Global Information Assurance Certification Paper

Understanding DDOS Attack, Tools and Free Anti -tools with Recommendation

DeokJo Jeon
Apr 7, 2001

E-Business is the popular business model of this Internet era and the business is spanning its border to the inter -business transaction area. The most severe threats for those e -Business players will be DDOS attack. The DDOS attacks were first identified in late 1999 in real world and in February 2000, major e -Business giants were brought down by DDOS attacks and experienced huge revenue losses. The victim list includes Yahoo, Amazon, eBay, E*Trade, ZDNet, CNN and so forth.

The DDOS attack is a continuous issue of many organizations and security expert communities. As evidence, on the mid January 2001, ZDNet published an article titled "*Defenses still weak against DDoS attacks".* The article mentioned that the U.S. Department of Commerce with 19 high-tech giants have established the Information Technology -Information Sharing and Analysis Center (IT-ISAC) for sharing information to prevent and minimize cyber crimes and damages.

One key trend of DDOS is that the attacks are becoming more prevalent in the world of Internet. Additionally the attack tools are getting more sophisticated and their schemes are getting increasingly more complex. Thus, to keep up with this continuous sophistication, we need to be well prepared in order not to give any damages or excuse to other organizations or people around the world.

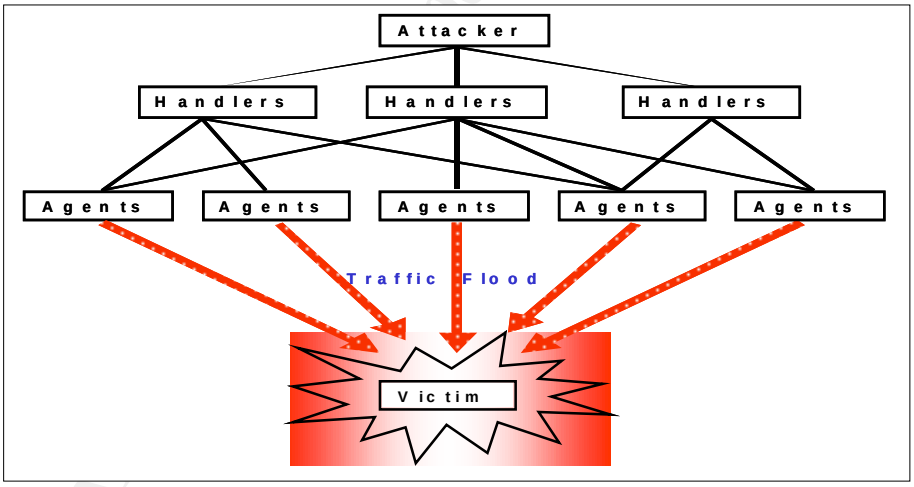
Currently, many security experts have identified more than seven DDOS tools and lots of variants are appear ing continuously. The main reasons of DDOS attack are following:

- TCP/IP protocols were designed without poignant consideration of security.
- -There are a huge number of unsecured computers with fast Internet connection are available in the Internet.

On the target side, even though many new start-ups are dedicated to developing DDOS defeat tools; we don't have any technical silver bullet for protecting web sites from the attack yet. However, if every system administrators or users could have full understanding of DDOS attack, at least, we can greatly reduce the attacker's chances. At the same time, we can minimize the usage of distributed attack against our systems. Here, we will concentrate on topics, which can help people to understand the concept of DDOS attack, tools, and possible solutions to protect our systems from attackers.

DDOS Attack Overview

A DDOS is a type of attack technique by saturating the victim system with enormous network traffic to the point of unresponsiveness to the legitimate users. A DDOS attack system has a complicated mechanism and entails an extreme cooperation between systems to maximize its attacking effectiveness.



The DDOS attack systems are very similar to the Client/Server model of ordinary IT system. The attack systems involved three system components: handlers, agents and a victim respectively. Figure 1 shows the general architecture of a DDOS attack system.

Figure 1 Distributed System Attack

As Figure 1 shows, A DDOS attack is possible by the coordination of many systems. To clog up the victim's network with enormous network traffic, the attacker need to use a number of systems as for handlers and agents. The

attacker commands handlers and the handlers control a troop of agents to generate network traffic. To make a successf ul attack, an attacker first need have a number of systems to secure a bridgehead, usually large systems with high-speed network connection. To compromise such systems as many as possible and install DDOS tools on each of them, an attacker must find those systems with various techniques such as network port scanning, OS Determination by TCP/IP stack fingerprinting and other known infiltrating techniques. Also, to hide those DDOS tool's presence after installation, the attacker may use other techniques such as IP address spoofing or rootkit and so forth. The installed DDOS tools turn the compromised systems into attack zombies. Once the DDOS tools are installed on many compromised systems, the attacker is easy to launch an attack by controlling agents through handlers via commands. Once an attack begins, the target is not able to handle the tremendous volume of the bogus traffic.

DDOS Tools and Their Attack Methods

Currently several security professionals identified a few DDOS tools and wrote analysis reports on them. The one big problem is that the variants of such tools with more sophistication are showing up continuously and, as a result, the abundance of such tools is amplifying the potential threats of DDOS.

Below is a table of showing some common DDOS too ls and their attack methods.

Tools	Flooding or Attack Methods
Trin00	UDP
Tribe Flood Network	UDP, ICMP, SYN. Smurf
Stacheldracht and variants	UDP, ICMP, SYN. Smurf
TFN 2K	UDP, ICMP, SYN. Smurf
Shaft	UDP, ICMP, SYN. combo
Mstream	Stream (ACK)
Trinity , Trinity V3	UDP, SYN, RST, Random Flag, ACK, Fragment, ...

Table 1 Some Recovered DDOS Tools

Table 1 shows some DDOS tools and their attack methods. As you may see in the table, DDOS tools are continuously becoming more sophisticated.

There are a few common attack methods known to the communities. They can be classified into two categories: Flood Attack and Malformed Packet Attack.

Flood Attack

- Smurf Flood Attack: An attacker sends forged ICMP echo packets to broadcast addresses of vulnerable networks. All the systems on these networks reply to the victim with ICMP echo replies. This rapidly exhausts the bandwidth available to the target, effectively denying its services to legitimate users.
- TCP SYN Flood Attack: Taking advantage of the flaw of TCP three-way handshaking behavior, an attacker makes connection requests aimed at the victim server with packets with unreachable source addresses. The server is not able to complete the connection requests and, as a result, the victim wastes all of its network resources. A relatively small flood of bogus packets will tie up memory, CPU, and applications, resulting in shutting down a server.
- UDP Flood Attack: UDP is a connectionless protocol and it does not require any connection setup procedure to transfer data. A UDP Flood Attack is possible when an attacker sends a UDP packet to a random port on the victim system. When the victim system receives a UDP packet, it will determine what application is waiting on the destination port. When it realizes that there is no application that is waiting on the port, it will generate an ICMP packet of destination unreachable to the forged source address. If enough UDP packets are delivered to ports on victim, the system will go down.
- ICMP Flood Attack: An attacker sends a huge number of ICMP echo request packets to victim and, as a result, the victim cannot respond promptly since the volume of request packets is high and have difficulty in processing all requests and responses rapidly. The attack will cause the performance degradation or system down.

Malformed Packet Attack

- Ping of Death Attack: An attacker sends an ICMP ECHO request packet that is much larger than the maximum IP packet size to victim. Since the received ICMP echo request packet is bigger than the normal IP packe t size, the victim cannot reassemble the packets. The OS may be crashed or rebooted as a result.
- Chargen Attack: A variant of UDP Flood Attack. An attacker sends forged UDP echo request packets to intermediary system's UDP port 19 (chargen). Then the system receives the packets on its chargen service port and responds by generating a string of characters to victim system. The victim system receives the packets on its echo service port and responds back to the chargen service system with an echo of the character string. Once this loop begins then the loop rapidly exhausts the bandwidth between victim and intermediary system .
- TearDrop Attack: An attacker sends two fragments that cannot be reassembled properly by manipulating the offset value of packet and cause reboot or halt of victim system. Many other variants such as targa, SYNdrop, Boink, Nestea Bonk, TearDrop2 and NewTear are available.
- Land Attack: An attacker sends a forged packet with the same source and destination IP address. The victim system will b e confused and crashed or rebooted.
- WinNuke Attack: Attackers send Out -of-band data to a specific port on Windows machine and the data cause a system crash.

Since a TCP/IP stack is the combination of many protocols, we can easily anticipate the appearance of various Malformed Packet Attacks. Most DDOS attack tools accommodate the above attack methods in a single or combined form.

Anti-tools with Recommendation

Knowing our enemy will be the first step to against DDOS attack. By having idea about their tools and methods of attack, we can get prepared. We have seen various attack tools and their attack methods. Now, let's identify some free DDOS detection tools to detect DDOS handlers and agents on our systems.

There are few promising host-based tools available in the Net with no costs. The first is National Infrastructure Protection Center (NIPC)'s "find_ddos" tool. The latest version is 4.2 and runs on Solaris and Linux platform. It is able to detect many old and recent DDOS tools including mstream, TFN2000 client and daemon, Trin00 daemon and master, TFN daemon and client, stacheldraht master, client and daemon and TFN-rush client. The NIPC tool can be downloaded from http://www.nipc.gov/warnings/advisories/2000/00-055.htm.

Few security experts including David Dittrich, Marcus Ranum, George Weaver, David Brumley developed a tools called "dds" and working on a trinoo, TFN, stacheldraht agents. The only problem is that the tool is in beta stage now and the authors recommend us to use RID instead. It can be downloaded from http://staff.washington.edu/dittrich/misc/ddos_scan.tar.

David Brumley at Stanford University wrote a remote DDOS detector called RID. The latest version is 1.11. The tool is able to detect Tri00, TFN, and stacheldraht agents. The tool can be downloaded from the following URL: http://theorygroup.com/Software/RID/.

Bindview Inc. wrote a tool called Zombie Zapper. Zombie Zapper works against Trinoo, TFN, Stacheldraht, Troj_Trinoo (the trinoo daemon ported to Windows), and Shaft but not works on TFN2K because of its password assumption policy. The tool is available at the following URL: http://razor.bindview.com/tools/ZombieZapper_form.shtml.

We have discussed about the basic concept of DDOS attacks, tools and some free anti-tools. However, we haven't touched any detailed guidelines to reduce the threat. As you already know, an attacker first should compromise a number of computers to make a DDOS attack. Thus, the first defense technique will be removing vulnerabilities from our system by following basic security rules and guidelines. A large number of such documents are available on the Internet and bookstores. Among them, I prefer to recommend SANS Institute's "Essential Security Actions: Step-By-Step". The document is available at the following URL: http://www.sans.org/newlook/resources/esa.htm. In that way, we can minimize attacker's chances to compromise from our system. More documents that directly deals with DDOS specific issues are also available at the same site.

Please refer the following URLs: http://www.sans.org/ddos_roadmap.htm, http://www.sans.org/dosstep/index.htm and http://www.sans.org/y2k/DDoS.htm.

In summary, a DDOS attack was possible in virtue of the cooperation of many vulnerable systems in the Internet. The most important thing for a DDOS attacker is compromising systems as many as possible. Most DDOS attack was possible because of the existence of several hundreds of thousands vulnerable systems on the Internet. As long as we follow basic Defense-in-depth principle and understand their methods, DDOS attack chances will be greatly reduced.

References:

1. NIPC ADVISORY 00-055: "Trinity v3/Stacheldraht 1.666" Distributed Denial of Service Tools, NIPC, October 13, 2000 http://www.nipc.gov/warnings/advisories/2000/00-055.htm
2. NIPC ADVISORY 00-063 "New Year's DDOS Advisory", NIPC, December 28, 2000 http://www.isc.org/products/BIND/bind-security.html.
3. NIPC ADVISORY 00-044 "MStream Distributed Denial of Service Tool", NIPC, May 24, 2000 http://www.nipc.gov/warnings/advisories/2000/00-044.htm
4. Carnegie Mellon Software Engineering Institute. " CERT® Incident Note IN-2000-05 "mstream" Distributed Denial of Service Tool, May 2, 2000 http://www.cert.org/incident_notes/IN-2000-05.html
5. David Dittrich, "The DoS Project's "trinoo" distributed Denial of Service attack tool, October 21, 1999, http://staff.washington.edu/dittrich/misc/trinoo.analysis.txt
6. David Dittrich, The "Tribe Flood Network" distributed denial of service attack tool, October 21, 199 http://staff.washington.edu/dittrich/misc/tfn.analysis.txt
7. David Dittrich, The "stacheldraht" distributed denial of service attack tool, December 31, 1999 http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt
8. Jason Barlow and Woody Thrower, Axent Security Team, "TFN2K - An Analysis", March 7, 2000 http://packetstorm.securify.com/distributed/TFN2k_Analysis-1.3.txt

9. Sven Dietrich, Neil Long, and David Dittrich, An analysis of the ``Shaft'' distributed denial of service tool, March 13, 2000, http://netsec.gsfc.nasa.gov/~spock/shaft_analysis.txt
10. David Dittrich, George Weaver, Sven Dietrich, and Neil Long, The "mstream" distributed denial of service attack tool, May 1, 2000, http://staff.washington.edu/dittrich/misc/mstream.analysis.txt
11. Dennis Fisher, Defenses still weak against DDoS attacks, January 19, 2001, http://www.zdnet.com/zdnn/stories/news/0,4586,2676260,00.htm
12. Dennis Fisher, Tech heavyweights team up to tackle cybercrime, January 16, 2001, http://www.zdnet.com/eweek/stories/general/0,11011,2674693,00.html
13. SANS Institute, Help Defeat Denial of Service Attacks: Step-by-Step, March 23, 2000, http://www.sans.org/dosstep/index.htm
14. SANS Institute, Incident Handling Step by Step: Unix Trojan Programs - Version 2.1, 1999-2000, http://www.sans.org/y2k/DDoS.htm
15. SANS Institute, Consensus Roadmap for Defeating Distributed Denial of Service Attacks, February 23, 2000, http://www.sans.org/ddos_roadmap.htm
16. SANS Institute, Essential Security Actions: Step By Step, 1999, http://www.sans.org/newlook/resources/esa.htm
17. Stephen Northcutt, Judy Novak, Network Intrusion Detection: An Analyst's Handbook, September, 2000, New Riders