# Global Information Assurance Certification Paper

# Trinity v3 DDOS: Tomorrow's headline?

David Sheridan
September 19, 2000

## Introduction

Distributed Denial of Service (DDOS) attacks achieved major public awareness when the news media revealed how these attack techniques were used to paralyze several of the Internet's biggest web sites. In February 2000 Yahoo, Amazon.com, Ebay and Buy.com web sites were taken down for extended periods of time by DDOS tools. The suspect? A Canadian teen is awaiting trial in Montreal.

A hacker is capable of installing the Distributed Denial of Service (DDOS) software on many unsuspecting computers on the Internet. Once the hacker enlists these "zombies", the hacker can then issue simultaneous commands to all of the "zombie" computers initializing an attack on the target server or network. The attacks overwhelm the target by flooding it with large amounts of specially crafted network traffic.

A new DDOS tool that is even more dangerous than the kind used against Yahoo and Amazon has been found in the wild according to Advisory 59 from the X-Force. X-Force is the research and development team of Atlanta based Internet Security Systems Inc. In a news interview with Chris Rouland (director of X-Force) revealed that the Forum of Incident Response and Security Team brought the new tool to the X-Force's attention after an educational institution found the program running on some of its computers. This new DDOS tool has been named "Trinity v3" by the X-Force because the word Trinity appears several times in the code after reverse engineering it. Internet Relay Chat (IRC) controls the Trinity v3 agents. The hacker controlling the "zombies" is more difficult to trace and the "zombies" are easier to manage by the hacker. Rouland says that, using this new tool, reportedly over 400 hosts are running the Trinity agent with IP addresses indicating most locations are in the United States, Romania, and Australia.

In an interview with Network World, Rouland suggested, "There appear to be other IRC channels like this one as well". X-Force states that as of September 5, 2000, one IRC channel has 50 compromised hosts with Trinity running with more hosts connecting everyday.

With the large number of insecure computers on the Internet as potential "zombies" for Trinity, the potential for this new tool could be devastating. Initially, the potential of this tool is dependant only on the creativity of the hacker or hackers that control the private IRC channels for Trinity.

## Trinity v3

X-Force has analyzed a version of Trinity v3 obtained from the educational institution that first reported the software. Their Advisory 59 eludes that the possibility of new strains appearing cannot be ruled out, however to date none have been identified.

The Trinity binary is installed on a Linux system in the /usr/lib directory. The binary /usr/lib/idle.so connects to an Undernet IRC server on port 6667. Inside the binary the following Undernet IRC servers are listed:

204.127.145.17
216.24.134.10
208.51.158.10
199.170.91.114
207.173.16.33
207.96.122.250
205.252.46.98
216.225.7.155
205.188.149.3
207.69.200.131
207.114.4.35

The program connects to the IRC server and sets its nickname to be the first 6 characters of the hostname plus 3 random characters. The Undernet IRC channel that it connects to is #b3eblebr0x. The #b3eblebr0x channel is protected by a special key or password that is coded into the binary. Once the computer is in the special channel it simply waits for commands. Commands can be sent to individual Trinity agents or all Trinity agents that are logged on to the channel.

The hacker will have a much easier job with this new tool. Traditionally, the hacker must track the computers that have the agent installed. Trinity agents report their presence by logging on to the IRC channel and "reporting for duty" to the hacker. This also helps the hacker hide his real identity by changing the IP address for use on the IRC server.

The flooding commands that Trinity will respond to are crafted with this format:
<flood> <password> <victim> <time>

<flood> is the type of flood.
<password> is the agent's password.
<victim> is the victim's host or network ip address.
<time> is the length of time to flood the victim.
<flood> command are as follows:

tudp: "udpflood"
tfrag: "fragmentflood"
tsyn: "synflood"
trst: "rstflood"
trnd: "randomflagsflood"
tack: "ackflood"
testab: "establishflood"
tnull: "nullflood"

Other commands available are "ping", "size", "port", and "ver?". The ping command will respond with "(trinity) someone needs a miracle …". The version will respond with " trinity v3

by self (an idle mind is the devil's playground)".

On every computer where Trinity was found on, another rogue binary was discovered. This binary /var/spool/uucp/uucico is meant to look very similar to the real UUCP file transfer daemon that typically exists at /usr/sbin, /usr/lib/uucp or other default locations. This code has nothing to do with UUCP. When it loads it changes it's name to fsflush and is a simple backdoor program that listens on port 33270 for logon via telnet by the hacker. The hacker must supply the hard coded password "!@#" to access the system with a root shell.

# Detection

Scanning your systems with a scanner will be difficult to test for the Trinity agent since it doesn't listen on ports. Since the Trinity agent communicates with IRC the only way to detect the agent from the network would be to monitor IRC traffic.

Some sources recommend blocking all IRC traffic. The IRC ports as listed by the Internet Assigned Numbers Authority (IANA) are listed as 6665 – 6669, however I have seen my own IRC client connect to servers on ports 6660 up to 6671.

ISS's RealSecure Intrusion Detection System software can be configured to detect Trinity. They suggest to enable the IRC_Nick, IRC_Msg, and IRC_Join decodes to detect joins to the IRC channel #b3eblebr0x. Additionally, connection events to port 33270 may be configured to detect connections to a Trinity portshell backdoor program.

The Security Auditor's Research Assistant (SARA) that is based on the once revolutionary SATAN program has been updated to test for Trinity in SARA 3.2.1. The rc.firewall v4.1 that is an ipchains based Linux firewall has been updated to block the Trinity v3 DDOS tool.

Scan systems for port 33270 connections. If you find any connections, perform a penetration test by using telnet to port 33270. If a connection is established type "!@#". A positive test will give you a root shell, and a reasonable assumption that the Trinity agent is installed. According to X-Force the program can be confirmed with the following commands on the Linux computer:

Use "ps" and "lsof" in the following manner to identify a port-shell installed by Trinity:

```
# /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
```

# Conclusion

The stage is being set as more new hosts are compromised and connect to the IRC channel every day. Almost any host computer on the Internet may be affected by this new threat either by becoming a zombie or by becoming the target of an attack. Be relentless with security techniques on the computers within your control. Keep your systems up to date. Be sure that your private computers are not used as zombies by blocking all IRC traffic to the Internet. Above all, reporting all incidents to the proper authorities with forensic data intact will help deter future attacks.

# References


Internet Security Systems Inc. “Trinity v3 Distributed Denial of Service Tool”, Advisory 59, September 5, 2000
URL: http://xforce.iss.net/alerts/advise59.php, September 18, 2000.

Messmer, Ellen. “New hacker weapon poses Web threat”, September 9, 2000
URL: http://www.nwfusion.com/archive/2000/106548_09-11-2000.html, September 18, 2000.

Packet Storm is a division of Securify, Inc. “100 most recent additions to Packet Storm”
URL: http://packetstorm.securify.com/whatsnew100.html, September 18, 2000.

Advanced Research Corporation. “What’s New”, September, 2000
URL: http://www.www-arc.com/wn.html, September 18, 2000.

Bonisteel, Steven. “Nasty Denial-Of-Service Tool On Network Hosts – Experts”, September 5, 2000
URL: http://www.info-sec.com/denial/00/denial_090600a_j.shtml, September 18, 2000.

Internet Assigned Numbers Authority. “Port Numbers”
URL: http://www.isi.edu/in-notes/iana/assignments/port-numbers, September 19, 2000