

# Re: Where Can I Buy a Zombie PC?

---

*Source:*

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2006-09/msg02887.html>

---

- *From:* "cquirke (MVP Windows shell/user)" <[cquirkenews@xxxxxxxxxxxxxxxxxxx](mailto:cquirkenews@xxxxxxxxxxxxxxxxxxx)>
  - *Date:* Sat, 09 Sep 2006 01:43:46 +0200
- 

On Thu, 13 Jul 2006 11:41:13 -0400, "Ground Cover"

The little PC running MS-DOS, security wasn't a concern. The idea was to have a "little" computer that could be used to type up stuff, do a bit of "Basic" or even run a spreadsheet [e.g. Lotus 1 2 3].

There's security, and that is based on safety. Security goes about not letting Fred do what only Pete is supposed to do, and that was indeed not a concern with stand-alone Personal Computer.

The Internet came along and one could also hook up the PC XT so that it could send and receive email etc.

Not really, no – unless you're referring to a handful of insiders, perhaps – and I suspect, not even that. After the XT came the 286, and only with the 386 that followed that, did Windows start to gain momentum. It was around this time that Internet started to catch on, as opposed to BBSs that pervaded earlier.

There were hardly any viruses at first ..

Wrong. The av industry started and flourished in the days of DOS, when viruses spread via infected disks and executable programs.

and these usually had to be physically introduced by, say, 5 1/4 infloppy disk.

Folks used diskettes all the time, in those days; it was how files, software etc. were distributed. If you wanted a shareware program, you'd take a diskette to someone with a modem who would look for it on

## Re: Where Can I Buy a Zombie PC?

various BBSs, download it, and copy it onto your diskette. If you liked it, you might upload it to other BBSs.

That's where the innocence was; in accepting host-to-user-to-host as a safe way to distribute shareware and free software. Often the code files on a BBS would be infected, and would infect whoever downloaded and used them. Everyone was aware of this; most BBSs would warn you of the risk, disclaim responsibility, and advise you to scan downloads with an antivirus utility before use.

There was a solid concern for safety – users knew about viruses and av, they knew that .exe, .com and .bat files were potentially dangerous, and the OS wasn't dumb enough to run any other files as code. IOW, the safety was from a clear data vs. code distinction.

And Microsoft eventually got around to putting a windowing system on these early machines. But the Windows ran on DOS.

There was a decided naivete to the whole thing. Like Pearl Harbour on December 5th or New York on September 10.

I disagree. Folks weren't so stupid as to automatically run macros in "documents", let BBSs automatically drop and run code on visitors' PCs the way web sites today, or auto-run scripts in email "message text".

That stupidity came later, and we are still paying for it.

Microsoft and many many others were having a great time too – like a prosperous and growing town everyone could take a shot and see if they could make it big – and then came two things: the World Wide Web followed shortly after by "Chicago" – Windows 95.

Windows 95 was the most successful and wonderful mistake ever envisioned by humankind. .... it ran on DOS ., [hense the mistake].

Total bollocks. Firstly, it was launched from DOS but did not "run on DOS" unless you chose to start up in Safe Mode. Secondly, there was more stability and design impact from the need to run programs written for Win3.yuk than DOS; whereas DOS sessions were pre-emptively multitasked like Win32 apps, Win16 apps competitively (sorry, "co-operatively") multitasked just as they did in the Mac.

The 64k heap issue also arose from Win3.yuk compatibility needs,

Re: Where Can I Buy a Zombie PC?

## Re: Where Can I Buy a Zombie PC?

rather than anything to do with DOS.

DOS wasn't the enemy...

Microsoft ... should have waited until they had a Windows 2000 like system ready and had spent some time in considerable consideration of security and privacy.

Win2000 is NT 5.0, and NT predated Win95. NT was originally supposed to be the new 32-bit Windows for everybody, but it became clear that it was not going to run faster, and would need far more RAM just to be able to run at the same speed.

So it was repositioned as a hi-end stability wonder, for big expensive servers and workstations.

Win95 followed this debacle, while NT continued as a niche product, through 3.1 to 3.5 to 4.0 and Service Packs. As a niche business product, it soon became network-centric and orientated towards professional network administration.

This is where your "security" (as opposed to "safety") came from – the need to administer different users with different levels of trust and expertise. But there was a downside to that, too.

But what's done was done. And it really was no one's fault. Most all of us made the demands. We wanted computers and the Internet "now". We accepted, no, almost begged, scratched and pleaded for Microsoft Windows and Microsoft Office and other Microsoft products – we all dumped Netscape Navigator like some filthy rag – we wanted the flush buttons and smooth scrolling – and the flash for the websites. We were having a whale of a time.

Actually, the early web wasn't such a dangerous place – and not only because ppl weren't nasty (viruses were already common, and generally far more destructive than today) but because plain HTML behaved like a true data type, i.e. it was safe to "view" without "running code".

The industry started to push scripting and cookies into HTML so that web sites could better exploit their visitors – use the visitor's storage as an ash tray (cookies) and push the processing load (and with it, risk of program errors) as well (scripts, Java).

Netscape and IE were competing, and trying to attract web developers with power that was unique to their particular browser. With Netscape, it was "buy the server software that is most likely to match the de facto browser standard that we give away free". With MS, it was "we'll give you even more ways to program users' PCs, and we will

Re: Where Can I Buy a Zombie PC?

## Re: Where Can I Buy a Zombie PC?

gain market share by giving our browser away free with Windows".

Then the storms of viruses, excessive pronography, scams and malware which hit some people like hurricane Katrina.

You can track the "virus storms" to design safety failures...

- macro viruses to MS Office auto-running scripts
- script malware to unfamiliar and hidden file name extensions
- Melissa etc. to Outlook's scriptability from Word, etc.
- Kak and similar to auto-running scripts in email "message text"
- Lovesan and Sasser etc. to NT's focus as "network client"

Win9x was designed as a stand-alone OS, whereas NT became a "network client". Until this "network client" was widely deployed through stand-alone consumerland via XP, we didn't see pure network worms that spread globally within minutes via clickless attack.

Many of Microsoft's problems, security-wise, is its users. They want JavaScript ON. They want Java ON .. always. They want ActiveX ON. Vulnerabilities get identified and patched, but the user .. the user wants to see the dancing bunnies – at all costs – and there's not much that can be done.

The user needs to regain the knowledge that was common in the DOS days; that data files can be safely viewed, and that other files are code and thus dangerous to run.

They lack this ability because Microsoft hides that information (file name extensions off by default, now multiple code extensions to worry about, and the dumb-ass "open" concept).

Not only that, but contexts that should be as safe as "viewing data" are no longer safe, because by design, MS breaks the code/data barrier (autorunning macros and scripts, CDs autorun when inserted, etc.).

It gets worse; even when MS does show you what a file is supposed to be, it will let the file lie successfully. The most dangerous file types (.exe) are free to set whatever icon they like, and thus (as file name extensions are hidden by default) they can pretend to be data files and appear to be low risk. In many contexts, if a hi-risk file type is named as if it is a lo-risk type, Windows considers this to be an "honest mistake" and runs it in the hi-risk way.

So, is this the "security" you were referring to? Or is this the point at which we became stupidly trusting and insecure?

A PC owner has the right to run as root.

Re: Where Can I Buy a Zombie PC?

## Re: Where Can I Buy a Zombie PC?

PC = Personal Computer. If you own your own computer and are not beholden to any boss or network admin, then YES, you have the right to run as root – in fact, you are the only one to have that right.

What modern PCs do, is leave the system so wide open that anything can walk right in and act with the same rights as the user – that is why today's users have to cower in the "lowered rights" basement, while all sorts of user-hostile code stomps around as "system" (think DRM).

but at some point the software company has to "hand over the keys" so to speak. Yet there's no requirement that the PC owner have ever read even a magazine article on how to run the thing ..

Why should consumers have to pretend to be certified sysadmins managing multiple office workers, just because that was how NT was designed before being dropped on consumers as-is?

XP SP2 was released. The number of extememe vulnerabilities discovered in Windows this past year is way fewer than say found in 2004. Many users are much more circumspect in their behaviour. And Linux still hasn't found the vendor support it needs for to "take the desktop" [and it probably never will] so Microsoft – not having to look over its shoulder– has been taking its time with Vista.

Ah, Vista's another story...

Vista will try – and will probably succeed – to rectify the security situation through an alert system [and without fanfare, running some of software e.g. Internet Explorer with only user privileges even if an Administrator is logged on]. Vista will probably substantially reduce the impact of malware much further than XP SP2.

Vista may fix old mistakes but make new ones. There's still the stupid "I'll do it for you!" and "you don't have to know anything!" nonsense that got us into trouble in the first place – underfootware services that grope files you had no intention to run, expanded directory metadata that gets complex enough to exploit, and a shell that encourages users to be clueless about where files are.

So there you have it. No matter what Microsoft or Linus Torvalds does, someone is going to log on as "root", regardless, and run /bin/dancing\_bunnies and there's nothing anyone can do about it.

## Re: Where Can I Buy a Zombie PC?

By definition, every user has the right to modify their data. So as long as the design is stupid enough to allow all software to run with the user's rights, any software can destroy the user's data.

That is why I consider lowered user rights as being near useless when it comes to protecting the user's interests. They may be helpful in reducing vendor support costs, but that's another set of needs.

Grumpy wrote:

Ground Cover

"Windows" OS has world dominance in business and home computing not because it is superior technically to other OS's such as Mac, UNIX, Linux, FreeBSD, etc..., for indeed it is inferior technically because it is a DOS based OS, even although DOS is a powerful language

Oh boy – the error count is offscale here. For starters, DOS isn't a "language" (nor is it particularly powerful), and Windows hasn't been DOS-based since the original Win95.

In fact, DOS itself started out as a CPM workalike, before it switched to copy UNIX functionality instead. That's why we have UNIX-like directories and redirection, yet CPM-like drive letter and path vs. parameter delimiter syntax.

However, DOS wasn't multitasking, multi-user, or as connectivity-savvy as UNIX. That would only be attempted once Intel came up with a protected mode that worked properly, after the 286 fiasco.

but Windows dominance is because ...

....DOS was already dominant, because the PC was already dominant.

The PC was dominant because it was open hardware (IBM tried to take the ball back with PS/2, and got kicked out of the game instead).

DOS was dominant because IBM adopted it, and Bill Gates et al were successful because IBM didn't lock DOS to the PC, so that Microsoft could sell it for any IBM-compatible PC.

Now let's look at the decisions your superior platforms were making at this time, and subsequently. Apple kept their sphincter screwed

Re: Where Can I Buy a Zombie PC?

Re: Where Can I Buy a Zombie PC?

tight, just like an '80s "home computer" dinosaur company, so that you had to buy Apple's computers to run Apple's OS. UNIX was split over numerous incompatible platforms, so that binary-level run-anywhere was but a dream, and hardware was costly and skills requirements high.

So yes, at both hardware and OS levels, Apple and UNIX (and Sun etc.) offered superior solutions at the outset, but were too piggy to get the big picture. With smaller market share, the platforms were slower to grow and improve, so that the PC overcame the handicap and won.

-----

Drugs are usually safe. Inject? (Y/n)

-----

.