

Re: Any Way to Run Windows 2000 From Read-Only CD?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2005-01/0166.html>

From: Karl Levinson, mvp (levinson_k_at_despammed.com)

Date: 01/13/05

Date: Wed, 12 Jan 2005 23:05:30 -0500

I concur, Bart's PE is a popular choice for making a boot CD. Any boot CD is going to run much slower, and a lot of RAM memory is recommended.

Many people in large environments with concerns like yours also consider using software that freezes and restores the configuration at reboot, like FreezeX / DeepFreeze, and/or a solution where the computer is re-imaged every now and then at reboot. You can also consider PivX or PrevX to harden the computer against unpatched vulnerabilities, or SecureEXE to prevent unapproved executables from running.

Note that absolutely none of these prevent your computer from becoming infected. What they will do is prevent anything from remaining after a reboot. However, while your system is running, it can be infecting other computers on the network. And then after your reboot, if your machine is then immediately re-infected, your read-only boot CD will have done little to help. This is similar to the advice in the 1990s to make your MS Word normal.dot file read-only to prevent Word macro viruses... this sensible-sounding idea ended up helping not at all. A network worm like Blaster / Welchia or Sasser would keep reinfecting your computer quickly after each reboot.

I must say I don't have the same problems you are having keeping Windows secure, or with securing it. Assuming you're on a large network, have you followed the hardening guides at www.microsoft.com/technet/security and www.nsa.gov/snac, and used group policy templates, active directory, script files and/or ghost images to automate the process of hardening machines? Most adware is prevented by doing one or more of the following: 1) using anti-virus like McAfee that detects spyware and adware, 2) using patch management software to install patches regularly, 3) using some sort of Internet content filtering like the Spybot Search & Destroy "Immunize" button or the Restricted zone adware .REG file at www.mvps.org, always logging in as a non-admin, non-power-user for web browsing, and/or upgrading to XP SP2 asap. Running a non-MS browser might help somewhat, for now.

I don't think Windows is any harder to harden than other OSes [except that some other OSes that are newer will naturally have better default settings].

microsoft.public.windows.server.security: Re: Any Way to Run Windows 2000 From Read-Only CD?

Windows 2000 was released about the same time as RedHat 6.x / 7.x, and that wasn't secure by default either. Windows XP SP2 on the other hand is pretty secure by default. For home users, the 1, 2, 3 of antivirus, firewall and patching is pretty effective, especially if the AV detects adware. More hardening guidelines are here:

<http://securityadmin.info/faq.asp#harden>

"Herb Martin" <news@LearnQuick.com> wrote in message
news:%23pLmcf9EHA.824@TK2MSFTNGP11.phx.gbl...
> "Will" <DELETE_westes@earthbroadcast.com> wrote in message
> news:uwDwILT9EHA.3076@TK2MSFTNGP15.phx.gbl...
> > I'm so disgusted by viruses and hackers that I would like a way to run
> > Windows 2000 from a read-only device that cannot be rewritten, in the
> event
> > that any service is compromised. Has anyone published instructions on
> how
> > to build a bootable Windows 2000 CD?
>
> BartPE.
>
> Nothing's perfect but this is close.
>
> --
> Herb Martin
>
>
> >
> > --
> > Will
> >
> >
>
>