

Rule Name	Rule Platform	Entity Path	Entity Attributes	Entity Type
O-00001: [MS- Windows-10] Files and Directories	Windows	C:\WINDOWS\System32\winmsd.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\wscript.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\xcopy.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\cluster.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\cmd.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\compact.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\command.com	attributes created deleted renamed	File
		C:\WINDOWS\System32\convert.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\cscript.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\dfscmd.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\diskcomp.com	attributes created deleted renamed	File
		C:\WINDOWS\System32\diskcopy.com	attributes created	File

	deleted renamed	
C:\WINDOWS\System32\doskey.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\exe2bin.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\expand.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\fc.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\find.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\findstr.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\finger.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\forcedos.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\format.com	attributes created deleted renamed	File
C:\WINDOWS\System32\hostname.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\iisreset.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ipconfig.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ipxroute.exe	attributes created	File

	deleted renamed	
C:\WINDOWS\System32\label.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\logoff.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\makecab.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\mem.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\mmc.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\mountvol.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\msiexec.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\msg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ntsd.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\pathping.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ping.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\rasdial.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\recover.exe	attributes created	File

	deleted renamed	
C:\WINDOWS\System32\replace.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\reset.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\routemon.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\runonce.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\shadow.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\share.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\syskey.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\taskmgr.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tlntsess.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tlntsvr.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tracert.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tree.com	attributes created deleted renamed	File
C:\WINDOWS\System32\tsadmin.exe	attributes created	File

	deleted renamed	
C:\WINDOWS\System32\tscon.exe	attributes created deleted renamed	File
C:\WINDOWS\system32\mshta.exe	attributes created deleted renamed	File
C:\Documents and Settings	attributes created deleted renamed	Directory
C:\Program Files	attributes created deleted renamed	Directory
C:\Documents and Settings\Administrator	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Documents\DrWatson	attributes created deleted renamed	Directory
C:\Documents and Settings\Default User	attributes created deleted renamed	Directory
C:\WINDOWS\Temp	attributes created deleted renamed	Directory
C:\WINDOWS\\$_NtServicePackUninstall\$	attributes created deleted renamed	Directory
C:\WINDOWS\CSC	attributes created deleted renamed	Directory
C:\WINDOWS\Debug	attributes created deleted renamed	Directory
C:\WINDOWS\Registration	attributes created	Directory

	deleted renamed	
C:\WINDOWS\repair	attributes created deleted renamed	Directory
C:\WINDOWS\Debug\UserMode	attributes created deleted renamed	Directory
C:\WINDOWS\System32\appmgmt	attributes created deleted renamed	Directory
C:\WINDOWS\config	attributes created deleted renamed	Directory
C:\WINDOWS\System32\DTCLLog	attributes created deleted renamed	Directory
C:\WINDOWS\System32\GroupPolicy	attributes created deleted renamed	Directory
C:\WINDOWS\System32\ias	attributes created deleted renamed	Directory
C:\WINDOWS\System32\NTMSData	attributes created deleted renamed	Directory
C:\WINDOWS\System32\reinstallbackups	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Setup	attributes created deleted renamed	Directory
C:\WINDOWS\System32\at.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\drwatson.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\drwtsn32.exe	attributes created	File

	deleted renamed	
C:\WINDOWS\System32\ledlin.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\net.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\reg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\regedt32.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\rexec.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\subst.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\telnet.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\spool\printers	attributes created deleted renamed	Directory
C:\Program Files\Resource Kit	attributes created deleted renamed	Directory
C:\WINDOWS\System32\rsh.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\dlldata	attributes created deleted renamed	Directory
C:\WINDOWS\security	attributes created deleted renamed	Directory

C:\WINDOWS\System32\cacls.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\debug.exe	attributes created deleted hash renamed size	File
C:\Temp	attributes created deleted renamed	Directory
C:\AUTOEXEC.BAT	attributes created deleted hash renamed size	File
C:\boot.ini	attributes created deleted hash renamed size	File
C:\config.sys	attributes created deleted hash renamed size	File
C:\io.sys	attributes created deleted hash renamed size	File
C:\msdos.sys	attributes created deleted hash renamed size	File
C:\ntbootdd.sys	attributes created deleted hash renamed size	File

C:\ntdetect.com	attributes created deleted hash renamed size	File
C:\ntldr	attributes created deleted renamed	Directory
C:\WINDOWS\System32\arp.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\nbtstat.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\netstat.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\nslookup.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ntbackup.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\regini.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\route.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\secedit.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\systeminfo.exe	attributes created deleted renamed	File
C:\Documents and Settings\All Users\Application Data\Microsoft\Media Index	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Application Data\Microsoft\User Account Pictures\guest.bmp	attributes created	File

	deleted renamed	
C:\Documents and Settings\All Users\DRM	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Documents	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\DRM\drm2.lic	attributes created deleted renamed	File
C:\Documents and Settings\All Users\DRM\drm2.sst	attributes created deleted renamed	File
C:\Documents and Settings\All Users\Application Data	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\DSS\MachineKeys	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys	attributes created deleted renamed	Directory
C:\WINDOWS\System32\append.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\chkdsk.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\chkntfs.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\cipher.exe	attributes created deleted renamed	File
C:\Programdata	attributes created deleted renamed	Directory
C:\WINDOWS\System32\CCM\Cache	attributes created	Directory

	deleted renamed	
C:\WINDOWS\System32\CCM\Cache\skpswi.dat	attributes created deleted renamed	File
C:\WINDOWS\System32\CCM\Inventory\idmifs	attributes created deleted renamed	Directory
C:\WINDOWS\System32\CCM\Inventory\noidmifs	attributes created deleted renamed	Directory
C:\WINDOWS\System32\CCM\Logs	attributes created deleted renamed	Directory
C:\WINDOWS\Debug\WPD	attributes created deleted renamed	Directory
C:\WINDOWS\PCHealth\ERRORREP\QHEADLES	attributes created deleted renamed	Directory
C:\WINDOWS\PCHealth\ERRORREP\QSIGNOFF	attributes created deleted renamed	Directory
C:\WINDOWS\Registration\CRMLog	attributes created deleted renamed	Directory
C:\WINDOWS\Debug\WIA	attributes created deleted renamed	Directory
C:\WINDOWS\System32\FxsTmp	attributes created deleted renamed	Directory
C:\WINDOWS\System32\com\dmp	attributes created deleted renamed	Directory
C:\WINDOWS\System32\spool\drivers\color	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Tasks	attributes created	Directory

	deleted renamed	
C:\WINDOWS\System32\Tasks\Microsoft\Windows\PLA\System	attributes created deleted renamed	Directory
C:\WINDOWS\tracing	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Tasks\Microsoft\Windows\WindowsCalendar	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Microsoft\Crypto\RSA\MachineKeys	attributes created deleted renamed	Directory
C:\WINDOWS\System32\eventtriggers.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\netsh.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\sc.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\regsvr32.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\lftp.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\attrib.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\ftp.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\net1.exe	attributes created	File

	deleted hash renamed size	
C:\WINDOWS\System32\rcp.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\runas.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32	attributes created deleted renamed	Directory
C:\WINDOWS\regedit.exe	attributes created deleted renamed	File
C:\users\All Users\Microsoft\Media Index	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\User Account Pictures	attributes created deleted renamed	Directory
C:\users\All users\Microsoft\User Account Pictures\Default Pictures	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\Crypto\DSS\MachineKeys	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\Crypto\RSA\MachineKeys	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\DRM\Server	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\Windows\DRM	attributes created deleted renamed	Directory

C:\users\All Users\Microsoft\Windows\DRM\Cache	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\leHome	attributes created deleted renamed	Directory
C:\users\Public\Recorded TV	attributes created deleted renamed	Directory
C:\users\Public\Recorded TV\Sample Media	attributes created deleted renamed	Directory
C:\WINDOWS\System32\ACW.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\alg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\AtBroker.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\audiodg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\autoconv.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\autofmt.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\bcdedit.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\BitLockerWizard.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\bitsadmin.exe	attributes created deleted renamed	File

C:\WINDOWS\System32\bootcfg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\cmdkey.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\DFDWiz.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dfmgfat.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dfmgfc.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dfmgui.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dfsrmgr.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dialer.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\diskpart.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dispdiag.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\eventcreate.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\FirewallControlPanel.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\FirewallSettings.exe	attributes created deleted renamed	File

C:\WINDOWS\System32\getmac.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\icacls.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\mobsync.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\MRINFO.EXE	attributes created deleted renamed	File
C:\WINDOWS\System32\mrt.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\rekeywiz.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\Robocopy.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\Rcping.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\schtasks.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\sysedit.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesAdvanced.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesComputerName.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesDataExecutionPrevention.exe	attributes created deleted renamed	File

C:\WINDOWS\System32\SystemPropertiesHardware.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesPerformance.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesProtection.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesRemote.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\systray.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\takeown.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tracert.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tscupgrd.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tsdiscon.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tskill.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tsshutdn.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\Utilman.exe	attributes created deleted renamed	File
C:\Windows	attributes created deleted renamed	Directory

O-00003: Windows Installed Software Activity	Windows *		created deleted installed_date installed_location publisher size version	InstalledSoftware
O-00004: Windows Service Activity	Windows *		created deleted image_path	Service
O-00008: [MS- Windows- 2008-DM] Files and Directories	Windows	C:\WINDOWS\System32\winmsd.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\wscript.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\xcopy.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\cluster.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\cmd.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\compact.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\command.com	attributes created deleted renamed	File
		C:\WINDOWS\System32\convert.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\cscript.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\dfscmd.exe	attributes created deleted renamed	File

C:\WINDOWS\System32\diskcomp.com	attributes created deleted renamed	File
C:\WINDOWS\System32\diskcopy.com	attributes created deleted renamed	File
C:\WINDOWS\System32\doskey.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\exe2bin.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\expand.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\fc.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\find.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\findstr.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\finger.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\forcedos.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\format.com	attributes created deleted renamed	File
C:\WINDOWS\System32\hostname.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\iisreset.exe	attributes created deleted renamed	File

C:\WINDOWS\System32\ipconfig.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ipxroute.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\label.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\logoff.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\makecab.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\mem.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\mmc.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\mountvol.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\msiexec.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\msg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ntsd.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\pathping.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ping.exe	attributes created deleted renamed	File

C:\WINDOWS\System32\rasdial.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\recover.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\replace.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\reset.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\routemon.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\runonce.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\shadow.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\share.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\syskey.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\taskmgr.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tlntsess.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tlntsvr.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tracert.exe	attributes created deleted renamed	File

C:\WINDOWS\System32\tree.com	attributes created deleted renamed	File
C:\WINDOWS\System32\tsadmin.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tscon.exe	attributes created deleted renamed	File
C:\WINDOWS\system32\mshta.exe	attributes created deleted renamed	File
C:\Documents and Settings	attributes created deleted renamed	Directory
C:\Program Files	attributes created deleted renamed	Directory
C:\Documents and Settings\Administrator	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Documents\DrWatson	attributes created deleted renamed	Directory
C:\Documents and Settings\Default User	attributes created deleted renamed	Directory
C:\WINDOWS\Temp	attributes created deleted renamed	Directory
C:\WINDOWS\$NtServicePackUninstall\$	attributes created deleted renamed	Directory
C:\WINDOWS\CSC	attributes created deleted renamed	Directory

C:\WINDOWS\Debug	attributes created deleted renamed	Directory
C:\WINDOWS\Registration	attributes created deleted renamed	Directory
C:\WINDOWS\repair	attributes created deleted renamed	Directory
C:\WINDOWS\Debug\UserMode	attributes created deleted renamed	Directory
C:\WINDOWS\System32\appmgmt	attributes created deleted renamed	Directory
C:\WINDOWS\config	attributes created deleted renamed	Directory
C:\WINDOWS\System32\DTCLLog	attributes created deleted renamed	Directory
C:\WINDOWS\System32\GroupPolicy	attributes created deleted renamed	Directory
C:\WINDOWS\System32\ias	attributes created deleted renamed	Directory
C:\WINDOWS\System32\NTMSData	attributes created deleted renamed	Directory
C:\WINDOWS\System32\reinstallbackups	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Setup	attributes created deleted renamed	Directory
C:\WINDOWS\System32\at.exe	attributes created deleted renamed	File

C:\WINDOWS\System32\drwatson.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\drwtsn32.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\edlin.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\net.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\reg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\regedt32.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\rexec.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\subst.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\telnet.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\spool\printers	attributes created deleted renamed	Directory
C:\Program Files\Resource Kit	attributes created deleted renamed	Directory
C:\WINDOWS\System32\rsh.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\dlldata	attributes created	Directory

	deleted renamed	
C:\WINDOWS\security	attributes created deleted renamed	Directory
C:\WINDOWS\System32\cacls.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\debug.exe	attributes created deleted hash renamed size	File
C:\Temp	attributes created deleted renamed	Directory
C:\AUTOEXEC.BAT	attributes created deleted hash renamed size	File
C:\boot.ini	attributes created deleted hash renamed size	File
C:\config.sys	attributes created deleted hash renamed size	File
C:\io.sys	attributes created deleted hash renamed size	File
C:\msdos.sys	attributes created deleted hash renamed size	File

C:\ntbootdd.sys	attributes created deleted hash renamed size	File
C:\ntdetect.com	attributes created deleted hash renamed size	File
C:\ntldr	attributes created deleted renamed	Directory
C:\WINDOWS\System32\arp.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\nbtstat.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\netstat.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\nslookup.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ntbackup.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\regini.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\route.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\secedit.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\systeminfo.exe	attributes created deleted renamed	File

C:\Documents and Settings\All Users\Application Data\Microsoft\Media Index	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Application Data\Microsoft\User Account Pictures\guest.bmp	attributes created deleted renamed	File
C:\Documents and Settings\All Users\DRM	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Documents	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\DRM\drm2.lic	attributes created deleted renamed	File
C:\Documents and Settings\All Users\DRM\drm2.sst	attributes created deleted renamed	File
C:\Documents and Settings\All Users\Application Data	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\DSS\MachineKeys	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys	attributes created deleted renamed	Directory
C:\WINDOWS\System32\append.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\chkdsk.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\chkntfs.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\cipher.exe	attributes created deleted renamed	File

C:\Programdata	attributes created deleted renamed	Directory
C:\WINDOWS\System32\CCM\Cache	attributes created deleted renamed	Directory
C:\WINDOWS\System32\CCM\Cache\skpswi.dat	attributes created deleted renamed	File
C:\WINDOWS\System32\CCM\Inventory\idmifs	attributes created deleted renamed	Directory
C:\WINDOWS\System32\CCM\Inventory\noidmifs	attributes created deleted renamed	Directory
C:\WINDOWS\System32\CCM\Logs	attributes created deleted renamed	Directory
C:\WINDOWS\Debug\WPD	attributes created deleted renamed	Directory
C:\WINDOWS\PCHealth\ERRORREP\QHEADLES	attributes created deleted renamed	Directory
C:\WINDOWS\PCHealth\ERRORREP\QSIGNOFF	attributes created deleted renamed	Directory
C:\WINDOWS\Registration\CRMLog	attributes created deleted renamed	Directory
C:\WINDOWS\Debug\WIA	attributes created deleted renamed	Directory
C:\WINDOWS\System32\FxsTmp	attributes created deleted renamed	Directory
C:\WINDOWS\System32\com\dmp	attributes created deleted renamed	Directory

C:\WINDOWS\System32\spool\drivers\color	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Tasks	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Tasks\Microsoft\Windows\PLA\System	attributes created deleted renamed	Directory
C:\WINDOWS\tracing	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Tasks\Microsoft\Windows\WindowsCalendar	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Microsoft\Crypto\RSA\MachineKeys	attributes created deleted renamed	Directory
C:\WINDOWS\System32\eventtriggers.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\netsh.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\sc.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\regsvr32.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tftp.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\attrib.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\ftp.exe	attributes created	File

	deleted hash renamed size	
C:\WINDOWS\System32\net1.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\rpc.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\runas.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32	attributes created deleted renamed	Directory
C:\WINDOWS\regedit.exe	attributes created deleted renamed	File
C:\users\All Users\Microsoft\Media Index	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\User Account Pictures	attributes created deleted renamed	Directory
C:\users\All users\Microsoft\User Account Pictures\Default Pictures	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\Crypto\DSS\MachineKeys	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\Crypto\RSA\MachineKeys	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\DRM\Server	attributes created	Directory

	deleted renamed	
C:\users\All Users\Microsoft\Windows\DRM	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\Windows\DRM\Cache	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\leHome	attributes created deleted renamed	Directory
C:\users\Public\Recorded TV	attributes created deleted renamed	Directory
C:\users\Public\Recorded TV\Sample Media	attributes created deleted renamed	Directory
C:\WINDOWS\System32\ACW.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\alg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\AtBroker.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\audiodg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\autoconv.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\autofmt.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\bcdedit.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\BitLockerWizard.exe	attributes created	File

	deleted renamed	
C:\WINDOWS\System32\bitsadmin.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\bootcfg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\cmdkey.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\DFDWiz.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dfrgfat.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dfrgifc.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dfrgui.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dfsrmgr.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dialer.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\diskpart.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dispdiag.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\eventcreate.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\FirewallControlPanel.exe	attributes created	File

	deleted renamed	
C:\WINDOWS\System32\FirewallSettings.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\getmac.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\icacls.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\mobsync.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\MRINFO.EXE	attributes created deleted renamed	File
C:\WINDOWS\System32\mrt.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\rekeywiz.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\Robocopy.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\Rcping.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\schtasks.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\sysedit.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesAdvanced.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesComputerName.exe	attributes created	File

	deleted renamed	
C:\WINDOWS\System32\SystemPropertiesDataExecutionPrevention.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesHardware.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesPerformance.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesProtection.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesRemote.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\systray.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\takeown.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tracert.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tscupgrd.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tsdiscon.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tskill.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tsshutdn.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\Utilman.exe	attributes created	File

O-00009: [MS- Windows- 2012-DM] Files and Directories	Windows		deleted renamed	
		C:\Windows	attributes created deleted renamed	Directory
		C:\WINDOWS\System32\winmsd.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\wscript.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\xcopy.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\cluster.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\cmd.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\compact.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\command.com	attributes created deleted renamed	File
		C:\WINDOWS\System32\convert.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\cscript.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\dfscmd.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\diskcomp.com	attributes created deleted renamed	File
		C:\WINDOWS\System32\diskcopy.com	attributes created	File

	deleted renamed	
C:\WINDOWS\System32\doskey.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\exe2bin.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\expand.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\fc.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\find.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\findstr.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\finger.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\forcedos.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\format.com	attributes created deleted renamed	File
C:\WINDOWS\System32\hostname.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\iisreset.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ipconfig.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ipxroute.exe	attributes created	File

	deleted renamed	
C:\WINDOWS\System32\label.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\logoff.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\makecab.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\mem.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\mmc.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\mountvol.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\msiexec.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\msg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ntsd.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\pathping.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ping.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\rasdial.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\recover.exe	attributes created	File

	deleted renamed	
C:\WINDOWS\System32\replace.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\reset.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\routemon.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\runonce.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\shadow.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\share.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\syskey.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\taskmgr.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tlntsess.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tlntsvr.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tracert.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tree.com	attributes created deleted renamed	File
C:\WINDOWS\System32\tsadmin.exe	attributes created	File

	deleted renamed	
C:\WINDOWS\System32\tscon.exe	attributes created deleted renamed	File
C:\WINDOWS\system32\mshta.exe	attributes created deleted renamed	File
C:\Documents and Settings	attributes created deleted renamed	Directory
C:\Program Files	attributes created deleted renamed	Directory
C:\Documents and Settings\Administrator	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Documents\DrWatson	attributes created deleted renamed	Directory
C:\Documents and Settings\Default User	attributes created deleted renamed	Directory
C:\WINDOWS\Temp	attributes created deleted renamed	Directory
C:\WINDOWS\\$\NtServicePackUninstall\$	attributes created deleted renamed	Directory
C:\WINDOWS\CSC	attributes created deleted renamed	Directory
C:\WINDOWS\Debug	attributes created deleted renamed	Directory
C:\WINDOWS\Registration	attributes created	Directory

	deleted renamed	
C:\WINDOWS\repair	attributes created deleted renamed	Directory
C:\WINDOWS\Debug\UserMode	attributes created deleted renamed	Directory
C:\WINDOWS\System32\appmgmt	attributes created deleted renamed	Directory
C:\WINDOWS\config	attributes created deleted renamed	Directory
C:\WINDOWS\System32\DTCLLog	attributes created deleted renamed	Directory
C:\WINDOWS\System32\GroupPolicy	attributes created deleted renamed	Directory
C:\WINDOWS\System32\ias	attributes created deleted renamed	Directory
C:\WINDOWS\System32\NTMSData	attributes created deleted renamed	Directory
C:\WINDOWS\System32\reinstallbackups	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Setup	attributes created deleted renamed	Directory
C:\WINDOWS\System32\at.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\drwatson.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\drwtsn32.exe	attributes created	File

	deleted renamed	
C:\WINDOWS\System32\ledlin.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\net.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\reg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\regedt32.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\rexec.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\subst.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\telnet.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\spool\printers	attributes created deleted renamed	Directory
C:\Program Files\Resource Kit	attributes created deleted renamed	Directory
C:\WINDOWS\System32\rsh.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\dlldata	attributes created deleted renamed	Directory
C:\WINDOWS\security	attributes created deleted renamed	Directory

C:\WINDOWS\System32\cacs.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\debug.exe	attributes created deleted hash renamed size	File
C:\Temp	attributes created deleted renamed	Directory
C:\AUTOEXEC.BAT	attributes created deleted hash renamed size	File
C:\boot.ini	attributes created deleted hash renamed size	File
C:\config.sys	attributes created deleted hash renamed size	File
C:\io.sys	attributes created deleted hash renamed size	File
C:\msdos.sys	attributes created deleted hash renamed size	File
C:\ntbootdd.sys	attributes created deleted hash renamed size	File

C:\ntdetect.com	attributes created deleted hash renamed size	File
C:\ntldr	attributes created deleted renamed	Directory
C:\WINDOWS\System32\arp.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\nbtstat.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\netstat.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\nslookup.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ntbackup.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\regini.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\route.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\secedit.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\systeminfo.exe	attributes created deleted renamed	File
C:\Documents and Settings\All Users\Application Data\Microsoft\Media Index	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Application Data\Microsoft\User Account Pictures\guest.bmp	attributes created	File

	deleted renamed	
C:\Documents and Settings\All Users\DRM	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Documents	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\DRM\drmrv2.lic	attributes created deleted renamed	File
C:\Documents and Settings\All Users\DRM\drmrv2.sst	attributes created deleted renamed	File
C:\Documents and Settings\All Users\Application Data	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\DSS\MachineKeys	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys	attributes created deleted renamed	Directory
C:\WINDOWS\System32\append.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\chkdsk.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\chkntfs.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\cipher.exe	attributes created deleted renamed	File
C:\Programdata	attributes created deleted renamed	Directory
C:\WINDOWS\System32\CCM\Cache	attributes created	Directory

	deleted renamed	
C:\WINDOWS\System32\CCM\Cache\skpswi.dat	attributes created deleted renamed	File
C:\WINDOWS\System32\CCM\Inventory\idmifs	attributes created deleted renamed	Directory
C:\WINDOWS\System32\CCM\Inventory\noidmifs	attributes created deleted renamed	Directory
C:\WINDOWS\System32\CCM\Logs	attributes created deleted renamed	Directory
C:\WINDOWS\Debug\WPD	attributes created deleted renamed	Directory
C:\WINDOWS\PCHealth\ERRORREP\QHEADLES	attributes created deleted renamed	Directory
C:\WINDOWS\PCHealth\ERRORREP\QSIGNOFF	attributes created deleted renamed	Directory
C:\WINDOWS\Registration\CRMLog	attributes created deleted renamed	Directory
C:\WINDOWS\Debug\WIA	attributes created deleted renamed	Directory
C:\WINDOWS\System32\FxsTmp	attributes created deleted renamed	Directory
C:\WINDOWS\System32\com\dmp	attributes created deleted renamed	Directory
C:\WINDOWS\System32\spool\drivers\color	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Tasks	attributes created	Directory

	deleted renamed	
C:\WINDOWS\System32\Tasks\Microsoft\Windows\PLA\System	attributes created deleted renamed	Directory
C:\WINDOWS\tracing	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Tasks\Microsoft\Windows\WindowsCalendar	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Microsoft\Crypto\RSA\MachineKeys	attributes created deleted renamed	Directory
C:\WINDOWS\System32\eventtriggers.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\netsh.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\sc.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\regsvr32.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\lftp.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\attrib.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\ftp.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\net1.exe	attributes created	File

	deleted hash renamed size	
C:\WINDOWS\System32\rcp.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\runas.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32	attributes created deleted renamed	Directory
C:\WINDOWS\regedit.exe	attributes created deleted renamed	File
C:\users\All Users\Microsoft\Media Index	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\User Account Pictures	attributes created deleted renamed	Directory
C:\users\All users\Microsoft\User Account Pictures\Default Pictures	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\Crypto\DSS\MachineKeys	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\Crypto\RSA\MachineKeys	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\DRM\Server	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\Windows\DRM	attributes created deleted renamed	Directory

C:\users\All Users\Microsoft\Windows\DRM\Cache	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\leHome	attributes created deleted renamed	Directory
C:\users\Public\Recorded TV	attributes created deleted renamed	Directory
C:\users\Public\Recorded TV\Sample Media	attributes created deleted renamed	Directory
C:\WINDOWS\System32\ACW.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\alg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\AtBroker.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\audiodg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\autoconv.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\autofmt.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\bcdedit.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\BitLockerWizard.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\bitsadmin.exe	attributes created deleted renamed	File

C:\WINDOWS\System32\bootcfg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\cmdkey.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\DFDWiz.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dfmgfat.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dfmgfc.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dfmgui.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dfsrm.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dialer.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\diskpart.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dispdiag.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\eventcreate.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\FirewallControlPanel.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\FirewallSettings.exe	attributes created deleted renamed	File

C:\WINDOWS\System32\getmac.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\icacls.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\mobsync.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\MRINFO.EXE	attributes created deleted renamed	File
C:\WINDOWS\System32\mrt.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\rekeywiz.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\Robocopy.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\Rcping.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\schtasks.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\sysedit.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesAdvanced.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesComputerName.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesDataExecutionPrevention.exe	attributes created deleted renamed	File

C:\WINDOWS\System32\SystemPropertiesHardware.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesPerformance.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesProtection.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesRemote.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\systray.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\takeown.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tracert.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tscupgrd.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tsdiscon.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tskill.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tsshutdn.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\Utilman.exe	attributes created deleted renamed	File
C:\Windows	attributes created deleted renamed	Directory

O-00010: [MS- Windows- 2016] Files and Directories	Windows	C:\WINDOWS\System32\winmsd.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\wscript.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\xcopy.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\cluster.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\cmd.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\compact.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\command.com	attributes created deleted renamed	File
		C:\WINDOWS\System32\convert.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\cscript.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\dfscmd.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\diskcomp.com	attributes created deleted renamed	File
		C:\WINDOWS\System32\diskcopy.com	attributes created deleted renamed	File
		C:\WINDOWS\System32\doskey.exe	attributes created deleted renamed	File

C:\WINDOWS\System32\exe2bin.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\expand.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\fc.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\find.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\findstr.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\finger.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\forcedos.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\format.com	attributes created deleted renamed	File
C:\WINDOWS\System32\hostname.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\iisreset.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ipconfig.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ipxroute.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\label.exe	attributes created deleted renamed	File

C:\WINDOWS\System32\logoff.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\makecab.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\mem.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\mmc.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\mountvol.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\msiexec.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\msg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ntsd.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\pathping.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ping.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\rasdial.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\recover.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\replace.exe	attributes created deleted renamed	File

C:\WINDOWS\System32\reset.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\routemon.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\runonce.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\shadow.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\share.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\syskey.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\taskmgr.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tlntsess.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tlntsvr.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tracert.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tree.com	attributes created deleted renamed	File
C:\WINDOWS\System32\tsadmin.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tscon.exe	attributes created deleted renamed	File

C:\WINDOWS\system32\mshta.exe	attributes created deleted renamed	File
C:\Documents and Settings	attributes created deleted renamed	Directory
C:\Program Files	attributes created deleted renamed	Directory
C:\Documents and Settings\Administrator	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Documents\DrWatson	attributes created deleted renamed	Directory
C:\Documents and Settings\Default User	attributes created deleted renamed	Directory
C:\WINDOWS\Temp	attributes created deleted renamed	Directory
C:\WINDOWS\$NtServicePackUninstall\$	attributes created deleted renamed	Directory
C:\WINDOWS\CSC	attributes created deleted renamed	Directory
C:\WINDOWS\Debug	attributes created deleted renamed	Directory
C:\WINDOWS\Registration	attributes created deleted renamed	Directory
C:\WINDOWS\repair	attributes created deleted renamed	Directory

C:\WINDOWS\Debug\UserMode	attributes created deleted renamed	Directory
C:\WINDOWS\System32\lppmgmt	attributes created deleted renamed	Directory
C:\WINDOWS\config	attributes created deleted renamed	Directory
C:\WINDOWS\System32\DTCLog	attributes created deleted renamed	Directory
C:\WINDOWS\System32\GroupPolicy	attributes created deleted renamed	Directory
C:\WINDOWS\System32\ias	attributes created deleted renamed	Directory
C:\WINDOWS\System32\NTMSData	attributes created deleted renamed	Directory
C:\WINDOWS\System32\reinstallbackups	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Setup	attributes created deleted renamed	Directory
C:\WINDOWS\System32\at.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\drwatson.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\drwtsn32.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\edlin.exe	attributes created deleted renamed	File

C:\WINDOWS\System32\net.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\reg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\regedt32.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\rexec.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\subst.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\telnet.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\spool\printers	attributes created deleted renamed	Directory
C:\Program Files\Resource Kit	attributes created deleted renamed	Directory
C:\WINDOWS\System32\rsh.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\dlldata	attributes created deleted renamed	Directory
C:\WINDOWS\security	attributes created deleted renamed	Directory
C:\WINDOWS\System32\cacls.exe	attributes created deleted hash renamed size	File

C:\WINDOWS\System32\debug.exe	attributes created deleted hash renamed size	File
C:\Temp	attributes created deleted renamed	Directory
C:\AUTOEXEC.BAT	attributes created deleted hash renamed size	File
C:\boot.ini	attributes created deleted hash renamed size	File
C:\config.sys	attributes created deleted hash renamed size	File
C:\io.sys	attributes created deleted hash renamed size	File
C:\msdos.sys	attributes created deleted hash renamed size	File
C:\ntbootdd.sys	attributes created deleted hash renamed size	File
C:\ntdetect.com	attributes created deleted hash renamed size	File

C:\ntldr	attributes created deleted renamed	Directory
C:\WINDOWS\System32\arp.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\nbtstat.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\netstat.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\nslookup.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ntbackup.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\regini.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\route.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\secedit.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\systeminfo.exe	attributes created deleted renamed	File
C:\Documents and Settings\All Users\Application Data\Microsoft\Media Index	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Application Data\Microsoft\User Account Pictures\guest.bmp	attributes created deleted renamed	File
C:\Documents and Settings\All Users\DRM	attributes created deleted renamed	Directory

C:\Documents and Settings\All Users\Documents	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\DRM\drmrv2.lic	attributes created deleted renamed	File
C:\Documents and Settings\All Users\DRM\drmrv2.sst	attributes created deleted renamed	File
C:\Documents and Settings\All Users\Application Data	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\DSS\MachineKeys	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys	attributes created deleted renamed	Directory
C:\WINDOWS\System32\append.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\chkdsk.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\chkntfs.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\cipher.exe	attributes created deleted renamed	File
C:\Programdata	attributes created deleted renamed	Directory
C:\WINDOWS\System32\CCM\Cache	attributes created deleted renamed	Directory
C:\WINDOWS\System32\CCM\Cache\skpswi.dat	attributes created deleted renamed	File

C:\WINDOWS\System32\CCM\Inventory\idmifs	attributes created deleted renamed	Directory
C:\WINDOWS\System32\CCM\Inventory\noidmifs	attributes created deleted renamed	Directory
C:\WINDOWS\System32\CCM\Logs	attributes created deleted renamed	Directory
C:\WINDOWS\Debug\WPD	attributes created deleted renamed	Directory
C:\WINDOWS\PCHealth\ERRORREP\QHEADLES	attributes created deleted renamed	Directory
C:\WINDOWS\PCHealth\ERRORREP\QSIGNOFF	attributes created deleted renamed	Directory
C:\WINDOWS\Registration\CRMLog	attributes created deleted renamed	Directory
C:\WINDOWS\Debug\WIA	attributes created deleted renamed	Directory
C:\WINDOWS\System32\FxsTmp	attributes created deleted renamed	Directory
C:\WINDOWS\System32\com\dmp	attributes created deleted renamed	Directory
C:\WINDOWS\System32\spool\drivers\color	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Tasks	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Tasks\Microsoft\Windows\PLA\System	attributes created deleted renamed	Directory

C:\WINDOWS\tracing	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Tasks\Microsoft\Windows\WindowsCalendar	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Microsoft\Crypto\RSA\MachineKeys	attributes created deleted renamed	Directory
C:\WINDOWS\System32\eventtriggers.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\netsh.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\sc.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\regsvr32.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ftpsvc.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\attrib.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\ftp.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\net1.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\rpc.exe	attributes created deleted	File

	hash renamed size	
C:\WINDOWS\System32\runas.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32	attributes created deleted renamed	Directory
C:\WINDOWS\regedit.exe	attributes created deleted renamed	File
C:\users\All Users\Microsoft\Media Index	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\User Account Pictures	attributes created deleted renamed	Directory
C:\users\All users\Microsoft\User Account Pictures\Default Pictures	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\Crypto\DSS\MachineKeys	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\Crypto\RSA\MachineKeys	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\DRM\Server	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\Windows\DRM	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\Windows\DRM\Cache	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\leHome	attributes created	Directory

	deleted renamed	
C:\users\Public\Recorded TV	attributes created deleted renamed	Directory
C:\users\Public\Recorded TV\Sample Media	attributes created deleted renamed	Directory
C:\WINDOWS\System32\ACW.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\alg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\AtBroker.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\audiodg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\autoconv.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\autofmt.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\bcdedit.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\BitLockerWizard.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\bitsadmin.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\bootcfg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\cmdkey.exe	attributes created	File

	deleted renamed	
C:\WINDOWS\System32\DFDWiz.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dfrgfat.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dfrgfc.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dfrgui.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dfsrmgr.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dialer.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\diskpart.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dispdiag.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\eventcreate.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\FirewallControlPanel.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\FirewallSettings.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\getmac.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\icacls.exe	attributes created	File

	deleted renamed	
C:\WINDOWS\System32\mobsync.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\MRINFO.EXE	attributes created deleted renamed	File
C:\WINDOWS\System32\mrt.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\rekeywiz.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\Robocopy.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\Rcping.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\schtasks.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\sysedit.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesAdvanced.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesComputerName.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesDataExecutionPrevention.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesHardware.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesPerformance.exe	attributes created	File

			deleted renamed	
		C:\WINDOWS\System32\SystemPropertiesProtection.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\SystemPropertiesRemote.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\systray.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\takeown.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\tracert.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\tscupgrd.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\tsdiscon.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\tskill.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\tsshutdn.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\Utilman.exe	attributes created deleted renamed	File
		C:\Windows	attributes created deleted renamed	Directory
O-00011: [MS- Windows- 2019] Files and Directories	Windows	C:\WINDOWS\System32\winmsd.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\wscript.exe	attributes created	File

	deleted renamed	
C:\WINDOWS\System32\xcopy.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\cluster.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\cmd.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\compact.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\command.com	attributes created deleted renamed	File
C:\WINDOWS\System32\convert.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\cscript.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dfscmd.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\diskcomp.com	attributes created deleted renamed	File
C:\WINDOWS\System32\diskcopy.com	attributes created deleted renamed	File
C:\WINDOWS\System32\doskey.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\exe2bin.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\expand.exe	attributes created	File

	deleted renamed	
C:\WINDOWS\System32\fc.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\find.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\findstr.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\finger.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\forcedos.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\format.com	attributes created deleted renamed	File
C:\WINDOWS\System32\hostname.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\iisreset.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ipconfig.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ipxroute.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\label.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\logoff.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\makecab.exe	attributes created	File

	deleted renamed	
C:\WINDOWS\System32\mem.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\mmc.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\mountvol.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\msiexec.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\msg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ntsd.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\pathping.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ping.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\rasdial.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\recover.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\replace.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\reset.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\routemon.exe	attributes created	File

	deleted renamed	
C:\WINDOWS\System32\runonce.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\shadow.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\share.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\syskey.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\taskmgr.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tlntsess.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tlntsvr.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tracert.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tree.com	attributes created deleted renamed	File
C:\WINDOWS\System32\tsadmin.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tscon.exe	attributes created deleted renamed	File
C:\WINDOWS\system32\mshta.exe	attributes created deleted renamed	File
C:\Documents and Settings	attributes created	Directory

	deleted renamed	
C:\Program Files	attributes created deleted renamed	Directory
C:\Documents and Settings\Administrator	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Documents\DrWatson	attributes created deleted renamed	Directory
C:\Documents and Settings\Default User	attributes created deleted renamed	Directory
C:\WINDOWS\Temp	attributes created deleted renamed	Directory
C:\WINDOWS\\$NtServicePackUninstall\$	attributes created deleted renamed	Directory
C:\WINDOWS\CSC	attributes created deleted renamed	Directory
C:\WINDOWS\Debug	attributes created deleted renamed	Directory
C:\WINDOWS\Registration	attributes created deleted renamed	Directory
C:\WINDOWS\repair	attributes created deleted renamed	Directory
C:\WINDOWS\Debug\UserMode	attributes created deleted renamed	Directory
C:\WINDOWS\System32\appmgmt	attributes created	Directory

	deleted renamed	
C:\WINDOWS\config	attributes created deleted renamed	Directory
C:\WINDOWS\System32\DTCLLog	attributes created deleted renamed	Directory
C:\WINDOWS\System32\GroupPolicy	attributes created deleted renamed	Directory
C:\WINDOWS\System32\ias	attributes created deleted renamed	Directory
C:\WINDOWS\System32\NTMSData	attributes created deleted renamed	Directory
C:\WINDOWS\System32\reinstallbackups	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Setup	attributes created deleted renamed	Directory
C:\WINDOWS\System32\at.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\drwatson.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\drwtsn32.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\edlin.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\net.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\reg.exe	attributes created	File

	deleted renamed	
C:\WINDOWS\System32\regedt32.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\rexec.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\subst.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\telnet.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\spool\printers	attributes created deleted renamed	Directory
C:\Program Files\Resource Kit	attributes created deleted renamed	Directory
C:\WINDOWS\System32\rsh.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\dlldata	attributes created deleted renamed	Directory
C:\WINDOWS\security	attributes created deleted renamed	Directory
C:\WINDOWS\System32\cacs.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\debug.exe	attributes created deleted hash renamed size	File

C:\Temp	attributes created deleted renamed	Directory
C:\AUTOEXEC.BAT	attributes created deleted hash renamed size	File
C:\boot.ini	attributes created deleted hash renamed size	File
C:\config.sys	attributes created deleted hash renamed size	File
C:\io.sys	attributes created deleted hash renamed size	File
C:\msdos.sys	attributes created deleted hash renamed size	File
C:\ntbootdd.sys	attributes created deleted hash renamed size	File
C:\ntdetect.com	attributes created deleted hash renamed size	File
C:\ntldr	attributes created deleted renamed	Directory
C:\WINDOWS\System32\arp.exe	attributes created	File

	deleted renamed	
C:\WINDOWS\System32\nbtstat.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\netstat.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\nslookup.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ntbackup.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\regini.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\route.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\secedit.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\systeminfo.exe	attributes created deleted renamed	File
C:\Documents and Settings\All Users\Application Data\Microsoft\Media Index	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Application Data\Microsoft\User Account Pictures\guest.bmp	attributes created deleted renamed	File
C:\Documents and Settings\All Users\DRM	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Documents	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\DRM\drm2.lic	attributes created	File

	deleted renamed	
C:\Documents and Settings\All Users\DRM\drm2.sst	attributes created deleted renamed	File
C:\Documents and Settings\All Users\Application Data	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\DSS\MachineKeys	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys	attributes created deleted renamed	Directory
C:\WINDOWS\System32\append.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\chkdsk.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\chkntfs.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\cipher.exe	attributes created deleted renamed	File
C:\Programdata	attributes created deleted renamed	Directory
C:\WINDOWS\System32\CCM\Cache	attributes created deleted renamed	Directory
C:\WINDOWS\System32\CCM\Cache\skpswi.dat	attributes created deleted renamed	File
C:\WINDOWS\System32\CCM\Inventory\idmifs	attributes created deleted renamed	Directory
C:\WINDOWS\System32\CCM\Inventory\noidmifs	attributes created	Directory

	deleted renamed	
C:\WINDOWS\System32\CCMLogs	attributes created deleted renamed	Directory
C:\WINDOWS\Debug\WPD	attributes created deleted renamed	Directory
C:\WINDOWS\PCHealth\ERRORREP\QHEADLES	attributes created deleted renamed	Directory
C:\WINDOWS\PCHealth\ERRORREP\QSIGNOFF	attributes created deleted renamed	Directory
C:\WINDOWS\Registration\CRMLog	attributes created deleted renamed	Directory
C:\WINDOWS\Debug\WIA	attributes created deleted renamed	Directory
C:\WINDOWS\System32\FxsTmp	attributes created deleted renamed	Directory
C:\WINDOWS\System32\com\dmp	attributes created deleted renamed	Directory
C:\WINDOWS\System32\spool\drivers\color	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Tasks	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Tasks\Microsoft\Windows\PLA\System	attributes created deleted renamed	Directory
C:\WINDOWS\tracing	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Tasks\Microsoft\Windows\WindowsCalendar	attributes created	Directory

	deleted renamed	
C:\WINDOWS\System32\Microsoft\Crypto\RSA\MachineKeys	attributes created deleted renamed	Directory
C:\WINDOWS\System32\eventtriggers.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\netsh.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\sc.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\regsvr32.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\lftp.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\attrib.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\lftp.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\net1.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\rpc.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\runas.exe	attributes created deleted	File

	hash renamed size	
C:\WINDOWS\System32	attributes created deleted renamed	Directory
C:\WINDOWS\regedit.exe	attributes created deleted renamed	File
C:\users\All Users\Microsoft\Media Index	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\User Account Pictures	attributes created deleted renamed	Directory
C:\users\All users\Microsoft\User Account Pictures\Default Pictures	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\Crypto\DSS\MachineKeys	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\Crypto\RSA\MachineKeys	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\DRM\Server	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\Windows\DRM	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\Windows\DRM\Cache	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\leHome	attributes created deleted renamed	Directory
C:\users\Public\Recorded TV	attributes created deleted renamed	Directory

C:\users\Public\Recorded TV\Sample Media	attributes created deleted renamed	Directory
C:\WINDOWS\System32\ACW.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\alg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\AtBroker.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\audiodg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\autoconv.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\autofmt.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\bcdedit.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\BitLockerWizard.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\bitsadmin.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\bootcfg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\cmdkey.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\DFDWiz.exe	attributes created deleted renamed	File

C:\WINDOWS\System32\dfmgfat.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dfmgfsc.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dfmgui.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dfsrmgr.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dialer.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\diskpart.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dispdiag.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\eventcreate.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\FirewallControlPanel.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\FirewallSettings.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\getmac.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\icacls.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\mobsync.exe	attributes created deleted renamed	File

C:\WINDOWS\System32\MRINFO.EXE	attributes created deleted renamed	File
C:\WINDOWS\System32\mrt.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\rekeywiz.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\Robocopy.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\Rpcping.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\schtasks.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\sysedit.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesAdvanced.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesComputerName.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesDataExecutionPrevention.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesHardware.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesPerformance.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesProtection.exe	attributes created deleted renamed	File

		C:\WINDOWS\System32\SystemPropertiesRemote.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\systray.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\takeown.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\tracert.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\tscupgrd.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\tsdiscon.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\tskill.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\tsshutdn.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\Utilman.exe	attributes created deleted renamed	File
		C:\Windows	attributes created deleted renamed	Directory
O-00012: [MS- Windows-7] Files and Directories	Windows	C:\WINDOWS\System32\winmsd.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\wscript.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\xcopy.exe	attributes created deleted renamed	File

C:\WINDOWS\System32\cluster.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\cmd.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\compact.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\command.com	attributes created deleted renamed	File
C:\WINDOWS\System32\convert.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\cscript.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dfscmd.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\diskcomp.com	attributes created deleted renamed	File
C:\WINDOWS\System32\diskcopy.com	attributes created deleted renamed	File
C:\WINDOWS\System32\doskey.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\exe2bin.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\expand.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\fc.exe	attributes created deleted renamed	File

C:\WINDOWS\System32\find.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\findstr.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\finger.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\forcedos.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\format.com	attributes created deleted renamed	File
C:\WINDOWS\System32\hostname.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\iisreset.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ipconfig.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ipxroute.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\label.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\logoff.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\makecab.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\mem.exe	attributes created deleted renamed	File

C:\WINDOWS\System32\mmc.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\mountvol.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\msiexec.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\msg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ntsd.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\pathping.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ping.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\rasdial.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\recover.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\replace.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\reset.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\routemon.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\runonce.exe	attributes created deleted renamed	File

C:\WINDOWS\System32\shadow.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\share.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\syskey.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\taskmgr.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tlntsess.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tlntsvr.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tracert.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tree.com	attributes created deleted renamed	File
C:\WINDOWS\System32\tsadmin.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\tscon.exe	attributes created deleted renamed	File
C:\WINDOWS\system32\mshta.exe	attributes created deleted renamed	File
C:\Documents and Settings	attributes created deleted renamed	Directory
C:\Program Files	attributes created deleted renamed	Directory

C:\Documents and Settings\Administrator	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Documents\DrWatson	attributes created deleted renamed	Directory
C:\Documents and Settings\Default User	attributes created deleted renamed	Directory
C:\WINDOWS\Temp	attributes created deleted renamed	Directory
C:\WINDOWS\\$NtServicePackUninstall\$	attributes created deleted renamed	Directory
C:\WINDOWS\CSC	attributes created deleted renamed	Directory
C:\WINDOWS\Debug	attributes created deleted renamed	Directory
C:\WINDOWS\Registration	attributes created deleted renamed	Directory
C:\WINDOWS\repair	attributes created deleted renamed	Directory
C:\WINDOWS\Debug\UserMode	attributes created deleted renamed	Directory
C:\WINDOWS\System32\appmgmt	attributes created deleted renamed	Directory
C:\WINDOWS\config	attributes created deleted renamed	Directory

C:\WINDOWS\System32\DTCLLog	attributes created deleted renamed	Directory
C:\WINDOWS\System32\GroupPolicy	attributes created deleted renamed	Directory
C:\WINDOWS\System32\ias	attributes created deleted renamed	Directory
C:\WINDOWS\System32\NTMSData	attributes created deleted renamed	Directory
C:\WINDOWS\System32\reinstallbackups	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Setup	attributes created deleted renamed	Directory
C:\WINDOWS\System32\lat.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\drwatson.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\drwtsn32.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\edlin.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\net.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\reg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\regedt32.exe	attributes created deleted renamed	File

C:\WINDOWS\System32\rexec.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\subst.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\telnet.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\spool\printers	attributes created deleted renamed	Directory
C:\Program Files\Resource Kit	attributes created deleted renamed	Directory
C:\WINDOWS\System32\rsh.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\dlldata	attributes created deleted renamed	Directory
C:\WINDOWS\security	attributes created deleted renamed	Directory
C:\WINDOWS\System32\cacls.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\debug.exe	attributes created deleted hash renamed size	File
C:\Temp	attributes created deleted renamed	Directory
C:\AUTOEXEC.BAT	attributes created deleted	File

	hash renamed size	
C:\boot.ini	attributes created deleted hash renamed size	File
C:\config.sys	attributes created deleted hash renamed size	File
C:\io.sys	attributes created deleted hash renamed size	File
C:\msdos.sys	attributes created deleted hash renamed size	File
C:\ntbootdd.sys	attributes created deleted hash renamed size	File
C:\ntdetect.com	attributes created deleted hash renamed size	File
C:\ntldr	attributes created deleted renamed	Directory
C:\WINDOWS\System32\arp.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\nbtstat.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\netstat.exe	attributes created	File

	deleted renamed	
C:\WINDOWS\System32\lslookup.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\ntbackup.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\regini.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\route.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\secedit.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\systeminfo.exe	attributes created deleted renamed	File
C:\Documents and Settings\All Users\Application Data\Microsoft\Media Index	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Application Data\Microsoft\User Account Pictures\guest.bmp	attributes created deleted renamed	File
C:\Documents and Settings\All Users\DRM	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Documents	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\DRM\drm2.lic	attributes created deleted renamed	File
C:\Documents and Settings\All Users\DRM\drm2.sst	attributes created deleted renamed	File
C:\Documents and Settings\All Users\Application Data	attributes created	Directory

	deleted renamed	
C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\DSS\MachineKeys	attributes created deleted renamed	Directory
C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys	attributes created deleted renamed	Directory
C:\WINDOWS\System32\append.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\chkdsk.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\chkntfs.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\cipher.exe	attributes created deleted renamed	File
C:\Programdata	attributes created deleted renamed	Directory
C:\WINDOWS\System32\CCM\Cache	attributes created deleted renamed	Directory
C:\WINDOWS\System32\CCM\Cache\skpswi.dat	attributes created deleted renamed	File
C:\WINDOWS\System32\CCM\Inventory\idmifs	attributes created deleted renamed	Directory
C:\WINDOWS\System32\CCM\Inventory\noidmifs	attributes created deleted renamed	Directory
C:\WINDOWS\System32\CCM\Logs	attributes created deleted renamed	Directory
C:\WINDOWS\Debug\WPD	attributes created	Directory

	deleted renamed	
C:\WINDOWS\PCHealth\ERRORREP\QHEADLES	attributes created deleted renamed	Directory
C:\WINDOWS\PCHealth\ERRORREP\QSIGNOFF	attributes created deleted renamed	Directory
C:\WINDOWS\Registration\CRMLog	attributes created deleted renamed	Directory
C:\WINDOWS\Debug\WIA	attributes created deleted renamed	Directory
C:\WINDOWS\System32\FxsTmp	attributes created deleted renamed	Directory
C:\WINDOWS\System32\com\dmp	attributes created deleted renamed	Directory
C:\WINDOWS\System32\spool\drivers\color	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Tasks	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Tasks\Microsoft\Windows\PLA\System	attributes created deleted renamed	Directory
C:\WINDOWS\tracing	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Tasks\Microsoft\Windows\WindowsCalendar	attributes created deleted renamed	Directory
C:\WINDOWS\System32\Microsoft\Crypto\RSA\MachineKeys	attributes created deleted renamed	Directory
C:\WINDOWS\System32\eventtriggers.exe	attributes created	File

	deleted renamed	
C:\WINDOWS\System32\netsh.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\sc.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\regsvr32.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\lftp.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\attrib.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\lftp.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\net1.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\rpc.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32\rundll32.exe	attributes created deleted hash renamed size	File
C:\WINDOWS\System32	attributes created deleted renamed	Directory

C:\WINDOWS\regedit.exe	attributes created deleted renamed	File
C:\users\All Users\Microsoft\Media Index	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\User Account Pictures	attributes created deleted renamed	Directory
C:\users\All users\Microsoft\User Account Pictures\Default Pictures	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\Crypto\DSS\MachineKeys	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\Crypto\RSA\MachineKeys	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\DRM\Server	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\Windows\DRM	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\Windows\DRM\Cache	attributes created deleted renamed	Directory
C:\users\All Users\Microsoft\leHome	attributes created deleted renamed	Directory
C:\users\Public\Recorded TV	attributes created deleted renamed	Directory
C:\users\Public\Recorded TV\Sample Media	attributes created deleted renamed	Directory
C:\WINDOWS\System32\ACW.exe	attributes created deleted renamed	File

C:\WINDOWS\System32\alg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\AtBroker.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\audiodg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\autoconv.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\autofmt.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\bcdedit.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\BitLockerWizard.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\bitsadmin.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\bootcfg.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\cmdkey.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\DFDWiz.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dfrgfat.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dfrgifc.exe	attributes created deleted renamed	File

C:\WINDOWS\System32\dfgui.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dfsrmgr.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dialer.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\diskpart.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\dispdiag.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\eventcreate.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\FirewallControlPanel.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\FirewallSettings.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\getmac.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\icacls.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\mobsync.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\MRINFO.EXE	attributes created deleted renamed	File
C:\WINDOWS\System32\mrt.exe	attributes created deleted renamed	File

C:\WINDOWS\System32\rekeywiz.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\Robocopy.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\Rcping.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\schtasks.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\sysedit.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesAdvanced.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesComputerName.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesDataExecutionPrevention.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesHardware.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesPerformance.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesProtection.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\SystemPropertiesRemote.exe	attributes created deleted renamed	File
C:\WINDOWS\System32\systray.exe	attributes created deleted renamed	File

		C:\WINDOWS\System32\takeown.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\tracert.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\tscupgrd.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\tsdiscon.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\tskill.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\tsshutdn.exe	attributes created deleted renamed	File
		C:\WINDOWS\System32\Utilman.exe	attributes created deleted renamed	File
		C:\Windows	attributes created deleted renamed	Directory
O-00019: [Mitre Matrix] Masquerading	Windows	C:\Windows\System32\wscript.exe	attributes created deleted renamed	File
		C:\Windows\System32\mshta.exe	attributes created deleted renamed	File
O-00020: [Mitre Matrix] Scheduled Task/Job on Windows	Windows	HKLM\SYSTEM\CurrentControlSet\Control\Lsa\submitcontrol	hash last_modified	RegistryValue
O-00021: [Mitre Matrix] Registry Modification Attacks	Windows	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer	values	RegistryKey
		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DRM	values	RegistryKey
		HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office	values	RegistryKey
		HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	values	RegistryKey
		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers	values	RegistryKey

O-00022: [Mitre Matrix] Event Triggered Execution on Windows	Windows	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Security	values	RegistryKey
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest	values	RegistryKey
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\NullSessionPipes	hash last_modified	RegistryValue
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\BootExecute	hash last_modified	RegistryValue
	Windows	C:\WINDOWS\System32\Utilman.exe	attributes created deleted hash renamed	File
		C:\Windows\System32\sethc.exe	attributes created deleted hash renamed	File
		C:\Windows\System32\lsk.exe	attributes created deleted hash renamed	File
		C:\Windows\System32\Magnify.exe	attributes created deleted hash renamed	File
		C:\Windows\System32\Narrator.exe	attributes created deleted hash renamed	File
		C:\Windows\System32\DisplaySwitch.exe	attributes created deleted hash renamed	File
		C:\Windows\System32\AtBroker.exe	attributes created deleted hash renamed	File
		HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts	values	RegistryKey
		HKEY_CURRENT_USER\Control Panel\Desktop	values	RegistryKey
		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NetSh	values	RegistryKey
		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	values	RegistryKey
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager	values	RegistryKey
		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows	values	RegistryKey
		HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Windows	values	RegistryKey
		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Custom	values	RegistryKey
		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\LoadAppInit_DLLs	hash last_modified	RegistryValue

		HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Windows\ApplInit_DLLs	hash last_modified	RegistryValue
		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\ApplInit_DLLs	hash last_modified	RegistryValue
		HKEY_CURRENT_USER\Control Panel\Desktop\ScreenSaveActive	hash last_modified	RegistryValue
O-00023: [Mitre Matrix] Boot or Logon Autostart Execution on Windows	Windows	C:\Windows\System32\spool\prtprocs\x64\winprint.dll	attributes created deleted hash renamed	File
		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost	values	RegistryKey
		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	values	RegistryKey
		HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	values	RegistryKey
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa	values	RegistryKey
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders	values	RegistryKey
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Monitors	values	RegistryKey
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Monitors\Local Port	values	RegistryKey
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Monitors\Standard TCP/IP Port	values	RegistryKey
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Monitors\USB Monitor	values	RegistryKey
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Monitors\WSD Port	values	RegistryKey
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Environments\Windows x64\Print Processors	values	RegistryKey
		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components	values	RegistryKey
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\BootExecute	hash last_modified	RegistryValue
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Authentication Packages	hash last_modified	RegistryValue
O-00024: [Mitre Matrix] Abuse Elevation Control Mechanism	Windows	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\ms-settings\Shell\Open\Command	values	RegistryKey
		HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shell\runas\command\IsolatedCommand	hash last_modified	RegistryValue
O-00025: [Mitre Matrix] Adversary-in- the-Middle	Windows	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient	values	RegistryKey
O-00026: [Mitre Matrix] Impair Defenses	Windows	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\AMSI\Providers	deleted values	RegistryKey
		HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender	values	RegistryKey
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile	values	RegistryKey
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy	values	RegistryKey
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl	values	RegistryKey
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl\CrashDumpEnabled	hash last_modified	RegistryValue

O-00031: Windows User Activity	Windows *		created deleted	User
O-00033: [MS- Windows] Windows Hosts File	Windows	C:\WINDOWS\System32\drivers\etc\hosts	attributes created deleted renamed hash size	File