ID: 450724
Sample Name: RICHIESTA DI OFFERTA.exe
Cookbook: default.jbs
Time: 16:43:16
Date: 19/07/2021
Version: 33.0.0 White Diamond

Table of Contents

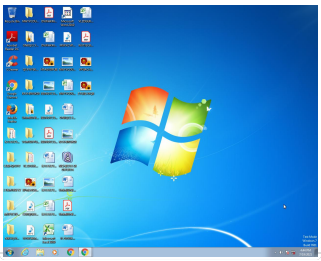
Windows Analysis Report RICHIESTA DI OFFERTA.exe

Overview

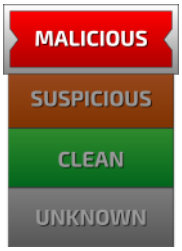
General Information

Sample Name:	RICHIESTA DI OFFERTA.exe
Analysis ID:	450724
MD5:	73bb5c4b690b8d..
SHA1:	60adddd91b6038..
SHA256:	a3feb5265e6d027.
Infos:	

Most interesting Screenshot:



Detection

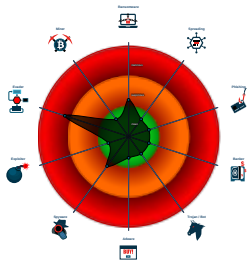


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Detected RDTSC dummy instruction…
- Tries to detect virtualization through…
- Abnormal high CPU Usage
- Allocates memory within range whic…
- Contains functionality for execution …
- Contains functionality to query CPU …
- Contains functionality to read the PEB
- Detected potential crypto function
- PE file contains strange resources
- Program does not show much activi…
- Sample file is different than original …
- Uses 32bit PE files

Classification



Process Tree

- **System is w7x64**
- RICHIESTA DI OFFERTA.exe (PID: 2660 cmdline: 'C:\Users\user\Desktop\RICHIESTA DI OFFERTA.exe' MD5: 73BB5C4B690B8D6DF88D6BC18FB3A553)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Malware Analysis System Evasion:

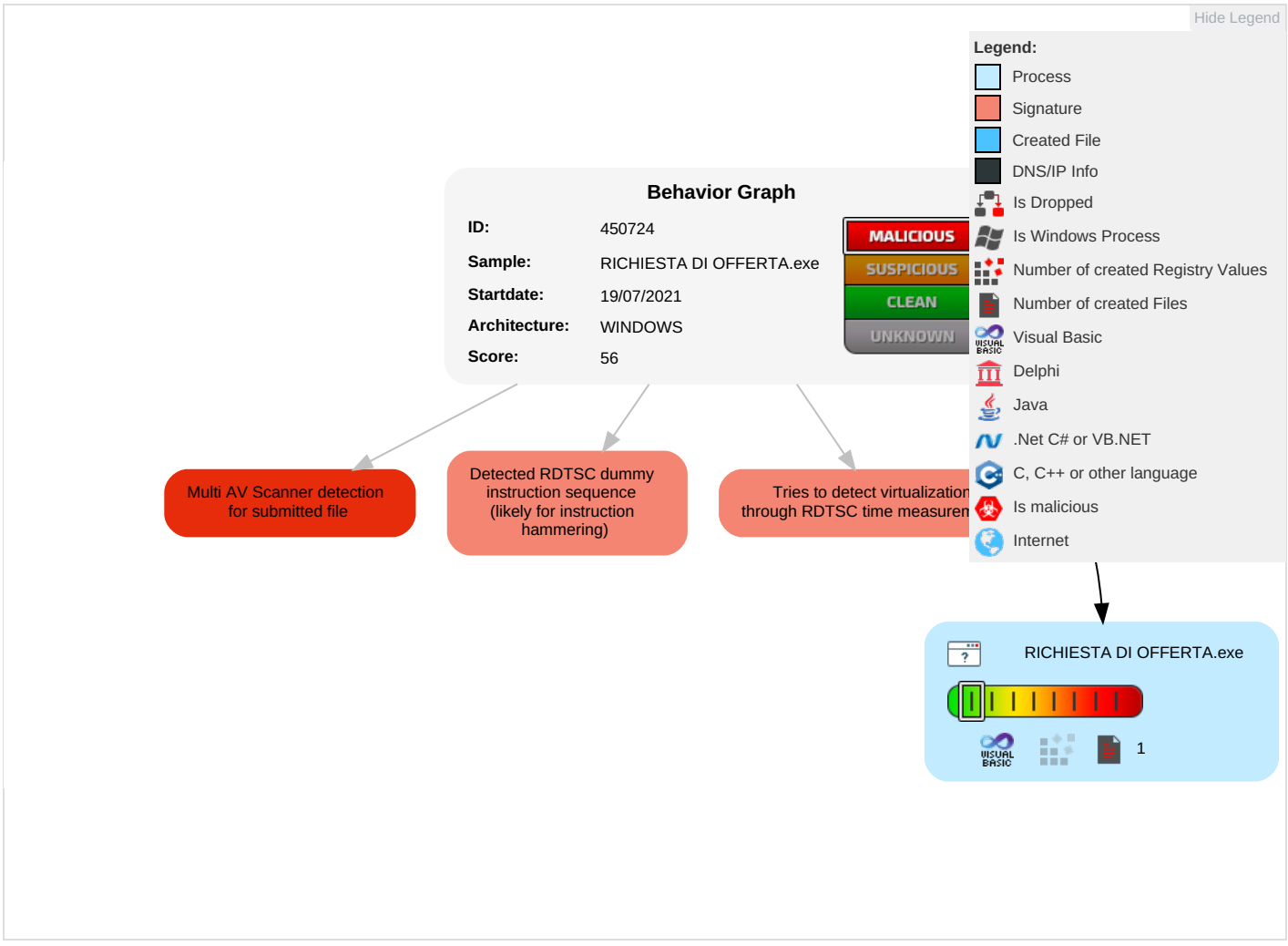
Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impac
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Obfuscated Files or Information 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	Remotely Track Device Without Authorization	Modify Syste Partiti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	System Information Discovery 2 1 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Locko

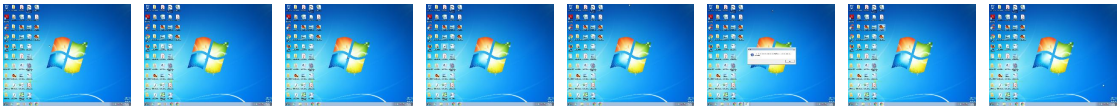
Behavior Graph



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
RICHIESTA DI OFFERTA.exe	21%	Virustotal		Browse
RICHIESTA DI OFFERTA.exe	9%	ReversingLabs	Win32.Backdoor.Remcos	

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:	450724
Start date:	19.07.2021
Start time:	16:43:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RICHIESTA DI OFFERTA.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Run name:	Suspected Instruction Hammering Hide Perf
Number of analysed new started processes analysed:	2
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:	mal56.evad.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 60.9% (good quality ratio 25.5%) • Quality average: 22.8% • Quality standard deviation: 31.7%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated
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:	• 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:	RICHIESTA DI OFFERTA.exe
File size:	241664
MD5:	73bb5c4b690b8d6df88d6bc18fb3a553
SHA1:	60adddd91b6038fc9d819cf6d647ce3be0b11d38
SHA256:	a3feb5265e6d02710f04ff618e966e9da9ba8fc8dc5692d6f7633fe0a3037b66
SHA512:	9c023dc66d9bcfb2f5bc0274001d92948ac058fc8765d2178907dfd8fb9885ede57acc3836d583ad97516dce1a97c50f081800b41a1f42ea938efb8b23e87567
SSDEEP:	3072:+3BepJlZa/xao5JKwI7V4R4iUW/qcijw2HJlZapGBR:EiUIo5JKPgU99vHP
File Content Preview:	MZ.....@.....!..L.!This 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: RICHIESTA DI OFFERTA.exe PID: 2660 Parent PID: 2032

General

Start time:	16:43:32
Start date:	19/07/2021
Path:	C:\Users\user\Desktop\RICHIESTA DI OFFERTA.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RICHIESTA DI OFFERTA.exe'
Imagebase:	0x400000
File size:	241664 bytes
MD5 hash:	73BB5C4B690B8D6DF88D6BC18FB3A553
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis