REMOVING MALWARE FROM YOUR "WINDOWS.." COMPUTER

by Francis Chao
fchao2@yahoo.com

Web location for this presentation:

http://aztcs.org

Click on

“Meeting Notes”

SUMMARY

To remove malware from a "Windows.." computer, start off by configuring the "Windows.." operating system to make sure that malware is not hidden from view. Then run various "scans" with an antivirus program. Finally, you can run scans with various free "rescue disks".

TOPICS

- Making sure that malware is not hidden from view
- A "recipe" for removing malware involves scanning in regular and then "safe mode" with both "SuperAntiSpyware" and "ComboFix"

TOPICS (continued)

- Configuring your "Windows.." computer so that bootable CDs/DVDs/USB flash drives can boot it up
- Using free "rescue disks" to detect and remove malware

MAKING SURE THAT MALWARE IS NOT HIDDEN FROM VIEW

- Malware often hides from view as hidden files and folders so make sure that you can see hidden files and folders by following the procedure at http://aztcs.org/meeting_notes/winhardsig/win/win-easier.pdf

A STANDARDIZED PROCEDURE FOR REMOVING MALWARE

- Our how-to document on a **Procedure for Cleaning a Virus/Malware-Infected Computer** is located at http://aztcs.org/meeting_notes/winhardsig/malwarecleanup/malwarecleanup.htm

A STANDARDIZED PROCEDURE FOR REMOVING MALWARE (continued)

- This procedure is based on a presentation made by Harry Elver of Tucson, Arizona on March 18, 2011

A STANDARDIZED PROCEDURE FOR REMOVING MALWARE (continued)

- This procedure is very similar to the advice in a article in the November 15, 2011 issue of **"PC World"** magazine entitled "**How to Remove Malware From Your Windows PC".**
  See http://www.pcworld.com/article/243818/how_to_remove_malware_from_your_windows_pc.html

A STANDARDIZED PROCEDURE FOR REMOVING MALWARE (continued)

- We used the standardized procedure to remove "FBI PC Lock Ransomware"
  See http://aztcs.org/meeting_notes/winhardsig/malwarecleanup/2012-10-03-FBI-ransomware.pdf

A STANDARDIZED PROCEDURE FOR REMOVING MALWARE (continued)

- We used the standardized procedure to remove a Trojan called "Win32/FakeSysdef". See http://aztcs.org/meeting_notes/winhardsig/malwarecleanup/2011-12-03-example.pdf

A STANDARDIZED PROCEDURE FOR REMOVING MALWARE (continued)

- We used the standardized procedure to remove a Trojan called "Win32/WinMaximizer". See http://aztcs.org/meeting_notes/winhardsig/malwarecleanup/2012-02-04-Win32-WinMaximer.pdf

USING FREE RESCUE DISKS TO DETECT AND REMOVE MALWARE

- To use various free rescue CDs/DVDs/USB flash drives, you have to configure the BIOS or UEFI of your "Windows.." computer so that it will boot up from one of these devices.
  See http://aztcs.org/meeting_notes/winhardsig/BIOStoUEFI/BIOStoUEFI.pdf

USING FREE RESCUE DISKS TO DETECT AND REMOVE MALWARE (continued)

- If you have a "Windows XP", or a "Windows Vista", or a "Windows 7" computer,
  ImgBurn is a great free software application for burning and copying DVDs and CDs.
  It can also create *.iso image files of actual CDs, DVDs, and any files/folders on a hard drive.

USING FREE RESCUE DISKS TO DETECT AND REMOVE MALWARE (continued)

- You can get ImgBurn at http://www.imgburn.com/

USING FREE RESCUE DISKS TO DETECT AND REMOVE MALWARE (continued)

- If you have a "Windows 8" or a "Windows 8.1" or a "Windows 10" computer, you do not need "ImgBurn" for burning CDs and DVDs from .ISO files. However, "ImgBurn" is still handy for making .ISO files from CDs and DVDs.

USING FREE RESCUE DISKS TO DETECT AND REMOVE MALWARE (continued)

- Our technical advice on using various free rescue disks to remove malware can be found at http://aztcs.org/meeting_notes/winhardsig/malwarecleanup/rescue_disks.pdf

USING FREE RESCUE DISKS TO DETECT AND REMOVE MALWARE (continued)

- "Ransomware" is malware that takes over your computer or part of your computer and offers to give you back access to it when you pay a ransom fee. In a "Windows.." computer, some of the more benign variants of "ransomware" can be removed by booting up the computer in "Safe Mode".

USING FREE RESCUE DISKS TO DETECT AND REMOVE MALWARE (continued)

- The more sophisicated instances of "ransomware" can only be removed by booting up with a free **bootable** "rescue media" CD-R disc, DVD-R disc, or USB flash drive.
  For details about removing "ransomware" see http://aztcs.org/meeting_notes/winhardsig/malwarecleanup/ransomware.pdf