

# Re: Why most run Microsoft, not RedHat

---

*Source:* <http://linux.derkeiler.com/Mailing-Lists/Fedora/2007-04/msg03475.html>

---

- *From:* Les Mikesell <[lesmikesell@xxxxxxxxxx](mailto:lesmikesell@xxxxxxxxxx)>
  - *Date:* Mon, 30 Apr 2007 13:23:04 -0500
- 

Zoltan Boszormenyi wrote:

It's all a matter of programmer-vs.-programmer wars to show who is in control.

My questions above weren't about war. Again, different POVs.  
I tried to give some examples of ease of use vs manual control.

It's about *\*who\** is in control. The *\*how\** is a matter of programming. Is it your machine or the package manager's? What happens when the package manager is compromised?

A1. you have package manager because you want easy installation and you don't want to wait while the stuff compiles

And after this is in place you add something that theoretically only you are supposed to be able to control.

A3. because it's easier to have everything have the proper permissions, let rpm handle it.

and

A2. the packager may consider a file to be so essential that he wants it immutable. but the upgrade of the package must also work without manual override, i.e. without clearing immutable flag first.

Ahh, but then that thing you just added to give yourself an extra layer of control doesn't work any more.

You can compare it to the person who thought that the passwd program should only talk directly to a tty and that programs should not be able to use it. That lasted a few months – until another programmer wanted his program

Re: Why most run Microsoft, not RedHat

to be able to change passwords and wrote 'expect' to do it. A big waste of both people's time...

Agreed, that's unfortunate.

But your POV in the question above is wrong.  
The point is to take advantage of something  
where available.

Beg your pardon? The point of adding the immutable bit was so the file couldn't be changed by ordinary means. It is, again, a waste of both parties efforts as soon as someone adds the programming to bypass its attempt at control.

But you already have it – you can use `chattr` from shell scripts or manually.  
But `chattr` works only as root and you can only run `rpm -[iU]` as root successfully anyway.  
Hm. You can use `chattr` in pre and post scriptlets in rpm today. :-)  
But `rpmv` won't tell you whether the fs-special flags were set by rpm or by someone else.

Yes, just like the `passwd/expect` example. If there is a possible way to circumvent your special-exception case, there wasn't much sense it adding it in the first place – it just makes everything harder without serving its original purpose.

I can certainly remember if I set this flag myself (e.g. have it documented) or ask the colleagues. If no one authorized has set it (like it was in the case of the intrusion) then I would expect that rpm were able to replace a package with `--force`, even if some files have the immutable flag set. (Or similar in case of other FSes than ext2/3/4.)

Back to the programmer-vs.-programmer. If rpm does this, the rootkits will just supply a modified rpm program that only pretends to do it but doesn't really replace the trojan files.

—  
Les Mikesell  
lesmikesell@xxxxxxxxxx

—  
fedora-list mailing list  
fedora-list@xxxxxxxxxx  
To unsubscribe: <https://www.redhat.com/mailman/listinfo/fedora-list>