

Forum:[Hack Forums](#)

Thread: [How do I determine if a USB contains a virus?](#)

louzhi - February 6, 2018, 5:56 pm

1. How would I be able to tell if there is a virus on my USB?
2. Would encrypting my USB provide added protection against viruses while connected to an infected PC?
3. Would reformatting my USB remove any viruses which were once on the USB?

my main concern is how to keep my USB from infecting a whole bunch of devices I own...

thanks for the help!!!

Hashflare - February 6, 2018, 5:57 pm

What makes you think your USB has a virus?

louzhi - February 6, 2018, 6:04 pm

(Feb 6, 2018 06:57 PM)Hashflare Wrote: [\[CITE\]](#) What makes you think your USB has a virus? Nothing, I'm just speaking hypothetically. I'd like to know how to prevent such a thing from happening.

Armada - February 6, 2018, 6:48 pm

(Feb 6, 2018 06:56 PM)louzhi Wrote: [\[CITE\]](#) 1. How would I be able to tell if there is a virus on my USB?

2. Would encrypting my USB provide added protection against viruses while connected to an infected PC?
3. Would reformatting my USB remove any viruses which were once on the USB?

my main concern is how to keep my USB from infecting a whole bunch of devices I own...

thanks for the help!!!

1(a) - Ensure your system has Autorun for USB disabled (Most all recent versions of windows do by default)

(b) - Install/Update your Anti virus ensure it is a registered copy, and fully functional and activated, no freeware crap.

© - Plugin the USB device and do a full scan of the USB drive.

2. No - you still have to decrypt the files, and secondly it likely could still be placed in the USBs free space.

3. Yes, do a full format, not a quick format however.

?

louzhi - February 6, 2018, 7:01 pm

(Feb 6, 2018 07:48 PM)Armada Wrote: [CITE](#) 1(a) - Ensure your system has Autorun for USB disabled (Most all recent versions of windows do by default)

(b) - Install/Update your Anti virus ensure it is a registered copy, and fully functional and activated, no freeware crap.

© - Plugin the USB device and do a full scan of the USB drive.

2. No - you still have to decrypt the files, and secondly it likely could still be placed in the USBs free space.

3. Yes, do a full format, not a quick format however.

?

thanks! I appreciate the help! ?

also,

how would you scan a usb on Linux? would it even be necessary?

SysAdmin - February 7, 2018, 1:39 am

(Feb 6, 2018 07:48 PM)Armada Wrote: [CITE](#) 1(a) - Ensure your system has Autorun for USB disabled (Most all recent versions of windows do by default)

(b) - Install/Update your Anti virus ensure it is a registered copy, and fully functional and activated, no freeware crap.

© - Plugin the USB device and do a full scan of the USB drive.

2. No - you still have to decrypt the files, and secondly it likely could still be placed in the USBs free space.

3. Yes, do a full format, not a quick format however.

?

Adding onto Armada's post, the Anti-Virus part is a bit.. Difficult to go by. With the amount of crypters and obfuscation around that even skids can use, bypassing an Anti-Virus scan isn't as hard as it seems.

Mad76e - February 7, 2018, 3:49 am

(Feb 6, 2018 06:56 PM)louzhi Wrote: [CITE](#) 1. How would I be able to tell if there is a virus on my USB?

2. Would encrypting my USB provide added protection against viruses while connected to an infected PC?

3. Would reformatting my USB remove any viruses which were once on the USB?

my main concern is how to keep my USB from infecting a whole bunch of devices I own...

thanks for the help!!!

1. Nerver use any unidentified USB stick in your computer

2. Well it depends on the virus actually. In worst case scenario you will end up with corrupted files, or infected files when youre trying to decrypt EM

3. Yeah

CyberStrike - February 7, 2018, 7:02 am

Well OP why wouldn't you use an AV in linux to scan your USB? Don't you want to know what you

may have spread about your computers? At least now you can have some IOC's (indicators of compromise) so you can fix it. ClamAV and yes you can use a front end ClamTK to scan the device.

Something further you may want to dedicate an older machine to scan USB devices before you plug in to your other computers. Also if you already infected multiple USB keys you may want to start placing logging/tools on your Windows computers.

https://www.nirsoft.net/utils/usb_log_view.html

<https://www.pcworld.com/article/2940859/windows/how-to-lock-and-unlock-your-usb-ports.html>

<https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/usbview>

I tend to believe that I want to know what I am dealing with before nuking it, that way I can quickly deal with multiple machines that maybe infected with the same crap. And formatting should get rid of it,

louzhi - February 7, 2018, 10:53 am

(Feb 7, 2018 08:02 AM)sirru5h Wrote: [\[CITE\]](#) Well OP why wouldn't you use an AV in linux to scan your USB? Don't you want to know what you may have spread about your computers? At least now you can have some IOC's (indicators of compromise) so you can fix it. ClamAV and yes you can use a front end ClamTK to scan the device.

Something further you may want to dedicate an older machine to scan USB devices before you plug in to your other computers. Also if you already infected multiple USB keys you may want to start placing logging/tools on your Windows computers.

I tend to believe that I want to know what I am dealing with before nuking it, that way I can quickly deal with multiple machines that maybe infected with the same crap. And formatting should get rid of it,

You're right, I don't know why I didn't think of using Linux based anti virus...also the "use an old pc to test USB's" is a good idea that I'm definitely going to do.

CyberStrike - February 7, 2018, 11:27 am

Cool hope it helps here are a couple of resources:

<https://community.spiceworks.com/topic/603983-standalone-linux-box-to-scan-flash-drives-for-malware>

[https://en.wikipedia.org/wiki/Sheep_dip_\(computing\)](https://en.wikipedia.org/wiki/Sheep_dip_(computing))

Most important thing make sure you keep clamav updated I am sure that upon detection of a USB being plugged in you can probably do it with just a shell script where it queries lsusb even df if it automounts the USB and if anything "new" is plugged in then it executes an update of clamav and then scans the drive. Also allow it to scan large files clamav has an option for ignoring over 20 MB files.

If you really are not sure on a file you can have linux as the base OS and run a Windows VM have processhacker/wireshark/procmon and see what it does see where it writes to files being downloaded..etc If you find odd behaviour and want you can also use vboxmanage to dump the RAM then use volatility to see all that happened there as well.

<https://askubuntu.com/questions/166420/how-to-detect-an-usb-device>