



CNET tech sites: [Price comparisons](#) | [Product reviews](#) | [Tech news](#) | [Dow](#)

Front Page

Enterprise

E-Business

Communications

Media

Personal Technology

advertisement

BE READY
for the next IT outage to strike.

Create a disaster recovery plan now to:

- ✓ Keep your data safe
- ✓ Recover faster
- ✓ Minimize lost productivity costs

[Learn More](#)

Hacker discloses new Internet attack software

By [Stephen Shankland](#)

Staff Writer, CNET News.com

February 14, 2000, 6:30 PM PT

A programmer familiar with attack software has disclosed three new attack programs of the type believed to have taken down major Internet sites last week, complicating the jobs of security experts trying to fight the malicious programs.

Three new versions, called Fapi, Shaft and Trank, are disclosed in a [paper](#) published today by the programmer known as "Mixer" at [Packet Storm](#), a site that publishes malicious software so security professionals can scrutinize it. Mixer is the purported author of a similar attack tool, Tribe Flood Network, and its sequel, TFN2K.

The software, of a breed called "distributed denial of service" ([DDoS](#)), is used to harness the collective abilities of a host of computers to swamp a target computer by inundating it with packets of information sent over the Internet. Some varieties are known, but apparently there are other versions of the software in circulation.



The newly disclosed versions likely evade programs [posted](#) by the [FBI](#) and others to detect TFN and two other publicly known versions, Stacheldraht and Trinoo.

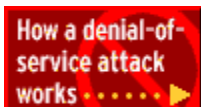
Another DDoS package, called Blitznet, also has been publicly available for at least two months at the Packet Storm site. Mixer said it was written by someone called "phreeon." Trinoo was written by "phifli," he said. As previously [reported](#), Mixer said Stacheldraht was written by "randomizer."

The newly disclosed DDoS software might sneak under the radar, but security companies are turning up some instances of the known versions.

Network Associates and its subsidiary [MyCIO.com](#) has discovered seven cases of computers infected with DDoS attack software, MyCIO chief executive Zach Nelson said.

His company provides an online detection tool that has been in high demand since the 100-person company unveiled it Feb. 10. Of more than 10,000 who have used it to scan their systems, the MyCIO software has found five cases of Stacheldraht, one of TFN and one of Trinoo, Nelson said.

Six of the seven instances were at educational institutions. The affiliation of the seventh couldn't be determined, Nelson said. In addition, six of the seven were in the United States, with the seventh in Germany. All seven systems have been taken offline, he added.



Search News:

[Advanced search](#)

Latest Headlines

[display on desktop](#)

[HP unveils new p](#)

[Execs point to wh the Web](#)

[3Com to leave Sil](#)

[U.S.-Singapore tr echoes DMCA](#)

[Software giant thi](#)

[Mozilla's Firebird clipped](#)

[Microsoft shows c prototype](#)

[House bets again gambling](#)

[Next Palm OS du](#)

[Protection sought critics](#)

[Former FCC offic AOL reprieve](#)

[XML group cooks database](#)

[Cisco profit up bu](#)

[Verizon rising in k data](#)

[PeopleSoft heads](#)

[HP's high-end str adaptive](#)

[Palm to work with licensees](#)

[DSL price war to i crown?](#)

[Emachines back i race](#)

[MSN Photo no lor](#)

[This week's hear](#)

News Tool

Nelson said MyCIO leaves it to the sites themselves to contact the FBI, which has [launched](#) an investigation into last week's attacks.

Gerhard Eschelbeck, vice president for MyCIO's security software, said his company's software detects the DDoS attack software by attempting to communicate with it. In addition, the software looks for blocks of text characteristic of the software.

Eschelbeck acknowledged that changes to the software or other versions won't necessarily be detected by MyCIO, but he said some fingerprints likely will remain.

[Print story](#)[E-mail story](#)[Order reprints](#)[Send us news tips](#)[Get news by](#)[XML](#) [What i](#)[Content licen](#)[Display news](#)

☒ **Enterprise**
Senior edi
Kanellos c
servers, ar
hardware t
business. (

☒ **Daily Disp**
Our award
editors del
stories rig
inbox. (dai

Your e-mai

Sign me up!

[All News.com ne](#)

[Send us news tips](#) | [Contact Us](#) | [Corrections](#) | [Privacy Policy](#)



Featured services: [Job Search](#) | [IT Community](#) | [Compare Prices](#) | [IT/IS Policies](#) | [MS Access](#)

CNET Networks: [Builder.com](#) | [CNET](#) | [GameSpot](#) | [mySimon](#) | [TechRepublic](#) | [ZDNet](#)

[Copyright](#) ©1995-2003 CNET Networks, Inc. All rights reserved.