ID: 338151
Sample Name: Coopera.exe
Cookbook: default.jbs
Time: 18:11:01
Date: 11/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

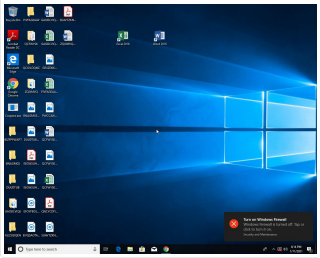
Analysis Report Coopera.exe

Overview

General Information

Sample Name:	Coopera.exe
Analysis ID:	338151
MD5:	e6ed395de0f1e8a.
SHA1:	0029721036587c..
SHA256:	78789f0a216d91b.

Most interesting Screenshot:



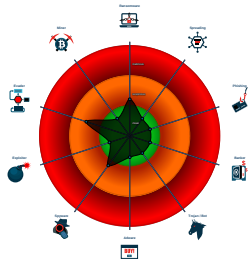
Detection

Score:	6
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…
- Detected potential crypto function
- Found potential string decryption / a…
- PE file contains sections with non-s…
- Program does not show much activi…
- Tries to load missing DLLs
- Uses 32bit PE files
- Uses Microsoft's Enhanced Cryptog…
- Uses code obfuscation techniques (…

Classification



Startup

- **System is w10x64**
- Coopera.exe (PID: 5276 cmdline: 'C:\Users\user\Desktop\Coopera.exe' MD5: E6ED395DE0F1E8A1CE346506452609F1)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

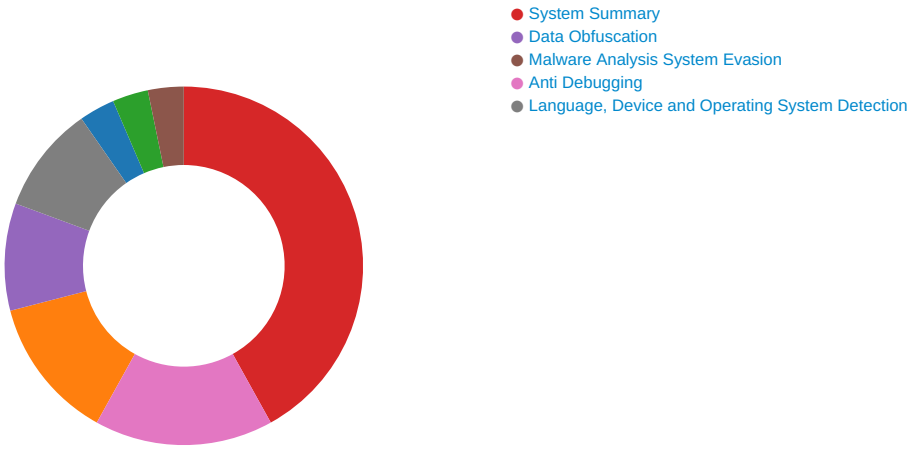
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- Cryptography
- Compliance
- Networking



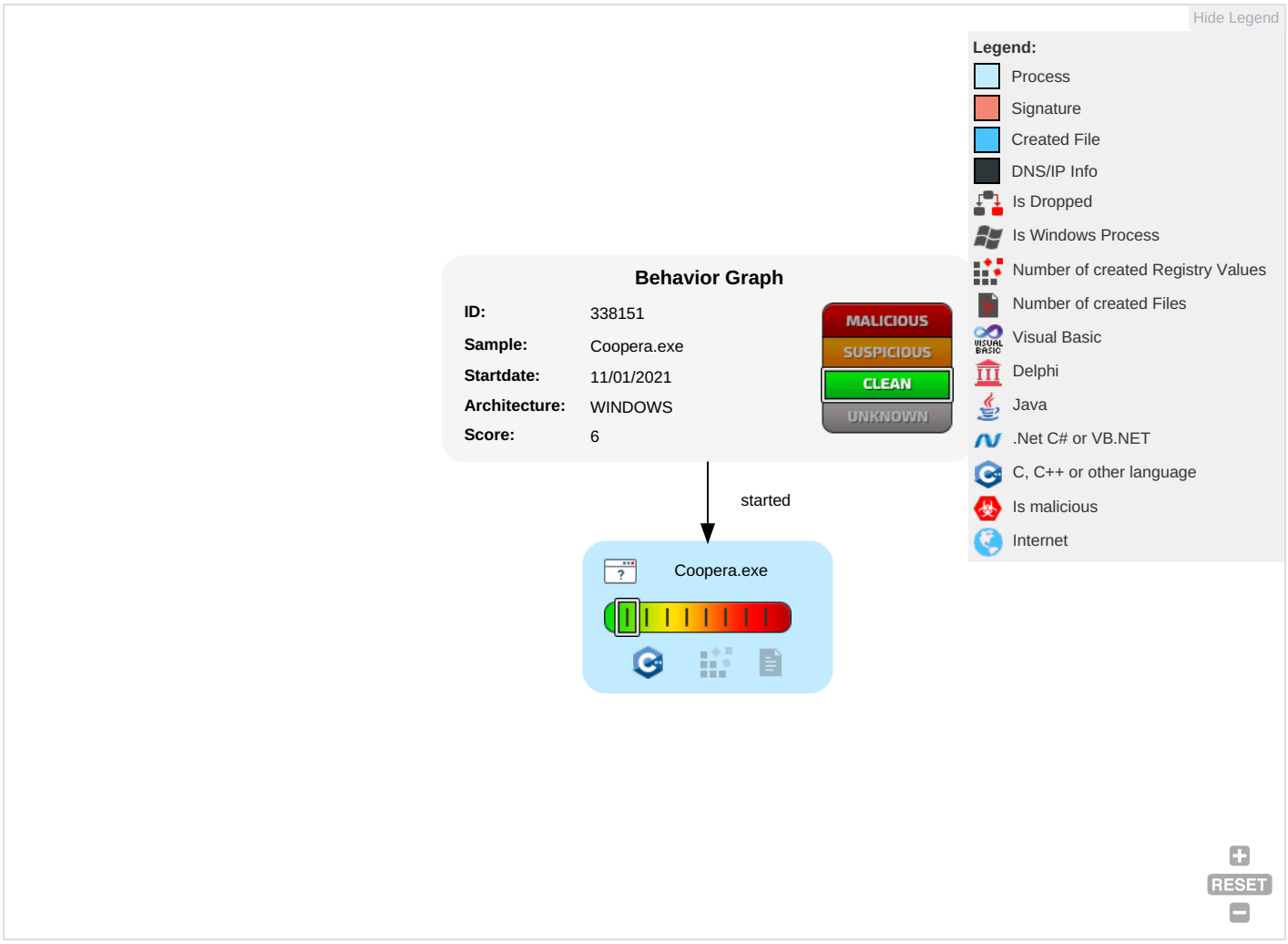
Click to jump to signature section

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	Remo Servi Effec
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	Access Token Manipulation 1	Access Token Manipulation 1	OS Credential Dumping	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remo Track Witho Autho
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Software Packing 1	LSASS Memory	Security Software Discovery 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remo Wipe Witho Autho
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	System Information Discovery 1 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtai Devic Cloud Backu
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	DLL Side-Loading 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

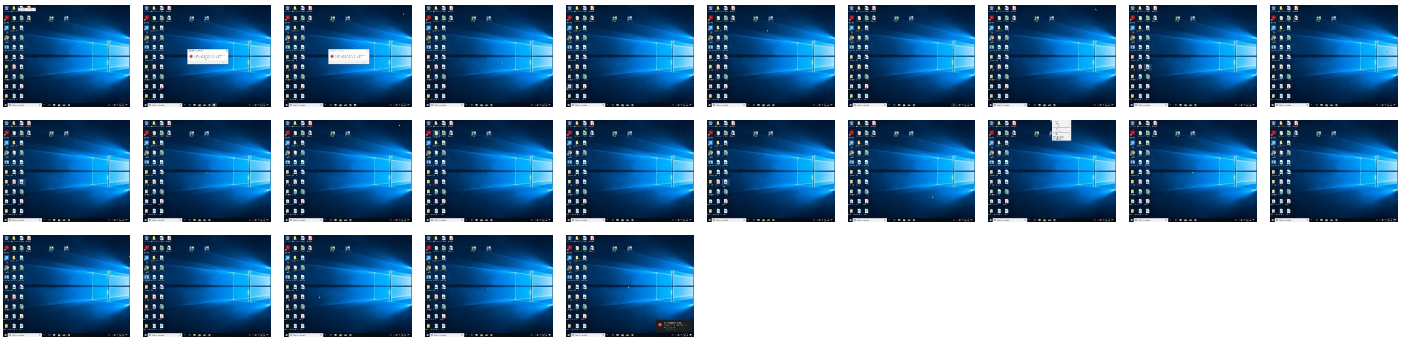
Behavior Graph



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
Coopera.exe	0%	Virustotal		Browse
Coopera.exe	3%	Metadefender		Browse
Coopera.exe	3%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

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 Red Diamond
Analysis ID:	338151
Start date:	11.01.2021
Start time:	18:11:01
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Coopera.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:	26
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:	clean6.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 37.3% (good quality ratio 35.9%) • Quality average: 75.5% • Quality standard deviation: 25.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Execution Graph export aborted for target Coopera.exe, PID 5276 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 (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.6327217713226005
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:	Coopera.exe
File size:	444256
MD5:	e6ed395de0f1e8a1ce346506452609f1
SHA1:	0029721036587ca7aa3657749e63e94e47ed76d4
SHA256:	78789f0a216d91b67b3dc6a2d0c3da7219f6eb30968c376 1437367a143ab0a81
SHA512:	7d538882873d34e6ed04abf189dbfb17047a6868e2ad39 9fb580f27795a1964c0bf0e13f383f388d8bcd79667554e5 71a0787085294bc46e820638af8297360
SSDEEP:	6144:URRuqQDnkNX+DDhjOGxOfat7tfpkmwloEaAR7h XEJGskMEwBi5EZWHo:U2LkNOncGxOSptfEloErBS03 wleo
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A.....s...s...s.....s.....@.s.....s..)....s...r...s...r.s.s..H....s.....s..H.....s.Rich..s.....PE..L..

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x430447
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5DBB4157 [Thu Oct 31 20:17:27 2019 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:	a2f71f2284892c973494e91fbe1a6543

Authenticode Signature

Signature Valid:	**true**
Signature Issuer:	CN=DigiCert High Assurance Code Signing CA-1, OU=www.digicert.com, O=DigiCert Inc, C=US
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 9/14/2017 5:00:00 PM 11/15/2019 4:00:00 AM
Subject Chain	• CN=Gas Informatica Ltda, O=Gas Informatica Ltda, L=BrasÃlia, C=BR
Version:	3
Thumbprint MD5:	864DE7C1DF11A46E1D194902B4FF381E
Thumbprint SHA-1:	5BF49ACAA112EEC09AED8B78AF6783C2F4877A71
Thumbprint SHA-256:	EE2F6AC114F5725761066FDC0163CF6D17E0A8645463D0BD320C7ED5C1F1016F
Serial:	024E4DBC3CE7F612E666A167EE4A1299

Entrypoint Preview

Instruction
call 00007FA8E0EE8B1Bh
jmp 00007FA8E0EDE825h
push 00000014h
push 004606C8h
call 00007FA8E0EE6278h
call 00007FA8E0EE21BDh
movzx esi, ax
push 00000002h
call 00007FA8E0EE8AAEh
pop ecx
mov eax, 00005A4Dh
cmp word ptr [00400000h], ax
je 00007FA8E0EDE826h
xor ebx, ebx
jmp 00007FA8E0EDE855h
mov eax, dword ptr [0040003Ch]
cmp dword ptr [eax+00400000h], 00004550h
jne 00007FA8E0EDE80Dh
mov ecx, 0000010Bh
cmp word ptr [eax+00400018h], cx
jne 00007FA8E0EDE7FFh
xor ebx, ebx

Instruction
cmp dword ptr [eax+00400074h], 0Eh
jbe 00007FA8E0EDE82Bh
cmp dword ptr [eax+004000E8h], ebx
setne bl
mov dword ptr [ebp-1Ch], ebx
call 00007FA8E0EE826Dh
test eax, eax
jne 00007FA8E0EDE82Ah
push 0000001Ch
call 00007FA8E0EDE901h
pop ecx
call 00007FA8E0EE738Fh
test eax, eax
jne 00007FA8E0EDE82Ah
push 00000010h
call 00007FA8E0EDE8F0h
pop ecx
call 00007FA8E0EE8B27h
and dword ptr [ebp-04h], 00000000h
call 00007FA8E0EE8257h
test eax, eax
jns 00007FA8E0EDE82Ah
push 0000001Bh
call 00007FA8E0EDE8D6h
pop ecx
call dword ptr [004520CCh]
mov dword ptr [00466C48h], eax
call 00007FA8E0EE8B42h
mov dword ptr [00464CA8h], eax
call 00007FA8E0EE84E5h
test eax, eax
jns 00007FA8E0EDE82Ah

Rich Headers

Programming Language:	• [C++] VS2013 UPD5 build 40629 • [C] VS2013 build 21005 • [IMP] VS2015 UPD3.1 build 24215 • [LNK] 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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x60ddc	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6d000	0x4c2	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x68c00	0x3b60	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x68000	0x4050	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x52230	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x5b068	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x52000	0x1c8	.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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x50bce	0x50c00	False	0.495186726006	data	6.63716411727	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x52000	0xf87c	0xfa00	False	0.3491875	data	4.79187748188	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x62000	0x4c4c	0x2a00	False	0.252232142857	data	4.47952514089	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.dbld0	0x67000	0xe70	0x1000	False	0.793701171875	data	7.10695931514	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0x68000	0x4050	0x4200	False	0.723011363636	data	6.57580097283	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x6d000	0x4c2	0x600	False	0.356770833333	data	3.58182395838	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x6d0a0	0x2c8	data	Portuguese	Brazil
RT_MANIFEST	0x6d368	0x15a	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
nss3.dll	PK11_ImportCert, PK11_GetInternalKeySlot, PK11_FreeSlot, CERT_DecodeTrustString, CERT_ChangeCertTrust, CERT_DecodeCertFromPackage, CERT_GetDefaultCertDB, CERT_DestroyCertificate, PR_GetOpenFileInfo, PR_Read, PR_Close, PR_Open, SECITEM_FreeItem_Util, SECITEM_AllocItem_Util, ATOB_ConvertAsciiToItem_Util, NSS_Shutdown, NSS_Initialize, PORT_Free_Util, PORT_ZAlloc_Util
CRYPT32.dll	CryptBinaryToStringA, CertFreeCertificateContext, CertFindCertificateInStore, CertCloseStore, CertOpenStore
KERNEL32.dll	IsValidCodePage, SetFilePointerEx, GetACP, LoadLibraryExW, GetOEMCP, HeapReAlloc, GetTimeZoneInformation, ReadFile, CreateFileA, CloseHandle, OutputDebugStringW, SetStdHandle, WriteConsoleW, ReadConsoleW, CreateFileW, SetEndOfFile, SetEnvironmentVariableA, FlushFileBuffers, GetConsoleMode, SetLastError, ExpandEnvironmentStringsA, GetFileAttributesA, GetLastError, GetCurrentProcess, AreFileApisANSI, MultiByteToWideChar, WideCharToMultiByte, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, EncodePointer, DecodePointer, GetStringTypeW, RaiseException, RtlUnwind, GetCommandLineA, HeapFree, GetCPInfo, HeapAlloc, UnhandledExceptionFilter, SetUnhandledExceptionFilter, FreeEnvironmentStringsW, InitializeCriticalSectionAndSpinCount, Sleep, TerminateProcess, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, GetStartupInfoW, GetModuleHandleW, GetProcAddress, IsProcessorFeaturePresent, GetDateFormatW, GetTimeFormatW, CompareStringW, LCMapStringW, GetLocaleInfoW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, ExitProcess, GetModuleHandleExW, HeapSize, IsDebuggerPresent, GetCurrentThreadId, GetProcessHeap, GetStdHandle, GetFileType, GetModuleFileNameA, WriteFile, GetModuleFileNameW, QueryPerformanceCounter, GetCurrentProcessId, GetSystemTimeAsFileTime, GetEnvironmentStringsW, GetConsoleCP
ADVAPI32.dll	LookupPrivilegeValueW, AdjustTokenPrivileges, OpenProcessToken, RegUnLoadKeyA, RegOpenKeyExA, RegLoadKeyA, RegEnumKeyA, RegCloseKey, RegQueryValueExA

Version Infos

Description	Data
LegalCopyright	Copyright 2019 - Diebold Nixdorf
FileVersion	1.2.1.27501
CompanyName	Diebold Nixdorf
ProductName	Diebold Nixdorf - Protection
ProductVersion	1.2.1.27501
FileDescription	Diebold Nixdorf - Protection Module
Translation	0x0416 0x04b0

Possible Origin

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

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: Coopera.exe PID: 5276 Parent PID: 5704

General

Start time:	18:11:49
Start date:	11/01/2021
Path:	C:\Users\user\Desktop\Coopera.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Coopera.exe'
Imagebase:	0x890000
File size:	444256 bytes
MD5 hash:	E6ED395DE0F1E8A1CE346506452609F1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis