

20 August 2003

Robert Lemos
CNet News.com
235 Second Street, 6F
San Francisco, CA 94536
Phone: (415) 344-2975

FOIA/Privacy Act Officer
U.S. Nuclear Regulatory Commission
Mail Stop T-6 D8
Washington, DC 20555-0001
Fax: 301-415-5130

FOI/PA REQUEST

Case No. 2003-0399
Date Rec'd. 8-21-03
Action Off. Phamling
Referral Case: _____

RE: Freedom of Information Act (FOIA) Request -- Expedited

Dear FOIA Officer:

CNet News.com, a major technology news Web site, makes the following request of the U.S. Nuclear Regulatory Commission (NRC) pursuant to the Freedom of Information Act (FOIA), 5 U.S.C. 552.

CNet requests the release of any documents produced on or after July 16, 2003 that detail whether computers at any federally regulated energy company or industry organization were vulnerable to or compromised by a computer worm, in particular MSBlast. We also request the release of any documents that discuss the effects of a computer worm on the computers that manage, control or are connected to the energy networks and any document that discusses whether a computer worm may have caused the outage, or contributed to the outage, that struck the northeast United States and Canada on August 14, 2003.

The following companies and organizations may have provided information to NRC that falls within this request:

- 1) FirstEnergy Corp., Akron, Ohio
- 2) Midwest Independent Transmission System Operator
- 3) Consolidated Edison, New York
- 4) North American Electric Reliability Council
- 5) Northeast Power Coordinating Council
- 6) New York Independent System Operator


MSBlast--also known as W32/Blaster and W32.Lovsan--hit computers running the Microsoft Windows operating systems on August 11, 2003. The worm used a vulnerability in Microsoft Windows to propagate. Information about that vulnerability was first released on July 16, 2003. Energy companies may have analyzed their systems for the vulnerability to gauge their security posture on or after that date.

Many of the systems used to control and monitor energy networks--called supervisory control and data acquisition (SCADA) systems--run on Windows NT and 2000 computers and could have been disrupted by the MSBlast computer worm on or after August 11, 2003.

CNet News.com believes that the vulnerability of energy systems to an Internet attack of this nature is of significant public interest and intends to publicly report the results of this inquiry. CNet will pay reasonable fees of up to \$250 for any expenses incurred by FERC to prepare the information. CNet asks that the request be expedited because, without public dissemination, companies responsible for critical portions of the United States' infrastructure may remain vulnerable to such threats in the near future.

These statements are true and correct.

Sincerely,


Robert Lemos
Senior writer, CNET News.com