

Re: Windows 98 box is "owned"

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-10/0097.html>

From: Charles Otstot (charles.otstot_at_ncmail.net)

Date: 10/01/04

Date: Fri, 01 Oct 2004 08:56:35 -0400

To: security-basics@securityfocus.com

Darren Kirby wrote:

>>Hello all,

>>

>>First of all, thanks for all the replies, it is way more than I was expecting.

>>

>>After following the link provided by Bob Bermingham:

>>

>>

>

>

>>>>Sounds like the box is "owned", but not in the way you suspect. From

>>>>your description, it looks like she is infected with Netsky.P:

>>>>

>>>>

>>

>>

>>

>>

>>

>

>

>>>><http://antivirus.about.com/cs/allabout/a/netskyp.htm>

>>>>

>>>>

>>

>>

>>

>>I can confirm this is indeed the Netsky.P virus. The filenames listed are

>>EXACTLY the ones on this box. From reading the description it would seem this

>>is very old virus...so she (my mom) is running a very old unpatched windows

>>98? Please let me reiterate at this point that I am really ignorant of

>>windows...but I have heard that Microsoft has ended support for this old OS.

>>Is there still a patch available?

>>

>

SecurityFocus BASICS: Re: Windows 98 box is "owned"

>

Microsoft officially is no longer issuing *new* updates for Windows 98, however, you can find archived updates at both Windows update and in Microsoft's Security site.

Please note that although there is some overlap, the two sites do have some different updates available. You may not find all security updates on Windows update, although you will find all the "critical" (as defined by MS) updates. Microsoft has released a couple of updates since support ended for particularly nasty security issues, so I won't rule out that they will *never* issue anything else for 98, but don't hold your breath either.

>>

>>*James Grant posted:*

>>

>>

>

>

>>>>2) *Install ZoneAlarm. It's free and it will give her network protection. Set it up for her, because she may not want to read the pop-up questions it asks at the start to know what to allow.*

>>>>

>>>>

>>

>>

>>

>>*Ironically, she installed this herself...I presume after she was already infected. The problem with this she tells me, is that the pop-ups tell her "foobar.exe is trying to access the internet" and she can not ever tell if foobar.exe is legitimate or not. Unfortunately I don't think I could help her on this point, as I would not know either...*

>>

>>*You all pretty much suggest installing software firewall, spyware checkers, anti-virus scanners, even a hardware firewall...all my mom does is play freecell, check email once a day, and browse the web infrequently (1-2 times per week), so this hardware firewall seems a bit extreme.*

>>

>>*RandyW posted:*

>>

>>

>

>

>>>>*Without constant monitoring though, the PC WILL become infected again, it's just a matter of time.*

>>>>

>>>>

>>

>>

>>

SecurityFocus BASICS: Re: Windows 98 box is "owned"

>>*This is discouraging, as I don't have the time (nor knowledge) to monitor this
>>computer all the time. Perhaps it is time to say screw it and install
>>Slackware with a nice KDE desktop for her, because at least I would know how
>>to help with her problems, and it seems a lot easier than:*
>>
>>*1) reinstall OS
>>2) install firewall, AV, etc...
>>3) patch OS in 5 minute window available (as mentioned by Kelly Martin)
>>4) educate Mom on use of AV, anti-spyware, good web practices (don't open
>>attachments, click on pop-ups etc...)
>>5) monitor until eventually another virus finds its way in.
>>6) Lather/rinse/repeat.*
>>
>>*Sorry if I sound affected here, but being a unix guy I do not see how this
>>makes windows an 'easier' desktop to use. What do you all think? Is this
>>really what you have to do to have a usable windows networked machine?
>>Again, not trying to be a troll here, it is an honest question.*
>>
>>
>
>

Please understand that what I'm about to say is NOT how I would suggest handling a business system in a *corporate* network environment. My points are all predicated on the premise that this is a home machine (as noted in your posts) that is apparently not used to maintain or communicate highly critical or confidential data.

Overall, you can go a couple of different ways. Reinstalling the OS is probably a reasonable course, just as with any server that has been compromised. It will likely be the quickest method of assuring the integrity of the system. *However*, if you feel reasonably confident that the NetSky infection is all you're looking at, then simply installing (or updating) AV may be sufficient for returning the system to use, it depends on your confidence and your (and your mother's) aversion to risk. If you go with the latter, just make sure you follow the vendor's recommendations for scanning a suspect system as a precaution. You noted that your mother has ZA. While none of the personal software firewalls out are overly difficult, they can be a bit daunting for the novice. Your mother may not grasp all of the nuances, however, you can pretty safely tell her that if she didn't initiate an application, then anything outbound should probably not be permitted until you've looked at it. Conversely, if she launched an app (say OE) and she gets popups from ZA, she is likely safe to allow those things to pass. **Note, this assumes you have taken steps to assure that you have reasonable confidence in the system's integrity.

Patching the system should not be overly difficult. Yes, the 5 minute window sounds extreme, but if you connect to Windows Update and let Windows Update install the patches for you, you will probably be ok. There are risks, as yes, there are worms still lurking (looking for NetBIOS shares, etc.), but if you follow a few precautions, you will

SecurityFocus BASICS: Re: Windows 98 box is "owned"

substantially reduce your risk. Most importantly, absent a need otherwise, remove all of the Windows Networking client components. You can install the TCP/IP stack on a Windows 98 box independent of any client software, so there is no need for NetBIOS unless you have a network. This will also have the benefit of increasing system performance (albeit marginally). This one step will eliminate the risk of attack from probably 95% of the nasties that can get you before patching.

Educating Mom on good practices is something you should probably do anyway (platform independent). It really won't take long, and you get to spend a little quality time together :). Sadly, today the extra utilities do tend to be more of a necessity than a luxury, but using automation makes their use much less onerous. One item you mentioned that some anti-spyware apps will take care of for you is pop-ups. Most have pop-up blockers that quite effectively block the popups that install a high percentage of spyware on people's systems, so your Mom can surf safely without ever being knowing that a site was loading popups (if you so desire, I set mine to prompt me). Fortunately, current system protection apps (AV, anti-spyware, etc.) generally allow you to set up automated schedules for their important tasks (e.g scans and def file downloads). For the most part, you can "Set it and forget it". When you're visiting, you can randomly take a few minutes to ensure that everything is continuing to run up to snuff, but neither you or your mother will be unduly burdened.

Something may or may not "eventually find its way in", but the above will make it a lot harder and a lot less likely. All told, I would expect that you can remove the offending malware (NetSky) either through a rebuild or cleaning, return the system to working status and educate and reassure your mother in an afternoon.

Being an old Windows guy, I will admit to my biases, but as to installing Linux and KDE, I would expect it will take you longer than that to install and educate her on the new software system to where she feels comfortable with the technology. I would think your support call volume would go way up for at least a while :). However, you did mention one important point that may actually make it a good course to take... being able to help more effectively. If your mother has a lot of trouble running her current platform and you are unable to assist her, then perhaps Linux/KDE would be a good choice. I *would* say that if she has a lot of trouble running 98, you may want to consider whether her assistance needs are really more OS-related or technology-related; i.e are her problems due to a lack of Windows knowledge or to a general lack of computer knowledge. If the former, jump on Linux/KDE where you're on familiar ground. If the latter, consider recommending some education regardless of which platform you ultimately have her on. Many locales have local community college classes (generally cheap) and other classes designed for novice/home users to help them understand the absolute basics of computing and help make them more comfortable with the computers.

SecurityFocus BASICS: Re: Windows 98 box is "owned"

>>*Thanks again for all the helpful information,*
>>*much obliged,*
>>
>>*-d*
>>
>
>

Hope this helps, at least a little.

Charlie

>>
>