ID: 385074
Sample Name: 7FzERy9xWc
Cookbook: default.jbs
Time: 15:49:45
Date: 11/04/2021
Version: 31.0.0 Emerald

Table of Contents

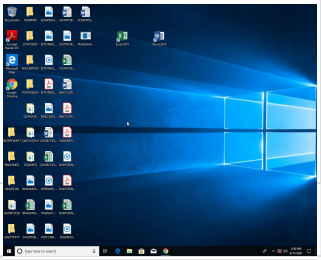
Analysis Report 7FzERy9xWc

Overview

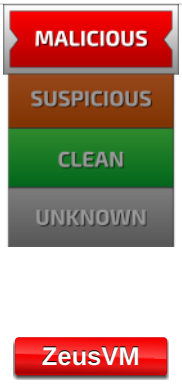
General Information

Sample Name:	7FzERy9xWc (renamed file extension from none to exe)
Analysis ID:	385074
MD5:	8f250f634de721f…
SHA1:	8e177de1f0ec9d4.
SHA256:	5971fcdcf0f563f5..
Tags:	uncategorized
Infos:	

Most interesting Screenshot:



Detection

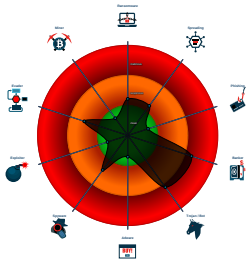


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Detected ZeusVM e-Banking Trojan
- Multi AV Scanner detection for subm…
- Contains VNC / remote desktop func…
- Machine Learning detection for samp…
- Antivirus or Machine Learning detec…
- 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 PEB
- Contains functionality to read the cli…

Classification



Startup

- **System is w10x64**
- 7FzERy9xWc.exe (PID: 2788 cmdline: 'C:\Users\user\Desktop\7FzERy9xWc.exe' MD5: 8F250F634DE721FEC7B002A805DDDC24)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

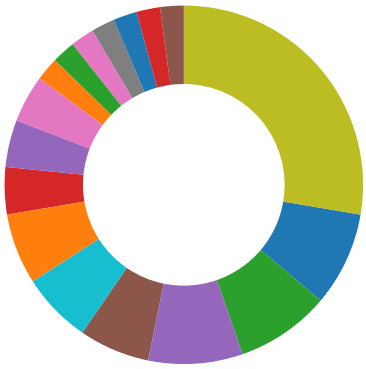
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Cryptography
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- Protection of GUI



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

E-Banking Fraud:

Detected ZeusVM e-Banking Trojan

Remote Access Functionality:

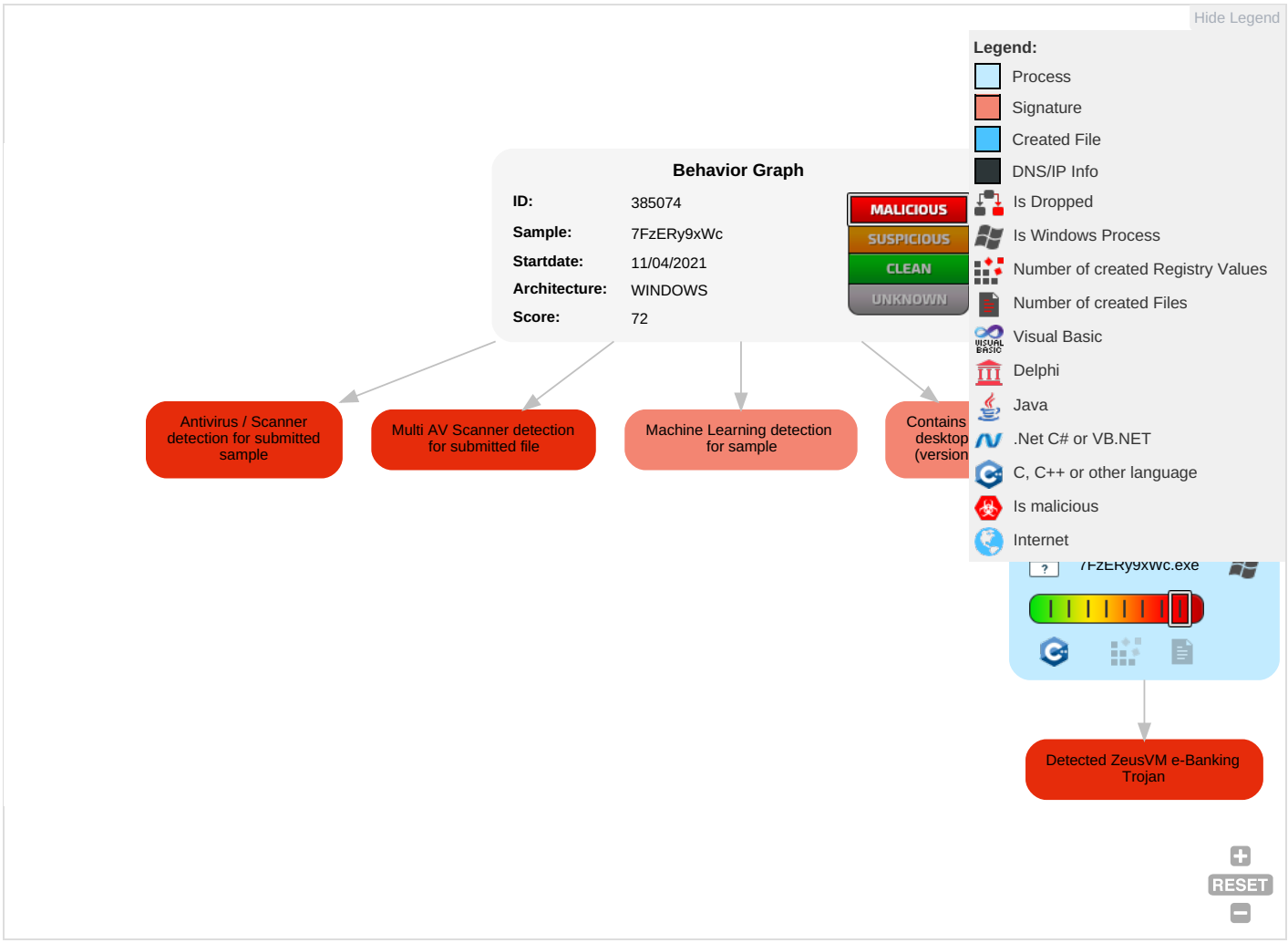
Contains VNC / remote desktop functionality (version string found)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts 1	Native API 1	Create Account 1	Valid Accounts 1	Valid Accounts 1	Input Capture 2 1	Network Share Discovery 1	Remote Desktop Protocol 1	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Valid Accounts 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	Remote Access Software 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Application Shimming 1	Application Shimming 1	Obfuscated Files or Information 2	Security Account Manager	Security Software Discovery 1 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Ingress Tool Transfer 1	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 3	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 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
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



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
7FzERy9xWc.exe	88%	Virustotal		Browse
7FzERy9xWc.exe	92%	ReversingLabs	Win32.Trojan.Zeus	
7FzERy9xWc.exe	100%	Avira	TR/Spy.Gen	
7FzERy9xWc.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.7FzERy9xWc.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen		Download File
0.2.7FzERy9xWc.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385074
Start date:	11.04.2021
Start time:	15:49:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	7FzERy9xWc (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:	5
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:	Failed
HDC Information:	• Successful, ratio: 32.2% (good quality ratio 30.7%) • Quality average: 80.9% • Quality standard deviation: 25.6%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	MS-DOS executable
Entropy (8bit):	7.912987012643321
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:	7FzERy9xWc.exe
File size:	188928
MD5:	8f250f634de721fec7b002a805dddc24
SHA1:	8e177de1f0ec9d45417b27e47973b8ded74242c7
SHA256:	5971fcdcf0f563f502c8ab017f34567c15e3e76c7a3c1497ae8513c305f77798
SHA512:	d42a259868824429c4d6c7ed4aa5de1ddb3805d300feb39b51480a5232c0c05a74d9f27266ce60a796545f23e5de75896a8aa871ed93e5ab73ec01647175c191
SSDEEP:	3072:k8pY9M8j32Jwk95kLvkIuBEn/VnEXC1gDtfgBtW8cNhSw4L7Qpo977jurOC:k9j3SwOucIWX1fI6NATF9n6rp
File Content Preview:	MZ..... ....PE..L...YJ.P.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x41dd30
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:	0x50164A59 [Mon Jul 30 08:48:25 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:	87b3a93d03af93f2e664ed65d7224e1a

Entrypoint Preview

Instruction
push 00409D4Bh
ret
or al, FCh
adc al, ADh
xchg eax, ecx
mov esp, C114C940h
add ecx, dword ptr [edi-62h]
push edx
xchg eax, edx
jmp 00007F50B208EC5Fh
cmc
fldcw word ptr [edx-71h]
paddsw mm5, qword ptr [ebp+79725C5Dh]
aas
cmp bl, byte ptr [ecx+edi*2]
clc

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2a364	0x118	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x30000	0x1eb4	.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	0x5a0	.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
.text	0x1000	0x2b244	0x2b400	False	0.956478052746	data	7.96218490454	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x2d000	0x2054	0x400	False	0.2080078125	data	1.53050726795	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x30000	0x23f4	0x2400	False	0.709418402778	data	6.27055584577	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	HeapDestroy, HeapCreate, Thread32Next, ReadFile, GetTimeZoneInformation, MultiByteToWideChar, GetTempPathW, GetFileSizeEx, OpenMutexW, VirtualAlloc, VirtualProtectEx, VirtualAllocEx, FindClose, LoadLibraryA, RemoveDirectoryW, FindNextFileW, VirtualProtect, CreateToolhelp32Snapshot, GetFileTime, FileTimeToLocalFileTime, GetVolumeNameForVolumeMountPointW, DeleteFileW, GetFileInformationByHandle, GetSystemTime, WriteProcessMemory, GetNativeSystemInfo, GetThreadContext, GetProcessId, GetFileAttributesExW, GetCurrentThreadId, TlsGetValue, TlsSetValue, TerminateProcess, GetCommandLineW, SetErrorMode, GetComputerNameW, OpenEventW, DuplicateHandle, GetCurrentProcessId, GlobalLock, GlobalUnlock, GetLocalTime, MapViewOfFile, UnmapViewOfFile, CreateFileMappingW, TlsAlloc, TlsFree, CreateRemoteThread, Process32FirstW, Process32NextW, SetFileAttributesW, WTSGetActiveConsoleSessionId, ReadProcessMemory, VirtualFreeEx, WideCharToMultiByte, Thread32First, OpenProcess, VirtualQueryEx, SetFileTime, IsBadReadPtr, GetProcessHeap, lstrcmpiA, LoadLibraryW, VirtualFree, HeapFree, SetFilePointerEx, SystemTimeToFileTime, HeapAlloc, CreateProcessW, SetEndOfFile, FindFirstFileW, CreateMutexW, HeapReAlloc, GetTempFileNameW, FileTimeToDosDateTime, GetEnvironmentVariableW, LocalFree, SetThreadContext, GetVersionExW, CreateDirectoryW, FreeLibrary, ExitProcess, SetThreadPriority, GetCurrentThread, ExpandEnvironmentStringsW, GetUserDefaultUILanguage, lstrcmpiW, GetModuleFileNameW, Sleep, GetTickCount, MoveFileExW, ResetEvent, SetLastError, GetLastError, SetEvent, EnterCriticalSection, GetProcAddress, GetPrivateProfileIntW, FlushFileBuffers, CreateFileW, GetFileAttributesW, LeaveCriticalSection, InitializeCriticalSection, WriteFile, GetPrivateProfileStringW, GetModuleHandleW, CloseHandle, WaitForMultipleObjects, CreateEventW, ReleaseMutex, CreateThread, WaitForSingleObject
USER32.dll	SwitchDesktop, DefDlgProcA, DefMDIChildProcA, ReleaseCapture, RegisterClassW, CallWindowProcA, CallWindowProcW, GetMessagePos, DefFrameProcW, RegisterClassA, EndPaint, GetUpdateRgn, GetMessageW, GetWindowDC, FillRect, PostMessageW, GetWindowInfo, DefMDIChildProcW, BeginPaint, GetUpdateRect, IntersectRect, GetDCEx, PostThreadMessageW, EqualRect, PrintWindow, ToUnicode, DefWindowProcW, IsRectEmpty, CharLowerBuffA, CreateDesktopW, SetProcessWindowStation, GetWindowRect, GetParent, GetKeyboardState, GetClassLongW, GetAncestor, SetWindowPos, IsWindow, MapWindowPoints, RegisterWindowMessageW, GetMenuItemID, SetKeyboardState, GetSubMenu, MenuItemFromPoint, GetMenu, GetMenuItemRect, TrackPopupMenuEx, SystemParametersInfoW, GetClassNameW, GetMenuState, GetMenuItemCount, HiliteMenuItem, EndMenu, GetWindowThreadProcessId, CharLowerW, MapVirtualKeyW, DefWindowProcA, DrawIcon, GetShellWindow, DrawEdge, GetIconInfo, GetCursorPos, RegisterClassExA, SetCapture, GetSystemMetrics, ExitWindowsEx, DefDlgProcW, DefFrameProcA, OpenInputDesktop, GetCapture, GetThreadDesktop, CloseWindowStation, CreateWindowStationW, GetProcessWindowStation, OpenDesktopW, CloseDesktop, SetThreadDesktop, GetUserObjectInformationW, OpenWindowStationW, GetTopWindow, LoadImageW, MsgWaitForMultipleObjects, WindowFromPoint, GetDC, TranslateMessage, GetWindowLongW, CharLowerA, RegisterClassExW, SetCursorPos, GetClipboardData, PeekMessageA, SendMessageW, CharToOemW, DispatchMessageW, GetWindow, SendMessageTimeoutW, SetWindowLongW, CharUpperW, ReleaseDC, PeekMessageW, GetMessageA
ADVAPI32.dll	InitiateSystemShutdownExW, EqualSid, ConvertSidToStringSidW, CryptGetHashParam, OpenProcessToken, GetSidSubAuthority, CryptAcquireContextW, OpenThreadToken, GetSidSubAuthorityCount, GetTokenInformation, RegCreateKeyExW, CryptReleaseContext, RegQueryValueExW, CreateProcessAsUserW, InitializeSecurityDescriptor, SetSecurityDescriptorDacl, SetNamedSecurityInfoW, LookupPrivilegeValueW, CryptCreateHash, ConvertStringSecurityDescriptorToSecurityDescriptorW, RegOpenKeyExW, GetSecurityDescriptorSacl, SetSecurityDescriptorSacl, CryptDestroyHash, AdjustTokenPrivileges, RegCloseKey, RegSetValueExW, CryptHashData, IsWellKnownSid, GetLengthSid, RegEnumKeyExW
SHLWAPI.dll	PathQuoteSpacesW, PathRenameExtensionW, StrStrIW, StrStrIA, wvnsprintfA, StrCmpNIA, PathMatchSpecW, PathRemoveBackslashW, PathUnquoteSpacesW, PathAddExtensionW, PathCombineW, SHDeleteKeyW, PathSkipRootW, SHDeleteValueW, PathAddBackslashW, PathFindFileNameW, PathIsDirectoryW, wvnsprintfW, UrlUnescapeA, StrCmpNIW, PathIsURLW, PathRemoveFileSpecW
SHELL32.dll	ShellExecuteW, SHGetFolderPathW, CommandLineToArgvW
Secur32.dll	GetUserNameExW
ole32.dll	StringFromGUID2, CLSIDFromString, CoUninitialize, CoCreateInstance, CoInitializeEx
GDI32.dll	CreateCompatibleDC, SetRectRgn, SaveDC, DeleteDC, SetViewportOrgEx, RestoreDC, CreateDIBSection, GetDeviceCaps, GetDIBits, CreateCompatibleBitmap, GdiFlush, SelectObject, DeleteObject
WS2_32.dll	recv, sendto, select, getaddrinfo, recvfrom, getpeername, listen, send, WSASend, WSAIoctl, connect, WSAAddressToStringW, WSAStartup, shutdown, setsockopt, bind, socket, WSASetLastError, freeaddrinfo, WSAEventSelect, getsockname, accept, WSAGetLastError, closesocket
CRYPT32.dll	CertDuplicateCertificateContext, CertEnumCertificatesInStore, CertCloseStore, CertOpenSystemStoreW, CertDeleteCertificateFromStore, CryptUnprotectData, PFXImportCertStore, PFXExportCertStoreEx
WININET.dll	InternetQueryOptionA, InternetOpenA, HttpOpenRequestA, InternetSetOptionA, InternetCrackUrlA, InternetQueryOptionW, InternetConnectA, InternetCloseHandle, HttpSendRequestA, HttpAddRequestHeadersA, HttpAddRequestHeadersW, InternetSetStatusCallbackW, GetUrlCacheEntryInfoW, HttpSendRequestW, InternetReadFile, InternetReadFileExA, InternetQueryDataAvailable, HttpSendRequestExW, HttpQueryInfoA, HttpSendRequestExA
OLEAUT32.dll	VariantInit, SysAllocString, VariantClear, SysFreeString
NETAPI32.dll	NetApiBufferFree, NetUserEnum, NetUserGetInfo

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: 7FzERy9xWc.exe PID: 2788 Parent PID: 5724

General

Start time:	15:50:28
Start date:	11/04/2021
Path:	C:\Users\user\Desktop\7FzERy9xWc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\7FzERy9xWc.exe'
Imagebase:	0x400000
File size:	188928 bytes
MD5 hash:	8F250F634DE721FEC7B002A805DDDC24
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis