ID: 708235
Sample Name:
WCTBt2z7KE.exe
Cookbook: default.jbs
Time: 07:54:01
Date: 23/09/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Copyright Joe Security LLC 2022

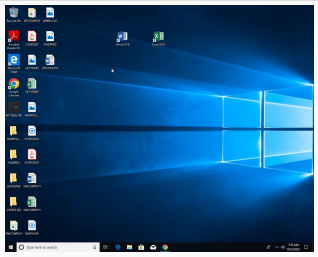
Windows Analysis Report

WCTBt2z7KE.exe

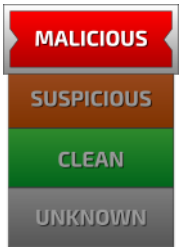
Overview

General Information

Sample Name:	WCTBt2z7KE.exe
Analysis ID:	708235
MD5:	612955e16c4580..
SHA1:	016c2f953e1c7a...
SHA256:	2a39458d3161f7..
Tags:	exe morpheus
Infos:	



Detection

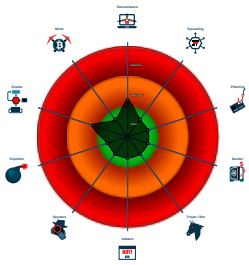


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Machine Learning detection for sam…
- Contains functionality to call native …
- Contains functionality to dynamicall…
- PE file contains executable resourc…
- Program does not show much activi…
- Uses code obfuscation techniques (…
- Detected potential crypto function

Classification



Process Tree

- **System is w10x64**
- WCTBt2z7KE.exe (PID: 1804 cmdline: "C:\Users\user\Desktop\WCTBt2z7KE.exe" MD5: 612955E16C4580BBC11798215426FF35)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Copyright Joe Security LLC 2022

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

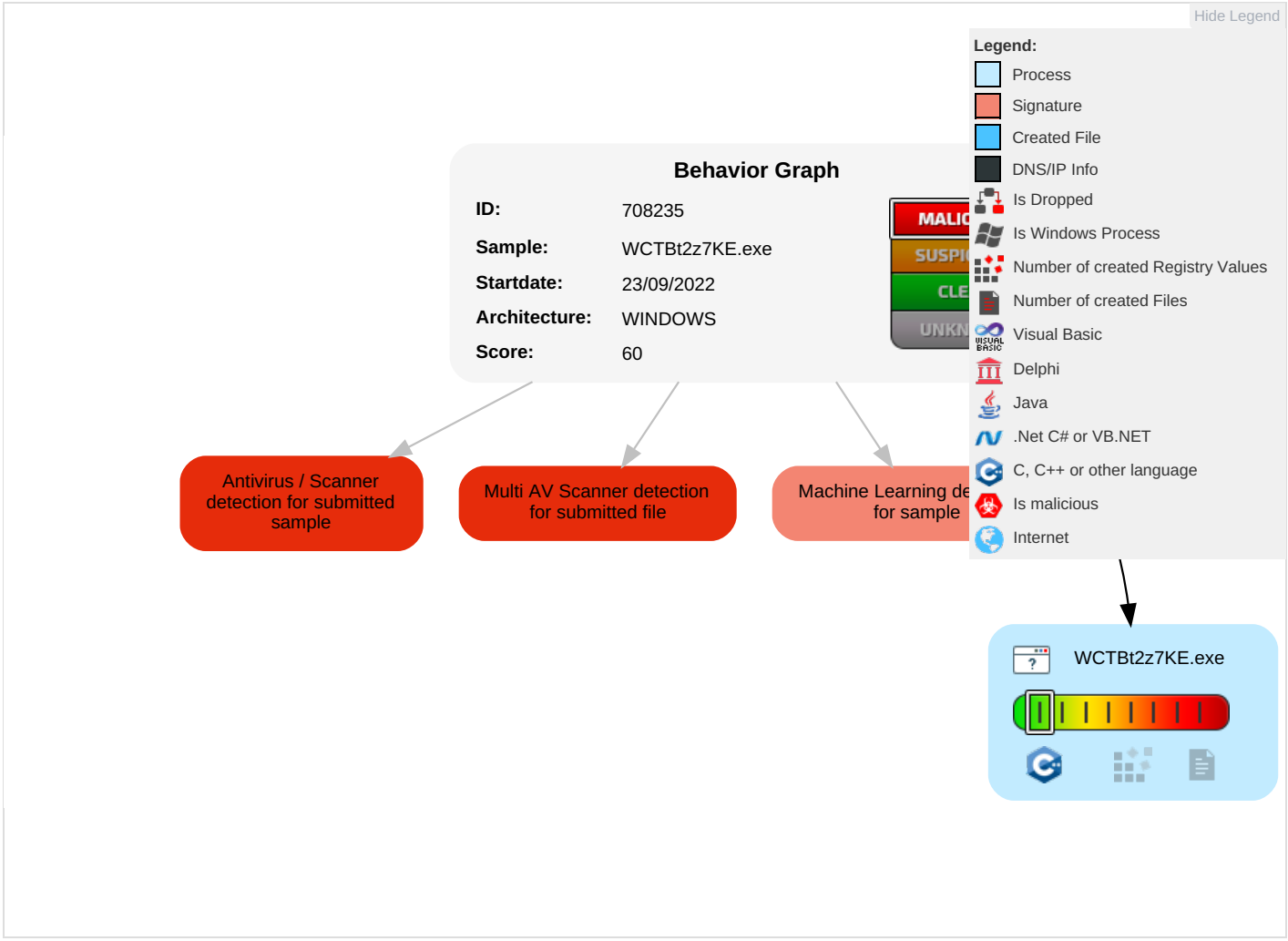
Multi AV Scanner detection for submitted file

Machine Learning detection for sample

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	Impact
Valid Accounts	1 Native API	Path Interception	Path Interception	1 Software Packing	OS Credential Dumping	1 System Information Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 1 Obfuscated Files or Information	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

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
WCTBt2z7KE.exe	22%	ReversingLabs		
WCTBt2z7KE.exe	33%	Virustotal		Browse
WCTBt2z7KE.exe	17%	Metadefender		Browse
WCTBt2z7KE.exe	100%	Avira	HEUR/AGEN.1226841	
WCTBt2z7KE.exe	100%	Joe Sandbox ML		

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

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	708235
Start date and time:	2022-09-23 07:54:01 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	WCTBt2z7KE.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	1
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:	mal60.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 65% (good quality ratio 39.1%) • Quality average: 38% • Quality standard deviation: 36.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

Simulations

Behavior and APIs

No simulations

Copyright Joe Security LLC 2022

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

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) x86-64, for MS Windows
Entropy (8bit):	3.06384833991322
TrID:	• Win64 Executable GUI (202006/5) 81.25% • UPX compressed Win32 Executable (30571/9) 12.30% • Win64 Executable (generic) (12005/4) 4.83% • Generic Win/DOS Executable (2004/3) 0.81% • DOS Executable Generic (2002/1) 0.81%
File name:	WCTBt2z7KE.exe
File size:	325632
MD5:	612955e16c4580bbc11798215426ff35
SHA1:	016c2f953e1c7a1ba88c1812d70751925ab9e3e0
SHA256:	2a39458d3161f7dae38dbad7e846ebecdbd802392f4cd0b845440914532a28d7
SHA512:	1e766f005a182e6d5c1f8d83fef6a216935246501a6b175face5ee780daa660d75e5c314346ee1788ff0a4bb7a4320c93b3f37a9af6c20f5f153b40577113916
SSDEEP:	1536:24dJooh0Wa0aer344Jw/ytUqVS5EklijQ1fTN7nCcfrHc:24dzVTaer344JzthRZijQ1JWcfr
TLSH:	B964AF8EFD64BCE8C41ED3720692087C61399116DA1B670DD5BFD5B7DBA2A843F40683
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...E.@]......./....2.....0.....`.....@.....

File Icon

Icon Hash:	008039c4c4384000

Static PE Info

General

Entrypoint:	0x1400660a0
Entrypoint Section:	UPX1
Digitally signed:	false
Imagebase:	0x140000000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, LARGE_ADDRESS_AWARE
DLL Characteristics:	
Time Stamp:	0x5D400545 [Tue Jul 30 08:52:21 2019 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:	a50e815adb2cfe3e58d388c791946db8

Entrypoint Preview

Instruction
push ebx
push esi
push edi
push ebp
dec eax
lea esi, dword ptr [FFFF3F7Ah]
dec eax
lea edi, dword ptr [esi-00059025h]
push edi
mov eax, 00064A7Fh
push eax
dec eax
mov ecx, esp
dec eax
mov edx, edi
dec eax
mov edi, esi
mov esi, 0000C075h
push ebp
dec eax
mov ebp, esp
inc esp
mov ecx, dword ptr [ecx]
dec ecx
mov eax, edx
dec eax
mov edx, esi
dec eax
lea esi, dword ptr [edi+02h]
push esi
mov al, byte ptr [edi]
dec edx
mov cl, al
and al, 07h
shr cl, 00000003h
dec eax
mov ebx, FFFFFD00h
dec eax
shl ebx, cl
mov cl, al

Instruction
dec eax
lea ebx, dword ptr [esp+ebx*2-00000E78h]
dec eax
and ebx, FFFFFFC0h
push 00000000h
dec eax
cmp esp, ebx
jne 00007F759126C5BBh
push ebx
dec eax
lea edi, dword ptr [ebx+08h]
mov cl, byte ptr [esi-01h]
dec edx
mov byte ptr [edi+02h], al
mov al, cl
shr cl, 00000004h
mov byte ptr [edi+01h], cl
and al, 0Fh
mov byte ptr [edi], al
dec eax
lea ecx, dword ptr [edi-04h]
push eax
inc ecx
push edi
dec eax
lea eax, dword ptr [edi+04h]
inc ebp
xor edi, edi
inc ecx
push esi
inc ecx
mov esi, 00000001h
inc ecx
push ebp
inc ebp
xor ebp, ebp
inc ecx
push esp
push ebp
push ebx
dec eax
mov dword ptr [esp-10h], ecx
dec eax
mov dword ptr [esp-28h], eax
mov eax, 00000001h
dec eax
mov dword ptr [esp-08h], esi
dec esp
mov dword ptr [esp-18h], eax
mov ebx, eax
inc esp
mov dword ptr [esp-1Ch], ecx
movzx ecx, byte ptr [edi+02h]
shl ebx, cl
mov ecx, ebx
dec eax
mov ebx, dword ptr [esp+38h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa955c	0x28c	.rsrc
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x67000	0x4255c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x1d000	0x10d4	UPX0
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
UPX0	0x1000	0x59000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
UPX1	0x5a000	0xd000	0xce00	False	0.9676501820388349	data	7.969338587590873	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x67000	0x43000	0x42800	False	0.03488457471804511	data	1.4954359032844007	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x672b0	0x42028	data		
RT_RCDATA	0x642d4	0x93	data		
RT_RCDATA	0x64368	0xd	DOS executable (COM, 0x8C-variant)		
RT_RCDATA	0x64378	0xcf	data		
RT_RCDATA	0x64448	0x1	very short file (no magic)		
RT_GROUP_ICON	0xa92dc	0x14	data		
RT_MANIFEST	0xa92f4	0x267	XML 1.0 document, ASCII text		

Imports

DLL	Import
COMCTL32.DLL	InitCommonControlsEx
GDI32.DLL	GetStockObject
KERNEL32.DLL	LoadLibraryA, ExitProcess, GetProcAddress, VirtualProtect
msvcrt.dll	free
OLE32.DLL	CoInitialize
SHELL32.DLL	ShellExecuteExW
SHLWAPI.DLL	PathRemoveArgsW
USER32.DLL	SetFocus
WINMM.DLL	timeBeginPeriod

Network Behavior

No network behavior found

Copyright Joe Security LLC 2022

Statistics

No statistics

System Behavior

Analysis Process: WCTBt2z7KE.exe PID: 1804, Parent PID: 6032

General	
Target ID:	0
Start time:	07:55:00
Start date:	23/09/2022
Path:	C:\Users\user\Desktop\WCTBt2z7KE.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\WCTBt2z7KE.exe"
Imagebase:	0x140000000
File size:	325632 bytes
MD5 hash:	612955E16C4580BBC11798215426FF35
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly