
Distributed Denial of Service (DDoS) Attacks Is your web site at risk?

Distributed Denial of Service attacks have a single aim - to ensure that the folks who want to visit your web site can't. Extortionists - often international criminal rings - use the power of the Internet and its open transmission protocols to flood your web site's servers with packets. These packets, sent in huge numbers from geographically distributed devices flood servers - and block your users from access. Additionally, some attacks use incomplete packets, forcing the server to do more processing - and again, block legitimate users from access to your site.

The two most common forms of attacks are:

- Bandwidth attacks - that consume network bandwidth or server resources by overwhelming them with a high volume of packets. The targets are routers, servers and firewalls - and the attacks can even force them to fail under the load. The most common form of this attack is a packet flooding attack where seemingly legitimate TCP, UDP or ICMP packets are directed at a specific site or network component. Often the source address of the attack is "spoofed" or masked, making identification of the attacker difficult if not impossible.
- Application attacks - that use the standard behavior of TCP and HTTP to tie up processing resources and stop them from taking care of legitimate requests. HTTP half-open and HTTP error attacks are examples of this attack type.

What does all of this mean to you?

1. If you're paying your hosting company for bandwidth, a DDoS attack could not only wreak havoc with your site, it could also make for a huge increase in your hosting bill for the month (bandwidth overage charges).
2. Extortionists could contact you and ask for \$\$'s to stop the attack and not perform new ones. (A large number of enterprise companies are known to pay extortionists huge fees to free them from DDoS attacks.)

What should you do?

1. Contact your web hosting company and find out what their policy/procedures and protections are against DDoS attacks.
2. If you find that your provider does not have a DDoS mitigation solution in place, ask if they have plans for one, and if not, seek one that does!
3. Ask your hosting provider about their policy regarding bandwidth overage incurred as a result of a DDoS attack. If they aren't sympathetic, a new hosting provider is in order.

DDoS attacks are a growing threat and big international criminal activity. Even if you don't think

you'll ever need it, DDoS protection is like insurance, you'll never know how important it is until you've experienced an attack.

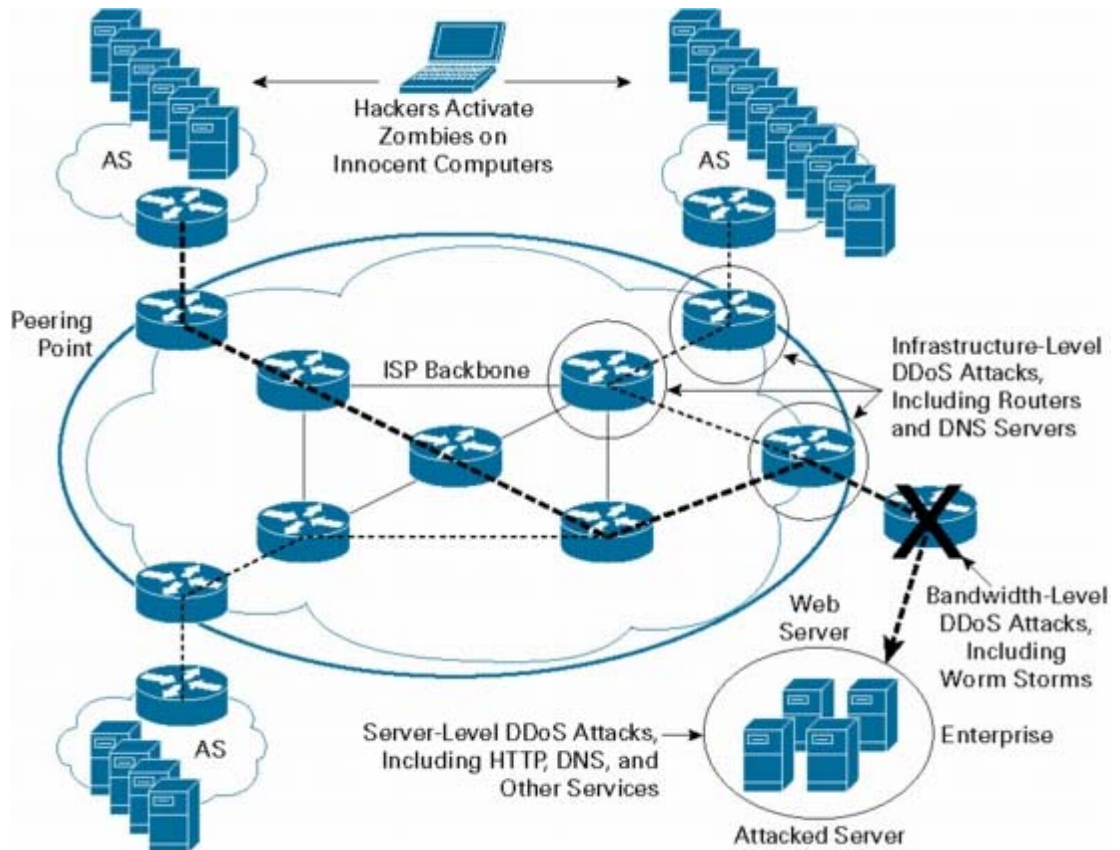


Illustration: Cisco Systems, Inc.

June, 2006