

RE: Controlling specific USB devices on Windows XP

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2006-06/msg00042.html>

- *From:* <mcclenbw@xxxxxxxxxxxxx>
 - *Date:* Thu, 15 Jun 2006 15:27:20 -0400
-

See inline...

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

From: George Njoku [<mailto:george@xxxxxxxxxxxxx>]
Sent: Thursday, June 15, 2006 10:30 AM
To: Focus Microsoft
Subject: RE: Controlling specific USB devices on Windows XP

The whole ideology of Controlling USB access for security issues is some what redundant and most companies might deem it unnecessary.

I agree the safest thing to do is to restrict all the USB access to all no privileged users to avoid xfer of data; Similarly as you'll do for CD-R and floppies (afterall these a also external storage devices).

Then, think of internet access; data can be downloaded or uploaded. So to be secure, connection goes though a proxy.

It boils down to 'privilege'; who can access what files and who cannot. Who has administrative/'power users' privileges and who doesn't. Who is allowed access to the net and who isn't.

Not really. Say I work at a bank, and I require the 'privilege' to access to people bank records while performing my job at work. Do I need to be able to take that information home with me? No, but what's stopping me from downloading thousands of records to my thumb drive and taking it home and selling it to whomever will buy the information?

After all, the lower level goal is to prevent "viruses, worms and Trojans get into the corporate network this way, but valuable data can leave the company in huge quantities" right?

RE: Controlling specific USB devices on Windows XP

No completely. As stated above, you need be concerned about data leaving in many cases too.

But the issue of "locking down Windows computers to only allow specific USB devices to attach" is just like saying...

Locking down certain cd-r brands and models
Locking down certain web browsers (IE can access but firefox cannot)

I don't see how this is true. The goal is no USB storage devices can be attached and used. USB input devices are fine (keybaord, mouse, etc.) and USB output device (printer), but nothing they can bring data in on or take data out with. Of course, I guess you could argue you can use a printer to take data out.

That leaves one scenario:

If an administrator leaves his computer unattended without logging out and the Janitor takes a break from mopping to steal information...

*solution

1. Use USB device – Janitors USB his brand is locked
2. Use CD-R – Computer has no CD-R or no blank Disks; Can upload virus
3. Use floppys – File is too large; Can upload virus
4. Use internet – Assuming admin didn't already authenticate, Proxy.
5. Open file and write down content – Not a fast writer.... "hurry admins coming back"

Solutions 3 "File is too large" seems to be based entirely on assumption. Also, why would computer have no CD-R but have a floppy drive. Seems like an unlikely assumption these days. Especially since I would hope those worried about USB storage devices have already address the CD-R and floppy drive issue already.

RE: Controlling specific USB devices on Windows XP

6. Use Admins USB device: If an admin or privileged user is dumb to leave his computer unattended, there is a very high chance that he'll leave his USB device still plugged in the USB port or lying by somewhere.

No we've jumped to petite larceny and "the lazy admin" security issue together.

Gentlemen, this USB lock down for certain device is a nice idea, but just not necessary

Except for the worker that requires access at work, but shouldn't be able to take it home issue. Sure with some type of rights management system, perhaps it wouldn't be necessary, but then again if we gave them no way to copy data somewhere the rights management system could be deemed unnecessary too. It's just another solution. If it's the solution you choose, then it IS necessary.

George Njoku
Turner Engineering, Inc.
973.263.1000
george@xxxxxxxxxxxxx

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

From: Trevor [<mailto:trevor@xxxxxxxxxxxxx>]
Sent: Wednesday, June 14, 2006 1:52 PM
To: focus-ms@xxxxxxxxxxxxxxxxxxx; security-basics@xxxxxxxxxxxxxxxxxxxxx
Subject: RE: Controlling specific USB devices on Windows XP

Yes, Vista contains quite a few USB control options. Many specifically relate to USB Mass Storage devices, so if you don't want to lock down the mice but instead target USB key chains, etc. it will be possible.

We currently use the XP SP2 ability to lock down writing to USB devices.

While that is only 50% of the equation we really need, it is effective.

Since there are business justifications for being able to use these devices in a write mode, the GPO is separate from all others. We have a group that has Deny access to that GPO.

We just add computers to the GPO and manually reverse the registry entry controlling the USB device to allow users to

RE: Controlling specific USB devices on Windows XP

write to them. It works...

-Trevor

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

From: Steven Hay [mailto:shay@xxxxxxxxxxxxxxxxxxxxxx]
Sent: Wednesday, June 14, 2006 7:05 AM
To: security-basics@xxxxxxxxxxxxxxxxxxxxxx; focus-ms@xxxxxxxxxxxxxxxxxxxxxx
Subject: RE: Controlling specific USB devices on Windows XP

Just curious, does anyone know if Vista is going to have any intelligence for USB control built in either by registry key or additional GPO?

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

From: Ken S [mailto:ken.securitylist@xxxxxxxxxx]
Sent: June 13, 2006 3:06 PM
To: security-basics@xxxxxxxxxxxxxxxxxxxxxx; focus-ms@xxxxxxxxxxxxxxxxxxxxxx
Subject: Controlling specific USB devices on Windows XP

I am investigating the possibility of locking down Windows computers to only allow specific USB devices to attach. I'm considering the mtrust product from www.m-systems.com, which the marketing materials say can force users to only use their particular USB storage devices (or those that they OEM to others, like Kingston, Verbatim, etc.).

Does anyone have experience with this package? If so, what are the pros and cons?

Also, are there other solutions out there that can ensure only specific USB storage devices are allowed on a system?

Is there anything specific for biometric USB storage?

Any comments on the effectiveness of such software?

Thanks,

Ken S

RE: Controlling specific USB devices on Windows XP

