



[Home](#) | [Forums](#) | [Archives](#) | [Search](#) | [Speedtest](#) | [Advertising](#) | [Contact](#) | [About & Link](#) | [RSS](#)

Links

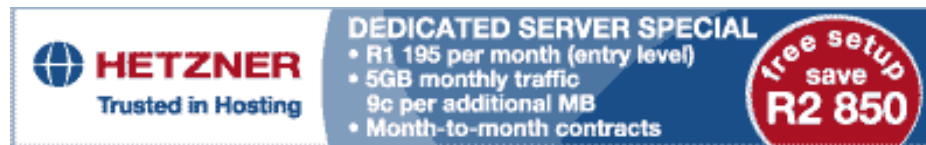
- [Home](#)
- [Speak Your Mind](#)
- [Blogs](#)
- [Podcast](#)
- [Downloads](#)

Categories

- [Telecoms](#)
- [Broadband](#)
- [ADSL](#)
- [3G & Cellular](#)
- [MyWireless](#)
- [iBurst](#)
- [Gaming](#)
- [Hardware & Software](#)
- [International](#)
- [Business & General](#)

News Partners

[Home](#) ▸ [Hardware & Software](#)



Trojan takes files to hostage, asks for ransom

By ICTWorld, 7 June 2006



There are more reports of infections of a new Ransomware, which started circulating in the first week of May. 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 Web site at virtual gunpoint.

Ransomware is often a Trojan that steals files, encrypts them and then asks for a ransom in return for a password that lets users 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 the case will not help, they do not know the password. Reporting somewhere about our e-mail account will not help you to restore files. Moreover, you and other people will lose contact with us, and consequently, all the encrypted information."

Related Articles

- [Killer products fail to show at Taipei IT fair](#) 06/08/06
- ['Dell workstations 155% faster'](#) 06/07/06
- [Flash memory - a key element in digital lifestyle technology](#) 06/06/06
- [Microsoft's ad attack](#) 06/05/06
- [Computer pack top dogs lose their bite](#) 06/05/06
- [Microsoft delivers desktop designed for Mac users](#) 06/02/06
- [FLAT PANEL TV MANUFACTURERS SET TO BE WINNERS](#) 06/02/06
- [Turning conceptual ideas into usable technology](#) 06/02/06
- [Double the trojans, half the worms](#) 06/01/06
- [New spyware program blackmails users](#) 05/31/06

Sponsor

[Financial Mail](#)
[Business Day](#)
[Business Report](#)
[MoneyWeb](#)
[ICT World](#)
[Finweek/Fin24](#)

Sponsor

As the only way to get their files back, it directs victims to spurious online drug stores, and tells them to buy from a few medicines listed there. As soon as the order is verified, it guarantees to send the password to unlock the files.

“Our products eScan and MailScan have been updated with the cure for this Trojan since May 9 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 for the hijacked files. Ransomware is definitely on the rise, and its writers 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 is another breed trying to cash in on the general ignorance of users. A recently found malware termed as Ransom.A, attempts to 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 that the files will be restored when the user pays up \$10,99 via Western Union. The fact is that the Trojan is just a pretentious bully, and does not do what it claims!

© 2006 MyADSL, All Rights Reserved.



Platinum
ADSL
for sheer
internet pleasure
DataPro
INTERNET SOLUTIONS FOR THE REAL WORLD
[click here](#)

News Discussions

Advertisement