ID: 532850
Sample Name: DHL Waybill receipt.exe
Cookbook: default.jbs
Time: 18:49:38
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report DHL Waybill receipt.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
Networking: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
System Summary: 5
Data Obfuscation: 5
Malware Analysis System 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 9
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 9
Public 9
Private 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 12
General 12
File Icon 12
Static PE Info 12
General 12
Entrypoint Preview 13
Data Directories 13
Sections 13
Resources 13
Imports 13
Version Infos 13
Network Behavior 13
Snort IDS Alerts 13
Network Port Distribution 13
TCP Packets 13
UDP Packets 13
DNS Queries 13
DNS Answers 13
SMTP Packets 14
Code Manipulations 14
Statistics 14
Behavior 14
System Behavior 14
Analysis Process: DHL Waybill receipt.exe PID: 6312 Parent PID: 5828 15

Copyright Joe Security LLC 2021

General 15
File Activities 15
File Created 15
File Written 15
File Read 15
Analysis Process: DHL Waybill receipt.exe PID: 3276 Parent PID: 6312 15
General 15
Analysis Process: DHL Waybill receipt.exe PID: 3688 Parent PID: 6312 15
General 15
File Activities 16
File Created 16
File Read 16
Disassembly 16
Code Analysis 16

Copyright Joe Security LLC 2021

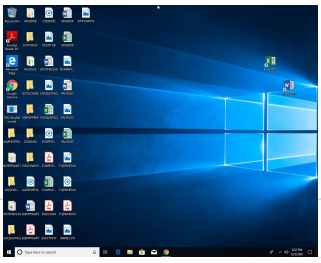
Windows Analysis Report DHL Waybill receipt.exe

Overview

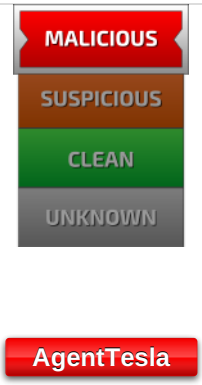
General Information

Sample Name:	DHL Waybill receipt.exe
Analysis ID:	532850
MD5:	fccf07d7a10aff74..
SHA1:	8e7d667885cdc3..
SHA256:	854fdbaa39b3da5.
Tags:	AgentTesla DHL exe
Infos:	

Most interesting Screenshot:



Detection



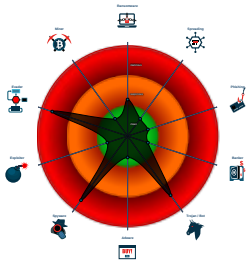
AgentTesla

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
- Yara detected AntiVM3
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fil…
- Initial sample is a PE file and has a …
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Contains functionality to register a lo…

Classification



Process Tree

- **System is w10x64**
- DHL Waybill receipt.exe (PID: 6312 cmdline: "C:\Users\user\Desktop\DHL Waybill receipt.exe" MD5: FCCF07D7A10AFF74CEDC0E93FBE77F90)
  - DHL Waybill receipt.exe (PID: 3276 cmdline: C:\Users\user\Desktop\DHL Waybill receipt.exe MD5: FCCF07D7A10AFF74CEDC0E93FBE77F90)
  - DHL Waybill receipt.exe (PID: 3688 cmdline: C:\Users\user\Desktop\DHL Waybill receipt.exe MD5: FCCF07D7A10AFF74CEDC0E93FBE77F90)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "john.ramos@unitedappliencesgroup.com",
  "Password": "fYmh*3R6#+sv",
  "Host": "smtp.unitedappliencesgroup.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.249607108.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000000.249607108.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.254418452.0000000002A91000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000003.00000000.251632964.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000000.251632964.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 14 entries				

Copyright Joe Security LLC 2021

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.DHL Waybill receipt.exe.400000.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.0.DHL Waybill receipt.exe.400000.8.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
3.0.DHL Waybill receipt.exe.400000.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.0.DHL Waybill receipt.exe.400000.6.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
3.0.DHL Waybill receipt.exe.400000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 16 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

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

Contains functionality to register a low level keyboard hook

System Summary:

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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)

Copyright Joe Security LLC 2021

Stealing of Sensitive Information:

- **Yara detected AgentTesla**
- **Tries to steal Mail credentials (via file / registry access)**
- **Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)**
- **Tries to harvest and steal ftp login credentials**
- **Tries to harvest and steal browser information (history, passwords, etc)**

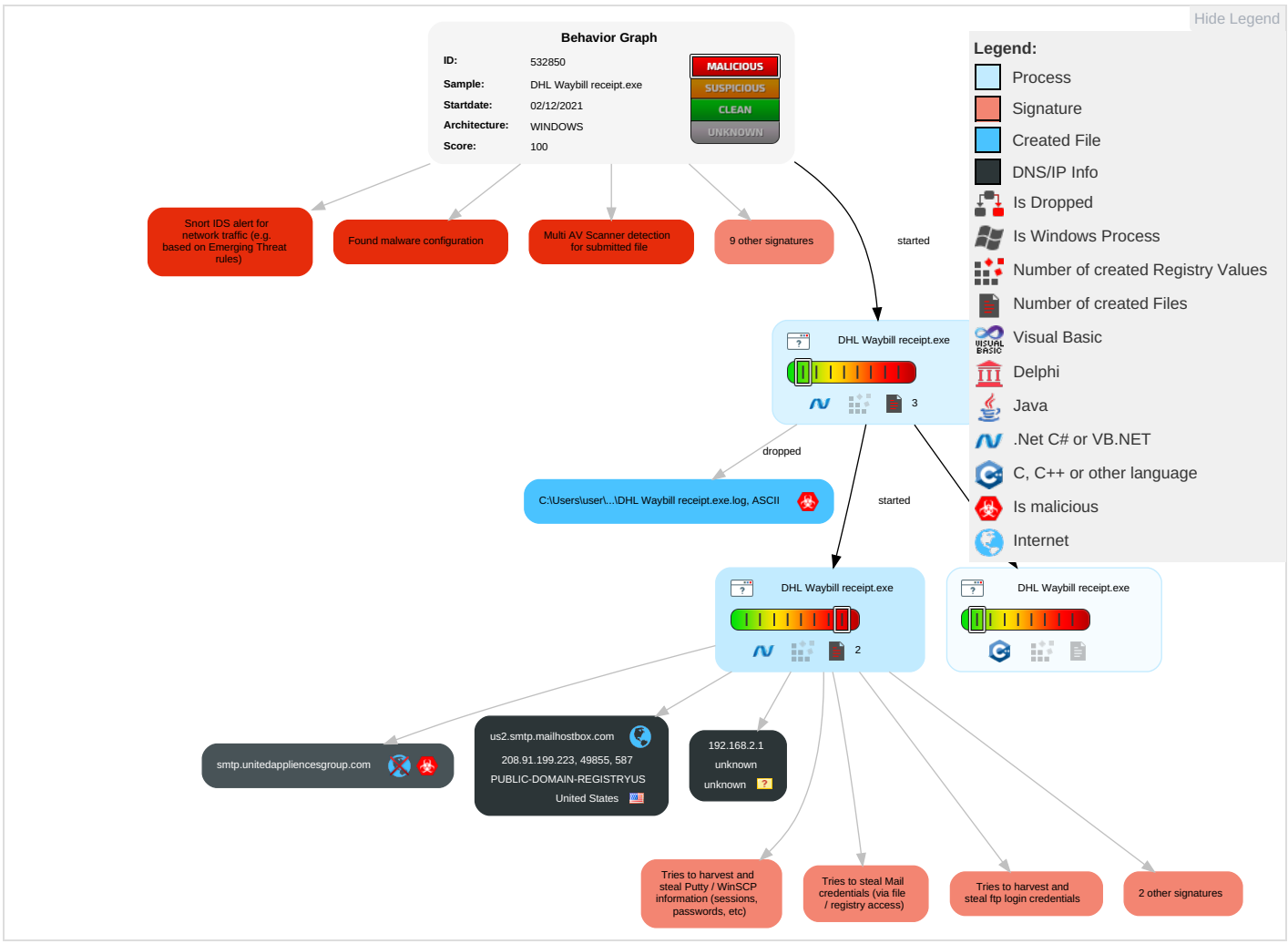
Remote Access Functionality:

- **Yara detected AgentTesla**

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Cor
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypte Channel
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Input Capture 2 1 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Input Capture 2 1 1	Exfiltration Over Bluetooth	Non-Sta Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Credentials in Registry 1	Process Discovery 2	SMB/Windows Admin Shares	Archive Collected Data 1 1	Automated Exfiltration	Non-Applicati Layer Protocol
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Applicati Layer Protocol
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channel
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiban Commur
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commor Used Po

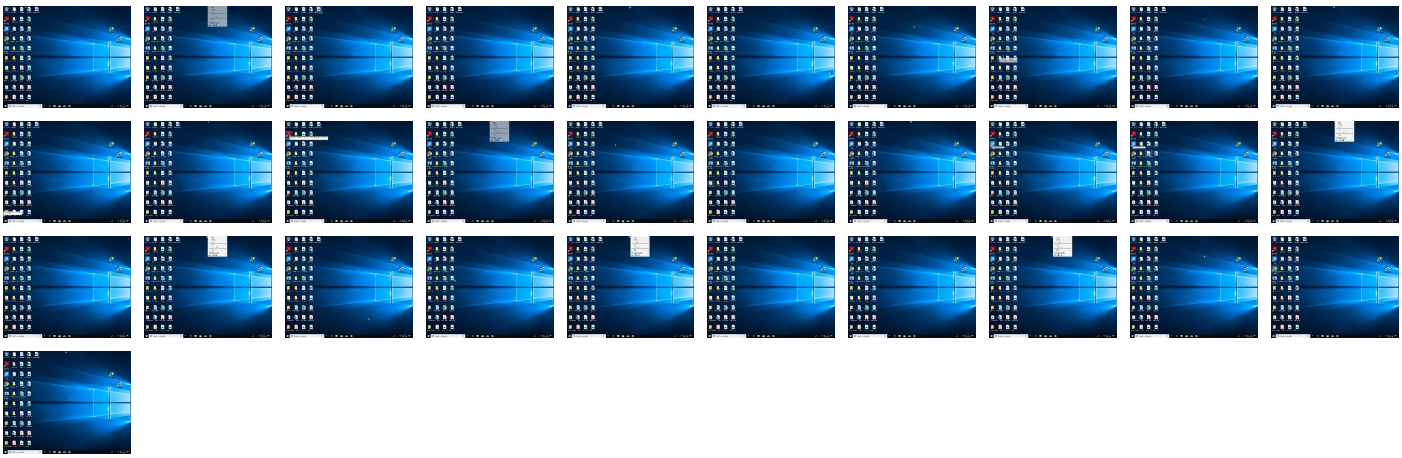
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Copyright Joe Security LLC 2021

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
DHL Waybill receipt.exe	31%	ReversingLabs	ByteCode-MSIL.Trojan.DarkStealerLoader	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.DHL Waybill receipt.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.DHL Waybill receipt.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.DHL Waybill receipt.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.DHL Waybill receipt.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.DHL Waybill receipt.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.DHL Waybill receipt.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

Copyright Joe Security LLC 2021

URLs

Source	Detection	Scanner	Label	Link
http://https://YDMv4fA4ajY4A2Rc.net	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://KjvtHQ.com	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://smtp.unitedappliencesgroup.com	0%	Avira URL Cloud	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	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.223	true	false		high
smtp.unitedappliencesgroup.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.199.223	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532850
Start date:	02.12.2021
Start time:	18:49:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL Waybill receipt.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:	26
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

Copyright Joe Security LLC 2021

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@5/1@2/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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
18:50:36	API Interceptor	692x Sleep call for process: DHL Waybill receipt.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.199.223	DHL SHIPMENT NOTIFICATION 284748395PD.exe	Get hash	malicious	Browse	
	yYa94CeATF8h2NA.exe	Get hash	malicious	Browse	
	BOQ.exe	Get hash	malicious	Browse	
	Documento de env.exe	Get hash	malicious	Browse	
	PO_783992883.exe	Get hash	malicious	Browse	
	OUTWARD SWIFT-103 MSG Payment Transcript.PDF.exe	Get hash	malicious	Browse	
	ROfr29tilpUhTHx.exe	Get hash	malicious	Browse	
	Transaction advice Nov-2021 20211129678pdf.exe	Get hash	malicious	Browse	
	Payment copy $95,914.38MT103_0987658999643PDF.exe	Get hash	malicious	Browse	
	Payment copy $95,914.38MT103_0987658999643PDF.exe	Get hash	malicious	Browse	
	Details To Be Reconfirmed.doc	Get hash	malicious	Browse	
	Payment slip URhcolexFq2SKzCxls.exe	Get hash	malicious	Browse	
	03SPwb995m.exe	Get hash	malicious	Browse	
	Reconfirm The Details.doc	Get hash	malicious	Browse	
	MT_101_SWIFT.doc	Get hash	malicious	Browse	
	DOCUMENTS.exe	Get hash	malicious	Browse	
	TOP QUOTATION RFQ 2021.exe	Get hash	malicious	Browse	
	UY2021 Ta-Ho Maritime Schedule.exe	Get hash	malicious	Browse	
	Purchase Order.exe	Get hash	malicious	Browse	
	StK0hTNVyxxIPrJ.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	DHL SHIPMENT NOTIFICATION 284748395PD.exe	Get hash	malicious	Browse	• 208.91.199.223
	Swift MT103 pdf.exe	Get hash	malicious	Browse	• 208.91.199.225
	Scan096355.exe	Get hash	malicious	Browse	• 208.91.199.225
	yYa94CeATF8h2NA.exe	Get hash	malicious	Browse	• 208.91.199.223
	PG4636 - Confirmed .xls.exe	Get hash	malicious	Browse	• 208.91.198.143
	PG4636 - Confirmed .xls.exe	Get hash	malicious	Browse	• 208.91.199.225
	BOQ.exe	Get hash	malicious	Browse	• 208.91.199.223
	RFQ-Spares and tools.exe	Get hash	malicious	Browse	• 208.91.198.143
	CARTASCONF.xlsx	Get hash	malicious	Browse	• 208.91.199.224

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Documento de env.exe	Get hash	malicious	Browse	• 208.91.199.223
	hkpg4iBhY1.exe	Get hash	malicious	Browse	• 208.91.199.224
	account details and invoice.exe	Get hash	malicious	Browse	• 208.91.198.143
	justificantepago_es_180208779493.xlsx	Get hash	malicious	Browse	• 208.91.199.224
	winlogon.exe	Get hash	malicious	Browse	• 208.91.198.143
	PO_783992883.exe	Get hash	malicious	Browse	• 208.91.199.223
	OUTWARD SWIFT-103 MSG Payment Transcript.PDF.exe	Get hash	malicious	Browse	• 208.91.199.223
	ROfr29tilpUhTHx.exe	Get hash	malicious	Browse	• 208.91.199.223
	Transaction advice Nov-2021 20211129678pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	shipping documents.exe	Get hash	malicious	Browse	• 208.91.198.143
	Payment copy $95,914.38MT103_0987658999643PDF.exe	Get hash	malicious	Browse	• 208.91.199.223

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	Shipping Document BL Copy.exe	Get hash	malicious	Browse	• 103.195.185.115
	DHL SHIPMENT NOTIFICATION 284748395PD.exe	Get hash	malicious	Browse	• 208.91.199.223
	SHIPPING DOCUMENT & PL.exe	Get hash	malicious	Browse	• 103.195.185.115
	Swift MT103 pdf.exe	Get hash	malicious	Browse	• 208.91.199.225
	Scan096355.exe	Get hash	malicious	Browse	• 208.91.199.225
	yYa94CeATF8h2NA.exe	Get hash	malicious	Browse	• 208.91.199.223
	part-1500645108.xlsb	Get hash	malicious	Browse	• 103.76.231.42
	part-1500645108.xlsb	Get hash	malicious	Browse	• 103.76.231.42
	item-40567503.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	item-40567503.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	PG4636 - Confirmed .xls.exe	Get hash	malicious	Browse	• 208.91.198.143
	item-107262298.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	item-107262298.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	item-1202816963.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	item-1202816963.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	DHL Receipt.html	Get hash	malicious	Browse	• 199.79.62.126
	BOQ.exe	Get hash	malicious	Browse	• 208.91.199.223
	RFQ-Spares and tools.exe	Get hash	malicious	Browse	• 208.91.198.143
	box-1688169224.xlsb	Get hash	malicious	Browse	• 199.79.62.54
	box-1689035414.xlsb	Get hash	malicious	Browse	• 199.79.62.54

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL Waybill receipt.exe.log

Process:	C:\Users\user\Desktop\DHL Waybill receipt.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE47mE4Ko88:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz6
MD5:	D918C6A765EDB90D2A227FE23A3FEC98
SHA1:	8BA802AD8D740F114783F0DADC407CBFD2A209B3

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL Waybill receipt.exe.log	
SHA-256:	AB0E9F716E31502A4C6786575C5E64DFD9D24AF99056BBE2640A2FA322CFF4D6
SHA-512:	A937ABD8294BB32A612F8B3A376C94111D688379F0A4DB9FAA2FCEB71C25E18D621EEBCFDA5706B71C8473A4F38D8B3C4005D1589B564F9B1C9C441B6D3378 4
Malicious:	**true**
Reputation:	moderate, 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.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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.850196340535848
TrID:	• 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:	DHL Waybill receipt.exe
File size:	723456
MD5:	fccf07d7a10aff74cedc0e93fbe77f90
SHA1:	8e7d667885cdc3646d46c3a72ee13451c86cbd4d
SHA256:	854fdbaa39b3da5ed2d094c57511d14dc97c392358da47e42fbbd7b2d03101d2
SHA512:	155e4dee572bfef147250bdf28801a8c158a8b99c249ac927f3fb87c4131951eb76f2d718557c56bf71e34303275f2707979f94cc21578972f0b849cf9ee899c
SSDEEP:	12288:kf/kc7PDpCS1FzPleXSiEHNIK52FUFiGTApRHWtRWS14Gfo9THSMRcQ4crgtP:cscPpzPleXSiANIiFT02tweA9bSMur
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...\?.a.....0.....N.... ... .@.. .....`.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4b1c4e
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:	0x61A83F5C [Thu Dec 2 03:37:00 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4

General

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	0xafc54	0xafe00	False	0.918482364961	data	7.85914519961	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb2000	0x618	0x800	False	0.33837890625	data	3.4628856937	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb4000	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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/02/21-18:52:33.092255	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49855	587	192.168.2.5	208.91.199.223

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 18:52:30.986301899 CET	192.168.2.5	8.8.8.8	0xf50f	Standard query (0)	smtp.unite dapplience sgroup.com	A (IP address)	IN (0x0001)
Dec 2, 2021 18:52:31.656506062 CET	192.168.2.5	8.8.8.8	0x1ea3	Standard query (0)	smtp.unite dapplience sgroup.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 18:52:31.309015036 CET	8.8.8.8	192.168.2.5	0xf50f	No error (0)	smtp.unite dapplience sgroup.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 18:52:31.309015036 CET	8.8.8.8	192.168.2.5	0xf50f	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Dec 2, 2021 18:52:31.309015036 CET	8.8.8.8	192.168.2.5	0xf50f	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 18:52:31.309015036 CET	8.8.8.8	192.168.2.5	0xf50f	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Dec 2, 2021 18:52:31.309015036 CET	8.8.8.8	192.168.2.5	0xf50f	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Dec 2, 2021 18:52:31.676522017 CET	8.8.8.8	192.168.2.5	0x1ea3	No error (0)	smtp.unitedappliancesgroup.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 18:52:31.676522017 CET	8.8.8.8	192.168.2.5	0x1ea3	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Dec 2, 2021 18:52:31.676522017 CET	8.8.8.8	192.168.2.5	0x1ea3	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Dec 2, 2021 18:52:31.676522017 CET	8.8.8.8	192.168.2.5	0x1ea3	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Dec 2, 2021 18:52:31.676522017 CET	8.8.8.8	192.168.2.5	0x1ea3	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)

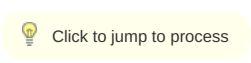
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 2, 2021 18:52:32.173089981 CET	587	49855	208.91.199.223	192.168.2.5	220 us2.outbound.mailhostbox.com ESMTP Postfix
Dec 2, 2021 18:52:32.177587986 CET	49855	587	192.168.2.5	208.91.199.223	EHLO 562258
Dec 2, 2021 18:52:32.326097965 CET	587	49855	208.91.199.223	192.168.2.5	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Dec 2, 2021 18:52:32.327333927 CET	49855	587	192.168.2.5	208.91.199.223	AUTH login am9obi5yYW1vc0B1bml0ZWRhcHBsaWVuY2VzZ3JvdXAuY29t
Dec 2, 2021 18:52:32.476557970 CET	587	49855	208.91.199.223	192.168.2.5	334 UGFzc3dvcmQ6
Dec 2, 2021 18:52:32.628686905 CET	587	49855	208.91.199.223	192.168.2.5	235 2.7.0 Authentication successful
Dec 2, 2021 18:52:32.629769087 CET	49855	587	192.168.2.5	208.91.199.223	MAIL FROM:<john.ramos@unitedappliancesgroup.com>
Dec 2, 2021 18:52:32.779227972 CET	587	49855	208.91.199.223	192.168.2.5	250 2.1.0 Ok
Dec 2, 2021 18:52:32.779747963 CET	49855	587	192.168.2.5	208.91.199.223	RCPT TO:<john.ramos@unitedappliancesgroup.com>
Dec 2, 2021 18:52:32.941848993 CET	587	49855	208.91.199.223	192.168.2.5	250 2.1.5 Ok
Dec 2, 2021 18:52:32.942272902 CET	49855	587	192.168.2.5	208.91.199.223	DATA
Dec 2, 2021 18:52:33.090878963 CET	587	49855	208.91.199.223	192.168.2.5	354 End data with <CR><LF>.<CR><LF>
Dec 2, 2021 18:52:33.093197107 CET	49855	587	192.168.2.5	208.91.199.223	.
Dec 2, 2021 18:52:33.343266964 CET	587	49855	208.91.199.223	192.168.2.5	250 2.0.0 Ok: queued as D31A6DA4A0

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: DHL Waybill receipt.exe PID: 6312 Parent PID: 5828

General

Start time:	18:50:34
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\DHL Waybill receipt.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\DHL Waybill receipt.exe"
Imagebase:	0x690000
File size:	723456 bytes
MD5 hash:	FCCF07D7A10AFF74CEDC0E93FBE77F90
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.254418452.0000000002A91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.257252389.0000000003A99000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.257252389.0000000003A99000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: DHL Waybill receipt.exe PID: 3276 Parent PID: 6312

General

Start time:	18:50:37
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\DHL Waybill receipt.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\DHL Waybill receipt.exe
Imagebase:	0x1d0000
File size:	723456 bytes
MD5 hash:	FCCF07D7A10AFF74CEDC0E93FBE77F90
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: DHL Waybill receipt.exe PID: 3688 Parent PID: 6312

General

Start time:	18:50:39
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\DHL Waybill receipt.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHL Waybill receipt.exe
Imagebase:	0xb00000

Copyright Joe Security LLC 2021

File size:	723456 bytes
MD5 hash:	FCCF07D7A10AFF74CEDC0E93FBE77F90
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: 00000003.00000000.249607108.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.249607108.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.251632964.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.251632964.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.250868237.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.250868237.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.509034503.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.509034503.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.515087639.0000000002F81000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.515087639.0000000002F81000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.250192706.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.250192706.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021