

Re: I am REALLY Getting Tired of Probes on 445 and 135

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2004-11/0169.html>

From: Leythos (void_at_nowhere.org)

Date: 11/19/04

Date: Fri, 19 Nov 2004 15:24:44 GMT

In article <ggurp05td66uqe1mg17ii5tkajd94hgb8v@4ax.com>, NoSpam@NoSpam.net says...

> *On Thu, 18 Nov 2004 10:13:27 -0500, Lars M. Hansen*

> *<badnews@hansenonline.net> wrote:*

>

> *>Oh, we changed the topic from Windows to IIS? Did I miss a memo*

> *>somewhere?*

>

> *It wasn't a topic change, it was an illustration that lager*

> *marketshare does not mean more security problems.*

The illustration is flawed in this discussion. IIS is no more a security risk, when properly configured, than any other web server service.

> *Poorly designed software means more security problems. Software that*

> *is not designed with security in mind means more security problems.*

There is a difference between poorly designed software on any platform and a poorly designed Operating System. And Poorly is subjective.

As a typical example, MS OS based systems are used in their default configuration by most users that are compromised.

The vast majority of users on the internet are running a MS OS.

Even Linux systems, which make up an almost insignificant number of users on the Internet, are compromised on a daily basis.

Both platforms have poorly designed software – you can see this by the number of software (we're not talking OS) updates release for the applications running on the platforms.

The background chatter on 135/445 is at the current level because the MS OS is set to default to a non-secured, non-locked down, mode by default.

The non-MS bases platforms are much less open to the MS types security

comp.security.misc: Re: I am REALLY Getting Tired of Probes on 445 and 135

default problems, but they are also open to security flaws in many of the applications installed on the non-MS based platforms.

What you need to do is understand that the percentage of compromised systems takes into account for the NUMBER of installed systems, it's proportional to the installed base.

If you look at the probes we get on our servers, the amount of activity from MS based systems is the same as non-MS based systems when you consider the installed BASE.

Now, so that you don't misunderstand, even the MS Based OS's can be secured as well as the non-MS based OS's, you just have to understand them in order to do it.

--
--

spamfree999@rrohio.com
(Remove 999 to reply to me)