

JOeSandbox Cloud BASIC



ID: 431163

Sample Name:

Odeme_310521657_876007850.exe

Cookbook: default.jbs

Time: 14:46:17

Date: 08/06/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report Odeme_310521657_876007850.exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Overview	3
Initial Sample	3
Sigma Overview	3
Signature Overview	3
AV Detection:	4
System Summary:	4
Data Obfuscation:	4
Malware Analysis System Evasion:	4
Anti Debugging:	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	7
Contacted Domains	7
Contacted IPs	7
General Information	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	8
IPs	8
Domains	8
ASN	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	8
General	8
File Icon	8
Static PE Info	8
General	9
Entrypoint Preview	9
Data Directories	9
Sections	9
Resources	9
Imports	9
Version Infos	9
Possible Origin	9
Network Behavior	9
Code Manipulations	9
Statistics	9
System Behavior	10
Analysis Process: Odeme_310521657_876007850.exe PID: 6940 Parent PID: 5828	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10

Analysis Report Odeme_310521657_876007850.exe

Overview

General Information

Sample Name:

Odeme_310521657_876007850.exe

Analysis ID:

431163

MD5:

391ca3cf343a25b..

SHA1:

07392a3e453fbf5..

SHA256:




6abdca229afbc80..

Tags:

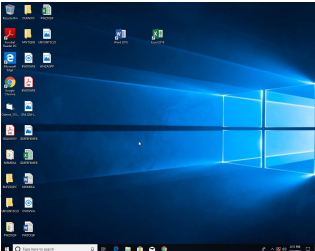
exe

GuLoader

Infos:

Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

GuLoader

Score:

80

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Multi AV Scanner detection for subm...

Potential malicious icon found

Yara detected GuLoader

Contains functionality to detect hard...

Detected RDTSC dummy instruction...

Found potential dummy code loops (...)

Tries to detect virtualization through...

Abnormal high CPU Usage

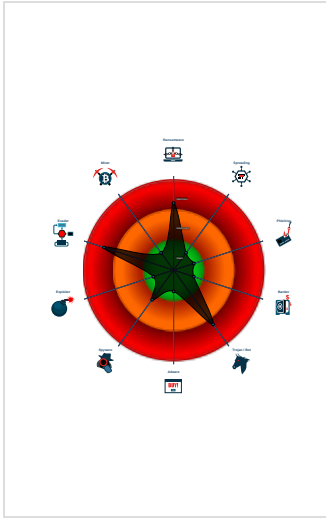
Contains functionality for execution ...

Contains functionality to call native f...

Contains functionality to read the PEB


Creates a DirectInput object (often fo...

Classification



Process Tree

System is w10x64

 Odeme_310521657_876007850.exe (PID: 6940 cmdline: 'C:\Users\user\Desktop\Odeme_310521657_876007850.exe' MD5: 391CA3CF343A25BFD2B452478E54591B)

cleanup

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Odeme_310521657_876007850.exe	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:



Multi AV Scanner detection for submitted file

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:

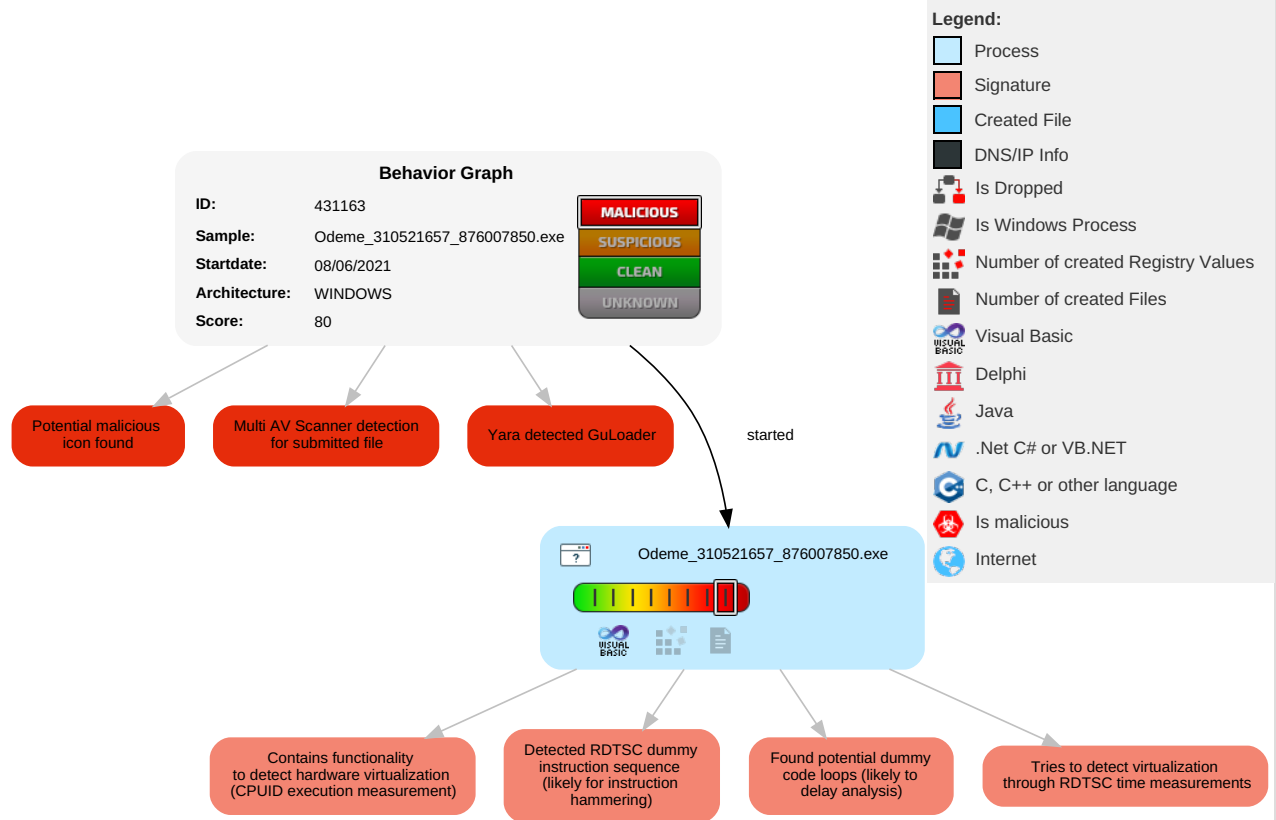


Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Recovery
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	Recovery
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	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Recovery
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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Be

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
Odeme_310521657_876007850.exe	32%	ReversingLabs	Win32.Trojan.Graftor	

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:	32.0.0 Black Diamond
Analysis ID:	431163
Start date:	08.06.2021
Start time:	14:46:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Odeme_310521657_876007850.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:	<ul style="list-style-type: none">• HCA enabled• EGA enabled• HDC enabled• AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none">• Successful, ratio: 5.4% (good quality ratio 1.3%)• Quality average: 13.8%• Quality standard deviation: 25.2%
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none">• 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):	4.618776972416774
TrID:	<ul style="list-style-type: none">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:	Odeme_310521657_876007850.exe
File size:	147456
MD5:	391ca3cf343a25bfd2b452478e54591b
SHA1:	07392a3e453bf57a85190e0342e15c83e4eaffb
SHA256:	6abdca229afbc8050590a71d0a4be6dcaaaa44725e19d4eab23df6152465116d
SHA512:	dc230172a32d092f3a34a94d3bfaf05d07e6ae657d6898acfd02a11b53f677bfb81513bcb98678baa7c508b70d3fac8e137233a555e7def301667217d5073f516
SSDEEP:	1536:t28QwqzWiG9dErUYmetkhpRnV3hRHOjSfteYwThUIHkfA2S0:cMoWiG4rUVetWvRHOjSftnwTSIHkv
File Content Preview:	MZ.....@.....!..!Th is program cannot be run in DOS mode...\$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L.....`.....0..... @.....

File Icon

	
Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x4014b8
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:	0x60BF1EFE [Tue Jun 8 07:40:46 2021 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:	b1d5215cf0ff1abab4dacdc311d642d4

Entrypoint Preview

Data Directories

Sections


Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2002c	0x21000	False	0.328095407197	data	4.86222481282	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x22000	0x1234	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x24000	0xa04	0x1000	False	0.181640625	data	2.18911865835	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
Sesotho (Sutu)	South Africa	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: Odeme_310521657_876007850.exe PID: 6940 Parent PID: 5828

General

Start time:	14:47:03
Start date:	08/06/2021
Path:	C:\Users\user\Desktop\Odeme_310521657_876007850.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Odeme_310521657_876007850.exe'
Imagebase:	0x400000
File size:	147456 bytes
MD5 hash:	391CA3CF343A25BFD2B452478E54591B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis