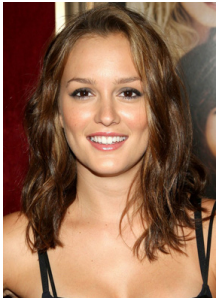


25 June 2009

By: Lucian Constantin, Web News Editor



Searching for Leighton Meester's leaked video can lead to malware Prohaircut

[Leighton Meester Leaked Tape Search Results Lead to Malware](#)

Guy Kawasaki unintentionally spreads the malicious link on Twitter

In their attempt to profit from the recent Leighton Meester leaked tape scandal, malware distributors have resorted to their usual blackhat search engine optimization tricks. Unfortunately, this also affected former Apple Evangelist Guy Kawasaki, when one of the spam messages spreading a computer trojan ended up on his Twitter feed.

Rumor has it that an explicit video featuring "Gossip Girl" TV star Leighton Meester and her boyfriend, back when she was 18 years old, has been leaked onto the Internet. Similar past [incidents](#) involving other celebrities are proof that such leaks generate a lot of search traffic and a fair amount of public interest.

However, events like these are also perfect for cybercriminals to spread some more malware through the old, fake video codec trick. Once the trap page has been set up, by masquerading a popular video service such as YouTube, the malware distributors go on to poison the top search results on the subject in order to make sure that enough potential victims reach it.

One link about an alleged Leighton Meester video made it on an unmoderated feed at NowPublic, a Vancouver-based participatory news-gathering platform. Unfortunately, Guy Kawasaki, now a Silicon Valley venture capitalist and famous blogger, happens to re-post NowPublic content on his Twitter feed through the "auto-feed" feature, thus causing the rogue message to be sent to his almost 140,000 followers.

Opening the spammed link and attempting to view the fake movie will prompt the download of an allegedly required video codec, which is actually a malicious file. "The webpage can tell if you are visiting the site using an Apple Mac or a Windows computer, and will serve up the relevant piece of malware. In the case of Macs the malware is detected by Sophos as OSX/Jahlav-C," Graham Cluley, senior technology consultant at Sophos, [explains](#).

This attack appears to have been quite successful. Rik Ferguson, solutions architect at Trend Micro, [notes](#) that the fake page has been accessed so many times that the image masquerading as the embedded video has been automatically replaced with a message reading, "Intensity of requests of the image has exceeded and admissible limit. The image is temporarily disabled." The Windows version of this malware is [detected](#) by Trend Micro products as TROJ_JAHLAV.B.