

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



Finjan gives you protection that signature-based products **cannot even see**

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

- [Home](#)
- [About](#)
- [Submit News](#)
- [Search News](#)
- [IT Events](#)
- [Time & Money](#)
- [European Media](#)

Trojan Comes As Codec, Brings In Many Malware

Published 24th December 2007

It may come in an email asking you to check out a movie file. Or it may seek to push its way to your computer from malicious websites. In both cases a 'codec' will be offered in the guise of helping you watch a streaming video (a steamy one on many occasions), but instead of showing the movie it will install a stealthy Trojan Downloader in your computer. That's Zlob Trojan for you!..

Security experts at MicroWorld Technologies warn that a new Zlob variant named Zlob.fes is spreading among unsuspecting computer users. When a user visits certain websites, a harmful code named 'Trojan.HTML.Agent.e' is downloaded without the user's knowledge. This file prompts an error message that says the browser has encountered an Active-X error and needs to download a codec to play a video file.

When a user clicks on 'Yes' button and proceeds to download the codec, a License Agreement is displayed to make him believe that the program is authentic. The name of the downloaded file is 'VideoAccessCodecInstall.exe', which in fact is Zlob.fes. Once inside the computer, Zlob.fes downloads many other kinds of malware.

"Codec is a program used to encode or decode video clips so that large files can be downloaded faster," explains Vikas Vishwasrao, Assistant Manager R&D, MicroWorld. "Most web users are familiar with codecs and naturally some wouldn't think twice before

clicking on the 'yes' button to download it. Since the Trojan shows no sign of its presence in the infected computer, a victim may never know about the infection till the time the computer screen gets all filled up with annoying pop-ups that simply refuse to cease!"

The first Zlob appeared in year 2005 and since then several variants of the Trojan Downloader have been coming out with no sign of a let-up, trying out different baits and spreading routines. Initially most Zlobs came only from porn sites. But of late, keeping pace with the Web2.0 phenomenon, the Trojan Downloader has migrated into Social Networking and Video sharing websites. The user posted content in these sites offer perfect opportunities for malware authors to upload harmful files and lure victims into downloading them.

Many Zlob variants are seen bringing in a range of malware like Spyware, Adware, Rogue-AntiSpyware, Rogue-AntiVirus, Backdoor, Bots, Rootkits and more to compromised machines. A computer infected with a Zlob is thus exposed to a chain of many more online threats.

MicroWorld's AntiVirus, AntiSpam and Content Security software eScan provides protection against all spreading routines of Zlob family. The email route is checked as it scans and cleans all incoming mails. Browser vulnerabilities are guarded against as the software plugs those loopholes. It can block HTML agents like the one used in the case of Zlob.fes, as well as detect the malware on the fly during manual download.

Company Profiles powered by ITReseller.com

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