

JOeSandbox Cloud BASIC



ID: 339385

Sample Name: Shipping
Documents.exe

Cookbook: default.jbs

Time: 22:01:21

Date: 13/01/2021

Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents	2
Analysis Report Shipping Documents.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	4
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	7
Domains and IPs	8
Contacted Domains	8
Contacted IPs	8
General Information	8
Simulations	8
Behavior and APIs	9
Joe Sandbox View / Context	9
IPs	9
Domains	9
ASN	9
JA3 Fingerprints	9
Dropped Files	9
Created / dropped Files	9
Static File Info	9
General	9
File Icon	10
Static PE Info	10
General	10
Entrypoint Preview	10
Data Directories	11
Sections	12
Resources	12
Imports	12
Version Infos	12
Possible Origin	12
Network Behavior	12
Code Manipulations	12
Statistics	13

System Behavior	13
Analysis Process: Shipping Documents.exe PID: 6460 Parent PID: 5668	13
General	13
File Activities	13
Disassembly	13
Code Analysis	13

Analysis Report Shipping Documents.exe

Overview

General Information

Sample Name:

Shipping Documents.exe

Analysis ID:

339385

MD5:

a13297a6096403..

SHA1:

e02adaeb53e136..

SHA256:

35eaf7cfa69be2..

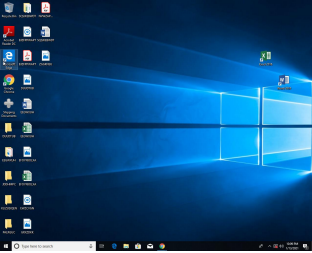
Tags:

DHL

exe

GuLoader

Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

GuLoader

Score:

88

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Multi AV Scanner detection for subm...

Yara detected GuLoader

Contains functionality to detect hard...

Executable has a suspicious name (...

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...

Yara detected VB6 Downloader Gen...

Abnormal high CPU Usage


Contains functionality for execution ...

Contains functionality to query CPU

Classification



Startup

- System is w10x64
-  [Shipping Documents.exe](#) (PID: 6460 cmdline: 'C:\Users\user\Desktop\Shipping Documents.exe' MD5: A13297A6096403F5A7511265E151BB)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

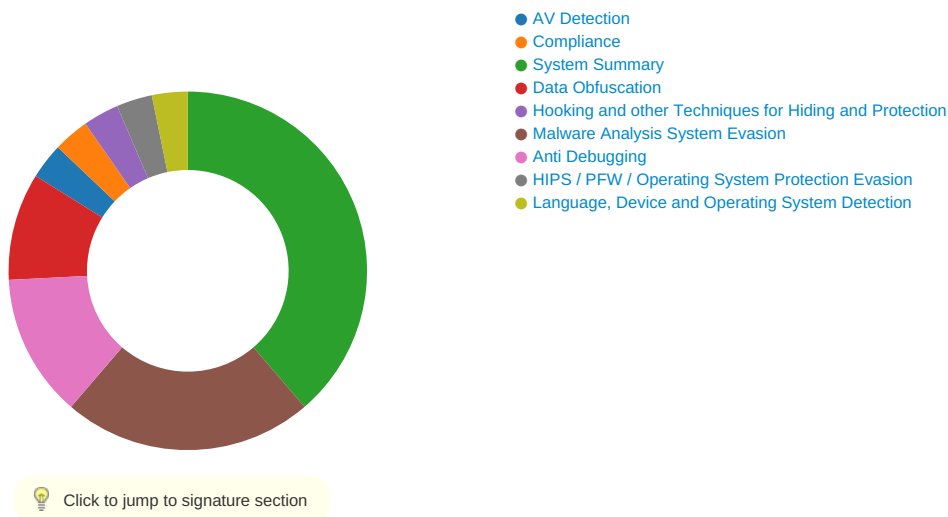
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: Shipping Documents.exe PID: 6460	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: Shipping Documents.exe PID: 6460	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



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)

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	Risk Score
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 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	Risk Score
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 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	Risk Score
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 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	Risk Score



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Shipping Documents.exe	34%	Virustotal		Browse
Shipping Documents.exe	2%	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:	339385
Start date:	13.01.2021
Start time:	22:01:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Shipping Documents.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:	35
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:	<ul style="list-style-type: none">• 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:	<ul style="list-style-type: none">• Successful, ratio: 10.7% (good quality ratio 5.9%)• Quality average: 33.4%• Quality standard deviation: 32.5%
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, MusNotifyIcon.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.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):	5.1712166162996285
TrID:	<ul style="list-style-type: none">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 Documents.exe
File size:	65536
MD5:	a13297a6096403fbf5a7511265e151bb
SHA1:	e02adaeb53e1362281d565fa14b23485aeb758d4
SHA256:	35eaf7cfa69be622c7fae2b72daf3ab245c0237475288ff81568a5fa597fd2f5
SHA512:	5580458078df372c45c1b21a71e3d3329fad06d383add76510d44c0f784e06657fc0fc0d25c247cb22616c390c0524c10b0564bc29d08df1f057aae7fc5559dd
SSDEEP:	768:2xoEO3vkfhGkEe40B68NgDaPGTVk4wl3MYxroGfHsPE64FsmSnOCCmEdQxFT:el8fhGwt8du43P94F67bEds
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.....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:	0x4DC0B19B [Wed May 4 01:53:31 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 00401E5Ch
call 00007FE620AB9995h
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+19536D6Eh], ah
sub byte ptr [ebx], ch
inc esp
lea eax, dword ptr [ecx+5Bh]
outsb
or eax, 009CDF0Eh
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [edx+6Fh], al
jc 00007FE620AB9A06h
jc 00007FE620AB99F3h
jc 00007FE620AB9A11h
push 00000065h
arpl word ptr [ecx+esi+00h], si
or eax, 7061430Ah
je 00007FE620AB9A0Bh
add byte ptr [eax], al
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
add edx, edi

Name	Virtual Address	Virtual Size	Is in Section
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	0xc5f8	0xd000	False	0.520395132212	data	5.87567926879	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	0x8d8	0x1000	False	0.139404296875	data	1.33983584341	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x10370	0x568	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x1035c	0x14	data		
RT_VERSION	0x100f0	0x26c	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	__vbaCyForInit, __Clicos, __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, __vbaCyl2, __vbaStrCmp, __vbaCyl4, __adj_fpatan, EVENT_SINK_Release, __CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptionHandler, __adj_fprem, __adj_fdivr_m64, __vbaFPException, __vbaCyForNext, __Cilog, __vbaNew2, __adj_fdiv_m32i, __adj_fdivr_m32i, __vbaI4Str, __vbaFreeStrList, __adj_fdivr_m32, __adj_fdiv_r, __Clatan, __vbaStrMove, __allmul, __Cltan, __Clexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	HandlerIsaTernes5
FileVersion	2.00
CompanyName	Axis Corp
Comments	Axis Corp
ProductName	Project1
ProductVersion	2.00
OriginalFilename	HandlerIsaTernes5.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: Shipping Documents.exe PID: 6460 Parent PID: 5668

General

Start time:	22:02:12
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\Shipping Documents.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Shipping Documents.exe'
Imagebase:	0x400000
File size:	65536 bytes
MD5 hash:	A13297A6096403FBF5A7511265E151BB
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