Science Translations
Established 1990
PC410.COM™
PC Updater News

Trojan Horses on Flash Drives

The first virus I ever cleaned up was the Cookie virus, back in 1991. Computers still had 5.25" floppy disk drives. The Cookie virus ‘lived’ on a diskette, and if you booted the computer from an infected diskette, it would ask for a cookie. Typing ‘cookie’ would shut it up. And it copied itself to every other diskette it could reach. Cleanup was just removing two files, from every diskette you owned, one at a time. It was annoying, but not destructive like modern malware.

Well, removable device malware is back. ArsTechnica has a writeup on it.

USB worm unleashed by Russian state hackers spreads worldwide
https://arstechnica.com/security/2023/11/normally-targeting-ukraine-russian-state-hackers-spread-usb-worm-worldwide/

Short version: ‘LitterDrifter’ is a trojan horse on a USB drive. It infects computers and spreads itself to other USB drives, and phones home to a command and control server (to update payloads), and it spreads quickly. It’s mostly being seen in Ukraine right now, but has also arrived in the USA. The past history of such drives is that they’re scattered near takeover-target businesses and agencies, left in lunch areas or parking lots, where they’re picked up and infect any unprotected computer they’re plugged into.

How to avoid it:

- Don’t take storage devices from strangers.
- Lost USB flash drive left to be found? Nope, that’s standard business infection procedure.
- Don’t buy storage devices from any ‘marketplace’ vendor, especially those who ship from overseas.
- Re-format all new flash drives before use, from an offline computer with all autoplay settings turned OFF.
- If you receive files from outside your office on USB devices, turn off all autoplay options in Windows, and have your antivirus software manually scan that drive.

To turn off autoplay, search Settings for Autoplay. Slide the setting left to Off. Or click Start (logo), Settings (gear), Bluetooth & Devices, Autoplay, and choose Off.

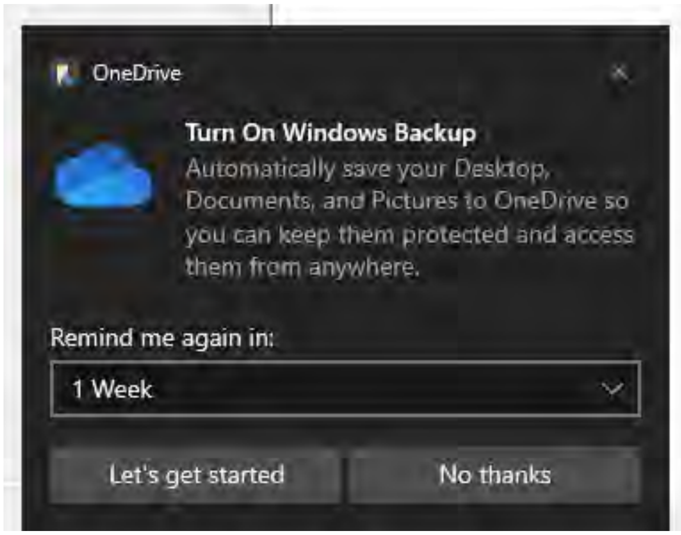
Fake Drives Again

Last year’s warnings about 16Tb SSD drives that only contain 32Mb of slow flash storage, plus a trick BIOS that lies about capacity, have evolved. Now, they’re less obvious, selling 1Tb flash drives for $19. The 1Tb drives, when real, sell for $85 to $130 right now. Again, do not buy storage of any kind from marketplace (third-party) vendors on Walmart.com or Amazon or any other online site with non-company sellers.

Too late? Gibson Research has a free test program to identify this fraudulent junk. ValiDrive will check new drives for both read/write errors and capacity fraud. Get it from GRC.com:
https://www.grc.com/validrive.htm

Buying a new flash drive? Stick with name brands, shipped domestically directly by the seller (not marketplace and not eBay), and check the return policy before buying. These brands are reliable if genuine: PNY, Kingston, and SanDisk. At this point, ALL flash drives you buy should use USB 3.0 or 3.1; stop buying slow USB 2.0 drives that have been sitting in a warehouse for a decade.

Just What is the New Windows Backup?



Windows is promoting a new 'Windows Backup' app now, including popping up reminders in the bottom corner of your screens to set it up and use it. It’s in Windows 11, feature version 23H2 now-that's the 2023 second-half version. It will show up in Windows 10 soon. It may have some limited use, but be aware that this is not a computer backup. It backs up documents and pictures and sends them to Microsoft’s OneDrive. So that requires signing into a Microsoft account. If you have not bought the monthly Office subscription (called Microsoft 365, as of 2023), then you have 5 Gb of free cloud storage on OneDrive. If you are using Microsoft 365, you probably have 1 Tb (1000 Gb) of storage.

But there’s a big however coming: OneDrive is not backup. It’s a file sharing web site, suitable for synchronizing data files between your computers, as long as the files are NOT subject to regulatory rules for encryption in storage, like HIPAA (medical records), PCI (credit card data), or Sarbanes-Oxley (publicly-traded companies). In short, records that must be stored securely must be stored in a way that is tamper-proof, password protected, read-only, and searchable. The requirements vary with the particular law–this is a starting point; if these regulations apply to you, work with an expert.

So what’s missing, and why is OneDrive not backup? Backups are collections of files by date, stored so that tampering would be obvious, and preferably encrypted and immutable (unchangable). Multiple file sets allow going back in time to get an older version of a current file: The number one data backup emergency call that I receive is this one: “We overwrote our master spreadsheet list of ___, and need one from last week.” Or month. A proper backup has multiple copies, by date. Sharing services like OneDrive, Google Drive, and DropBox don’t do that.

The multiple copies by date are not just for grabbing files after an office mistake. Ransomware encrypts all files on a PC, server, or network. And backup software will blindly back those encrypted files up. So going back in time in a backup is frequently needed, to get good files, from before a mistake or ransomware or hardware file corruption happened.

The new Windows Backup doesn't do any of that, and it doesn't backup to a drive you could lock up, either. If you want to use it as a convenience copy of your documents so that you can read them from a second device, sure. Just check that the files you will back up, in the Documents, Photos, and Music folders, are smaller than your OneDrive file space.

So what is a proper first backup?

If you will only have one kind of backup of a Windows computer, it should be a system backup. The software that creates it makes a single file out of everything on your C: drive, plus the Windows boot-up files, and stores that on an external drive. With that file, I can restore everything, software and all, after a drive failure or ransomware. For home users, a system backup may be all you need, done manually once a month, or anytime you've just entered a lot of data. Like right after doing your tax return. For business users, add timed automatic backups and monitor that they're actually happening.

Second backup?

The second backup should be a cloud backup. Choose a service provider that makes uploaded backups immutable (unchanging and undeleteable), allows encryption BEFORE uploading, and keeps multiple copies of all files for a known amount of time. A year has become the standard now. I recommend BackBlaze for this, and you can buy it directly from them, or call me; I add monitoring and setup help.
https://www.backblaze.com/#af99we

And a Third backup?

For businesses, add a nightly or real-time backup of data ONLY, not system backups, to a local network-attached drive. Nightly backups protect files created since the last system backup. Local backups have a much quicker restore time than cloud backups, while having the cloud backup provides the off-site and disconnected protection needed against fire, ransomware, lightning, and employee issues.

Call for help choosing the scale, software, and monitoring options for your backups.

For computer help, call 410-871-2877

Missed a newsletter? Back Issues