Global Information Assurance Certification Paper

“Trinity” - distributed denial-of-service attack tool

Michael Marchesseau
September 11, 2000

Overview

At one time Denial-of-service (DoS) attacks were a graceful maneuver of crafting packets with strange, out of sequence information that would be sent to a device that would not know how to handle them, resulting in the systems shutting down or rebooting. The goal of DoS is to cripple a device or network so that external users no longer have access to the network resources. Almost with pinpoint precision, a single packet could deny service to and entire web site or network.

The goals have not changed, but the methods have gotten much more sophisticated with Distributed Denial-of-Service (DDoS) attacks. DDoS attacks are the latest generation of denial-of -service aimed at devices and networks with exposure to the Internet. So now there does not have to be such careful manipulation to place that single packet on a system that would currently know how to deal with such an event.

Hackers now exploit many un-witting computers attached and exposed on the Internet to do there biding for them, all at once. Who cares if the packets alone do not bring the target down? Without hacking password files or stealing sensitive data, a distributed denial-of-service hacker simply fires up a program that will generate enough traffic to a site that it denies service to the site's legitimate users. Trinity v3 is just the latest in a series of DDoS attack tools used for this type of job.

Trinity Defined

The Trinity DDoS tool is like similar tools that were used in February 2000 for attacks against the eBay, Inc., CNN, and Yahoo! Web sites, in that the tool must be installed on a compromised server running the open-source Linux operating system. This machine, along with others that have been compromised will form an army of un-wittingly remote controlled computers that launch packet floods against targeted web servers.

It has been discovered, however, that Trinity seems to be more sophisticated than these predecessors, because it allows the hacker to control the “zombied” machines through Internet Relay Chat (IRC) channels or America Online Inc.’s ICQ online chat service. [2]

Also, with earlier DDoS tools, attackers have to keep lists of all the machines they've broken into. But systems compromised by Trinity report back to an attacker via agents that appear in a single chat room.

How Trinity Works

In the following example from the Alert issued by Internet Security Systems (ISS), the agent binary is installed on a Linux system at /usr/lib/idle.so. When idle.so is started, it connects to an Undernet IRC server on port 6667. There is a list of servers in the binary:

204.127.145.17	205.252.46.98
216.24.134.10	216.225.7.155
208.51.158.10	205.188.149.3
199.170.91.114	207.69.200.131
207.173.16.33	207.114.4.35
207.96.122.250	

When Trinity connects online, it sets its nickname to the first 6 characters of the host name of the affected machine, plus 3 random letters or numbers.

i.e. compromised.machine.com → compro???

Trinity joins the IRC channel #b3eblebr0x using a special key. Once it's in the channel, the agent will wait for commands that can be sent to individual Trinity agents, or sent to the channel and all agents will process the command.

The flooding commands have this format: <flood> <password> <victim> <time>, where flood is the type of flood, password is the agent's password, victim is the victim's IP address, and time is the length of time to flood the agent, in seconds. [4]

There are many types of floods that can be issued to cause a DDoS. One of the most common are SYN attacks, which takes advantage of the IP handshake that connects two computers for data transfer. The hacker issues a flood of crafted SYN packets to the target machine with bad or non-existent origination IP addresses. The receiving machine sends its response in the form of a SYN-ACK and waits for the completion of the handshake by receiving the final ACK from the originator. However, since the original SYN had a bad IP address the SYN-ACK never reaches the perceived sender of the SYN. Since most host computers can only accept a rather small number of simultaneous connections, it is rather easy to fill the buffer of the host while it waits on the final ACK response. Once this occurs, a denial of service of service is created.

The next major DDoS is UDP flooding. Since UDP does not require formal connections to be established before data can be transmitted, this is a popular way for hackers to bombard a device that has known ports open to this protocol. Normally used as an internal on internal networks for applications to communicate, UDP essentially uses the broadcast method of transmitting data. This would potentially create a non-stop flood of data passing between the two systems disallowing much, if any legitimate data to pass.

Security conscious system administrators who use their firewalls and routers to filter such data patterns without causing their own DoS against themselves by denying all can eliminate both of these examples of DDoS attacks. There is a fine balance between filtering for bad or crafted data and creating your own denial of service, in which the bad-hats win anyway.

Scan and Removal

In order to determine if a specific system is has been compromised you must scan port 33270 for any connections. If found, telnet to that port and type "!@#". A system has been compromised if there is a root shell present after a successful connection to port 33270.

ISS gives the following in their Alert to identify a port-shell installed by Trinity:
Use "ps" and "lsof" [4]

```
# /usr/sbin/lsof -i TCP:33270
COMMAND  PID USER   FD   TYPE DEVICE SIZE NODE NAME
uucico  6862 root    3u  IPv4  11199       TCP *:33270 (LISTEN)

# /usr/sbin/lsof -c uucico
COMMAND  PID USER   FD   TYPE DEVICE    SIZE   NODE NAME
uucico  6862 root  cwd    DIR    8,1    4096 306099 /home/jlarimer
uucico  6862 root  rtd    DIR    8,1    4096      2 /
uucico  6862 root  txt    REG    8,1    4312 306589 /home/jlarimer/uucico
uucico  6862 root  mem    REG    8,1  344890 416837 /lib/ld-2.1.2.so
uucico  6862 root  mem    REG    8,1 4118299 416844 /lib/libc-2.1.2.so
uucico  6862 root    0u   CHR  136,2             4 /dev/pts/2
uucico  6862 root    1u   CHR  136,2             4 /dev/pts/2
uucico  6862 root    2u   CHR  136,2             4 /dev/pts/2
uucico  6862 root    3u  IPv4  11199           TCP *:33270 (LISTEN)

# ps 6862
  PID TTY      STAT   TIME COMMAND
 6862 pts/2    S      0:00 fsflush
```

Since the Trinity agent does not listen on any ports, it may be difficult to detect unless you are watching for suspicious IRC traffic. If a machine that has a Trinity agent installed is found, it may have been completely compromised. ISS recommends the operating system be completely reinstalled along with any available security patches. [4]

When it comes down to resolutions to DDoS, there are simple things that could be done by prudent security officers and network administrators that take proactive measures, instead of reactive measures, after being attacked. Like traffic heading into the office in the mornings, crafted packets targeted for a computer on your network can consume the bandwidth to your routers until all data communication is slowed to a crawl. Some devices have taken care of these problems, for example, if a web server is receiving too many hits, it starts throttling, or rejecting new connections so that existing connections

can still view pages or interact with the site. This also could be construed as a DoS by definition, but only to the affected web server, not the entire network.

If more routers were configured to implement this same practice, crafted packet traffic would be dropped before slowing the entire network down. Hackers that control remote computers to launch a DDoS have these "zombied" computers flood the target with crafted packets. Any router on that network receiving such packets should refuse to pass them along to the next router. Also, if a router detected a sudden surge in traffic to a destination machine in which every packet claims to originate from a different IP address (a sign of an attack using spoofed packets) it should not pass that traffic down the network. The router should throttle the traffic to avoid the packet flooding and alert and administrator so monitoring and analysis can begin as to the origin of the attack.

Not knowing where the crafted packets are originating from, and being hit by literally hundreds of computers acting on instruction to flood your router, web server or other vulnerable device on your network, makes DDoS attacks much harder to block than their DoS predecessors. With DDoS network administrators would find it a daunting task attempting to block address or ports *during* an attack at the firewall, by this time it is too late. Appropriate measures should be taken prior to such attacks. Closing the TCP and UDP ports on all your critical machines, firewalls and routers that your network or its users don't require, and monitoring the well-known ports that are used for any suspicious traffic, are prudent steps for any IT professional.

Conclusion

Reports indicate that at this writing, at least 400 Linux computers -- with IP addresses indicating they may be located mainly in the U.S., Romania and Australia -- have already been compromised by Trinity.[4] Information managers must take serious precautions to ensure their machines are not part of the unknowing solders of the Trinity warfare game and use approved scanners and implement sound policies and procedures to keep other DDoS attacks from causing legitimate e-businesses to loose valuable customer orders or employee communication to "Wiley Hackers".

As with the traffic on the highways, the first impulse to fix the problem would be to build larger roads with more lanes or install that larger pipe for data flow. But as high-speed internet connections become more and more prevalent for everyone and the tools for DDoS become smarter, like the Trinity tool taking advantage of known vulnerabilities in widely used operating systems, this would only be throwing money at a problem in hopes that we can eventually make the roads so large that we would never fill them up, with legitimate or crafted packets. The only real solution would be to control the access of what is traveling these roads, by implementing and monitoring the filters that are configurable in most equipment today. This however, relies on the necessity of having a security specialist working in every company who is attached to the Internet to ensure all networks are a safe place for data to travel.

Sources

[1] CERT Incident Note IN-2000-08. "Chat Clients and Network Security." CERT. 21 June 2000. URL: http://www.cert.org/incident_notes/IN-2000-08.html

[2] Harrison, Ann. "Denial-of-service aftermath." Computerworld. 02 February 2000. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO43013,00.html

[3] Harrison, Ann. "Users on guard against new denial-of-service tool." Computerworld. 08 September 2000. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO49889,00.html

[4] X-Force. "Internet Security Systems Security Alert." Internet Security Systems. 05 September 2000.URL: http://xforce.iss.net/alerts/advise59.php