About the author

Victor DeMarines, vice president of products at V.i. Laboratories brings extensive product management and marketing experience in the security industry to his current position, which he has held since May 2006. He is responsible for the marketing and product management activities to support V.i. Laboratories' application security products and technology.
For additional information on V.i. Labs you may visit, www.vilabs.com or contact Victor at vdemarines@vilaboratories.com.

References

1. "Virus detail: Win32/Stration Family." Computer Associates. 19 May 2008. <www.ca.com/us/securityadvisor/virusinfo/virus.aspx?id=58375> and "Stration." Wikipedia. 19 May 2008. <http://en.wikipedia.org/wiki/Stration>
2. Mashevsky, Yury. "The Virtual Conflict – Who Will Triumph?" Viruslist. 19 May 2008. <www.viruslist.com/en/analysis?pubid=204791915>
3. "Yoda's Protector." Sourceforge.net. 19 May 2008. <http://sourceforge.net/projects/yodap/>
4. "W32/Sdbot.worm!811a7027." McAfee. 19 May 2008. <http://vil.nai.com/vil/content/v_140978.htm>
5. Hunt, Galen and Brubacher, Doug. "Detours: Binary Interception of Win32 Functions." Microsoft Research. 19 May 2008. <http://research.microsoft.com/~galenh/Publications/HuntUsenixNt99.pdf>
6. Raber, Jason. "Deobfuscator: An Automated Approach to the Identification and Removal of Code Obfuscation." Riverside Research Institute, Inc. <www.rri-usa.org/Deobfuscator.pdf>

DDoS attack evolution

Dr. Jose Nazario, senior security researcher, Arbor Networks

A distributed denial of service (DDoS) attack is designed to overwhelm victims with traffic and prevent their network resources from working correctly for their legitimate clients. DDoS attacks require a significant amount of bandwidth to successfully attack a big adversary, such as a Web-based media company, so they often command thousands of hosts in a botnet to simultaneously send traffic to a victim. This action has the effect of aggregating bandwidth to match or surpass the victim's network resources, as well as making specific host filtering difficult, since the attack is coming from so many places all at once.

Arbor Networks has measured DDoS attacks for many years in a variety of ways. For several years it used a large portion of unused internet address space to look for 'backscatter' from attacks and infer attack patterns. More recently it gathered a great deal more intelligence on the attacks by using direct global internet backbone measurements to gauge attack frequencies and types. It also now monitors hundreds of botnets for attack commands, which gives it further insights into the nature of DDoS attacks on the internet.

The dramatic upswing of attack sizes over the years ranges from the estimated 200 Mbps of Code Red's zombie network to a maximum observed attack of about 40 Gbps in 2007. These attacks can cause widespread disruptions when aimed at key infrastructure points. Arbor Networks works with its customers and the wider internet security community to detect and disrupt these attacks.

DDoS background

DDoS attacks may use many different approaches to achieve the disruption of normal services. Their two major goals are to consume bandwidth and overwork the server.

"The dramatic upswing of attack sizes over the years ranges from the estimated 200 Mbps of Code Red's zombie network to a maximum observed attack of about 40 Gbps in 2007"

Consuming bandwidth can be done using any traffic types. Most of the "zombies" in a DDoS army will send the same kinds of traffic. The most common means are ICMP Echo Request floods, commonly referred to as "ping" floods, although any traffic can be used, including UDP or TCP. Over the years, the most common choice for attackers has been the TCP SYN flood, with the ping flood a distant second. Application layer attacks are increasing, such as HTTP GET request floods and 'mail bombs' or floods from spam networks. DNS-based attacks, in which attackers flood DNS servers with bogus but well formed requests, are also quite popular.

Intelligent attackers will choose traffic that looks similar to a victim's normal traffic. If the victim has a Web server, the attackers send TCP port 80 traffic (which is also used by legitimate HTTP traffic) or, better still, HTTP GET requests. If the victim has a DNS server, the attackers send UDP port 53 traffic to mimic the normal traffic. Because of this, network operators cannot simply drop all of the attack traffic without disrupting normal services for the end host.

A normal request flood, which makes the victim's server work hard

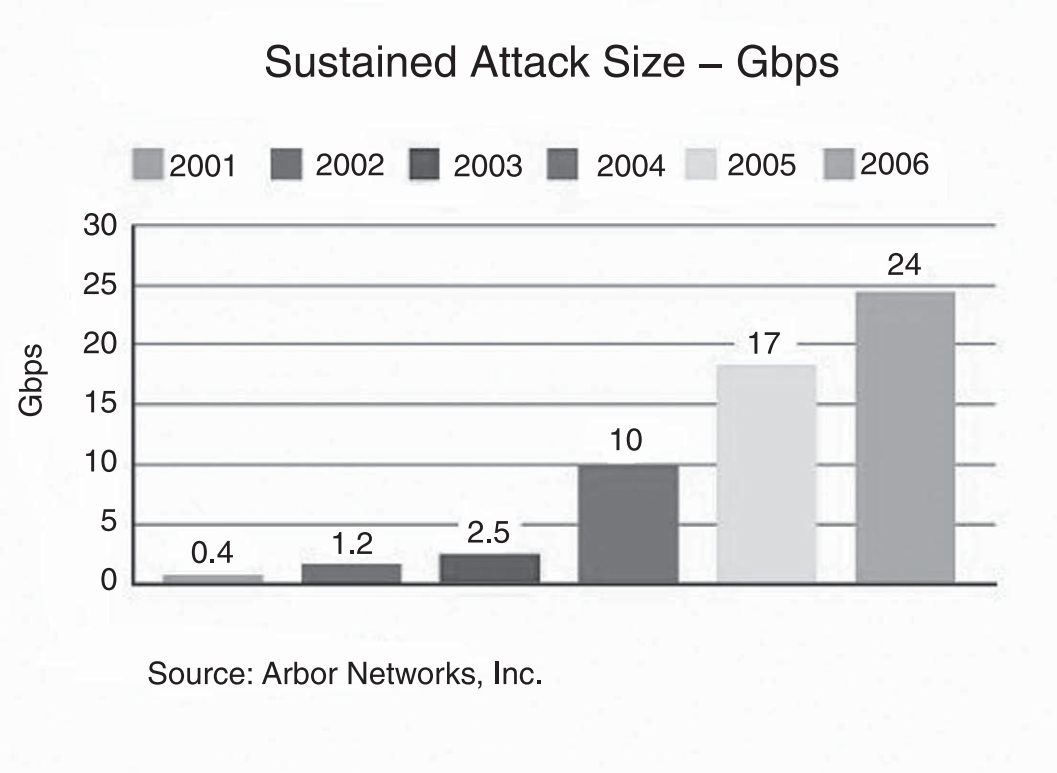

Figure 1: Source: Arbor Networks 2007 Worldwide Infrastructure Security Report.

to service what it sees as legitimate requests, may overwork the server. For example, a rapid fire series of HTTP GET requests from a botnet to a Web server will cause the server to attempt so many connections that normal clients will be choked out and it may even fall apart under the service load. At the protocol level, a TCP SYN flood attempts to do the following: the server will spawn connection handlers in response to the connection request from the client – a TCP SYN packet. When the server's kernel networking tables fill up, they can't handle new connection requests and legitimate clients may fail to operate.

For connectionless floods – i.e. flinging packets at the victim and ignoring the replies – the source addresses can be spoofed. This forgery can make it hard to track down the sources of the attack and subsequently block them by doing ingress IP address filtering.

Zombie army evolution

The first DDoS attack armies were simple scripts that listened to IRC channels, usually for management. People noticed that arbitrary commands, such as the 'ping' command, on the hosts could be executed where the channel management scripts (e.g. "eggdrop") run. Multiple hosts were commanded to send as much traffic to the victim as possible and thus the first DDoS attacks were born.

In the late 1990s, dedicated command and control networks appeared, called Shaft, 'Trinoo', Tribe Flood Network and so on. One of the more well known DDoS network builders and operators at the time, a young Israeli who used the nickname Mixter, openly discussed the tools and techniques used by the attackers and also provided some of the early techniques for detecting and stopping the emerging DDoS attack tools.

A major new Windows worm, Code Red, highlighted the start of a new attack era in 2001. This worm spread quickly, built up hundreds of thousands of hosts in zombie armies, and had a specific, predefined DDoS attack target; one of the IP addresses used by the White House. Similar worms followed suit, including the MyDoom worm in 2003, which targeted the Microsoft Windows Update Web server.

IRC-based botnets were already on the scene at this point and quickly became popular just after the big worm days of the early 2000s. Botnets such as Agobot, Nesebot, Spybot, RxBot and many others were common and most included some form of DDoS or packet flooding capabilities. The Kaiten botnet codebase, popular on Linux, is also commonly used to launch DDoS attacks.

"Simple retaliations are fairly frequent, for example, against anti-spam or anti-phishing organisations such as Spamhaus or Castlecops"

In 2006, Arbor noticed the continuation of an earlier trend; a widespread shift from IRC-based botnets by certain more dedicated attackers. Examples of botnet codebases in this class include the peer-to-peer Storm worm, which has a DDoS component often used against attackers, the Russian Black Energy, and the Chinese Hitpop. Arbor is presently tracking

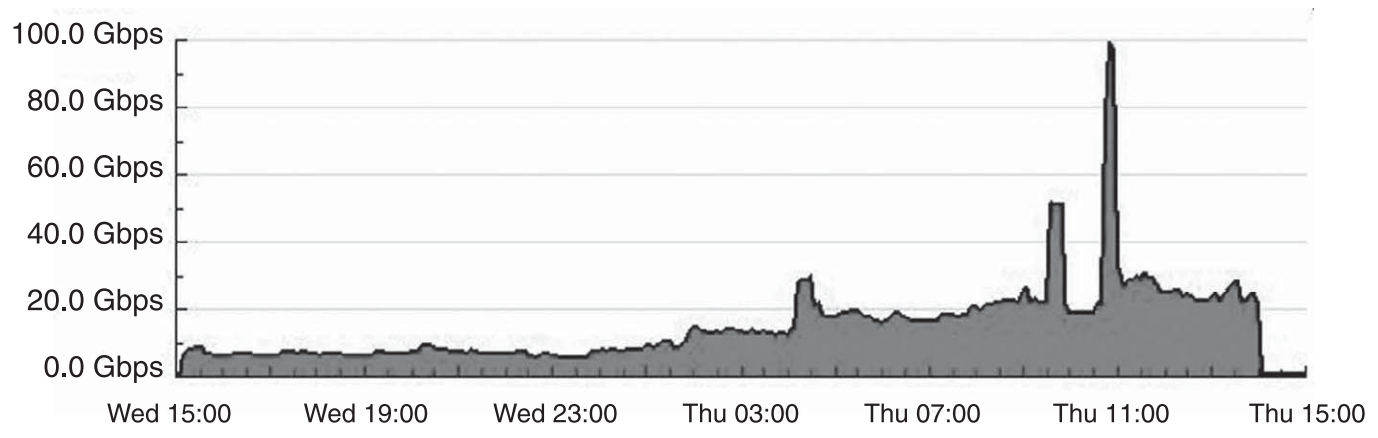

Figure 2: DDoS traffic shows a spike as a result of an attack.

highly specialised communication infrastructures that are coordinating thousands of bots to launch sophisticated attacks. This usage of more specialised tools for DDoS attacks instead of generic bots represents a step backwards in some ways.

DDoS motivation evolution

Arbor tracks over 1000 sizable DDoS attacks around the world every day. The bulk of these attacks are aimed at non-prominent targets such as home users or small Websites, or are so insignificant in size that network operators can stop them quite easily, which implies that most are motivated by spite or anger towards specific victims.

From among the many people who target the internet infrastructure, such as the root DNS servers, about two per year are able to build a botnet big enough to cause a noticeable impact.

Simple retaliations are fairly frequent, for example, against anti-spam or anti-phishing organisations such as Spamhaus or Castlecops. These counter attacks are usually run by the spammers or phishing teams that are constantly shutting down these scammer teams. Similar attacks occur in the spam and phishing underground between independent gangs competing for market space.

A small subset of denial of service attacks is financially motivated. In these, attackers threaten or demonstrate that they can disrupt an e-commerce site and demand a ransom from the victim to prevent further attacks. Banks, commercial organisations, and even ISPs have been hit by these attacks, but the most lucrative victims appear to be pornography or online gambling sites.

Arbor is tracking a series of DDoS attacks against online gambling sites at present. These attacks are orchestrated by a small set of attackers and may be related to extortion schemes, although there is no direct evidence to support this theory. Several poker and casino sites have suffered attacks lasting days and in some cases, weeks. These can cripple the victims' sites and impact their businesses directly, leading to real dollar losses.

A subset of DDoS attacks appear to be politically motivated. In these, the victim is thought to have wronged someone on the side of the attacker. A recent high-profile case is several weeks' worth of DDoS attacks suffered by the government and national infrastructure of Estonia, which coincided with street protests over Russia's history in Estonia.[1] Many assumed Russian authorities had orchestrated the attacks, but no evidence was found to support the claim. Arbor found that botnets as well as manual coordination were behind most of the DDoS attacks, and that Russian-language forums had assisted their organisation. The attacks resumed in the winter of 2007 against the Estonian newspaper, DELFI, while they were covering the trials of ethnic Russians charged with street-level crimes during the protests.

Other politically motivated DDoS attacks include those against the Russian politician Gary Kasparov and his political party during the run up to the winter 2008 elections. In this case, their Website was disabled and rendered unusable for a short period of time. No significant damage was done to the political party itself, though, so the effect of these attacks could be likened more to that of riots and protests than looting and pillaging.

Political DDoS attacks are not limited to Russian and European networks. Most of the attacks that Arbor measures through its ATLAS system are sourced from the US and they target US victims. This makes sense, given the amount of address space located in the US. In the past, DDoS attacks related to Indian and Pakistani conflicts, and more recently Iranian, have been seen.

Lately Arbor tracked attacks against Radio Free Europe in the Czech Republic and Belarus, supposedly motivated by the Belorussian government against RFE/RL for their coverage of the Chernobyl disaster anniversary.[2] Arbor has not been able to discover who ordered the attacks or if they were independently operated, even though it knows the botnet behind the attacks.

Chinese language attackers lately launched a politically motivated and

anticipated attack against CNN's website.[3] A large portion of the attack failed, and though a number of tools were released to help in the attack it clearly failed to materialise.

DDoS attack traffic and strategy evolution

In the late 1990s, the Smurf attack method, an early form of amplification attack, spread quickly and became well known. In a Smurf attack, an ICMP echo request packet is sent. The attackers forge the source address to be the ultimate attack victim's IP address, and send the traffic to the broadcast address of a network. All of the hosts on the network will do their best to reply to the traffic (sending an ICMP echo reply packet in response to every echo request packet received), but in fact they send it to the victim. In this way, a single attacker can multiply their traffic by one or more orders of magnitude.

"Anyone can encourage others to visit a site, effectively creating a request flood and disrupting a site's stability"

Some attacks work by creating network router load, sending a high rate of very small packets. These greatly inflate the workload on the router, which has to process all the packets to the best of its abilities, despite the modest bandwidth usage. Some routers will fail under such a load, causing a network denial of service.

A fairly uncommon attack is a DNS amplification attack. By using open recursive resolvers and specifically formatted queries, attackers can send a packet destined to the DNS server, pretending to be from the victim. The DNS server will reply with a grossly inflated response – sometimes 20 times larger than the query – and send this traffic to the victim. This can effectively grow a botnet's aggregate bandwidth by up to 20-fold.

DDoS mitigation strategies

It will be forever impossible to stop a DDoS attack due to the nature of the internet. Even in the absence of botnets and sophisticated tools, anyone can encourage others to visit a site, effectively creating a request flood and disrupting a site's stability. We have seen this countless times with the Slashdot effect, and also in Estonia and Korea, where an upset populace flooded victims with requests and consequently disrupted services. However, the attacks can be managed and infrastructure configurations can be changed to prevent their abuse in such an attack.

Just as the late 1990s saw a concerted effort to prevent the Smurf attack by changing default router configurations, open recursive DNS servers threaten the internet infrastructure because they can be used in DNS amplification attacks. Discovering these and getting them reconfigured is a significant challenge and little progress has been made on this front.

If the traffic is distinctly different, then it can be discarded wholesale at an ingress point with minimal disruption to normal traffic; for example, filtering all ICMP Echo Request traffic at an upstream router to disrupt a ping flood attack. Even when the attackers send random packets at the victim, the unusual traffic for that profile can be safely discarded, reducing the bandwidth.

Very little can be done at the DNS level, however, to thwart a DDoS attack unless the endpoint has access to a significant distributed hosting infrastructure such as Akamai. If this is the case, the attack traffic can be dispersed across multiple, highly connected nodes, raising the bar for the attackers. Short time to live (TTL) values on the DNS entries will not help defeat the attack unless the DNS entry is pulled entirely. However, attackers can always use victims' IP addresses as their targets.

The most successful strategy to deal with a large-scale DDoS attack is a multi-vector approach. If flooding source IPs can be identified, they can be shut down at the source or, if the ISP cannot be contacted, routing tricks can be employed to drop their traffic on the way into the network (by enforcing unicast reverse path forwarding on the routers). Depending on the attack type, defensive techniques like SYN proxies may also work. In addition, extraneous traffic can be dropped or shaped down to acceptable levels using high-speed line filtering devices. Finally, reaching out to other ISPs to help filter traffic is necessary when the attacks reach tens of gigabits per second in size, as no ISP can work with that amount of attack traffic and maintain normal traffic levels.

References

1. "Massive DDoS attacks target Estonia; Russia accused." ars technica. 12 June 2008. <http://arstechnica.com/news.ars/post/20070514-massive-ddos-attacks-target-estonia-russia-accused.html>
2. "Radio Free Europe hit by DDoS attack." Security Focus. 12 June 2008. <www.securityfocus.com/news/11515>
3. "CNN Website Targeted by DoS." Slashdot. 12 June 2008. <http://it.slashdot.org/article.pl?sid=08/04/19/1149219&from=rss>