ID: 483686
Sample Name: packing list commercial invoice and bl termplate draft for export.exe
Cookbook: default.jbs
Time: 11:35:17
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

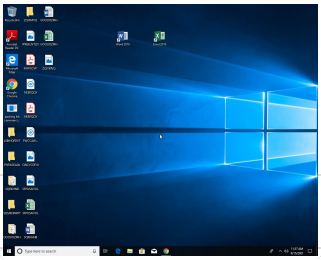
Windows Analysis Report packing list commercial invoi…

Overview

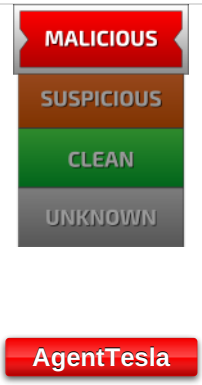
General Information

Sample Name:	packing list commercial invoice and bl termplate draft for export.exe
Analysis ID:	483686
MD5:	ddf2ae4b85ec6e2.
SHA1:	b07236d7dcd264..
SHA256:	34c8be34215e94..
Tags:	AgentTesla exe Invoice
Infos:	

Most interesting Screenshot:



Detection

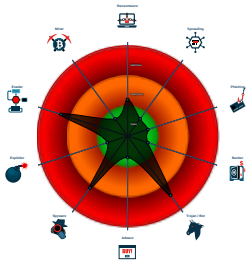


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Initial sample is a PE file and has a …
- Tries to harvest and steal Putty / Wi…
- Machine Learning detection for samp…
- .NET source code contains potentia…
- .NET source code contains very larg…
- Machine Learning detection for dropp…
- Queries sensitive network adapter in…
- Uses schtasks.exe or at.exe to add …

Classification



Process Tree

- **System is w10x64**
- packing list commercial invoice and bl termplate draft for export.exe (PID: 6936 cmdline: 'C:\Users\user\Desktop\packing list commercial invoice and bl termplate draft for export.exe' MD5: DDF2AE4B85EC6E277713BA1B5C844ED7)
  - schtasks.exe (PID: 2572 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\wVhpvdZWIB' /XML 'C:\Users\user\AppData\Local\Temp\tmpCAE9.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6424 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - packing list commercial invoice and bl termplate draft for export.exe (PID: 6588 cmdline: {path} MD5: DDF2AE4B85EC6E277713BA1B5C844ED7)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "sales4@italfood.ae",
  "Password": "Sales@634@$",
  "Host": "mail.italfood.ae"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.931203784.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000009.00000002.931203784.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000009.00000002.933232285.000000000321000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000009.00000002.933232285.000000000321000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
Process Memory Space: packing list commercial invoice and bl termplate draft for export.exe PID: 6588	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.packing list commercial invoice and bl termplate draft for export.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
9.2.packing list commercial invoice and bl termplate draft for export.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

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

Machine Learning detection for dropped file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System Summary:

Initial sample is a PE file and has a suspicious name

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:

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

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

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

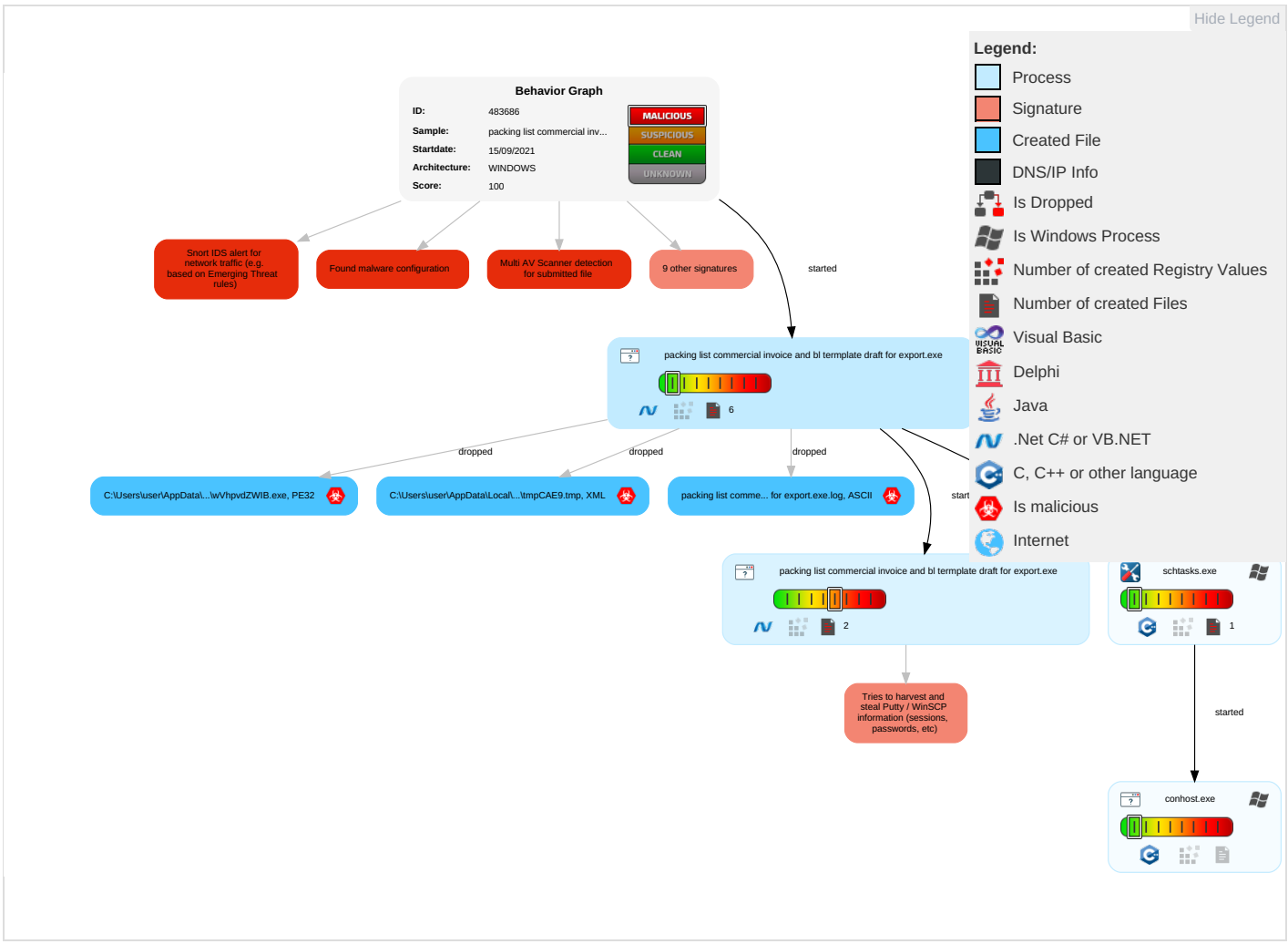
Remote Access Functionality:

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	Net Effe
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 2	Masquerading 1	Credentials in Registry 1	Security Software Discovery 1 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eav Inse Net Cor
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exp Red Call
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Virtualization/Sandbox Evasion 1 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exp Tra Loc
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mar Dev Cor
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Der Ser

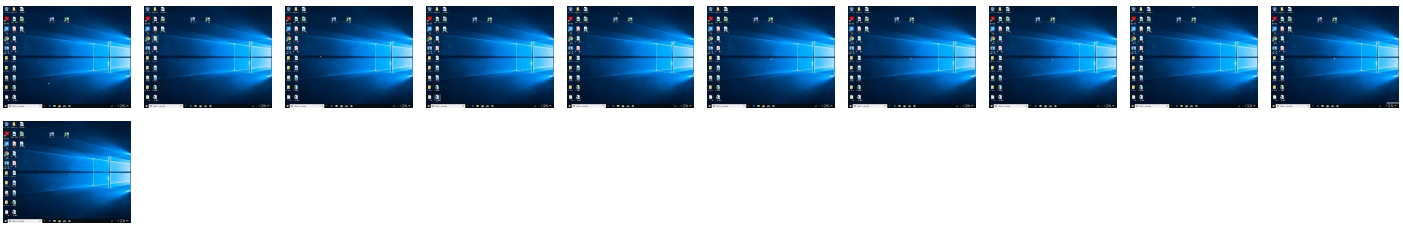
Behavior Graph



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
packing list commercial invoice and bl termplate draft for export.exe	45%	Virustotal		Browse
packing list commercial invoice and bl termplate draft for export.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\wVhpvdZWIB.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.packing list commercial invoice and bl termplate draft for export.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cntte12z	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/X	0%	URL Reputation	safe	
http://www.fonts.comc	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.jiyu-kobo.co.jp/J	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://Q1q5wm8CcDOVVgnVHl2.net	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/C	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//t	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htmQ$	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/5	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/d	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/sv-s	0%	Avira URL Cloud	safe	
http://mail.italfood.ae	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/s_tr	0%	URL Reputation	safe	
http://www.itcfonts.	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/d	0%	URL Reputation	safe	
http://pUvlwl.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/X	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://italfood.ae	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnantE3&	0%	Avira URL Cloud	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:	483686
Start date:	15.09.2021
Start time:	11:35:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	packing list commercial invoice and bl termplate draft for export.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:	17
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:	mal100.troj.spyw.evad.winEXE@6/3@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.7% (good quality ratio 0.2%) • Quality average: 6.7% • Quality standard deviation: 21.5%
HCA Information:	• Successful, ratio: 99% • 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

Simulations

Behavior and APIs

Time	Type	Description
11:36:40	API Interceptor	642x Sleep call for process: packing list commercial invoice and bl termplate draft for export.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\packing list commercial invoice and bl termplate draft for export.exe.log

Process:	C:\Users\user\Desktop\packing list commercial invoice and bl termplate draft for export.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\packing list commercial invoice and bl termplate draft for export.exe.log	
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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.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\f1d8480152e0da9a60ad49c6d16a3b6d\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=b77a

C:\Users\user\AppData\Local\Temp\tmpCAE9.tmp	
Process:	C:\Users\user\Desktop\packing list commercial invoice and bl termplate draft for export.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1643
Entropy (8bit):	5.186254784704947
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGMOtn:cbhK79lNQR/rydbz9I3YODOLNdq3/o
MD5:	C28D1B999BA6E0FA6518407B0192D343
SHA1:	B8909B2B932A913CD21574FE2FC4870E8C65DAEB
SHA-256:	3B7690E16C7E6B1F7A1C421EF9291463E7107DA4A698AF75EA2C01329D77FF20
SHA-512:	73C09E84B34F74803D4530DC59C00A30A7D37438252C7B5D7D2E1801ECCD0C8727334ADD8F7CDBD0D6200E9535163C82F155EE96AACE2F479ED08D6757F3BE
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\wVhpvdZWIB.exe	
Process:	C:\Users\user\Desktop\packing list commercial invoice and bl termplate draft for export.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	878080
Entropy (8bit):	6.2019750608396755
Encrypted:	false
SSDEEP:	6144:6y87fViis7lBGZ1jwtbo9WgnORPsxXwptpMG3CTDkyiegmIqukTNgZ63tCv6pbK4:+twOnTitpBCTDzll5YgS6p55n0F
MD5:	DDF2AE4B85EC6E277713BA1B5C844ED7
SHA1:	B07236D7DCD264152BDB989840C2B78BDFD84764
SHA-256:	34C8BE34215E94BD3FFAB958EA56583EF0E40ADCFA306609A2CB275E3E552D8F
SHA-512:	D7E6E0C8AC12D4E135E756F31AED8FAD433F134534CBB9CD4668B204376BD8059D6D4E81BC98FB0487E4D1C1BDC093EB26548594EAA6FE440F4FF60220A0A51
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...\.Aa.....\.....nz... .....@.. ....@..... z..K..... ....H.....text...tZ... ...\..... ..`.rsrc.....^.....@..@.reloc..... .....d.....@..B.....Pz.....H.....^.....]..... .....0.....(....(.....(.....o.....*.....(.....(.....(.....(.....(....*.N..(....o....(....*&..(....*...s.....s.....s.....s.....s.....*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....,.....o....+....9....~.....,2~.....(....o .....,.

Static File Info

General

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.2019750608396755
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	packing list commercial invoice and bl termplate draft for export.exe
File size:	878080
MD5:	ddf2ae4b85ec6e277713ba1b5c844ed7
SHA1:	b07236d7dcd264152bdb989840c2b78bdfd84764
SHA256:	34c8be34215e94bd3ffab958ea56583ef0e40adcfa306609a2cb275e3e552d8f
SHA512:	d7e6e0c8ac12d4e135e756f31aed8fad433f134534cbb9cd4668b204376bd8059d6d4e81bc98fb0487e4d1c1bdc093eb26548594eaa6fe440f4ff60220a0a511
SSDEEP:	6144:6y87fViis7lBGZ1jwtbo9WgnORPsxXwptpMG3CTDkyiegmIqukTNgZ63tCv6pbK4:+twOnTitpBCTDzll5YgS6p55n0F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...\.Aa.....\.....nz... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d7a6e
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:	0x6141955C [Wed Sep 15 06:40:28 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	0xd5a74	0xd5c00	False	0.520642589547	data	6.20638181174	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd8000	0x600	0x600	False	0.44140625	data	4.23967348971	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0xda000	0xc	0x200	False	0.044921875	data	0.0980041756627	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: packing list commercial invoice and bl termplate draft for export.exe PID: 6936 Parent PID: 5932

General

Start time:	11:36:14
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\packing list commercial invoice and bl termplate draft for export.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\packing list commercial invoice and bl termplate draft for export.exe'
Imagebase:	0x9f0000
File size:	878080 bytes
MD5 hash:	DDF2AE4B85EC6E277713BA1B5C844ED7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 2572 Parent PID: 6936

General

Start time:	11:36:42
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\wVhpvdZWIB' /XML 'C:\Users\user\AppData\Local\Temp\tmpCAE9.tmp'
Imagebase:	0x2d0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6424 Parent PID: 2572

General

Start time:	11:36:42
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: packing list commercial invoice and bl termplate draft for export.exe PID: 6588 Parent PID: 6936

General

Start time:	11:36:43
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\packing list commercial invoice and bl termplate draft for export.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xcc0000
File size:	878080 bytes
MD5 hash:	DDF2AE4B85EC6E277713BA1B5C844ED7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.931203784.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000002.931203784.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.933232285.0000000003211000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000002.933232285.0000000003211000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis