

28 September 2007

By: Marius Oiaga, Technology News Editor



Free Windows Porn

And the downloads lying beneath

Free pornographic content and the Windows platform simply mix. There is a very thin line between scantily clothed girls in sexually explicit scenarios and the Windows operating system, especially if Internet Explorer is involved. The promise of free porn is hard to resist, and generally it is a sufficient incentive for users to willingly agree to become victims of malicious Internet attacks. While software vulnerabilities and their exploit is perhaps the perfect mechanism to achieve silent remote code execution on a victim's machine, social engineering schemes are more manageable simply because they involve not quite as much technical knowledge, and because they are not correlated with an attack window that the developers could close at any time with a security update. There is simply no way to patch against social engineering. "The use of porn as a lure is demonstrated perfectly by a family of Trojans for the Windows platform known as Zlob. The installation mechanism used within these campaigns involves the creation of numerous web sites offering pornographic content. When an attempt to access certain content (typically some enticing porn movie) is made, the user is presented with an error message such as that in. Clicking on the link in order to install the missing video codec leads to the download of a fake codec installer from other sites (created for the purposes of this attack). When the installer runs, malicious Zlob components are installed, and the victim machine infected," revealed Fraser Howard, principal virus researcher at SophosLabs, in the "Modern web attacks" [technical paper](#). The Windows operating system is the most attacked platform worldwide, mainly because of its ubiquity. And no matter how secure Windows XP or even Windows Vista is, the software can do nothing to protect the users against malware that are installing themselves. "Nowadays, with improved connectivity and advancements in client technologies, the demand for increasingly rich content through the browser has never been higher. Users expect web pages to contain embedded audio, animation or video content. For malware authors this makes it increasingly attractive (and easier) to construct social engineering attacks over the web", Howard added.