

THE COMPUTER CORNER

No. 227: Junkware Removal Tool **and** Cybereason RansomFree

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

At the ORC breakfast the other Saturday, Ed Rate again railed against unwanted toolbars and browser helper objects, as well as popup ads. Well, I came across a tiny program, now owned by Malwarebytes, that will do the job in a short time. It is a FREE, portable app (it does not need installing) that takes very little memory and bails out when it is done. Thus, you run it, it does its job and it is finished. I run it directly on my desktop, which works fine. JRT.exe will remove little unobvious bits of code that breed popup ads. It also removes PUPs (Potentially Unwanted Programs) and any leftover PUP fragments. And it takes very little time – you can watch it do its thing in a minute or two or three (on a reasonably clean machine).

When run, JRT.exe requests a restore point (but don't worry if creation of a restore point fails ... you can continue to run JRT anyway). Then it begins to scan:

- | | |
|-------------------------------|-----------------|
| 1. Processes. | 5. File System. |
| 2. Startup -Logon. | 6. Browsers. |
| 3. Startup – scheduled Tasks. | 7. Shortcuts. |
| 4. Services. | |

...and then it prepares a short text file containing a report.

There are a couple of “gotcha”s to be aware of. When run, it opens a Command Prompt (DOS) window, and works within that. However, you can follow the progress just fine on your screen. Also, there are no options when it is run – it does its thing as it wishes and then it quits when the job is done. It will sometimes close running applications, so be sure to save all your work before you start it and have available any programs that you might want to start back up after it has finished in case they are closed.

Probably the best thing to do is to go to <http://www.majorgeeks.com> where you can get the program – JRT.exe) Best also to run the short video there by Tim which explains what to expect. Now, Tim says that JRT is mainly for techs, but I maintain it will do a great job for anyone at any skill level who wishes to touch-up a system. I ran it on four of my computers with no major problems. One failed to create a restore point but I proceeded anyway. Oddly enough, only wife Nancy's (KC9FZK) computer had nothing for JRT to clean up. Fancy that!

NOW I HAVE A FLASH. RANSOMWARE is a particularly nasty type of malware that gets into your machine one way or another and begins to encrypt your personal files, then delete the non-encrypted versions. It presents you with a message like this:

I want to play a game with you. Let me explain the rules. Your personal files are being deleted. Your photos, videos, documents, etc. ... But don't worry! It will only happen if you don't comply. However, I've already encrypted your personal files, so you cannot access them.

Every hour I select some of them to delete permanently, therefore I won't be able to access them, either.

Are you familiar with the concept of exponential growth? Let me help you out. It starts out slowly then increases rapidly. During the first 24 hours, you will only lose a few files, the second day a few hundred, the third day a few thousand, and so on.

If you turn off your computer or try to close me, when I start next time you will get 1000 files deleted as a punishment.

Yes, you will want me to start next time, since I am the only one that is capable to decrypt your personal data for you.

Now, let's start and enjoy our little game together!

After that, arrangements are typically made for you to send \$150 or more in bitcoin funds for the malware authors to free your files. Nasty. Costly. Impossible for the average user to bypass. Traditional antivirus software cannot stop it, so don't be complacent and think you are protected, because you are not. But there is a no-cost solution for the average home user.

A new company, Cybereason, was founded from a corps of experts who had experience in a military cybersecurity branch of the IDF (Israel Defense Force). Their new venture is aimed at protecting companies from attacks in real time, for a fee. But, they are making a free program available for non-commercial computer users – to prevent hijacking by ransomware. When installed, the program will alert you immediately of any activity that smacks of ransomware, on your machine or on a network drive, and give you the ability to stop that attack with no consequences.

This is an easy decision, folks. Go to <http://www.majorgeeks.com>, look at the FILES pane on the left, and click Antimalware. In the list that comes up, select Ransomware Removal and look at Cybereason RansomFree. Read about it and optimally run the video supplied. When you are convinced, download the program, install it and forget it. It will not bother you unless you are attacked or a new version is out. Oh yes, it will stash a bit of code on your desktop and elsewhere, clearly labeled:

!Don't delete me! I'm helping Cybereason hunt for ransomware!

That is your only cost, so install it and forget it. How is that for an answer to a problem you may not have known existed until it was too late? Happy Computing!