JoeSandbox Cloud BASIC

ID: 383850
Sample Name: New Text Document.exe
Cookbook: default.jbs
Time: 11:03:29
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

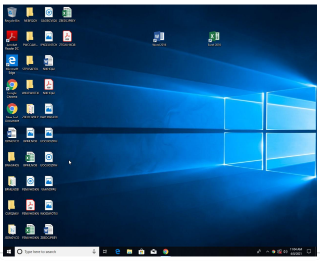
Analysis Report New Text Document.exe

Overview

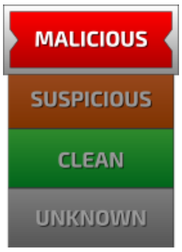
General Information

Sample Name:	New Text Document.exe
Analysis ID:	383850
MD5:	4e79b531f4f6813..
SHA1:	addcb0a2aac14b..
SHA256:	9445838c514498..
Infos:	

Most interesting Screenshot:



Detection

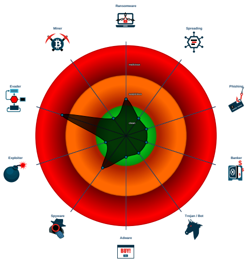


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Icon mismatch, binary includes an ic…
- Multi AV Scanner detection for subm…
- Binary is likely a compiled AutoIt sc…
- Found API chain indicative of debug…
- Initial sample is a PE file and has a …
- Uses Windows timers to delay exec…
- Contains functionality to check if a d…
- Contains functionality to check if a d…
- Contains functionality to check if a w…
- Contains functionality to retrieve info…
- Contains functionality to simulate ke…
- Detected potential crypto function
- Found a high number of Window / Us

Classification



Startup

- **System is w10x64**
- New Text Document.exe (PID: 6780 cmdline: 'C:\Users\user\Desktop\New Text Document.exe' MD5: 4E79B531F4F6813CC8E21894A13C5537)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

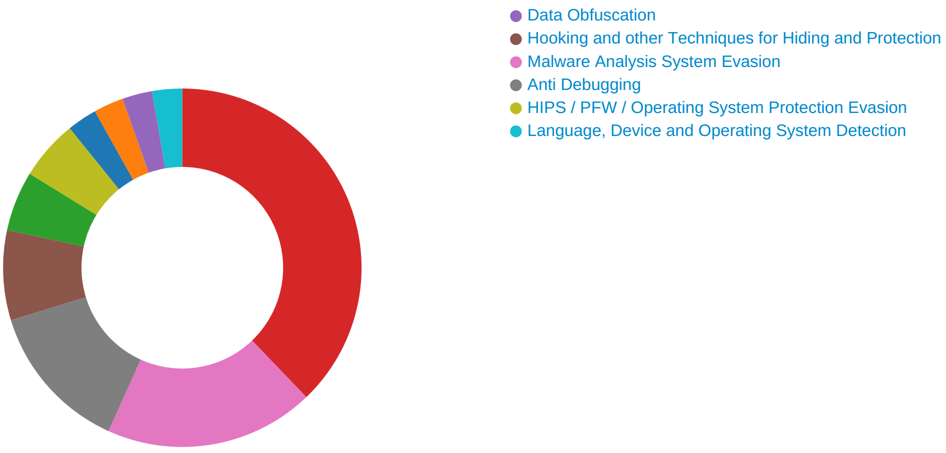
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- ● AV Detection
- ● Compliance
- ● Key, Mouse, Clipboard, Microphone and Screen Capturing
- ● System Summary



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

System Summary:

Binary is likely a compiled AutoIt script file

Initial sample is a PE file and has a suspicious name

Hooking and other Techniques for Hiding and Protection:

Icon mismatch, binary includes an icon from a different legit application in order to fool users

Malware Analysis System Evasion:

Uses Windows timers to delay execution

Anti Debugging:

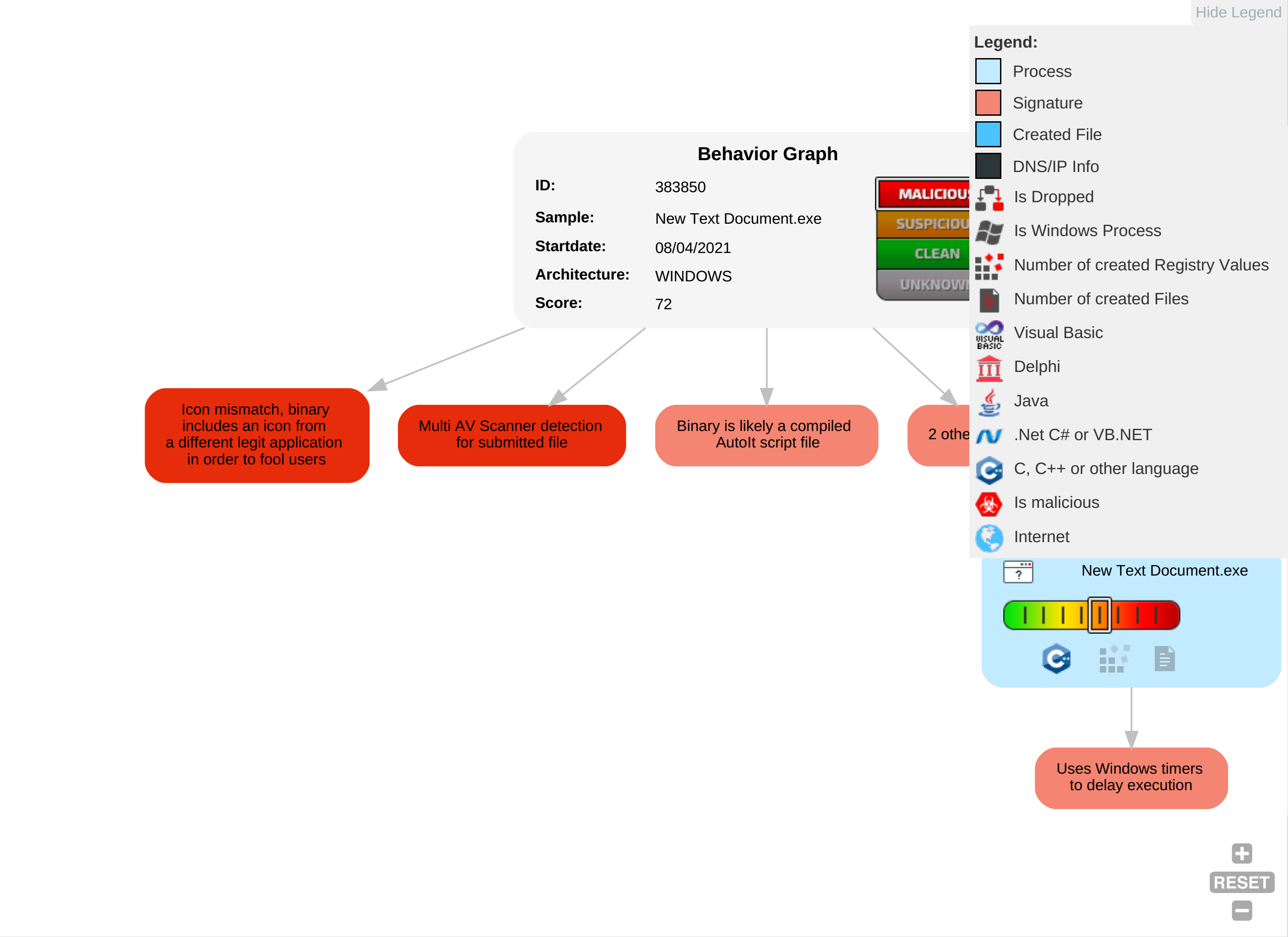
Found API chain indicative of debugger detection

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	Input Capture 2 1	System Time Discovery 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communi
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 2	LSASS Memory	Security Software Discovery 1 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Data	Exploit SS Redirect F Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Virtualization/Sandbox Evasion 2 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Application Window Discovery 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communi

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service

Behavior Graph



Legend:

- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

Behavior Graph

ID:	383850
Sample:	New Text Document.exe
Startdate:	08/04/2021
Architecture:	WINDOWS
Score:	72

Icon mismatch, binary includes an icon from a different legit application in order to fool users

Multi AV Scanner detection for submitted file

Binary is likely a compiled AutoIt script file

2 othe

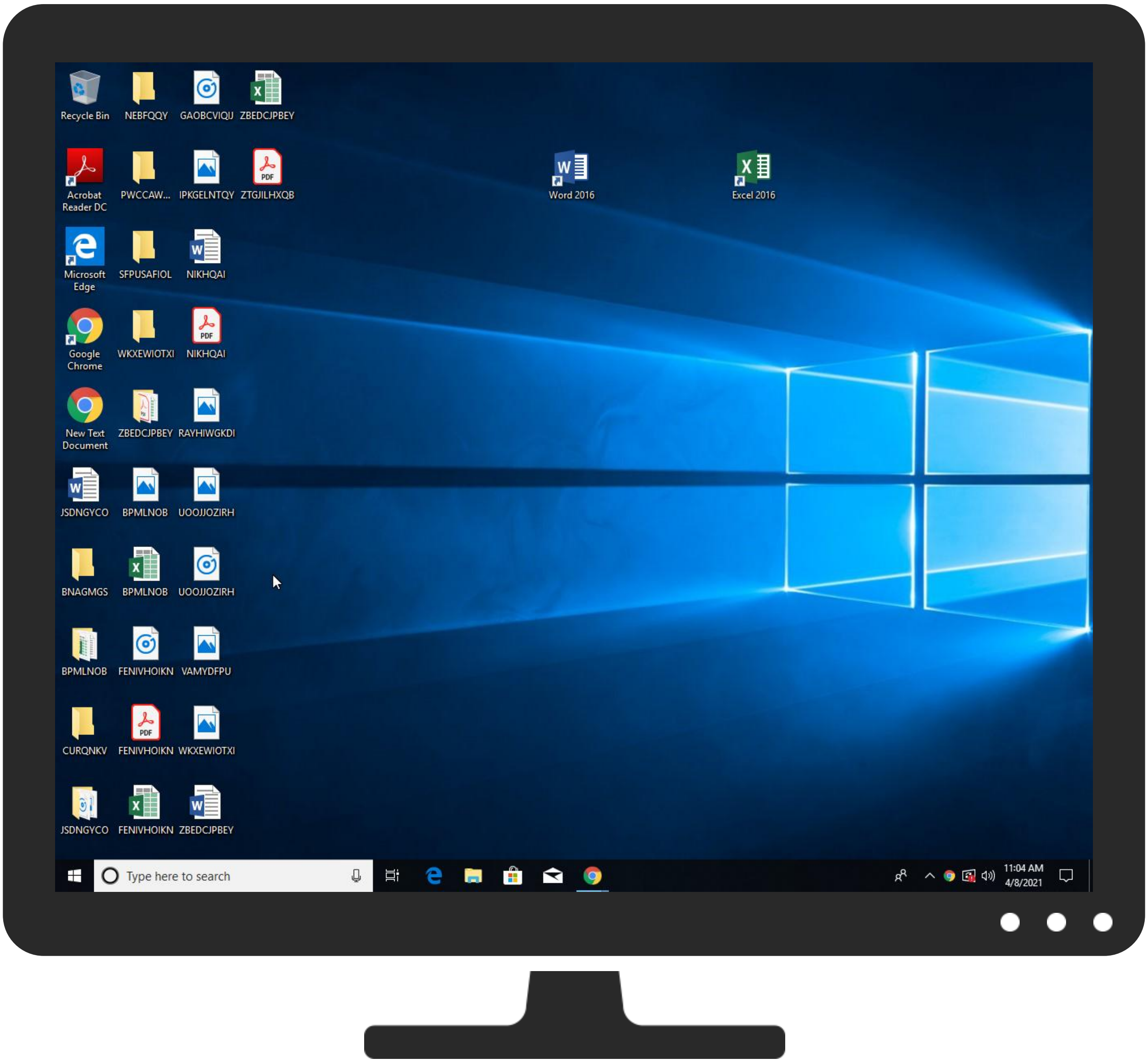
New Text Document.exe

Uses Windows timers to delay execution

Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
New Text Document.exe	14%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383850
Start date:	08.04.2021
Start time:	11:03:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	New Text Document.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	8
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.evad.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.8% (good quality ratio 0.8%) • Quality average: 83.8% • Quality standard deviation: 10.5%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.662141005544995
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	New Text Document.exe
File size:	894976
MD5:	4e79b531f4f6813cc8e21894a13c5537
SHA1:	addcb0a2aac14befcb9f8c9185e365c47a86b40c
SHA256:	9445838c51449888abaeac1c5d1953212a0205a6b4038e 6a404ca752cbda3f2f
SHA512:	aae6406f2feedfbae51433a697bbaf3d7a80570c0f86a1f5f 9e09ac2699651049fbd882d27de21ede2ffa215e28ed73d 8b3a16aca003c2213ebcfe421a581cde
SSDEEP:	24576:aAHnh+eWsN3skA4RV1Hom2KXMmHahxl5:th+ZkldoPK8YahV
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$........s..R...R ...R....C..P.....;.S..._@#.a..._@......_@..g...[j..[...[jo.w...R. ..r.............#.S..._@'.S...R.k.S.....".S...RichR..

File Icon

Icon Hash:	e8d6a08c8882c461

Static PE Info

General

Entrypoint:	0x42800a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE
Time Stamp:	0x606EC3E3 [Thu Apr 8 08:50:43 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	afcdf79be1557326c854b6e20cb900a7

Entrypoint Preview

Instruction
call 00007F0C74947E8Dh
jmp 00007F0C7493AC44h
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push edi
push esi
mov esi, dword ptr [esp+10h]
mov ecx, dword ptr [esp+14h]
mov edi, dword ptr [esp+0Ch]
mov eax, ecx
mov edx, ecx
add eax, esi
cmp edi, esi
jbe 00007F0C7493ADCAh
cmp edi, eax
jc 00007F0C7493B12Eh
bt dword ptr [004C41FCh], 01h
jnc 00007F0C7493ADC9h
rep movsb
jmp 00007F0C7493B0DCh
cmp ecx, 00000080h
jc 00007F0C7493AF94h
mov eax, edi
xor eax, esi
test eax, 0000000Fh
jne 00007F0C7493ADD0h
bt dword ptr [004BF324h], 01h
jc 00007F0C7493B2A0h
bt dword ptr [004C41FCh], 00000000h
jnc 00007F0C7493AF6Dh
test edi, 00000003h
jne 00007F0C7493AF7Eh
test esi, 00000003h

Instruction
jne 00007F0C7493AF5Dh
bt edi, 02h
jnc 00007F0C7493ADCFh
mov eax, dword ptr [esi]
sub ecx, 04h
lea esi, dword ptr [esi+04h]
mov dword ptr [edi], eax
lea edi, dword ptr [edi+04h]
bt edi, 03h
jnc 00007F0C7493ADD3h
movq xmm1, qword ptr [esi]
sub ecx, 08h
lea esi, dword ptr [esi+08h]
movq qword ptr [edi], xmm1
lea edi, dword ptr [edi+08h]
test esi, 00000007h
je 00007F0C7493AE25h
bt esi, 03h

Rich Headers

Programming Language:	• [C] VS2013 build 21005 • [C] VS2008 SP1 build 30729 • [LNK] VS2013 UPD5 build 40629 • [ASM] VS2013 UPD5 build 40629 • [C++] VS2013 build 21005 • [ASM] VS2013 build 21005 • [RES] VS2013 build 21005 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbc0cc	0x17c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc8000	0x10114	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd9000	0x7134	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x92bc0	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xa4b50	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8f000	0x884	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x8dfdd	0x8e000	False	0.573560258033	data	6.67524835171	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8f000	0x2fd8e	0x2fe00	False	0.328288185379	data	5.76324400576	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xbf000	0x8f74	0x5200	False	0.10175304878	data	1.19638192355	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xc8000	0x10114	0x10200	False	0.654236312984	data	6.89152935379	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd9000	0x7134	0x7200	False	0.761753015351	data	6.78395555713	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xc8578	0x128	GLS_BINARY_LSB_FIRST	English	Great Britain
RT_ICON	0xc86a0	0x128	GLS_BINARY_LSB_FIRST	English	Great Britain
RT_ICON	0xc87c8	0x128	GLS_BINARY_LSB_FIRST	English	Great Britain
RT_ICON	0xc88f0	0x568	GLS_BINARY_LSB_FIRST	English	Great Britain
RT_ICON	0xc8e58	0x8a8	data	English	Great Britain
RT_ICON	0xc9700	0xea8	data	English	Great Britain
RT_ICON	0xca5a8	0x468	GLS_BINARY_LSB_FIRST	English	Great Britain
RT_ICON	0xcaa10	0x10a8	data	English	Great Britain
RT_ICON	0xcbab8	0x25a8	data	English	Great Britain
RT_ICON	0xce060	0x763d	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	Great Britain
RT_MENU	0xd56a0	0x50	data	English	Great Britain
RT_STRING	0xd56f0	0x594	data	English	Great Britain
RT_STRING	0xd5c84	0x68a	data	English	Great Britain
RT_STRING	0xd6310	0x490	data	English	Great Britain
RT_STRING	0xd67a0	0x5fc	data	English	Great Britain
RT_STRING	0xd6d9c	0x65c	data	English	Great Britain
RT_STRING	0xd73f8	0x466	data	English	Great Britain
RT_STRING	0xd7860	0x158	data	English	Great Britain
RT_RCDATA	0xd79b8	0x1eb	data		
RT_GROUP_ICON	0xd7ba4	0x68	data	English	Great Britain
RT_GROUP_ICON	0xd7c0c	0x14	data	English	Great Britain
RT_GROUP_ICON	0xd7c20	0x14	data	English	Great Britain
RT_GROUP_ICON	0xd7c34	0x14	data	English	Great Britain
RT_VERSION	0xd7c48	0xdc	data	English	Great Britain
RT_MANIFEST	0xd7d24	0x3ef	ASCII text, with CRLF line terminators	English	Great Britain

Imports

DLL	Import
WSOCK32.dll	WSACleanup, socket, inet_ntoa, setsockopt, ntohs, recvfrom, ioctlsocket, htons, WSAStartup, __WSAFDIsSet, select, accept, listen, bind, closesocket, WSAGetLastError, recv, sendto, send, inet_addr, gethostbyname, gethostname, connect
VERSION.dll	GetFileVersionInfoW, GetFileVersionInfoSizeW, VerQueryValueW
WINMM.dll	timeGetTime, waveOutSetVolume, mciSendStringW
COMCTL32.dll	ImageList_ReplaceIcon, ImageList_Destroy, ImageList_Remove, ImageList_SetDragCursorImage, ImageList_BeginDrag, ImageList_DragEnter, ImageList_DragLeave, ImageList_EndDrag, ImageList_DragMove, InitCommonControlsEx, ImageList_Create
MPR.dll	WNetUseConnectionW, WNetCancelConnection2W, WNetGetConnectionW, WNetAddConnection2W
WININET.dll	InternetQueryDataAvailable, InternetCloseHandle, InternetOpenW, InternetSetOptionW, InternetCrackUrlW, HttpQueryInfoW, InternetQueryOptionW, HttpOpenRequestW, HttpSendRequestW, FtpOpenFileW, FtpGetFileSize, InternetOpenUrlW, InternetReadFile, InternetConnectW
PSAPI.DLL	GetProcessMemoryInfo
IPHLPAPI.DLL	IcmpCreateFile, IcmpCloseHandle, IcmpSendEcho
USERENV.dll	DestroyEnvironmentBlock, UnloadUserProfile, CreateEnvironmentBlock, LoadUserProfileW
UxTheme.dll	IsThemeActive

DLL	Import
KERNEL32.dll	DuplicateHandle, CreateThread, WaitForSingleObject, HeapAlloc, GetProcessHeap, HeapFree, Sleep, GetCurrentThreadId, MultiByteToWideChar, MulDiv, GetVersionExW, IsWow64Process, GetSystemInfo, FreeLibrary, LoadLibraryA, GetProcAddress, SetErrorMode, GetModuleFileNameW, WideCharToMultiByte, lstrcpyW, lstrlenW, GetModuleHandleW, QueryPerformanceCounter, VirtualFreeEx, OpenProcess, VirtualAllocEx, WriteProcessMemory, ReadProcessMemory, CreateFileW, SetFilePointerEx, SetEndOfFile, ReadFile, WriteFile, FlushFileBuffers, TerminateProcess, CreateToolhelp32Snapshot, Process32FirstW, Process32NextW, SetFileTime, GetFileAttributesW, FindFirstFileW, SetCurrentDirectoryW, GetLongPathNameW, GetShortPathNameW, DeleteFileW, FindNextFileW, CopyFileExW, MoveFileW, CreateDirectoryW, RemoveDirectoryW, SetSystemPowerState, QueryPerformanceFrequency, FindResourceW, LoadResource, LockResource, SizeofResource, EnumResourceNamesW, OutputDebugStringW, GetTempPathW, GetTempFileNameW, DeviceIoControl, GetLocalTime, CompareStringW, GetCurrentProcess, EnterCriticalSection, LeaveCriticalSection, GetStdHandle, CreatePipe, InterlockedExchange, TerminateThread, LoadLibraryExW, FindResourceExW, CopyFileW, VirtualFree, FormatMessageW, GetExitCodeProcess, GetPrivateProfileStringW, WritePrivateProfileStringW, GetPrivateProfileSectionW, WritePrivateProfileSectionW, GetPrivateProfileSectionNamesW, FileTimeToLocalFileTime, FileTimeToSystemTime, SystemTimeToFileTime, LocalFileTimeToFileTime, GetDriveTypeW, GetDiskFreeSpaceExW, GetDiskFreeSpaceW, GetVolumeInformationW, SetVolumeLabelW, CreateHardLinkW, SetFileAttributesW, CreateEventW, SetEvent, GetEnvironmentVariableW, SetEnvironmentVariableW, GlobalLock, GlobalUnlock, GlobalAlloc, GetFileSize, GlobalFree, GlobalMemoryStatusEx, Beep, GetSystemDirectoryW, HeapReAlloc, HeapSize, GetComputerNameW, GetWindowsDirectoryW, GetCurrentProcessId, GetProcessIoCounters, CreateProcessW, GetProcessId, SetPriorityClass, LoadLibraryW, VirtualAlloc, IsDebuggerPresent, GetCurrentDirectoryW, lstrcmpiW, DecodePointer, GetLastError, RaiseException, InitializeCriticalSectionAndSpinCount, DeleteCriticalSection, InterlockedDecrement, InterlockedIncrement, GetCurrentThread, CloseHandle, GetFullPathNameW, EncodePointer, ExitProcess, GetModuleHandleExW, ExitThread, GetSystemTimeAsFileTime, ResumeThread, GetCommandLineW, IsProcessorFeaturePresent, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, SetLastError, UnhandledExceptionFilter, SetUnhandledExceptionFilter, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, GetStartupInfoW, GetStringTypeW, SetStdHandle, GetFileType, GetConsoleCP, GetConsoleMode, RtlUnwind, ReadConsoleW, GetTimeZoneInformation, GetDateFormatW, GetTimeFormatW, LCMapStringW, GetEnvironmentStringsW, FreeEnvironmentStringsW, WriteConsoleW, FindClose, SetEnvironmentVariableA
USER32.dll	AdjustWindowRectEx, CopyImage, SetWindowPos, GetCursorInfo, RegisterHotKey, ClientToScreen, GetKeyboardLayoutNameW, IsCharAlphaW, IsCharAlphaNumericW, IsCharLowerW, IsCharUpperW, GetMenuStringW, GetSubMenu, GetCaretPos, IsZoomed, MonitorFromPoint, GetMonitorInfoW, SetWindowLongW, SetLayeredWindowAttributes, FlashWindow, GetClassLongW, TranslateAcceleratorW, IsDialogMessageW, GetSysColor, InflateRect, DrawFocusRect, DrawTextW, FrameRect, DrawFrameControl, FillRect, PtInRect, DestroyAcceleratorTable, CreateAcceleratorTableW, SetCursor, GetWindowDC, GetSystemMetrics, GetActiveWindow, CharNextW, wsprintfW, RedrawWindow, DrawMenuBar, DestroyMenu, SetMenu, GetWindowTextLengthW, CreateMenu, IsDlgButtonChecked, DefDlgProcW, CallWindowProcW, ReleaseCapture, SetCapture, CreateIconFromResourceEx, mouse_event, ExitWindowsEx, SetActiveWindow, FindWindowExW, EnumThreadWindows, SetMenuDefaultItem, InsertMenuItemW, IsMenu, TrackPopupMenuEx, GetCursorPos, DeleteMenu, SetRect, GetMenuItemID, GetMenuItemCount, SetMenuItemInfoW, GetMenuItemInfoW, SetForegroundWindow, IsIconic, FindWindowW, MonitorFromRect, keybd_event, SendInput, GetAsyncKeyState, SetKeyboardState, GetKeyboardState, GetKeyState, VkKeyScanW, LoadStringW, DialogBoxParamW, MessageBeep, EndDialog, SendDlgItemMessageW, GetDlgItem, SetWindowTextW, CopyRect, ReleaseDC, GetDC, EndPaint, BeginPaint, GetClientRect, GetMenu, DestroyWindow, EnumWindows, GetDesktopWindow, IsWindow, IsWindowEnabled, IsWindowVisible, EnableWindow, InvalidateRect, GetWindowLongW, GetWindowThreadProcessId, AttachThreadInput, GetFocus, GetWindowTextW, ScreenToClient, SendMessageTimeoutW, EnumChildWindows, CharUpperBuffW, GetParent, GetDlgCtrlID, SendMessageW, MapVirtualKeyW, PostMessageW, GetWindowRect, SetUserObjectSecurity, CloseDesktop, CloseWindowStation, OpenDesktopW, SetProcessWindowStation, GetProcessWindowStation, OpenWindowStationW, GetUserObjectSecurity, MessageBoxW, DefWindowProcW, SetClipboardData, EmptyClipboard, CountClipboardFormats, CloseClipboard, GetClipboardData, IsClipboardFormatAvailable, OpenClipboard, BlockInput, GetMessageW, LockWindowUpdate, DispatchMessageW, TranslateMessage, PeekMessageW, UnregisterHotKey, CheckMenuRadioItem, CharLowerBuffW, MoveWindow, SetFocus, PostQuitMessage, KillTimer, CreatePopupMenu, RegisterWindowMessageW, SetTimer, ShowWindow, CreateWindowExW, RegisterClassExW, LoadIconW, LoadCursorW, GetSysColorBrush, GetForegroundWindow, MessageBoxA, DestroyIcon, SystemParametersInfoW, LoadImageW, GetClassNameW
GDI32.dll	StrokePath, DeleteObject, GetTextExtentPoint32W, ExtCreatePen, GetDeviceCaps, EndPath, SetPixel, CloseFigure, CreateCompatibleBitmap, CreateCompatibleDC, SelectObject, StretchBlt, GetDIBits, LineTo, AngleArc, MoveToEx, Ellipse, DeleteDC, GetPixel, CreateDCW, GetStockObject, GetTextFaceW, CreateFontW, SetTextColor, PolyDraw, BeginPath, Rectangle, SetViewportOrgEx, GetObjectW, SetBkMode, RoundRect, SetBkColor, CreatePen, CreateSolidBrush, StrokeAndFillPath
COMDLG32.dll	GetOpenFileNameW, GetSaveFileNameW
ADVAPI32.dll	GetAce, RegEnumValueW, RegDeleteValueW, RegDeleteKeyW, RegEnumKeyExW, RegSetValueExW, RegOpenKeyExW, RegCloseKey, RegQueryValueExW, RegConnectRegistryW, InitializeSecurityDescriptor, InitializeAcl, AdjustTokenPrivileges, OpenThreadToken, OpenProcessToken, LookupPrivilegeValueW, DuplicateTokenEx, CreateProcessAsUserW, CreateProcessWithLogonW, GetLengthSid, CopySid, LogonUserW, AllocateAndInitializeSid, CheckTokenMembership, RegCreateKeyExW, FreeSid, GetTokenInformation, GetSecurityDescriptorDacl, GetAclInformation, AddAce, SetSecurityDescriptorDacl, GetUserNameW, InitiateSystemShutdownExW
SHELL32.dll	DragQueryPoint, ShellExecuteExW, DragQueryFileW, SHEmptyRecycleBinW, SHGetPathFromIDListW, SHBrowseForFolderW, SHCreateShellItem, SHGetDesktopFolder, SHGetSpecialFolderLocation, SHGetFolderPathW, SHFileOperationW, ExtractIconExW, Shell_NotifyIconW, ShellExecuteW, DragFinish
ole32.dll	CoTaskMemAlloc, CoTaskMemFree, CLSIDFromString, ProgIDFromCLSID, CLSIDFromProgID, OleSetMenuDescriptor, MkParseDisplayName, OleSetContainedObject, CoCreateInstance, IIDFromString, StringFromGUID2, CreateStreamOnHGlobal, OleInitialize, OleUninitialize, CoInitialize, CoUninitialize, GetRunningObjectTable, CoGetInstanceFromFile, CoGetObject, CoSetProxyBlanket, CoCreateInstanceEx, CoInitializeSecurity
OLEAUT32.dll	LoadTypeLibEx, VariantCopyInd, SysReAllocString, SysFreeString, SafeArrayDestroyDescriptor, SafeArrayDestroyData, SafeArrayUnaccessData, SafeArrayAccessData, SafeArrayAllocData, SafeArrayAllocDescriptorEx, SafeArrayCreateVector, RegisterTypeLib, CreateStdDispatch, DispCallFunc, VariantChangeType, SysStringLen, VariantTimeToSystemTime, VarR8FromDec, SafeArrayGetVartype, VariantCopy, VariantClear, OleLoadPicture, QueryPathOfRegTypeLib, RegisterTypeLibForUser, UnRegisterTypeLibForUser, UnRegisterTypeLib, CreateDispTypeInfo, SysAllocString, VariantInit

Version Infos

Description	Data
Translation	0x0809 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	Great Britain	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: New Text Document.exe PID: 6780 Parent PID: 5956

General

Start time:	11:04:19
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\New Text Document.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\New Text Document.exe'
Imagebase:	0x12d0000
File size:	894976 bytes
MD5 hash:	4E79B531F4F6813CC8E21894A13C5537
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis