

Under Attack!

Mike Bromwich, Technical Director, PDMS

Crime is rife on the Internet, and one of the exploits which has received significant press recently is the Distributed Denial of Service (DDoS) attack. There have been numerous high-profile outages caused by such assaults, and the nature of these attacks makes protection from them difficult and costly. With an increasing proportion of businesses becoming reliant on the Internet to carry out their day-to-day business, online assets are considered an easy target. There are few more profitable crimes which can be undertaken in comfort, from thousands of miles away, and insulated from the victim by national boundaries.

WorldPay, the Royal Bank of Scotland's Internet payment business, has been the target of several DDoS attacks over the last year. Although it stresses that its systems remain uncompromised and secure, the attacks have caused significant outages during which their services were either unavailable or severely impaired. This undoubtedly cost their estimated 30,000 customers significantly.

Carrying out an effective DDoS attack takes planning and effort, but since the attacks themselves are usually coupled with extortion demands, such investment is often considered worthwhile. A typical DDoS attack starts with the perpetrators compromising a single, vulnerable machine from which often many thousands of other machines are subsequently compromised. The compromise usually takes the form of the loading of a 'trojan' application which is designed to go unnoticed. This trojan application sits dormant, awaiting further instructions. The troops are now deployed ready for combat.

Where there is a commercial goal, the next step is to make contact with your chosen victim (usually by E-Mail), and to make an extortion demand. Typically, this demand will be for a significant five-figure sum which must be paid by a given deadline using a prescribed means.

Should payment not be forthcoming, the perpetrator's next move is to send an instruction to the trojan machines to launch their onslaught against the victim. There are numerous variants of attack used at this stage – sometimes, the trojan will generate an overwhelming amount of ordinary traffic, designed to overwhelm the victim's infrastructure. More often than not, however, the traffic will consist of mutant data – carefully crafted to confuse or disable target devices. Location information is often 'spoofed' – making it difficult or impossible to determine its source.

The usual first line of network defence – the firewall – is of little use against a DDoS attack. At best, the firewall will prevent any mutant data from reaching your servers, but if the traffic is designed to appear legitimate, the firewall is likely to let it through. Either way, the firewall cannot lessen the impact on 'upstream' infrastructure – links to your ISP, or subsequent links within their network.

Equally, an IDS (Intruder Detection System) is of little use. It can notify you that an attack is underway, but is often unable to determine the source of the attack. Since the traffic often originates from many thousands of machines, even identifying the sources is often of little help anyway.

There are, however, defences available to deal with DDoS attacks. In all cases, the most important allegiance in countering the threat is with your ISP – ideally an ISP with the level of infrastructure and knowledge required to tackle the issue promptly and effectively. Often, attacks are launched at deliberately inopportune moments, and so it is important to ensure that the support is there whenever required.

A DDoS attack against your infrastructure is likely to cause problems for your ISP anyway, and so it is important to discuss a response plan in advance. In the event of an attack against a single customer, a high priority for an ISP is likely to be to limit the effect of the attack on other customers. In the absence of other measures, the provider is likely to 'black-hole' your traffic. This amounts to a short-term withdrawal of the routing information required to deliver your traffic across the Internet – the side-effect being that all your traffic, legitimate and malicious, is suspended.

Less destructive solutions are available. One solution is to subscribe to sufficient bandwidth to allow the DDoS traffic to flow. It is not necessary for this bandwidth to be delivered to your premises or systems, since the upstream service provider can often identify and filter the legitimate traffic and drop the remainder. For such a solution to be effective, it is usually necessary to subscribe to several gigabits of DDoS-protection bandwidth, and as hence this is often a costly approach. Since the scale of attacks is set to increase, so will the amount of protection required.

Naturally, network infrastructure manufacturers see DDoS protection as an opportunity to devise and sell devices which counter DDoS attacks. One of the manufacturers most prominent in this space is Riverhead Networks (recently acquired by Cisco Systems). Their solution is split into two parts – a detector and a guard. The detector sits on the perimeter of your network and analyses incoming traffic. When it detects traffic which appears to form part of a DDoS attack, it sends instructions to guard devices distributed at strategic points on the Internet or service provider's network. These guard devices act on the instructions by blocking the malicious traffic from entering the network before it can cause disruption. The system can act quickly to block many thousands of distributed sources – something which could never be achieved manually.

Law enforcement authorities too have had a degree of success in bringing the perpetrators or such attacks to justice – although the fact that many attacks originate from the former Soviet Union does not simplify the matter. Authorities of such countries often have what they consider to be more serious issues to address, and so getting co-operation can be difficult. In the UK, the National High-Tech Crime Unit (NHTCU), working with overseas authorities, have brought about a number of successful arrests in Russia and elsewhere.

Unfortunately, it appears that DDoS attacks are becoming something of a daily occurrence. Although it has taken some time, the industry has clearly woken-up to the threat and significant progress has been made in addressing the issues. Until recently, the Internet has relied on a degree of trust and co-operation to ensure its wellbeing. It is disappointing yet inevitable that this is no longer sufficient.