This is a very common type that is centralized with a C&C server, which provides the resources by individual client request. This network is completely based on the client-server model. Usually, this type of botnet gets to communicate with internet relay chat (IRC).
2. IRC is a computer program which user can easily install in their system.
3. Through the chat server, clients can send transfer messages to the other client.
4. IRC is not so simple, and it uses the low bandwidth communication method, which makes them a broader use to host botnets.
5. They look straightforward for the construction, and it gets used to getting moderate success so that it can coordinate with DDoS attacks and switch the channel so that they can avoid them.

Decentralized or Peer-to-Peer

Desperately using centralized servers has its advantage. There is a problem with using centralized servers if that is used by IRC. Every botnet client must know about the IRC server, port, and other channels. To halting the botnet attack, anti-malware organisations detect the server and make it shut down. To bring down a centralized server, you have to leave the zombies dead, and the botnet army will have no work with the attackers.

The Overview of Infection Methods

You might be wondering how C&C recruitment has been done and how to create an army for botnets? Let us inform you there are multiple ways to turn the computer into a botnet. Those are discussing below:

1. **Email**: Usually, attackers send you an email with a code in an attached file, or sometimes they even send a link with malicious code. After clicking on the link will

lure the attacker which drops the malware within the machine and it will turn into a Zombie.

2. **Exploiting Vulnerabilities**: Much vulnerability gets exploited, which offer from the backdoor of the machine. This mainly gets used by the attacker who drops the malware into the machine. Vulnerabilities include browser plug-in, add-ons and other software which are already installed in the machine.

What will you do when the computer will turns into Zombie?

- You can use some Sysinternals tool that can find the process to consume more memory. If it finds any suspicious process, then you can kill that process.
- You always need to scan the machine with a different antivirus engine to recheck whether it is getting detected or not malware. This cannot be the complete solution, but it has to identify the malware with the latest signature.
- Maximum antivirus gets fails to detect and remove the malware if it's the most advanced one. It can link by itself with the operating system and process.
- If the rootkit is hard and cannot remove the infection then the most effective thing is to clean the machine and restore the backup. But before you start, make sure that you keep the backup of everything so that you do not lose any data.
- After you clean the malware, you can regularly apply the security update to avoid future infection.