ID: 1436386
Sample Name: app.exe
Cookbook: default.jbs
Time: 00:18:08
Date: 05/05/2024
Version: 40.0.0 Tourmaline

Table of Contents

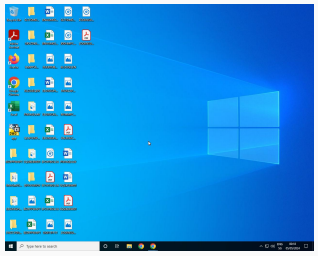
Windows Analysis Report

app.exe

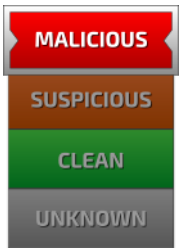
Overview

General Information

Sample name:	app.exe
Analysis ID:	1436386
MD5:	75b9ef9142a78..
SHA1:	0461f1c46644a..
SHA256:	e9bc44cf548a7..
Tags:	185213208245 exe
Infos:	



Detection

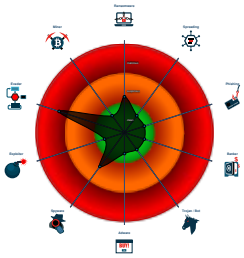


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Contains functionality to infect the b…
- Machine Learning detection for sam…
- PE file contains section with specia…
- PE file has a writeable .text section
- Queries memory information (via WM…
- Tries to detect sandboxes and other…
- Contains functionality for execution …
- Contains functionality to call native …
- Contains functionality to check if a d…
- Contains functionality to check if a w…
- Contains functionality to communica…

Classification



Process Tree

- **System is w10x64**
- app.exe (PID: 5348 cmdline: "C:\Users\user\Desktop\app.exe" MD5: 75B9EF9142A78671D449C8D22AB6BE14)
  - conhost.exe (PID: 6568 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary

PE file contains section with special chars

PE file has a writeable .text section

Persistence and Installation Behavior

Contains functionality to infect the boot sector

Boot Survival

Contains functionality to infect the boot sector

Malware Analysis System Evasion

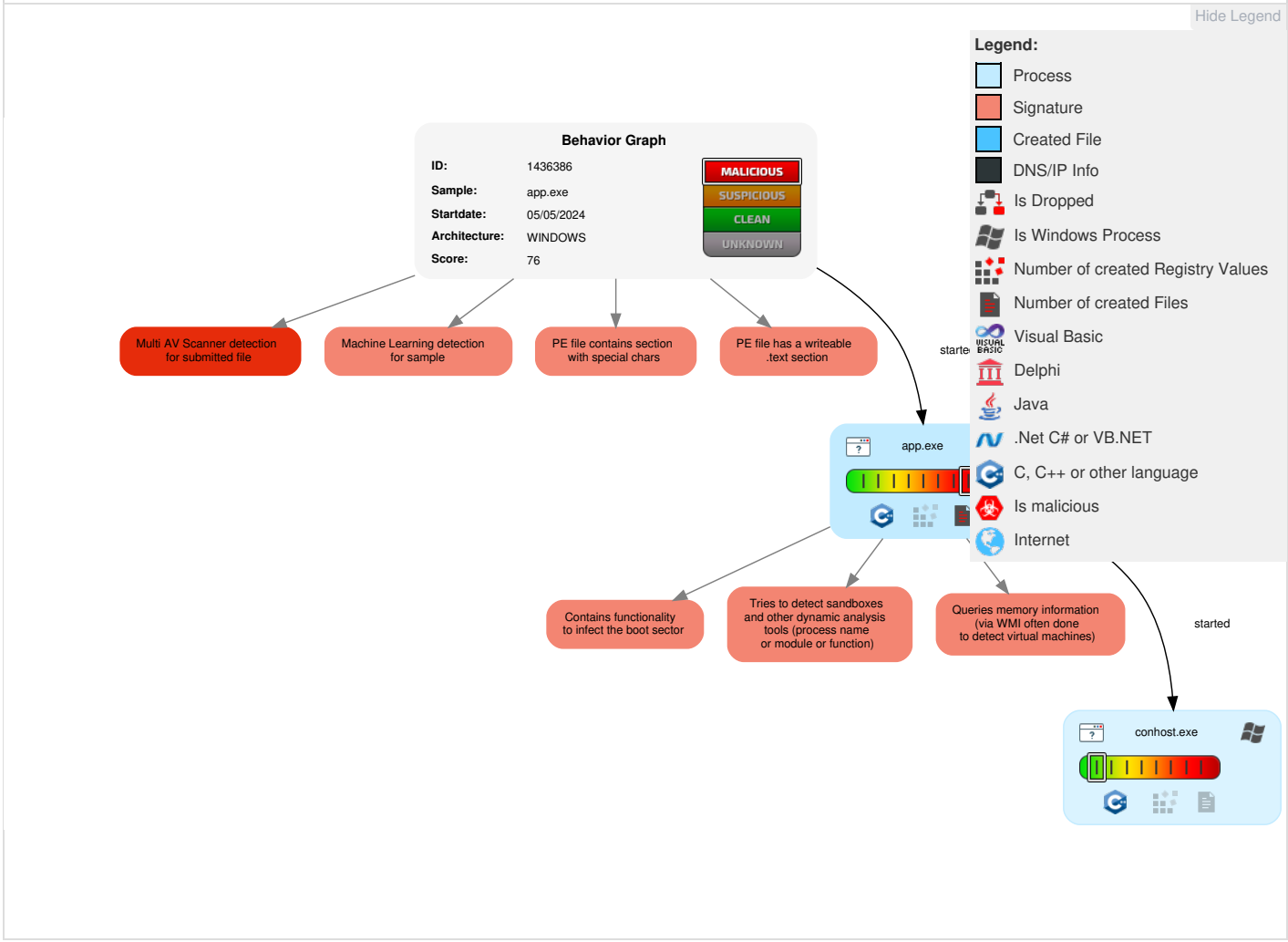
Queries memory information (via WMI often done to detect virtual machines)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Mitre Att&ck Matrix

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	2 1 Windows Management Instrumentation	1 Bootkit	1 Process Injection	1 Disable or Modify Tools	1 Input Capture	1 System Time Discovery	Remote Services	1 Input Capture	2 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	1 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 Process Injection	LSASS Memory	3 3 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Junk Data	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	1 Deobfuscate/Decode Files or Information	Security Account Manager	1 Application Window Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Steganography	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	2 Obfuscated Files or Information	NTDS	1 System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Protocol Impersonation	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 Bootkit	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 DLL Side-Loading	Cached Domain Credentials	2 5 System Information Discovery	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop

Behavior Graph



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
app.exe	11%	ReversingLabs		
app.exe	11%	Virustotal		Browse
app.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://POSTHTTP/1.1Content-Type:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://POSTHTTP/1.1Content-Type:	app.exe, 00000000.00000002.2022098881.00000000002300000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1436386
Start date and time:	2024-05-05 00:18:08 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 2m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	3
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	app.exe
Detection:	MAL
Classification:	mal76.evad.winEXE@2/0@0/0
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing disassembly code.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

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 (console) Intel 80386, for MS Windows
Entropy (8bit):	7.441704402192102
TrID:	• Win32 Executable (generic) a (10002005/4) 99.83% • Windows Screen Saver (13104/52) 0.13% • 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:	app.exe
File size:	1'290'240 bytes
MD5:	75b9ef9142a78671d449c8d22ab6be14
SHA1:	0461f1c46644acde8020bb59b53b1e34b65977ca
SHA256:	e9bc44cf548a70e7285499209973faf44b7374dece1413dfcdc03bf25a6c599c
SHA512:	14ef889f580c02e319b6d9d899ddbd1bd523c1d8b493eab8b98da6d3d276d76efb9b5694759df7d68bb9d002a8ace8fc82d22121a7b4ea236d5f9cef38cc809c
SSDEEP:	24576:CIFxe+AY3rqYsavMOQdbac5IQH97wiI3dzAr09UDZ5YUD8:1xeSNR0vbac5/d8P3diDZ6q
TLSH:	8255CF05F3D2B8B1D15192772DC96161B6ED993048D83F0732D0EE5E1B3B9A6B40FE2A
File Content Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....P(..>{..>{..>{?.c{..>{v..{..>{...{..>{f."{..>{e."{..>{F.'{..>{..?{..>{F.~{..>{F."{&.>{...{..>{..5{..>{..^{..>{F.#{..>{F.{{..>

File Icon

Icon Hash:	0f4ecda7ae5d1715

Static PE Info

General

Entrypoint:	0x415dde
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	
Time Stamp:	0x500F9507 [Wed Jul 25 06:41:11 2012 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	26600adf486f72b556f917a64c8fd23f

Entrypoint Preview

Instruction
push 00000060h
push 0043A478h
call 00007FD5D0B6F503h
mov edi, 00000094h
mov eax, edi
call 00007FD5D0B6DA5Fh
mov dword ptr [ebp-18h], esp
mov esi, esp
mov dword ptr [esi], edi
push esi
call dword ptr [0042F2B4h]
mov ecx, dword ptr [esi+10h]
mov dword ptr [0044B190h], ecx
mov eax, dword ptr [esi+04h]
mov dword ptr [0044B19Ch], eax
mov edx, dword ptr [esi+08h]
mov dword ptr [0044B1A0h], edx
mov esi, dword ptr [esi+0Ch]
and esi, 00007FFFh
mov dword ptr [0044B194h], esi
cmp ecx, 02h
je 00007FD5D0B6E3FEh
or esi, 00008000h
mov dword ptr [0044B194h], esi
shl eax, 08h
add eax, edx
mov dword ptr [0044B198h], eax
xor esi, esi
push esi
mov edi, dword ptr [0042F20Ch]
call edi
cmp word ptr [eax], 5A4Dh
jne 00007FD5D0B6E411h
mov ecx, dword ptr [eax+3Ch]
add ecx, eax

Instruction
cmp dword ptr [ecx], 00004550h
jne 00007FD5D0B6E404h
movzx eax, word ptr [ecx+18h]
cmp eax, 0000010Bh
je 00007FD5D0B6E411h
cmp eax, 0000020Bh
je 00007FD5D0B6E3F7h
mov dword ptr [ebp-1Ch], esi
jmp 00007FD5D0B6E419h
cmp dword ptr [ecx+00000084h], 0Eh
jbe 00007FD5D0B6E3E4h
xor eax, eax
cmp dword ptr [ecx+000000F8h], esi
jmp 00007FD5D0B6E400h
cmp dword ptr [ecx+74h], 0Eh
jbe 00007FD5D0B6E3D4h
xor eax, eax
cmp dword ptr [ecx+000000E8h], esi
setne al
mov dword ptr [ebp-1Ch], eax

Rich Headers

Programming Language:	• [ASM] VS2002 (.NET) build 9466 • [C] VS2002 (.NET) build 9466 • [C++] VS2003 (.NET) build 3077 • [C++] VS2002 (.NET) build 9466 • [RES] VS2002 (.NET) build 9466 • [LNK] VS2002 (.NET) build 9466

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3f924	0x118	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4d000	0x2f5f0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2f000	0x594	.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	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2db32	0x2e000	7868e2f41e5b3ab908ac5a72a66f5953	False	0.6095076851222826	data	6.670624963209676	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0x2f000	0x126c6	0x13000	efd458d4cde7206fd4c5482997a30ba9	False	0.4482421875	data	5.736665908168061	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x42000	0xa9f4	0x4000	07b79e131c84ddfb0842641915843ec1	False	0.4459228515625	data	5.072911159589167	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x4d000	0x2f5f0	0x30000	2686df77c23e2ca3144ababd1a5e1501	False	0.2823994954427083	data	4.484521144858898	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
)m&	0x7d000	0xc5000	0xc5000	acab40631ef6f655b384348be6aac2b9	False	0.841724996034264	data	7.775469163423906	IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
JPG	0x4f2b0	0x2b1e6	PC bitmap, Windows 3.x format, 635 x 276 x 8, cbSize 176614, bits offset 1078	Chinese	China	0.27774128891254374
RT_CURSOR	0x7a498	0x134	Targa image data - RGB 64 x 65536 x 1 +32 "\001"	Chinese	China	0.4805194805194805
RT_CURSOR	0x7a5d0	0xb4	Targa image data - Map 32 x 65536 x 1 +16 "\001"	Chinese	China	0.7
RT_CURSOR	0x7a6b0	0x134	AmigaOS bitmap font "(", fc_YSize 4294967264, 5120 elements, 2nd "\377\360?\377\377\370\177\377\377\374\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377\377", 3rd	Chinese	China	0.36363636363636365
RT_CURSOR	0x7a800	0x134	Targa image data - RLE 64 x 65536 x 1 +32 "\001"	Chinese	China	0.35714285714285715
RT_CURSOR	0x7a950	0x134	data	Chinese	China	0.37337662337662336
RT_CURSOR	0x7aaa0	0x134	data	Chinese	China	0.37662337662337664
RT_CURSOR	0x7abf0	0x134	Targa image data 64 x 65536 x 1 +32 "\001"	Chinese	China	0.36688311688311687
RT_CURSOR	0x7ad40	0x134	Targa image data 64 x 65536 x 1 +32 "\001"	Chinese	China	0.37662337662337664
RT_CURSOR	0x7ae90	0x134	Targa image data - Mono - RLE 64 x 65536 x 1 +32 "\001"	Chinese	China	0.36688311688311687
RT_CURSOR	0x7afe0	0x134	Targa image data - RGB - RLE 64 x 65536 x 1 +32 "\001"	Chinese	China	0.38636363636363635
RT_CURSOR	0x7b130	0x134	data	Chinese	China	0.44155844155844154
RT_CURSOR	0x7b280	0x134	data	Chinese	China	0.4155844155844156
RT_CURSOR	0x7b3d0	0x134	AmigaOS bitmap font "(", fc_YSize 4294966847, 3840 elements, 2nd "\377?\374\377\377\300\003\377\377\300\003\377\377\340\007\377\377\360\017\377\377\370\037\377\377\374?\377\377\376\177\377\377\377\377\377\377\377\377\377\377\377\377\377", 3rd	Chinese	China	0.5422077922077922
RT_CURSOR	0x7b520	0x134	data	Chinese	China	0.2662337662337662
RT_CURSOR	0x7b670	0x134	data	Chinese	China	0.2824675324675325
RT_CURSOR	0x7b7c0	0x134	data	Chinese	China	0.3246753246753247
RT_BITMAP	0x7b9f8	0xb8	Device independent bitmap graphic, 12 x 10 x 4, image size 80	Chinese	China	0.44565217391304346
RT_BITMAP	0x7bab0	0x144	Device independent bitmap graphic, 33 x 11 x 4, image size 220	Chinese	China	0.37962962962962965
RT_ICON	0x4db70	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Chinese	China	0.6042418772563177
RT_ICON	0x4e430	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Chinese	China	0.6042418772563177
RT_DIALOG	0x4ecf0	0x23e	data	Chinese	China	0.5174216027874564
RT_DIALOG	0x4ef30	0x94	data	Chinese	China	0.6959459459459459
RT_DIALOG	0x7b910	0xe2	data	Chinese	China	0.6637168141592921
RT_STRING	0x7bbf8	0x46	data	Chinese	China	0.6857142857142857
RT_STRING	0x7bc40	0x54	data	Chinese	China	0.8571428571428571
RT_STRING	0x7bc98	0x2c	data	Chinese	China	0.5909090909090909
RT_STRING	0x7bcc8	0x74	data	Chinese	China	0.8448275862068966
RT_STRING	0x7bd40	0x1d0	data	Chinese	China	0.8060344827586207
RT_STRING	0x7c088	0x164	data	Chinese	China	0.48314606741573035

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_STRING	0x7bf50	0x132	data	Chinese	China	0.6405228758169934
RT_STRING	0x7c570	0x50	data	Chinese	China	0.725
RT_STRING	0x7bf10	0x40	data	Chinese	China	0.65625
RT_STRING	0x7c4d8	0x6a	data	Chinese	China	0.7452830188679245
RT_STRING	0x7c1f0	0x1d6	data	Chinese	China	0.6723404255319149
RT_STRING	0x7c3c8	0x110	data	Chinese	China	0.625
RT_STRING	0x7c548	0x24	data	Chinese	China	0.4444444444444444
RT_STRING	0x7c5c0	0x30	data	Chinese	China	0.625
RT_GROUP_CURSOR	0x7a688	0x22	Lotus unknown worksheet or configuration, revision 0x2	Chinese	China	1.0294117647058822
RT_GROUP_CURSOR	0x7ae78	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_CURSOR	0x7a7e8	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_CURSOR	0x7ad28	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_CURSOR	0x7abd8	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_CURSOR	0x7b508	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_CURSOR	0x7aa88	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_CURSOR	0x7b118	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_CURSOR	0x7a938	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_CURSOR	0x7afc8	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_CURSOR	0x7b268	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_CURSOR	0x7b3b8	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_CURSOR	0x7b658	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_CURSOR	0x7b7a8	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_CURSOR	0x7b8f8	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China	1.3
RT_GROUP_ICON	0x4e418	0x14	data	Chinese	China	1.15
RT_GROUP_ICON	0x4ecd8	0x14	data	Chinese	China	1.25
RT_VERSION	0x4efc8	0x2e8	data	Chinese	China	0.5631720430107527

Imports

DLL	Import
KERNEL32.dll	LockFile, UnlockFile, SetEndOfFile, DuplicateHandle, FindClose, FindFirstFileA, GetFullPathNameA, GetCPInfo, GetOEMCP, FileTimeToSystemTime, SetErrorMode, FileTimeToLocalFileTime, GetFileAttributesA, GetFileTime, GetTickCount, HeapAlloc, HeapFree, RtlUnwind, GetStartupInfoA, GetCommandLineA, RaiseException, GetSystemTimeAsFileTime, ExitProcess, TerminateProcess, HeapReAlloc, HeapSize, FlushFileBuffers, HeapCreate, VirtualFree, VirtualAlloc, IsBadWritePtr, GetStdHandle, UnhandledExceptionFilter, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, SetHandleCount, GetFileType, SetUnhandledExceptionFilter, GetStringTypeA, GetStringTypeW, GetCurrentProcessId, LCMapStringA, LCMapStringW, GetTimeZoneInformation, IsBadReadPtr, IsBadCodePtr, VirtualProtect, GetSystemInfo, VirtualQuery, SetStdHandle, SetEnvironmentVariableA, SetFilePointer, GlobalFlags, WritePrivateProfileStringA, TlsFree, DeleteCriticalSection, LocalReAlloc, TlsSetValue, TlsAlloc, InitializeCriticalSection, TlsGetValue, EnterCriticalSection, GlobalHandle, GlobalReAlloc, LeaveCriticalSection, LocalAlloc, GlobalGetAtomNameA, GlobalFindAtomA, lstrcatA, lstrcmpW, GlobalAddAtomA, GetCurrentThread, GetCurrentThreadId, GlobalDeleteAtom, lstrcmpA, ConvertDefaultLocale, EnumResourceLanguagesA, lstrcpyA, SetLastError, GlobalFree, MulDiv, GlobalAlloc, GlobalLock, GlobalUnlock, GetModuleHandleA, GetProcAddress, FormatMessageA, LocalFree, CopyFileA, GetCurrentDirectoryA, FreeResource, OpenFile, GetCurrentProcess, SetPriorityClass, lstrcpynA, DeviceIoControl, ReadFile, GetFileSize, GetLastError, QueryPerformanceCounter, QueryPerformanceFrequency, GetSystemDirectoryA, CreateFileA, WriteFile, CloseHandle, DeleteFileA, GetModuleFileNameA, LoadLibraryA, FreeLibrary, GetVolumeInformationA, OutputDebugStringA, DebugBreak, InterlockedIncrement, InterlockedDecrement, FindResourceA, LoadResource, LockResource, SizeofResource, lstrlenA, lstrcmpiA, CompareStringW, lstrlenW, CompareStringA, GetVersion, WideCharToMultiByte, MultiByteToWideChar, GetVersionExA, GetThreadLocale, GetLocaleInfoA, GetACP, HeapDestroy, InterlockedExchange

DLL	Import
USER32.dll	InvalidateRgn, SetCapture, ReleaseCapture, GetNextDlgGroupItem, MessageBeep, RegisterClipboardFormatA, PostThreadMessageA, GetForegroundWindow, GetTopWindow, UnhookWindowsHookEx, GetMessagePos, MapWindowPoints, SetForegroundWindow, UpdateWindow, GetMenu, GetSysColor, AdjustWindowRectEx, EqualRect, GetClassInfoA, RegisterClassA, UnregisterClassA, GetDlgCtrlID, DefWindowProcA, CallWindowProcA, SetWindowLongA, OffsetRect, IntersectRect, SystemParametersInfoA, GetWindowPlacement, GetWindowRect, CopyRect, PtInRect, GetWindow, SetWindowContextHelpId, MapDialogRect, SetWindowPos, GetDesktopWindow, SetActiveWindow, EndPaint, DestroyWindow, IsWindow, InvalidateRect, GetNextDlgTabItem, EndDialog, SetMenuItemBitmaps, GetFocus, ModifyMenuA, EnableMenuItem, CheckMenuItem, GetMenuCheckMarkDimensions, LoadBitmapA, SetWindowsHookExA, CallNextHookEx, GetMessageA, TranslateMessage, DispatchMessageA, GetActiveWindow, IsWindowVisible, GetKeyState, PeekMessageA, GetCursorPos, ValidateRect, GetParent, GetWindowLongA, GetLastActivePopup, IsWindowEnabled, SetCursor, PostMessageA, PostQuitMessage, wsprintfA, GetMenuState, GetMenuItemID, GetMenuItemCount, CharLowerA, CharUpperA, BeginPaint, GetWindowDC, ReleaseDC, GetDC, ClientToScreen, GetSubMenu, MessageBoxA, CharNextA, wvsprintfA, GetSystemMetrics, LoadIconA, EnableWindow, GetClientRect, IsIconic, GetSystemMenu, SendMessageA, AppendMenuA, CopyAcceleratorTableA, SetRect, IsRectEmpty, DrawIcon, LoadCursorA, GetDlgItem, GetSysColorBrush, GrayStringA, DrawTextExA, DrawTextA, TabbedTextOutA, DestroyMenu, ShowWindow, MoveWindow, SetWindowTextA, IsDialogMessageA, RegisterWindowMessageA, WinHelpA, GetCapture, CreateWindowExA, GetClassLongA, GetClassInfoExA, GetClassNameA, SetPropA, GetPropA, RemovePropA, SendDlgItemMessageA, SetFocus, IsChild, GetWindowTextLengthA, CreateDialogIndirectParamA, GetWindowTextA, GetMessageTime
GDI32.dll	SetMapMode, DeleteObject, GetViewportExtEx, GetWindowExtEx, PtVisible, RectVisible, TextOutA, Escape, SelectObject, SetViewportOrgEx, OffsetViewportOrgEx, SetViewportExtEx, ScaleViewportExtEx, SetWindowExtEx, ScaleWindowExtEx, ExtSelectClipRgn, DeleteDC, GetStockObject, GetBkColor, GetTextColor, CreateRectRgnIndirect, GetRgnBox, GetMapMode, RestoreDC, SaveDC, ExtTextOutA, GetObjectA, SetBkColor, SetTextColor, GetClipBox, CreateBitmap, GetDeviceCaps
comdlg32.dll	GetFileTitleA
WINSPOOL.DRV	ClosePrinter, DocumentPropertiesA, OpenPrinterA
ADVAPI32.dll	RegEnumKeyA, RegSetValueExA, RegCreateKeyExA, RegQueryValueA, RegCloseKey, RegDeleteKeyA, RegOpenKeyExA, RegQueryValueExA, RegOpenKeyA
COMCTL32.dll	
SHLWAPI.dll	PathFindExtensionA, PathFindFileNameA, PathStripToRootA, PathIsUNCA
oledlg.dll	
ole32.dll	CreateILockBytesOnHGlobal, StgCreateDocfileOnILockBytes, StgOpenStorageOnILockBytes, CoGetClassObject, CLSIDFromString, CLSIDFromProgID, CoTaskMemAlloc, OleInitialize, OleUninitialize, CoTaskMemFree, CoCreateInstance, CoSetProxyBlanket, CoInitialize, CoUninitialize, CoRevokeClassObject, OleIsCurrentClipboard, OleFlushClipboard, CoFreeUnusedLibraries, CoRegisterMessageFilter
OLEAUT32.dll	VariantInit, SysAllocStringLen, VariantClear, VariantChangeType, SysStringLen, SysAllocStringByteLen, OleCreateFontIndirect, SystemTimeToVariantTime, SafeArrayDestroy, VariantCopy, SysAllocString, SysFreeString
iphlpapi.dll	GetAdaptersInfo
OLEACC.dll	LresultFromObject, CreateStdAccessibleObject

Possible Origin

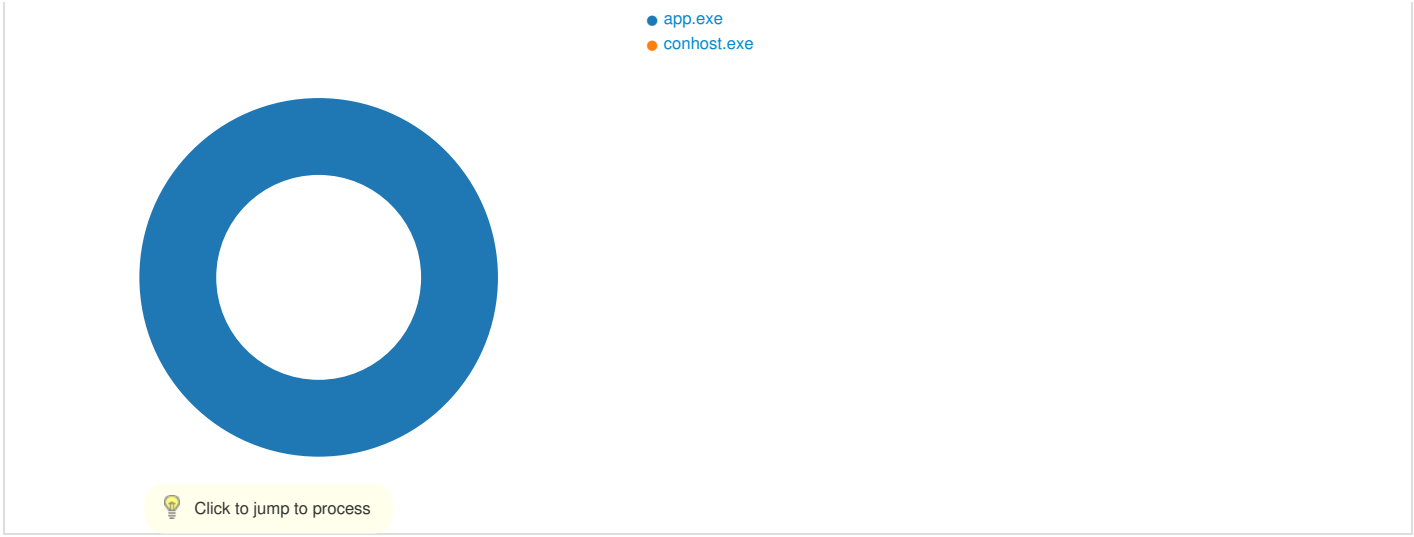
Language of compilation system	Country where language is spoken	Map
Chinese	China	

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: app.exe PID: 5348, Parent PID: 1028

General	
Target ID:	0
Start time:	00:18:52
Start date:	05/05/2024
Path:	C:\Users\user\Desktop\app.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\app.exe"
Imagebase:	0x400000
File size:	1'290'240 bytes
MD5 hash:	75B9EF9142A78671D449C8D22AB6BE14
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

File Activities

Analysis Process: conhost.exe PID: 6568, Parent PID: 5348

General	
Target ID:	1
Start time:	00:18:52
Start date:	05/05/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6d64d0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly