Distributed Denial of Service (DDoS) Attacks: Latest Motivations and Methods

An iDefense Security Report
The iDefense® Intelligence Team

Originally Published: July 12, 2007
Revised: July 11, 2008

CONTENTS

Executive Summary

A distributed denial of service (DDoS) attack aims to intentionally deprive legitimate users of a resource (or service) provided by a system, typically by overloading that system with a flood of data packets from multiple sources. Attackers normally create a denial of service (DoS) condition by either breaking down the communication channel to the server (by consuming server bandwidth), or by bringing down the server completely or impairing its efficiency considerably. This can be accomplished by exploiting a vulnerability in the server or by consuming server resources (e.g., memory, hard disk, etc.).

There are many incentives to launching DDoS attacks, but the primary motive remains quick and relatively easy money through extortion. There are several means by which attackers can leverage a DDoS against a target. The versatility of the botnet has been likened to that of a Swiss Army knife, and DDoS attacks are one of the most destructive and effective tools in the bot herder's arsenal. Today, improvements in botnet technology are making it increasingly difficult for the security industry to effectively track and neutralize these cyber threats.

Although there is very little public information concerning DDoS attacks, analyzing the few available and reliable sources helps to gain a better understanding of the current motives and methods of DDoS attackers. iDefense predicts that the number of financially motivated cyber criminals will grow. Thus, online businesses and indeed anyone with a Web presence need to be aware of the growing threat from these kinds of attacks. The cyber security plans of any organization must include deep consideration of this type of threat to adequately prepare against it. The DDoS attack that seemed a negligible risk and a mere news story on "how the other guy was attacked" could easily turn into a pressing problem that quickly becomes too difficult to handle.

Introduction

+ Definition

A distributed denial of service (DDoS) attack aims to intentionally deprive legitimate users of a resource (or service) provided by a system, typically by overloading that system with a flood of data packets from multiple sources. Attackers normally create a denial of service (DoS) condition by either breaking down the communication channel to the server (by consuming server bandwidth), or by bringing down the server completely or impairing its efficiency considerably. This can be accomplished by exploiting a vulnerability in the server or by consuming server resources (e.g., memory, hard disk, etc.).

+ DDoS Types

DDoS attacks can be classified into bandwidth depletion attacks and resource depletion attacks. While such a classification encompasses all currently known DDoS attack types, some analysts have classified DDoS attacks into additional classes.[1]

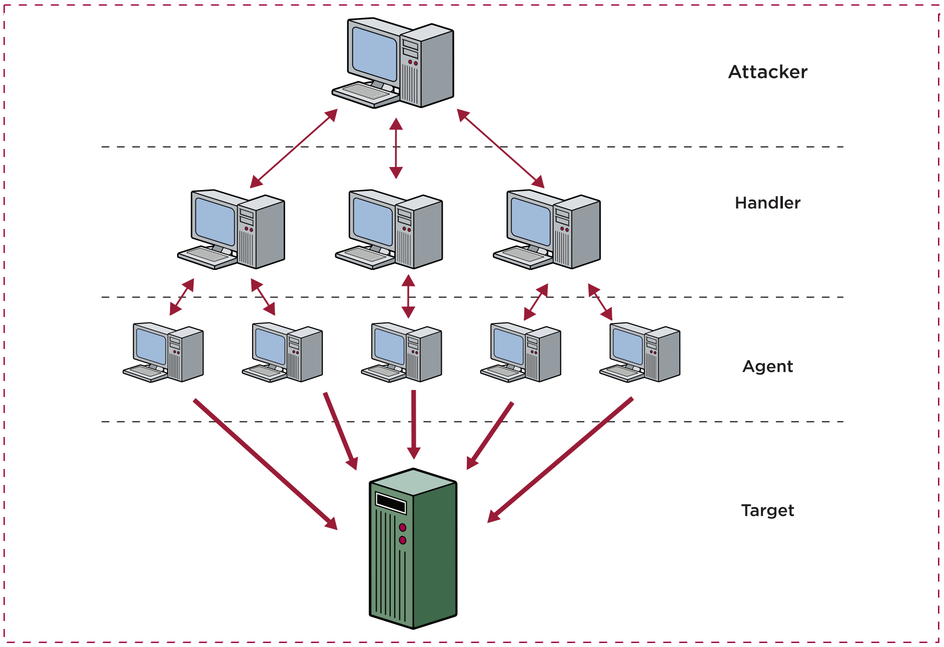
Bandwidth Depletion Attacks

Bandwidth depletion attacks seek to overwhelm the target with massive amounts of unwanted traffic, which ultimately prevents legitimate requests from reaching the affected host. Such flooding attacks are categorized as:[2]

1. DDoS Attacks (Direct Flood attacks)
2. Distributed Reflection Denial of Service Attacks (Reflection Flood attacks)

In direct flood attacks, the attacking agents send multiple packets directly to the victim. Because a large number of agents perform this action simultaneously, the bandwidth of the victim is not sufficient to handle the spike in activity. In all such attacks, the packets are generally spoofed.

DDoS Attacks - Direct Flood Attacks

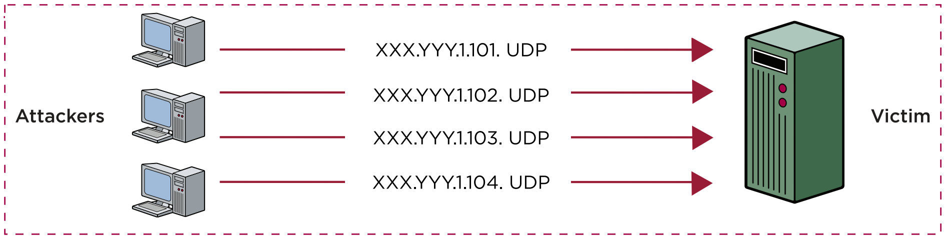


[1] Taxonomy of DDoS Attack and DDoS Defense Mechanisms, ACM SIGCOMM Computer Communication Review, Volume 34, Issue 2, April 2004.

[2] Tracing the Development of Denial of Service Attacks: A Corporate Analogy, http://www.acm.org/crossroads/xrds10-1/tracingDOS.html

In UDP flood attacks, attackers send multiple UDP packets to the victim. This large volume of UDP packets saturates the bandwidth of the victim.

UDP Flood Attack



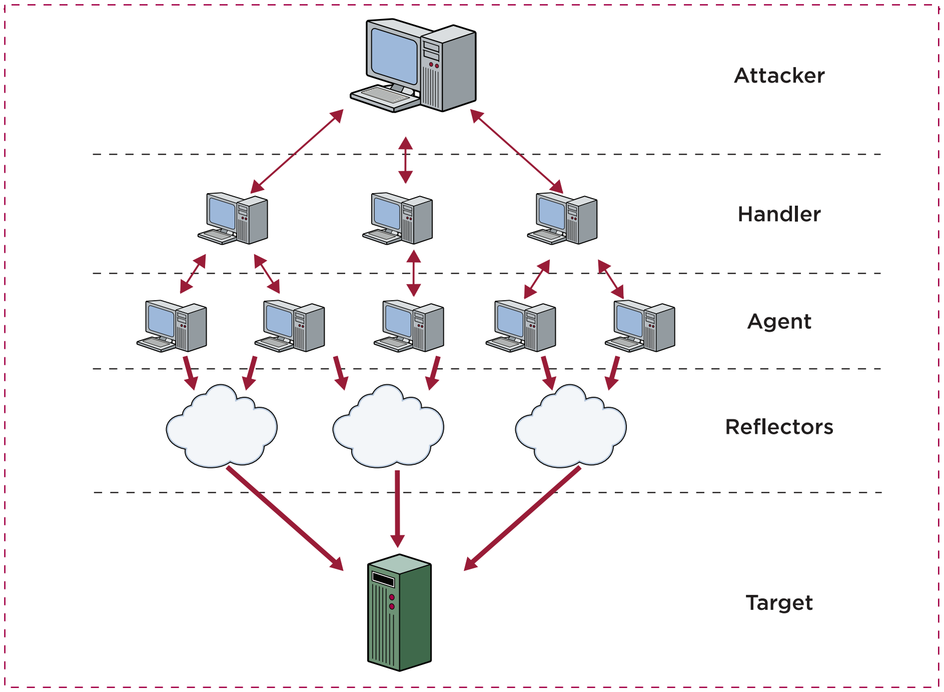
Ping Flood Attacks

In a ping flood attack, attackers send out multiple ICMP echo (ping) packets to the target and saturate its bandwidth. This could be a very effective method when the target's open port information is unknown.

Reflection Attacks

In reflection attacks, the attacker makes use of reflectors (i.e., recursive DNS servers) to "bounce" their attacks, making identifying the source of the attack even more difficult. In these attacks, the packets sent to the reflectors need to be spoofed as the victim's IP address to ensure that the reflector sends packets back to the victim's IP address.

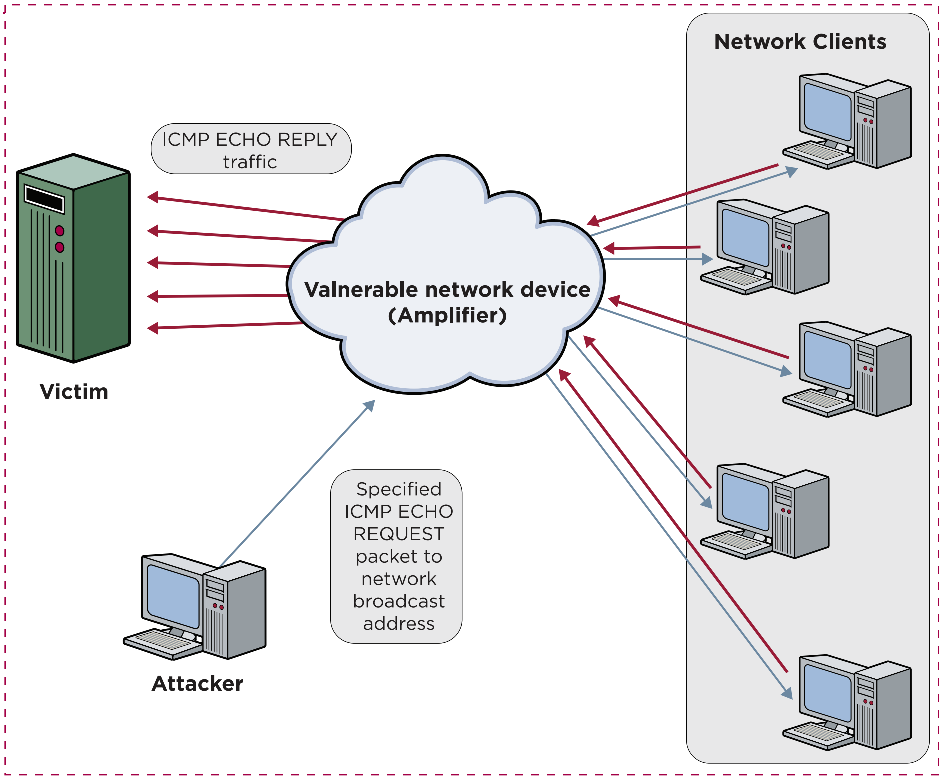
Distributed Reflection Denial of Service (DrDos) Attacks



Smurf and Fraggle Reflection Attacks

These attacks make use of poorly configured networks to reflect and amplify packets to the victim. In a Smurf attack, bots send a large number of ICMP echo packets to the broadcast IP address of a network that allows such packets from the Internet. All computers on this network reply back to the ping message, flooding the victim with a large number of reply packets. A list of such poorly configured networks can be found online.[3] In a Fraggle attack, the attacker sends UDP packets instead of TCP/IP packets.

Smurf Attack


Network Clients
ICMP ECHO REPLY traffic
Valnerable network device (Amplifier)
Victim
Specified ICMP ECHO REQUEST packet to network broadcast address
Attacker

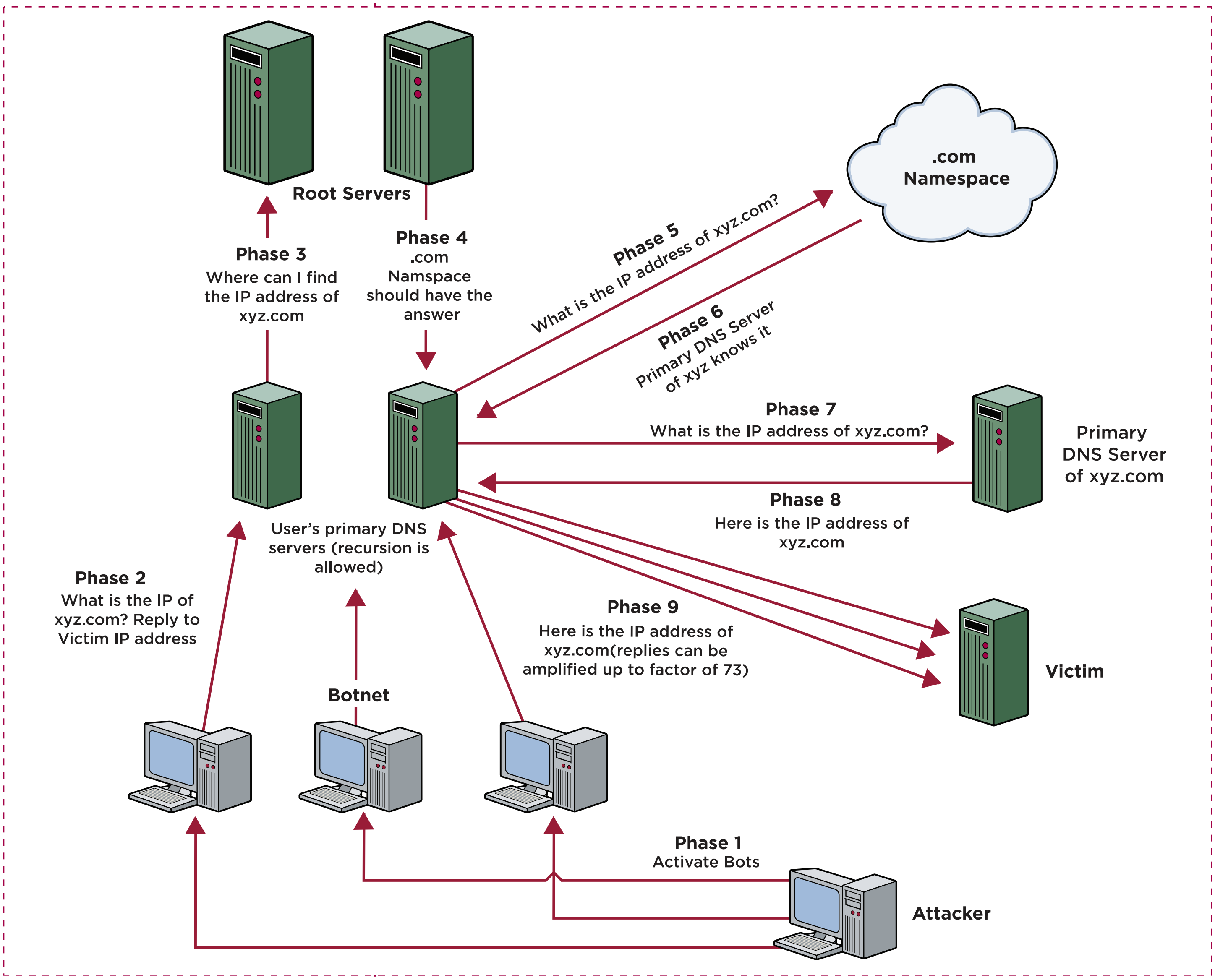
DNS Reflection Attacks

Some DDoS attacks exploit recursive DNS servers. A resolver facilitates a client's request to determine a site's domain (e.g., XYZ.com) via DNS requests. Through recursion, this type of server contacts root servers and authoritative name servers to resolve the requested name. As a rule, a recursive name server should only accept queries from local or authorized clients. However, attackers can manipulate Open Resolvers, which are DNS servers that offer recursion to non-local users, to amplify DoS attacks.

An attacker can employ a botnet to send queries with a spoofed address to an open resolver. Similar to a smurf attack, this motion triggers the resolver to send an amplified response to the spoofed address that corresponds to the targeted victim. This amplified response derives from relatively small DNS requests that soon turn into massive replies sent to the victim.

[3] Smurf Amplifier Registry, http://www.powertech.no/smurf/

DNS Reflection Attacks


Root Servers
.com Namespace
Phase 3
Where can I find the IP address of xyz.com
Phase 4
.com Namspace should have the answer
Phase 5
What is the IP address of xyz.com?
Phase 6
Primary DNS Server of xyz knows it
Phase 7
What is the IP address of xyz.com?
Primary DNS Server of xyz.com
Phase 8
Here is the IP address of xyz.com
User's primary DNS servers (recursion is allowed)
Phase 2
What is the IP of xyz.com? Reply to Victim IP address
Phase 9
Here is the IP address of xyz.com(replies can be amplified up to factor of 73)
Victim
Botnet
Phase 1
Activate Bots
Attacker

The amplification spawned in a recursive DNS attack occurs because small queries generate large UDP packets in response. In the original DNS requirement, UDP packets were restricted to 512 bytes. However, RFC specifications, in support of IPv6 and other extensions to the DNS system, require name servers to return much larger responses to queries.[4] This increased UDP payload capability is now used to launch bigger DDoS attacks with larger results.

[4] Vaughn, Randal and Evron, Gadi (2006), http://www.isotf.org/news/DNS-Amplification-Attacks.pdf

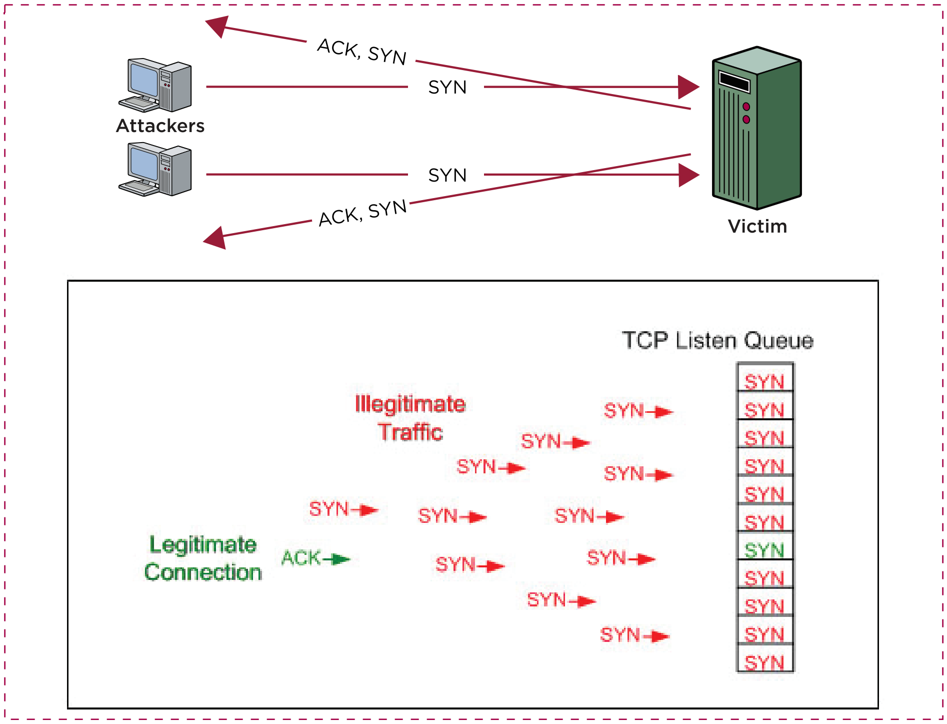
Resource Depletion Attacks

Resource depletion attacks attempt to exhaust the target system's resources; these attacks depend greatly upon internal vulnerabilities or simplistic system configurations. Such factors can be addressed to mitigate such an attack.

TCP SYN Flood Attack

A TCP SYN flood attack involves sending multiple SYN packets, often with a forged sender address, to a target in an attempt to exhaust the victim's resources. When an attacker sends TCP SYN packets with a forged address, a half-open connection is created on the receiving computer waiting for a TCP ACK packet in response from the initiator. These half-open connections consume resources on the server and limit the number of legitimate connections.

TCP SYN Flood Attack



Recursive HTTP Flood (Spidering)

This attack involves "spidering" a website via the HTTP protocol in a recursive manner to deplete resources on the targeted Web server.

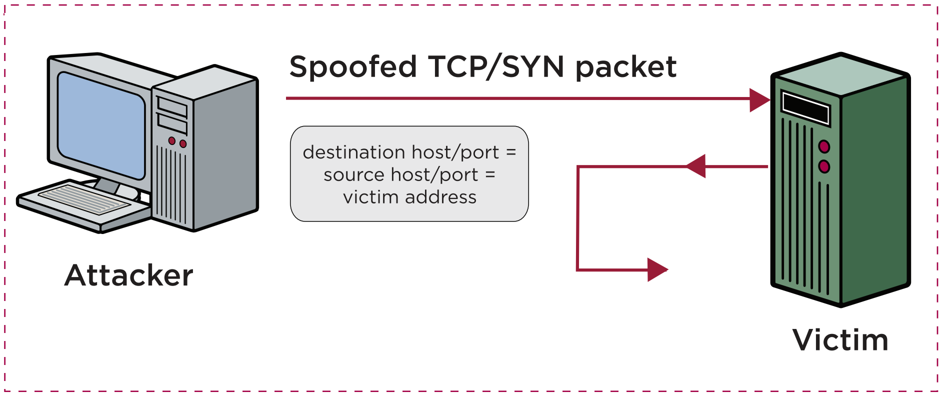
PUSH and ACK Attacks

These attacks are similar to a SYN flood but involve sending TCP packets with the PUSH and ACK bits set to a value of one. The target loads all of the data into a TCP buffer and then sends an ACK packet. When many packets of this nature are sent to a target, it may overload the buffer and cause the target to crash, effectively creating a DoS condition.

Land Attack

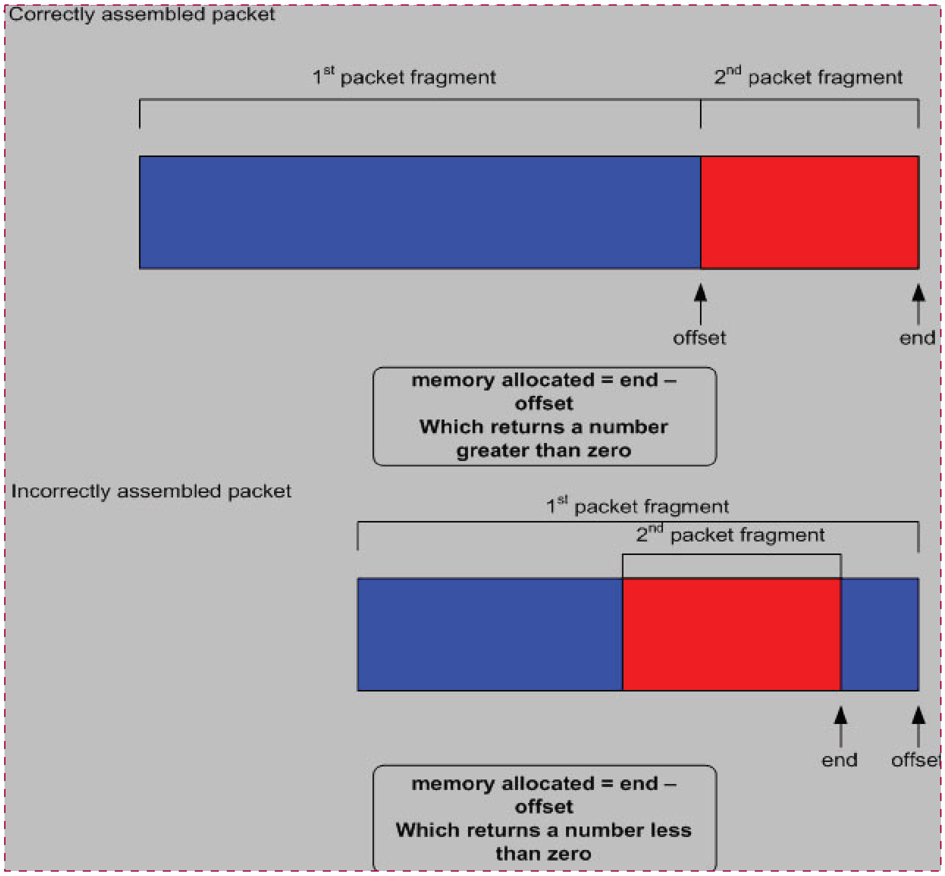
A land attack involves a specially crafted IP packet with the source address and port set to be the same as the destination address and port. This attack causes the targeted computer to continuously reply to itself, which eventually causes a system crash. However, this type of attack does is ineffective against an updated system.

Teardrop Attack (Bong and Boink)



The following diagram illustrates an older attack that attempted to exploit TCP/IP stacks that improperly handle overlapping IP fragments. This attack would result in a host crash and a DoS.

TCP/IP Stack Attack


Correctly assembled packet
1st packet fragment
2nd packet fragment
offset
end
memory allocated = end – offset Which returns a number greater than zero
Incorrectly assembled packet
1st packet fragment
2nd packet fragment
end
offse
memory allocated = end – offset Which returns a number less than zero

+ DDoS Tools

The following are some common DDoS tools:

- **Trinoo (aka Trin00)** - This tool sends out a large number of UDP packets to the victim. The large number of packets sent to the victim, in combination with the "ICMP port unreachable" message for each UDP packet generated by the victim, swamps the victim's network completely, resulting in the DDoS condition.
- **The Tribe Flood Network** (**TFN**) - This tool is able to attack victims with ICMP flood, SYN flood, UDP flood and Smurf attacks.
- **Stacheldraht** - This DDoS tool combines the features of earlier DDoS tools "trinoo" and "TFN." The interesting aspect of Stacheldraht is that the attacking agents use a "Telnet-like" program that uses encryption to communicate with the controllers.
- **Trinity** - This DDoS tool can launch ACK, establish, fragment, null, random flags, RST, SYN and UDP flood attacks. The tool uses Internet Relay Chat (IRC) as a means of communication.
- **Tribe Flood Network 2K** (**TFN2K**) - This tool was the successor to the TFN DDoS tool. Attackers use TCP/SYN, UDP, ICMP/Ping or a Smurf packet flood to target a victim.

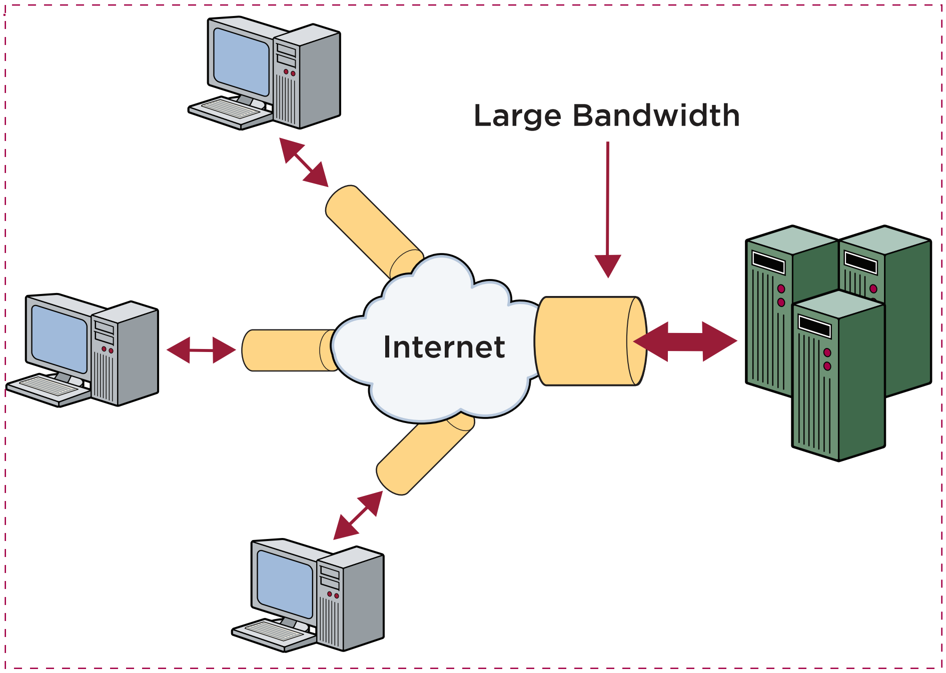
Other commonly used tools include mstream, Shaft and Omega.

Motivations for Conducting DDoS Attacks

In the past, relatively simple, single-source DoS attacks were successful in bringing down Web servers; however, these types of DoS attacks rarely occur anymore. There are many reasons for this trend.

Currently, Web servers are very powerful machines with large amounts of disk storage and processing capacity. Moreover, the bandwidth employed by modern-day Web servers is large compared to that of the past. Thus, it has become increasingly difficult for a single attacking computer to bring down a well-provisioned Web server; hence, the need for multiple sources.

DDoS Attacks against Servers



+ DDoS as Cyber Crime

Initially, attackers did not conduct DDoS attacks for monetary gain. As time passed, however, malicious actors realized the money-making potential of these attacks; thus, the goal of DDoS attackers has evolved from bragging rights to monetary gain.

Extortion

The most lucrative use of the DDoS attack is for blackmail. In these attacks, the attackers threaten online businesses with an attack unless the companies pay them. One can naturally and rightly assume that victim organizations do not reveal most extortion attacks they experience; however, the few attacks revealed to the public do illuminate the extent of the problem.

A UK-based college student's idea to make money for his fees resulted in the million dollar home page project.[5] The project unexpectedly took off and soon became a major success. On Jan. 11, 2006, an attacker subjected this site, whose whole revenue model depends on being online, to a DDoS attack after a failed extortion threat; the DDoS attack resulted in six days of down time. Because the servers were based in the US, the FBI is investigating the issue.[6]

A prime target for DDoS extortion has been the online gambling industry. The business model of this industry requires it to be online at all times. The profit from these sites is often so great that extortion payments are less costly than down time.

A Russian gang used DDoS extortion effectively in at least 50 blackmail threats against at least 30 different countries over a six-month period. The gang was finally arrested and fined, but not before they had made more than $4 million from British companies alone. This group primarily targeted online casinos and other gambling websites.[7]

Security experts believe that most companies pay, rather than report, DDoS extortionists. While some companies think that it would lead to bad publicity, others feel that paying is much cheaper than fighting the DDoS attacks; however, in the long run, bowing down to the demands of the extortionists is likely more costly. Some researchers have indicated that, although the DDoS attacker might not go through with the attack after a company pays, extortionists most often return, asking for more money, knowing that the victim is likely to pay again. Also, news spreads within the underground, and other attackers will likely soon make similar DDoS threats knowing that the victim will probably pay. Legally speaking, the law does not require companies to report an extortion attempt, and it is not illegal to pay an extortionist.[8]

Online Christmas Shopping and DDoS Attacks

A new DDoS trend seems to have emerged in 2006. DDoS attacks were stepped up against online merchants in and around the Christmas shopping season. These attacks could be by either extortion or inter-company rivalry.

On Cyber Monday, Nov. 27, 2006, a DDoS attack against CrystalTech's DNS servers shut down its systems for at least four hours. Cyber Mondays have the highest online buying activity historically, and the downtime resulted in huge losses to the online stores hosted on these servers. The company clarified that this was an unusually well-planned and professional DDoS attack, in which more than 5,000 computers took part. What is not certain is whether this was an extortion attack, whether any money was paid, and whether this was an attack against the hosting provider or specifically against one of its clients.[9]

In late December 2006, attackers subjected an online marketplace, cafepress.com, to a DDoS attack. Not much is known about the motivation for this attack. Circumstantial evidence indicating that it was timed to occur just before the shopping season suggests that this was either an extortion attack or an attempt by some competitor to impact the sales of the victim.[10]

[5] http://www.milliondollarhomepage.com/

[6] Million Dollar Homepage felled by DDoS attack, http://www.computing.co.uk/vnunet/news/2148578/million-dollar-homepage-felled, http://www.milliondollarhomepage.com/blog.php

[7] Online Russian blackmail gang jailed for extorting $4m from gambling websites, http://www.sophos.com/pressoffice/news/articles/2006/10/extort-ddos-blackmail.html, http://www.channelregister.co.uk/2006/10/04/russian_bookmaker_hackers_jailed/

[8] Extortion via DDoS on the rise, http://www.computerworld.com/printthis/2005/0,4814,101761,00.html

[9] CrystalTech hit By Cyber Monday DDoS, http://news.netcraft.com/archives/2006/12/01/crystaltech_hit_by_cyber_monday_ddos.html

[10] DDoS Attack Targets CafePress.com, http://news.netcraft.com/archives/2006/12/22/ddos_attack_targets_cafepresscom.html

DDoS and Phishing Attacks

There has been some suggestion among security researchers that DDoS attacks on major banks are in some way related to a rise in phishing e-mails. In such cases, after a bank website suffers a DDoS, phishers send customers e-mails stating that the website is experiencing some technical difficulties, advising the customers to use the alternate link provided in the e-mail to log on. The alternate link is a spoofed website that records the logon credentials of the customers. Customers unable to resolve their banking information due to a DDoS attack are susceptible to such phishing schemes.

In October 2006, "The National Australia Bank" (NAB) suffered a DDoS attack. The bank sent out warning e-mails to its customers about phishing e-mails since it was concerned that phishers would try to take advantage of this situation.[11] The veracity of the claim that the phishing and DDoS attackers were working together could never be proven in this case, but security researchers do believe that such cooperation and coordination is possible.

Irrespective of whether the phishers pay to inflict a DDoS and then send the phishing e-mails or whether they are simply opportunistic and take advantage of a DDoS attack already underway, the end result is that users are likely more susceptible to phishing techniques during such attacks.

Business Rivalry

Another common motive of DDoS attacks against online businesses is competition. Rivals have used DDoS attacks to impact the profits and even shut down competing businesses.

In March 2006, an online company in Vietnam, Vietco JSC, was severely affected by a DDoS attack. The website and the business took almost a month to recover. In this case, the company went public with the information that it was suffering from a DDoS attack and asked for legal help. In July 2006, another online company, the Nhan Hoa Hosting Company, was subjected to a DDoS attack; in September 2006, PeaceSoft's e-commerce website was brought down via similar means.[12]

Thus, in Vietnam, malicious actors used DDoS attacks as a tool to bring down the competing Web services. This trend resulted in the Vietnam CERT stating that the most popular method to damage business competition in Vietnam was through the services of hackers.

In the Jan. 15, 2007, edition of the iDefense Weekly Threat Report,[13] analysts pointed out an advertisement on the Russian hacker website "web-hack.ru," in which an attacker advertises DDoS attacks by asking the following questions:

- Have your competitors begun to squeeze [you]?
- Is someone bothering your business?
- Is it necessary for the website of your "opponent" to be put out of action?

The DDoS attacker in this ad claimed that such problems could be easily solved using DDoS attacks. The attacker bragged that he or she had control over botnets across different time zones, enabling an uninterrupted DDoS attack in countries where it is difficult to shut the botnets down.

[11] National Australia Bank hit by DDoS attack, http://www.zdnet.com.au/news/security/soa/National_Australia_Bank_hit_by_DDoS_attack/0,130061744,339271790,00.htm

[12] 2006: E-security in Vietnam shaken by crimes, http://www.vneconomy.com.vn/eng/?param=article&catid=03&id=faf86d8a1be4f2 and http://english.vietnamnet.vn/biz/2007/01/654412/

[13] iDefense Weekly Threat Report, Jan. 15, 2007, Vol. V, No. 3.

Apart from a 10-minute free test, the DDoS attacker outlined the following price structure for DDoS attacks:

- 1 hour of DDoS attack - $15
- A 24-hour attack runs from $70-$100
- More powerful DDoS projects: start at $150

Operation Cyberslam
In August 2004, the FBI discovered and arrested a DDoS group in the US.[14] In this case, organizational rivalry was the motivation for a CEO to hire members of this group to cause a DDoS attack on a rival company's site. Details from this story are particularly interesting since they illuminate the motivations of the attackers. Of the three attackers, one had from 5,000 to 10,000 bots under his control. A variant of the Agobot worm had been reportedly used to amass the bots for this army. While money was the motivation for these three attackers to commit the crime, one of them was able to subcontract this task to another hacker who agreed to do so in exchange for a free shell account. The attackers started with a simple SYN attack and then gradually raised their attack sophistication to HTTP flood attacks, culminating in a DDoS attack against the DNS providers to remain effective while the targets were working on mitigation efforts.

+ DDoS as Revenge

In May 2006, the anti-spam company BlueSecurity bore the brunt of a DDoS attack. This attack was so massive and continued for such a long time that the company ultimately closed its operations. The company tried to redirect all the traffic to its blog page, but that resulted in the blog service provider company (Six Apart Ltd, which runs the popular LiveJournal and TypePad blogging services) also being subjected to a DDoS, affecting thousands of other blog users. The DDoS attack resulted in intermittent and limited availability for TypePad, LiveJournal, TypeKey, sixapart.com, movabletype.org and movabletype.com users.[15]

Attackers subjected Spamhaus, a leading anti-spam organization, to a DDoS attack in September 2006, which led to a few hours of downtime.[16]

An online site stopecg.org, which was set up to spread information about alleged postal mail scams in Europe, has also been subjected to a DDoS several times, apparently to shut it down completely so that the scams against which it warns could continue.[17] In October 2006, a story ran on an Internet news portal in which the site's founder issued an appeal for help against the attacks.

On Jan. 12, 2007, a large number of anti-spam websites were the target of a DDoS attack by malicious code dropped by the "Storm" worm (W32/Small.DAM or Trojan. Peacomm). The malicious code was able to cause a DDoS attack on the target by using a TCP SYN flood to port 80, an ICMP ping flood and both.

[14] FBI busts alleged DDoS Mafia, http://www.securityfocus.com/news/9411
[15] BlueFrog spammer war whacks blog site, http://www.cbronline.com/article_news.asp?guid=F7152D27-E10F-433B-B1E6-57B3B48EF892
[16] Spamhaus repels DDoS attack, http://www.theregister.com/2006/09/18/spamhaus_ddos_attack/
[17] Anti-scam website hit by DDOS attacks, http://www.theregister.co.uk/2006/10/27/stop_ecg_needs_help/

In its report on this DDoS attack, SecureWorks mentioned the IP addresses of the affected websites.[18] The DDoS victims can be classified into two types. The first were security companies such as anti-spam and anti-virus companies, and the second group was related to another malicious code group.

Target IP Address	Corresponding Domain Names
67.15.52.145	stockpatrol.com
63.251.19.36	spamnation.info

Target IP Address	Corresponding Domain Names
216.118.117.38	esunhuitionkdefunhsadwa.com (Warezov)
208.66.194.155	krovalidajop.com, traferreg.com (Warezov)
66.246.246.69	shionkertunhedanse.com (Warezov)
208.66.72.202	adesuikintandefunhandesun.com (Warezov)
66.246.252.206	huirefunkionmdesa.com (Warezov)

One malicious code group initiating a DDoS attack against another malicious code group is not a recent development. Such infighting among the cyber criminal gangs has occurred for years. The latest DDoS attack against a security organization began on Feb. 13, 2007, against CastleCops.[19] The attack was massive and also affected the site's ISP. At its peak on Feb. 19, the website was flooded with almost 1 Gbps of traffic.

+ Propaganda - Hacktivism

DDoS as a tool for silencing any form of online expression to which one does not is also on the rise. One of the most recent cases involved a website that attackers subjected to a DDoS because some did not agree with the views it aired. This website reported on the events that led up to Saddam Hussein's hanging. Some of the comments and remarks made on it infuriated some of its readers, which reportedly led an attacker to subject the website to a DDoS attack.[20]

Terrorists are increasingly using the Internet in support of their physical attacks. Hence, some experts believe that DDoS as a tool for cyber terrorism is not far off.

+ Nationalism

Patriotic feelings have also been a cause for many of the recent DDoS attacks. The best example for a DDoS attack motivated by such feelings is the April 2007 DDoS attack on Estonia by Russian cyber enthusiasts.[21]

Chinese hackers and cyber enthusiasts planned a DDoS attack against CNN in April 2008. The reason for their attack was that they thought that the Western media had been unfair to them in its news reports of the situation in Tibet.[22] The most recent example is the DDoS attack against Spain just because they won the Euro 2008 soccer cup.[23]

[18] Storm Worm DDoS Attack, http://www.secureworks.com/research/threats/view.html?threat=storm-worm

[19] Massive DDoS attack KOs CastleCops, http://blogs.zdnet.com/security/?p=41

[20] Controversial Website HusseinHanging.com has been Relaunched - Sans Controversy, http://www.emediawire.com/releases/2006/12/emw494292.htm

[21] Digital Fears Emerge After Data Siege in Estonia http://www.nytimes.com/2007/05/29/technology/29estonia.html

[22] Cyberprotests planned in support of China http://news.cnet.com/8301-10789_3-9922546-57.html

[23] Spain Wins Euro 2008, Comes under DDoS Attack http://asert.arbornetworks.com/2008/06/spain-wins-euro-2008-comes-under-ddos-attack/

+ Miscellaneous

A large number of DDoS attacks can be classified under this category since in most cases there are very few details about the motivation for the attack. DDoS attacks that are leveraged without malicious intent also fall into this category. These “fun” or “practice” DDoS attacks are believed to be the largest percentage of all DDoS attacks that occur in a given time frame.

The lack of information about DDoS attacks could be due to many reasons ranging from information security to law enforcement agencies taking over the case. DNS provider ZoneEdit was subjected to a massive DDoS attack in December 2006.[24] Four of its 25 DNS servers were attacked, resulting in two days of down time. The motivation for this attack is not known.

On Dec. 2, 2006, EveryDNS, a company offering free domain name management services, was hit by a massive 400 Mbps DDoS attack.[25] This resulted in an average of 90 minutes of downtime for Web pages hosted by EveryDNS. The botnet attackers were supposedly attacking particular websites with DNS information hosted by EveryDNS. Thus, although EveryDNS was not the intended target of the attack, it suffered damage as it was the easiest vector to reach the attackers’ intended targets. The exact motivations for this attack are unknown.

The high-profile DDoS attack on root DNS servers and TLD servers on Feb. 6, 2007, has many security experts puzzled.[26] The motive for this attack is still unknown, but some researchers believe that it was a practice in preparation for something much more significant. Two of the 13 DNS root servers, the G server (maintained by the US Department of Defense) and the L server (maintained by ICANN) were temporarily crippled in the attack while the M root server (maintained by Japan) was affected to a lesser degree. Botnets sending abnormally large and bogus packets to the DNS servers were the primary tool used in this attack. Although this attack was significant, users were for the most part unaware of any incident, which some believe is a testament to the resiliency of the Internet.

[24] DNS Provider ZoneEdit Downed by Denial of Service Attack, http://www.informationweek.com/management/showArticle.jhtml?articleID=196701245

[25] EveryDNS Under Botnet DDoS Attack, http://securitywatch.eweek.com/exploits_and_attacks/everydns_opendns_under_botnet_ddos_attack.html

[26] DNS attack puts in perspective, http://www.pcworld.idg.com.au/index.php/id;1653053785;fp;2;fpid;3

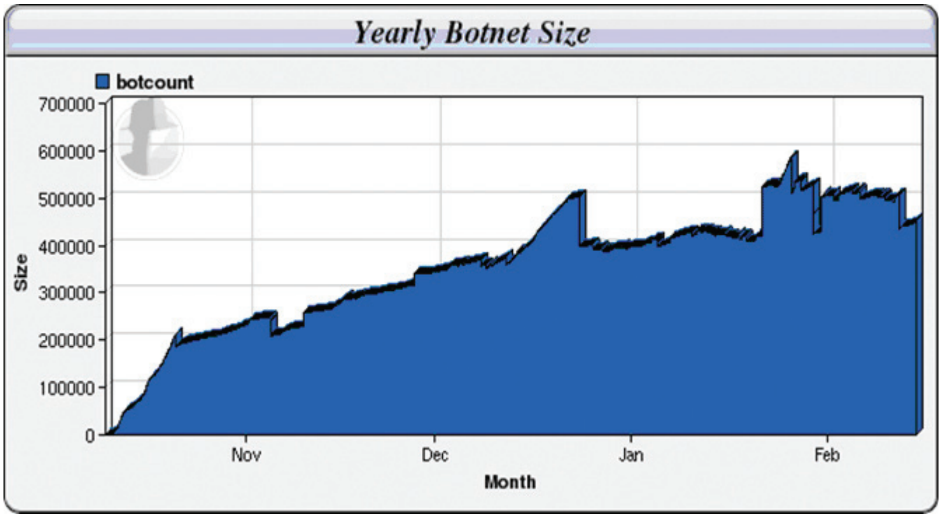
DDoS and Botnets

No discussion of DDoS attacks can be complete without a discussion about botnets. A botnets is a group of compromised, infected computers running malicious code and controlled remotely by an attacker, called a “bot master” or “bot herder.”

Attackers have used botnets for many purposes such as launching DDoS attacks, sending spam, hosting phishing sites, installing malicious code and others. The use of botnets for DDoS attacks is perhaps the most devastating activity possible in a limited timeframe, and the ratio of damage done to time spent is the highest with this kind of botnet activity. The number of botnets on the Internet is a controversial topic among security researchers, illustrating the difficulty in ascertaining the true number (and the true threat) of by botnets.

According to statistics released by Symantec Corp., an average of 57,000 active bots was observed per day over the first six months of 2006. During that period, the anti-virus vendor discovered a whopping 4.7 million distinct computers being actively used in botnets to distribute spam, launch DoS attacks, install malicious code or log keystrokes for identity theft.[27] The Dutch botnet gang convicted in 2007 had up to 1.5 million computers in its botnet alone.[28]

Feb. 14, 2007



Feb. 14, 2007

Source: http://www.shadowserver.org/wiki/pmwiki.php?n=Stats.BotCounts

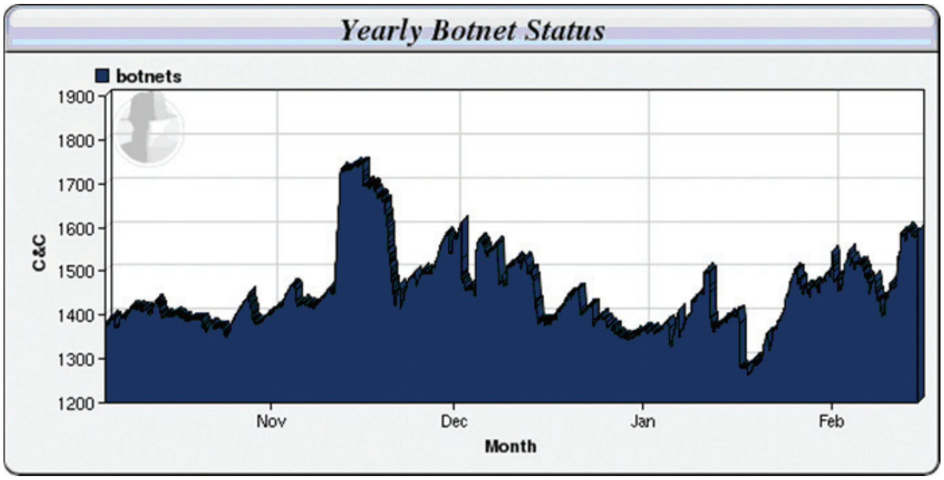
[27] Is the Botnet Battle Already Lost?, http://www.eweek.com/article2/0,1895,2029720,00.asp

[28] Dutch botnet gang facing jail, http://www.vnunet.com/vnunet/news/2172694/botnet-herders-face-jailtime

Feb. 14, 2007

Source: http://www.shadowserver.org/wiki/pmwiki.php?n=Stats.Botnets

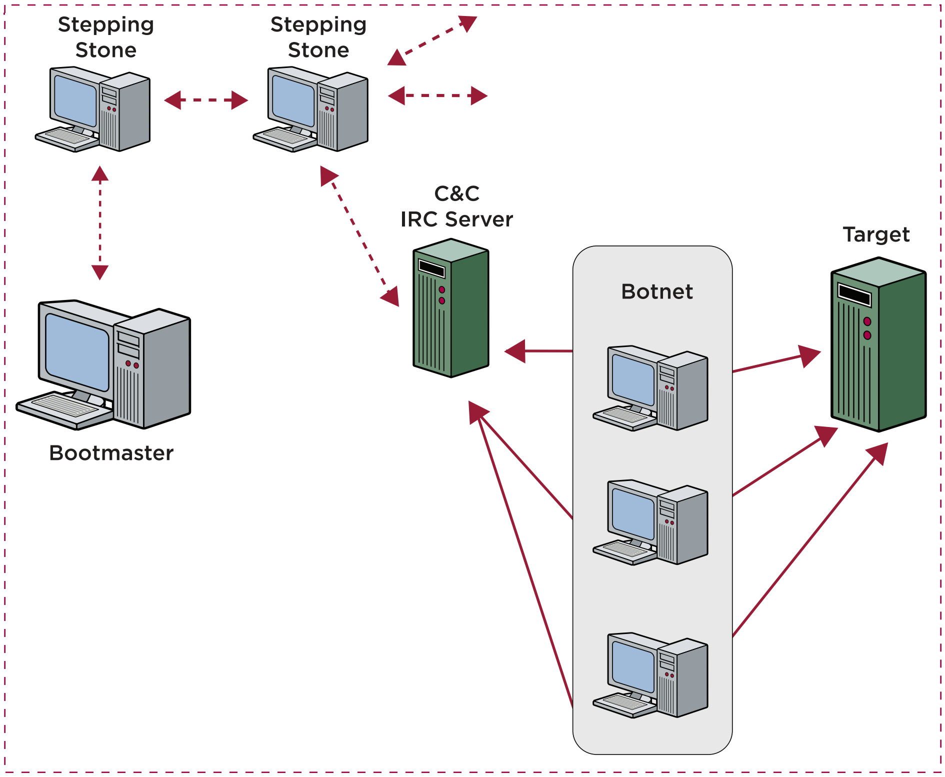
Feb. 14, 2007



The first use of bots to perform a DDoS attack was by IRC network operators. Turf battles and attempts to become the administrator of a particular channel would lead to frequent DDoS attacks. Those fights went on to develop into the DDoS attacks seen today.

Botnets make an excellent DDoS tool since they are composed of a large number of bots (in the range of thousands) that have a combined bandwidth that can inundate the large bandwidths of their victims. Added to that, the distributed nature of the botnets makes shutting them down very difficult.

Typical Botnet



Widespread use of malicious bots really began in 2004, when malicious actors released the code for AgoBot/GaoBot. Various modifications in the source code led to different families of bots. For instance, AgoBot morphed into PhatBot, FortBot and XtrmBot. Botnets can be further subdivided into smaller botnets by their controllers depending on various factors such as speed, bandwidth, processor capacity, uptime, physical location, etc. For example, when the command “http.speedtest” is issued to a PhatBot, the bot performs a speed test. To determine the bandwidth available, the bot posts a large number of packets to websites such as:

- www.st.lib.keio.ac.jp
- www.lib.nthu.edu.tw
- www.stanford.edu
- www.xo.net
- www.utwente.nl
- www.schlund.net

These kinds of tests enable the bot master to determine the speed, bandwidth at which the bot can send out packets and thus judiciously group the bot with similarly powered bots.

+ The DDoS Players

Any botnet typically consists of:

- Bot Master or Bot Herder (a human being)
- “Stepping Stones” (compromised computers)
- “Handlers” or “Masters” (compromised computers)
- “Agents/Bots/Drones/Zombies/etc.” (compromised computers)

Bot Master

The bot master or herder is the human attacker. The bot master initiates various activities, such as scanning for new hosts (in the recruitment phase) and starting and controlling a DDoS attack.

Stepping Stones

So-called “stepping stones” are compromised computers like every other computer in the botnet. The bot master logs on to the handlers via the stepping stones. This makes tracing the origin of the botnet almost impossible. Such stepping stones might be computers in far-away countries where cyber laws are non-existent or difficult to enforce. Any investigation to reveal the identity of the bot master will, in all probability, end at these stepping stone computers, which provides the bot master with an added layer of immunity.

Handlers

The handlers are the computers that communicate with and control the bots in a botnet.

Agents/Bots/Drones/Zombies

Bots are the computers that form the core of the botnet. These computers attack the target directly and have an aggregated effect on either the bandwidth or resources of a target.

+ Creating a Botnet

There are several steps that a bot master goes through to develop and strengthen his botnet, including recruitment, establishing control, propagating malicious code and directing the botnet to attack a target. The following sections explore these steps in detail.

Recruiting an Army - The Scanning Phase

The distributed nature of the DDoS attack requires distributed attackers. Large botnets are comprised of compromised computers across a large geographical area, generally spanning continents.

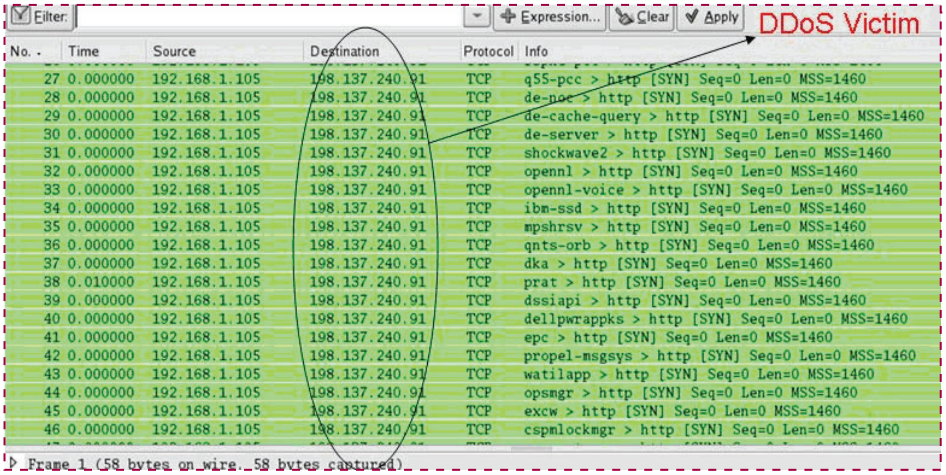
Recruiting such a large army spread over multiple countries is a challenging task. The best recruits for the botnet are computers with good Internet connectivity, enough resources and poor security. The widespread prevalence of home computers that are typically always on, are connected via a high-speed Internet connection and are generally poorly maintained has made the recruitment process easier than ever before, making these computers prime targets for expanding botnet armies.

Botnet recruiting has also evolved over the years with the development of DDoS technology. Attackers must first detect vulnerable computers. The degree of vulnerability depends on exposure to either known software vulnerabilities or zero-day exploits. Another widely exploited vulnerability is weak passwords. Weak passwords can easily be exploited through brute-force attacks (i.e., repeated password guessing).

Attackers used to perform the scanning phase for new computers manually; however, bots currently scan automatically for other vulnerable systems. When bots discover vulnerable systems, they are quickly attacked and compromised.

Internet worms are also a very effective tool to recruit agents for the botnet, since most worms can automatically find new hosts and compromise them. Their payloads currently contain a DDoS tool, allowing attackers to use compromised computers in a DDoS attack. The Code Red worm is an excellent example of this recruiting tactic. The worm attempted a DDoS attack on the White House website (198.137.240.91).[29]

Code Red Worm Packet Capture
- DDoS Attack on White House Website



```
No. .  Time      Source          Destination      Protocol Info
   27 0.000000  192.168.1.105   198.137.240.91   TCP      q55-pcc > http [SYN] Seq=0 Len=0 MSS=1460
   28 0.000000  192.168.1.105   198.137.240.91   TCP      de-noc > http [SYN] Seq=0 Len=0 MSS=1460
   29 0.000000  192.168.1.105   198.137.240.91   TCP      de-cache-query > http [SYN] Seq=0 Len=0 MSS=1460
   30 0.000000  192.168.1.105   198.137.240.91   TCP      de-server > http [SYN] Seq=0 Len=0 MSS=1460
   31 0.000000  192.168.1.105   198.137.240.91   TCP      shockwave2 > http [SYN] Seq=0 Len=0 MSS=1460
   32 0.000000  192.168.1.105   198.137.240.91   TCP      opennl > http [SYN] Seq=0 Len=0 MSS=1460
   33 0.000000  192.168.1.105   198.137.240.91   TCP      opennl-voice > http [SYN] Seq=0 Len=0 MSS=1460
   34 0.000000  192.168.1.105   198.137.240.91   TCP      ibm-ssd > http [SYN] Seq=0 Len=0 MSS=1460
   35 0.000000  192.168.1.105   198.137.240.91   TCP      mpshrsv > http [SYN] Seq=0 Len=0 MSS=1460
   36 0.000000  192.168.1.105   198.137.240.91   TCP      qnts-orb > http [SYN] Seq=0 Len=0 MSS=1460
   37 0.000000  192.168.1.105   198.137.240.91   TCP      dka > http [SYN] Seq=0 Len=0 MSS=1460
   38 0.010000  192.168.1.105   198.137.240.91   TCP      prat > http [SYN] Seq=0 Len=0 MSS=1460
   39 0.000000  192.168.1.105   198.137.240.91   TCP      dssiapi > http [SYN] Seq=0 Len=0 MSS=1460
   40 0.000000  192.168.1.105   198.137.240.91   TCP      dellpwrappks > http [SYN] Seq=0 Len=0 MSS=1460
   41 0.000000  192.168.1.105   198.137.240.91   TCP      epc > http [SYN] Seq=0 Len=0 MSS=1460
   42 0.000000  192.168.1.105   198.137.240.91   TCP      propel-msgsys > http [SYN] Seq=0 Len=0 MSS=1460
   43 0.000000  192.168.1.105   198.137.240.91   TCP      watilapp > http [SYN] Seq=0 Len=0 MSS=1460
   44 0.000000  192.168.1.105   198.137.240.91   TCP      opsmgr > http [SYN] Seq=0 Len=0 MSS=1460
   45 0.000000  192.168.1.105   198.137.240.91   TCP      excw > http [SYN] Seq=0 Len=0 MSS=1460
   46 0.000000  192.168.1.105   198.137.240.91   TCP      cspmlockmgr > http [SYN] Seq=0 Len=0 MSS=1460
▷ Frame 1 (58 bytes on wire, 58 bytes captured)
```

[29] Wireshark & Ethereal Network Protocol Analyzer Toolkit, Syngress Publications

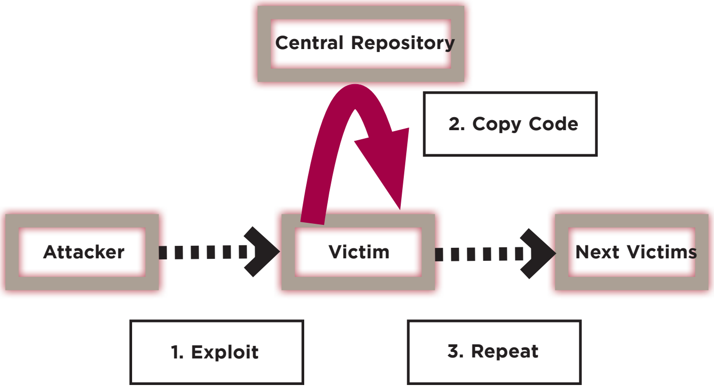
Taking Control

Once the bot herder or other compromised system has found a vulnerable system, those systems are often quickly compromised using exploits. This could either be accomplished automatically, as with the worms, or at the command of the botnet master.

Malicious Code Propagation

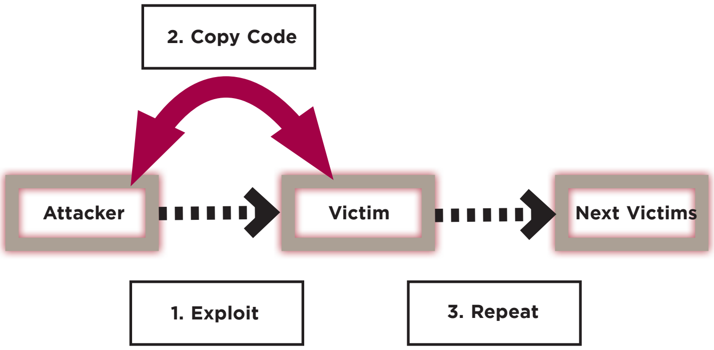
The systems that attackers compromise generally do not have DDoS tools or other malicious code installed on them, so the next step is to ensure that these computers have these tools installed. This is accomplished in the malicious code propagation step. In a CERT report, the malicious code propagation steps are characterized into three different classes:[30]

Propagation through a Central Repository



In this class, each newly compromised computer makes a connection to a central repository for malicious code and downloads from there. The central repository, for instance, could be an FTP server or a Web server. The disadvantage of this method for the botnet master is that such central repositories can be taken offline; thus, this method has fallen out of favor over the years.

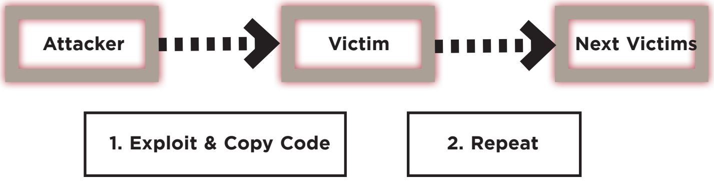
Propagation via Back Chaining



In this type of propagation, the newly infected computer pulls the malicious code from the computer that infects it. In this way, malicious code propagates through the chain.

[30] Trends in Denial of Service Attack Technology, October 2001

Autonomous Propagation

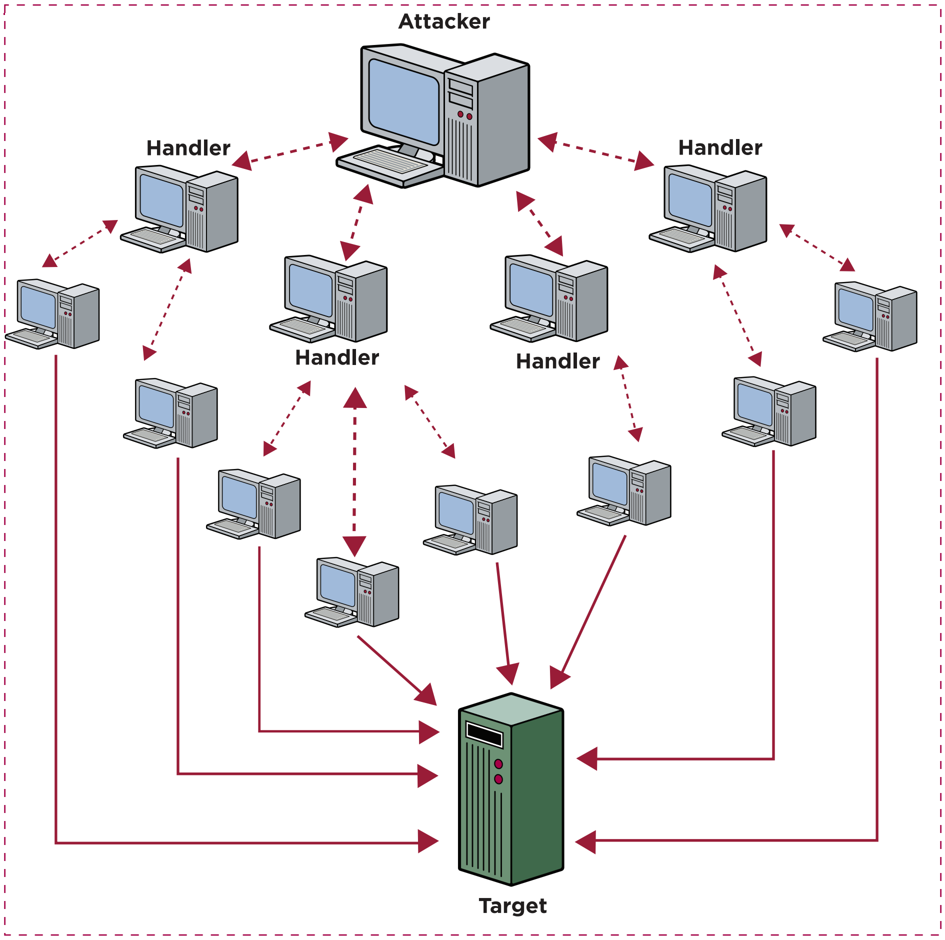


In this method, the exploit code that is used to compromise a system also has the malicious code. This makes the initial malicious code larger in size but, on the other hand, frees the newly compromised computer from having to seek the malicious code.

Controlling the Army

Controlling thousands of bots in a manner that is difficult for investigators to trace back was initially a challenge to the bot herders. The earlier botnets relied on a direct communication structure. In this structure, the IP addresses of the handlers were hard-coded into the software running on the agent computers. This was true of earlier DDoS tools such as trinoo, Stacheldraht, Shaft and others.

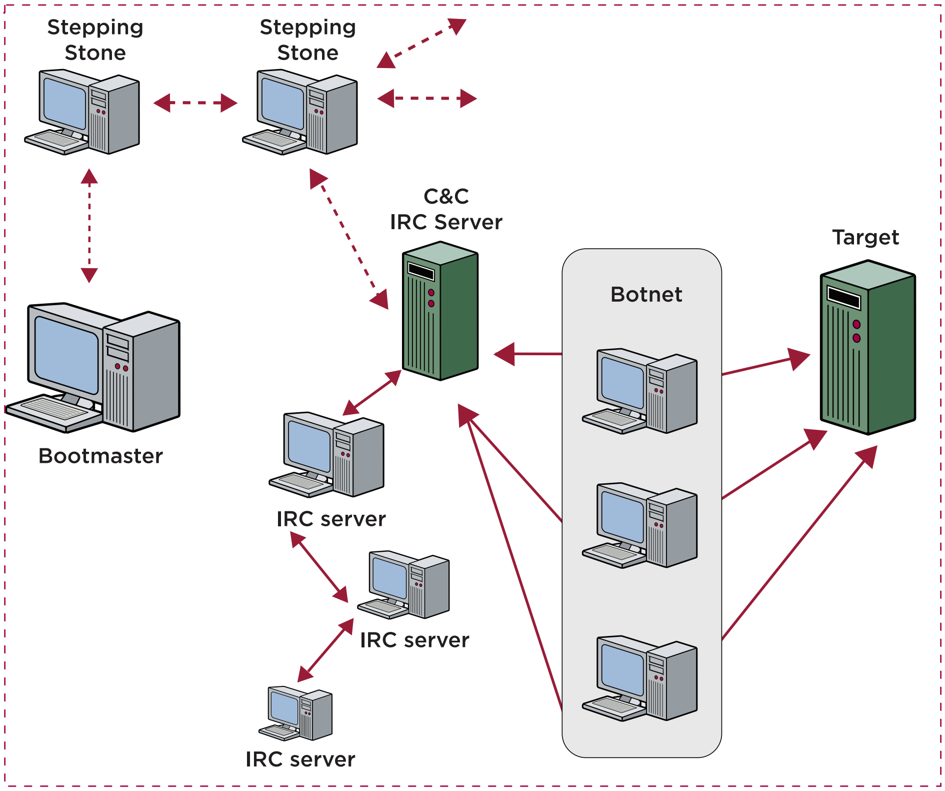
Direct Communication Model



The disadvantages inherent to using the direct communication model led to the development of the indirect communication model. In this model, there is no need for the agents to know the IP addresses of the handlers. The use of IRC servers by present-day botnets is an example of indirect communication.

In the indirect communication model, using IRC, bots join a specific hard-coded IRC channel with a password, and the command-and-control (C&C) center issues new commands to the bots through the IRC channel. This makes it easy for the botnets to continue operating because bringing down IRC servers is a difficult task, especially if the server is in another country. To make identification even more difficult, the botnet frequently shifts to a different channel.

Indirect Communication Model Using IRC



The next change seen in mode of communication was in PhatBot, which used peer-to-peer communication using the "WASTE" protocol. This makes it difficult to bring down since there is no central facility, which if brought down, would mean the end of the botnet as a whole.

Recent Advancements in Botnet Control

The use of IRC to communicate between the bots and the central C&C server is being replaced by more innovative means of communication. Some bots use HTTP requests, some use peer-to-peer communication and some even use DNS queries as means to communicate "under the radar." Analysts predict that the trend of not using IRC for communication will continue as it makes bot detection much more difficult.[31]

[31] Botnets Don Invisibility Cloaks, http://www.darkreading.com/document.asp?doc_id=113849&f_src=darkreading_node_1946

The Stration botnet and the Storm botnet are examples of HTTP communication-based botnets. Botnets following the peer-to-peer model have been found that contain no single central point of failure (e.g., the Nugache and Storm botnets).

Other advancements include the use of encryption in sending and receiving messages. This makes the task of the security analyst nearly impossible as the messages cannot be deciphered. Apart from this sophistication, botnet herders are now making use of dynamic DNS services that allow them to change the IP addresses of the computers dynamically. In some cases the DNS servers were themselves operating on compromised computers.[32]

Disbanding botnets seems a losing battle. Security experts who had success previously in disbanding them are increasingly becoming frustrated with the advances in botnet technology. Generally, security experts would volunteer their time and effort to pinpoint the botnet C&C centers and then, with the help of legal action, shut them down; however, with increasing sophistication on the botnet herders' part, this is becoming a more difficult and often futile task. Apart from the technical improvements, legal hurdles of dealing with international laws and policies make it very tough to bring down C&C centers in various countries.

[32] Is the Botnet Battle Already Lost?, http://www.eweek.com/article2/0,1895,2029720,00.asp

5 Quantifying DDoS Attacks

+ Bandwidth

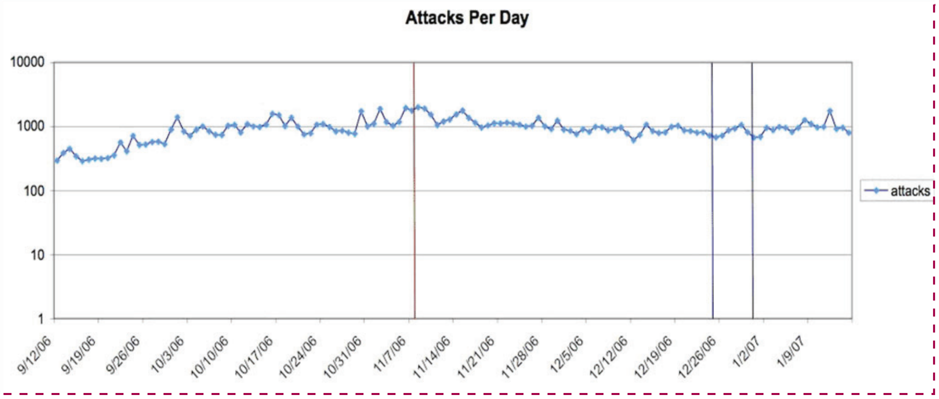
The traffic generated in DDoS attacks increased from around 3.5 Gbps in 2005 to more than 10 Gbps in 2006. The December 2006 DDoS attack on EveryDns peaked at 400 Mbps of traffic. The attack on CastleCops peaked at 1 Gbps of traffic on Feb. 19, 2007.

+Number of Attacks

Determining the true number of DDoS attacks that take place is almost an impossible job. First, the victims do not always reveal the DDoS attack; second, determining if a DDoS attack is taking place from a non-victim location is still an inexact science.

Thus, analysts are left with scattered reports from a few victims, numbers from studies conducted by research labs and the numbers revealed by the anti-DDoS industry. This result is surely much lower than the true number. Arbor networks, which has one of the leading products to fight DDoS attacks, analyzed[33] data collected from certain Internet providers for the months of October 2006 to January 2007 and concluded that the highest number of DDoS attacks in a day was 1,991 attacks, on Nov. 8, 2006, and that the daily average number of attacks during this four-month period was 954 attacks per day:

Arbor Networks



Arbor Networks

Source: http://asert.arbornetworks.com/2007/01/on-ddos-attack-activity

As mentioned earlier, there is a lack of real verifiable data and reports often conflict. Arbor Networks, in another press release, said that it was of the opinion that there were at least 10,000 DDoS cases every day.[34]

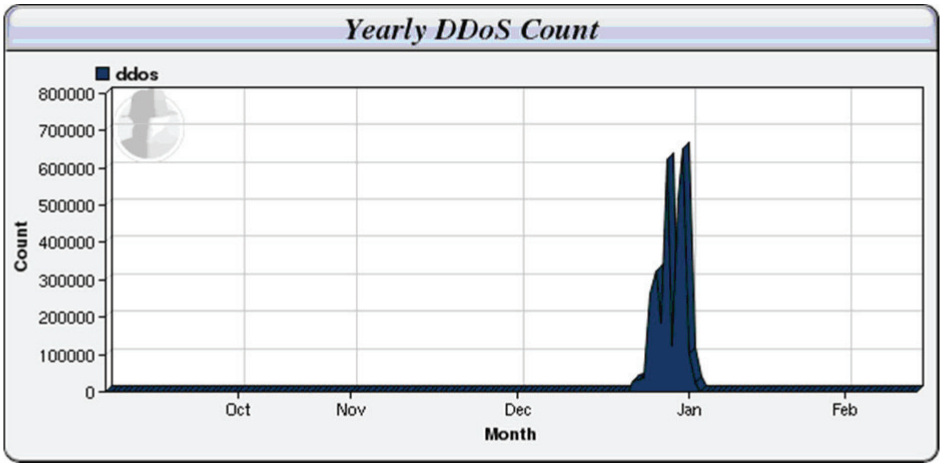
The Shadowserver Foundation is an organization of voluntary security experts who gather, track and report on malicious code, botnet activity and electronic fraud.[35] This foundation releases statistics on the DDoS attacks that it tracks. The following graphs show Shadowserver.org's figures for DDoS attacks for the years 2007 and 2008:

[33] On DDoS Attack Activity, http://asert.arbornetworks.com/2007/01/on-ddos-attack-activity/

[34] Cyber extortion, A very real threat, http://www.it-observer.com/articles/1153/cyber_extortion_very_real_threat/

[35] http://www.shadowserver.org

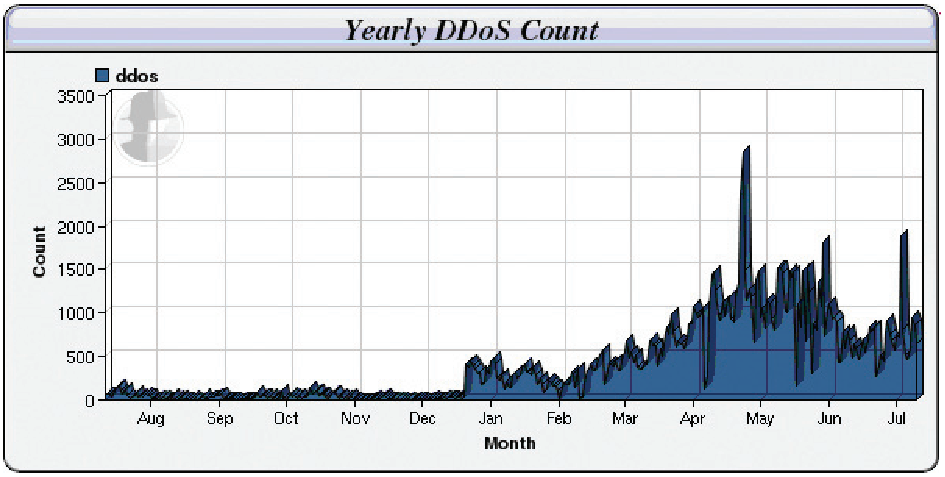
Feb. 14, 2007



Feb. 14, 2007

Source: http://www.shadowserver.org/wiki/pmwiki.php?n=Stats.DDos

July 10, 2008



July 10, 2008

Source: http://www.shadowserver.org/wiki/pmwiki.php?n=Stats.DDos

Also, during the period of November 2004 to January 2005, a Honeynet team running a honeypot observed 226 DDoS attacks against 99 unique targets.[36]

+ Financial Gain

It is difficult to determine the exact amount of money made from DDoS attacks. At best, analysts can tabulate the details of the publicly known cases in which such details were provided, keeping in mind that the figures are always an approximation and likely much lower than the true number.

The Russian gang arrested for DDoS in October 2006 made around $4 million from blackmailing online gambling and casino websites.[37] The same gang had demanded $10,000 from Canbet Sports Bookmakers. This ransom demand was turned down, and during the Breeders' Cup Races the website was subjected to a DDoS attack.

[36] Know your Enemy: Tracking Botnets, http://www.honeynet.org/papers/bots/

[37] Online Russian blackmail gang jailed for extorting $4M from gambling websites, http://www.sophos.com/pressoffice/news/articles/2006/10/extort-ddos-blackmail.html, http://www.channelregister.co.uk/2006/10/04/russian_bookmaker_hackers_jailed/

Extortionists threatened the Million Dollar Homepage Project with a DDoS attack unless a payment of $5,000 was made. This sum was then increased to $50,000. No money was paid to the extortionists in this case.[38]

+ DDoS Capabilities

Defending against DDoS attacks presumes that we know the most often used DDoS types. Again, as is the case with the subject of DDoS, there is not much public information.

In 2006, Arbor Networks reported that of all the DDoS attacks it monitored, the ranking of DDoS attacks, in terms of overall number, showed TCP-based attacks (SYN flood attacks, NULL attacks, Christmas Tree attacks) first, followed by ICMP- and UDP-based attacks.[39]

In an online posting on a Russian hacker website, a DDoS attacker offers the following kinds of DDoS attacks:

- HTTP Flood attack using URL GET/POST requests
- ICMP Flood attacks
- SYN/ACK flood attacks
- UDP Flood attacks

To get a good idea of the kind of attacks that are possible in the absence of data from live incidents, analysts can examine the different botnets for their DDoS capabilities. Since botnets are used predominantly in DDoS attacks, this approach will result in a more thorough understanding of the different kinds of attacks. A few of the DDoS commands for popular bots follows.[40]

5.4.1 AgoBot/PhatBot DDoS Commands

- .ddos.udpflood <target> <port> - Starts a UDP flood
- .ddos.synflood <host> <time> <delay> <port> - Starts a SYN flood
- .ddos.httpflood <url> <number> <referrer> <delay> <recursive> - Starts an HTTP flood
- .ddos.phatsyn <host> <time> <delay> <port> - Starts a PHAT SYN flood
- .ddos.phaticmp <host> <time> <delay> - Starts a PHAT ICMP flood
- .ddos.phatwonk <host> <time> <delay> - Starts PHATWONK flood
- .ddos.targa3 [host] [time] - Starts a targa3 flood

In a phatwonk flood, a SYN flood is started against ports 21, 22, 23, 25, 53, 80, 81, 88, 110, 113, 119, 135, 137, 139, 143, 443, 445, 1024, 1025, 1433, 1500, 1720, 3306, 3389, 5000, 6667, 8000 and 8080.

5.4.2 SdBot DDoS Commands

- udp <host> <# of packets> <packet size> <delay> [port] - Starts a UDP flood
- ping <host> <# of pings> <packet size> <timeout> - Starts a ping flood
- ddos (syn|ack|random) <ip address> <port> <packet size> - Starts a packet flood attack with the given options

[38] Million Dollar Homepage felled by DDoS attack, http://www.computing.co.uk/vnunet/news/2148578/million-dollar-homepage-felled, http://www.milliondollarhomepage.com/blog.php

[39] On DDoS Attack Activity, http://asert.arbornetworks.com/2007/01/on-ddos-attack-activity/

[40] Phatbot Trojan Analysis, http://www.lurhq.com/phatbot.html; PhatBot:Command Reference, http://www.stanford.edu/~stinson/misc/curr_res/bot_refs/phatbot_commandref.html

The Law

Since the individual zombies reside physically in various countries, it is a daunting task to use legal means to shut down the entire botnet. Laws governing cyber crime vary across countries, and law enforcement officials might find it very tough prosecuting attackers operating from overseas. This distributed aspect of the botnets gives it a degree of immunity from law enforcement. Nevertheless, there has been increased cooperation among various countries in shutting down botnets. A few examples and details of successful prosecution follow.

The Russian DDoS cyber criminals jailed in October 2006 were each sentenced to eight years in prison and a $3,700 fine.[41] The person responsible for the Akamai DDoS in 2004 was charged in the end of 2006. He faces up to two years in prison, to be followed by one year of supervised release, and a $100,000 fine.[42]

From a legal perspective, there has been increased awareness among lawmakers to come up with new laws that can deal specifically with DDoS threats and their instigators. For instance, the UK passed a law in November 2006 that made it an offense to launch a DDoS attack, and a conviction could carry a maximum prison sentence of 10 years.[43] This was the fallout of a court case in which an attacker, who sent five million e-mails to a mail server, could not be sentenced due to then existing laws in the UK.

To increase deterrence, it is vital that more DDoS attackers be prosecuted and punished for their actions. This requires more participation in the form of reporting from businesses that have been threatened with a DDoS attack or have undergone an attack. Until and unless victims do not report the crime, there is very little law enforcement can do.

[41] Online Russian blackmail gang jailed for extorting $4M from gambling websites, http://www.sophos.com/pressoffice/news/articles/2006/10/extort-ddos-blackmail.html, http://www.channelregister.co.uk/2006/10/04/russian_bookmaker_hackers_jailed/

[42] Florida 'botmaster' charged with Akamai DDOS attack, http://www.theregister.com/2006/10/24/akamai_ddos_attack_man_charged/

[43] UK bans denial of service attacks, http://www.theregister.com/2006/11/12/uk_bans_denial_of_service_attacks/

Conclusion

iDefense predicts that the number of financially motivated cyber criminals will grow. Thus, online businesses and indeed any organizations with a Web presence need to be aware of the growing threat from these kinds of attacks. Cyber security plans of any organization must include deep consideration of this type of threat, and organizations must familiarize themselves and their security personnel on the current motives and methods of DDoS attackers. The DDoS attack that seems a negligible risk and a mere news story on "how the other guy was attacked" could easily turn into a pressing problem that quickly becomes too difficult to handle.