JoeSandbox Cloud BASIC

ID: 435339
Sample Name: KDVTOodd7T
Cookbook: default.jbs
Time: 12:41:13
Date: 16/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

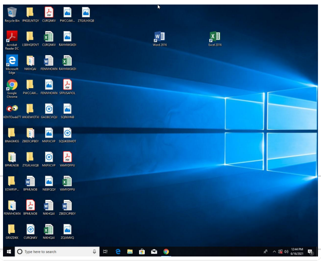
Windows Analysis Report KDVTOodd7T

Overview

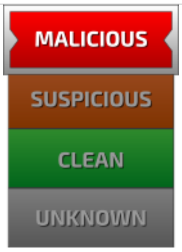
General Information

Sample Name:	KDVTOodd7T (renamed file extension from none to exe)
Analysis ID:	435339
MD5:	457fcb32ec7df18..
SHA1:	8bd3a8d8e0f6a48.
SHA256:	c7d1295093d411..
Tags:	32 exe GuLoader
Infos:	

Most interesting Screenshot:



Detection



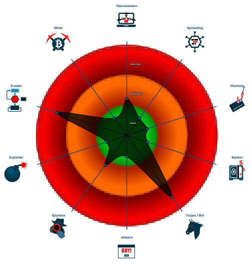
GuLoader

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Yara detected GuLoader
- 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 call native f…

Classification



Process Tree

- **System is w10x64**
- KDVTOodd7T.exe (PID: 6064 cmdline: 'C:\Users\user\Desktop\KDVTOodd7T.exe' MD5: 457FCB32EC7DF1868DF42F31CCE2A301)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://bara-seck.com/bin_dwjDbyFc82.bin, http://benvenuti.rs/wp-content/bin_dwjDbyFc82.bin"
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
KDVTOodd7T.exe	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.692826646.00000000021E0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000001.00000000.328525876.0000000000401000.00000020.00020000.sdmp	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
00000001.00000002.692341563.0000000000401000.00000020.00020000.sdmp	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.KDVTOodd7T.exe.400000.0.unpack	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
1.0.KDVTOodd7T.exe.400000.0.unpack	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:

Antivirus detection for URL or domain

Found malware configuration

Networking:

C2 URLs / IPs found in malware configuration

Data Obfuscation:

Yara detected GuLoader

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:

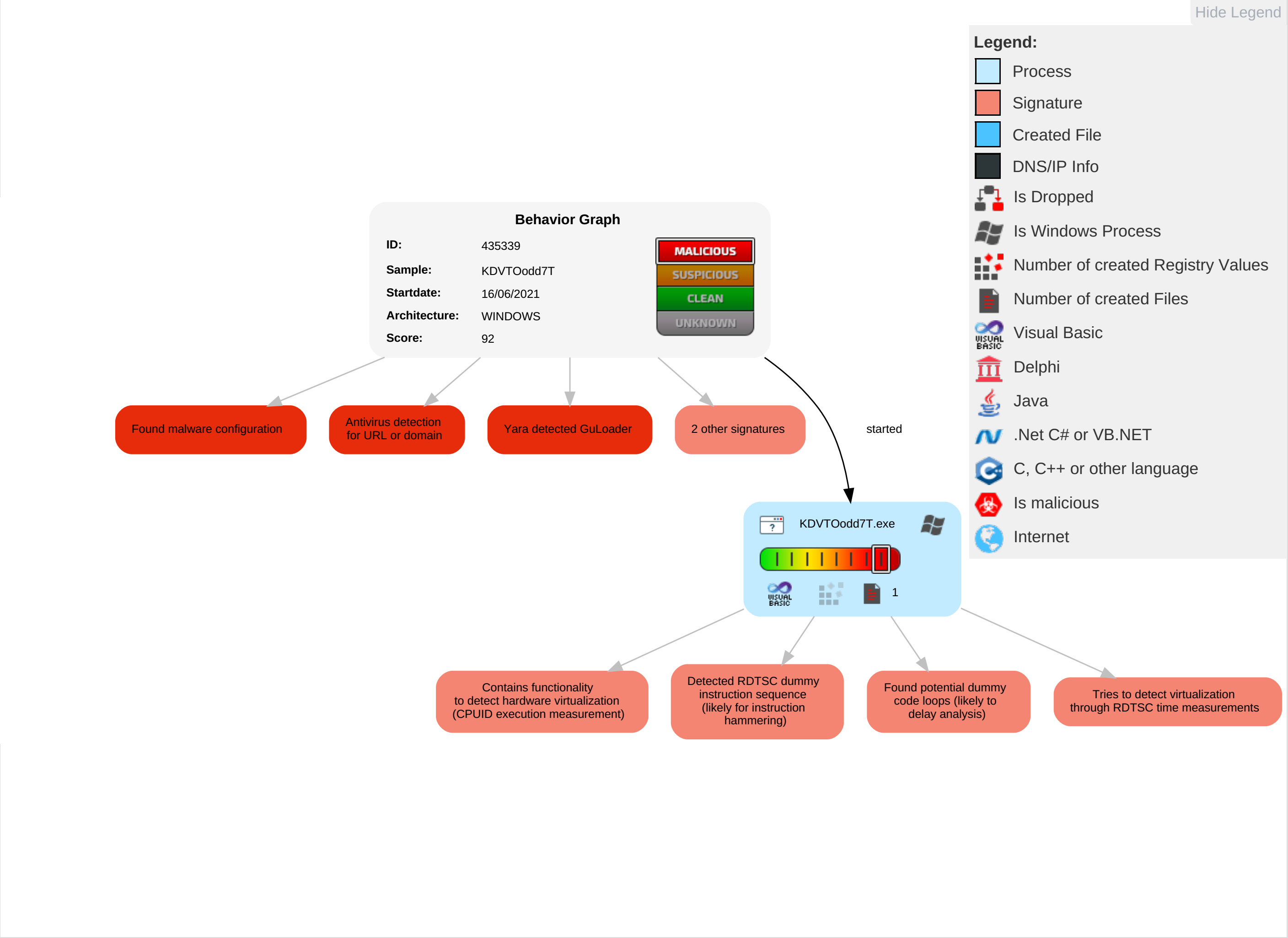
Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
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	R T W A
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	R W W A
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	O D C B

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
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	

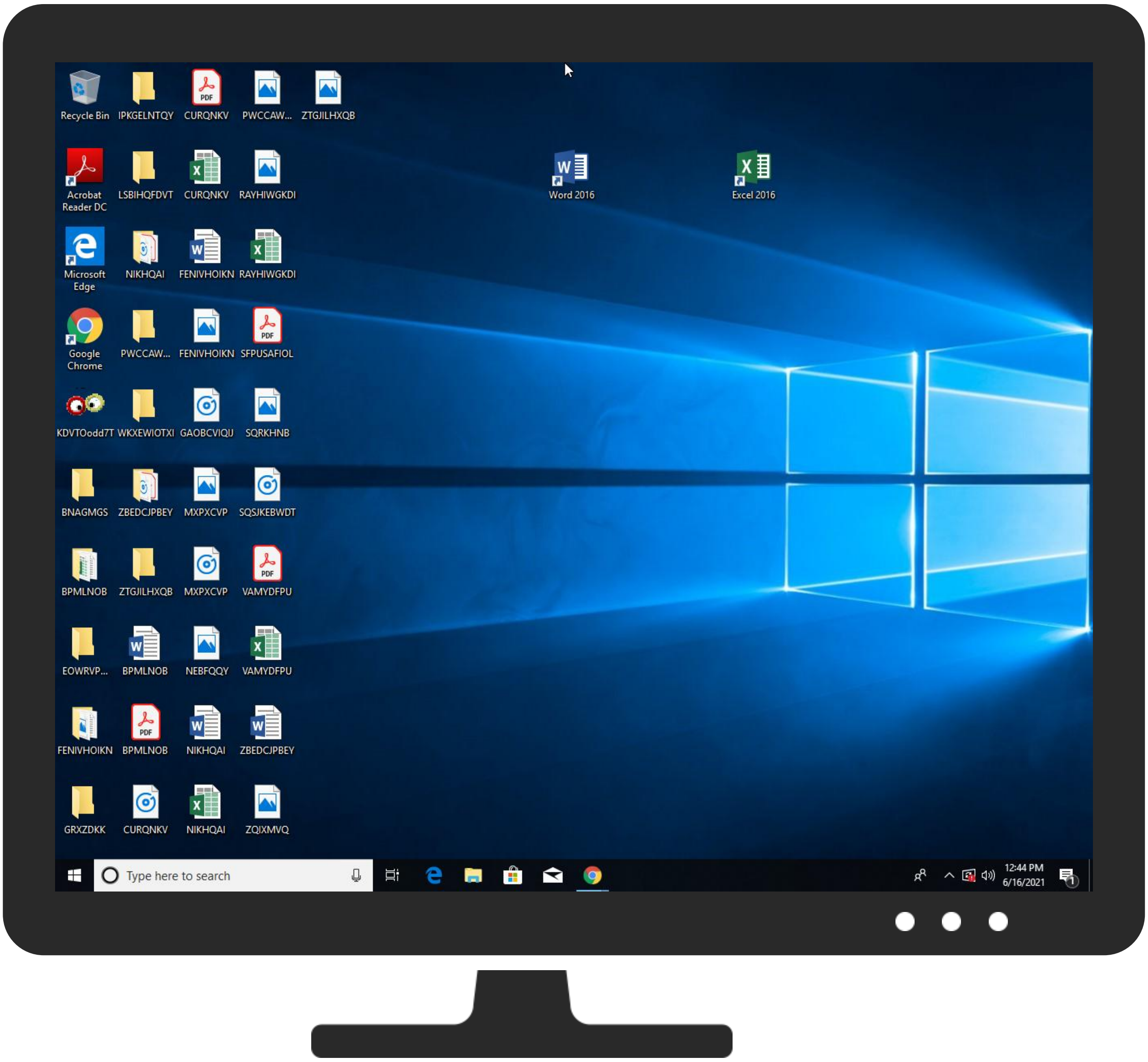
Behavior Graph


Hide Legend
Behavior Graph
ID: 435339
Sample: KDVTOodd7T
Startdate: 16/06/2021
Architecture: WINDOWS
Score: 92
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Found malware configuration
Antivirus detection for URL or domain
Yara detected GuLoader
2 other signatures
started
KDVTOodd7T.exe
1
Contains functionality to detect hardware virtualization (CPUID execution measurement)
Detected RDTSC dummy instruction sequence (likely for instruction hammering)
Found potential dummy code loops (likely to delay analysis)
Tries to detect virtualization through RDTSC time measurements
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet

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
KDVTOodd7T.exe	7%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://bara-seck.com/bin_dwjDbyFc82.bin, benvenuti.rs/wp-content/bin_dwjDbyFc82.bin	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://bara-seck.com/bin_dwjDbyFc82.bin, benvenuti.rs/wp-content/bin_dwjDbyFc82.bin	true	• Avira URL Cloud: malware	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	435339
Start date:	16.06.2021
Start time:	12:41:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	KDVTOodd7T (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:	24
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:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal92.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 21.5% (good quality ratio 11.6%) • Quality average: 33.5% • Quality standard deviation: 36.6%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • 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):	6.031806399752245
TrID:	• 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:	KDVTOodd7T.exe
File size:	94208
MD5:	457fcb32ec7df1868df42f31cce2a301
SHA1:	8bd3a8d8e0f6a48b51e5b3fbc119b154304044ec
SHA256:	c7d1295093d4112a976f0c13be811d2a1fb6dc5928e1fabefe7b1315f7b0e95f
SHA512:	503902cb165b587751270b511c13dd7ae6065814f2ea2ca4b145d831c77d1b36735526827ac185c99b81bb702628f26e9f43f5ccbd075cc491bcd4c836708708
SSDEEP:	1536:L10ol0/gh4343HqtCJWg4edfJPVo8xZSsIgO4jcYzy6ipu5W3EUanOYA2nJ29GLN:L6UdJ/4edfA0ZSsmVu5W3EUanOYA2nJn
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........c.S............&........ ....$......Rich....................PE..L...6..T.................@...0......D........P....@........

File Icon

Icon Hash:	11c0c48c86cc08c4

Static PE Info

General

Entrypoint:	0x401644
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:	0x54EF7F36 [Thu Feb 26 20:16:54 2015 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:	d5d16d1b76210dd28c8586fe9bac3119

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x137a8	0x14000	False	0.502783203125	data	6.41658995771	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x15000	0x1b84	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x17000	0xd6a	0x1000	False	0.348876953125	data	3.58378808404	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: KDVTOodd7T.exe PID: 6064 Parent PID: 5956

General

Start time:	12:42:04
Start date:	16/06/2021
Path:	C:\Users\user\Desktop\KDVTOodd7T.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\KDVTOodd7T.exe'
Imagebase:	0x400000
File size:	94208 bytes
MD5 hash:	457FCB32EC7DF1868DF42F31CCE2A301
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.692826646.00000000021E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000001.00000000.328525876.0000000000401000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000001.00000002.692341563.0000000000401000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 32.0.0 Black Diamond