

## ADVISORIES

- Apple Security Update - Safari 3 Beta 3.0.4 Security Update v1.1 • Apple Security Update - Security Update 2007-009 v1.1
- US-CERT Technical Cyber Security Alert - Adobe Updates for Multiple Vulnerabilities (TA07-355A)

## VULNERABILITIES

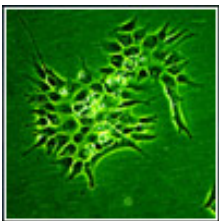
- TIBCO Rendezvous RVD Daemon Remote Memory Leak DoS • CA BrightStor ARCserve Backup Message Engine Insecure Method Exposure Vulnerability • Mac OS X TIOCSETD IOCTL Kernel Memory Corruption Vulnerability



**Qualys:** [Free Whitepaper: Operationalizing Security & Policy Compliance - A Unified Approach for IT, Audit and Operation Teams](#)

## Trojan comes as codec, brings in many malware

Posted on 24.12.2007



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.

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.



**QUALYS™**

EFFECTIVE REMEDIATION  
OF NETWORK  
VULNERABILITIES AND  
POLICY COMPLIANCE

DOWNLOAD GUIDE >



Find out more today and  
benefit from this limited offer!



**NEW! FOCUS ON ATTACKS AND WIRELESS SECURITY**

**New Threats, New Solutions.**



February 18-21  
Westin DC City Center

**Black Hat** DC 2008

SPONSORED LINKS

[Vulnerability Scanning](#)

[Network Vulnerabilities](#)

[Kaspersky Internet Security 7.0](#)

[Network Server Monitor](#)

[Security Camera DVR](#)

[Home Security](#)

[Security software Australia](#)