

12 September 2008

By: Lucian Constantin, Web News Editor

Spammer
Word Sell Inc.

[Obama's Adult Video, Nuclear Explosions and Suspended Internet Access](#)

These are the latest malware spreading e-mail spam campaigns

Three new spam campaigns have been circulating around the web in the recent few days. One claims to contain an adult video featuring the US presidential candidate, senator Barack Obama, another announces that a nuclear power station exploded near London and the authorities keep it secret and the third warns that users' Internet access will be suspended due to illegal activities. All of them spread trojans.

Spammers are inventive, to say the least, when it comes to tricking users into running infected files, buying fake drugs or signing up for adult content websites. The latest spam campaigns that have been launched close to one day apart are no different and they have probably been successful in infecting many computers. If it weren't for the poor English, generally common with spam e-mails, some of them would actually look real enough.

The first campaign makes use of the interest in the US elections. The e-mail contains a link to an adult video that is supposed to present the US Senator of Illinois Barack Obama engaging in sexual activities with several Ukrainian girls back in 2007 when he "was travel in Ukraine". The link really contains what appears to be a homemade X-rated video, obviously not featuring Mr. Obama though. While watching the video, the Mal/Hupig-D (according to Sophos) trojan gets installed on the user's computer.

The second campaign addresses rather conspiracy theorists than a large audience as it reads that "on Internet forums there appeared messages" about an explosion that took place at a nuclear power plant station located in London's suburbs. The e-mail further claims that the UK government has succeeded in containing this news from spreading, and now a radiation cloud is moving towards Canada. You're not convinced yet? The e-mail offers an attachment called victims.zip which is supposed to contain pictures portraying the affected population. The zip actually contains Troj/Agent-HQE (according to Sophos). Graham Cluley, Senior Technology Consultant at Sophos, [notes](#) on his blog that "once installed, the hackers can use the malware to spy on the victim's computer and steal information for financial gain".

The third campaign, and the most believable yet, claims to be from the "ICS Monitoring Team" of the "Internet Service Provider Consortium" and notifies users that their Internet access is going to be suspended. According to the e-mail, this "Consortium" of ISPs is protecting the rights of software developers and digital artists by monitoring network traffic. Apparently, they got to the conclusion that you had been downloading copyrighted material and broke the law. As a result, you risk to lose your Internet access if you don't stop immediately. The e-mail has an attachment named user-EA49943X-activities.zip which is supposed to contain your traffic reports for the past six months. Instead, it contains Troj/Meredrop-A or Troj/Agent-HQK (according to Sophos).