

JoeSandbox Cloud BASIC



ID: 456986

Sample Name:

ogvcqbOEQs.exe

Cookbook: default.jbs

Time: 18:03:24

Date: 30/07/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report ogvcqbOEQs.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	4
AV Detection:	4
Networking:	4
Data Obfuscation:	4
Malware Analysis System Evasion:	4
Anti Debugging:	4
HIPS / PFW / Operating System Protection Evasion:	4
Stealing of Sensitive Information:	4
Mitre Att&ck Matrix	4
Behavior Graph	5
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	7
Domains and IPs	7
Contacted Domains	7
Contacted URLs	7
Contacted IPs	7
General Information	7
Simulations	8
Behavior and APIs	8
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	9
Static PE Info	9
General	9
Entrypoint Preview	9
Data Directories	9
Sections	9
Resources	9
Imports	9
Version Infos	9
Possible Origin	9
Network Behavior	10
Code Manipulations	10
Statistics	10
Behavior	10
System Behavior	10
Analysis Process: ogvcqbOEQs.exe PID: 7100 Parent PID: 6112	10
General	10
File Activities	10
Analysis Process: ieinstal.exe PID: 6160 Parent PID: 7100	10
General	11
Disassembly	11
Code Analysis	11

Windows Analysis Report ogvcqbOEQs.exe

Overview

General Information

Sample Name:

ogvcqbOEQs.exe

Analysis ID:

456986

MD5:

f00e0bf11a316d6..

SHA1:

a25674d3d8285a..

SHA256:

06b51823317ace..

Tags:

32 exe

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

GuLoader

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

Signatures

Found malware configuration

GuLoader behavior detected

Multi AV Scanner detection for subm...

Yara detected GuLoader

C2 URLs / IPs found in malware con...

Contains functionality to detect hard...

Detected RDTSC dummy instruction...

Found potential dummy code loops (...)

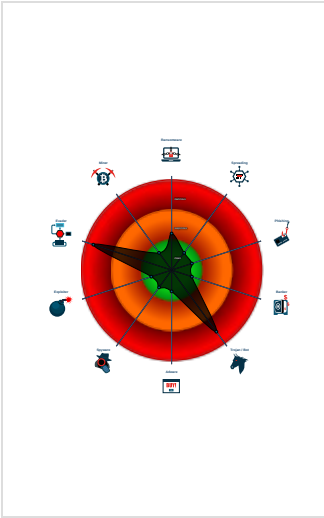
Hides threads from debuggers

Tries to detect Any.run

Tries to detect sandboxes and other...

Tries to detect virtualization through...

Classification



Process Tree

System is w10x64

ogvcqbOEQs.exe (PID: 7100 cmdline: 'C:\Users\user\Desktop\ogvcqbOEQs.exe' MD5: F00E0BF11A316D65AB59574825F125BF)

ieinstal.exe (PID: 6160 cmdline: 'C:\Users\user\Desktop\ogvcqbOEQs.exe' MD5: DAD17AB737E680C47C8A44CBB95EE67E)

cleanup

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://d-bin.duckdns.org/remcos_dyno_xLTzJv"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.1721956987.0000000000C 10000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000000.00000002.1311529373.00000000021 F0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	


Sigma Overview

No Sigma rule has matched

Copyright Joe Security LLC 2021

Page 3 of 11

Jbx 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

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 Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:



Found potential dummy code loops (likely to delay analysis)

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:



Writes to foreign memory regions

Stealing of Sensitive Information:



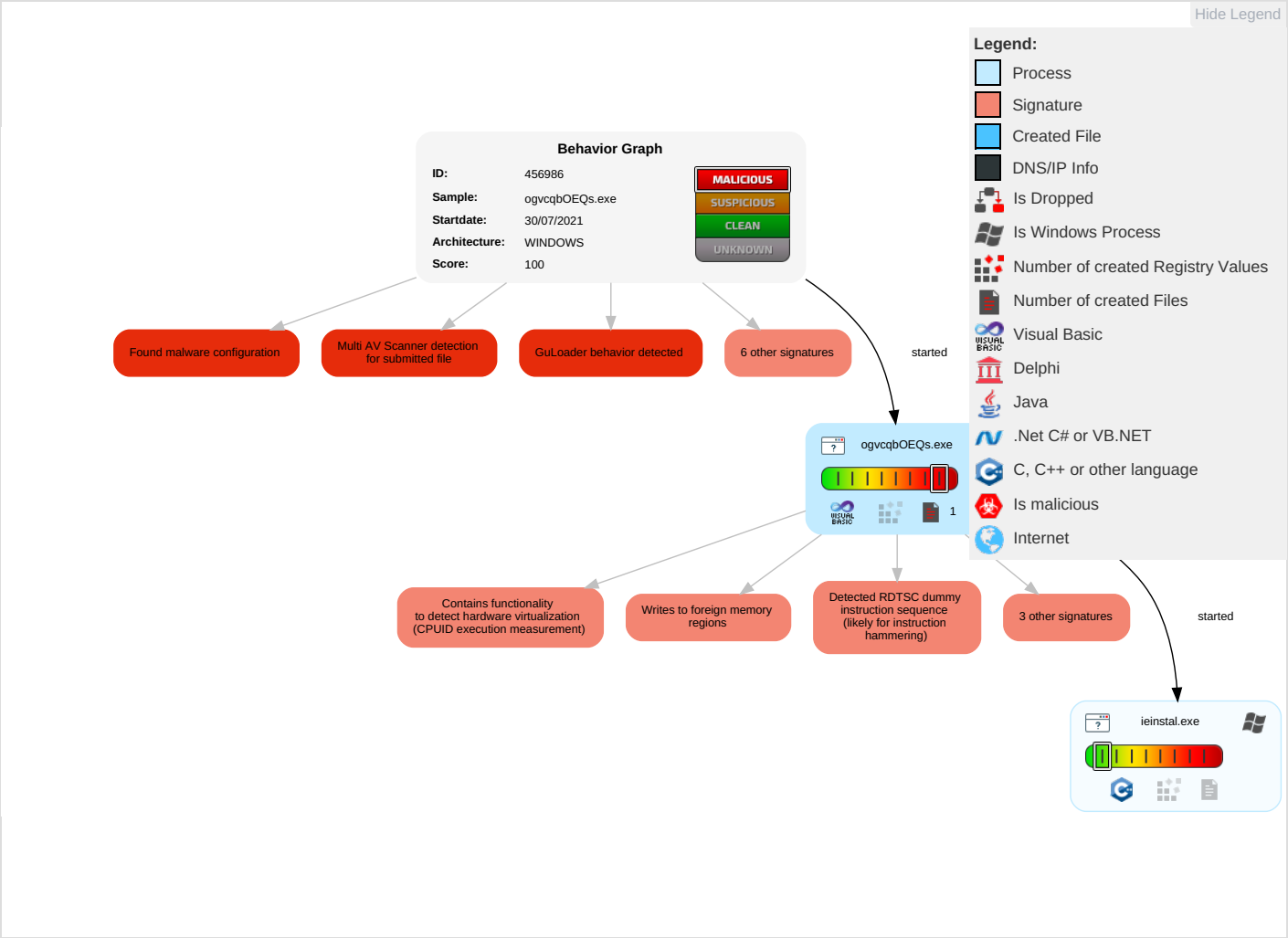
GuLoader behavior detected

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1 2	Virtualization/Sandbox Evasion 3 1 1	OS Credential Dumping	Security Software Discovery 7 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 1 2	LSASS Memory	Virtualization/Sandbox Evasion 3 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS
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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 3 2	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

Source	Detection	Scanner	Label	Link
ogvcqbOEQs.exe	19%	Virustotal		Browse
ogvcqbOEQs.exe	11%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://d-bin.duckdns.org/remcos_dyno_xLTzJv	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://d-bin.duckdns.org/remcos_dyno_xLTzJv	true	<ul style="list-style-type: none">Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	456986
Start date:	30.07.2021
Start time:	18:03:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 19m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ogvcqbOEQs.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
Run name:	Suspected Instruction Hammering Hide Perf
Number of analysed new started processes analysed:	28
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 enabledEGA enabledHDC enabledAMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@3/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none">Successful, ratio: 26% (good quality ratio 14%)Quality average: 31.6%Quality standard deviation: 35.4%
HCA Information:	<ul style="list-style-type: none">Successful, ratio: 69%Number of executed functions: 0Number of non-executed functions: 0
Cookbook Comments:	<ul style="list-style-type: none">Adjust boot timeEnable AMSIFound application associated with file extension: .exe
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):	7.998638224332722
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:	ogvcqbOEQs.exe
File size:	10571776
MD5:	f00e0bf11a316d65ab59574825f125bf
SHA1:	a25674d3d8285ad9216e61cfe923bc4b4a0c833a
SHA256:	06b51823317ace5ebfb38121fce872db43c72042d7ef657e3830d46c5572f0c3
SHA512:	3330bdeb213a3e8f2ec104a7018bf4accdd715b4eb7891f2cf29e8a2a3b5109ef143beba0ba51c5e13d92d5992dc9c809c52b1aa181c265d950e181a6a8c14fd

General

SSDEEP:	24576:tkELLVtinQL/2HkZQwTLniGZQwCwTrVtLTrzVQe2wCwX:SnGOHHQiGuHHHwCQ
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$......i.....*.....Rich.....PE..L...JQW.....0.....d.....@.....

File Icon

	
Icon Hash:	e2b0d8d8d2d8c400

Static PE Info

General

Entrypoint:	0x401364
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:	0x57514AAD [Fri Jun 3 09:15:25 2016 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:	9c8c8bb37b14de578924ac09be0d5cc5

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x105dc	0x11000	False	0.509966681985	data	6.08573946634	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x12000	0xd24	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x13000	0x12a4	0x2000	False	0.166381835938	data	2.77658216516	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

Language of compilation system	Country where language is spoken	Map
English	United States	


Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

 Click to jump to process

System Behavior

Analysis Process: ogvcqbOEQs.exe PID: 7100 Parent PID: 6112

General

Start time:	18:04:07
Start date:	30/07/2021
Path:	C:\Users\user\Desktop\ogvcqbOEQs.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ogvcqbOEQs.exe'
Imagebase:	0x400000
File size:	10571776 bytes
MD5 hash:	F00E0BF11A316D65AB59574825F125BF
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: 00000000.00000002.1311529373.00000000021F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: ieinstal.exe PID: 6160 Parent PID: 7100

General	
Start time:	18:08:15
Start date:	30/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\logvcqbOEQs.exe'
Imagebase:	0xf40000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	<ul style="list-style-type: none"> Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000D.00000002.1721956987.0000000000C10000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Disassembly

Code Analysis