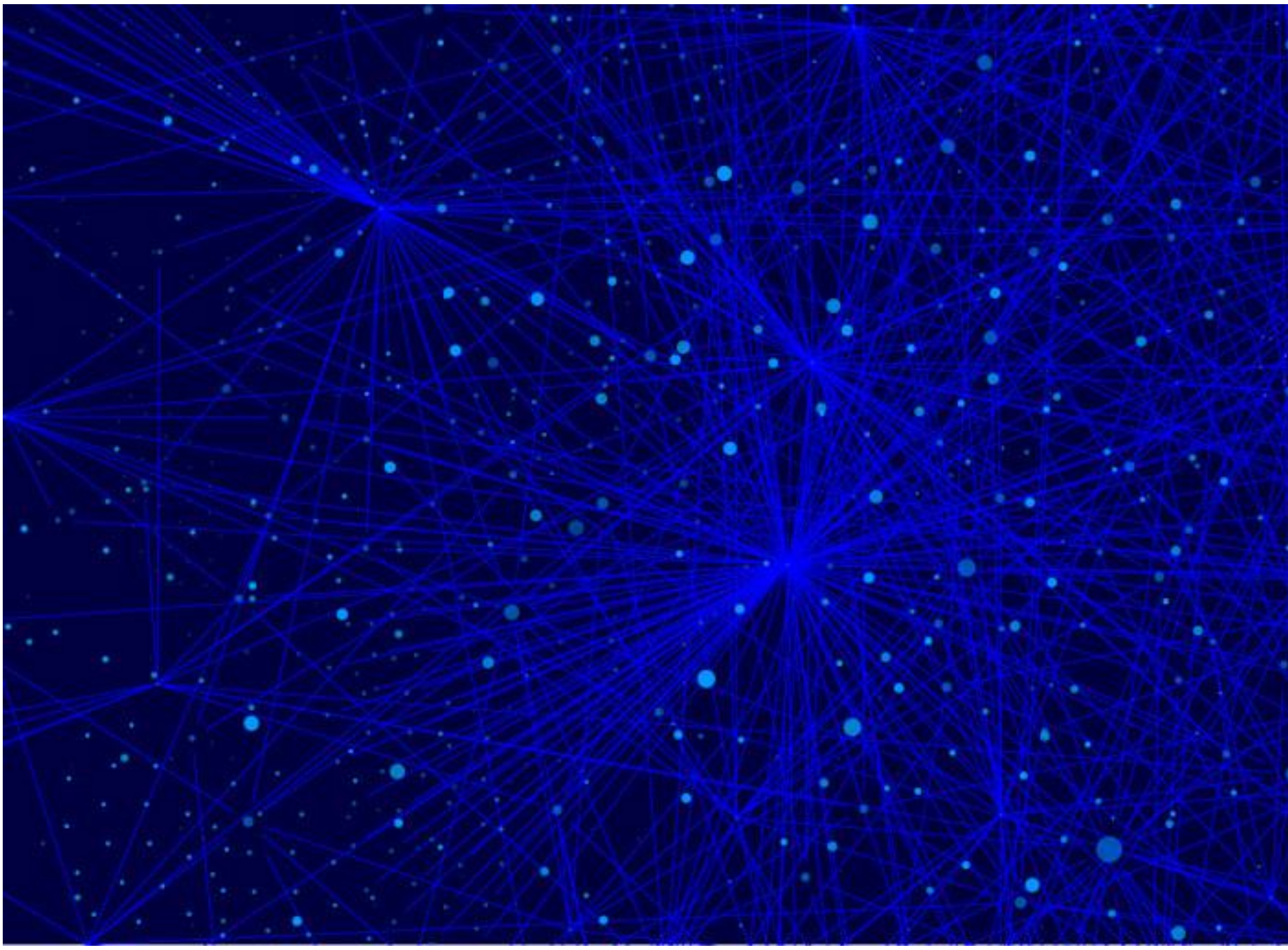
- Author: Kim Zetter. Kim Zetter Security
- Date of Publication: 01.16.16. 01.16.16
- Time of Publication: 7:00 am. 7:00 am

Hacker Lexicon: What Are DoS and DDoS Attacks?



Click to Open Overlay Gallery Then One/WIRED

You see them mentioned in the news all the time. DoS and DDoS attacks are on the rise, and they are getting more sophisticated and intense every year. The US government accused Iran of conducting a prolonged series of DDoS against the web sites of Bank of America and other financial institutions, presumably as retaliation for economic sanctions levied against Iran for its nuclear program. Recently DDoS attacks by extortionists have targeted banks in Greece and Sweden. So what are DoS and DDoS attacks?

DoS stands for “denial of service” and refers to an attack that overwhelms a system with data—most commonly a flood of simultaneous requests sent to a website to view its pages, causing the web server to crash or simply become inoperable as it struggles to respond to more requests than it can handle. As a result, legitimate users who try to access the web site controlled by the server are unable to do so. There are other types of DoS attacks that use different tactics, but they all have the same effect: preventing legitimate users from accessing a system or site.

Simple DoS attacks, performed from a single machine, are uncommon these days. Instead, they've been supplanted by DDoS attacks, distributed denial-of-service attacks that come from many computers distributed across the internet, sometimes hundreds or thousands of systems at once. The attacking machines are generally not initiating the assault on their own but are compromised machines that are part of a botnet controlled by hackers who use the machines as an army to target a website or system. Because these attacks emanate from thousands of machines at once, they can be difficult to combat by simply blocking traffic from machines, especially when attackers forge the IP address of attacking computers, making it difficult for defenders to filter traffic based on IP addresses.

Perpetrators launch DDoS attacks for a variety of reasons. Hacktivists have used them to express displeasure against targets—for example when members of Anonymous launched attacks against the sites of PayPal, Visa, and MasterCard in 2011 after the payment service providers refused to process financial donations intended for WikiLeaks.

In 2013, spammers apparently launched a punishing attack against the spam-fighting site Spamhaus, after the site added a Dutch hosting company called Cyberbunker to its spam blacklist. Spamhaus provides blacklists to email providers to help them filter out spam sent from known spammers. Cyberbunker got on the list because it was accused of providing hosting services to spammers. At the attack's peak, 75 gigabits of traffic per second reportedly flooded Spamhaus servers.

The online gaming industry has also been plagued with DDoS attacks for several years, with the blame going to disgruntled players and even to competitors. A number of DDoS-for-hire services, for examples, will take down a competitor's website for any business that wants to hire them.

Some DDoS attacks are launched for political purposes. The most famous of these were the DDoS attacks that targeted Estonia and Georgia. In 2007, a barrage of traffic knocked government and media sites in Estonia offline and was later attributed to Russian nationalists who were angry about Estonia's decision to relocate a Soviet war monument in Tallinn from the center of the city to a military cemetery.

In 2008, web sites in Georgia were hit with DDoS attacks weeks before Russian troops invaded South Ossetia, prompting Georgia and others to blame Russia for the digital attacks.

More recently, DDoS attacks have been used as a criminal extortion technique. Several encrypted email providers like ProtonMail and Hushmail, as well as banks in Sweden and Greece, have been struck with DDoS attacks after declining to pay a "ransom" the attackers had demanded to not assault their web sites.

DDoS attacks can also be used as a smokescreen to camouflage or draw attention away from other nefarious activity an attacker might be doing, such as stealing data from the victim's network. Hackers who targeted the UK telecom TalkTalk last year used a DDoS attack as a smokescreen while they siphoned data on 4 million of the company's customers.

DDoS attacks are not limited to computers and web servers, however. A variation of the attack can also target phones and phone systems. In December, when hackers caused a power outage at two plants in Ukraine, they also launched a telephony denial-of-service attack against customer call centers, to prevent local residents from reporting the outage to the companies.

DDoS attacks have become more powerful over time, with hackers varying their techniques to amplify their effects and make them more difficult to mitigate or thwart. Every year it seems, a new mega-DDoS attack shows up that dwarfs those that preceded it.

Last year the San Francisco-based security firm CloudFlare, which helps sites improve their performance and security in part by mitigating DDoS attacks, said it had battled a massive DDoS attack against an unidentified client in Europe. The attack, at its peak, spewed nearly 400 gigabits of data per second at its target. The average DDoS attack is about 50 gbps.

Though the power of DDoS attacks is growing, the media often mischaracterize them and exaggerate their significance. Many news outlets, for example, have erroneously referred to the attacks against Estonia's websites in 2007 as cyberwarfare (among them, a WIRED magazine article). And in a 2012 Bloomberg story describing DDoS attacks against US banks, the news outlet wrote that the assaults had "breached some of the nation's most advanced computer defenses" and that such attacks rank "among the worse-case scenarios envisioned by the National Security Agency."

In truth, DDoS attacks alone are an annoyance to web users and can cost a company lost business during the time they deny access to customers, but they're fairly easy to defend against. When used in conjunction with a data breach or some other nefarious activity they can certainly assist in the success of that breach, but they hardly qualify as catastrophic or a worst-case scenario under anyone's definition of the term.

http://www.wired.com/2016/01/hacker-lexicon-what-are-dos-and-ddos-attacks/