- \\registry\machine\system\controlset001\services\vboxservice
- \\registry\machine\system\controlset003\control\safeboot
- \\registry\user\%user%\software\policies\microsoft\office
- \\registry\machine\system\controlset001\control\lsa\skew1
- \\registry\user\%user%\software\wow6432node\microsoft\active setup\installed components
- \\registry\machine\software\policies\google\chrome\extensioninstallforcelist
- \\registry\machine\system\currentcontrolset001\services\physmem2profit
- \\registry\machine\system\controlset002\control\safeboot
- \\registry\user\%user%\software\microsoft\command processor
- \\registry\machine\system\controlset003\control\bootverificationprogram
- \\registry\machine\software\wow6432node\teamviewer
- \\registry\user\%user%\software\microsoft\windows\currentversion\run
- \\registry\machine\software\microsoft\windows\currentversion\controls folder
- \\registry\machine\system\controlset001\control\terminal server\fdenytsconnections
- \\registry\machine\system\currentcontrolset\services
- \\software\microsoft\windows\currentversion\run
- \\registry\machine\system\currentcontrolset\control\securityproviders\wdigest
- \\registry\user\%user%\software\microsoft\windows\currentversion\runonceobjects
- \\registry\user\%user%\system\currentcontrolset\control\safeboot
- \\registry\machine\software\win6432node\microsoft\windows\currentversion\uninstall
- \\registry\user\%user%\control panel\desktop
- \\registry\user\%user%\software\policies\microsoft\previousversions
- \\registry\machine\software\microsoft\windows nt\currentversion\aedebug
- \\registry\machine\system\windows nt\currentversion\image file execution options\sethc.exe\debugger
- \\registry\machine\system\controlset001\services\vboxguest
- \\registry\user\%user%\software\microsoft\windows\currentversion\policies\system
- \\registry\machine\software\microsoft\virtualmachine
- \\registry\machine\system\controlset001\services\xensvc
- \\registry\machine\software\microsoft\active setup\installed components
- \\registry\machine\software\microsoft\windows nt\currentversion\terminal server\install\software\microsoft\windows\currentversion\run

- \\registry\machine\software\microsoft\windows nt\currentversion\print\printers
- \\registry\machine\software\microsoft\windows\currentversion\run
- \\registry\user\%user%\software\microsoft\windows nt\currentversion\aedebug
- \\registry\user\%user%\software\wannacrypt
- \\registry\user\%user%_classes\exefile\shell\open\command
- \\registry\user\%user%\software\classes\ms-settings\shell\open\command
- \\registry\machine\software\microsoft\cryptography\providers\trust
- \\registry\user\%user%\software\microsoft\windows nt\currentversion\svchost
- \\registry\machine\software\classes\exefile
- \\registry\machine\software\microsoft\security center
- \\registry\machine\system\controlset002\services
- \\registry\user\%user%\software\wow6432node\microsoft\command processor
- \\registry\machine\software\localnetservice
- \\registry\machine\software\microsoft\windows nt\currentversion\winlogon
- \\registry\machine\software\microsoft\windows\currentversion\policies\system
- \\registry\machine\software\microsoft\windows\currentversion\runonceex
- \\registry\user\software\microsoft\windows\currentversion\internet settings
- \\registry\user\%user%\system\currentcontrolset\control\network
- \\registry\machine\security\policy\secrets\$machine.acc
- \\registry\machine\system\currentcontrolset\control\terminal server\fdenytsconnections
- \\registry\machine\system\currentcontrolset\hardwareprofiles
- \\registry\machine\software\wow6432node\microsoft\active setup\installed components
- \\registry\machine\software\microsoft\tracing
- \\registry\user\%user%\software\internetexplorer\appdatalow\software\microsoft\internetexplorer
- \\registry\machine\software\oracle\virtualbox guest additions
- \\registry\machine\system\currentcontrolset\control\bootverificationprogram
- \\registry\user\%user%\software\classes\exefile\shell\open\command
- \\registry\machine\software\microsoft\windows nt\currentversion\terminal server\install\software\microsoft\windows\currentversion\runonceex
- \\registry\machine\sam\sam
- \\registry\machine\software\microsoft\windows nt\currentversion\svchost

- \\registry\user\%user%\software\microsoft\office
- \\registry\machine\software\microsoft\windows\currentversion\shell extensions\approved
- \\registry\machine\software\microsoft\windows nt\currentversion\terminal server\install\software\microsoft\windows\currentversion\runonce
- \\registry\machine\system\controlset002\control\bootverificationprogram
- \\registry\machine\system\controlset001\services\xenvdb
- \\registry\machine\system\controlset002\control\session
- \\registry\user\%user%\software\microsoft\windows\currentversion\contentdeliverymanager
- \\registry\user\%user%\software\microsoft\windows\currentversion\policies\system\consentpromptbehavioradmin
- \\registry\machine\software\wow6432node\localnetservice
- \\registry\machine\software\microsoft\windows nt\currentversion\schedule\configuration
- \\registry\machine\software\microsoft\netsh
- \\registry\machine\software\classes\comfile
- \\registry\machine\system\currentcontrolset\control\print\environments
- \\registry\user\%user%\software\classes\folder\shell\open\command
- \\registry\user\%user%\software\crypto
- \\registry\user\%user%_classes\scripting.dictionary
- \\registry\machine\system\currentcontrolset\control\print\monitors
- \\registry\machine\software\wow6432node\microsoft\windows\currentversion\authentication\plap providers
- \\registry\machine\system\controlset001\control\print\environments
- \\registry\user\%user%\software\wannacrypt0r
- \\registry\user\%user%\software\microsoft\windows\currentversion\apphost
- \\registry\machine\bcd00000000\objects
- \\registry\machine\software\microsoft\cryptography\oid
- \\registry\user\.default\software\microsoft\windows\currentversion\run
- \\registry\user\%user%\software\microsoft\windows\currentversion\shell extensions\approved
- \\registry\machine\system\controlset001\control\safeboot
- \\registry\machine\system\controlset001\control\lsa\jd
- \\registry\machine\system\controlset001\control\lsa\gbg
- \\registry\user\%user%\software\microsoft\windows\currentversion\packagedappxdebug

- \\registry\user\%user%\software\microsoft\windows nt\currentversion\terminal server\install\software\microsoft\windows\currentversion\runonce
- \\registry\user\%user%\software\microsoft\windows\currentversion\internet settings
- \\registry\user\%user%\software\wow6432node\microsoft\windows nt\currentversion\windows
- \\registry\machine\software\classes\folder\shell\open\command
- \\registry\machine\software\microsoft\windows nt\currentversion\appcompatflags\installedsdb
- \\registry\machine\system\currentcontrolset\control\session manager\environment
- \\registry\machine\system\controlset001\control\securityproviders\wdigest
- \\registry\machine\software\win6432node\microsoft\cryptography\providers\trust
- \\registry\user\%user%\environment
- \\registry\user\%user%\software\microsoft\windows\currentversion\explorer\shellserviceobjectdelayload
- \\registry\user\%user%_classes\ms-settings\shell\open\command
- \\registry\machine\software\microsoft\windows defender\exclusions\processes
- \\registry\machine\software\wow6432node\microsoft\windows\currentversion\explorer\browser helper objects
- \\registry\machine\system\controlset001\control\print\monitors
- \\registry\user\%user%\software\wow6432node\microsoft\windows\currentversion\explorer\shellserviceobjectdelayload
- \\registry\machine\software\microsoft\systemcertificates\root\certificates
- \\registry\machine\software\classes\exefile\shell\runas\command\isolatedcommand
- \\registry\user\%user%\software\microsoft\windows\currentversion\runonceex
- \\registry\machine\hardware\description\system
- \\registry\machine\software\wow6432node\microsoft\windows\currentversion\explorer\shellserviceobjectdelayload
- \\registry\machine\hardware\description\system\bios
- \\registry\machine\system\controlset001\services\vpcuhub
- \\registry\machine\software\wow6432node\microsoft\windows\currentversion\explorer\shellexecutehooks
- \\registry\user\%user%\system\controlset002\control\safeboot
- \\registry\user\%user%\software\wow6432node\microsoft\windows nt\currentversion\drivers32
- \\registry\machine\software\microsoft\drm
- \\registry\user\%user%\software\classes\clsid
- \\registry\machine\software\classes\.bat
- \\registry\machine\system\controlset001\control\lsa
- \\registry\user\%user%\software\microsoft\windows\currentversion\policies\system\promptonsecuredesktop

- \\registry\machine\hardware\acpi\fadt
- \\registry\user\%user%\software\wow6432node\microsoft\windows nt\currentversion\winlogon
- \\registry\machine\system\controlset001\services\vmtools
- \\registry\machine\software\policies\microsoft\mrt
- \\registry\user\%user%\clsid
- \\registry\machine\software\microsoft\windows nt\currentversion\accessibility\ats
- \\registry\machine\system\controlset001\services\acpi
- \\registry\machine\system\controlset001\control\print\environments\windows x64\print processors\printfiiterpipelinesvc\driver
- \\registry\machine\software\microsoft\windows nt\currentversion\appcompatflags\custom
- \\registry\machine\system\controlset001\control\sam
- \\registry\user\%user%\software\classes\local settings\software\microsoft\windows\currentversion\appcontainer\storage\microsoft.microsoftedge_8wekyb3d8bbwe\microsoftedge\phishingfilter
- \\registry\machine\system\controlset001\services\vmmemctl
- \\registry\machine\software\policies\microsoft\windows nt\systemrestore
- \\registry\machine\software\policies\microsoft\windows nt\dnsclient
- \\registry\machine\system\currentcontrolset\services\acpi
- \\registry\machine\software\policies\microsoft\windows defender
- \\registry\machine\system\controlset001\services\vmicexchange
- \\registry\user\%user%\software\licenses
- \\registry\machine\system\currentcontrolset\control\securityproviders\securityproviders
- \\registry\machine\software\teamviewer
- \\registry\machine\software\wow6432node\microsoft\windows nt\currentversion\drivers32
- \\registry\machine\software\tightvnc\server
- \\registry\machine\system\controlset002\services\acpi
- \\registry\machine\system\controlset001\control\securityproviders\securityproviders
- \\registry\machine\system\controlset001\services\vpc-s3
- \\registry\user\%user%\software\microsoft\windows\currentversion\explorer\fileexts
- \\registry\user\%user%\software\microsoft\windows script host\settings\amsienable
- \\registry\machine\software\microsoft\internet explorer\extensions
- \\registry\machine\system\currentcontrolset\control\wmi\autologger\eventlog-system

- \\registry\machine\system\controlset002\control\network
- \\registry\machine\software\classes\batfile
- \\registry\user\%user%\software\wow6432node\microsoft\windows\currentversion\explorer\browser helper objects
- \\registry\user\%user%\software\microsoft\windows nt\currentversion\windows messaging subsystem\profiles\outlook
- \\registry\machine\software\classes\clsid
- \\registry\machine\software\policies\microsoft\microsoft antimalware
- \\registry\machine\software\vmware, inc.\vmware tools
- \\registry\machine\software\policies\microsoft\windows\bits
- \\registry\machine\system\currentcontrolset\control\terminal server
- \\registry\machine\system\controlset001\services\sharedaccess\parameters\firewallpolicy
- \\registry\user\%user%\software\microsoft\windows script\settings\amsienable
- \\registry\user\%user%\software\microsoft\windows\currentversion\app paths\control.exe
- \\registry\machine\software\wow6432node\microsoft\command processor
- \\registry\machine\software\win6432node\microsoft\cryptography\oid
- \\registry\machine\software\microsoft\windows\currentversion\app paths\control.exe
- \\registry\machine\software\microsoft\hyper-v
- \\registry\user\%user%\software\microsoft\windows nt\currentversion\accessibility
- \\registry\machine\software\microsoft\windows\currentversion\control panel
- \\registry\user\%user%\software\microsoft\windows\currentversion\explorer\user shell folders
- \\registry\machine\software\microsoft\windows nt\currentversion\appcompatflags
- \\registry\machine\software\microsoft\windows\currentversion\policies\explorer
- \\registry\machine\system\currentcontrolset\control\crashcontrol
- \\registry\user\%user%\software\microsoft\active setup\installed components
- \\registry\machine\system\currentcontrolset\services\nlasvc
- \\registry\user\%user%\system\controlset003\control\safeboot
- \\registry\machine\system\controlset003\control\network
- \\registry\user\%user%\software\wow6432node\microsoft\windows\currentversion\packagedappxdebug
- \\registry\user\%user%_classes\appx82a6gwre4fdg3bt635tn5ctqjf8msdd2\shell\open\command
- \\registry\user\%user%\software\microsoft\office\16.0\outlook\profiles\outlook
- \\registry\user\%user%\software\microsoft\windows\currentversion\runonce
- \\registry\machine\system\currentcontrolset\control\network

- \\registry\machine\software\policies\microsoft\windows\windowsupdate
- \\registry\machine\hardware\acpi\rsdt
- \\registry\machine\system\controlset001\hardwareprofiles
- \\registry\machine\security\policy\secrets
- \\registry\machine\software\wow6432node\microsoft\windows nt\currentversion\aedebug
- \\registry\machine\software\microsoft\windows\currentversion\explorer\shellserviceobjectdelayload
- \\registry\machine\system\controlset001\services\msvmmouf
- \\registry\machine\software\classes\mscfile\shell\open\command
- \\registry\machine\system\controlset001\services\wuauserv
- \\registry\machine\system\controlset001\control\terminal server\fsinglesessionperuser
- \\registry\user\%user%\software\microsoft\windows\currentversion\authentication\credential provider
- \\registry\machine\software\policies\microsoft\pushtoinstall
- \\registry\machine\system\controlset001\services
- \\registry\machine\software\microsoft\windows\currentversion\authentication\credential provider filters
- \\registry\machine\software\microsoft\windows\currentversion\authentication\plap providers
- \\registry\machine\software\microsoft\internet explorer\download
- \\registry\machine\system\currentcontrolset\control\hivelist
- \\registry\machine\software\microsoft\windows nt\currentversion\drivers32
- \\registry\machine\software\microsoft\internet explorer\toolbar
- \\registry\machine\software\policies\microsoft\previousversions
- \\registry\machine\software\win6432node\microsoft\windows nt\currentversion\image file execution options
- \\registry\machine\hardware\acpi\dsdt
- \\registry\machine\system\controlset001\services\securityhealthervice
- \\registry\machine\software\microsoft\.netframework\etwenabled
- \\registry\user\%user%\software\wow6432node\microsoft\windows nt\currentversion\aedebug
- \\registry\machine\control panel\desktop
- \\registry\machine\software\microsoft\systemcertificates\authroot\certificates
- \\registry\machine\software\microsoft\windows\currentversion\policies
- \\registry\user\%user%\software\classes\mscfile\shell\open\command
- \\registry\machine\system\controlset001\services\xennet6
- \\registry\machine\software\microsoft\enterprisecertificates\root\certificates

- \\registry\user\%user%\software\policies\google\chrome\extensioninstallforcelist
- \\registry\machine\system\currentcontrolset\control\safeboot
- \\registry\user\%user%\software\classes\appx82a6gwre4fdg3bt635tn5ctqjf8msdd2\shell\open\command
- \\registry\machine\system\currentcontrolset\control\sam
- \\registry\user\%user%\software\wow6432node\localnetservice
- \\registry\machine\system\currentcontrolset001\control\session manager
- \\registry\machine\software\microsoft\windows\windows error reporting
- \\registry\user\%user%\software\microsoft\office\15.0\outlook\profiles\outlook
- \\registry\machine\software\classes\.com
- \\registry\machine\software\policies\microsoft\windowsstore
- \\registry\machine\system\controlset001\services\vmmouse
- \\registry\user\system\currentcontrolset\services\nlasvc
- \\registry\user\%user%\system\controlset001\control\safeboot
- \\registry\machine\system\controlset001\services\xennet
- \\registry\user\%user%\software\microsoft\systemcertificates\root\certificates
- \\registry\user\%user%\software\wanacrypt
- \\registry\machine\software\wow6432node\microsoft\windows nt\currentversion\svchost
- \\registry\machine\software\microsoft\office test\special\perf
- \\registry\machine\software\microsoft\windows nt\currentversion\image file execution options
- \\registry\machine\system\controlset001\control\network
- \\registry\machine\system\controlset001\services\wscsvc
- \\registry\user\%user%\software\microsoft\windows\currentversion\policies\explorer
- \\registry\user\%user%\software\msys
- \\registry\machine\software\microsoft\windows\currentversion\policies\windowsupdate
- \\registry\machine\system\controlset001\services\sense
- \\registry\machine\system\controlset001\control\session manager\environment
- \\registry\machine\software\microsoft\windows\currentversion\packagedappxdebug
- \\registry\machine\software\win6432node\microsoft\windows nt\currentversion\windows
- \\registry\machine\software\classes\exefile\shell\open\command
- \\registry\user\%user%\software\microsoft\windows\currentversion\explorer\browser helper objects
- \\registry\user\%user%\software\wow6432node\microsoft\windows nt\currentversion\svchost

- \\registry\user\%user%\software\wanacrypt0r
- \\registry\user\%user%\volatile environment
- \\registry\machine\software\microsoft\windows\currentversion\explorer\shellexecutehooks
- \\registry\user\%user%\software\microsoft\windows nt\currentversion\terminal server\install\software\microsoft\windows\currentversion\run
- \\registry\machine\system\controlset001\services\vboxsf
- \\registry\user\%user%\software\zsys
- \\registry\machine\software\microsoft\enterprisecertificates\authroot\certificates
- \\registry\machine\software\microsoft\windows\currentversion\uninstall
- \\registry\machine\software\classes\.exe
- \\registry\machine\software\microsoft\windows\currentversion\explorer
- \\registry\machine\software\google
- \\registry\machine\system\controlset001\services\vboxmouse
- \\registry\machine\software\microsoft\windows\currentversion\runonce
- \\registry\machine\software\wow6432node\microsoft\windows\currentversion\packagedappxdebug
- \\registry\machine\software\microsoft\windows nt\currentversion\windows
- \\registry\machine\software\policies\microsoft\systemcertificates\root\certificates
- \\registry\machine\software\wow6432node\microsoft\windows nt\currentversion\windows
- \\registry\user\%user%\software\microsoft\windows nt\currentversion\winlogon
- \\registry\user\%user%\software\microsoft\windows\currentversion\explorer\shell folders
- \\registry\user\%user%\software\classes\.
- \\registry\machine\system\controlset001\services\vmdebug
- \\registry\user\%user%\software\microsoft\windows\currentversion\internet settings\zonemap
- \\software\microsoft\windows nt\currentversion
- \\registry\machine\system\controlset001\control\computername\computername
- \\registry\machine\system\controlset001\control\session manager
- \\registry\machine\system\controlset001\control\bootverificationprogram
- \\registry\user\%user%_classes\folder\shell\open\command
- \\registry\machine\system\currentcontrolset\control\lsa
- \\registry\machine\system\currentcontrolset\control\session manager
- \\registry\user\%user%\software\localnetservice

- \\registry\user\%user%\software\wow6432node\microsoft\windows\currentversion\shell extensions\approved
- \\registry\machine\system\controlset001\services\xenevtchn
- \\registry\machine\software\microsoft\systemcertificates\root\protectedroots
- \\registry\user\%user%\software\microsoft\windows\currentversion\explorer\shelliconoverlayidentifiers
- \\registry\user\%user%\software\policies\microsoft\systemcertificates\root\certificates
- \\registry\machine\system\currentcontrolset\control\nls\language
- \\registry\machine\software\microsoft\command processor
- \\registry\machine\software\microsoft\windows\currentversion\explorer\browser helper objects
- \\registry\machine\software\microsoft\windows nt\currentversion\silentprocessexit
- \\registry\machine\system\controlset003\services
- \\registry\machine\software\win6432node\microsoft\windows nt\currentversion\systemrestore
- \\registry\user\%user%\software\microsoft\windows nt\currentversion\drivers32
- \\registry\machine\software\microsoft\enterprisecertificates\ca\certificates
- \\registry\machine\software\microsoft\windows\currentversion\internet settings
- \\registry\user\%user%\software\locky
- \\registry\machine\system\currentcontrolset\control\terminal server\fsinglesessionperuser
- \\registry\machine\software\wow6432node\microsoft\windows\currentversion\shell extensions\approved
- \\registry\machine\software\wow6432node\wanacrypt0r\wd
- \\registry\user\%user%\software\microsoft\windows nt\currentversion\terminal server\install\software\microsoft\windows\currentversion\runonceex
- \\registry\machine\software\wow6432node\microsoft\windows\currentversion\authentication\credential provider filters
- \\registry\machine\software\microsoft\internet explorer\main
- \\registry\machine\software\microsoft\internet explorer\phishingfilter
- \\registry\machine\software\wow6432node\microsoft\windows\currentversion\run
- \\registry\user\%user%\software\microsoft\windows\currentversion\policies\system\consentpromptbehavioruser