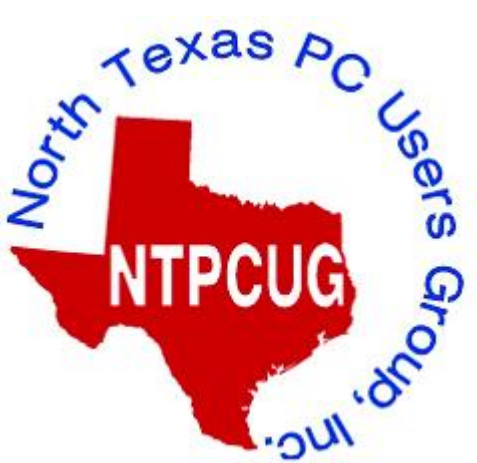
0-STRATEGIES FOR RESOLVING A MALWARE INFECTION IN A "WINDOWS.." COMPUTER

by Francis Chao
fchao2@yahoo.com



Web location for this presentation:

http://aztcs.apcug.org

Click on

"Meeting Notes"

SUMMARY

My "Windows 11" computer was infected with a zero-day malware item on December 10, 2023. Here is my advice on how to deal these sorts of malware infections.

TOPICS

1) Cloning a SSD as a Proactive Defense Against Malware Infections In A "Windows.." Computer
2) Logical Procedure For Malware Infections In A "Windows.." Computer
3) Malware Infection on December 10, 2023
4) Trial and Error To Resolve the Problem

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" to clone the existing SSD
- 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)

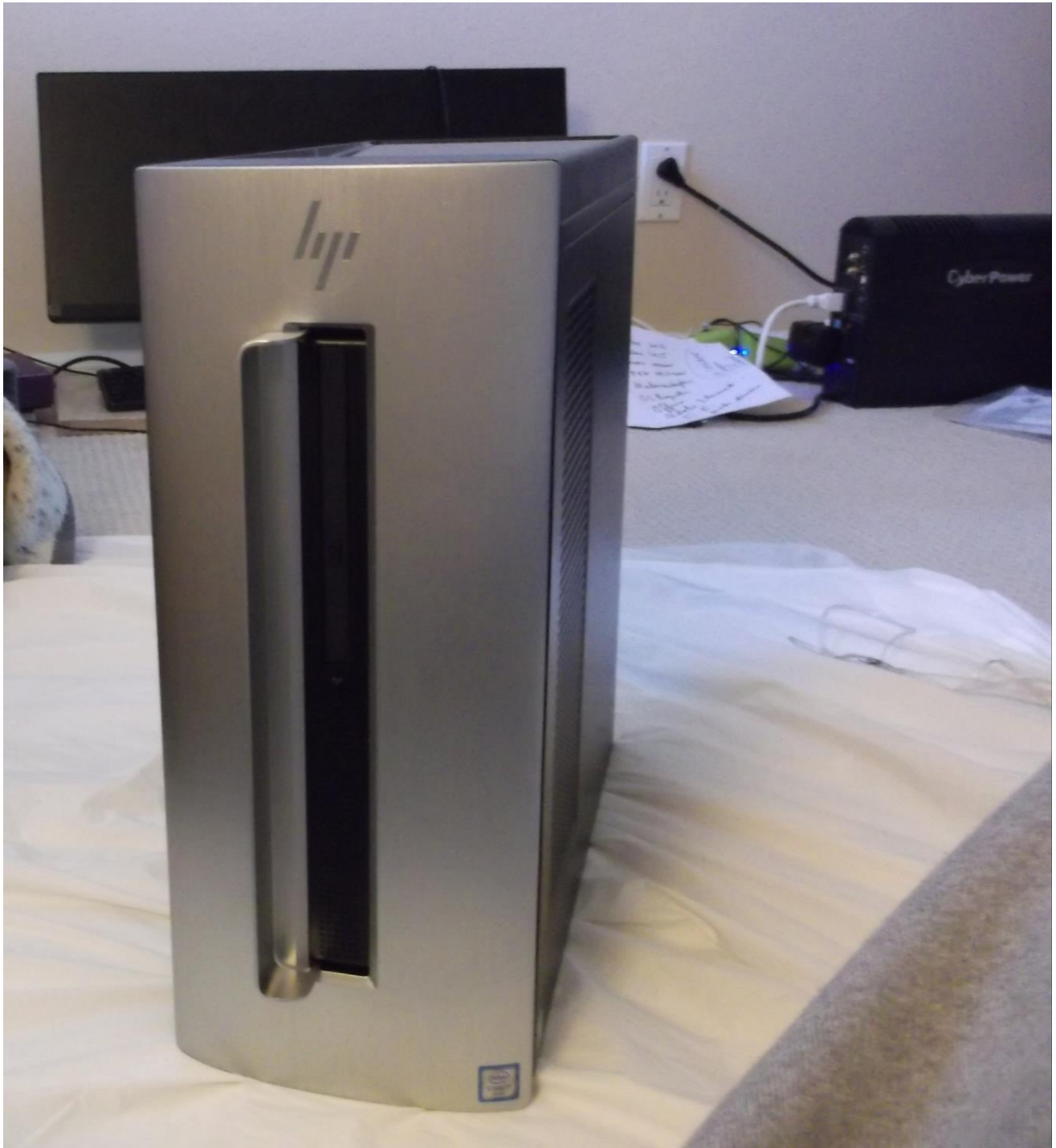
- Instructions for using Clonezilla are available at:
- https://www.makeuseof.com/tag/how-to-use-clonezilla/
- https://clonezilla.org/show-live-doc-content.php?topic=clonezilla-live/doc/03_Disk_to_disk_clone
- https://www.wikihow.com/Use-Clonezilla

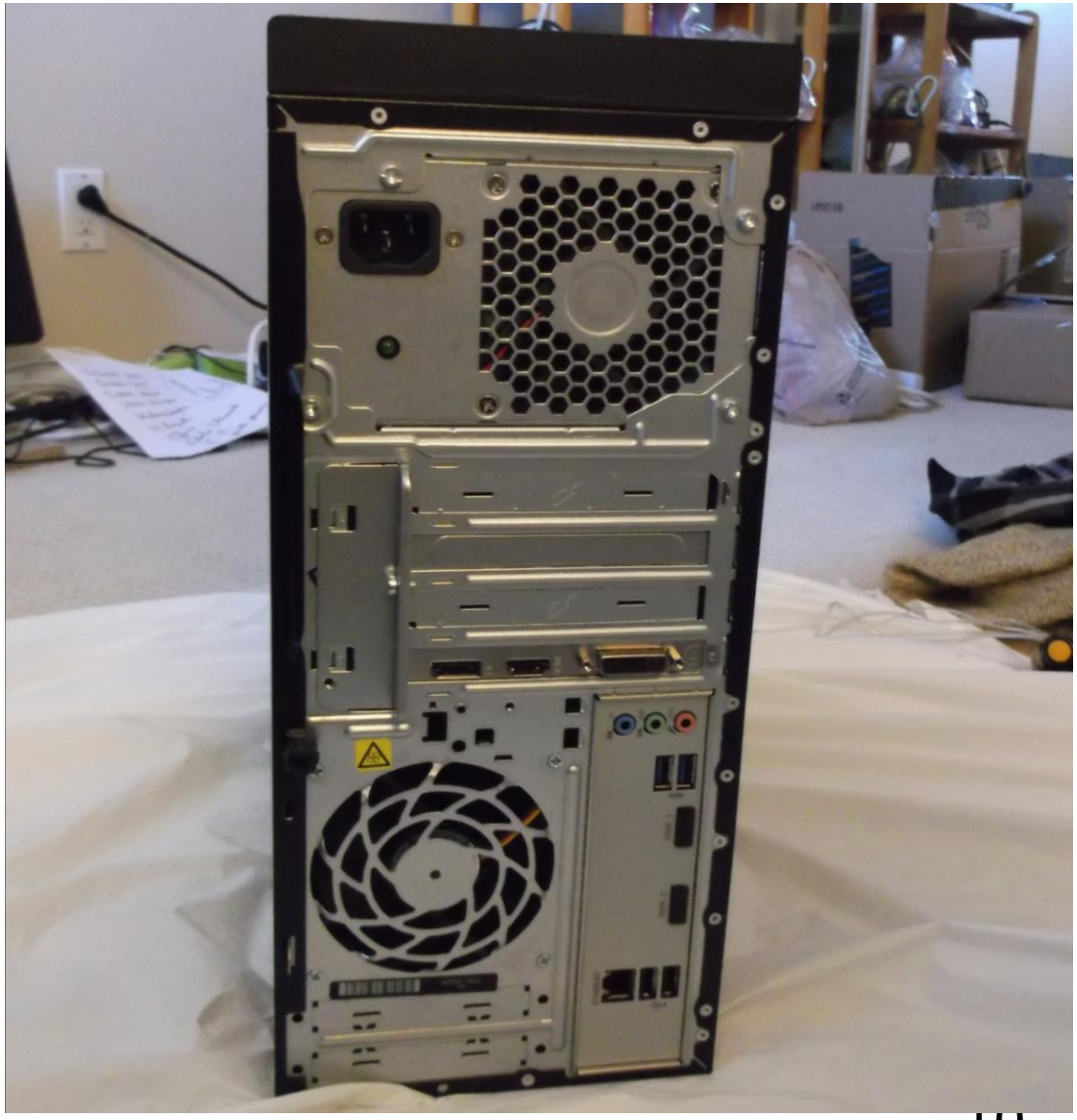
PROACTIVE DEFENSE AGAINST MALWARE INFECTIONS (continued)

- Before booting up the computer with the bootable hard drive or bootable SSD or bootable CD or bootable DVD or bootable USB flash drive, make sure that the source SSD (the one that you wish to clone) is attached to the computer
- Attached the target SSD (the blank one) to the computer only when clonezilla tells you to do so.

LOGICAL PROCEDURE FOR RESOLVING MALWARE INFECTIONS IN "WINDOWS.."

- BIG STEP 100:
  Run a "Quick Scan" with "Windows Security
- BIG STEP 200:
  Use the bundled "Task Manager" to see if the malware "task" can be identified
- BIG STEP 300:
  Use "Revo Uninstaller Portable" to remove the possibly infected "apps"


CyberPower



HP 750-427C (continued)

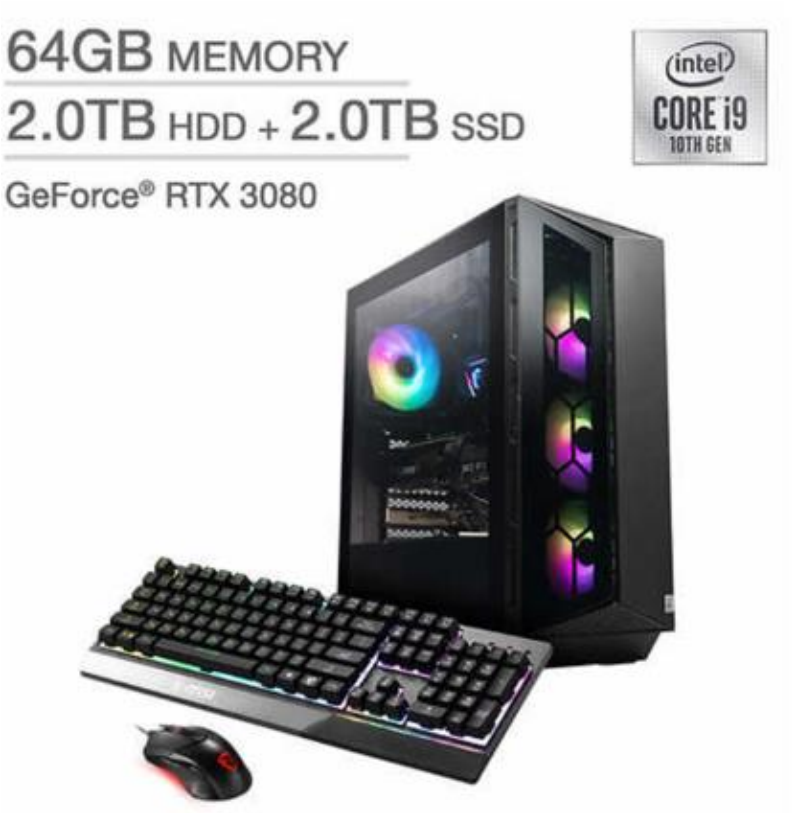
- 2016-12-28 Purchased HP 750-427C at a Costco store in California for $899.99
- 2017-01-01 motherboard-based Ethernet adapter failed--new USB Ethernet adapter installed by F.C.

HP 750-427C (continued)

- 2018-02-20 ATX power supply failed--replaced with a new ATX power supply by F.C.
- 2018-02-22 original Seagate 1TB ST1000DM003 hard drive failed--replaced with a new hard drive by F.C.
- 2020-05-02 Main front fan failed--replaced by F.C.

MSI Aegis i9

- MSI Aegis i9 purchased in 2021



MSI Aegis RS Gaming Desktop - 10th Gen Intel Core i9-10900K - GeForce RTX 3080

Item 1513363 | Model Aegis RS 10TE-058US

★★★★½ 4.5 (30)

Your Price $2,999.99

MSI Aegis i9 (continued)

- 2021-06-19 Purchased online from Costco.com for $2999.99
  The passive cooling device for the Adata 2TB M.2 SSD is inadequate and "CrystalDiskInfo Portable" indicates that the SSD is overheating which causes this computer to run very slowly.
  Immediately replaced the Adata 2TB SSD with a new Seagate 2TB SATA SSD to resolve the problem.

MSI Aegis i9 (continued)

- 2022-09-05 Attempted to put the original bundled Adata 2TB back into service--it immediately overheated and failed.
- 2022-10-19 16-Gigabytre ADATA RAM module #4 failed--RAM modules #2 and #4 replaced by F.C.

MSI Aegis i9 (continued)

- 2022-12-15 CR2023 button battery on the motherboard failed
- 2023-01-01 Replaced the 2TB SATA SSD with a 2TB Samsung M.2 SSD inside an elaborate active cooling device as explained at https://aztcs.apcug.org/meeting_notes/winhardsig/harddrives/SSDs/M.2/M.2-upgrade.pdf
  This resolved the overheating problem.

MSI Aegis i9 (continued)

- 2023-02-11: NVIDIA GeForce RTX 3080 10GB graphics adapter failed. Reconfigured the UEFI firmware and used the motherboard-based Intel graphics adapter to connect to the Viewsonic monitor.