



NISCC

NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE

NISCC Viewpoint 05/2006

Issued 20 April 2006

Distributed Denial of Service (DDoS)

This paper provides advice on how to protect your organisation from DDoS attacks. It includes background information on how a DDoS attack works and methods of defence and response.

NISCC Viewpoint papers are intended to provide an overview of emerging technologies and other issues facing the IT sector. A Viewpoint will not necessarily offer mitigation advice; other NISCC products will do this.

**National Infrastructure
Security Co-ordination Centre**
PO Box 832
London, SW1P 1BG

Tel: 0870 487 0748
Fax: 0870 487 0749
Email: enquiries@nisc.gov.uk
Web: www.nisc.gov.uk

Introduction

1. A Denial-of-Service attack (DoS) describes the situation where a malicious attempt is made to disrupt the operation of a computer system or network that is connected to the Internet. The most common form of attack is one which disrupts the operation of the computer system or network by consuming the bandwidth of the victim network or overloading the computational resources of the victim system.

2. DoS attacks are particularly concerning because they usually target a specific organisation. As a consequence the attacker might be the same sort of person who creates viruses or worms, but the range of possible attackers¹ includes many others who will have the motive, knowledge and resources to do considerable damage.

3. The most common form of defence against a DoS attack is to locate the source of the attack and to filter out the attacking messages from that source. A Distributed Denial-of-Service (DDoS) attack is a more dangerous evolution of a DoS attack because it utilises a network of computers to mount the attack, so there is no identifiable single source.

4. A DDoS attack is launched by the attacker from a network (called a *botnet*) of compromised computers (called *zombies* or *bots*), which are usually broadband-connected home PCs that do not have adequate defences, such as a well configured firewall and up-to-date virus checking software. The attacker compromises the computers using a specially crafted piece of malicious software (called *malware*) that allows the attacker to instruct the zombies to send messages to the computer(s) of the victim organization. The purpose of the messages is to overload one of the finite resources of the victims computer(s), typically network bandwidth, processor power (CPU cycles), or disk space.

5. Botnets are used for other purposes as well as DDoS, most commonly for sending spam email. They are so widely used that there is even a black market where a person or organization wishing to launch a DDoS attack can purchase access to a large number of existing zombies.

6. The main purpose of this paper is to answer the question “how can I protect my organisation from a DDoS attack?” The available methods of launching a DDoS attack are numerous and many of them are technically complex to explain. If the reader wishes to read up on the technicalities of DDoS attacks then a very useful resource to read is the Wikipedia entry on DDoS² which contains a most informative summary of common attacks and

¹ For example, professional criminals, organisations and individuals with political agendas, and organisations and individuals with a grudge.

² http://en.wikipedia.org/wiki/Denial_of_service

has many excellent references to help the reader understand the technical complexities of DDoS.

7. In order to understand the methods an organisation can use to defend itself from DDOS attacks it is useful to explain some high level technical issues relating to DDOS.

8. Many commercial Internet applications are built on the TCP/IP protocol. For example, a web site will use the http protocol layered on top of TCP/IP. A DDoS attack may use TCP/IP but often it will use another protocol such as ICMP – the Internet Control Message Protocol – which is primarily used by networked computers' operating systems to send error messages (again see the Wikipedia entry for further details³). The distinction between TCP/IP and non TCP/IP attacks is important because:

- TCP/IP is a connection-oriented protocol in which the victim's computer must exchange information with the zombie in order for the attack to work. This means that the victim knows the real identities of the zombies attacking it. In contrast most non-TCP/IP protocols such as ICMP are connectionless so the zombies can forge the sender's address and the victim will not know where the attacking messages originated from; and
- non TCP/IP messages are unlikely to be carrying the data an organization wants to exchange with its customers/partners. As a consequence they can often be filtered out without losing contacts from legitimate customers/partners.

9. Another key attribute of an attack is whether the attacking messages all have some common property (called a *signature*). If the attacking messages have an identifiable signature then it is much easier to manage the attack by the use of filters that remove messages with that signature. It is however possible that an attack floods the victim with seemingly random legitimate messages – e.g. requests for web pages from a web server, which by definition will have no signature to distinguish them from real requests.

10. One of the most threatening aspects of a DDoS attack is that an organisation may not be able to deal with attack without outside assistance. For example a flood of messages designed to overload the bandwidth of the Internet connections of a victim's computer may overload an upstream Internet pathway before the messages arrive at the victim's connection to the Internet.

11. In the next section we examine the mechanisms available for repelling a DDoS attack.

³ <http://en.wikipedia.org/wiki/ICMP>

Defences against a DDoS attack

12. Countering a DDoS attack can be thought of as a trial of strength. The attacker is seeking to saturate a finite resource of the victim, be it bandwidth, CPU cycles or disk space, and the defender is seeking to provide sufficient resource, or to stop sufficient of the attacker's messages, to prevent that saturation. The simplest form of defence is to have larger resources or the ability to increase those resources in the event of an attack.

Have appropriately large reserves of bandwidth, CPU power and disk space

13. When sizing the purchase of bandwidth, CPU and disk space, consider how large a DDoS attack you want to be able to handle. In addition, you may want to consider in advance how resources such as bandwidth can be increased by your suppliers at very short notice. These reserves will also help handle unexpected peaks in demand – which raises an interesting issue:

Have access to sufficiently skilled system and network administrators

14. The very first thing that needs to be done is to distinguish a DDoS attack from a legitimate spike in demand. This can be more complex than it sounds because a mention on one of the very popular web sites (such as Slashdot⁴) or a high profile article in the media can lead to a massive spike in demand, which can be every bit as dangerous as a malicious DDoS attack. In defending against a DDoS attack you must either have a skilled in-house pool of system and network administrators, or have such a pool as part of an outsourcing contract. If you have neither, or want access to up-to-date skills in handling DDoS there are a number of commercial suppliers who will provide expert support in the event of a DDoS attack, as well as advising on the preparations that should be made in advance of a possible future attack.

15. Once these skilled staff have identified that a DDoS attack is underway they will do a number of things:

Identify the nature of the attack

16. Your staff, outsourcing supplier or consultants will have to ascertain (as a minimum):

- Is the attack TCP/IP or non-TCP/IP?
- Can the attack be repelled by simply increasing computational or bandwidth resources?

⁴ We chose Slashdot as an example because this phenomenon is often referred to as the Slashdot effect.

- Does the attack have a signature?
- Can the attacking messages be filtered out without losing an unacceptable amount of legitimate traffic?
- Where are the best places to apply that filtering?
- Are there upstream problems of Internet pathways being overloaded before the traffic reaches your network?

17. Defences then need to be activated.

Respond to the attack

18. Possible actions your staff, outsourcing supplier or consultants will take include the following:

- Increasing computational or bandwidth resources, for example by calling on additional bandwidth that you had negotiated could be quickly provided by your supplier, or exploiting reconfigurability that you had designed into your data centre;
- Implementing filtering rules on routers and/or firewalls – a number of hardware suppliers advertise capabilities that help with filtering in the event of a DDoS attack;
- Contacting the owner of the core router that is passing the DDoS messages to your border router and asking for their assistance in tracing back from their router to ascertain the source, and manage the effects, of the attack. This will be essential if upstream Internet pathways are clogged with DDoS messages. There are commercial providers who provide bandwidth to organisations, who specialize in the ability to mitigate DDoS attacks;
- Changing the IP address of the victim computer and passing that new address to key customers and partners;
- Blocking messages from the source, if the attack originates from a specific provider or core router, although this will almost certainly affect some legitimate traffic.

How do you prepare for a possible DDoS attack?

19. Given the technical complexities of handling a DDoS attack and the fact that it may take many hours (or even days) to mitigate an attack, preparation is key. The following preparations should be considered.

Have pre-prepared processes ready to handle a DDoS attack

20. You should know who is tasked to do what in the event of an attack. You need access to staff with the requisite skills to identify, analyse and then repel an attack.

Have existing processes set up with people you need to contact

- Contact the owners of core routers you may need assistance from to mitigate an attack.
- Have contractual processes in place for quickly increasing resources such as bandwidth.
- Decide if you want to hire anti-DDoS experts to assist you in the event of an attack (and follow their advice about necessary preparations).

Put DDoS resistance into your Internet facing resources

- Size your computational and bandwidth resources appropriately. The magnitude of DDoS attacks tends to increase with time, so you need to research the likely size of an attack and also allow a margin for future growth in the size of attacks.
- Decide if you want to host your static web content on commercial caching services, whose design makes them significantly resistant to DDoS attacks.
- Decide if you want a fall-back capability that utilizes a minimum of CPU, disc and bandwidth resources (e.g. a web site with no images) for the duration of the attack.
- Buy commercial products and services that provide aspects of DDOS resistance.
- Design your architecture to degrade gracefully in the face of a DDoS attack, so that you throttle at appropriate points in the system to avoid your service crashing. For example, if the service is based on the user initiating a session then you can decide to have an upper limit on the number of active sessions.
- Test your service's resistance to, and degradation under, DDoS attack. Retest after major updates.

Conclusions

21. The rise of the DDoS phenomenon is one of the most serious threats to an organisation's Internet-facing computer resources. There is little or nothing

to stop an individual or organisation launching a DDoS attack against you, and it is very difficult to determine who was responsible, so there is little that can be done to deter potential attackers. There are no straightforward ways of stopping a determined and sophisticated DDoS attack very quickly, and even if you are prepared to repel such an attack you can expect service interruptions measured in hours not minutes. An organisation that is unprepared for such an attack could be off-line for days, and there have even been a few examples where small companies have been driven out of business. This document outlines the sort of preparations to defend yourself against a DDoS attack that you would be unwise to ignore.

This paper was produced for NISCC by QinetiQ

About NISCC

The role of NISCC is to minimise the risk to the Critical National Infrastructure from electronic attack. NISCC was set up in 1999 and is an interdepartmental



centre drawing on contributions from across government. Defence, Central Government Policy, Trade, the Intelligence Agencies and Law Enforcement all contribute expertise and effort. Further information can be found at www.niscc.gov.uk

About QinetiQ

QinetiQ is one of the world's leading defence technology and security companies.

For further information please call us on 08700 100 942 or refer to our website: www.QinetiQ.com

