

February 2008 Technology News Editor

[From Paris Hilton to Avril Lavigne - Free Porn Slaughters Windows](#)

Courtesy of Troj/Exchan-Gen

There are little incentives as popular in their inherent association with widespread malware spamming campaigns as sexual references/invitations/promises. The ultimate combination designed to easily convince users in becoming victims of malicious code infections is a bundle of free pornography with high profile celebrities. The latest spam campaign set up to spread the Troj/Exchan-Gen Trojan horse makes good use of the same old items in the spammers' bag of tricks in order to have users hand over their Windows-based machines. "Spammers have changed the distribution method of Troj/Exchan-Gen. The [attackers] are still using 'Celebrities' to lure users into installing their malware. Obviously the spammers are hoping that people will want to know more about the their favorite stars," revealed a member of the SophosLabs. The links served via unsolicited email do not point directly to the malicious website hosting malware, but instead use a Google redirection in an attempt to fool the end users, but also ensure a difficult detection for anti-spam solutions. Celebrity news is without a doubt a very attractive and active lure for malware, and the combo with porn is a recipe designed for "success." The links spammed include references to Paris Hilton, Jennifer Lopez, Avril Lavigne, Jessica Alba, Madonna, Milla Jovovich, Jennifer Aniston, Demi Moore, Penelope Cruz, and many more Hollywood stars, along with the promise of pornographic content. What the users will indeed get is Troj/Exchan-Gen. "[Troj/Exchan-Gen](#) is a family of Trojans for the Windows platform. Members of Troj/Exchan-Gen usually attempt to copy themselves to the Windows system folder, often with a filename of CbEvtSvc.exe or CcEvtSvc.exe, and create a service with the same name to run this file automatically on startup, creating registry entries at the following location: HKLM - SYSTEM - CurrentControlSet - . Members of Troj/Exchan-Gen typically attempt to connect to a remote website and may download and execute further files from there. Some members of Troj/Exchan-Gen drop a file to the Windows system folder, often with a filename of Apwcmdnt.dll. This file is also detected as Troj/Exchan-Gen," Sophos explained.