

# Re: Why not patch all windows and not just legal copies

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2006-06/msg00245.html>

---

- *From:* "Roger Abell [MVP]" <[mvpNoSpam@xxxxxxx](mailto:mvpNoSpam@xxxxxxx)>
  - *Date:* Sun, 18 Jun 2006 07:28:00 -0700
- 

"Michael Davis (Comcast.Net)" <[netguru@xxxxxxxxxxxx](mailto:netguru@xxxxxxxxxxxx)> wrote in message [news:uofZJtokGHA.1508@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:uofZJtokGHA.1508@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

I disagree with this line on many levels but also see the logic of the reasoning that leads to it.

briefly,  
allowing a reservoir of unpatched computers to remain on the global network

"allow" is the wrong verb here

As indicated before, you assume patching of binaries that have been altered into unknown states would work.

Rootkits would have come more and more prevalent no matter what choice was made on this specific issue.

The systems would have only become modified to not patch key aspects, if as desired, but to appear to be getting patched. This is a pattern seen already where one side escalates the efforts (in you exhortation this would be providing patches to the illicit, which includes owned, machines) just to see the other deploy countering measures.

Again, the real problem is your assumption of "allow"; it is too presumptive of an actual capability/capacity. More to the point would have been "choosing not to attempt patching of a . . ."

directly relates to the Polio analogy I used earlier. The only difference is that the epidemic hot spots are global in scale. Now we are seeing Webroot and other tools being deployed to detect and manage Malware as well as seeing our old friends AdAware, Spybot S&D and new friends like Microsoft Defender completely bamboozled by Malware that loads as kernel mode / stealth mode root kits with encrypted registry keys.

"now we are seeing" and we would have by now anyway.

## Re: Why not patch all windows and not just legal copies

A very large percentage of the owned machines are owned due to user practices and (perhaps not informed) choices/actions.

In a perfect world there would be no pirate systems, in the real world there are literally millions. HOW do we redress them.

1. dont patch
2. patch
3. block access (simple enough in theory but impossible in practice).

and I am indicating that choice 2 is not so clearly possible.

Yes, a number would/could be patched for this/that/the-next . . .

Again, a critical point to consider is the illicit code is not always just the genuine binaries with a pilfered key or disabled WPA.

The simple fact is that there is a lot of money in having unpatched systems around. Since we have to spend money to protect ourselves (what would the current IT landscape look like if Windows didnt have over 100,000 virus / malware issues). The problem with this worldview is that we are constantly in a reactive mode and dont know what is coming next. Some believe that SPI firewalls are enough, others understand that no single technology can protect us from todays environmental malware vectors.

Consider the MS position. Due to its prior crapware written for non-networked systems, etc.. there is a plague on their installed base. If they purchase and supply free means for people to deal with this they are being anti-competitive potentially putting an entire industry out of business. In an idealized world, where the redesigned software engineering process and objectives/priorities now in use might result in a totally immunized system, there is a question what the lawyers that believe themselves able to make software engineering decisions will attempt in the courts.

Finally,

It's important to remember that the needs of the few are outweighed by the needs of the many and doing nothing for bootleg OS is doing something to the

Re: Why not patch all windows and not just legal copies

You have totally lost me . . . I attempt to see logic in that but fail.  
Who is the few? Those dupped into buying in good faith computer systems  
that after the Genuine programs started discovered that they had been taken,  
sold a non-genuine, pirated knock-off ??  
Who knows what is on those (privacy violating, identity forwarding,  
keylogging . . .)  
What is the need of those few?  
I would say it is the discovery of their peril and getting them to a  
position in  
which they can have the use of a trustable computing system, which is what  
they were in the belief that they did have.

rest of us. Can we harden Windows to resist arbitrary attacks? Lets look  
to the past for the answer, where we find a resounding no. Can we shrink  
the attack surface? IMHO the answer is yes.

Safety is a user choice issue as much as it is one of the software  
involved and choices for that software's default config/behaviors.

Also, the past is often not a good indicator of the present/future.  
And, just as this is so for comparing Wilson's America to today's, this is  
also so for comparisons of pre-W2k3, pre-XP-SP2 era code to the  
current generation. Things really have changed, not perfectly sure, but  
changed in very significant ways and extents. On the other hand, I still  
wait for the decade where I feel that using sendmail's past as a predictor  
for its future is invalid.

its an effort of will and bootleg systems are bots

Perhaps it is time for beneware (mal contra beni)

I was not happy when MS made its intentions known relative to  
patch availability. My thinking then was that the decision would  
fail to help calm the storm then raging on the network – demons  
knocking on every protocol/port, uselessly consumed bandwidth,  
etc.. Today I am thinking I did not see some factors about the  
larger ecosystem that is Windows on the world network. There  
are quite a few people/businesses that now run certifiably real  
OS versions, that at the time did not. I know this as I saw many,  
many people posting about the scum that had sold them . . .  
yada, yada . . . when the genuine tests first deployed. Now,  
knowing those that post here are a sliver sized sample of what is  
happening out there I can only guess that there are quite a few

Re: Why not patch all windows and not just legal copies

people now with real OS bits that otherwise would not have them. (Yes, genuine program could have said Oh, we see you are running fake or illicit Windows, we really suggest you pay up and also go through the pain of getting real bits in use. I do not believe all those seeing that would have acted on that. I do believe we would be seeing small businesses and home users "buying" bits with everything already in place for them to be bot net zombies, identity leaking junk).

There are issues at work that are larger than the ones you have indicated in your initial and follow-up posts. You are not on the wrong bandwagon, you just are not seeing all of the road.

Roger

"Roger Abell [MVP]" <mvpNoSpam@xxxxxxx> wrote in message [news:%23JJrIsnkGHA.2280@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:%23JJrIsnkGHA.2280@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

The debate raged for a few months over a couple years ago (between some MSFT people and some MVPs) with the reasoning being much as some of what you presented – i.e. vast network impacts from illicit and corrupted systems. That was when automatic updates was just emerging as an effective force (hmmm, perhaps that raging debate was more like three years ago now).

There were some surprising reasons presented.

One obvious one that you are apparently overlooking is that it is not a simple matter to patch something that is not in a known condition (i.e. a valid patch to valid OS binaries could blow away illicit binaries);

and that there might be legal issues as a result in some countries.

There were other issues, more subtle than I can recall/repeat.

Now, MS did recognize the parts of the argument about the unhealthy state of the network globally due to unfit systems, and not much later brought out the almost free lite versions of XP available in some parts of the world. Since that time they have also made investments in anti-malware technologies and you have seen these being rolled out to legitimate OS owners at from zero to little cost, and they also made major investment in things pumped into XP via SP2.

While at the time I questioned some of their decisions about leaving the rogue, illegal systems to fend for themselves. In retrospect now it seems that they were right. Not only did not making patches available make "owning" an illegal system less attractive, it has probably also had an impact on the size of that population (the network sicknesses raged intensely among the unprotected/unprotectable). At the same time, the aggressive push to get all legitimate machines made into loyal clients of the automatic update service seems to have had a vast impact on the patch-state of legitimate machines on a gross average.

"Michael Davis (Comcast.Net)" <netguru@xxxxxxxxxxxx> wrote in message [news:uz8Q5vIkGHA.4224@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:uz8Q5vIkGHA.4224@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

## Re: Why not patch all windows and not just legal copies

It seems to me that its a bad idea to deny owners of illegal copies of windows the ability to patch their computers. Windows is running on hundreds of millions of computers and hundreds of millions of computers are not being patched. Here are the issues which lead to the perfect storm we are in right now.

1. Computer programming languages like C that do not check for buffer overflow (require that the programmer code for buffer overflow checking within the application itself)
2. monolithic adoption of a singular operating system for servers and client computing.
3. stolen code for NT 4.0, Windows 2000 and Windows XP.
4. majority of Microsoft code run in pacific rim and former USSR is not legit

Microsoft Policy requiring validation to patch operating systems.

5. windows available from WAREZ and other download sites, hacked, infected etc.
6. rapid adoption of new code practices without consideration of the security consequences
7. botnets composed of compromised systems
8. adware, spyware, malware, virus (to me, if I didnt install it, its a virus)
9. The Internet and nature of TCP/IP

To fight this perfect storm Billions of dollars are being spent to simply stay current. Meaning that the legit systems are constantly being assaulted by botnets comprised of hacked unpatched computers and

Re: Why not patch all windows and not just legal copies

networks have to respond to new emerging threats arising from the sea of unpatched computers.

It is simply prudent to realize the nature of the situation and allow all windows systems to be patched or at the very least someone should offer 3rd party alternative patches to bootleg since we know they will not buy Windows and they are being exploited.