

IT BackbonesTM

Security News



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](#)
- [Contact](#)
- [Submit PR](#)
- [Search News](#)
- [What We Can Offer You](#)
- [IT Events](#)
- [Time & Money](#)

Trojan Takes Files To Hostage, Asks For Ransom!

Published 6th June 2006

A new Ransomware that started circulating since the first week of May is getting wider in proliferation with more reports of its infections coming in from various sources. Security Experts at MicroWorld Technologies inform that the malware named as 'Trojan.Win32.MayArchive.a', directs users to buy pharmaceuticals worth \$75 from a Russian website at virtual gunpoint...

Ransomware is often a Trojan that steals files, encrypts them and then asks for a ransom in return of a password that lets you regain access to those files. MayArchive is a bit different in that sense as it does not encrypt files but strings them together and archives them in a file by the name 'EncryptedFiles.als'. Then it deletes all the original files and creates a text file in the same folder by name "INSTRUCTIONS HOW TO GET YOUR FILES BACK".

It reads,

"Do not try to search for a program that encrypted your information – it simply does not exist in your hard disk anymore. Reporting to police about a case will not help you, they do not know the password. Reporting somewhere about our email account will not help you to restore files. Moreover, you and other people will lose contact with us, and consequently, all the encrypted information."

As the only way to get your files back, it directs you to spurious online drug stores and

tells you to buy from a few medicines listed over there. As soon as your order is verified, it guarantees to send you the password to unlock the files.

“Our products eScan and MailScan have been updated with the cure for this Trojan since May 9, 2006 and users updating the software regularly have no reasons to worry,” says Sulabh Mahant, Security Analyst, MicroWorld Technologies. “MicroWorld had reported about ‘Win32.Zippo.10’ in the month of March, which asked for a \$300 direct transaction into an E-Gold account in return of the hijacked files! Definitely, Ransomware is on the rise and they are trying different technologies and modes of transaction.”

In the wake of these emerging Ransomwares and the increasing media attention that they are attracting, there’s another breed trying to make the most of it by cashing in on the general ignorance of users. A recently found malware termed as Ransom.A, would scare the infected user with a full screen message every time he logs on. The coercing message tells the user that one file per 30 minutes will be deleted from the hard drive and the files will be restored when user pays up \$10.99 via Western Union. The fact is that the Trojan is just a pretentious bully and doesn’t do what it claims!

Experts at MicroWorld have been closely monitoring the metamorphosis of Ransomware and how it could play out in the future. Govind Rammurthy, CEO, MicroWorld Technologies, observes “Ransomware is in its fledgling stages and has still not grown to a level where it can become a large scale threat. But what’s worrying is the fact that this breed is fast advancing in technology and can be used in enterprise level information hijack and extortion. Its newfound connection with international Drug Syndicate, emerging with ‘MayArchive’, is another cause of concern as well.”

Company Profiles powered by ITReseller.com

- MicroWorld - [View profile](#)

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

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