CORSAIRE

The natural choice for information security solutions

A Corsaire White Paper:

Surviving Distributed Denial of Service (DDoS) Attacks

Author	Stephen de Vries
Document Reference	Surviving DDOS Attacks.doc
Document Revision	V1.0 Released
Date	11 February 2004

Table of Contents

Introduction

Distributed denial of service (DDoS) attacks aim to disrupt the service of information systems by overwhelming the processing capacity of systems or by flooding the network bandwidth of the targeted business.

Recently, these attacks have been used to deny service to commercial web sites that rely on a constant Internet presence for their business. The attacks differ from traditional DDoS attacks in the targeted nature and shear number of attacking hosts. Even hardened Internet companies such as the SCO group and Microsoft are not immune to attack, and historically high-profile e-tailers such as eBay have had their services disrupted.

The threat from the latest attacks has become greater due to the political and financial agendas of those instigating them, particularly the involvement of international organised crime in protection extortion attempts.

There is no simple solution to mitigate the risk of these attacks, but there are strategies that can help minimize the impact of a large-scale attack.

1. Attack types

Recent reports from the NHTCU have warned of DDoS attacks that use SYN flooding and SMTP flooding to saturate the bandwidth of targeted sites. Although, these are by no means the only attack vectors, they will be the main focus of this paper as they pose the greatest threat to the availability of business sites.

SYN flood attacks exploit a feature of the TCP connection by making seemingly legitimate connection requests, and then discarding the responses. This results in the attacked server responding to requests and waiting for connections to complete that never do. The server wastes resources on maintaining these non-existent connections and the bandwidth suffers as a result of the high volume of traffic generated by the initial request and server response.

It is believed that SMTP attacks simply send a high volume of e-mails to the targeted server thereby overwhelming both the server and the available bandwidth.

Both types of attack effectively deny service to legitimate users by reducing the performance of the site to make it unusable, or causing it to fail altogether.

2. Mitigation strategies

2.1 Management strategies

2.1.1 Planning for attack

Without proper planning and forethought, a sustained DDoS attack can find your organisation without the necessary resources or procedures to deal with the attack. It is essential that the response procedures are clear and that enough resource, both people and technology, are available to effectively handle the attack.

2.1.2 Defining critical services

In order to better protect your online business, it is important to identify the most critical part of your online presence. In many cases, organisations use the same connection to the Internet for various purposes such as outbound web traffic, incoming web traffic, SMTP e-mail and DNS traffic. When this connection comes under attack, there should be a clearly identified priority of

services that are essential to the business. Once this is decided, further technical mitigation strategies become easier to implement.

2.1.3 Communicating with the ISP

In many cases when a sustained high bandwidth attack reaches your servers it will not be possible to contain the attack at your border gateway as the offending packets have already consumed the finite bandwidth available on the connection to the ISP. In this case, having a good relationship and clear communication channels with your ISP are essential in containing the attack. High bandwidth attacks will have an impact on the ISP's network and they have a vested interest in assisting you. In addition, since they are closer to the source of the attack they are in a better position to filter the offending traffic.

The ISP may already have procedures in place for dealing with this kind of attack. Understanding these procedures and your responsibilities can greatly reduce the time taken to contain an attack. If not already negotiated, such protection mechanisms could form part of the standard SLAs.

2.1.4 Resources

The resources needed to deal with an attack should already be in place when an attack occurs. More bandwidth, additional load balanced servers and support staff should be ready to be deployed in the live environment when the need arises.

2.1.5 Response procedures

Clearly defined and understood incident response procedures should be in place both at your organisation and at your ISP. The ISP may be able to provide guidance on how best to respond to DDoS attacks and what procedures need to be followed by your organisation's technical staff so that a timely defence is ensured. The escalation procedures, including contact details at the ISP should be documented and if DDoS protection is part of the SLAs, the response times should be specified.

The technical team should understand their responsibility in detecting and responding to an attack, and if the need arises, how to escalate the response to the ISP. When the DDoS attack originates from many compromised hosts, it is likely that your organisation is not the only victim and it may be necessary to contact the National High Tech Crime Unit (www.nhtcu.org). Remediation and investigation efforts can be expedited by contacting the NHTCU prior to an attack to establish a clear communication and escalation procedure.

2.1.6 Insurance

Where the availability of online services is a critical function to the business, it may be possible to procure insurance to protect against the loss of business as a result of a successful attack.

2.2 Technical strategies

2.2.1 Detecting attacks

Certain types of DDoS attacks are easy to detect as they make use of unusual protocols or attempt to send specific non-standard packets to the targeted systems. Attacks that mimic the behaviour of legitimate users by making repeated requests to the website or by sending a large volume of e-mails can be much harder to detect.

Having an understanding of normal user behaviour and traffic can help in identifying anomalous traffic. Some network based Intrusion Detection Systems (IDS) and network monitoring tools

can be used to identify anomalous behaviour on the network and configured to send alerts to the appropriate personnel. In some cases attacks may be indistinguishable (at the protocol level) from legitimate traffic and it is important that detection mechanisms are able to detect these attacks by analysing the volume of connections per host and not simply relying on attack signatures.

The network monitoring tools currently used within your network should be investigated to determine whether they support detecting anomalous traffic patterns. Secondary monitoring procedures should also be in place to detect attacks that are not identified by the primary detection tool. These could be bespoke scripts that check the availability of the web site periodically, or a service provided by the ISP or other partner.

It is important that the detection mechanism chosen can identify and log details of the attack, such as the source IP address, the protocol used and the payload.

2.2.2 Filtering at the border gateway

Unnecessary traffic destined for your network should be filtered at the border gateway as a matter of course. Protection mechanisms that prevent SYN Flood attacks from reaching servers should also be considered. Popular commercial and open source firewall products now offer this feature and can provide a limited degree of protection against low bandwidth attacks. However, if the attacks succeed in saturating the available bandwidth between your organisation and the ISP then the protection offered by these devices is negated, in this case it will be necessary to contact your ISP to assist in managing the attack.

Furthermore, SYN protecting in firewalls is often a processor intensive function, especially when under a DDoS attack. It is important to ensure the device has sufficient processor and memory capacity to function effectively under heavy load.

For these reasons, SYN defences should be provided by devices as far upstream as possible – ideally on the ISP side of the connection.

2.2.3 Filtering at the ISP

Since the ISP has more available bandwidth and is closer to the source of the attack, they are in a better position to perform filtering of the malicious traffic. This filtering can usually be done based on two criteria:

a) The source and destination IP addresses of the traffic

b) The type of traffic

In order for the ISP to use the source and destination IP addresses to filter traffic, they will need to know the sources of the attack. The sources should be identified by the detection mechanism and communicated to the ISP. Where distinct IP addresses are known, the ISP may be able to filter these individually, but there may be occasions where the offending traffic is identified as originating at another network (or even an entire country). Many DoS attacks used spoofed packets that do not reveal the true source address of the attacking host. In these cases, the ISP will have to communicate with upstream providers to block traffic from the offending networks. An agreement with the ISP will have to be reached on whether it is feasible to deny traffic from an entire network node, as opposed to individual IP addresses as this may deny access to legitimate users on that network.

ISPs can also perform traffic shaping based on the type of traffic. This allows them to permit certain types of traffic while denying others. Where the services critical to the business have been identified, the ISP can give priority to these services while denying or delaying others.

2.2.4 Segmentation

Once critical services are identified, it is possible to segregate these services from other less critical services. If the organisations web site is critical to the business, then hosting at a high bandwidth provider should be considered. Other less critical Internet services such as email or FTP could be hosted locally. When designing network defences, it is important to identify bottlenecks in the architecture that could be exploited by attackers. Where possible secondary DNS and email servers should be hosted at different ISPs and at different physical locations.

3. Conclusion

DDoS attacks present a very real threat to online business, even more so when the availability of the service is an essential business function. Traditional firewalls and sensible security at the border gateway can provide some degree of protection against low bandwidth attacks. But more and more attacks are using flooding techniques to saturate the bandwidth of online companies, thereby denying legitimate users access to their services. It is difficult to defend against these attacks at the border gateway, but by careful planning and by communicating with your ISP, it is possible to provide some level of protection from loss of business.

Acknowledgement

This White Paper was written by Stephen de Vries, Principal Consultant, Corsaire Limited.

About The Author

Stephen de Vries is a Principal Consultant in Corsaire's Security Assessment team. He has worked in IT Security since 1998, and has been programming since 1997. He has spent the last four years focused on Ethical Hacking, Security Assessment and Audit at Corsaire, KPMG and Internet Security Systems. He was a contributing author and trainer on the ISS Ethical Hacking course and Technical Leader for the Automated Perimeter Scanning project co-coordinating a team of six developers in three countries.

Stephen's past roles have included that of a Security Consultant at a leading City of London Financial institution and also Security Engineer at SMC Electronic Commerce. At both positions he was involved in corporate security at many levels and was responsible for consulting on the paper security policies and procedures, conducting vulnerability assessments, designing, deploying and managing the security infrastructure of the organisation.

About Corsaire

Corsaire are experts at securing information systems. Through our commitment to excellence we help organisations protect their information assets, whilst communicating more effectively. Whether they are interacting with customers, employees, business partners or shareholders, our sound advice can help our clients reduce corporate risk and achieve tangible value from their investments.

Privately founded in 1997 and with offices in the UK and Australia, Corsaire are known for our personable service delivery and an ability to combine both technical and commercial aspects into a single business solution. With over eight years experience in providing information security solutions to the UK Government's National Security Agencies, Government departments and major private and non-profit sectors, we are considered a leading specialist in the delivery of information security planning, assessment, implementation and management.

Corsaire take a holistic view to information security. We view both business and security objectives as inseparable and work in partnership with our clients to achieve a cost-effective balance between the two. Through our consultative, vendor-neutral methods we ensure that whatever solution is recommended, an organisation will never be overexposed, nor carry the burden of unnecessary technical measures.

Corsaire have one of the most respected and experienced teams of principal consultants available in the industry and have consistently brought fresh ideas and innovation to the information security arena. We take pride in being a knowledge-based organisation, but we don't just stop there. Through a culture of knowledge-share, we are also committed to improving our client's internal understanding of security principles.

It is this approach to knowledge that differentiates us from most other information security consultancies. As a mark of this, we are known globally through our active contribution to the security research community, publishing papers and advisories on a regular basis. These we share freely with our clients, providing them with immediate access to the most up-to-date information risk management advice available, allowing them to minimize their exposure and gain an instant competitive advantage.

Whilst it is imperative for us to offer a high level of security to our clients, we believe that it is of equal bearing to provide a high level of service. At Corsaire our clients are not only protected

but valued too. We work hard at building strong relationships that are founded on the cornerstones of respect and trust. With 80% of our customer base deriving from referrals we are certain that our clients value the quality, flexibility and integrity that partnering with Corsaire brings.

For more information contact us at **info@corsaire.com** or visit our website at **www.corsaire.com**