

13 November 2007

By: Bogdan Popa, Security and Search Engines Editor



The fake YouTube page  
F-Secure

## **Fake YouTube Attempting to Infect Visitors**

### *Phishers targeting YouTube*

A new phishing scheme is now aiming to lure users into visiting a malicious copy of YouTube in order to infect their computers with Trojan-Dropper.W32/Agent.CPL. Security vendor F-Secure today reported that some Internet consumers received spam messages asking them to click on a YouTube clip attached to the message. The link is actually redirecting the users to a fake YouTube website which informs them that they must install Adobe Flash Player in order to view the video. "Hello, you either have JavaScript turned off or an old version of Adobe's Flash Player. Get the latest Flash player," the message reads. Clicking on the provided link to download the Flash Player will bring you to a new page to get install\_flash\_player.exe, an executable containing the requested file. "The page, located on a .cn server, prompts for the installation of Adobe's Flash Player. If you download the file, it's named install\_flash\_player.exe. Just as the real Flash Player download would be...", F-Secure wrote in a blog post published today. Obviously, the executable file comes with Trojan-Dropper.W32/Agent.CPL but it's not pretty clear how dangerous it is for computers... Probably the Trojan horse is supposed to enable the attackers to bring other infected material on the victims' computers in order obtain administrator privileges and get any data they want. "Firefox browser is already warning about the fraudulent nature of this site, and we have detection with our 2007-11-12\_04 database, so we don't expect a very big catch for this particular rock phishing site", F-Secure continued. If you want to avoid a successful exploitation through the phishing scheme, you're advised to avoid clicking on the links inserted into the spam messages and refuse installing applications which come from other pages than the genuine one. Just look in your browser address bar to be sure the website you visit is not part of a phishing attack.