Stop Microsoft's Security Plans

Information security.

Flaws in Outlook, IIS, Microsoft SQL Server, and the Windows DCOM service have exposed millions of computers to increasingly serious virus outbreaks:

Melissa infected 150,000 hosts in 4 days in 1999 [1]. ILoveYou infected 500,000 hosts in 24 hours in 2000 [1]. Code Red infected 360,000 hosts in 14 hours in 2001 [1]. Sapphire infected 76,000 hosts in 10 minutes in January 2003 [2]. SoBig has now generated tens of millions of messages, becoming the worst e-mail virus in history [3].

The Melissa [4], ILoveYou [5, 6], and SoBig [7] viruses are all made possible only due to features Microsoft chose to incorporate into Word, Outlook, and Windows that give incoming documents the power to do anything they want to your computer when you try to view them. Microsoft has not announced any plans to fix this problem.

Windows assists viruses in fooling the user by obscuring the extensions on file names. The .PIF and .SHS extensions are always hidden even if the user turns off the option to hide file extensions [8, 9]. *(In particular, this "feature" helped the latest version of SoBig distribute itself.)*

Microsoft's Passport system, used by over 200 million people, contained security bugs that allow others to easily steal your personal information and credit card numbers within minutes of sending mail to you on Hotmail [10].

Information freedom.

Microsoft's new security initiative, NGSCB, will enable its software to encrypt documents in such a way that they cannot be read by any other software or computer [11]. *(This would allow Word to hold your documents hostage.)*

Microsoft's attestation feature in NGSCB will enable software and media providers to verify and require that you are running approved software [12]. *(This will concentrate control of the software industry in the hands of a few players that maintain the lists of approved software.)*

Microsoft's Rights Management Services will require your computer to contact and notify a Windows rights server before opening any rights-controlled document [13, 14]. *(This will enable and promote constant monitoring of computer use, and impede employees from blowing the whistle on their companies' illegal practices.)*

Microsoft's Rights Management Services incorporate little or no support for fair use of information [15]. They will enable Microsoft to remotely disable non-Microsoft media players [16]. They will also enable Microsoft to remotely revoke your media content. Copyright holders would have to appeal to Microsoft to get content licenses revoked [17].

Microsoft's new security initiative, NGSCB, will not stop spam or viruses, according to Microsoft's own information about NGSCB [18].

Microsoft will make sure that you have neither.

Please help spread the word about NGSCB, Windows Rights Management, and the dangers they pose to innovation, competition, and freedom. For more information, see http://zesty.ca/microsoft/.

Facts are upright. *Inferences are italicized.*
Information collected by Ka-Ping Yee <ping@zesty.ca>.

[1] http://www.cerias.purdue.edu/homes/spaf/presents/RE01-spaf.pdf
[2] http://www.cs.berkeley.edu/~nweaver/sapphire/
[3] http://sg.news.yahoo.com/030822/1/3dlxh.html
[4] http://www.cert.org/advisories/CA-1999-04.html
[5] http://zdnet.com.com/2100-11-520479.html
[6] http://www.pbs.org/cringely/pulpit/pulpit20010802.html
[7] http://www.pcworld.com/news/article/0,aid,108793,00.asp
[8] http://www.antichip.org/virusinfo/extensions.html
[9] http://www.pc-help.org/security/scrap.htm
[10] http://www.wired.com/news/technology/0,1282,48105,00.html
[11] http://www.eweek.com/print_article/0,3668,a=41223,00.asp
[12] http://www.law.berkeley.edu/institutes/ bclt/drm/slides/bl_slides.pdf
[13] http://news.com.com/2100-1001-985496.html
[14] http://www.securityfocus.com/columnists/165
[15] http://cryptome.org/ms-drm.htm
[16] http://www.smh.com.au/articles/2002/08/24/1030052995857.html
[17] http://www.vnunet.com/News/1131606
[18] http://www.microsoft.com/technet/security/news/NGSCB.asp