GIAC
CERTIFICATIONS

# Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

# Distributed Denial of Service Attack Tools: trinoo and wintrinoo
# A Research Report Submitted in Partial Fulfilment of the SANS GIAC Program

Phillip Boyle

## Introduction

The week from February 6th to 12th, 2000, saw a number of attacks on prominent e-commerce internet sites such as Amazon, CNN, E*Trade, Yahoo and eBay. These attacks can be generically classed as Denial of Service (Dos) attacks with a further defining feature – the compromise of many distributed hosts to act as daemon or zombie machines. Each zombie carries out a Dos attack resulting in a vastly distributed and amplified attack – the Distributed Denial of Service (DDos).

The DDos attack relies on the covert existence of certain program tools on compromised machines. These tools enable an attacker to formulate, prepare and implement a DDos attack. The current report collates information on two common and related DDos attack tools: trinoo, a Unix based tool, and wintrinoo, a recent Windows based tool. To this end, details are provided of the attack anatomy, the tool structure and function, and possible lines of defence. Although details pertain directly to the (win)trinoo tools, certain generalities can be extracted that provide a coherent view of all DDos attacks (such as the TFN, TFN2K, Stacheldraht, and Smurf Attacks).

## Trinoo

Trinoo (also known as trin00) was the first well known DDos attack used against the University of Minnesota in August 1999. This two day attack involved flooding servers with UDP packets originating from thousands of machines. Source addresses were not spoofed, so systems running the offending daemons were contacted. However, the attacker responded simply by introducing new daemon machines into the attack. Trinoo was first found as a binary daemon on a number of compromised Solaris 2.x systems. Malicious code had been introduced through exploitation of buffer over-run bugs in the remote procedure call (RPC) services ‘statd’, ‘cmsd’ and ‘ttdbserverd’. (See CERT IN-99-04 for a description of these exploits).

The trinoo DDos formulation begins with the attacker compromising one of many master systems. These systems are set-up with vulnerability scanning tools, root kits (to conceal malicious programs, files and connections), the master and trinoo daemon programs, and a list of vulnerable hosts (which are potential daemon systems). DDos attack preparation involves the master(s) scanning for systems exhibiting the vulnerabilities described above (typically Solaris 2.x and Linux systems). A list of vulnerable systems is then passed to an exploit script that compromises each system, sets up and connects a listening shell (tcp port 1524), and compiles a list of successful compromises – or ‘owned’ systems. The list of ‘owned’ systems is passed to another script that installs the trinoo daemon and a root kit via the open tcp port 1524 – completing the construction of the ‘trinoo network’. (David Dittrich, 1999).

The DDos attack begins when the attacker connects (to masters) via telnet to tcp port 27665 and enters a password (the password was "betaalmostdone" in the case examined by Dittrich). Masters then pass command lines to daemons via UDP port 27444. These commands are password protected and are of the form: arg1 password arg2. Daemons respond to masters on UDP port 31335. Masters form a list of alive daemons by listening for the text "*HELLO*" in the data portion of UDP packets originating from daemons.

Attackers can send a number of commands to masters. Examples are:

- `quit` - to logoff from the master
- `dos IP` - to launch a DDos attack against the address IP
- `mdos` - to launch a multiple DDos attack
- `bcast` - to form a list of started daemons

Masters can send commands to daemons according to what the attacker has ordered. For example:

© SANS Institute 2000 - 2005 Author retains full rights.

- `aaa password IP` - Dos attack address IP by sending UDP packets to random (0-65534) UDP ports.
- `bbb password N` - Period of time in seconds to run Dos attack.
- `rsz N` - Set size of UDP packets to N bytes.
- `d1e` - Shutdown the daemon

Trinoo programs can be detected if active on the master and daemon systems unless root kits have been installed. The command: netstat -a --inet will show tcp port 27665 and UDP port 27444 open on the master, and UDP port 31335 open on the daemon.

### Wintrinoo

The addition of Windows machines to the pool of potential zombies increases the overall threat and destructive capability of DDos attacks. Wintrinoo is a Windows version of trinoo that was first reported to CERT on February 16th 2000 (CERT IN-2000-01). (Note that TFN2K, derived from TFN, also runs on NT and appeared in December 1999). In the wintrinoo case, zombies are formed by machines that run the program `service.exe`. Typically, this program comes to be executed in a number of ways:

- users run the program when it arrives as an e-mail attachment
- it is executed by document macros
- it is installed and run via Back Orifice.

When executed, `service.exe` installs a copy of itself to \windows\system and adds a registry entry making it restart when the system restarts. The pertinent key is:

```
HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/

CurrentVersion/Run
```

When running, `service.exe` will appear in the Windows task-list and it can be ended. However, `service.exe` will restart unless the registry entry is deleted. It must be noted that `service.exe` is distinct from the normal `services.exe`.

`service.exe` is approximately 23kB in size and will run on Windows NT4, 95 and 98. It differs from the trinoo daemon in that it listens for masters on UDP port 34555 and passes information to the masters on UDP port 35555. As with trinoo, this can be observed using the command: netstat -an. `service.exe` has been found on systems concurrently infected with Back Orifice suggesting that this trojan horse may have been the method of entry. (Gary Flynn, 2000).

### Defenses

The best defence against DDos attacks is to prevent initial system compromises. Generally, this involves installing patches, anti virus software, using a firewall and monitoring for intruders. However, even vigilant hosts can become targets because of lesser prepared, less security aware hosts (especially if these hosts have always-on high-speed internet connections). Many systems are compromised because patches for vulnerabilities reported and fixed months beforehand were never installed. Similarly, such systems have anti-virus software that is not up to date.

It is difficult to specifically defend against becoming the ultimate target of a DDos attack but protection against being used as a daemon or master system is more easily attainable. To this end, the following measures should be met (Gary Flynn, 2000):

- Check for frequent patches and subscribe to automatic vendor notifications
- Attempt to understand the vulnerabilities in your software and configuration
- Disable unnecessary network software
- Only accept program files from trusted sources (or at least be cautious)

For Unix operators:

© SANS Institute 2000 - 2005 Author retains full rights.

- Limit accessibility with network access control tools e.g. TCP Wrappers
- Use file system integrity checks e.g. Tripwire
- Download programs to test for common DDos attacks. For example:
  http://www.fbi.gov/nipc/trinoo.htm for Sun and Linux boxes
  http://www.theorygroup.com/Software/RID for all unix platforms. (Remote Intrusion Detector for detecting trinoo, TFN and stacheldraht DDos tools).

For Windows operators:

- Keep anti-virus (e.g. Norton) and anti-trojan (e.g. BOClean) software up to date
- Disable scripting on browsers and e-mail clients
- Run a desktop firewall
- Download Wtrinscan.exe which scans for wintrinoo

  http://www.jmu.edu/info-security/engineering/tools/wtrinscan.exe

### Conclusion

DDos attack tools are readily available and any internet host is targetable as either a zombie or the ultimate DDos focus. These attacks can be costly and frustrating and are difficult, if not impossible to eradicate. The best defence is to hinder attackers through vigilant system administration. Applying patches, updating anti-malicious software programs, system monitoring, and reporting incidents go further than retarding DDos attacks – these defences also protect against other attacks.

### References


CERT Incident Note 99-04. Similar Attacks using RPC Services. July 22, 1999. URL: http://www.cert.org/incident_notes/IN-99-04.html (April 17, 2000).

CERT Incident Note 99-07. Distributed Denial of Service Tools. Nov 18, 1999. URL: http://www.cert.org/incident_notes/IN-99-07.html (April 18, 2000).

CERT Incident Note 2000-01. Windows Based DDos Agents. Feb 18, 1999. URL: http://www.cert.org/incident_notes/IN-2000-01.html (April 18, 2000).

Dittrich, David . The DoS Project's "trinoo" Distributed Denial of Service Attack Tool. October, 1999. URL: http://www.staff.washington.edu/dittrich/misc/trinoo.analysis (April 18, 2000)

Flynn, Gary. DDos Attacks. March 30, 2000. URL: http://www.jmu.edu/info-security/engineering/issues/Ddos.htm (April 18, 2000).

Flynn, Gary. Wintrinoo. April 10, 2000. URL: http://www.jmu.edu/info-security/engineering/issues/wintrinoo.htm (April 17, 2000).

WatchGuard Technologies, Inc. Distributed Denial of Service. Feburary 2000. URL: http://www.watchguard.com/docs/ddos_wp.pdf (April 17, 2000).


© SANS Institute 2000 - 2005 Author retains full rights.