ID: 383976
Sample Name:
DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe
Cookbook: default.jbs
Time: 13:30:42
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

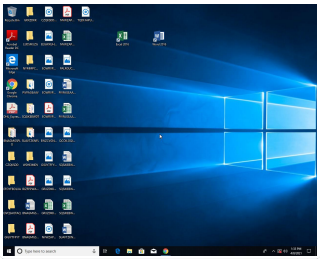
Analysis Report DHL_Express_Shipment_Invoice_Confi…

Overview

General Information

Sample Name:	DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe
Analysis ID:	383976
MD5:	edae8c184a250c..
SHA1:	6042a0f078faad9..
SHA256:	0a572e4a9f5d166.
Tags:	AgentTesla DHL exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

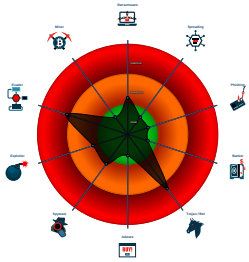
AgentTesla

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- .NET source code contains very larg…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Contains capabilities to detect virtua…
- Contains long sleeps (>= 3 min)
- Creates a process in suspended mo…
- Detected potential crypto function
- Drops PE files
- Enables debug privileges
- Found a high number of Window / Us…

Classification



Startup

- **System is w10x64**
- DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe (PID: 5716 cmdline: 'C:\Users\user\Desktop\DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe' MD5: EDAE8C184A250CCCBA45C023E805E12D)
  - cmd.exe (PID: 3412 cmdline: 'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'Files' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\Files.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 4060 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - reg.exe (PID: 5432 cmdline: REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'Files' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\Files.exe' MD5: CEE2A7E57DF2A159A065A34913A055C2)
  - Files.exe (PID: 6280 cmdline: 'C:\Users\user\AppData\Roaming\Files.exe' MD5: EDAE8C184A250CCCBA45C023E805E12D)
- Files.exe (PID: 5980 cmdline: 'C:\Users\user\AppData\Roaming\Files.exe' MD5: EDAE8C184A250CCCBA45C023E805E12D)
- Files.exe (PID: 6332 cmdline: 'C:\Users\user\AppData\Roaming\Files.exe' MD5: EDAE8C184A250CCCBA45C023E805E12D)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "sammorris@askoblue.comP)RTDOg8mail.privateemail.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.299807783.0000000003E6 6000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.300534811.000000000402 B000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.299471132.0000000003DB 7000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: DHL_Express_Shipment_Invoice _Confirmation_CBJ190517000131_74700456XXXX.exe PID: 5716	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

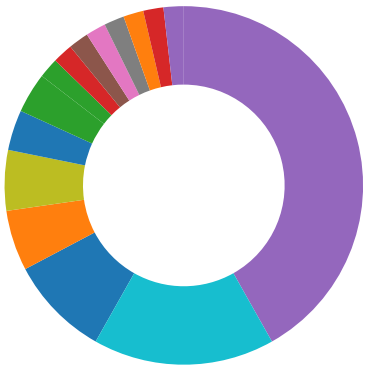
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.DHL_Express_Shipment_Invoice_Confirmation_CBJ1 90517000131_74700456XXXX.exe.3f1bb92.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.DHL_Express_Shipment_Invoice_Confirmation_CBJ1 90517000131_74700456XXXX.exe.3ec0f92.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.DHL_Express_Shipment_Invoice_Confirmation_CBJ1 90517000131_74700456XXXX.exe.3f76782.5.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.DHL_Express_Shipment_Invoice_Confirmation_CBJ1 90517000131_74700456XXXX.exe.3f76782.5.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.DHL_Express_Shipment_Invoice_Confirmation_CBJ1 90517000131_74700456XXXX.exe.3db76a0.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 5 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

System Summary:

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Stealing of Sensitive Information:

Yara detected AgentTesla

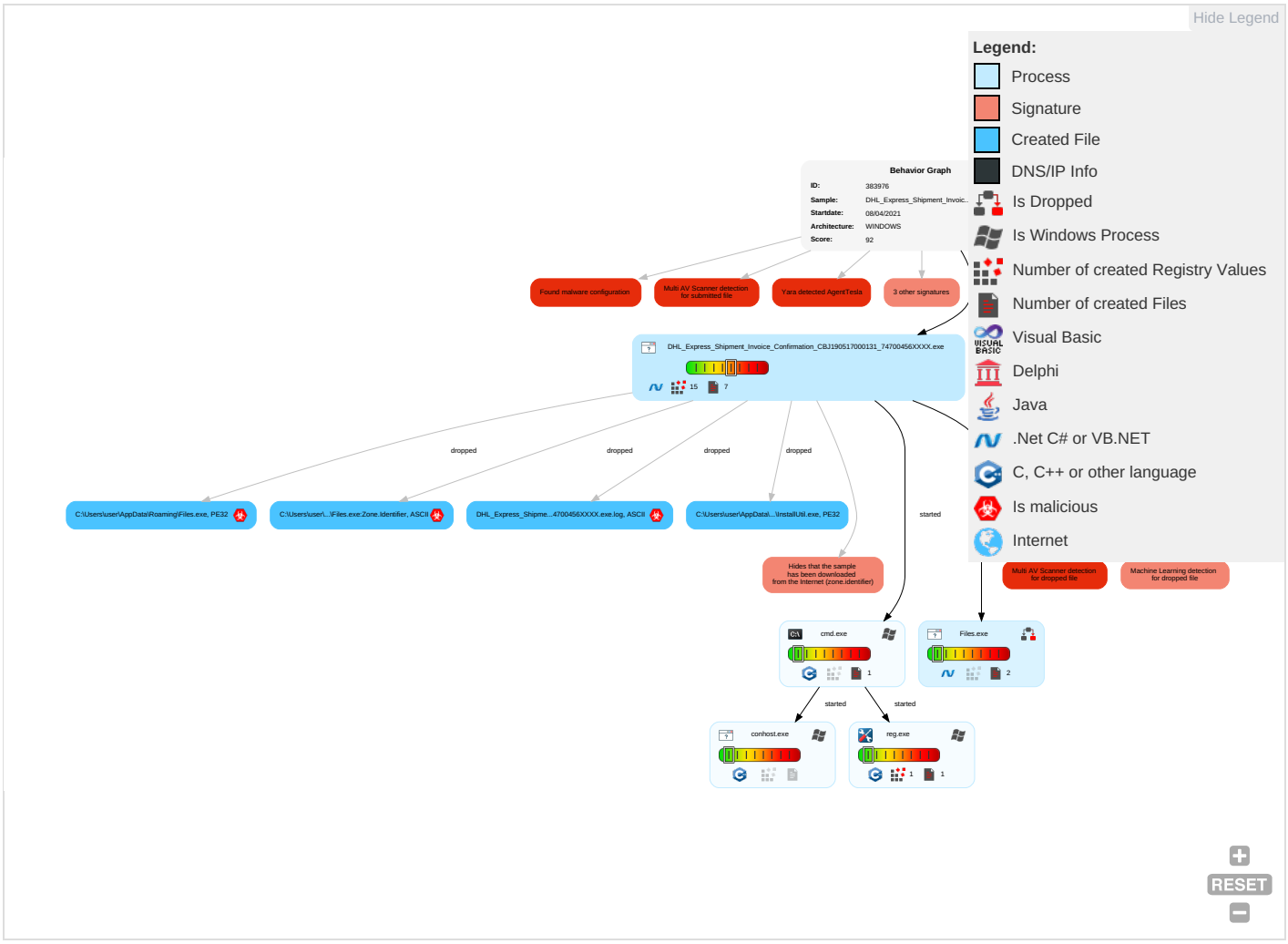
Remote Access Functionality:

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	Network Effects
Valid Accounts	Windows Management Instrumentation	Registry Run Keys / Startup Folder 1	Process Injection 1 1	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Modify Registry 1	LSASS Memory	Security Software Discovery 1 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Virtualization/Sandbox Evasion 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

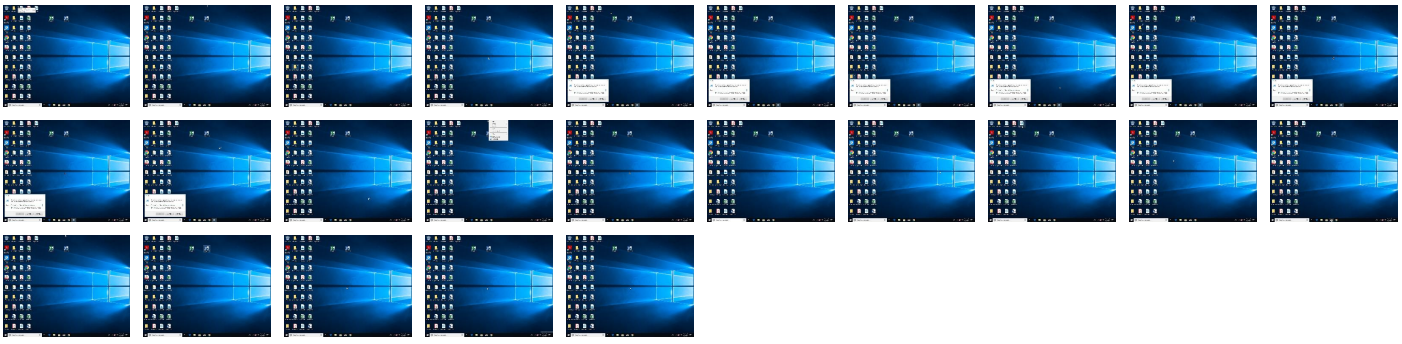
Behavior Graph



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_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe	29%	Virustotal		Browse
DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe	38%	ReversingLabs	Win32.Trojan.Wacatac	
DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Files.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Files.exe	38%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ns.adobe.c/g%%	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	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://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://ocsp.m	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

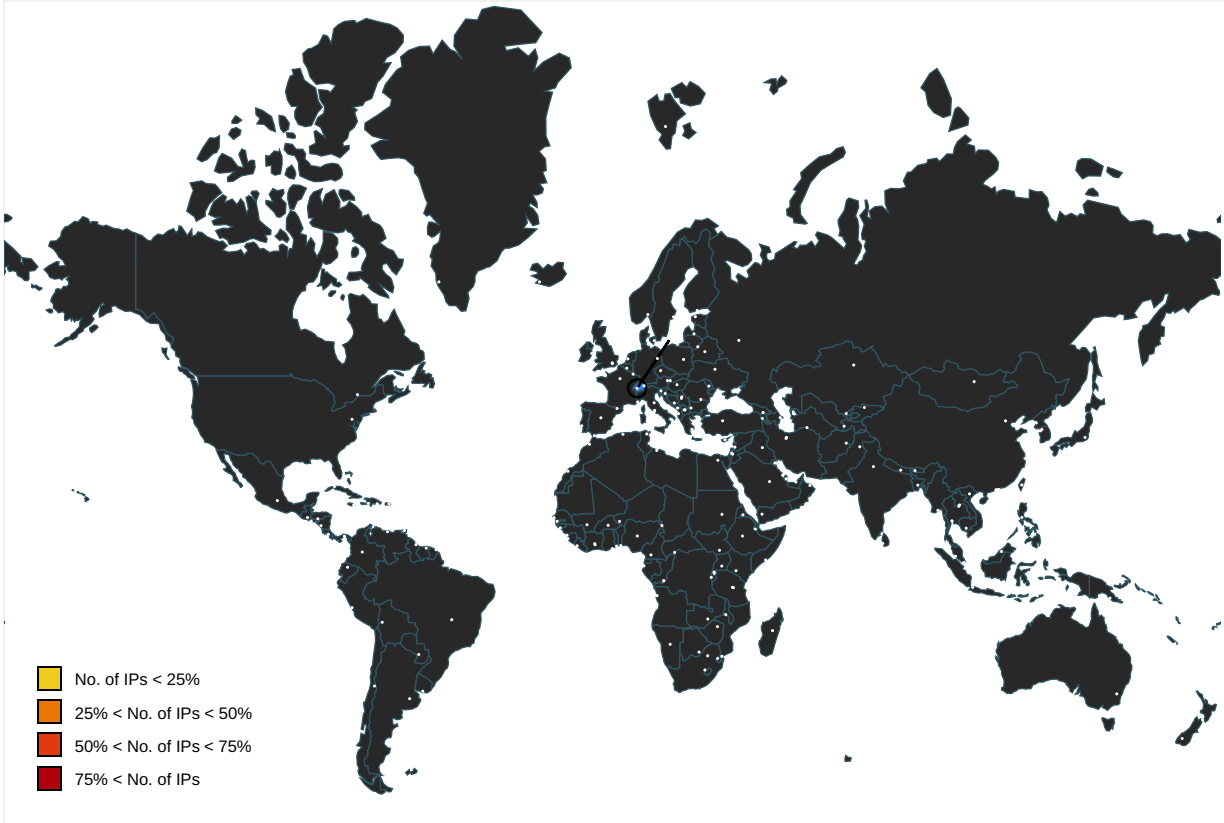
No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ns.adobe.c/g%%	DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe, 00000000.00000002.305089826.00000000070D2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki.goog/gsr2/GTS1O1.crt0	Files.exe, 0000000D.00000002.306747199.00000000025C6000.00000004.00000001.sdmp, Files.exe, 00000015.00000002.325347261.00000000029DF000.00000004.00000001.sdmp, Files.exe, 00000016.00000002.328565365.00000000013D1000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.c/g	DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe, 00000000.00000003.232439693.00000000070D3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/gsr2/gsr2.crl0?	Files.exe, 0000000D.00000002.306747199.00000000025C6000.00000004.00000001.sdmp, Files.exe, 00000015.00000002.325347261.00000000029DF000.00000004.00000001.sdmp, Files.exe, 00000016.00000002.328565365.00000000013D1000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/repository/0	Files.exe, 0000000D.00000002.306747199.00000000025C6000.00000004.00000001.sdmp, Files.exe, 00000015.00000002.325347261.00000000029DF000.00000004.00000001.sdmp, Files.exe, 00000016.00000002.328565365.00000000013D1000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe, 00000000.00000002.297204343.0000000002D41000.00000004.00000001.sdmp, Files.exe, 0000000D.00000002.306692734.0000000002591000.00000004.00000001.sdmp, Files.exe, 00000015.00000002.329046892.0000000002DF7000.00000004.00000001.sdmp, Files.exe, 00000016.00000002.329364718.00000000030E1000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe, 00000000.00000002.299807783.0000000003E66000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/WebPage	DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe, 00000000.00000002.297284689.0000000002D6E000.00000004.00000001.sdmp, Files.exe, 0000000D.00000002.306747199.00000000025C6000.00000004.00000001.sdmp, Files.exe, 00000015.00000002.325378597.00000000029FC000.00000004.00000001.sdmp, Files.exe, 00000015.00000002.325347261.00000000029DF000.00000004.00000001.sdmp, Files.exe, 00000016.00000002.329505639.0000000003135000.00000004.00000001.sdmp	false		high
http://crl.pki.goog/GTS1O1core.crl0	Files.exe, 0000000D.00000002.306747199.00000000025C6000.00000004.00000001.sdmp, Files.exe, 00000015.00000002.325347261.00000000029DF000.00000004.00000001.sdmp, Files.exe, 00000016.00000002.328565365.00000000013D1000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.m	Files.exe, 00000015.00000002.322781369.0000000000A9C000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383976
Start date:	08.04.2021
Start time:	13:30:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.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:	35
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:	mal92.troj.evad.winEXE@10/5@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.7% (good quality ratio 0.2%) • Quality average: 20.1% • Quality standard deviation: 29.5%
HCA Information:	• Successful, ratio: 81% • 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 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, wermgr.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 13.88.21.125, 172.217.168.4, 204.79.197.200, 13.107.21.200, 168.61.161.212, 104.83.127.80, 104.83.87.75, 13.107.42.23, 13.107.5.88, 40.126.31.138, 20.190.159.135, 40.126.31.5, 40.126.31.142, 20.190.159.137, 40.126.31.3, 20.190.159.131, 20.190.159.133, 93.184.220.29, 95.100.54.203, 2.22.152.11, 20.82.210.154, 205.185.216.10, 205.185.216.42, 23.54.113.53, 20.82.209.183, 23.10.249.26, 23.10.249.43 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, cdn.onenote.net.edgekey.net, www.tm.a.prd.aadg.trafficmanager.net, skypedataprdcoleus15.cloudapp.net, ocsp.digicert.com, wildcard.weather.microsoft.com.edgekey.net, login.live.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, www.google.com, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, www.bing.com, afdo-tas-offload.trafficmanager.net, fs.microsoft.com, dual-a-0001.a-msedge.net, skypedataprdcolcus17.cloudapp.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, e1553.dspg.akamaiedge.net, www.tm.lg.prod.aadmsa.trafficmanager.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, client-office365-tas.msedge.net, ocos-office365-s2s.msedge.net, config.edge.skype.com.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, e-0009.e-msedge.net, config-edge-skype.l-0014.l-msedge.net, e15275.g.akamaiedge.net, l-0014.config.skype.com, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, storeedgefd.xbetservices.akadns.net, arc.msn.com, e12564.dspb.akamaiedge.net, arc.trafficmanager.net, img-prod-cms-rt-microsoft-com.akamaized.net, cdn.onenote.net, prod.fs.microsoft.com.akadns.net, config.edge.skype.com, storeedgefd.dsx.mp.microsoft.com, tile-service.weather.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, login.msa.msidentity.com, ocos-office365-s2s-msedge-net.e-0009.e-msedge.net, a-0001.a-afdentry.net.trafficmanager.net, dub1.current.a.prd.aadg.trafficmanager.net, l-0014.l-msedge.net, e16646.dscg.akamaiedge.net, skypedataprdcolwus15.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:31:53	API Interceptor	46x Sleep call for process: DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_7470 0456XXXX.exe modified
13:31:57	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Files C:\Users\user\AppData\Roaming\Files.exe
13:32:06	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Files C:\Users\user\AppData\Roaming\Files.exe
13:32:18	API Interceptor	3x Sleep call for process: Files.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe	Get hash	malicious	Browse	
	DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe	Get hash	malicious	Browse	
	DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe	Get hash	malicious	Browse	
	DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe	Get hash	malicious	Browse	
	Sample Qoutation List.exe	Get hash	malicious	Browse	
	DHL_Express_Shipment_Confirmation_BKKR005545473_88700456XXXX.exe	Get hash	malicious	Browse	
	APRILQUOTATION#QQO2103060_SAMPLES_KHANGHY_CO_CORPORATION.exe	Get hash	malicious	Browse	
	Thalesnano.exe	Get hash	malicious	Browse	
	DHL_SHIPMENT_ADDRESS_CONFIRMATION_00000001.exe	Get hash	malicious	Browse	
	RFQ#040820.exe	Get hash	malicious	Browse	
	payment swift copy.exe	Get hash	malicious	Browse	
	I201002X430 CIF #20210604.exe	Get hash	malicious	Browse	
	PO#29710634.exe	Get hash	malicious	Browse	
	PO_66202009475352576 62_Arabico.PDF.exe	Get hash	malicious	Browse	
	payment notification.exe	Get hash	malicious	Browse	
	Payment Notification.exe	Get hash	malicious	Browse	
	s.exe	Get hash	malicious	Browse	
	MV.exe	Get hash	malicious	Browse	
	e.exe	Get hash	malicious	Browse	
	SL_PO8192.PDF.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe.log	
Process:	C:\Users\user\Desktop\DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1402
Entropy (8bit):	5.338819835253785
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4bE4Ko84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7csX3:MIHK5HKXE1qHbHKoviYHKhQnoPtHoxHH
MD5:	EB9F730FB5388BB883772033EA3CCE59
SHA1:	7DFF24FBD26D0ED7065882AE0A9A52E459D7F2A9
SHA-256:	B7192E58E5E91CF2CA113CA1C9575AADEAD3C417076AB83D8EF0720D5E473887
SHA-512:	1FB4FF9E7E85C4F4B2395B948A4B69180E602259FFC582A067B96420C60BA4B49D091F3D525333E07930AA21A8254AF1C9F90B29CCD31AA97C368CB1CB7EF322
Malicious:	**true**
Reputation:	low
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..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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.Configu

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Files.exe.log	
Process:	C:\Users\user\AppData\Roaming\Files.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1402
Entropy (8bit):	5.338819835253785
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4bE4Ko84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7csX3:MIHK5HKXE1qHbHKoviYHKhQnoPtHoxHH
MD5:	EB9F730FB5388BB883772033EA3CCE59
SHA1:	7DFF24FBD26D0ED7065882AE0A9A52E459D7F2A9
SHA-256:	B7192E58E5E91CF2CA113CA1C9575AADEAD3C417076AB83D8EF0720D5E473887
SHA-512:	1FB4FF9E7E85C4F4B2395B948A4B69180E602259FFC582A067B96420C60BA4B49D091F3D525333E07930AA21A8254AF1C9F90B29CCD31AA97C368CB1CB7EF322
Malicious:	false
Reputation:	low
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..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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.Configu

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Process:	C:\Users\user\Desktop\DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	41064
Entropy (8bit):	6.164873449128079
Encrypted:	false
SSDEEP:	384:FtpFVLK0MsihB9VKS7xdgE7KJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+sPZTd:ZBMs2SqdD86lq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Joe Sandbox View:	• Filename: DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe, Detection: malicious, Browse • Filename: DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe, Detection: malicious, Browse • Filename: DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe, Detection: malicious, Browse • Filename: DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe, Detection: malicious, Browse • Filename: Sample Qoutation List.exe, Detection: malicious, Browse • Filename: DHL_Express_Shipment_Confirmation_BKKR005545473_88700456XXXX.exe, Detection: malicious, Browse • Filename: APRILQUOTATION#QQO2103060_SAMPLES_KHANG HY_CO_CORPORATION.exe, Detection: malicious, Browse • Filename: Thalesnano.exe, Detection: malicious, Browse • Filename: DHL_SHIPMENT_ADDRESS_CONFIRMATION_00000001.exe, Detection: malicious, Browse • Filename: RFQ#040820.exe, Detection: malicious, Browse • Filename: payment swift copy.exe, Detection: malicious, Browse • Filename: I201002X430 CIF #20210604.exe, Detection: malicious, Browse • Filename: PO#29710634.exe, Detection: malicious, Browse • Filename: PO_662020094753525766 2_Arabico.PDF.exe, Detection: malicious, Browse • Filename: payment notification.exe, Detection: malicious, Browse • Filename: Payment Notification.exe, Detection: malicious, Browse • Filename: s.exe, Detection: malicious, Browse • Filename: MV.exe, Detection: malicious, Browse • Filename: e.exe, Detection: malicious, Browse • Filename: SL_PO8192.PDF.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..T.....r... .....@.. ....`.....4r..O.....b..h>.....p..... ..... ..H.....text....R... ...T..... ..`.rsrc.....V.....@..@.rel oc.....`.....@..B.....hr.....H.....".|J.....lm.....o.....2~.....o...*.r...p(....*VrK..p(....s.....*..0.....(....(....o....o....(....o.... ....T(....o....(....o....o ...o!....4(....o....(....o....o ...o".....(....rm..ps#...o....($.....(%....o&....ry..p.....%.r...p.%.(.....(....('....((.....o)...('.....*.*.....".(*...*..{Q...-...}Q.....(+...(....(.....(+...*"..(- ...*..(....*..(.....r...p.(/...o0...s....}T...*....0.. .....~S...-.s

C:\Users\user\AppData\Roaming\Files.exe	
Process:	C:\Users\user\Desktop\DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	888320
Entropy (8bit):	6.555631827817538
Encrypted:	false
SSDEEP:	12288:Xd+vpIV1Fn6OAVo1TXiJM8R0aJEu0AxTd9lB3pa77FMHK25PPlXU:UC65o1OMCPabAd7pk7F+K25ZU
MD5:	EDAE8C184A250CCCBA45C023E805E12D
SHA1:	6042A0F078FAAD9525F052A561120D1E2551160F
SHA-256:	0A572E4A9F5D166E563F1C63AA7AA029C2C206D23767BD6AB033A95D7D7027CB
SHA-512:	A2880BEF10470D56E87452FD1C6FEB27C4D1DDE1FCAE5F00901254EA99D1A743190AA3E802B1A492F107A54445FE5FC0C98C4B1C2A3123CCF2DCFEAE1FF6E 68
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 38%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...5..S..... .....@.. ....`.....x...S..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....b...k.....*....M..B.....X..e)..c.....[.....Z....E..w.....q...<.....9...f..,$.....)+..j.....;....t..rC..<o..\[..V...B...8... 4.....[.....Q.....#.....D.....hp...:.....W...@...R.....,..8_..o...1...;..*...R...I...q...=x..}...._..K...B...J.....l.....XV...]...#.....e...K....W...>..<.....@.....v8 ..p.....U...t..%....._....=...?.....!.....

C:\Users\user\AppData\Roaming\Files.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.555631827817538
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_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe
File size:	888320
MD5:	edae8c184a250cccba45c023e805e12d
SHA1:	6042a0f078faad9525f052a561120d1e2551160f
SHA256:	0a572e4a9f5d166e563f1c63aa7aa029c2c206d23767bd6ab033a95d7d7027cb
SHA512:	a2880bef10470d56e87452fd1c6feb27c4d1dde1fcae5f00901254ea99d1a743190aa3e802b1a492f107a54445fe5fc0c98c4b1c2a3123ccf2dcfeae1ff6ed68
SSDEEP:	12288:Xd+vpIV1Fn6OAVo1TXiJM8R0aJEu0AxTd9lB3pa77FMHK25PPlXU:UC65o1OMCPabAd7pk7F+K25ZU
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...5..S..... .....@.. .....`.....

File Icon

Icon Hash:	eaee8e96b2a8e0b2

Static PE Info

General

Entrypoint:	0x4ccece
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, HIGH_ENTROPY_VA
Time Stamp:	0x531A1D35 [Fri Mar 7 19:25:41 2014 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

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xcce78	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xce000	0xd8ca	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xdc000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xcaed4	0xcb000	False	0.619055235914	data	6.57686671715	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xce000	0xd8ca	0xda00	False	0.0914922591743	data	3.77202593589	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xdc000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xce130	0xd228	data		
RT_GROUP_ICON	0xdb358	0x14	data		
RT_VERSION	0xdb36c	0x374	data		
RT_MANIFEST	0xdb6e0	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2004 :=C=G=2A<F?<AHJI:52
Assembly Version	1.0.0.0
InternalName	BDHL.exe
FileVersion	5.7.10.12
CompanyName	:=C=G=2A<F?<AHJI:52
Comments	65>=BBIJ@55F:>8G
ProductName	B422A<96:DJ>@;I;
ProductVersion	5.7.10.12
FileDescription	B422A<96:DJ>@;I;
OriginalFilename	BDHL.exe

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:31:24.494191885 CEST	56961	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:24.507533073 CEST	53	56961	8.8.8.8	192.168.2.3
Apr 8, 2021 13:31:25.217374086 CEST	59353	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:25.230161905 CEST	53	59353	8.8.8.8	192.168.2.3
Apr 8, 2021 13:31:26.666817904 CEST	52238	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:26.678715944 CEST	53	52238	8.8.8.8	192.168.2.3
Apr 8, 2021 13:31:27.399626970 CEST	49873	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:27.412344933 CEST	53	49873	8.8.8.8	192.168.2.3
Apr 8, 2021 13:31:28.605986118 CEST	53196	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:28.618580103 CEST	53	53196	8.8.8.8	192.168.2.3
Apr 8, 2021 13:31:29.491197109 CEST	56777	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:29.503729105 CEST	53	56777	8.8.8.8	192.168.2.3
Apr 8, 2021 13:31:30.359407902 CEST	58643	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:30.372710943 CEST	53	58643	8.8.8.8	192.168.2.3
Apr 8, 2021 13:31:31.243885040 CEST	60985	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:31.256592989 CEST	53	60985	8.8.8.8	192.168.2.3
Apr 8, 2021 13:31:32.217641115 CEST	50200	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:32.230163097 CEST	53	50200	8.8.8.8	192.168.2.3
Apr 8, 2021 13:31:32.985733032 CEST	51281	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:33.002245903 CEST	53	51281	8.8.8.8	192.168.2.3
Apr 8, 2021 13:31:34.239829063 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:34.253031969 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 8, 2021 13:31:34.505069017 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:34.517946959 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 8, 2021 13:31:34.535218000 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:34.568444014 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 13:31:37.783739090 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:37.796343088 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 8, 2021 13:31:38.595550060 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:38.609460115 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 8, 2021 13:31:39.379354000 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:39.392750978 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 8, 2021 13:31:40.140357018 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:40.153753042 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 8, 2021 13:31:40.774282932 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:40.786783934 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 8, 2021 13:31:41.515301943 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:41.528565884 CEST	53	58361	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:31:42.290077925 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:42.303049088 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 8, 2021 13:31:48.665591002 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:48.666646004 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:48.683274984 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 8, 2021 13:31:48.684961081 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 8, 2021 13:31:51.926831961 CEST	58722	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:51.939348936 CEST	53	58722	8.8.8.8	192.168.2.3
Apr 8, 2021 13:31:52.008577108 CEST	56596	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:52.008682966 CEST	64101	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:52.020414114 CEST	53	56596	8.8.8.8	192.168.2.3
Apr 8, 2021 13:31:52.021186113 CEST	53	64101	8.8.8.8	192.168.2.3
Apr 8, 2021 13:31:58.441668987 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:58.455288887 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 8, 2021 13:31:58.596616983 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:31:58.609157085 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 8, 2021 13:32:00.560795069 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:32:00.580951929 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 8, 2021 13:32:02.775338888 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:32:02.787714958 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 8, 2021 13:32:03.951311111 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:32:03.988884926 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 8, 2021 13:32:04.086729050 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:32:04.099466085 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 8, 2021 13:32:11.381330013 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:32:11.394567966 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 8, 2021 13:32:11.756453037 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:32:11.769443989 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 8, 2021 13:32:11.786787033 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:32:11.799402952 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 8, 2021 13:32:16.429428101 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:32:16.442076921 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 8, 2021 13:32:16.835311890 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:32:16.847729921 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 8, 2021 13:32:16.864099026 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:32:16.876862049 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 8, 2021 13:32:18.615900993 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:32:18.628416061 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 8, 2021 13:32:19.072899103 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:32:19.099473000 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 8, 2021 13:32:19.116641045 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:32:19.129224062 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 8, 2021 13:32:20.696052074 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:32:20.708268881 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 8, 2021 13:32:33.232908010 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:32:33.250751019 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 8, 2021 13:32:41.438473940 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:32:41.450948954 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 8, 2021 13:33:27.003259897 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:33:27.017275095 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 8, 2021 13:33:34.521936893 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:33:34.540304899 CEST	53	61292	8.8.8.8	192.168.2.3

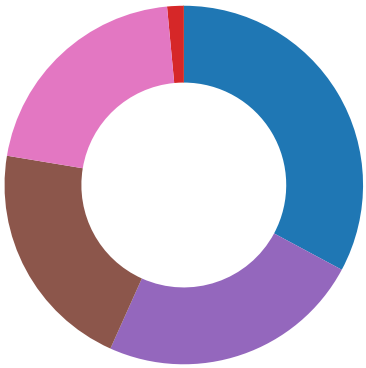
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 13:31:58.455288887 CEST	8.8.8.8	192.168.2.3	0x5fcc	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior



DHL_Express_Shipment_Invoice_C..
cmd.exe
conhost.exe
reg.exe
Files.exe
Files.exe
Files.exe

Click to jump to process

System Behavior

Analysis Process:
DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe
PID: 5716 Parent PID: 5704

General

Start time:	13:31:32
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe'
Imagebase:	0x9a0000
File size:	888320 bytes
MD5 hash:	EDAE8C184A250CCCBA45C023E805E12D
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: 00000000.00000002.299807783.0000000003E66000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.300534811.000000000402B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.299471132.0000000003DB7000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C6701B	CopyFileExW
C:\Users\user\AppData\Roaming\Files.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6C6701B	CopyFileExW
C:\Users\user\AppData\Roaming\Files.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C6701B	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3BC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0	41064	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 07 5a 8e 5a 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 54 00 00 00 0c 00 00 00 00 00 00 86 72 00 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 c0 00 00 00 02 00 00 9a 80 01 00 03 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....Z.Z.......... ....0..T...........r... ....@.. ....`................	success or wait	1	6C6701B	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Files.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 35 1d 1a 53 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 b0 0c 00 00 dc 00 00 00 00 00 00 ce ce 0c 00 00 20 00 00 00 e0 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 e0 0d 00 00 02 00 00 00 00 00 00 02 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...5..S.......... ....@.. ....`................	success or wait	4	6C6701B	CopyFileExW
C:\Users\user\AppData\Roaming\Files.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6C6701B	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe.log	unknown	1402	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	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_v4.0.3	success or wait	1	6E3BC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 3412 Parent PID: 5716

General

Start time:	13:31:52
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'Files' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\Files.exe'
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 4060 Parent PID: 3412

General

Start time:	13:31:52
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: reg.exe PID: 5432 Parent PID: 3412

General

Start time:	13:31:53
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'Files' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\Files.exe'
Imagebase:	0x1b0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Files	unicode	C:\Users\user\AppData\Roaming\Files.exe	success or wait	1	1B5A1D	RegSetValueExW

Analysis Process: Files.exe PID: 5980 Parent PID: 3388

General

Start time:	13:32:07
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Roaming\Files.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Files.exe'
Imagebase:	0x120000
File size:	888320 bytes
MD5 hash:	EDAE8C184A250CCCBA45C023E805E12D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 38%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Files.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3BC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Files.exe.log	unknown	1402	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	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_v4.0.3	success or wait	1	6E3BC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: Files.exe PID: 6280 Parent PID: 5716

General

Start time:	13:32:13
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Roaming\Files.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Files.exe'
Imagebase:	0x3c0000
File size:	888320 bytes
MD5 hash:	EDAE8C184A250CCCBA45C023E805E12D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile

Analysis Process: Files.exe PID: 6332 Parent PID: 3388

General

Start time:	13:32:15
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Roaming\Files.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Files.exe'
Imagebase:	0xc30000
File size:	888320 bytes
MD5 hash:	EDAE8C184A250CCCBA45C023E805E12D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile

Disassembly

Code Analysis