VALKYRIE COMODO

Summary

File Name: 03bebc007311f303fd442d966d3c4da9976dd7a141f06f24ebd01484c6fae233

File Type: Microsoft Excel 2007+

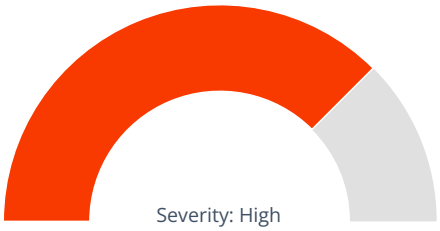
SHA1: 5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea

MD5: 0f0127570013aaf629f9aaf50b94bb79

MALWARE

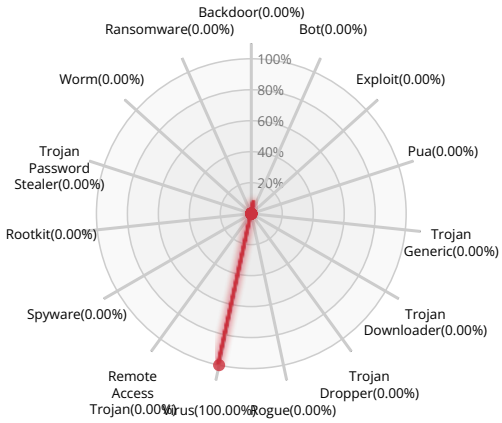
Valkyrie Final Verdict

DETECTION SECTION

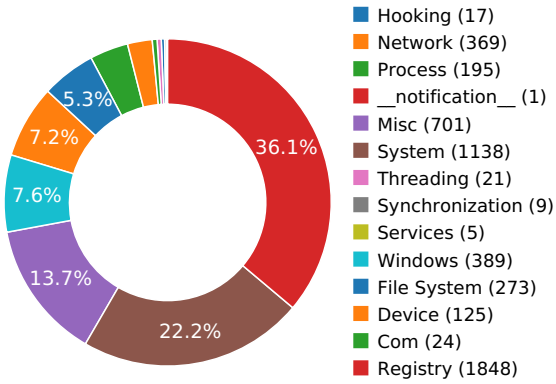


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Expresses interest in specific running processes — Show sources

NETWORKING

Attempts to connect to a dead IP:Port (1 unique times) — Show sources

Performs some HTTP requests — Show sources

A document file initiated network communications indicative of a potential exploit or payload download — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

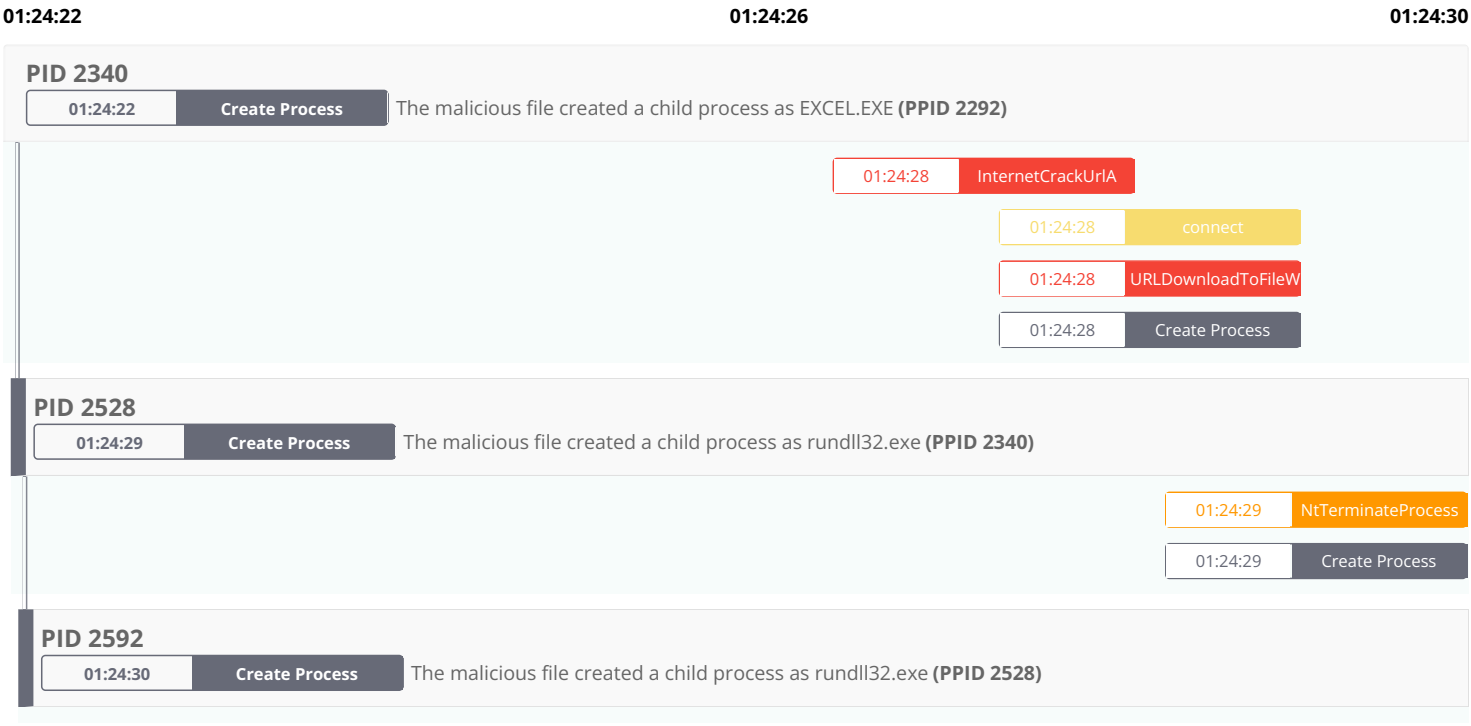
Martian Subprocess Started By Office Process — Show sources

MALWARE ANALYSIS SYSTEM EVASION

Possible date expiration check, exits too soon after checking local time — Show sources

VALKYRIE COMODO

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea
C:\Users\user\AppData\Local\Temp\~$5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea
C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\RICHED20.DLL
C:\Program Files (x86)\Microsoft Office\Office12\EXCEL.EXE.Local\
C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc
C:\Users\user\AppData\Roaming\
C:\Users\user\AppData\Roaming\Microsoft\Templates\
C:\Users\user\AppData\Roaming\Microsoft
C:\Users\user\AppData\Roaming\Microsoft\Templates
C:\Users\user\AppData\Roaming\Microsoft\Excel\XLSTART\
C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\1033\ALRTINTL.DLL
C:\Program Files (x86)\Microsoft Office\Office12\imageres.dll
C:\Windows\System32\imageres.dll
C:\Users\user\AppData\Roaming\Microsoft\Office\
C:\Users\user\AppData\Roaming\Microsoft\Office\review.rcd
C:\Users\user\AppData\Roaming\Microsoft\Office\adhoc.rcd
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso8F9E.tmp
C:\ProgramData\Microsoft\Network\Connections\Pbk\rasphone.pbk
C:\ProgramData\Microsoft\Network\Connections\Pbk*.pbk
C:\Windows\System32\ras*.pbk
C:\Users\user\AppData\Roaming\Microsoft\Network\Connections\Pbk\rasphone.pbk
C:\Users\user\AppData\Roaming\Microsoft\Network\Connections\Pbk*.pbk
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\RmsWtx[1].dll
C:\Users\user\AppData\Local\Microsoft\Schemas\MS Excel_restart.xml
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp\5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea:Zone.Identifier
C:\Program Files (x86)\Microsoft Office\Office12\ID_00030.DPC

C:\Users\user\ourl.ocx
C:\Users\user\ourl.ocx.manifest
C:\Users\user\ourl.ocx.123.Manifest
C:\Users\user\ourl.ocx.124.Manifest
C:\Users\ourl.ocx
C:\Windows\ourl.ocx
C:\ourl.ocx
C:\Windows\SysWOW64\rundll32.exe.Local\
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll
C:\Users\user\oledlg.dll
C:\Windows\System32\oledlg.dll
C:\Windows\Globalization\Sorting\sortdefault.nls
\Device\KsecDD
C:\Windows\SysWOW64\rundll32.exe
C:\
C:\Windows\SysWOW64
C:\Windows\SysWOW64\SysWOW64*

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\riched20.dll
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Options\DefaultSheetR2L
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Options\A4Letter
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Options\CursorVisual
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Options\ControlCharacters
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Options\DefaultFormat
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Options\AutomaticPictureCompressionDefault
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Options\QFE_Saskatchewan
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Security\ExtensionHardening
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\General\UserTemplates
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\General\Templates
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\General\SharedTemplates
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\General\Xlstart
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Options\Wizard Timestamp

HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Options\QFE_17407
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\QMEnable
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Components\2C418690CEFD69F479F69ED9E8B66816\1033
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Features\00002109E60090400000000000F01FEC\ProductNonBootFilesIntl_1033
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109E60090400000000000F01FEC\Features\ProductNonBootFilesIntl_1033
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\869C0C701D584D115AF3000972A8B18B\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\0F65D0D37A27C3840A1500571C8A02AD\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\C7F79FDAFA4D737438D03B465465C6CD\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\CE8A6E800CDAB6E4ABB9DA4B7903E29F\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\1542AEC87C5AB624197ACEDC5D5E546F\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\80F8A534CE34C37479A36408DF607B90\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\91A187C8354F85E409AC201B893A4BA0\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\D7AD2E79A44585A4994A8C99F5B1A62C\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\13BF891EA7D724040A511B4AA04C9FF0\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\5E91DFF0B8F46B14EA1AE378F670B819\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\C7F5FD8FE48395B48BCA14CB88C7442F\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\CCA383400EA17D241A7DC837A8F056D2\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\A4F01BFDB207D9748A1A71E4ADBB2B90\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\ACF660D8C07A6A04794E2ADD15B58C77\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\EA5F97CBCB5F9944DB53275D6BE780AF\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\77ED11277E13FCF4BB8C47FDC65086F1\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\829A131E5CE21D944A67B52DE1268EA2\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\CBD521FB6DFE3D115AF2000A9CAC24AB\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\FBD521FB6DFE3D115AF2000A9CAC24AB\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\2CD521FB6DFE3D115AF2000A9CAC24AB\00002109E60090400000000000F01FEC

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\B055A4C037A53D115A02000A9C32B11A\00002109E600904000000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\5CD521FB6DFE3D115AF2000A9CAC24AB\00002109E600904000000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\8CD521FB6DFE3D115AF2000A9CAC24AB\00002109E600904000000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\BCD521FB6DFE3D115AF2000A9CAC24AB\00002109E600904000000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\ECD521FB6DFE3D115AF2000A9CAC24AB\00002109E600904000000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\1DD521FB6DFE3D115AF2000A9CAC24AB\00002109E600904000000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\D811316032AC49B4E8BCC33454B31F61\00002109E600904000000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\F0B5D1A7DE3021C43A14422F0005333C\00002109E600904000000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Features\00002109E600904000000000000F01FEC\ProductFilesIntl_1033
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109E600904000000000000F01FEC\Features\ProductFilesIntl_1033
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\D2FFBA7ACD4FACF41929F6CCFE88DBDA\00002109E600904000000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\1650EACF3C291D11A92C0006794C4E25\00002109E600904000000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\110D06364BE0F08438A5ACEED069DCBC\00002109E600904000000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\7716FB73E5A23CA4180309AA54335EF9\00002109E600904000000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\1AD24949EBEB1D742A3F9F38DEF500BE\00002109E600904000000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\2154EBF3EFF04B048A77A9F7181445D6\00002109E600904000000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\D795BC613D313574CBB1FBE0448BFFA9\00002109E600904000000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\826BE7CCECB5A07419E4D5FC61E63C4A\00002109E600904000000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\F7CD01816C53D32438CF043106011676\00002109E600904000000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109E600904000000000000F01FEC\Usage\ProductNonBootFilesIntl_1033
HKEY_CURRENT_USER\Software\Classes\.html\(Default)
HKEY_CURRENT_USER\Software\Classes\FirefoxHTML\shell\open\command\(Default)
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\General\CustomizableAlertBaseURL
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\General\UseOfficeUIFont
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\DisableRibbonForMinimizedWindow
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Security\Trusted Locations\AllLocationsDisabled

HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Security\Trusted Locations\BlockFQDNFileProtocol
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Security\VBAWarnings
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\General\NoTrack
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\DisableDocumentAssemblies
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Options\FullCalcOnLoadOldFile
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Office\12.0\Common\VbaOff
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\VbaOff
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Features\00002109030000000000000000F01FEC\VBAFiles
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Features\VBAFiles
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\4EEF86DD963C1D111A37000A9CA05BF0\00002109030000000000000000F01FEC

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\~$5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea
C:\Users\user\AppData\Local\Temp\5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso8F9E.tmp
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\RmsWtx[1].dll

RESOLVED APIS

mso.dll.#8703
mso.dll.#403
mso.dll.#836
mso.dll.#5347
mso.dll.#7845
mso.dll.#8041
oleaut32.dll.#8
oleaut32.dll.#12
oleaut32.dll.#9
kernel32.dll.HeapSetInformation
oleaut32.dll.VariantInit
oleaut32.dll.VariantClear
oleaut32.dll.VariantChangeType
oleaut32.dll.VariantChangeTypeEx
oleaut32.dll.VariantTimeToDosDateTime
oleaut32.dll.DosDateTimeToVariantTime
oleaut32.dll.SysAllocString

oleaut32.dll.SysAllocStringLen
oleaut32.dll.SysFreeString
oleaut32.dll.SysStringLen
oleaut32.dll.SafeArrayGetDim
oleaut32.dll.SafeArrayAccessData
oleaut32.dll.SafeArrayUnaccessData
oleaut32.dll.SafeArrayGetUBound
oleaut32.dll.SafeArrayGetLBound
oleaut32.dll.LoadRegTypeLib
oleaut32.dll.LoadTypeLib
oleaut32.dll.QueryPathOfRegTypeLib
oleaut32.dll.VariantCopy
oleaut32.dll.SafeArrayCreate
oleaut32.dll.SafeArrayCreateVector
oleaut32.dll.SafeArrayDestroy
oleaut32.dll.SafeArrayGetElement
oleaut32.dll.RegisterTypeLib
oleaut32.dll.CreateErrorInfo
oleaut32.dll.SetErrorInfo
oleaut32.dll.GetErrorInfo
oleaut32.dll.GetActiveObject
oleaut32.dll.SysReAllocStringLen
oleaut32.dll.SysReAllocString
oleaut32.dll.SysAllocStringByteLen
oleaut32.dll.SafeArrayUnlock
oleaut32.dll.SafeArrayLock
oleaut32.dll.OleCreatePropertyFrameIndirect
oleaut32.dll.SysStringByteLen
oleaut32.dll.SafeArrayRedim
oleaut32.dll.SystemTimeToVariantTime
oleaut32.dll.SafeArrayGetElemsize
oleaut32.dll.VarBstrFromR8
oleaut32.dll.OleLoadPicture
oleaut32.dll.RevokeActiveObject
oleaut32.dll.RegisterActiveObject

oleaut32.dll.DispGetIDsOfNames
oleaut32.dll.DispInvoke
oleaut32.dll.CreateTypeLib2
oleaut32.dll.LHashValOfNameSys
oleaut32.dll.VarDateFromUdate
oleaut32.dll.VarUdateFromDate
oleaut32.dll.GetAltMonthNames
oleaut32.dll.SafeArrayPutElement
oleaut32.dll.VariantCopyInd
oleaut32.dll.SafeArrayAllocData
oleaut32.dll.SafeArrayDestroyData
oleaut32.dll.VarR4FromR8
oleaut32.dll.VarR8FromR4
oleaut32.dll.VarUI4FromStr
oleaut32.dll.OaBuildVersion
oleaut32.dll.LoadTypeLibEx
oleaut32.dll.VariantTimeToSystemTime
oleaut32.dll.SafeArrayCopy
oleaut32.dll.UnRegisterTypeLib
oleaut32.dll.SafeArrayPtrOfIndex
mso.dll.#8652
mso.dll.#7291
oleaut32.dll.#4
kernel32.dll.NlsGetCacheUpdateCount

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1821EED\1821EED
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Max Display
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 1
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 2
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 3
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 4
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 5
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 6
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 7

HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 8
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 9
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 10
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 11
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 12
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 13
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 14
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 15
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 16
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 17
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 18
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 19
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 20
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 21
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 22
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 23
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 24
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 25
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 26
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 27
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 28
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 29
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 30
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 31
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 32
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 33
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 34
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 35
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 36
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 37
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 38
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 39
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 40
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 41
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 42

HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 43
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 44
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 45
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 46
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 47
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 48
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 49
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 50

REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Office\12.0\Common\Security
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Office\12.0\Common\OpenXMLFormat
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\riched20.dll
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Options\DefaultSheetR2L
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Options\A4Letter
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Options\CursorVisual
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Options\ControlCharacters
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Options\DefaultFormat
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Options\AutomaticPictureCompressionDefault
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Options\QFE_Saskatchewan
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Security\FileOpenBlock
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Security
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Security\ExtensionHardening
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\General\UserTemplates
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\General\Templates
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\General\SharedTemplates
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\General\Xlstart
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Options\Wizard Timestamp
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Options\QFE_17407
HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\Alerts
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\QMEnable
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-2298303332-66077612-2598613238-1000\Installer\Components\2C418690CEFD69F479F69ED9E8B66816

HKEY_USERS\S-1-5-21-2298303332-66077612-2598613238-1000\Software\Microsoft\Installer\Components\2C418690CEFD69F479F69ED9E8B66816
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Components\2C418690CEFD69F479F69ED9E8B66816
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Components\2C418690CEFD69F479F69ED9E8B66816\1033
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-2298303332-66077612-2598613238-1000\Installer\Features\00002109E60090400000000000F01FEC
HKEY_USERS\S-1-5-21-2298303332-66077612-2598613238-1000\Software\Microsoft\Installer\Features\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Features\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Features\00002109E60090400000000000F01FEC\ProductNonBootFilesIntl_1033
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109E60090400000000000F01FEC\Features
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109E60090400000000000F01FEC\Features\ProductNonBootFilesIntl_1033
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\869C0C701D584D115AF3000972A8B18B
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\869C0C701D584D115AF3000972A8B18B\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\0F65D0D37A27C3840A1500571C8A02AD
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\0F65D0D37A27C3840A1500571C8A02AD\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\C7F79FDAFA4D737438D03B465465C6CD
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\C7F79FDAFA4D737438D03B465465C6CD\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\CE8A6E800CDAB6E4ABB9DA4B7903E29F
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\CE8A6E800CDAB6E4ABB9DA4B7903E29F\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\1542AEC87C5AB624197ACEDC5D5E546F
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\1542AEC87C5AB624197ACEDC5D5E546F\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\80F8A534CE34C37479A36408DF607B90
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\80F8A534CE34C37479A36408DF607B90\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\91A187C8354F85E409AC201B893A4BA0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\91A187C8354F85E409AC201B893A4BA0\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\D7AD2E79A44585A4994A8C99F5B1A62C
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\D7AD2E79A44585A4994A8C99F5B1A62C\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\13BF891EA7D724040A511B4AA04C9FF0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\13BF891EA7D724040A511B4AA04C9FF0\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\5E91DFF0B8F46B14EA1AE378F670B819
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\5E91DFF0B8F46B14EA1AE378F670B819\00002109E60090400000000000F01FEC

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\C7F5FD8FE48395B48BCA14CB88C7442F

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\C7F5FD8FE48395B48BCA14CB88C7442F\00002109E60090400000000000F01FEC

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\CCA383400EA17D241A7DC837A8F056D2

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\CCA383400EA17D241A7DC837A8F056D2\00002109E60090400000000000F01FEC

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\A4F01BFDB207D9748A1A71E4ADBB2B90

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\A4F01BFDB207D9748A1A71E4ADBB2B90\00002109E60090400000000000F01FEC

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\ACF660D8C07A6A04794E2ADD15B58C77

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\ACF660D8C07A6A04794E2ADD15B58C77\00002109E60090400000000000F01FEC

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\EA5F97CBCB5F9944DB53275D6BE780AF

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\EA5F97CBCB5F9944DB53275D6BE780AF\00002109E60090400000000000F01FEC

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\77ED11277E13FCF4BB8C47FDC65086F1

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\77ED11277E13FCF4BB8C47FDC65086F1\00002109E60090400000000000F01FEC

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\829A131E5CE21D944A67B52DE1268EA2

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\829A131E5CE21D944A67B52DE1268EA2\00002109E60090400000000000F01FEC

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\CBD521FB6DFE3D115AF2000A9CAC24AB

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\CBD521FB6DFE3D115AF2000A9CAC24AB\00002109E60090400000000000F01FEC

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\FBD521FB6DFE3D115AF2000A9CAC24AB

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\FBD521FB6DFE3D115AF2000A9CAC24AB\00002109E60090400000000000F01FEC

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\2CD521FB6DFE3D115AF2000A9CAC24AB

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\2CD521FB6DFE3D115AF2000A9CAC24AB\00002109E60090400000000000F01FEC

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\B055A4C037A53D115A02000A9C32B11A

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\B055A4C037A53D115A02000A9C32B11A\00002109E60090400000000000F01FEC

EXECUTED COMMANDS

C:\Windows\SysWow64\rundll32.exe ..\ourl.ocx,D"&"l"&"lR"&"egister"&"Serve"&"r

C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\ourl.ocx",DllRegisterServer

READ FILES

C:\Users\user\AppData\Local\Temp\5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea

C:\Users\user\AppData\Local\Temp\~$5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea

C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\RICHED20.DLL
C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\1033\ALRTINTL.DLL
C:\Windows\System32\imageres.dll
C:\Users\user\AppData\Roaming\Microsoft\Office\review.rcd
C:\Users\user\AppData\Roaming\Microsoft\Office\adhoc.rcd
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso8F9E.tmp
C:\Program Files (x86)\Microsoft Office\Office12\ID_00030.DPC
C:\Users\user\ourl.ocx
C:\Users\user\ourl.ocx.123.Manifest
C:\Users\user\ourl.ocx.124.Manifest
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll
C:\Windows\System32\oledlg.dll
C:\Windows\Globalization\Sorting\sortdefault.nls
\Device\KsecDD
C:\Windows\SysWOW64

MUTEXES

Global\MTX_MSO_Formal1_S-1-5-21-2298303332-66077612-2598613238-1000
Global\MTX_MSO_AdHoc1_S-1-5-21-2298303332-66077612-2598613238-1000
IESQMMUTEX_0_208
Local\!IETld!Mutex

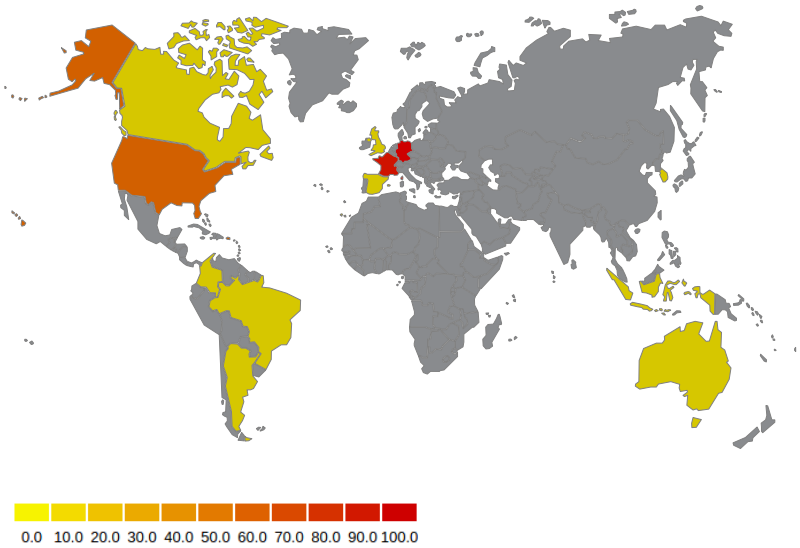
MODIFIED REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109E60090400000000000F01FEC\Usage\ProductNonBootFilesIntl_1033
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1821EED\1821EED
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\ReviewCycle
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\ReviewCycle\ReviewToken
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\182266F
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\182266F\182266F
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Max Display
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadNetworkName

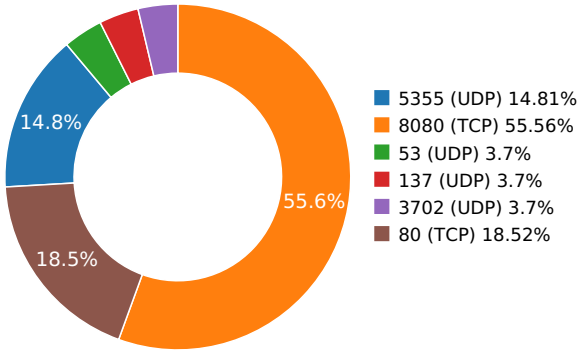
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadLastNetwork
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DBB8B4CD1B191052E8F325736

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
	128.199.192.135	Singapore	14061	DigitalOcean, LLC	Malware Process
	142.4.219.173	Canada	16276	OVH Hosting, Inc.	Malware Process
	168.197.250.14	Argentina	264776	Omar Anselmo Ripoll (TDC NET...	Malware Process
	69.16.218.101	United States	32244	Liquid Web, L.L.C	Malware Process
	85.214.67.203	Germany	6724	Strato Rechenzentrum, Berlin	Malware Process
	78.47.204.80	Germany	24940	Hetzner Online GmbH Datacen...	Malware Process
	78.46.73.125	Germany	24940	Hetzner Online AG	Malware Process
	66.42.57.149	Singapore	20473	SGP_VULTR_CUST	Malware Process
	62.171.178.147	United Kingdom	51167	Contabo GmbH	Malware Process
	54.38.242.185	France	16276	Not known	Malware Process
	54.37.228.122	France	16276	Not known	Malware Process
	51.210.242.234	France	16276	Not known	Malware Process
	45.138.98.34		9009	Not known	Malware Process
	37.59.209.141	France	16276	OVH	Malware Process
	37.44.244.177	Germany	47583	Hostinger International Ltd.	Malware Process
	217.182.143.207	France	16276	OVH	Malware Process
	210.57.209.142	Indonesia	38142	Universitas Airlangga Universit...	Malware Process
	207.148.81.119	Australia	20473	AUS_VULTR_CUST	Malware Process
	195.77.239.39	Spain	3352	SOLUCIONES INTERNET S.L. In...	Malware Process
	195.154.146.35	France	12876	Iliad Entreprises Customers	Malware Process
	191.252.103.16	Brazil	27715	Locaweb Servios de Internet S...	Malware Process
	190.90.233.66	Colombia	262589	CABLE Y TELECOMUNICACION...	Malware Process

Name	IP	Country	ASN	ASN Name	Trigger Process Type
	185.148.168.220	Germany	24679	Everscale GmbH	Malware Process
	185.148.168.15	Germany	24679	Everscale GmbH	Malware Process
	159.69.237.188	Germany	24940	HOS-132910	Malware Process
	104.131.62.48	United States	14061	DigitalOcean, LLC	Malware Process
avionxpress.com	162.240.27.36	United States	46606	Unified Layer	Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
avionxpress.com	80	GET	1.1	Mozilla/4.0 (compatible; MSIE...	1	15.0640280247
Path: /lp/T9b1Bga4FdDfP5HI/ **URI:** http://avionxpress.com/lp/T9b1Bga4FdDfP5HI/						

DNS QUERIES

Request	Type
avionxpress.com	A
Answers - 162.240.27.36 (A)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
15.0640280247	Sandbox	162.240.27.36	80
35.6844820976	Sandbox	69.16.218.101	8080
35.724271059	Sandbox	69.16.218.101	8080
35.7622959614	Sandbox	69.16.218.101	8080
58.2578520775	Sandbox	142.4.219.173	8080
58.2990131378	Sandbox	142.4.219.173	8080
58.3335371017	Sandbox	142.4.219.173	8080
85.2342841625	Sandbox	168.197.250.14	80
85.5718071461	Sandbox	168.197.250.14	80
85.9345741272	Sandbox	168.197.250.14	80
151.912255049	Sandbox	116.124.128.206	8080
152.295017004	Sandbox	116.124.128.206	8080
152.679214001	Sandbox	116.124.128.206	8080
153.301679134	Sandbox	128.199.192.135	8080
153.759042025	Sandbox	128.199.192.135	8080
154.216524124	Sandbox	128.199.192.135	8080
211.852311134	Sandbox	69.16.218.101	8080
211.891766071	Sandbox	69.16.218.101	8080
211.929709196	Sandbox	69.16.218.101	8080

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
6.87648510933	Sandbox	224.0.0.252	5355
6.87713909149	Sandbox	224.0.0.252	5355
6.87807202339	Sandbox	239.255.255.250	3702
6.94049310684	Sandbox	192.168.56.255	137
9.44143104553	Sandbox	224.0.0.252	5355
12.3750891685	Sandbox	224.0.0.252	5355
14.9411420822	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\25233734.Od	**Type :** ASCII text, with CRLF line terminators **MD5 :** 0676f96fd5bdd1d4dbc2bfae982f75d5 **SHA-1 :** 9b04a75768f0153479ccba5e9512320d0a709fc9 **SHA-256 :** 5b7b63dc1d737e8a0a862db21f1828beb56a9e8 **SHA-512 :** 77dddde6a93ab66ad78f842d3a284cae82c238cf **Size :** 0.134 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	03bebc007311f303fd442d966d3c4da9976dd7a141f06f24ebd01484c6fae233
File Type:	Microsoft Excel 2007+
SHA1:	5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea
MD5:	0f0127570013aaf629f9aaf50b94bb79
First Seen Date:	2022-01-17 14:41:01.534696 (about a year ago)
Number Of Clients Seen:	3
Last Analysis Date:	2022-01-17 14:41:01.534696 (about a year ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

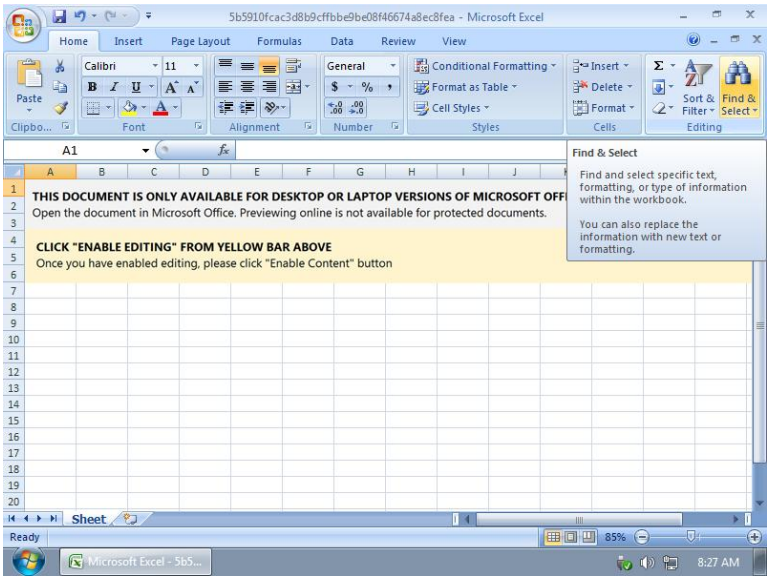
PE Headers

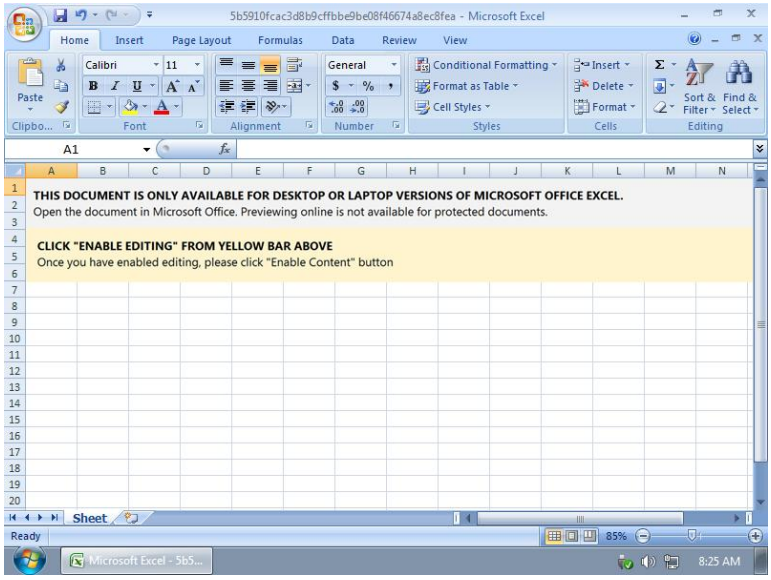
PROPERTY	VALUE
Magic Literal Enum	None
File Type Enum	14
File Size	101473
Sha256	03bebc007311f303fd442d966d3c4da9976dd7a141f06f24ebd01484c6fae233
Mime Type	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet

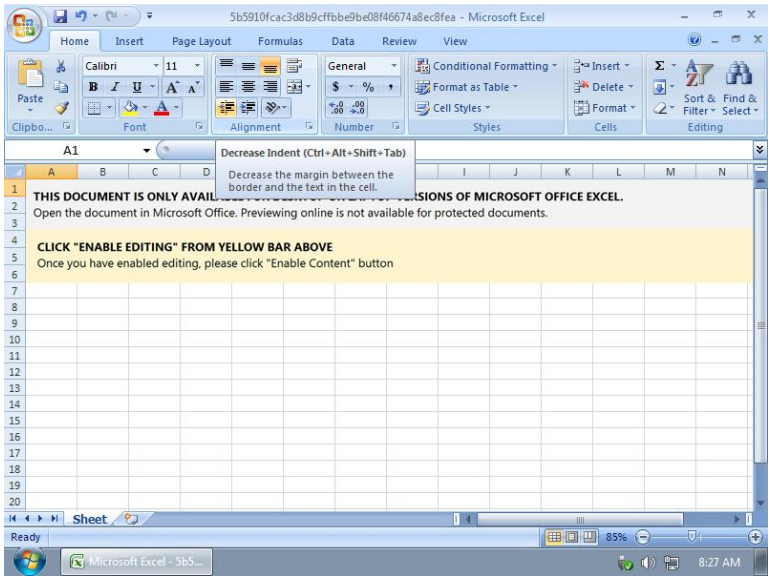
CERTIFICATE VALIDATION

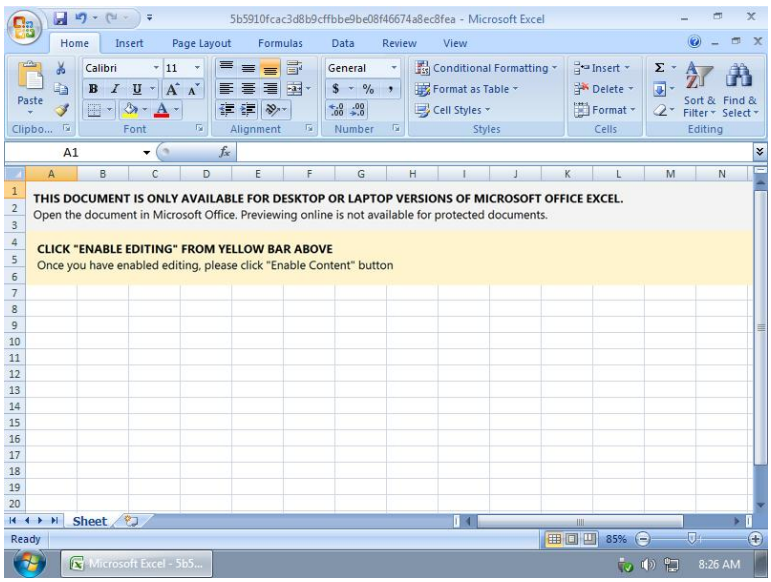
- Certificate Validation is not Applicable ?

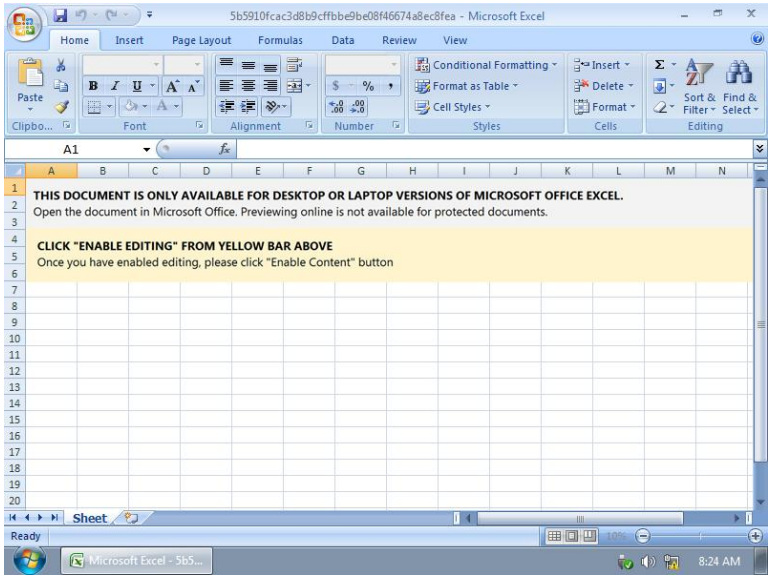
SCREENSHOTS

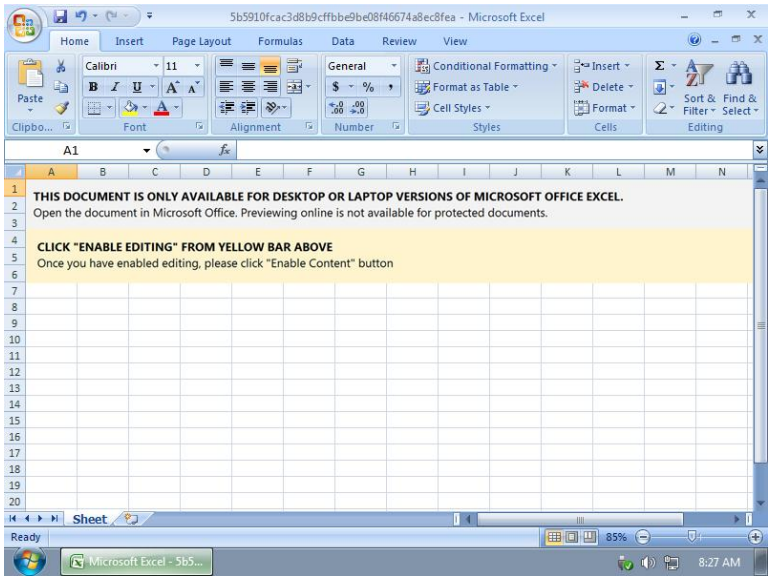


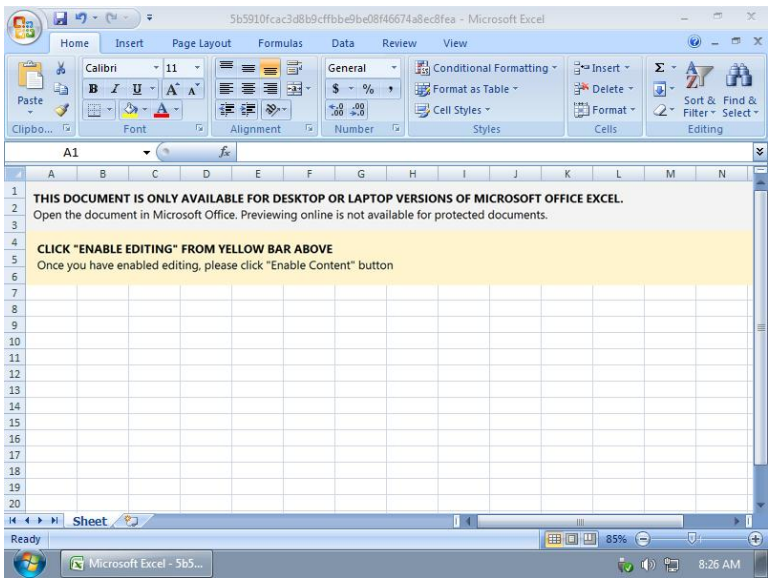

5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea - Microsoft Excel
THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCEL.
Open the document in Microsoft Office. Previewing online is not available for protected documents.
CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button
Sheet
Ready
8:25 AM

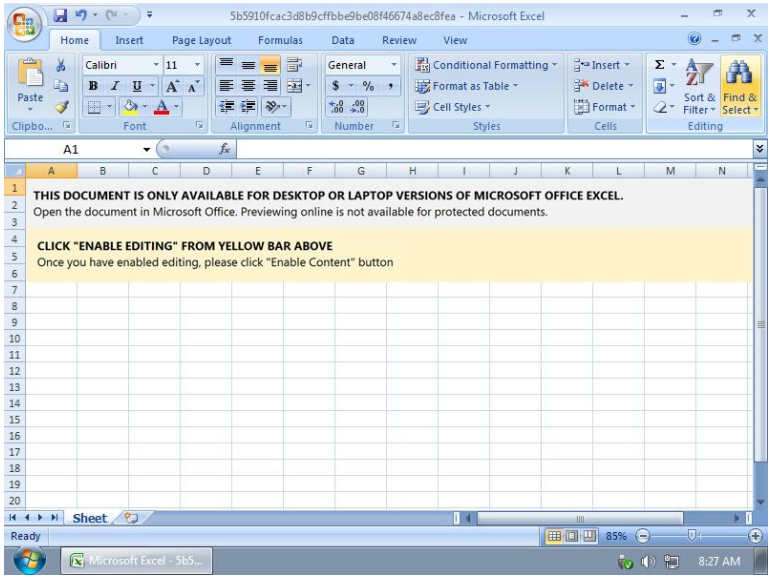

5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea - Microsoft Excel
Decrease Indent (Ctrl+Alt+Shift+Tab)
Decrease the margin between the border and the text in the cell.
THIS DOCUMENT IS ONLY AVAIL
Open the document in Microsoft Office. Previewing online is not available for protected documents.
CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button
Sheet
Ready
8:27 AM

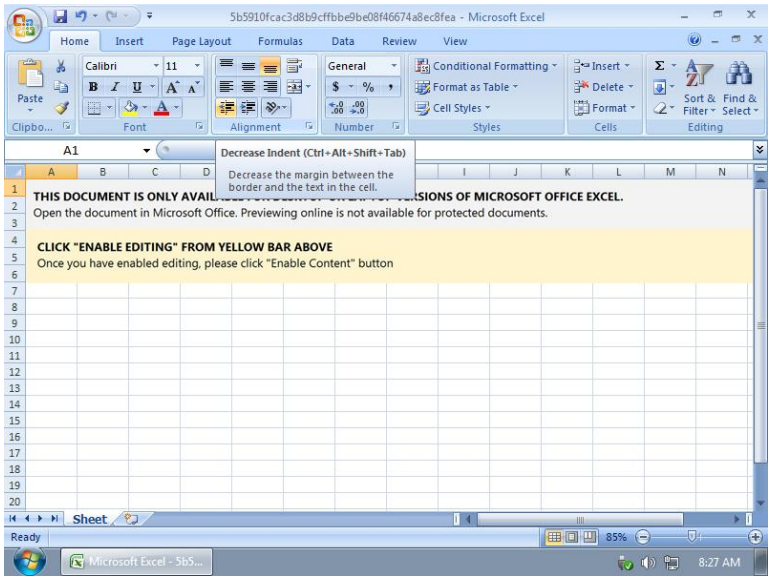

5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea - Microsoft Excel
THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCEL.
Open the document in Microsoft Office. Previewing online is not available for protected documents.
CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button
Sheet
Ready
8:26 AM

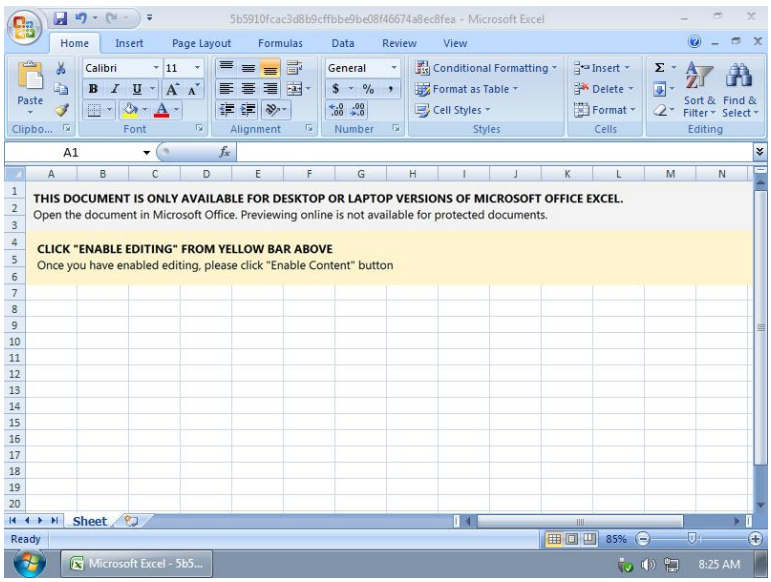

5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea - Microsoft Excel
Home
Insert
Page Layout
Formulas
Data
Review
View
Paste
Conditional Formatting
Format as Table
Cell Styles
Insert
Delete
Format
Sort & Filter
Find & Select
Clipbo...
Font
Alignment
Number
Styles
Cells
Editing
A1
THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCEL.
Open the document in Microsoft Office. Previewing online is not available for protected documents.
CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button
Sheet
Ready
Microsoft Excel - 5b5...
8:24 AM

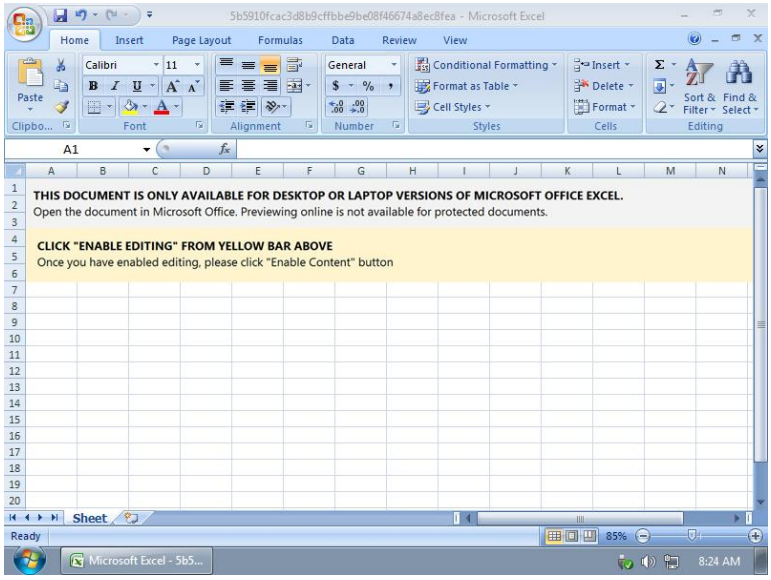

5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea - Microsoft Excel
Home
Insert
Page Layout
Formulas
Data
Review
View
Paste
Calibri
11
General
Conditional Formatting
Format as Table
Cell Styles
Insert
Delete
Format
Sort & Filter
Find & Select
Clipbo...
Font
Alignment
Number
Styles
Cells
Editing
A1
THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCEL.
Open the document in Microsoft Office. Previewing online is not available for protected documents.
CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button
Sheet
Ready
85%
Microsoft Excel - 5b5...
8:27 AM

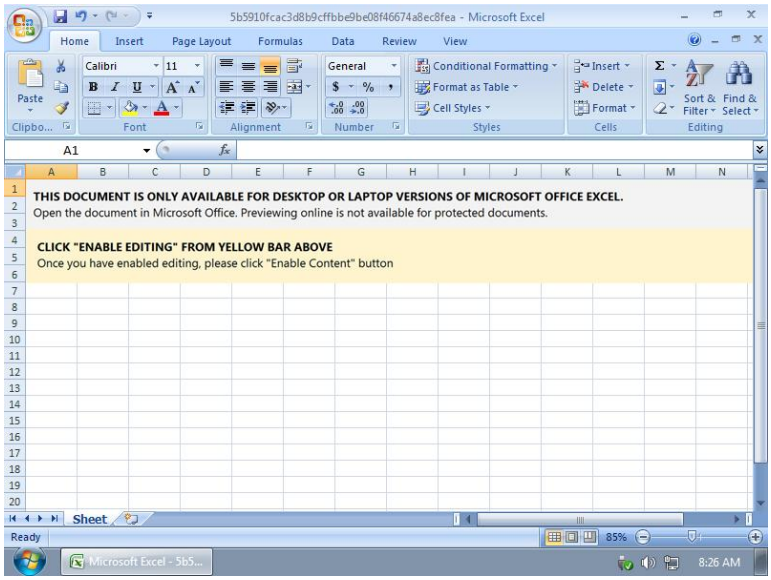

5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea - Microsoft Excel
Home
Insert
Page Layout
Formulas
Data
Review
View
Paste
Calibri
11
General
Conditional Formatting
Format as Table
Cell Styles
Insert
Delete
Format
Sort & Filter
Find & Select
Clipbo...
Font
Alignment
Number
Styles
Cells
Editing
A1
THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCEL.
Open the document in Microsoft Office. Previewing online is not available for protected documents.
CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button
Sheet
Ready
85%
Microsoft Excel - 5b5...
8:26 AM

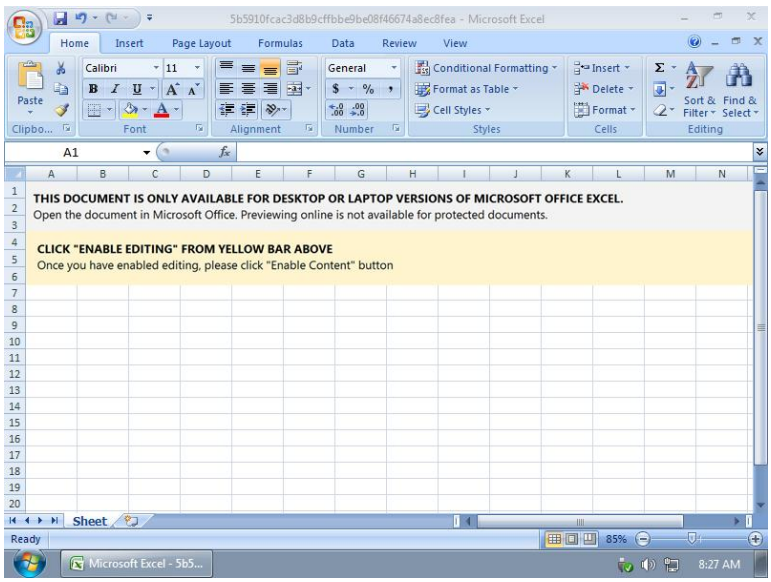

5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea - Microsoft Excel
Home
Insert
Page Layout
Formulas
Data
Review
View
Paste
Calibri
11
General
Conditional Formatting
Format as Table
Cell Styles
Insert
Delete
Format
Sort & Filter
Find & Select
Clipbo...
Font
Alignment
Number
Styles
Cells
Editing
A1
THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCEL.
Open the document in Microsoft Office. Previewing online is not available for protected documents.
CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button
Sheet
Ready
85%
Microsoft Excel - 5b5...
8:27 AM

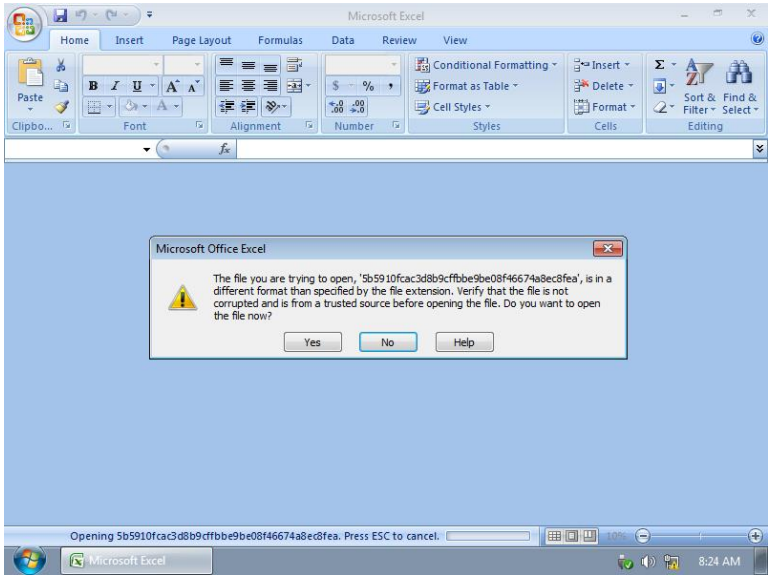

5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea - Microsoft Excel
Home
Insert
Page Layout
Formulas
Data
Review
View
Paste
Calibri
11
General
Conditional Formatting
Format as Table
Cell Styles
Insert
Delete
Format
Sort & Filter
Find & Select
Clipbo...
Font
Alignment
Number
Styles
Cells
Editing
A1
Decrease Indent (Ctrl+Alt+Shift+Tab)
Decrease the margin between the border and the text in the cell.
THIS DOCUMENT IS ONLY AVAIL
SIONS OF MICROSOFT OFFICE EXCEL.
Open the document in Microsoft Office. Previewing online is not available for protected documents.
CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button
Sheet
Ready
85%
Microsoft Excel - 5b5...
8:27 AM


5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea - Microsoft Excel
Home
Insert
Page Layout
Formulas
Data
Review
View
Paste
Calibri
11
General
Conditional Formatting
Format as Table
Cell Styles
Insert
Delete
Format
Sort & Filter
Find & Select
Clipbo...
Font
Alignment
Number
Styles
Cells
Editing
A1
THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCEL.
Open the document in Microsoft Office. Previewing online is not available for protected documents.
CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button
Sheet
Ready
85%
Microsoft Excel - 5b5...
8:25 AM

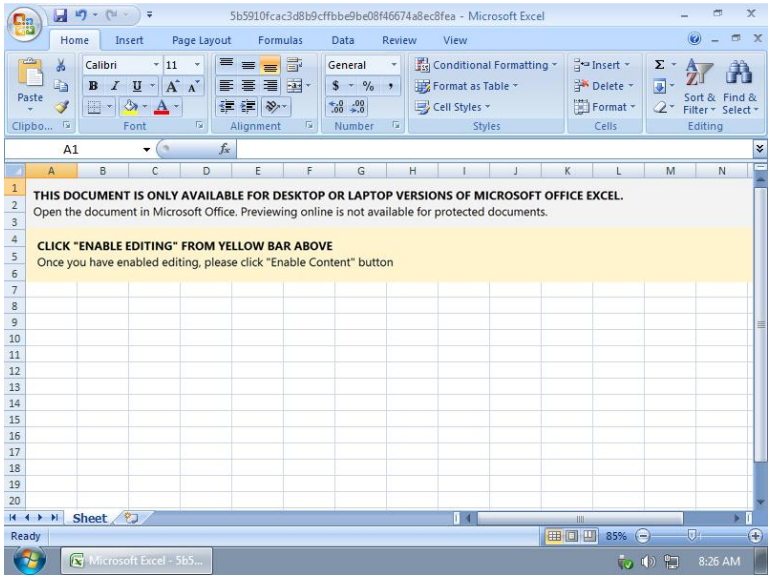

5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea - Microsoft Excel
THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCEL.
Open the document in Microsoft Office. Previewing online is not available for protected documents.
CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button
Sheet
Ready
8:24 AM

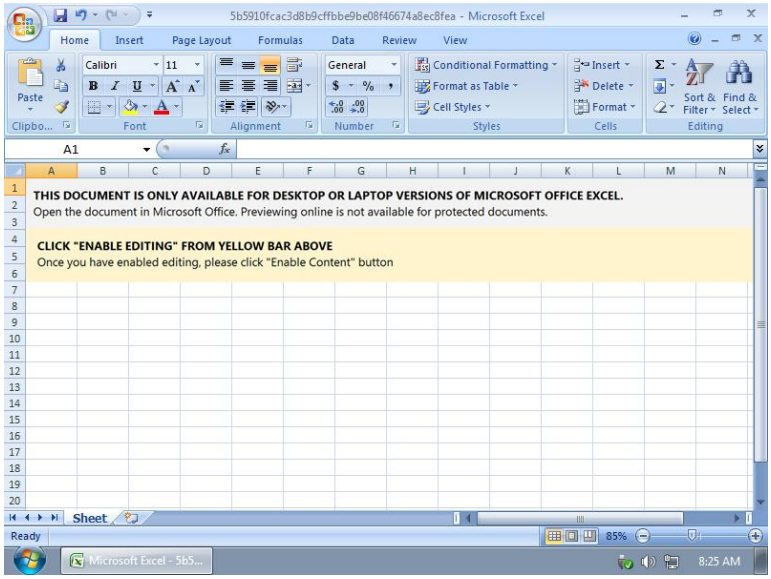

5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea - Microsoft Excel
THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCEL.
Open the document in Microsoft Office. Previewing online is not available for protected documents.
CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button
Sheet
Ready
8:26 AM

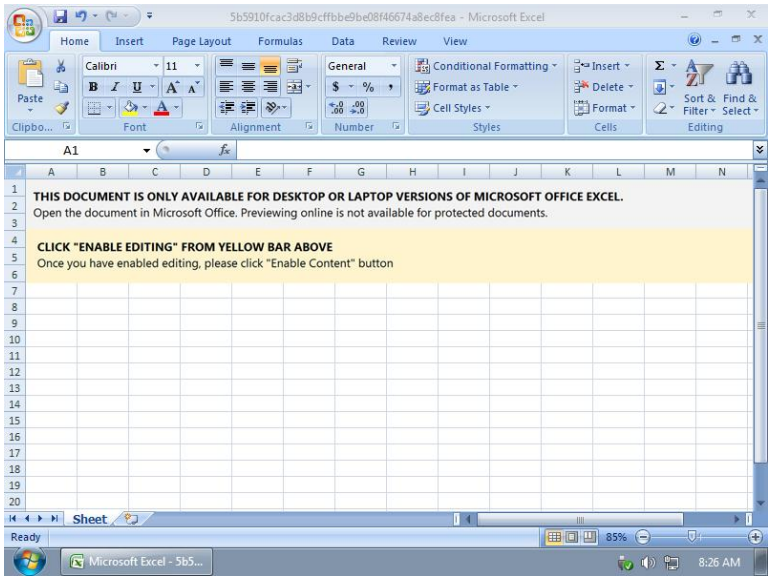

5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea - Microsoft Excel
THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCEL.
Open the document in Microsoft Office. Previewing online is not available for protected documents.
CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button
Sheet
Ready
8:27 AM

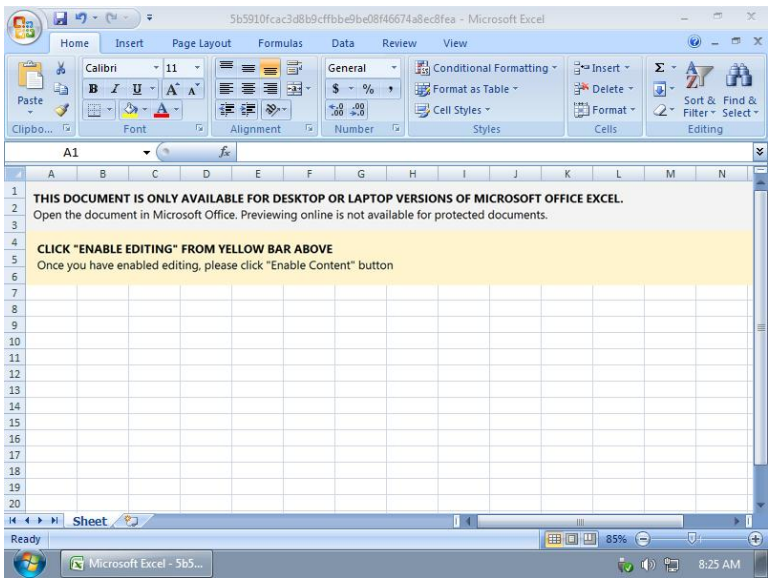

Microsoft Excel
Home
Insert
Page Layout
Formulas
Data
Review
View
Microsoft Office Excel
The file you are trying to open, '5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea', is in a different format than specified by the file extension. Verify that the file is not corrupted and is from a trusted source before opening the file. Do you want to open the file now?
Yes
No
Help
Opening 5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea. Press ESC to cancel.
8:24 AM

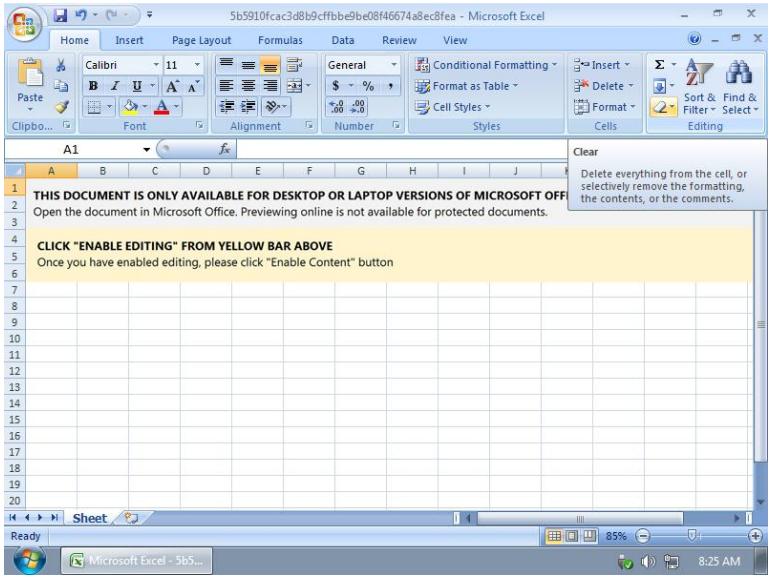

Computer
8:24 AM

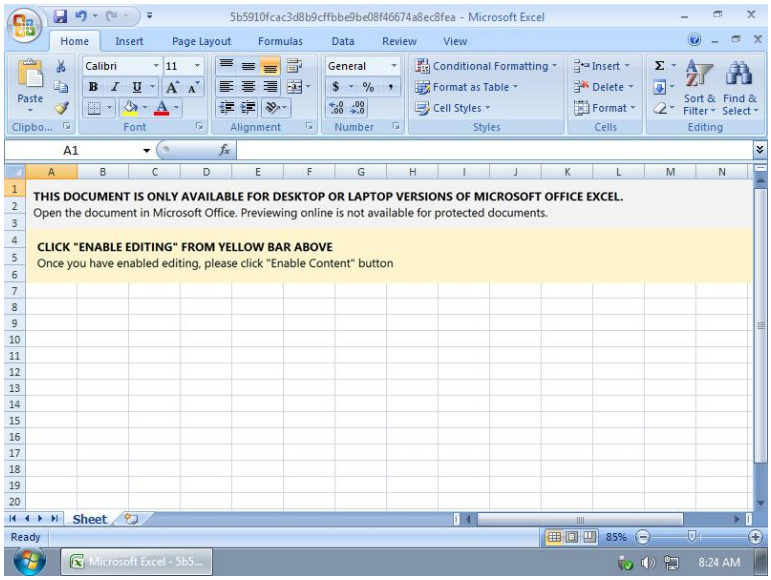

5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea - Microsoft Excel
THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCEL.
Open the document in Microsoft Office. Previewing online is not available for protected documents.
CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button
Sheet
Ready
85%
8:26 AM

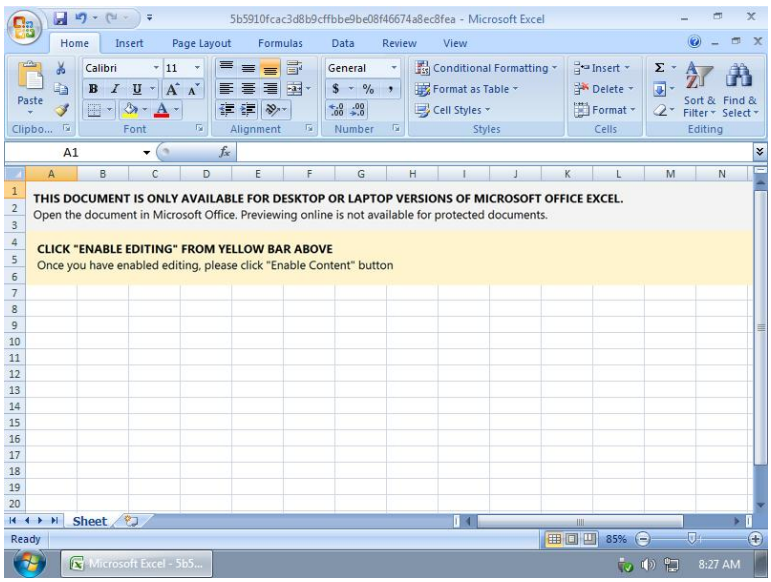

5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea - Microsoft Excel
THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCEL.
Open the document in Microsoft Office. Previewing online is not available for protected documents.
CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button
Sheet
Ready
8:25 AM

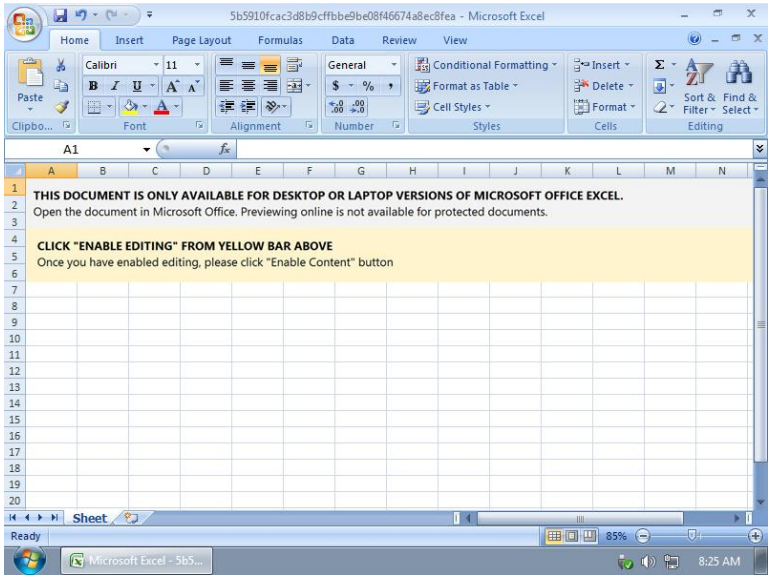

5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea - Microsoft Excel
THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCEL.
Open the document in Microsoft Office. Previewing online is not available for protected documents.
CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button
Sheet
Ready
8:26 AM

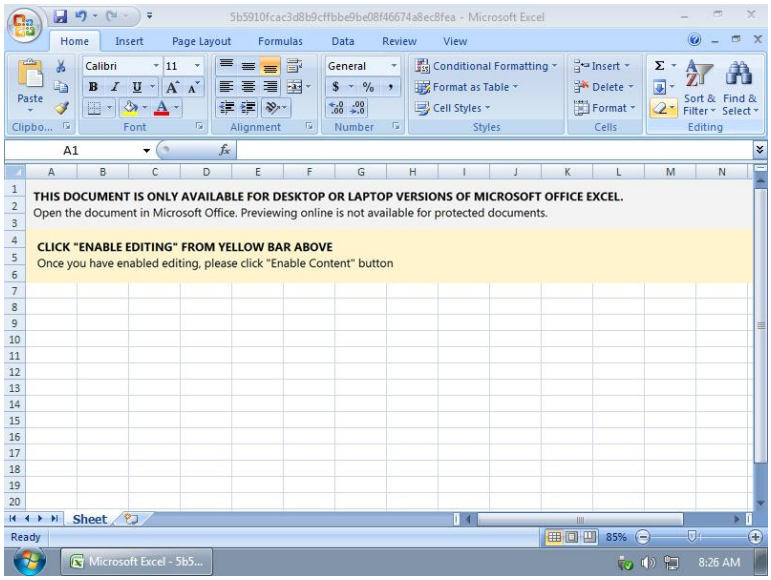

5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea - Microsoft Excel
THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCEL.
Open the document in Microsoft Office. Previewing online is not available for protected documents.
CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button
Sheet
Ready
8:25 AM

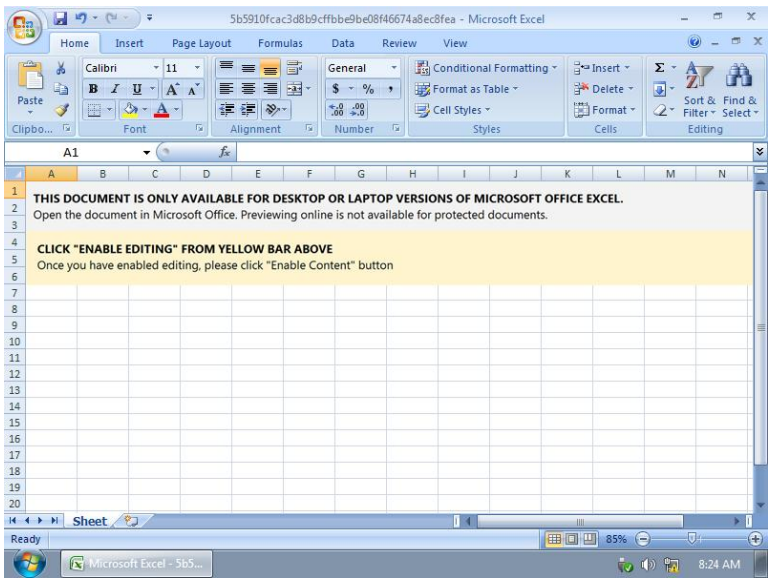

5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea - Microsoft Excel
Home
Insert
Page Layout
Formulas
Data
Review
View
Clear
Delete everything from the cell, or selectively remove the formatting, the contents, or the comments.
THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFI
Open the document in Microsoft Office. Previewing online is not available for protected documents.
CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button
Sheet
Ready
85%
8:25 AM

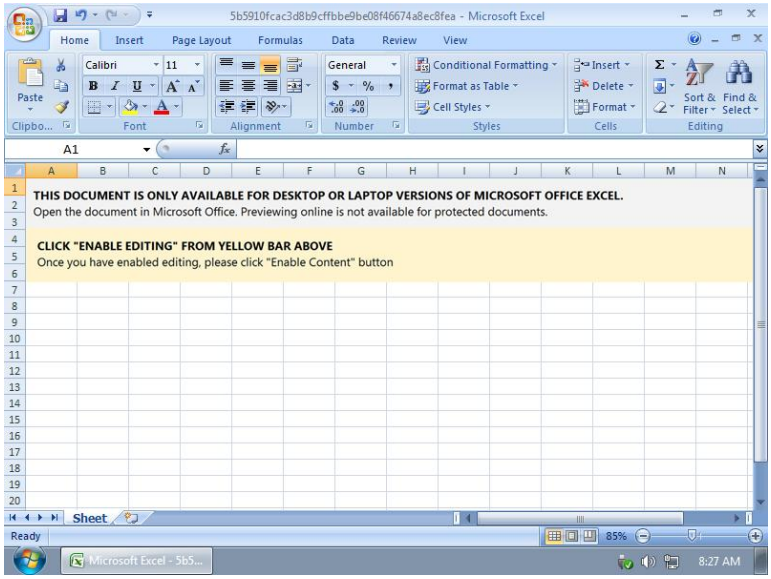

5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea - Microsoft Excel
Home
Insert
Page Layout
Formulas
Data
Review
View
THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCEL.
Open the document in Microsoft Office. Previewing online is not available for protected documents.
CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button
Sheet
Ready
85%
8:24 AM


5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea - Microsoft Excel
Home
Insert
Page Layout
Formulas
Data
Review
View
THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCEL.
Open the document in Microsoft Office. Previewing online is not available for protected documents.
CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button
Sheet
Ready
85%
8:27 AM


5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea - Microsoft Excel
THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCEL.
Open the document in Microsoft Office. Previewing online is not available for protected documents.
CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button
Sheet
Ready
8:25 AM


5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea - Microsoft Excel
THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCEL.
Open the document in Microsoft Office. Previewing online is not available for protected documents.
CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button
Sheet
Ready
8:26 AM


5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea - Microsoft Excel
THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCEL.
Open the document in Microsoft Office. Previewing online is not available for protected documents.
CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button
Sheet
Ready
8:24 AM


5b5910fcac3d8b9cffbbe9be08f46674a8ec8fea - Microsoft Excel
Home
Insert
Page Layout
Formulas
Data
Review
View
Calibri
11
General
Conditional Formatting
Format as Table
Cell Styles
Insert
Delete
Format
Sort & Filter
Find & Select
Paste
Font
Alignment
Number
Styles
Cells
Editing
A1
THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCEL.
Open the document in Microsoft Office. Previewing online is not available for protected documents.
CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button
Sheet
Ready
85%
Microsoft Excel - 5b5...
8:27 AM