Ping of Death (POD)

imperva.com/learn/ddos/ping-of-death

What is a ping of death attack

Ping of Death (a.k.a. PoD) is a type of Denial of Service (DoS) attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command.

While PoD attacks exploit legacy weaknesses which may have been patched in target systems. However, in an unpatched systems, the attack is still relevant and dangerous. Recently, a new type of PoD attack has become popular. This attack, commonly known as a Ping flood, the targeted system is hit with ICMP packets sent rapidly via ping without waiting for replies.

Attack description

The size of a correctly-formed IPv4 packet including the IP header is 65,535 bytes, including a total payload size of 84 bytes. Many historical computer systems simply could not handle larger packets, and would crash if they received one. This bug was easily exploited in early TCP/IP implementations in a wide range of operating systems including Windows, Mac, Unix, Linux, as well as network devices like printers and routers.

Since sending a ping packet larger than 65,535 bytes violates the Internet Protocol, attackers would generally send malformed packets in fragments. When the target system attempts to reassemble the fragments and ends up with an oversized packet, memory overflow could occur and lead to various system problems including crash.

Ping of Death attacks were particularly effective because the attacker’s identity could be easily spoofed. Moreover, a Ping of Death attacker would need no detailed knowledge of the machine he/she was attacking, except for its IP address.

It is worthy of note that this vulnerability, though best recognized for its exploitation by PoD attacks, can actually be exploited by anything that sends an IP datagram – ICMP echo, TCP, UDP and IPX.

See how Imperva DDoS Protection can help you with Ping of Death attacks.

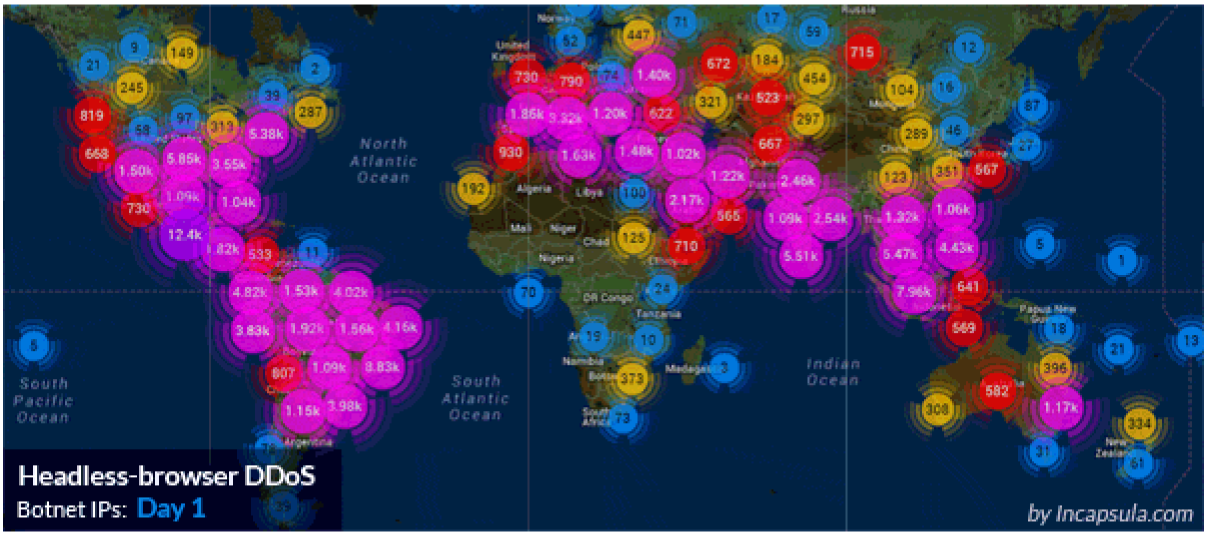
Request demo Learn more

Methods of mitigation

To avoid Ping of Deatch attacks, and its variants, many sites block ICMP ping messages altogether at their firewalls. However, this approach is not viable in the long term.

Firstly, invalid packet attacks can be directed at any listening port—like FTP ports—and you may not want to block all of these, for operational reasons.

Moreover, by blocking ping messages, you prevent legitimate ping use – and there are still utilities that rely on ping for checking that connections are live, for example.



Imperva mitigates a massive HTTP flood: 690,000,000 DDoS requests from 180,000 botnets IPs.

The smarter approach would be to selectively block fragmented pings, allowing actual ping traffic to pass through unhindered.