NIPC ADVISORY 99-013

"Explorer Zip Worm"

June 10, 1999

The National Infrastructure Protection Center (NIPC) has received reports that tens of thousands of computer systems in several major U.S. companies have had their files infected,damaged or destroyed by the Explore.Zip Worm. This program arrives as an e-mail message and utilizes MAPI commands and Microsoft Outlook on Windows systems to propagate itself. The virus e-mails itself out as an attachment with the filename zipped_files.exe. The virus selects addresses from the infected computer's e-mail in-box and therefore appears to come from a known e-mail correspondent. Most significantly, the virus searches through system drives and destroys a series of files by making them zero bytes long, resulting in irrecoverable data and/or systems. Updated commercial anti-virus software appears to successfully protect against this virus. Updated software has been posted on the Internet web sites of Symantec and Network Associates Incorporated.

NIPC Director Michael A. Vatis states, "Because of the destructive payload delivered by this virus, its potential impact is significant. All e-mail users should exercise caution when reading their e-mail for the next few days and bring unusual messages to the attention of their system administrator. As was the case with Melissa, the transmission of a virus can be a criminal matter, and the FBI is investigating."

The public is requested to please report information concerning damage from infections by these viruses to your local FBI Office, the NIPC, or Computer Incident Response Group, as appropriate. The NIPC Watch and Warning Unit can be reached via e-mail at nipc.watch@fbi.gov, or by telephone at (202) 323-3204.

More information on this virus and how to protect against it is available through the Carnegie Mellon CERT web homepage, and through commercial anti-virus vendors.