GENERAL ANALYSIS OF THE ECONOMY BEHIND *DDoS* ATTACKS

Ciprian Andrei TAIS[*]

Abstract. *Distributed Denial of Service (DDoS) attacks are large-scale, coordinated attacks on the availability of services of a victim system or network resource, launched indirectly through many compromised computers on the Internet, forming a massive botnet. DDoS attacks and botnets have become an increasing security concern in today's Internet and cost the economy world-wide billions of dollars. This paper focuses on DDoS attacks, solutions for protection against them, strategies and economical implications that these attacks have and the botnet structures that are being constructed in order to initiate DDoS attacks. We have focused on the economical aspects of botnets, as well as the underground economy that has emerged to support the building, selling and buying of botnet attack tools, an economy that was named botconomics.*

Keywords: *Distributed Denial of Service attacks, Internet, Security, Botnets, Botconomics.*

1. Introduction

Distributed denial of service (DDoS) attacks first appeared in the news in February 2000 and have maintained a high media profile ever since – a fact made evident by the following headlines:

"Amazon.com, eBay, Yahoo Crippled by DoS Attacks" – February 2000

"Massive DDoS Attack Hits Internet DNS Root Servers"– October 2002

"MyDoom Becomes the Internet's Fastest Spreading Worm Ever"– January 2004

"Top Threats in 2006: SQL Slammer & Blaster Worm"– October 2006

[*] Hyperion University of Bucharest, 169 Calea Călăraşilor, St., Bucharest, Romania; Polytechnic University of Bucharest, 313 Splaiul Independenței St., Bucharest, Romania; email: ciprian.tais@gmail.com

"Storm Worm Rages Through Internet Over the Weekend"– January 2007
"Cyber Attacks on Estonia"– May 2007.

Victims of these crippling and widespread Internet-based attacks include Internet service providers (ISPs), enterprises and broadband subscribers alike. To make matters worse, Internet service subscribers are often unknowing participants in the proliferation and execution of many such attacks. This occurs when hackers covertly pirate subscribers' high-speed connections and compromise their PCs – turning them into zombies that form a huge army of malicious botnets. Remotely controlled by hackers, these botnets wreak havoc throughout the Internet by executing all kinds of malware and DDoS attacks. According to recent studies made by different security organizations [1], botnets and DDoS attacks are the top concerns of today's Internet services providers. Together with large-scale malware, these threats can severely compromise an ISP's core equipment, resources and business-critical IP services.

Emerging technologies introduce additional vulnerabilities that put today's networks at even greater risk of security threats. Service providers around the world, eager to obtain the operational and competitive advantages of new technological innovations, are accelerating their deployment of networks built on high-speed fiber optics and IP-based services, such as MPLS, IPTV, VoIP and VPN. Although there clearly is a broad range of benefits available from these new networks and services, there is an equally broad range of security threats that can seriously curtail or even wipe out those benefits. Service providers recognize that if they are to realize the promise of next-generation IP-based services, they must understand the nature and power of their cyber-enemies. Armed with this knowledge, providers can deploy the necessary solutions designed to defend their networks and services from the threats that are out there today – and the ones that surely will emerge in the future.

2. Strategies and economic implications of DDoS attacks

The primary aim in a DoS attack is to render the target system completely useless. This is usually done using one of two strategies. The first strategy, a flood attack, involves flooding the target with spurious

traffic and overloading it. Consequently, any legitimate traffic, which becomes a fraction of the total traffic, is denied service. For example, a legitimate buyer may not be able to complete a transaction at Amazon.com because the Amazon servers are too busy processing illegitimate information requests. The second strategy, a logic attack, exploits known software bugs on the target system in an effort to take it offline. Some common names given to flood attacks include ICMP attack, SYN attack, Smurf attack and Fraggle attack. Some common logic attacks are known as Ping of Death, Teardrop, Land and Chargen. Clearly, these Internet-based attacks are not only limited to commercial enterprises but could easily cripple any communications infrastructure that uses the Internet for its operation. A DDoS attack has the same impact on a target as does a DoS attack. A DDoS attack differs in that the spurious traffic originates from multiple machines on the Internet versus originating from a single machine as in a DoS attack. Consequently, DDoS attacks have a much quicker impact and are more difficult to fight. From an implementation perspective, the attacker generally hunts for insecure user computers and impregnates them with either "zombie software" or "handler software." Both pieces of software enable the attacker to take control of the impregnated computers at a later time. Zombie software is used to directly attack the target, while Handler software is used to control the zombies. This complete process – from initial search for insecure computers to their transformation into handlers and zombies – can be highly automated. How Big Is the Impact? One method to gauge the impact of DDoS/DoS attacks is to look at the financial damage caused by such attacks. Financial losses from a 24 hour outage at a brokerage firm are estimated at $156 million. Clearly, as organizations become more dependent on the Web for revenue generation, the financial stakes will continue to grow higher. Consider the rate at which the recent Code Red worm spread. Taking advantage of vulnerability in Microsoft's IIS product, these worms had infected more than 350,000 computers worldwide within 14 hours. If these worms were recruiting zombies, within 14 hours the hackers would have had an army of 350,000 slave computers – sufficient to successfully launch a devastating DDoS attack against any known network. Another approach to estimate the potential impact is to understand how widespread these attacks are. In 2000, 36 percent of the respondents to CSI/FBI annual surveys indicated experiencing DDoS/DoS attacks, up from 27 percent in 1999. The first academic study on this subject [2] suggests that as many as 4,000 DDoS attacks happen across the Internet each week. What's more alarming in this study are the estimated attack rates. Studies have shown that an attack rate

of 500 packets per second is enough to overwhelm a commercial server. When specialized firewall designs are used to resist such attacks, a flood of 14,000 packets per second can disable the server. Forty percent of all attacks in the Moor, Voelker and Stefan study had estimated attack rates of 500 packets per second or higher, and 2.4 percent of all attacks could break through highly tuned/optimized firewalls. Until now, we have talked about the impact of such attacks only on the commercial sector. Numerous civil and federal communication systems are equally vulnerable to such attacks.

3. Statistical data of DDoS attacks

Deliberate attacks on service provider networks are – and will continue to be – a major headache for ISPs and their customers. The U.S. Federal Bureau of Investigation (FBI) estimates that computer crime costs American companies alone a staggering $62 billion a year.

According to data received from a survey [13], there has been a 140 percent increase in the size of the largest detected DDoS attack over the last three years. In 2006, the largest observed sustained attack was 24 Gbps, compared to 17 Gbps in 2005. Thirty-six percent of the surveyed ISPs reported that they had observed attacks of over 1 Gbps in 2007. This is significant because most Internet backbone links are 10 GB and enterprise circuits are multi-gigabit in size.

The charts below (Fig. 1 and Fig. 2) were taken from the "Worldwide Infrastructure Security Report" [1].

The figure 1 shows the sustained attack size of the largest attacks from 2001-2006. As seen, the attack size is increasing exponentially in time because the magnitude of the attacks is also increasing considerably. Both the biggest largest attacks (22 and 24 Gbps) made in 2006 reported to have been DNS reflective attacks, which is a newer trend in DDoS attacks. This issue shall be discussed later in this paper as a type of a "degradation of service" attack, rather than the normal "denial of service" attack.

The figure 2 shows the largest attacks observed in the last 12 months. One can easily distinguish two peaks rising above 20% of the total number of attacks which classify the DDoS attacks in two big categories depending on the target of their attack: small attacks usually targeting local ISPs or routers which have a size of less than 100 Mbps and the big attacks that usually target commercial sites and global ISPs that jump to a scale of one to four Gbps.

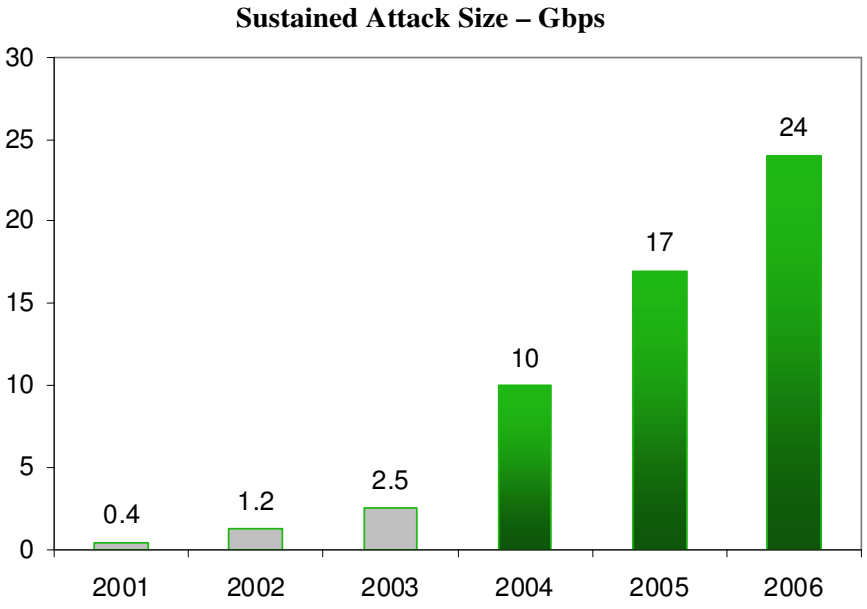

Figure 1. The largest botnet attacks from the 2001-2006 years.

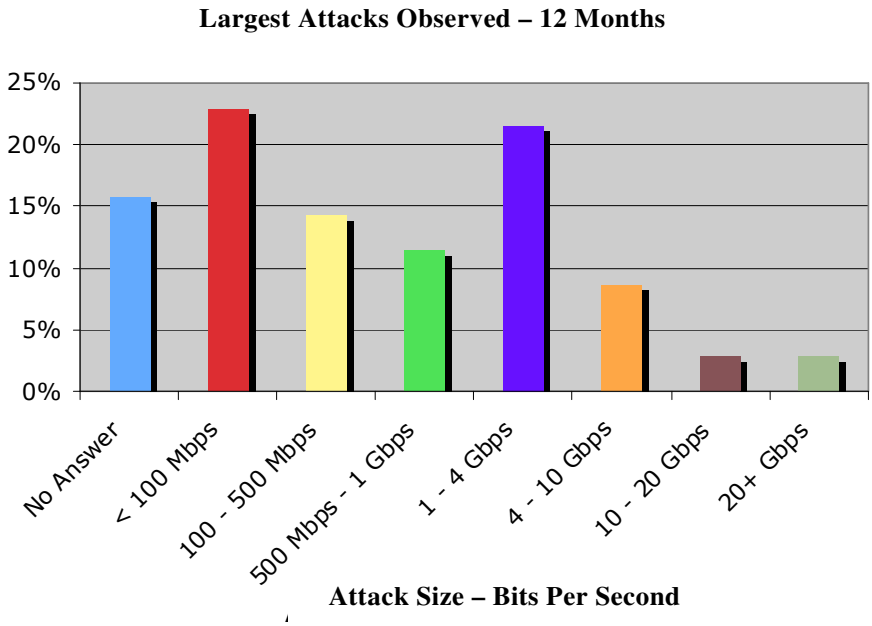

Figure 2. The largest botnet attacks observed during 2006 year.

Additionally, Arbor research conducted from September 2006 through August 2007 [1], a period of 321 days, revealed that there were 362,394 DDoS attacks – an average of 1,128 attacks per day.

4. Botnet Patterns

Botnets, a major problem identified by ISPs, continue to plague the Internet. In fact, botnets are considered a growth sector within the attacker underground, with new code bases, uses and operators frequently appearing. For ISPs and network operators, botnets represent a multi-faceted threat. First, they remain a major source of DDoS attacks. Secondly, they have become a serious source of spam email traffic, which burdens the email processing infrastructure of all providers. Finally, the scanning and attack activity of a large botnet can disrupt normal network operations and cause outages. For all these reasons, most ISPs are concerned with large-scale malcode, most commonly embodied in botnets.

ISPs observed that botnets were used for:

– DDoS attacks (71 percent);
– Sending spam (64 percent);
– Parts of phishing systems (37 percent);
– Open proxies (34 percent);
– Storing ID theft information (16 percent);
– Other (6 percent).

According to survey respondents, these new botnets exhibited the following characteristics:

– They were smaller but more targeted, effective and organized.

– They employed protected and deployed encryption, peer-peer and MD05 SHA-1 [14] counter reconnaissance.

– They were distributed in nature, making the attacks more complicated and the location of the master controller more difficult.

Recent ASERT research [13] shows that botnet server lifetimes fall into a very specific pattern commonly referred to as a long-tailed distribution. The data from this research clearly indicates that most botnet servers – nearly 65 percent – are found and disabled within the first day of their operation. This suggests that there are very effective networks for gathering information about new botnets and sharing it with the right network or system operators. It is this communication that leads to disabling the host with the botnet IRC server. Overall, if a botnet is able to make it past the first day, it has a fair chance of surviving for several months or more. Research also shows that some botnets remain active for nearly a year. The fact that known botnets can operate for this long should be a call-to-arms for all ISPs.

Apart from a few bursts of activity, between 10 and 20 new botnet servers are found every day. Factoring in the number of such servers disabled daily, approximately 1500-1800 botnet servers are currently active – a number that is slowly rising. This trend is likely to continue as the number of IRC botnet servers keeps growing for the foreseeable future.

5. Botconomics: The Underground Economy of Botnets

There are many reasons for a miscreant to initiate a botnet attack. Some attacks have religious or political motivation behind them. Some are simply ego-driven as professional hackers or script kiddies compete to see who can cause the most damage by infiltrating the biggest and most secure sites. With that said, the most serious attacks usually have financial goals in mind. Extortion, stealing money from compromised online bank accounts, luring innocent users to phishing sites, the illegal use of stolen credit cards – these are common results of botnet attacks. In fact, there is an underground economy emerging to support the building, selling and buying of botnet attack tools, an economy that Arbor Networks has coined "Botconomics".

Botconomics is fueling the rapid growth of the botnet world. The simple motivation behind the rise in botnets is money. Years ago, hackers had to be technically savvy and know how to write code to initiate an attack or create a botnet. Today, they can buy and sell that code in online markets, which are likened to traditional underground markets. In fact, there are such online communities available to anyone who earns their trust usually demonstrated by getting a certain quantity of stolen credit cards, bandwidth or email addresses to build street credibility. ASERT [13] has uncovered numerous sites which boldly market their botnets and booty. Here are some examples of common advertisements and related costs: Often these disreputable sites advertise their botnets via discreet email campaigns. A recently discovered email [15] touted botnet servers that provided excellent ping and uptime, rotating IP addresses, different ISPs, intuitive user interface [16][17] and online technical support:

– .net Domain Names: 0.05 $
– nasa.gov Domain Names: 0.05 $
– Proxies: 0.5-3 $
– Credit Cards: 0.5-5 $
– Email Passwords: 1-350 $

– Email Addresses: 2-4 $/MB
– Compromised UNIX Shells: 2-10 $
– Social Security Numbers: 5-7 $
– Mailers: 8-10 $
– Scams: 10 $/week
– Full Identity: 10-150 $
– Bank Accounts: 30-400.

6. The Next Generation of attacks

While the Internet community is still struggling with DoS and DDoS attacks, the hackers are busy creating even smarter versions. Consider new types of DoS attacks that do not result in denial of service but cause degradation of service. These attacks are even more difficult to find because the target server is never shut down completely but is "always slow". The server owner notices increased bandwidth cost for the increased traffic, without any accompanying increase in revenues. Another version of the attack involves "pulsating zombies" [8], which are active only on a periodic basis in short bursts versus normal zombies that are always on. It is much harder to detect them because the pulsating zombies are never active for sufficiently long durations. Yet another new type of attack involves "reflectors", which are essentially IP hosts that return a packet in response to a packet being sent to them. For example, the sent packet could be a SYN packet and the returned packet could be a SYN acknowledge packet. All Web servers, DNS servers, and routers are reflectors. In this attack, the zombies (a couple of hundred) send packages to reflectors (hundreds of thousands) after spoofing the victim's source address. The reflectors think the packets are coming from the victim (because the victim's source address was spoofed) and end up sending reply packages to the victim. These attacks are more potent because they can be massively scaled-up by using ubiquitous network devices (routers, Web servers, DNS servers etc.) versus regular attacks that require more effort at spotting zombies and handlers.

In the figure 3, taken from McAfee Avert Laboratories [3], a normal and legitimate client contacts his local DNS server and requests him the IP for bob.com. The local DNS server does not have this IP, so he interrogates the ".com" DNS server asking him about bob.com's IP. The ".com" server responds, giving him the bob.com DNS server. Knowing all this procedure,

an illegitimate attacker could pretend to be bob.com DNS server and, when the local DNS server requests the bob.com IP from its own DNS server, the attacker sends a false message before the bob.com DNS server's response, giving the local server a false IP for bob.com. Therefore, the DNS server returns to the client the attacker's false IP, and so, bob.com has been spoofed by the attacker. The client could then contact the attacker believing it is bob.com, and more of it, if the attacker has an identical visual web page as bob.com had, which in most of the cases it does happen, the client will give his identification to the attacker. In this kind of attack, the client has done nothing wrong and, therefore, the "fault", if we could find a "fault" at someone, would be on the local DNS server's side, and the client could theoretically accuse the DNS server of not giving him the right IP address. Therefore, these kinds of attacks are harder to spot than normal attacks because it involves more than the security of a single machine or server.

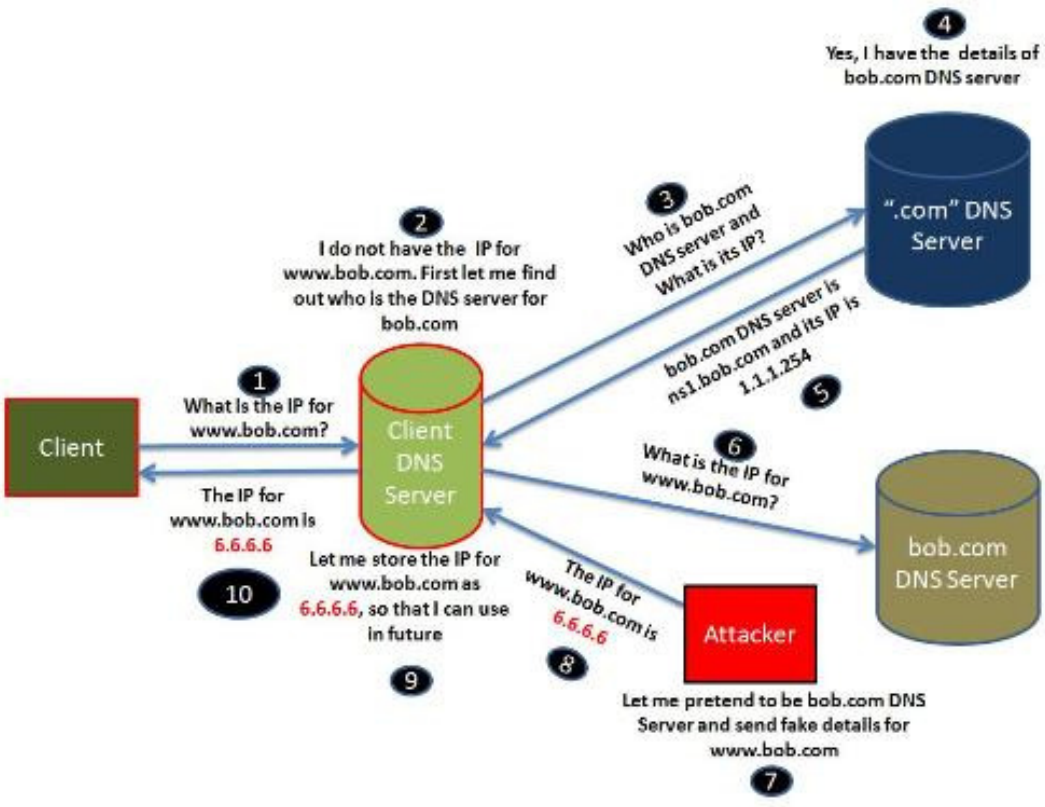

Figure 3. A very simple DNS attack scenario where a client is trying to look for the IP address of bob.com.

7. Tackling DDoS

There are three aspects to tackling DDoS: detection, identification of the source, and solution. The toughest part of reliable detection is separating normal traffic from spurious traffic. Several algorithms are used for detection, including signature analysis (comparing traffic against a known attack signature), protocol anomaly analysis (looking for traffic that is stepping out of an expected behavior pattern), and trend analysis (e.g., abnormally high traffic in the middle of the night). Identification of the source involves backward tracing the path of attack and identifying the key devices (routers, servers etc.) that are responsible for the spurious traffic. The solution aspect is multidimensional and may involve filtering the traffic and/or the complete/partial shut down of a certain network path. Commercially available solutions take similar approaches to this problem [4][5][6][7]. In-line or sampled data are usually gathered from multiple points on a network, followed by a detailed analysis of these data. The analysis may deploy signature and/or anomaly-based techniques, deep packet analysis, forensic analysis, or correlation analysis to identify attacks. Counter measures focus on assisting network administrators to tackle the problem as quickly as possible. The assistance could come in the form of simple notification of attack, automatic filtering of suspect traffic, or complete shutdown of connection to a network segment. As coordination among network owners increases, the counter measures will likely move toward a higher degree of automation.

8. Conclusions

Clearly, DDoS attacks could result in billions of dollars in lost business within hours. Not surprisingly, the VC community has supported DDoS solution vendors with enthusiasm. Over the past 18 months this sector has attracted more than $60 million in venture capital. Prominent pure play DoS/DDoS solution providers include Arbor Networks [1], Asta Networks [9], Captus Networks [10], and Mazu Networks [11]. Given the distributed nature of the problem, for a higher degree of success, most of these vendors support and recommend a distributed version of their solution. Clearly, this requires highly-coordinated efforts across multiple

networks and may involve several infrastructure owners (backbone operators, ISPs, and carriers). The current level of security-related coordination among the infrastructure owners is relatively low. Consequently, there is no shared incentive for network owners to open their networks for a coordinated effort against DDoS attacks – an effort that will only directly benefit the end customer. We believe that as DDoS attacks become more prevalent, large customers such as Amazon will force their hosting partners or ISPs to fortify their systems against DDoS attacks [12]. Such catalysts have the potential of triggering a network effect, forcing the keepers of Internet infrastructure to take preventive measures. While it is too early to predict which technology and company will ultimately succeed against DDoS attacks, one thing is for sure: DDoS and other hacker attacks, irrespective of their place of origination (within or outside the national boundaries), are enjoying a big popularity through federal investigations and military departments conducted by the U.S. Congress.

REFERENCES

[1] *Worldwide Infrastructure Security Report,* Volume III, Arbor Networks.

[2] David Moor, Geoffrey M. Voelker, Stefan Savage, *Inferring Internet Denial of-Service Activity*, 2001.

[3] McAfee Avert Labs Threat Library, http://vil.nai.com/vil/default.aspx.

[4] Tata Communications, *DDoS Detection and Mitigation: Ensure Application Availability*, http://www.tatacommunications.com/.

[5] Cisco Guard DDoS Mitigation Appliances, *Cisco Traffic Anomaly Detection and Mitigation Solutions,* http://www.cisco.com/.

[6] AT&T Intellectual Property, *LADS: Large-Scale Automated DDoS Detection System*, http://techrepublic.com.com/.

[7] Arbor Networks Peakflow SP http://www.arbornetworks.com/peakflowsp.

[8] John McCormick, *Pulsing zombie: DoS attack hits research networ*", 2001.

[9] Rutrell Yasin, *DoS protection: What's right for you?*, 2002.

[10] Intel Networking Case Study, *Captus Networks Helps Prevent Denial of Service Attacks.*

[11] Riverbed Technologies, *Advanced network and application performance analysis and reporting*, http://www.riverbed.com/products/cascade/.

[12] Silicon India Magazine http://www.siliconindia.com/.

[13] Arbor Security Engineering and Response Team, http://asert.arbornetworks.com/.

[14] Reinhard Wobst, Jurgen Schmidt, *Hash cracked*, The H-Security, 2006 http://www.h-online.com/security/Hash-cracked--/features/75686/0.

[15] Symantec Enterprise Security, *Symantec Global Internet Security Threat Report*, March 2007 and April 2009.
[16] Luis Corrons, *MPack Uncovered!*, Panda Laboratories, 2007 http://pandalabs.pandasecurity.com/.
[17] The Washington Post, F-Secure Security Labs, http://www.f-secure.com/weblog/.
[18] Yu Chen, Kai Hwang, Wei-Shinn Ku, *Distributed Change-Point Detection of DDoS Attacks: Experimental Results on DETER Testbed.*
[19] Zhen Li, Qi Liao, Aaron Striegel, *Botnet Economics: Uncertainty Matters.*