

Sound like busy days for anti-virus folkies ?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2004-02/1210.html>

From: 1/2 pint (*anonymous_esboella_at_yahoo.com*)

Date: 02/16/04

Date: Sun, 15 Feb 2004 16:48:38 -0800

Hey Hey, looks like the Anti-Virus folks will be busy !

Regards

half_pint

esboella@yahoo.com

LONDON/AMSTERDAM – Internet users on Friday were ferociously downloading pirate versions of Microsoft Corp's Windows source code, stoking concerns hackers and virus writers could use it for a new wave of cyber attacks.

The world's largest software maker alerted the public on Thursday that parts of its valuable source code for its Windows NT and Windows 2000 operating systems had been leaked to various online file-sharing networks. Microsoft said the released code amounted to a fraction of the entire program, but that wasn't stopping the curious and the malevolent from checking it out for themselves. Noting the size of the files being swapped on Internet file-sharing networks on Friday, security experts feared there could be enough compromised code available to crack open vital pieces of a software that run millions of computers.

"Whilst we do not know exactly what's in circulation, every coder, every malware jockey and every hacker who has a reasonable understanding of programming is going to be looking to get their hands on this source code," said Richard Starnes, an information security specialist who works with various law enforcement agencies on cyber-crime investigations.

SOURCE CODE FOR THE TAKING Various computer security firms were reporting on Friday that two compressed files – one at 203 megabytes and another at 229 megabytes of Windows NT and Windows 2000 operating systems -- were being widely distributed on scores of online exchanges. Security officials said the compressed files amounted to

microsoft.public.security: Sound like busy days for anti-virus folks ?

a CD-Rom's worth of data and represented less than five percent of Windows code. However, they warned it may relate critical security functions.

"I do not believe Microsoft would have issued a public statement if the source code for solitaire had been released," said Starnes. The concern is that in the wrong hands, virus writers and hackers could discover vulnerabilities in the software and use it to break into PCs running on Windows 2000 or NT to destroy or steal data. Microsoft on Thursday was quick to dismiss this as unlikely, but that hasn't deterred Internet users from downloading the files. "The source code leak spread quickly in the underground," said Ken Dunham, Malicious Code Intelligence manager for security consultancy iDefense. Microsoft said it believed the leak could be a