

# Windowx 200x/XP virus proof document released

**Source:**

<http://www.tech-archive.net/Archive/Scripting/microsoft.public.scripting.virus.discussion/2004-06/0006.html>

---

**From:** Wellington Terumi Uemura (*wellington\_at\_fakemail.com*)

**Date:** 05/31/04

Date: Mon, 31 May 2004 11:36:33 -0300

Hello!

Some time ago, i was asking people to send me virus and worms to my personal research:

<http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-03/1673.html>

And I did receive many jokes about it, people telling me that "if was that good others "specialists" would have released the information before" or that this kind of "stuff" is IMPOSSIBLE. E-mail from every where, includind some people from Microsoft Brasil telling me to show then what this "magic" was all about.

The good part is that, after sending this document to a person in Microsoft Brasil, it never replied or make any comments about it or others "specialists" that got the document some how, telling me that "I knew that, nothing new about it"!

Is strange that security magazines and sites, their focus about worms and virus issue is "Firewall and antivirus" or don't open unknow files that come in to your e-mail box, don't do this, don't do that. I know that users dont care about it thinking that a antivirus will prevent infection, many os us was using antivirus when Mblaster came out and many others to date.

It's well know that a antivirus can protect you after infection, not before, Mblaster, Mydoom, Netsky, Sasser, etc, are very good examples of that. Who never downloaded the last remove tool for a last worm or virus before they could have time to criate a "cure" for it?

I am not against antivirus software, not at all, but they have some limitations, some are not smart enough to identify if a change that you are making in your system are benefic or not, some will prevent system modifications other won't.

As I have said before, i came from a Linux enviroment and in moust cases a non root user can't do any damage to the system, this is also true with the last Windows Systems that use NTFS partition.

microsoft.public.scripting.virus.discussion: Windowx 200x/XP virus proof document released

After nights of research, i've find out that the only way to get infected in OS Windows 200x/XP with NTFS partition is that I must have administrative permission to make system changes. My tests shows that a worm or virus would not add it self to system partition without permission or make changes in registry, in special the key:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Following the linux security basics I've make som