Windows Maintenance, Diagnosis & Restoration

CPD Seminar
23 May 2012

1

Signature PC

- http://www.zdnet.com/blog/hardware/microsoft-to-charge-customers-99-to
- Microsoft charged $99 to remove crap ware from PC

2

Routine Maintenance (1105)

- Windows typically suffers for file system, registry & startup bloat as well as disk fragmentation issues.
- These issues are compounded when applications are installed & uninstalled. Uninstalls are typically never clean & leave clutter behind.
- A mechanical disk that is more than 50% full will have higher seek latency & lower internal data rates, when a Disk is 100% full it is typically 4 times slower than when it is new. It is therefore always a good idea to over spec your disk storage OR use an SSD.
- Do NOT use the Compress Files option in the Disk Cleanup Wizard. Preferably do not use the Disk Cleanup Wizard at all. Compressed files are a performance hit.

3

Optimising a PC (1105)

- Process of Optimising a PC:
  - Identify
    - Use Add/Remove Programs and SysInternal Autoruns to ID obsolete or unnecessary software.
    - SysInternal Autoruns from Applications Folder or http://technet.microsoft.com/en-us/sysinternals/bb963902
  - Remove/Disable
  - Clean
  - Defragment

4

Optimising a PC 2

- Identify (done)
- Remove/Disable
  - Use Add/Remove Programs to Uninstall. Autoruns can be used to delete any remnants from the uninstalled application or disable a specific startup application, driver or service.

5

Optimising a PC 3

- Identify (done)
- Remove / Disable (done)
- Clean
  - Clean Temp Folders & Caches etc.
  - Tools like CCleaner can perform this task for you:
  - CCleaner http://www.piriform.com/ccleaner
    - The CCLeaner Registry Cleaner is effective but note that it can inadvertently remove offline resources like temporarily inaccessible network install set sources.
    - CCleaner can also remove Hotfix Uninstallers but you will need to remove the Uninstall entries in the Registry using the Registry Cleaner.

6

Optimising a PC 4/4

- Identify (done)
- Remove / Disable (done)
- Clean (done)
- Defragment
  - Clear the System Restore periodically but do not disable it.
  - Defragment the Hard Drive. Windows Defrag limited functionality.
  - MyDefrag http://www.mydefrag.com/
    - Supports Consolidation to beginning of drive
    - Defragment only
    - Daily Defragment modes can be scheduled

7

Optimising a PC 4/4 Cont

- Identify (done)
- Remove / Disable (done)
- Clean (done)
- Defragment
  - Note that large files may not successfully defragment using a File System defragmentation. Use Windows Defrag report to ID files with high levels of fragmentation & target with SysInternals Contig tool http://technet.microsoft.com/en-us/sysinternals/bb897428

8

Windows Fault Diagnosis & Recovery (1105)

- Diagnosis of any problem is inherently driven by visual cues which lead you down a path to a resolution. As a result it is very difficult to proceduralise
  - System Crash
    - With BSOD or Minidump use a Crashdump Analyser.
    - Freeze or Slow Response indicates a Kernel level issue such as a driver or device filter driver.
  - Tools to gain visibility
    - Event Log
    - Task Manager (or SysInternals Process Explorer) / Performance Monitor
    - SysInternal Process Monitor (File & Registry)

9

Diagnosis & Recovery 2

- Tools to Narrow down scope of issue
  - Windows Safe Mode
  - Application Safe Mode (typically /safe)
- Brute Force Resolution Methods (without identifying underlying cause)
  - Last Known Good Configuration
  - System Restore
  - Restore from Backup
- Tools to aid in recovery & offline analysis
  - WinRE
  - WinPE based such as Win7PE Winbuilder Project. http://reboot.pro/forum/22/
  - DaRT – WinPE with SysInternals ERD Toolset (Not Free)

10

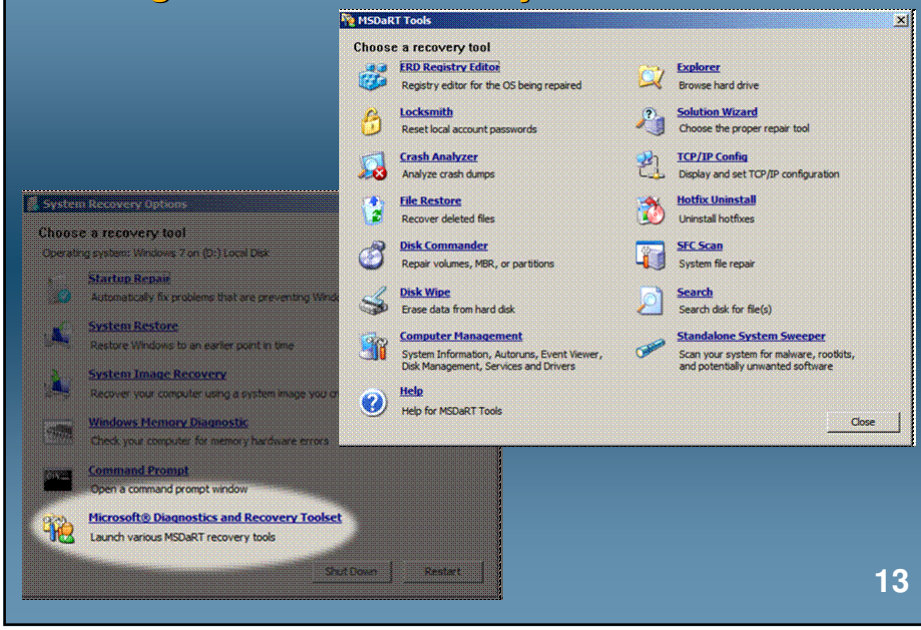
Diagnosis & Recovery 3

- Unexplained Behaviour or Performance issues indicating Malware
  - Check regedit.exe & taskmgr.exe can run & verify the Antivirus software can update.
  - Check number of network connections netstat –a –b (-b shows associated application) and where they are established too.
  - Always be aware of the possibility of a Zero Day exploit.

Diagnosis & Recovery 4

- Analysing Windows Dump Files
  - Debugging Tools for Windows (Windbg)
    - 32bit: http://msdn.microsoft.com/en-us/windows/hardware/gg463016
    - 64bit: http://msdn.microsoft.com/en-us/windows/hardware/gg463012
    - Set File Menu > Symbol File Path to: SRV*d:\symbols*http://msdl.microsoft.com/download/symbols
    - This will automatically download & install all requires symbols to analyse a specific .dmp file.
  - Nirsoft BlueScreenView
    - http://www.nirsoft.net/utils/blue_screen_view.html
    - Use Options Menu > Advanced Options to change default Minidump File Location.

Diagnostic and Recovery Toolset



13

Malware Identification & Removal (1105)

- Current Entry Vectors for Malware are via Web Browser exploits or Social Engineering. Disk Based & Email attachment attack Vectors as less common.
- Zero day exploits, or variations that are not detected by the Heuristic Engine, often mean that the Antivirus Software gets an update which allows it to detect the Malware after the system has already been infected.
- Effective Scanning for Malware by Antivirus Software needs to be done Offline
  - Boot Recovery CD such as NOD32 Rescue CD.
  - Remove HDD & connect as secondary to technicians PC.
  - Be aware of inaccessible files, some Malware change the security permissions on the folder they are running from to exclude the Administrator. Recovery Disks that typically run as Administrator & Technicians PC's will not be able to scan these folders without taking ownership or resetting the file permissions. Inspect the Scan Logs carefully.
- Malware Scanning Tools Examples
  - Malwarebytes http://www.malwarebytes.org/
  - Spybot S&D http://www.safer-networking.org/en/index.html

14

Malware Identification & Removal 2 (1105)

- Manual Identification of Rootkits
  - Less common but difficult to identify.
  - SysInternals Rootkit Revealer http://technet.microsoft.com/en-us/sysinternals/bb897445
  - Gmer http://www.gmer.net/
- Manual Identification of Malware
  - Use Autoruns to identify all non rootkit malware. The Malware has to have a startup entry point. http://technet.microsoft.com/en-us/sysinternals/bb963902.aspx
  - Be wary of Autoruns Hide Microsoft Entries as these typically hide Image File Execution Options. When looking for malware always show everything.
  - Vet all entries that do not have a Publisher or do not have a Verified Publisher
  - Entries that point to temp or cache folders & user profile locations are suspect.
  - Once Identified use a recovery disk to disable.
  - Can be run against Offline Drive or Image.

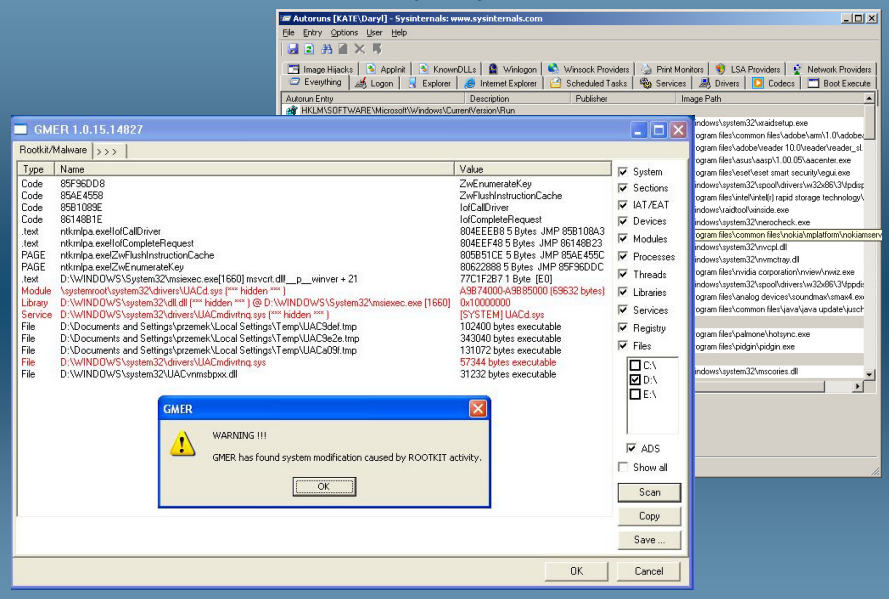
15

Malware Identification & Removal 3 (1105)

- Always clear System Restore & Recycle Bin after a Malware infection.
- Consideration: Roaming profiles can restore viruses on next login if you remove them using a recovery disk. Ensure you ID what the recovery disk removed from the Local PC Users Profile & remove it from the Users Profile on the Server before logging in.

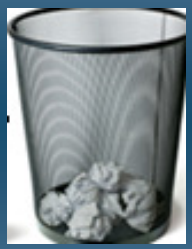
16

GMER & Autoruns (1105)



Post Malware Cleanup (1105)

- Often Malware makes changes to the system to prevent it from being identified or removed. After the Malware has been removed these can block certain functionality.
- Always Disable and Re-enable the System Restore feature after you have removed a Virus or Malware. This will clean the System Restore History & any copies of the Virus or Malware that I contains.
- Always Clear the Recycle Bin for the same reason.



Post Malware Cleanup 2 (1105)

- Restrict Applications via Group Policy
  - Blocks specific applications from running, typically Antivirus or Malware Removal Software.
  - http://support.microsoft.com/kb/323525
- Image File Execution Options
  - Microsoft Debugging Interface can be used to stop an specific application from running or start an unrelated application in it's place. Typically included invalid debugger options for Antivirus or Malware Removal Software.
  - http://isc.sans.org/diary.html?storyid=4039

19

Post Malware Cleanup 3 (1105)

- Disable System Restore via Group Policy
  - The System Restore Tab may not be visible in System Properties.
  - http://support.microsoft.com/kb/283073
- Disable Task manager via Group Policy
  - You get *"Task Manager has been disabled by your administrator"* if you press Ctrl-Shift-Esc, run Taskmgr.exe or Ctrl-Alt-Del & Click the Task manager Button.
  - http://support.microsoft.com/kb/555480

20

Post Malware Cleanup 4 (1105)

- Reset Internet Proxy Setting
  - Unable to access the internet using Internet Explorer or other proxy aware applications.
  - Control Panel > Internet Options > Connections Tab > Lan Settings Button > Disable Proxy Server.
  - http://support.microsoft.com/kb/2289942
- Reset hosts file back to default
  - The hosts file can redirect DNS lookups. This can block Antivirus Updates, redirect or disable specific fully qualified domain names.
  - Clean all entries except the IPV4 & IPV6 localhost entries from C:\Windows\System32\Drivers\etc\hosts
  - http://support.microsoft.com/kb/972034

21

Post Malware Cleanup 5 (1105)

- Recover from Winsock2 Corruption
  - "netsh winsock reset" from an Administrator command prompt.
- Reset TCP/IP to default state
  - "netsh int ip reset c:\resetlog.txt" from an Administrator command prompt.
  - http://support.microsoft.com/kb/299357

22

Post Malware Cleanup 5 (1105)

- Restore Missing Folders Option in Windows Explorer
  - Prevents access to Show Hidden Files & Folders.
  - http://www.mydigitallife.info/how-to-fix-folder-options-missing-in-windows-explorer/
- Show Hidden Files & Folders not working
  - http://www.teeeh.com/troubleshooting-and-fixes/show-hidden-files-and-folders-not-working/
  - http://en.kioskea.net/forum/affich-21376-not-showing-hidden-files-and-folders

23

Sysinternals (1105)

- All Sysinternals Utilities are available from
  - http://technet.microsoft.com/en-us/sysinternals
- Sysinternals Live
  - Sysinternals Live is a service that enables you to execute Sysinternals tools directly from the Web without hunting for and manually downloading them. Simply enter a tool's Sysinternals Live path into Windows Explorer or a command prompt as http://live.sysinternals.com/<toolname> or \\live.sysinternals.com\tools\<toolname>.
  - You can view the entire Sysinternals Live tools directory in a browser at http://live.sysinternals.com.
  - Download zip versions at http://live.sysinternals.com/Files/

24

Further Reading.. (1105)

- Malware Cleaning using Sysinternals Tools
  - http://live.sysinternals.com/files/SysinternalsMalwareCleaning.pdf
- Presented August 2011 by Mark Russinovich of Sysinternals, part Book Launch.
- Covers indepth analysis of Zero Day Malware and use of Sysinternals Tools to identify.
- Analysis of historical infections.