

NUKE & PAVE CHECKLIST FOR INFECTED PC's



Jim McKnight

www.jimopi.net

NukeAndPaveChecklist.lwp

revised 4-12-2013

Owner: _____ Phone: _____

PC Make, Model: _____

Operating System: _____ Work Date/s: _____

Do NOT plug this PC into the Network !! It is probably infected!!

COLLECT OWNER INFORMATION:

- ☐ Ask the owner if any user data is stored in locations other than in "My Documents". If so, you will need to tell your AUTOBACKUP where to find this data when you get to the step where it is run.

Data locations: _____

- ☐ Collect any log-on and admin PASSWORDS. _____
- ☐ Collect any original Application Program or Recovery CD/DVD's from the User, if possible.
- ☐ DEFAULT BROWSER AND HOMEPAGES. _____

BEFORE SHUTTING DOWN THE OLD SYSTEM

- ☐ SYSTEM INFORMATION: If possible, go to "System Properties" and copy down the Operating System & Hardware info. If it won't boot, skip this step.
- ☐ USER ACCOUNT NAMES: If possible, write down the exact User Account names for each User.

- ☐ USER LOG-ON ICON PICTURES: If possible, write down the Welcome Screen User Icon picture description for each User. Get the location if possible. _____

- ☐ DESKTOP INFO: If possible, write down the Theme, Wallpaper, Window Color for each User.

- ☐ SAVE PRODUCT KEYS AND INSTALLED PROGRAM INFO:

- ☐ If system boots OK:

- ☐ BELARC ADVISOR: Install & run Belarc Advisor. This will collect Product Keys and list the installed programs. Save to a Flash-drive.

- ☐ If system will NOT boot:

- ☐ PRODUCT KEYS LIST - (Run PRODUKEY): Boot HIREN's BOOT CD. Run PRODUKEY and save to a flash-drive. (Boot > choose Mini Windows XP > HBCD Menu > Passwords/keys > Product Keys > Produkey). To get the keys: (File > Select source > choose Load Product Keys from all disks currently plugged into System > OK). To save the keys, plug in a flash-drive, then: (Highlight all items > File > Save selected items > name the file as desired.txt > select the flash drive)

- ☐ INSTALLED PROGRAMS LIST - (Run SIW): First, plug in a Flash-drive, then boot a UBCD4WIN CD and run SIW(Remote). Save the results as an HTML Report to a flash-drive. (Start > Programs > System Information > Info and Diag Tools > SIW(Remote). "Load Remote User? = Yes > check "Load all Users". Then click File > Create Report File > HTML. Save to flash drive).

- ☐ SAVE DRIVERS: (DD=DOUBLE DRIVER Utility):

- ☐ If system boots OK, copy the DD Program from a file-protected Flash drive to the Desktop and start it (Portable App), Before running DD, make sure that .Net Framework 2.0 or higher is installed (from Windows Update). Look in Add/Remove Programs if you are not sure.

- ☐ If system will NOT boot, then boot HIREN's BOOT CD and start DD from there. (Boot > choose Mini Windows XP > HBCD Menu > Device Driver > Double Driver).

- ☐ Run DD to back up all the device drivers directly to a flash-drive or external hard-drive.

- ☐ AUTO-BACKUP: *(Saves all user data files, system settings, e-mails, etc)*
 - ☐ If system boots OK, run either WINDOWS EASY TRANSFER TOOL or FAB's AUTOBACKUP (version 3 or 4). Save the data & settings for all User Accounts to an external drive.
 - ☐ If system will NOT boot, install the hard-drive as a slave-drive in a bench PC and run FAB's AUTOBACKUP Version 4 from there. Select the infected drive for backup, then save the data and settings for all User Accounts to a flash-drive or external Hard-drive. **WARNING: The infected hard-drive can easily infect your bench PC! Scan your bench PC when done.**
- ☐ IMAGE BACKUP *(In case all goes wrong, this allows you to start over or find data files that were not transferred)*
 - ☐ Plug backup media: Power down and plug in an external USB hard-drive (or Network cable).
 - ☐ Boot an Acronis Rescue CD and back up the disk image to an external hard-drive. This includes ALL partitions on the main hard-drive.
 - ☐ Unplug the external USB Drive or Network cable! ***(Remember, the PC is infected)***
- ☐ PC HEALTH:
 - ☐ FANS: Make sure all the cooling fans are running.
 - ☐ TEMPERATURES: If system boots OK, install and run SPEEDFAN. If the system will not boot, then boot UBCD4WIN and run SPEEDFAN from there. Record PC Temps: _____
 - ☐ MEMTEST86+: Boot and run MEMTEST86+
 - ☐ DUST: Power down and BLOW the dust out of the PC!
 - ☐ BATTERY: With PC unplugged, check the keep-alive Battery voltage > 3.0vdc
- ☐ BIOS: Verify that the BIOS Date, Time, and AM/PM are correct (Even if the System time is correct)
- ☐ MALWARE SCANS: Either boot a UBCD4WIN CD or mount drives on another PC and.....
 - ☐ Scan any secondary hard-drives for malware before re-installing Windows on the main drive.
 - ☐ Scan the FAB's AUTOBACKUP saved files and Double Driver saved files for malware. This includes ANY saved data that is to be transferred to the new system. **WARNING: Malware can follow your personal data files, so scan them thoroughly for malware before restoring data to a new system.**

HARD-DRIVE: TEST, WIPE, AND PREPARE

- ☐ HARD-DRIVE HEALTH:
 - ☐ HDTUNE: *(If necessary, run it from a UBCD4WIN CD or HIREN's BOOT CD).*
Make sure the ☐ hard-drive health is OK and the scanning speed is normal. ☐ _____ MB/sec
 - ☐ SPINRITE: Boot and run a level 4 SpinRite scan on the hard-drive. + Verify temperature is OK.
- ☐ Unplug all hard-drives except the main hard-drive before booting DBAN *(just in case).*
- ☐ Boot DBAN and run it on the infected hard-drive. *NOTE: This will destroy any Original OEM partitions on the drive that are for diagnostics or recovery. This is necessary as newer malware can infect those hidden partitions as well as the MBR. Note: The DBAN utility is available on both the UBCD4WIN and HIREN's BOOT CD boot menus.*
- ☐ Re-partition and reformat the hard-drive as NTFS using UBCD, UBCD4WIN, or EASEUS.

RE-INSTALL WINDOWS *(See my Install Checklists for XP or Windows 7)*

- ☐ RESTORE/REINSTALL SYSTEM:
 - ☐ ACRONIS with Universal Restore: If a known clean ACRONIS backup Image of the system is available, use it to restore the system. *NOTE: If you are restoring an image with multiple partitions, always check the box that will do all the partitions at once including the MBR. Also, choose: "Copy the NT Signature from the Image". Do not choose: "Generate a new Signature". Otherwise, the Manufacturer's Recovery and Diagnostic Partitions may not boot.*
 - ☐ Otherwise, if a Hidden Recovery Partition is available in the PC, use it to re-install the system.
 - ☐ Otherwise, if an Original Mfg Recovery CD/DVD is available, use it to re-install the system.
 - ☐ Otherwise, install the Operating System shown on the COA Sticker using an authentic Microsoft Windows Install CD/DVD.
- ☐ Restore User data & settings from the AUTOBACKUP. Change User's pictures as desired.
- ☐ Re-install and activate all necessary Application programs.