

## RECENT POSTS

- What are the tools commonly used by a blogger?  
(<https://www.stepskochi.com/blog/what-are-the-tools-commonly-used-by-a-blogger/>)
- Why Python is so popular with developers?  
(<https://www.stepskochi.com/blog/why-python-is-so-popular-with-developers/>)
- REPOSITORIES AND APPLICATION STREAMS IN RHEL 8  
(<https://www.stepskochi.com/blog/repositories-and-application-streams-in-rhel-8/>)
- TAXONOMY OF DDOS ATTACK  
(<https://www.stepskochi.com/blog/taxonomy-of-ddos-attack/>)
- Important 5 tips for successful Android app development  
(<https://www.stepskochi.com/blog/important-5-tips-for-successful-android-app-development/>)

## ARCHIVES

- September 2021  
(<https://www.stepskochi.com/blog/2021/09/>)
- August 2021  
(<https://www.stepskochi.com/blog/2021/08/>)
- July 2021  
(<https://www.stepskochi.com/blog/2021/07/>)
- June 2021  
(<https://www.stepskochi.com/blog/2021/06/>)
- May 2021  
(<https://www.stepskochi.com/blog/2021/05/>)
- April 2021  
(<https://www.stepskochi.com/blog/2021/04/>)
- March 2021  
(<https://www.stepskochi.com/blog/2021/03/>)
- February 2021  
(<https://www.stepskochi.com/blog/2021/02/>)
- January 2021  
(<https://www.stepskochi.com/blog/2021/01/>)
- December 2020  
(<https://www.stepskochi.com/blog/2020/12/>)
- November 2020  
(<https://www.stepskochi.com/blog/2020/11/>)
- October 2020  
(<https://www.stepskochi.com/blog/2020/10/>)
- September 2020  
(<https://www.stepskochi.com/blog/2020/09/>)
- August 2020  
(<https://www.stepskochi.com/blog/2020/08/>)
- March 2020  
(<https://www.stepskochi.com/blog/2020/03/>)
- February 2020  
(<https://www.stepskochi.com/blog/2020/02/>)

## TAXONOMY OF DDOS ATTACK

Attacks on denial-of-service are reflected in a clear attempt to prevent the official use of the service. A distributed denial-of-service attack deploys multiple attacking entities to attain this goal. Distributed attacks (DDoS) pose a serious threat to the Internet, and a number of measures have been proposed to prevent this problem. Attackers constantly change their tools to circumvent these security systems, and investigators change their tactics to deal with new attacks.

In order to establish a classification for DDoS attacks, we look at the methods used to prepare and execute attacks (recruit, exploiting and infecting categories), the characteristics of the actual attack (use phase) and the effect it has on the victim.

## Manual

The attacker manually scans remote machines for vulnerabilities, breaks into them, installs attack code, and then commands the onset of the attack. Only the early DDoS attacks belonged to the manual category. All the recruitment action was soon automated.

The attacker manually scans remote machines to detect vulnerabilities, enters them, enters the attack code, and commands the start of the attack. Only the original DDoS attacks were in the manual category. All hiring actions are instantly automatic.

## Semi-Automatic

In semi-automatic attack, the DDoS network contains administrative (master) and agent (slave, daemon, zombie) equipment. The stages of search, exploitation and infection are automatic. In the use phase, the attacker specifies the type of attack, the start, the length of time and the victim with a handle on the agents, who send packets to the victim.

Based on the communication mechanism adopted in between agent and handler machines, we divide semi-automatic attacks into two. One is direct communication and another one is, indirect communication.

## Semi-Automatic attack with Direct communication

During an attack on direct communication, the agent and handler machines have to know each other's identity for the proper communication. This is usually achieved by encrypting the IP address of the attackers on the attack code, which is later added to the agent's machine. Each of the agent then report their willingness to the handlers, who store its IP address for later communication.

The obvious backlash of this approach to the attacker is that the detection of a single fixed machine can expose the entire DDoS network. Also, as agents and handlers both of them are listening to the network communications, they can be identified by network scanners or network intrusion detection system.

## Semi-automatic attack with Indirect communication

In an indirect communication, attacker use some authorized communication service to synchronize agent actions. Recent attacks have used IRC (Internet chat program) channels. The use of IRC services replaces the function of a handler, because the IRC channel provides enough anonymity to the attacker. The agents do not actively listen to network communications (meaning they cannot be detected by scanners), but instead use the official IRC service and their control packets cannot be easily separated from the official chat channel.

One-agent acquisition can lead to the identification of one or more IRC servers and channel names used by the DDoS network. From there, identifying the DDoS network depends on the ability to track the agents currently connected to the IRC server (which can be the basis for all distorted devices). To further avoid detection, attackers often use channel rotation, using any given IRC channel for a short period of time.

As the IRC service is maintained in a distributed way, and an IRC server hosting a specific IRC channel may be available anywhere in the world, this precludes investigations. Although the IRC service is the only known example of indirect communication to date, nothing can prevent it attackers in destroying other legal services for the same purposes.

## Automatic

DDoS automatic attacks make the application phase more than recruiting, exploiting and infecting categories, and thus avoids the need for any communication between attackers and agent equipment. The start time of the attack, the type of attack, the duration of the attack and the victim are set for the attack code. The modes of delivery of this phase of the attack provide little exposure to the attacker, because he is only involved in issuing a single command at the beginning of the recruitment process.

The encrypted attack specification suggests a single-purpose use of the DDoS network, or a static system state. However, distribution methods often leave the back door on an open disabled machine, allowing for easy future access and modification of the attack code. In addition, when providers communicate with IRC channels, these channels can be used to modify existing code.

STEPS, the best CEH training in cochin (<https://www.stepskochi.com/cyber-security-training-kochi>), will help you learn the concepts of Ethical Hacking and Cyber Security. You will learn about the different types of cyber attacks and behavioral hacking tools used to prevent such attacks. There are many demos in several tools for this moral hacking. You will also learn how to become a Behavior Hacker.

You will learn what Cyber Security, Cyber Security Engineer, Cyber Security Skills, Introduction to Ethical Hacking, Phishing & DDos, SQL Inject Demo, Security Risk and Management, Software Development and Security, Ethical Communication Questions, the top ten reasons to learn cyber security. Online Ethical Hacking training (<https://www.stepskochi.com/>) is ideal for both beginners and professionals who want to understand the concepts of Cyber Security. This course is ideal for anyone who wants to learn Cyber Security and work on it.



Author: STEPS (<http://www.stepskochi.com>)

Written by: STEPS

(<https://www.stepskochi.com/blog/2>)  
January 2020  
(<https://www.stepskochi.com/blog/2>)  
December 2019  
(<https://www.stepskochi.com/blog/2>)  
November 2019  
(<https://www.stepskochi.com/blog/2>)  
October 2019  
(<https://www.stepskochi.com/blog/2>)  
September 2019  
(<https://www.stepskochi.com/blog/2>)  
August 2019  
(<https://www.stepskochi.com/blog/2>)  
July 2019  
(<https://www.stepskochi.com/blog/2>)  
June 2019  
(<https://www.stepskochi.com/blog/2>)  
May 2019  
(<https://www.stepskochi.com/blog/2>)  
April 2019  
(<https://www.stepskochi.com/blog/2>)  
March 2019  
(<https://www.stepskochi.com/blog/2>)  
February 2019  
(<https://www.stepskochi.com/blog/2>)  
January 2019  
(<https://www.stepskochi.com/blog/2>)  
July 2018  
(<https://www.stepskochi.com/blog/2>)  
March 2018  
(<https://www.stepskochi.com/blog/2>)  
January 2018  
(<https://www.stepskochi.com/blog/2>)  
November 2017  
(<https://www.stepskochi.com/blog/2>)  
August 2017  
(<https://www.stepskochi.com/blog/2>)  
July 2017  
(<https://www.stepskochi.com/blog/2>)  
June 2017  
(<https://www.stepskochi.com/blog/2>)

#ETHICAL HACKING COURSE IN COCHIN

(<https://www.stepskochi.com/blog/tag/ethical-hacking-course-in-cochin/>)

#ONLINE CYBER SECURITY TRAINING IN KOCHI

(<https://www.stepskochi.com/blog/tag/online-cyber-security-training-in-kochi/>)

Tweet ([http://twitter.com/share?text=TAXONOMY OF](http://twitter.com/share?text=TAXONOMY%20OF)

DDOS ATTACK&url=<https://www.stepskochi.com/blog/taxonomy-of-ddos-attack/>)

Share ([http://www.facebook.com/sharer.php?u=https://www.stepskochi.com/blog/taxonomy-of-ddos-attack/&t=TAXONOMY OF DDOS ATTACK](http://www.facebook.com/sharer.php?u=https://www.stepskochi.com/blog/taxonomy-of-ddos-attack/&t=TAXONOMY%20OF%20DDOS%20ATTACK))

Leave a Reply

Your email address will not be published. Required fields are marked \*

**Name \***

**Email \***

**Website**

[Post Comment](#)

## Address

### STEPS

Floor I, Spectrum IT Park  
Mahakavi G Road  
[Near Iyyattil Jn., Chittoor Rd.]  
Ernakulam South  
Kochi - 682 011, Kerala

## Training Courses

[SEO Training](#) (<https://www.stepskochi.com/seo-training-kochi>)  
[Java Training](#) (<https://www.stepskochi.com/java-training-kochi>)  
[PHP Training](#) (<https://www.stepskochi.com/php-training-kochi>)  
[Digital Marketing Training](#) (<https://www.stepskochi.com/digital-marketing-training-kochi>)  
[Web Designing Training](#) (<https://www.stepskochi.com/web-designing-training-kochi>)  
[.Net Training](#) (<https://www.stepskochi.com/asp-dot-net-training-kochi>)  
[Android Training](#) (<https://www.stepskochi.com/android-training-kochi>)

## Main Links

[Blog](#) (<https://www.stepskochi.com/blog>)  
[About Us](#) (<https://www.stepskochi.com/about-it-training-courses>)  
[Free Workshop](#) (<https://www.stepskochi.com/IPv6-Workshop>)  
[Industry Association](#) (<https://www.stepskochi.com/industry-association>)  
[News Room](#) (<https://www.stepskochi.com/newsroom>)  
[Industry Internship Registration](#) (<https://www.stepskochi.com/industrial-internship>)  
[Industrial Visit Registration](#) (<https://www.stepskochi.com/industrial-visits>)

## Contact Us

(<https://twitter.com/stepskochi>)      (<https://www.facebook.com/stepskochi>)      (<https://www.linkedin.com/in/stepskochi>)

TEL:- +91-484-4082111

Mobile: +91-9895682000

Fax : +91-484-4082408

**Email:** [info@stepskochi.com](mailto:info@stepskochi.com)