

JoeSandbox Cloud BASIC



ID: 450819

Sample Name: VZghv7yI7g

Cookbook: default.jbs

Time: 18:34:13

Date: 19/07/2021

Version: 33.0.0 White Diamond



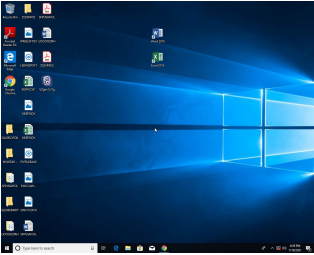
Table of Contents

Table of Contents	2
Windows Analysis Report VZghv7yl7g	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	7
Contacted Domains	7
Contacted URLs	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	9
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	10
Statistics	10
System Behavior	10
Analysis Process: VZghv7yl7g.exe PID: 2256 Parent PID: 5616	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10


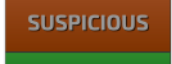
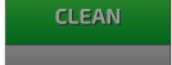


Windows Analysis Report VZghv7yl7g

Overview

General Information

Sample Name:	VZghv7yl7g (renamed file extension from none to exe)
Analysis ID:	450819
MD5:	73bb5c4b690b8d..
SHA1:	60adddd91b6038..
SHA256:	a3feb5265e6d027.
Infos:	 
Most interesting Screenshot:	
	

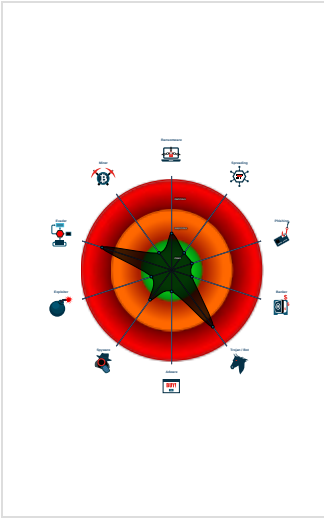
Detection

	
	
	
	
	
Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Found malware configuration
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 (...)
Tries to detect virtualization through...
Abnormal high CPU Usage
Contains functionality for execution ...
Contains functionality to query CPU ...
Contains functionality to read the PEB

Classification



Process Tree

System is w10x64
 VZghv7yl7g.exe (PID: 2256 cmdline: 'C:\Users\user\Desktop\VZghv7yl7g.exe' MD5: 73BB5C4B690B8D6DF88D6BC18FB3A553)
cleanup

Malware Configuration

Threatname: GuLoader

<pre>{ "Payload URL": "https://banontarquitectura.com.mx/IRANSAT_kowbB4.bi}"</pre>
--

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.756540382.0000000000225 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

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 virtualization through RDTSC time measurements

Anti Debugging:

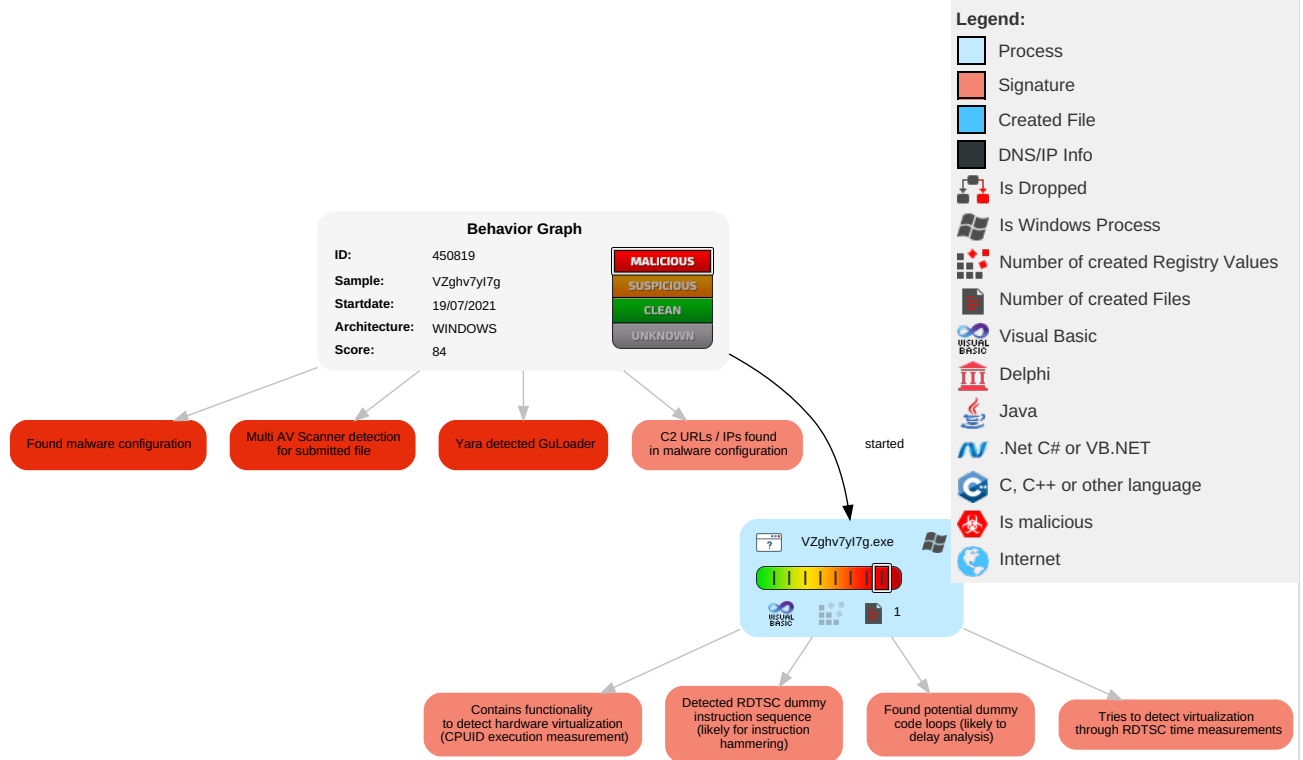


Found potential dummy code loops (likely to delay analysis)

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	OS Credential Dumping	Security Software Discovery 4 1	Remote Services	Archive Collected Data 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	Data from Removable Media	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 3 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

Source	Detection	Scanner	Label	Link
VZghv7yl7g.exe	30%	Virustotal		Browse
VZghv7yl7g.exe	13%	ReversingLabs	Win32.Backdoor.Remcos	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
https://bamontarquitectura.com.mx/IRANSAT_kowbB4.bi	0%	Virustotal		Browse
https://bamontarquitectura.com.mx/IRANSAT_kowbB4.bi	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://bamontarquitectura.com.mx/IRANSAT_kowbB4.bj}	true	<ul style="list-style-type: none">0%, Virustotal, BrowseAvira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	450819
Start date:	19.07.2021
Start time:	18:34:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	VZghv7yl7g (renamed file extension from none to 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:	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:	mal84.troj.evad.winEXE@1/0@0/0
EGA Information:	<ul style="list-style-type: none">Successful, ratio: 100%
HDC Information:	<ul style="list-style-type: none">Successful, ratio: 61.1% (good quality ratio 26.9%)Quality average: 24.1%Quality standard deviation: 32.8%
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none">Adjust boot timeEnable AMSIOverride 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):	6.2221702126738
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:	VZghv7yl7g.exe
File size:	241664
MD5:	73bb5c4b690b8d6df88d6bc18fb3a553
SHA1:	60adddd91b6038fc9d819cf6d647ce3be0b11d38
SHA256:	a3feb5265e6d02710f04ff618e966e9da9ba8fc8dc5692d6f7633fe0a3037b66
SHA512:	9c023dc66d9bcfb2f5bc0274001d92948ac058fc8765d2178907dfd8fb9885ede57acc3836d583ad97516dce1a97c50f081800b41a1f42ea938efb8b23e87567
SSDEEP:	3072:+3BepJlZa/xao5JKwl7V4R4iUW/qcijw2HJlZapGBR:EiUIo5JKPgU99vHP
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L...WS.N.....0...@.....

File Icon



Icon Hash: f8fcd4ccf4e4e8d0

Static PE Info

General

Entrypoint:	0x4019b0
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:	0x4EA15357 [Fri Oct 21 11:11:19 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:	e9f7dd0da1a2a1266893e1ae4ef42b67

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x318a4	0x32000	False	0.39177734375	data	6.3764832494	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x33000	0x1290	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x35000	0x6d0a	0x7000	False	0.481689453125	data	5.46300019784	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: VZghv7yl7g.exe PID: 2256 Parent PID: 5616

General

Start time:	18:35:02
Start date:	19/07/2021
Path:	C:\Users\user\Desktop\VZghv7yl7g.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\VZghv7yl7g.exe'
Imagebase:	0x400000
File size:	241664 bytes
MD5 hash:	73BB5C4B690B8D6DF88D6BC18FB3A553
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: 00000000.00000002.756540382.0000000002250000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis