

Re: Virus/adware/spyware -- is there all-in-one protection in one program?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-06/1538.html>

From: Alun Jones [MSFT] (alunj_at_online.microsoft.com)

Date: 06/23/04

Date: Tue, 22 Jun 2004 15:02:24 -0700

"Lionel Fourquaux" <use.reply.to@no-spam.invalid> wrote in message news:eMLw62JWEHA.3336@TK2MSFTNGP11.phx.gbl...

> *It's slightly paranoid, but short of a huge vulnerability in the OS,*
> *_and_ a vulnerability in the e-mail client, e-mail viruses are blocked.*

Weeell, not quite. If there were to be a vulnerability in the e-mail client, e-mail viruses would be able to exploit it to ... send email as if those messages came from you. Lots of email. Including reruns of the best of your inbox (and other mail folders).

I'm new at MS, so hopefully this won't come across as Microsoft Unix-bashing, but this is one of the things I have to remind my Unix-head friends about – removing administrator access from possible exploit means only that the administrator's account, and things limited to the administrator, are protected. Normal users have a huge level of capabilities. They can delete (or sometimes worse, overwrite) their own files, send email, communicate with other users, and maybe even lay traps for system administrators to execute. Even without the last item (privilege elevation), a virus can destroy or corrupt data, and reproduce. Is administrator / root privilege necessary for a virus to be bad? No. Most email viruses of today are quite capable of causing damage and reproducing under 'restricted' accounts.

I've used email clients from three different vendors that have, in their time, had vulnerabilities that could be triggered by overflows in processing text-based email. By now, they should know better, and the current crop of email clients is mostly solid enough that I trust them not to break on plain text (and I am very paranoid in that regard). So, while the current situation is good, history demonstrates that even your approach has not always been foolproof.

I think it's worthwhile to have defence in depth. So, I read my email in text mode, I don't investigate most attachments, I run an antivirus program, *_and_* I scan every month or so with a different antivirus program. Oh yes, and I keep backups.

microsoft.public.security.virus: Re: Virus/adware/spyware -- is there all-in-one protection in one program?

Alun.

~~~~