

Re: Yet another Mass e-mail worm TM – Gibe-F/Swen-A – E-mail from Microsoft

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2003-09/0474.html>

From: Rev Turd Fredericks (turdfred_at_catholic.org)

Date: 09/20/03

Date: Sat, 20 Sep 2003 03:21:27 GMT

Dave wrote:

- > *"Rev Turd Fredericks" <turdfred@catholic.org> wrote in message*
- > *news:PM0003C7B79D9EA844@dhcppc2.reshsg.uci.edu...*
- >>
- >> *My wife got the msblast virus merely by*
- >> *turning off her firewall to play a game.*
- >
- > *Microsoft advocates are claiming that XP is just as secure as Linux,*
- > *that*
- > *you can't get a virus without doing something stupid, like clicking on*
- > *an*
- > *email attachment. Could you tell us more about this incident. Does*
- > *"play*
- > *a game" mean download some program and run it? Why would you need to*
- > *turn*
- > *off a firewall to play a game on your own computer?*

It was an online game called Neverwinter nights. The program was not downloaded, it was purchased. She doesn't use email at home either. The firewall was disabled because it sometimes interferes with the game, I have since fixed that and the game can be played with the firewall on. There was no user interaction required. The only reason we found out was when she reenabled her firewall, the firewall warning window popped up and asked "msblast.exe requests a connection to IP xxx.xxx.xxx.xxx". msblast takes advantage of an RPC vulnerability. She doesn't use XP but it is also vulnerable to msblast in the same manner.

- >
- > *I've also heard that msblast can infect a computer without *any* user*
- > *interaction. I was told this by a system administrator who takes care*
- > *of*
- > *hundreds of Windows workstations. I asked him what network services*
- > *were*
- > *running on the computers (telnet, ftp, etc.) and he said none. The*
- > *virus*
- > *can apparently propagate with just the basic network communication*

comp.security.misc: Re: Yet another Mass e-mail worm TM – Gibe-F/Swen-A – E-mail from Microsoft

> *protocols*.

>

Yup.