ROBERT HASKINS

ISPadmin

UNDERSTANDING AND MITIGATING DDOS ATTACKS

Robert Haskins has been a UNIX system administrator since graduating from the University of Maine with a B.A. in computer science. Robert is employed by Renesys Corporation, a leader in real-time Internet connectivity monitoring and reporting. He is lead author of *Slamming Spam: A Guide for System Administrators* (Addison-Wesley, 2005).

rhaskins@usenix.org

IN THIS EDITION OF ISPADMIN, I TAKE a look at distributed denial of service (DDoS) attacks. No matter if you are a service provider, an organization with an Internet presence, or an individual with a high-speed Internet connection, you may be the unlucky recipient of a DDoS attack. The focus for this article will be on network-based attacks, though DDoS attacks can take many forms.

Denial-of-service attacks have been around since at least the mid-1990s. Famous DoS attacks are Smurf, Fraggle, and Ping of Death. These attacks often used spoofed IP addresses but were relatively easy to track down and mitigate.

Once people figured out filtering and other ways of mitigating DoS storms, attackers started using a distributed model for their attacks, making networks of compromised machines do their work for them. DDoS attacks, because of their distributed nature, are much more difficult to mitigate than the original DoS attacks. These attacks often take the form of SYN flooding, attempting to simply overwhelm the victim's ability to process packets. One of the first widely documented DDoS attack tools was trinoo in 1999 [1, 2].

A relatively new DDoS attack formulation is what is termed "flash crowd" attacks, where the perpetrator generates what appears to be legitimate traffic in attempting to bring down network-based services. There don't appear to be many case studies of flash crowd attacks or the tools used to perpetrate these attacks.

Background

Wikipedia defines a DoS attack as "an attack on a computer system or network that causes a loss of service to users, typically loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system." [3] It is useful, for the purposes of this article, to replace the phrase "victim system" with "victim network." The advent of high-speed data connections and raw computing power makes DoS attacks even more attractive to the perpetrators.

Motivation

When DoS attacks first started, the motivation was often for the personal, albeit nonfinancial, gain of the attacker. This motivation could take the form of:

REFERENCES

[1] Gary C. Kessler, "Defenses Against Distributed Denial of Service Attacks," http://www.garykessler.net/library/ddos.html.

[2] David Dittrich, "The DoS Project's 'trinoo' Distributed Denial of Service Attack Tool," http://staff.washington.edu/dittrich/misc/trinoo.analysis.

[3] Wikipedia entry for DoS: http://en.wikipedia.org/wiki/Denial_of_service.

[4] "How a Bookmaker and a Whiz Kid Took On an Extortionist—and Won," http://www.csoonline.com/read/050105/extortion.html.

[5] Natasha Staley, "Convergence—The Sinister Combination of Email Security Threats," http://www.ecominfo.net/arts/1007_messagelabs.htm.

[6] "A Tutorial on DoS/DDoS," http://www.lancs.ac.uk/ug/steelee/tutorial1/website/index.htm.

[7] Arbor Networks: http://www.arbornetworks.com/; Cisco Guard DDoS: http://www.cisco.com/en/US/products/ps5888/index.html.

[8] RFC 1546: http://www.ietf.org/rfc/rfc1546.txt.

[9] Srikanth Kandula et al., "Botz-4-Sale: Surviving Organized DDoS Attacks That Mimic Flash Crowds," http://nms.lcs.mit.edu/~kandula/data/killbots_paper/.

- Street credibility
- Personal vendetta
- Notoriety
- “Because it can be done”
- Curiosity/learning

Of course, the above reasons still motivate some attackers, but a new motivation has recently arisen: financial gain, as we have seen with extortion [4] and spamming/phishing [5]. Criminal DoS and DDoS attacks have become more frequent, attackers often working with organized crime, as the Internet has increasingly become a platform for conducting business. Nonfinancial reasons for DoS and DDoS attacks, meanwhile, have become less important. The growing importance of the Internet has garnered the attention of law enforcement and lawmakers, resulting in more regulation and stronger enforcement of existing laws.

DDoS Attack Profile

Distributed denial of service attacks are often SYN flood attacks from thousands of compromised hosts. This is an attempt to overwhelm the target network with millions of small packets, eating up CPU and other resources on the victim’s routers and other network-attached equipment. Of course, the additional SYN traffic uses up Internet bandwidth, causing additional headaches for the victim.(Since the packets are small, eating bandwidth is not the intent of the attacker but a side effect.)

Compromised hosts are usually high-speed Internet machines infected with malicious software that places them under the control of the attacker. The attacker makes no attempt to spoof the IP address, since such traffic would just be blocked at the edge of the network by network service providers checking the validity of the source IP address.

DDoS SYN flood attacks are difficult to differentiate from regular traffic due to the distributed nature of the attacking machines. However, with the proper tools, the distinction can be made.

DDoS Mitigation

The response to a DDoS attack depends on the size of the network you are responsible for. If you are a small network with a single upstream provider, then it is best to work with that provider to mitigate a DDoS attack. It is too easy to overwhelm small to medium-sized networks on a single network connection. The routers on such networks typically do not have the extra capacity required to fight such attacks.

Larger network operators have more choices. These options range from the drastic but low-cost (change IP addresses, null route traffic) to options that work quite well but can have significant costs (hardware and software solutions).

COMMON DEFENSIVE STRATEGIES

One of the simplest things the victim of an attack can do is to simply change change the IP address(es) hosting the service(s) being attacked. This can be quite disruptive to the operation of the victim’s business but does stop the attack quickly and efficiently. Of course, once the attackers figure out that the IP addresses have changed, they can simply change the target of their attacks. However, they might just decide to move on to another, easier victim and leave alone this victim who went to the trouble of changing IP addresses. This is similar to what Microsoft did when attackers threatened their Windows Update service [6].

Another approach is to have the upstream provider null route the victim’s traffic. Null routing traffic refers to the upstream provider(s) routing all traffic destined for the victim’s network to “dev/null” (dropping it). This very drastic move would cause the victim’s network to become totally inaccessible while their traffic is being dropped. However, from a network service provider’s perspective, at least traffic for other customers would get through. Null routing traffic might be a good stopgap measure while less drastic plans were being drawn up and implemented by the service provider.

Another approach is to manually track sources of DDoS attacks and block traffic at ingress points on the network. This option requires real-time knowledge of traffic flows, which can be gleaned from routers and other networking gear. Alternatively, commercial tools such as Arbor Networks and Cisco Guard DDoS (formerly Riverhead Networks) [7] can be used to generate this information. In this case, the attacker’s traffic flows are identified and the sources of the traffic are null routed. This is better than dropping all of the victim’s traffic, but requires very expensive commercial hardware and/or software to achieve this level of protection.

CONTROVERSIAL DDOS STRATEGIES

There are a few methods that are not used as widely as the ones outlined above, including overprovisioning and anycasting. These mitigation methods are controversial because there is no guarantee that you will have enough “overprovisioned” resources to handle the biggest attack.

Overprovisioning refers to having sufficient packet processing (routing) and network bandwidth capacity to accept any DDoS attacks that might be perpetrated against your network. This is a very costly option, as having idle routers and bandwidth is expensive and only saves money during attacks. However, this method can be useful for certain industries where excess capacity is an integral part of the business plan.

Anycasting is a methodology in which network traffic is distributed across a wide area network based upon the proximity of the source and destination of the traffic in question. The original intent of anycasting was to spread the network load across widely disparate servers to help in cases of geographically based outage. For IPv4, it is defined in RFC 1546 [8] and other standards. Anycasting is an integral part of the IPv6 protocol. This method essentially distributes the DDoS attack across a number of machines that can better handle the load. Additional capacity can quickly be added to address the attack loading.

Flash Crowd Attacks

Flash crowd (FC) attacks are one of the newest DDoS attack methods in use today. They are extremely difficult to identify and even harder to mitigate. This is because the traffic looks just like regular HTTP, DNS, and other traffic that is serviced by hosts on your network. With enough bots under their control, attackers can easily "fly under the radar" until your monitoring systems notice a problem. Once you have identified a problem, it is difficult to rectify it.

As with DDoS SYN flood attacks, unless you have a large network that has the resources to fight these attacks, it is probably best to work with your upstream provider(s) to mitigate FC attacks.

Flash crowd attack mitigation is not totally a lost cause, however. Some methods that can be used to mitigate FC attacks include:

- Requiring authorization for services
- Overprovisioning
- Anycasting

While some of the mitigation techniques are similar to those used against SYN flood DDoS attacks, one novel approach is to require authentication of all connections to services [9]. Very briefly, the approach is to authenticate users using a CAPTCHA (completely automated public Turing test to tell computers and humans apart). This approach works for certain network-based services where the end user is identifiable, such as HTTP/Web sites.

However, the authenticating-user approach doesn't work for many other FC attacks, namely DNS and similar attacks that don't require end-user authentication. Also, the CAPTCHA process is an inconvenience for users and is not appropriate for many publicly available Web sites that don't otherwise require authentication.

The surest way to mitigate FC attacks is by overprovisioning network resources and bandwidth. Anycasting could be used as a way to overprovision services. While expensive (and controversial), this approach will mitigate the attack at least to the extent possible by the additional resources and bandwidth.

Future of DDoS

DDoS attacks are going to get worse before they get better. One issue driving this is that network edges (e.g., DSL, cable modems) are increasing in speed faster than the core of the Internet. In other words, it takes fewer zombies to overwhelm the same core router today than it took a year ago. This makes it easier for attackers to do their thing with fewer machines. FC attacks will rise in popularity as regular SYN flood DDoS attack mitigation is improved.

Law enforcement is prosecuting more and more DDoS perpetrators every day; this may help to reduce the number of attacks by deterring would-be attackers. Also, as tools and methods to mitigate DDoS attacks become more sophisticated, attackers will need to find new avenues to exploit.

Conclusion

Denial-of-service attacks have been around for many years and will continue to be a problem into the foreseeable future. Having started with simple DoS attacks and moved toward distributed denial-of-service attacks, perpetrators have ready access to legions of worm-infested computers attached to high-speed DSL and cable modem connections.

DDoS attacks are going to continue to get worse, with the speed of edge networks (DSL, cable modem) increasing more rapidly than core Internet networks. DDoS attacks are here to stay until a "magic bullet" solution to them is found.

I would like to thank Todd Underwood and Rik Farrow for their input into this article.

FURTHER READING

"Protecting Networks from DoS Attacks and Malicious Traffic," http://www.allot.com/html/solutions_enterprise_dos_attacks.shtm

"Defeating DDOS Attacks," http://www.cisco.com/en/US/products/ps5887/products_white_paper0900aecd8011e927.shtml.