Joe Sandbox Cloud BASIC

ID: 431752
Sample Name:
2FQhmYZME4.exe
Cookbook: default.jbs
Time: 08:48:15
Date: 09/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

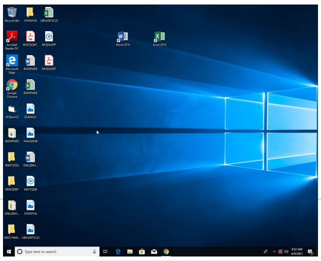
Analysis Report 2FQhmYZME4.exe

Overview

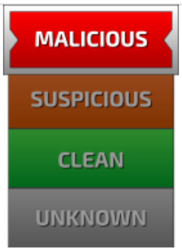
General Information

Sample Name:	2FQhmYZME4.exe
Analysis ID:	431752
MD5:	196b3c910b8d74..
SHA1:	37968cade61e54..
SHA256:	4f6b4079a3f1b56..
Tags:	exe GuLoader
Infos:	

Most interesting Screenshot:



Detection



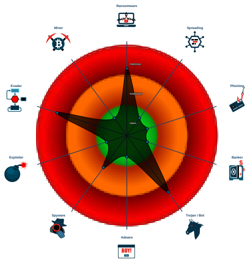
GuLoader

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Potential malicious icon found
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Found potential dummy code loops (…
- Tries to detect virtualization through…
- Abnormal high CPU Usage
- Contains functionality for execution …
- Contains functionality to call native f…

Classification



Process Tree

- **System is w10x64**
- 2FQhmYZME4.exe (PID: 6960 cmdline: 'C:\Users\user\Desktop\2FQhmYZME4.exe' MD5: 196B3C910B8D74C5916029F6EB037D5D)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://myurl/myfile.bin"
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
2FQhmYZME4.exe	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000000.645109161.0000000000401000.00000020.00020000.sdmp	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
00000001.00000002.1167637296.0000000000401000.00000020.00020000.sdmp	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
1.0.2FQhmYZME4.exe.400000.0.unpack	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
1.2.2FQhmYZME4.exe.400000.0.unpack	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Potential malicious icon found

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

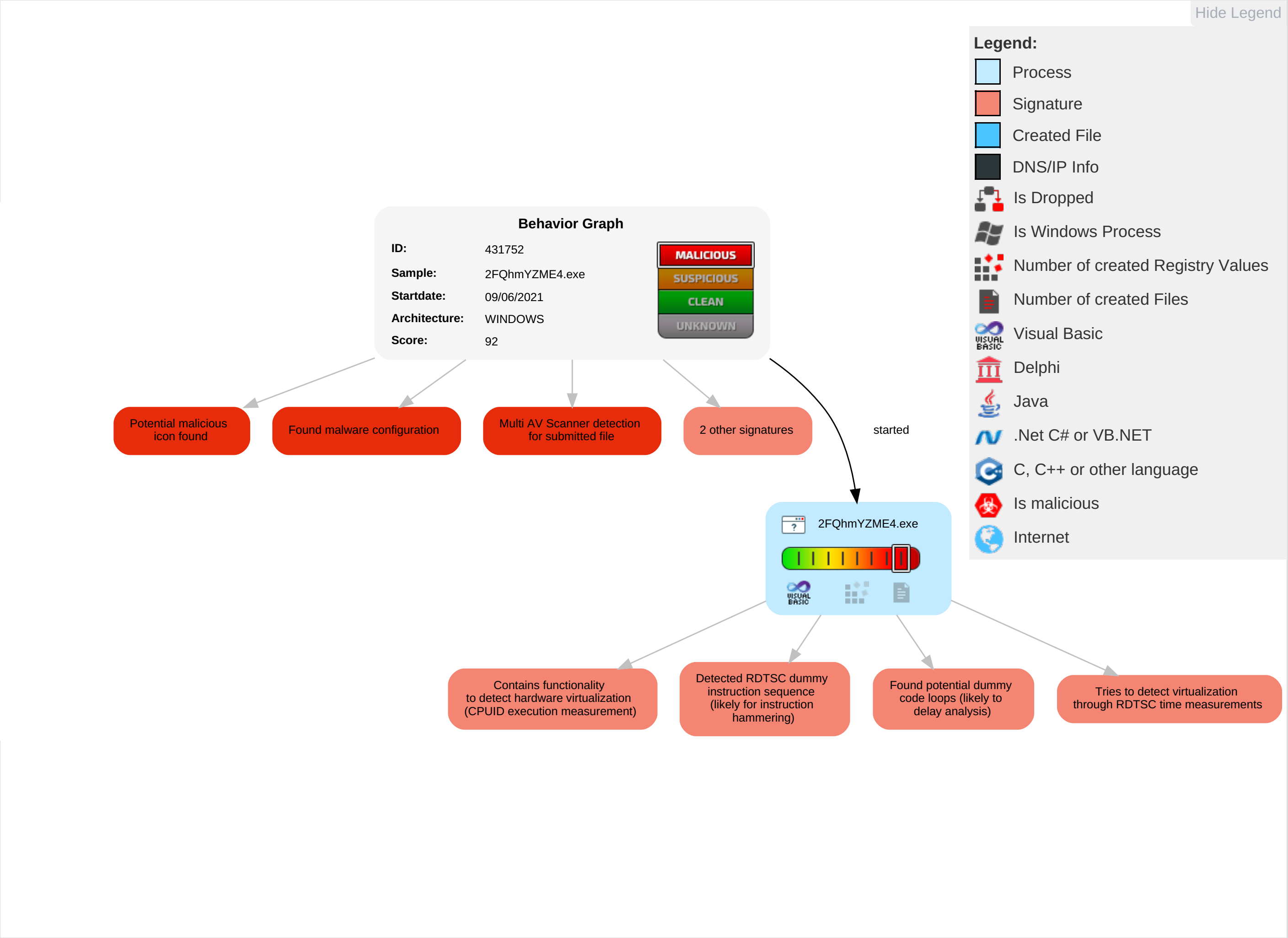
Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Ef
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	Input Capture 1	Security Software Discovery 4 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Re Tr W Au
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Re W W Au

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Ef
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 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	Ol De Cl Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 3 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Behavior Graph



Behavior Graph

ID: 431752
Sample: 2FQhmYZME4.exe
Startdate: 09/06/2021
Architecture: WINDOWS
Score: 92

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
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Potential malicious icon found
Found malware configuration
Multi AV Scanner detection for submitted file
2 other signatures
started
2FQhmYZME4.exe
Contains functionality to detect hardware virtualization (CPUID execution measurement)
Detected RDTSC dummy instruction sequence (likely for instruction hammering)
Found potential dummy code loops (likely to delay analysis)
Tries to detect virtualization through RDTSC time measurements

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
2FQhmYZME4.exe	26%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://myurl/myfile.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://myurl/myfile.bin	true	• Avira URL Cloud: safe	low

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	431752
Start date:	09.06.2021
Start time:	08:48:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	2FQhmYZME4.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:	19
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:	mal92.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
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

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

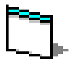
No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.650237570705559
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:	2FQhmYZME4.exe
File size:	147456
MD5:	196b3c910b8d74c5916029f6eb037d5d
SHA1:	37968cade61e54ce0c4ec24e83c35fadd583019f
SHA256:	4f6b4079a3f1b56421cbca34d112ba6a867ff8a6bd706010bfe931ac6d635361
SHA512:	94197b2135bf0317494a30c1e800b3dba1fcc0a76299627 f2361cfadafbf245dca47b8abbe9530d94f1b65013d5eccff e1e11af241c44425870553be6660d95c
SSDEEP:	1536:IFXJHkDZ+2HdXrK5feyoSP+6a3bQQ6GaXSt4lY5YGw12IjqQRsk:CJiUEXrKIIPcl6o4lBGw12IuMsk
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......M.....................0............... ....@................

File Icon



Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401c10
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:	0x4DF9EBE1 [Thu Jun 16 11:41:21 2011 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:	9b8686288ab82fdbf8ede30bc55c83b7

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x20568	0x21000	False	0.359463778409	data	5.90249486753	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x22000	0x1250	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x24000	0x950	0x1000	False	0.17138671875	data	2.02462742549	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

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: 2FQhmYZME4.exe PID: 6960 Parent PID: 5796

General

Start time:	08:49:02
Start date:	09/06/2021
Path:	C:\Users\user\Desktop\2FQhmYZME4.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\2FQhmYZME4.exe'
Imagebase:	0x400000
File size:	147456 bytes
MD5 hash:	196B3C910B8D74C5916029F6EB037D5D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000001.00000000.645109161.0000000000401000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000001.00000002.1167637296.0000000000401000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 32.0.0 Black Diamond