

JOeSandbox Cloud BASIC



ID: 501857

Sample Name:

ZAM#U00d3WIENIE.exe

Cookbook: default.jbs

Time: 10:38:13

Date: 13/10/2021

Version: 33.0.0 White Diamond





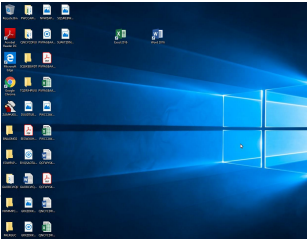
Table of Contents

Table of Contents	2
Windows Analysis Report ZAM#U00d3WIENIE.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	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: ZAM#U00d3WIENIE.exe PID: 2904 Parent PID: 1744	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10

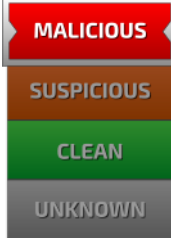
Windows Analysis Report ZAM#U00d3WIENIE.exe

Overview

General Information

Sample Name:	ZAM#U00d3WIENIE.exe
Analysis ID:	501857
MD5:	328b34adced9ad..
SHA1:	fa03cb6529d634b..
SHA256:	95f59bb24f6c239..
Tags:	
Infos:	  
Most interesting Screenshot:	
	

Detection

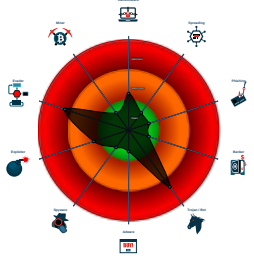


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%


Signatures

- Found malware configuration
- Multi AV Scanner detection for subm...
- Yara detected GuLoader
- Tries to detect virtualization through...
- C2 URLs / IPs found in malware con...
- Found potential dummy code loops (...)
- Uses 32bit PE files
- Found inlined nop instructions (likely...
- Sample file is different than original ...
- Contains functionality to read the PEB
- Uses code obfuscation techniques (...)
- Detected potential crypto function

Classification



Process Tree

- System is w10x64
-  **ZAM#U00d3WIENIE.exe** (PID: 2904 cmdline: 'C:\Users\user\Desktop\ZAM#U00d3WIENIE.exe' MD5: 328B34ADCED9AD8128D4079BCFFDE016)
- cleanup

Malware Configuration

Threatname: GuLoader

```
"Payload URL": "https://drive.google.com/uc?export=download&i"
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.808037224.0000000002A3 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:



Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

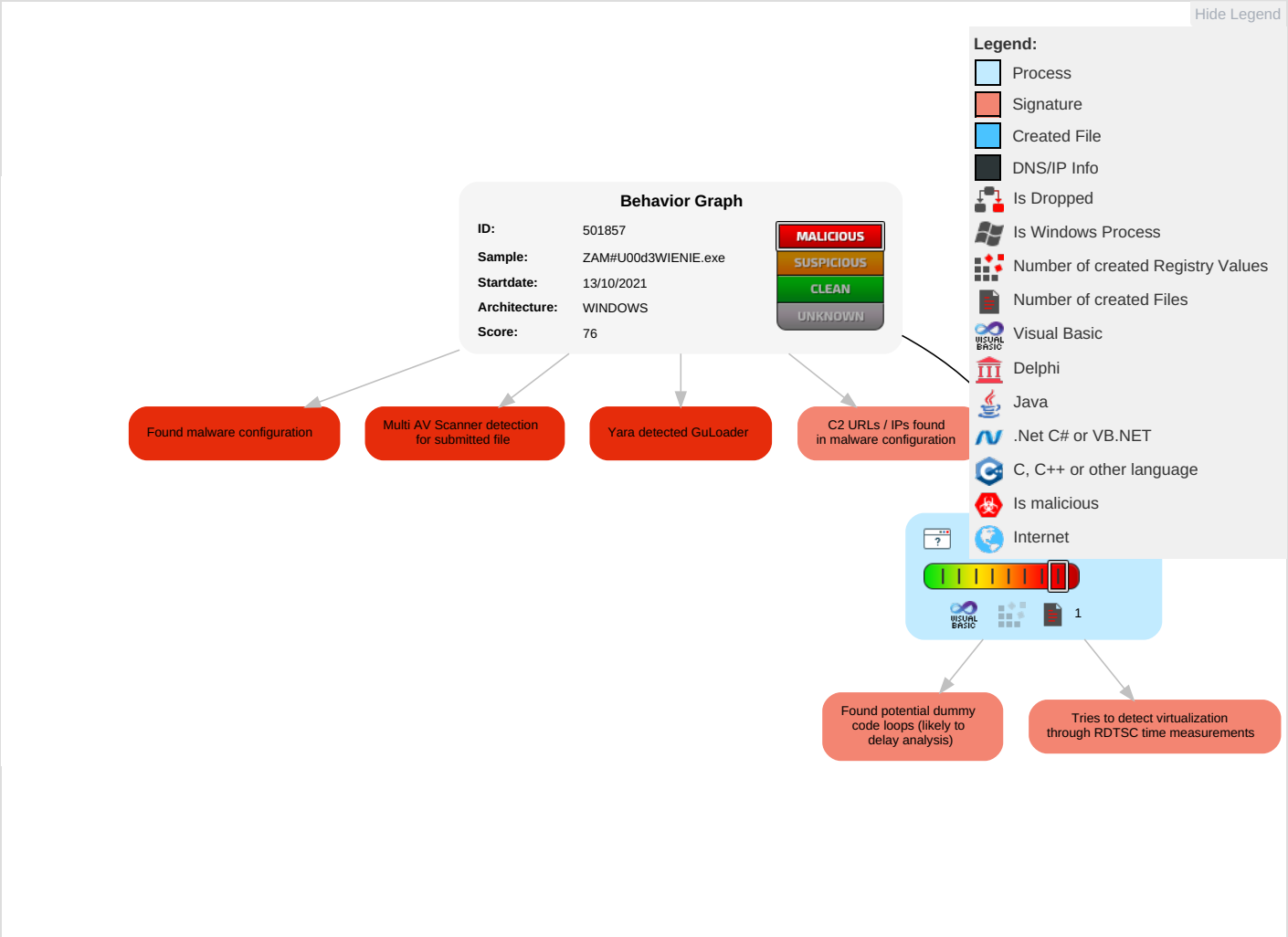


Found potential dummy code loops (likely to delay analysis)

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 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Recovery Time Window
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 Time Window
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Operational Capability
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 Time Window

Behavior Graph





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ZAM#U00d3WIENIE.exe	40%	Virustotal		Browse

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:	501857
Start date:	13.10.2021
Start time:	10:38:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ZAM#U00d3WIENIE.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:	10
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:	mal76.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none">• Successful, ratio: 11.2% (good quality ratio 5.3%)• Quality average: 29.6%• Quality standard deviation: 35.8%
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):	5.818386730128477
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:	ZAM#U00d3WIENIE.exe
File size:	102400
MD5:	328b34adced9ad8128d4079bcffde016
SHA1:	fa03cb6529d634b2e30d042491c0c13e39fd445e
SHA256:	95f59bb24f6c23995b22e40d5ba6785f9072da815451c04f61ee42f42a63089e
SHA512:	6beced8e1c5e365e787584afdce1d3d616afa7ea36b071cc0d7f77454dfe14c462d8b4b4ac9ae21a90c383840017caeff71e04d592f5604099baffca6026845c
SSDEEP:	1536:tIDnGkDi0pjX5utKdJxt2l7izvqpLnD:tlrGkJp9txt2l7ikn
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode...\$......i.....*.....Rich.....PE..L..G..... P...0.....X.....`.....@.....

File Icon

	
Icon Hash:	69e1c892f664c884

Static PE Info

General	
Entrypoint:	0x401378
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:	0x47858B36 [Thu Jan 10 03:04:22 2008 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:	669316531b5190f02843878b6ed87394

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x14318	0x15000	False	0.498500279018	data	6.25657633812	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x16000	0xd0c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x17000	0x1cb2	0x2000	False	0.348754882812	data	3.76993340498	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: ZAM#U00d3WIENIE.exe PID: 2904 Parent PID: 1744

General

Start time:	10:39:06
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\ZAM#U00d3WIENIE.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ZAM#U00d3WIENIE.exe'
Imagebase:	0x400000
File size:	102400 bytes
MD5 hash:	328B34ADCED9AD8128D4079BCFFDE016
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: 00000000.00000002.808037224.0000000002A30000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis