



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

Front Page

Enterprise

E-Business

Communications

Media

Personal Technology

New assault weapons pose threat to Web

By [Evan Hansen](#) and [John Borland](#)

Staff Writer, CNET News.com

February 8, 2000, 8:30 PM PT

A combination of new technologies and the rising stakes of online business may help explain this week's rash of outages at some of the largest companies driving the growth of the Internet.

The weapons used to execute "denial of service" attacks, which crippled major Web sites this week, have existed in rudimentary form for decades. But security experts say several effective [assault tools](#) that help automate the launch of such attacks have been released only recently.

With names like Trinoo, Tribe Flood Network and Stacheldraht (German for "barbed wire"), these tools take advantage of otherwise innocent computers connected to the global network to launch a vast flood of traffic at their targets.

Using these programs, attackers break into dozens or even hundreds of computers around the Net and install a kind of time bomb that is difficult to detect. At a later date, the attacker can send a command to all of the "slave" machines, which then wake up and start firing streams of information that clog their targets' networks.

Although these technologies have not been identified by the victims of the [last two days](#)--Yahoo, eBay, Amazon.com, Buy.com and CNN.com--most analysts predict that such attacks will become a fixture of the digital landscape. At a time when economic stakes and battles for control of the Internet are growing exponentially, the availability of these potential weapons may be too tempting for some perpetrators to resist.

"It does point out that high-profile attacks are likely," said Rob Enderle, an analyst at Giga Information Systems. "Companies need an action plan. They need to prepare."

Law enforcement authorities and Internet organizations have been worried about the spread of new assault technologies for some time. The FBI, the National Institute of Standards and Technology and Carnegie Mellon's Computer Emergency Response Team Center have issued warnings about the problem in recent months.

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 i crown?](#)

[Emachines back i race](#)

[MSN Photo no lo](#)

[This week's hear](#)

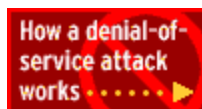
News Tools

[Get news by](#)

[XML](#) [What i](#)

[Content licen](#)

[Display news](#)



advertisement

Scale Security Service FREE Download

Repeat Intro

Service, meet Security.

Keep them together with Hostway.

30 DAYS FREE HOSTING

CLICK HERE!

Excluding Dedicated Servers

HOSTWAY THE HOSTING COMPANY

One of the first sites to be hit by this kind of massive, coordinated attack was the University of Minnesota, which was effectively shut down last August. In that incident, 227 computers were used to inundate the school's system with traffic, some of which were connected to the super-fast Internet 2 academic system.

No one has confirmed that these tools, or even something like them, have been used in any of the recent high-profile incidents. But security experts say it appears that this week's coordinated attacks are using something similar--and that means that the Web will continue to see such online terrorism.

"If this is someone who has a large collection of (slave) sites waiting to attack, they could literally fire off one attack after another," said Jim Magdych, director of security research for PGP Security, a division of Network Associates.

Many security analysts are betting that a single individual or coordinated group is responsible for the incidents of the last 48 hours. But that doesn't mean that other, unrelated attacks aren't lurking around the corner.

These tools are easy to download from the Net, experts say. The FBI already said it has found traces of the attack tools widely distributed on potential host networks, raising the possibility of a new wave of outages.

Network administrators say there are few [sure-fire defenses](#) against such attacks. Yet industry analysts said they see little evidence of a crippling threat to Internet commerce in the long term.

This week's strikes were relatively brief, presumably to help keep the perpetrators from being easily caught. In addition, blitzes of the scale that brought down Yahoo are still thought to be difficult to organize.

"It could last for days," Magdych said. "But in that case, the odds of somebody noticing go up a lot."

Theoretically, sites have been vulnerable to such attacks for years--and knowledgeable Internet users have not been shy about using them, generally as a means of protest. Online toy seller eToys, for example, was targeted last month by Net users upset over the company's [legal efforts](#) to shut down the domain name of an art group going by the name of etoy.



Other victims include various government sites, such as those operated by the U.S. Navy and NASA.

But this week's attacks have raised the ante in terms of scale. The Yahoo incident, for example, involved as many as 50 computers working in tandem and delivered at the peak a crippling gigabit of data per second to disable the system.

Some observers said they see a link between the first attack and the timing of a network service provider conference this week. The North American Network Operators Group (NANOG) gave a presentation yesterday on denial of service attacks at about the same time Yahoo was hit, leading to speculation that hackers may have used the occasion to send a message.

"I don't think that was a coincidence," said Daniel Todd, director of public services for Keynote Systems, which tracks the performance of Internet sites.

As of late today, however, no one had stepped forward to claim responsibility for the attacks.



- ☒ **Enterprise**
Senior edi
Kanellos c
servers, ar
hardware t
business. (
- ☒ **Daily Disp**
Our award
editors del
stories righ
inbox. (dai

Your e-mail

Sign me up!

[All News.com ne](#)

Although federal investigators met with Yahoo today to discuss the outage, no formal inquiry has been announced.

Regardless of magnitude or motive, many believe that this kind of high-profile attack may now be a fact of digital life.

"This is relatively easy to do and not easy to defend against," said Peter Neumann, a security analyst for consulting firm SRI International.

"People have been pretty complacent in the past. But that's like saying we've never had an electronic Pearl Harbor, so there's no need to worry."

[Print story](#)

[E-mail story](#)

[Order reprints](#)

[Send us news tips](#)

Related News

- [Computer security teams brace for attacks](#) December 20, 1999
- [Get this story's "Big Picture"](#)

[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.