ID: 433258
Sample Name: DHL Original Receipt_pdf.exe
Cookbook: default.jbs
Time: 14:49:19
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

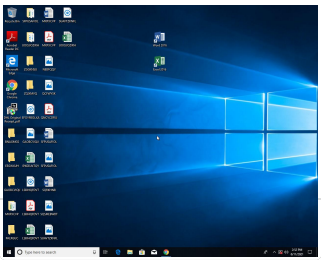
Analysis Report DHL Original Receipt_pdf.exe

Overview

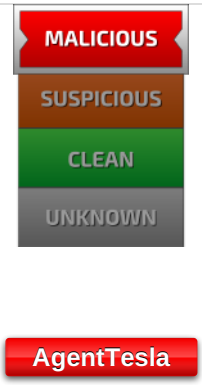
General Information

Sample Name:	DHL Original Receipt_pdf.exe
Analysis ID:	433258
MD5:	c376cef609a1826..
SHA1:	72523a0124ddd3..
SHA256:	c42b7b1630553b..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

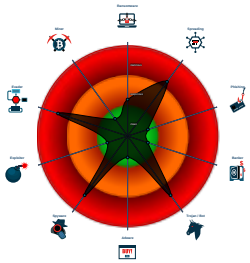


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Sigma detected: MSBuild connects …
- Yara detected AgentTesla
- Yara detected AgentTesla
- .NET source code contains very larg…
- Found evasive API chain (trying to d…
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…

Classification



Process Tree

- **System is w10x64**
- DHL Original Receipt_pdf.exe (PID: 648 cmdline: 'C:\Users\user\Desktop\DHL Original Receipt_pdf.exe' MD5: C376CEF609A18260213571D06233BA20)
  - MSBuild.exe (PID: 1404 cmdline: 'C:\Users\user\Desktop\DHL Original Receipt_pdf.exe' MD5: 88BBB7610152B48C2B3879473B17857E)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "coco@gmicaprelam.incoco2424@gmicaprelam.in"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.233952436.00000000025E0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.233952436.00000000025E0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.491039762.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.491039762.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.495614720.000000000341000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 4 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.DHL Original Receipt_pdf.exe.25e0000.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.DHL Original Receipt_pdf.exe.25e0000.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.DHL Original Receipt_pdf.exe.25e0000.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.DHL Original Receipt_pdf.exe.25e0000.3.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.MSBuild.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Overview

Networking:

Sigma detected: MSBuild connects to smtp port

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:

System Summary:

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

Malware Analysis System Evasion:

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

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

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

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

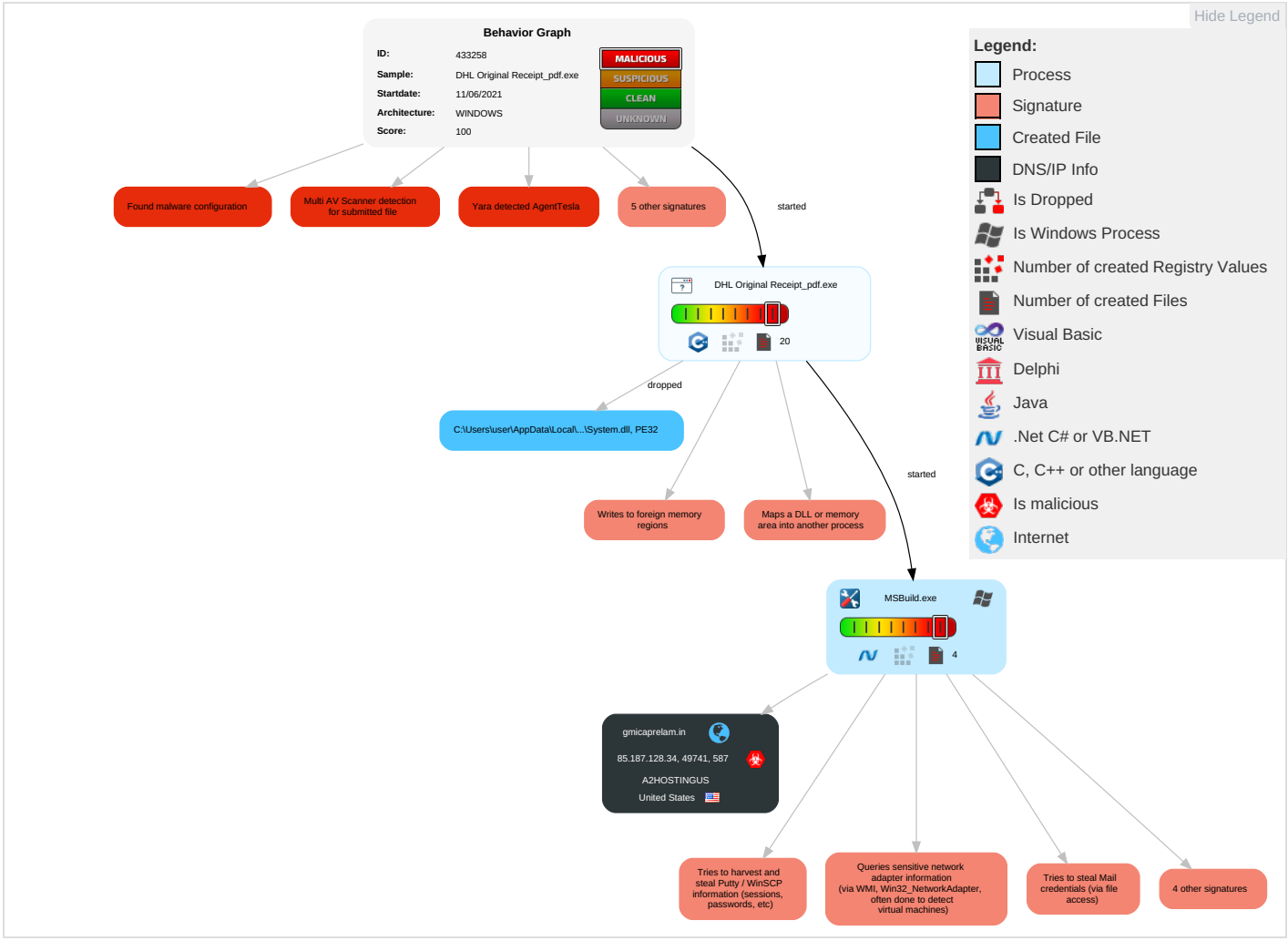
Yara detected AgentTesla

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
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Access Token Manipulation 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	File and Directory Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1
Default Accounts	Native API 1 1	Boot or Logon Initialization Scripts	Process Injection 2 1 2	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	System Information Discovery 1 1 6	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Standard Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	Security Software Discovery 1 2 1	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 1 4 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 2 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc

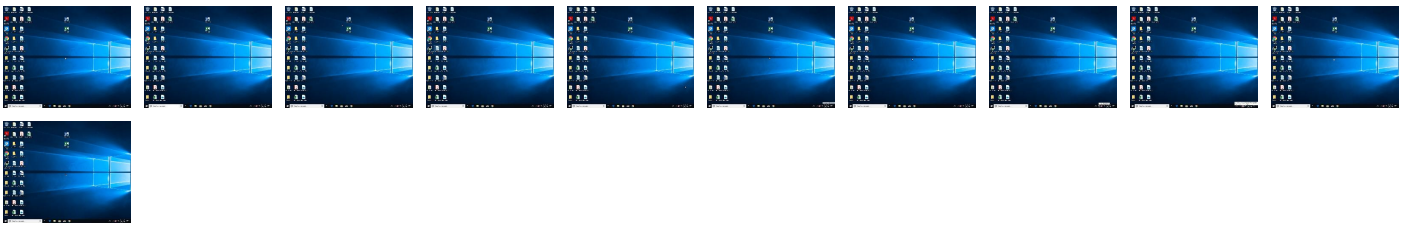
Behavior Graph



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 Original Receipt_pdf.exe	30%	Virustotal		Browse
DHL Original Receipt_pdf.exe	41%	ReversingLabs	Win32.Trojan.AgentTesla	
DHL Original Receipt_pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsvDCD7.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsvDCD7.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.0.DHL Original Receipt_pdf.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
0.2.DHL Original Receipt_pdf.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File

Domains

Source	Detection	Scanner	Label	Link
gmicaprelam.in	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://8isgha7nUwa6.net	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://LUhbZz.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%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%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%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	
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.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	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
gmicaprelam.in	85.187.128.34	true	true	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
85.187.128.34	gmicaprelam.in	United States	🇺🇸	55293	A2HOSTINGUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433258
Start date:	11.06.2021
Start time:	14:49:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL Original Receipt_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:	23
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.spre.troj.spyw.evad.winEXE@3/4@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 64.7% (good quality ratio 63.6%) • Quality average: 88.3% • Quality standard deviation: 22%
HCA Information:	• Successful, ratio: 86% • 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
14:50:22	API Interceptor	998x Sleep call for process: MSBuild.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
85.187.128.34	TNT Consignment Details_pdf.exe	Get hash	malicious	Browse	
	DHL Original Invoice_pdf.exe	Get hash	malicious	Browse	
	Sanbook Equip Machines Trading Inquiry.exe	Get hash	malicious	Browse	
	TNT Consignment Detail_pdf.exe	Get hash	malicious	Browse	
	Consignment Details_pdf.exe	Get hash	malicious	Browse	
	DHL delivery documents.exe	Get hash	malicious	Browse	
	Consignment Details_pdf.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
gmicaprelam.in	TNT Consignment Details_pdf.exe	Get hash	malicious	Browse	• 85.187.128.34
	DHL Original Invoice_pdf.exe	Get hash	malicious	Browse	• 85.187.128.34
	Sanbook Equip Machines Trading Inquiry.exe	Get hash	malicious	Browse	• 85.187.128.34
	TNT Consignment Detail_pdf.exe	Get hash	malicious	Browse	• 85.187.128.34
	Consignment Details_pdf.exe	Get hash	malicious	Browse	• 85.187.128.34
	DHL delivery documents.exe	Get hash	malicious	Browse	• 85.187.128.34
	Consignment Details_pdf.exe	Get hash	malicious	Browse	• 85.187.128.34

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
A2HOSTINGUS	DNPr7t0GMY.exe	Get hash	malicious	Browse	• 199.195.117.147
	ITAPQJikGw.exe	Get hash	malicious	Browse	• 199.195.117.147
	audit-1349817595.xlsb	Get hash	malicious	Browse	• 85.187.132.224

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TNT Consigment Details_pdf.exe	Get hash	malicious	Browse	• 85.187.128.34
	DHL Original Invoice_pdf.exe	Get hash	malicious	Browse	• 85.187.128.34
	Sanbook Equip Machines Trading Inquiry.exe	Get hash	malicious	Browse	• 85.187.128.34
	TNT Consignment Detail_pdf.exe	Get hash	malicious	Browse	• 85.187.128.34
	Consignment Details_pdf.exe	Get hash	malicious	Browse	• 85.187.128.34
	SCAN_20161017_151638921_002.xlsx	Get hash	malicious	Browse	• 68.66.224.18
	1zJU42cQVX.exe	Get hash	malicious	Browse	• 68.66.224.18
	DHL delivery documents.exe	Get hash	malicious	Browse	• 85.187.128.34
	GoRnrfZlAG.exe	Get hash	malicious	Browse	• 199.195.11 7.147
	SCAN_20161017_151638921_002.xlsx	Get hash	malicious	Browse	• 68.66.224.18
	XRFQX#P000001488.xlsx	Get hash	malicious	Browse	• 68.66.224.18
	templex.exe	Get hash	malicious	Browse	• 68.66.224.18
	e6f8edeb_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 68.66.224.18
	Request Quote212021#P000001488.pdf.exe	Get hash	malicious	Browse	• 68.66.224.18
	b02c0831_by_Libranalysis.exe	Get hash	malicious	Browse	• 199.195.11 7.147
	Swift.pdf.exe	Get hash	malicious	Browse	• 68.66.224.18
	vZMIGFMR.exe	Get hash	malicious	Browse	• 85.187.149.197

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsvDCD7.tmp\System.dll	HALKBANK - Dekont_pdf.exe	Get hash	malicious	Browse	
	Quote-TSL-1037174_4810.exe	Get hash	malicious	Browse	
	SX365783909782021.exe	Get hash	malicious	Browse	
	moq fob order.exe	Get hash	malicious	Browse	
	0900000000000090000.exe	Get hash	malicious	Browse	
	444890321.exe	Get hash	malicious	Browse	
	Packing-List_00930039.exe	Get hash	malicious	Browse	
	2435.exe	Get hash	malicious	Browse	
	INVOICE.exe	Get hash	malicious	Browse	
	Shipment Invoice & Consignment Notification.exe	Get hash	malicious	Browse	
	KY4cmAI0jU.exe	Get hash	malicious	Browse	
	5t2CmTUhKc.exe	Get hash	malicious	Browse	
	8qdfmqz1PN.exe	Get hash	malicious	Browse	
	New Order PO2193570O1.doc	Get hash	malicious	Browse	
	L2.xlsx	Get hash	malicious	Browse	
	Agency Appointment VSL Tbn-Port-Appointment Letter-2100133.xlsx	Get hash	malicious	Browse	
	New Order PO2193570O1.pdf.exe	Get hash	malicious	Browse	
	2320900000000.exe	Get hash	malicious	Browse	
	CshpH9OSkc.exe	Get hash	malicious	Browse	
	5SXTKXCnqS.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\nsvDCD6.tmp	
Process:	C:\Users\user\Desktop\DHL Original Receipt_pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	322013
Entropy (8bit):	7.48504577375667
Encrypted:	false
SSDEEP:	6144:8S85eJ8UxDlFbNvsxgCCAo0BuWKJE5285RLk5fO20OIesyN6Y2it:785fQFbXCfwDKTImdOIINQS
MD5:	CFDD4CCF7F714F82444F81B771F81F5A
SHA1:	CBA5F09C9F6466E2E159721D95A98C45521ACA30
SHA-256:	599B93F8209DEC77381A7EBD384369BF46974C38604BFD2689E5677E6C984C0A

C:\Users\user\AppData\Local\Temp\nsvDCD6.tmp	
SHA-512:	F21F28DB62BFBF8E0212531FF13C96C3C9D872D5EDC5F0AA5EFD94E7D6E3C496F3534F5F36E3908EB2A11F9B037C24DDF8F550997FC21CF5735222595FA589C
Malicious:	false
Reputation:	low
Preview:	.r.....,.....V.....q.....r.....2..... .....J.....j.....q.....f..... ....

C:\Users\user\AppData\Local\Temp\nsvDCD7.tmp\System.dll	
Process:	C:\Users\user\Desktop\DHL Original Receipt_pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: HALKBANK - Dekont_pdf.exe, Detection: malicious, Browse • Filename: Quote-TSL-1037174_4810.exe, Detection: malicious, Browse • Filename: SX365783909782021.exe, Detection: malicious, Browse • Filename: moq fob order.exe, Detection: malicious, Browse • Filename: 0900000000000090000.exe, Detection: malicious, Browse • Filename: 444890321.exe, Detection: malicious, Browse • Filename: Packing-List_00930039.exe, Detection: malicious, Browse • Filename: 2435.exe, Detection: malicious, Browse • Filename: INVOICE.exe, Detection: malicious, Browse • Filename: Shipment Invoice & Consignment Notification.exe, Detection: malicious, Browse • Filename: KY4cmAI0jU.exe, Detection: malicious, Browse • Filename: 5t2CmTUhKc.exe, Detection: malicious, Browse • Filename: 8qdfmqz1PN.exe, Detection: malicious, Browse • Filename: New Order PO2193570O1.doc, Detection: malicious, Browse • Filename: L2.xlsx, Detection: malicious, Browse • Filename: Agency Appointment VSL Tbn-Port-Appointment Letter- 2100133.xlsx, Detection: malicious, Browse • Filename: New Order PO2193570O1.pdf.exe, Detection: malicious, Browse • Filename: 2320900000000.exe, Detection: malicious, Browse • Filename: CshpH9OSkc.exe, Detection: malicious, Browse • Filename: 5SXTKXCnqS.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L.....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Local\Temp\rayiid	
Process:	C:\Users\user\Desktop\DHL Original Receipt_pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	60209
Entropy (8bit):	4.971325407303197
Encrypted:	false
SSDEEP:	1536:5BgIe8ZXI1WsPrkvnDgpZdAk39T9ry6/zFkjpaD7lNTfa3D:5BgIe8ZtWkLgb+kNN/ya9N23D
MD5:	9E2895F6220DC4CA141D4C52B949C915
SHA1:	6FB2FB7F7FEDD604545A1F91B50AFFEFF6286278
SHA-256:	6E1FEDDECB4F11F73B42F8004BD8D6B3E22C67FDC58A80B3D87A24F11F876D79
SHA-512:	58BD0A7BBA74306B9F5C11136E26C9BA6E7C9E9D1DF60163FE8D7DD919ECD5C2CA735A7B667043C1F31CFC6E67780875BEADA5A95919854E7ECB8F918C5F1A FA
Malicious:	false
Reputation:	low
Preview:	U..!.....H.....I...4.J.....K.....L.....M.....N.....O.....P...X.Q.....R.....S.....T.....U.....V.....W...D.X.....Y.....Z.....[.....\.....]...F.^...@._...7.`.....a.....b.....c...;.d...!.e...,.f...`.g.....h.....i.....j... ..k.....l.....m...;.n...!.o...,.p...`.q.....r.....s.....t.....u.....v.....w...;.x...!.y...,.z...`.{.....|.....}.....~.....;.....!.....,.....`.....;.....!.....,.....`..... .....;.....!.....,.....`.....?.....;.....!.....,.....`.....;.....!.....,.....`.....;.....!.....,.....`.....;.....!.....,.....`... .....;.....!.....,.....`.....;.....!.....,.....`

C:\Users\user\AppData\Local\Temp\zjhfet5v8giw	
Process:	C:\Users\user\Desktop\DHL Original Receipt_pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	220672
Entropy (8bit):	**7.999008107054153**
Encrypted:	**true**
SSDEEP:	6144:i85eJ8UxDlFbNvsxgCCAo0BuWKJE5285RLk5fO20N:i85fQFbXCfwDKTImdN
MD5:	F17CDB23A72208A0CC23C168F8D13A62
SHA1:	DB703E287110E72E71CF91E856742C3AB2B8F832
SHA-256:	2608F735EEBB0A24D76CF467C3AFB1AAFC50D44B366DFD9757CB78285338EF5A
SHA-512:	0C25ECF6DCA780A1E83D2B6B80392709EF9208818258A6D3E371ACD52E4997D32045F2CCA2103ADEC9DA9323706F4E48B920164EB8622D493720DF97D865EF9
Malicious:	false
Reputation:	low
Preview:	.....o..`.-yt....ag.w.^'e.(.i..^.>..iR....8..c.B^..<..O.^.j....y.e.qz..."7.....`.W..<....B.Z.s.t.6K...,&..k..{d.....P...t...b.<...ex~p..C.1..}l..X.3.`....yAT'2..&.|..$..y..sJ~.....+....6+".w...[d.o.l..X.o.?..../.....z..B[{.$.....5..T.q\..R.....e.|8...?.Q.....?..o9.4W...p+.JN.8.^c..!..d.....3.6&..A!e.3..*3. ...M.Z_..X.7T..I9..Hn)..S,s....m..G.V..\..6..K...8..C.5...~%..[..xx ..T$a?..Um .'.D'\|...[...^to>.&.R.SX.N.....>.../....=.+...W..u?j].he\|.S..k.'.;...udBqV..k..7._\|.}....G....7.RT.....%..o...S..... .....i....>..U...\|.\./....N...+px.D....y..C.....{..-.5BK=..k'...f.. U.,....zj.K.b..''v...h.6BwHez.S.;..T,Bvt..U.....!%....(.E+.....,x..).....L.....t.....b..Rj.....lJ..6_K..".%d.oF.Z.....lk..B..1'+..}..{.E..D).:*.,].5$>.....$.5.....g.V.y!-Ya.*.7.....}... t...kL.._.K.\|..y..''?".....M8XN(.*h...K.o..K]X....;u.L.6...d...E..2}(.4..0-u.;.$'+WN+;...['..C...w.n...d....z.|.-nY...U....K.{..<....b...T....>$._.b...[...f..-..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.94012628065006
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • 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 Original Receipt_pdf.exe
File size:	282745
MD5:	c376cef609a18260213571d06233ba20
SHA1:	72523a0124ddd34ce6fa21901b4648311ae04b72
SHA256:	c42b7b1630553baa3aeb65e40b04244910822c175e9b6c b3f7f365264171196b
SHA512:	0691af013f3012b999c69ef1331b011798a8b6802d6a91f ba370a78a1d9dbb57dab2c1aaab1e3d89611fd0e645776 40eaed9334d153b601418b9f5ed8ba845a2
SSDEEP:	6144:Ds9aphdmtsKdoFHOxDW+s6IVlzINDQCzvDj:yap hUtToFHSTs6IVl4QqvDj
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..:u..iu..iu..i...iw..iu..i...i...id..i!..i...i...it..iRichu..i.....PE..L.....K.....\.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40323c
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

General

DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x4B1AE3C6 [Sat Dec 5 22:50:46 2009 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:	099c0646ea7282d232219f8807883be0

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5a5a	0x5c00	False	0.660453464674	data	6.41769823686	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.4453125	data	5.18162709925	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55859375	data	4.70902740305	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x9e0	0xa00	False	0.45625	data	4.51012867721	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 14:51:44.978660107 CEST	192.168.2.7	8.8.8.8	0x95d8	Standard query (0)	gmicaprelam.in	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 14:51:45.042718887 CEST	8.8.8.8	192.168.2.7	0x95d8	No error (0)	gmicaprelam.in		85.187.128.34	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jun 11, 2021 14:51:45.879563093 CEST	587	49741	85.187.128.34	192.168.2.7	220-sg1-ts2.a2hosting.com ESMTP Exim 4.94.2 #2 Fri, 11 Jun 2021 20:51:45 +0800 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jun 11, 2021 14:51:45.879584074 CEST	587	49741	85.187.128.34	192.168.2.7	421 sg1-ts2.a2hosting.com lost input connection

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: DHL Original Receipt_pdf.exe PID: 648 Parent PID: 5752

General

Start time:	14:50:12
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\DHL Original Receipt_pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHL Original Receipt_pdf.exe'
Imagebase:	0x400000
File size:	282745 bytes
MD5 hash:	C376CEF609A18260213571D06233BA20
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.233952436.00000000025E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.233952436.00000000025E0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: MSBuild.exe PID: 1404 Parent PID: 648

General

Start time:	14:50:13
Start date:	11/06/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHL Original Receipt_pdf.exe'
Imagebase:	0xce0000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
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: 00000001.00000002.491039762.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.491039762.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.495614720.0000000003471000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.495614720.0000000003471000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis