

## Re: msblast virus

**Source:**

[http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security\\_admin/2004-02/0532.html](http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2004-02/0532.html)

---

**From:** cquirke (MVP Win9x) ([cquirkenews\\_at\\_nospam.mvps.org](mailto:cquirkenews_at_nospam.mvps.org))

**Date:** 02/04/04

Date: Wed, 04 Feb 2004 11:06:30 +0200

On Fri, 30 Jan 2004 19:55:39 -0600, "Carey Frisch [MVP]"  
<[mrxp2004@nospamyahoo.com](mailto:mrxp2004@nospamyahoo.com)> wrote:

>Unfortunately, the penalty for not having a good antivirus program installed,  
>not enabling a firewall, and not downloading the critical updates  
>available from the Windows Update website, is an opportunity  
>to perform a "clean install" of your operating system.

Generally speaking, "just re-install" should NOT be necessary every time malware goes active on the PC.

Or are you saying XP is so fragile and unmaintainable that every passing malware is a death sentence?

Or are you thinking of the inherently unbounded nature of RATs (Remote Access Trojans), and suggesting this as the only 100% way to avoid non-spreading code (which av would miss) that may have been uploaded by humans that may have grabbed the RAT's tail?

>Virus files are designed to inflict damage to a PC

Actually, few of today's malware seem to have destructive payloads. More often they want to harness your PC and put it to work, either as an identity-theft money-tree, a source of resellable info, a "zombie" to use as a foot-soldier in some mass attack or other, a cat's paw to hack systems that may automate strike-back, or as a spam relay.

Imagine if Lovesan had a CIH payload on a short fuse - e.g. four hours or as soon as the PC goes offline? Point being; things are not as disastrous as they could be, only because the black hats are merciful, not because we are now So Secure.

>I would suggest backing up your important documents and files  
>and proceed with a "clean install" of Windows XP:

If you do that, you will be shot to pieces as soon as you go online; the CD you paid for lacks all patches and is unroadworthy for the

Information Highway. It's a bit less broken if you have the Internet firewall switched on (which may bonk your LAN connectivity, if you use the same adapter to access LAN and Internet).

>4. *The setup menu will appear and you should elect to delete the existing Windows partitions, then create a new partition, then format the primary partition (preferably NTFS) and proceed to install Windows XP.*

Reconsider that "preferably NTFS" bit. If you were on FATxx (which Carey appears to assume you aren't) then you could have done a formal virus check instead – far cleaner, although not conclusive if you did have live RAT-pullers in the house.

See <http://users.iafrica.com/c/cq/cquirke/virtest.htm> on how to do a formal virus check, and why it's recommended.

If your malware did damage your data, you'd also have a chance to recover it from DOS mode, if you were FATxx rather than NTFS. With NTFS, the road is much longer, if it exists at all.

Folks are advocating NTFS on the ASSumption that it's going to be used effectively, as it would typically be in NT's traditional professionally-administered environment...

You'd have industrial-grade backups with someone paid to perform them, so if NTFS dies and takes your data with it, you'd shrug and move on.

You'd have properly-setup user accounts and file permissions, so that NTFS would actually protect you from malware to some extent.

You'd have set the registry so that a Recovery Console boot would be able to access and wildcard-copy off your data to another disk.

You'd have the firewall on, as well as regularly-updated av.

You'd have good hardware, probably with a UPS, fault-tolerant HD, and at least a high-capacity backup system.

...and with those bricks in place, NTFS forms a very useful part of the overall strategy; possibly indispensable, in fact.

But as a consumer, you have none of that. Your user accounts may have to run with full admin rights so the kids could play games, for example, and you probably don't have a good backup to hand.

In that context, NTFS can amount to a data death-sentence, held in abeyance only as long as it takes for some disaster to strike. That may not be long, given how wide-open consumer users and systems are to

malware attack and natural disasters (bad exits, rough power etc.)

>5. *Clean Install Windows XP*

> <http://michaelstevensstech.com/cleanxpinstall.html>

> [Courtesy of Michael Stevens, MS-MVP]

>

>6. ==> *Immediately after installing Windows XP, turn on XP's Firewall.*

> ==> <http://www.microsoft.com/security/protect/>

>7. *After Windows XP is installed, visit the Windows Update website*

> *and download the available "Critical Updates".*

That does rather assume a broadband connection, does it not? At least he could apply the small anti-Lovesan/Blaster RPC patch directly, unlike Win2000 users who'd have to pull 100M+ SP2 first.

>8. *After installing the critical updates, be sure and visit the support website*

> *of the manufacturer of the computer to download and install any*

> *available Windows XP compatible drivers, such as video adapter*

> *and audio drivers.*

Better hope said drivers don't include those needed to access the 'net

>9. *If you happen to run into any installation difficulties, use the following resources:*

>

> *How to Troubleshoot Windows XP Problems During Installation*

> <http://support.microsoft.com/default.aspx?scid=kb;EN-US;310064>

>

> *Troubleshooting Windows XP Setup*

> [http://www.kellys-korner-xp.com/xp\\_setup.htm](http://www.kellys-korner-xp.com/xp_setup.htm)

>

> [Courtesy of MS-MVP Kelly Theriot]

Carey: Are you really suggesting that every malware strike has to be "fixed" by a scorch and rebuild? No MS OS to date has been that pathetically incapable of survival/maintenance – another XP "first"?

>-----

Dreams are stack dumps of the soul

>-----