nLightened Thoughts

July 2018

William Blinn Communications
Worthington, Ohio 43085
www.blinn.com • 718.577.1054

Backup Means Never Having to Say @&#$@%!!!

CRIMINALS THOUGHT TO BE ASSOCIATED WITH THE RUSSIAN GOVERNMENT HAVE DEPLOYED MALWARE THAT TAKES OVER ROUTERS COMMONLY USED IN HOMES AND SMALL OFFICES. "VPNFILTER" EXPOSES ALL DATA SENT TO OR FROM YOUR COMPUTER. AND IT GETS WORSE.

You've probably heard about this exploit and updated the firmware in your router. If not, that's something you should do right now. Log on to the router and work through the menus until you find an option to check for a firmware update. This varies slightly from one router to another, so contact the vendor who sold you the router if you get stuck.

Once you've updated the router's firmware, you're safe, right? Sorry, but no.

VPNFilter Is Just One Trick

IT'S THE *THREAT OF THE DAY*, BUT OTHER THREATS TARGET THE OPERATING SYSTEM, APPLICATIONS YOU RUN, AND EMAIL.

So many people are using so many tricks to gain access to your computer that you might think the situation is hopeless and – if you think that – you're not far from the truth. Threats include hardware flaws, software flaws, operating system flaws, and user errors.

Hardware flaws (router vulnerabilities), software flaws (attacks that use Adobe Flash), operating system flaws (Microsoft patched 11 critical faults in June) and user errors (phishing emails). Email is the primary means that crooks use to plant malware used to steal credentials, encrypt files and hold them for ransom, or exfiltrate important information.

No matter how smart, paranoid, or suspicious you are, somebody who sincerely wants access to your computer will find a way to get it. There's only one safeguard: Backup.

TO UPDATE THE ROUTER'S BIOS, (1) FIND THE ADVANCED SETTINGS, (2) SELECT THE UPDATE OPTION, AND (3) CHECK TO SEE IF AN UPDATE IS AVAILABLE. IF YOUR ROUTER HAS AN (4) AUTOMATIC UPDATE FUNCTION, ENABLE IT.

If a crook stages an attack on your system that encrypts files or deletes them, recovery can be easy if you have a solid, verified backup.

"Easy" is a relative term. If you must spend hours or days to recover data that has been encrypted or destroyed, you may not think that "easy" is the right term. But if the only other option is losing the data, the "easy" takes on a more nuanced meaning.

Consider an author who loses every novel or article being worked on. Or a videographer whose latest project disappears before it's complete. And regardless of your business, would you be able to recover if your accounts receivable files were no longer available?

The Gartner Group says that 43% of companies were immediately out of business following a major loss of computer records. Another 51% permanently closed within 2 years. The survival rate: 6%. The odds are not in your favor.

Because of the VPNFilter exploit, I updated my Wi-Fi router and then it seemed like a good time to review the backup procedures, which is something I do every year because the only thing worse than no backup is depending on a backup system that doesn't work.

Backup Is Not Just A Copy

SOME PEOPLE CREATE A DIRECTORY CALLED "BACKUP" ON THE HARD DRIVE AND COPY IMPORTANT FILES THERE, THINKING THAT THEY HAVE CREATED A BACKUP.

What they don't realize is that a simple disk failure would render both the original and the duplicate files unusable. So would any attack intended to encrypt or damage files.

Minimally data should be backed up to a drive that's stored off-site or to a cloud-based backup system such as CrashPlan.

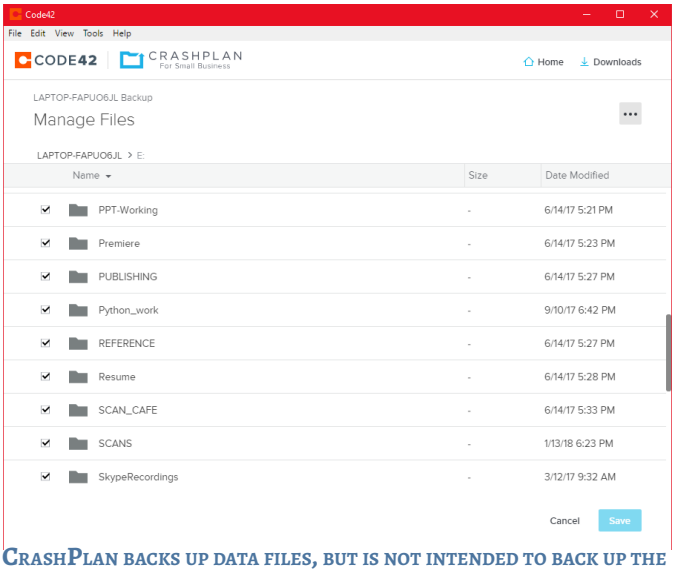
Even with a backup service such as CrashPlan, you could still lose files. Although hightly unlikely, the potential exists.

Some high-priced backup systems add another precaution by backing up files on their system to a separate off-site location. This extra step slightly reduces the chances of data loss, but increases the cost a lot.

To lose data with a cloud-based backup system, two failures would need to occur: The disk drive on your computer would have to fail and the off-site system's disk drive with your data would also have to fail. That's possible, but unlikely.

Another potential threat exists. An automatic backup system could back up files that have been damaged or encrypted. In that case,

nLightened Thoughts (ISSN 1543-1533) is for clients and friends of William Blinn Communications, Worthington, Ohio. Phone 614.785.9359 (Columbus) and 718.577.1054 (NYC). On the Web at www.blinn.com.



CrashPlan backs up data files, but is not intended to back up the operating system. For that task, you need an application such as Acronis TrueImage and an external hard drive.

the backup would be unable to restore good files. Some on-line backup systems include file versioning so that older versions of files can be recovered.

Versioning offers two advantages: The ability to recover earlier good versions of files that have been damaged by malware and also the ability to recover previous versions of files that have been corrupted by user error.

User error? Maybe you opened a Word document, planning to use only some of the text to create a new version of the file. After making changes, you saved the new file using the old file name. Oops! Versioning would allow you to recover the earlier file.

GoodSync is the most reliable system I've found for copying data files to local USB drives or to a network drive.

More Is Better

I use a multi-step backup process that combines on-line backup with multiple local file copies.

The boot drive is imaged using Acronis True Image on Wednesday and Sunday to different disk drives. It is not backed up to an off-site drive and this is a defect, but one I'm willing to live with.

If the boot drive and both backups are lost, I would need to obtain a new computer and reinstall all the applications.

Essential files are backed up continuously to CrashPlan. Essential files are also backed up daily to a local network attached storage (NAS) drive and all data drives are backed up weekly to local USB drives. Files on the NAS drive are never more than 1 day old. Files on the local USB drives are never more than 1 week old. Files on the CrashPlan server are rarely more than 1 hour old. Files on the NAS and USB drives can be recovered faster, but could also be destroyed by a fire or other event that destroys the primary computer.

To lose a file, several things would have to happen simultaneously:

- Data disk drives in a separate enclosure would need to be damaged or destroyed.
- External USB backup drives would need to be damaged or destroyed.
- The NAS drive would need to be damaged or destroyed.
- The cloud-based CrashPlan server would need to be damaged or destroyed.

A fire or earthquake could destroy the data drives, the external USB drives, and the NAS drive. If that happened and the cloud-based CrashPlan server was also destroyed, I would lose a lot of data; but if something like that happened, there would be a lot more to be concerned about than lost data files.

The backup system I use is not perfect. It might not be the right plan for you. Regardless, now is a good time to review how your files are safeguarded and how you might improve that system. Ω

Backup Software Sources

Here are some of the backup applications described in this article.

CrashPlan: Continuous backup of data files, but not the operating system.
WWW.CRASHPLAN.COM

TrueImage: My choice for imaging the boot drive. Although Acronis offers on-line storage, I feel that CrashPlan is better.
WWW.ACRONIS.COM

GoodSync: An excellent choice for scheduled backup to various media types.
WWW.GOODSYNC.COM

Selecting, installing, and maintaing backup software is a chore, but not doing so will eventually become an even larger chore. Ω