

Trojan-pics in newsgroups

Source: <http://sci.tech-archive.net/Archive/sci.med.transcription/2004-09/4503.html>

From: Michelle (mishellr71_at_netscape.net)

Date: 09/29/04

Date: Wed, 29 Sep 2004 01:33:21 GMT

http://netscape.com.com/2100-1009_22-5385995.html?part=netscape&subj=technews&tag=mynetscape

Trojan horse exploits image flaw

By Declan McCullagh and Robert Lemos CNET News.com September 28, 2004, 8:32 AM PT

Internet watchers say they've spotted infected images that could implant a back door into a Windows computer if they are viewed.

EasyNews, a provider of Usenet newsgroups, said it has identified two JPEG images that take advantage of a previously identified flaw in the way Microsoft software handles graphics files. Windows users could have their computers infected merely by opening one of those Trojan horse images.

The report of the widely expected exploit comes less than a week after sample code appeared that demonstrated how to take advantage of Microsoft's programming error. Some security researchers worry that the ubiquity of JPEG images provides an unprecedented opportunity to spread malicious code through file-trading networks, the Web or spamming.

But the Trojan horse images may not be as threatening as a more sophisticated version of the exploit could be.

"These JPEGs did not replicate, so this is not a virus," antivirus software company F-Secure stated in its Weblog. "Apparently they tried to use these JPEGs to download Trojan (horse programs) to vulnerable computers, but the download sites should be down by now."

Windows' Graphic Device Interface Plus (GDI+) software contains a JPEG-processing vulnerability that affects dozens of Microsoft products, including the Office suite. Windows XP and Windows Server versions are vulnerable unless a Microsoft patch has been installed in the last few weeks or, in the case of XP, if the systems have been upgraded to Service Pack 2.

Other Windows versions may be at risk depending on what applications are installed. The issue does not affect non-Microsoft operating systems such as Linux and Mac OS X.

sci.med.transcription: Trojan-pics in newsgroups

Developers at Santa Monica, Calif.-based EasyNews created a short program to scan JPEG files flowing through their system for identifying features of the GDI+ exploit.

"It paged my cell phone at 6:47pm PDT on 9/26/2004 for the first hit, and 7:52pm PDT on 9/26/2004 for the second hit," one of the developers wrote in a Web posting.

Mike Minor, EasyNews' chief technology officer, said he had been monitoring the Usenet feed for 36 hours before discovering an infected image. "We couldn't find any other trace of any other posts from that IP address," Minor said. EasyNews has not spotted any infected JPEGs since the two it identified late Sunday.

Once the Trojan horse is activated by viewing the image, it connects to an FTP (File Transfer Protocol) site and downloads software that installs a back door in the infected Windows machine.