DDoS IP/ICMP Fragmentation attack

Internet Protocol (IP)/Internet Control Message Protocol (ICMP) Fragmentation DDoS attack is a common form of denial of service attack. In such an attack, datagram fragmentation mechanisms are used to overwhelm the network.

What is DDoS IP/ICMP Fragmentation attack?

Internet Protocol (IP)/Internet Control Message Protocol (ICMP) Fragmentation DDoS attack is a common form of denial of service attack. In such an attack, datagram fragmentation mechanisms are used to overwhelm the network.

IP fragmentation occurs when IP datagrams are broken into small packets, which are then transmitted across the network and finally reassembled into the original datagram, as part of the normal communication process. This process is necessary to meet the size limits that each network can handle. Such a limit is described as a maximum transmission unit (MTU).

When a packet is too large, it must be divided into smaller fragments to be transmitted successfully. This results in several packets being sent, one containing all information about the packet, including source/destination ports, length, etc. This is the initial fragment.

The remaining fragments only include an IP header (IP header) plus a data payload. These fragments do not contain information about protocols, capacity or ports.

Attackers can use IP fragmentation to target communication systems, as well as security components. ICMP-based fragmentation attacks often send fake fragments that cannot be defragmented. This in turn causes fragments to be placed in temporary memory, taking up memory and in some cases, exhausting all available memory resources.

Signs of an IP/ICMP Fragmentation DDoS attack

IP/ICMP Fragmentation bombards the destination with fragmented packets, causing it to use memory to reassemble all the fragments and overwhelm the targeted network.

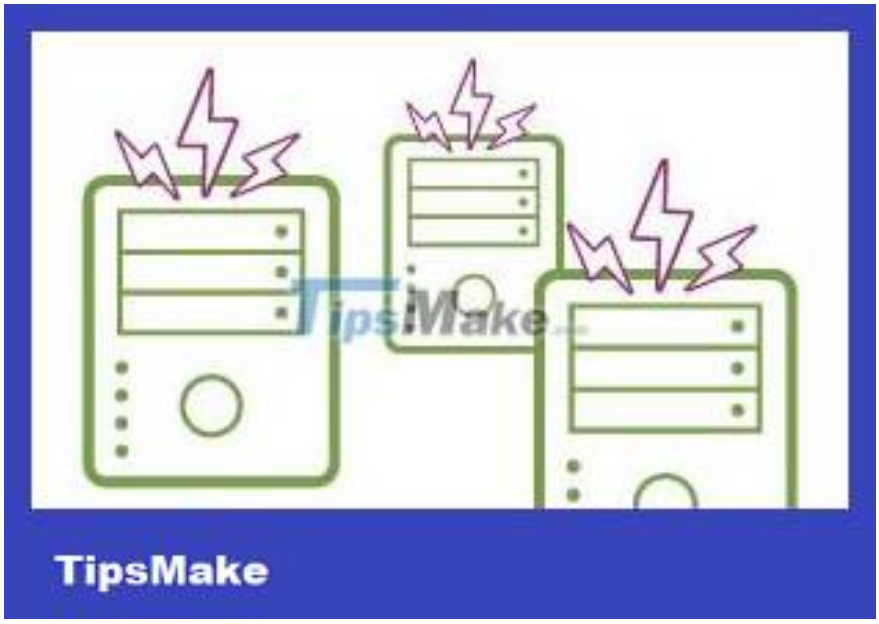
Such attacks manifest in a number of different ways:

- **UDP flooding** - In this type of DDoS attack, attackers use a botnet to send large volumes of fragments from multiple sources. In many cases, the receiver will not see the starting fragment (these fragments are often lost in the chaos of incoming packets). It just sees a lot of packets without protocol header fragments. Those non-initial fragments are tricky because they may belong to a legitimate session, but in most cases will be junk traffic. The receiver has no clue as to which is legitimate and which is not, because the original fragment has been lost.

- **UDP & ICMP Fragmentation DDoS Attack** - In this type of DDoS attack, fake UDP or ICMP packets are transmitted. These packets are designed to look like they are larger than the network's MTU, but only parts of the packet are actually sent. Because the packets are fake and cannot be reassembled, the server's resources are quickly consumed, which eventually makes the server unavailable to legitimate traffic.

- **DDoS TCP Fragmentation Attack** - This type of DDoS attack, also known as a Teardrop attack, targets TCP/IP reassembly mechanisms. In this case, fragmented packets will not be reassembled. As a result, data packets overlap and the targeted server becomes completely overloaded and eventually stops working.

Why are IP/ICMP Fragmentation attacks dangerous?



IP/ICMP Fragmentation attacks, like many other DDoS attacks, will overwhelm the target server's resources by the large volume of traffic. However, this DDoS attack will also force the target server to use resources trying to reassemble packets, which often leads to network devices and servers crashing. Finally, because non-fragment fragments do not initially contain any information about the service they belong to, it is difficult to decide which packets are safe and which are not.

How to mitigate and prevent IP/ICMP Fragmentation attacks?

The approach to preventing DDoS IP/ICMP Fragmentation attacks depends on the type and extent of the attack. The most common mitigation methods involve ensuring that malicious packets are prevented from reaching targeted hosts. This involves examining incoming packets to determine whether they violate fragmentation rules.

One potential denial-of-service attack mitigation method is to block all fragments other than the starting fragment, but this would lead to problems with legitimate traffic relying on those fragments. A better solution is to use rate limiting, which will drop the majority of packets (both good and bad, as rate limiting does not differentiate between one) and the attacked target server will Unaffected.

This approach risks creating problems with legitimate services that rely on fragments, but the trade-off may be worth it. There is no method that brings 100% success. If you are using services that rely on fragments, such as DNS, you can whitelist the specific servers you rely on and use rate limiting for the rest.