

7 January 2008

By: Bogdan Popa, Security and Search Engines Editor



Don't visit the website
unless you're
protected!
dkimages.com

[New York Jets Fansite Drops Yahoo Webcam Vulnerability Exploit](#)

One more website distributing malware

Yet another web attack targeting the visitors of a very popular website and the vulnerabilities discovered on their computers. This time, the affected page is a New York Jets fansite, which obviously has a lot of visitors every day. Just like the past attacks, the website has been compromised with an embedded Iframe that attempts to take the visitors on another website, apparently hosted in Estonia. "First, the iFrame (or an obfuscated JavaScript iFrame) contains a redirect to another website hosting FirePack engine infection (we have also seen it loop through an intermediary redirect first), which then checks for the browser being used (MS-IE/Firefox/Opera) by the unwitting user", Paul Ferguson of Trend Micro wrote on the security company's blog. FirePack contains several exploits for recent vulnerabilities reported in multiple software solutions, like Yahoo Messenger or Windows Media Player. Using these exploits, the attackers attempt to deploy a piece of malware on the vulnerable systems. "This malware creates one of the infamous NTOS.exe or WSNPOEM variants in the infected system - and their purpose is but for one reason, and one reason only: information theft", the Trend Micro official added. Here are the software vulnerabilities which are currently exploited by FirePack and which may support the installation of the malware on your computer: - Vulnerability in Microsoft XML Core Services Allows Remote Code Execution (MS06-071); - Yahoo Webcam vulnerability; - Microsoft Internet Explorer CreateTextRange Remote Code Execution Vulnerability (MS06-13); - Windows Media Player Plug-In EMBED Overflow Universal Exploit (MS06-006); - Vulnerability in Vector Markup Language Could Allow Remote Code Execution (MS07-004); - Also, an Opera 0day 9.0-9.2 vulnerability released in October 2007! If you're afraid that you may be one of the vulnerable users, you should apply the latest patches for your operating system / software applications, in order to be sure there is no vulnerability to be exploited by these dangerous people.