

## Re: Is MSIE dead as a browser – if Microsoft does not patch it then it is as far as I am concerned!

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-06/1826.html>

---

*From:* WinGuy (no\_spam\_at\_nomail.bot)

*Date:* 06/26/04

Date: Sat, 26 Jun 2004 02:51:49 GMT

"henry baker" <holmes@sherlock.buz> wrote in message  
news:pan.2004.06.26.01.03.17.211000@sherlock.buz...

> WinGuy after telling us that the game's afoot, managed on Fri, 25 Jun 2004

> 23:58:20 +0000, to write:

>

>

> > *The fact that a fully updated IE is vulnerable to this exploit would  
have*

> > *made almost no difference if the servers had all been patched as they*

> > *should have been.*

>

> *\*IF\* the servers had been patched.*

> *\*IF\* wishes were horses, beggars would ride.*

> *You are attempting to spin the classic victim/criminal switcheroo*

I'm just stating facts as I strongly suspect them to be true. This has nothing to do with wishes, it has to do only with ultimate responsibility. This doesn't mean IE should not be patched (again) and it only means that some few webserver admins got caught this time – being lazy or worse and now the price is being paid. Is that not a fact? All but a very few admins, worldwide, have historically been very responsible in this regard. IE users might not know better when it comes to doing timely security updates, but server admins — it's their job to know better. It's their job, and their responsibility to the people who use the servers they admin.

> *The fact is that a perfectly fully patched home computer with*

> *up-to-date AV definitions is vulnerable to an attack by a hacker.*

You are probably mostly saying that as a byte comes into a buffer then the byte count should be kept track of so that a buffer overflow can not occur. Most malware uses some sort of buffer overflow exploit. That's fine with today's fast machines, but it wasn't fine with slower machines when coding had to be compact and execute in fewer machine cycles than is needed with today's faster machines. There had to be trade-offs in coding versus worst possible scenarios. But then, not all worst possible scenarios are

anticipated to begin with, since until recently (historically speaking) malware was not a major problem like it now is and especially the problem it has been in the last year or so. Look, over 900 new virus were detected in May 2004 alone. I'd say there's a substantial effort underway to hurt the world economy. Not that I want to go into just why that is probably true (it would be off topic).

> *And people wonder why some do not like Microsoft's attitude toward security?*

What's wrong with it? Knee jerk, is what you think? So ok, and so it is that very same knee jerk way for every company that suddenly finds itself with a product being exploited somehow – they didn't anticipate it during product development. Microsoft might be the most popular for exploits, perhaps because it's so widely used and an exploit of it has such widespread and with dramatically noticeable effects. But theirs are not the only products that get exploited. Unless one subscribes to the theory that a company truly wants customers to hate their products then I fail to see a factual basis concerning a bad Microsoft attitude. I think MS takes security very seriously and now wishes they had anticipated all this sort of stuff to begin with and they are trying, and have been trying very hard and responsibly, to improve security. If the majority of people didn't see that and think that same way then they'd be using different web browsers to a much higher degree than they do now, I say. A minority uses different products, don't they.

> *Fortunately, the russian site has been shut down; but who knows what's next. How many patches will it take to make my XP OX as secure as my Panther or SuSE OS? That's the question – and the answer is not that there are some bad people out there – we all know that.*

I don't know, but once MS products have finally been well secured and MS thereby foils the malware authors and those malware authors have to look for less secure products – perhaps you'll then find out. And MS products are, patch by patch, getting secured. And the next MS OS is supposed to be being designed, for the first time and out of previously unanticipated necessity I might point out, with security uppermost in mind. Then you can toss XP and go for something else better, although I think that expecting absolute perfection is unrealistic in an imperfect world.

> *What we want is good programmers at MS.*

I think you really mean that you want better or perhaps even perfect security incorporated into MS products. Really, it seems evident to me that MS is doing the best that they can and they are making good progress. Very good progress. How much malware did you or others suffer when Win95 was popular? Well, put it online today and see how long it lasts. I think 95 came out in August 24, 1995. Less than 10 years ago, but we forget such things so quickly. Things have changed greatly in malware land since then, primarily within the last 2 or 3 years, and MS is indeed trying to change

too and just as quickly. How about a little credit where credit is due.

- > *Maybe they could get rid of some of their liars and hire*
- > *some programmers in their place? Patenting the human body interface or*
- > *the double-click is cute; but it doesn't make XP any more secure, does it?*

I don't see the relativity. What do those 2 things have to do with security, beyond possibly bringing some more \$ to fund the things you want?

- > *I still use MS products and to date have never gotten an infection, but*
- > *that day may come, and I am in the business and very careful.*

Well, I think you're exceptional. You're in the business and so am I. The "business" reminds me of people who want to rely on automotive airbags instead of learning how to drive defensively. We don't have perfect cars or Hal just yet, and that means it's not a perfect computer world. Humans are still responsible, even at the user level. People like me remember that when a computer was first turned on then nothing at all much would happen beyond a blinking cursor on a black screen. That doesn't seem so long ago, either (less than 25 years, actually). People are so impatient and intolerant in pursuit of elusive perfection. Maybe irrational is a better term, because the expectations are really beyond what is instantaneously practical in the real world. But be assured, many (even MS) are really working very hard to change that.

- > *In truth, today I have become very disillusioned with MS security. The*
- > *hackers are smarter than the MS programmers, and certainly smarter than*
- > *the MS liars.*

What lies? Exactly what "lies" related to product security? MS said their products are 100% secure? When did that occur? For that matter, what manufacture makes that absolute claim in their company literature? Perhaps you and many others are just impatient and even a little unrealistic. Every manufacture gets surprised, every one of them, eventually and in some unexpected way. Then they try to fix things so that a problem doesn't happen again exactly like that. That's called innovation and product improvement. This is not a perfect world, it needs constant perfecting. I think most people realize the fact, and that's why they might express annoyance and even anger – but by and large they use MS products anyway. And they like it, even though it is not perfect.