

Re: A Very Dangerous Worm in Windows Metafile Images (WMF)

Source: <http://sci.tech-archive.net/Archive/sci.electronics.design/2006-01/msg00449.html>

- *From:* "Rich Grise, but drunk" <yahright@xxxxxxxxxxxx>
 - *Date:* Tue, 03 Jan 2006 19:13:19 GMT
-

On Mon, 02 Jan 2006 13:40:03 -0800, Bob Monsen wrote:

> On Mon, 02 Jan 2006 15:43:30 +0000, Rich Grise wrote:

>> On Mon, 02 Jan 2006 03:40:50 -0800, Mike Monett wrote:

>>

>>> The IM worm that was released yesterday was "[http://\[snip\]/xmas-2006](http://[snip]/xmas-2006)

>>> FUNNY.jpg".

>>

>> Aww, c'mon! Post the whole URL, with warnings, so I can go look at it -

>> I'm running Linux, so I don't get worms. ;-P

>

> Nautilus whines if you try to open a WMF which has the wrong extension. It

> only lets you do it by selecting the application, and the warning

> indicates that the file can do damage.

>

> I wouldn't trust linux to protect you on on this one, particularly if you

> like to run as root.

Actually, I think one of the major problems with Windoze is that they don't tell their customers not to run as "ADMINISTRATOR". I know not to run as root, but take a moment to consider - even if I did decide to download a wmf file, and it had executable code, that code would only execute on a Windoze box. In the first place, it doesn't have execute permission. In the second place, it was written to interface to Windoze, so its first system call would give a segment violation, and Linux would let you know, and quietly shut it down and unload it from memory. (well, 'free()' the memory.) In the third place, even if it got through all of those hoops, it wouldn't have write permission on system files, so it wouldn't be able to do anything malicious even if it could execute on a Linux box.

So, of course, I stand behind my assertion that Bill Gates should clue up, download a Linux, have his codemonkeys port the eye candy, drivers, and easy install scripts (but smarten them up a bit - I'm available for that task, BTW), and sell it as ***Microsoft Linux***! It's totally legal! If I had his resources, I'd do it myself!

As it is, the best we can do today is support, for example, Patrick Volkerding, who put together the Slackware distribution. It was my

Re: A Very Dangerous Worm in Windows Metafile Images (WMF)

first Linux, back in the late 1990's, and I picked it because of the name. <http://www.slackware.com> . I don't work for him or anything, I'm just a satisfied customer. :-)

There's only about two things I still need windows for, and I'm kind of working on narrowing that down if I can. ;-)

Cheers!
Rich

• *Follow-Ups:*

- ◆ [Re: A Very Dangerous Worm in Windows Metafile Images \(WMF\)](#)
◇ From: Bob Monsen

• *References:*

- ◆ [A Very Dangerous Worm in Windows Metafile Images \(WMF\)](#)
◇ From: Mike Monett
- ◆ [Re: A Very Dangerous Worm in Windows Metafile Images \(WMF\)](#)
◇ From: John Larkin
- ◆ [Re: A Very Dangerous Worm in Windows Metafile Images \(WMF\)](#)
◇ From: Mike Monett
- ◆ [Re: A Very Dangerous Worm in Windows Metafile Images \(WMF\)](#)
◇ From: Rich Grise
- ◆ [Re: A Very Dangerous Worm in Windows Metafile Images \(WMF\)](#)
◇ From: Bob Monsen

- Prev by Date: [Re: Oscillator not...well, oscillating](#)
- Next by Date: [Re: Embedded Electronics Design Engineers wanted...](#)
- Previous by thread: [Re: A Very Dangerous Worm in Windows Metafile Images \(WMF\)](#)
- Next by thread: [Re: A Very Dangerous Worm in Windows Metafile Images \(WMF\)](#)
- Index(es):
 - ◆ [Date](#)
 - ◆ [Thread](#)