ID: 376942
Sample Name: vovy0jYEM7
Cookbook: default.jbs
Time: 03:46:23
Date: 28/03/2021
Version: 31.0.0 Emerald

Table of Contents

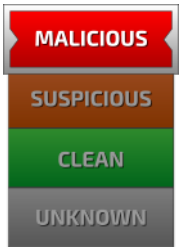
Analysis Report vovy0jYEM7

Overview

General Information

Sample Name:	vovy0jYEM7 (renamed file extension from none to exe)
Analysis ID:	376942
MD5:	ac98d2d71f3a499.
SHA1:	76b5d3fd16c3e76.
SHA256:	98d33cf483b14fb..
Tags:	uncategorized
Infos:	

Detection

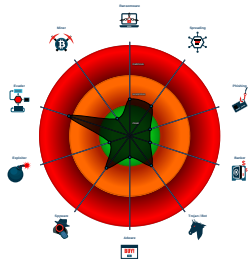


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Contains functionality to detect slee…
- Machine Learning detection for samp…
- Antivirus or Machine Learning detec…
- Contains functionality to access load…
- Contains functionality to call native f…
- Contains functionality to dynamically…
- Contains functionality to enumerate …
- Contains functionality to launch a pr…
- Contains functionality to open a port…
- Contains functionality to read the cli…
- Contains functionality to retrieve info…

Classification



Startup

- **System is w10x64**
- vovy0jYEM7.exe (PID: 6588 cmdline: 'C:\Users\user\Desktop\vovy0jYEM7.exe' MD5: AC98D2D71F3A4998ABE80DD6E0695FBA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

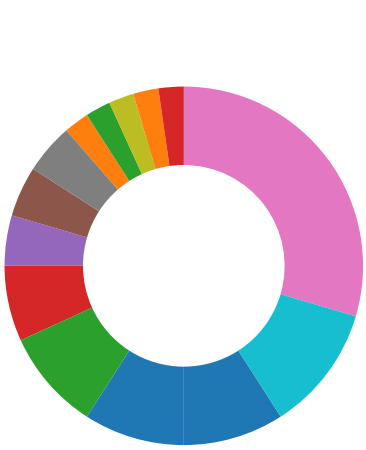
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Cryptography
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

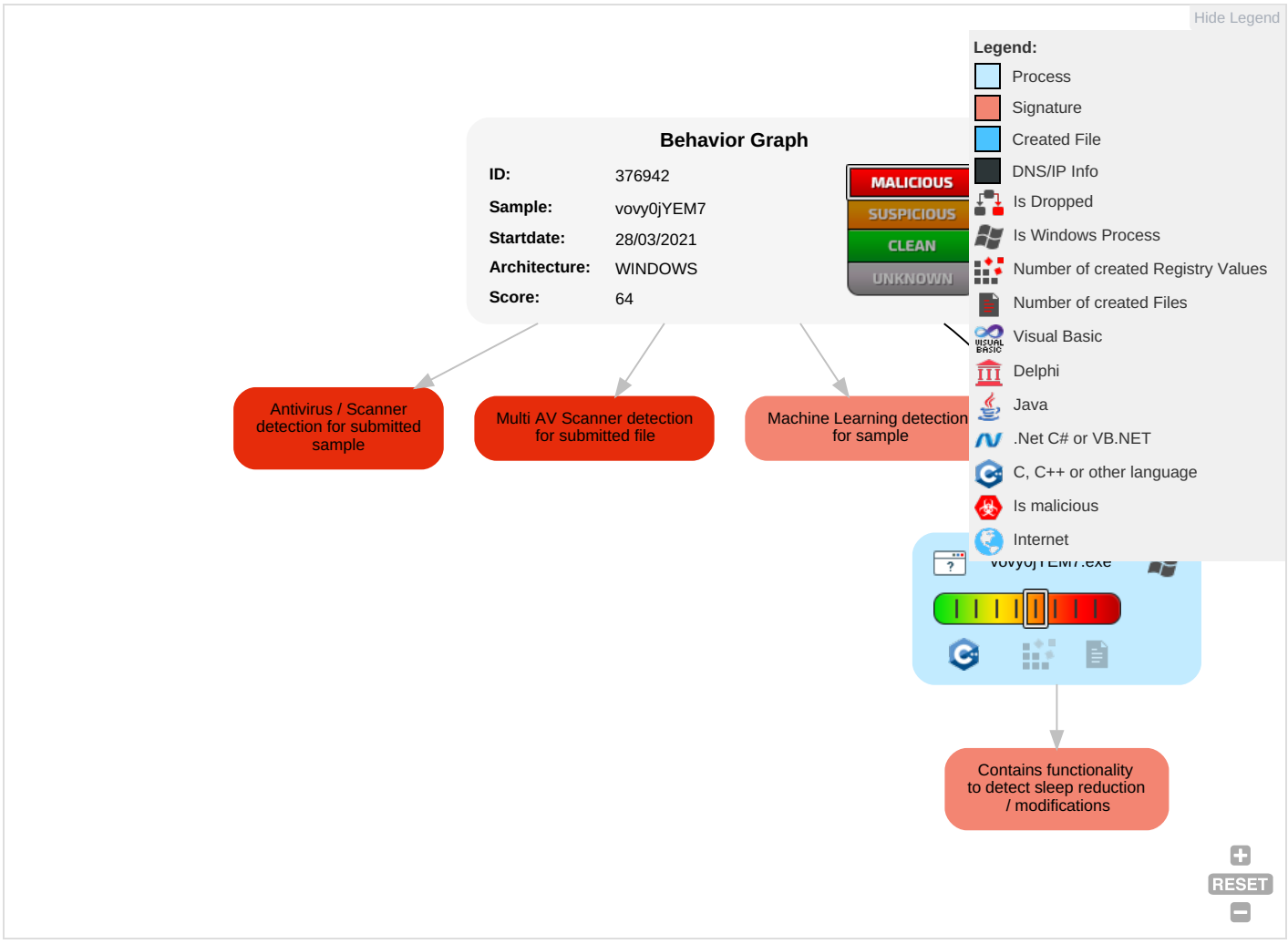
Malware Analysis System Evasion:

Contains functionality to detect sleep reduction / modifications

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 1	Native API 1	Valid Accounts 1	Valid Accounts 1	Valid Accounts 1	Input Capture 1 1	Network Share Discovery 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Application Shimming 1	Access Token Manipulation 1 1	Access Token Manipulation 1 1	LSASS Memory	System Time Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Application Shimming 1	Obfuscated Files or Information 1	Security Account Manager	Security Software Discovery 1 2	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Install Root Certificate 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
vovy0jYEM7.exe	89%	Virustotal		Browse
vovy0jYEM7.exe	96%	ReversingLabs	Win32.Trojan.Zeus	
vovy0jYEM7.exe	100%	Avira	TR/Kazy.MK	
vovy0jYEM7.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.vovy0jYEM7.exe.400000.0.unpack	100%	Avira	TR/Kazy.MK		Download File
0.0.vovy0jYEM7.exe.400000.0.unpack	100%	Avira	TR/Kazy.MK		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://adrotate.sytes.net/cfgg.bin	3%	Virustotal		Browse
http://adrotate.sytes.net/cfgg.bin	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://adrotate.sytes.net/cfgg.bin	vovy0jYEM7.exe	false	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	376942
Start date:	28.03.2021
Start time:	03:46:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	vovy0jYEM7 (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:	1
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:	mal64.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 99.6% (good quality ratio 92.1%) • Quality average: 82.2% • Quality standard deviation: 29.9%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated

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:	MS-DOS executable
Entropy (8bit):	6.666462810016037
TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • DOS Executable Borland Pascal 7.0x (2037/25) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00%
File name:	vovy0jYEM7.exe
File size:	143360
MD5:	ac98d2d71f3a4998abe80dd6e0695fba
SHA1:	76b5d3fd16c3e761022ebd7f3f5fc34f022fcc04
SHA256:	98d33cf483b14fbdab3a470a9452bcea672da54da113133 0babcbb40572719e8
SHA512:	190893c1511573db160bcfae275ac4b7ac43b6a1cb67f34 8e1043a98698241c96b44bfd65ebef1a18b80e8955118ae 71e4384bf061781984427cee6251bafff7
SSDEEP:	3072:BpJJwr9xIGE2q/DB9WMnuwutBE+XjlE2fX7kiknVi BXMlaT0S:BpkYGOBRjutBE+XvjkiGV6HTh
File Content Preview:	MZ..... ....PE..L...".O.....6.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x405f45
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x4F8CFD22 [Tue Apr 17 05:18:26 2012 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:	5aa18671f1cb1cc96a51c8f1958d6f84

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
push ecx
push ebx
push 00000000h
xor bl, bl
call 00007FA290D7332Eh
test al, al
je 00007FA290D744C6h
push 00008007h
add bl, 00000002h
call dword ptr [00401240h]
lea eax, dword ptr [ebp-04h]
push eax
call dword ptr [00401244h]
push eax
call dword ptr [00401284h]
test eax, eax
je 00007FA290D74463h
xor edx, edx
cmp dword ptr [ebp-04h], edx
jle 00007FA290D74455h
mov ecx, dword ptr [eax+edx*4]
test ecx, ecx
je 00007FA290D74448h
cmp word ptr [ecx], 002Dh
jne 00007FA290D74442h
movzx ecx, word ptr [ecx+02h]
cmp ecx, 66h
je 00007FA290D74436h
cmp ecx, 69h
je 00007FA290D7442Ch
cmp ecx, 6Eh
jne 00007FA290D7442Fh
and bl, FFFFFFFDh

Instruction
jmp 00007FA290D7442Ah
or bl, 00000008h
jmp 00007FA290D74425h
or bl, 00000001h
inc edx
cmp edx, dword ptr [ebp-04h]
jl 00007FA290D743EFh
push eax
call dword ptr [00423808h]
test bl, 00000008h
je 00007FA290D74429h
call 00007FA290D73DCAh
jmp 00007FA290D74438h
mov al, bl
shr al, 1
and al, 01h
movzx eax, al
push eax
and bl, 00000001h
movzx eax, bl
push eax
call 00007FA290D73FA0h
mov bl, al
test bl, bl
je 00007FA290D74436h
test byte ptr [004222A8h], 00000002h
je 00007FA290D7442Dh
push FFFFFFFFh
call dword ptr [00423818h]
pop ebx
leave
ret
xor eax, eax
test bl, bl
sete al
push eax
call dword ptr [00401248h]
int3
test esi, esi

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x20b04	0xf0	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x24000	0x10	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x25000	0x10c4	.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	0x1000	0x394	.text
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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x20ec6	0x21000	False	0.63339695786	data	6.68700480051	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x22000	0x1d4c	0x200	False	0.20703125	data	1.30631439164	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x24000	0x10	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x25000	0x14c2	0x1800	False	0.689127604167	data	6.04503144547	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	lstrcpynW, FileTimeToSystemTime, ReadFile, lstrcatA, lstrcmpW, lstrlenW, GetFileInformationByHandle, lstrcpyW, ExpandEnvironmentStringsW, GetEnvironmentVariableW, FileTimeToDosDateTime, HeapReAlloc, CreateMutexW, FindFirstFileW, SetEndOfFile, CreateProcessW, HeapAlloc, SetFilePointerEx, HeapFree, CreateDirectoryW, GetProcessHeap, IsBadReadPtr, SetFileTime, VirtualQueryEx, OpenProcess, Thread32First, LoadLibraryW, ReadProcessMemory, HeapDestroy, HeapCreate, Thread32Next, GetTimeZoneInformation, CreateThread, MultiByteToWideChar, WideCharToMultiByte, OpenMutexW, GetLastError, SetLastError, VirtualProtectEx, VirtualAllocEx, FindClose, RemoveDirectoryW, FindNextFileW, VirtualProtect, CreateToolhelp32Snapshot, GetFileTime, ReleaseMutex, FileTimeToLocalFileTime, DeleteFileW, SetFileAttributesW, GetThreadContext, SetThreadContext, GetProcessId, GetDriveTypeA, Sleep, GetLogicalDriveStringsA, MoveFileW, ResetEvent, GetNativeSystemInfo, WTSGetActiveConsoleSessionId, GlobalLock, GlobalUnlock, MoveFileExW, GetUserDefaultUILanguage, CreateRemoteThread, Process32FirstW, Process32NextW, GetSystemTime, GetLocalTime, SystemTimeToFileTime, UnmapViewOfFile, lstrlenA, SetFilePointer, GetFileSize, FreeLibrary, lstrcmpiA, GetPrivateProfileIntW, InitializeCriticalSection, FlushFileBuffers, SetThreadPriority, GetTempPathW, GetCurrentThread, CreateFileW, GetFileAttributesW, WriteFile, GetPrivateProfileStringW, lstrcpyA, WriteProcessMemory, GetCurrentProcessId, CloseHandle, DuplicateHandle, OpenEventW, GetFileAttributesExW, lstrcmpiW, WaitForMultipleObjects, CreateEventW, GetProcAddress, GetModuleFileNameW, GetVersionExW, VirtualFreeEx, VirtualFree, GetTickCount, GetModuleHandleW, SetEvent, GetComputerNameW, SetErrorMode, GetCommandLineW, ExitProcess, EnterCriticalSection, LeaveCriticalSection
USER32.dll	CharToOemW, wsprintfA, ExitWindowsEx, CharLowerBuffA, MsgWaitForMultipleObjects, LoadImageW, CharLowerA, PeekMessageW, CharUpperW, wsprintfW, CharLowerW, ToUnicode, GetKeyboardState, GetCursorPos, GetIconInfo, DrawIcon, GetClipboardData, TranslateMessage, DispatchMessageW
ADVAPI32.dll	LookupPrivilegeValueW, SetNamedSecurityInfoW, SetSecurityDescriptorDacl, InitializeSecurityDescriptor, CreateProcessAsUserW, RegQueryValueExW, CryptReleaseContext, RegCreateKeyExW, GetTokenInformation, GetSidSubAuthorityCount, OpenThreadToken, CryptAcquireContextW, GetSidSubAuthority, CryptGetHashParam, InitiateSystemShutdownExW, GetLengthSid, IsWellKnownSid, CryptCreateHash, ConvertStringSecurityDescriptorToSecurityDescriptorW, RegOpenKeyExW, GetSecurityDescriptorSacl, CryptDestroyHash, AdjustTokenPrivileges, RegCloseKey, RegSetValueExW, CryptHashData, RegEnumKeyExW, ConvertSidToStringSidW, EqualSid
SHLWAPI.dll	PathIsDirectoryW, UrlUnescapeA, PathRemoveFileSpecW, SHDeleteValueW, PathSkipRootW, SHDeleteKeyW, PathCombineW, PathAddExtensionW, PathUnquoteSpacesW, StrCmpNIA, wvnsprintfA, StrStrIA, StrStrIW, StrCmpNIW, PathIsURLW, PathQuoteSpacesW, PathRemoveBackslashW, PathRenameExtensionW
SHELL32.dll	SHFileOperationW, ShellExecuteW, CommandLineToArgvW, SHGetFolderPathW
Secur32.dll	GetUserNameExW
ole32.dll	StringFromGUID2, CoUninitialize, CoCreateInstance, CoInitializeEx
WS2_32.dll	connect, WSAIoctl, sendto, WSAEventSelect, WSAAddressToStringW, WSAStartup, getaddrinfo, select, WSAGetLastError, getsockname, setsockopt, bind, socket, freeaddrinfo, listen, WSASend, closesocket, send
CRYPT32.dll	CertOpenSystemStoreW, PFXExportCertStoreEx, PFXImportCertStore, CryptUnprotectData, CertDeleteCertificateFromStore, CertCloseStore, CertEnumCertificatesInStore, CertDuplicateCertificateContext
OLEAUT32.dll	VariantInit, SysAllocString, VariantClear, SysFreeString
NETAPI32.dll	NetApiBufferFree, NetUserEnum, NetUserGetInfo

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: vovy0jYEM7.exe PID: 6588 Parent PID: 6032

General

Start time:	03:47:07
Start date:	28/03/2021
Path:	C:\Users\user\Desktop\vovy0jYEM7.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\vovy0jYEM7.exe'
Imagebase:	0x400000
File size:	143360 bytes
MD5 hash:	AC98D2D71F3A4998ABE80DD6E0695FBA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis