ID: 323820
Sample Name: Shipping Document INVPLBL_pdf.exe
Cookbook: default.jbs
Time: 15:47:28
Date: 27/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report Shipping Document INVPLBL_pdf.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 5
AV Detection: 5
System Summary: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 5
Anti Debugging: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
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 8
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 10
Created / dropped Files 10
Static File Info 10
General 10
File Icon 10
Static PE Info 10
General 10
Entrypoint Preview 11
Data Directories 12
Sections 12
Resources 12
Imports 12
Version Infos 13
Possible Origin 13
Network Behavior 13
UDP Packets 13

DNS Queries 14
DNS Answers 14
Code Manipulations 14
Statistics 14
Behavior 14
System Behavior 15
Analysis Process: Shipping Document INVPLBL_pdf.exe PID: 7072 Parent PID: 5852 15
General 15
File Activities 15
Analysis Process: Shipping Document INVPLBL_pdf.exe PID: 6704 Parent PID: 7072 15
General 15
File Activities 16
File Created 16
Disassembly 16
Code Analysis 16

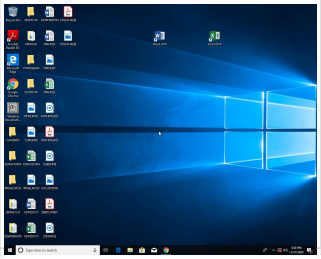
Analysis Report Shipping Document INVPLBL_pdf.exe

Overview

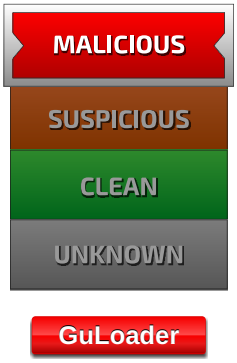
General Information

Sample Name:	Shipping Document INVPLBL_pdf.exe
Analysis ID:	323820
MD5:	40e23535eaeb38..
SHA1:	115391590b015b..
SHA256:	f76e242ad82adab.
Tags:	exe GuLoader

Most interesting Screenshot:



Detection

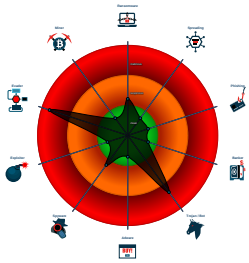


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Contains functionality to detect hard…
- Contains functionality to hide a threa…
- Detected RDTSC dummy instruction…
- Executable has a suspicious name (…
- Hides threads from debuggers
- Initial sample is a PE file and has a …
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Yara detected VB6 Downloader Gen…

Classification



Startup

- **System is w10x64**
- Shipping Document INVPLBL_pdf.exe (PID: 7072 cmdline: 'C:\Users\user\Desktop\Shipping Document INVPLBL_pdf.exe' MD5: 40E23535EAEB38100848D2544F29425D)
  - Shipping Document INVPLBL_pdf.exe (PID: 6704 cmdline: 'C:\Users\user\Desktop\Shipping Document INVPLBL_pdf.exe' MD5: 40E23535EAEB38100848D2544F29425D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

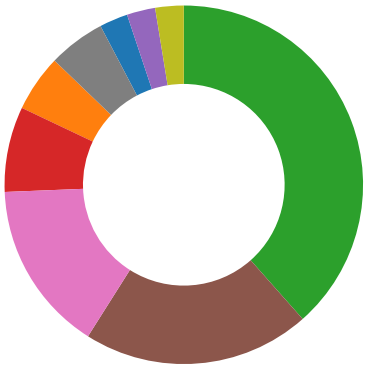
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: Shipping Document INVPLBL_pdf.exe PID: 6704	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: Shipping Document INVPLBL_pdf.exe PID: 6704	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: Shipping Document INVPLBL_pdf.exe PID: 7072	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: Shipping Document INVPLBL_pdf.exe PID: 7072	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Networking
- 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:

Multi AV Scanner detection for submitted file

System Summary:

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

Initial sample is a PE file and has a suspicious name

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 Any.run

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:

Contains functionality to hide a thread from the debugger

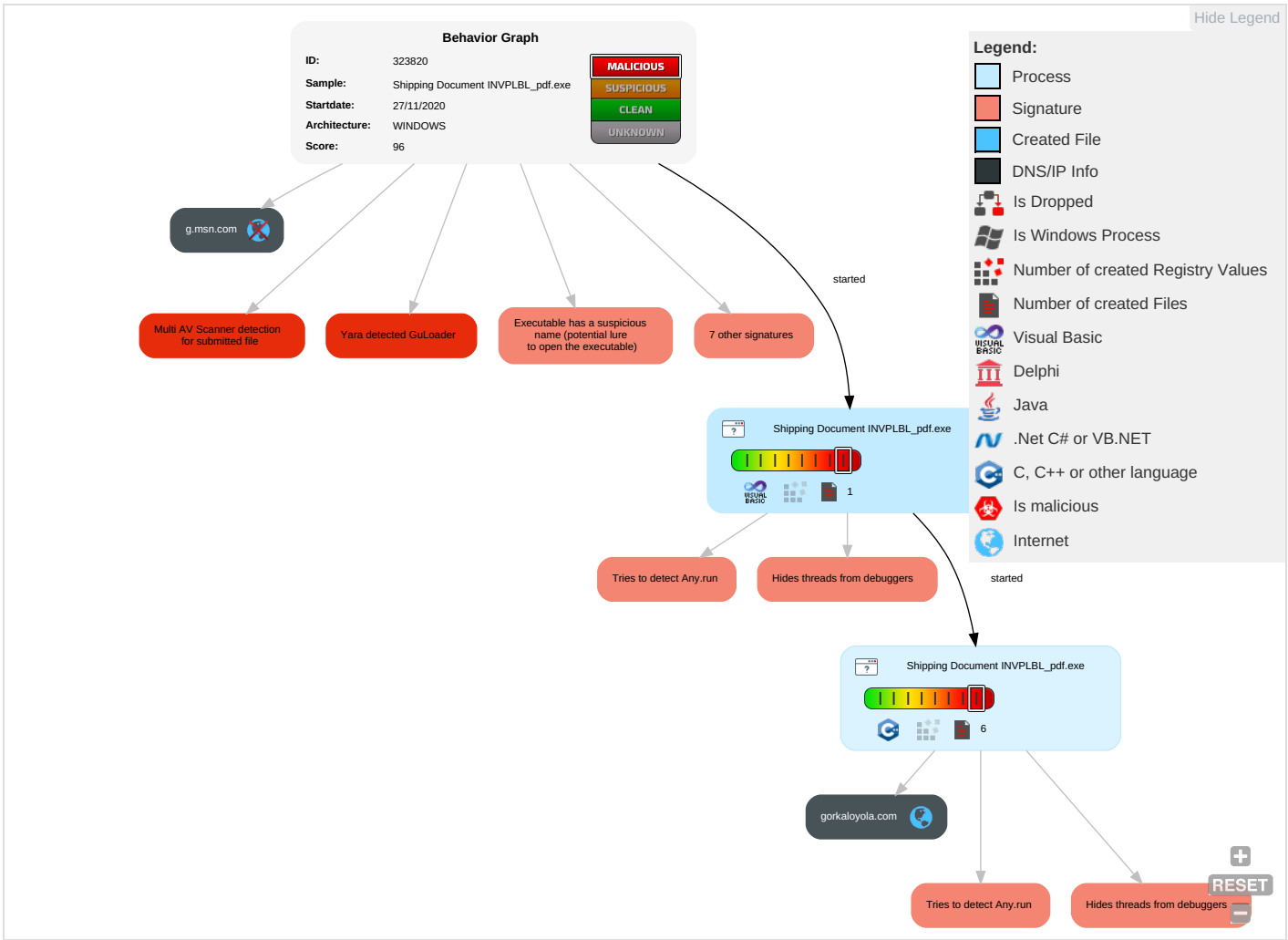
Hides threads from debuggers

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 2	Virtualization/Sandbox Evasion 2 1	OS Credential Dumping	Security Software Discovery 7 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicati

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Virtualization/Sandbox Evasion 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 t Redirect Pho Calls/SMS
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	Application Layer Protocol 1	Exploit SS7 t Track Device Location
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
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Service Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

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
Shipping Document INVPLBL_pdf.exe	31%	Virustotal		Browse
Shipping Document INVPLBL_pdf.exe	19%	ReversingLabs	Win32.Trojan.Wacatac	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
gorkaloyola.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://gorkaloyola.com/cashout/Kalied_zgFWOmD234.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gorkaloyola.com	192.185.170.106	true	false	• 0%, Virustotal, Browse	unknown
g.msn.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://gorkaloyola.com/cashout/Kalied_zgFWOmD234.bin	Shipping Document INVPLBL_pdf.exe, 0000000A.00000002.596081636.0000000000560000.00000040.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323820
Start date:	27.11.2020
Start time:	15:47:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Shipping Document INVPLBL_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:	18
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:	mal96.troj.evad.winEXE@3/0@2/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.6% (good quality ratio 0.5%) • Quality average: 36.2% • Quality standard deviation: 21.3%

HCA Information:	• Successful, ratio: 88% • 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
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 52.255.188.83, 51.104.139.180, 40.67.251.132, 52.155.217.156, 20.54.26.129, 52.142.114.176, 92.122.213.194, 92.122.213.247, 23.210.248.85, 51.11.168.160 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, g-msn-com-nsatc.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, par02p.wns.notify.windows.com.akadns.net, db5p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey 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):	5.089976510884923
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:	Shipping Document INVPLBL_pdf.exe
File size:	86016
MD5:	40e23535eaeb38100848d2544f29425d
SHA1:	115391590b015b30e742095c3355b63f4ae29335
SHA256:	f76e242ad82adab98e38fbdcc1469a7066031c5345d4904035d545713355629d
SHA512:	981249b64fb0d86ae22f45a669d209605cb4d0dd17bbd440685f9dc161bfc7754e2c47f4620cf3b91d29ef8ffcc30c7f8548e0b755b4048ab89f63c6882d625d
SSDEEP:	768:JzJPpJ4xUMiQj1tKl6lfWRGt55Pi5G2wVHRyEkP:Jzl421K1tKlDQGtau
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...C.TN.....@..... ....@.....

File Icon

Icon Hash:	e9e1c5c9d5d9d1aa

Static PE Info

General

Entrypoint:	0x40120c
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:	0x4E54D443 [Wed Aug 24 10:36:51 2011 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0

General	
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	d1e6b215baa9cbbcb95c5c9eee80175d

Entrypoint Preview

Instruction
push 0040297Ch
call 00007F0EA0728FB3h
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+3A5E7E9Ch], bh
and eax, CAAC4075h
dec ebp
cmpsd
mov esi, 002543FEh
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [edx+00h], al
push es
push eax
add dword ptr [ecx], 50h
jc 00007F0EA0729031h
push 00000065h
arpl word ptr [ecx+esi+00h], si
add byte ptr [eax], al
add ah, al
sub dword ptr [edx], ecx
add eax, dword ptr [eax]
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
sub al, 30h
mov al, byte ptr [A282ECD9h]
out dx, eax
dec ebp
xchg eax, ecx
mov bl, 95h
mov ah, 3Ch
sbb ah, byte ptr [eax-68h]
loop 00007F0EA0728F69h
retf 0F39h
sti
mov word ptr [ebp+ebx*4-56h], es
mov al, byte ptr [CDA1847Fh]
fstp tbyte ptr [edx]
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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x111c4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x14000	0x119e	.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	0xc0	.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	0x10580	0x11000	False	0.425680721507	data	5.67635669522	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x12000	0x1150	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x14000	0x119e	0x2000	False	0.219116210938	data	2.9662217016	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x148f6	0x8a8	data		
RT_ICON	0x1438e	0x568	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x1436c	0x22	data		
RT_VERSION	0x14120	0x24c	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaFreeVar, __vbaEnd, __vbaFreeVarList, _adj_fdiv_m64, _adj_fprem1, __vbaStrCat, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaBoolStr, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaFpR8, __vbaVarTstLt, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaAryConstruct2, _adj_fpatan, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaI2Str, __vbaFPException, _CIlog, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, _CIatan, __vbaStrMove, _allmul, _CItan, __vbaFPInt, _CIexp

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	Skaget
FileVersion	2.00
CompanyName	Madrigal Corp
Comments	Madrigal Corp
ProductName	Project1
ProductVersion	2.00
OriginalFilename	Skaget.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:48:21.044915915 CET	58384	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:48:21.082891941 CET	53	58384	8.8.8.8	192.168.2.6
Nov 27, 2020 15:48:22.241636038 CET	60261	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:48:22.268754005 CET	53	60261	8.8.8.8	192.168.2.6
Nov 27, 2020 15:48:23.654417038 CET	56061	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:48:23.681477070 CET	53	56061	8.8.8.8	192.168.2.6
Nov 27, 2020 15:48:25.483433008 CET	58336	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:48:25.510389090 CET	53	58336	8.8.8.8	192.168.2.6
Nov 27, 2020 15:48:26.202280998 CET	53781	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:48:26.229373932 CET	53	53781	8.8.8.8	192.168.2.6
Nov 27, 2020 15:48:27.250709057 CET	54064	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:48:27.277700901 CET	53	54064	8.8.8.8	192.168.2.6
Nov 27, 2020 15:48:28.031394005 CET	52811	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:48:28.058437109 CET	53	52811	8.8.8.8	192.168.2.6
Nov 27, 2020 15:48:28.713527918 CET	55299	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:48:28.740658045 CET	53	55299	8.8.8.8	192.168.2.6
Nov 27, 2020 15:48:30.389445066 CET	63745	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:48:30.425527096 CET	53	63745	8.8.8.8	192.168.2.6
Nov 27, 2020 15:48:31.447170019 CET	50055	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:48:31.482527971 CET	53	50055	8.8.8.8	192.168.2.6
Nov 27, 2020 15:48:32.112328053 CET	61374	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:48:32.139417887 CET	53	61374	8.8.8.8	192.168.2.6
Nov 27, 2020 15:48:32.868566990 CET	50339	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:48:32.895838022 CET	53	50339	8.8.8.8	192.168.2.6
Nov 27, 2020 15:48:34.463712931 CET	63307	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:48:34.491255999 CET	53	63307	8.8.8.8	192.168.2.6
Nov 27, 2020 15:48:35.195472002 CET	49694	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:48:35.222491980 CET	53	49694	8.8.8.8	192.168.2.6
Nov 27, 2020 15:48:45.788101912 CET	54982	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:48:45.815256119 CET	53	54982	8.8.8.8	192.168.2.6
Nov 27, 2020 15:49:06.379210949 CET	50010	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:49:06.416075945 CET	53	50010	8.8.8.8	192.168.2.6
Nov 27, 2020 15:49:13.421981096 CET	63718	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:49:13.457546949 CET	53	63718	8.8.8.8	192.168.2.6
Nov 27, 2020 15:49:14.304552078 CET	62116	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:49:14.342350006 CET	53	62116	8.8.8.8	192.168.2.6
Nov 27, 2020 15:49:14.780752897 CET	63816	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:49:14.818800926 CET	53	63816	8.8.8.8	192.168.2.6
Nov 27, 2020 15:49:15.112642050 CET	55014	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:49:15.148348093 CET	53	55014	8.8.8.8	192.168.2.6
Nov 27, 2020 15:49:15.565212965 CET	62208	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:49:15.592267990 CET	53	62208	8.8.8.8	192.168.2.6
Nov 27, 2020 15:49:15.980247974 CET	57574	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:49:16.015897036 CET	53	57574	8.8.8.8	192.168.2.6
Nov 27, 2020 15:49:16.489033937 CET	51818	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:49:16.530077934 CET	53	51818	8.8.8.8	192.168.2.6
Nov 27, 2020 15:49:17.026971102 CET	56628	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:49:17.062434912 CET	53	56628	8.8.8.8	192.168.2.6
Nov 27, 2020 15:49:17.666729927 CET	60778	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:49:17.693818092 CET	53	60778	8.8.8.8	192.168.2.6
Nov 27, 2020 15:49:18.044378996 CET	53799	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:49:18.079725027 CET	53	53799	8.8.8.8	192.168.2.6
Nov 27, 2020 15:49:18.969459057 CET	54683	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:49:19.005215883 CET	53	54683	8.8.8.8	192.168.2.6
Nov 27, 2020 15:49:21.326265097 CET	59329	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:49:21.361706018 CET	53	59329	8.8.8.8	192.168.2.6
Nov 27, 2020 15:49:26.910702944 CET	64021	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:49:26.946363926 CET	53	64021	8.8.8.8	192.168.2.6
Nov 27, 2020 15:49:44.968725920 CET	56129	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:49:45.004426956 CET	53	56129	8.8.8.8	192.168.2.6
Nov 27, 2020 15:49:50.758688927 CET	58177	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:49:50.794290066 CET	53	58177	8.8.8.8	192.168.2.6
Nov 27, 2020 15:50:09.024199009 CET	50700	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:50:09.051368952 CET	53	50700	8.8.8.8	192.168.2.6
Nov 27, 2020 15:50:25.283133030 CET	54069	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:50:25.445837975 CET	53	54069	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 27, 2020 15:49:21.326265097 CET	192.168.2.6	8.8.8.8	0xea1	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Nov 27, 2020 15:50:25.283133030 CET	192.168.2.6	8.8.8.8	0x47c2	Standard query (0)	gorkaloyola.com	A (IP address)	IN (0x0001)

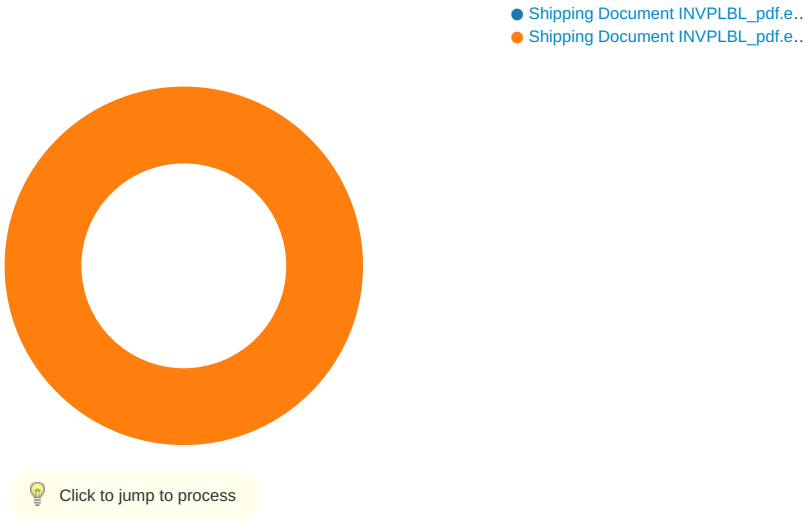
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 15:49:21.361706018 CET	8.8.8.8	192.168.2.6	0xea1	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:50:25.445837975 CET	8.8.8.8	192.168.2.6	0x47c2	No error (0)	gorkaloyola.com		192.185.170.106	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Shipping Document INVPLBL_pdf.exe PID: 7072 Parent PID: 5852

General

Start time:	15:48:21
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\Shipping Document INVPLBL_pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Shipping Document INVPLBL_pdf.exe'
Imagebase:	0x400000
File size:	86016 bytes
MD5 hash:	40E23535EAEB38100848D2544F29425D
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: Shipping Document INVPLBL_pdf.exe PID: 6704 Parent PID: 7072

General

Start time:	15:49:16
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\Shipping Document INVPLBL_pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Shipping Document INVPLBL_pdf.exe'
Imagebase:	0x400000
File size:	86016 bytes
MD5 hash:	40E23535EAEB38100848D2544F29425D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564676	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564676	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564676	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564676	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564676	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564676	InternetOpenUrlA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis