INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

INTEGRATED ANALYSIS ON CASE STUDY OF STEVE GIBSON DDOS ATTACK MAY 4TH, 2001: PERFORMANCE OF TESTING TOOLS AND IN THE CONTEXT OF BUSINESS

Ali Tariq Bhatti

Department of Electrical & Computer engineering
North Carolina A&T State University, Greensboro NC USA
Email: atbhatti@aggies.ncat.edu, ali_tariq302@hotmail.com

Abstract:- *The Internet Infrastructure should be secure before the network become threatened by the various number of bad packets. In this case study paper "Steve Gibson" creator of SpinRite, ShieldsUP, suffered a very hard problem due to a Distributed denial of service (DDoS) attack on his website (http://www.grc.com). In this paper, our analysis point of view that he figured out by his analytical advance skills that how they attack on his website and what tools they use? Steve Gibson use different tools and testing to protect his website from the attackers. He knows that 13 year old hacker and his partners had not created this tool because they were script kiddies and only know how to operate this attack. There was a disruption between Gibson & Wicked; due to saying the word "Script Kiddies" but Gibson doesn't say it. There were 474 computers which were performed to attack on his website. Attackers were running a "IRC bots" that takes command from the central server. They were just giving the commands and the bots started flooding with the millions of TCP packets. These types of attack don't affect the attacker's computer or data. The purpose of this attack was that legitimate request can't get through due to flooding the website with so much data.*

Keywords:- DDoS, Botnet, Back Ice Defender, Zombie, IRC, TCP, UDP, Intrusion Detection, Firewalls, Routers

1. Introduction

(a) Distributed denial of service (DDoS)

Distributed denial of service is one of the common attacks that are caused by botnet, and it usually makes a large quantity of financial loss [1, 13, 14]. Distributed denial-of-service (DDoS) attacks commonly overwhelm their victims by sending a vast amount of legitimate-like packets from multiple attack sites. Hence, the victim spends its key resources processing the attack packets and cannot attend to its legitimate clients. DDoS traffic also creates a heavy congestion in the Internet core which disrupts communication between all Internet users whose packets cross congested routers during very large attacks, [2].

(b) Botnet

Botnet is an urgent problem that has impact on information security and reduces confidentiality, integrity and availability of certain service [8]. In the research of information security, three standards, including confidentiality, integrity and availability, are discussed [9,1 0]. Botnet network is formed for commercial reasons, either in order to earn money by sending SPAM mail or tampering of rivals. The biggest problem which the organizer can have is Command and Control (C&C) of the net [11].

(c) Back Ice Defender

Systems such as BINDER [7], Norton Personal Firewall, and Black Ice Defender would have been an alternative approach to detecting the spyware programs. However, they are also unable to identify the seven spyware programs missed by Web Tap because these programs run as plug-ins inside of the browser, which is a trusted process receiving legitimate input.

2. Analysis Of Steve Gibson DDoS Attack:

This DDoS attack was occurred on the evening of May 4th, 2001, and grc.com was dropped of the internet. In the beginning of this attack that occurred to Steve Gibson website, they analyze two types of attack i.e. 1) Packet Flooding Attack 2) Brute Force Flood Attack. The starting time of the first attack, they analyze and experience that this type of attack is Packet Flooding Attack. They use Cisco routers for the two T1 lines to the internet were receiving 1.54 megabit rate. There was a mishap occur that outbound traffic was approximately to zero because inbound traffic was not reaching to their server. DDoS attacks are not limited only to Web servers, but almost all kinds of service available on the Internet can be targets of the attacks [4].

From my logical point of view, then, he reconfigured his network to capture the packet traffic and began logging the attack. Over there he analyzed and saw that huge UDP packets are at the bogus port of 666 at grc.com. It then fragmented over the internet showing the result of 1500-byte IP packets. His local router and firewall was not giving trouble and his machines were not affected.

Then, he analyze that it is a simple brute force attack which is used to consume all the bandwidth of our connection to the internet. Therefore Steve Gibson provided two pairs of 1.54 megabits (3.08 megabits) of bandwidth in each direction. Then their T1 relieved of the bad packets that had been filtered before leaving VERIO's router. In this way, the high bandwidth of the T1 would stop the packet flood in order to allow good packets. Seventeen hours passed for the first attack, Steve Gibson able to get a competent VERIO engineer with his analysis of the attack. In two minutes they applied brute force filters to the VERIO router to shut down the UDP and ICMP traffic. In this way, http://www.grc.com again popped up back onto the internet. During seventeen hours passed for the first attack Steve Gibson and his corporation captured 16.1 gigabytes of packet log data. He determined that they are attacked by 474 Windows PC's after choosing UDP packets at on port 666.

3. Five Additional Steve Gibson DDoS Attacks

Five Additional Attacks (6th Attack is not counted as a attack):

Steve Gibson & his Research Corporation faced to bear five attacks:

First Attack: This attack occurred on May 4th and it was remained till for 8 days. In this attack, 17 hours passed, they able to filter it their ISP, so that attack cannot behind the filters.

Second Attack: This attack occurred on May 13th and it is similar to first attack. For eight hours, they are dropped of the internet until and unless VERIO re-establish their previous filters.

Third Attack: This attack occurred on May 14th. This type of attack was retargeted at the IP of their firewall. They again and again dropped off from the internet. Talking back again to VERIO Engineer, they decided to shut down T1 completely. GRC.com pop up on the internet due to single T1.

Forth Attack: This attack occurred on May 15th. They were bugs in Cisco routing software, and for this reason they were unable to filter their attack. In this forth attack, he talk with VERIO engineer on phone to design and test the comprehensive set of cisco router filters to protect the http://www.grc.com site. During these attacks, He also design the exact profile of the malicious traffic generated due to these attacks.

Fifth Attack: This attack occurred on May 16th. In this attack, attacking machine generate 64K byte of UDP packets which is of maximum size but the packet port "666" destination is carried by the first 1500 byte fragment of each packet. That night of this attack, his VERIO router block at least 538,916,268 malicious packets.

Sixth Attack: This attack was occurred on May 17th, 18th, 19th and 20th.These are not exact dates but when they check the router UDP/666 hit counter on Monday 21th. In this attack, filter has occurred to conclude at-least 2,399,237, 016 malicious packets.
Steve Gibson was having FBI conversation and also having conversation with "wicked" during the attacks.

4. Tools to test for Steve Gibson DDoS

From my analytical thinking and observation that tools used were as:

i) Testing Zombies: So he sacrificed to choose Zombies. He reformatted his laptop with the machine name "Sitting Duck" and turned it on. Then this program was connected to the IRC chat server which is remotely programmed and after that it joins the secret and password key protected channel on that server. His aim of using zombies is to kill its ability of sending damaging packets. The Zombie program, he received was rundll.exe. As zombies are continuous joining and leaving the IRC Server, so Sub7Server Trojan was downloaded by the zombie from a free web pages web server. Sub7Server Trojan defines as user with sub7 in their machine might as well as having the hacker standing right. It starts listening on the random port it choose during installation.. It joins it special Sub7 IRC chat server where it posts a notice listing all the details required for its connection and use. At the same time, identical information is posted to a newsgroup server through a web server CGI script. Hackers no longer need to scan the internet for vulnerable machines running sub7. He use spy-bot to analyze and collecting the binaries of zombies. By this way, he finally found that the hacker (^boss^) because zombies "wicked" had hex edited in order to create that had been grc.com.

The benefit of using zombies was 1) Understanding the technology. 2) He wanted to know the issues around the internet security and privacy 3) He also wanted to know everything worked so that he possibly defended against future similar attack. 4) Needed to get through to "Wicked" any way.

Logging into the wkdbots IRC server and joining his boots on the "#pines" IRC channel, the wick use the two commands.(1)!p4 207.71.92.193 (2)!udp 207.71.92.193 9999999 0. !p4 command use by the grc.com server and executes the ping command with following arguments i.e Ping.exe 207.71.92.193 –l 65500 –n 10000. This command sends 10,000 which are 64 kbyte ping packets to the machine at the specified IP. The !Udp command do more damage. Target IP, the number of huge UDP packets to send and inter-packet delay are specified from this command. This command also allows udp packets for each bot to send 9,999,999 to the grc.com server.

This is all the testing, Steve Gibson did using Zombies. His spy-bot pick up this command The "!r" command , when his "^boss^" gave him which stands for Ready/Report/Rally. It is interesting command in this attack because it causes connecting & listening zombies to report in.

From DDoS attack, Steve Gibson did a quick and easy check for IRC Zombie/ Bots by using the command on the IRC default port of 6667 i.e Netstat –an | find ": 6667". To quick check for an identical server, then type:: Netstat –an | find ": 113". Permanently update operational system and other software; since Bots use security failures in operating system and other software, it is necessary to update them permanently, or install the patches and update [6]. Some Bots have special function of collecting electronic addresses. Besides, they are used for sending phishing-mail [3].

ii) Personal Firewalls and IRC Zombie/Bot Intrusions: So, by handling this type of situation, he downloaded the completely free version of Zone Alarm 2.6 from the Zone labs website and after he installed it. When he restart his laptop, zombie was notifying that zombie is making outbound connection to its IRC chat server and therefore

Sub7 Trojan was waiting for someone to connect. So he used another machine to telnet to the Sub7 Server Trojan port so it can listen. Then the zone alarm popped up and telling that Sub7server Trojan is allowed to accept a connection from the internet. The problem doesn't become solve, and then he used Black Ice Defender v2.5 (lame personal firewall) to remove all traces of Zone Alarm and restarted the machine. Everything was settled down and restarted the machine with his packet sniffer running on a adjacent PC.

iii) Using Black-Ice Defender: Using another tool/testing: It having features like: 1) Zombie/Bot happily connected 2) Sub7 Trojan sent email containing the machine to the port, it was listening. It was connected and logged itself to the Sub7 Server 3)No alerts 4)There was no flashing in the System Tray.5)Trojans were not hampered**.**

After using Black-Ice Defender, he performed one final test: The final test, he did with Zone Alarm. Using his laptop, when he was doing a final test with Zone Alarm, he then connected to the Sub7 Server Trojan. Sub 7 Server Trojan was listening the port number over the internet. Then he received Sub7's PWD prompt asking him to login.

5. What information learned from Steve Gibson DDoS Attack?

The information I learned from this attack as:

1) Steve Gibson have analyzed their tools and conversation.2) When asking help for Internet security, so Industry leading consumer ISP's are useless.3) The future in the United State Government have no tolerance in case of Internet hacking.4) The internetwork must be secure before it produces malicious attacks.5) We need to have a tool that can hold and demonstrate ISP irresponsibility for the future.

6. How would you attempt to keep a business from suffering a similar (DDoS attack)?

From my analysis and observation, DDoS also have its own tools for attempting to keep a business suffering.

In this case, malicious user can find out which physical servers the victim is using then by implanting a malicious virtual machine at that location to launch an attack [12]. There are different ways for attempting to keep a business suffering from a similar (DDoS) attack:

- **Black-holing or sink-holing:** It can block all traffic and it is discarded from where it diverts to a black-hole. The downside of this traffic is discarded in two ways: 1) Combination of good & bad packets 2) The business is targeted off-line.
- **Routers & Firewall:** Routers can stop in two ways: It is filtering nonessential protocols which can be configured to stop simple ping attacks. It stops invalid IP addresses. Routers are ineffective against in two ways: 1) More sophisticated spoofed attack 2) Application-level attacks using valid IP addresses. Firewall don't support anti-spoofing, so firewall can shut down a specific flow associated with an attack.
- **Intrusion-detection systems:** Anomaly-detection capabilities to be provide for IDS solutions. They will recognize when valid protocols are being used as an attack vehicle.
- IP-Spoofing & Bandwidth Flooding Attack etc. and as well as block all Inbound packets which having highly number service ports. All common ports fall in the range of 1-1023.

Conclusion

In this case study paper, DDoS attack use hundreds or thousands of computer and sends unwanted traffic to the victim computer via victim resources and preventing it from serving its legitimate clients. Besides, it is possible to overload the communication channel if DDoS attack sends too many packages per second. TCP and UDP "flood" are mostly used [5]. Several attacks occurred and tools applied to test this Steve Gibson DDoS attack, so to get his system in normal position. In my analysis for business point of view: 1) DDoS attacks can shutter a business because these attacks behave as a Destructive Stealth Weapons. 2) The threat of DDoS attack continues to increase in the business due to reliance on the internet continues to grow. 3) If anyone wanted to conduct Business, Organizations & Companies etc. as usual, so they need to notify operational continuity and resource availability with the DDoS mitigation approach.

REFERENCES

[1] Wei, W., Chen, F., Xia, Y. and Jin, G., "A Rank Correlation Based Detection against Distributed Reflection DoS Attacks", Communications Letters, 2013, vol.17, pp. 173-175

[2] Jelena Mirkovic, Max Robinson, Peter Reiher, George Oikonomou ,"Distributed Defense Against DDoS Attacks" Available:http://www.isi.edu/~mirkovic/publications/udel_tech_report_2005-02.pdf

[3] Yinglian Xie, Fang Yu, Kannan Achan, Rina Panigrahy, Geoff Hulten, Ivan Osipkov, Spamming Botnets: Signatures and Characteristics, Computer Communication Review, 2008.

[4] Bojan Jovičić, Dejan Simić, Common Web Application Attack Types and Security Using ASP.NET, ComSIS. December 2006.

[5] Markus Koetter Know your Enemy: Tracking Botnets, The Honeynet Project, 2009. (http://www.honeynet.org/papers/bots/)

[6] Massimiliano Romano, Simone Rosignoli, Ennio Giannini , Robot Wars – How Botnets Work, Window Security, 2009. (http://www.windowsecurity.com/articles/Robot-Wars-How-Botnets-Work.html)

[7] W Cui, R. Katz, and W. Tan. BINDER: An Extrusion-Based Break-In Detector for Personal Computers. In Proc. USENIX Annual Technical Conference, 2005.

[8] Feily, M., "A Survey of Botnet and Botnet Detection", Third International Conference On Emerging Security Information, Systems and Technologies, 2009, pp. 268-273

[9] Baker, W.H., "Is Information Security Under Control?: Investigating Quality in Information Security Management", Security & Privacy, 2007, vol.5, pp. 36-44

[10] Hwang, S.Y. and Lee,C.H., "Reliable Web service selection in choreographed environments", Decision Support Systems, 2013, vol.54, pp. 4796-1476

[11] Ryan Vogt, John Aycock, and Michael J. Jacobson, Army of Botnets, Proceedings of the 2007 Network and Distributed System Security Symposium (NDSS 2007), 2007, pp. 111-123.

[12] Farzad Sabahi Cloud Computing Security Threats and Responses

[13] Zhang, C. W., Cai, C. P., Chen, W. F., Luo, X. and Yin, J., "Flow level detection and filtering of low-rate DDoS", COMPUTER NETWORKS, 2012, vol.56, pp. 3417-3431

[14] Yu, S., Zhou, W., Doss, R. amd Jia, W., "Traceback of DDoS Attacks Using Entropy Variations", IEEE Transactions on Parallel and Distributed Systems, 2011, vol. 22, pp. 412-425

BIOGRAPHY

Ali Tariq Bhatti received his Associate degree in Information System Security (Highest Honors) from Rockingham Community College, NC USA, B.Sc. in Software engineering (Honors) from UET Taxila, Pakistan, M.Sc in Electrical engineering (Honors) from North Carolina A&T State University, NC USA, and currently pursuing PhD in Electrical engineering from North Carolina A&T State University. Working as a researcher in campus and working off-campus too. His area of interests and current research includes Coding Algorithm, Networking Security, Mobile Telecommunication, Biosensors, Genetic Algorithm, Swarm Algorithm, Health, Bioinformatics, Systems Biology, Control system, Power, Software development, Software Quality Assurance, Communication, and Signal Processing. For more information, contact **Ali Tariq Bhatti** at ali_tariq302@hotmail.com.