Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

March 15, 2006

MALICIOUS SOFTWARE BEING USED IN EXTORTION SCHEME

The FBI has been alerted to an Internet extortion scheme in which malicious software is utilized to hold a user's files hostage until a ransom is paid.

The scheme involves the use of a Trojan called Cryzip. When run, Cryzip searches the hard drive of the infected computer for files which it will then zip and encrypt. When the victim attempts to open one of his files, Cryzip opens a text file which informs the victim that his files have been encrypted with an unbreakable password, and he must pay the sum of $300.00 to get the password to have access to his files. The victim is given instructions on how to open an E-gold account and transfer the payment. The text file provides an E-gold account number which is randomly generated from a list embedded in Cryzip's code. The text file advises that within 24 hours of payment confirmation, the victim will receive a link to the password to unzip the files.

The computer security company LURHQ Corporation reports that at this time this does not appear to be a widespread attack but may be indicative of a future trend in malicious software use.

Consumers are reminded to keep backup copies of important files stored on external media, and to be sure that their anti-virus software is updated regularly. **CONSUMERS ARE FURTHER ADVISED TO USE CAUTION WHEN OPENING E-MAIL ATTACHMENTS OR WHEN DOWNLOADING FILES FROM THE INTERNET.**

If you have received this, or a similar hoax, please file a complaint at www.IC3.gov.