Joe Sandbox Cloud BASIC

ID: 410830
Sample Name:
NP__000009116_11-05-2021_08_40_37.exe
Cookbook: default.jbs
Time: 11:15:14
Date: 11/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

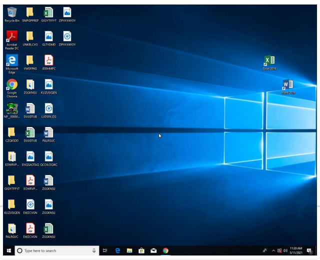
Analysis Report NP__000009116_11-05-2021_08_40_37….

Overview

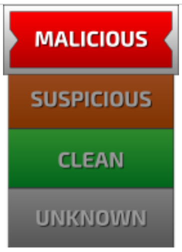
General Information

Sample Name:	NP__000009116_11-05-2021_08_40_37.exe
Analysis ID:	410830
MD5:	3f695fa46992bd2..
SHA1:	83d7a6cb77eff28..
SHA256:	e0f53d67eb5d4a5.
Tags:	GuLoader
Infos:	🔍 ⚙ HCA

Most interesting Screenshot:



Detection



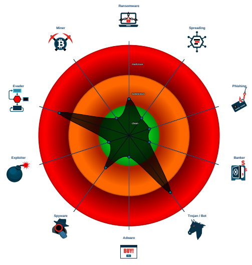
GuLoader

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Found potential dummy code loops (…
- Tries to detect virtualization through…
- Abnormal high CPU Usage
- Contains functionality for execution …
- Contains functionality to call native f…
- Contains functionality to query CPU …

Classification



Startup

- **System is w10x64**
- NP__000009116_11-05-2021_08_40_37.exe (PID: 480 cmdline: 'C:\Users\user\Desktop\NP__000009116_11-05-2021_08_40_37.exe' MD5: 3F695FA46992BD20300728E9245C87F8)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1RnNEBf_Y19f_pduK4zvHqPJHGwMdQKtO"
}
```

Yara Overview

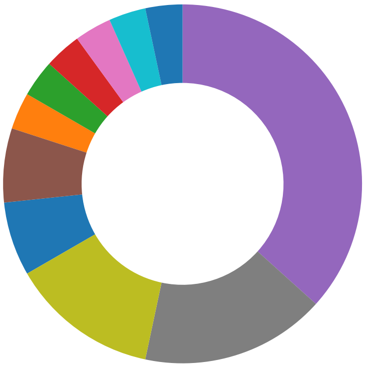
Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.767064760.00000000029F0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- ● AV Detection
- ● Compliance
- ● 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
- ● Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

C2 URLs / IPs found in malware configuration

Data Obfuscation:

Yara detected GuLoader

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 virtualization through RDTSC time measurements

Anti Debugging:

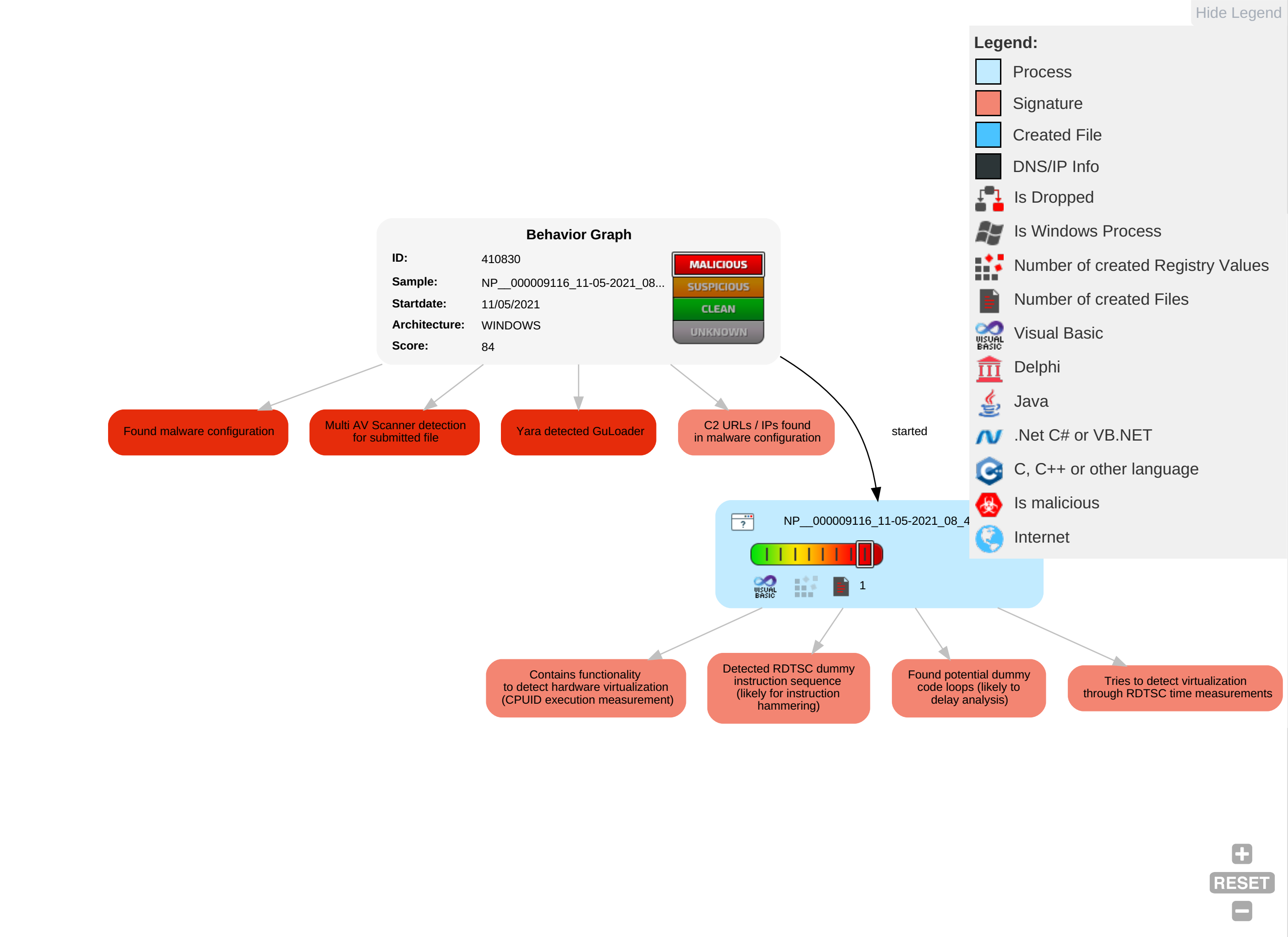
Found potential dummy code loops (likely to delay analysis)

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 4 1	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	System Information Discovery 3 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Behavior Graph

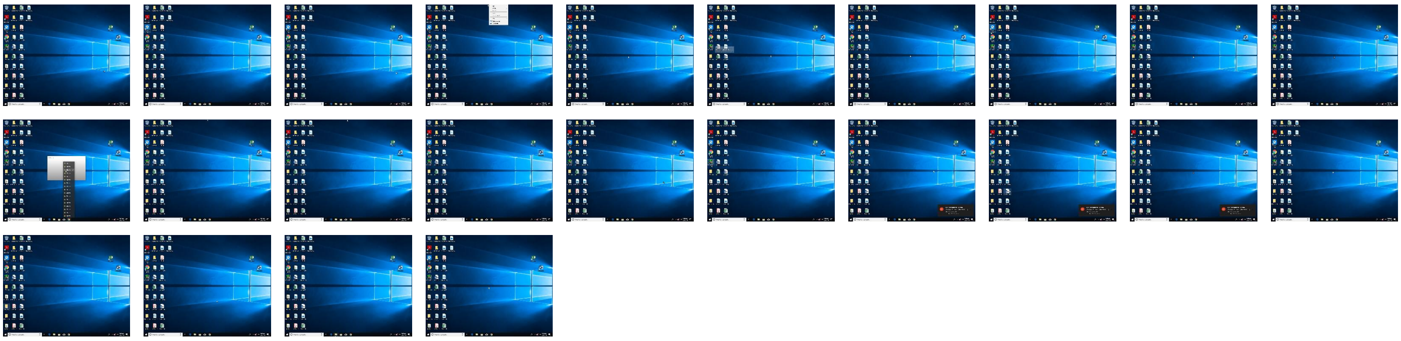

Hide Legend
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet
Behavior Graph
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Found malware configuration
Multi AV Scanner detection for submitted file
Yara detected GuLoader
C2 URLs / IPs found in malware configuration
started
NP__000009116_11-05-2021_08_4
1
Contains functionality to detect hardware virtualization (CPUID execution measurement)
Detected RDTSC dummy instruction sequence (likely for instruction hammering)
Found potential dummy code loops (likely to delay analysis)
Tries to detect virtualization through RDTSC time measurements
RESET

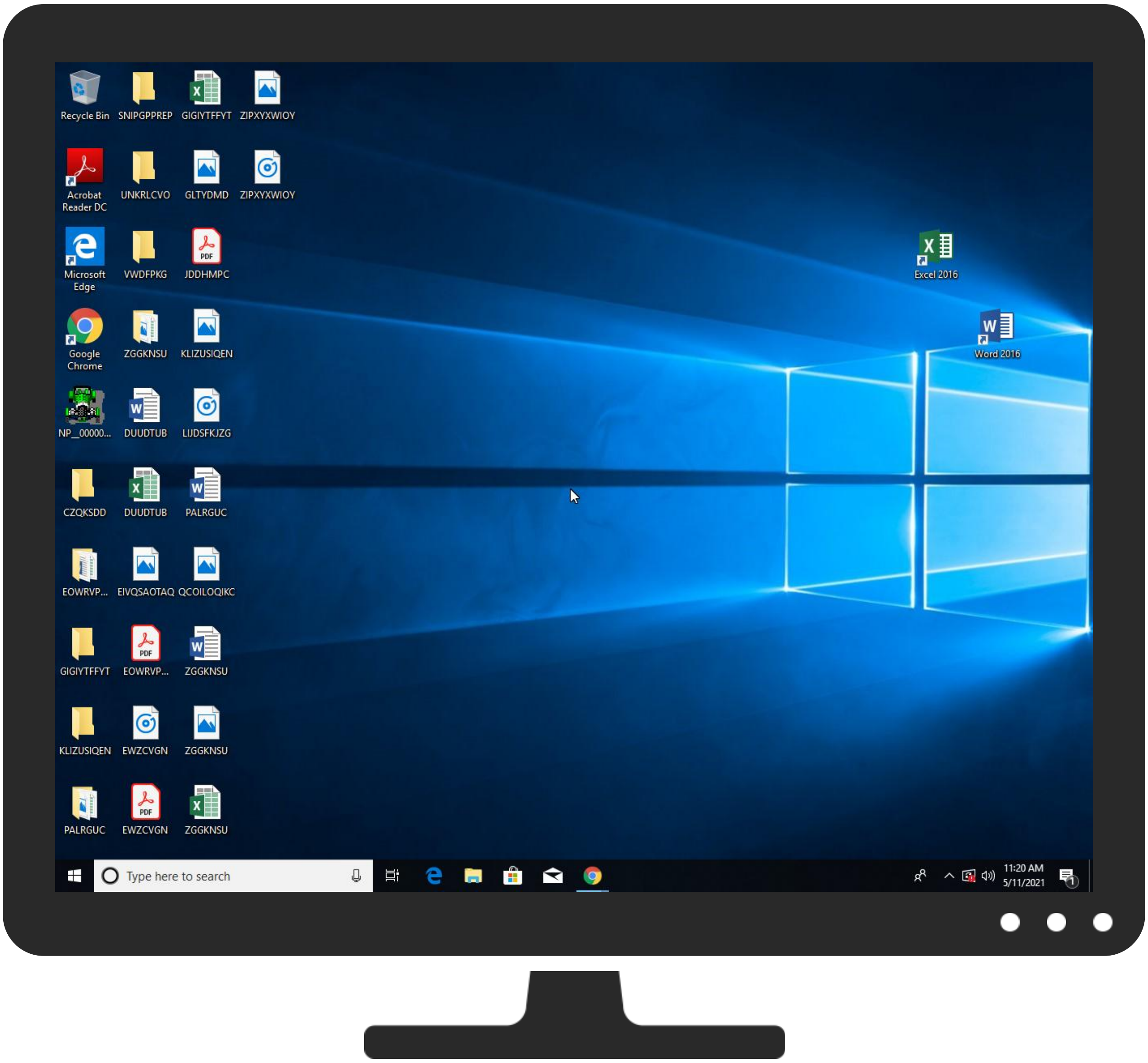
ID: 410830
Sample: NP__000009116_11-05-2021_08...
Startdate: 11/05/2021
Architecture: WINDOWS
Score: 84

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
NP__000009116_11-05-2021_08_40_37.exe	26%	Virustotal		Browse
NP__000009116_11-05-2021_08_40_37.exe	9%	ReversingLabs	Win32.Trojan.Vebzenpak	

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:	32.0.0 Black Diamond
Analysis ID:	410830
Start date:	11.05.2021
Start time:	11:15:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NP__000009116_11-05-2021_08_40_37.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:	36
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:	mal84.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18% (good quality ratio 4.8%) • Quality average: 14.4% • Quality standard deviation: 24.7%
HCA Information:	• Successful, ratio: 53% • Number of executed functions: 0 • Number of non-executed functions: 0
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

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

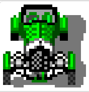
No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.68647587130183
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:	NP__000009116_11-05-2021_08_40_37.exe
File size:	81920
MD5:	3f695fa46992bd20300728e9245c87f8
SHA1:	83d7a6cb77eff285ed7b1950438fa3573d5b31fd
SHA256:	e0f53d67eb5d4a5bab2f6d0bbaff502896e12572b97bf035 0c88cfac3fcc5b8f
SHA512:	04e7fdd44934be48435ae8ccb143b8d0d95a1ea002a549 da5ed7b7a39e9bdcb1be1d942200ce39b3119d4bf29d0e acc9fdefed3dc38e1d25b689e747f9348aef
SSDEEP:	1536:1HDgHBRiC/5r4b01V/M7FWf0Nq7Iz/a2GeD:JY4+ 542/YFWfea2Ge
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$........#...B...B ...B..L^...B...`...B...d...B..Rich.B..........PE..L......`.............. ....0.............. ....@................

File Icon

	
Icon Hash:	b09298b8cc8a19c6

Static PE Info

General

Entrypoint:	0x4013f0
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:	0x6099E2D3 [Tue May 11 01:50:11 2021 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:	ec8e962978786706cf0189109090c85e

Entrypoint Preview

Instruction
push 00401FC8h
call 00007F37C4DD6B53h
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 [esi], bl
xchg eax, edi
push edi
out dx, eax
inc edx
push edi
imul ecx, dword ptr [ecx-47h], 23h
mov ebp, 6200D058h
cmp al, byte 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], ah

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x11074	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x14000	0xc04	.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	0x158	.text

Name	Virtual Address	Virtual Size	Is in Section
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	0x10674	0x11000	False	0.414435891544	data	6.16645068295	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x12000	0x11f4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x14000	0xc04	0x1000	False	0.287353515625	data	3.00270676998	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1435c	0x8a8	data		
RT_GROUP_ICON	0x14348	0x14	data		
RT_VERSION	0x140f0	0x258	data	Chinese	Taiwan

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaAryMove, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaRecAnsiToUni, __vbaStrCat, __vbaSetSystemError, __vbaHresultCheckObj, __vbaLenVar, _adj_fdiv_m32, __vbaAryDestruct, __vbaVarForInit, __vbaObjSet, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaVarTstLt, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, __vbaAryConstruct2, __vbaVarTstEq, __vbaI2I4, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, __vbaRecUniToAnsi, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaStrVarVal, _CIlog, __vbaNew2, __vbaVar2Vec, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaStrToAnsi, __vbaVarDup, __vbaFpI4, __vbaVarCopy, _CIatan, __vbaStrMove, __vbaCastObj, _allmul, __vbaLateIdSt, _CItan, __vbaVarForNext, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0404 0x04b0
InternalName	rammier
FileVersion	1.00
CompanyName	Asso Filler
ProductName	Asso Filler
ProductVersion	1.00
FileDescription	Asso Filler
OriginalFilename	rammier.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: NP__000009116_11-05-2021_08_40_37.exe PID: 480 Parent PID: 5648

General

Start time:	11:16:09
Start date:	11/05/2021
Path:	C:\Users\user\Desktop\NP__000009116_11-05-2021_08_40_37.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NP__000009116_11-05-2021_08_40_37.exe'
Imagebase:	0x400000
File size:	81920 bytes
MD5 hash:	3F695FA46992BD20300728E9245C87F8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.767064760.00000000029F0000.00000040.00000001.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