ID: 396529
Sample Name:
qhw7KZSA53.exe
Cookbook: default.jbs
Time: 14:29:55
Date: 23/04/2021
Version: 31.0.0 Emerald

Table of Contents

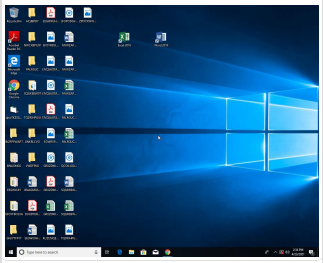
Analysis Report qhw7KZSA53.exe

Overview

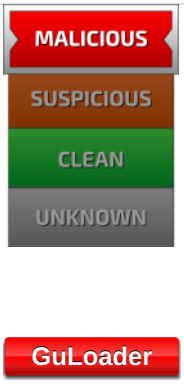
General Information

Sample Name:	qhw7KZSA53.exe
Analysis ID:	396529
MD5:	4b7687321980c9..
SHA1:	5e27cc0eddb864..
SHA256:	3a51813adeabd1..
Tags:	exe GuLoader
Infos:	

Most interesting Screenshot:



Detection

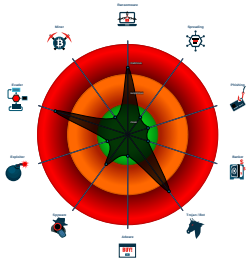


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Potential malicious icon found
- Yara detected GuLoader
- Detected RDTSC dummy instruction…
- Found potential dummy code loops (…
- Machine Learning detection for samp…
- 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

Classification



Startup

- **System is w10x64**
- qhw7KZSA53.exe (PID: 5380 cmdline: 'C:\Users\user\Desktop\qhw7KZSA53.exe' MD5: 4B7687321980C96093C8E6A43B764728)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

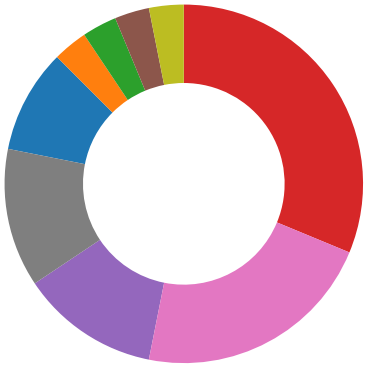
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: qhw7KZSA53.exe PID: 5380	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: qhw7KZSA53.exe PID: 5380	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary:

Potential malicious icon found

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:

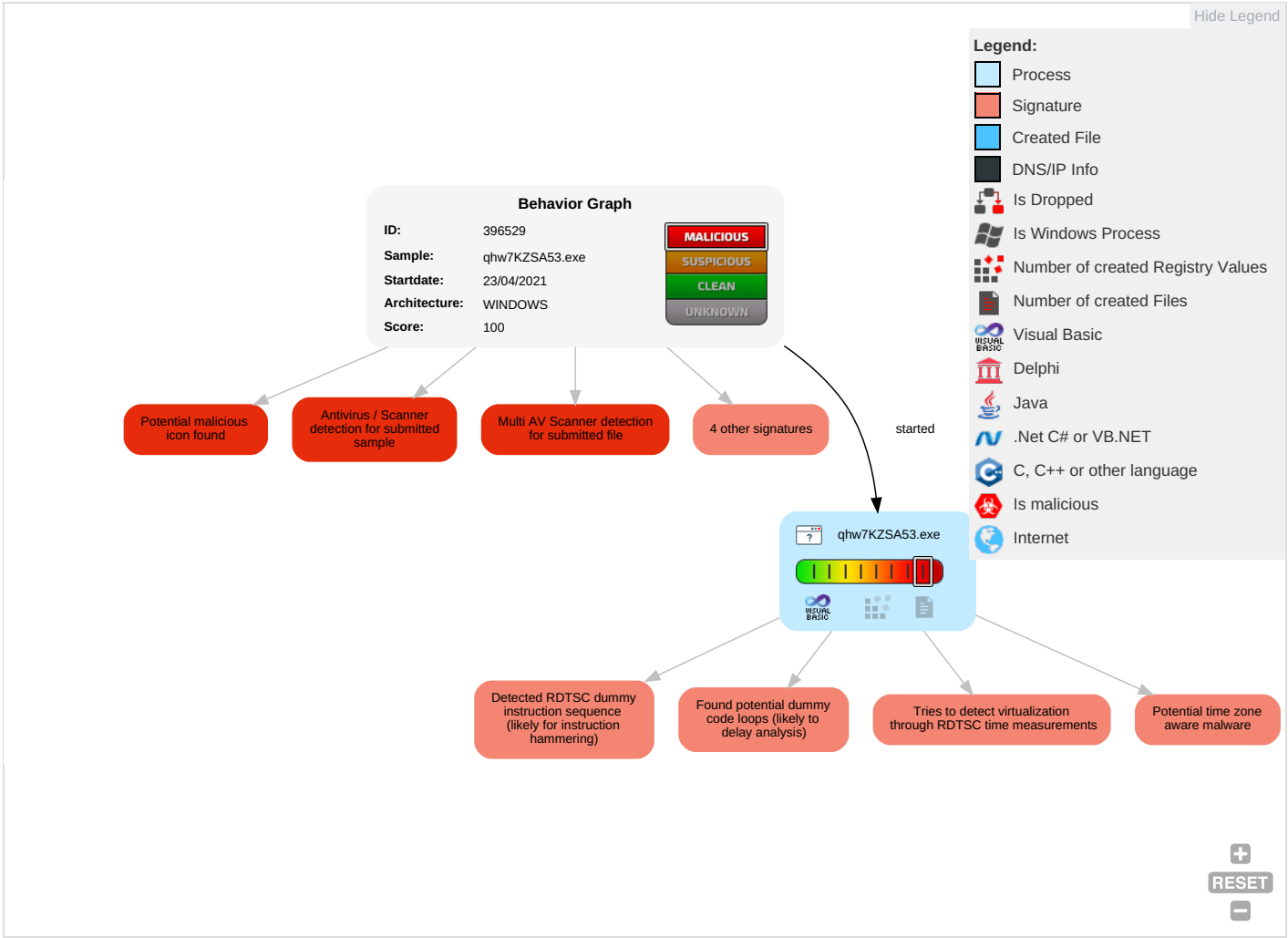
Found potential dummy code loops (likely to delay analysis)

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	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
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	

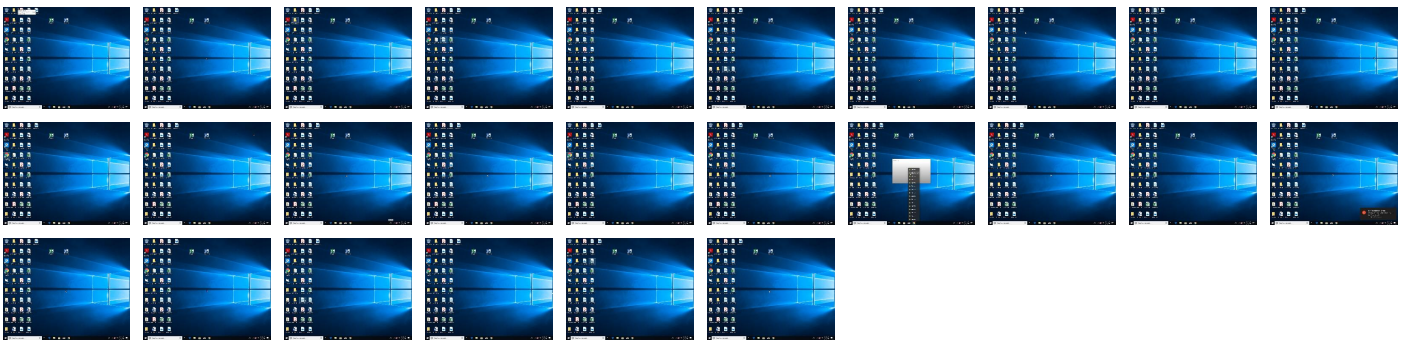
Behavior Graph



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
qhw7KZSA53.exe	25%	Virustotal		Browse
qhw7KZSA53.exe	23%	ReversingLabs	Win32.Trojan.GuLoader	
qhw7KZSA53.exe	100%	Avira	HEUR/AGEN.1109931	
qhw7KZSA53.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.qhw7KZSA53.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1109931		Download File
1.0.qhw7KZSA53.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1109931		Download File

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 Emerald
Analysis ID:	396529
Start date:	23.04.2021
Start time:	14:29:55
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	qhw7KZSA53.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:	29
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:	mal100.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 14.2% (good quality ratio 8.8%) • Quality average: 37.6% • Quality standard deviation: 33.4%
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): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.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):	5.551859861514489
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:	qhw7KZSA53.exe
File size:	98304
MD5:	4b7687321980c96093c8e6a43b764728
SHA1:	5e27cc0eddb8646e26b72a7ff4f608df45c0eb8a
SHA256:	3a51813adeabd17d4939280137288152b2a3f25f7bf9e738c8f25df5ef49be31
SHA512:	17ea0dbc1e4144bafd45fc7683ce6d8bf1a43610a5abb11f70593f1e33b668c2a0e18c98398351af6c8b659be7256db82f8c1c4c988046258d4d5ad7996526c4
SSDEEP:	768:kd2uNErYGMJDKf0aJxvOlu/ir5SGM7YMTdxIXX5ewWYOW75CZ8ZngsCBf1lC8Ym1:nd6VivjvO3lYCdxmL5rnGf1l/Ymas
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...Ab.O.....P...0.....`....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x4017b0
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:	0x4FA66241 [Sun May 6 11:36:33 2012 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:	f401ad1c560f85eb5aae8e91f258deba

Entrypoint Preview

Instruction
push 0040C3F0h
call 00007FE234C66F63h
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
dec eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], bl
sbb eax, A18B28B3h
dec ecx
dec esi
mov bl, B9h
inc ecx
cmpsb
ror dword ptr [edi+00006325h], 1
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
outsb
and byte ptr [41462220h], bh
jnc 00007FE234C66FE6h
jc 00007FE234C66FE1h
jo 00007FE234C66FDAh
outsd
je 00007FE234C66FE1h
insd
je 00007FE234C66FE5h
imul esp, dword ptr [ebx+61h], 6500326Ch
imul esp, dword ptr [edi+68h], 00000000h

Instruction
dec esp
xor dword ptr [eax], eax
pop es
jnl 00007FE234C66FDDh
adc byte ptr [ecx+5Ah], dl
lahf
add dword ptr [ebp-50h], 2201F807h
jecxz 00007FE234C66F20h
lds eax, fword ptr [eax]
movsd
in al, dx
mov ch, 47h
fisubr dword ptr [ecx+ecx*2]
mov cl, 30h
enter 1563h, 6Bh
imul edi, dword ptr [edx]
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
pop ebp
stosb
add byte ptr [eax], al
xor byte ptr [ecx+09000000h], ch
add byte ptr [edx+65h], cl
jnc 00007FE234C66FE2h
push 0000006Ch
jnc 00007FE234C66FABh
add byte ptr [00000001h], cl

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x151b4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x18000	0x910	.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	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x198	.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	0x14820	0x15000	False	0.394542875744	data	6.01789488966	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x16000	0x1278	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x18000	0x910	0x1000	False	0.1689453125	data	1.97442049534	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x187e0	0x130	data		
RT_ICON	0x184f8	0x2e8	data		
RT_ICON	0x183d0	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x183a0	0x30	data		
RT_VERSION	0x18150	0x250	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaHresultCheck, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaRecAnsiToUni, __vbaSetSystemError, __vbaRecDestruct, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaFpR8, __vbaVarTstLt, _CIsin, __vbaErase, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, __vbaR4Str, __vbaObjVar, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, __vbaRedim, __vbaRecUniToAnsi, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaFileOpen, __vbaNew2, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaI4Str, __vbaFreeStrList, __vbaDerefAry1, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaLateMemCall, __vbaStrToAnsi, __vbaVarDup, __vbaStrComp, __vbaFpI4, __vbaRecDestructAnsi, __vbaLateMemCallLd, _CIatan, __vbaStrMove, _allmul, __vbaLateIdSt, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	Intuitioners4
FileVersion	1.00
CompanyName	Cybill Technologies
ProductName	Cybill Technologies
ProductVersion	1.00
OriginalFilename	Intuitioners4.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: qhw7KZSA53.exe PID: 5380 Parent PID: 5800

General

Start time:	14:30:48
Start date:	23/04/2021
Path:	C:\Users\user\Desktop\qhw7KZSA53.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\qhw7KZSA53.exe'
Imagebase:	0x400000
File size:	98304 bytes
MD5 hash:	4B7687321980C96093C8E6A43B764728
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

Disassembly

Code Analysis