

JOeSandbox Cloud BASIC



ID: 502566

Sample Name: Orden de
compra M244545.exe

Cookbook: default.jbs

Time: 04:05:24

Date: 14/10/2021

Version: 33.0.0 White Diamond


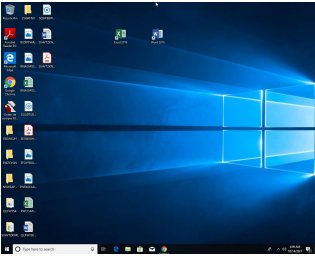
Table of Contents

Table of Contents	2
Windows Analysis Report Orden de compra M244545.exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Threatname: GuLoader	3
Yara Overview	3
Memory Dumps	3
Sigma Overview	3
Jbx Signature Overview	3
AV Detection:	4
Networking:	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	6
Contacted Domains	7
Contacted IPs	7
General Information	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	7
IPs	7
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	8
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	9
Analysis Process: Orden de compra M244545.exe PID: 7096 Parent PID: 5104	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10




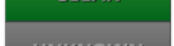

Windows Analysis Report Orden de compra M244545.exe

Overview

General Information

Sample Name:	Orden de compra M244545.exe
Analysis ID:	502566
MD5:	7c04ecf5dc69998..
SHA1:	905c177e8ea3a2..
SHA256:	cf7bd1c802c044a..
Tags:	exe guloader
Infos:	
Most interesting Screenshot:	
	

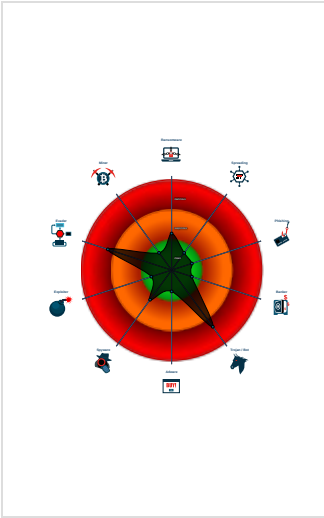
Detection

	
	
	
	
	
Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%


Signatures

Found malware configuration
Yara detected GuLoader
Found potential dummy code loops (...)
Tries to detect virtualization through...
C2 URLs / IPs found in malware con...
Creates a DirectInput object (often fo...
Uses 32bit PE files
Contains functionality to call native f...
Sample file is different than original ...
Contains functionality to read the PEB
Program does not show much activi...
Uses code obfuscation techniques (...)

Classification



Process Tree

System is w10x64
 Orden de compra M244545.exe (PID: 7096 cmdline: 'C:\Users\user\Desktop\Orden de compra M244545.exe' MD5: 7C04ECF5DC6999877E87CF9C1C933A3F)
cleanup

Malware Configuration

Threatname: GuLoader

<pre>{ "Payload URL": "https://drive.google.com/uc?export=download&id=13CKgFgBbMK4vER" }</pre>
--

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.815267418.0000000000217 0000.00000040.00000001.sdump	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

AV Detection:



Found malware configuration

Networking:



C2 URLs / IPs found in malware configuration

Data Obfuscation:



Yara detected GuLoader

Malware Analysis System Evasion:



Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

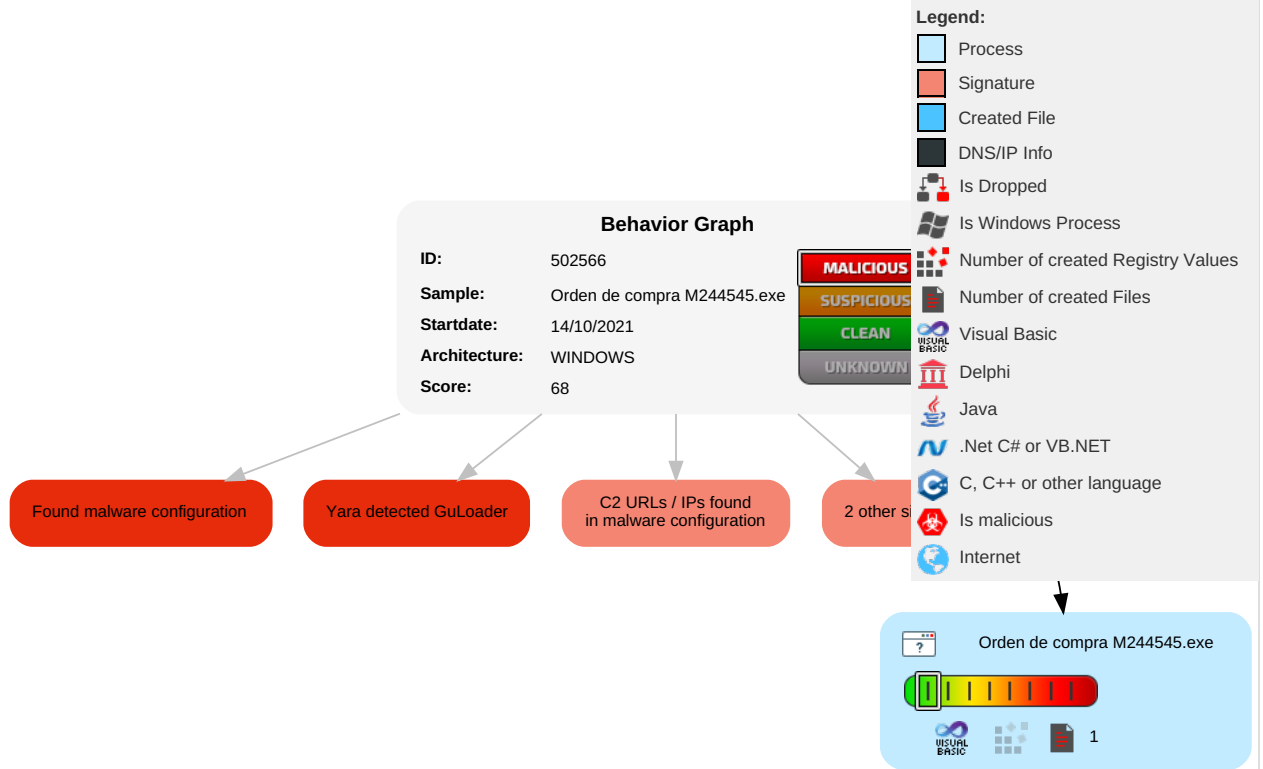


Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Recovery
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	Input Capture 1	Security Software Discovery 2 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	Application Layer Protocol 1	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	Recovery
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Recovery

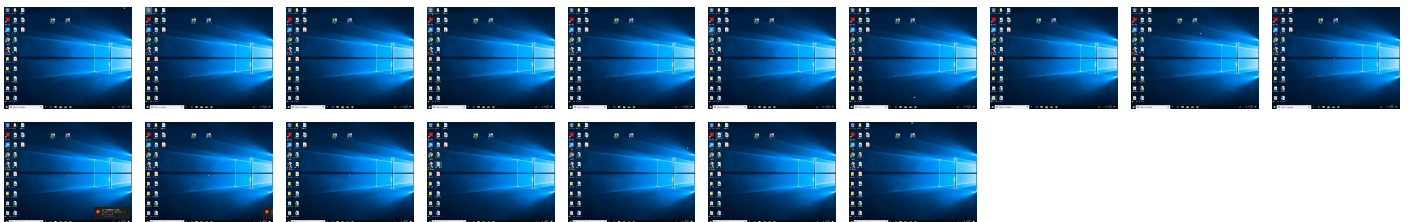
Behavior Graph



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:	33.0.0 White Diamond
Analysis ID:	502566
Start date:	14.10.2021
Start time:	04:05:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Orden de compra M244545.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:	23
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:	mal68.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none">• Successful, ratio: 21% (good quality ratio 11.9%)• Quality average: 38%• Quality standard deviation: 38.1%
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):	5.7855993258224325
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:	Orden de compra M244545.exe
File size:	98304
MD5:	7c04ecf5dc6999877e87cf9c1c933a3f
SHA1:	905c177e8ea3a2173e322c13b25cd156bd6dea39
SHA256:	cf7bd1c802c044a777529246743d3a5c907e4c02a29525afe2c48daee9b2fd9d
SHA512:	125d0c2e70138bac0c6fb7416085b993c24ed67a8881be2b5f6a9361f4814dbd0084b99b182d7275d02ee0dcb877f8ad5c04f7711a454abf7359c5ef4aaf8459
SSDEEP:	1536:tNDLZynUIR5qVCSbwmNYDsbYFSrZbQFsnD+ljjDID:tNB7U5qVC8wkkFg73jDI
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode.....\$......i.....*.....Rich.....PE..L.....K..... @...0.....P....@.....

File Icon

	
Icon Hash:	69e1c892f664c884

Static PE Info

General

Entrypoint:	0x4012b4
Entrypoint Section:	.text
Digitally signed:	false

General	
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4BCDC590 [Tue Apr 20 15:17:36 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:	3d3cd1bd8dcc611a5734bf41f4e1a6a6

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x13518	0x14000	False	0.510925292969	data	6.24325085767	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x15000	0xcc4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x16000	0x1c2a	0x2000	False	0.346069335938	data	3.69516488298	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

General

Start time:	04:06:20
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\Orden de compra M244545.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Orden de compra M244545.exe'
Imagebase:	0x400000
File size:	98304 bytes
MD5 hash:	7C04ECF5DC6999877E87CF9C1C933A3F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	<ul style="list-style-type: none">Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.815267418.0000000002170000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

[Show Windows behavior](#)

Disassembly

Code Analysis