ID: 343751
Sample Name: Tracking No_SINI0035249718.exe
Cookbook: default.jbs
Time: 15:28:19
Date: 25/01/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report Tracking No_SINI0035249718.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
Compliance: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 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: Tracking No_SINI0035249718.exe PID: 6032 Parent PID: 5908 13
General 13
File Activities 13
Disassembly 13
Code Analysis 13

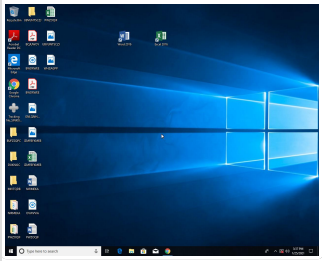
Analysis Report Tracking No_SINI0035249718.exe

Overview

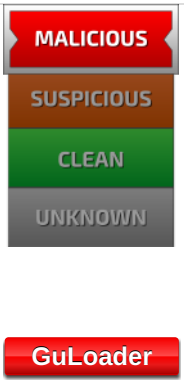
General Information

Sample Name:	Tracking No_SINI0035249718.exe
Analysis ID:	343751
MD5:	9d7f4dcaf5e6ef7…
SHA1:	0e81a911c016cb..
SHA256:	dd2e44f31e3158a.
Tags:	exe

Most interesting Screenshot:



Detection



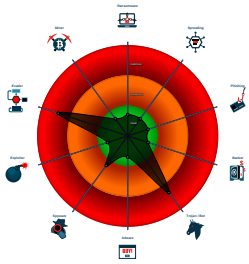
GuLoader

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Yara detected VB6 Downloader Gen…
- Abnormal high CPU Usage
- Contains functionality for execution …
- Contains functionality to read the PEB
- Creates a DirectInput object (often fo…
- PE file contains strange resources
- Sample file is different than original …

Classification



Startup

- **System is w10x64**
- Tracking No_SINI0035249718.exe (PID: 6032 cmdline: 'C:\Users\user\Desktop\Tracking No_SINI0035249718.exe' MD5: 9D7F4DCAF5E6EF75ED4EAE0F16DFC7D7)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

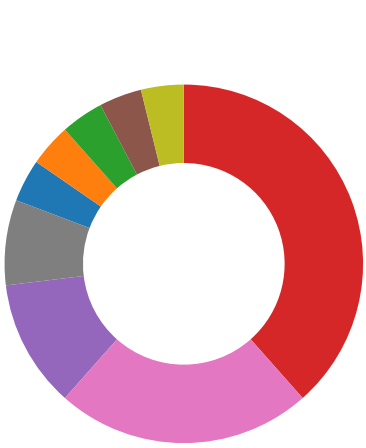
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: Tracking No_SINI0035249718.exe PID: 6032	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: Tracking No_SINI0035249718.exe PID: 6032	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

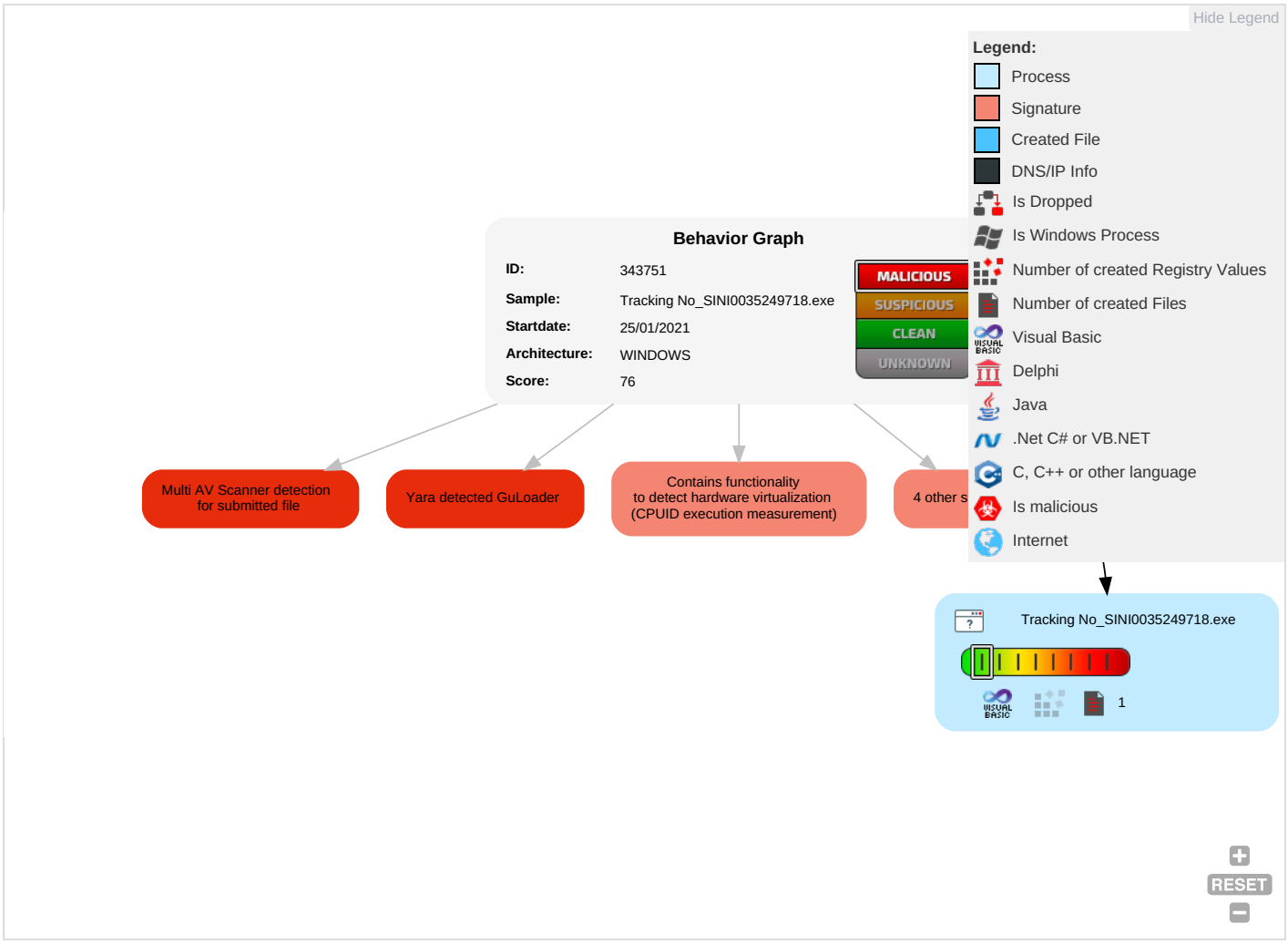
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

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
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Process Injection 1	Input Capture 1	Security Software Discovery 4 1 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	System Information Discovery 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups

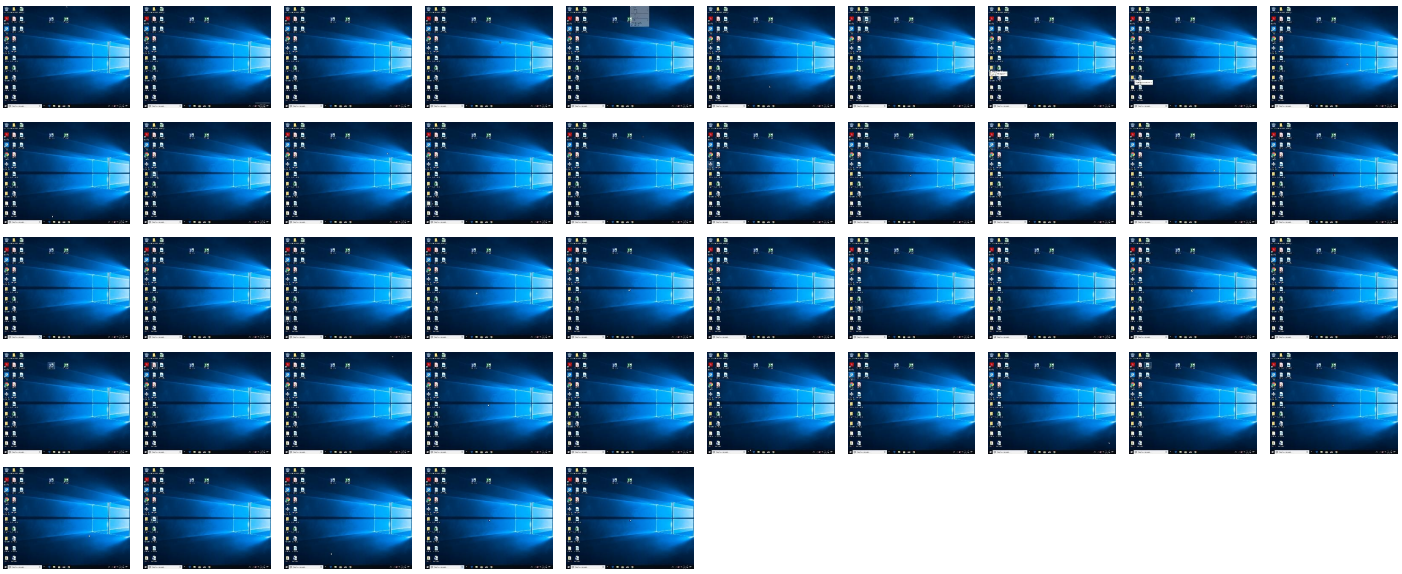
Behavior Graph



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
Tracking No_SINI0035249718.exe	23%	Virustotal		Browse
Tracking No_SINI0035249718.exe	15%	ReversingLabs	Win32.Trojan.Generic	

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:	343751
Start date:	25.01.2021
Start time:	15:28:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Tracking No_SINI0035249718.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:	28
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:	mal76.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 5.5% (good quality ratio 5%) • Quality average: 52% • Quality standard deviation: 18.9%
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): BackgroundTransferHost.exe, RuntimeBroker.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Report size getting too big, too many NtAllocateVirtualMemory calls found.

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):	5.820289814070592
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:	Tracking No_SINI0035249718.exe
File size:	102400
MD5:	9d7f4dcaf5e6ef75ed4eae0f16dfc7d7
SHA1:	0e81a911c016cb15a0f4bcb80c0ba0427953edc7
SHA256:	dd2e44f31e3158a713931d11f336664a5b23890471461ffd06a5515bca9485c1
SHA512:	5832d4e862e5855a3dce9029651151cf37ecbdc26bf582c922bc2b66e57adadc1878f096760be8ccd208a6db881d0f69c56cfdebf4f1717622e7b89d139efea9
SSDEEP:	1536:RWZsVu2tSB8dwLgo/WDkfzvx1IbxuO0zd2gGOc4cffuxX1:i8u2I63iFfzp1iD0B2gGOc4cut1
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...._.T.....`...0.....p....@.....

File Icon

Icon Hash:	f030f0c6f030b100

Static PE Info

General

Entrypoint:	0x401480
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:	0x548B5FA0 [Fri Dec 12 21:35:28 2014 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:	901434c98a0ac9771b4195fb76cfab24

Entrypoint Preview

Instruction
push 00402120h
call 00007F60887DC6F5h
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 byte ptr [eax-5060F6DBh], bl
xchg byte ptr [edx-68h], cl
pop ds
fcomi st(0), st(4)
shr edi, FFFFFFC6h
push ds
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
or eax, 200A0D0Ah
and byte ptr [eax+72h], dl
outsd
push 00000065h
arpl word ptr [ecx+esi+00h], si
push ebp
xor dh, byte ptr [edx+esi+33h]
cmp byte ptr [eax], al
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
add al, 58h
xor al, dl

Instruction
sub ecx, dword ptr [edi-52BC388Ah]
sal byte ptr [esi-42h], FFFFFF9Eh
push ds
retf
in al, dx
push ss
loopne 00007F60887DC720h
fxch4 st(4)
outsb
inc esi
xchg dword ptr [edx-319A1A0Ch], ebx
sbb dword ptr [esi+33AD4F3Ah], esi
cdq
iretw
adc dword ptr [edi+00AA000Ch], esi
pushad
rcl dword ptr [ebx+00000000h], cl
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
out dx, al
or eax, dword ptr [eax]
add byte ptr [0000000Bh], bh
or al, byte ptr [eax]
push ebx
dec ebx
dec edi
push esi
dec esp
inc esi
push ebp
dec esp
inc esp
inc ebp
add byte ptr [54000901h], cl
outsb
je 00007F60887DC779h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x15c94	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x19000	0xa2c	.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	0x124	.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	0x15190	0x16000	False	0.474165482955	data	6.23820218517	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x17000	0x11a4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x19000	0xa2c	0x1000	False	0.15478515625	data	1.66464717922	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x194c4	0x568	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x194b0	0x14	data		
RT_VERSION	0x190f0	0x3c0	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaFreeVarList, __vbaEnd, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaLateMemSt, __vbaVarForInit, __vbaObjSet, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaVarTstLt, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, __vbaAryConstruct2, __vbaObjVar, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaLateMemCall, __vbaVarDup, __vbaLateMemCallLd, _CIatan, __vbaStrMove, _allmul, _CItan, __vbaVarForNext, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0409 0x04b0
LegalCopyright	Trademark International
InternalName	Gimpy
FileVersion	1.00
CompanyName	Native Instruments Nanosystems S.r.l.
LegalTrademarks	Trademark International
Comments	Native Instruments Nanosystems S.r.l.
ProductName	Native Instruments Nanosystems S.r.l.
ProductVersion	1.00
FileDescription	Native
OriginalFilename	Gimpy.exe

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: Tracking No_SINI0035249718.exe PID: 6032 Parent PID: 5908

General

Start time:	15:29:06
Start date:	25/01/2021
Path:	C:\Users\user\Desktop\Tracking No_SINI0035249718.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Tracking No_SINI0035249718.exe'
Imagebase:	0x400000
File size:	102400 bytes
MD5 hash:	9D7F4DCAF5E6EF75ED4EAE0F16DFC7D7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis