ID: 626617
Sample Name: dinhVFAbgo
Cookbook: default.jbs
Time: 16:17:10
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

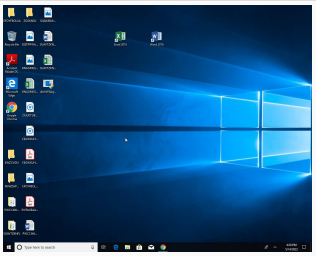
Windows Analysis Report

dinhVFAbgo

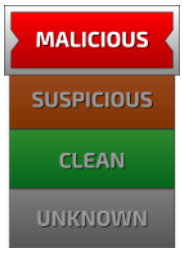
Overview

General Information

Sample Name:	dinhVFAbgo (renamed file extension from none to exe)
Analysis ID:	626617
MD5:	de3eafb5fa64237.
SHA1:	bbb3d8d70e1416.
SHA256:	93d2edbc498f6f8..
Tags:	32 exe
Infos:	



Detection

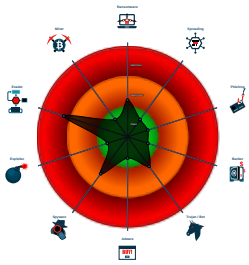


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Found evasive API chain (may stop…
- Tries to detect sandboxes and other…
- Uses 32bit PE files
- Found decision node followed by no…
- Contains functionality to check if a d…
- Contains functionality to query local…
- Uses code obfuscation techniques (…
- Tries to connect to HTTP servers, b…
- Detected potential crypto function
- Contains functionality to create guar…
- Found potential string decryption / a…

Classification



Process Tree

- **System is w10x64**
- dinhVFAbgo.exe (PID: 6440 cmdline: "C:\Users\user\Desktop\dinhVFAbgo.exe" MD5: DE3EAFB5FA64237CB2D54949C432F19C)
  - cmd.exe (PID: 6460 cmdline: C:\Windows\system32\cmd.exe /c md C:\DownLoad-Helper MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6472 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **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

Malware Analysis System Evasion

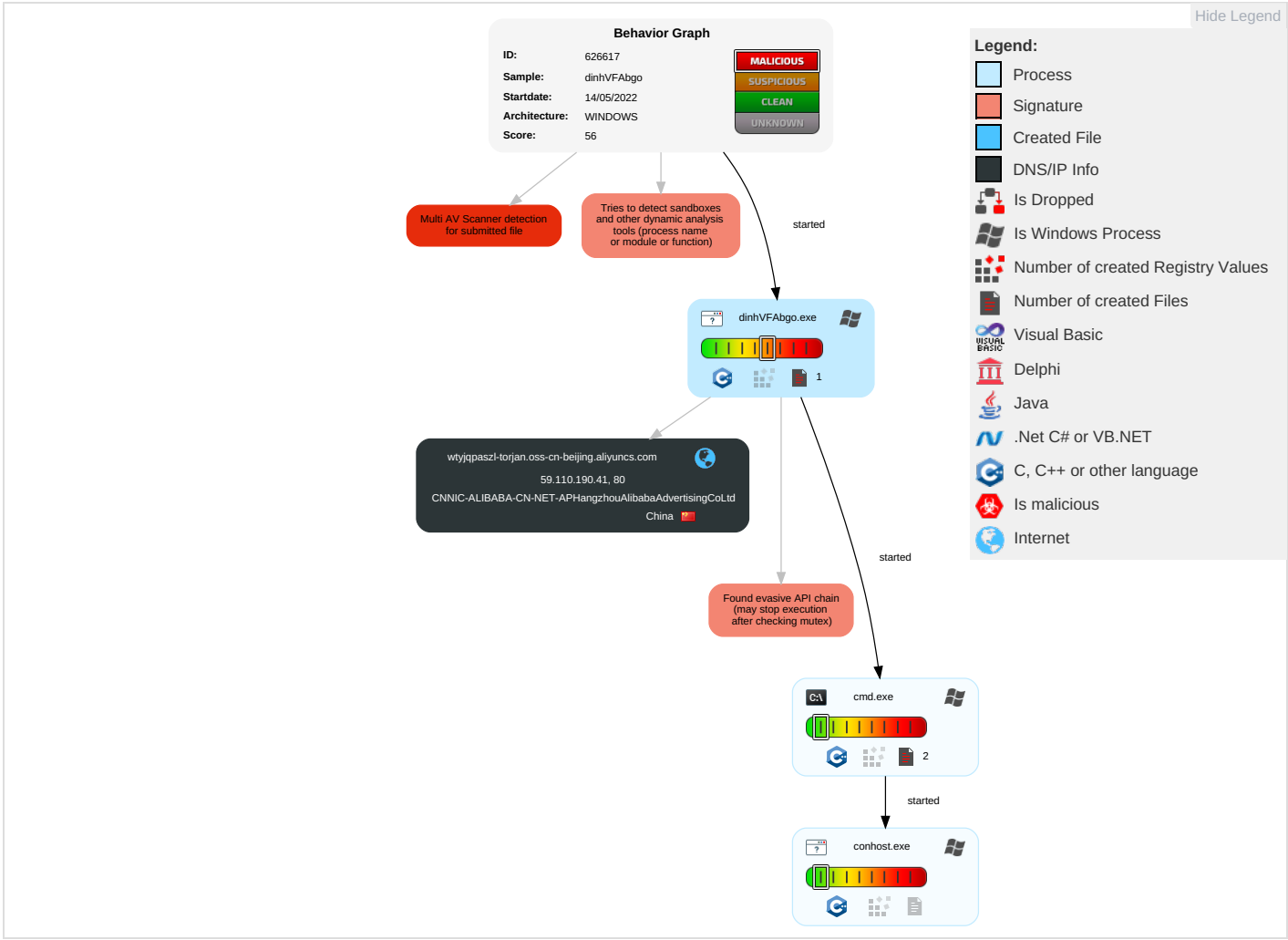
Found evasive API chain (may stop execution after checking mutex)

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Command and Scripting Interpreter	1 2 Windows Service	1 2 Windows Service	1 Disable or Modify Tools	2 1 Input Capture	1 System Time Discovery	Remote Services	2 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 2 Service Execution	Boot or Logon Initialization Scripts	1 1 Process Injection	1 1 Process Injection	LSASS Memory	1 3 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 1 Native API	Logon Script (Windows)	Logon Script (Windows)	1 Deobfuscate/Decode Files or Information	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	1 Clipboard Data	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 Obfuscated Files or Information	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	2 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

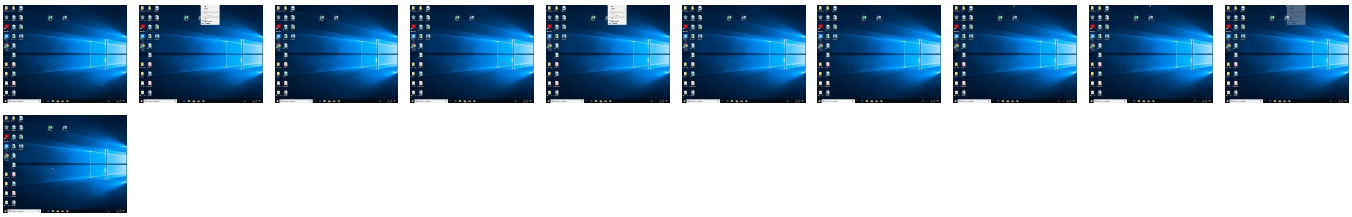
Behavior Graph



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
dinhVFAbgo.exe	10%	Virustotal		Browse
dinhVFAbgo.exe	5%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

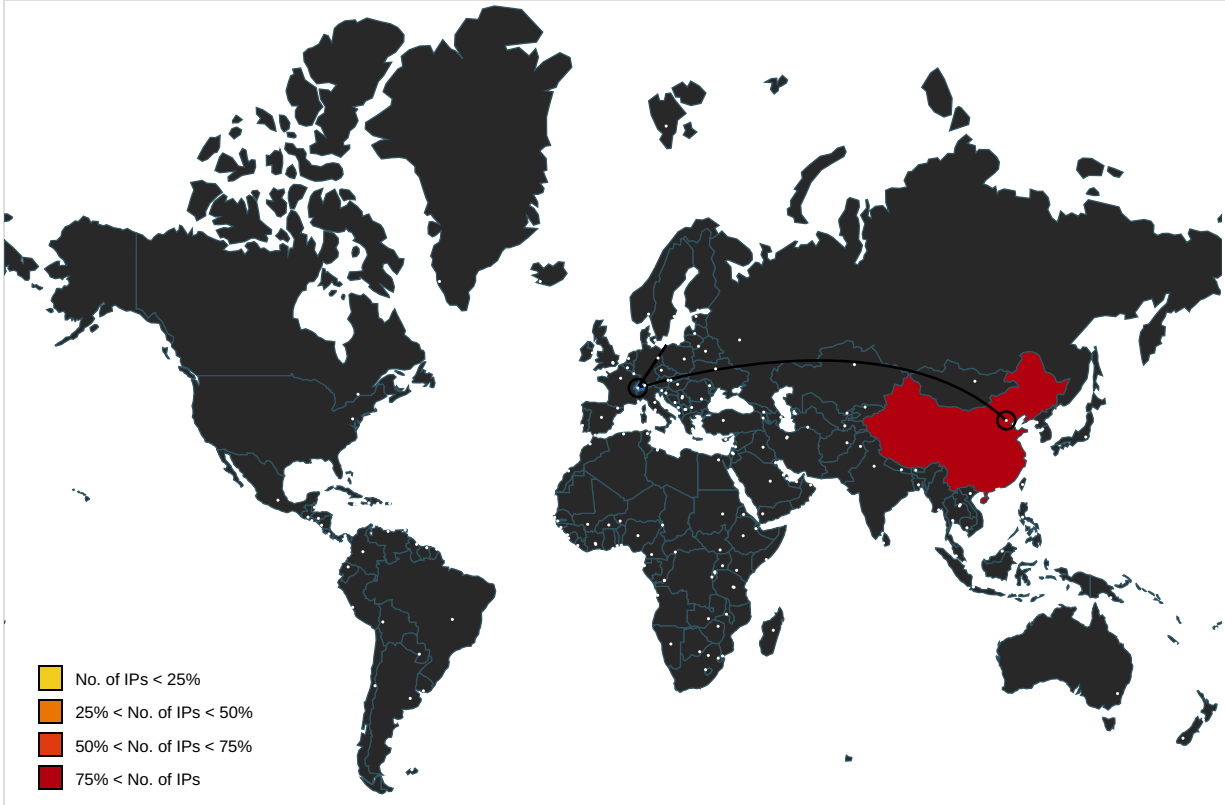
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
wtyjqpaszl-torjan.oss-cn-beijing.aliyuncs.com	59.110.190.41	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wtyjqpaszl-torjan.oss-cn-beijing.aliyuncs.com/TorJanFile/UpdateInit/Agent.exe	dinhVFAbgo.exe	false		high
http://https://wtyjqpaszl-torjan.oss-cn-beijing.aliyuncs.com/TorJanFile/ProtectDriver/x64_Defender.dat	dinhVFAbgo.exe	false		high
http://https://wtyjqpaszl-torjan.oss-cn-beijing.aliyuncs.com/TorJanFile/ProtectDriver/x64_FsFilter.dat	dinhVFAbgo.exe	false		high
http://https://wtyjqpaszl-torjan.oss-cn-beijing.aliyuncs.com/TorJanFile/SHA128Driver/x64_Defender.dathttps:	dinhVFAbgo.exe	false		high
http://https://wtyjqpaszl-torjan.oss-cn-beijing.aliyuncs.com/TorJanFile/SHA128Driver/x64_FsFilter.dat	dinhVFAbgo.exe	false		high
http://https://wtyjqpaszl-torjan.oss-cn-beijing.aliyuncs.com/TorJanFile/UpdateInit/Update.ini	dinhVFAbgo.exe	false		high
http://https://wtyjqpaszl-torjan.oss-cn-beijing.aliyuncs.com/TorJanFile/SHA128Driver/x64_Defender.dat	dinhVFAbgo.exe	false		high
http://https://wtyjqpaszl-torjan.oss-cn-beijing.aliyuncs.com/TorJanFile/UpdateInit/Update.inihttps://wtyjqp	dinhVFAbgo.exe	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
59.110.190.41	wtyjqpaszl-torjan.oss-cn-beijing.aliyuncs.com	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626617
Start date and time: 14/05/202216:17:10	2022-05-14 16:17:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	dinhVFAbgo (renamed file extension from none to 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:	26
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:	mal56.evad.winEXE@4/0@6/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 21.4% (good quality ratio 20.6%) • Quality average: 72% • Quality standard deviation: 24.4%
HCA Information:	• Successful, ratio: 81% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- 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 (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.69479192175591
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:	dinhVFAbgo.exe
File size:	2117120
MD5:	de3eafb5fa64237cb2d54949c432f19c
SHA1:	bbb3d8d70e1416241b469c3f58596986957ac39d
SHA256:	93d2edbc498f6f8689223bcb079143a97627efe9c1f7b23687a94a1eaf223d78
SHA512:	e01e963313fdede9144ddd4133a2f101177659902d821c994527ab4db627d5ce56e2e34d8c818b4bcbebe2fdfe74e9f0d15b715afa5df89ecfbe8eb73427b0c6
SSDEEP:	49152:UrvyLvF8NpuhRmx6uh9ooXXLEUajSrD7mp46RleP1qKcb1Rckjv+cAc3r4dbC:gvYvFclhEx6uboonLzQSrD7mpdRleP1G
TLSH:	13A57E21798048B7C1231E31B94BF379F2BD65FC0B3549C7F3B49A682966082962DD6F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%.~.v.~.v.~.v...w.~.v..6v.~.v...w.~.v...wn~.v...w.~.v...w.~.v.~.v.}.v...w.~.v...w.~.v...w...v!..w.~.v!.4v.~.v!..w.~.vRich.~.

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x53d4f0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x627F900D [Sat May 14 11:18:37 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6

OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	6568687b2c9d225811191553890bdbf0

Entrypoint Preview

Instruction
call 00007F26A8ABD40Bh
jmp 00007F26A8ABC9C9h
mov ecx, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], ecx
pop ecx
pop edi
pop edi
pop esi
pop ebx
mov esp, ebp
pop ebp
push ecx
ret
mov ecx, dword ptr [ebp-10h]
xor ecx, ebp
call 00007F26A8ABC20Bh
jmp 00007F26A8ABCB32h
mov ecx, dword ptr [ebp-14h]
xor ecx, ebp
call 00007F26A8ABC1FCh
jmp 00007F26A8ABCB23h
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [005C8DD4h]
xor eax, ebp
push eax
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [005C8DD4h]
xor eax, ebp
push eax
mov dword ptr [ebp-10h], eax

Instruction
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [005C8DD4h]
xor eax, ebp
push eax
mov dword ptr [ebp-10h], esp

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1c44f0	0x190	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1ea000	0x290	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x1eb000	0x212fc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1ac8c8	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x1ac9c0	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x1ac900	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x177000	0xa64	.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	0x17503b	0x175200	False	0.536344482831	data	6.49979287563	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x177000	0x50d5c	0x50e00	False	0.313683346213	data	5.22429967148	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1c8000	0x218ac	0x1d200	False	0.851579265021	data	7.76150366143	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1ea000	0x290	0x400	False	0.3388671875	data	3.88622144753	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1eb000	0x212fc	0x21400	False	0.464740953947	data	6.57292806881	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x1ea060	0x22f	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	LCMapStringW, CompareStringW, GetStdHandle, QueryPerformanceFrequency, GetCommandLineW, GetCommandLineA, HeapQueryInformation, SetStdHandle, FreeLibraryAndExitThread, ExitThread, EnumSystemLocalesW, ReadConsoleW, CreateFileW, GetModuleHandleExW, VirtualQuery, VirtualAlloc, RtlUnwind, GetStringTypeW, LCMapStringEx, InitializeCriticalSectionEx, OutputDebugStringW, IsValidLocale, SetFilePointerEx, GetConsoleOutputCP, GetFileType, GetFileAttributesExW, GetExitCodeProcess, CreateProcessW, GetTimeZoneInformation, FindFirstFileExW, FindNextFileW, IsValidCodePage, GetEnvironmentStringsW, FreeEnvironmentStringsW, SetEnvironmentVariableW, WriteConsoleW, InitializeSListHead, GetSystemTimeAsFileTime, QueryPerformanceCounter, GetStartupInfoW, IsDebuggerPresent, IsProcessorFeaturePresent, SetUnhandledExceptionFilter, UnhandledExceptionFilter, CreateEventW, GetUserDefaultLCID, GetTempFileNameA, SearchPathA, GetProfileIntA, GetTempPathA, VerifyVersionInfoA, VerSetConditionMask, GetWindowsDirectoryA, FindResourceExW, GetCurrentDirectoryA, GetConsoleMode, GetACP, GetCPInfo, GetOEMCP, VirtualProtect, GetUserDefaultUILanguage, GetLocaleInfoW, GlobalFlags, GlobalFindAtomA, GlobalAddAtomA, FindResourceA, lstrcmpW, GlobalDeleteAtom, GetSystemDirectoryW, EncodePointer, GetFileTime, GetFileSizeEx, GetFileAttributesExA, FileTimeToLocalFileTime, GlobalGetAtomNameA, lstrcmpA, GetCurrentProcessId, LocalReAlloc, GlobalHandle, GlobalReAlloc, TlsFree, TlsSetValue, TlsGetValue, TlsAlloc, InitializeCriticalSection, CompareStringA, ResumeThread, SetThreadPriority, GetCurrentThreadId, GetModuleFileNameA, DuplicateHandle, GetVolumeInformationA, WriteFile, UnlockFile, SetFilePointer, SetEndOfFile, ReadFile, LockFile, GetFileSize, FlushFileBuffers, FindFirstFileA, FindClose, FileTimeToSystemTime, SystemTimeToTzSpecificLocalTime, LoadLibraryW, LoadLibraryExW, GetModuleHandleW, GetModuleFileNameW, FreeLibrary, LeaveCriticalSection, EnterCriticalSection, OutputDebugStringA, CopyFileA, FormatMessageA, MulDiv, GlobalFree, GlobalLock, GlobalUnlock, GlobalSize, GlobalAlloc, GetFileAttributesA, GetFullPathNameA, OpenThread, GetConsoleWindow, LocalFree, CreateThread, LoadLibraryA, TerminateThread, GetCurrentThread, LocalAlloc, CreateMutexA, Thread32First, Thread32Next, HeapFree, GetCurrentProcess, SetLastError, lstrcmpiA, lstrcpyA, GetProcAddress, GetSystemInfo, Process32Next, GetVersionExA, CreateToolhelp32Snapshot, OpenProcess, GetModuleHandleA, TerminateProcess, Process32First, GetTickCount, GetPrivateProfileStringA, ExitProcess, WritePrivateProfileStringA, CreateFileA, DeviceIoControl, Sleep, CreateProcessA, FindResourceW, LoadResource, CloseHandle, DeleteFileA, LockResource, WaitForSingleObject, SizeofResource, WideCharToMultiByte, GetProcessHeap, DeleteCriticalSection, DecodePointer, HeapAlloc, RaiseException, HeapReAlloc, GetLastError, MultiByteToWideChar, HeapSize, InitializeCriticalSectionAndSpinCount
USER32.dll	SetTimer, DeleteMenu, SetCursor, ShowOwnedPopups, LoadImageW, InvalidateRect, TrackMouseEvent, IntersectRect, MapDialogRect, GetAsyncKeyState, GetNextDlgTabItem, EndDialog, CreateDialogIndirectParamA, PostQuitMessage, OffsetRect, SetRectEmpty, CopyImage, SystemParametersInfoA, InflateRect, GetMenuItemInfoA, DestroyMenu, FillRect, GetWindowDC, TabbedTextOutA, GrayStringA, DrawTextExA, DrawTextA, RealChildWindowFromPoint, ClientToScreen, DestroyIcon, IsDialogMessageA, SetWindowTextA, SendDlgItemMessageA, CheckDlgButton, MoveWindow, ShowWindow, GetMonitorInfoA, MonitorFromWindow, WinHelpA, GetScrollInfo, SetScrollInfo, LoadIconW, LoadIconA, GetWindow, GetTopWindow, GetClassLongA, SetWindowLongA, PtInRect, EqualRect, KillTimer, MapWindowPoints, ScreenToClient, AdjustWindowRectEx, GetClientRect, RemovePropA, GetPropA, SetPropA, ShowScrollBar, GetScrollRange, SetCursorPos, CopyIcon, FrameRect, DrawIcon, UnionRect, WaitForInputIdle, GetSystemMetrics, SetScrollRange, GetScrollPos, SetScrollPos, ScrollWindow, UpdateLayeredWindow, EndPaint, BeginPaint, SetForegroundWindow, GetForegroundWindow, SetClipboardData, UpdateWindow, TrackPopupMenu, SetMenu, GetMenu, GetCapture, SetFocus, GetDlgCtrlID, GetDlgItem, IsIconic, EndDeferWindowPos, DeferWindowPos, BeginDeferWindowPos, SetWindowPlacement, GetWindowPlacement, SetWindowPos, DestroyWindow, IsChild, IsMenu, IsWindow, CreateWindowExA, GetClassInfoExA, GetClassInfoA, RegisterClassA, CallWindowProcA, DefWindowProcA, PostMessageA, GetMessageTime, GetMessagePos, GetNextDlgGroupItem, SetCapture, ReleaseCapture, DrawFocusRect, IsRectEmpty, LoadImageA, DrawIconEx, GetIconInfo, MessageBeep, EnableScrollBar, HideCaret, InvertRect, LoadCursorW, NotifyWinEvent, CreatePopupMenu, GetMenuDefaultItem, MapVirtualKeyA, GetKeyNameTextA, SetLayeredWindowAttributes, EnumDisplayMonitors, OpenClipboard, CopyRect, GetCursorPos, FindWindowA, EnableMenuItem, WindowFromPoint, GetClassNameA, GetWindowRect, GetSystemMenu, MessageBoxA, GetMenuStringA, GetMenuState, GetSubMenu, GetMenuItemID, GetMenuItemCount, InsertMenuA, AppendMenuA, RemoveMenu, GetDesktopWindow, CharUpperA, GetMessageA, TranslateMessage, DispatchMessageA, PeekMessageA, SendMessageA, IsWindowVisible, GetActiveWindow, GetKeyState, ValidateRect, SetWindowsHookExA, CallNextHookEx, UnhookWindowsHookEx, GetDC, ReleaseDC, GetSysColor, GetSysColorBrush, LoadCursorA, EnableWindow, IsWindowEnabled, GetWindowLongA, GetParent, GetWindowThreadProcessId, GetLastActivePopup, GetWindowTextA, GetWindowTextLengthA, GetFocus, CheckMenuItem, SetMenuItemBitmaps, GetMenuCheckMarkDimensions, SetMenuItemInfoA, LoadBitmapW, RegisterWindowMessageA, MonitorFromPoint, LoadAcceleratorsA, TranslateAcceleratorA, LoadMenuA, EmptyClipboard, DrawStateA, SetClassLongA, CloseClipboard, SetWindowRgn, SetParent, DrawEdge, DrawFrameControl, IsZoomed, LoadMenuW, SetActiveWindow, BringWindowToTop, InsertMenuItemA, UnpackDDElParam, ReuseDDElParam, GetComboBoxInfo, PostThreadMessageA, WaitMessage, GetKeyboardLayout, IsCharLowerA, MapVirtualKeyExA, GetKeyboardState, ToAsciiEx, LoadAcceleratorsW, CreateAcceleratorTableA, DestroyAcceleratorTable, CopyAcceleratorTableA, SetRect, LockWindowUpdate, SetMenuDefaultItem, GetDoubleClickTime, ModifyMenuA, RegisterClipboardFormatA, CharUpperBuffA, IsClipboardFormatAvailable, GetUpdateRect, DrawMenuBar, DefFrameProcA, DefMDIChildProcA, TranslateMDISysAccel, SubtractRect, DestroyCursor, GetWindowRgn, CreateMenu, RedrawWindow
GDI32.dll	SetBkMode, SetMapMode, SetLayout, GetLayout, SetPolyFillMode, SetTextAlign, MoveToEx, TextOutA, ExtTextOutA, SetViewportExtEx, SetViewportOrgEx, SetWindowExtEx, SetWindowOrgEx, OffsetViewportOrgEx, OffsetWindowOrgEx, ScaleViewportExtEx, ScaleWindowExtEx, CreateFontIndirectA, GetTextExtentPoint32A, CombineRgn, CreateRectRgnIndirect, PatBlt, SetRectRgn, DPtoLP, GetTextMetricsA, EnumFontFamiliesExA, CreatePalette, GetNearestPaletteIndex, GetPaletteEntries, GetSystemPaletteEntries, RealizePalette, SelectPalette, CreateCompatibleBitmap, CreateDIBitmap, EnumFontFamiliesA, GetTextCharsetInfo, SetPixel, StretchBlt, CreateDIBSection, SetDIBColorTable, CreateEllipticRgn, Ellipse, GetTextColor, CreatePolygonRgn, Polygon, Polyline, CreateRoundRectRgn, LPtoDP, Rectangle, GetRgnBox, OffsetRgn, RoundRect, FillRgn, FrameRgn, GetBoundsRect, PtInRegion, ExtFloodFill, SetPaletteEntries, SetPixelV, GetWindowOrgEx, GetViewportOrgEx, GetTextFaceA, SelectObject, ExtSelectClipRgn, SelectClipRgn, SaveDC, RestoreDC, RectVisible, PtVisible, LineTo, IntersectClipRect, GetWindowExtEx, GetViewportExtEx, GetStockObject, GetPixel, GetObjectType, GetClipBox, ExcludeClipRect, Escape, CreateSolidBrush, CreateRectRgn, CreatePatternBrush, CreatePen, CreateHatchBrush, CreateCompatibleDC, BitBlt, DeleteObject, GetObjectA, SetTextColor, SetBkColor, CreateBitmap, DeleteDC, GetDeviceCaps, CreateDCA, GetBkColor, SetROP2, CopyMetaFileA
MSIMG32.dll	AlphaBlend, TransparentBlt
WINSPOOL.DRV	DocumentPropertiesA, ClosePrinter, OpenPrinterA

DLL	Import
ADVAPI32.dll	RegEnumKeyExA, RegDeleteValueA, RegDeleteKeyA, RegQueryValueExA, RegOpenKeyExA, RegCloseKey, RegCreateKeyExA, RegFlushKey, RegSetValueExA, SetSecurityDescriptorDacl, RevertToSelf, AccessCheck, SetSecurityDescriptorOwner, AllocateAndInitializeSid, ImpersonateSelf, IsValidSecurityDescriptor, OpenProcessToken, FreeSid, InitializeSecurityDescriptor, InitializeAcl, GetLengthSid, AddAccessAllowedAce, OpenThreadToken, SetSecurityDescriptorGroup, CreateServiceA, CloseServiceHandle, OpenSCManagerA, DeleteService, ControlService, StartServiceA, OpenServiceA
SHELL32.dll	SHGetFileInfoA, SHGetPathFromIDListA, SHGetSpecialFolderLocation, SHGetDesktopFolder, DragQueryFileA, DragFinish, SHAppBarMessage, SHBrowseForFolderA, ShellExecuteA
SHLWAPI.dll	PathStripToRootA, PathFindExtensionA, UrlUnescapeA, PathRemoveFileSpecW, StrFormatKBSizeA, PathFindFileNameA, PathIsUNCA
UxTheme.dll	DrawThemeText, DrawThemeParentBackground, OpenThemeData, CloseThemeData, DrawThemeBackground, GetThemeColor, GetCurrentThemeName, GetWindowTheme, IsAppThemed, IsThemeBackgroundPartiallyTransparent, GetThemeSysColor, GetThemePartSize
ole32.dll	OleDestroyMenuDescriptor, OleCreateMenuDescriptor, OleLockRunning, RevokeDragDrop, RegisterDragDrop, CoLockObjectExternal, OleGetClipboard, DoDragDrop, CreateStreamOnHGlobal, CoDisconnectObject, ReleaseStgMedium, OleDuplicateData, CoTaskMemAlloc, CoTaskMemFree, StringFromCLSID, CoInitialize, CoInitializeEx, CoInitializeSecurity, CoCreateInstance, CoUninitialize, OleTranslateAccelerator, IsAccelerator
OLEAUT32.dll	LoadTypeLib, VariantInit, SysFreeString, SysStringByteLen, SysAllocStringByteLen, SysAllocString, VariantClear, VariantTimeToSystemTime, VariantCopy, VariantChangeType, VarBstrFromDate, SysStringLen, SysAllocStringLen, SystemTimeToVariantTime
WS2_32.dll	getprotobyname, WSAStartup, gethostbyname, closesocket, connect, WSACleanup, recv, htons, setsockopt, WSAGetLastError, socket, send
SETUPAPI.dll	SetupDiGetDeviceInstanceIdA, SetupDiEnumDeviceInfo, SetupDiGetClassDevsA, SetupDiChangeState, SetupDiSetClassInstallParamsA, SetupDiClassNameFromGuidA, SetupDiDestroyDeviceInfoList
PSAPI.DLL	GetMappedFileNameA
gdiplus.dll	GdipCreateFromHDC, GdipSetInterpolationMode, GdipDrawImageRectI, GdipDeleteGraphics, GdiplusShutdown, GdipAlloc, GdipCreateBitmapFromHBITMAP, GdiplusStartup, GdipCloneImage, GdipBitmapUnlockBits, GdipBitmapLockBits, GdipCreateBitmapFromScan0, GdipFree, GdipCreateBitmapFromStream, GdipGetImagePaletteSize, GdipGetImagePalette, GdipGetImagePixelFormat, GdipGetImageHeight, GdipGetImageWidth, GdipGetImageGraphicsContext, GdipDrawImageI, GdipDisposeImage
WININET.dll	InternetCanonicalizeUrlA, InternetCrackUrlA
OLEACC.dll	AccessibleObjectFromWindow, LresultFromObject, CreateStdAccessibleObject
IMM32.dll	ImmReleaseContext, ImmGetOpenStatus, ImmGetContext
WINMM.dll	PlaySoundA

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

Total Packets: 24

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 16:18:12.350311995 CEST	49735	80	192.168.2.3	59.110.190.41
May 14, 2022 16:18:15.361134052 CEST	49735	80	192.168.2.3	59.110.190.41
May 14, 2022 16:18:21.361754894 CEST	49735	80	192.168.2.3	59.110.190.41
May 14, 2022 16:18:34.459714890 CEST	49744	80	192.168.2.3	59.110.190.41
May 14, 2022 16:18:37.472537041 CEST	49744	80	192.168.2.3	59.110.190.41
May 14, 2022 16:18:43.488518000 CEST	49744	80	192.168.2.3	59.110.190.41
May 14, 2022 16:18:57.303878069 CEST	49753	80	192.168.2.3	59.110.190.41
May 14, 2022 16:19:00.318156958 CEST	49753	80	192.168.2.3	59.110.190.41
May 14, 2022 16:19:06.366174936 CEST	49753	80	192.168.2.3	59.110.190.41
May 14, 2022 16:19:19.467772007 CEST	49801	80	192.168.2.3	59.110.190.41
May 14, 2022 16:19:22.476288080 CEST	49801	80	192.168.2.3	59.110.190.41
May 14, 2022 16:19:28.492398977 CEST	49801	80	192.168.2.3	59.110.190.41
May 14, 2022 16:19:41.820693016 CEST	49834	80	192.168.2.3	59.110.190.41
May 14, 2022 16:19:44.822033882 CEST	49834	80	192.168.2.3	59.110.190.41
May 14, 2022 16:19:50.838013887 CEST	49834	80	192.168.2.3	59.110.190.41
May 14, 2022 16:20:03.928900957 CEST	49839	80	192.168.2.3	59.110.190.41
May 14, 2022 16:20:06.933067083 CEST	49839	80	192.168.2.3	59.110.190.41
May 14, 2022 16:20:12.949462891 CEST	49839	80	192.168.2.3	59.110.190.41

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 16:18:12.306220055 CEST	55923	53	192.168.2.3	8.8.8.8
May 14, 2022 16:18:12.337354898 CEST	53	55923	8.8.8.8	192.168.2.3
May 14, 2022 16:18:34.429152012 CEST	57723	53	192.168.2.3	8.8.8.8
May 14, 2022 16:18:34.446933985 CEST	53	57723	8.8.8.8	192.168.2.3
May 14, 2022 16:18:56.994458914 CEST	49873	53	192.168.2.3	8.8.8.8
May 14, 2022 16:18:57.302799940 CEST	53	49873	8.8.8.8	192.168.2.3
May 14, 2022 16:19:19.448194981 CEST	63861	53	192.168.2.3	8.8.8.8
May 14, 2022 16:19:19.466698885 CEST	53	63861	8.8.8.8	192.168.2.3
May 14, 2022 16:19:41.650743008 CEST	50450	53	192.168.2.3	8.8.8.8
May 14, 2022 16:19:41.669198990 CEST	53	50450	8.8.8.8	192.168.2.3
May 14, 2022 16:20:03.908246994 CEST	64941	53	192.168.2.3	8.8.8.8
May 14, 2022 16:20:03.927833080 CEST	53	64941	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 14, 2022 16:18:12.306220055 CEST	192.168.2.3	8.8.8.8	0xbee5	Standard query (0)	wtyjqpaszl-torjan.oss-cn-beijing.aliyuncs.com	A (IP address)	IN (0x0001)

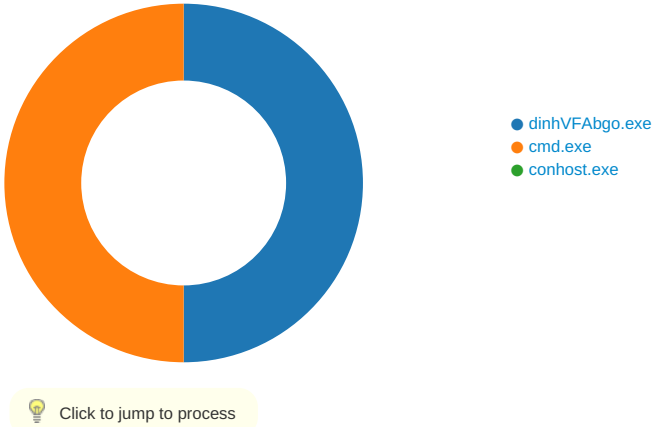
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 14, 2022 16:18:34.429152012 CEST	192.168.2.3	8.8.8.8	0x9b5	Standard query (0)	wtyjqpaszl-torjan.oss-cn-beijing.aliyuncs.com	A (IP address)	IN (0x0001)
May 14, 2022 16:18:56.994458914 CEST	192.168.2.3	8.8.8.8	0xa9b7	Standard query (0)	wtyjqpaszl-torjan.oss-cn-beijing.aliyuncs.com	A (IP address)	IN (0x0001)
May 14, 2022 16:19:19.448194981 CEST	192.168.2.3	8.8.8.8	0x4986	Standard query (0)	wtyjqpaszl-torjan.oss-cn-beijing.aliyuncs.com	A (IP address)	IN (0x0001)
May 14, 2022 16:19:41.650743008 CEST	192.168.2.3	8.8.8.8	0xa329	Standard query (0)	wtyjqpaszl-torjan.oss-cn-beijing.aliyuncs.com	A (IP address)	IN (0x0001)
May 14, 2022 16:20:03.908246994 CEST	192.168.2.3	8.8.8.8	0x6cb5	Standard query (0)	wtyjqpaszl-torjan.oss-cn-beijing.aliyuncs.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 14, 2022 16:18:12.337354898 CEST	8.8.8.8	192.168.2.3	0xbee5	No error (0)	wtyjqpaszl-torjan.oss-cn-beijing.aliyuncs.com		59.110.190.41	A (IP address)	IN (0x0001)
May 14, 2022 16:18:34.446933985 CEST	8.8.8.8	192.168.2.3	0x9b5	No error (0)	wtyjqpaszl-torjan.oss-cn-beijing.aliyuncs.com		59.110.190.41	A (IP address)	IN (0x0001)
May 14, 2022 16:18:57.302799940 CEST	8.8.8.8	192.168.2.3	0xa9b7	No error (0)	wtyjqpaszl-torjan.oss-cn-beijing.aliyuncs.com		59.110.190.41	A (IP address)	IN (0x0001)
May 14, 2022 16:19:19.466698885 CEST	8.8.8.8	192.168.2.3	0x4986	No error (0)	wtyjqpaszl-torjan.oss-cn-beijing.aliyuncs.com		59.110.190.41	A (IP address)	IN (0x0001)
May 14, 2022 16:19:41.669198990 CEST	8.8.8.8	192.168.2.3	0xa329	No error (0)	wtyjqpaszl-torjan.oss-cn-beijing.aliyuncs.com		59.110.190.41	A (IP address)	IN (0x0001)
May 14, 2022 16:20:03.927833080 CEST	8.8.8.8	192.168.2.3	0x6cb5	No error (0)	wtyjqpaszl-torjan.oss-cn-beijing.aliyuncs.com		59.110.190.41	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: dinhVFAbgo.exe PID: **6440**, Parent PID: **5816**

General

Target ID:	0
Start time:	16:18:08
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\dinhVFAbgo.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\dinhVFAbgo.exe"
Imagebase:	0xca0000
File size:	2117120 bytes
MD5 hash:	DE3EAFB5FA64237CB2D54949C432F19C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\DownLoad-Helper\Update.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	5	CAC019	CreateFileA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **6460**, Parent PID: **6440**

General

Target ID:	1
Start time:	16:18:09
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c md C:\DownLoad-Helper
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\DownLoad-Helper	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	C2BFE7	CreateDirectoryW

Analysis Process: conhost.exe PID: **6472**, Parent PID: **6460**

General	
Target ID:	2
Start time:	16:18:10
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly