Teardrop Attack - What is it?

wallarm.com/what/teardrop-attack-what-is-it

Wallarm Inc.

The definition and Why is it known by its current name

To begin with, the simplest teardrop attack definition is an attack wherein a minute fraction of corrupted code Is introduced in the aimed software/application/system. In a customary DDoS attack, a huge amount of request/traffic is forwarded to the targeted system to make it inaccessible for authorized users. The aim of the teardrop attack is the same. But, the insertion of malicious code or requests is slow and continuous.

Mostly, it's used to destroy old or outdated computer systems. These systems have slow processing and cannot congregate the corrupted packets as their IP/TCP fragments are buggy. Over time, the intended system becomes overwhelmed with these bugs and crashes.

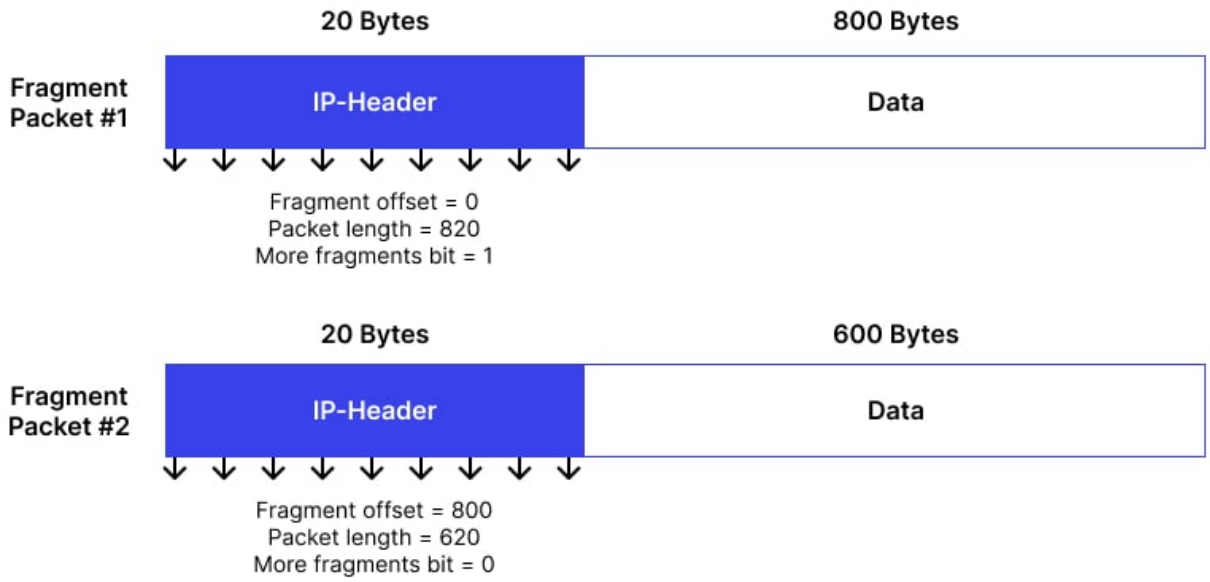
As the attack involves IP/TCP fragments, it's also a part of the IP Fragmentation Attack.

Now, let's understand how it got its name, i.e., 'teardrop attack'. The buggy code used in the attack is very small and fragmented. It's a small section of a huge part and is inserted slowly. A teardrop is almost the same as this. It's a small part of the endless tears that humans can produce in a lifetime. A teardrop, when it comes alone, won't make any difference. But, when it comes in huge quantities it means an emotional breakdown.

Teardrop Attack in action

Every system is designed to process only a small set of information at a time. Because of this, the network breaks the traffic into small fragments, and each fragment has a number assigned to it in the fragment offset field. Once all the fragments are received, they are arranged to generate the message that was bound to be delivered as per the fragment offset field value.

In an IP teardrop attack, a hacker introduces a bug in the fragment offset field and makes fragment sequencing impossible. Without sequencing/rearrangement, corrupted fragment offset fields start accumulating in the system and crash with time.



The importance of Teardrop attacks

Legacy systems, receiving no support from the vendor, will completely crash down on facing a teardrop attack. The most common teardrop attack example is the attack that happened on The Office of Personnel Management (OPM) in 2014. As a result of the attack, millions of US government employee records went under the control of a Chinese hacker. As the systems were too old, data could be encrypted.

The main victims of this attack are

Teardrop attacks are capable of harming only the legacy systems and such systems are spotted at places like hospitals, government offices/agencies, banks, and financial institutes. In a survey, it was revealed that around 56% of hospitals and health care professionals are using outdated OS-based computers. Hence, they are prime victims of this attack.

Mitigating and preventing a Teardrop attack

As per recent research, around 30% of organizations are still using computers/laptops running on old OS like Windows 3.1x, Windows NT, and so on. All these systems are prone to teardrop attacks. Hence, effective and viable teardrop mitigation actions should be in place.

One of the most viable teardrop attack preventions is disabling 139 and 445 ports for blocking server messages in systems that aren’t receiving the patches from the vendors.

Using a firewall in the network layer is imperative as it filters the data and reduces the odds of a teardrop DDoS attack.

One can avoid teardrop exploits with a caching server as it ensures the continuous availability of the website even when a DDoS attack has happened. With proxy servers, it's easy to watch out for the incoming traffic and spot the data fragments in the early stages.