**NIPC ADVISORY 00-055**

# "Trinity v3/ Stacheldraht 1.666" Distributed Denial of Service Tool

October 13, 2000

New variants of the Trinity and Stacheldraht Distributed Denial of Service (DDoS) tools have been found in the wild. As was demonstrated in February of this year, DDoS attacks can bring down networks by flooding target machines with more traffic than the machines can process. This advisory provides an update to previous NIPC DDoS advisories (issued since December 1999) on similar tools such as "mstream," "Tribal Flood Network," and "trinoo." The NIPC has recently determined that masters tied to zombies have been placed on many users' systems, heightening the possibility of a DDoS attack in the future. In addition to large corporate and university systems, affected users also include those with home computers having broadband access such as DSL and cable modem. The NIPC recommends that all computer network owners and organizations examine their systems for evidence of DDoS tools, including Trinity and Stacheldraht.

The "Trinity v3" Distributed Denial of Service (DDoS) exploit represents a potentially serious and continuing threat to networked computers running certain versions of the Linux operating system**.** Trinity v3 is a DDoS tool that is controlled via IRC or ICQ. When a system has been compromised and the Trinity v3 tool installed, each compromised machine joins a specified IRC channel and waits for commands. The Trinity v3 tool enables intruders to use multiple, Internet-connected systems to launch packet flooding denial of service attacks against one or more target systems. At least eight variations of Trinity have been found on the Undernet Internet Relay Chat network, each reporting to a different IRC channel. Trinity v3 responds to commands in IRC channels on lines beginning with "(trinity)," and the "Entitee" version of Trinity responds to lines beginning with "(entitee)."

System administrators should ensure their TCP Port Scanners are configured to scan port 33270 as machines found listening at this port may have the Trinity portshell installed. Trinity v3 is difficult to detect because the agent does not listen to specific ports to receive commands, but receives them over IRC. Watching for suspicious IRC traffic is useful in detecting Trinity v3. It is important to note that if Trinity v3 is found on a system, the system may have experienced root level compromise.

Stacheldraht consists of three parts -- a master server, a client, and an agent program -- and runs on Linux and Solaris machines. Stacheldraht performs several types of flooding attacks, and has IRC flooding options. The latest Stracheldraht variants, "Stacheldraht 1.666+antigl+yps" and "Stacheldraht 1.666+smurf+yps" prompt the user for a password when building the binaries.

The NIPC DDoS detection tool has been modified to detect Trinity v3 and some new variants of Stacheldraht. While the tool is designed to detect mutations of these DDoS tools, it may not detect all variants of the tools. NIPC will continue to update the detection tool as we receive new DDoS variants. Currently, the NIPC tool (find_ddos) detects the DDoS exploit in the following operating systems: Solaris on Sparc or Intel platforms, and Linux on Intel platforms. The tool currently detects mstream, tfn2k client, tfn2k daemon, trinoo daemon, trinoo master, tfn daemon, tfn client, stacheldraht master, stacheldraht client, stachelddraht daemon and trn-rush client. Please refer to http://www.nipc.gov/warnings/alerts/1999/trinoo.htm for more information.

- Readme
- Solaris on Sparc Executable File (tar, compressed format) version 4.2
- Linux on Intel Executable File (tar, compressed format) version 4.2
- Solaris on Intel Executable File (tar, compressed format) version 4.2
- Checksums (The MD5 Checksums are provided to verify the integrity of the files.)

Alternatively, specific technical instructions are available from CERT Coordination Center, SANS Institute, and other competent sources. CERT/CC, SANS Institute, and the University of Washington have

published information on distributed denial of service exploits that can be readily found at the following web sites:

http://cert.org/reports/dsit_workshop.pdf

http://www.sans.org/dosstep/index.htm

http://www.staff.washington.edu/dittrich/misc/ddos/elias.txt

Please report any illegal or malicious activities to your local FBI office or the NIPC, and to your military or civilian computer incident response group, as appropriate.