

Re: Security Problems Plague XP SP2 via Symantec/McAfee

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2005-02/17594.html>

From: Gary S. Terhune (*grystnews_at_mvps.org*)

Date: 02/15/05

Date: Tue, 15 Feb 2005 03:14:52 -0800

http://story.news.yahoo.com/news?tmpl=story&u=/tpcworld/20050210/tech_tues_pcworld/119627&cid=1740&ncid

If the above link doesn't work for you, try this:

<http://tinyurl.com/7ybuc>

That is the "more" you're asking for. More than this, Dan doesn't know, I'm sure. My take on the subject is a bit different. While acknowledging that I am not a fan of either product, and I've not hesitated to say so on innumerable occasions, what is described by the article isn't a real security risk, per se.

The way I read the article is this:

One of the new features in Windows XP Service Pack 2 is the "Windows Security Center". It keeps track of what, if any, antivirus and firewall apps are installed, and whether they are up to date. If you are lacking in a firewall or antivirus, or if they are simply not running, the WSC advises you of the situation. However, as anyone who pays attention will know, when you first install such applications, they are **never** up to date and should be updated immediately. One result of this combination of affairs is that while installing such apps, the new Windows Security Center may warn, repeatedly, that the programs are not up to date. Symantec and McAfee consider this detrimental to the "user experience"—and in a way, I can't blame them. It **is** disconcerting to get repeated warnings that you aren't protected while you are in the very act of installing protection.

Norton solves this by deliberately disabling Windows Security Center during installation (which makes one wonder about the architecture of Windows Security Center, doesn't it?) McAfee changes the dates of certain files to "now" as they are copied into the system. This convinces Windows Security Center that there is now up-to-date protection installed and it keeps quiet. However, apparently, the antivirus app now thinks it's up to date, also, and may not initiate an update, leaving the user with a very out of date antivirus until

sufficient time has passed and it then updates. Or perhaps it still initiates an update during the normal course of installation, but in many cases this isn't feasible due to the system not being able to connect to the internet. I don't know the particulars.

For myself, the most alarming thing about this whole affair is that the Windows Security Center *can* be disabled by any means other than user intervention. Makes it rather useless, don't you think? Plus, McAfee's methods would tend to leave a user with a false sense of security between the time of installation and the first actual update. Judging by the usual amount of time that such apps consider reasonable between updates (a horribly long time in my opinion), a person could be running several days without real antivirus protection and not realize it.

Of course, this has always been the case—automatic updaters are famous for failing in their duties, especially where the systems aren't connected to an always-on internet connection, or are used sporadically for relatively short periods of time, or simply being inadvertently disabled. This is why Windows Security Center was developed. And this is why I always admonish users to *check* that AV and Firewall is running when they startup and periodically throughout the day, and that they run the updater(s) manually, on an at *least* daily basis. These are habits that should be as deeply ingrained as checking your rear-view mirrors regularly while driving.

--

Gary S. Terhune
MS MVP Shell/User

<http://www.grystmill.com/articles/cleanboot.htm>

<http://www.grystmill.com/articles/security.htm>

"Daniel Royer" <daniel@royer.ch> wrote in message
news:4211c945\$1@nntp.unige.ch...

>

> " Microsoft Window users need to be aware that McAfee and Symantec
(aka

> Norton)

> products can disable advanced security features of XP SP2"

>

> Could you elaborate a little more on that?

>

>

>

> _____
> Daniel Royer, University of Geneva

> daniel at royer dot ch

>

>

> "jane" <jane@internet.com> wrote in message

> news:u7BdUG0EFHA.1524@TK2MSFTNGP09.phx.gbl...

> >

> >> Microsoft Window users need to be aware that McAfee and Symantec
(aka

> > Norton)

> >> products can disable advanced security features of XP SP2. I
advise

> >> users

> > to

> >> rid their operating systems of these terrible products and use

other

> >> means

> > to

> >> protect themselves in the on-line world.

> >>

> >

> > Hi Dan,

> > Is it only XP users that are affected?

> > I see you posted this in a 98 group so I have to ask.

> >

> > regards Jane

> >

> >

>

>

>