

ID: 338418
Sample Name: RFQ-PR#20211201.exe
Cookbook: default.jbs
Time: 08:45:54
Date: 12/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report RFQ-PR#20211201.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 4
Signature Overview 4
AV Detection: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 5
Anti Debugging: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 8
URLs 8
Domains and IPs 8
Contacted Domains 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
Entrypoint Preview 10
Data Directories 12
Sections 12
Resources 12
Imports 12
Version Infos 12
Possible Origin 12
Network Behavior 13
Code Manipulations 13
Statistics 13
System Behavior 13

Copyright null 2021

Analysis Process: RFQ-PR#20211201.exe PID: 7148 Parent PID: 6104 13
General 13
File Activities 13
Disassembly 13
Code Analysis 13

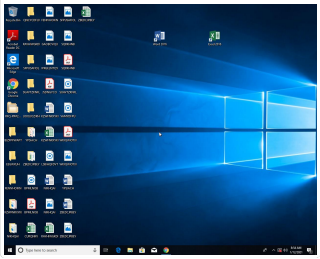
Analysis Report RFQ-PR#20211201.exe

Overview

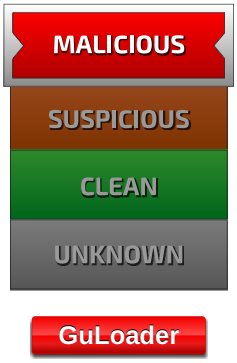
General Information

Sample Name:	RFQ-PR#20211201.exe
Analysis ID:	338418
MD5:	7f460fbf235c5e6…
SHA1:	6cda9cecf924e6e..
SHA256:	1c9344d3993bafb.
Tags:	exe GuLoader

Most interesting Screenshot:



Detection

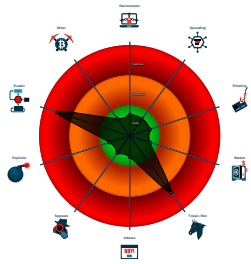


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Detected RDTSC dummy instruction…
- Found potential dummy code loops (…
- Potential time zone aware malware
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Yara detected VB6 Downloader Gen…
- Abnormal high CPU Usage
- Contains functionality for execution …
- Contains functionality to read the PEB
- PE file contains strange resources
- Program does not show much activi…

Classification



Startup

- **System is w10x64**
- RFQ-PR#20211201.exe (PID: 7148 cmdline: 'C:\Users\user\Desktop\RFQ-PR#20211201.exe' MD5: 7F460FBF235C5E678B553EDD2113D890)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

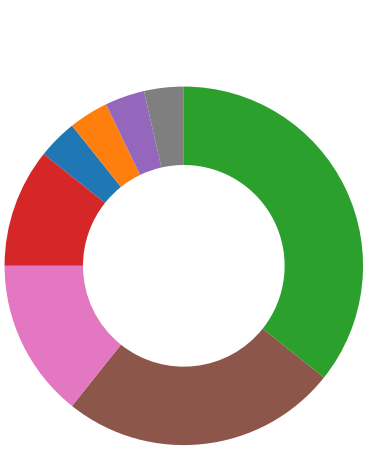
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: RFQ-PR#20211201.exe PID: 7148	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: RFQ-PR#20211201.exe PID: 7148	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Potential time zone aware malware

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

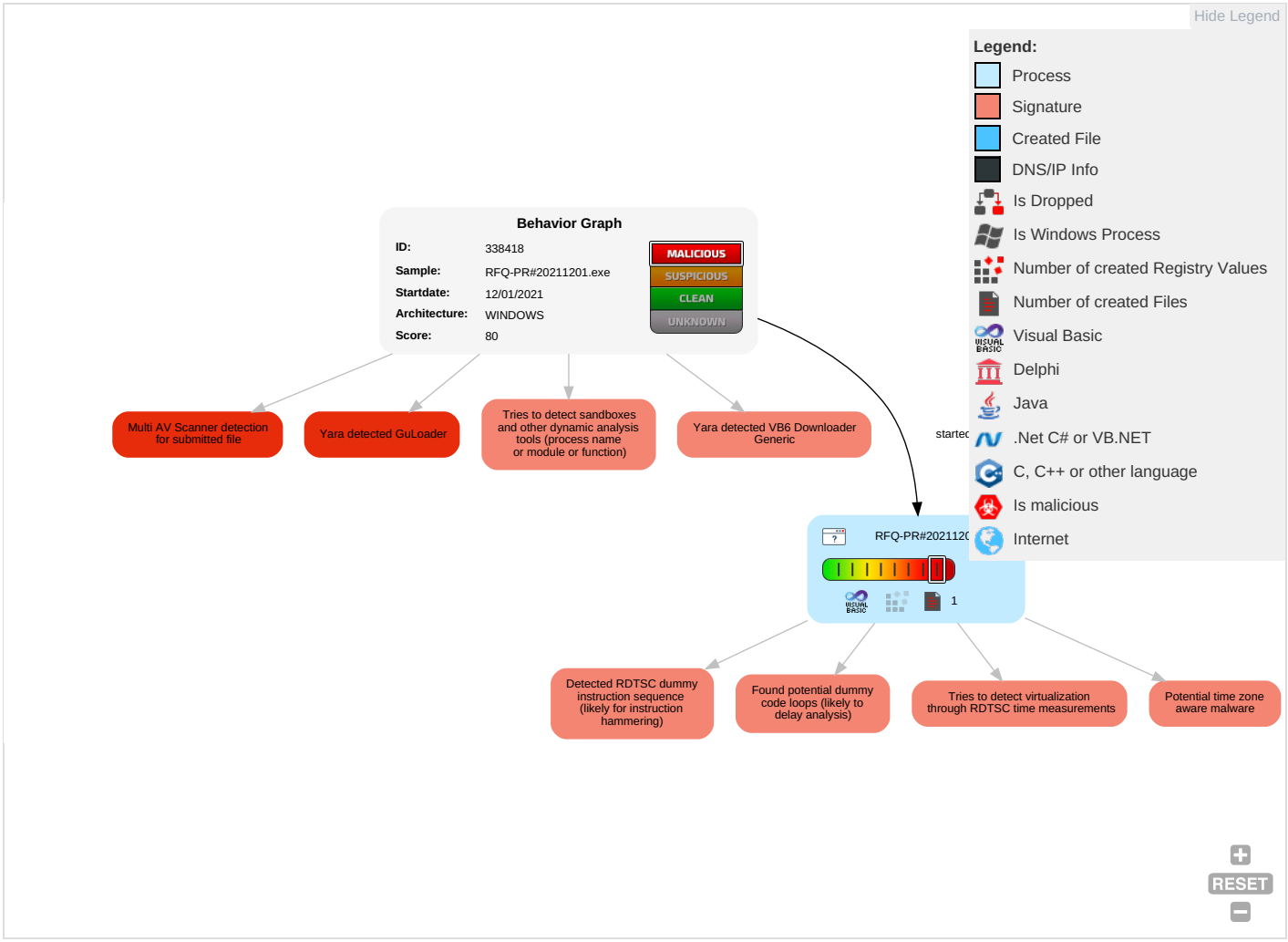
Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	R T W A
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Security Software Discovery 4 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	R W W A
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Virtualization/Sandbox Evasion 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	O D C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	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	LSA Secrets	System Information Discovery 2 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

Copyright null 2021

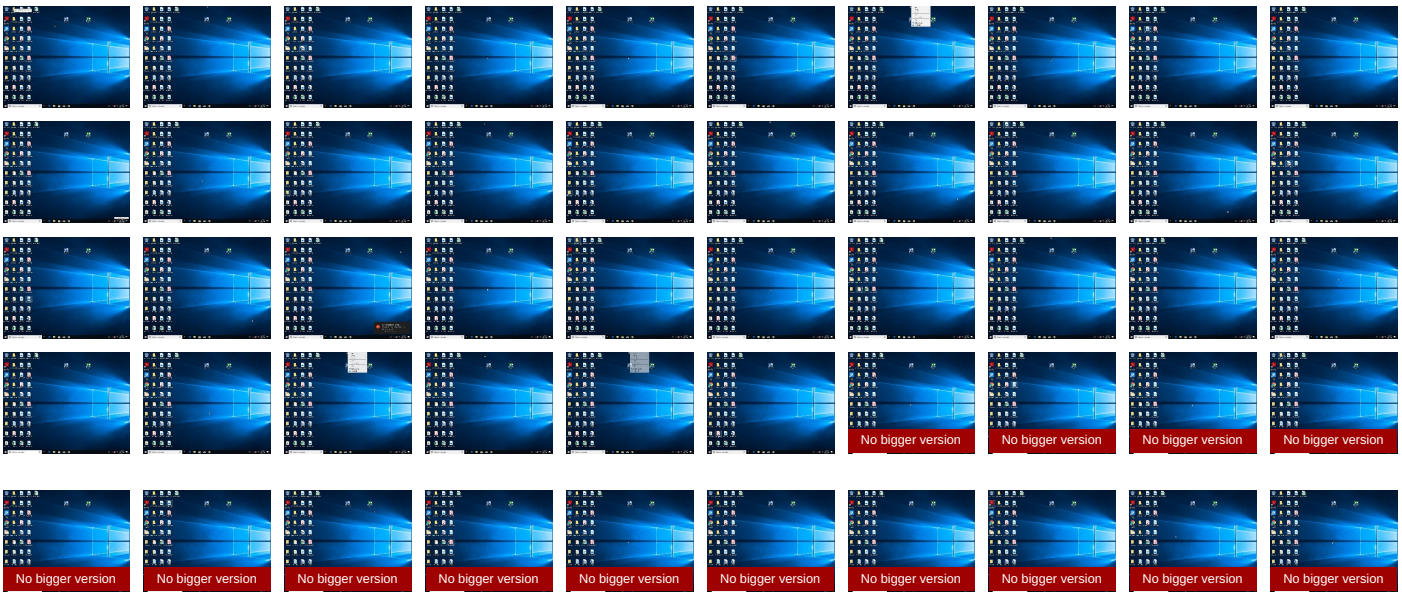
Behavior Graph

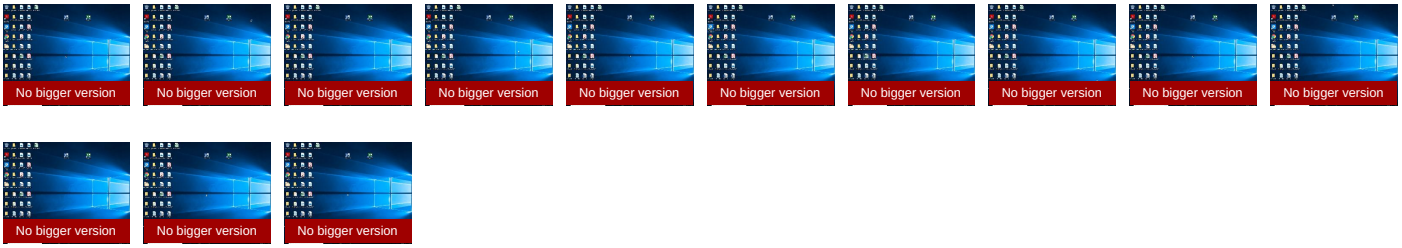


Screenshots

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
RFQ-PR#20211201.exe	13%	ReversingLabs	Win32.Infostealer.PonyStealer	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Copyright null 2021

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:	338418
Start date:	12.01.2021
Start time:	08:45:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFQ-PR#20211201.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:	23
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:	mal80.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 26.1% (good quality ratio 2.9%) • Quality average: 5.5% • Quality standard deviation: 15.8%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption

Copyright null 2021

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.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:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.89482429017858
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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:	RFQ-PR#20211201.exe
File size:	90112
MD5:	7f460fbf235c5e678b553edd2113d890

General

SHA1:	6cda9cecf924e6e2fe967ed0ad0c1d189e41fb81
SHA256:	1c9344d3993bafbe60739644d0fae336276c4ffd835da89d44b58ef4d744eee0
SHA512:	50055fc24c925117f463075b86dd68457ee193751926582a070017d76a1ce99b14d4dcd27a77cb2a8891a96289847b5aa3283930afc51ae533cc6ff0191b12ea
SSDEEP:	768:7UD0AyHMB8Q9+FAjnNGvM591DZH+vcLt/Wfu1FXpuIUQUzYRT:7JM9PEvy1HDh/MuPXIQCW
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L....._.....0...0.....\.....@....@.....

File Icon



Icon Hash:	6eeed0e4a4a4e0d2

Static PE Info

General

Entrypoint:	0x40135c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5FFCDAD5 [Mon Jan 11 23:10:13 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	2a71f44ac1c823400003a5bea275b301

Entrypoint Preview

Instruction
push 00401E08h
call 00007F8358990B55h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dh, bh
dec edx
cmp dword ptr [esi+4C6F8B44h], eax
mov edx, 9677A334h
and byte ptr [eax-0Ah], cl
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al

Copyright null 2021

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
push esp
dec ecx
dec ebp
dec edi
dec esi
inc ebp
inc ebp
push edx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
and edx, ebp
mul dword ptr [edx+ecx*8+4A6F2DE6h]
mov dword ptr [748B69F4h], eax
salc
dec eax
lds ecx, fword ptr [ecx+09h]
popad
out dx, eax
call far EE98h : B34D2D1Ah
sub byte ptr [ebp+3A3EA90Eh], ah
dec edi
lodsd
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
clc
or dword ptr [eax], eax
add cl, bl
add eax, 0C000000h
add byte ptr [ecx+74h], al
push 6F697265h
popad
popad
xor al, 00h
or eax, 45000A01h
jns 00007F8358990BC7h

Copyright null 2021

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x12e84	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x16000	0x894	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x10c	.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	0x12338	0x13000	False	0.389327199836	data	6.32360628392	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x14000	0x1174	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x16000	0x894	0x1000	False	0.3310546875	data	3.03052529206	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1632c	0x568	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x16318	0x14	data		
RT_VERSION	0x160f0	0x228	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaStrCat, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaLateMemSt, __vbaObjSet, __vbaCyAdd, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaCyI2, __vbaStrCmp, __vbaVarTstEq, __vbaR4Str, __vbaObjVar, _adj_fpatan, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaFpCmpCy, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaStrVarVal, _CIlog, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarAdd, __vbaVarDup, __vbaVarLateMemCallLd, __vbaLateMemCallLd, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	Credo8
FileVersion	1.00
CompanyName	Cloud Share
ProductName	Effektiviteternes
ProductVersion	1.00
OriginalFilename	Credo8.exe

Possible Origin

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

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: RFQ-PR#20211201.exe PID: 7148 Parent PID: 6104

General

Start time:	08:46:47
Start date:	12/01/2021
Path:	C:\Users\user\Desktop\RFQ-PR#20211201.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RFQ-PR#20211201.exe'
Imagebase:	0x400000
File size:	90112 bytes
MD5 hash:	7F460FBF235C5E678B553EDD2113D890
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis