ID: 527215
Sample Name:
Doc0011222003.exe
Cookbook: default.jbs
Time: 14:27:15
Date: 23/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

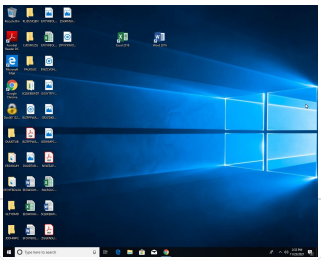
Windows Analysis Report Doc0011222003.exe

Overview

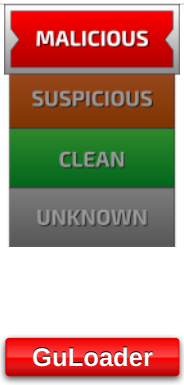
General Information

Sample Name:	Doc0011222003.exe
Analysis ID:	527215
MD5:	e70022c5636db7..
SHA1:	4589b37f02bb95d.
SHA256:	0226b26f82ea7ab.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

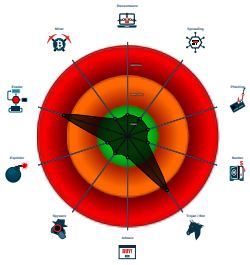


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected GuLoader
- Found potential dummy code loops (…
- Tries to detect virtualization through…
- Uses 32bit PE files
- Sample file is different than original …
- PE file contains strange resources
- Program does not show much activi…
- Uses code obfuscation techniques (…
- Abnormal high CPU Usage

Classification



Process Tree

- **System is w10x64**
- Doc0011222003.exe (PID: 5604 cmdline: "C:\Users\user\Desktop\Doc0011222003.exe" MD5: E70022C5636DB76B71C8B2C56552C60C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.826048690.00000000004F0000.00000040.00000010.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

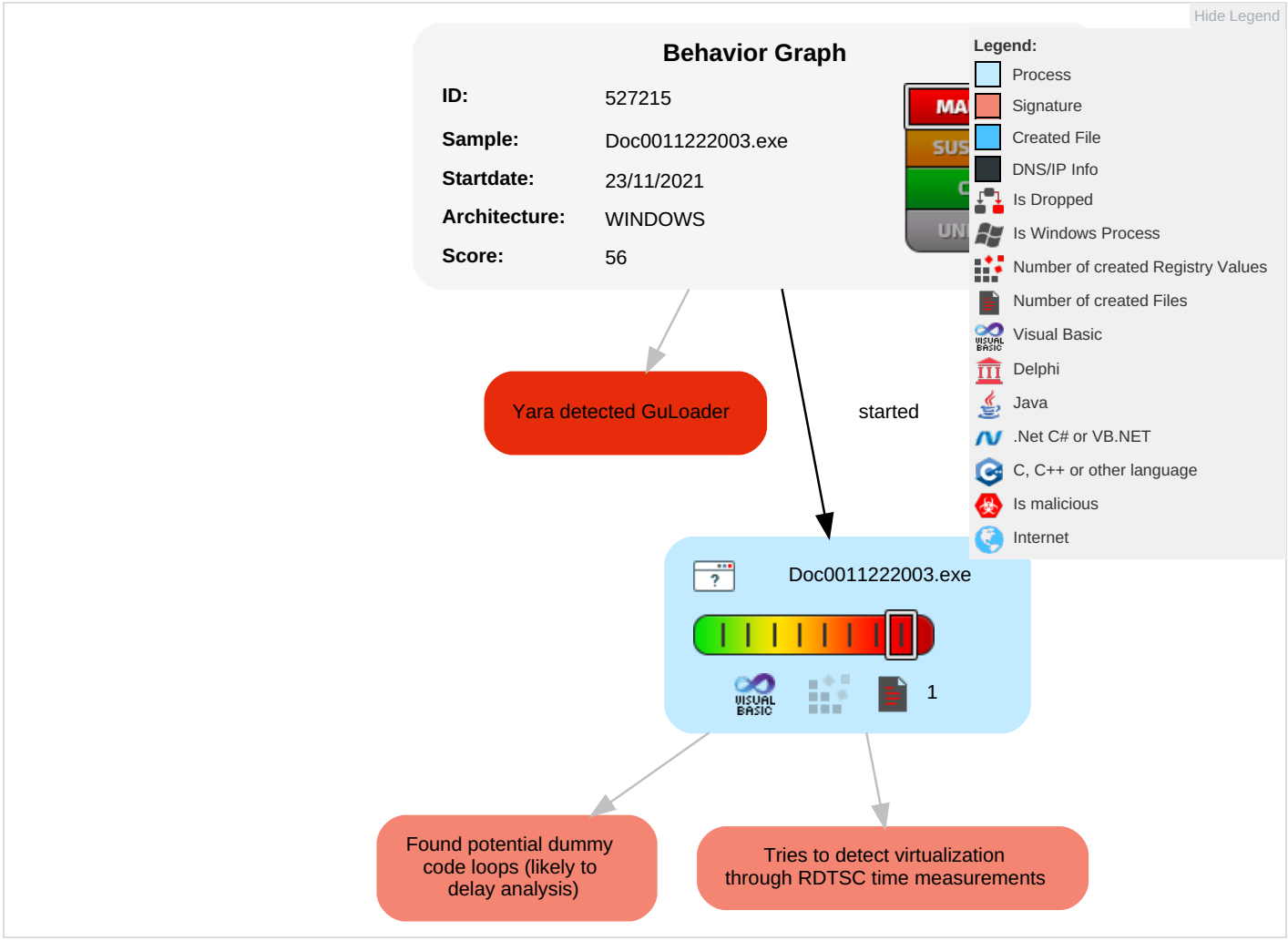
Anti Debugging:

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 2	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	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 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

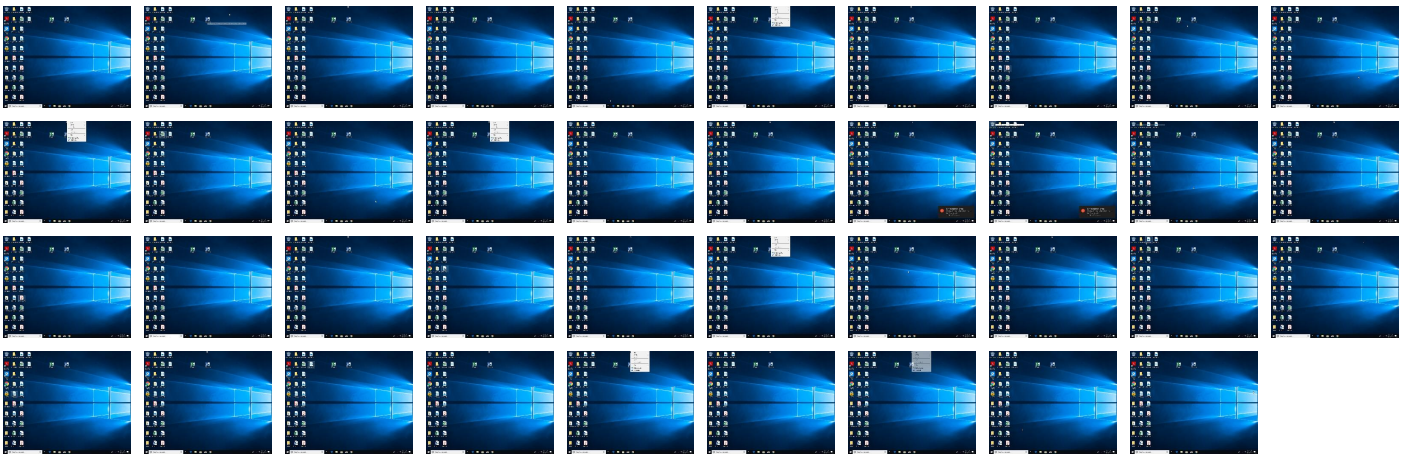
Behavior Graph



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

No Antivirus matches

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:	34.0.0 Boulder Opal
Analysis ID:	527215
Start date:	23.11.2021
Start time:	14:27:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Doc0011222003.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:	17
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:	mal56.troj.evad.winEXE@1/1@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 33.7% (good quality ratio 13%) • Quality average: 16.9% • Quality standard deviation: 24.4%
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

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

C:\Users\user\AppData\Local\Temp\~DFC89CDF2998EDD482.TMP	
Process:	C:\Users\user\Desktop\Doc0011222003.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.3424693381122756
Encrypted:	false
SSDEEP:	48:rMereSiNgxcqYmOCA3OgUTZzR+MYVAJf3L:onTFCSBUTZzgMYVA
MD5:	8BE47FF78C4F694E6577D8CB72B022C9
SHA1:	A32191D769A55B59B38A93EBEA848166EA27F0D6
SHA-256:	A1005C0FAF60AA8C70AD16C4369E6D3FA2357687BC10EE55656363B01DDD633E
SHA-512:	D19109A2AB8141E8A7AF066204652CEE0938A10B45E46B929C825B4844323FB6D184F1BA90D8007ADEAC0CE31F84F25B482153DEA1BEA881E7B5ABE43545A2A3
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.527320740089958
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:	Doc0011222003.exe
File size:	81920
MD5:	e70022c5636db76b71c8b2c56552c60c
SHA1:	4589b37f02bb95d26bb2ba369c46c99268ce2985
SHA256:	0226b26f82ea7ab25ad85a4cfda530f7b28f91b1d57f8ca0361b7b03e8ce59bb
SHA512:	d9d16ded54f7424145aba6f423b82ab4c010cc1ee67acb152a1d79b61f23fedc9250dd482b78e3c84ac4b82cdc9283099a06ee5a2d5d14d34e78734f60dd7f61

General

SSDEEP:	1536:tGs2yzOSOXbgSXZXMyETdwDgL/UQdz+mehpITwHM/kho:tGOzvOXbgSXZXA2Dk/UQHehiTMM8o
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i.....*.....Rich.....PE..L....e.L.....0..... ....@.....

File Icon

Icon Hash:	78ecccecccceec70

Static PE Info

General

Entrypoint:	0x4013cc
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:	0x4CDA65A9 [Wed Nov 10 09:28:09 2010 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:	37fe5edb896809a8dcea667d1a5d3341

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x10bb4	0x11000	False	0.628547219669	data	7.08459440381	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x12000	0x1428	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x14000	0xe08	0x1000	False	0.452880859375	data	4.20020036066	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: Doc0011222003.exe PID: 5604 Parent PID: 6080

General

Start time:	14:29:09
Start date:	23/11/2021
Path:	C:\Users\user\Desktop\Doc0011222003.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Doc0011222003.exe"
Imagebase:	0x400000
File size:	81920 bytes
MD5 hash:	E70022C5636DB76B71C8B2C56552C60C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.826048690.00000000004F0000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis