

Re: FAT32 partition and NTFS

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2002-10/15508.html

From: Ken G. (Viper007@charter.net)

Date: 10/20/02

From: "Ken G." <Viper007@charter.net>

Date: Sun, 20 Oct 2002 14:55:32 -0400

Hi Linda,

The first mistake that most new users make is to over estimate the situation. If it seems that you are kicking a dead horse, just walk away and go watch TV or have a cup of coffee. Then come back and try it again. On the subject of your machine;

Golden Rule No. 1

If you think you have been compromised, you probably have.

There are a number of ways to deal with this, the easiest would be to wipe your drive clean and reinstall your OS (Operating System).

Personally, I've never been a fan of OEM setups. Do yourself a HUGE favor and purchase a Full version of Windows. Preferably, Windows 2000 or WindowsXP Professional. The reason being that the focal point of those two OSes is SECURITY and stability. At last check, WinXP Pro {Full} was \$299.00. The same for Win2000. While your at it, get {WindowsXP Inside Out} by Ed Bott and Carl Siechert (Barnes & Noble should have it). It is for the power user as well as the newbie.

At the very least, do reinstall your OS and get WindowsXP Inside Out. It will answer a lot of your questions. Including the benefits of FAT32 vs. NTFS partitions.

On the subject of permissions though, you are VERY limited in that respect using WinXP Home and would do well to get the Professional version instead. But do note Linda, that Windows XP is NOT secure right out of the box. It is the user that has to make it that way. Hence the name; Administrator.

Good luck ;)

"Linda J." <lj86004@yahoo.com> wrote in message
news:5ea201c2760d\$636ff810\$3bef2ecf@TKMSFTNGXA10...

> Kinda long, but please help me understand this if you care
> to take the time.
>
> I think my D:\System_Save recovery partition for my Compaq
> has been compromised. At first, I thought maybe SP1
> activated some service, because it turned on everything
> imaginable and maybe it was trying to write to the D:
> partition. I also had a problem with Set Programs and
> Defaults, so I uninstalled SP1. A couple of other 54xx
> series had same problem. But the D:\ drive shrunk some
> more. And kept shrinking. I looked for errors, but didn't
> find any. So I started going through my security events
> one by one, looking up what each and every one meant so I
> could halfway understand what I was reading. It then led
> me to the conclusion that a Server was running. I checked
> file and printer sharing in network properties, and it was
> not installed. But, when I checked Services, saw the
> Server running on automatic so I turned it off. I read
> more info. Looking for suspect files. This time I searched
> all drives. That is when I noticed EVERYBODY (caps) for
> all the files. Eventually found the "net share" command
> using Help and Support. Saw it wouldn't work, so I turned
> the Server services back on, and discovered my D:\drive
> was included! So I turned it off again. I'm new with
> Windows, so forgive me if I ask this, but I've read about
> FAT32 here in the newsgroups, and also that Home Edition
> is rather liberal with what it shares, then can I assume
> that as long as there is a FAT32 partition, it will always
> be vulnerable? Right now, it's available to everybody
> (lower case) and that's how it is. I didn't do anything to
> make it that way. The Server was IIS. I thought Home
> wasn't supposed to have this. I didn't do this. It's part
> of the Compaq files too, even on my QR's. A couple of
> weeks ago, found anonymous log-ons. Saw questions asked by
> other users about it, but no answers. Since Norton
> Internet Security was set to automatic, put it back to
> full reporting again. I was getting a lot of FTP so I
> created rules to block it. The anonymous logons stopped.
> So it was just trying to figure out what all this meant.
> But I think the computer has been compromised and the
> D:\System_Save is trashed, and I question Compaq's wisdom
> with this type of setup.
>
> >-----Original Message-----
> >FAT32 has no security. Period. If you have a FAT32
> >share, then you will have permissions on the share, which
> >people remotely accessing the share will have to pass
> >first.
> >
> >NTFS is what allows actual security rights to be put in
> >place. FAT32 is FAT32, insecure.

> >
> >>-----Original Message-----
> >>*I can't find an answer at Compaq. I want to know if a*
> >>*FAT32 partition on a preinstalled Windows XP Home*
> >*Edition*
> >>*that says it's available to "EVERYBODY" (caps)*
> >>*and/or "everybody" (lower case) is a security risk.*
> >>.
> >>
> >.
> >