ID: 490026
Sample Name: DHL.com
Cookbook: default.jbs
Time: 21:26:50
Date: 24/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Windows Analysis Report DHL.com

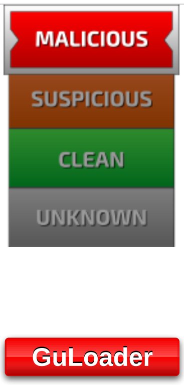
Overview

General Information

Sample Name:	DHL.com (renamed file extension from com to exe)
Analysis ID:	490026
MD5:	8fab6753620475b.
SHA1:	d1d7badd885b82..
SHA256:	83e4ae7f04653b0.
Tags:	com DHL exe GuLoader
Infos:	

Most interesting Screenshot:

Detection

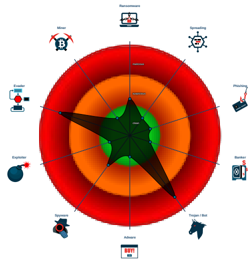


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- GuLoader behavior detected
- Yara detected GuLoader
- Hides threads from debuggers
- Writes to foreign memory regions
- Tries to detect Any.run
- C2 URLs / IPs found in malware con…
- Tries to detect sandboxes and other…
- Found potential dummy code loops (…
- Machine Learning detection for samp…
- Creates a DirectInput object (often fo…

Classification



Process Tree

- **System is w10x64**
- DHL.exe (PID: 5732 cmdline: 'C:\Users\user\Desktop\DHL.exe' MD5: 8FAB6753620475B356FB55CB3339AA8F)
  - ieinstal.exe (PID: 7140 cmdline: 'C:\Users\user\Desktop\DHL.exe' MD5: DAD17AB737E680C47C8A44CBB95EE67E)
  - ieinstal.exe (PID: 6800 cmdline: 'C:\Users\user\Desktop\DHL.exe' MD5: DAD17AB737E680C47C8A44CBB95EE67E)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://107.189.4.115/ncHJfummF147.bin"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.712369007.00000000023A0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000001A.00000002.791045987.00000000030D0000.00000040.00000001.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

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Tries to detect Any.run

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

Anti Debugging:

Hides threads from debuggers

Found potential dummy code loops (likely to delay analysis)

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

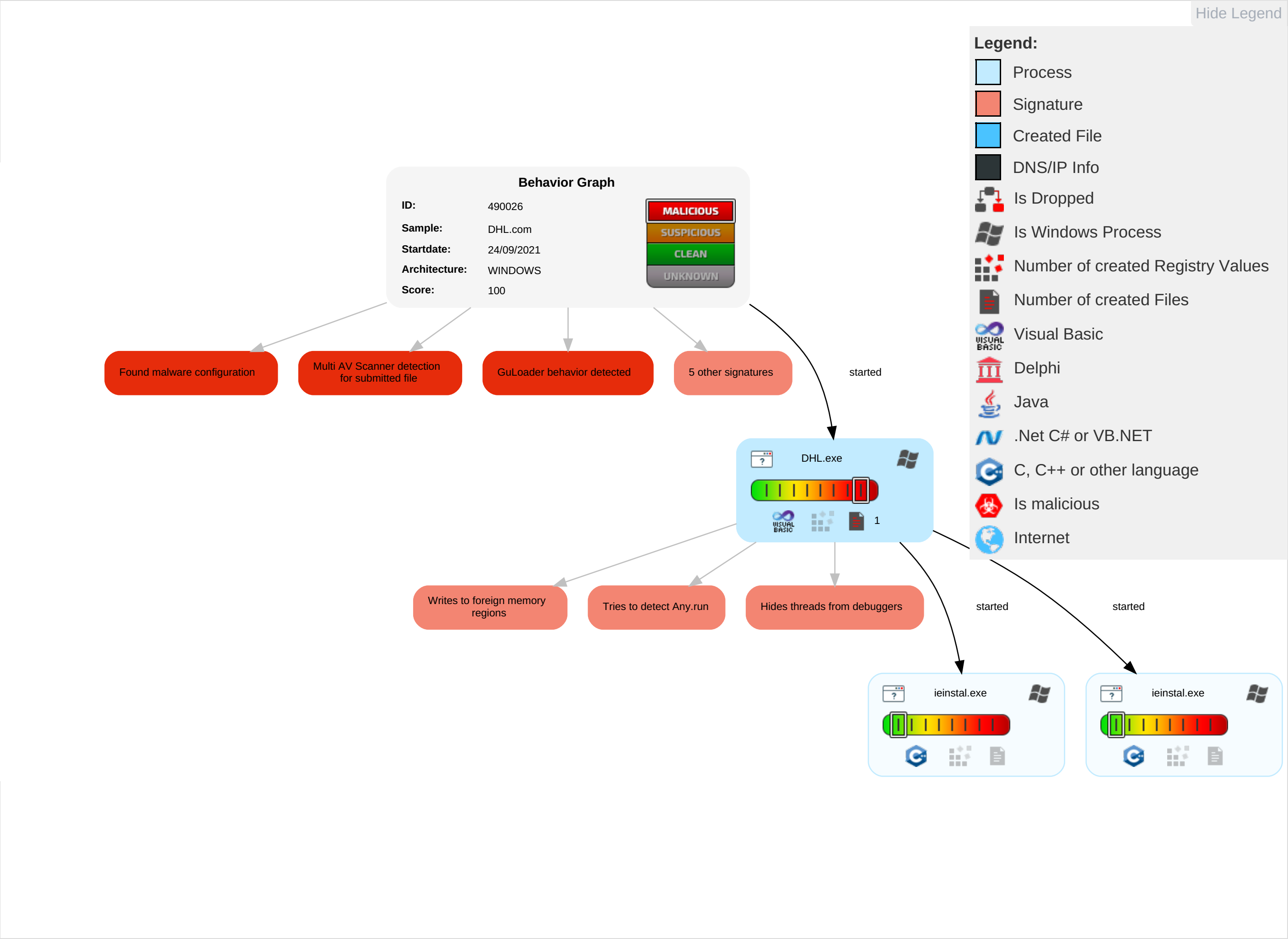
Stealing of Sensitive Information:

GuLoader behavior detected

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1 2	Virtualization/Sandbox Evasion 3 1	Input Capture 1	Security Software Discovery 4 1 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop or Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Software Packing 1	LSASS Memory	Virtualization/Sandbox Evasion 3 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Information Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap

Behavior Graph



Behavior Graph

ID: 490026

Sample: DHL.com

Startdate: 24/09/2021

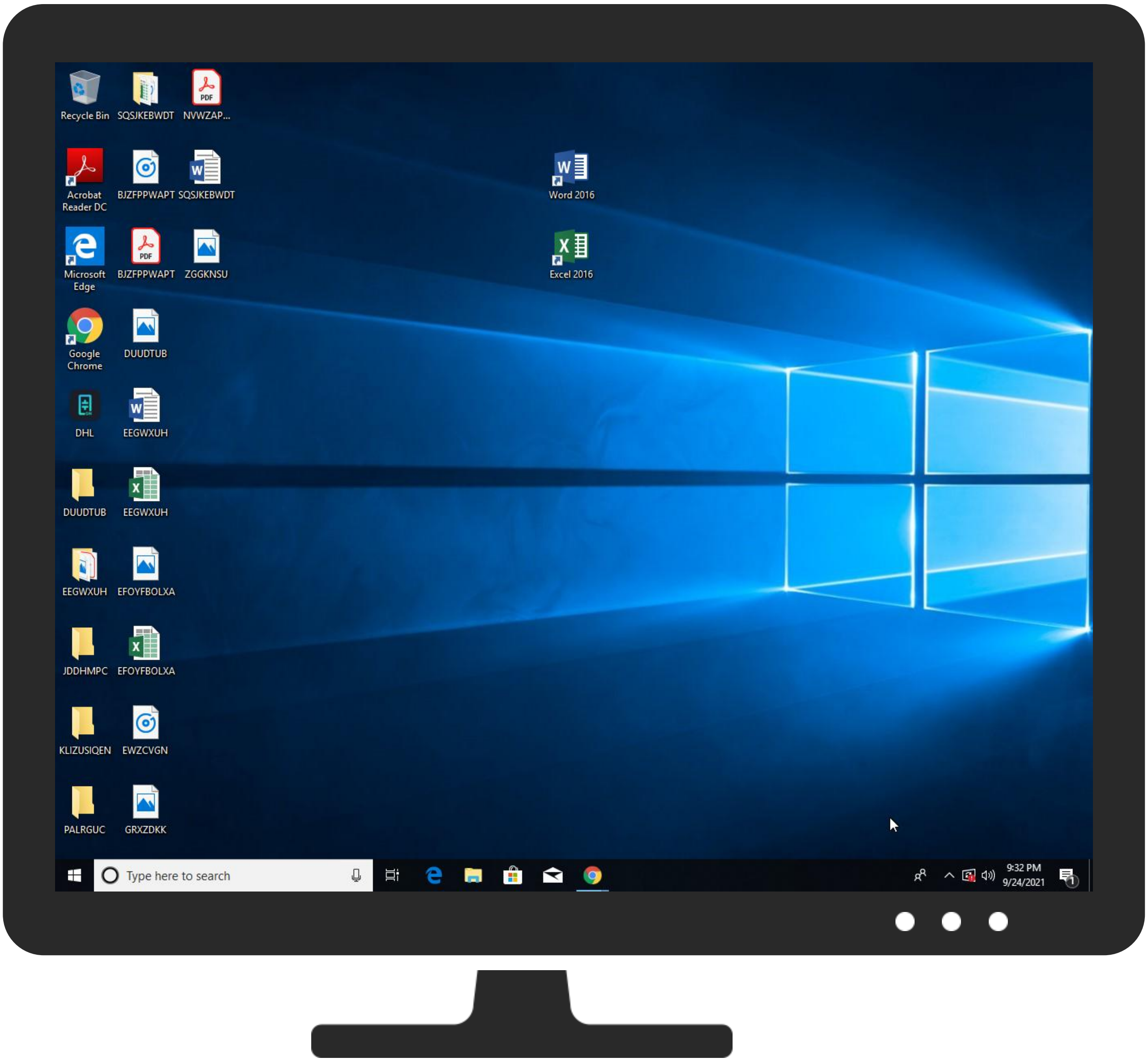
Architecture: WINDOWS

Score: 100

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.exe	29%	Virustotal		Browse
DHL.exe	11%	ReversingLabs	Win32.Trojan.Mucc	
DHL.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.DHL.exe.400000.0.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File
1.0.DHL.exe.400000.0.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://107.189.4.115/ncHJfummF147.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://107.189.4.115/ncHJfummF147.bin	true	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	490026
Start date:	24.09.2021
Start time:	21:26:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL.com (renamed file extension from com to 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:	27
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.evad.winEXE@5/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 20.6% (good quality ratio 6.2%) • Quality average: 13.2% • Quality standard deviation: 24.5%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • 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):	6.36618367187466
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.exe
File size:	147456
MD5:	8fab6753620475b356fb55cb3339aa8f
SHA1:	d1d7badd885b824b212be62c7caa7ff33d419d05
SHA256:	83e4ae7f04653b03a31836d92b1d70b1d9264a2fe7a457 cf39f4be1bf134e2b
SHA512:	f2b2c1fc9739bd3421455de4c71556d44efa29715756c0c f4d804465c6ebb577d891e9cbf6853059929373355ce5b7 82b8e5e3c47848b129b9a5751e1d0dcd6d
SSDEEP:	3072:gGFZ3bD6eWdxHrDZ9PM/zw0q8Lwtp1eW:gmqJlr 19Pp0q8ctTe
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.............i...i... i...d...i.Rich..i.................PE..L......R.................................. ....@........................

File Icon

Icon Hash:	ccf0e8f8e8e8f864

Static PE Info

General

Entrypoint:	0x401088
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:	0x52FFCCE0 [Sat Feb 15 20:24:00 2014 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:	48a41634a91a3d58d7574e90175db383

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x19f30	0x1a000	False	0.496300330529	data	6.35084151068	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1b000	0x1e50	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1d000	0x8654	0x9000	False	0.488498263889	data	5.80900365728	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
English	United States	

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

Behavior

💡 Click to jump to process

System Behavior

Analysis Process: DHL.exe PID: 5732 Parent PID: 5432

General

Start time:	21:27:57
Start date:	24/09/2021
Path:	C:\Users\user\Desktop\DHL.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHL.exe'
Imagebase:	0x400000
File size:	147456 bytes
MD5 hash:	8FAB6753620475B356FB55CB3339AA8F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.712369007.00000000023A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: ieinstal.exe PID: 7140 Parent PID: 5732

General

Start time:	21:30:19
Start date:	24/09/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\DHL.exe'
Imagebase:	0x300000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: 6800 Parent PID: 5732

General

Start time:	21:30:20
Start date:	24/09/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHL.exe'
Imagebase:	0x300000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000001A.00000002.791045987.00000000030D0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 33.0.0 White Diamond