ID: 385457
Sample Name:
PP05492110.exe
Cookbook: default.jbs
Time: 14:44:39
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

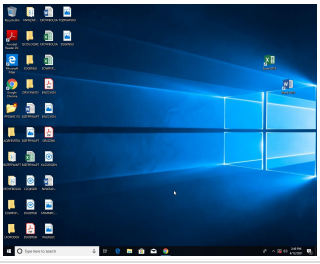
Analysis Report PP05492110.exe

Overview

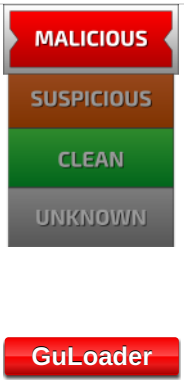
General Information

Sample Name:	PP05492110.exe
Analysis ID:	385457
MD5:	9cb24f7919feb0b..
SHA1:	4910e701802ff27..
SHA256:	e14114a3eabaaf8.
Infos:	

Most interesting Screenshot:



Detection

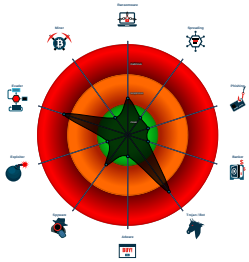


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Found potential dummy code loops (…
- Machine Learning detection for samp…
- Tries to detect virtualization through…
- Abnormal high CPU Usage
- 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 …

Classification



Startup

- **System is w10x64**
- PP05492110.exe (PID: 2888 cmdline: 'C:\Users\user\Desktop\PP05492110.exe' MD5: 9CB24F7919FEB0B91FF6071D6FDDBAF6)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=150ztyABrKIbvulchlM9fuv9fi1p1lVIL",
  "Injection Process": [
    "RegAsm.exe",
    "RegSvcs.exe",
    "MSBuild.exe"
  ]
}
```

Yara Overview

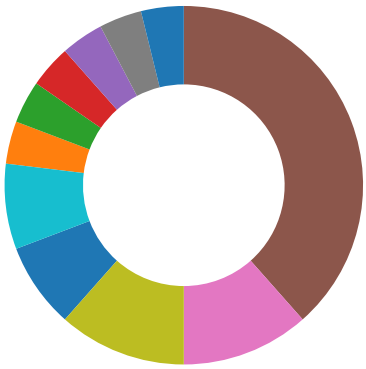
Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.753553871.0000000000500000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion

Click to jump to signature section

AV Detection:

Found malware configuration

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

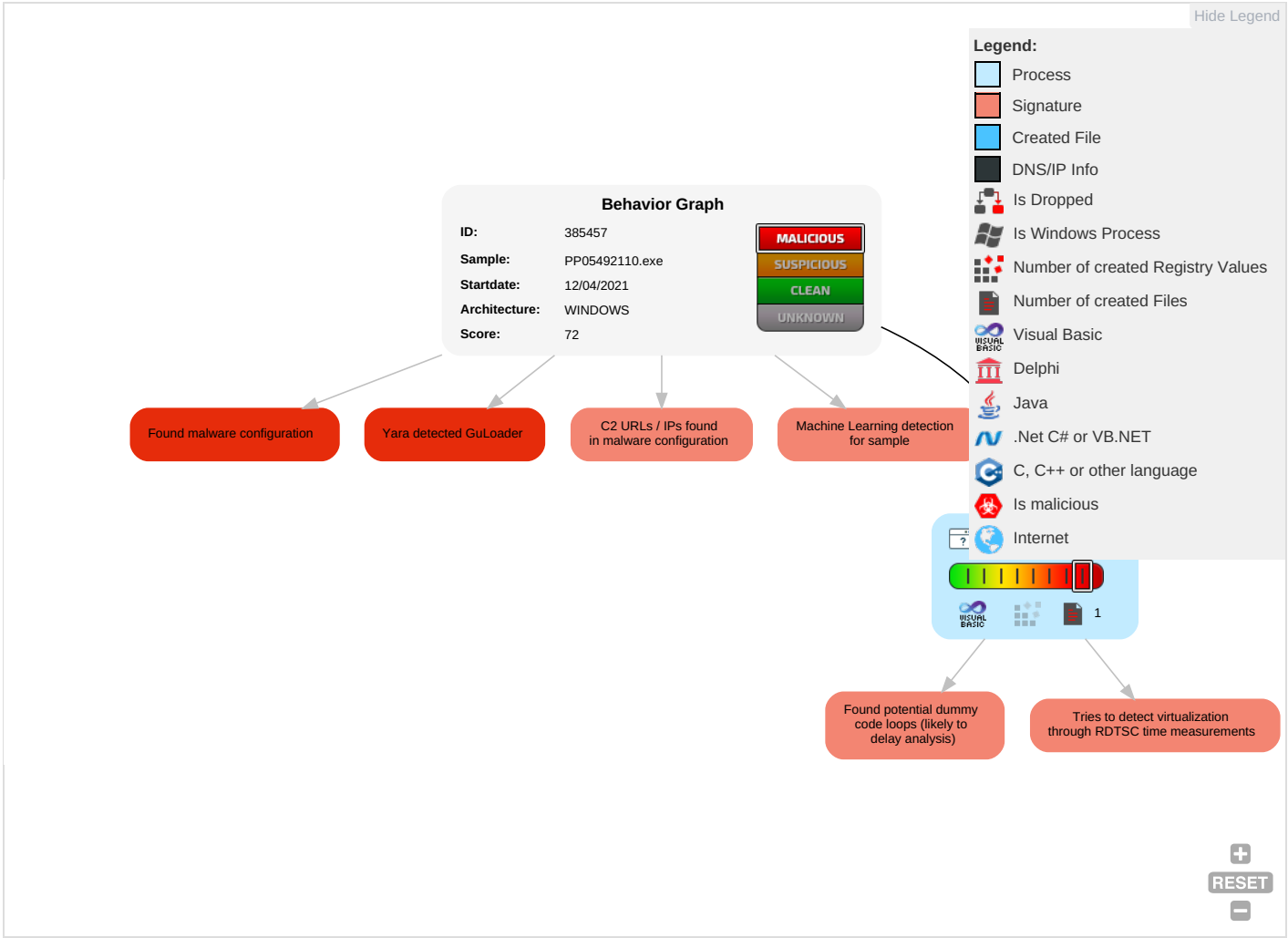
Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Ef
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	Input Capture 1	Security Software Discovery 2	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Re Tr W Au
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	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Re W W Au
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	Ol De Cl Ba

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Ef
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

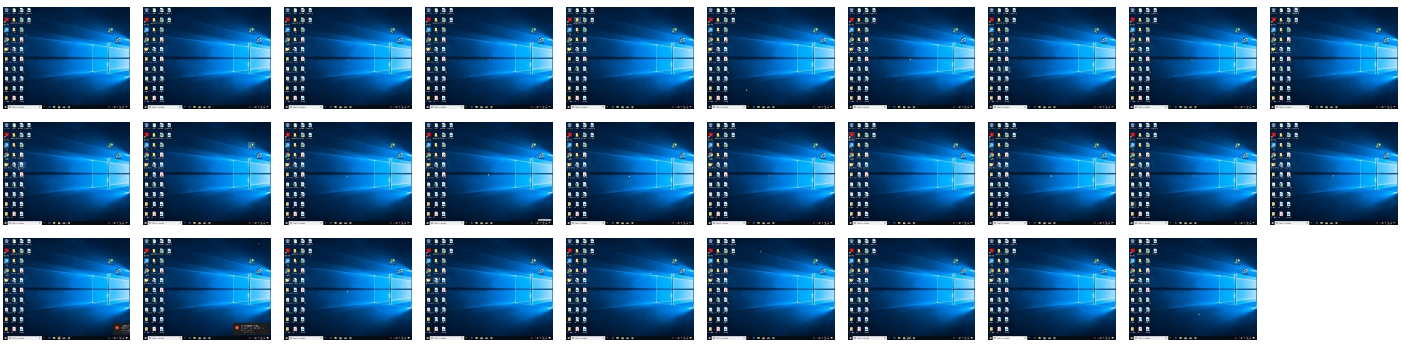
Behavior Graph



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
PP05492110.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:	385457
Start date:	12.04.2021
Start time:	14:44:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PP05492110.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:	14
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:	mal72.troj.evad.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 89.1% (good quality ratio 34.9%) • Quality average: 22.9% • Quality standard deviation: 31.2%
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, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe • VT rate limit hit for: /opt/package/joesandbox/database/analysis/385457/sample/PP05492110.exe

Simulations

Behavior and APIs

No simulations

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):	5.733443572399981
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:	PP05492110.exe
File size:	147456
MD5:	9cb24f7919feb0b91ff6071d6fddbaf6
SHA1:	4910e701802ff270266954f34bd384fcf987d429
SHA256:	e14114a3eabaaf81a42459e2dab69cf044fe90909d7bf7ccb9db62e4d12a51ce
SHA512:	51a86f12d4dba21d538d8ad2255b17fc3bdb86c9f7feac2adf4fb6f5ce19c61e2a9644171ea445103ff301d2f9ab7b1c711aac36cbe23c6ad96a6fd773a63374
SSDEEP:	3072:LHefjwxF+0v8Vm2XULJ0is0Y4W71TVmy:6wHxv8s2CjY4Wxsy
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....Q.V.....I.....@.....

File Icon

Icon Hash:	c0c6f2e0e4fefe3f

Static PE Info

General

Entrypoint:	0x40166c
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:	0x56EA51D8 [Thu Mar 17 06:42:32 2016 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:	879f5bbda1e2f48716a0325e5b7fa215

Entrypoint Preview

Instruction
push 004110B0h
call 00007FDE6C325363h
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 bl, bh
out 99h, al
xor edi, ebx
std
imul eax, dword ptr [esi-64h], 8Fh
inc edx
lahf
jnc 00007FDE6C325392h
retf
bound eax, dword ptr [eax]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [edx+45h], dl
dec ebp
push ebp
inc ecx
inc edx
dec esp
inc ebp
add byte ptr [eax], al

Instruction
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
dec esp
xor dword ptr [eax], eax
or al, 27h
aaa
dec edi
mov eax, 44C3B89Fh
sahf
dec ebp
push 00000014h
jc 00007FDE6C3253BAh
mov edi, AFA9FF41h
add dword ptr [edi+75h], 84A0456Bh
sbb al, C4h
xor eax, 3AF35FC2h
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
wait
stc
add byte ptr [eax], al
mov bh, dh
add byte ptr [eax], al
add byte ptr [edx], cl
add byte ptr [ebx+41h], dl
inc ecx
dec ebx
dec edi
push edx
dec esi
inc ebp
dec esi
inc ebp
add byte ptr [56000A01h], cl
popad
insb
push 00000000h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1be44	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1f000	0x5c42	.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	0x1c0	.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	0x1b4e0	0x1c000	False	0.400408063616	data	6.02633035795	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1d000	0x12f0	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1f000	0x5c42	0x6000	False	0.359944661458	data	5.27700643593	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x23d9a	0xea8	data		
RT_ICON	0x234f2	0x8a8	data		
RT_ICON	0x22f8a	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x209e2	0x25a8	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x1f93a	0x10a8	data		
RT_ICON	0x1f4d2	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x1f478	0x5a	data		
RT_VERSION	0x1f1e0	0x298	data	Guarani	Paraguay

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaHresultCheck, __vbaFreeVar, __vbaAryMove, __vbaStrVarMove, __vbaEnd, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaRecAnsiToUni, __vbaStrCat, __vbaSetSystemError, __vbaHresultCheckObj, __vbaLenBstrB, _adj_fdiv_m32, __vbaAryDestruct, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaFpR8, __vbaVarTstLt, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, __vbaAryConstruct2, __vbaVarTstEq, __vbaObjVar, DllFunctionCall, _adj_fpatan, __vbaRecUniToAnsi, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaVarErrI4, __vbaFPException, __vbaStrVarVal, _CIlog, __vbaInStr, __vbaNew2, __vbaVar2Vec, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaLateMemCall, __vbaVarAdd, __vbaStrToAnsi, __vbaVarDup, __vbaFpI4, __vbaLateMemCallLd, _CIatan, __vbaStrMove, __vbaCastObj, _allmul, __vbaLateIdSt, _CItan, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0474 0x04b0
InternalName	Laboredly5
FileVersion	1.00
CompanyName	Pana-sonic
Comments	Pana-sonic
ProductName	Pana-sonic
ProductVersion	1.00
FileDescription	Pana-sonic

Description	Data
OriginalFilename	Laboredly5.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: PP05492110.exe PID: 2888 Parent PID: 5640

General

Start time:	14:45:29
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\PP05492110.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PP05492110.exe'
Imagebase:	0x400000
File size:	147456 bytes
MD5 hash:	9CB24F7919FEB0B91FF6071D6FDDBAF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000000.00000002.753553871.0000000000500000.00000040.00000001.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