



Webbmedia Group, LLC

DDoS Attacks Explained

From Webbmedia Group's Knowledge Base

Summary: A *Denial of Service* (DoS) attack is a malicious effort to keep authorized users of a website or web service from accessing it, or limiting their ability to do so. A *Distributed Denial of Service* (DDoS) attack is a type of DoS attack in which many computers are used to cripple a web page, website or web-based service. A common form of DDoS is a massive number of computers being used to send requests to a web site, overwhelming it to the point where it can't respond to legitimate requests from normal users. This is essentially what happened when Twitter was rendered unresponsive on August 6th, 2009: Requests to the website were sent over and over again until its servers were unable to keep up. In the end, Twitter was unavailable for several hours.

Corporate Explanation: While personal websites and blogs are not generally targeted for DDoS attacks, every organization with a website or web service critical to its operation should be aware of these attacks and be prepared for the possibility of being targeted. Quite obviously, having your site or service rendered inaccessible for even an hour can result in lost revenue; worse, some organizations have even reported blackmail attempts on the part of the attackers. In 2007, Webbmedia Group experienced a blackmail attempt. We were ordered to pay the attackers \$10,000 immediately, or they would keep attacking our site. We'll explain more on how we solved that problem later...

Key Definitions

A Denial of Service (DoS) attack is a malicious effort to keep authorized users of a website or web service from accessing it, or limiting their ability to do so.

A Distributed Denial of Service (DDoS) attack is a type of DoS attack in which many computers are used to cripple a web page, website or web-based service.

Why DDoS Attacks Matter

- Twitter was rendered unresponsive on August 6th, 2009. Requests to the website were sent over and over again until its servers were unable to keep up.
- Just about anyone can become the target of a DDoS attack: news organizations, universities, banks, governments and even individuals with blogs.
- DDoS attacks can cost your company money and disrupt the services you provide.

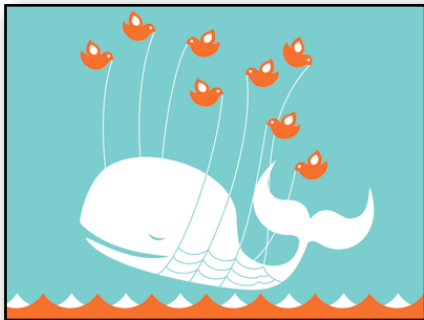


Webbmedia Group, LLC

How do DDoS Attacks Work?

There are several different ways attackers can bring down a site with a DDoS attack. Some prevent legitimate network connections from being completed by keeping the host's resources busy with bogus requests; others overwhelm a network with a large number of data packets, consuming the available network bandwidth. A site can be rendered unavailable even as a result of large numbers of legitimate requests. One example of this is the so-called "Slashdot effect," wherein the popular "news for nerds" site Slashdot (<http://www.slashdot.com>) links to another website, and the massive number of Slashdot users clicking on the link temporarily brings down the other site. While this is not considered a DDoS *attack*, it has essentially the same result. If you've ever heard your staff talking about a site "got so much traffic" the "servers crashed," she's likely referencing a DDoS issue and not an actual broken server.

Other modes of attack are possible, but increasingly, most DDoS attacks have one thing in common: the rise of botnets.



Twitter's infamous "Fail Whale" is displayed anytime the service experienced an outage.

In this context, a *botnet* is a collection of computers that can be remotely controlled by an attacker, whether directly or via peer-to-peer communication. Typically this control is accomplished through the use of malware installed on each individual machine. The individual computers are sometimes called "zombies" because they can be controlled remotely without the knowledge of their owners. Such computers are often used to send spam. It's estimated that the majority of spam originates from compromised zombie machines.

A recent example of a botnet was the collection of computers compromised by the Conficker worm, first detected in 2008. The estimated number of infected computers varied widely, but was as high as 15 million at one point. Such a collection of machines could be used to instigate a DDoS attack. In fact, some hackers even "rent out" botnets, offering them for use by others for a fee per machine.



Webbmedia Group, LLC

What's the motivation for a DDoS attack?

The origin of a DDoS attack is extremely difficult to pinpoint, and without knowing who's behind it, it's hard to determine the motivation for an attack. However, it's reasonable to assume that some attacks are politically motivated, such as efforts to bring down both Georgian and Russian websites during the conflict between the countries in August of 2008. The most recent DDoS attack in August 2009, which brought both Twitter and Facebook down, was actually directed at one person: a Georgian blogger who maintains accounts on Twitter, LiveJournal and Facebook. Political activists were attempting to stop him from communicating, but the attack disabled all three networks for all users worldwide.

On the other hand, some attacks may have no motivation at all. The culprit behind a DDoS attack against popular websites including CNN, eBay, and Amazon in February 2000 turned out to be a Canadian high school student with no clear reason for launching the attack, other than that he could. Some security experts, however, warn that attacks are becoming increasingly financially motivated. For example, there are more and more documented cases of attackers attempting to hold websites for ransom, demanding payment in exchange for stopping their onslaught.

How can DDoS Attacks be Prevented?

There is no guaranteed safeguard against a DDoS attack, but measures can be taken to prevent them. Organizations can limit their risk by securing more servers and bandwidth for their websites than is needed to meet typical demand, and by blocking typical DDoS attack methods. These efforts are undertaken by the web hosting company, not the organization itself, but you should talk to your hosting company to find out what measures they have in place.

End users can take steps to prevent individual computers from ending up in a botnet by securing their systems with the latest operating system updates and antivirus software. Of course you don't want your company targeted by a DDoS attack--but you don't want your systems being used against anyone else, either.

When Webbmedia Group's website was under attack and being ransomed for \$10,000, we undertook an investigation ourselves. In our case, the hacker wasn't too clever and mistakenly left his malicious files in an open area on our server, where we could identify and remove them. We then took additional steps to move our files to a more secure server and we now monitor all activity throughout the day.



Webbmedia Group, LLC

How might DDoS attacks evolve?

Web sites are not the only potential targets of DDoS attacks. As technology advances, the number of possible targets increases: mobile phones, or the mobile network, could also be targeted, just to offer one example.

One of the topics we learned about at this year's Black Hat hacker conference in Las Vegas involved hacking and exploiting SMS to manipulate private data on mobile phones. Researchers have demonstrated that a mobile phone can be rendered temporarily useless by barraging it with text messages -- something that doesn't require thousands of computers, but can be accomplished by one user sending "junk" messages over and over again to the same phone. This specific attack is unlikely: a mobile service provider could quickly uncover the origin of the malicious messages if they were limited to one source, and block the source from sending further requests. A large collection of attack machines, however, could be used to send malicious messages in an attempt to overwhelm the network.

Mobile service disruptions have occurred simply as a result of heavy usage by legitimate users: call attempts at 12:00AM on New Year's Day often fail because of the large number of calls being placed, for example. That a malicious attack could be launched along the same lines is certainly possible. Security experts are just now learning about mobile DDoS vulnerabilities and how to prevent against attacks. Organizations should be aware of the vulnerability of their systems to these types of attacks as they develop and expand.

Additional Resources:

US-CERT (United States Computer Emergency Readiness Team) Reading Room:
http://www.us-cert.gov/reading_room/

SANS (SysAdmin, Audit, Network, Security) Institute <http://www.sans.org/>

For Additional Information:

Webbmedia Group, LLC
2336 Cambridge Walk, Ste 400
Baltimore, MD 21224
tel: 267.342.4300
info@webbmediagroup.com
<http://www.webbmediagroup.com>