



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

Front Page

Enterprise

E-Business

Communications

Media

Personal Technology

advertisement



Execute your projects with expert proficiency

- Define your projects and resources
- Manage changes to avoid scope creep
- Implement quality management processes

- Minimize project costs
- Empower and lead your team
- Schedule effectively and avoid bottlenecks

BONUS CD includes: entire book contents, customizable project templates, plus, 4 Microsoft Project tutorials

CI

Hackers attack NASA, Navy

By [Paul Festa](#)

Staff Writer, CNET News.com

March 4, 1998, 2:40 PM PT

update [NASA](#), the [Navy](#), and university campuses throughout the nation were the targets Monday evening of "denial of service" attacks on computers running [Microsoft](#) Windows NT and Windows 95 operating systems.

The attacks, waged over the Internet, made computers crash and caused what is known as the "blue screen of death" --a reference to the blue screen that accompanies Microsoft's "fatal error" message.

NASA and university systems managers said that, while the attacks cost them time, there was no reported data loss or other permanent damage.



CNET Radio talks to Strong Crypto's Chris DiBona

Educational institutions including the University of California campuses at [Berkeley](#), [Los Angeles](#), [San Diego](#), and [Irvine](#); the [Twin Cities Campus](#) of the University of Minnesota; the [Massachusetts Institute of Technology](#); [Cornell University](#); [Princeton University](#); the [University of Washington](#); the [University of Texas at Austin](#); and the [University of Wisconsin at Madison](#), a NASA research partner, also were targeted. A reported attack on computers at [Northwestern University](#) could not be confirmed.

Navy computers in Point Loma, California; Charleston, South Carolina; Norfolk, Virginia; and elsewhere also were affected, according to a report by the [San Diego Union-Tribune](#).

The attacks were of the type known variously as "New Tear," "Bonk," or "Boink," according to Microsoft security product manager Jason Garms. Microsoft [in January](#) posted patches to protect against "New Tear" attacks.

Microsoft is working with affected NASA centers and educational institutions to hunt the source of the attacks. Some of the targeted institutions are enlisting the aid of the [FBI](#), according to Garms. The FBI declined to comment on the matter.

Garms declined to specify which others in addition to the NASA, Navy, and university sites were attacked. But he did describe the targeted group as "a large cross segment of government sites and educational institutions."

Last night, Microsoft posted a [security bulletin](#) on the attack describing the problem and advising users to implement its fix.

[MCI Communications](#) also circulated a security announcement on the attack to its network

Search New:

[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 k 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

customers, according to a systems engineer at [Yale University](#). Yale did not report being targeted in the attack.

Systems were restored simply by rebooting the computers. In some cases, the computers were programmed to reboot automatically in response to the attack, so users returned to work this morning without any knowledge that their computers had been targeted.

"Denial of service" attacks prevent servers from answering network connections and can crash individual computers. In one form, for example, servers are fooled into thinking they are going to receive a certain type of data packet. When that particular packet never arrives, the servers hang up.

Systems administrators reported that some computers with patched operating systems did fend off the attack.

"There's a patch Microsoft has for it," said [Ames Research Center](#) computer security manager John Ray. "It hit some of our systems that didn't have the patch."

About 50 of Ames's approximately 3,000 computers were affected, Ray said.

At the [Jet Propulsion Laboratory](#) in Pasadena, California, spokesman Frank O'Donnell questioned whether the lab could have protected against the attack with a patch.

"Microsoft actually issues a steady stream of patches in the general area of network connectivity," O'Donnell said. "It's not certain to us at this point how this particular attack came in, so I don't think we can say with certainty that there's a patch that would have prevented this attack."

But Microsoft's Garms said preliminary evidence collected yesterday from the targeted sites suggested that the problem was of the same type the January fix addressed, and that only computers lacking the fix were affected.

"There's no new issue here," Garms said. "But many sites haven't secured up-to-date security patches."

O'Donnell said the matter was under investigation and that, pending a decision on the implementation of patches, a network protective solution had been imposed. He declined to specify what measures the JPL had taken.

O'Donnell stressed that no sensitive information affecting space missions was endangered during the attack and that all systems that control spacecraft were behind firewalls.

The attack comes as the nation's attention is focused on the issue of hacking after two California boys allegedly [hacked computers](#) at the Pentagon. Monday night's attack also coincided with testimony by Microsoft chief executive Bill Gates before the Senate Judiciary Committee regarding competitive practices in the software industry.

NASA sites reporting the attack are as follows: [NASA Headquarters](#) in Washington; [Ames Research Center](#) in California; [Dryden Flight Research Center](#) in California, [Goddard Space Flight Center](#) in Maryland; [Independent Validation and Verification Facility](#) in West Virginia; [Jet Propulsion Laboratory](#) in California; [Kennedy Space Center](#) in Florida, [Langley Research Center](#) in Virginia; [Lewis Research Center](#) in Ohio; [Marshall Space Flight Center](#) in Alabama; [Moffett Federal Airfield](#) in California; [Stennis Space Center](#) in Mississippi; [Wallops Flight Facility](#) in Virginia; and [White Sands Test Facility](#) in New Mexico.

[Johnson Space Center](#) in Houston did not send out an automated security incident report,

[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](#)

according to Ames spokesman John Bluck.

[Print story](#)

[E-mail story](#)

[Order reprints](#)

[Send us news tips](#)

Related News

- [A question of safety](#) February 19, 1998
- [IE 4 URL bug resurfaces](#) January 14, 1998
- [Get this story's "Big Picture"](#)

Also from CNET Networks

- [IT professionals needed at top companies now](#)
- [Check out the car of tomorrow in CNET's guide to car tech](#)
- [Tech QA and discussions for IT pros](#)
- [Configure a DSL modem for your home](#)
- [New digital camera book plus free CD-ROM](#)

[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.