1-CLONING AS A PROACTIVE DEFENSE AGAINST MALWARE

by Francis Chao
fchao2@yahoo.com

TuCSon COMPUTER SOCIETY

apcug

Web location for this presentation:

http://aztcs.apcug.org

Click on

"Meeting Notes"

SUMMARY

The most time-saving defense against malware is to clone and set aside a separate SSD or hard drive so that you can swap to it if your "Windows.." computer gets infected with malware

PROACTIVE DEFENSE AGAINST MALWARE INFECTIONS

- Procure an SSD that is similar or larger than the existing SSD inside your "Windows.." computer.
- Use a third-party software app such as "Clonezilla" (free) or "Macrium Reflect Home" (not free) to clone the existing SSD

PROACTIVE DEFENSE AGAINST MALWARE INFECTIONS (continued)

- Test the cloned SSD and store it in a static-proof bag and/or container
- Swap to the cloned SSD if your computer get infected with malware

PROACTIVE DEFENSE AGAINST MALWARE INFECTIONS (continued)

- Instructions for using Clonezilla to clone a SSD or a hard disk are available at:
- https://www.makeuseof.com/tag/how-to-use-clonezilla/
- https://clonezilla.org/show-live-doc-content.php?topic=clonezilla-live/doc/03_Disk_to_disk_clone
- https://www.wikihow.com/Use-Clonezilla

PROACTIVE DEFENSE AGAINST MALWARE INFECTIONS (continued)

- Instructions for using "Macrium Reflect 8 Home" to clone a SSD or a hard disk are available at:
- https://www.macrium.com/blog/cloning-a-disk-with-macrium-reflect-v8
- https://jameslcurtis.medium.com/how-to-clone-your-hard-drive-to-a-new-ssd-using-macrium-reflect-e239759a8292

PROACTIVE DEFENSE AGAINST MALWARE INFECTIONS (continued)

- Before booting up the computer with the bootable hard drive or bootable SSD, make sure that the source SSD (the one that you wish to clone) is attached to the computer.

PROACTIVE DEFENSE AGAINST MALWARE INFECTIONS (continued)

- If the source SSD or hard drive that you wish to clone has a bootable copy of Windows.. on it, you will find that it is attached to your computer by means of SATA or M.2
- This is because, unlike Linux distributions or macOS distributions, an activated copy Windows.. 10 and 11 cannot reside on a USB-attached SSD or hard drive.

PROACTIVE DEFENSE AGAINST MALWARE INFECTIONS (continued)

- Attach the target SSD or target hard drive (the blank one) to the computer BY MEANS OF A USB EXTERNAL ADAPTER OR A USB EXTERNAL ENCLOSURE after the Windows.. computer is powered on

PROACTIVE DEFENSE AGAINST MALWARE INFECTIONS (continued)

- Use the RIGHT mouse button to click on the Start button and select "Disk Management" to make sure that the USB-attached target SSD or target hard drive is successfully connected to the Windows.. computer

PROACTIVE DEFENSE AGAINST MALWARE INFECTIONS (continued)

- Start up "Clonezilla" or "Macrium" and use it to clone that source SSD or hard drive to the target SSD or hard drive

PROACTIVE DEFENSE AGAINST MALWARE INFECTIONS (continued)

- Close out of the "Clonezilla" or "Macrium.." app
- Power down the computer
- With the Windows.. computer totally powered off, remove the source SSD from the Windows.. computer and set it temporarily aside.

PROACTIVE DEFENSE AGAINST MALWARE INFECTIONS (continued)

- Attach the target SSD to the "Windows.." computer via M.2 or SATA
- Power up the Windows.. computer

PROACTIVE DEFENSE AGAINST MALWARE INFECTIONS (continued)

- Use the RIGHT mouse button to click on the Start button of "Windows..
- Start up an administrative Powershell window or an administrative Command Prompt window.
- Run sfc /scannow
- Run sfc /scannow
  again multiple times until it states that no problems are detected

PROACTIVE DEFENSE AGAINST MALWARE INFECTIONS (continued)

- Power down the Windows.. computer
- Remove and store the target SSD in a static-proof container
- Label the container with the year-date-month
- Re-attach the original source SSD to the computer
- Power up the Windows.. computer