VALKYRIE COMODO

Summary

File Name: P1804201801.xls

File Type: Composite Document File V2 Document, Can't read SAT

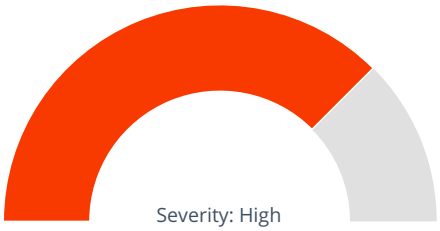
SHA1: 60eb4dcd71a666be0f5955c9c94427f5e4ec647d

MD5: ba38dbd2052f530fa8199fda35f0af80

MALWARE

Valkyrie Final Verdict

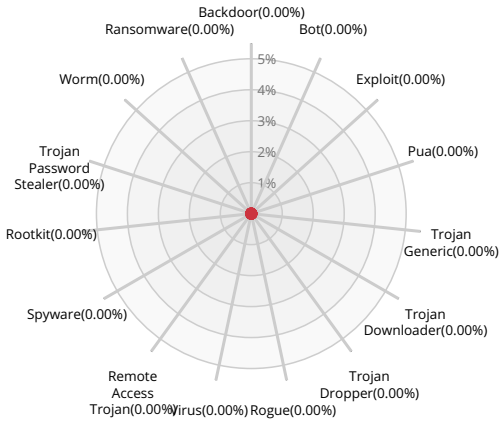
DETECTION SECTION



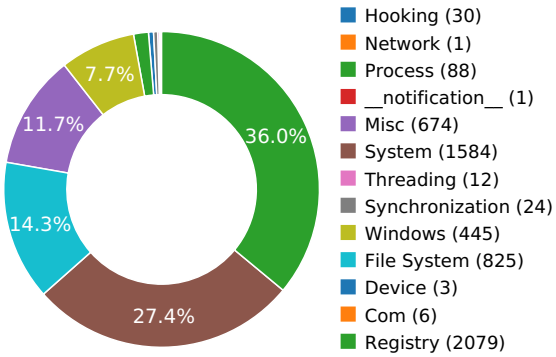
Severity: High

Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

NETWORKING

Performs some HTTP requests — Show sources

Generates some ICMP traffic

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

MALICIOUS DOCUMENT

The office file has a unconventional code page: ANSI Cyrillic; Cyrillic (Windows)

The office file has a macro. — Show sources

VALKYRIE COMODO

Behavior Graph

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\60eb4dcd71a666be0f5955c9c94427f5e4ec647d
C:\Users\user\AppData\Local\Temp\~DF0D6998647566FB5E.TMP
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:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
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:\Program Files (x86)\Common Files\microsoft shared\VBA\VBA6\VBE6.DLL
C:\Windows\AppPatch\sysmain.sdb
C:\Program Files (x86)\Common Files\microsoft shared\VBA\VBA6\
C:\Program Files (x86)
C:\Program Files (x86)\Common Files
C:\Program Files (x86)\Common Files\microsoft shared
C:\Program Files (x86)\Common Files\microsoft shared\VBA
C:\Program Files (x86)\Common Files\microsoft shared\VBA\VBA6
C:\Program Files (x86)\Common Files\microsoft shared\VBA\VBA6*.*
C:\Program Files (x86)\Common Files\microsoft shared\VBA\VBA6\1033\VBE6INTL.DLL
C:\Windows\sysnative\C_932.NLS
C:\Windows\sysnative\C_949.NLS
C:\Windows\sysnative\C_950.NLS
C:\Windows\sysnative\C_936.NLS
C:\Users\user\AppData\Local\Temp\~DF5F670B06F7747DD0.TMP
C:\Program Files (x86)\Microsoft Office\Office12\EXCEL.EXE
C:\Windows\SysWOW64\stdole2.tlb
C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\MSO.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\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\60eb4dcd71a666be0f5955c9c94427f5e4ec647d:Zone.Identifier
C:\Program Files (x86)\Microsoft Office\Office12\ID_00030.DPC
C:\Windows\SysWOW64\msiexec.exe.Local\
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
C:\Windows\WindowsShell.Manifest
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\Documents\http:\canyoning-austria.at\dashost
C:\Users\user\AppData\Local\Temp\
A:
B:
F:
G:
H:
I:
J:
K:
L:
M:
N:
O:
P:
Q:
R:
S:
T:

U:
V:
W:
X:
Y:
Z:
C:\
C:\Users\user\AppData\Local\Temp\MSIa561b.LOG
C:\Windows\SysWOW64\msimsg.dll

READ REGISTRY KEYS

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_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\QFE_Saskatchewan
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Options\QFE_Honshu
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\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\5CD521FB6DFE3D115AF2000A9CAC24AB\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\8CD521FB6DFE3D115AF2000A9CAC24AB\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\BCD521FB6DFE3D115AF2000A9CAC24AB\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\ECD521FB6DFE3D115AF2000A9CAC24AB\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-

18\Components\1DD521FB6DFE3D115AF2000A9CAC24AB\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\D811316032AC49B4E8BCC33454B31F61\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\F0B5D1A7DE3021C43A14422F0005333C\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Features\00002109E60090400000000000F01FEC\ProductFilesIntl_1033
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109E60090400000000000F01FEC\Features\ProductFilesIntl_1033
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\D2FFBA7ACD4FACF41929F6CCFE88DBDA\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\1650EACF3C291D11A92C0006794C4E25\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\110D06364BE0F08438A5ACEED069DCBC\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\7716FB73E5A23CA4180309AA54335EF9\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\1AD24949EBEB1D742A3F9F38DEF500BE\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\2154EBF3EFF04B048A77A9F7181445D6\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\D795BC613D313574CBB1FBE0448BFFA9\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\826BE7CCECB5A07419E4D5FC61E63C4A\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\F7CD01816C53D32438CF043106011676\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109E60090400000000000F01FEC\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_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
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\2EEF86DD963C1D111A37000A9CA05BF0\00002109030000000000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\359E92CC2CB71D119A12000A9CE1A22A\00002109030000000000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\A457B2D1A9DC1D112897000CF42C6133\00002109030000000000000000F01FEC

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

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\60eb4dcd71a666be0f5955c9c94427f5e4ec647d
C:\Users\user\AppData\Local\Temp\~DF0D6998647566FB5E.TMP
C:\Users\user\AppData\Local\Temp\~DF5F670B06F7747DD0.TMP
C:\Users\user\AppData\Local\Temp\MSIa561b.LOG

RESOLVED APIS

mso.dll.#8703
mso.dll.#6547
mso.dll.#8399
mso.dll.#2821
mso.dll.#3120
mso.dll.#8987
mso.dll.#581
mso.dll.#2727
mso.dll.#7045
mso.dll.#7038
mso.dll.#639
mso.dll.#7046
mso.dll.#7048
mso.dll.#2815
mso.dll.#7351
mso.dll.#7348
mso.dll.#8040
mso.dll.#6165
mso.dll.#7037
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

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1CB5CBE\1CB5CBE
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
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName

REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\DRM
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Security\FileOpenBlock
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1CB5CBE
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1CB5CBE\1CB5CBE
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_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\QFE_Saskatchewan
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Options\QFE_Honshu
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

READ FILES

C:\Users\user\AppData\Local\Temp\60eb4dcd71a666be0f5955c9c94427f5e4ec647d

C:\Users\user\AppData\Local\Temp\~DF0D6998647566FB5E.TMP

C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\RICHED20.DLL

C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui

C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\1033\ALRTINTL.DLL

C:\Windows\System32\imageres.dll

C:\Program Files (x86)\Common Files\microsoft shared\VBA\VBA6\VBE6.DLL

C:\Windows\AppPatch\sysmain.sdb

C:\Program Files (x86)\Common Files\microsoft shared\VBA\VBA6\

C:\Program Files (x86)\Common Files\microsoft shared\VBA\VBA6\1033\VBE6INTL.DLL

C:\Users\user\AppData\Local\Temp\~DF5F670B06F7747DD0.TMP
C:\Program Files (x86)\Microsoft Office\Office12\EXCEL.EXE
C:\Windows\SysWOW64\stdole2.tlb
C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\MSO.DLL
C:\Users\user\AppData\Roaming\Microsoft\Office\review.rcd
C:\Users\user\AppData\Roaming\Microsoft\Office\adhoc.rcd
C:\Program Files (x86)\Microsoft Office\Office12\ID_00030.DPC
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
C:\Windows\WindowsShell.Manifest
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\Documents\http:\canyoning-austria.at\dashost
C:\Windows\SysWOW64\msimsg.dll
\Device\KsecDD

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
Local\ZoneAttributeCacheCounterMutex
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex
Global\MSILOG_0e978c4a1d4fb02GOL.b165aISM_pmeT_lacoL_ataDppA_resu_sresU_:C
Global_MSIExecute

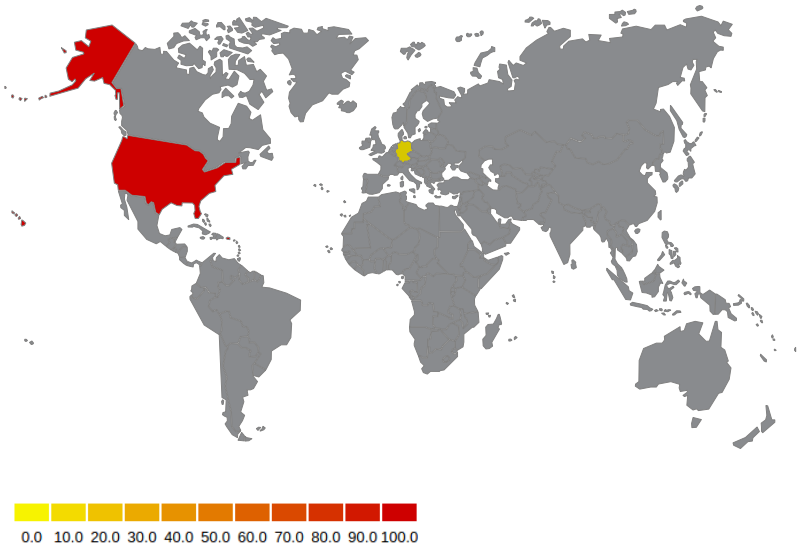
MODIFIED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1CB5CBE\1CB5CBE
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109E60090400000000000F01FEC\Usage\ProductNonBootFilesIntl_1033
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\VBAFiles
HKEY_CURRENT_USER\Software\Microsoft\VBA\6.0\Common
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\1CB6624
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1CB6624\1CB6624
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Max Display
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet

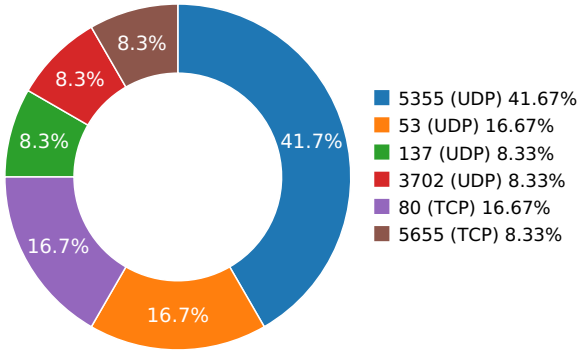
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DBB8B4CD1B191052E8F325736

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
	104.17.210.9	United States	13335	Cloudflare, Inc.	Malware Process
	104.18.20.226	United States	13335	Cloudflare, Inc.	Malware Process
www.cloudflare.com	104.17.209.9	United States	13335	Cloudflare, Inc.	Malware Process
canyoning-austria.at	194.177.142.4	Austria	6798		Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
canyoning-austria.at	80	GET	1.1	Windows Installer	1	12.3337190151
Path: /dashost **URI:** http://canyoning-austria.at/dashost						

DNS QUERIES

Request	Type
canyoning-austria.at	A
Answers - 194.177.142.4 (A)	
www.cloudflare.com	A
Answers - 104.17.209.9 (A) - 104.17.210.9 (A)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
12.3337190151	Sandbox	194.177.142.4	80
58.7972919941	Sandbox	159.69.48.50	5655

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.03948688507	Sandbox	239.255.255.250	3702
3.04058098793	Sandbox	224.0.0.252	5355
3.04140496254	Sandbox	224.0.0.252	5355
3.11093401909	Sandbox	192.168.56.255	137
5.5955119133	Sandbox	224.0.0.252	5355
9.54390287399	Sandbox	224.0.0.252	5355
12.0963928699	Sandbox	8.8.4.4	53
43.2450199127	Sandbox	224.0.0.252	5355
45.2342779636	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\~DF5F670B06F7747DD0.TMP	**Type :** Composite Document File V2 Document, No summary info **MD5 :** 3df5ee19ca6fa6c673e02f4d0b259491 **SHA-1 :** 151c7a17912b8c9c7c4c5d7c8ab5d0f221867597 **SHA-256 :** 002b6c904ead15a44f31df9346ef252e46f22cd24 **SHA-512 :** 8ffe5e5372ff6d0c74ab76505442bc7a8cd89c074 **Size :** 16.384 Kilobytes.
C:\Users\User\AppData\Local\Temp\60eb4dcd71a666be0f5955c9c94427f5e4ec647d	**Type :** Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1251, Author: Microsoft Office, Last Saved By: 1, Name of Creating Application: Microsoft Excel, Create Time/Date: Wed Dec 19 10:42:12 2018, Last Saved Time/Date: Thu Apr 18 13:01:17 2019, Security: 0 **MD5 :** 9aad32093ecf58b8805fecedafec2b3d **SHA-1 :** bc43347dcb902c6fcf6ad7be4de45ea52af64e68 **SHA-256 :** 57f33e3e0888a8020bd2a58655e3d92e300f37bf **SHA-512 :** 1303a72cbd974fb1c0903e32a6b23c02a5cb4b7c **Size :** 160.768 Kilobytes.
C:\Users\User\AppData\Local\Temp\MSIa561b.LOG	**Type :** data **MD5 :** b7a3d4f199044fd0d40b7f9f4cde8233 **SHA-1 :** f9ccf2924d13c024b500fa9807df307ca7116cd7 **SHA-256 :** 7e9ad5b22cbc4aa1df0d0123be34703d8571d55l **SHA-512 :** 7993be4366ed1eaabd56c311a60a50ab31948f68 **Size :** 171.878 Kilobytes.
C:\Users\User\AppData\Local\Temp\30033750.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:	P1804201801.xls
File Type:	Composite Document File V2 Document, Can't read SAT
SHA1:	60eb4dcd71a666be0f5955c9c94427f5e4ec647d
MD5:	ba38dbd2052f530fa8199fda35f0af80
First Seen Date:	2019-04-19 13:07:48.331251 (6 days ago)
Number Of Clients Seen:	5
Last Analysis Date:	2019-04-19 13:19:17.397412 (6 days ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

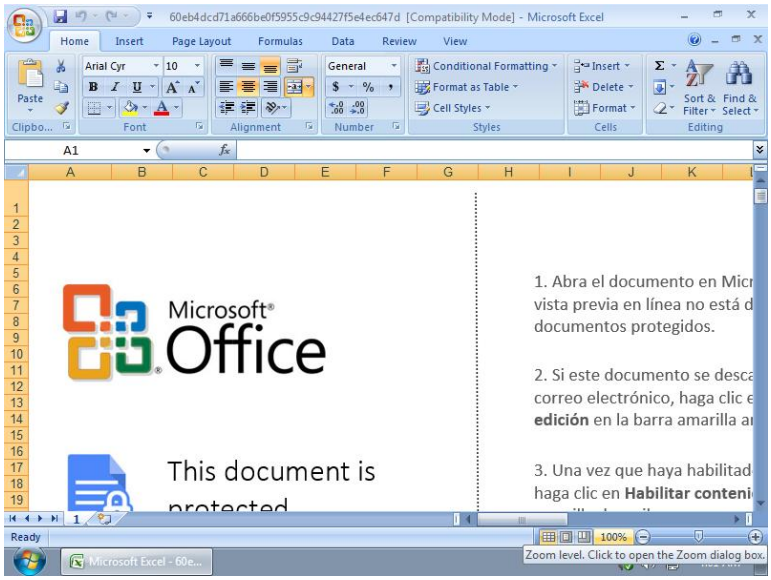
PE Headers

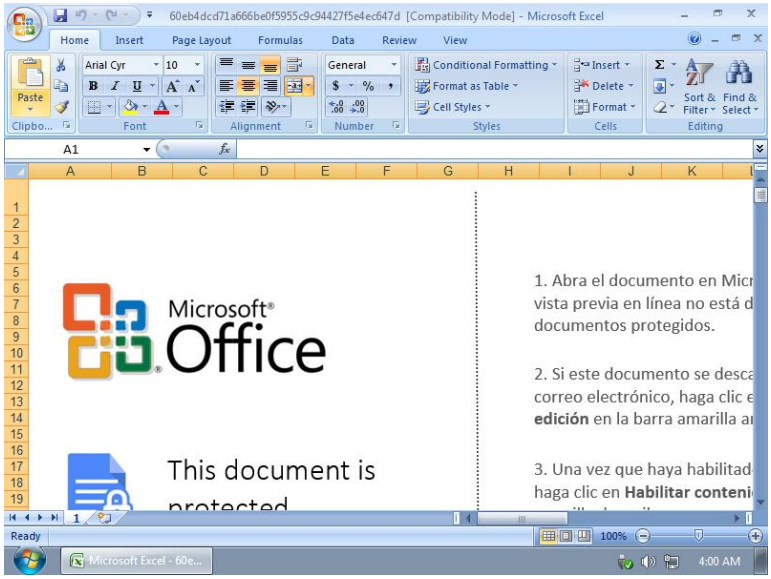
PROPERTY	VALUE
Magic Literal Enum	43
File Type Enum	8
File Size	160768
Sha256	3d69e426426eaf5756aff41391fd74f34a52f983de8ed2ff75a800a9f5a4037f
Mime Type	application/CDFV2-unknown

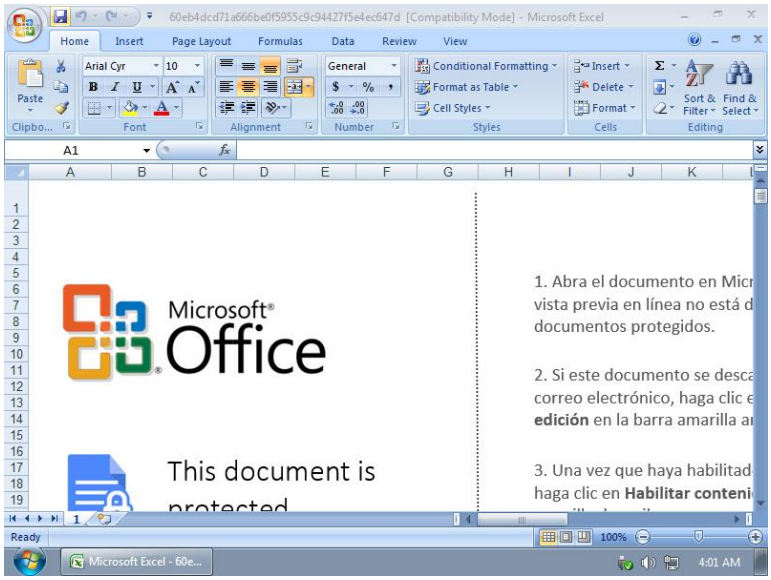
CERTIFICATE VALIDATION

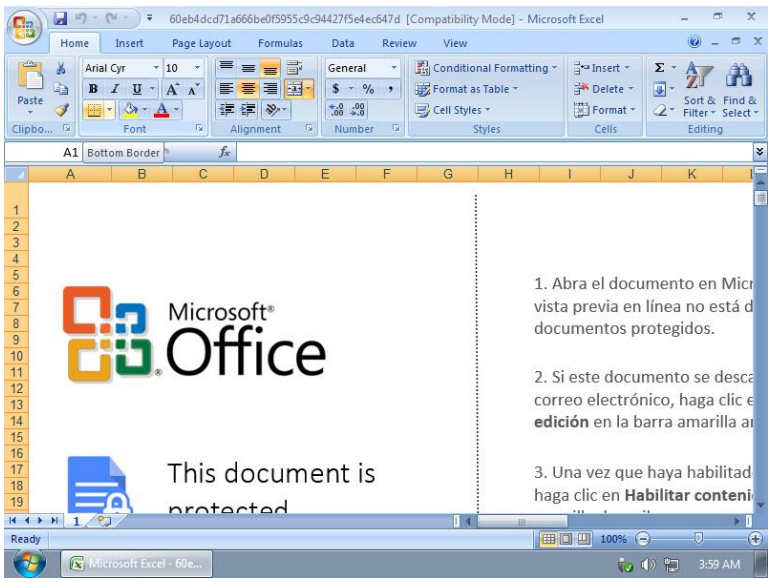
- Certificate Validation is not Applicable ?

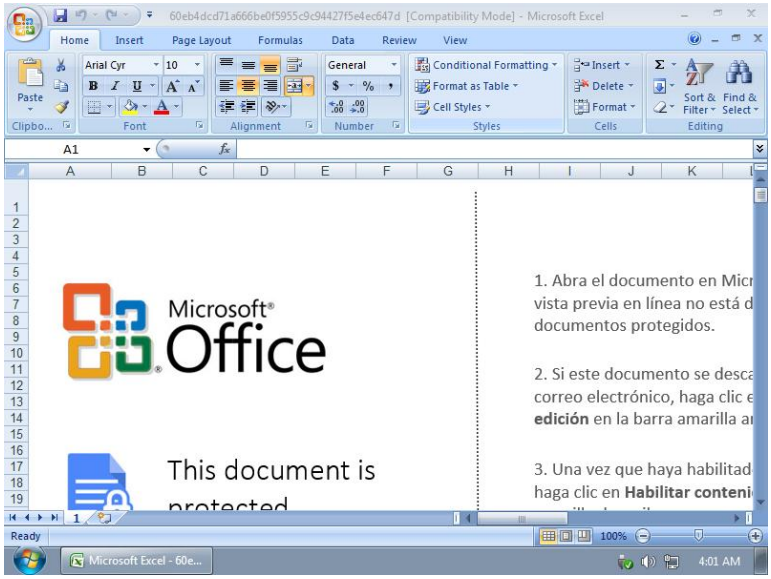
SCREENSHOTS

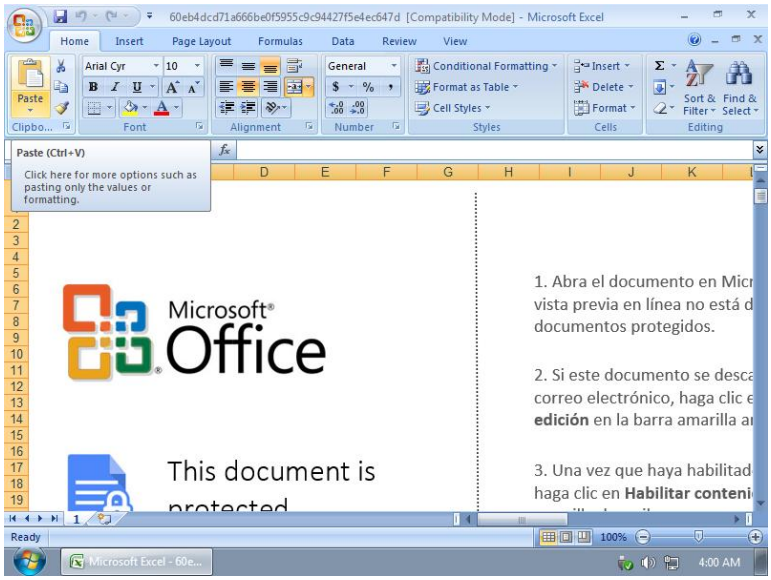


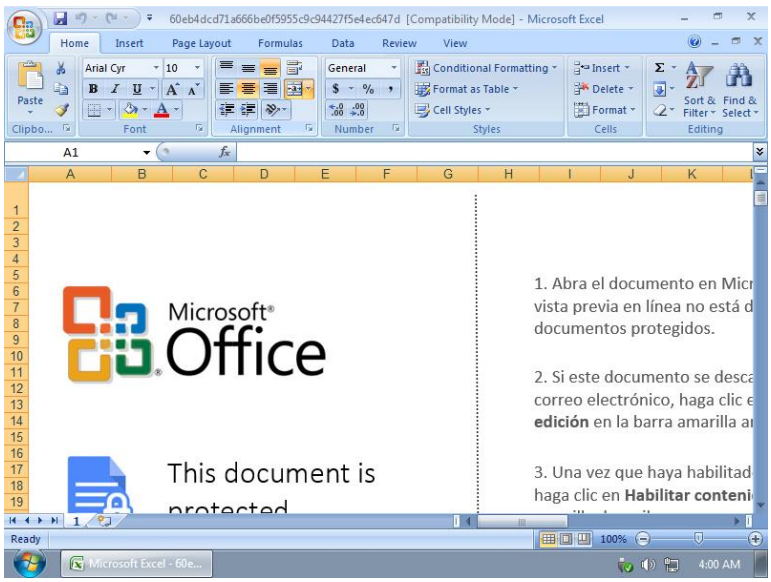

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
4:00 AM

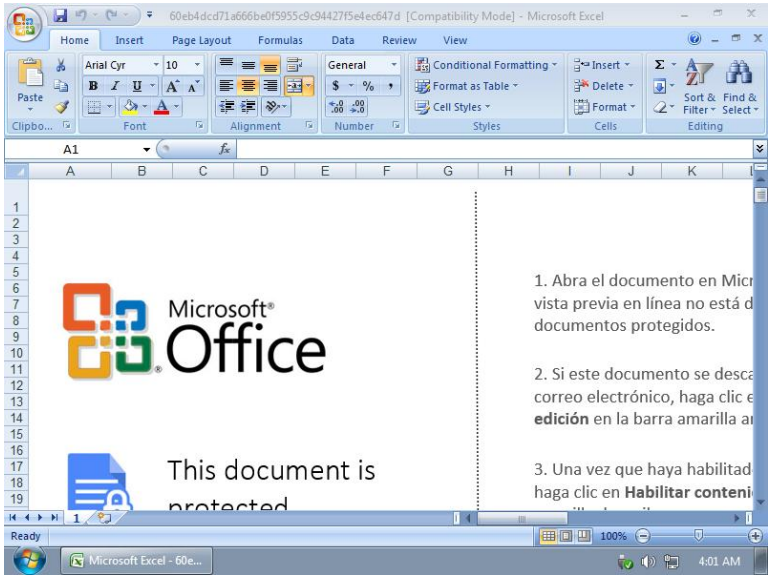

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
4:01 AM

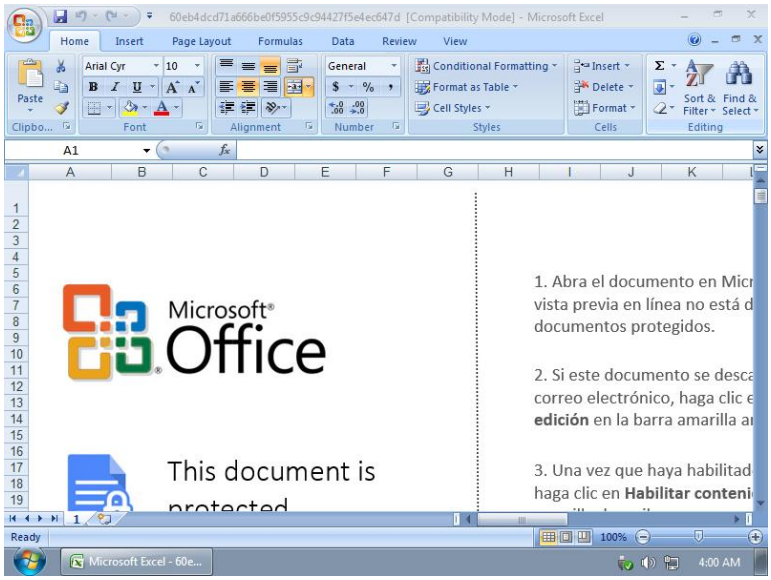

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Bottom Border
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
3:59 AM

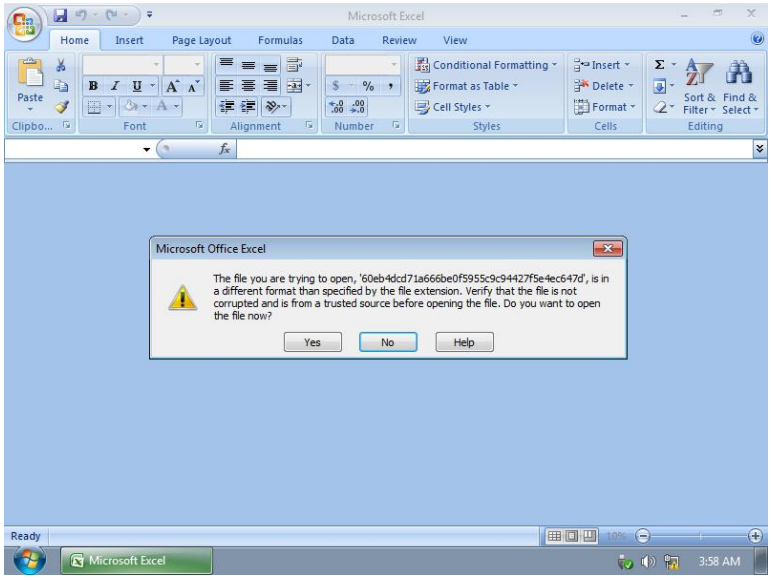

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
4:01 AM

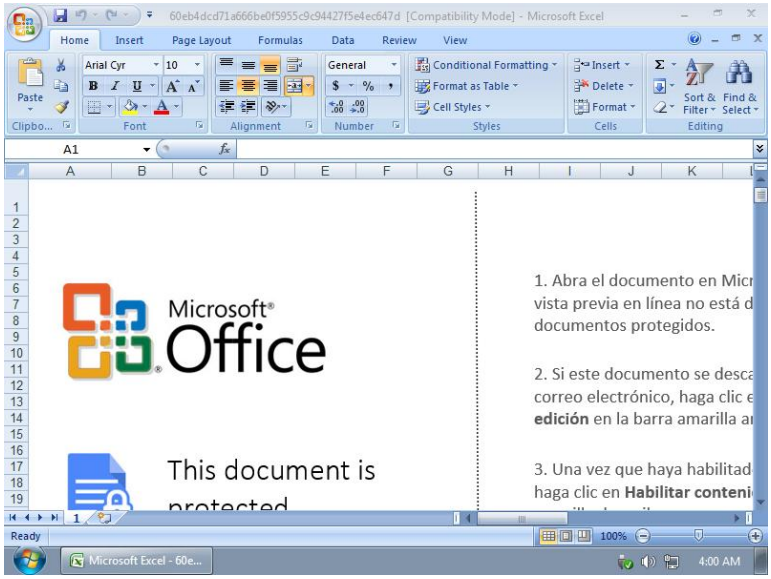

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Paste (Ctrl+V)
Click here for more options such as pasting only the values or formatting.
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
4:00 AM

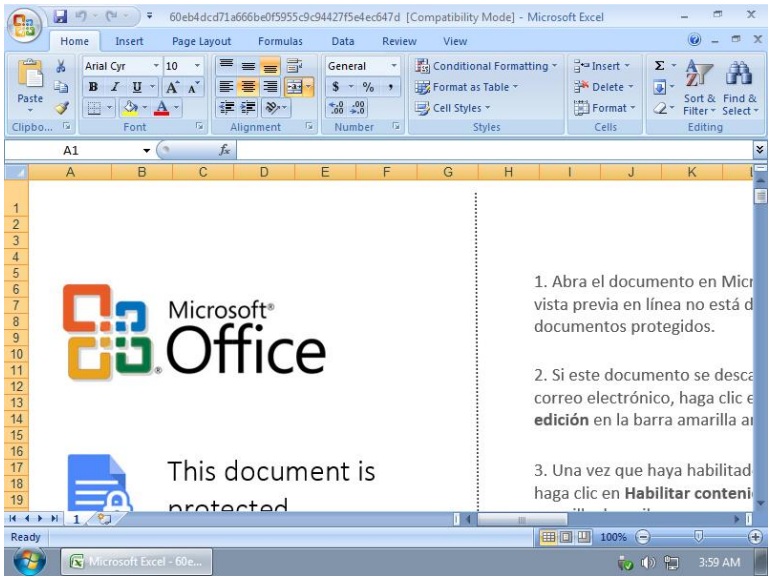

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
4:00 AM

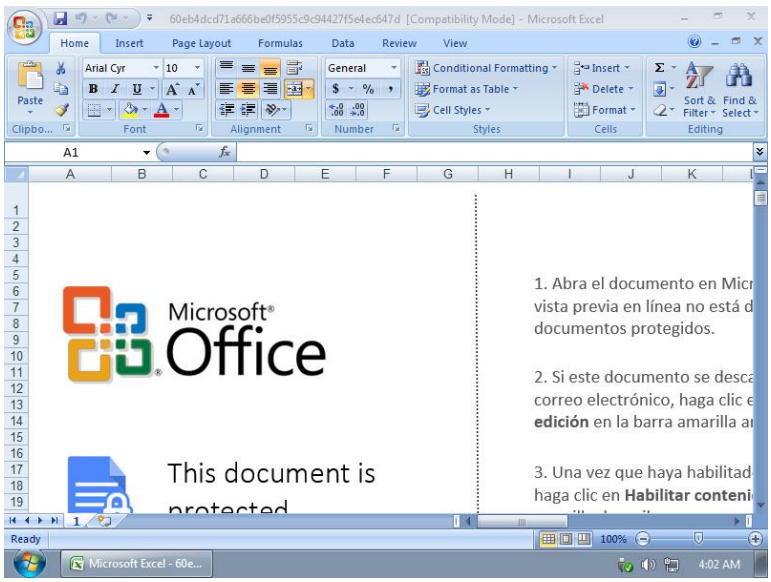

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
Microsoft Excel - 60e...
4:01 AM

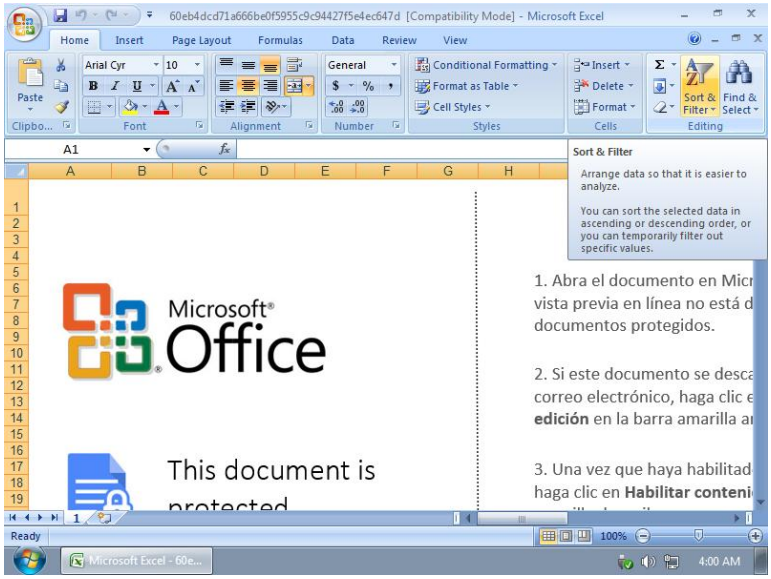

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
Microsoft Excel - 60e...
4:00 AM

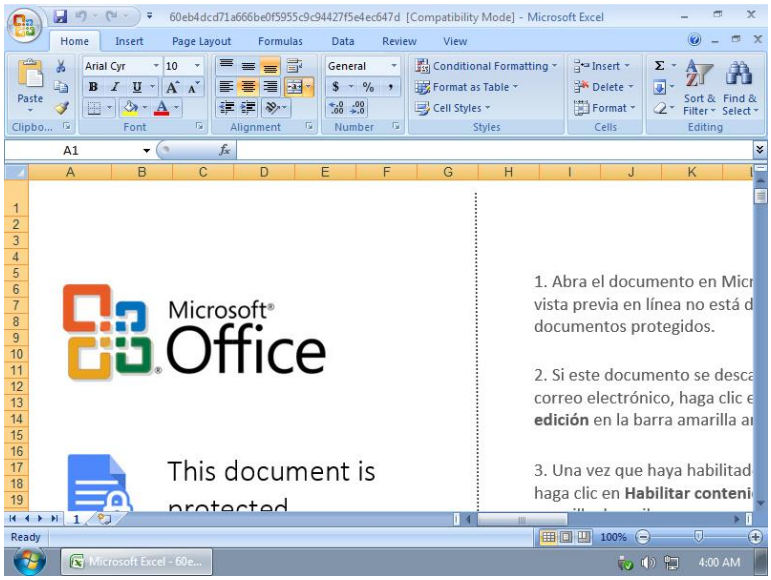

Microsoft Excel
Microsoft Office Excel
The file you are trying to open, '60eb4dcd71a666be0f5955c9c94427f5e4ec647d', is in a different format than specified by the file extension. Verify that the file is not corrupted and is from a trusted source before opening the file. Do you want to open the file now?
Yes
No
Help
Ready
Microsoft Excel
3:58 AM

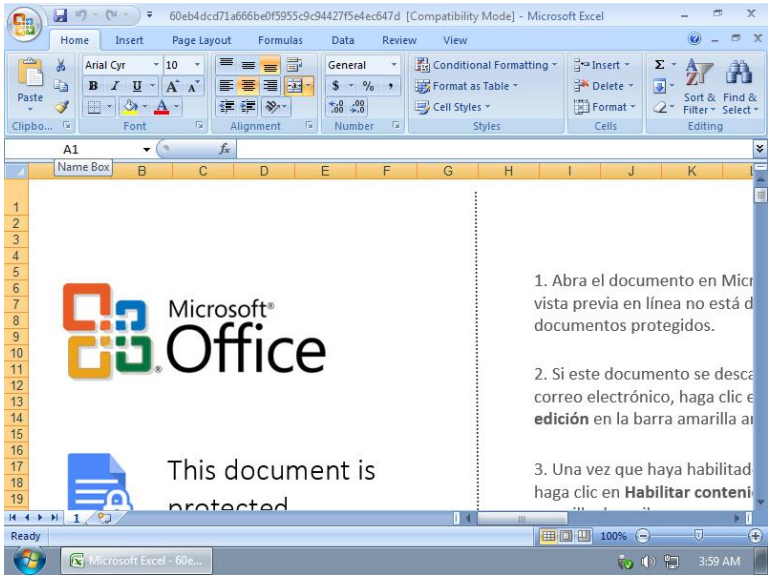

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
4:00 AM

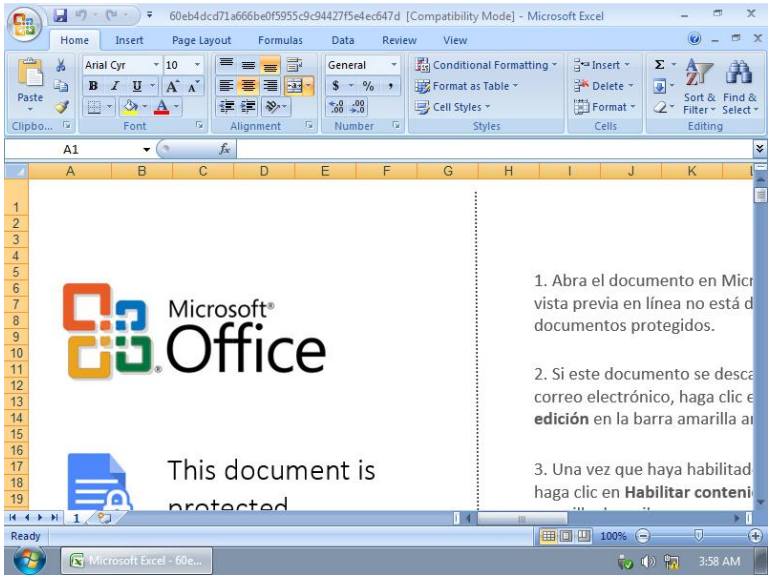

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
3:59 AM

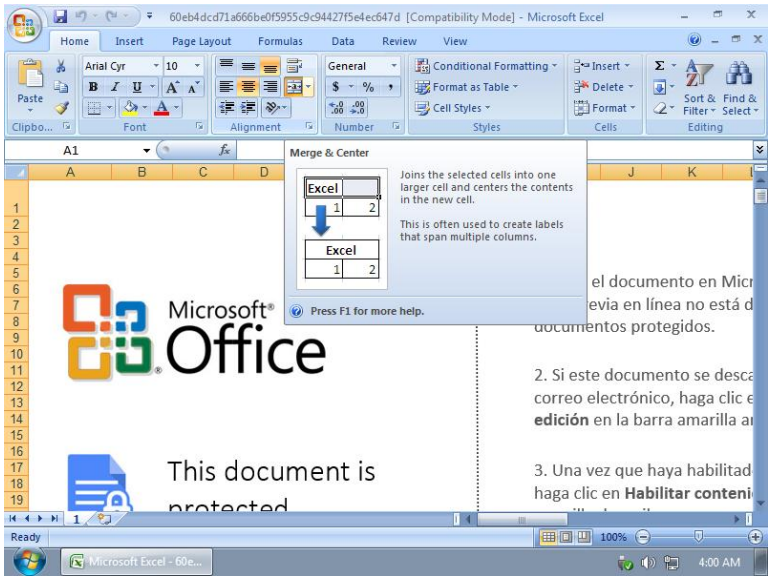

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
4:02 AM

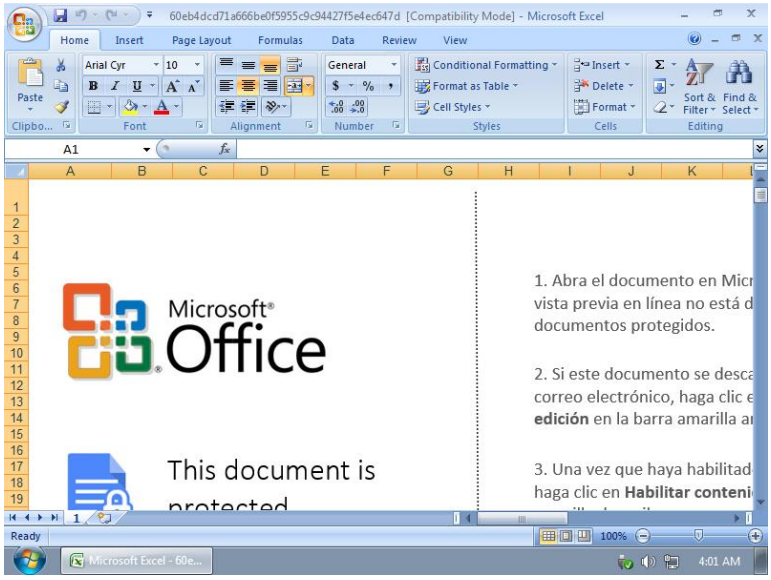

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Sort & Filter
Arrange data so that it is easier to analyze.
You can sort the selected data in ascending or descending order, or you can temporarily filter out specific values.
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
4:00 AM

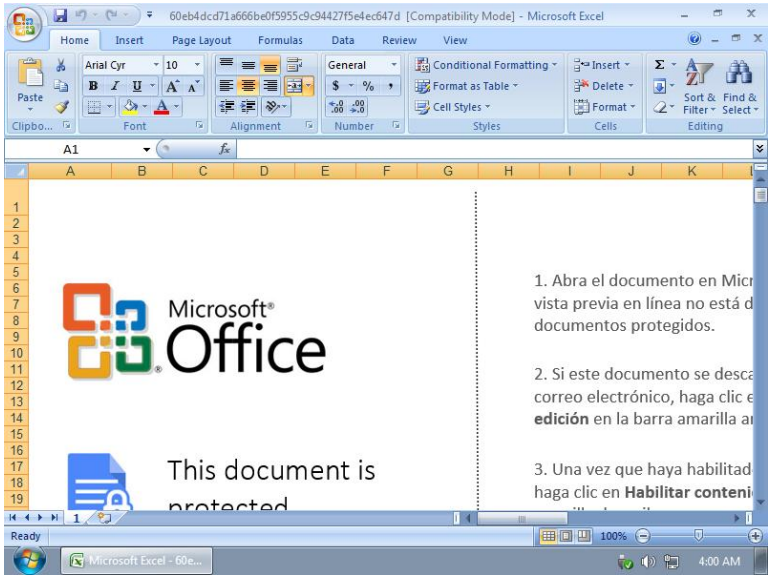

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
4:00 AM

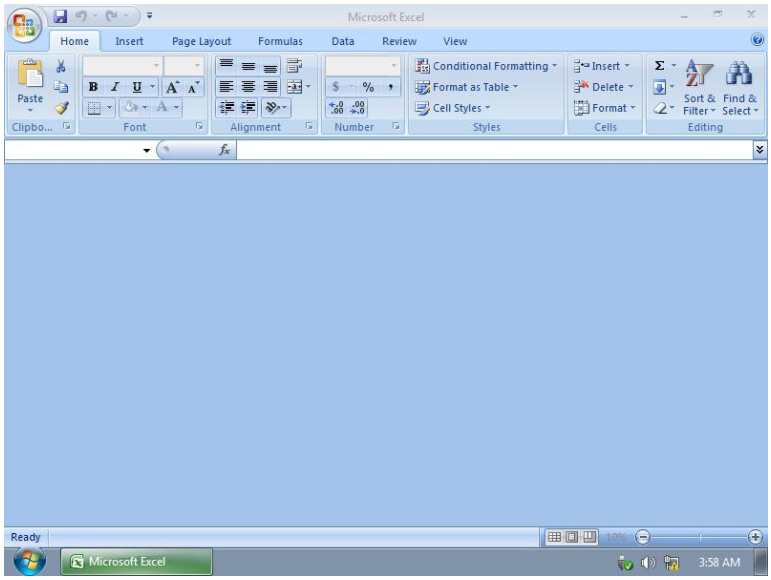

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Name Box
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
3:59 AM

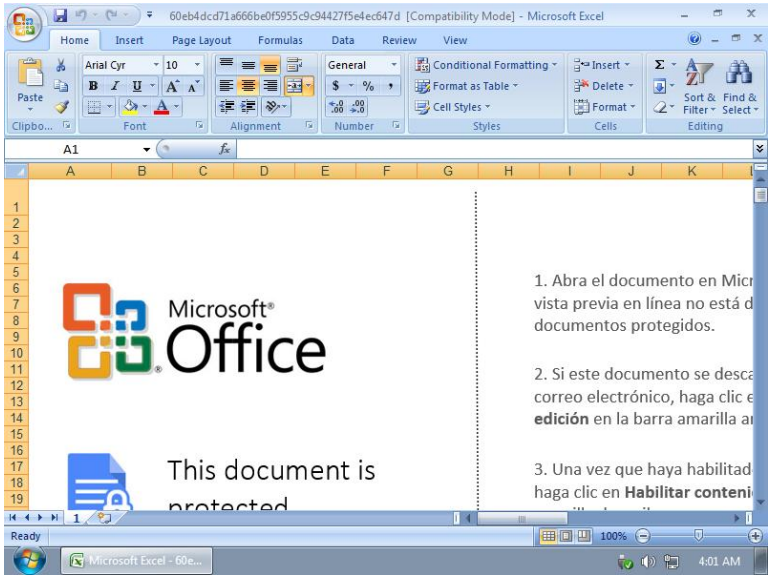

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
3:58 AM

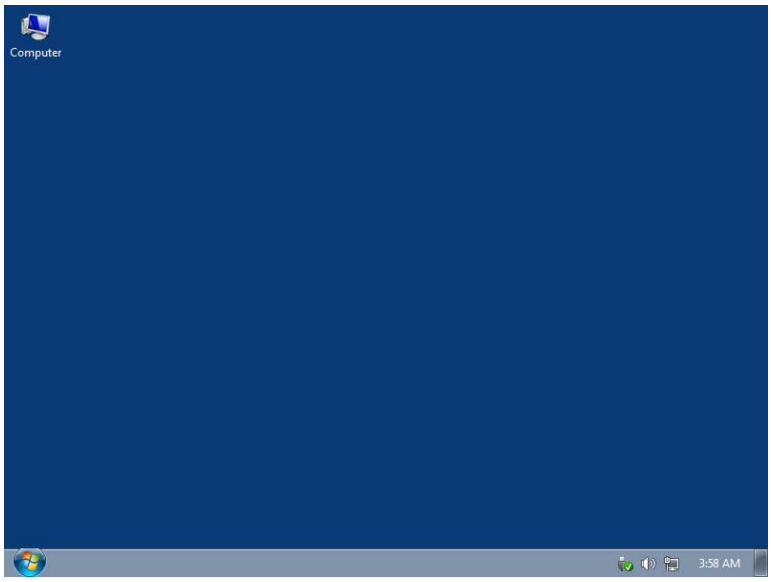

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Merge & Center
Excel
1
2
Joins the selected cells into one larger cell and centers the contents in the new cell.
This is often used to create labels that span multiple columns.
Press F1 for more help.
Microsoft Office
This document is
Ready
4:00 AM

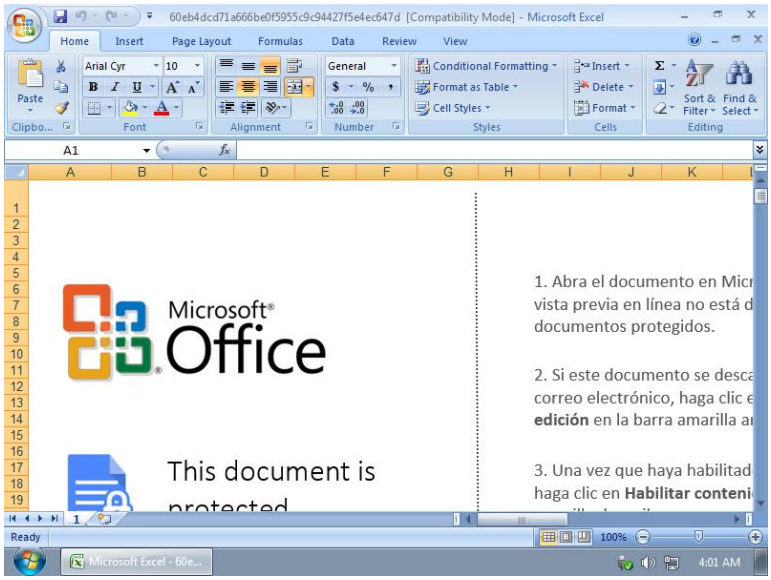

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
4:01 AM

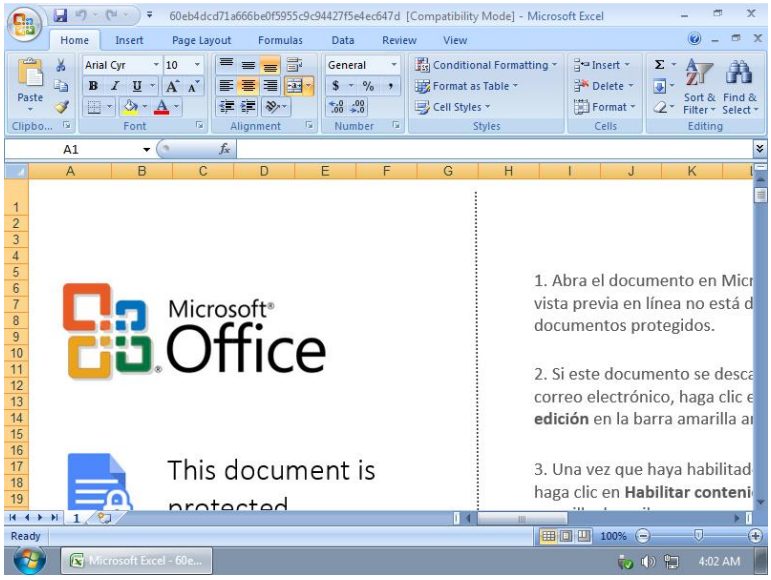

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
4:00 AM

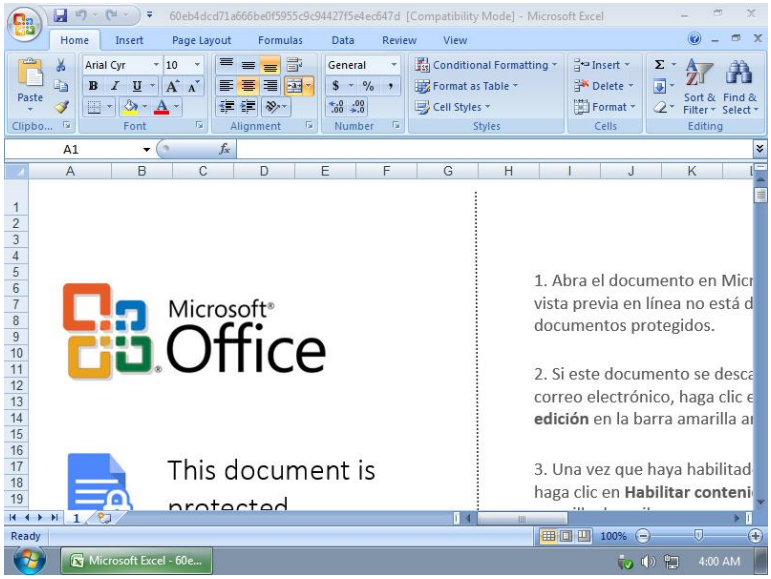

Microsoft Excel
Ready
3:58 AM

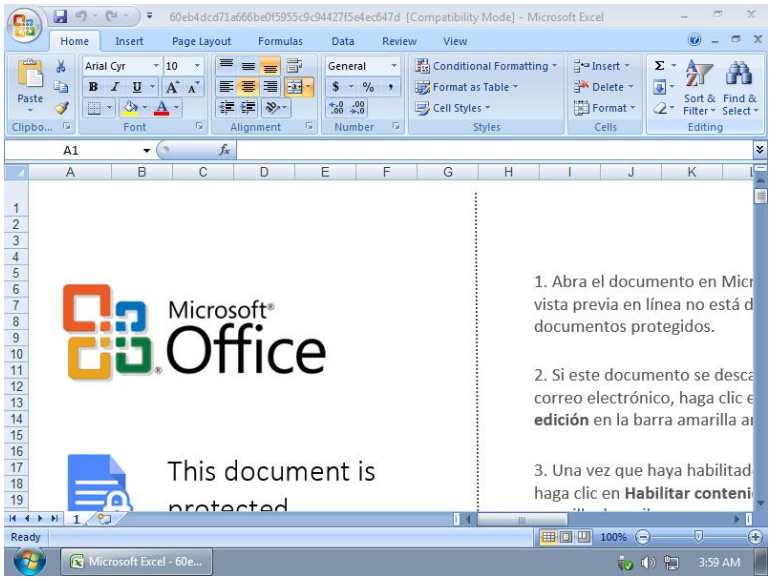

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
4:01 AM

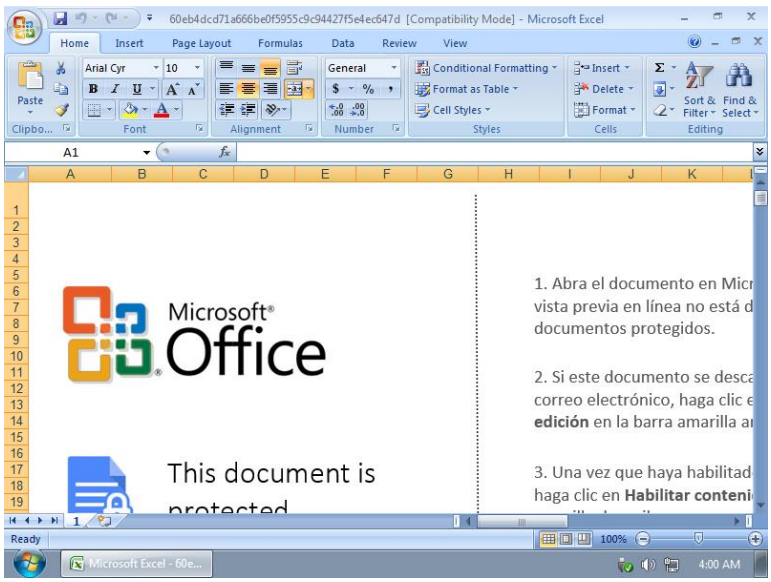

Computer
3:58 AM

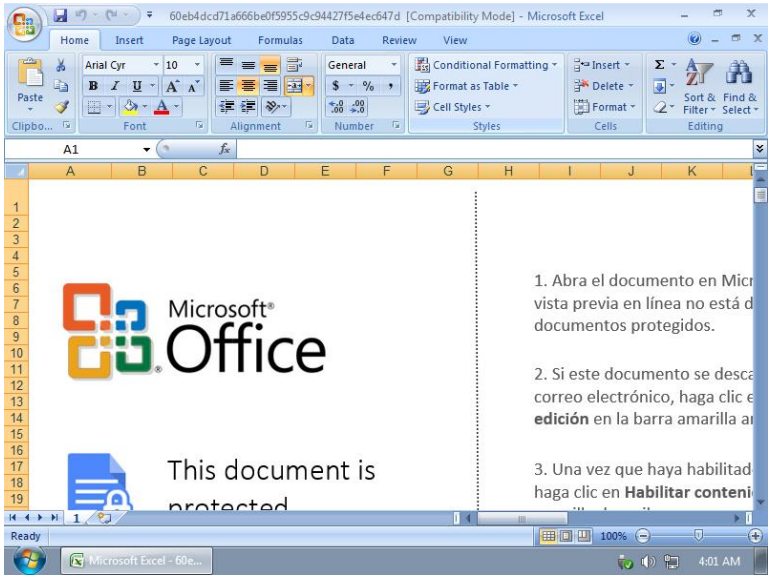

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Home
Insert
Page Layout
Formulas
Data
Review
View
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
100%
4:01 AM

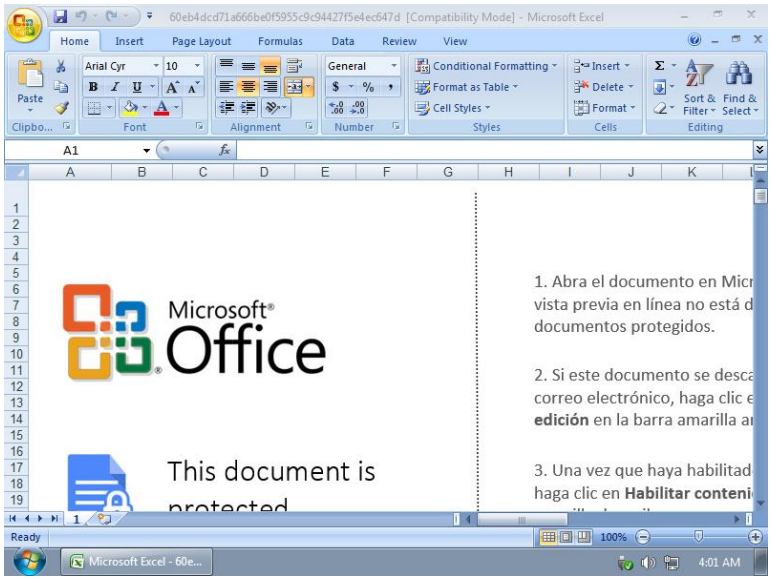

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Home
Insert
Page Layout
Formulas
Data
Review
View
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
100%
4:02 AM

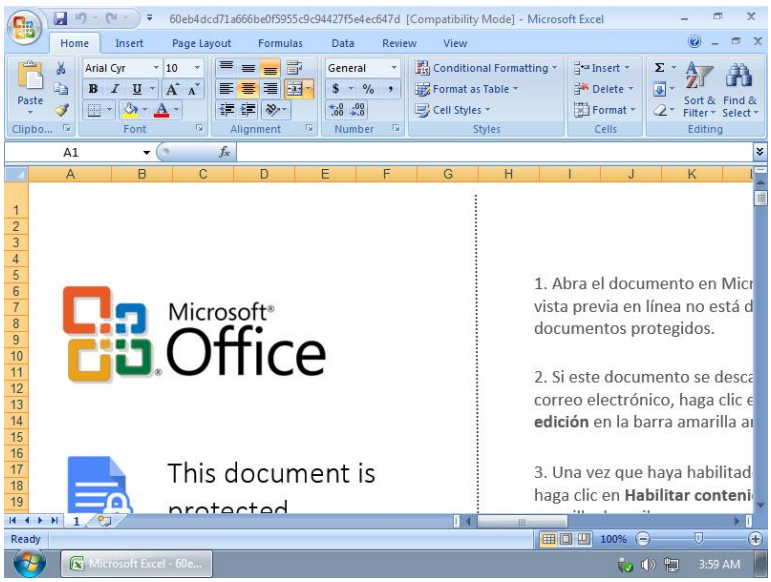

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
4:00 AM

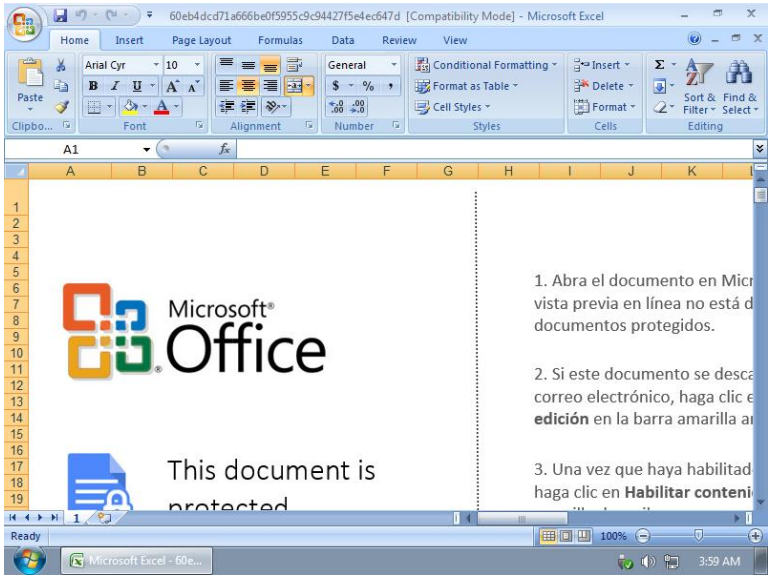

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
3:59 AM

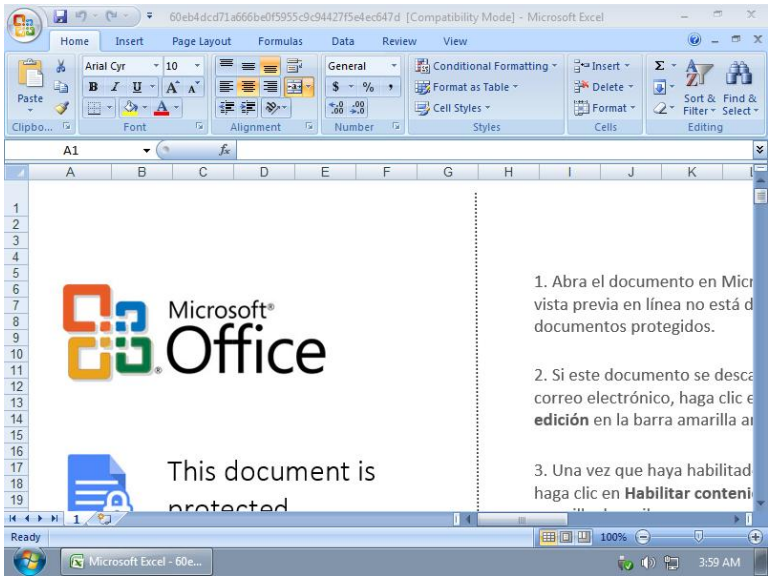

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
4:00 AM

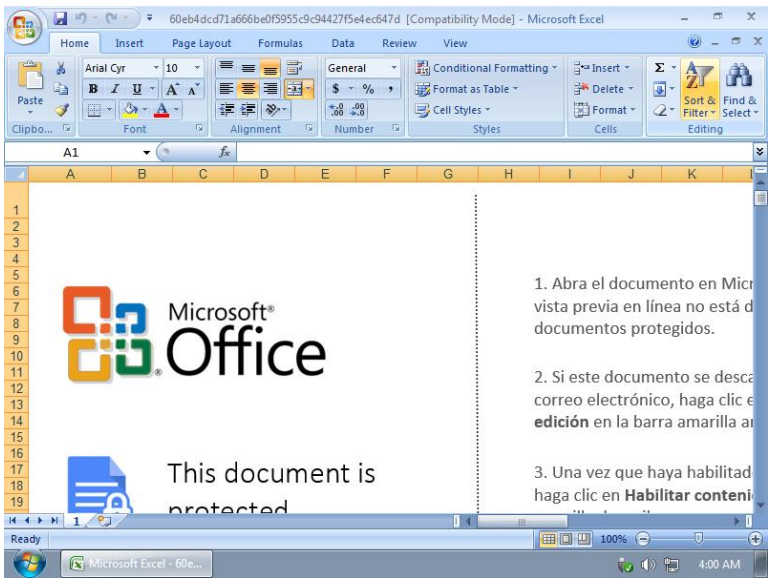

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
4:01 AM

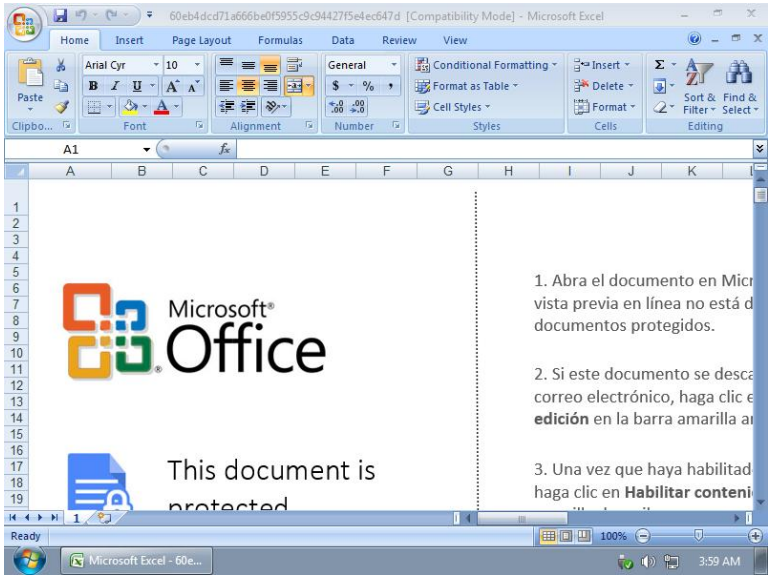

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
4:01 AM

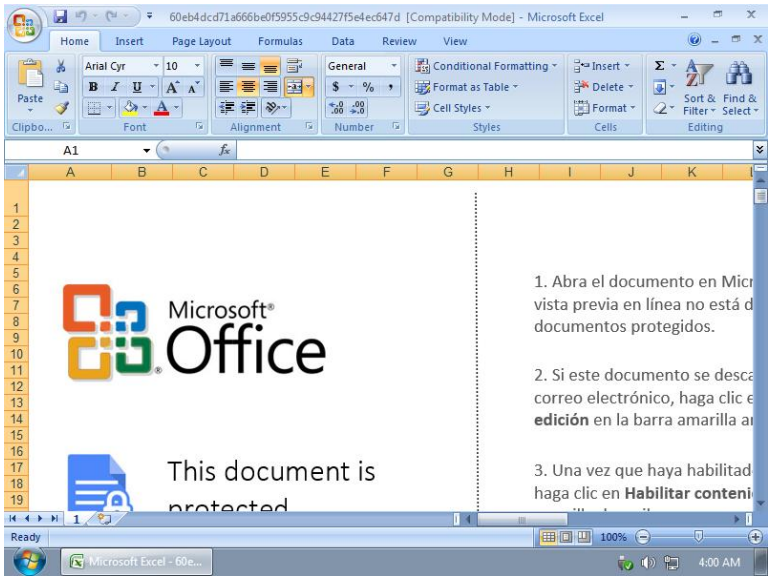

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
3:59 AM

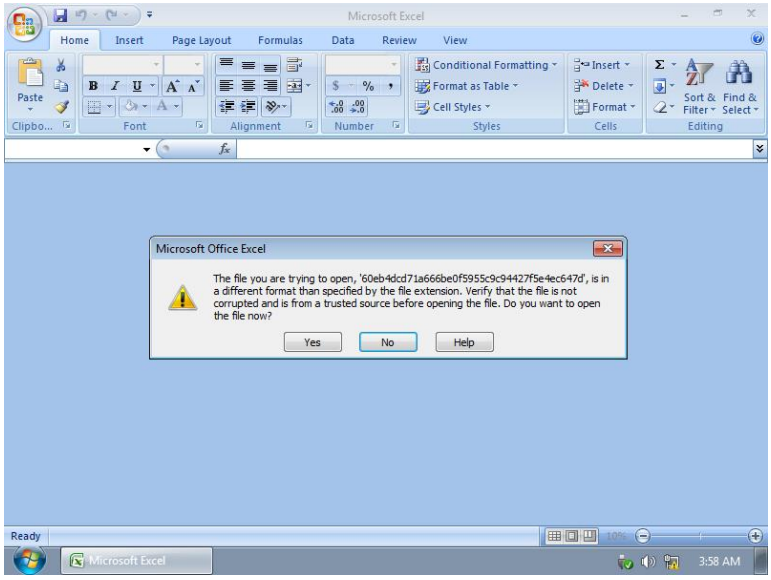

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
3:59 AM

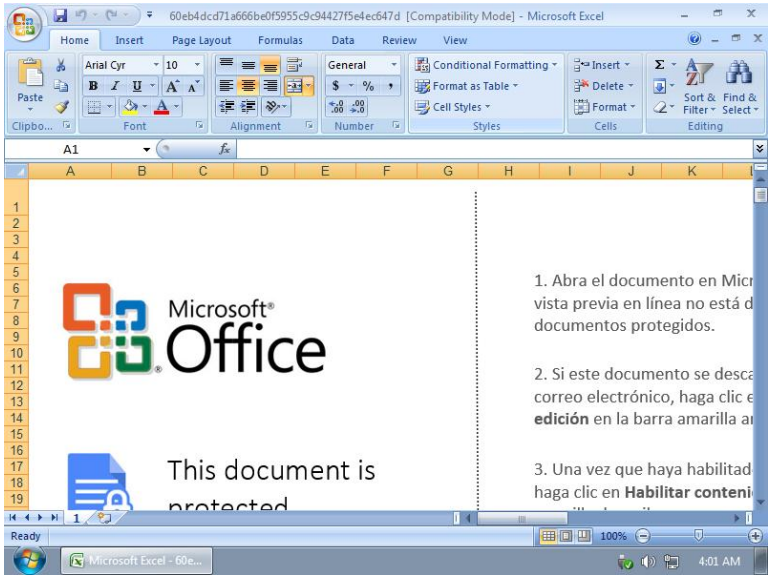

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
3:59 AM

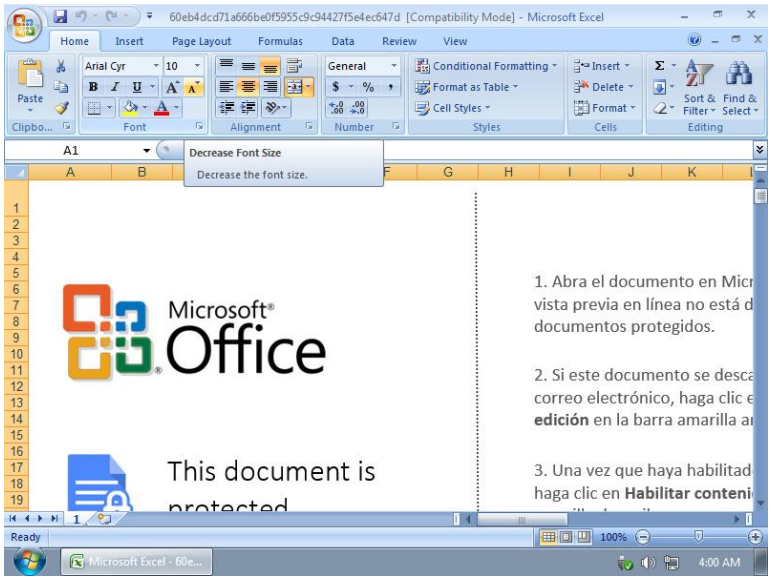

60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
4:00 AM


60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
Microsoft Excel - 60e...
3:59 AM


60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Microsoft Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
Microsoft Excel - 60e...
4:00 AM


Microsoft Excel
Microsoft Office Excel
The file you are trying to open, '60eb4dcd71a666be0f5955c9c94427f5e4ec647d', 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
Ready
Microsoft Excel
3:58 AM


60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Home
Insert
Page Layout
Formulas
Data
Review
View
Paste
Arial Cyr
10
General
Conditional Formatting
Format as Table
Cell Styles
Insert
Delete
Format
Sort & Filter
Find & Select
Clipbo...
Font
Alignment
Number
Styles
Cells
Editing
A1
Microsoft® Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
100%
4:01 AM


60eb4dcd71a666be0f5955c9c94427f5e4ec647d [Compatibility Mode] - Microsoft Excel
Home
Insert
Page Layout
Formulas
Data
Review
View
Paste
Arial Cyr
10
General
Conditional Formatting
Format as Table
Cell Styles
Insert
Delete
Format
Sort & Filter
Find & Select
Clipbo...
Font
Alignment
Number
Styles
Cells
Editing
A1
Decrease Font Size
Decrease the font size.
Microsoft® Office
This document is
1. Abra el documento en Micr
vista previa en línea no está d
documentos protegidos.
2. Si este documento se desca
correo electrónico, haga clic e
edición en la barra amarilla a
3. Una vez que haya habilitad
haga clic en Habilitar conteni
Ready
100%
4:00 AM