



ID: 372989
Sample Name:
ciscovideoguard.exe
Cookbook: default.jbs
Time: 16:35:47
Date: 22/03/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report ciscovideoguard.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 9
General 9
File Icon 10
Static PE Info 10
General 10
Authenticode Signature 10
Entrypoint Preview 10
Rich Headers 12
Data Directories 12
Sections 12
Resources 13
Imports 13
Exports 14
Version Infos 14
Possible Origin 14
Network Behavior 14
Code Manipulations 15
Statistics 15
Behavior 15
System Behavior 15

Copyright Joe Security LLC 2021

Analysis Process: ciscovideoguard.exe PID: 7164 Parent PID: 5996 15
General 15
File Activities 15
Analysis Process: conhost.exe PID: 4824 Parent PID: 7164 15
General 15
Disassembly 16
Code Analysis 16

Copyright Joe Security LLC 2021

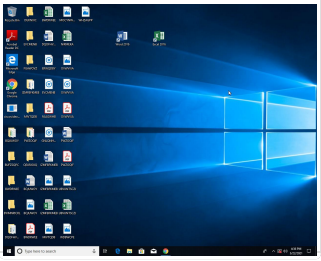
Analysis Report ciscovideoguard.exe

Overview

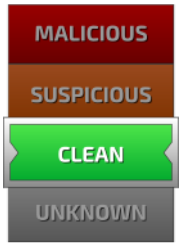
General Information

Sample Name:	ciscovideoguard.exe
Analysis ID:	372989
MD5:	01eb1a2e5fc8d46.
SHA1:	e5b76b9344ebe7..
SHA256:	40c71df5baff986…
Infos:	

Most interesting Screenshot:



Detection

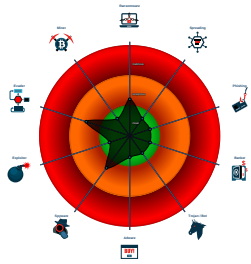


Score:	5
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Contains functionality to check if a d…
- Contains functionality to check if a d…
- Contains functionality to query locale…
- Contains functionality which may be…
- Creates a DirectInput object (often fo…
- Detected potential crypto function
- Program does not show much activi…
- Tries to load missing DLLs
- Uses 32bit PE files
- Uses code obfuscation techniques (…

Classification



Startup

- **System is w10x64**
- ciscovideoguard.exe (PID: 7164 cmdline: 'C:\Users\user\Desktop\ciscovideoguard.exe' MD5: 01EB1A2E5FC8D464431A34AB5E28255C)
  - conhost.exe (PID: 4824 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

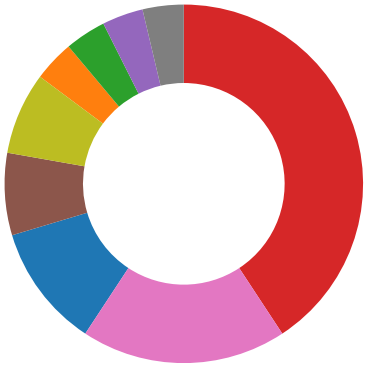
Sigma Overview

No Sigma rule has matched

Signature Overview

- Compliance
- Networking

Copyright Joe Security LLC 2021



- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

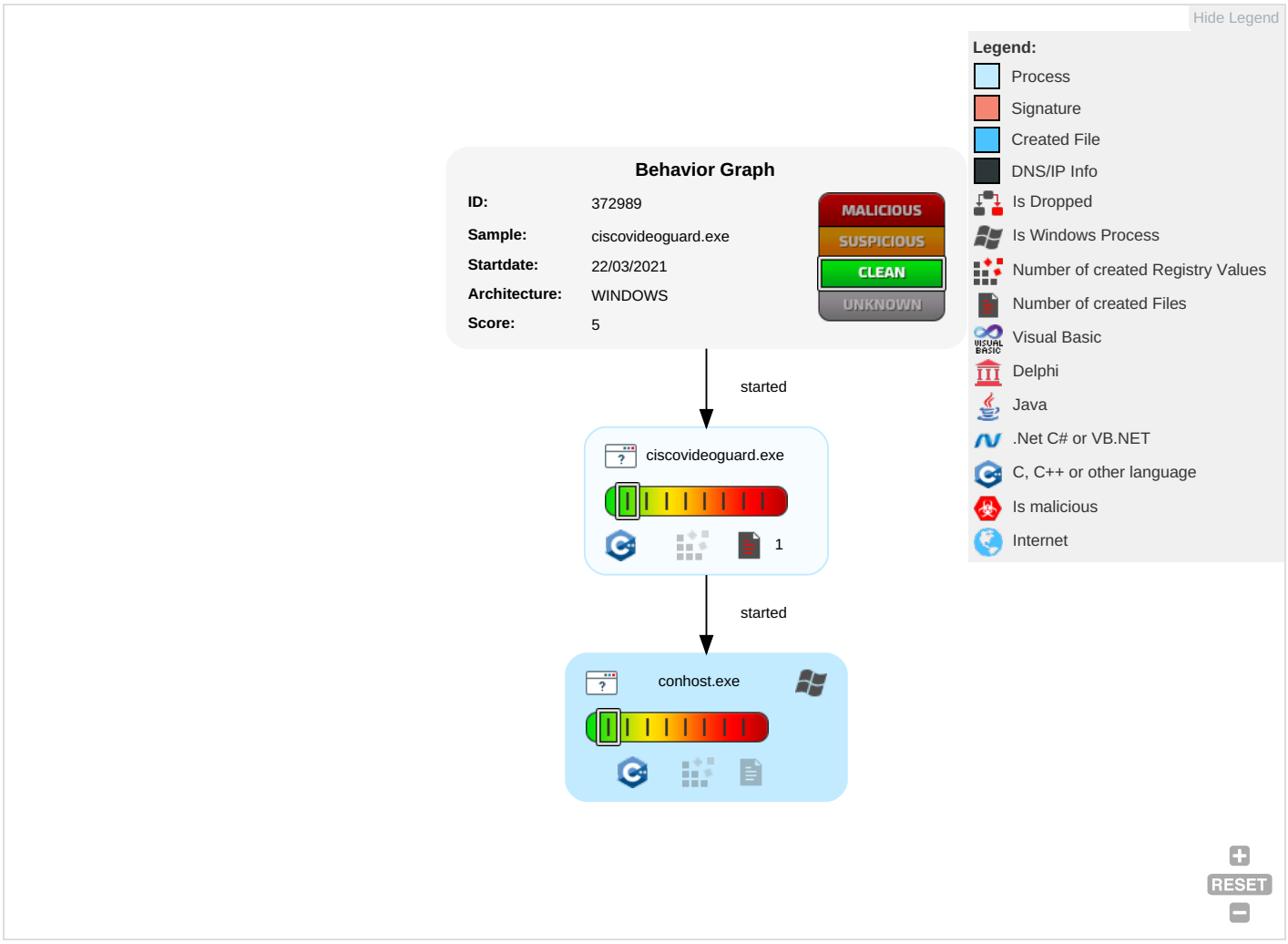
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

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	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 1	Process Injection 1	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	DLL Side-Loading 1	LSASS Memory	Security Software Discovery 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	System Information Discovery 1 3	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

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Copyright Joe Security LLC 2021



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ciscovideoguard.exe	0%	Virustotal		Browse
ciscovideoguard.exe	0%	Metadefender		Browse
ciscovideoguard.exe	2%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.thawte.com/ThawteTimestampingCA.crl0	ciscovideoguard.exe	false		high
http://www.symauth.com/cps0(	ciscovideoguard.exe	false		high
http://www.symauth.com/rpa00	ciscovideoguard.exe	false		high
http://ocsp.thawte.com0	ciscovideoguard.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	372989
Start date:	22.03.2021
Start time:	16:35:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ciscovideoguard.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:	4
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:	CLEAN
Classification:	clean5.winEXE@2/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 93.7%) • Quality average: 78% • Quality standard deviation: 29.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Copyright Joe Security LLC 2021

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, svchost.exe • Execution Graph export aborted for target ciscovideoguard.exe, PID 7164 because there are no executed function

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:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	5.81979014038173
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:	ciscovideoguard.exe
File size:	1074416
MD5:	01eb1a2e5fc8d464431a34ab5e28255c

Copyright Joe Security LLC 2021

General

SHA1:	e5b76b9344ebe7f90aaa38aa1ec9962fdce3cafb
SHA256:	40c71df5baff986e7ce4e668e3d6bd8f5e149c7c479f97ebc47d7f1bc4a3c33c
SHA512:	9ddf849c3617896836aa94c5c7b39c74f95cb288a27d07b382a7c45bc0c3b290e7499e7445511551c881ccf11f377b79dcdbf15adfe5121d0355f00a3441fefb
SSDEEP:	12288:hAWwvNhXOX+mYESA4i/W/nSyIyFuPxH3tYLQhvB4f9gJAhPxMg4/PNjED/UoVex1:jwvNhXOXPpmPFuRtY4Z4fPxMvnNjgcx1
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....q0...c...c...c.!.c...c...c...c...c...cY..c8..c...cP~.c...c...cE..c8..c...c8..c...c...c...c8..c...c Rich...c.....PE..L..

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4611a5
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5B53B952 [Sat Jul 21 22:53:06 2018 UTC]
TLS Callbacks:	0x459800
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:	1b55c4f365c89fe7c8c9a2fdf8146547

Authenticode Signature

Signature Valid:	**true**
Signature Issuer:	CN=Symantec Class 3 SHA256 Code Signing CA, OU=Symantec Trust Network, O=Symantec Corporation, C=US
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 5/2/2018 2:00:00 AM 6/3/2021 1:59:59 AM
Subject Chain	• CN=Cisco Video Technologies Israel Ltd., O=Cisco Video Technologies Israel Ltd., L=Jerusalem, S=Israel, C=IL
Version:	3
Thumbprint MD5:	D8DE15DBDA95401A15B581DC4DB60D44
Thumbprint SHA-1:	C08DAD2700F46A025A9750F3D40CEB84E76B1ECC
Thumbprint SHA-256:	EB025069CC593AC490356CDD1A3A9DDDEBC4C35B25A37F1FED4F7C0176CD662D
Serial:	14DF0863FB064CA7FC83894D5ED4DD29

Entrypoint Preview

Instruction
call 00007F1F749BF992h
jmp 00007F1F749B0AFAh
push ebp
mov ebp, esp
push esi
call 00007F1F749BFAADh
mov esi, eax
test esi, esi
je 00007F1F749B0CD5h
push dword ptr [ebp+08h]

Instruction
push esi
call 00007F1F749B0CD2h
neg eax
pop ecx
sbb eax, eax
not eax
pop ecx
and eax, esi
pop esi
pop ebp
ret
push ebp
mov ebp, esp
sub esp, 18h
and dword ptr [ebp-04h], 00000000h
mov eax, dword ptr [ebp+08h]
push esi
test eax, eax
jne 00007F1F749B0CD8h
call 00007F1F749B46C9h
push 00000016h
pop esi
mov dword ptr [eax], esi
call 00007F1F749BBCF9h
mov eax, esi
jmp 00007F1F749B0EC3h
push 00000024h
push 000000FFh
push eax
call 00007F1F749B054Ch
mov eax, dword ptr [ebp+0Ch]
add esp, 0Ch
test eax, eax
je 00007F1F749B0C95h
push ebx
mov ebx, dword ptr [eax]
mov eax, dword ptr [eax+04h]
mov dword ptr [ebp-14h], eax
cmp eax, FFFFFFFFh
jnle 00007F1F749B0CCCh
jl 00007F1F749B0CDBh
cmp ebx, FFFF5740h
jc 00007F1F749B0CD3h
push 00000007h
pop ecx
cmp eax, ecx
jl 00007F1F749B0CDDh
jnle 00007F1F749B0CCAh
cmp ebx, 934126CFh
jbe 00007F1F749B0CD3h
call 00007F1F749B4673h
push 00000016h
pop esi
mov dword ptr [eax], esi
mov eax, esi
jmp 00007F1F749B0E71h
push edi
push 00000000h
push 01E13380h
push eax
push ebx
call 00007F1F749B0E69h
add eax, 46h
mov ecx, 00000190h

Instruction
mov dword ptr [ebp-08h], eax
push 00000064h
pop edi
lea esi, dword ptr [eax-01h]

Rich Headers

Programming Language:	• [C++] VS2013 UPD5 build 40629 • [C] VS2013 build 21005 • [LNK] VS2013 UPD5 build 40629 • [EXP] VS2013 UPD5 build 40629 • [IMP] VS2013 UPD5 build 40629 • [C++] VS2013 build 21005 • [ASM] VS2013 build 21005 • [RES] VS2013 build 21005

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0xf5350	0x2c5	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0xfd4bc	0x8c	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x101000	0x4b8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x104800	0x1cf0	.reloc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x102000	0x7fd8	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xe41a4	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xe0450	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xfd000	0x4bc	.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	0xca79f	0xca800	False	0.343883825231	data	5.69751401426	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xcc000	0x29615	0x29800	False	0.35505106363	data	4.3374442412	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xf6000	0x6d50	0x4400	False	0.189165900735	data	3.97572058422	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0xfd000	0x209c	0x2200	False	0.305606617647	data	4.93464353767	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tls	0x100000	0x202	0x400	False	0.0166015625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Copyright Joe Security LLC 2021

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x101000	0x4b8	0x600	False	0.380208333333	data	4.60852746093	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x102000	0x926c	0x9400	False	0.600506756757	data	6.21661739735	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x1010a0	0x2d0	data	English	United States
RT_MANIFEST	0x101370	0x145	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	GetTempPathW, SetFileTime, SetFileAttributesW, SetEndOfFile, RemoveDirectoryW, GetFullPathNameW, GetFileTime, GetFileInformationByHandle, GetFileAttributesExW, GetFileAttributesW, GetDiskFreeSpaceExW, FindNextFileW, FindFirstFileW, FindClose, DeleteFileW, CreateDirectoryW, GetCurrentDirectoryW, SetCurrentDirectoryW, OutputDebugStringA, DeviceIoControl, CreateDirectoryExW, CopyFileW, MoveFileExW, FileTimeToLocalFileTime, PeekNamedPipe, FileTimeToSystemTime, CreateEventA, SetEvent, CloseHandle, GetStartupInfoA, GetCurrentThreadId, VerSetConditionMask, GetLastError, WaitForSingleObject, CreateEventW, GetSystemTimeAsFileTime, VerifyVersionInfoW, GetProcAddress, GetModuleHandleA, GetTickCount, HeapAlloc, HeapFree, GetProcessHeap, OpenProcess, WaitForMultipleObjects, DuplicateHandle, ReleaseSemaphore, WaitForSingleObjectEx, GetCurrentProcess, CreateSemaphoreA, PostQueuedCompletionStatus, EnterCriticalSection, LeaveCriticalSection, TlsAlloc, TlsFree, GetSystemInfo, CreateFileA, WriteFile, GetModuleHandleW, LocalFree, FormatMessageW, SetConsoleCtrlHandler, SetLastError, CreateIoCompletionPort, GetQueuedCompletionStatus, InitializeCriticalSectionAndSpinCount, DeleteCriticalSection, SleepEx, SetWaitableTimer, QueueUserAPC, TerminateThread, TlsGetValue, TlsSetValue, GetModuleFileNameW, GetModuleHandleExW, MultiByteToWideChar, WideCharToMultiByte, EncodePointer, DecodePointer, GetStringTypeW, CreateEventExW, OpenEventW, WaitForMultipleObjectsEx, Sleep, GetCurrentProcessId, ResetEvent, ResumeThread, GetLogicalProcessorInformation, CreateWaitableTimerA, SystemTimeToFileTime, AreFileApisANSI, ExitProcess, RaiseException, RtlUnwind, GetCommandLineA, CreateThread, ExitThread, LoadLibraryExW, FatalAppExitA, GetCPInfo, UnhandledExceptionFilter, SetUnhandledExceptionFilter, TerminateProcess, GetStartupInfoW, CreateSemaphoreW, IsProcessorFeaturePresent, GetDateFormatW, GetTimeFormatW, CompareStringW, LCMapStringW, GetLocaleInfoW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, HeapSize, IsDebuggerPresent, GetStdHandle, FreeLibrary, IsValidCodePage, GetACP, GetOEMCP, GetCurrentThread, GetFileType, GetModuleFileNameA, QueryPerformanceCounter, GetEnvironmentStringsW, FreeEnvironmentStringsW, HeapReAlloc, FlushFileBuffers, GetConsoleCP, GetConsoleMode, ReadFile, SetFilePointerEx, GetTimeZoneInformation, OutputDebugStringW, SetStdHandle, WriteConsoleW, ReadConsoleW, CreateFileW, SetEnvironmentVariableA, LoadLibraryW, SetProcessShutdownParameters
USER32.dll	ReleaseDC, TranslateMessage, DispatchMessageA, PostThreadMessageA, SetWindowRgn, GetWindowThreadProcessId, MonitorFromWindow, GetDC, GetMessageA

Copyright Joe Security LLC 2021

DLL	Import
PCShowServer.dll	?setActiveBrand@VgkConfig@@SAXABV?$basic_string@DU?$char_traits@D@std@@V?$allocator@D@2@@std@@@Z, ??0PCShowServer@@QAE@XZ, ??1PCShowServer@@UAE@XZ, ?init@PCShowServer@@UAEXAAV?$basic_string@DU?$char_traits@D@std@@V?$allocator@D@2@@std@@_N@Z, ?init@PCShowServer@@UAEXHHAAV?$basic_string@DU?$char_traits@D@std@@V?$allocator@D@2@@std@@_N@Z, ?sendMessage@PCShowServer@@UAEXABV?$basic_string@DU?$char_traits@D@std@@V?$allocator@D@2@@std@@@Z, ?setMessageCallback@PCShowServer@@UAEXP6AXPBD@Z@Z, ?setVideoWindowHandle@PCShowServer@@UAEXPAX@Z, ?terminate@PCShowServer@@UAEXXZ, ?getConnClosedSync@@YAPAVSynchronizer@util@nds@@XZ, ?getFD@LogStore@util@nds@@SA?AV?$shared_ptr@U?$pair@HV?$shared_ptr@Vrecursive_mutex@boost@@@boost@@@std@@@boost@@PBD@Z, ?writeStr@LogStore@util@nds@@SAJV?$shared_ptr@U?$pair@HV?$shared_ptr@Vrecursive_mutex@boost@@@boost@@@std@@@boost@@PBD@Z, ?isOpen@LogStore@util@nds@@SA_NV?$shared_ptr@U?$pair@HV?$shared_ptr@Vrecursive_mutex@boost@@@boost@@@std@@@boost@@@Z, ??0PropertiesFile@@QAE@ABV?$basic_string@DU?$char_traits@D@std@@V?$allocator@D@2@@std@@_N1@Z, ??0PropertiesFile@@QAE@AAV?$basic_istream@DU?$char_traits@D@std@@@std@@@Z, ??1PropertiesFile@@QAE@XZ, ?optionalString@VgkConfig@@SA?AV?$shared_ptr@V?$basic_string@DU?$char_traits@D@std@@V?$allocator@D@2@@std@@@boost@@ABV?$basic_string@DU?$char_traits@D@std@@V?$allocator@D@2@@std@@0@Z, ?optionalInt@VgkConfig@@SAHABV?$basic_string@DU?$char_traits@D@std@@V?$allocator@D@2@@std@@HHH_N@Z, ?optionalBool@VgkConfig@@SA_NABV?$basic_string@DU?$char_traits@D@std@@V?$allocator@D@2@@std@@_N@Z, ?getProjectString@VgkConfig@@SAABV?$basic_string@DU?$char_traits@D@std@@V?$allocator@D@2@@std@@XZ
WS2_32.dll	WSASendTo, WSASocketW, WSASend, freeaddrinfo, WSARecvFrom, WSAGetLastError, WSASetLastError, setsockopt, select, ioctlsocket, closesocket, WSACleanup, getaddrinfo, WSAStartup
GDI32.dll	GetDeviceCaps, ExtCreateRegion, EqualRgn, DeleteObject, CreateRectRgn, CombineRgn, GetRegionData
ADVAPI32.dll	RegQueryValueExA, ConvertStringSecurityDescriptorToSecurityDescriptorW, SetSecurityInfo, GetSecurityDescriptorSacl, SetSecurityDescriptorDacl, InitializeSecurityDescriptor, RegCloseKey, RegCreateKeyExA

Exports

Name	Ordinal	Address
??0AppConfig@@AAE@AAV?$basic_istream@DU?$char_traits@D@std@@@std@@@Z	1	0x4358e0
??0AppConfig@@AAE@ABV?$basic_string@DU?$char_traits@D@std@@V?$allocator@D@2@@std@@_N1@Z	2	0x435910
??0LogStore@util@nds@@QAE@XZ	3	0x435b40
??1AppConfig@@QAE@XZ	4	0x435f40
??1VgkConfig@@QAE@XZ	5	0x436090
?MAX_LINE@PropertiesFile@@2IB	6	0x4ce3a8

Version Infos

Description	Data
LegalCopyright	Copyright<A9> 2009-2018, Cisco
InternalName	CiscoVideoGuard
FileVersion	11,5,0x11dce5da,1107
ProductName	VideoGuard
ProductVersion	11, 5
FileDescription	Cisco VideoGuard
OriginalFilename	CiscoVideoGuard.exe
Translation	0x0409 0x04b0

Possible Origin

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

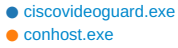
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: ciscovideoguard.exe PID: 7164 Parent PID: 5996

General

Start time:	16:36:30
Start date:	22/03/2021
Path:	C:\Users\user\Desktop\ciscovideoguard.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ciscovideoguard.exe'
Imagebase:	0x8f0000
File size:	1074416 bytes
MD5 hash:	01EB1A2E5FC8D464431A34AB5E28255C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Sy

Analysis Process: conhost.exe PID: 4824 Parent PID: 7164

General

Start time:	16:36:30
Start date:	22/03/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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

Code Analysis

Copyright Joe Security LLC 2021