VALKYRIE COMODO

Summary

File Name: None

File Type: PE32 executable (GUI) Intel 80386, for MS Windows

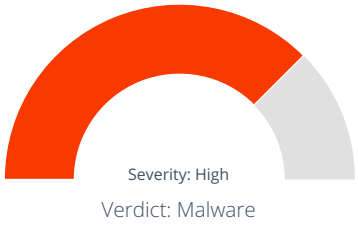
SHA1: 12af0c0e047b70ff8406407a6c5b49050f413fa7

MD5: 3b1086235aead2a5cf61ec6e8728edb9

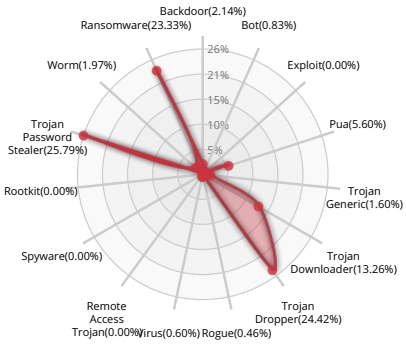
MALWARE

Valkyrie Final Verdict

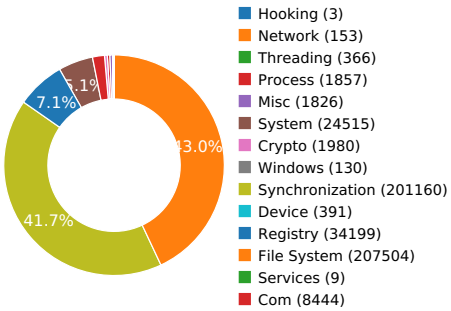
DETECTION SECTION



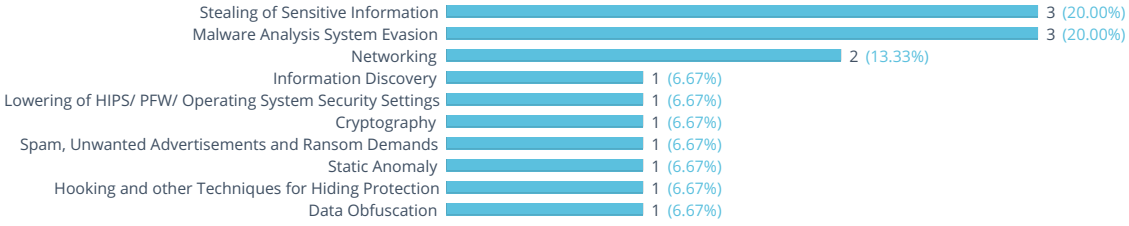
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image	Show sources

NETWORKING

Attempts to connect to a dead IP:Port (3 unique times)	Show sources
Performs some HTTP requests	Show sources

LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS

Attempts to block SafeBoot use by removing registry keys	Show sources

CRYPTOGRAPHY

At least one IP Address, Domain, or File Name was found in a crypto call	Show sources

STEALING OF SENSITIVE INFORMATION

Collects information to fingerprint the system	Show sources
Attempts to create or modify system certificates	Show sources
Steals private information from local Internet browsers	Show sources

SPAM, UNWANTED ADVERTISEMENTS AND RANSOM DEMANDS

Exhibits possible ransomware file modification behavior	Show sources

STATIC ANOMALY

Anomalous binary characteristics	Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory	Show sources

DATA OBFUSCATION

Drops a binary and executes it	Show sources

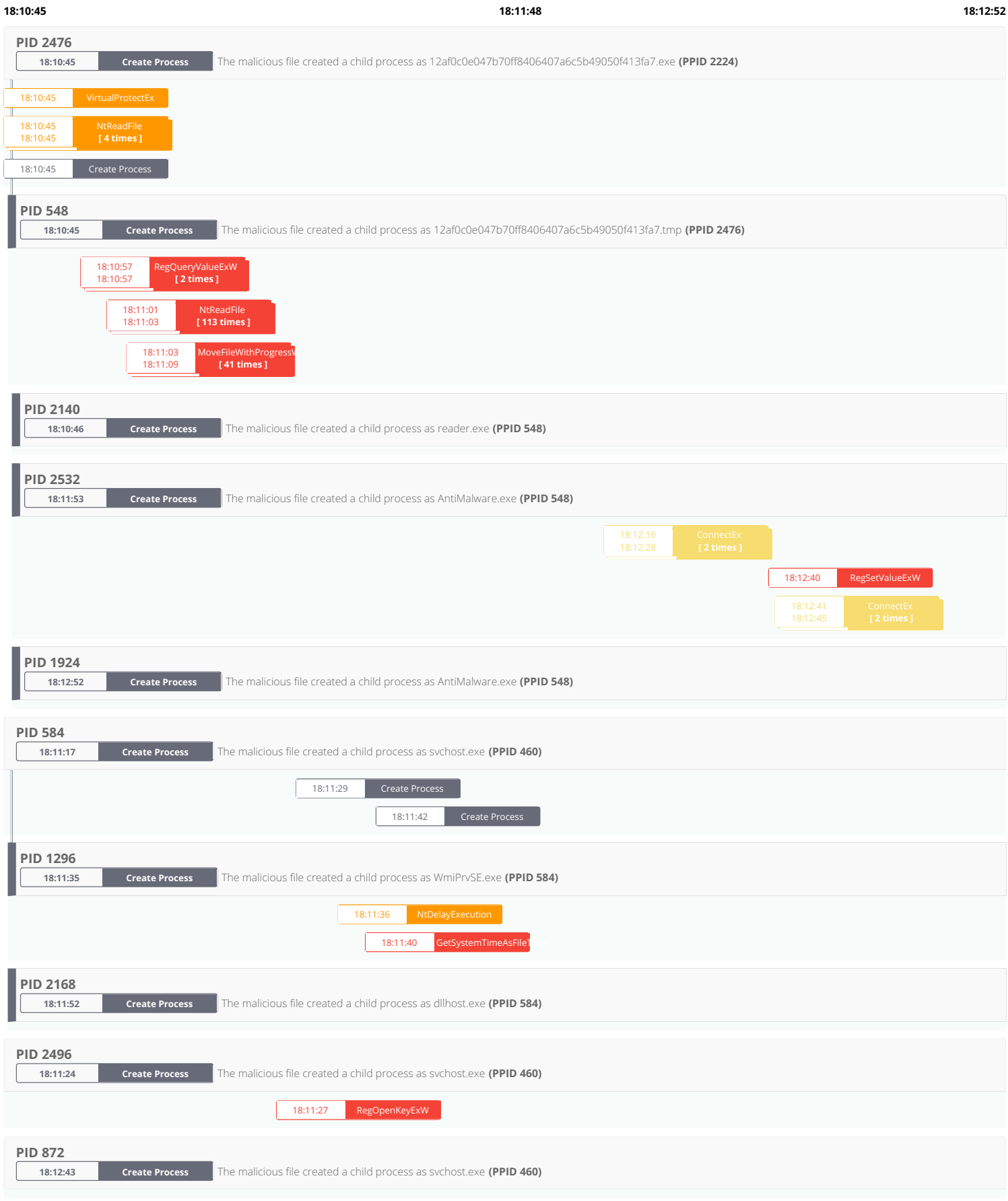
VALKYRIE COMODO

MALWARE ANALYSIS SYSTEM EVASION

A process attempted to delay the analysis task.	Show sources
Checks the version of Bios, possibly for anti-virtualization	Show sources
Attempts to repeatedly call a single API many times in order to delay analysis time	Show sources

VALKYRIE COMODO

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\12af0c0e047b70ff8406407a6c5b49050f413fa7.ENU
C:\Users\user\AppData\Local\Temp\12af0c0e047b70ff8406407a6c5b49050f413fa7.ENU.DLL
C:\Users\user\AppData\Local\Temp\12af0c0e047b70ff8406407a6c5b49050f413fa7.EN
C:\Users\user\AppData\Local\Temp\12af0c0e047b70ff8406407a6c5b49050f413fa7.EN.DLL
C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
C:\Users\user\AppData\Local\Temp\netmsg.dll
C:\Windows\System32\netmsg.dll
C:\Users\user\AppData\Local\Temp\12af0c0e047b70ff8406407a6c5b49050f413fa7.exe
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\is-LIT24.tmp
C:\Users\user\AppData\Local\Temp\is-LIT24.tmp\12af0c0e047b70ff8406407a6c5b49050f413fa7.tmp
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\AppData\Local\Temp\is-LIT24.tmp\12af0c0e047b70ff8406407a6c5b49050f413fa7.ENU
C:\Users\user\AppData\Local\Temp\is-LIT24.tmp\12af0c0e047b70ff8406407a6c5b49050f413fa7.ENU.DLL
C:\Users\user\AppData\Local\Temp\is-LIT24.tmp\12af0c0e047b70ff8406407a6c5b49050f413fa7.EN
C:\Users\user\AppData\Local\Temp\is-LIT24.tmp\12af0c0e047b70ff8406407a6c5b49050f413fa7.EN.DLL
\Device\KsecDD
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Local\Temp\is-LIT24.tmp\netmsg.dll
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp_isetup
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp_isetup_shfoldr.dll
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\reader.exe
\??\MountPointManager
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\AntiMalware.exe
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\SetupCustom.dll
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\CFAHelper.dll
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\AxBrowsers.dll
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\sqlite3.dll
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\CommonForms.Site.dll
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\Localizer.dll
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\AxComponentsRTL.bpl
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\AxComponentsVCL.bpl
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\rtl160.bpl
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\vcl160.bpl
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\vclimg160.bpl
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\EULA.rtf
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\enu.lng
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\deu.lng
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\esp.lng

C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\fra.lng
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\ita.lng
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\jpn.lng
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\rus.lng
C:\Users\user\AppData\Local\Temp\is-LIT24.tmp\rtl160.bpl
C:\Windows\System32\rtl160.bpl
C:\Windows\system\rtl160.bpl
C:\Windows\rtl160.bpl
C:\Users\user\AppData\Local\Temp\is-LIT24.tmp\wsock32.dll
C:\Windows\System32\wsock32.dll
C:\Users\user\AppData\Local\Temp\is-LIT24.tmp\oleacc.dll
C:\Windows\System32\oleacc.dll
C:\Users\user\AppData\Local\Temp\is-LIT24.tmp\odbc32.dll
C:\Windows\System32\odbc32.dll
C:\Users\user\AppData\Local\Temp\is-LIT24.tmp\vcl160.bpl
C:\Windows\System32\vcl160.bpl
C:\Windows\system\vcl160.bpl
C:\Windows\vcl160.bpl
C:\Users\user\AppData\Local\Temp\is-LIT24.tmp\winspool.drv
C:\Windows\System32\winspool.drv
C:\Users\user\AppData\Local\Temp\is-LIT24.tmp\oledlg.dll
C:\Windows\System32\oledlg.dll
C:\Users\user\AppData\Local\Temp\is-LIT24.tmp\AxComponentsRTL.bpl
C:\Windows\System32\AxComponentsRTL.bpl
C:\Windows\system\AxComponentsRTL.bpl
C:\Windows\AxComponentsRTL.bpl
C:\Users\user\AppData\Local\Temp\is-LIT24.tmp\AxComponentsVCL.bpl
C:\Windows\System32\AxComponentsVCL.bpl
C:\Windows\system\AxComponentsVCL.bpl
C:\Windows\AxComponentsVCL.bpl
C:\Users\user\AppData\Local\Temp\is-LIT24.tmp\vclimg160.bpl
C:\Windows\System32\vclimg160.bpl
C:\Windows\system\vclimg160.bpl
C:\Windows\vclimg160.bpl
C:\Users\user\AppData\Local\Temp\is-LIT24.tmp\winmm.dll

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\MS Shell Dlg 2
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\CommonFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CommonFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOwner
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOrganization
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledProcesses\E74C67D3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\MachineThrottling
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\GlobalSession
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Auslogics\Anti-Malware\1.x\Settings\General.Cookie
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Auslogics\Anti-Malware\1.x\Settings\General.CookieLastAction
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\Environment\Path
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Auslogics\Anti-Malware\1.x\Settings\General.Language
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\vclimg160.bpl
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\AxComponentsVCL.bpl

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\SetupCustom.dll
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\MachineGuid
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\ProductId
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\SystemBiosVersion
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus\FontCachePath
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\ar
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\ar
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\ar-SA
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\ar-SA
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\bg
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\bg
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\bg-BG
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\bg-BG
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\ca
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\ca
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\ca-ES
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\ca-ES
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\zh-Hans
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\zh-Hans
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\zh-CN
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\zh-CN
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\cs
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\cs
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\cs-CZ
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\cs-CZ
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\da
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\da

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\is-LIT24.tmp\12af0c0e047b70ff8406407a6c5b49050f413fa7.tmp
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp_isetup_shfoldr.dll
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\reader.exe
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\AntiMalware.exe
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\SetupCustom.dll
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\CFAHelper.dll
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\AxBrowsers.dll
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\sqlite3.dll
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\CommonForms.Site.dll
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\Localizer.dll
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\AxComponentsRTL.bpl
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\AxComponentsVCL.bpl
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\rtl160.bpl

C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\vcl160.bpl
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\vclimg160.bpl
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\EULA.rtf
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\enu.lng
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\deu.lng
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\esp.lng
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\fra.lng
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\ita.lng
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\jpn.lng
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\rus.lng
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\GASender.exe
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\GoogleAnalyticsHelper.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\AntiMalware.exe
C:\Program Files (x86)\Auslogics\Anti-Malware\AntiMalwareHelper.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\DebugHelper.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\Localizer.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\CommonForms.Routine.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\Engine\savapi.exe
C:\Program Files (x86)\Auslogics\Anti-Malware\ActionCenterHelper.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\CommonForms.Site.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\GASender.exe
C:\Program Files (x86)\Auslogics\Anti-Malware\GoogleAnalyticsHelper.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\Setup\SetupCustom.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\sqlite3.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\ActionCenterForms.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\AxBrowsers.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\CFAHelper.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\Engine\avupdate.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\Engine\savapi.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\TaskSchedulerHelper.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\Engine\savapi_stub.exe
C:\Program Files (x86)\Auslogics\Anti-Malware\SendDebugLog.exe
C:\Program Files (x86)\Auslogics\Anti-Malware\unins000.dat
C:\Program Files (x86)\Auslogics\Anti-Malware\is-7HI2E.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\unins000.exe
C:\Program Files (x86)\Auslogics\Anti-Malware\is-L2D15.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\EULA.rtf
C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\is-EM2MU.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\enu.lng
C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\is-BQ1H4.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\deu.lng
C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\is-2AVM9.tmp

C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\esp.lng
C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\is-LRIRA.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\fra.lng
C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\is-1D8CQ.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\ita.lng
C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\is-UV8TG.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\jpn.lng
C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\is-7QRF4.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\rus.lng
C:\Program Files (x86)\Auslogics\Anti-Malware\Setup\is-FIFUI.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Data\main.ini
C:\Program Files (x86)\Auslogics\Anti-Malware\is-JVFCQ.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\rtl160.bpl
C:\Program Files (x86)\Auslogics\Anti-Malware\is-7R16O.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\vcl160.bpl
C:\Program Files (x86)\Auslogics\Anti-Malware\is-2Q7BL.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\vclimg160.bpl
C:\Program Files (x86)\Auslogics\Anti-Malware\is-4CFKF.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\AxComponentsRTL.bpl

RESOLVED APIS

kernel32.dll.SetDllDirectoryW
kernel32.dll.SetSearchPathMode
kernel32.dll.SetProcessDEPPolicy
kernel32.dll.GetDiskFreeSpaceExW
kernel32.dll.Wow64DisableWow64FsRedirection
kernel32.dll.Wow64RevertWow64FsRedirection
kernel32.dll.GetUserDefaultUILanguage
comctl32.dll.RegisterClassNameW
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
dwmapi.dll.DwmIsCompositionEnabled
uxtheme.dll.EnableThemeDialogTexture
oleaut32.dll.VariantChangeTypeEx
oleaut32.dll.VarNeg
oleaut32.dll.VarNot
oleaut32.dll.VarAdd
oleaut32.dll.VarSub
oleaut32.dll.VarMul
oleaut32.dll.VarDiv
oleaut32.dll.VarIdiv

oleaut32.dll.VarMod
oleaut32.dll.VarAnd
oleaut32.dll.VarOr
oleaut32.dll.VarXor
oleaut32.dll.VarCmp
oleaut32.dll.VarI4FromStr
oleaut32.dll.VarR4FromStr
oleaut32.dll.VarR8FromStr
oleaut32.dll.VarDateFromStr
oleaut32.dll.VarCyFromStr
oleaut32.dll.VarBoolFromStr
oleaut32.dll.VarBstrFromCy
oleaut32.dll.VarBstrFromDate
oleaut32.dll.VarBstrFromBool
kernel32.dll.InitializeConditionVariable
kernel32.dll.WakeConditionVariable
kernel32.dll.WakeAllConditionVariable
kernel32.dll.SleepConditionVariableCS
user32.dll.WINNLSEnableIME
imm32.dll.ImmGetContext
imm32.dll.ImmReleaseContext
imm32.dll.ImmGetConversionStatus
imm32.dll.ImmSetConversionStatus
imm32.dll.ImmSetOpenStatus
imm32.dll.ImmSetCompositionWindow
imm32.dll.ImmSetCompositionFontW
imm32.dll.ImmGetCompositionStringW
imm32.dll.ImmIsIME
imm32.dll.ImmNotifyIME
user32.dll.GetMonitorInfoA
user32.dll.GetSystemMetrics
user32.dll.EnumDisplayMonitors
cryptbase.dll.SystemFunction036
gdi32.dll.GetLayout
gdi32.dll.GdiRealizationInfo
gdi32.dll.FontIsLinked
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryInfoKeyW
gdi32.dll.GetTextFaceAliasW
advapi32.dll.RegEnumValueW
advapi32.dll.RegCloseKey
advapi32.dll.RegQueryValueExW
gdi32.dll.GetFontAssocStatus

advapi32.dll.RegQueryValueExA
advapi32.dll.RegEnumKeyExW
gdi32.dll.GdiIsMetaPrintDC
user32.dll.AnimateWindow
comctl32.dll.InitializeFlatSB
comctl32.dll.UninitializeFlatSB
comctl32.dll.FlatSB_GetScrollProp
comctl32.dll.FlatSB_SetScrollProp
comctl32.dll.FlatSB_EnableScrollBar
comctl32.dll.FlatSB_ShowScrollBar
comctl32.dll.FlatSB_GetScrollRange

DELETED FILES

C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\main.ini
C:\Program Files (x86)\Auslogics\Anti-Malware\is-7HI2E.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\is-L2D15.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\is-EM2MU.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\is-BQ1H4.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\is-2AVM9.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\is-LRIRA.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\is-1D8CQ.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\is-UV8TG.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\is-7QRF4.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Setup\is-FIFUI.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Data\is-2CL02.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\is-JVFCQ.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\is-7R16O.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\is-2Q7BL.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\is-4CFKF.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\is-FFGHR.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\is-JUIQS.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\is-37QNA.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\is-C2OHP.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\is-CT5JA.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\is-196D9.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\is-E7GAA.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\is-7D73N.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\is-H0RC0.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\is-R7K3M.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\is-MMP1C.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\is-EK7Q1.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\is-DC8AK.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\is-AP47S.tmp

C:\Program Files (x86)\Auslogics\Anti-Malware\is-NJMD8.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\is-6MQ8G.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Data\is-A62HV.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Data\is-TPT7I.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\is-6H0IO.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Engine\is-4FF6S.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Engine\is-K2LOP.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Engine\is-1UHKH.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Engine\is-7VCAH.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Engine\is-O26GS.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Engine\is-J9P9O.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Engine\is-EGE4G.tmp
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Auslogics\Anti-Malware\Auslogics Anti-Malware.lnk
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Auslogics\Anti-Malware\Auslogics Anti-Malware.pif
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Auslogics\Anti-Malware\Auslogics Anti-Malware.url
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Auslogics\Anti-Malware\Auslogics Anti-Malware on the Web.lnk
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Auslogics\Anti-Malware\Auslogics Anti-Malware on the Web.pif
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Auslogics\Anti-Malware\Auslogics Anti-Malware on the Web.url
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Auslogics\Anti-Malware\Uninstall Auslogics Anti-Malware.lnk
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Auslogics\Anti-Malware\Uninstall Auslogics Anti-Malware.pif
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Auslogics\Anti-Malware\Uninstall Auslogics Anti-Malware.url
C:\Users\user\Desktop\Auslogics Anti-Malware.lnk
C:\Users\user\Desktop\Auslogics Anti-Malware.pif
C:\Users\user\Desktop\Auslogics Anti-Malware.url
C:\Users\user\AppData\Local\Temp\AntiMalware.madExcept
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\AntiMalware.madExcept\

DELETED REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\WMIBinaryMofResource.HighDateTime=30016564,LowDateTime=3292279056,Name="C:\Windows\system32\advapi32.dll[MofResourceName]"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\503006091D97D4F5AE39F7CBE7927D7D652D3431

REGISTRY KEYS

HKEY_CURRENT_USER\Software\CodeGear\Locales
HKEY_LOCAL_MACHINE\Software\CodeGear\Locales
HKEY_CURRENT_USER\Software\Borland\Locales
HKEY_CURRENT_USER\Software\Borland\Delphi\Locales
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\MS Shell Dlg 2
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Segoe UI
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Keyboard Layouts\04090409
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\12af0c0e047b70ff8406407a6c5b49050f413fa7.tmp
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\KnownClasses
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\CommonFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CommonFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOwner
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOrganization

HKEY_LOCAL_MACHINE\Software\Microsoft\SQMClient\Windows\DisabledProcesses\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledProcesses\E74C67D3
HKEY_LOCAL_MACHINE\Software\Microsoft\SQMClient\Windows\DisabledSessions\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\MachineThrottling
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\GlobalSession
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Owner
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\SessionHash
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Sequence
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{A5A6F7C9-F91E-45C7-8DAA-289CBB0C817D}_is1
HKEY_LOCAL_MACHINE\Software\Auslogics\Anti-Malware\1.x\Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Auslogics\Anti-Malware\1.x\Settings\General.Cookie
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Auslogics\Anti-Malware\1.x\Settings\General.CookieLastAction
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data

EXECUTED COMMANDS

"C:\Users\user\AppData\Local\Temp\is-LIT24.tmp\12af0c0e047b70ff8406407a6c5b49050f413fa7.tmp" /SL5="$80148,7833315,154112,C:\Users\user\AppData\Local\Temp\12af0c0e047b70ff8406407a6c5b49050f413fa7.exe"
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\reader.exe "C:\Users\user\AppData\Local\Temp\12af0c0e047b70ff8406407a6c5b49050f413fa7.exe" " (x32)HKEY_LOCAL_MACHINE\\Software\\Auslogics\\Anti-Malware\\1.x\\Settings"
C:\Program Files (x86)\Auslogics\Anti-Malware\AntiMalware.exe /install /setautostart
C:\Program Files (x86)\Auslogics\Anti-Malware\AntiMalware.exe /FromInstall
C:\Windows\system32\wbem\wmiprvse.exe -Embedding
C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}

READ FILES

C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
C:\Windows\System32\netmsg.dll
C:\Users\user\AppData\Local\Temp\12af0c0e047b70ff8406407a6c5b49050f413fa7.exe
C:\Windows\Globalization\Sorting\sortdefault.nls
\Device\KsecDD
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp_isetup_shfoldr.dll
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\SetupCustom.dll
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\rtl160.bpl
C:\Windows\System32\wsock32.dll

C:\Windows\System32\oleacc.dll
C:\Windows\System32\odbc32.dll
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\vcl160.bpl
C:\Windows\System32\winspool.drv
C:\Windows\System32\oledlg.dll
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\AxComponentsRTL.bpl
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\AxComponentsVCL.bpl
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\vclimg160.bpl
C:\Windows\System32\winmm.dll
C:\Windows\System32\tzres.dll
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT
C:\Windows\Fonts\lucon.ttf
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\main.ini
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\AntiMalware.exe
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\GoogleAnalyticsHelper.dll
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\CFAHelper.dll
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\Localizer.dll
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\enu.lng
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\CommonForms.Site.dll
C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Users\user\AppData\Local\Temp\is-TF58U.tmp\AxBrowsers.dll
C:\Windows\System32\imageres.dll
C:\Windows\System32\shell32.dll
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@c1.microsoft[2].txt
C:\Windows\win.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@microsoft[2].txt
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@google[2].txt
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@downloads.sourceforge[1].txt
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\Low\index.dat
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\index.dat
C:\
C:\Program Files (x86)\Auslogics\Anti-Malware\AntiMalware.exe
C:\Program Files (x86)\Auslogics\Anti-Malware\AntiMalwareHelper.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\DebugHelper.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\Localizer.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\CommonForms.Routine.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\Engine\savapi.exe
C:\Program Files (x86)\Auslogics\Anti-Malware\ActionCenterHelper.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\CommonForms.Site.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\GASender.exe

C:\Program Files (x86)\Auslogics\Anti-Malware\GoogleAnalyticsHelper.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\Setup\SetupCustom.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\sqlite3.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\ActionCenterForms.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\AxBrowsers.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\CFAHelper.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\Engine\avupdate.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\Engine\savapi.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\TaskSchedulerHelper.dll
C:\Program Files (x86)\Auslogics\Anti-Malware\Engine\savapi_stub.exe
C:\Program Files (x86)\Auslogics\Anti-Malware\SendDebugLog.exe
C:\Program Files (x86)\Auslogics\Anti-Malware\unins000.dat
C:\Windows\winsxs\FileMaps\program_files_x86_auslogics_anti-malware_4cf884916eac656c.cdf-ms
C:\Program Files (x86)\Auslogics\Anti-Malware\is-7HI2E.tmp
C:\Users\user\AppData\Local\Temp\is-LIT24.tmp\12af0c0e047b70ff8406407a6c5b49050f413fa7.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\is-L2D15.tmp
C:\Windows\winsxs\FileMaps\program_files_x86_auslogics_anti-malware_lang_a6f41b3fc52fd806.cdf-ms
C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\is-EM2MU.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\enu.lng
C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\is-BQ1H4.tmp
C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\deu.lng
C:\Program Files (x86)\Auslogics\Anti-Malware\Lang\is-2AVM9.tmp

MUTEXES

CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
Local\RstrMgr3887CAB8-533F-4C85-B0DC-3E5639F8D511
Local\RstrMgr-3887CAB8-533F-4C85-B0DC-3E5639F8D511-Session0000
8D622ABC-7F4F-49CF-A95A-86F8A21753BA_global_auslogics_.exe_setup
DefaultTabtip-MainUI
madExceptSettingsMtx$9e4
HookTThread$9e4
8D622ABC-7F4F-49CF-A95A-86F8A21753BA_global_auslogics_antimalware
8D622ABC-7F4F-49CF-A95A-86F8A21753BA_local_auslogics_antimalware
madExceptSettingsMtx$784
HookTThread$784

MODIFIED REGISTRY KEYS

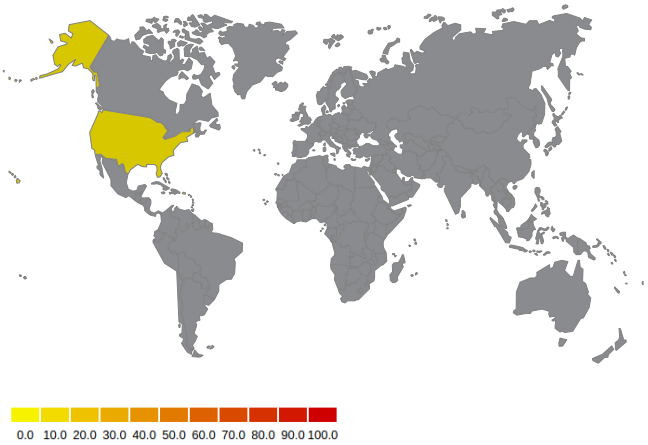
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Owner
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\SessionHash
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Sequence
HKEY_LOCAL_MACHINE\Software\Auslogics\Anti-Malware\1.x\Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Auslogics\Anti-Malware\1.x\Settings\General.Cookie

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Auslogics\Anti-Malware\1.x\Settings\General.CookieLastAction
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{98A79B43-35BB-C373-7747-6040708DB024}\Version
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{98A79B43-35BB-C373-7747-6040708DB024}\Version\Assembly
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Auslogics\ClientID
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Auslogics\Anti-Malware\1.x\Settings\General.Language
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegFiles0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegFilesHash
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{A5A6F7C9-F91E-45C7-8DAA-289CBB0C817D}_is1
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{A5A6F7C9-F91E-45C7-8DAA-289CBB0C817D}_is1\Inno Setup: Setup Version
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{A5A6F7C9-F91E-45C7-8DAA-289CBB0C817D}_is1\Inno Setup: App Path
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{A5A6F7C9-F91E-45C7-8DAA-289CBB0C817D}_is1\InstallLocation
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{A5A6F7C9-F91E-45C7-8DAA-289CBB0C817D}_is1\Inno Setup: Icon Group
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{A5A6F7C9-F91E-45C7-8DAA-289CBB0C817D}_is1\Inno Setup: User
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{A5A6F7C9-F91E-45C7-8DAA-289CBB0C817D}_is1\Inno Setup: Language
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{A5A6F7C9-F91E-45C7-8DAA-289CBB0C817D}_is1\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{A5A6F7C9-F91E-45C7-8DAA-289CBB0C817D}_is1\DisplayIcon
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{A5A6F7C9-F91E-45C7-8DAA-289CBB0C817D}_is1\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{A5A6F7C9-F91E-45C7-8DAA-289CBB0C817D}_is1\QuietUninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{A5A6F7C9-F91E-45C7-8DAA-289CBB0C817D}_is1\DisplayVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{A5A6F7C9-F91E-45C7-8DAA-289CBB0C817D}_is1\Publisher
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{A5A6F7C9-F91E-45C7-8DAA-289CBB0C817D}_is1\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{A5A6F7C9-F91E-45C7-8DAA-289CBB0C817D}_is1\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{A5A6F7C9-F91E-45C7-8DAA-289CBB0C817D}_is1\URLUpdateInfo
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{A5A6F7C9-F91E-45C7-8DAA-289CBB0C817D}_is1\Readme
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{A5A6F7C9-F91E-45C7-8DAA-289CBB0C817D}_is1\Contact
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{A5A6F7C9-F91E-45C7-8DAA-289CBB0C817D}_is1\NoModify
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{A5A6F7C9-F91E-45C7-8DAA-289CBB0C817D}_is1\NoRepair
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{A5A6F7C9-F91E-45C7-8DAA-289CBB0C817D}_is1\InstallDate
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{A5A6F7C9-F91E-45C7-8DAA-289CBB0C817D}_is1\MajorVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{A5A6F7C9-F91E-45C7-8DAA-289CBB0C817D}_is1\MinorVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{A5A6F7C9-F91E-45C7-8DAA-289CBB0C817D}_is1\EstimatedSize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\LastServiceStart
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Transports\Decoupled\Server
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\CreationTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\MarshaledProxy
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\ProcessIdentifier
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ConfigValueEssNeedsLoading
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\List of event-active namespaces
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\ESSV/./root/CIMV2\SCM Event Provider
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\IDE\DiskVBOX_HARDDISK_____1.0____\5&33d1638a&0&0.0.0_0-{05901221-D566-11d1-B2F0-00A0C9062910}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\advapi32.dll[MofResourceName]
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042

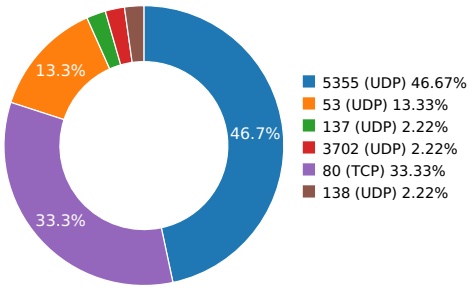
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\503006091D97D4F5AE39F7CBE7927D7D652D3431\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Auslogics\Anti-Malware\1.x\Settings\General.InstallDateTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{7A0F498F-2409-402C-8967-2584DE20B134}\Path
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{7A0F498F-2409-402C-8967-2584DE20B134}\Hash
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Auslogics\Anti-Malware\Start Anti-Malware \xd0\xben user logon\Id
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Auslogics\Anti-Malware\Start Anti-Malware \xd0\xben user logon\Index
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{7A0F498F-2409-402C-8967-2584DE20B134}\Triggers
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{7A0F498F-2409-402C-8967-2584DE20B134}\DynamicInfo

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Parent, LLC	Malware Process
	104.31.75.124	United States	13335	Cloudflare, Inc.	Malware Process
	184.26.44.97	United States	20940	Akamai Technologies, Inc.	OS Process
	209.48.71.168	United States	2828	MCI Communications Services, Inc. d/...	OS Process
ocsp.digicert.com	72.21.91.29	United States	15133	MCI Communications Services, Inc. d/...	Malware Process
crl4.digicert.com	66.225.197.197	United States	30081	Server Central Network	Malware Process
crl.globalsign.net	104.31.74.124	United States	13335	Cloudflare, Inc.	Malware Process
crl3.digicert.com	72.21.91.29	United States	15133	MCI Communications Services, Inc. d/...	Malware Process
crl.microsoft.com	209.107.208.81	United States	12989	BandCon	OS Process
ctldl.windowsupdate.com	209.107.208.58	United States	12989	BandCon	OS Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	82.048607111
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?37996abac9aa1534 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?37996abac9aa1534						
ocsp.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	94.2784280777
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBT3xL4LQLXDRDM9P665TW442vrsUQQUReuir%2FSSy4IxLVGLp6chnfNtyA8CEAQJGBtf1btmdVNDtW%2BVUAg%3D **URI:** http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBT3xL4LQLXDRDM9P665TW442vrsUQQUReuir%2FSSy4IxLVGLp6chnfNtyA8CEAQJGBtf1btmdVNDtW%2BVUAg%3D						
ocsp.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	101.781961918
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSnR4FoxLLkI7vkvsUIFlZt%2BlGH3gQUWsS5eyoKo6XqcQPAYPkt9mV1DlgCEAydKURKNdF6QYkQe19WQV0%3D **URI:** http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSnR4FoxLLkI7vkvsUIFlZt%2BlGH3gQUWsS5eyoKo6XqcQPAYPkt9mV1DlgCEAydKURKNdF6QYkQe19WQV0%3D						
crl3.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	107.930133104
Path: /sha2-assured-cs-g1.crl **URI:** http://crl3.digicert.com/sha2-assured-cs-g1.crl						
crl4.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	111.408811092
Path: /sha2-assured-cs-g1.crl **URI:** http://crl4.digicert.com/sha2-assured-cs-g1.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	164.702135086
Path: /pki/crl/products/tspca.crl **URI:** http://crl.microsoft.com/pki/crl/products/tspca.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	170.173187017
Path: /pki/crl/products/CodeSignPCA2.crl **URI:** http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	175.503479004
Path: /pki/crl/products/WinPCA.crl **URI:** http://crl.microsoft.com/pki/crl/products/WinPCA.crl						
crl.globalsign.net	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	180.85317111
Path: /primobject.crl **URI:** http://crl.globalsign.net/primobject.crl						

DNS QUERIES

Request	Type
ctldl.windowsupdate.com	A
Answers - ctldl.windowsupdate.nsatc.net (CNAME) - a1621.g.akamai.net (CNAME) - 209.48.71.144 (A) - 209.48.71.168 (A) - ctldl.windowsupdate.com.edgesuite.net (CNAME)	
ocsp.digicert.com	A
Answers - cs9.wac.phicdn.net (CNAME) - 72.21.91.29 (A)	
crl3.digicert.com	A
crl4.digicert.com	A
Answers - digicert.cachefly.net (CNAME) - 66.225.197.197 (A) - rvip1.ue.cachefly.net (CNAME)	
crl.microsoft.com	A
Answers - 184.26.44.97 (A) - 184.26.44.98 (A) - crl.www.ms.akadns.net (CNAME) - a1363.dscg.akamai.net (CNAME)	
crl.globalsign.net	A
Answers - 104.31.75.124 (A) - global.prd.cdn.globalsign.com (CNAME) - cdn.globalsigncdn.com.cdn.cloudflare.net (CNAME) - 104.31.74.124 (A)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
82.048607111	Sandbox	209.48.71.168	80
94.2784280777	Sandbox	72.21.91.29	80
107.930133104	Sandbox	72.21.91.29	80
111.408811092	Sandbox	66.225.197.197	80
164.702135086	Sandbox	184.26.44.97	80
180.85317111	Sandbox	104.31.75.124	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.23838400841	Sandbox	224.0.0.252	5355
3.28646302223	Sandbox	192.168.56.255	137
3.33368802071	Sandbox	224.0.0.252	5355
3.37640690804	Sandbox	239.255.255.250	3702
5.89276003838	Sandbox	224.0.0.252	5355
9.31402993202	Sandbox	192.168.56.255	138
75.2931129932	Sandbox	224.0.0.252	5355
78.6578540802	Sandbox	224.0.0.252	5355
81.6892559528	Sandbox	8.8.4.4	53
87.7592821121	Sandbox	224.0.0.252	5355
91.103976965	Sandbox	224.0.0.252	5355
94.2040860653	Sandbox	8.8.4.4	53
95.8373479843	Sandbox	224.0.0.252	5355
99.0643880367	Sandbox	224.0.0.252	5355
101.555022001	Sandbox	224.0.0.252	5355
104.700700998	Sandbox	224.0.0.252	5355
104.829384089	Sandbox	224.0.0.252	5355
107.535702944	Sandbox	8.8.4.4	53
108.363231897	Sandbox	224.0.0.252	5355
111.34683609	Sandbox	8.8.4.4	53
159.317404032	Sandbox	224.0.0.252	5355
162.012157917	Sandbox	224.0.0.252	5355
164.629028082	Sandbox	8.8.4.4	53
164.774133921	Sandbox	224.0.0.252	5355
167.584994078	Sandbox	224.0.0.252	5355
170.246599913	Sandbox	224.0.0.252	5355
172.924094915	Sandbox	224.0.0.252	5355
175.573209047	Sandbox	224.0.0.252	5355
178.239684105	Sandbox	224.0.0.252	5355
180.832628012	Sandbox	8.8.4.4	53

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp\Rus.Lng **C:\Program Files (X86)\Auslogics\Anti-Malware\Lang\Rus.Lng**	**Type :** data **MD5 :** e6504c0019035549de659bea0c0f0fbb **SHA-1 :** 57b92cd3e17f498ffc1722d31302967bf0a65b6a **SHA-256 :** c1eddc3f94c6e843c357b1018d826e209c7c4af7c379f1721b0f612 **SHA-512 :** a1a394b8ccf787ea67751226edc36260e8b64c20283bb39917303 **Size :** 101.902 Kilobytes.
C:\Windows\Sysnative\Tasks\Auslogics\Anti-Malware\Start Anti-Malware \Xd0\Xben User Logon	**Type :** XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators **MD5 :** d99ce12fa7328bb64f58c21ef33ac09e **SHA-1 :** c1acb13e92194a1cbfe83c4b3437b16ab9edea74 **SHA-256 :** e1fb3a4d164072d208a5a59869decf543063ada59a9b4f45f03cac **SHA-512 :** d1924b163cd20d99f8c142cd5a788924a48cdcd22ef8dbed3d899 **Size :** 3.576 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp\AxComponentsRTL.Bpl **C:\Program Files (X86)\Auslogics\Anti-Malware\AxComponentsRTL.Bpl**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 62d0be44a93b8cbd8b55beba4f4af702 **SHA-1 :** 955ccbfb8b9b92cdd19efd6d936817f5e1244193 **SHA-256 :** 387466f1c000fd10e45924ce978ec243be661f11a5fd3badc01f024 **SHA-512 :** df9c30a8bba33ba87b82485d33cd06fa91c03dfbbf031a16ffc0303 **Size :** 1792.584 Kilobytes.
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Auslogics\Anti-Malware\Auslogics Anti-Malware.Lnk	**Type :** MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Archive, ctime=Tue May 15 12:11:11 2018, mtime=Tue May 15 12:11:11 2018, atime=Mon Apr 16 08:27:50 2018, length=1904712, window=hide **MD5 :** 070d3a913408f75a6e1c7229499c9405 **SHA-1 :** ac14108cf46c1d1e0a415e0eac6a63676c9cd036 **SHA-256 :** 56b0300cb4d9d6dda8f291f1e4b47ce6d67c5cb3c9e515c0b314ac **SHA-512 :** ab1f81608cacbb02fc6208983dc06850185be7164a30363b839222 **Size :** 1.305 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp\Vclimg160.Bpl **C:\Program Files (X86)\Auslogics\Anti-Malware\Vclimg160.Bpl**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 23f4de2a720448099e7c33803b3f1b7b **SHA-1 :** 42c4e965a5168969c825cb9dd0374de1ac97345f **SHA-256 :** 7303a73ff4326d5ecabb6fdf52c0170db89b35ec67f5c5c960c4994 **SHA-512 :** 8c124c3a30f13ef9f1b67daea7945850f533df7e0847a28ddbe713t **Size :** 362.568 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** Microsoft Cabinet archive data, 6509 bytes, 1 file **MD5 :** 33b39e2a516ef730a8fa922894f0fbd5 **SHA-1 :** 03d455583dda59215d945af76af6293b202f586f **SHA-256 :** 9446e8f2056fea3ac1365a809ada04602606242c396f72ffe42fd1b **SHA-512 :** 75763aa13b43eb96294b0f84e13106611198872e06fb79f4af4f35 **Size :** 6.509 Kilobytes.
C:\Program Files (X86)\Auslogics\Anti-Malware\DebugHelper.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 36768d6cce882b3a7c6f7fc7fe5a2740 **SHA-1 :** 33a81ab7362efac343268d90378476d791f3c1e5 **SHA-256 :** 4db28b8c96b2494a21091948b38c34d413dc62a65d10174a6744 **SHA-512 :** 91425962a48783ce3e74c7e9d1b414858464787ef24db995073fe **Size :** 1099.848 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F4EA555947766F67C3BB52DEDFD509C5	**Type :** data **MD5 :** 76124fa025a43660f17bb93252e9664a **SHA-1 :** ffbe4c8533e3db11a57a83a5b19cfada44c71021 **SHA-256 :** 4703d71a179a93b4c131313cd3a676f23974d40ebfb8718ba7fc34 **SHA-512 :** bc7c36032418838e3c215e5679e809618dd5e1f8a960fe1e2c57ae **Size :** 0.212 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp\AntiMalware.Exe **C:\Program Files (X86)\Auslogics\Anti-Malware\AntiMalware.Exe**	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 268c75b169cd4ed8a4c6987e9538e8b5 **SHA-1 :** 28659896cfdc843b4740bbf3aba7446b9723da88 **SHA-256 :** 8e1cee98fc697664669112a4fd87b85d296cf60560c9e8afc6cabba **SHA-512 :** 0f4796fc651bc06ac2d1f929cb19a6dfe55c39ec1c5d365cee52a36 **Size :** 1904.712 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** data **MD5 :** bd07cd3b8f58f5a6bc89a500da708005 **SHA-1 :** 1e184ff7661736ec311c7b5cb49aecfbc23e0d1d **SHA-256 :** f9bfce47fb989312a3a56ea565694968a011412512397ccf2f7f253 **SHA-512 :** 7b6d16b501f508c9c591f490021386a4a643e7df99adae2e605a25 **Size :** 0.342 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Auslogics\Anti-Malware\Uninstall_Icon.Ico	**Type :** MS Windows icon resource - 8 icons, 16x16, 256-colors **MD5 :** fc1ac7453918b607f349dbbc776b940d **SHA-1 :** 4d090429b072f3545a4741d0a04521458f9eab0b **SHA-256 :** 94ae9d061102e1e8d3bc570115bf8836f42ddf1e04beed6cc6575 **SHA-512 :** 206b68d57c0a318f8ce7e12e8f1ac4eec336c8cc8a579f6ca0ba434 **Size :** 33.87 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp\Reader.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** 56efb0f436bc2a9cf61dc723b03558da **SHA-1 :** ee530e1d27b1fc7b3518c063270779a568e8f0f7 **SHA-256 :** e201cabb4803a83c2f5852a26ee07952258aaac6a9030d98dacb3 **SHA-512 :** 89e958c4c247be1c2cee2c74adc36755adc1e3964a1ef04f803266 **Size :** 514.048 Kilobytes.
C:\Program Files (X86)\Auslogics\Anti-Malware\CommonForms.Routine.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** f7556737aaa85dbdd14b78c405f6e971 **SHA-1 :** 4ea79b3bd236cad68c93b733ee001b069d6c4264 **SHA-256 :** 271bb737d4f6a4d2410f591973c6845e8968917b22258f725725a **SHA-512 :** b297b4a21e9e5fb6f91703c925ebcea81bb4396b51ed0bd3e591d **Size :** 670.28 Kilobytes.
C:\Windows\Sysnative\Wbem\Repository\OBJECTS.DATA	**Type :** data **MD5 :** aa5d461ceba38d4dba3a063fb04d012c **SHA-1 :** e1e4d4a078e92559474273bbb0eeae21c12661cb **SHA-256 :** 8586fabcc3a6fa57dd5446aab488879974588f1d4ce333c318b3b0 **SHA-512 :** 3be26d11b657ab420ac0db6ec0d2288bba308cd7a98803c3715a **Size :** 15450.112 Kilobytes.
C:\Program Files (X86)\Auslogics\Anti-Malware\Engine\Savapi.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** e04ef6cc6c067f0a269d36697d5802cb **SHA-1 :** 0c12dc3167ec1b20f277f7082dbcbedd4e24fbc6 **SHA-256 :** 0a80f1c72e13cb180dcf5b9602aa94175d0f32043ee7b737bbb352 **SHA-512 :** 858fed668802e22e1060120acd6905d86dd672b7d08aa36244d0 **Size :** 475.28 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp_isetup_shfoldr.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386 (stripped to external PDB), for MS Windows **MD5 :** 92dc6ef532fbb4a5c3201469a5b5eb63 **SHA-1 :** 3e89ff837147c16b4e41c30d6c796374e0b8e62c **SHA-256 :** 9884e9d1b4f8a873ccbd81f8ad0ae257776d2348d027d811a5647 **SHA-512 :** 9908e573921d5dbc3454a1c0a6c969ab8a81cc2e8b5385391d46b **Size :** 23.312 Kilobytes.
C:\Program Files (X86)\Auslogics\Anti-Malware\Data\Products.Json	**Type :** Little-endian UTF-16 Unicode text, with CRLF, CR line terminators **MD5 :** 27ae91b01c98ab68d44c919af67e0893 **SHA-1 :** 8705308b1370f21a69248100b4e27f8cd1983052 **SHA-256 :** e8546420af3600c447b806fc45786bcfd50e3e0c3eda7f847ccc031 **SHA-512 :** c0b038f695192066572fcc515d3c05bcbdd0fb740f1c62242715d5 **Size :** 7.15 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp\Esp.Lng **C:\Program Files (X86)\Auslogics\Anti-Malware\Lang\Esp.Lng**	**Type :** data **MD5 :** 768933e5818107e618c5043069f75743 **SHA-1 :** cbe857f81399e55d7d6ac25dcb8dffb791ad7a63 **SHA-256 :** 09aa2732107c46bab37268d4728e3cec164f1c673a09bcbebf3eb **SHA-512 :** 3b0558db8013917be8509507a30bdddd7640bbc933ee0ddbef16 **Size :** 109.724 Kilobytes.
C:\Program Files (X86)\Auslogics\Anti-Malware\Engine\Avupdate.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** b5b0dd04ddddb44972de19ef75a4ae9c **SHA-1 :** c6a6de68a431eea9f2ed1ede3abbdc3e22365e8b **SHA-256 :** dc1f006cab4270a6a3e60b42f33623d5f34a870ed4e9d6ea200542 **SHA-512 :** b371f0b0804f1594ff4d6a20fe7b7ec6bcc39b556b513ee36f0474a **Size :** 1713.104 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp\SetupCustom.Dll **C:\Program Files (X86)\Auslogics\Anti-Malware\Setup\SetupCustom.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 10de28c7f38f5422b41872fcf0285578 **SHA-1 :** f0681e47afdeb07041b905671285d95f1be21a16 **SHA-256 :** 0e7c7de5207f12b511d15bf77f45d89d878588261e1a391fea2367 **SHA-512 :** 86e0c7cbbd9061f147903d22917c6df07dd99f71ffaab0f7506457b **Size :** 671.816 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp\AxBrowsers.Dll **C:\Program Files (X86)\Auslogics\Anti-Malware\AxBrowsers.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 88584a00f1aca51770506d608d24a62f **SHA-1 :** f50e631ef2a34bac9ed4987d0359ae158a6acc03 **SHA-256 :** 6a01b3edd60b2ac06a0eded6bff4d295b70287ed36c38548a0ea3 **SHA-512 :** c1b94e76941fc9830bdf1661b4bf0013f7a42d00d15fb4a24c51c4 **Size :** 1642.568 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Auslogics\Anti-Malware\Engine\Savapi.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 8349856ac3008fd7b7b739d1d72bd5be **SHA-1 :** 41fc08e09643c1c31dac6b422623a045e3c13678 **SHA-256 :** 906fbbadab6fcd8adf71e35c66377f17078a5a23fac846c360655b6 **SHA-512 :** 4c948453e70586dff9f473d77637fd948d3d751e3b5e099cef959a **Size :** 507.784 Kilobytes.
C:\Windows\Sysnative\Wbem\Repository\INDEX.BTR	**Type :** data **MD5 :** 73fb0c58d683f0d4e3a6c688e57c0cc7 **SHA-1 :** 1e97f8a7f61c9c14dab1a7a41d1c6aed805da5fc **SHA-256 :** 91bbc39dbf7c37a8cfb5ea5bb7241282af3099cbd61b10efb1b304 **SHA-512 :** cbe21716154a7782ba5718645900c88d787c2da811c802e6b9be2 **Size :** 4587.52 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp\Fra.Lng **C:\Program Files (X86)\Auslogics\Anti-Malware\Lang\Fra.Lng**	**Type :** data **MD5 :** cc0bf8486fc8ed14b13237d2d5357652 **SHA-1 :** 3ca42d5d661a8b65e1e52686031a1580c8199e58 **SHA-256 :** fb9f3c11a2258364bba16a93089a5b9eed8786cde7ab68765481c **SHA-512 :** 3f371209dc71b1c458c8cc7de05baca343746c1045df39555ffc950 **Size :** 114.084 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-LIT24.Tmp\12af0c0e047b70ff8406407a6c5b49050f413fa7.Tmp **C:\Program Files (X86)\Auslogics\Anti-Malware\Unins000.Exe**	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 30f31bce70f8c1db468206e091d0a133 **SHA-1 :** a530f5bea69161833271716 00c7bb67456cd09d8 **SHA-256 :** 82df78393e37b9ae0243b1e3207c01d5ead52af99d9079024fa18 **SHA-512 :** ed4d0b949779de71e1dbb42315896241d0cc7d222d2eb76f4a8b **Size :** 1225.288 Kilobytes.
C:\Program Files (X86)\Auslogics\Anti-Malware\Engine\Avupdatelib_msg.Avr	**Type :** data **MD5 :** 38f689e76d38b04aef97e9fe195f3a08 **SHA-1 :** 04974454a1bc504f793170fda2327edaaf7f9262 **SHA-256 :** f886f2403502a2870523a609d2adb9dc6486129edccda9008d7ab **SHA-512 :** 9fba917bb987efc1b04d3c2c3bcf67dab02838d8ec8da6c3c74ad3 **Size :** 6.384 Kilobytes.
C:\Program Files (X86)\Auslogics\Anti-Malware\ActionCenterHelper.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** ac7cb71eb4cb9a98a3b6bf5282b0859f **SHA-1 :** 36ef5c94e0f42d8a06904b539a9c30c8b27b56f4 **SHA-256 :** a471f4bab053a3ecd2df6027333cb61b2650331b63dcd2ec29f6b8 **SHA-512 :** cf69c960bb7197b823790f969fce39e4db386e8c0de7bdac46073b **Size :** 373.32 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp\CommonForms.Site.Dll **C:\Program Files (X86)\Auslogics\Anti-Malware\CommonForms.Site.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 10c14c84b607e6dee1e661c9485e941d **SHA-1 :** 9f993d907e3353ba2128492ccdb9848f4d96a075 **SHA-256 :** b64d7602ec7770f9746316ce88e1aa8f8f78eadf6bf4b32a52904c8 **SHA-512 :** 9860d483b78280438169b3f51133139b3290b43c5dd123b1c98c9 **Size :** 606.792 Kilobytes.
C:\Program Files (X86)\Auslogics\Anti-Malware\Data\Database.Dat	**Type :** Zip archive data, at least v2.0 to extract **MD5 :** 3a91bdeaa2766100aec96c88e539d24a **SHA-1 :** dc43bd8cbdb9f4288a3cccb57be571bc61bae120 **SHA-256 :** 9102e71c5a03f825bd28d3a6b21f9dd61515441d1ea0633154833 **SHA-512 :** 7513241714d5692367144f715d7ab83ad9baff7cfe741349917e12 **Size :** 1.917 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp_isetup_setup64.Tmp	**Type :** PE32+ executable (console) x86-64, for MS Windows **MD5 :** e4211d6d009757c078a9fac7ff4f03d4 **SHA-1 :** 019cd56ba687d39d12d4b13991c9a42ea6ba03da **SHA-256 :** 388a796580234efc95f3b1c70ad4cb44bfddc7ba0f9203bf4902b9 **SHA-512 :** 17257f15d843e88bb78adcfb48184b8ce22109cc2c99e709432728 **Size :** 6.144 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp\GASender.Exe **C:\Program Files (X86)\Auslogics\Anti-Malware\GASender.Exe**	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 0b7f861a428b850ae72335c233ef9038 **SHA-1 :** 9927d3e5c3adfec290ea37b47681038944b4c59c **SHA-256 :** b6acaec75ad50ec30d88919624e86128fbf397228062c225ccff340 **SHA-512 :** 19eb0d9f0fabe5f8300938df301a5345565db94af64d1596b9a7fbl **Size :** 40.52 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp\Enu.Lng **C:\Program Files (X86)\Auslogics\Anti-Malware\Lang\Enu.Lng**	**Type :** data **MD5 :** aceb000de11f8ce4d4b52ba54585e627 **SHA-1 :** da38044bae6a1ce543ef41adf7697ffde64539af **SHA-256 :** 04fa5455348f8b9bd877b332fc55c7e585d41b09c154841b2e1c41 **SHA-512 :** ae25115f3b317ec1648b92eb1213515d875d20995dfc36b40969e **Size :** 100.922 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp\Jpn.Lng **C:\Program Files (X86)\Auslogics\Anti-Malware\Lang\Jpn.Lng**	**Type :** data **MD5 :** 82b2fd229bdf53b8468be214f15319a1 **SHA-1 :** 9cbc4acbe0be04123126a86d8582f86933293e7a **SHA-256 :** 9923232c86175709c9597aa3af2ca0b221527dd32f04cf6b2563b1 **SHA-512 :** d9541661b01601ff94accb3356b32af164e6874c99c28c4c2a4228f **Size :** 81.006 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp\Localizer.Dll **C:\Program Files (X86)\Auslogics\Anti-Malware\Localizer.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 6af74bebdf3c1d19a0ea156a72c6f795 **SHA-1 :** 939b4e720bf5d4fc9c172ee5673a0910e96c6057 **SHA-256 :** 8ee3a0d5d8941fabc1a97fcbc491439ed4838d7b6370d78a85f31e **SHA-512 :** 5fcacb733c5b2078cfdb95d723857435f74017810a6289331cabdd **Size :** 187.464 Kilobytes.
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Auslogics\Anti-Malware\Uninstall Auslogics Anti-Malware.Lnk	**Type :** MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Icon number=0, Archive, ctime=Tue May 15 12:11:06 2018, mtime=Tue May 15 12:11:06 2018, atime=Tue May 15 12:10:45 2018, length=1225288, window=hide **MD5 :** 3544cf78f4a4aa700cdefcf9454bd040 **SHA-1 :** 8559afb68f6d891d528c42d9090a290c34424544 **SHA-256 :** 64b27fa9e6952d37c132d6126d7bdc78dab65e2d1398c4a2a6942 **SHA-512 :** e366eb324ddd1f1f0bb108de5df7bd30ea177c23b7543acd61d0a **Size :** 1.321 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp\Vcl160.Bpl **C:\Program Files (X86)\Auslogics\Anti-Malware\Vcl160.Bpl**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** b1a711606d65dbf08f92d85f255b4723 **SHA-1 :** eda2b8a7e73b2e9afa21da58763ef56cfd780d4f **SHA-256 :** 35b546b3db4ef5e0644816f5c1e400cc4b81670a35d1dea71a386a **SHA-512 :** 7475ebab04894869236a604af6c2e3ef2b8b7280c45704cf808ef7(**Size :** 3425.352 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp\Rtl160.Bpl **C:\Program Files (X86)\Auslogics\Anti-Malware\Rtl160.Bpl**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 21de1536d26fc7095a938a6b1fc163f9 **SHA-1 :** ea3a0cc04d95da28717059a8e787f0a836c335e4 **SHA-256 :** 2df34a963fc546a6ed433bea9b722d71911e0a2242e5f67db994ab **SHA-512 :** e6739d6071fb97104c60fbd385282aa41c2a7a04249042490c3a0e **Size :** 2897.48 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp\AxComponentsVCL.Bpl **C:\Program Files (X86)\Auslogics\Anti-Malware\AxComponentsVCL.Bpl**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** b9d42f50450f4fc3e594af510376b168 **SHA-1 :** 90dc7f72fd0d7e9d29872d2f99150505dc91874d **SHA-256 :** e9b2cfd3cc03b3e6e1b96caf935c208033771d9f64ecf2d0db3108 **SHA-512 :** 068f9d8779ee8ab9341d3b0798c4c90076cdf0a73ca2649ad59547 **Size :** 4179.016 Kilobytes.
C:\Users\User\Desktop\Auslogics Anti-Malware.Lnk	**Type :** MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Archive, ctime=Tue May 15 12:11:11 2018, mtime=Tue May 15 12:11:11 2018, atime=Mon Apr 16 08:27:50 2018, length=1904712, window=hide **MD5 :** 9e16deaf1436ee97c7e44357d7624413 **SHA-1 :** dbe17d04bf84435e45c5b1884fa348f3143a679e **SHA-256 :** 0fac07e01e3fef6f144b61c122281df14237367b7b3c4ddbcadda39 **SHA-512 :** 2a6765d613fb44a5298871065bed8abac8b5a1fb323bc783cfccd7 **Size :** 1.281 Kilobytes.
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Auslogics\Anti-Malware\Auslogics Anti-Malware On The Web.Url	**Type :** MS Windows 95 Internet shortcut text (URL=< >), **MD5 :** 3291ffc8ba4faa0bd89f3c790a172462 **SHA-1 :** 3b8eb67e402bf1233c06268da055e9104544d864 **SHA-256 :** 6bbeec6fa7d52623d326014b0104dad120d43dd1b020cdb9b476 **SHA-512 :** 823f98a037e992d7c6eaca465115082e5b7bf1ba12fd74440a9fdd **Size :** 0.127 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\0E506CEBBC8B162CFB2D72DB4891DCAE **C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\F4EA555947766F67C3BB52DEDFD509C5**	**Type :** data **MD5 :** 628e84a3fb23cf90dcb17f68761d7955 **SHA-1 :** ff88dce72d56a8d566a2a2a6b7e3bf96ec4ad64d **SHA-256 :** 6c80e5ff73e51032954ba3e81a2d04649246bd8fc5894be7f38d02 **SHA-512 :** 2932ae962aaa9b4128869f760f4561dbf106be43a7adbdb1b5a7e **Size :** 17.019 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp\GoogleAnalyticsHelper.Dll **C:\Program Files (X86)\Auslogics\Anti-Malware\GoogleAnalyticsHelper.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** add0b39c6d77f72d25742cb75de481d9 **SHA-1 :** 1b3030fe828811ae69801efc5f21ede19fccb0ab **SHA-256 :** 7b5490298245b9b33c1500cd456c0476b61f511f0c39c64041a04c **SHA-512 :** 45084c41e541ba23ba970fd2c0ed4f2f8672214fdbbcf5215f4bc6b **Size :** 368.2 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Windows\Sysnative\Wbem\Repository\MAPPING3.MAP	**Type :** data **MD5 :** 74b57351c8e8a14e090917d231fbca90 **SHA-1 :** 170bb7085e232a1ab83fb53ca50694dbc5829e0e **SHA-256 :** 02ac6f89d9544165b6e3551f3cb612d85e2eaf950e9bf472a7be4e **SHA-512 :** 8a695a95653300f6f3c7182e05f61f65f0d79e1321074d10cd8736c **Size :** 50.536 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\42B9A473B4DAF01285A36B4D3C7B1662_178C086B699FD6C56B804AF3EF759CB5	**Type :** data **MD5 :** 793399451376281d0360abe4fca8f735 **SHA-1 :** 9548ed797472af17d43e3e00ab543d197f6a6a7c **SHA-256 :** 244d27e718bfedcaac21ee9592dc59e1c56d45469a6fb22e6137ce **SHA-512 :** 1591f907b274382e006af8aca8e0330059d0855bc09088d59dbe2 **Size :** 0.434 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp\CFAHelper.Dll **C:\Program Files (X86)\Auslogics\Anti-Malware\CFAHelper.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** ce6412354a97cdce986b775279c6c07e **SHA-1 :** 4013410bbacb4484bd2de298a028e4747741d3e6 **SHA-256 :** 723b5990bca5d25a7f12eb3bcb6d2bc73d51841bec8d95af48551 **SHA-512 :** 25595d73df8e2439e4fc3afb75dd13f9b325d70e24bc046134cc1fc **Size :** 93.768 Kilobytes.
C:\Users\User\AppData\Local\GDIPFONTCACHEV1.DAT	**Type :** data **MD5 :** 696bad2ef23da7f0ccaaa7f76ab9fdf0 **SHA-1 :** 0efe907b47e8331cf56a95c0c06d324257ece202 **SHA-256 :** bd27979561fac15e4043fc980ad62f24f00738cba1f22b8e45cf1d5 **SHA-512 :** fb1a4afdbf5f9e3d7e55eb806f660057927d6c35740c69ed2790fd7 **Size :** 84.528 Kilobytes.
C:\Program Files (X86)\Auslogics\Anti-Malware\ActionCenterForms.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** a8538ef0c20fb33db0a15a8d1b994680 **SHA-1 :** 533f202e17683dde5e82873c61bfaad741982c6a **SHA-256 :** 6f51d1dd6a861afc86e67843a073cbde51fe4838774b39bdfb2e5d **SHA-512 :** 777a52f012ac91817fca17c2b5ab11f136589d5e04a07a2fd56c98t **Size :** 1169.992 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\42B9A473B4DAF01285A36B4D3C7B1662_178C086B699FD6C56B804AF3EF759CB5	**Type :** data **MD5 :** d0ca602196cc5fbf561d2fe9c1d9ef69 **SHA-1 :** 60ca266818a8c53f7dd81c369451d0c4301a506b **SHA-256 :** c6c025aa73d6ed18081e0ec65fb3df98ca2db5c2dea5c7af3fb1e5(**SHA-512 :** 7e406d558b834e07076ee78e80a145853b5edd2c621fc82ba2960 **Size :** 0.471 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp\Sqlite3.Dll **C:\Program Files (X86)\Auslogics\Anti-Malware\Sqlite3.Dll**	**Type :** PE32 executable (DLL) (console) Intel 80386, for MS Windows **MD5 :** 09f8221b5b0b08dd30c42fb11f9fb082 **SHA-1 :** ce853139e6a028cde457837400230c4203644f5a **SHA-256 :** 6ef6f1ec27fc1b74a9e3e84708aacb015b324246980db090b13c35 **SHA-512 :** 1732e35bc068560025e23f295173b8a2f5f6a8eba6f7e29ec43788 **Size :** 674.232 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp\Deu.Lng **C:\Program Files (X86)\Auslogics\Anti-Malware\Lang\Deu.Lng**	**Type :** data **MD5 :** 4e0ffab92339277ceff25b564e5753f6 **SHA-1 :** a52f8a791b081cb077d8fe24b83eb1ba110e2079 **SHA-256 :** 49c8be4f36adc2a1d282a04bf16becdd4324fd49ab08e2391a414 **SHA-512 :** 2c53fe25730e4c0fbae68dc35e207c3fb066b703acb44014304aae **Size :** 112.486 Kilobytes.
C:\Program Files (X86)\Auslogics\Anti-Malware\Engine\Savapi_stub.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** 615a882bb1c71805036fea4fc9dbedeb **SHA-1 :** 3b2c7704b9ca20b09236883e9c6ca5d051952ca6 **SHA-256 :** 12756161383f1064ad9d3a2fefffff0ddbc5a77838f04e5760bf41d6(**SHA-512 :** 154b5210ac31875114f6f517412200567fc76f8cb0468955ba1d21 **Size :** 84.424 Kilobytes.
C:\Program Files (X86)\Auslogics\Anti-Malware\TaskSchedulerHelper.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 0c3e0c8d97c6993b4164d8b4b968caf0 **SHA-1 :** 6832d78d772951c6403f9ef84de639974f94f3f0 **SHA-256 :** abf9b8f581a24866e853500244f6696771131630e282f548c29798 **SHA-512 :** 6c9683baf4fee46a5f5fef3c4057b438c165779b7586b1e91a4385b **Size :** 289.352 Kilobytes.
C:\Program Files (X86)\Auslogics\Anti-Malware\Engine\Productname.Dat	**Type :** ASCII text, with no line terminators **MD5 :** 0871de36436c555db30372ce9978fbd4 **SHA-1 :** 839409bd05faffe4c275081a7e6a2ca2376490c7 **SHA-256 :** e697202592e0a5477dc8ffe32d9ba72a0618efefbe8e03f2031242(**SHA-512 :** 4af09f5884d6a5af3281e4f06438f2cfd75452191cad82c64dffb871 **Size :** 0.015 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Auslogics\Anti-Malware\Unins000.Msg	**Type :** data **MD5 :** 5f38274fc51ec35b61e925153e26ef1c **SHA-1 :** 6ebc957cc000873b9b88e32c271fc1c63a5c22e5 **SHA-256 :** 946195c199c2f798ed0ab3dc8ae4511be30ad70e5fb994d677bee **SHA-512 :** 1f99244af85ef4d175426a38c5181bf0205f9dfc0deb4fc1136f43cc **Size :** 22.701 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\66AE3BFDF94A732B262342AD2154B86E_25904FBC7E43A1F0AEF65C8ED7D7B472	**Type :** data **MD5 :** 13890387f7984356a32b045e76a65da3 **SHA-1 :** e478e7609e9fcc9e36d2005787b4eb1d8e7b3824 **SHA-256 :** d05b29411f0caf7739ed30db2461febf693d9f025fa97dc8e5227c8 **SHA-512 :** b62af7e755e41abc73aed632937620ea8e124ea8af4f4037c95ec1 **Size :** 0.471 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\0E506CEBBC8B162CFB2D72DB4891DCAE	**Type :** data **MD5 :** caa1507f155e216d8a6edffa4ba84dee **SHA-1 :** 79fda8d21c2865ed39d148562b516e9b52d6e512 **SHA-256 :** a8b295ebf8a798f5f57b929e1d66c1e8d6288b1dff6ae52f849504 **SHA-512 :** e63623f6403692b1ad20d27b366356d154727cc437fe02d7313ba **Size :** 0.236 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\66AE3BFDF94A732B262342AD2154B86E_25904FBC7E43A1F0AEF65C8ED7D7B472	**Type :** data **MD5 :** 26ed6794b433404a9e89a423c9c34223 **SHA-1 :** 0ca9accbe913342332b9efc25c73cf9fb9bc4d3a **SHA-256 :** 311c2356750932ab607ed5694cb46e70e66b2395103796462f3b8 **SHA-512 :** 5d0517c43192cd2a328135e0db699cd9aba686f85023b8ea6c50f **Size :** 0.43 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp\EULA.Rtf **C:\Program Files (X86)\Auslogics\Anti-Malware\EULA.Rtf**	**Type :** Rich Text Format data, version 1, ANSI **MD5 :** 2b62c4eb0b0fb6c38a88dc54d909c84d **SHA-1 :** 6800cd0ac9e99c3dbaf6077a1d12a7d419908ed2 **SHA-256 :** ec31153959c8fe031ea552beaed98cd32f8ccded36955ad7f70773 **SHA-512 :** 305bca65661836dc24875a6231d81be0f73b9df763d93917fe6b2 **Size :** 24.714 Kilobytes.
C:\Program Files (X86)\Auslogics\Anti-Malware\SendDebugLog.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 882bc47a6131785fe13325a5047a4b3e **SHA-1 :** b43796a71afa01d67e466163e9859d795b3a0f6c **SHA-256 :** 91b9003683e21a157073c69127aaeec95b7da591efc55fec2917e7 **SHA-512 :** adcedec921a2f61bd8067d0ed491eda4b38a10d50b81acdcf32df **Size :** 523.848 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp\Main.Ini **C:\Program Files (X86)\Auslogics\Anti-Malware\Data\Main.Ini**	**Type :** ASCII text, with CRLF line terminators **MD5 :** 3c3b6065a814abd792ec2ce2f61b9cab **SHA-1 :** ce62f0ae60fc75c965e6a87ab59ea6ba9647b66e **SHA-256 :** bc17562ae2723c29b74e6a2e90471d76b60af7b3839db3b4adb3c **SHA-512 :** 5bc316bd2ddbe3e6309ee66d51796a31c3d904a970b52f78b194f **Size :** 0.745 Kilobytes.
C:\Program Files (X86)\Auslogics\Anti-Malware\Unins000.Dat	**Type :** data **MD5 :** 4396a6dbf926995ea4511312f579b436 **SHA-1 :** a3b874a86fe616bb2ac01666a9e0bfa0bedb2763 **SHA-256 :** b25972264298dbe3f49c6a7a4c417b17b3a6394cca25be6d8aaa5 **SHA-512 :** dc04aeb40d8c621c4bc1d40cf2abe5b2dbeb883c28d5c691742ff2 **Size :** 47.739 Kilobytes.
C:\Program Files (X86)\Auslogics\Anti-Malware\Engine\HBEDV.Key	**Type :** data **MD5 :** a68d4746af14eef57ff17bbdb3902c23 **SHA-1 :** 9ee0d7471c4a31420827f58ed90f39106e6bf872 **SHA-256 :** 4427157b5fa1ba2954020ac4b7f30054aa3bebab1e8f98eb6dcf37 **SHA-512 :** 1228db598c0e39c1a5d42eaec892d22b919ec81131acd5b258e98 **Size :** 0.512 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-TF58U.Tmp\Ita.Lng **C:\Program Files (X86)\Auslogics\Anti-Malware\Lang\Ita.Lng**	**Type :** data **MD5 :** 7f8fc8ba70d84ad4420d80a4ee69e459 **SHA-1 :** 08b46f4b750b202362feabf8b183ea33a1362442 **SHA-256 :** 343601b704e41dd197441f662f84bc56458f770a90f30838f0009c **SHA-512 :** 897d8bebafc38e24aab4d414ce701762edd6bfb096b4662c1b439 **Size :** 110.934 Kilobytes.
C:\Program Files (X86)\Auslogics\Anti-Malware\AntiMalwareHelper.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 6269f779ae7f693a5af822a57da6ea59 **SHA-1 :** 656146d978f77cc3f6d009c3734013392b0a5ed0 **SHA-256 :** e736784e1c064b4ff52a9bde9871e761cef91339341c8122f1f17aa **SHA-512 :** e6d76caf14dd75d6011582f25752d96d8ac282ff8c0fecdc0008bb1 **Size :** 747.08 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	None
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	12af0c0e047b70ff8406407a6c5b49050f413fa7
MD5:	3b1086235aead2a5cf61ec6e8728edb9
First Seen Date:	2018-05-15 12:55:16.233717 (about a year ago)
Number Of Clients Seen:	2
Last Analysis Date:	2018-05-15 12:55:16.233717 (about a year ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	8
Trid	[[57.2, u'Win32 Executable Delphi generic'], [18.2, u'Win32 Executable (generic)'], [8.3, u'Win16/32 Executable Delphi generic'], [8.0, u'Generic Win/DOS Executable'], [8.0, u'DOS Executable Generic']]
Compilation Time Stamp	0x55A7B084 [Thu Jul 16 13:24:20 2015 UTC]
LegalCopyright	Copyright \xa9 2008-2018 Aus\x98logics Labs Pty Ltd
FileVersion	1.x
CompanyName	Auslog\x98ics
Comments	This installation was built with Inno Setup.
ProductName	Auslog\x98ics Anti-Mal\x98ware
ProductVersion	1.13.0.0
FileDescription	Auslog\x98ics Anti-Mal\x98ware Installation File
Translation	0x0000 0x04b0
Entry Point	0x4113bc (.itext)
Machine Type	Intel 386 or later - 32Bit
File Size	8269720
Ssdeep	196608:Ihkpcy+byBtjkrcrEYINuzdvo7dSeH5zXYaZ5yzaTO:h8OBxtIIASeH5blyR
Sha256	550628db5a084ae116740d7167aa437bce5302b0f8fdd69a33c58317c4b93733
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/1/2/a/f/12af0c0e047b70ff8406407a6c5b49050f413fa7', u'EXE:ProductName': u'Auslog\x98ics Anti-Mal\x98ware ', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2018:05:15 11:38:33+00:00', u'EXE:InitializedDataSize': 88064, u'File:FileModifyDate': u'2018:05:15 11:38:33+00:00', u'EXE:FileVersionNumber': u'1.13.0.0', u'EXE:FileVersion': u'1.x ', u'File:FileSize': u'7.9 MB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:ProductVersion': u'1.13.0.0 ', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'Auslog\x98ics ', u'File:FileName': u'12af0c0e047b70ff8406407a6c5b49050f413fa7', u'EXE:ImageVersion': 6.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 5.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2015:07:16 13:24:20+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LegalCopyright': u'Copyright \xa9 2008-2018 Aus\x98logics Labs Pty Ltd ', u'EXE:LinkerVersion': 2.25, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/1/2/a/f', u'EXE:FileDescription': u'Auslog\x98ics Anti-Mal\x98ware Installation File ', u'EXE:EntryPoint': u'0x113bc', u'EXE:SubsystemVersion': 5.0, u'EXE:CodeSize': 65024, u'EXE:Comments': u'This installation was built with Inno Setup.', u'File:FileInodeChangeDate': u'2018:05:15 11:38:33+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'Neutral', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'1.13.0.0'}]
Mime Type	application/x-dosexec
Imphash	48aa5c8931746a9655524f67b25a47ef

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0xf134	0xf200	6.39164664964	1b89617b988c8bd575544f47f0d04258
.itext	0x11000	0xb44	0xc00	5.74123824537	25478d452b599b551fe11bfb5904d2d0
.data	0x12000	0xc88	0xe00	2.24753305436	0c3e63b09234b01ce16cff38df28bb6f
.bss	0x13000	0x56b8	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.idata	0x19000	0xdd0	0xe00	4.97188203377	93d91a2b90e60bd758fc0c4908856ae1
.tls	0x1a000	0x8	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0x1b000	0x18	0x200	0.20448815744	3dffc444ccc131c9dcee18db49ee6403
.rsrc	0x1c000	0x138e0	0x13a00	5.28443886421	4b82b8a35a5c473de7d9dfbc7df01547

PE Imports

- oleaut32.dll
  - SysFreeString
  - SysReAllocStringLen
  - SysAllocStringLen
- advapi32.dll
  - RegQueryValueExW
  - RegOpenKeyExW
  - RegCloseKey
- user32.dll
  - GetKeyboardType
  - LoadStringW
  - MessageBoxA
  - CharNextW
- kernel32.dll
  - GetACP
  - Sleep
  - VirtualFree
  - VirtualAlloc
  - GetSystemInfo
  - GetTickCount
  - QueryPerformanceCounter
  - GetVersion
  - GetCurrentThreadId
  - VirtualQuery
  - WideCharToMultiByte
  - MultiByteToWideChar
  - lstrlenW
  - lstrcpynW
  - LoadLibraryExW
  - GetThreadLocale
  - GetStartupInfoA
  - GetProcAddress
  - GetModuleHandleW
  - GetModuleFileNameW
  - GetLocaleInfoW
  - GetCommandLineW
  - FreeLibrary
  - FindFirstFileW
  - FindClose
  - ExitProcess
  - WriteFile
  - UnhandledExceptionFilter
  - RtlUnwind
  - RaiseException
  - GetStdHandle
  - CloseHandle
- kernel32.dll
  - TlsSetValue
  - TlsGetValue
  - LocalAlloc
  - GetModuleHandleW
- user32.dll
  - CreateWindowExW
  - TranslateMessage
  - SetWindowLongW
  - PeekMessageW
  - MsgWaitForMultipleObjects
  - MessageBoxW
  - LoadStringW
  - GetSystemMetrics
  - ExitWindowsEx
  - DispatchMessageW
  - DestroyWindow
  - CharUpperBuffW
  - CallWindowProcW
- kernel32.dll
  - WriteFile
  - WideCharToMultiByte
  - WaitForSingleObject
  - VirtualQuery
  - VirtualProtect
  - VirtualFree
  - VirtualAlloc
  - SizeofResource
  - SignalObjectAndWait
  - SetLastError
  - SetFilePointer
  - SetEvent
  - SetErrorMode
  - SetEndOfFile
  - ResetEvent
  - RemoveDirectoryW
  - ReadFile
  - MultiByteToWideChar
  - LockResource
  - LoadResource
  - LoadLibraryW
  - GetWindowsDirectoryW
  - GetVersionExW
  - GetUserDefaultLangID

- GetThreadLocale
- GetSystemInfo
- GetStdHandle
- GetProcAddress
- GetModuleHandleW
- GetModuleFileNameW
- GetLocaleInfoW
- GetLastError
- GetFullPathNameW
- GetFileSize
- GetFileAttributesW
- GetExitCodeProcess
- GetEnvironmentVariableW
- GetDiskFreeSpaceW
- GetCurrentProcess
- GetCommandLineW
- GetCPInfo
- InterlockedExchange
- InterlockedCompareExchange
- FreeLibrary
- FormatMessageW
- FindResourceW
- EnumCalendarInfoW
- DeleteFileW
- CreateProcessW
- CreateFileW
- CreateEventW
- CreateDirectoryW
- CloseHandle

- advapi32.dll
  - RegQueryValueExW
  - RegOpenKeyExW
  - RegCloseKey
  - OpenProcessToken
  - LookupPrivilegeValueW
- comctl32.dll
  - InitCommonControls
- kernel32.dll
  - Sleep
- advapi32.dll
  - AdjustTokenPrivileges

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 115980, u'sha256': u'33a31ef9260ae895b7a79c341a0f8f246cc9f9f153519ff02d6e7656831a52c5', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 117108, u'sha256': u'c0ff506db9e74711cce2085055b2d88d28e3208a93c14e783c69122c7613eb32', u'type': u'data', u'size': 1720}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 118828, u'sha256': u'19a1958500ad997bb739fc0f5453f56e5d932cf4cc1a2a46dac8d5c03abe883b', u'type': u'data', u'size': 2440}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 121268, u'sha256': u'268afc977ceb9a3278dc61d103283f6a56feb302847f6600e175b84717b45faa', u'type': u'data', u'size': 2848}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 124116, u'sha256': u'd623118038f7295789dd4be0cf0ae0b102fbddaa5863dfb7aa6ec752e9509147', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 128380, u'sha256': u'fd3b6166d835cf4107f05d13787325c73784617b1f0f9b7fc76644aa2d8ac26c', u'type': u'data', u'size': 4936}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 133316, u'sha256': u'02cea9b0bb85cc5376eafbb282304ee712f2388f0eecbd627f74e950ba936a69', u'type': u'data', u'size': 5512}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 138828, u'sha256': u'527eeb0fcd9420d1faa2130c406e284563e2c1faa9c401d547ac019f4235cb63', u'type': u'dBase III DBT, version number 0, next free block index 40', u'size': 6760}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 145588, u'sha256': u'fc718cc3bc4ad183363b4eccfb984fe7376697d52743404bdb5155dd1b027c6b', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 155228, u'sha256': u'34ea1c2173226ecc593f8a2b0224c51ebbee1928715bda9339eec7717a822b89', u'type': u'data', u'size': 104}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 155332, u'sha256': u'e1d818d622875ce2cf81883816ef982aa05a724c46f82b3e67875e0bc24228b1', u'type': u'data', u'size': 212}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 155544, u'sha256': u'80bc91470ef70d527d0c4e0824945bc3b17ff84f464bca425661c3e7e1972ce7', u'type': u'data', u'size': 164}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 155708, u'sha256': u'33ef72f38fc1fe2842c44e11bb351f94385bb186fee0fadbefc9364ed52aeb93', u'type': u'data', u'size': 684}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 156392, u'sha256': u'7f63f3f944a0b62f8f3b35a60141081599f7f175605ced7e1b4dcb80fda58c8a', u'type': u'data', u'size': 844}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 157236, u'sha256': u'cb21f2b28bfc6b8046348c7a96bf97149dc5f91e1cc1a4f2904a1044a008425a', u'type': u'data', u'size': 660}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_RCDATA', u'offset': 157896, u'sha256': u'677245e2a6b2eb5495b4965b8c26025a4b26e8b8c21a825f658cb390b493b9a0', u'type': u'data', u'size': 33512}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 191408, u'sha256': u'88d14cc6638af8a0836f6d868dfab60df92907a2d7becaefbbd7e007acb75610', u'type': u'Sendmail frozen configuration ', u'size': 16}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 191424, u'sha256': u'abd66b63471de2699c97d06e41cfe0702144237079f76a9e0bd965b1a1862231', u'type': u'data', u'size': 336}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 191760, u'sha256': u'3ef928fab6e499178cb29b0708a88d2243b9e3ad49254869b7f241ae60f682b8', u'type': u'data', u'size': 44}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 191804, u'sha256': u'92c60f55cdcac8b941351dad3052fbfadb4726d9a95a27efd3d0d8c5066d44df', u'type': u'MS Windows icon resource - 9 icons, 16x16', u'size': 132}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 191936, u'sha256': u'77f5e91df14c99f6640e729b32d97fa9d4856ac03068515af08260fd858344ee', u'type': u'data', u'size': 1268}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 193204, u'sha256': u'356ca8abf11d97bf9dcbff47c04bf1ddcb8685ef84d38e6850ec6c28a37655b9', u'type': u'XML 1.0 document, ASCII text, with CRLF line terminators', u'size': 1580}

CERTIFICATE VALIDATION

- Success ✔

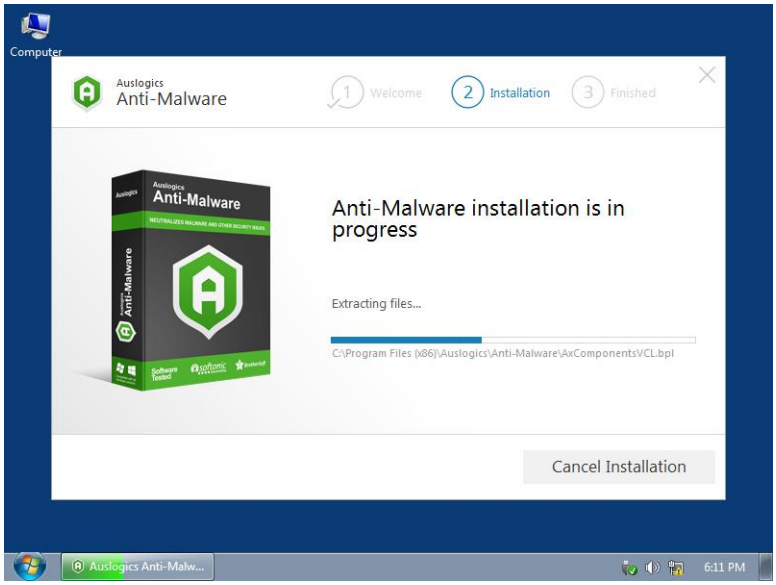
[+] Auslogics Labs Pty Ltd	
Status	NoError ✔
Start Date	2017-12-26 02:00:00
End Date	2021-02-25 02:00:00
Sha256	09ebf174caf21d029b4b3765ddb93060d49e1b299e02987abdc864b7868159a5
Serial	0CE3393B656B06DD15D58A60C4C05DD7
Subject Key Identifier	f4 37 82 92 8f 86 29 be fa 9c 6e 17 16 6e 7f 10 a7 55 b7 da
Issuer Name	DigiCert EV Code Signing CA (SHA2)
Issuer Key Identifier	8f e8 7e f0 6d 32 6a 00 05 23 c7 70 97 6a 3a 90 ff 6b ea d4
Crl link	http://crl3.digicert.com/EVCodeSigningSHA2-g1.crl,http://crl4.digicert.com/EVCodeSigningSHA2-g1.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

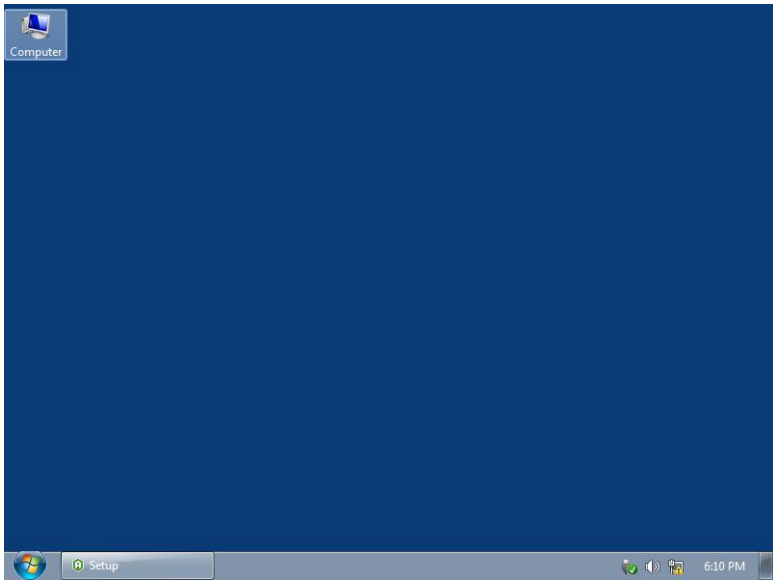
[+] DigiCert EV Code Signing CA (SHA2)	
Status	NoError ✔
Start Date	2012-04-18 03:00:00
End Date	2027-04-18 03:00:00
Sha256	a692c7403bfd72f70438cf1a7fb928c92820e4c0c1cfd457497aa0b69b67a5ed
Serial	03F1B4E15F3A82F1149678B3D7D8475C
Subject Key Identifier	8f e8 7e f0 6d 32 6a 00 05 23 c7 70 97 6a 3a 90 ff 6b ea d4
Issuer Name	DigiCert High Assurance EV Root CA
Issuer Key Identifier	b1 3e c3 69 03 f8 bf 47 01 d4 98 26 1a 08 02 ef 63 64 2b c3
Crl link	http://crl3.digicert.com/DigiCertHighAssuranceEVRootCA.crl,http://crl4.digicert.com/DigiCertHighAssuranceEVRootCA.crl
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

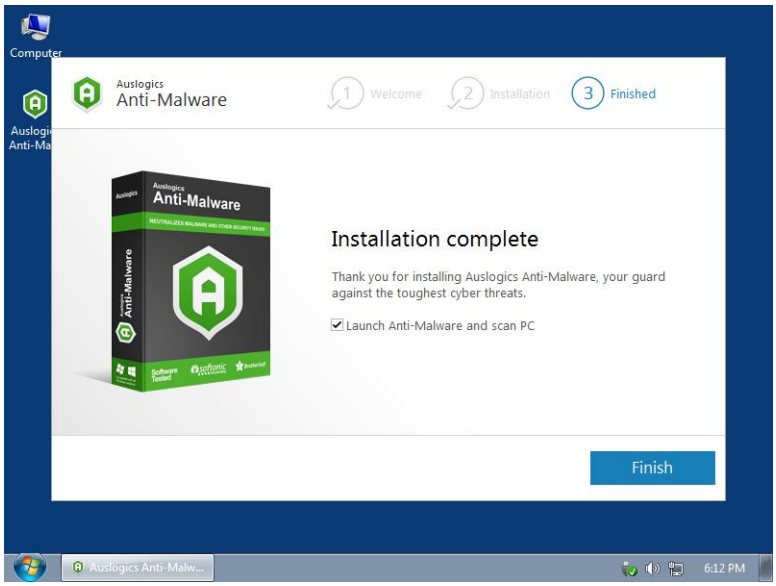
[+] DigiCert High Assurance EV Root CA	
Status	NoError ✔
Start Date	2006-11-10 02:00:00
End Date	2031-11-10 02:00:00
Sha256	ed960860d0e06c89fa3ff7723437b6812c6d7e1ad370c7885b1251d2e1c2a938
Serial	02AC5C266A0B409B8F0B79F2AE462577
Subject Key Identifier	b1 3e c3 69 03 f8 bf 47 01 d4 98 26 1a 08 02 ef 63 64 2b c3
Issuer Name	DigiCert High Assurance EV Root CA
Issuer Key Identifier	b1 3e c3 69 03 f8 bf 47 01 d4 98 26 1a 08 02 ef 63 64 2b c3
Crl link	undefined
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	undefined

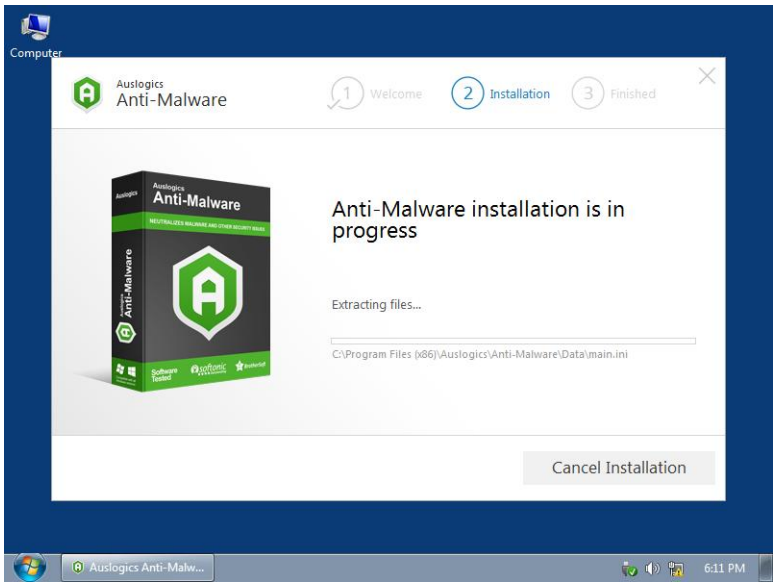
[+] DigiCert High Assurance EV Root CA	
Status	NoError ✔
Start Date	2006-11-10 02:00:00
End Date	2031-11-10 02:00:00
Sha256	ed960860d0e06c89fa3ff7723437b6812c6d7e1ad370c7885b1251d2e1c2a938
Serial	02AC5C266A0B409B8F0B79F2AE462577
Subject Key Identifier	b1 3e c3 69 03 f8 bf 47 01 d4 98 26 1a 08 02 ef 63 64 2b c3
Issuer Name	DigiCert High Assurance EV Root CA
Issuer Key Identifier	b1 3e c3 69 03 f8 bf 47 01 d4 98 26 1a 08 02 ef 63 64 2b c3
Crl link	undefined
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	undefined

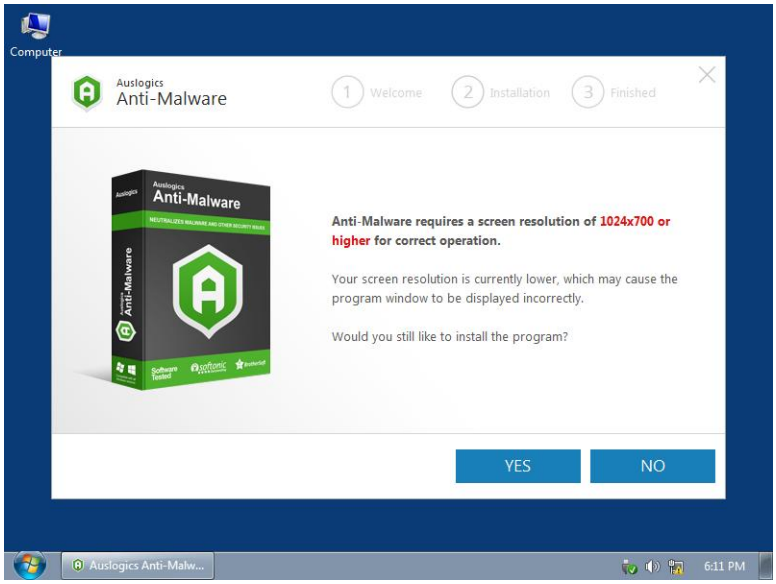
SCREENSHOTS



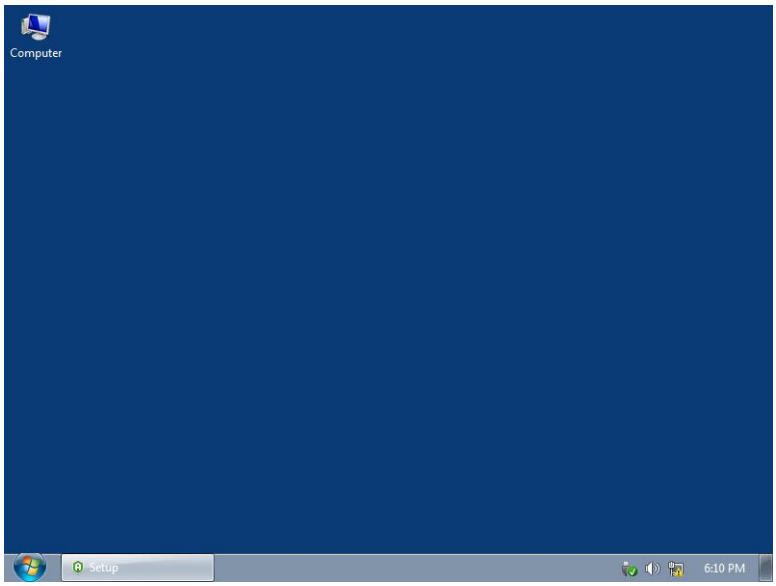

Computer
Setup
6:10 PM


Computer
Auslogics Anti-Malware
1 Welcome
2 Installation
3 Finished
Installation complete
Thank you for installing Auslogics Anti-Malware, your guard against the toughest cyber threats.
Launch Anti-Malware and scan PC
Finish
Auslogics Anti-Malw...
6:12 PM

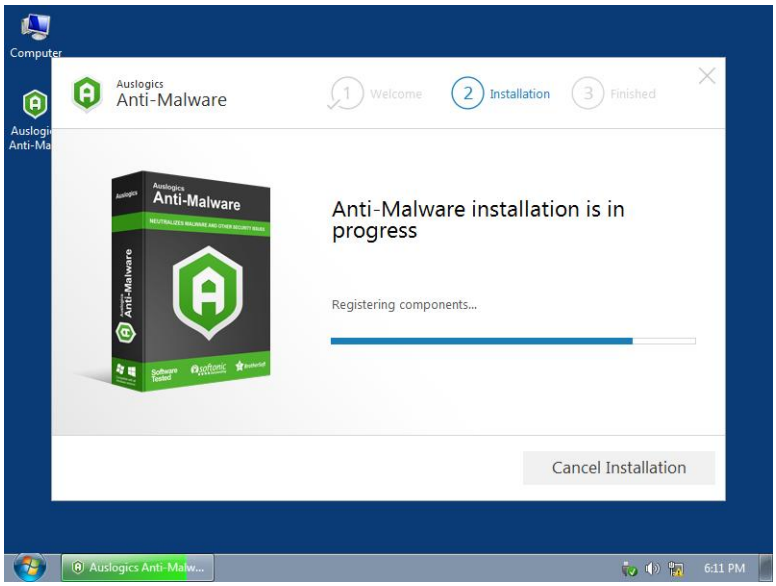

Computer
Auslogics Anti-Malware
1 Welcome
2 Installation
3 Finished
Anti-Malware installation is in progress
Extracting files...
C:\Program Files (x86)\Auslogics\Anti-Malware\Data\main.ini
Cancel Installation
Auslogics Anti-Malw...
6:11 PM

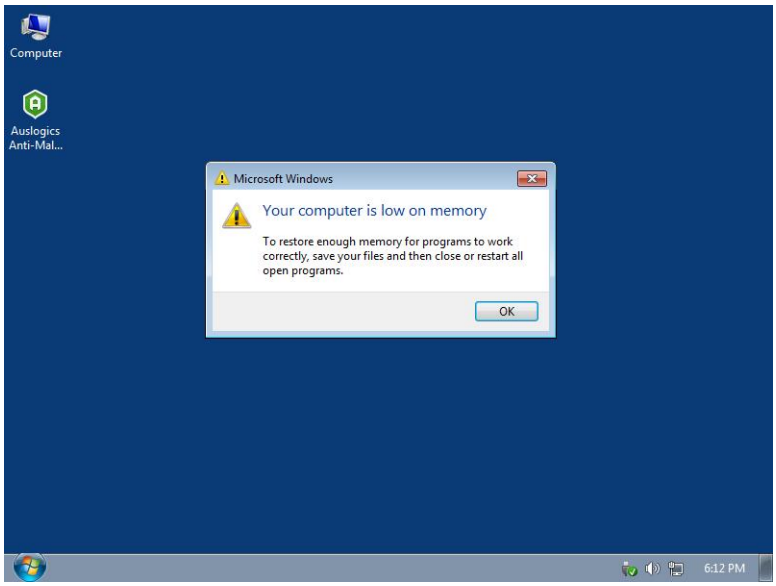

Computer
Auslogics
Anti-Malware
1 Welcome
2 Installation
3 Finished
Anti-Malware requires a screen resolution of 1024x700 or higher for correct operation.
Your screen resolution is currently lower, which may cause the program window to be displayed incorrectly.
Would you still like to install the program?
YES
NO
Auslogics Anti-Malw...
6:11 PM

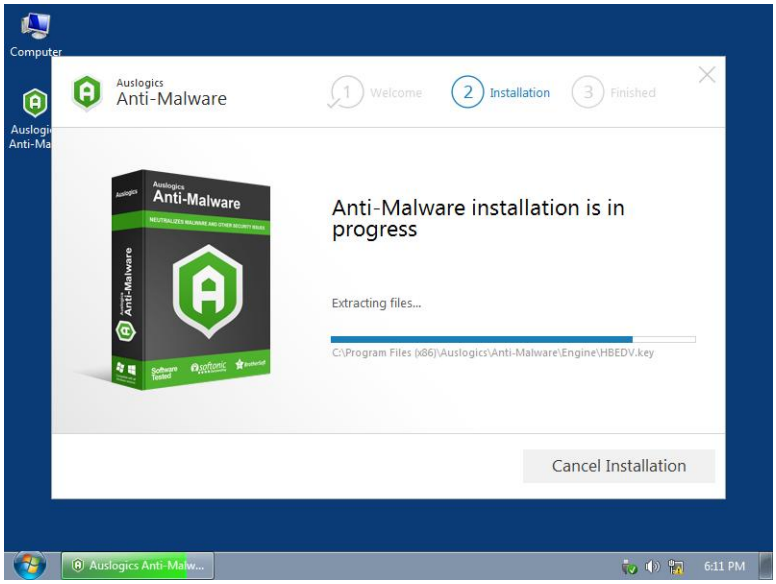

Computer
Auslogics
Anti-Mal...
6:13 PM

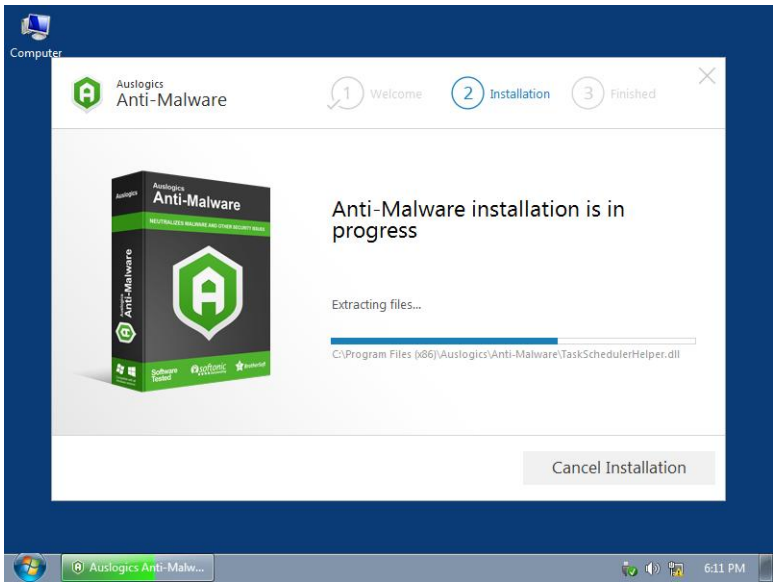

Computer
Setup
6:10 PM

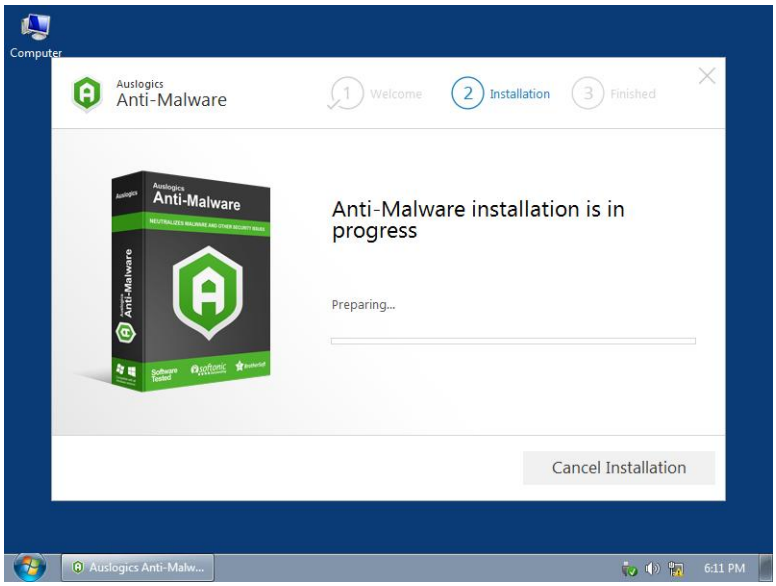

Computer
6:10 PM

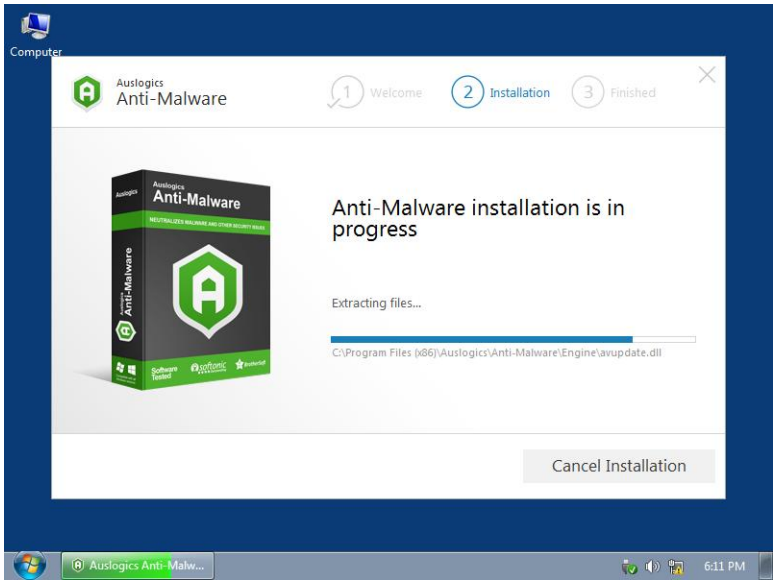

Computer
Auslogics Anti-Malware
1 Welcome
2 Installation
3 Finished
Anti-Malware installation is in progress
Registering components...
Cancel Installation
Auslogics Anti-Malw...
6:11 PM

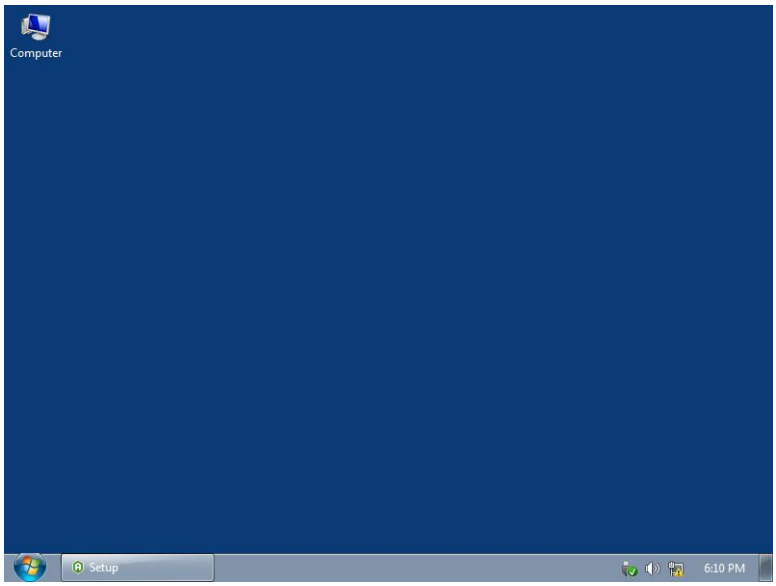

Computer
Auslogics Anti-Mal...
Microsoft Windows
Your computer is low on memory
To restore enough memory for programs to work correctly, save your files and then close or restart all open programs.
OK
6:12 PM


Computer
Auslogics Anti-Malware
1 Welcome
2 Installation
3 Finished
Anti-Malware installation is in progress
Extracting files...
C:\Program Files (x86)\Auslogics\Anti-Malware\Engine\HBEDV.key
Cancel Installation
Auslogics Anti-Malw...
6:11 PM


Computer
Auslogics Anti-Malware
1 Welcome
2 Installation
3 Finished
Anti-Malware installation is in progress
Extracting files...
C:\Program Files (x86)\Auslogics\Anti-Malware\TaskSchedulerHelper.dll
Cancel Installation
Auslogics Anti-Malw...
6:11 PM


Computer
Auslogics Anti-Malware
1 Welcome
2 Installation
3 Finished
Anti-Malware installation is in progress
Preparing...
Cancel Installation
Auslogics Anti-Malw...
6:11 PM


Computer
Auslogics
Anti-Malware
1 Welcome
2 Installation
3 Finished
Anti-Malware installation is in progress
Extracting files...
C:\Program Files (x86)\Auslogics\Anti-Malware\Engine\avupdate.dll
Cancel Installation
Auslogics Anti-Malw...
6:11 PM


Computer
Setup
6:10 PM