Do you know what is the preferred 'prey' of DDoS attack?

Distributed denial of service (DDoS) is a common method used by hackers to try to bring down a website.

Distributed denial of service (DDoS) is a common method used by hackers to try to bring down a website. Hackers will try to overwhelm their target, websites and online services. Users have difficulty, or even cannot access these websites and services.

DDoS attacks can target any organization, no matter how big or small.

Sadly, there is currently no complete solution to this nasty attack. We can only limit the damage or reduce the intensity of the attack only.

However, DDoS is not a form of `` indiscriminate " attack, organizations and businesses in certain business areas are more likely to suffer from DDoS attacks than companies operating in a Other field numbers. According to a report from Imperva, most of the DDoS attacks in 2019 are aimed at entertainment companies, especially gaming and gambling. So why is this field often targeted by hackers?

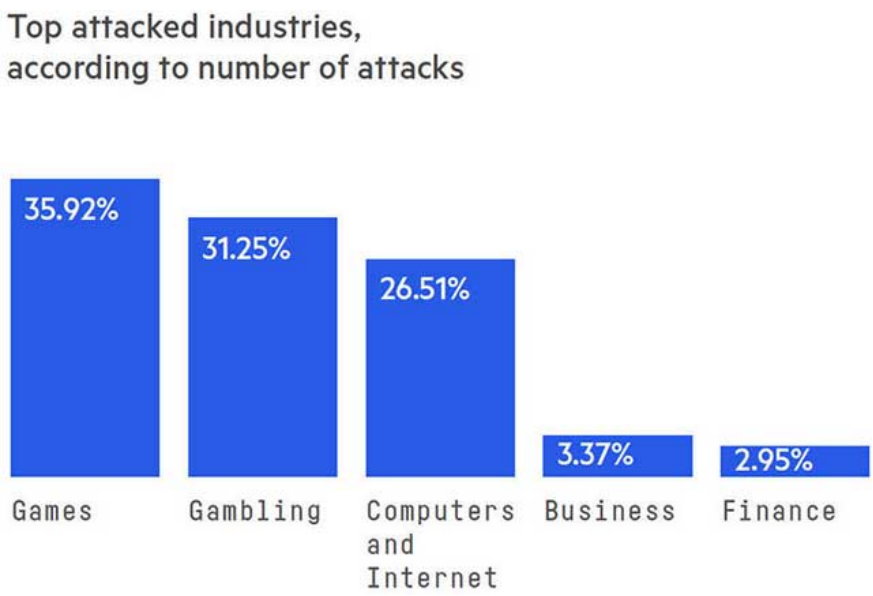
In 2019, most of the DDoS attacks observed by Imperva were smaller than in previous years. About 25% lasts less than 10 minutes and 15% less than 30 minutes, only about 5% of the recorded DDoS cases last more than 24 hours. This can be explained by the fact that the trend of DDoS attacks has changed a lot in recent years. The 'quick hit, shorten' approach, causing great damage during mounting so that the target could not respond in time is more effective than the traditional 'long beam of rain'.

The scale of DDoS attacks is measured by two different factors:

1. **Millions of packets per second (Mpps):** A measure of the forwarding rate or the rate at which packets are delivered.
2. **Gigabits per second:** A measure of total or total load on a network.

A DDoS attack peaked at 580Mbps and 680Gbps. Cases of 200Mpps and 300 + Gbps are sometimes recorded, but the most common are below 50Mpps and 50Gbps. This is usually the result of DDoS-for-hire services.

Although the duration of DDoS attacks in 2019 is shorter, the target is "bombarded" more. 1/3 of the targets have been DDoS up to 5 times, especially 25% have been attacked 10 times or more. Highly configurable targets can be attacked multiple times through various means.



UDP (User Data Protocol) was the most popular attack vector last year, used in 36% of attacks. UDP is popular because it is vulnerable to spoofing and can be used in most DNS amplification attacks, exploiting vulnerabilities in domain name system (DNS) servers. In addition to UDP, other common attack vectors include SYN Flood, DNS Response, TCP, and NTP.

In general, every large organization risks being the target of persistent DDoS attacks, often carried out by competitors or extortion.

Games and gambling are highly competitive areas involving risk factors and in which players do not necessarily follow the rules. Nearly 36% of DDoS attacks were launched against gaming companies, while 31% attacked gambling sites.

Computing and internet companies ranked third with 36% of DDoS attacks targeted in 2019. Internet service providers, web servers and domain name providers are often victims of DDoS because these are high-value goals.

In addition, the adult entertainment industry is also a favorite DDoS attack in 2019. The adult websites that Imperva tracks are hacked on average 84 times from May to December, for a total of about 10.5 attacks / 1 website / 1 month.