

8 September 2008

By: Denisa Ilascu, Internet / SEO News Editor

[Fake YouTube Infects with Trojans](#)

Warn Sophos experts



Fake YouTube promises exclusive videos that, in fact, hide trojans hip-hop

Seeing one's favorite celebrity in an exclusive video might be tempting enough for many people to click on a link that promises to show them precisely this, especially if we're talking a link on a trusted website. Even more, if that website happens to be YouTube, then 90% of the people receiving it will most surely click it. However, security experts warn us that we must be cautious even when we're dealing with a video allegedly hosted by YouTube. This happens because, during these past days, hijackers have used the name of Google's property to launch Trojan attacks. By using a legitimate website host that has been corrupted, and applying to it YouTube identification marks, such as the logo and the page layout, hackers have managed to attack unwary victims. Researchers at the security company Sophos have posted on the official blog the names of some of the files that presumably were YouTube videos. It seems like attackers didn't even bother to manually change the names of the celebrities to match the context they were used in, thus the "videos" contained totally unusual situations, like, for instance, actresses Angelina Jolie, Monica Bellucci or Meg Ryan supposedly singing. Others, more vague, promised "shocking mp3s," or R-rated clips with the same celebrities. "The good news is that we're still detecting this malware as Troj/Injects-CR. But it is scary to think about how many unprotected users would fall for this trick," says Dmitry Samosseiko from the SophosLabs Canada, assuring users that, as long as they employ a security solution that can detect the trojan, the situation is under control. The domain hosting the fake YouTube is also being used to distribute the same trojan, this time on pages that resemble the design of the Windows Media Player. In order to see a video, users are advised to download a codec, which is in fact a piece of malicious software. Experts warn that the media player is just a static picture and that no one should fall for the trick.