

7 January 2009

By: Lucian Constantin, Web News Editor



Hackers spread
malware through
LinkedIn fake profiles
LinkedIn (for the logo)

[Fake LinkedIn Profiles Spread Malware](#)

Bogus accounts for numerous celebrities have been created

Hackers are using the LinkedIn professional networking service to spread trojans, antivirus researchers warn. The fake profiles of tens of celebrities are enticing users to visit malicious links claiming to point to their nude videos.

LinkedIn is a popular social networking website for professionals, allowing them to maintain business relationships with each other. The site currently has a global traffic rank of 190, according to Alexa, which makes it a very profitable place for hackers to spread their malware.

Trend Micro's TrendLabs Malware Blog [reports](#) that threats researcher Ivan Macalintal has identified bogus profiles for personalities such as Beyoncé; Knowles, Victoria Beckham, Christina Ricci, Kirsten Dunst, Salma Hayek, Kate Hudson, and others.

Graham Cluley, senior technology consultant for antivirus vendor Sophos, who also [investigated](#) the matter, has completed the celebrity list with the likes of Paris Hilton, Kim Kardashian, Jaime Pressly, Christina Aguilera, Keri Russell, Zooey Deschanel, Lizzy Caplan, Brooke Hogan, and Tila Tequila.

When visiting the alleged nude video links, a user is taken through several redirects, which eventually lead to a website distributing a trojan. The malicious application is detected as [TROJ_DLOAD.ML](#) by Trend Micro, and as [Troj/Decdec-A](#) by Sophos. If successfully deployed, the trojan will proceed to downloading and installing even more malware, including a rogue security application identified as TROJ_FAKEAV.GDS.

"Undoubtedly, spammers, malware authors, and other cybercriminals may be abusing the system to link to their webpages in the hope that it will generate a higher ranking in search engines like Google," Graham Cluley explains. In addition to providing a solid base of potential victims, using social networking websites increases the credibility of these scams, because people tend to trust messages coming from users in their friends lists. This is demonstrated by the constant phishing campaigns hitting networks like [Facebook](#), MySpace, [hi5](#), or [Twitter](#).

The Trend Micro report points out that there is actually an entire underground business focused on pre-registering and leasing or selling such high profile accounts on popular websites. Clearly, LinkedIn is not the only [service abused](#) by hackers, but this is no excuse for not developing better security policies; in order to filter out such attacks. "It's a shame that LinkedIn aren't keeping a closer eye on obviously bogus profiles being created on their site," Graham Cluley also concludes.