JoeSandbox Cloud BASIC

ID: 372416
Sample Name: RFlc8JHObG
Cookbook: default.jbs
Time: 14:07:10
Date: 20/03/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2

Analysis Report RFlc8JHObG 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
  - AV Detection: 5
  - Compliance: 5
  - Data Obfuscation: 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 7
  - URLs 8
- 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
    - Entrypoint Preview 10
    - Rich Headers 11
    - Data Directories 11
    - Sections 11
    - Resources 11
    - Imports 11
    - Possible Origin 11
- Network Behavior 12
- Code Manipulations 12
- Statistics 12
- System Behavior 12
  - Analysis Process: RFlc8JHObG.exe PID: 5988 Parent PID: 5904 12

General 12
Disassembly 12
Code Analysis 12

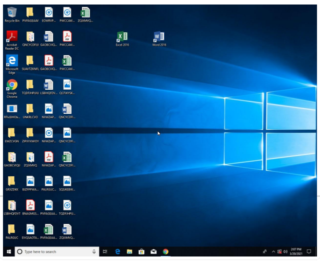
Analysis Report RFlc8JHObG

Overview

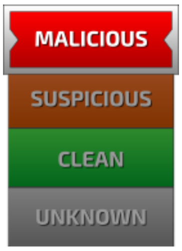
General Information

Sample Name:	RFlc8JHObG (renamed file extension from none to exe)
Analysis ID:	372416
MD5:	9babe52f985b2b4.
SHA1:	b4b4772d485d7d..
SHA256:	ca2ab2eb8249afc..
Tags:	unnamed9
Infos:	

Most interesting Screenshot:



Detection

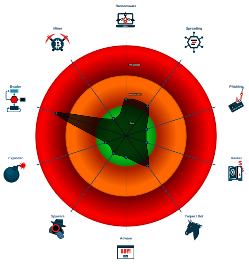


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Multi AV Scanner detection for subm…
- Machine Learning detection for samp…
- Antivirus or Machine Learning detec…
- Contains functionality to access load…
- Contains functionality to call native f…
- Contains functionality to dynamically…
- Contains functionality to enumerate …
- Contains functionality to launch a pr…
- Contains functionality to open a port…
- Contains functionality to read the PEB

Classification



Startup

- System is w10x64
- RFlc8JHObG.exe (PID: 5988 cmdline: 'C:\Users\user\Desktop\RFlc8JHObG.exe' MD5: 9BABE52F985B2B4193113D5C260EB195)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

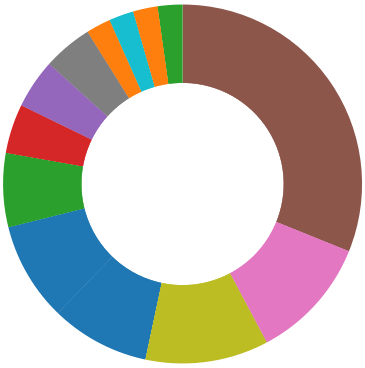
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- ● AV Detection
- ● Cryptography
- ● Compliance
- ● Spreading
- ● Networking



● System Summary
● Data Obfuscation
● Malware Analysis System Evasion
● Anti Debugging
● HIPS / PFW / Operating System Protection Evasion
● Language, Device and Operating System Detection
● Lowering of HIPS / PFW / Operating System Security Settings
● Remote Access Functionality

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

Compliance:

Detected unpacking (overwrites its own PE header)

Data Obfuscation:

Detected unpacking (changes PE section rights)

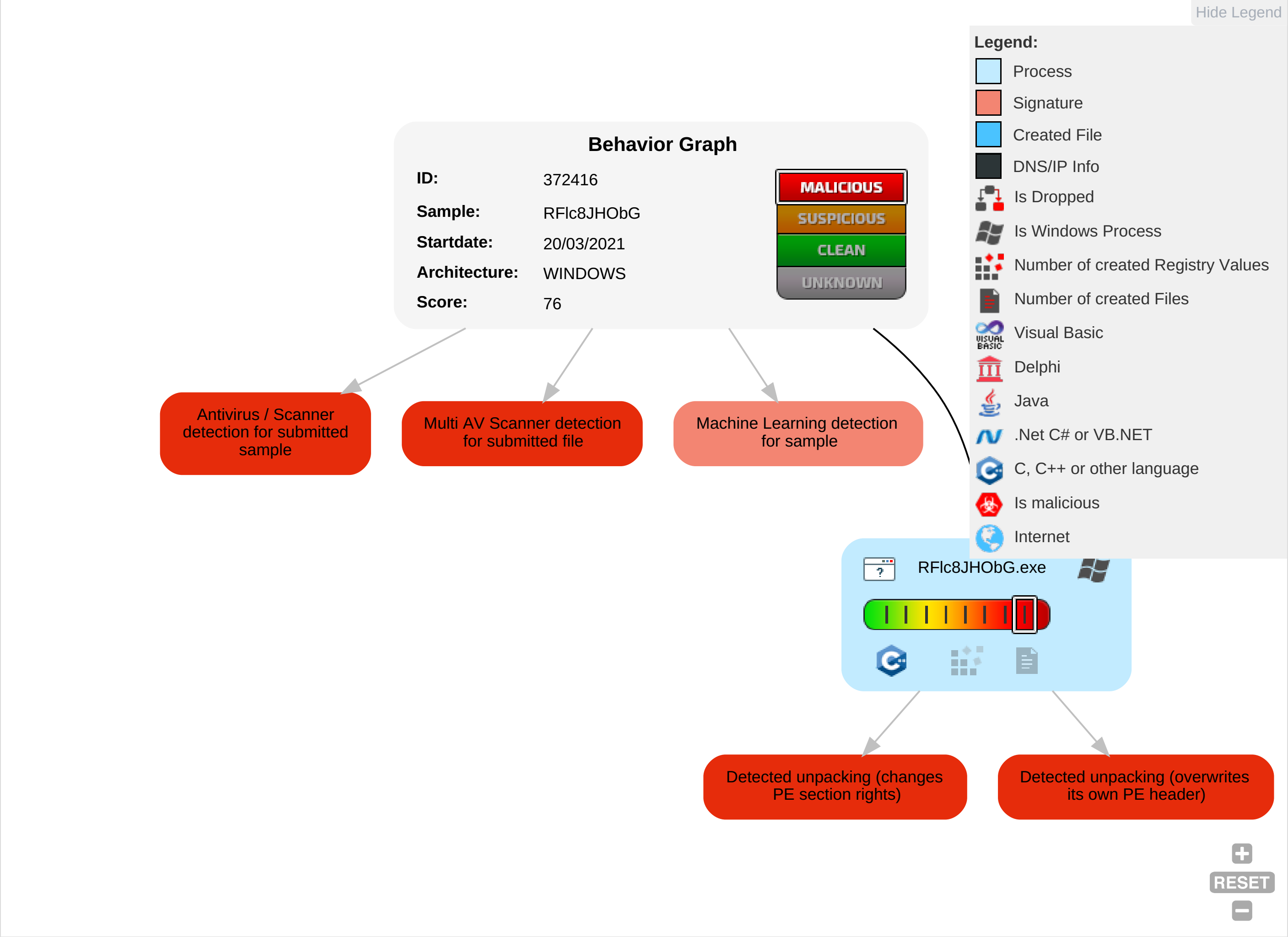
Detected unpacking (overwrites its own PE header)

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
Valid Accounts 1	Native API 1	Valid Accounts 1	Valid Accounts 1	Valid Accounts 1	OS Credential Dumping	Network Share Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remote Track D Without Authoriz
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Access Token Manipulation 1 1	Access Token Manipulation 1 1	LSASS Memory	System Time Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	Remote Wipe Da Without Authoriz
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	Security Software Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Install Root Certificate 1	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 2 3	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols	

Behavior Graph



Hide Legend

Legend:

- ▢ Process
- 🟥 Signature
- 🟦 Created File
- ■ DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

Behavior Graph

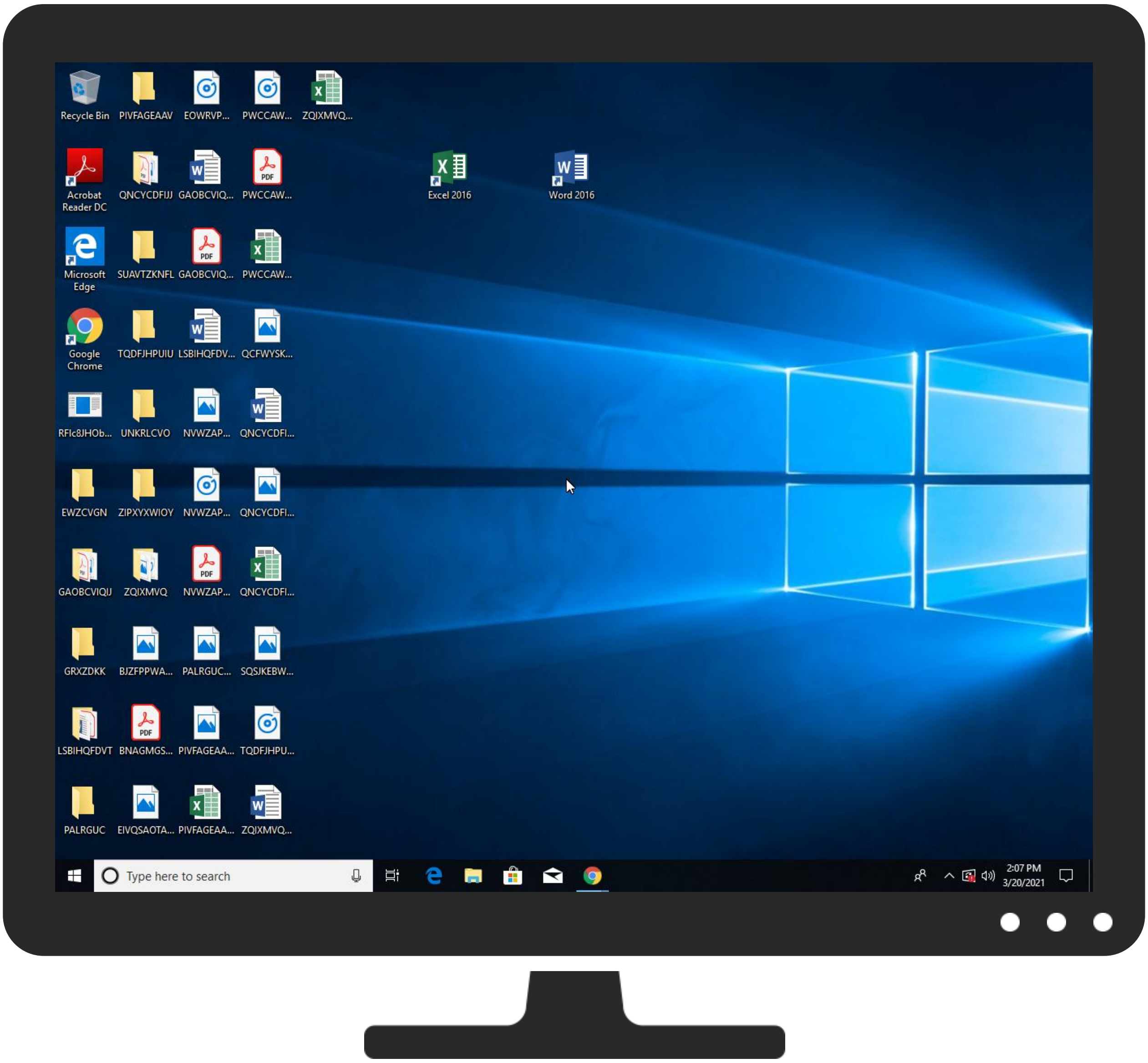
ID:	372416
Sample:	RFlc8JHObG
Startdate:	20/03/2021
Architecture:	WINDOWS
Score:	76

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Antivirus / Scanner detection for submitted sample
Multi AV Scanner detection for submitted file
Machine Learning detection for sample
RFlc8JHObG.exe
Detected unpacking (changes PE section rights)
Detected unpacking (overwrites its own PE header)
RESET

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
RFlc8JHObG.exe	85%	Virustotal		Browse
RFlc8JHObG.exe	88%	ReversingLabs	Win32.Trojan.Zeus	
RFlc8JHObG.exe	100%	Avira	TR/Crypt.XPACK.Gen	
RFlc8JHObG.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.RFlc8JHObG.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.RFlc8JHObG.exe.2bd0000.2.unpack	100%	Avira	TR/Kazy.MK		Download File
1.2.RFlc8JHObG.exe.2440000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.RFlc8JHObG.exe.400000.0.unpack	100%	Avira	TR/Kazy.MK		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.internic.net/images/internic.gif	RFlc8JHObG.exe	false		high
http://www.internic.net/images/internic.gifbclih6h5h4h3h2h1divtdtrhrbr	RFlc8JHObG.exe, 00000001.00000002.200757968.0000000002BD0000.00000004.00000001.sdmp	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	372416
Start date:	20.03.2021
Start time:	14:07:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFlc8JHObG (renamed file extension from none to 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:	2
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.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 56.5% (good quality ratio 48%) • Quality average: 71.2% • Quality standard deviation: 37.2%
HCA Information:	• Successful, ratio: 59% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated

Warnings:	Show All - Exclude process from analysis (whitelisted): svchost.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):	7.186773887815174
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:	RFlc8JHObG.exe
File size:	130560
MD5:	9babe52f985b2b4193113d5c260eb195
SHA1:	b4b4772d485d7d4192774aca3a9c594f82717adb
SHA256:	ca2ab2eb8249afceb6b9f42bac54fe8635fb5ccbf4e497c35ed700d9dae1c2d1

General

SHA512:	61f41678334ea638dd3dc02d280739910d4b64cc31289c 3f99bf41067bdfee1a9ab2114920b7b162862046b06d59d 2bb6168557cc1a4463113a2ad00f526af8b
SSDEEP:	3072:WhBFnGu6BYxbu75pZlgpXor85hfuHwhxqn9fI2uW +It:WhHGzK475pUpXiwgxExIt
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$..........9@d.j @d.j@d.j@d.jMd.jI..jQd.j[.9jOd.j[..jAd.j[..jAd.j[..jAd.jRich @d.j........PE..L....!.M..................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x401ee0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	
Time Stamp:	0x4D8C21A2 [Fri Mar 25 05:01:22 2011 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:	d2d0d8d094caedbfe934e30be29bea57

Entrypoint Preview

Instruction
xor eax, eax
xor eax, 000077A8h
push ebp
mov ebp, esp
sub esp, 10h
push esi
inc esi
mov esi, dword ptr [0043C00Ch]
and dword ptr [0040978Dh], 004097FDh
mov dword ptr [ebp-0Ch], C6F8E435h
sub dword ptr [00409741h], 00000A4Ch
push 004092F8h
mov dword ptr [ebp-0Ch], C6F8E434h
or dword ptr [0040974Dh], 0000382Ch
call esi
mov dword ptr [00409811h], 00003433h
cmp eax, 00000498h
jng 00007F2C58B3B831h
sbb dword ptr [00409805h], 004097CDh
xor eax, eax
mov dword ptr [00409811h], 00001618h
jmp 00007F2C58B3BA71h
mov dword ptr [00409861h], 00001374h
push 00409318h
or dword ptr [00409839h], 00409815h

Instruction
call esi
mov dword ptr [0040974Dh], 00005BB7h
cmp eax, 00000837h
jnl 00007F2C58B3B7CBh
mov eax, dword ptr [0040977Dh]
mov eax, dword ptr [0040942Ch]
cmp eax, 919D6EFDh
mov dword ptr [0040978Dh], 00006584h
jne 00007F2C58B3B82Ah

Rich Headers

Programming Language:	• [LNK] VS2010 SP1 build 40219 • [RES] VS2010 SP1 build 40219 • [EXP] VS2010 SP1 build 40219 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x3c014	0x257	.itext
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3e664	0x23c	
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3d000	0x8e8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x3e000	0x638	.idata
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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x3c000	0x14	.itext
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	0x7029	0x7200	False	0.791563870614	data	6.99040926415	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x9000	0x32f3e	0x17200	False	0.825274493243	data	7.18553169486	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.itext	0x3c000	0x26b	0x400	False	0.2412109375	data	3.78647081365	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3d000	0x8e8	0xa00	False	0.459375	data	3.29475958072	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.idata	0x3e000	0x6fe	0x800	False	0.7529296875	data	6.17155304092	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x3d31c	0x27c	data	English	United States
RT_DIALOG	0x3d598	0x350	data	English	United States

Imports

DLL	Import
USER32.dll	GetWindowDC, IsCharAlphaNumericW
KERNEL32.dll	lstrlenW

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: RFlc8JHObG.exe PID: 5988 Parent PID: 5904

General

Start time:	14:07:52
Start date:	20/03/2021
Path:	C:\Users\user\Desktop\RFlc8JHObG.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RFlc8JHObG.exe'
Imagebase:	0x400000
File size:	130560 bytes
MD5 hash:	9BABE52F985B2B4193113D5C260EB195
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis