

SecurityFocus BASICS: RE: Windows 98 box is 'owned'

RE: Windows 98 box is 'owned'

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-10/0064.html>

From: Randy Williams (randyw_at_techsource.com)

Date: 10/01/04

To: <bulliver@badcomputer.no-ip.com>, <security-basics@securityfocus.com>

Date: Fri, 1 Oct 2004 10:43:14 -0400

Greetings,

Ahh the curse of the Netskyp!

Microsoft has indicated that support for the Win9x/ME series of OS's will no longer have support in the future. I am unsure of the exact date, but it is a safe bet going forward that you should plan for support to not be available.

Your mother inadvertently has discovered the weakness of the software firewall, if the user tells the firewall to compromise itself; it will do as it's told!

If you Mom is up for a change (some aren't by the way), then I would agree that a move to Slackware, Gentoo, or whatnot (insert favorite distro here) would be the best answer. Windows PC's require a lot of overhead to keep running in proper shape, and while in a corporate environment that isn't so bad, at home it can be a real challenge if the user(s) don't keep up with it.

I've field tested some Linux distro's with Windows 9x/ME users before and as long as I had all the shortcuts they'll need on the desktop they didn't even notice the difference. If my own mother didn't require Office for her job, she'd be running Linux right now!

Don't worry about being "affected", when I talk to my friends (after cleaning up a completely hosed machine) and explain what it takes to keep a Windows machine properly running, they don't like it either. "I just want it to work!" (trans. Without putting any effort into it.)

They really are becoming quite a bother to keep safe at home, and if you are going to have to support it, why not use something that you can keep in sniffy top shape (remotely too, if Linux based)?

Just my \$.02 again though... (As a disclaimer, I run Win2K at home behind a Linksys NAT box, have ZoneAlarm Pro 5.x, SAV 9.0 CE, Adaware, Spybot, Firefox/Netscape, Thunderbird and regular cleanings twice a month and I

RE: Windows 98 box is 'owned'

SecurityFocus BASICS: RE: Windows 98 box is 'owned'

STILL find junk that slips through IE on the rare times we have to use it!)

RandyW

-----Original Message-----

From: Darren Kirby [mailto:bulliver@badcomputer.no-ip.com]

Sent: Thursday, September 30, 2004 5:48 PM

To: security-basics@securityfocus.com

Subject: Re: Windows 98 box is 'owned'

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?

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

RE: Windows 98 box is 'owned'

SecurityFocus BASICS: RE: Windows 98 box is 'owned'

>*just a matter of time.*

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.

Thanks again for all the helpful information,
much obliged,

-d

--

Part of the problem since 1976

<http://badcomputer.no-ip.com>

Get my public key from

<http://keyserver.linux.it/pks/lookup?op=index&search=bulliver>

"...the number of UNIX installations has grown to 10, with more expected..."

- Dennis Ritchie and Ken Thompson, June 1972