

IT Backbones™

Security News



**INTERNET CONTENT
RATING ASSOCIATION**

An independent, non-profit organization
whose mission is to protect children
from potentially harmful material

The IT Shield - Dedicated To IT Security Issues, Featuring News, Press Releases, IT Directory & Links

[Home](#)[About Us](#)[Contact](#)[News Archive](#)[Submit PR](#)[Product Reviews](#)[Web PR](#)[Briefings](#)[Advertising](#)[Pricing](#)

- [ITReseller.com](#)
- [Video News](#)
- [Events Diary](#)
- [Quick2IT](#)
- [Need2Source](#)
- [Time & Money](#)
- [Free Web Conferencing](#)

Virus Blackmails You Into Paying Ransom

Published 16th March 2006

Call it Internet imitating real life! The hostage and ransom situation is coming to the cyber space in the form of a Trojan that holds up your files for a cool \$300. You pay up the money to get your files back. Bold and bizarre? You bet!

Experts at MicroWorld Technologies inform that the Trojan named 'Win32.Zippo.10' or 'cryzip' is a sophisticated variety that encrypts user files into Zip format. Once your data is locked up, you are left with a ransom note kept in a file 'AUTO_ZIP_REPORT.txt'

Written in poor English fraught with typos, the threat message goes like this, "INSTRUCTIONS HOW TO GET YUOR FILES BACK READ CAREFULLY. Your computer caught our software while browsing illigal porn pages, all your documents, text files, databases was archived with long enought password."

It warns strictly against any attempt at cracking the password of the encrypted data. To get the files back you can pay the ransom of \$300 to an E-Gold account owned by the Trojan creator. A random E-Gold account number gets displayed at the top of the mail from a smartly embedded list. The culprit operates with numerous accounts that make it hard to pin him down.

"This online extortion is direct and on the face! The ploy can be quite effective in a targeted attack on sensitive and confidential files of a corporate house or an individual.

To safeguard the information integrity, one would just like to get done with it by paying the sum,” views Govind Rammurthy, CEO, MicroWorld Technologies.

Originated in May 2005, this brand of Trojan is generically referred to as ‘ransomware’. Technologically, they are advancing and evolving to make it hard to detect for many AntiVirus solutions that merely depend on signature scanning. Since the writer of the Trojan seems to be quite an expert, high variance in code pattern and fundamental mutations are observed.

“The degree of proliferation is low at this point of time, primarily due to the targeted nature of attack. These guys deliberately keep a low profile to escape wide-spread attention as they mean business,” points out Govind Rammurthy.

MicroWorld security solutions eScan and MailScan are updated automatically to ensure round the clock protection for users from new and emerging threats like these. You change your code or change your face, but you can’t escape the MicroWorld RADAR. Because it firmly believes in staunchly protecting users from broad day light robbery on Information Super Highway.

Company Profiles powered by ITReseller.com

- MicroWorld Technologies Inc - [View profile](#)

[Links](#) | [About Us](#) | [Privacy Policy](#) | [Contact Us](#) | © 2004-2006 IT Backbones Limited

Site developed and hosted by [Design Solution](#) Ltd.