1-CLONING AS A PROACTIVE DEFENSE AGAINST MALWARE

by Francis Chao
fchao2@yahoo.com

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

- Obtain an SSD that is similar or larger than the existing SSD inside your "Windows.." computer.
- Obtain an USB enclosure for this new SSD
- Insert the new SSD into the enclosure
- Attach the enclosure to a USB port in the computer.

PROACTIVE DEFENSE AGAINST MALWARE INFECTIONS

- Use a third-party software app such as "Rescuezilla" (free), "Clonezilla" (free) or "Macrium Reflect Home" (not free) to clone the existing "source" SSD

PROACTIVE DEFENSE AGAINST MALWARE INFECTIONS (continued)

- Power down the computer.
- Disconnect the original bootable "source" SSD from the computer.
- Attach the cloned "target" SSD to the computer
- Boot up the computer with the cloned SSD

PROACTIVE DEFENSE AGAINST MALWARE INFECTIONS (continued)

- Power down the computer.
- Disconnect the enclosure that contains the cloned "target" SSD, and label it and the and store it somewhere.
- Re-attached the original "source" SSD to the computer
- Power up the computer