Website content

What is a DDoS Attack?

First, we must define the meaning of a DDoS attack. DDoS attacks are a main concern in internet security, and many people misunderstand what exactly they are.

A Distributed Denial of Service (DDoS) attack is a malicious attempt to upset typical internet traffic of a targeted server by overwhelming it with traffic from multiple sources. DDoS attacks target a plethora of important resources, from banks to news websites, and present a major challenge to making sure Internet users can publish and access important information. A DDoS attack is similar to a traffic jam on a highway, preventing typical traffic flow.

How does a DDoS attack work?

A DDoS attack requires the attacker to gain control of a network of online machines. Computers are infected with malware, turning them into a bot. Then, the attacker has control over the group of bots, now called a botnet.

Once a botnet is established, the attacker will send instructions to each bot from a remote control. Once the IP address is targeted, each bot will respond by sending requests to the target, causing the server to overflow, which will result in a DDoS attack.

How can you combat DDoS attacks?

If you are facing an isolated low- to mid-size Distributed Denial of Service (DDoS) attack, you can explore these logs and find the information you need to protect yourself from these attacks. However, with larger attacks, manual lookups are time consuming and ineffective. That’s why there need to be other plans in place to fight cyber-attacks.

However, if you are not experiencing a DDoS attack, and you just want to learn about top digital attack information from cybersecurity incidents around the world, where would you look? You can try internet service provider (ISP)’s stats or check out anti-DDOS providers, or you can see what’s happening right now by looking at digital attack maps.

To see how cybersecurity works globally, you can observe cyber-attacks and how malicious packets interact between countries. We are going to share with you the top cyber-attack maps that you can watch in order to visualize digital threat incidents.

Global Cyber Attacks Today

Today, cyber-attacks can affect anyone, but some of them are designed to leave global damage. A cyber-attack is any type of internet attack designed by individuals or entire organizations that targets computer information systems, networks, or infrastructures. When they appear, they come from a seemingly anonymous source that will attempt to destroy its victim through hacking into its system.

There have been many, many worldwide cyber-attacks, and some are happening right now. The [latest statistics](https://www.accenture.com/us-en/insights/security/cost-cybercrime-study) say that security breaches have increased by 11% since 2018 and 67% since 2014. In fact, hackers attack [every 39 seconds](https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds), so on average, 2,244 times a day.

**What is a Cyber Attack Map?**

Cyber-attack maps are valuable tools that give information on how to stay ahead of attacks. A cyber-attack map shows how the Internet functions in a graphical way and can be useful to see the big picture. Even though we’re talking about enormous amounts of damage that cybercriminals cause, the maps themselves can be fascinating to watch.

Every 39 seconds, a cyber-attack occurs. While some of these are manually-targeted cyber-attacks, most of them are botnets steadfast on shutting down infrastructures and destroying computers and systems of major organizations.

A DDoS attack map is a type of cyber-attack map that details just DDoS attacks.

Most current digital attack maps share these specifics:

* They are incorrectly advertised as “live maps”—most do not show live attack data, but records of past attacks.
* They only show Distributed Denial of Service (DDoS) attack, not other types of cybercrime.
* They only display anonymous traffic data.

Because most cyber-attack maps are not in real-time, it can be difficult to understand them. However, there are still positives to these maps.

**Is it Useful to Understand Cyber Attack Maps?**

The jury is still out on whether it is actually beneficial to understand cyber-attack maps and how they function.

Some Information Security industry experts claim that these maps aren’t useful at all, that they’re simply used as a sales tool by cybersecurity solution providers.

However, other experts believe that while these threat maps have no practical usage for mitigating attacks, threat maps can be used to study past attack styles, to recognize raw data behind DDoS attacks, or to even report outages on certain dates and times to their customer base.

Another essential point to keep in mind about the source of the attacks: even though these maps pinpoint particular countries launching attacks against others, that doesn’t mean the actual source of the attack is the same as the attacker location.

In actuality, the source of an attack is often forged, which means that it appears as though it was initiated from a certain country, but it is not from that country at all. When the map shows the correct location, it’s often not the real attacker behind the cyber-attack, but rather an infected computer working for a botnet.

Another noteworthy fact is that the largest attacks usually originate from high bandwidth nations, who are perfectly suited to launching huge attacks from thousands of infected devices led from more isolated locations.

One more important point to note is that while these maps provide valuable cyber-attack information, it is impossible to fully map all digital attacks online because they are constantly changing. These maps update regularly (usually hourly, but some are in real time), but they cannot show everything.