ID: 339336
Sample Name: Agreement Terms Sample.pdf.exe
Cookbook: default.jbs
Time: 21:13:29
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

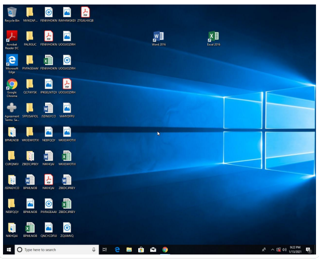
Analysis Report Agreement Terms Sample.pdf.exe

Overview

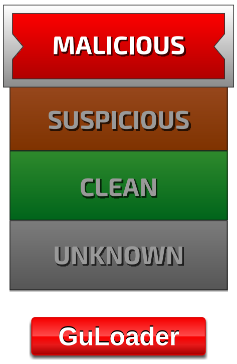
General Information

Sample Name:	Agreement Terms Sample.pdf.exe
Analysis ID:	339336
MD5:	76b6c2b227dd2a..
SHA1:	db06ffb667569ab..
SHA256:	128fa77a11cedbe.
Tags:	exe GuLoader

Most interesting Screenshot:



Detection

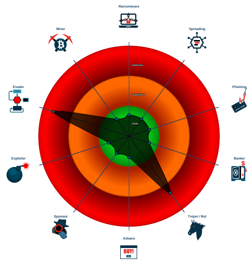


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Contains functionality to detect hard…
- Found potential dummy code loops (…
- Initial sample is a PE file and has a …
- Potential time zone aware malware
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Uses an obfuscated file name to hid…
- Yara detected VB6 Downloader Gen…
- Abnormal high CPU Usage
- Contains functionality for execution …
- Contains functionality to read the PEB

Classification



Startup

- System is w10x64
- Agreement Terms Sample.pdf.exe (PID: 6116 cmdline: 'C:\Users\user\Desktop\Agreement Terms Sample.pdf.exe' MD5: 76B6C2B227DD2AE92BB3B86A66A8FE52)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

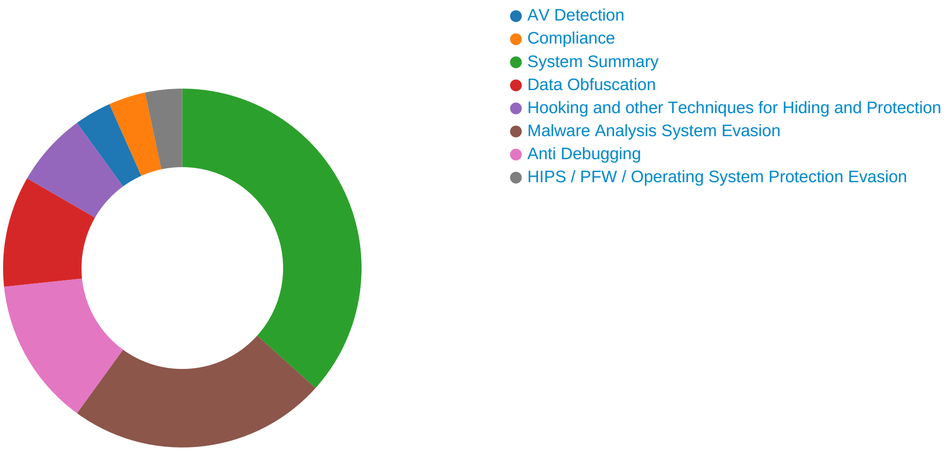
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: Agreement Terms Sample.pdf.exe PID: 6116	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: Agreement Terms Sample.pdf.exe PID: 6116	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

System Summary:

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Hooking and other Techniques for Hiding and Protection:

Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Potential time zone aware malware

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

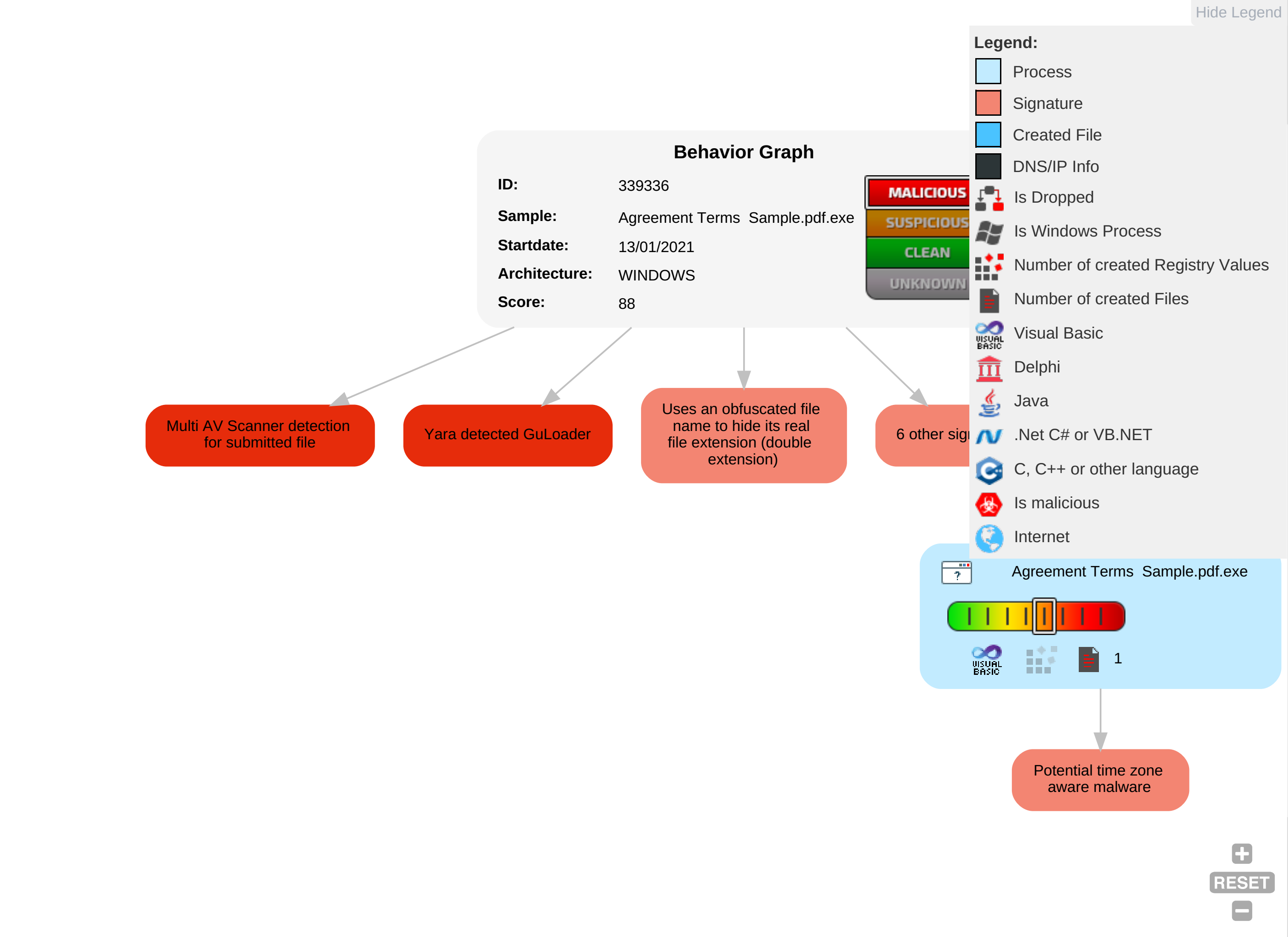
Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	R T W A
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1 1	LSASS Memory	Security Software Discovery 4 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	R W W A

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Virtualization/Sandbox Evasion 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	O D C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1 1	NTDS	Process 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 2 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

Behavior Graph



Behavior Graph

ID: 339336

Sample: Agreement Terms Sample.pdf.exe

Startdate: 13/01/2021

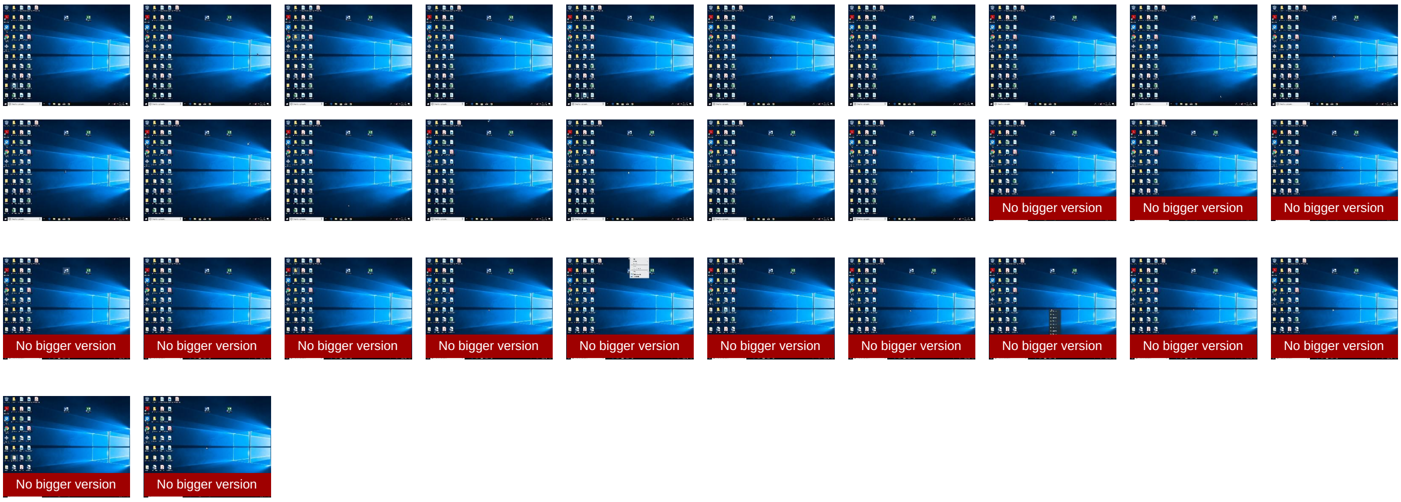
Architecture: WINDOWS

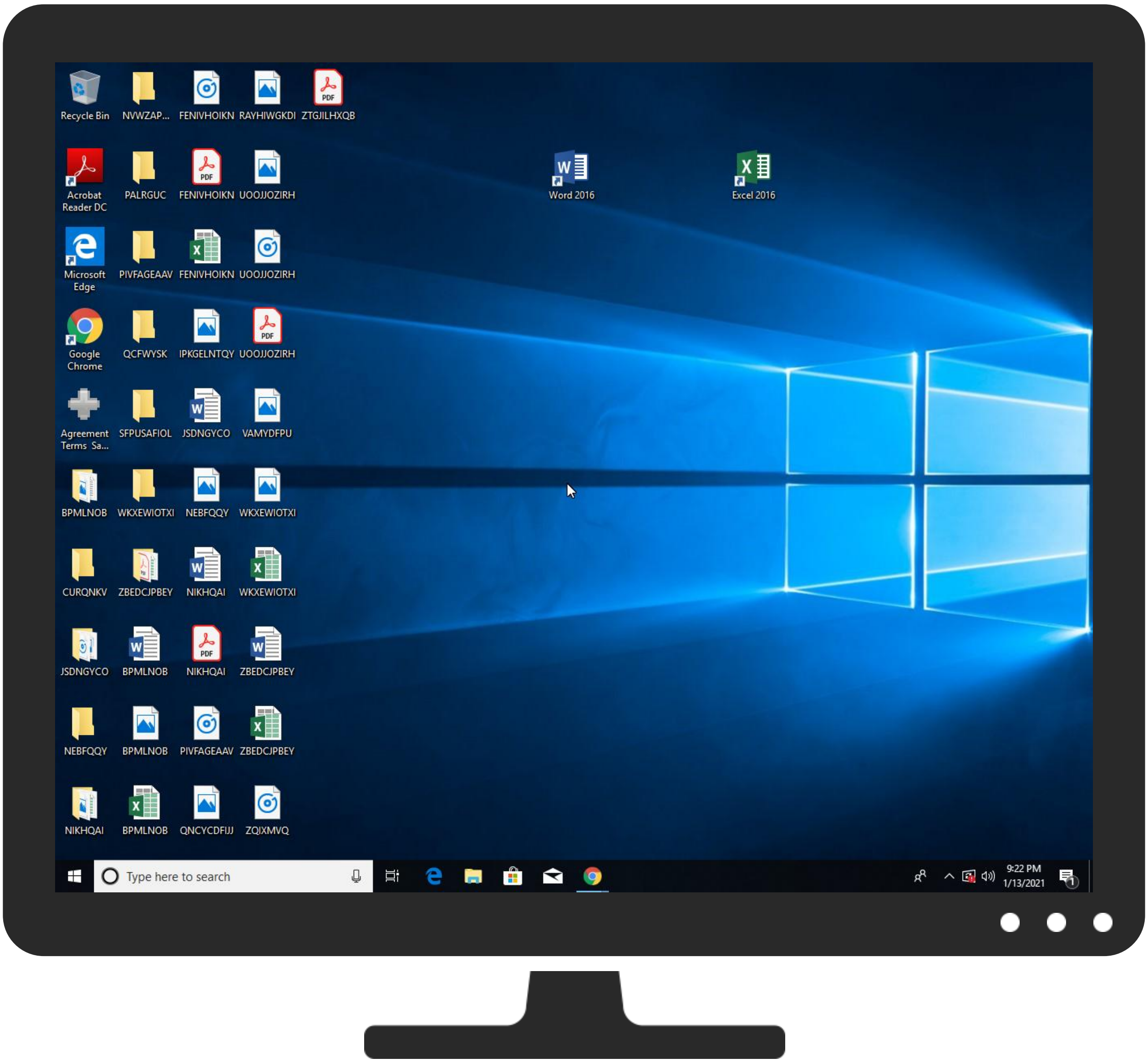
Score: 88

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
Agreement Terms Sample.pdf.exe	21%	Virustotal		Browse
Agreement Terms Sample.pdf.exe	4%	ReversingLabs		

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 Red Diamond
Analysis ID:	339336
Start date:	13.01.2021
Start time:	21:13:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Agreement Terms Sample.pdf.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:	11
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:	mal88.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 12.5% (good quality ratio 3.3%) • Quality average: 14.9% • Quality standard deviation: 28.3%
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, WMIADAP.exe, MusNotifyIcon.exe, conhost.exe, svchost.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):	5.164931273631205
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%

General

File name:	Agreement Terms Sample.pdf.exe
File size:	65536
MD5:	76b6c2b227dd2ae92bb3b86a66a8fe52
SHA1:	db06ffb667569ab3b379012567c27919c36d885a
SHA256:	128fa77a11cedbe782819f0d2e2666a04e4f8d2966a72f215c77b8933c914a47
SHA512:	74614ba4f06a95c07257896002b99023714b85da540a923e2dfa59fbcd3262d2bda715ff4a2a0384b9a7cca0c5dbb34298bda4ae5ebaba9eef51bfc5f87a176b
SSDEEP:	768:tdhWOzU3SN+0MX6x7Z4LNeLmKETN3rWCC0Kg:/hWSUCN+1Xc7ONeFIJ3Hp
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...S..M.....................0....................@................

File Icon

Icon Hash:	f030f0c6f030b100

Static PE Info

General

Entrypoint:	0x401200
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:	0x4DF4FD53 [Sun Jun 12 17:54:27 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:	e4e19abc2b8b3cdf6beb846e51c393a2

Entrypoint Preview

Instruction
push 00401E60h
call 00007FAB30B1BBF5h
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 [edi], cl
add bl, byte ptr [esi+09C8E7E3h]
dec edx

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd244	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x10000	0x8b0	.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	0xc4	.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	0xc5e8	0xd000	False	0.519193209135	data	5.8716351227	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0xe000	0x1158	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x10000	0x8b0	0x1000	False	0.135986328125	data	1.29485435267	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x10348	0x568	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x10334	0x14	data		
RT_VERSION	0x100f0	0x244	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	__vbaCyForInit, _CIcos, _adj_fptan, __vbaFreeVar, __vbaEnd, _adj_fdiv_m64, _adj_fprem1, __vbaStrCat, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaVarTstLt, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaCyI2, __vbaStrCmp, __vbaCyI4, _adj_fpatan, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaCyForNext, _CIlog, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaI4Str, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	Affolker
FileVersion	2.00
CompanyName	Axis Corp
Comments	Axis Corp
ProductName	Project1
ProductVersion	2.00
OriginalFilename	Affolker.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: Agreement Terms Sample.pdf.exe PID: 6116 Parent PID: 5880

General

Start time:	21:14:22
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\Agreement Terms Sample.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Agreement Terms Sample.pdf.exe'
Imagebase:	0x400000
File size:	65536 bytes
MD5 hash:	76B6C2B227DD2AE92BB3B86A66A8FE52
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