ID: 532143
Sample Name: DHL Express shipment notification.exe
Cookbook: default.jbs
Time: 19:03:59
Date: 01/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

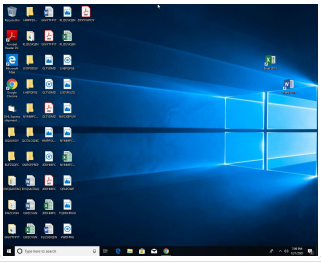
Windows Analysis Report DHL Express shipment notific…

Overview

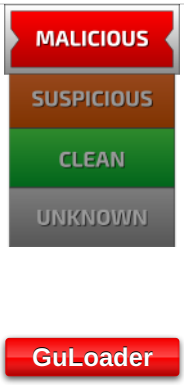
General Information

Sample Name:	DHL Express shipment notification.exe
Analysis ID:	532143
MD5:	26e034a56f86ed4.
SHA1:	a74551ce377aad..
SHA256:	60ab75a94e04aa..
Tags:	DHL exe GuLoader signed
Infos:	

Most interesting Screenshot:



Detection

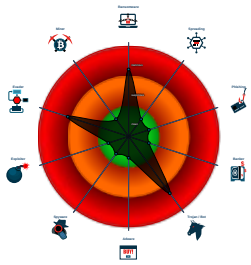


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Potential malicious icon found
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Sample file is different than original …
- PE file contains strange resources
- Contains functionality to read the PEB
- Uses code obfuscation techniques (…
- Detected potential crypto function
- PE / OLE file has an invalid certificate
- Contains functionality for execution …
- Abnormal high CPU Usage

Classification



Process Tree

- **System is w10x64**
- DHL Express shipment notification.exe (PID: 6368 cmdline: "C:\Users\user\Desktop\DHL Express shipment notification.exe" MD5: 26E034A56F86ED41CB3E869095EC73B7)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=downlo8"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.778696939.00000000021D0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	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

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Potential malicious icon found

Data Obfuscation:

Yara detected GuLoader

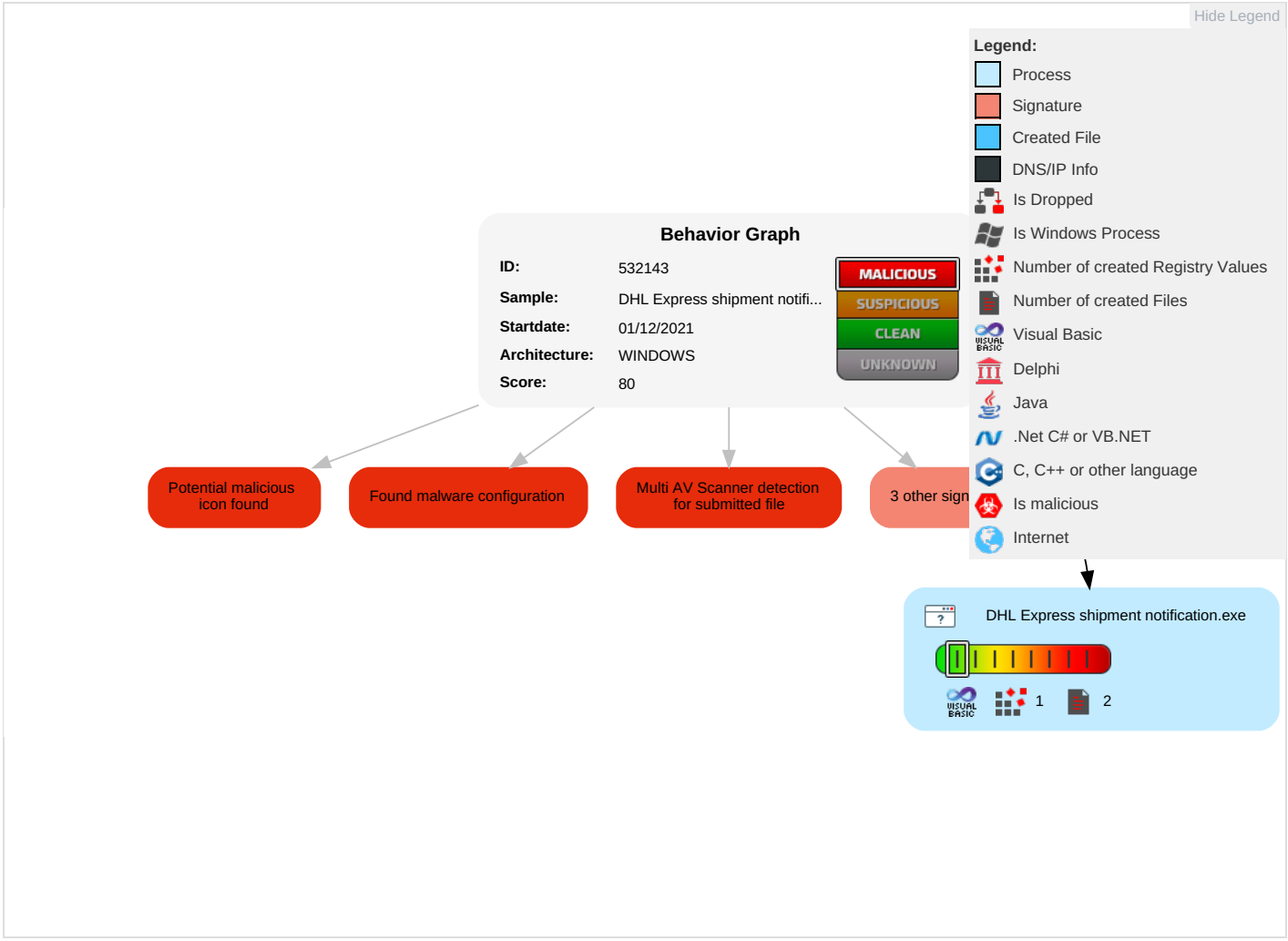
Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	System Information Discovery 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups

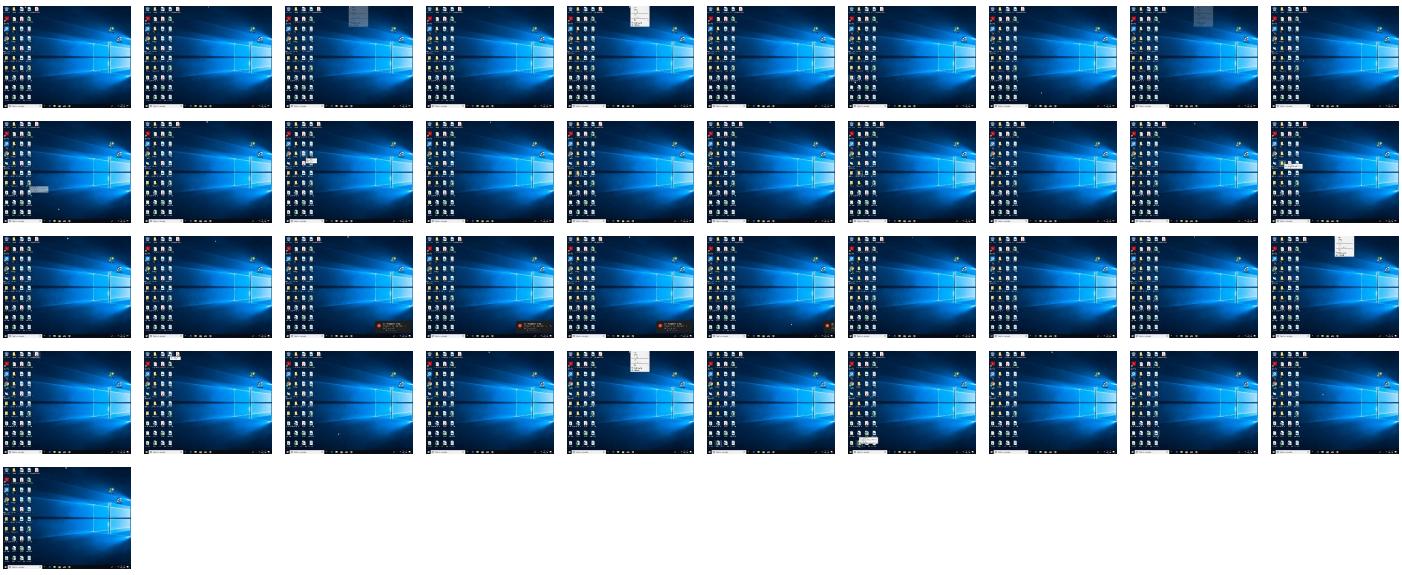
Behavior Graph



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
DHL Express shipment notification.exe	25%	Virustotal		Browse
DHL Express shipment notification.exe	11%	ReversingLabs	Win32.Trojan.Shelsy	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.DHL Express shipment notification.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1140082		Download File
0.0.DHL Express shipment notification.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1140082		Download File

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:	34.0.0 Boulder Opal
Analysis ID:	532143
Start date:	01.12.2021
Start time:	19:03:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL Express shipment notification.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:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 41.7% (good quality ratio 19.3%) • Quality average: 27.9% • Quality standard deviation: 32%
HCA Information:	Failed
Cookbook Comments:	• 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

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):	5.288330717800927
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:	DHL Express shipment notification.exe
File size:	152728
MD5:	26e034a56f86ed41cb3e869095ec73b7
SHA1:	a74551ce377aadbaae0b31b54b2536daaa832754
SHA256:	60ab75a94e04aa5dfab1a68da060a817e9f5ccb79f8a93d0c3dbfe47cb526b7d
SHA512:	283eb6c75e024fac46085ea526b96844466b6b27861dbe047d37d3bde1d59e207241426b812030e8cb22d45441df4bdfd5c6d841b39eb21c9ac01bd7b0b346d
SSDEEP:	1536:bSyEql7Tg8Xxo5HCSJndCcIVdPsw4Jaev0Cq5pg:WyEql7Tg6hhTdkHwphg
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.....D.....=.....Rich.....PE..L...|a.T.....0..... ....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401888
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x54B7617C [Thu Jan 15 06:43:08 2015 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:	b209c8634733456633136bfedc71877a

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=TVRESTES@ineluctable.Bir, CN=Studsendes, OU=Polyteknisk, O=Shelterdkkeren, L=DANNEBROGSKORS, S=Variabelerklringerne, C=BT
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 12/1/2021 4:31:58 AM 12/1/2022 4:31:58 AM
Subject Chain	• E=TVRESTES@ineluctable.Bir, CN=Studsendes, OU=Polyteknisk, O=Shelterdkkeren, L=DANNEBROGSKORS, S=Variabelerklringerne, C=BT
Version:	3
Thumbprint MD5:	6E23C2E0F1EAA5736459B248CD4F244F
Thumbprint SHA-1:	3EF79B4748A2F5E9C61B979020E0070FCAB22AF2
Thumbprint SHA-256:	1252758943828E279B0955645D9BFE6EBC24BAB29368FB5EFDC213D5B615F3A0
Serial:	00

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x20fa4	0x21000	False	0.377485795455	data	5.3781600227	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x22000	0x122c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x24000	0x958	0x1000	False	0.173828125	data	2.03797872425	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: DHL Express shipment notification.exe PID: 6368 Parent PID: 1972

General

Start time:	19:05:00
Start date:	01/12/2021
Path:	C:\Users\user\Desktop\DHL Express shipment notification.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\DHL Express shipment notification.exe"
Imagebase:	0x400000
File size:	152728 bytes
MD5 hash:	26E034A56F86ED41CB3E869095EC73B7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.778696939.00000000021D0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis