



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

Front Page

Enterprise

E-Business

Communications

Media

Personal Technology

advertisement

**ATTENTION
ALL IT MANAGERS**

IT Manager's Tool Kit, Volume 2

- ▶ HR Templates
- ▶ Training Assessment
- ▶ Strategic Planning
- ▶ Budget & Cost Control
- ▶ Project Management
- ▶ Disaster Recovery



Learn More

The making of weapons--underground

By [Stephen Shankland](#), [Michael Kanellos](#) and [Mike Yamamoto](#)

Staff Writer, CNET News.com

February 9, 2000, 4:40 PM PT

The weapons used to bring down some of the most powerful companies on the Internet bear the markings of a small circle of anonymous programmers who create hostile technologies in the name of security research.

Although none of these individuals is accused of any wrongdoing, at least one name has emerged in interviews with CNET News.com in relation to this week's wave of "denial of service" assaults. A computer expert in Germany who goes only by "Mixer" is believed by some to be the author of the type of software that has been used to attack Yahoo, eBay, Amazon.com and other online giants.

No one has suggested that Mixer or any of his peers have carried out the assaults, but some of the tools used in these incidents appear to carry his technological signature. Although his software could have been easily replicated by others in today's trend toward "open source" coding on the Net, security analysts say certain signs point to Mixer as the author of the original programs.



In an interview with News.com, Mixer denied any responsibility in the incidents of the last three days but confirmed that he has written programs that appear similar to those used in the attacks.

"He's the author. Absolutely," said Gia Threatte, an expert at a computer security site called [Packet Storm](#), who said she communicates with Mixer by phone and email. "When he was coming out with the tools, he worked with us" so that the site could post his software.

Regardless of who is behind these particular cases, the [weapons](#) used in them can be traced to a loosely knit nether-community whose work can raise troubling ethical--if not criminal--questions.

These technophiles, and the programs they create, stand at the nexus of the underground Internet of years past and the profit-obsessed enterprises that are driving much of its growth today. That dichotomy makes it difficult to determine who's on which side, as well as their motives, especially when politically charged issues such as commerce vs. community come into play.

Robert Clyde, vice president at security company Axent Technologies, said programmers can often be divided into "white hats" and "black hats"--those who write software to expose vulnerabilities and those who use them to exploit an issue. As with most things in life, however, things aren't so simple: While the white hats like to portray themselves as above

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 offici AOL reprieve](#)

[XML group cooks database](#)

[Cisco profit up bu](#)

[Verizon rising in l data](#)

[PeopleSoft heads](#)

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

[Palm to work with licensees](#)

[DSL price war to crown?](#)

[Emachines back i race](#)

[MSN Photo no lor](#)

[This week's hear](#)

News Tools

the fray, he said, they often know how their work will be used after they post potentially malicious programs on the Web.

"This is in the same spirit as the people on the Internet who post how to build pipe bombs. You do bear some responsibility," Clyde said. "But the advantage is that (others) have a chance to protect against it."

These programmers, whose technical backgrounds vary widely, work with security professionals ostensibly to identify potential threats. In doing so, they regularly create hostile technologies that are used to test the security of firewalls, much like biologists identify and isolate strains of the flu in developing vaccines.

But in the uncontrolled environment of independent Internet research, these programs can fall into the wrong hands. And once they are "in the wild," as researchers call it, anything can happen.

Even Mixer, for example, said he was stunned by this week's events.

"The fact that I authored these tools does in no way mean that I condone their active use. I must admit I was quite shocked to hear about the latest attacks," he wrote in an email interview with News.com. "It seems that the attackers are pretty clueless people who misuse powerful resources and tools for generally harmful and senseless activities just because they can."

Ironically, Mixer has been working to protect against the very attacks his software makes easier. Threatte said he is the winner of a \$10,000 Packet Storm [contest](#) for the best way to defend against distributed denial of service attacks, which swamp a computer with improperly encoded packets of information that eventually render it unable to respond to regular network traffic.

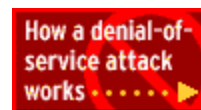
A security consultant at Security Focus said the tools used in the current attacks look like the software from a group of technologies known as the Tribe Flood Network family. The TFN family of software tools has been credited to Mixer, whose name appears in their code.

"I can't say for certain, but it looks just like the ones we've seen in the past," said Ryan Russell, MIS manager and security consultant at the company. "There is no reason to believe it is any different."

The exact nature and identity of the software used in the attacks won't be pinned down until one of the relay computers used in the incidents is examined. Nor is Mixer the only author of these types of tools. A program of undetermined origin called Trinoo came before Mixer's TFN, and a later one known as Stacheldraht Flood Network Demon was authored by someone who goes by the name "randomizer," according to the programming code.

One reason Mixer's work has become known is his postings on sites like Packet Storm and the Bugtraq computer security mailing list.

Threatte said the Packet Storm site has posted his attack tools so security professionals can examine them, adding that Mixer posts the tools elsewhere. Packet Storm, a division of security company [Kroll-O'Gara](#), advocates the philosophy that it's better to be able to scrutinize the tools doing the attacking.



Threatte said she believes that Mixer isn't involved in the attacks beyond writing software used in them. In addition, given the way these technologies work, it may be impossible to catch the perpetrators.

[Get news by](#)

[XML](#) [What's](#)

[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](#)

Tribe Flood Network 2K, or TFN2K, is an [updated version](#) of the earlier Tribe Flood Network. It has been used in the recent attacks, having been identified by a specific channel it uses to attack.

TFN2K hides the identity of the attacker by letting the attacker use other computers for the actual attack. These compromised intermediate systems used in recent attacks are scattered across many countries, Threatte said, making it more difficult for computer administrators to request that a particular attacking computer be shut down.

Groups and individuals have been bartering "constellations" of compromised computers that can be used in an attack, Threatte said, and the identity of the attacker is hard to know because TFN2K encrypts the signals used to control the software.

As she put it, "The evolution of these tools far outpaces anything that the security community is coming up with to protect against it."

[Print story](#)[E-mail story](#)[Order reprints](#)[Send us news tips](#)[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.