

microsoft.public.security: Re: So how secure is Windows XP with all current updates?

Re: So how secure is Windows XP with all current updates?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2004-06/1546.html>

From: Alun Jones [MSFT] (alunj_at_online.microsoft.com)

Date: 06/23/04

Date: Wed, 23 Jun 2004 09:18:15 -0700

"Paul Adare – MVP – Microsoft Virtual PC" <padare@newsguy.com> wrote in message news:MPG.1b43178f2eb5faa0989989@msnews.microsoft.com...

> *In article <edcOEWMWEHA.1652@TK2MSFTNGP09.phx.gbl>, in the*

> *microsoft.public.security news group, Kent W. England [MVP]*

> *<kwe@myps.org> says...*

>

> > *The Blaster worm is an example of an infection that ***got into patched*

> > *machines*** that didn't have extra firewall protection to block the*

> *NetBIOS*

> > *RPC port(s).*

>

> *How do you reconcile these two contradictory statements? (My emphasis*

> **** added)*

>

> > ****Anyone who was using Windows Automatic Updates was protected***,*

> > *since the MS patch came out before the exploit.*

> >

>

> *The first statement says that Blaster infected patched machines while*

> *the second statement says that those who were patched were protected.*

Kent may be reaching a bit, but I think I can reconcile his statements... sort of.

The Blaster worm was discovered on August 11, 2003.

<http://www.microsoft.com/technet/security/alerts/msblaster.msp>

The patch for MS03-026 was released July 16, 2003.

<http://www.microsoft.com/technet/security/bulletin/MS03-026.msp>

A machine that was fully patched prior to the release of the MS03-026 patch was still vulnerable to the exploit described in MS03-026, and if Blaster had been released then, or earlier, that patched machine would have been "owned" by the worm. Give a user a machine and tell them it's "fully patched", and a significant percentage of them will believe that this

Re: So how secure is Windows XP with all current updates?

microsoft.public.security: Re: So how secure is Windows XP with all current updates?

description applies a week later, a month later, a year later.

One postulated reason (and it's quite likely, IMHO) that the worm post-dated the patch is that the worm's authors reverse-engineered the patch, to see what it was designed to fix, and wrote the worm to attack the pre-patch hole. [Needless to say, that doesn't make their efforts in creating this worm look like a technical achievement worth bragging about – merely a criminal act by mindless vandals.]

I think the original poster is confusing patches with holes. Holes do not spring into existence when a patch for them is created, holes spring into existence when the code is written without fully considering all cases. When the holes are discovered in a piece of software, and that discovery is announced to the developers of that software, they will work feverishly(*) to create a patch (and then, they test the patch to make sure it doesn't create a hole somewhere else, or break features needlessly). When the discovery of a hole is announced to hackers and crackers, they work equally feverishly (although without as much care to testing or broken features) to find a way to exploit it to their own gain.

Once a patch is released, the pace of progress is in the hands of the users – and many of those are not sufficiently well-educated about the workings of their systems to understand how to patch them, or to understand why to patch them. You'll notice, when we release it, that we've ramped up a lot in Windows XP Service Pack 2 in that regard. More education, easier updating, better protection even in the event that a vulnerability occurs and is exploited.

But yes, the point is very valid – while the steps outlined at <http://www.microsoft.com/security/protect/> are the best first-line defence, they are not foolproof, at least in theory. So far, they have been very reliable in practice – though obviously not foolproof. The key, then, is to make sure that you remove yourself as far as possible from the pool of fools, by educating yourself as to safe behaviour on the Internet. Treat every email as if the address on the envelope was hand-written in thick black crayon. Attachments are dangerous – don't open them unless you are certain that they do not contain viruses. Keep your firewall locked down, and consider whether it would be a good idea to take your "always-on" Internet service, and turn it off when you're not actively using it. Don't share files – while it's [usually] illegal, and you shouldn't do it because of that alone, it's also a wonderful way for people to put viruses on your machine without you being able to trace where they came from.

Alun.

~~~~~

(\*) There is some debate on whether the level of fever is enough. Some people advocate announcing holes immediately to the general public, as a way of sticking a cattle prod into the sides of the developers concerned. As one of those developers (though I haven't yet been the cause of any vulnerabilities at Microsoft), I can definitely say that this doesn't improve my ability to rationally write a decent fix. I'm human – my first

Re: So how secure is Windows XP with all current updates?

microsoft.public.security: Re: So how secure is Windows XP with all current updates?

instinct is to grumble about why I wasn't told before the hackers and crackers.