

# Re: How About a Hardended Win2K Image to Bash?

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-01/1137.html>

---

**From:** Steven L Umbach (*n9rou\_at\_nospam-comcast.net*)

**Date:** 01/27/05

Date: Wed, 26 Jan 2005 23:23:37 -0600

*>From what I see most [including many admins] do not know how to properly lock down a computer or have the discipline to maintain it. Many realize this and to them antivirus protection has a low TCO considering the havoc it can wreak on a network and yes it may allow them to be a bit lazy, but alas that is human nature. Also many many small businesses do not have a full or part time admin that knows how to lock down a network or OS. Many networks also allow users to be local administrators for various reasons that may be political or due to uncooperative applications such Quickbooks which substantially increases the risk. Email attachments are probably one of the biggest threats as far as malware attachments yet people continue to open them up. There is also the possibility of a zero day threat that a antivirus program may be able to arrest even without the signature. I agree with you in that I don't consider W2K to be an insecure operating system as long as a few changes are made, and it is kept current with critical updates. I also believe that it can be hardened to a degree that is very resistant to malware while still largely being functional. However, not knowing the abilities/practices of the users or admins I will always recommend antivirus protection to users and for businesses the TCO is low and no admin in his right mind would want to take the blame for not using it in case something did go wrong. The threats of lawsuits and regulations to protect data/privacy also compel many to use antivirus software whether they think they need it or not.*

I don't know why McAfee was resistant to Melissa. If they were using NT workstations and servers they probably did lock the computers down at least somewhat. I don't know how it was spread, maybe host based firewalls were used on the network. Maybe that had implemented preliminary updates on their computers or took other precautions based on knowing about the malware before it came to them. --- Steve

"Gordon Fecyk" <gordonf@pan-am.ca> wrote in message  
news:u92dZ\$7AFHA.3820@TK2MSFTNGP11.phx.gbl...

>

> "Steven L Umbach" <n9rou@nospam-comcast.net> wrote in message  
> news:udbLm3oAFHA.1452@TK2MSFTNGP11.phx.gbl...

microsoft.public.security: Re: How About a Hardended Win2K Image to Bash?

>> *Antivirus is not an end all solution but a tool that has it's purpose.*  
>  
> *Sure. And that purpose is to act as a security blanket. It's not doing  
> much else.*  
>  
> *I'll ask you the same question I asked Karl: When Melissa came out,  
> McAfee  
> stayed up and uninfected while most of McAfee's customers were infected.  
> They hadn't released a patch for their anti-virus products until a few  
> days  
> after the first sightings, yet they stayed up and uninfected. Why?  
> Surely  
> they use Windows, and surely they use their own products as a matter of  
> corporate policy.*  
>  
> *I doubt they used the techniques I brought up here, because Win2K wasn't  
> released yet. So how did they stay up?*  
>  
>> *don't doubt that a stout version of the operation system can be built and  
>> use such myself. Note that it is trivial to take admin privileges when  
>> one  
>> has physical access to the computer so it will be hard to weed out  
> cheaters,  
>> though if the original admin password has been changed that would be a  
> give  
>> away.*  
>  
> *These are things that could happen on any system with any amount of  
> protection short of encrypting the entire file system. But how often does  
> it happen that some Joe Six-pack deliberately wants to hack their own PC?*  
>  
> *Besides when they forget their passwords, that is... heh heh*  
>  
> *The problem is keeping malicious, or ideally, unauthorized code from doing  
> damage. "Oh, it is so easy to poke someone's Windows PC while they're  
> on  
> the Internet, install something behind their backs, or make them install  
> something without realizing it, and monitor everything they do." No OS is  
> going to save you from some burglar physically breaking into your home and  
> stealing your PC to hack it later, but I insist that the "covert"  
> break-ins  
> are stoppable with what's built into the system right now.*  
>  
>> *I had a  
>> kiosk W2K computer at my business for over two years running Windows 2000  
>> without AV and never had a problem. It had a locked computer case and no  
>> cdrom or floppy drive, just internet connection.*  
>  
> *With examples like this, why are folks whining that Windows Is So  
> Insecure?  
> Not just insecure, but*

microsoft.public.security: Re: How About a Hardended Win2K Image to Bash?

> *"paper-thin-easily-hacked-to-pieces-by-two-bit-script-kiddies" insecure?*  
>  
>> *Having said that I am not an average user and that is what makes most of*  
> *the*  
>> *difference. For the average user I would consider virus protection a*  
>> *necessity and smart to do in a business environment as things tend to*  
>> *slip*  
>> *in between the cracks.*  
>  
> *OK, you're prepared to leave a public kiosk running Win2K open to use,*  
> *with*  
> *only an Internet connection without AV, yet would insist on AV in an*  
> *office*  
> *running the same thing? Even if you removed the CD-ROM drives and floppy*  
> *drives, and denied access to usbstor.inf/pnf to disable USB memory cards?*  
>  
> *I'd have thought office staff would be MORE trustworthy than the general*  
> *public.*  
>  
>> *Anyhow have fun and I will not take you up on your challenge.*  
>  
> *What are you afraid of?*  
>  
> *I won't even do the things you mentioned (disable Windows Scripting Host,*  
> *disable IIS, disable Telnet, set a ton of IP filters).*  
>  
> --  
> *PGP key (0x0AFA039E): <<http://www.pan-am.ca/consulting@pan-am.ca.asc>>*  
> *What's a PGP Key? See <<http://www.pan-am.ca/free.html>>*  
> *GOD BLESS AMER, er, THE INTERNET.*  
> *<<http://vmyths.com/rant.cfm?id=401&page=4>>*  
>  
>