

Re: Microsoft Browser Under Scrutiny

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.basics/2004-07/0619.html>

From: Carey Frisch [MVP] (mrxp2004_at_nospamyahoo.com)

Date: 07/03/04

Date: Sat, 3 Jul 2004 15:22:45 -0500

What You Should Know About Download.Ject

http://www.microsoft.com/security/incident/download_ject.msp

Important:

Users of Windows XP Service Pack 2 Release Candidate 2
(Windows XP SP2 RC2) are not at risk.

--

Carey Frisch

Microsoft MVP

Windows XP - Shell/User

Be Smart! Protect your PC!

<http://www.microsoft.com/security/protect/>

"Tom" no-way@not-here.com wrote in message:

news:%23JHJentYEHA.384@TK2MSFTNGP10.phx.gbl...

<http://www.cbsnews.com/stories/2004/07/03/tech/main627407.shtml>

NEW YORK, July 2, 2004

(AP) It's been a bad week for many users of Microsoft Corp.'s nearly ubiquitous Internet Explorer. A pair of virus attacks exploiting its vulnerabilities had led security experts to recommend that users consider such alternatives as Mozilla and Opera.

Until Microsoft made a software update available Friday, continuing to use Internet Explorer was "like the lottery," said Johannes B. Ullrich, chief technology officer of the nonprofit SANS Internet Security Center.

The respected research center was among security groups recommending other browsers as long as a vulnerability in IE remained unfixed, leaving it capable of running malicious code that's been hit by a number of popular Web sites.

It took a week for Microsoft to issue the update, which does not fix the flaw entirely but disables the ability to deliver malicious code with it. Ullrich said the update appeared to eliminate any immediate need to switch browsers, which can cause problems of its own.

The flaw had allowed a computer virus to spread through a new technique that converted popular Web sites into virus transmitters. That infection was designed to steal valuable information as Web users typed passwords and the like.

And this week, researchers discovered another password-stealing program hidden behind pop-up ads. The flaw enabling that Trojan infection was issued in April, many users had yet to patch their systems. IE is a frequent target for hacking because of its popularity; WebSideStory Inc. says 95 percent of users use it globally. The browser is closely integrated with Microsoft's Windows operating system and e-mail program, creating more room for programming error and making solutions more difficult.

Though many of IE's functions are not unique, IE tends to be more permissive in running code that helps Web developers create fancy features but allows hackers to more easily find weaknesses. A major Windows XP upgrade, known as a service pack, is due out this summer and would plug some of the holes. Last week's outbreak would not have occurred had those software plugs been installed, said Gary S. McGraw, Microsoft security director.

microsoft.public.windowsxp.basics: Re: Microsoft Browser Under Scrutiny

Microsoft also is developing a specific fix for the new vulnerability, but Schare said testing that fix is called it premature for independent security experts to recommend that people explore alternative browsers. Even if those recommendations were heeded, it's highly unlikely Microsoft could be unseated as the dominant browser business. After all, IE comes with Windows computers. The Justice Department, after initiating a lawsuit to force Microsoft to uncouple the browser from its operating systems, later backed down.

Many users don't care enough or know how to find other browsers, most of which are free or ad-supported. Software ASA, which offers the No. 3 browser for Windows, saw no significant change in downloads. Downloads of Mozilla doubled, but the increase is not nearly enough to significantly change its market share. "It's not that consumers are so loyal to Microsoft, but more they are apathetic," said Geoff Johnson, an analyst with WebSideStory, which tracks browser usage. "With it, there really is a cost to switch browsers. Users who install alternatives will find that some Web sites simply won't work. Movielink LLC says that movies need technology specific to IE, and America Online Inc. shuns its own Mozilla-based Netscape-based browser for new conferencing tools.

Browser-integrated toolbars from search leader Google Inc. and others are only available for Internet Explorer.

Many sites work on alternatives but display items incorrectly, often because developers fail to test on them. "All they know is it looks good to them ... on their own browser, and their own browser is most probably Internet Explorer," said Jakob Nielsen, a Web design expert with Nielsen Norman Group.

Ken Godskind, vice president of marketing at the Internet monitoring firm AlertSite, uses the Mozilla browser partly because of security concerns, but he accepts having to run IE now and then. "Rarely are you going to go someplace where you're going to avoid Microsoft technology," he said. But sites have gotten better about designing for other browsers, said Porter Glendinning, an Internet consultant who promotes adherence to Web standards. Until recently, he said, banking applications didn't work on anything else.

And leading Web application developers, including Opera, Apple Computer Inc. and Macromedia Inc., are collaborating on better plug-in technology to rival Microsoft's.

Opera's Christen Krogh said users would get the same functionality no matter their browser. Mark Rasch, chief security counsel for Solutionary Inc., favors alternatives "if for no reason other than to create heterogeneity," which dulls the impact of any single virus attack.

But alternatives can become targets, too, as more people use them, said Chris Kraft, senior security manager at Sophos Inc.

A better solution is to reconsider whether browsers ought to have evolved into Swiss Army knives for the Internet ? a development that can, and has, backfired on users.

These Web browsers have advanced over time to be extremely rich in terms of content, how they deliver content," Kraft said. "What's the compromise between a rich experience and creating a toolbox for a malicious community?"