ID: 343935
Sample Name: Proforma Invoice 1009745.exe
Cookbook: default.jbs
Time: 19:14:46
Date: 25/01/2021
Version: 31.0.0 Emerald

Table of Contents

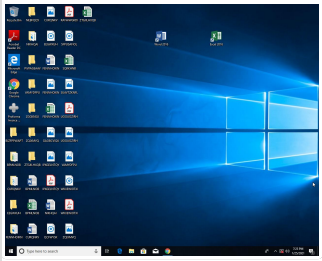
Analysis Report Proforma Invoice 1009745.exe

Overview

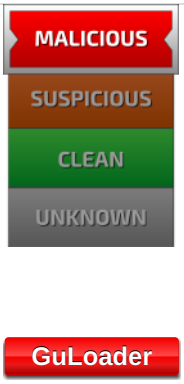
General Information

Sample Name:	Proforma Invoice 1009745.exe
Analysis ID:	343935
MD5:	71eee7537f1ac43.
SHA1:	5867ba045cb981..
SHA256:	956ec30b9191b8..
Tags:	exe GuLoader

Most interesting Screenshot:



Detection



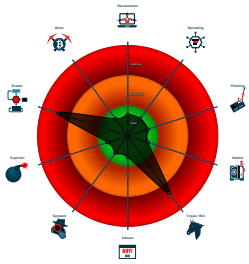
GuLoader

Score:	80
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…
- Executable has a suspicious name (…
- 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 call native f…
- Contains functionality to read the PEB
- PE file contains strange resources

Classification



Startup

- **System is w10x64**
- Proforma Invoice 1009745.exe (PID: 7064 cmdline: 'C:\Users\user\Desktop\Proforma Invoice 1009745.exe' MD5: 71EEE7537F1AC4347B00DB9D5777A078)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

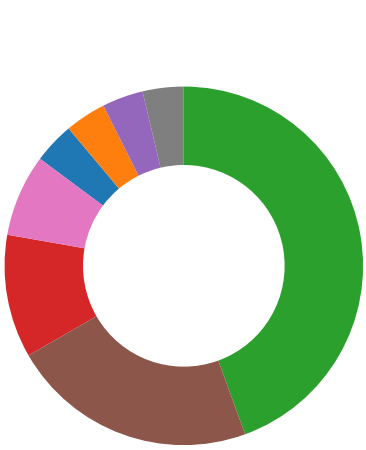
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: Proforma Invoice 1009745.exe PID: 7064	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: Proforma Invoice 1009745.exe PID: 7064	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

System Summary:

Executable has a suspicious name (potential lure to open the executable)

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)

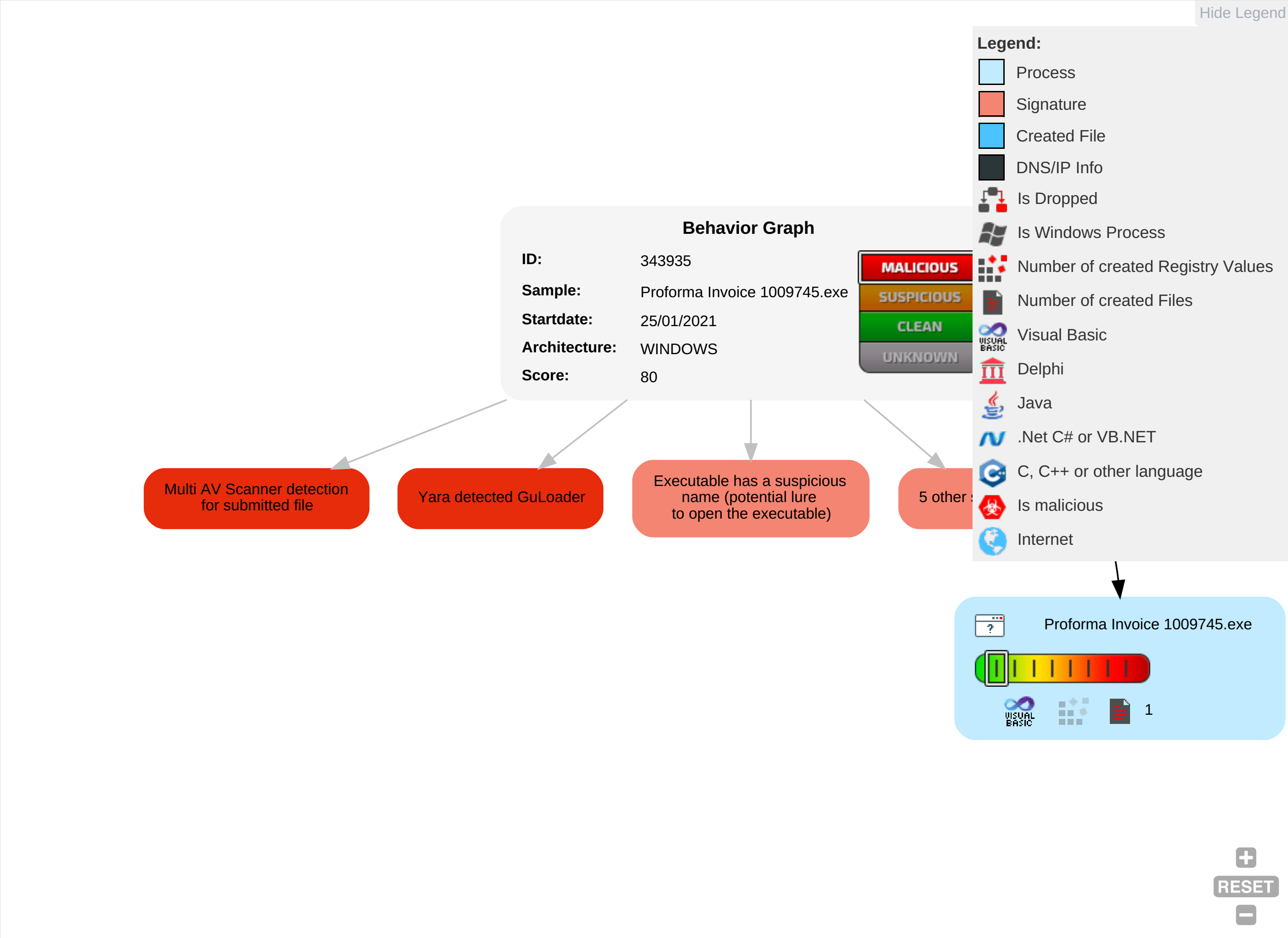
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

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	OS Credential Dumping	Security Software Discovery 4 1 1	Remote Services	Data from Local System	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

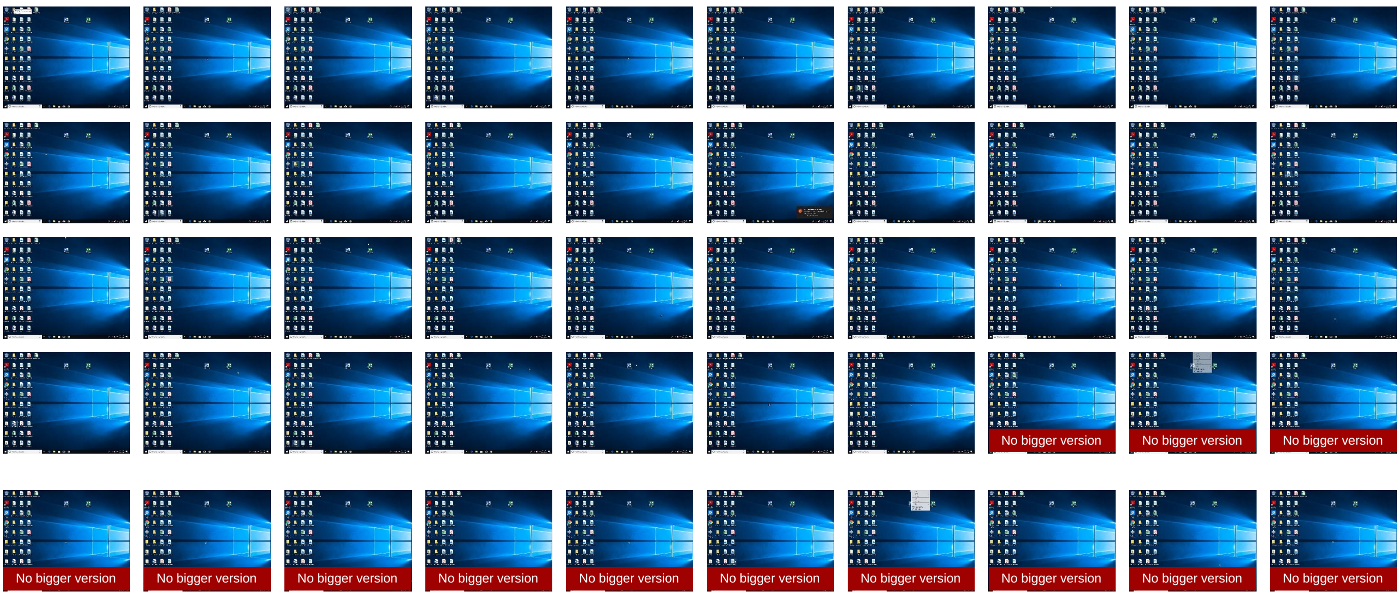
Behavior Graph



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
Proforma Invoice 1009745.exe	24%	Virustotal		Browse
Proforma Invoice 1009745.exe	24%	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:	343935
Start date:	25.01.2021
Start time:	19:14:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Proforma Invoice 1009745.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:	29
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:	mal80.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 10.3% (good quality ratio 4.1%) • Quality average: 22.5% • Quality standard deviation: 29.5%
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): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, conhost.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:	
Entropy (8bit):	5.832013404875337
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:	Proforma Invoice 1009745.exe
File size:	102400

General

MD5:	71eee7537f1ac4347b00db9d5777a078
SHA1:	5867ba045cb9817a6f15938d021db6839c5b346f
SHA256:	956ec30b9191b8755a1b879822317ccda7be9a0284a4df1f1f3efd53669f8928
SHA512:	31d626568310d36850e6ec84f7b4d61fffb8dd0b587974b5957e3c36fdd3e77954a57242a41ec4d2a65294c95221c14dce5e978629fa2bc3e12d8e8c812049f0
SSDEEP:	1536:WD9Ou2tSBrRY0419Xh2qw4H4kF9E2L6HiuUCWVD:Pu2IhRHy9ww4yC2L6HiN5
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...CZ.R.....`...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:	0x52F55A43 [Fri Feb 7 22:12:19 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 004021A8h
call 00007FB088BBBB25h
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 al, dl
push 00000021h
test byte ptr [edx-61BA80A6h], ah
pop edi
aas
fsub st(4), st(0)
insd
aad 46h
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
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 eax
jc 00007FB088BBBBA1h
push 00000065h
arpl word ptr [ecx+esi+00h], si
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 bh, bh
int3
xor dword ptr [eax], eax
add al, DFh
fldenv [ebp-4A24E1BFh]
inc eax
mov cl, B0h
inc dword ptr [esi+54h]
sub byte ptr [ecx], 00000006h
xor ch, byte ptr [ebp-23h]
pop ebx
pop ss
xchg eax, esp
mov ch, 40h
lahf
fbstp [ebp-0D25B5A6h]
sbb eax, 33AD4F3Ah
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
add byte ptr [eax], al
add byte ptr [eax], al
salc
or eax, dword ptr [eax]
add byte ptr [esi], dh
or eax, dword ptr [eax]
add byte ptr [eax], al
or eax, dword ptr [eax]
dec edi
jbe 00007FB088BBBB97h
jc 00007FB088BBBBA4h
jne 00007FB088BBBBA0h
popad

Instruction
jc 00007FB088BBBB32h
or eax, 67000501h
arpl word ptr [ebx+00h], bp

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x15c74	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x19000	0xa64	.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	
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	0x15170	0x16000	False	0.472156871449	data	6.2500820394	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	0xa64	0x1000	False	0.15966796875	data	1.73359437587	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x194fc	0x568	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x194e8	0x14	data		
RT_VERSION	0x190f0	0x3f8	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	ARBEJDSPSYKOLOGIEN
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	ARBEJDSPSYKOLOGIEN.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: Proforma Invoice 1009745.exe PID: 7064 Parent PID: 5868

General

Start time:	19:15:41
Start date:	25/01/2021
Path:	C:\Users\user\Desktop\Proforma Invoice 1009745.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Proforma Invoice 1009745.exe'
Imagebase:	0x400000
File size:	102400 bytes
MD5 hash:	71EEE7537F1AC4347B00DB9D5777A078
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