THE COMPUTER CORNER

No. 233: Ransomware

Stan Kaplan, WB9RQR 715 N. Dries Street Saukville, WI 53080-1664
(262) 268-1949 wb9rqr@att.net

This nasty, relatively new type of malware (starting around 2012) blocks your access to your data on your computer until you pay a ransom. Or it threatens to publish your inaccessible data or delete it, until a ransom is paid. It often encrypts your files in a way that makes them inaccessible to you or anyone without the encryption key. It claims that if you make payment of the ransom (often in Bitcoin, which is difficult to trace) it will send you a key that will unencrypt the files. However, don't believe it. Often, once the bad guys have their money, the key is not even sent. Or if it is sent, the key does not work properly, and the victim is still out of luck. Therefore, if you get hit with ransomware, the best procedure is not to pay the ransom.

How do you get it? Often, via a Trojan, disguised as a harmless file that you are tricked into downloading. Or, the infection may be hidden in an email attachment that you are enticed into opening. Or, it may just automatically travel from one computer to another on a network. The message: 1. Don't download stuff unless you are reasonably sure it is safe (Majorgeeks.com is a safe site for software, as I have told you before). 2. Don't open email from persons you do not know (that means do not even read it!). For sure, don't open any attachments from folks you don't know. 3. Stay off networks as much as you can (more on this later).

So, how can this bad boy be fought? It is a little like a bottle of poison pills. If you don't swallow any, you will be safe. If you swallow even one, you will die. Safety lies in not taking a pill. Safety lies in not getting infected. In other words, safety lies in prevention. Don't take any tablets. Don't get infected. Also, you can take some steps so that if you do get infected, you can reverse the effects of the infection. The latter ploy lies in being able to replace the data from another, non-infected source. Another computer, or CDs/DVDs that hold backups of your data. Let me tell you how we do it and you should be able to prepare your own ploy.

We have six, network-capable computers at our QTH. Five of them are networked 24/7. These five include my main machine, my laptop, Nancy's (KC9FZK) machine, my Winlink machine and a general ham computer. The first three are in our second-floor office, the latter two are in the basement. In each case, the stuff that we create (letters, photos, spreadsheets, etc., are kept on the E: drive of each machine (C: is for Windows or Linux, D: is for programs). E: contains the only truly irreplaceable data. E: is identical on all five machines. Whenever Nancy or I create something new (such as this article) it is copied to the other machines within a day, using a backup program. About every three months, we burn a DVD E: backup from one or another machine (it doesn't make any difference which machine is used for burning since the data on each E: drive is essentially identical to all the others).

So, we appear to be covered. If we ever find we are infected, we can simply replace the files from a non-infected DVD, after finding and killing the infection in all the computers. But, I have taken one more step recently. That's where the sixth machine comes in.

About once a week (more often if we are busy creating), we turn on the sixth machine. It, too, has an E: drive with our irreplaceable files on it. We update its E: drive from one of the others. Then we turn it off. Off means it cannot become infected. But it is a source of the last week's work.

Is that sixth machine a big expense? Nah. You've had many opportunities to buy a used laptop at the ORC auction for about $25 in the last year. Really good ones, too, since I rebuilt them! Perfect for such backups. Or, you can purchase a USB hard drive to make such backups. That will work, too. At the very least, periodically burn those DVD backups. You will love the added security, and you will like the archival nature of those DVDs. We have gone back to them at least twice a year to look up something that no longer existed on our E: drive, such as a copy of an old issue of the ORC Newsletter. We even move a backup DVD, about once every two years, to our safe deposit box! How's that for security? Happy computing!