

JoeSandbox Cloud BASIC



ID: 384218

Sample Name: Overworn.exe

Cookbook: default.jbs

Time: 18:49:52

Date: 08/04/2021

Version: 31.0.0 Emerald

Table of Contents

Table of Contents	2
Analysis Report Overworn.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Yara Overview	4
Memory Dumps	4
Sigma Overview	4
Signature Overview	4
AV Detection:	5
Data Obfuscation:	5
Malware Analysis System Evasion:	5
Anti Debugging:	5
Mitre Att&ck Matrix	5
Behavior Graph	5
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	7
URLs	7
Domains and IPs	8
Contacted Domains	8
Contacted IPs	8
General Information	8
Simulations	8
Behavior and APIs	8
Joe Sandbox View / Context	9
IPs	9
Domains	9
ASN	9
JA3 Fingerprints	9
Dropped Files	9
Created / dropped Files	9
Static File Info	9
General	9
File Icon	9
Static PE Info	10
General	10
Entrypoint Preview	10
Data Directories	11
Sections	12
Resources	12
Imports	12
Version Infos	12
Possible Origin	12
Network Behavior	12
Code Manipulations	13
Statistics	13
System Behavior	13

Analysis Process: Overworn.exe PID: 2200 Parent PID: 5624	13
General	13
File Activities	13
Disassembly	13
Code Analysis	13

Analysis Report Overworn.exe

Overview

General Information

Sample Name:	Overworn.exe
Analysis ID:	384218
MD5:	5e68ca13c917b9..
SHA1:	d0fd2b4757b4a02.
SHA256:	9b7f6820091a78b.
Tags:	exe
Infos:	
Most interesting Screenshot:	

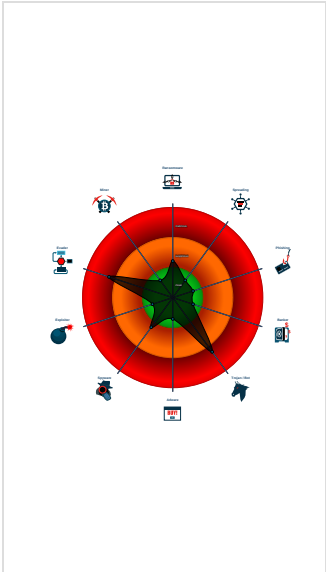
Detection

MALICIOUS SUSPICIOUS CLEAN UNKNOWN GuLoader	
Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Multi AV Scanner detection for subm...
Yara detected GuLoader
Found potential dummy code loops (...)
Machine Learning detection for samp...
Tries to detect virtualization through...
Abnormal high CPU Usage
Contains functionality for execution ...
Creates a DirectInput object (often fo...
Detected potential crypto function
PE file contains an invalid checksum
PE file contains strange resources
Program does not show much activi...
Sample file is different than original ...
Uses 32bit PE files

Classification



Startup

- System is w10x64
- Overworn.exe (PID: 2200 cmdline: 'C:\Users\user\Desktop\Overworn.exe' MD5: 5E68CA13C917B9126AD737AC0A570D66)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

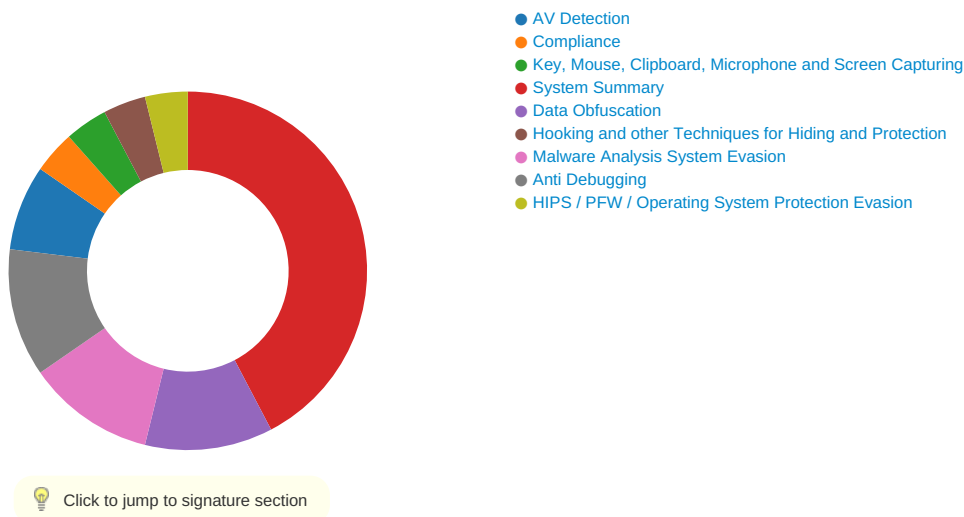
Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.731517060.00000000004F0000.0000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



AV Detection:



Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Data Obfuscation:



Yara detected GuLoader

Malware Analysis System Evasion:



Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

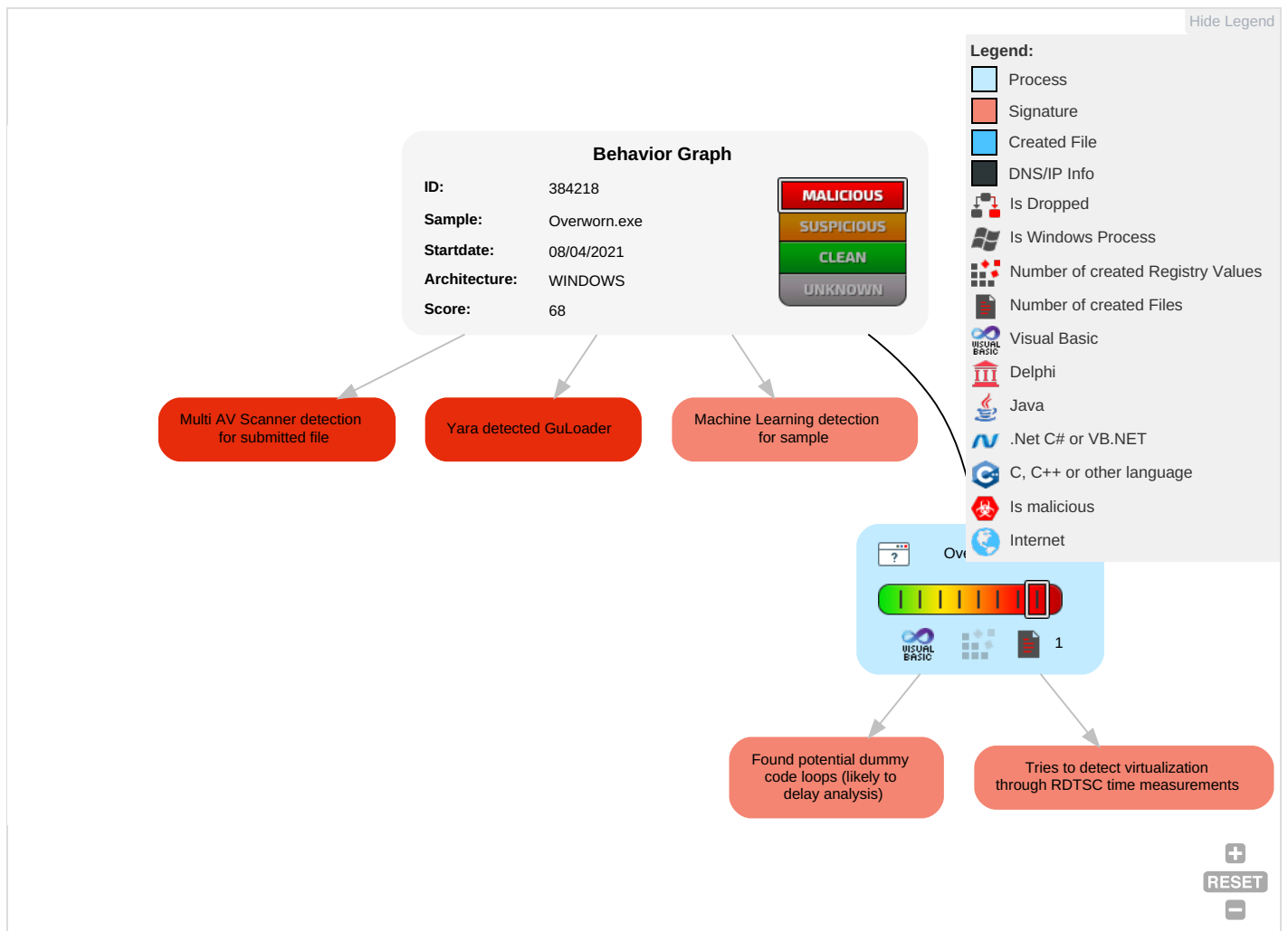


Found potential dummy code loops (likely to delay analysis)

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	Input Capture 1	Security Software Discovery 2 1	Remote Services	Input Capture 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	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Data	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 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Recovery

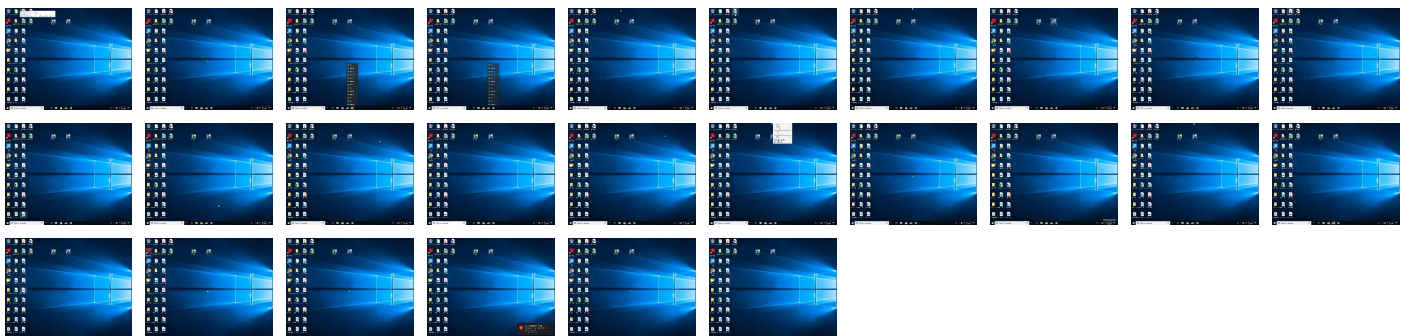
Behavior Graph



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
Overwon.exe	46%	Virustotal		Browse
Overwon.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

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	384218
Start date:	08.04.2021
Start time:	18:49:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Overworm.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:	32
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:	mal68.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 46.7% (good quality ratio 21.7%) • Quality average: 19.5% • Quality standard deviation: 22.9%
HCA Information:	Failed
Cookbook Comments:	• 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 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIDAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe

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):	5.575516391079876
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:	Overworn.exe
File size:	110592
MD5:	5e68ca13c917b9126ad737ac0a570d66
SHA1:	d0fd2b4757b4a0266cd548dd7307eec33ab4f9d3
SHA256:	9b7f6820091a78be8c817c46b864488a35faacb33a21c104953564e974050828
SHA512:	d531dc2b89622358822e849a0c8243682c3eeb7ee3a5cd8a769a6fed7ea99dc8c5d5a716a92e6dca8a8db4db6add0936d7f17050dc8c676452623dbd1f8bdd28
SSDEEP:	1536:P98REJz42DCgO72vL2M/FPV9vr8Zy0ksPVM9vDd2Mf2v:P8E+53z8Vm9tMVmy
File Content Preview:	MZ.....@.....!..!Th is program cannot be run in DOS mode...\$.....#...B...B ...B..L^...B...`...B...d...B..Rich.B.....PE..L...%.M.....0.....@.....@.....

File Icon



Icon Hash:	c0c6f2e0e4fefe3f
------------	------------------

Static PE Info

General

Entrypoint:	0x4013e8
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:	0x4DA78625 [Thu Apr 14 23:41:25 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:	d1ed0dda3501483d16a7ad09b76f3b08

Entrypoint Preview

Instruction

```
push 00410EA4h
call 00007F9EE47B86A3h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add ah, dh
sub byte ptr [ebp+4BE18418h], bh
stosb
sbb edi, edi
push ebp
movsd
add eax, 00001988h
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
push ebx
push esp
dec ecx
dec ebx
dec esp
inc ebp
inc esp
dec esi
dec ecx
dec esi
inc edi
inc ebp
push edx
dec esi
```

Instruction
inc ebp
add byte ptr [eax], al
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
or eax, dword ptr [edx-259BB489h]
jc 00007F9EE47B8634h
dec ecx
scasd
mov ecx, dword ptr [ebp+1Ah]
add byte ptr [ebx-6EA6279Ch], cl
pop ds
sbb ah, dh
fstcw word ptr [edx+42h]
wait
xchg eax, esp
cmp byte ptr [esp+3AA65790h], ah
dec edi
lodsd
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
imul edi, ecx, F7870000h
add byte ptr [eax], al
add byte ptr [65764F00h], cl
jc 00007F9EE47B871Fh
imul ebp, dword ptr [esi+65h], 73h
jnc 00007F9EE47B86E5h
add byte ptr [4F000801h], cl

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x132d4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x16000	0x5c3a	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
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	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x108	.text
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
.text	0x1000	0x1277c	0x13000	False	0.413021689967	data	5.97030490248	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x14000	0x117c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x16000	0x5c3a	0x6000	False	0.359659830729	data	5.26995713236	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1ad92	0xea8	data		
RT_ICON	0x1a4ea	0x8a8	data		
RT_ICON	0x19f82	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x179da	0x25a8	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x16932	0x10a8	data		
RT_ICON	0x164ca	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x16470	0x5a	data		
RT_VERSION	0x161e0	0x290	MS Windows COFF PA-RISC object file	Guarani	Paraguay

Imports

DLL	Import
MSVBVM60.DLL	_Clos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaLineInputStr, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, _adj_fprem1, __vbaHresultCheckObj, __vbaLenBstrB, _adj_fdiv_m32, __vbaAryDestruct, _vbaOnError, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaFpR8, __vbaVarTstLt, _CIsin, __vbaChkstk, __vbaFileClose, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, __vbaAryConstruct2, __vbaObjVar, _adj_fptan, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptionHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPEException, _Cilog, __vbaFileOpen, __vbaNew2, __vbaR8Str, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, _adj_fdivr_m32, _adj_fdiv_r, __vbaLateMemCall, __vbaVarAdd, __vbaVarDup, __vbaFpl4, _Clatan, __vbaStrMove, _allmul, _Cltan, _Clexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0474 0x04b0
InternalName	Overworn
FileVersion	1.00
CompanyName	Pana-sonic
Comments	Pana-sonic
ProductName	Pana-sonic
ProductVersion	1.00
FileDescription	Pana-sonic
OriginalFilename	Overworn.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Guarani	Paraguay	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: Overworn.exe PID: 2200 Parent PID: 5624

General

Start time:	18:50:41
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\Overworn.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Overworn.exe'
Imagebase:	0x400000
File size:	110592 bytes
MD5 hash:	5E68CA13C917B9126AD737AC0A570D66
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000001.00000002.731517060.00000000004F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
File Path	Offset		Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis