FAQ

DDOS

The internet attack of choice for gangsters, governments and bored geeks.

BEN EVERARD

Q Another acronym! First things first, how do I pronounce it? Dos? D'dos? Dee-dos? And how is it different from MS-DOS?

A For once, there seems to be a fairly accepted pronunciation: Dee-dos. It stands for Distributed Denial Of Service, and it's a way that bad people attempt to mess with your computer systems – so it's nothing at all to do with Microsoft's venerable Disk Operating System.

The idea behind a denial of service attack is that a bad guy wants to interrupt your service. Typically, this means 'take your website offline', but it could mean stop users from accessing anything such as email or the database back-end for a mobile app.

It's still possible in some cases for a single computer to take a website offline, but most of the time, denial of service attacks are carried out by large numbers of computers spread out across the world. These are distributed denial of service attacks.

> "You may remember Anonymous's DDOS attacks on financial institutions."

Often these DDOS attacks are carried out by networks of PCs infected with malware (botnets), but not always. For a while it became common for people to volunteer to use their computers to DDOS sites for Anonymous.

Q Right, I think I understand what it is, but how do the bad guys go about doing it?

A Whatever server you use to provide your service has a number of finite limitations. It only has so much bandwidth, memory, CPU power, etc. If you can overload any one of these, then the server will no longer be able to function properly.

Perhaps the simplest form of DDOS is to overload the network. In this sort of attack, you just send loads and loads of data to the server. The aim is simply to clog up their network port so much that legitimate traffic starts to time-out.

Q But surely most big servers can cope with so much traffic that a few virus-infected PCs won't have any impact?

A True. However, the targets aren't always the largest sites. Also, a cunning DDOS attacker can use what's called an amplification attack. This is where they use some way of increasing the amount of data that your computer can send. A DNS amplification attack is quite a common way of doing this.

A Domain Name Server (DNS) is what computers use to lookup information about a particular domain name. For example, if you type **www.google.com** into your browser, it sends a request to your DNS server asking what IP address is associated with **www.google.com**; then it sends an HTTP request to that IP address. However, DNS servers can be asked to return more than just the IP address. There's also a text field associated with domain names, which can hold up to 4,000 bytes. A DNS amplification attack works like this:

- A malicious computer sends a DNS request that will return a 4,000-byte text field to a DNS server, but spoofs the IP address.
- The DNS server responds with the 4,000-byte file. It doesn't send it to the malicious computer, but to the spoofed IP address (the victim server).

These two steps take a 60-byte DNS request, and turn it into a 4,000 byte packet that's sent to the server. These DNS packets won't make any sense to the server, and it'll just reject them once they arrive, but the damage will have already been done.

This form of amplification allows a fairly modest collection of computers to exert a huge force on a server.

An alternative is to work smart instead of hard. In this, you don't overwhelm the server with so much data that it can't function, but you use data such that a small amount can do a very large amount of damage.

Perhaps the most famous attack of this kind is the SYN flood. Whenever you start a connection to a web server, you do a three-way handshake. This is a simple way of establishing a TCP connection over which you can send and receive data. It has three steps. Firstly you send a SYN packet to the server, then the server responds with a SYN-ACK packet, then finally, you respond to that with an ACK packet.

A SYN flood abuses this process. The attacking computers send loads of SYN packets with the IP address spoofed. The server then responds with a SYN-ACK packet, but it doesn't respond to the malicious computer's IP, instead it send it to the spoofed IP. This computer won't respond, because it didn't send the SYN packet.

However, the server will hold this half-open TCP connection while it waits for a response. This half-open connection will lock up some of the resources of the server. If there are enough of them, even if the network isn't overloaded, the server will stop accepting new TCP connections.

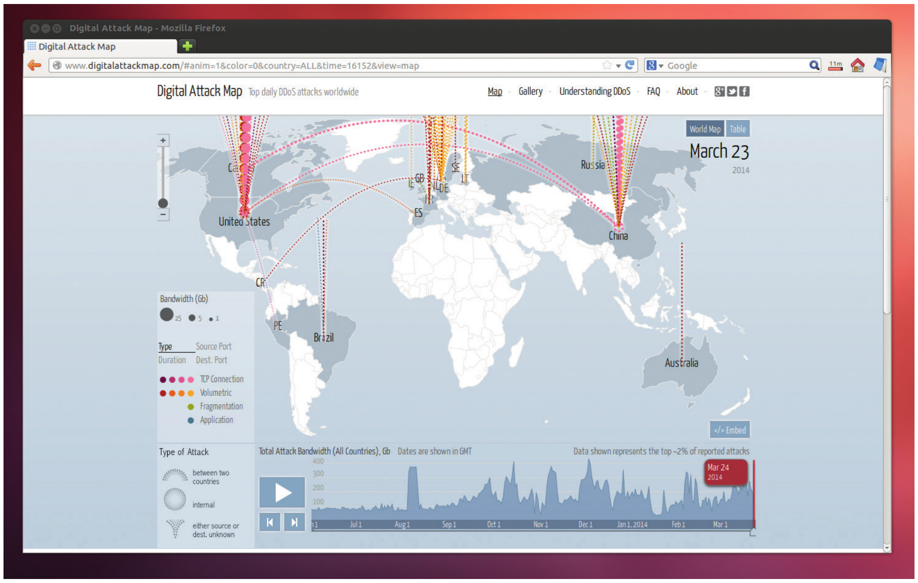
These are examples – there are many more ways to lock up resources and stop a server working properly.

Q But why do it? What's in it for the attackers?

A That varies. The most famous attacks have been politically motivated and were a show of force to try and punish organisations that the attackers felt were harming them. For example, you may remember Anonymous's DDOS attacks on financial institutions that refused to do business with Wikileaks.

One increasing area is digital extortion. In this, some internet bandits launch a DDOS attack against a site, and then tell the site that they'll only stop the attack if the site pays.

Other times, it's a business trying to cripple a competitor, or just bored geeks with a grudge. There are lots of reasons.



www.digitalattackmap.com shows a live feed of DDOS attacks, and can replay big ones from the past.

Q Hang on; people are setting up botnets to target their competition? That's a bit extreme!

A Actually no (well, a few people probably are). You can rent botnets set up for DDOS attacks, or pay people to do the DDOS for you. It's becoming quite a large industry.

Q Wow. That's scary. How bad can these attacks be?

A That really depends on how you define 'bad'. They can quite easily cripple even quite large operations. These days, a moderate volumeteric attack is measured in gigabits per second, a large one in tens of gigabits per second, and a huge one in hundreds of gigabits per second. Once they get to that size, they can be pretty damaging.

Another way of looking at it is how long they last. The largest attacks burn themselves out, because few people can sustain that level of bandwidth for long. However, experience shows that there are botnets capable of sustaining large attacks for several days or longer, which is long enough to dent the finances of a web-based company.

Q What can you do to stop these happening?

A If (for example) you're under a DNS amplification attack, you need to filter out all the rogue DNS packets, but you need to do this as far upstream as possible. The internet isn't just a randomly connected web; it has some structure, and different connections have more bandwidth than others. The key to mitigating a network volume attack is to block it before it gets to a bottleneck. This means adjusting the filtering rules on routers at the data centre, or sometimes even at internet exchange level.

If it's some other form of attack, it means making sure that you don't waste resources on malicious packets, and again, this means identifying them and filtering them out before they do damage. Sometimes you can do this at server level, but it often means getting help from the people running the datacentre or your internet connection.

Q But my server isn't in some fancy datacentre. Is there anything else I can do?

A There is another way, and that's to route all your traffic through a very high bandwidth router that does the filtering and sends on the appropriate requests with the malicious traffic filtered out. While this may sound exactly the same as the option above, the difference is that the router doesn't have to be physically between your server and the internet.

This is known as a scrubbing centre, and it's part of what a content delivery network (CDN) does (there's much more as well). There are a few that you can use without having to change the way you host your site, such as CloudFlare, Incapsula, and SkyFaster.