The Dyn DDoS Attack that Broke the Internet: Here's What Happened

Even internet giants can't consider themselves infallible in 2016, especially after the most recent DDOS attack that took down websites like Twitter, Reddit, and Netflix.

Understanding DDOS attacks is helpful to knowing why your favorite websites are down, but it also helpful when putting plans in place to protect your own website.

SiteUptime provides network performance monitoring services that make sure that your website is accessible throughout time and from multiple points of the internet.

In addition to our affordable service plans, SiteUpTime helps protect your website from hackers looking to steal information or bring your website down with a DDOS attack.

These attacks may seem random and unpredictable at times, and there seems to be little anyone can do to prevent the internet from "breaking" during the time when these hackers wreck their havoc.

What a DDOS attack is

"DDOS" stands for Distributed Denial of Service. These attacks occur when a number of hackers and their bots access a site at once, overwhelming their servers and causing the service to ultimately fail.

During this downtime, there is little web hosts, web developers, and individual users can do to bring the website back to working order. This is evident in the latest DDOS attack on Dyn, a widely used internet performance manager.

These attacks, sometimes coming from the "darknet" can cost just $150 if a week-long DDOS is desired. This makes the chances of a DDOS occurring higher, as these prices are within reach of most people with malicious intent.

Interestingly enough, these attacks do not typically occur as an attempt to steal data from websites, though this information *can* become compromised. Instead, they aim to block others from accessing the site and the information they have on it– such as favorite videos on Youtube, sending out orders on Etsy, or viewing your personal bank account information.

Ensuring that your website is secure is a first step in ensuring that a DDOS attack doesn't harm your business. Taking steps like giving your employees additional training in online security, and creating detailed online policies and strategies can help you avoid or recover from an attack.

Botnets

Botnets are a network of computers that have been infected by malicious viruses that remain hidden on the computer until an event like a DDOS attack occurs.

During this time, the "botmaster" is able to coordinate an attack and collect control of infected computers to such a large extent that one botnet could bring down a website.

However, these botnets may work collectively to target larger websites and networks in order to bring down the sites for a longer period of time and over a larger geographical area.

In the case of the Dyn DDoS attack, a collective of hackers and botnets worked together across the globe to completely take out Dyn databases on the east coast of the United States, targeting the Dyn servers that linked back to the East Cost but were located in other countries.

The Dyn DDoS attack

On October 21st, 2016, your access to many favorite websites may have suddenly stopped working.

Among the websites that were taken offline, Twitter, Reddit, GitHub, Etsy, Imgur, PayPal, Spotify, Yelp, and the PlayStation Network reported problems stemming from the Dyn DDoS attack.

Problematically, this attack stopped users from accessing their information and effectively costing these companies hours of business– which for internet-based companies can be devastating.

SiteUptime aids in internet performance monitoring to find out exactly how much downtime your web site endures. This information, along with the other data our services gather, can help with your personal understanding of DDoS attacks in relation to your business.

As some have noted, DDoS attacks typically target a single website– demonstrating that someone or some group has a personal agenda to remove that company from full online functionality for an uncertain amount of time.

In the case of the Dyn attack, the unprecedented incident took out a host that allowed multiple large websites to function. Surprisingly, for this DDoS attack, Network World reported that only 10% of the world's botnets were involved in the Dyn DDoS attack.

This particular DDoS attack took out websites for the east coast for almost the entire day– beginning at internet "primetime" in the morning and a third wave of the attack occurring just after 4pm est.

Conclusion

The DDoS attack on Dyn is a clear example of why internet security is an important topic that should be at the forefront of any business owner's mind– regardless of whether or not the company is small or large.

SiteUptime provides monitoring locations across the globe to test the functionality of your website from different points on the map. With multiple locations, SiteUptime checks that problems like DDoS attacks don't take down your website to different user groups.

Our various geographical locations, like New York City, San Fransisco, Portland, Brazil, Ireland, Australia, and Singapore, are just another step we take to ensure that your website is monitoring and prepared for problems like DDoS attacks.

As for Dyn, all of the websites taken down by the October 21st attack have returned to full function. Users can once again enjoy their services and business owners can go back to providing goods and making their living.

However, this massive attack has called for a review of the way websites and servers currently run. Improving the technology and coding behind websites like Dyn *may* be able to stave off a future attack, but staying one step ahead from massive networks of hackers is a difficult task to undertake.

The remedy to this problem is not very clearly, unfortunately. As with many things coming from the dark side of the internet, finding out motives and solutions will be difficult. Dyn has produced a piece that outlines the impact, timeline, and possible solutions to remove the possibility of DDoS attacks from happening in the future.

While SiteUptime is absolutely on board with fighting for a solution, it is our biggest priority to keep you up-to-date with the correct information that can help your business by monitoring the internet performance of your website in the meantime.