ID: 342865
Sample Name:
ZP1H92DwTq.exe
Cookbook: default.jbs
Time: 19:45:17
Date: 21/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

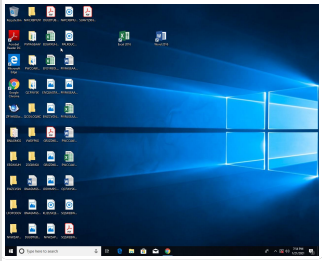
Analysis Report ZP1H92DwTq.exe

Overview

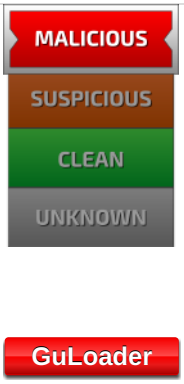
General Information

Sample Name:	ZP1H92DwTq.exe
Analysis ID:	342865
MD5:	3421ebb45a538c..
SHA1:	15766bfdbd612d1.
SHA256:	8d2f6b5af6dee65..
Tags:	exe GuLoader

Most interesting Screenshot:



Detection



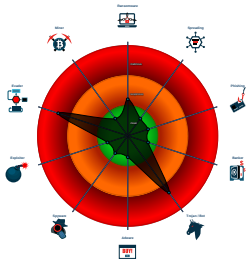
GuLoader

Score:	76
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 (…
- 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
- Detected potential crypto function
- PE file contains strange resources
- Program does not show much activi…

Classification



Startup

- **System is w10x64**
- ZP1H92DwTq.exe (PID: 4404 cmdline: 'C:\Users\user\Desktop\ZP1H92DwTq.exe' MD5: 3421EBB45A538C5044D484703448F2A7)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

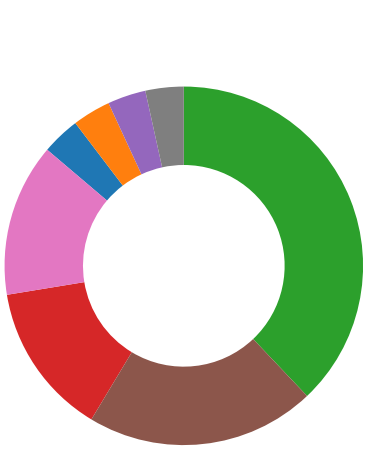
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: ZP1H92DwTq.exe PID: 4404	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: ZP1H92DwTq.exe PID: 4404	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

Compliance:

Uses 32bit PE files

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

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

Tries to detect virtualization through RDTSC time measurements

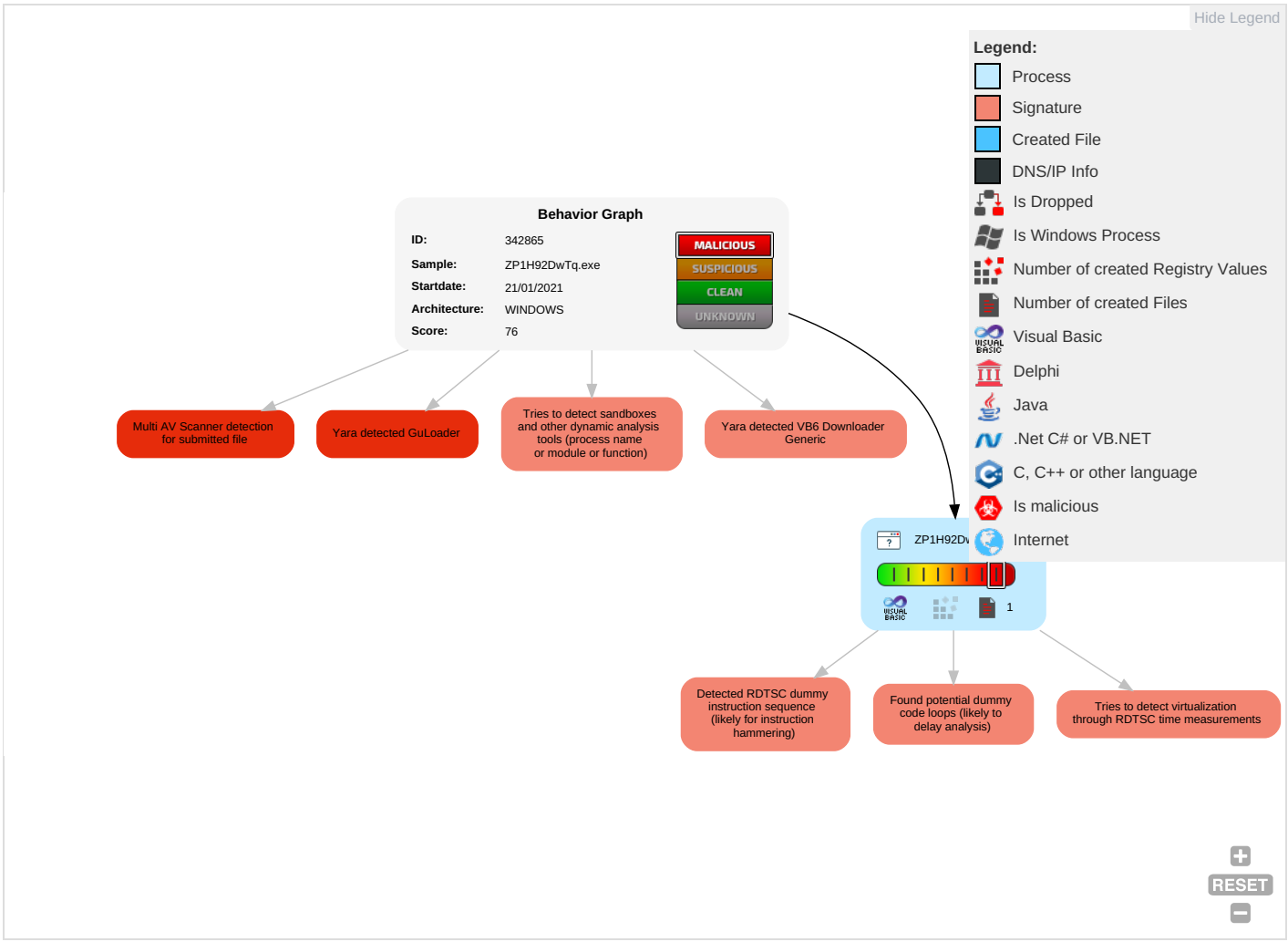
Anti Debugging:

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	Security Software Discovery 4 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	R T W A
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Software Packing 1	LSASS Memory	Virtualization/Sandbox Evasion 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)	Process Injection 1	Security Account Manager	Process Discovery 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)	Obfuscated Files or Information 2	NTDS	System Information Discovery 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

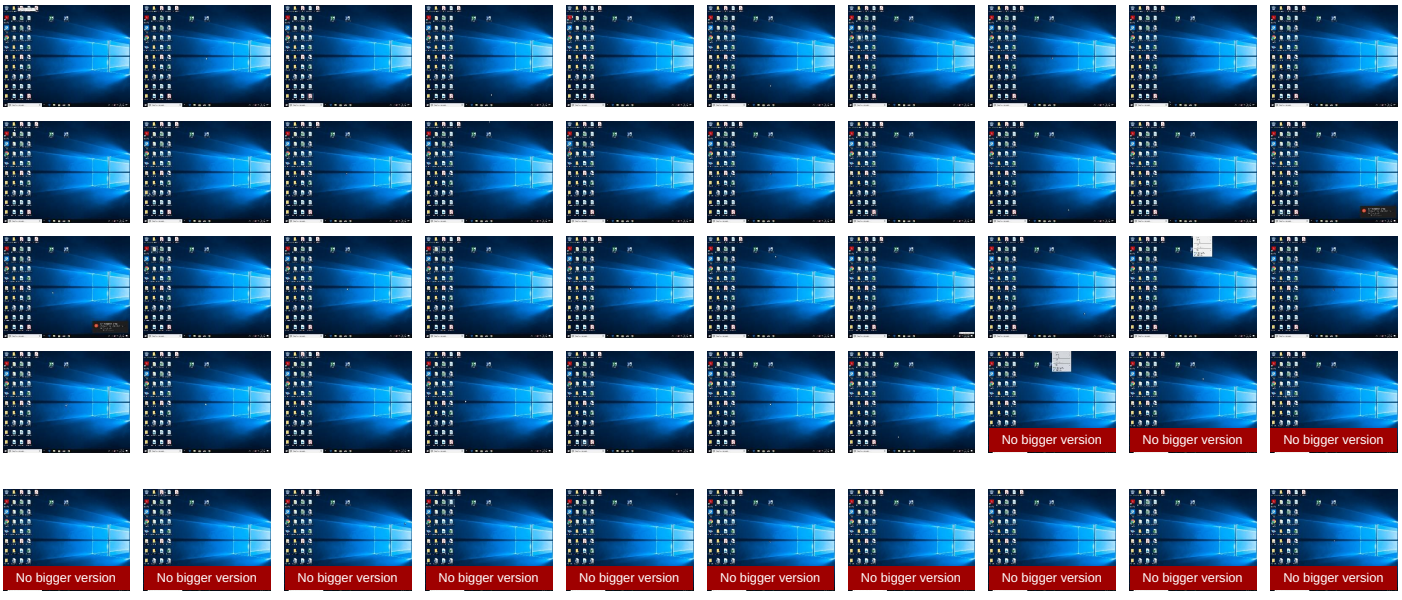
Behavior Graph

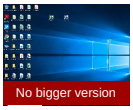


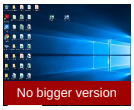
Screenshots

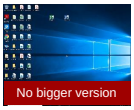
Thumbnails

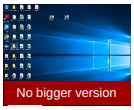
This section contains all screenshots as thumbnails, including those not shown in the slideshow.

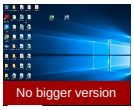












Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ZP1H92DwTq.exe	10%	Virustotal		Browse
ZP1H92DwTq.exe	7%	ReversingLabs	Win32.PUA.Wacapew	

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:	342865
Start date:	21.01.2021
Start time:	19:45:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ZP1H92DwTq.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:	39
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:	mal76.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 40.7% (good quality ratio 18.4%) • Quality average: 24.5% • Quality standard deviation: 29.8%
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
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.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):	6.441995489867964
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:	ZP1H92DwTq.exe
File size:	98304
MD5:	3421ebb45a538c5044d484703448f2a7
SHA1:	15766bfdbd612d174ee233dce4d466880728f8f3
SHA256:	8d2f6b5af6dee6568c8d9f58a3a618b47964bef00531f15063ed2e289d7e2abf
SHA512:	0c3acfa2d31e81af396ebb179c38bb883430a7955ad1008 1facd0c7ea9066f51e00bfbb6a612262526cb588368a9b9 d825f2288f617242c4490d7c22d19c7903
SSDEEP:	1536:VMmOBBPTp3C7uIaILxhhn3JbPMfIxvktHFoDZN DA87itMmO:CmAJTpSkUbaf+vktHClND7iqm

General

File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....I..... .....Rich.....PE..L.....%U..... .....@...@.....d.....P....@

File Icon

Icon Hash:	80c34adad868b0e0

Static PE Info

General

Entrypoint:	0x401364
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:	0x55251D86 [Wed Apr 8 12:22:30 2015 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:	f0b86fcdc858848465b74699359cbeef

Entrypoint Preview

Instruction
push 00402BF4h
call 00007F375C740165h
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 byte ptr [edi-17h], bl
inc ecx
mov edi, 40E4F2EBh
mov ebp, 6252C9A9h
mov ch, byte ptr [ecx+000000A1h]
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [edi], ah
add edx, dword ptr [edi+6D000000h]
imul esi, dword ptr [ebx+66h], 6F74726Fh
insb
imul esp, dword ptr [ebp+64h], 00h
pop es
inc ecx
add byte ptr [eax], al
add byte ptr [eax], al
add bh, bh

Instruction
int3
xor dword ptr [eax], eax
add dword ptr [esi-78h], edi
fld tbyte ptr [edi-4Bh]
insd
loop 00007F375C7401BEh
mov seg?, sp
aam A0h
sahf
jl 00007F375C7401CEh
test al, 20h
in eax, dx
sub eax, 4D5E8B1Eh
lodsb
mov esi, E4037676h
cmp bh, byte ptr [esi+3Ah]
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
mov al, byte ptr [80000015h]
adc eax, 05000000h
add byte ptr [ecx+61h], bh
arpl word ptr [eax+61h], bp
add byte ptr [73000601h], cl
je 00007F375C7401E7h
imul esp, dword ptr fs:[ebp+00h], 00000119h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x14934	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x17000	0x1926	.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	0x238	0x20	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x11c	.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	0x13e18	0x14000	False	0.639904785156	data	6.92993143866	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x15000	0x1568	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x17000	0x1926	0x2000	False	0.429809570312	data	4.46208591353	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1787e	0x10a8	data		
RT_ICON	0x17416	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x173f4	0x22	data		
RT_VERSION	0x17120	0x2d4	data	Chinese	Taiwan

Imports

DLL	Import
MSVBVM60.DLL	__vbaStrI2, _CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaStrVarMove, __vbaLenBstr, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaStrCat, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaExitProc, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaStrVarVal, _CIlog, __vbaErrorOverflow, __vbaNew2, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaVarDup, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0404 0x04b0
LegalCopyright	Fx Studio
InternalName	Embedshaver
FileVersion	2.00
LegalTrademarks	Fx Studio
Comments	FxCam 2020.
ProductName	FxCam 2020.
ProductVersion	2.00
FileDescription	FxCam 2020.
OriginalFilename	Embedshaver.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: ZP1H92DwTq.exe PID: 4404 Parent PID: 5664

General

Start time:	19:46:09
Start date:	21/01/2021
Path:	C:\Users\user\Desktop\ZP1H92DwTq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ZP1H92DwTq.exe'
Imagebase:	0x400000
File size:	98304 bytes
MD5 hash:	3421EBB45A538C5044D484703448F2A7
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

Disassembly

Code Analysis