ID: 691233
Sample Name: dmB3aYi8Bo.bin
Cookbook: default.jbs
Time: 03:52:44
Date: 27/08/2022
Version: 35.0.0 Citrine

Table of Contents

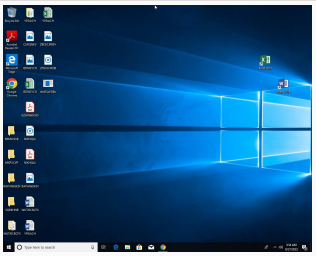
Windows Analysis Report

dmB3aYi8Bo.bin

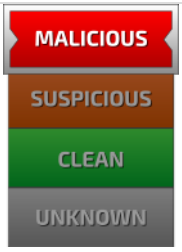
Overview

General Information

Sample Name:	dmB3aYi8Bo.bin (renamed file extension from bin to exe)
Analysis ID:	691233
MD5:	56aa2770810754.
SHA1:	e5870965f41cb8..
SHA256:	0eab1c5406f415..
Tags:	exe unnamed10
Infos:	



Detection



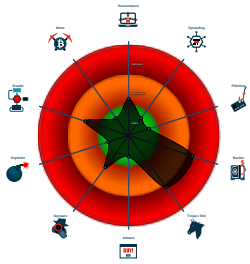
ZeusVM

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

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Detected ZeusVM e-Banking Trojan
- Contains VNC / remote desktop fun…
- Machine Learning detection for sam…
- Uses 32bit PE files
- Antivirus or Machine Learning detec…
- Contains functionality to read the PE…
- Contains functionality to shutdown /…
- Contains functionality to open a port…
- Detected potential crypto function
- May initialize a security null descrip…

Classification



Process Tree

- **System is w10x64**
- dmB3aYi8Bo.exe (PID: 6564 cmdline: "C:\Users\user\Desktop\dmB3aYi8Bo.exe" MD5: 56AA277081075438C3DBBEF841299172)
- **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

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

E-Banking Fraud

Detected ZeusVM e-Banking Trojan

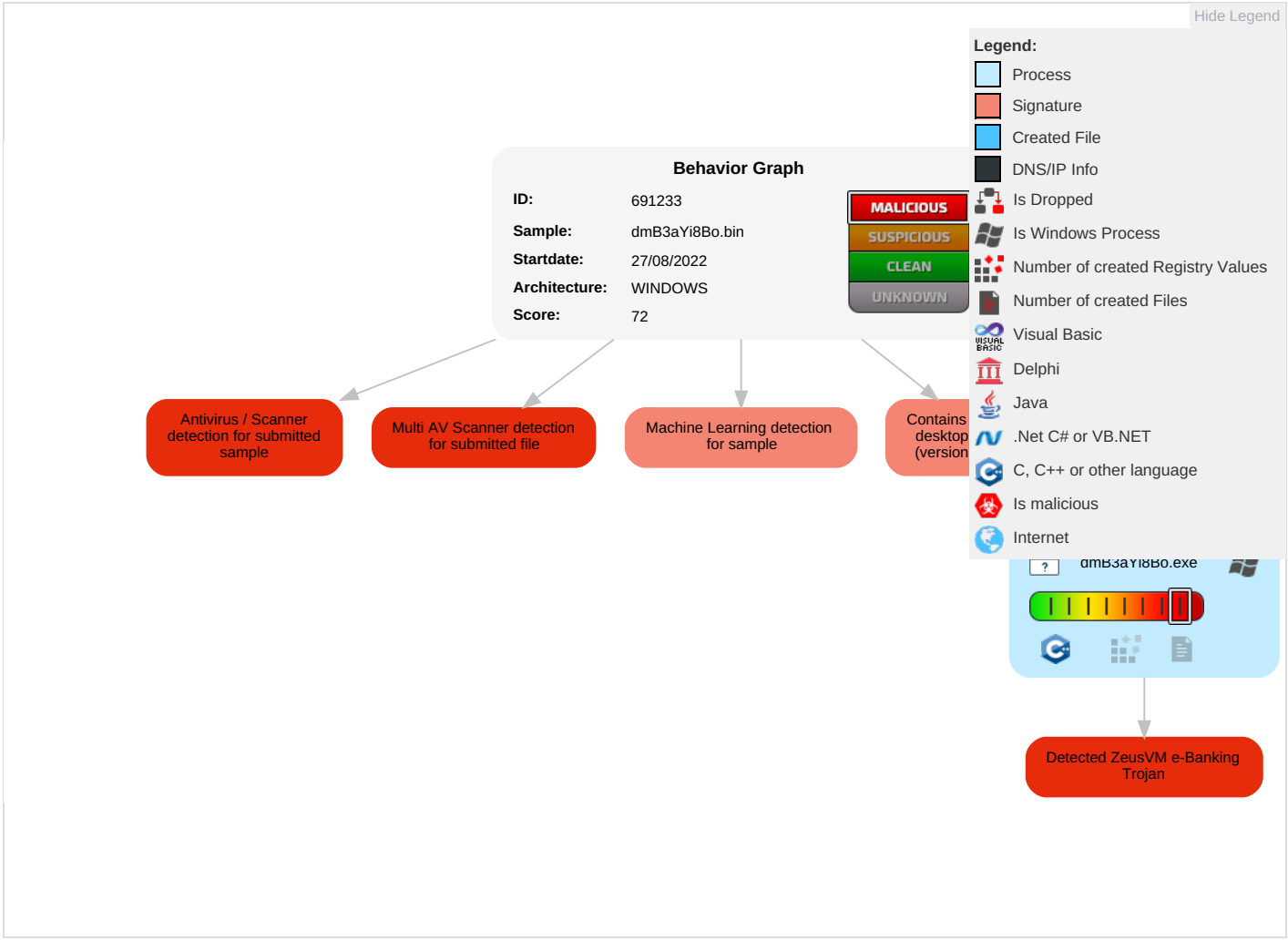
Remote Access Functionality

Contains VNC / remote desktop functionality (version string found)

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
1 Valid Accounts	2 Command and Scripting Interpreter	1 Create Account	1 Valid Accounts	1 Valid Accounts	1 1 Input Capture	2 System Time Discovery	1 Remote Desktop Protocol	1 1 Input Capture	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	2 1 Native API	1 Valid Accounts	1 1 Access Token Manipulation	1 1 Access Token Manipulation	LSASS Memory	1 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Remote Access Software	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Install Root Certificate	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	1 Clipboard Data	Automated Exfiltration	1 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Software Packing	NTDS	1 Account Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 System Owner/User 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	1 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	3 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

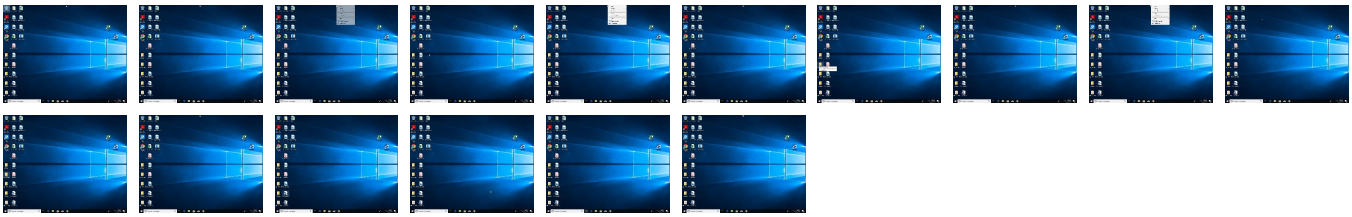
Behavior Graph



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
dmB3aYi8Bo.exe	58%	Virustotal		Browse
dmB3aYi8Bo.exe	77%	ReversingLabs	Win32.Trojan.Zeus	
dmB3aYi8Bo.exe	100%	Avira	TR/Spy.Zbot.afkmx	
dmB3aYi8Bo.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.dmB3aYi8Bo.exe.12b0000.0.unpack	100%	Avira	TR/Spy.Zbot.afkmx		Download File
0.2.dmB3aYi8Bo.exe.12b0000.0.unpack	100%	Avira	TR/Spy.Zbot.afkmx		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	691233
Start date and time:	2022-08-27 03:52:44 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	dmB3aYi8Bo.bin (renamed file extension from bin to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	11
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.bank.troj.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.9% (good quality ratio 95.4%) • Quality average: 88.3% • Quality standard deviation: 24.3%
HCA Information:	• Successful, ratio: 91% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): eudb.ris.api.iris.microsoft.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information

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):	5.974490890199798
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:	dmB3aYi8Bo.exe
File size:	187392
MD5:	56aa277081075438c3dbbef841299172
SHA1:	e5870965f41cb82f454043845641ae92b6c6b939
SHA256:	0eab1c5406f415f75ab39dbf3651cee9d41a0e0b6d5bdb51042412b57f0aea05
SHA512:	6f128a1a9d8b1bb96bc7fa92fad1170395b1ce9603168fb1925bbeb1a5d910f0f8b5999eabdcd4b1dacae376d4ff479d878920984ba68d951a46ac7056b7ad69
SSDEEP:	3072:bGVWrMNKUhjhoo7MQW/ieN6RzNLWV+1hpNaL+90tLsVXzJQYMUCb:bGArMNKUhjWl/ieNULu8h39SLSuYMUCb
TLSH:	2E04BF3EB9D15877C86F213149E9B6B432EED730136A49C7E1CD0E0938529E2A739397
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.......")..fH..fH..fH..fH..gH..o04. {H..fH..>I...>..zH...>:.gH..RichfH.....PE..L.....N.....V.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x401a1e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NO_ISOLATION, TERMINAL_SERVER_AWARE
Time Stamp:	0x4EF1CD9B [Wed Dec 21 12:14:19 2011 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:	f6a985405556b98acbdb7255917b9fb5

Entrypoint Preview

Instruction
jmp 00007F2E38A4556Eh
jmp 00007F2E38A40747h
jmp 00007F2E38A3A3D3h
jmp 00007F2E38A4493Fh
jmp 00007F2E38A49424h
jmp 00007F2E38A45EB6h
jmp 00007F2E38A45C09h
jmp 00007F2E38A4114Dh
jmp 00007F2E38A46240h
jmp 00007F2E38A40FABh
jmp 00007F2E38A4D9F6h
jmp 00007F2E38A3F627h
jmp 00007F2E38A3760Eh
jmp 00007F2E38A52351h
jmp 00007F2E38A4834Fh
jmp 00007F2E38A46C17h
jmp 00007F2E38A4AE0Eh
jmp 00007F2E38A4C913h
jmp 00007F2E38A3D105h
jmp 00007F2E38A379D6h
jmp 00007F2E38A38449h
jmp 00007F2E38A4756Dh
jmp 00007F2E38A40E8Fh
jmp 00007F2E38A515B7h
jmp 00007F2E38A3CCDEh
jmp 00007F2E38A36C3Eh
jmp 00007F2E38A408E5h
jmp 00007F2E38A373DEh
jmp 00007F2E38A3CD9Bh
jmp 00007F2E38A3D1FCh
jmp 00007F2E38A382B8h
jmp 00007F2E38A37061h

Instruction
jmp 00007F2E38A374CAh
jmp 00007F2E38A3D7D0h
jmp 00007F2E38A3E9A5h
jmp 00007F2E38A54798h
jmp 00007F2E38A3D7E0h
jmp 00007F2E38A403B8h
jmp 00007F2E38A375E4h
jmp 00007F2E38A461A4h

Rich Headers

Programming Language:	• [IMP] VS2008 SP1 build 30729 • [C++] VS2010 build 30319 • [LNK] VS2010 build 30319

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2e000	0x12c	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x31000	0x1350	.reloc
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	0x2e9f8	0x8cc	.idata
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	0x21f7b	0x22000	False	0.48848948759191174	data	5.9162227847345825	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
code	0x23000	0x35d1	0x3600	False	0.24254918981481483	data	3.993522758518666	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x27000	0x323c	0x3400	False	0.6225961538461539	data	5.636797675605685	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x2b000	0x2a3a	0x600	False	0.150390625	PGP symmetric key encrypted data - Plaintext or unencrypted data	1.1042325865513358	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0x2e000	0x2e8d	0x3000	False	0.3174641927083333	data	4.73911940856972	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0x31000	0x1649	0x1800	False	0.6793619791666666	data	5.9673223528898065	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import

DLL	Import
KERNEL32.dll	SystemTimeToFileTime, WideCharToMultiByte, MultiByteToWideChar, FormatMessageW, OpenProcess, CreateProcessW, FileTimeToDosDateTime, FileTimeToLocalFileTime, GetFileInformationByHandle, GetVolumeNameForVolumeMountPointW, GetOverlappedResult, RemoveDirectoryW, FindClose, FindNextFileW, FindFirstFileW, SetEndOfFile, GetEnvironmentVariableW, DuplicateHandle, CreateEventW, GetModuleFileNameW, SetErrorMode, GetVersionExW, GetCurrentProcessId, GetFileAttributesExW, SetEvent, OpenEventW, lstrcpyW, ExitProcess, MulDiv, InitializeCriticalSection, FlushFileBuffers, GetThreadContext, GetProcessId, LeaveCriticalSection, EnterCriticalSection, CreateRemoteThread, Process32NextW, Process32FirstW, DeleteCriticalSection, GetLocalTime, GetPrivateProfileStringW, GetPrivateProfileIntW, GetNativeSystemInfo, GetUserDefaultUILanguage, MoveFileExW, GlobalUnlock, GlobalLock, GetCurrentThreadId, TlsGetValue, TlsSetValue, TerminateProcess, ResetEvent, MapViewOfFile, CreateFileMappingW, TlsAlloc, UnmapViewOfFile, TlsFree, WaitForMultipleObjects, SetLastError, ExpandEnvironmentStringsW, GetFileAttributesW, CreateDirectoryW, GetFileTime, SetFileTime, GetTempPathW, GetTempFileNameW, SetFileAttributesW, LoadLibraryA, ReadFile, DeleteFileW, SetFilePointerEx, GetFileSizeEx, VirtualAlloc, VirtualFree, CreateFileW, SetFilePointer, WriteFile, VirtualFreeEx, IsBadReadPtr, VirtualAllocEx, VirtualProtectEx, ReadProcessMemory, WriteProcessMemory, SetThreadContext, VirtualQueryEx, OpenMutexW, ReleaseMutex, CreateMutexW, LocalFree, LoadLibraryW, FreeLibrary, CreateThread, GetModuleHandleW, GetProcAddress, GetLastError, CreateToolhelp32Snapshot, Thread32First, Thread32Next, CloseHandle, lstrcmpiW, Sleep, GetTickCount, GetTimeZoneInformation, HeapFree, HeapAlloc, HeapReAlloc, HeapDestroy, HeapCreate, GetProcessHeap, GetSystemTime, lstrcmpiA, GetCurrentThread, SetThreadPriority, GetCommandLineW, WaitForSingleObject
USER32.dll	RegisterClassA, RegisterClassExW, RegisterClassExA, CreateWindowStationW, OpenWindowStationW, SetProcessWindowStation, GetProcessWindowStation, CreateDesktopW, SetThreadDesktop, CloseWindowStation, CloseDesktop, GetUpdateRgn, GetUpdateRect, GetWindowDC, GetDCEx, EndPaint, BeginPaint, IntersectRect, EqualRect, CallWindowProcW, PrintWindow, PeekMessageA, GetMessageA, GetMessageW, GetCapture, ReleaseCapture, SetCapture, SetCursorPos, GetCursorPos, GetMessagePos, GetWindowInfo, GetAncestor, RegisterClassW, GetClassLongW, GetWindowRect, IsRectEmpty, GetParent, MapWindowPoints, SetWindowPos, IsWindow, DefMDIChildProcA, DefMDIChildProcW, DefFrameProcA, DefFrameProcW, DefDlgProcA, DefDlgProcW, DefWindowProcA, SwitchDesktop, OpenDesktopW, OpenInputDesktop, GetMenu, GetMenuItemCount, GetMenuState, HiliteMenuItem, MenuItemFromPoint, EndMenu, GetSubMenu, GetMenuItemRect, TrackPopupMenuEx, FillRect, GetMenuItemID, SetKeyboardState, GetShellWindow, SystemParametersInfoW, DrawEdge, GetUserObjectInformationW, GetWindowThreadProcessId, CallWindowProcA, RegisterWindowMessageW, GetClassNameW, PostThreadMessageW, DefWindowProcW, CharLowerBuffA, CharLowerW, CharLowerA, SendMessageW, MapVirtualKeyW, PostMessageW, GetSystemMetrics, GetClipboardData, GetKeyboardState, ToUnicode, ExitWindowsEx, CharToOemW, GetDC, ReleaseDC, LoadImageW, GetWindowTextLengthW, GetWindowTextW, WindowFromPoint, SendMessageTimeoutW, GetWindowLongW, SetWindowLongW, DispatchMessageW, TranslateMessage, PeekMessageW, MsgWaitForMultipleObjects, CharUpperW, GetWindow, GetTopWindow, GetThreadDesktop
ADVAPI32.dll	CryptReleaseContext, CryptDestroyHash, CryptGetHashParam, CryptHashData, CryptCreateHash, CryptAcquireContextW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, OpenThreadToken, GetSidSubAuthority, GetSidSubAuthorityCount, GetTokenInformation, SetSecurityDescriptorSacl, GetSecurityDescriptorSacl, ConvertStringSecurityDescriptorToSecurityDescriptorW, SetSecurityDescriptorDacl, InitializeSecurityDescriptor, SetNamedSecurityInfoW, RegCloseKey, RegQueryValueExW, RegOpenKeyExW, RegSetValueExW, RegCreateKeyExW, CreateProcessAsUserW, GetLengthSid, ConvertSidToStringSidW, InitiateSystemShutdownExW
SHLWAPI.dll	PathIsURLW, PathQuoteSpacesW, PathRenameExtensionW, PathIsDirectoryW, PathMatchSpecW, UrlUnescapeA, PathAddBackslashW, PathRemoveBackslashW, PathRemoveFileSpecW, PathAddExtensionW, PathFindFileNameW, wvnsprintfA, wvnsprintfW, PathCombineW, PathUnquoteSpacesW, PathSkipRootW, StrCmpNIA, SHDeleteValueW, SHDeleteKeyW, PathIsRelativeW, StrCmpNIW
SHELL32.dll	ShellExecuteW, CommandLineToArgvW, SHGetFolderPathW
Secur32.dll	GetUserNameExW
PSAPI.DLL	EnumProcessModules, GetModuleBaseNameW, GetModuleFileNameExW
ole32.dll	CLSIDFromString, StringFromGUID2
GDI32.dll	RestoreDC, SetViewportOrgEx, SaveDC, GdiFlush, CreateCompatibleDC, SetRectRgn, SelectObject, CreateCompatibleBitmap, DeleteObject, CreateDIBSection, GetObjectW, GetDIBits, DeleteDC, CreateFontIndirectW, GetDeviceCaps
COMCTL32.dll	InitCommonControlsEx
WS2_32.dll	select, send, WSACleanup, WSAStartup, closesocket, connect, recvfrom, sendto, WSASend, getpeername, WSAStringToAddressW, WSAAddressToStringW, getsockname, WSAGetLastError, setsockopt, WSAIoctl, shutdown, accept, WSASetLastError, bind, listen, getaddrinfo, freeaddrinfo, recv, socket
CRYPT32.dll	CertDuplicateCertificateContext, CertDeleteCertificateFromStore, CertOpenSystemStoreW, CertEnumCertificatesInStore, PFXExportCertStoreEx, CertCloseStore, PFXImportCertStore
WININET.dll	GetUrlCacheEntryInfoW, HttpAddRequestHeadersW, HttpSendRequestW, HttpSendRequestExW, HttpSendRequestExA, InternetReadFileExA, InternetQueryDataAvailable, HttpAddRequestHeadersA, InternetCrackUrlA, InternetReadFile, InternetQueryOptionW, HttpOpenRequestA, HttpSendRequestA, HttpQueryInfoA, InternetQueryOptionA, InternetOpenA, InternetSetOptionA, InternetConnectA, InternetCloseHandle, InternetSetStatusCallbackW
COMDLG32.dll	GetOpenFileNameW, GetSaveFileNameW

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: dmB3aYi8Bo.exe PID: 6564, Parent PID: 4240

General	
Target ID:	0
Start time:	03:53:44
Start date:	27/08/2022
Path:	C:\Users\user\Desktop\dmB3aYi8Bo.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\dmB3aYi8Bo.exe"
Imagebase:	0x12b0000
File size:	187392 bytes
MD5 hash:	56AA277081075438C3DBBEF841299172
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

No disassembly