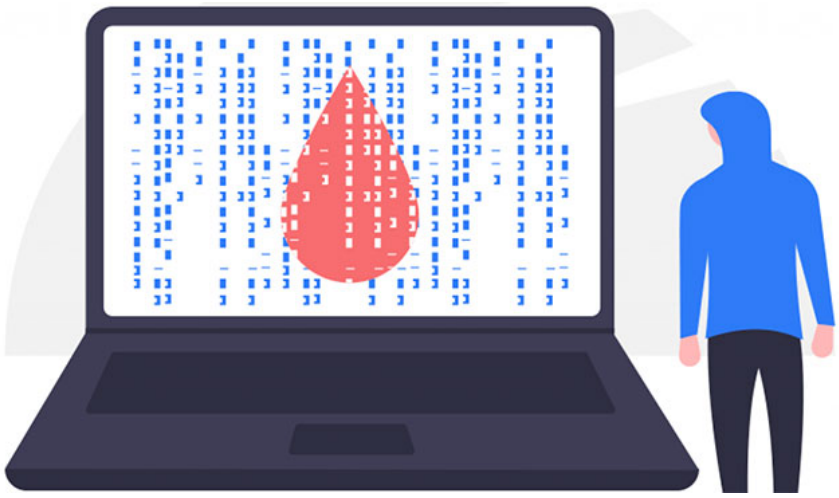
What is Teardrop attack?

In a Teardrop Denial of Service (DoS) attack, a client sends an incorrect packet of information to a machine and exploits an error that occurs when the packet is reassembled, resulting in a drop in server performance.

In a Teardrop Denial of Service (DoS) attack, a client sends an incorrect packet of information to a machine and exploits an error that occurs when the packet is reassembled, resulting in a drop in server performance.

What is Teardrop attack?

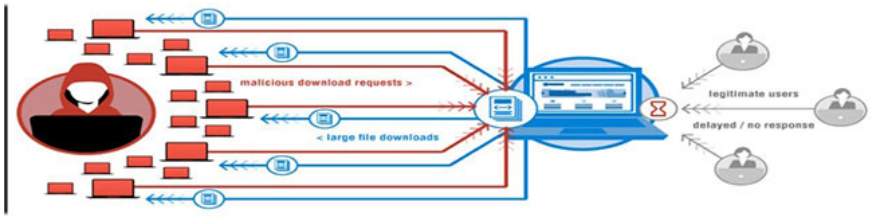
Teardrop attack is a type of denial of service (DoS) attack (an attack that tries to make computer resources unavailable by flooding the network or server with requests and data). Attackers send fragmented packets to the target server and in some cases TCP / IP vulnerability the server cannot regroup the packet, causing overload.



Why do Teardrop attacks have such a great effect?

Many organizations still rely on old, outdated, or unpatched operating systems to run legacy applications they need. Such organizations are susceptible to a Teardrop attack that threatens to bring down critical applications.

How does a Teardrop attack work?



TCP / IP implementations vary slightly between platforms. Some operating systems - especially older versions of Windows and Linux - have TCP / IP fragmentation errors. Teardrop attacks are designed to exploit this vulnerability.

In a Teardrop attack, the client sends a purposefully fragmented packet of information to a target device. Because the packages are overlapping, an error occurs when the device tries to reassemble the package. The attack takes advantage of the error to cause serious problems in the operating system or applications that handle packets.