ID: 632531
Sample Name: support.exe
Cookbook: default.jbs
Time: 18:44:16
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

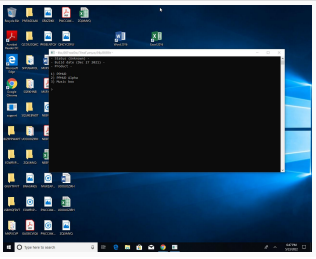
Windows Analysis Report

support.exe

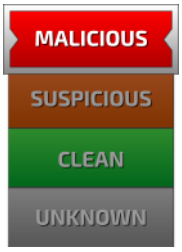
Overview

General Information

Sample Name:	support.exe
Analysis ID:	632531
MD5:	a2d24ba3b1c040..
SHA1:	ad9daad3cdfbe1..
SHA256:	348b351762c491..
Tags:	exe
Infos:	



Detection

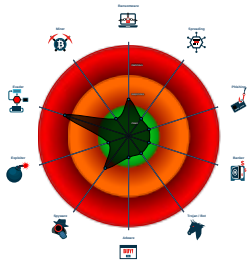


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Contains functionality to inject threa…
- Machine Learning detection for sam…
- Contains functionality to check if a d…
- Uses 32bit PE files
- Found a high number of Window / U…
- Queries the volume information (nam…
- Yara signature match
- Extensive use of GetProcAddress (…
- Contains functionality to check if a d…
- Contains functionality to read the PE…
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (

Classification



Process Tree

- **System is w10x64**
- support.exe (PID: 6060 cmdline: "C:\Users\user\Desktop\support.exe" MD5: A2D24BA3B1C040105083109B9912E223)
  - conhost.exe (PID: 2404 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.517890121.00000000003C5000.00000004.00000001.01000000.00000003.sdmp	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x76:$xo1:)\x15\x14\x0E]\x0D\x0F\x12\x1A\x0F\x1C\x10]\x1E\x1C\x13\x13\x12\x09]\x1F\x18]\x0F\x08\x13]\x14\x13]92.]\x10\x12\x19\x18
00000000.00000000.250484546.0000000000476000.00000008.00000001.01000000.00000003.sdmp	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x7e76:$xo1:)\x15\x14\x0E]\x0D\x0F\x12\x1A\x0F\x1C\x10]\x1E\x1C\x13\x13\x12\x09]\x1F\x18]\x0F\x08\x13]\x14\x13]92.]\x10\x12\x19\x18
00000000.00000002.518495863.0000000000476000.00000008.00000001.01000000.00000003.sdmp	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x7e76:$xo1:)\x15\x14\x0E]\x0D\x0F\x12\x1A\x0F\x1C\x10]\x1E\x1C\x13\x13\x12\x09]\x1F\x18]\x0F\x08\x13]\x14\x13]92.]\x10\x12\x19\x18
00000000.00000000.250216516.00000000003C5000.00000008.00000001.01000000.00000003.sdmp	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x76:$xo1:)\x15\x14\x0E]\x0D\x0F\x12\x1A\x0F\x1C\x10]\x1E\x1C\x13\x13\x12\x09]\x1F\x18]\x0F\x08\x13]\x14\x13]92.]\x10\x12\x19\x18

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

Anti Debugging

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

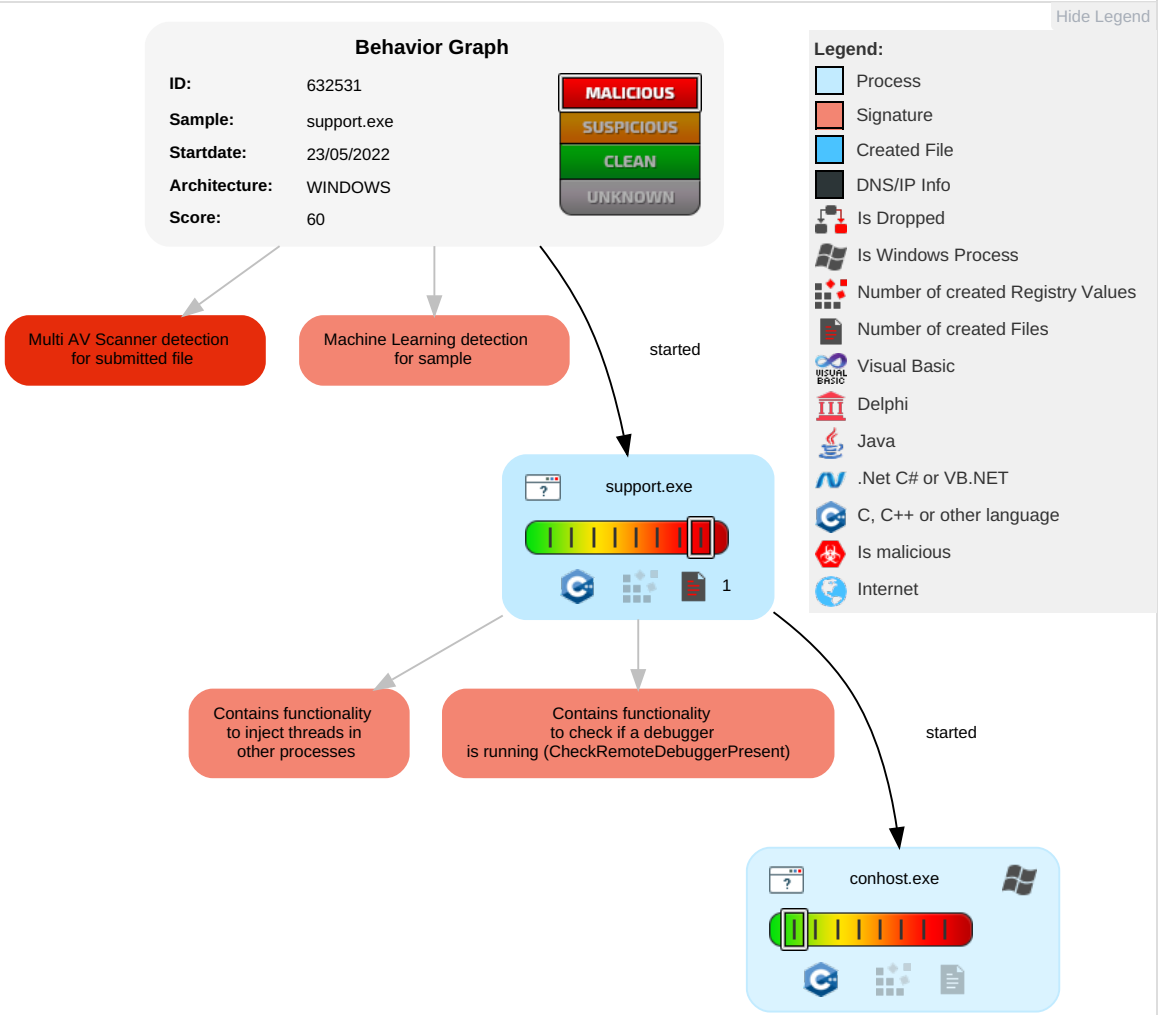
HIPS / PFW / Operating System Protection Evasion

Contains functionality to inject threads in other processes

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	Path Interception	1 Access Token Manipulation	2 Virtualization/Sandbox Evasion	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 1 Process Injection	1 Access Token Manipulation	LSASS Memory	1 2 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	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 1 Process Injection	Security Account Manager	2 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Obfuscated Files or Information	NTDS	1 Process 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 Application Window 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 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

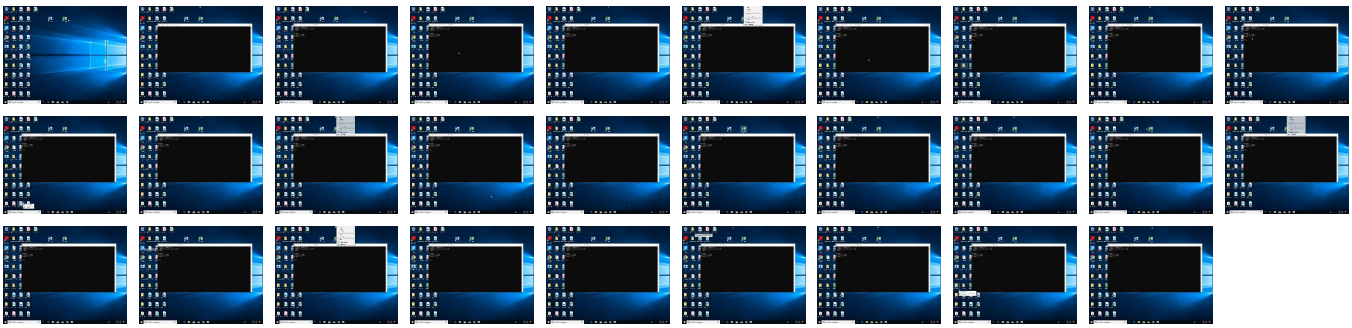
Behavior Graph



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
support.exe	60%	Virustotal		Browse
support.exe	24%	Metadefender		Browse
support.exe	68%	ReversingLabs	Win32.Trojan.GenericML	
support.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://www.exrock.com	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://vulpvibe.bandcamp.com/album/squaredance	support.exe	false		high
http://www.youtube.com/JamesPaddockMusic	support.exe	false		high
http://www.exrock.com	support.exe	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	632531
Start date and time: 23/05/202218:44:16	2022-05-23 18:44:16 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	support.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:	25
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:	mal60.evad.winEXE@2/1@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 82.2%) • Quality average: 40.9% • Quality standard deviation: 33.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.223.24.244

- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- 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

\Device\ConDrv

Process:	C:\Users\user\Desktop\support.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	118
Entropy (8bit):	4.611012807958004
Encrypted:	false
SSDEEP:	3:XdfLOSyod4nQIBFBdCFfFW1aBQSIovWv/tptE1nwobWyFuQyAov0:tB8xFB2fwamsOHt2WyFfye
MD5:	639D4A73EA7C12736FD64208AA50CBAA
SHA1:	8CFB31975C3EBF3EB4E31F8A827D832C80EDFE61
SHA-256:	A2BE64267B36E4AEDFDE03124CAB323AB6A998FDC6F4F99287B0459F7DF5EC29
SHA-512:	E2A0AD3BA1C86A46862FF6E24F8FE46C9990D0B6D9B9769EE623E631FA635A12DECD6CE3B5D62183BA706B3A000F1AE25C71AD7F09A52241BAB625A25E2CDBBA
Malicious:	false
Reputation:	low
Preview:	- Status (Unknown) -.. - Build date (Dec 27 2021) -.. - Product -.... 1) PPHUD.. 2) PPHUD Alpha.. 3) Music box.... >

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	6.833608978635711
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:	support.exe
File size:	3431424
MD5:	a2d24ba3b1c040105083109b9912e223
SHA1:	ad9daad3cdfbe1dacf4f077b98bb26f7af0854bd
SHA256:	348b351762c491c5d02cdfdf34d51faf67024f8f492ed46316d2adda6aac7412
SHA512:	6482efb73080840fde2e26e3137243dc73dcb12bd48db9722280c4f093e257afe65af91a2a1d7c83d8b0829b8933e05c0dfbfbf89d83021d329372e89f865c5f
SSDEEP:	49152:fym8dnvafFKnfyWDx2O52V3LZ4WtgDkPXqJ5O/srX3LochcQBPBPPhZBPBPPhZBn:6m8dvafFKfP93MF4WeDeX0oU0Qc
TLSH:	93F58D65025ABFE8CE37A5F110B6DF1E71E075FA4439AAAC4C95D4F173A00608C35AAF
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s... ... .c ... ...!... ...!... ...!... ...!... ...!... ... ... u..!... u.. ... u..!... Rich... .....PE..L...$..a...

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40eb61
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61C9B824 [Mon Dec 27 12:57:08 2021 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:	9f9653573673d8f6615fcab81ba51787

Entrypoint Preview

Instruction
call 00007F57D4F9C710h
jmp 00007F57D4F9BF49h
push ebp
mov ebp, esp
push 00000000h
call dword ptr [00411090h]
push dword ptr [ebp+08h]
call dword ptr [0041108Ch]
push C0000409h
call dword ptr [0041102Ch]
push eax
call dword ptr [00411094h]

Instruction
pop ebp
ret
push ebp
mov ebp, esp
sub esp, 00000324h
push 00000017h
call 00007F57D4F9C8B3h
test eax, eax
je 00007F57D4F9C0D7h
push 00000002h
pop ecx
int 29h
mov dword ptr [007460A0h], eax
mov dword ptr [0074609Ch], ecx
mov dword ptr [00746098h], edx
mov dword ptr [00746094h], ebx
mov dword ptr [00746090h], esi
mov dword ptr [0074608Ch], edi
mov word ptr [007460B8h], ss
mov word ptr [007460ACh], cs
mov word ptr [00746088h], ds
mov word ptr [00746084h], es
mov word ptr [00746080h], fs
mov word ptr [0074607Ch], gs
pushfd
pop dword ptr [007460B0h]
mov eax, dword ptr [ebp+00h]
mov dword ptr [007460A4h], eax
mov eax, dword ptr [ebp+04h]
mov dword ptr [007460A8h], eax
lea eax, dword ptr [ebp+08h]
mov dword ptr [007460B4h], eax
mov eax, dword ptr [ebp-00000324h]
mov dword ptr [00745FF0h], 00010001h

Rich Headers

Programming Language:	• [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1375c	0x12c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x347000	0x1e8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x348000	0xf00	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x12040	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x12118	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x12078	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x11000	0x2b4	.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	0xf441	0xf600	False	0.507637830285	data	6.47898584689	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x11000	0x3e9c	0x4000	False	0.454711914062	data	5.62734968604	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x15000	0x3313a4	0x331000	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x347000	0x1e8	0x200	False	0.5390625	data	4.7720374017	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x348000	0xf00	0x1000	False	0.791748046875	data	6.50058963945	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x347060	0x188	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	GetStdHandle, CreateToolhelp32Snapshot, Sleep, Process32Next, CloseHandle, FillConsoleOutputAttribute, SetConsoleCursorPosition, GetCurrentProcess, GetModuleHandleA, GetTickCount64, LoadLibraryA, SetConsoleTitleA, GetProcAddress, IsDebuggerPresent, CheckRemoteDebuggerPresent, SetLastError, Module32Next, Module32First, GetExitCodeProcess, WaitForSingleObject, SetEvent, CreateEventA, GetModuleFileNameA, GetConsoleScreenBufferInfo, Process32First, CreateThread, FillConsoleOutputCharacterA, InitializeCriticalSectionAndSpinCount, DeleteCriticalSection, CreateEventW, GetModuleHandleW, UnhandledExceptionFilter, SetUnhandledExceptionFilter, TerminateProcess, IsProcessorFeaturePresent, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead
ADVAPI32.dll	LookupPrivilegeValueA, OpenProcessToken, AdjustTokenPrivileges
MSVCP140.dll	?put@?$basic_ostream@DU?$char_traits@D@std@@@std@@QAEAAV12@D@Z, ?flush@?$basic_ostream@DU?$char_traits@D@std@@@std@@QAEAAV12@XZ, ?sgetc@?$basic_streambuf@DU?$char_traits@D@std@@@std@@QAEHXZ, ?sputc@?$basic_streambuf@DU?$char_traits@D@std@@@std@@QAEHD@Z, ??6?$basic_ostream@DU?$char_traits@D@std@@@std@@QAEAAV01@P6AAAV01@AAV01@@Z@Z, ?getloc@ios_base@std@@QBE?AVlocale@2@XZ, ?_Getcat@?$ctype@D@std@@SAIPAPBVfacet@locale@2@PBV42@@Z, ??Bid@locale@std@@QAEIXZ, ?widen@?$basic_ios@DU?$char_traits@D@std@@@std@@QBEDD@Z, ?_Fiopen@std@@YAPAU_iobuf@@PBDHH@Z, ?_Getcat@?$codecvt@DDU_Mbstatet@@@std@@SAIPAPBVfacet@locale@2@PBV42@@Z, ??0?$basic_streambuf@DU?$char_traits@D@std@@@std@@IAE@XZ, ?getloc@?$basic_streambuf@DU?$char_traits@D@std@@@std@@QBE?AVlocale@2@XZ, ??0?$basic_ios@DU?$char_traits@D@std@@@std@@IAE@XZ, ?_Init@?$basic_streambuf@DU?$char_traits@D@std@@@std@@IAEXXZ, ??0?$basic_ostream@DU?$char_traits@D@std@@@std@@QAE@PAV?$basic_streambuf@DU?$char_traits@D@std@@@1@_N@Z, ?unshift@?$codecvt@DDU_Mbstatet@@@std@@QBEHAAU_Mbstatet@@PAD1AAPAD@Z, ?_Pninc@?$basic_streambuf@DU?$char_traits@D@std@@@std@@IAEPADXZ, ?in@?$codecvt@DDU_Mbstatet@@@std@@QBEHAAU_Mbstatet@@PBD1AAPBDPAD3AAPAD@Z, ?out@?$codecvt@DDU_Mbstatet@@@std@@QBEHAAU_Mbstatet@@PBD1AAPBDPAD3AAPAD@Z, ??1?$basic_ios@DU?$char_traits@D@std@@@std@@UAE@XZ, ??1?$basic_streambuf@DU?$char_traits@D@std@@@std@@UAE@XZ, ?showmanyc@?$basic_streambuf@DU?$char_traits@D@std@@@std@@MAE_JXZ, ?xsgetn@?$basic_streambuf@DU?$char_traits@D@std@@@std@@MAE_JPAD_J@Z, ?xsputn@?$basic_streambuf@DU?$char_traits@D@std@@@std@@MAE_JPBD_J@Z, ??1?$basic_ostream@DU?$char_traits@D@std@@@std@@UAE@XZ, ?always_noconv@codecvt_base@std@@QBE_NXZ, ?sputn@?$basic_streambuf@DU?$char_traits@D@std@@@std@@QAE_JPBD_J@Z, ??1_Lockit@std@@QAE@XZ, ??0_Lockit@std@@QAE@H@Z, ?setstate@?$basic_ios@DU?$char_traits@D@std@@@std@@QAEXH_N@Z, ?_Osfx@?$basic_ostream@DU?$char_traits@D@std@@@std@@QAEXXZ, ?cout@std@@3V?$basic_ostream@DU?$char_traits@D@std@@@1@A, ?snextc@?$basic_streambuf@DU?$char_traits@D@std@@@std@@QAEHXZ, ?_Ipfx@?$basic_istream@DU?$char_traits@D@std@@@std@@QAE_N_N@Z, ?_Xlength_error@std@@YAXPBD@Z, ?id@?$ctype@D@std@@2V0locale@2@A, ?_Xout_of_range@std@@YAXPBD@Z, ?cin@std@@3V?$basic_istream@DU?$char_traits@D@std@@@1@A, ?uncaught_exception@std@@YA_NXZ, ?_Getgloballocale@locale@std@@CAPAV_Locimp@12@XZ, ?id@?$codecvt@DDU_Mbstatet@@@std@@2V0locale@2@A
WININET.dll	HttpSendRequestA, InternetConnectA, InternetReadFile, InternetOpenA, HttpOpenRequestA, InternetCloseHandle

DLL	Import
WINMM.dll	midiStreamClose, midiOutShortMsg, midiStreamRestart, midiOutReset, midiStreamProperty, midiStreamOpen, midiStreamStop, midiOutUnprepareHeader, midiStreamOut, midiOutPrepareHeader
VCRUNTIME140.dll	memcpy, __CxxFrameHandler3, __std_exception_destroy, __std_exception_copy, memchr, strstr, _CxxThrowException, _except_handler4_common, memset, __std_terminate, memmove
api-ms-win-crt-utility-l1-1-0.dll	rand, srand
api-ms-win-crt-time-l1-1-0.dll	_localtime64, _time64
api-ms-win-crt-stdio-l1-1-0.dll	ungetc, setvbuf, fgetpos, fsetpos, fwrite, __p__commode, _set_fmode, fgetc, fclose, fflush, fputc, fread, _get_stream_buffer_pointers, getchar, _fseeki64
api-ms-win-crt-runtime-l1-1-0.dll	_set_app_type, _get_initial_narrow_environment, _initterm_e, _register_onexit_function, _exit, _initialize_onexit_table, _seh_filter_exe, __p___argv, _c_exit, _register_thread_local_exe_atexit_callback, _cexit, _initterm, _initialize_narrow_environment, _configure_narrow_argv, _controlfp_s, terminate, __p___argc, _crt_atexit, _invalid_parameter_noinfo_noreturn, exit
api-ms-win-crt-heap-l1-1-0.dll	free, _callnewh, _set_new_mode, malloc
api-ms-win-crt-filesystem-l1-1-0.dll	_unlock_file, _lock_file
api-ms-win-crt-math-l1-1-0.dll	__setusermatherr
api-ms-win-crt-locale-l1-1-0.dll	_configthreadlocale

Possible Origin

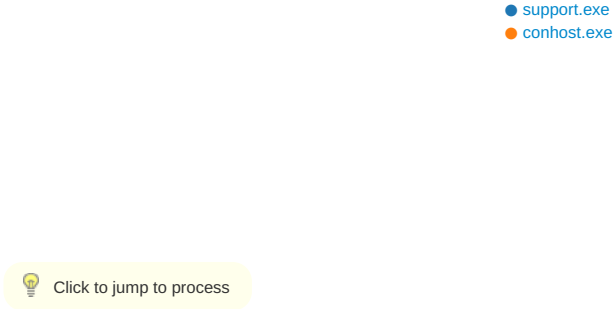
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: support.exe PID: **6060**, Parent PID: **5964**

General

Target ID:	0
Start time:	18:45:26
Start date:	23/05/2022
Path:	C:\Users\user\Desktop\support.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\support.exe"
Imagebase:	0x3b0000
File size:	3431424 bytes
MD5 hash:	A2D24BA3B1C040105083109B9912E223
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000000.00000002.517890121.00000000003C5000.00000004.00000001.01000000.00000003.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000000.00000000.250484546.0000000000476000.00000008.00000001.01000000.00000003.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000000.00000002.518495863.0000000000476000.00000008.00000001.01000000.00000003.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000000.00000000.250216516.00000000003C5000.00000008.00000001.01000000.00000003.sdmp, Author: Florian Roth
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **2404**, Parent PID: **6060**

General

Target ID:	1
Start time:	18:45:27
Start date:	23/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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