

JOESandbox Cloud BASIC



ID: 452548

Sample Name: shipping
documents approval.exe

Cookbook: default.jbs

Time: 15:12:06

Date: 22/07/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report shipping documents approval.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Agenttesla	4
Yara Overview	4
Memory Dumps	4
Unpacked PEs	5
Sigma Overview	5
Jbx Signature Overview	5
AV Detection:	5
System Summary:	5
Data Obfuscation:	5
Malware Analysis System Evasion:	5
Anti Debugging:	5
HIPS / PFW / Operating System Protection Evasion:	5
Stealing of Sensitive Information:	6
Remote Access Functionality:	6
Mitre Att&ck Matrix	6
Behavior Graph	6
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	10
Contacted Domains	10
URLs from Memory and Binaries	10
Contacted IPs	10
General Information	10
Simulations	11
Behavior and APIs	11
Joe Sandbox View / Context	11
IPs	11
Domains	11
ASN	11
JA3 Fingerprints	11
Dropped Files	11
Created / dropped Files	12
Static File Info	12
General	12
File Icon	12
Static PE Info	12
General	13
Entrypoint Preview	13
Data Directories	13
Sections	13
Resources	13
Imports	13
Version Infos	13
Network Behavior	13
Code Manipulations	13
Statistics	13
Behavior	13
System Behavior	13
Analysis Process: shipping documents approval.exe PID: 5640 Parent PID: 5780	14
General	14
File Activities	14
File Created	14
File Written	14
File Read	14
Analysis Process: shipping documents approval.exe PID: 4276 Parent PID: 5640	14
General	14
Analysis Process: shipping documents approval.exe PID: 4280 Parent PID: 5640	14
General	14
File Activities	15
File Created	15
File Read	15

Disassembly	15
Code Analysis	15

Windows Analysis Report shipping documents approval...

Overview

General Information

Sample Name:	shipping documents approval.exe
Analysis ID:	452548
MD5:	2cc7d328527b05..
SHA1:	e02b77a99a315d..
SHA256:	d9c12ca57571d1..
Tags:	exe
Infos:	
Most interesting Screenshot:	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

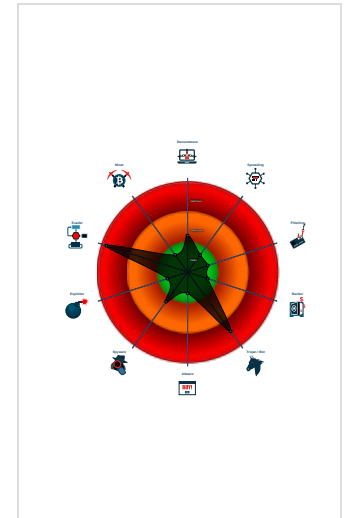
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm...
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains potentia...
- Initial sample is a PE file and has a ...
- Injects a PE file into a foreign proce...
- Machine Learning detection for samp...
- Potentially malicious time measurem...
- Queries sensitive BIOS Information ...
- Queries sensitive network adapter in...

Classification



Process Tree

- System is w10x64
- shipping documents approval.exe (PID: 5640 cmdline: 'C:\Users\user\Desktop\shipping documents approval.exe' MD5: 2CC7D328527B05A048F9A8386102420C)
 - shipping documents approval.exe (PID: 4276 cmdline: {path} MD5: 2CC7D328527B05A048F9A8386102420C)
 - shipping documents approval.exe (PID: 4280 cmdline: {path} MD5: 2CC7D328527B05A048F9A8386102420C)
- cleanup

Malware Configuration

Threatname: Agenttesla

```
{  
  "Exfil Mode": "SMTP",  
  "Username": "akibapen@saisianket-tech.com",  
  "Password": "oluwagozie123",  
  "Host": "smtp.saisianket-tech.com"  
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.478904402.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000E.00000002.478904402.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.309550378.00000000433 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.309550378.00000000433 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000E.00000002.481715251.000000002FC 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Click to see the 5 entries

Unpacked PEs


Source	Rule	Description	Author	Strings
0.2.shipping documents approval.exe.4428f88.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.shipping documents approval.exe.4428f88.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
14.2.shipping documents approval.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
14.2.shipping documents approval.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.shipping documents approval.exe.4428f88.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 1 entries

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

 Click to jump to signature section

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary:



Initial sample is a PE file and has a suspicious name

Data Obfuscation:



.NET source code contains potential unpacker

Malware Analysis System Evasion:



Yara detected AntiVM3

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

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

Anti Debugging:



Potentially malicious time measurement code found

HIPS / PFW / Operating System Protection Evasion:



Injects a PE file into a foreign processes

Stealing of Sensitive Information:



Yara detected AgentTesla

Yara detected AgentTesla

Remote Access Functionality:



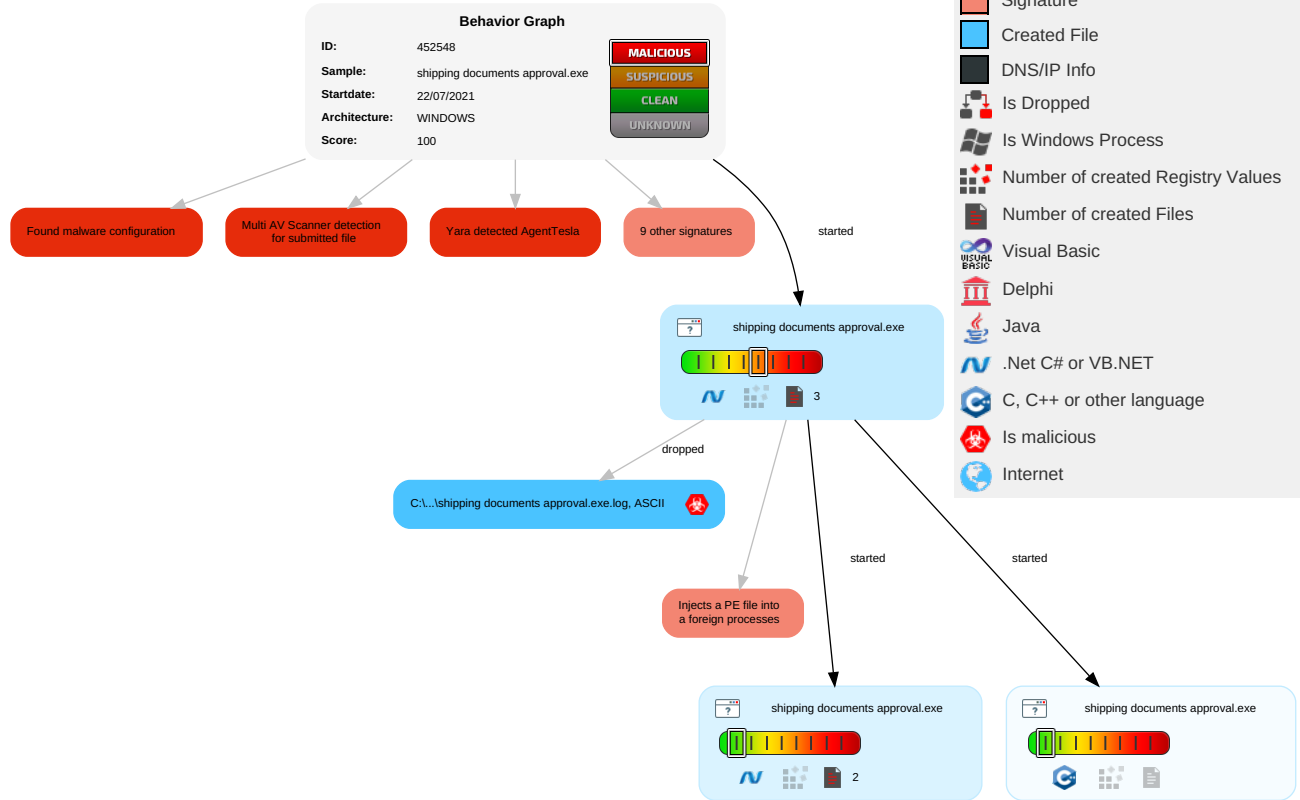
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 3	Cached Domain Credentials	Account Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Owner/User Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

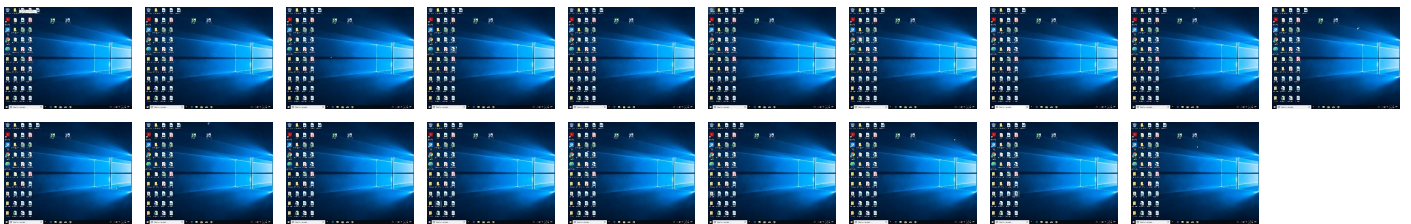
Behavior Graph



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 documents approval.exe	29%	Virusotal		Browse
shipping documents approval.exe	35%	ReversingLabs	ByteCode-MSIL.InfoStealer.DarkStealer	
shipping documents approval.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.shipping documents approval.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fontbureau.comalsFj	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/G	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd;	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.comMi	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.carterandcone.como.q	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/waX	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comrsiv	0%	URL Reputation	safe	
http://www.fontbureau.comrsiv	0%	URL Reputation	safe	
http://www.fontbureau.comrsiv	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cnei	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://EoZDnS.com	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.fontbureau.commetX	0%	Avira URL Cloud	safe	
http://www.carterandcone.comd	0%	URL Reputation	safe	
http://www.carterandcone.comd	0%	URL Reputation	safe	
http://www.carterandcone.comd	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Q	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Q	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Q	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.founder.com.cn/cnhe	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/G	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/G	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/G	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnMi	0%	Avira URL Cloud	safe	
http://www.fontbureau.comX	0%	Avira URL Cloud	safe	
http://www.fontbureau.comlic	0%	URL Reputation	safe	
http://www.fontbureau.comlic	0%	URL Reputation	safe	
http://www.fontbureau.comlic	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htmo	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452548
Start date:	22.07.2021

Start time:	15:12:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	shipping documents approval.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:	24
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:	mal100.troj.evad.winEXE@5/1@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none"> • Successful, ratio: 2.5% (good quality ratio 1.1%) • Quality average: 26.6% • Quality standard deviation: 35.3%
HCA Information:	<ul style="list-style-type: none"> • Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	<ul style="list-style-type: none"> • Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:14:09	API Interceptor	412x Sleep call for process: shipping documents approval.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\shipping documents approval.exe.log	
Process:	C:\Users\user\Desktop\shipping documents approval.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKHqNoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59D9850CF06FE5E7BBF56EAA00A
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F6
Malicious:	true
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System.4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.Core\ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core\ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration\ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\1b219d4630d26b88041b59c21

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.07773784763095
TrID:	<ul style="list-style-type: none"> Win32 Executable (generic) Net Framework (10011505/4) 49.83% Win32 Executable (generic) a (10002005/4) 49.78% Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% Generic Win/DOS Executable (2004/3) 0.01% DOS Executable Generic (2002/1) 0.01%
File name:	shipping documents approval.exe
File size:	922624
MD5:	2cc7d328527b05a048f9a8386102420c
SHA1:	e02b77a99a315dcb7b7f961a2a7adb285f96a58c
SHA256:	d9c12ca57571d19bea0f509e1f3b02b4a6022b5e82f8241756ab12909009542a
SHA512:	b2381091df640f0a2f824adac11b6b86ccf9f501e57b43f7ece88e3382061c6fbc590bd0d74b09e705a0a26f0a48eb59b6a230fc3c2111274a88f84127376
SSDEEP:	12288:EvzK4aoug3yvut646NymjiyUEDRSgcDeKCXSM PQipP5a:Q3lQNNc3g8BipA
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$.PE.L.....:.....0.....J... ..@.....@.....

File Icon



Icon Hash: f0debeffdfcec70

Static PE Info

General	
Entrypoint:	0x484abe
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60F912FB [Thu Jul 22 06:40:59 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x82ac4	0x82c00	False	0.859671889938	data	7.74217502455	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x86000	0x5e320	0x5e400	False	0.167326342838	data	5.64058854685	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe6000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: shipping documents approval.exe PID: 5640 Parent PID: 5780**General**

Start time:	15:12:59
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\shipping documents approval.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\shipping documents approval.exe'
Imagebase:	0xf50000
File size:	922624 bytes
MD5 hash:	2CC7D328527B05A048F9A8386102420C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	<ul style="list-style-type: none"> • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.309550378.0000000004331000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.309550378.0000000004331000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.306725374.0000000003398000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created**File Written****File Read****Analysis Process: shipping documents approval.exe PID: 4276 Parent PID: 5640****General**

Start time:	15:13:41
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\shipping documents approval.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x110000
File size:	922624 bytes
MD5 hash:	2CC7D328527B05A048F9A8386102420C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: shipping documents approval.exe PID: 4280 Parent PID: 5640**General**

Start time:	15:13:41
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\shipping documents approval.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xc10000

File size:	922624 bytes
MD5 hash:	2CC7D328527B05A048F9A8386102420C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	<ul style="list-style-type: none"> • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.478904402.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000002.478904402.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000002.481715251.0000000002FC1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis