International Journal of Electrical, Electronics and Computer Engineering **1**(1): 103-106(2012)

ISSN No. (Online) : 2277-2626

Distributed Denial of Service Using I-DFT

Zaheeruddin, Shambhu Kumar Suman and N.K. Mittal

Department of Electronics and Communication Engineering,

Oriental Institute of Science and Technology, Bhopal, (M.P.)

(Recieved 15 March 2012 Accepted 20 April 2012)

ABSTRACT : With the rapid development of information technology, internet has affect the people in all aspects such as public utilities, telecommunication, financial transaction and defense system, all depends on information technology and their security. The widespread deployment of new technologies had maximized the use of internet to a great extent. But at the same time, the potential attackers are success on discovering new ways to attack. Botnet is one of the most serious emerging threats and it refers to a number of compromised computers within a network. Malicious activities which are performed by a botnet are DDoS, spam, click fraud, phishing, identity theft, sniffing traffic, keylogging etc.

DDoS attack can significantly degrade the performance of a network or can completely disconnect a machine to achieve resource overloading. The objective of this dissertation is dealing with DDoS attack. This work is dividing into three phase. In first phase, we are simulating a botnet environment. In second phase, we are performing UDP flooding of DDoS attack. In third we are applying queuing theory to overcome the DDoS attack.

Keywords: Key words: Botnet, DDoS, Bots, IRC, DoS.

I. INTRODUCTION

A Denial of Service(DoS) attack is an attack is used preventing legitimate users from using a specified network resource such as a website, web service, or computer system. A Distributed Denial of Service (DDoS) attack is a coordinated attack on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems. The services under attack are those of the "primary victim", while the compromised systems used to launch the attack are often called the "secondary victims", these secondary systems are bot infected system. The use of secondary victims in a DDoS attack provides the attacker with the ability to perform a much larger and more destructive attack thus the secondary victims(compromised system) actually perform the attack and making it more difficult for network forensics to track down the real attacker. This paper proposes taxonomies for understanding different DDoS attacks, tools, and countermeasures [1, 2].

II. DDOS ATTACK STRATEGY

Two types of DDoS attack networks have been developed: the Agent-Handler model and the Internet Relay Chat (IRC)-based model.

A. Agent-Handler model

Clients, handlers, and agents are the three active participants of DDoS attack in Agent-Handler model as shown in Fig. 1. Clients can work as a real time attacker. Handlers are also known as masters. These masters are the infected systems or hosts which are able to control multiple agents. Attacker can communicate with any number of handlers to identify which agents are running or not. Agents are also a compromised system which includes infected software and carry out the attack. Most of the time owner and user of the agent system is unaware that their system is compromised or performing attack in the network [2].

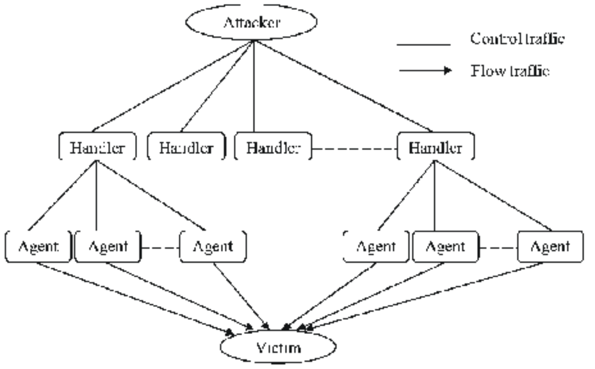

Fig.1. DDoS Agent-Handler Attack Model.

B. IRC-based Model

IRC based DDoS model is similar as agent-handler model but IRC based model uses IRC channel in place of handler. IRC communication channel provides communication between attackers or clients and agents. IRC channel provide some extra benefits to the attacker like it provide a legitimate IRC ports for sending command to agents, the attacker does not need to maintain a list of the agents, since attacker can log on to the IRC server and see a list of all available agents.

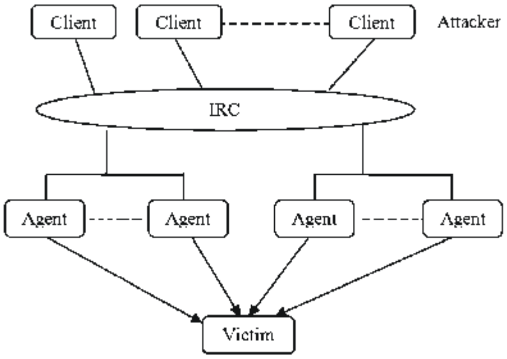

Fig. 2. DDoS IRC Based Atack Model.

III. FRAGGLE ATTACK

Fraggle attack is another type of DDoS amplification attack. In this attack, the attacker sends packets to a network amplifier, using UDP ECHO packets and UDP chargen services. Connecting to a UDP port running the chargen service produces a constant stream of data. A UDP port running the echo service simply bounces the packet back to the sender's source address. Creating a UDP connection between chargen and echo ports will create a huge amount of traffic between two systems. If a UDP packet is sent with a spoofed source broadcast address to victim's chargen port, multiple connections might be created between echo ports on machines in the spoofed broadcast domain and the victim machine amplifying the amount of traffic targeting the victim. The UDP Fraggle packet will target the character generator in the systems reached by the broadcast address. These systems each generate a character to send to the echo service in the victim system, which will send an echo packet back to the character generator, and the process repeats. This attack can generate more bad traffic and cause more damage than a Smurf attack [3].

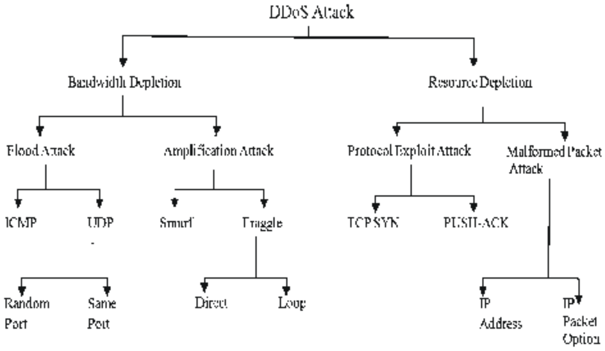

Fig. 3. DDoS Attack Variants.

IV. NAME OF BOTS WITH VERSION WHICH PERFORM WHICH PERFORMS MALICIOUS FUNCTION.

Table. 1. Latest Bot and Their Malicious Activities.

Name of bot	Version	Main Malicious Activites
SDbot	V0.6b	Get Host information, C.D.keys, UDP/ICMP Flood Attack, Execute command
Agobot	V4.0	Get Host information, Consume the bandwidth of victims' network, Get Software keys, Get e-mail list Spam DDoS Attack, Control PCs.
GT-Bot	With-draw	Get Host Information, UDP/ICMP Flood Attack
Rbot	Rbot.A	Get Host Information, Get Software keys, Password logging, Spam, DDoS

5. BOTNET DETECTION

A. Architecture

We propose an architecture of online botnet detection method as Fig. 2 shown. First, the raw network traffics are filtered to reduce the data volume. Then the feature streams are constructed from the traffics for further imilarity analysis.

After that, thousands of feature streams are monitored to measure the similarities efficiently by incremental Discrete Fourier Transform (DFT) technique. The hosts whose feature streams have similarities will be added into the candidate bots set for later activity analysis. The result will be reported after the final confirmation [5].

B. Filter

When network flows arrive to our system continuously, we need to filter irrelevant traffics and retain botnet event traffics as much as possible. Since botnet traffics occupies only a small part of huge network traffics, it is very hard to search for such small botnet traffics in large scale network environment. So, reducing the data volume is necessary. Meanwhile, reduction of the huge data volume can save the computation cost and improve the efficiency on next steps.

We perform the filter operation from the following areas. First, we filter out traffic flows by IP protocol to select TCPbased flows. Second, it is filtered according to the whitelist and the blacklist from some good-known sites such as Yahoo, Google etc. Third, we select some small packets to go through. Finally, some flows using unlikely C&C protocols, such as ICMP and UDP, are filtered.

C. Construction of Feature Stream

Here we compare the similarities among these traffic flows to capture the bots activities. A low is defined as a series of packets that belong to the communication between a source host and a destination host during certain time. We can describe the flow using a full packets trace certainly, but it will cost two much space.

Therefore, it's unrealistic to compare the flows directly. It's sufficient to extract some characteristics of a flow as the description, which will be much more compact. Flow characteristics can be easily expressed as time series. As time goes by, we just need to use these streaming time series to compare the similarities of raw flows [6, 7].

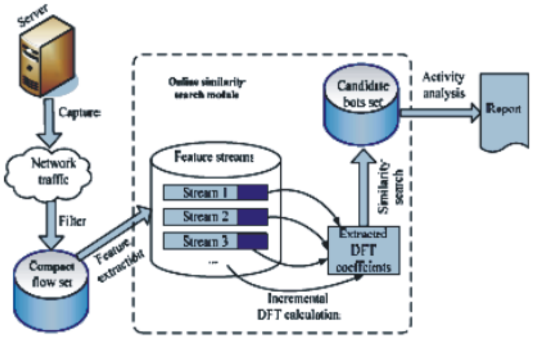

Fig. 5. Typical Botnet Structure.

Incremental DFT : We introduce a method to illustrate that the DFT coefficients can be updated incrementally by formula. We needn't to recalculate all the coefficients when the new value arrives.

Let X be a streaming time sequence with values $X(0)$, $X(1)$, …,$X(w-1)$ and the window length is w. Let *DFT*0 (X), *DFT*1 (X), …, *DFTw*–1(X) denote the *DFT* coefficients of X. If a new value arrives, we get the sequence $Y(1)$,$Y(2)$, …,$Y(w)$, where $X(i) = Y(i)$ for i w-1 and $Y(w)$ is the new value. The *DFT* coefficient of Y can be computed according to the following equation :

$$DFT_n(Y) = \frac{1}{\sqrt{w}}.(\sqrt{w}DFT_n(X) - X(0) + Y(w).e^{-j2\pi kn/w}$$

$(0 < n < w-1)$.

Next, we will explain the above formula in detail. It is noted that $X(i) = Y(i)$, where $1 < i < w$-1. The nth *DFT* coefficient of X is given by:

$$DFT_n(X) = \frac{1}{\sqrt{w}} \sum_{k=0}^{w=1} X(k).e^{-j2\pi kn/w}$$

Similarly, the nth *DFT* coefficient of Y is given by:

$$DFT_n(Y) = \frac{1}{\sqrt{w}} \cdot \sum_{k=0}^{w=1} Y(k+1)e^{-j2\pi kn/w}$$

And we know that

$$DFT_n(Y) = \frac{1}{\sqrt{w}}(Y(1) + Y(2)e^{-j2\pi kn/w} + ... + Y(w-1)$$
$$e^{-j\pi(w-2)n/w} + +Y(w))e^{-2j\pi(w-1)n/w})$$

By taking into consideration that $X(i) = Y(i)$ for, and $1 \le i \le w-1$, and that, $e^{-j2\pi n/w} = e^{-j2\pi(w-1)n/w}$, we get :

$$DFT_n(Y) = \frac{1}{\sqrt{w}}(Y(1) + Y(2)e^{-j2\pi n/w} + ... + Y(w-1)$$
$$e^{-j2\pi(w-2)n/w} + +Y(w))e^{-j2\pi(w-2)n/w})$$

So, when a new value arrives in the feature stream, the *DFT* coefficient can be obtained incrementally by the old *DFT* coefficient. In this way, we needn't to recalculate the *DFT* coefficient every time when the new value arrives. Consequently, the efficiency of similarity search is greatly enhanced.

VI. RESULTS AND DISCUSSIONS

Analysis of the results of the simulation experiments is given,

To evaluate the detection performance, five scenarios are designed: The network delay from the source to the victim server is set to 100ms and the bottleneck bandwidth for victim server is 10M. The attacking traffic begins at the 20 second and the whole simulation lasts for 80 seconds. The results shown from Fig. .

As shown in Fig.6, the value of the packet fluctuate 0 or above the threshold when there is transmit packet and received packet in simulated network.

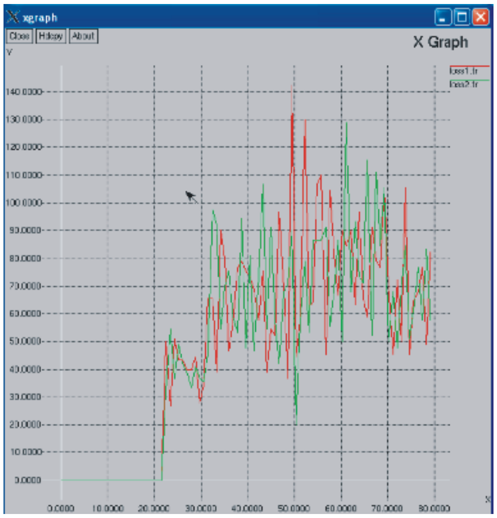

Fig. 6. Packets Loss at Network Normal Condition.

As shown in Fig. 6, show that variation of simulation started with 20s and the flooding of packet between boot node and host node.

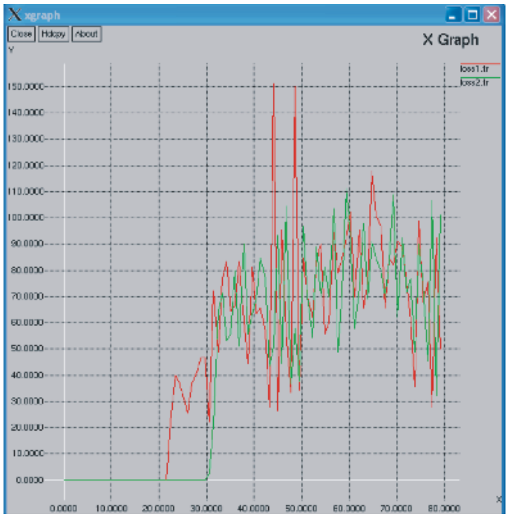

Fig. 7. Packets Loss at Network When Traffic Increased by 50 % Extra

As shown in Fig.7., show that variation of simulation started with 20s and the flooding of packet received start of simulation initially the maximum packet are received and after 10s the dropping rate of packet are increased.

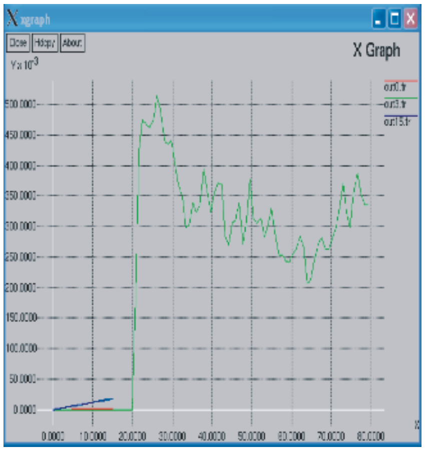

Fig. 8. Delivery of Packets at Normal Condition.

As shown in Fig.8., show the variation of lost packet between boots and server at the time of complete simulation 80s.

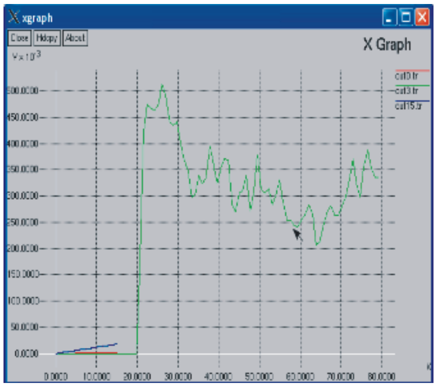

Fig. 9. Delivery of Packets at Traffic Increased by 50 % Extra.

As shown in Fig. 9., the value of the packet fluctuate 0 or above the threshold when there is transmit packet and received packet in simulated network.

CONCLUSION

Botnet is a new type of attack developed from a traditional form of malicious code, using a variety of propagation mechanisms so that the malicious code can infect a large number of computers on the Internet. Botnet is a milestone in the development of malware, because it is integrated with the features of virus, Trojans and worms. It takes full use of internet to facilitate the construction of platforms and resources for various network attacks. Botnets can cause extreme damage to companies by means of DDoS, information theft, and spam. IRC is a good tool to exchange ideas with other users, but be weary of the threats that accompany this service. Botnets exist because we are not very good at keeping our systems secure.

REFRENCES

[1] Hang Chau, Network Security - Defense Against DoS/ DDoS Attacks.

[2] Wesley M. Eddy, Verizon Federal, Defenses Against TCP SYN Flooding Attack,*The Internet Protocol Journal-* Vol. **9**, Number 4, December 2006.

[3] Prepaired by National Computer Emergency Response technical

[5] Maryam Feily, Alireza shahrestani, Sureswaran Ramadass, "A Survey of Botnet and Botnet Detection", third International conference on Emerging Security Information, System and Technology 2009.

[6] Wei Lu, MahbodTavallaee, GoaletsaRammidi and Ali A. Ghorbani "BotCop: An Online Botnet Traffic Classifier" 2009 Seventh Annual Communications Networks and Services Research Conference.

[7] W. Timothy Strayer, David Lapsely, Robert Walsh, and Carl Livadas, Botnet detection based on network behavior, Botnet Detection: Countering the Largest Security Threat, Springer Science Business Media, LLC, 2008, 1-24.