

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

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2006-06/msg00246.html>

- *From:* "Michael Davis \ (Comcast.Net)" <netguru@xxxxxxxxxxx>
 - *Date:* Sun, 18 Jun 2006 10:32:21 -0400
-

I agree completely,

This topic needs more dialog and not less, the logic is not flawed and the purpose is clear. Security is about reducing attack surfaces, getting secure and keeping secure. having a resting pool of rootkitted bots in the pool THAT CANT BE PATCHED BY THE AVERAGE OWNER with us just makes "some" of us a lot of money and causes a "lot" of us pain and suffering.

Think of that next time you are working on a system that has been hit by :exploit next" or DDOS attack, or Uber SPAM that blows thru that very expensive anti-SPAM system you just talked the CIO into buying.

"imhotep" <imhotep@xxxxxxxxxxx> wrote in message
news:mradnaVmF-pzwwjZnZ2dneKdnZydnZ2d@xxxxxxxxxxxxxxxxxxx

Roger Abell [MVP] wrote:

While you have many, and many-sided, views expressed in your post, I find the underlying reasoning somewhat flawed and conclusions too simplistic. If bootleg systems received patches, there would only be more and more of them, and they likely would be rootkitted bot daemons from the day they were born.

Now that reasoning is flawed. Let's "boil" this down:

Not patching pirated MS products helps Microsoft strong arm people into buying a legitimate copy at the expense of everyone else who has to deal with DOS Attacks, Bot'd PCs, the spreading of more viruses and malware....

Now Roger, Mr Microsoft "Spin Manager", stopping spinning and be honest...

I think the heath of the Internet, and the people and companies that use it, is more important than Microsoft getting yet another x million in profit.

Im

"Michael Davis (Comcast.Net)" <netguru@xxxxxxxxxxx> wrote in message 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 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.

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).

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 worldwiew 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

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

single technology can protect us from todays environmental malware vectors.

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 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.

its an effort of will and bootleg systems are bots

"Roger Abell [MVP]" <mvpNoSpam@xxxxxxx> wrote in message
news:%23JJrlnkGHA.2280@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

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

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

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@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

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 hundereds 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

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

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

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

spent to
simply stay current.
Meaning that the legit
systems are constantly
being assaulted by botnets
comprised of hacked
unpatched computers and
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.

--

Pass a Net Neutrality Law in the US!!!!

Save the Internet:

<http://www.savetheinternet.com/>

Its our net:

<http://www.itsournet.org/>
