

30 August 2006

By: Marius Oiaga, Technology News Editor



Zcodec Alters Search Engine Results

And the adware performs additional actions

Panda Software has reported through a press release the identification of a new malicious piece of software dubbed Zcodec. Disguised as an application that promises to install video codecs for a variety of multimedia formats, Zcodec is in actuality an adware program protected by a rootkit. Once on a compromised machine: "ZCodec creates an EXE file, in the directory C: Program Files HQ CODEC. This file is deleted once it is run. And another EXE file, with a random name, in the Windows system directory. This file is injected into the Internet Explorer process, in order to be activated whenever the user uses this web browser," stated Panda software. The infected machine will present altered DNS settings so that traffic via search engines is redirected to other Web pages than those displayed in the links of the returned results, in order to draw users to illicit pay-per-click systems or to data stealing schemes. Additionally, the adware performs two random actions. It either downloads and installs the Ruins.MB Trojan horse or repeatedly prompts the users with install notifications of a casino application. "The combination of different techniques is becoming a frequent trait of computer attacks. In this case we see social engineering, rootkits, Trojans and even the manipulation of computer settings. The aim of the creators is to infect computers without arousing suspicion. Given that there are many such malicious programs on the Internet, it is vital to protect systems with a good antivirus, which objectively scans each file on the computer," explains Luis Corrons, director of PandaLabs.