ID: 383910
Sample Name:
DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe
Cookbook: default.jbs
Time: 12:13:02
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

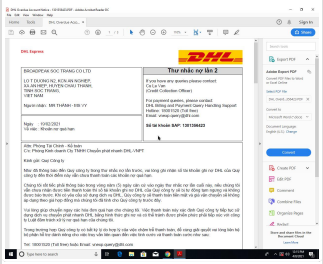
Analysis Report DHL_Express_Shipments_Invoice_Con…

Overview

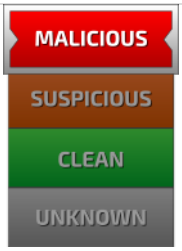
General Information

Sample Name:	DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe
Analysis ID:	383910
MD5:	56796a808359f3e.
SHA1:	2a640c1ceda881..
SHA256:	966f5fda32ac9ad..
Tags:	AgentTesla DHL exe
Infos:	

Most interesting Screenshot:



Detection



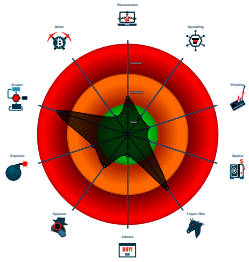
AgentTesla

Score:	100
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…
- Allocates memory in foreign process…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Writes to foreign memory regions
- Antivirus or Machine Learning detec…
- Contains capabilities to detect virtua…

Classification



Startup

- **System is w10x64**
- DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe (PID: 6572 cmdline: 'C:\Users\user\Desktop\DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe' MD5: 56796A808359F3EACD3DFAE75E530C7F)
  - cmd.exe (PID: 6884 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: 6892 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - reg.exe (PID: 6920 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: 6484 cmdline: 'C:\Users\user\AppData\Roaming\Files.exe' MD5: 56796A808359F3EACD3DFAE75E530C7F)
    - AcroRd32.exe (PID: 5488 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\AppData\Roaming\DHL Overdue Account Notice - 1301356423.PDF' MD5: B969CF0C7B2C443A99034881E8C8740A)
      - AcroRd32.exe (PID: 2200 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\AppData\Roaming\DHL Overdue Account Notice - 1301356423.PDF' MD5: B969CF0C7B2C443A99034881E8C8740A)
      - RdrCEF.exe (PID: 6524 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
        - RdrCEF.exe (PID: 5372 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1712,2401863177927084696,18206753643728564179,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=7717275198719545956 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=7717275198719545956 --renderer-client-id=2 --mojo-platform-channel-handle=1724 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
        - RdrCEF.exe (PID: 5424 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1712,2401863177927084696,18206753643728564179,131072 --disable-features=VizDisplayCompositor --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --lang=en-US --gpu-preferences=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=14898531479645788559 --mojo-platform-channel-handle=1744 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
        - RdrCEF.exe (PID: 5720 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1712,2401863177927084696,18206753643728564179,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=9725964129438127640 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=9725964129438127640 --renderer-client-id=4 --mojo-platform-channel-handle=1816 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
        - RdrCEF.exe (PID: 3120 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1712,2401863177927084696,18206753643728564179,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=2964269592299071020 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=2964269592299071020 --renderer-client-id=5 --mojo-platform-channel-handle=2148 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - InstallUtil.exe (PID: 1208 cmdline: C:\Users\user\AppData\Local\Temp\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
- Files.exe (PID: 6184 cmdline: 'C:\Users\user\AppData\Roaming\Files.exe' MD5: 56796A808359F3EACD3DFAE75E530C7F)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "aammorris@askoblue.comhbqtHu^3smtp.privateemail.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000015.00000002.604942356.0000000002D01000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000015.00000002.604942356.0000000002D01000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000E.00000002.618305567.000000000436D000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000E.00000002.617790683.00000000041A7000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000015.00000002.593141973.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 6 entries

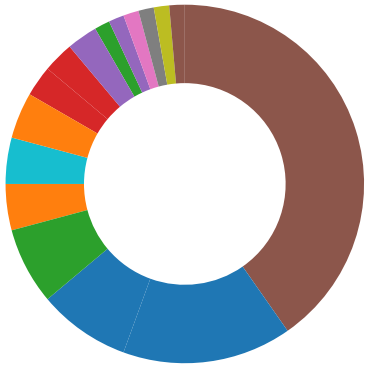
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.DHL_Express_Shipments_Invoice_Confirmation_CBJ 190517000131_74700456XXX.exe.42d930a.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
14.2.Files.exe.436d5fa.7.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
14.2.Files.exe.42b7e3a.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
21.2.InstallUtil.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
14.2.Files.exe.40f8d58.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 16 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- 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)

Malware Analysis System Evasion:

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:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

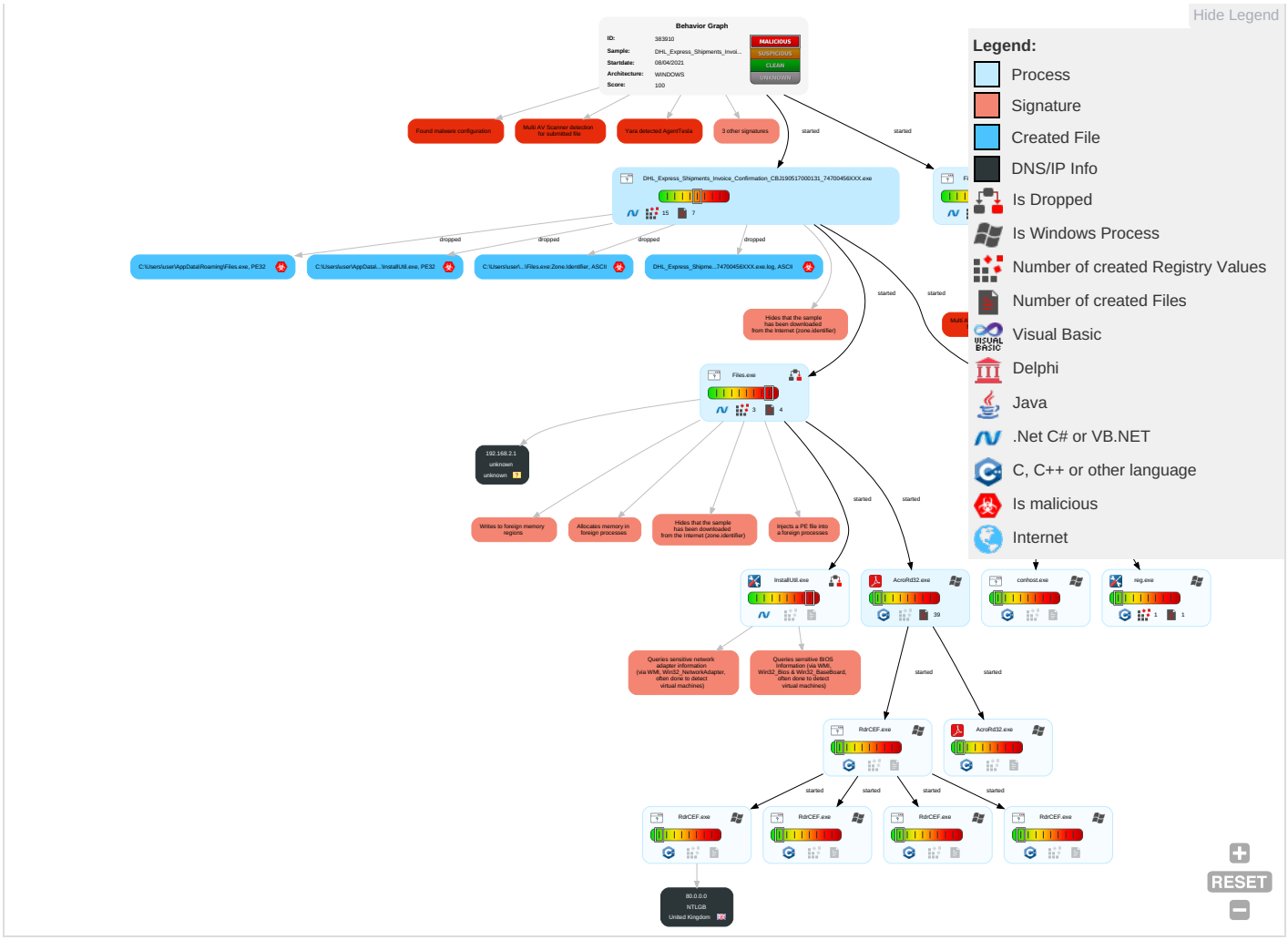
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C a
Valid Accounts 1	Windows Management Instrumentation 2 1 1	Valid Accounts 1	Valid Accounts 1	Masquerading 1	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	E C
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	Valid Accounts 1	LSASS Memory	Security Software Discovery 2 2 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	J
Domain Accounts	At (Linux)	DLL Side-Loading 1	Process Injection 3 1 2	Modify Registry 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	S
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	NTDS	Virtualization/Sandbox Evasion 1 4 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	F I
Cloud Accounts	Cron	Network Logon Script	DLL Side-Loading 1	Disable or Modify Tools 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	F C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	M C
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 3 1 2	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	C U
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	System Information Discovery 1 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	A L
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Obfuscated Files or Information 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	V
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Software Packing 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	F F
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	DLL Side-Loading 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	M

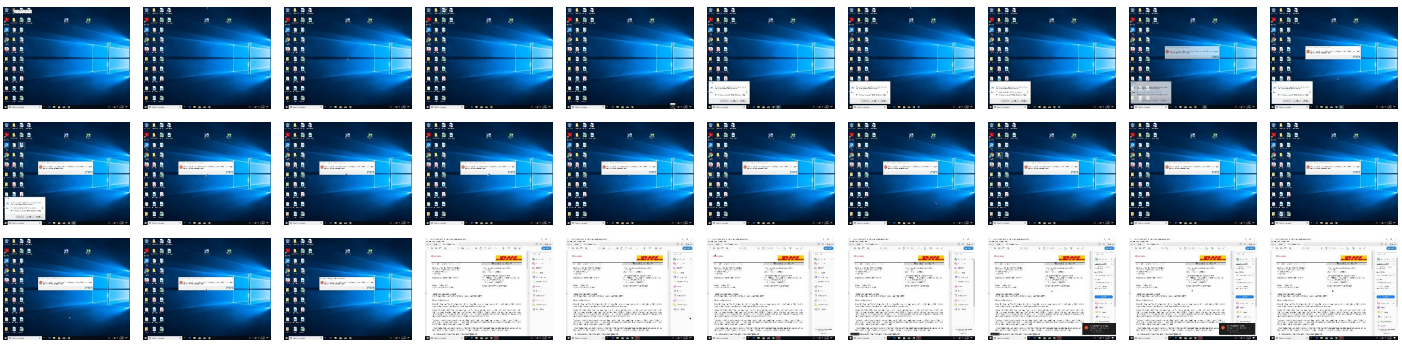
Behavior Graph

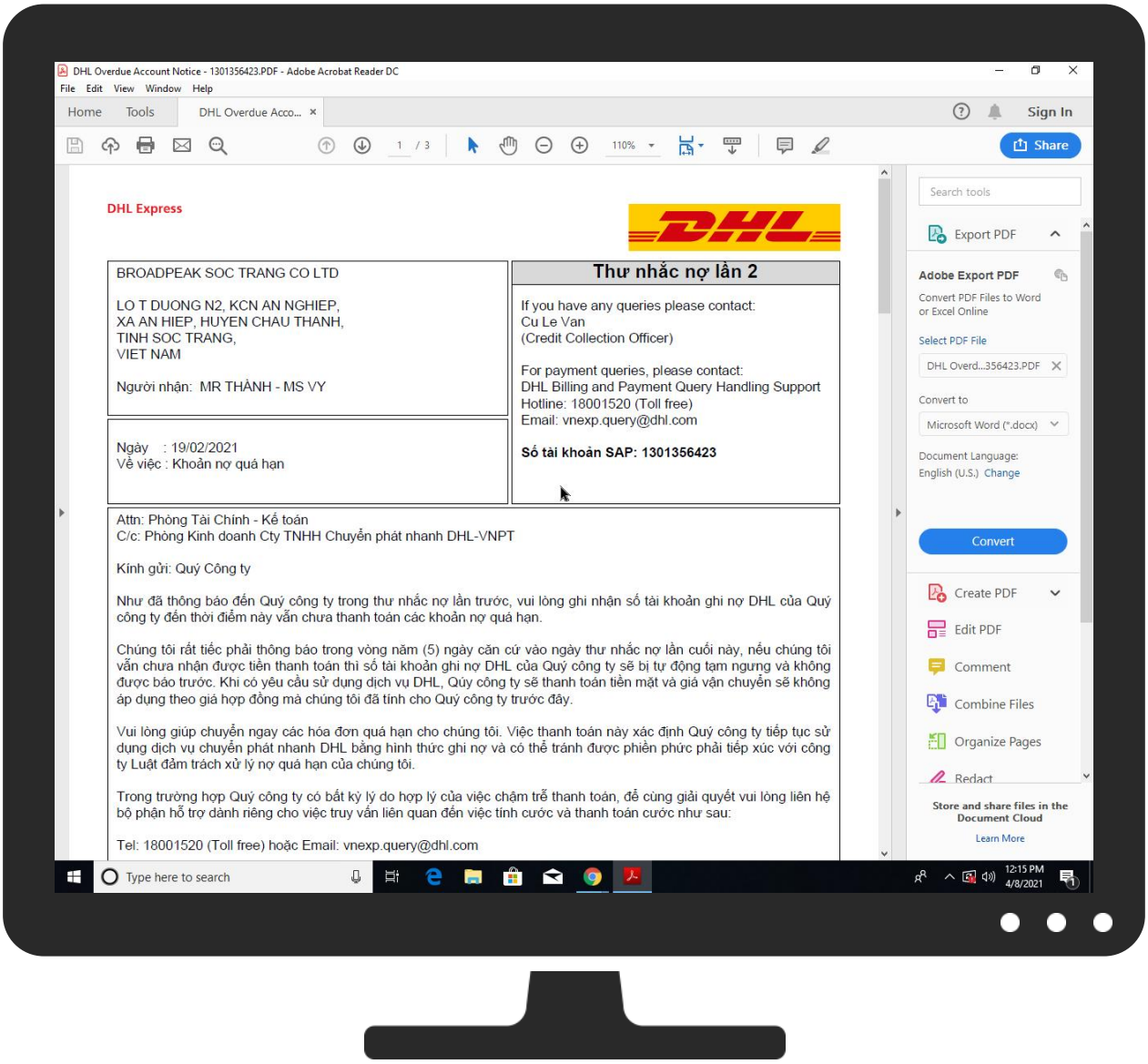


Screenshots

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_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe	36%	Virustotal		Browse
DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe	21%	ReversingLabs	Win32.Trojan.AgentTesla	
DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.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	21%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
21.2.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/Lu_RL	0%	Avira URL Cloud	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/&x	0%	Avira URL Cloud	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	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://ns.adobe.c/g	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/B	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	0%	Avira URL Cloud	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://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://ns.adb	0%	URL Reputation	safe	
http://ns.adb	0%	URL Reputation	safe	
http://ns.adb	0%	URL Reputation	safe	
http://ns.adb	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/pxYP	0%	Avira URL Cloud	safe	
http://ns.ado/11	0%	Avira URL Cloud	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://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/)R	0%	Avira URL Cloud	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/N	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://cipa.jp/exif/1.0/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/1.0/	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://pki.goog/repository/0	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/D	0%	Avira URL Cloud	safe	
http://https://api.echosign.comRL(	0%	Avira URL Cloud	safe	
http://crl.mu	0%	Avira URL Cloud	safe	
http://ns.adobe.c/g1	0%	Avira URL Cloud	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/YO	0%	Avira URL Cloud	safe	
http://ns.adobe.c/g8	0%	Avira URL Cloud	safe	
http://ns.adobe.c/g%%	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	0%	Avira URL Cloud	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	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://iptc.org/std/Iptc4xmpCore/1.0/xmlns/zu	0%	Avira URL Cloud	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

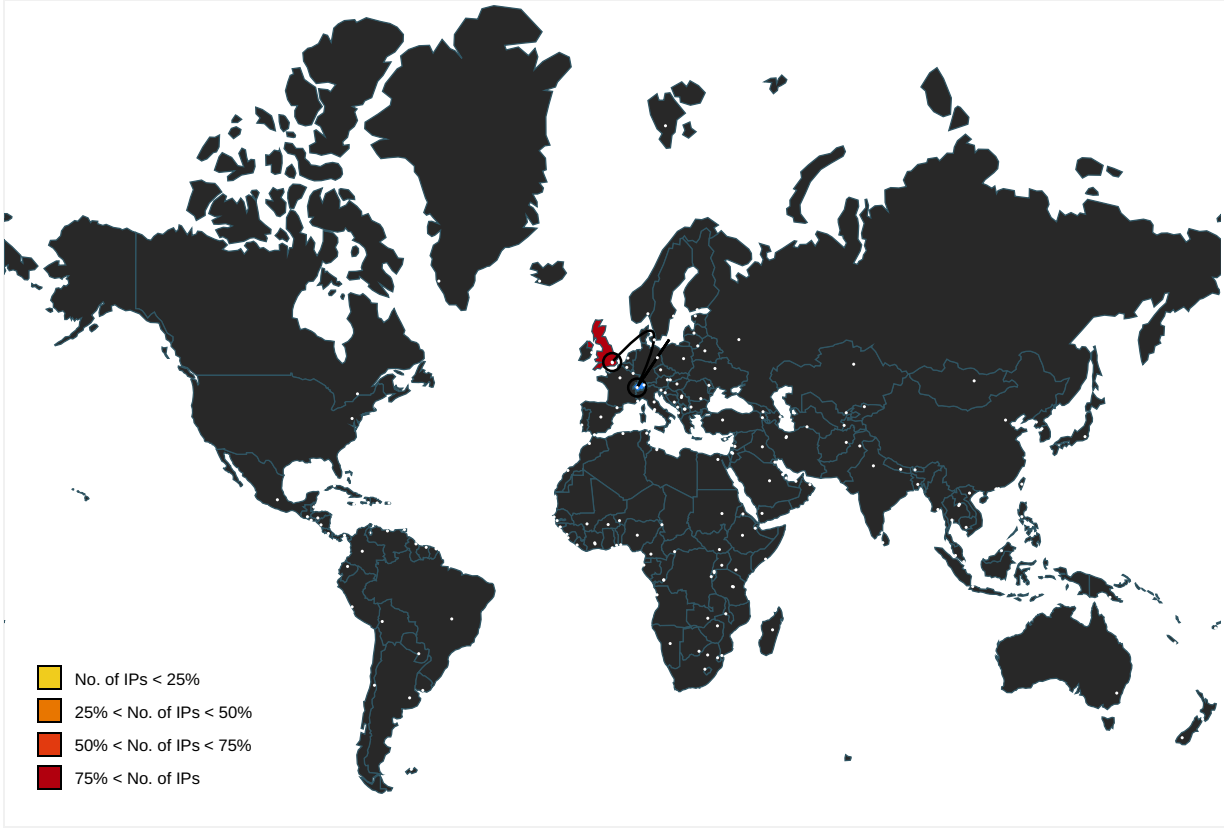
Name	Source	Malicious	Antivirus Detection	Reputation
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/Lu_RL	AcroRd32.exe, 00000014.00000003.515935868.000000000BAF4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/schema#	AcroRd32.exe, 00000014.00000003.515935868.000000000BAF4000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/type#QupRO	AcroRd32.exe, 00000014.00000003.515935868.000000000BAF4000.00000004.00000001.sdmp	false		high
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	AcroRd32.exe, 00000014.00000002.611035366.0000000008270000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/property#GufRM	AcroRd32.exe, 00000014.00000003.515935868.000000000BAF4000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/type#hu	AcroRd32.exe, 00000014.00000003.515935868.000000000BAF4000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/&x	AcroRd32.exe, 00000014.00000002.649710805.000000000E123000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://cipa.jp/exif/1.0/	AcroRd32.exe, 00000014.00000002.649611201.000000000E0B7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.c/g	DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe, 00000000.00000003.354223291.000000000723A000.00000004.00000001.sdmp, DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe, 00000000.00000002.425822118.000000000724B000.00000004.00000001.sdmp, Files.exe, 0000000E.00000003.469317818.00000000074A3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	AcroRd32.exe, 00000014.00000002.611035366.0000000008270000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/WebPage	Files.exe, 0000000E.00000002.605804441.00000000030AE000.00000004.00000001.sdmp, Files.exe, 0000000E.00000002.605886421.00000000030C4000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/type#	AcroRd32.exe, 00000014.00000003.515935868.000000000BAF4000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/B	AcroRd32.exe, 00000014.00000003.515935868.000000000BAF4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.echosign.com	AcroRd32.exe, 00000014.00000002.650509786.000000000E418000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	AcroRd32.exe, 00000014.00000002.649710805.000000000E123000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://crl.pki.goog/GTS1O1core.crl0	DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe, 00000000.00000002.416790426.00000000012EC000.00000004.00000020.sdmp, Files.exe, 0000000A.00000003.411483153.000000000100B000.00000004.00000001.sdmp, Files.exe, 0000000E.00000003.465280195.000000000155B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.npes.org/pdfx/ns/id/	AcroRd32.exe, 00000014.00000002.649611201.000000000E0B7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/drm/default	AcroRd32.exe, 00000014.00000002.611035366.0000000008270000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adb	Files.exe, 0000000E.00000003.443115256.00000000074A3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	AcroRd32.exe, 00000014.00000002.611035366.0000000008270000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/pxYP	AcroRd32.exe, 00000014.00000002.649710805.000000000E123000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://mybill.dhl.com/	AcroRd32.exe, 00000014.00000003.503961105.000000000B995000.00000004.00000001.sdmp, AcroRd32.exe, 00000014.00000002.649611201.000000000E0B7000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/extension/	AcroRd32.exe, 00000014.00000003.515935868.000000000BAF4000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe, 00000000.00000002.417319845.00000000030A1000.00000004.00000001.sdmp, Files.exe, 0000000A.00000002.425647475.0000000002C41000.00000004.00000001.sdmp, Files.exe, 0000000E.00000002.605716042.0000000003081000.00000004.00000001.sdmp	false		high
http://ns.ado/11	DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe, 00000000.00000003.354223291.000000000723A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe, 00000000.00000002.420461900.000000000411A000.00000004.00000001.sdmp, Files.exe, 0000000E.00000002.618305567.000000000436D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/subclip/1.0	AcroRd32.exe, 00000014.00000002.611035366.0000000008270000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cipa.jp/exif/1.0/)R	AcroRd32.exe, 00000014.00000002.649611201.000000000E0B7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/property#	AcroRd32.exe, 00000014.00000003.515935868.000000000BAF4000.00000004.00000001.sdmp	false		high
http://ns.useplus.org/ldf/xmp/1.0/	AcroRd32.exe, 00000014.00000003.515935868.000000000BAF4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.cobj	Files.exe, 0000000E.00000003.469317818.00000000074A3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/id/	AcroRd32.exe, 00000014.00000002.649611201.000000000E0B7000.00000004.00000001.sdmp	false		high
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	AcroRd32.exe, 00000014.00000003.515935868.000000000BAF4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/layout/anchor	AcroRd32.exe, 00000014.00000002.611035366.0000000008270000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	AcroRd32.exe, 00000014.00000003.515935868.000000000BAF4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfe/ns/id/	AcroRd32.exe, 00000014.00000002.649611201.000000000E0B7000.00000004.00000001.sdmp	false		high
http://www.npes.org/pdfx/ns/id/N	AcroRd32.exe, 00000014.00000002.649611201.000000000E0B7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki.goog/gsr2/GTS1O1.crt0	DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe, 00000000.00000002.416790426.00000000012EC000.00000004.00000020.sdmp, Files.exe, 0000000A.00000003.411483153.000000000100B000.00000004.00000001.sdmp, Files.exe, 0000000E.00000003.465280195.000000000155B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cipa.jp/exif/1.0/1.0/	AcroRd32.exe, 00000014.00000002.649611201.000000000E0B7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/repository/0	DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe, 00000000.00000002.416790426.00000000012EC000.00000004.00000020.sdmp, Files.exe, 0000000A.00000003.411483153.000000000100B000.00000004.00000001.sdmp, Files.exe, 0000000E.00000003.465280195.000000000155B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.npes.org/pdfx/ns/id/D	AcroRd32.exe, 00000014.00000002.649611201.000000000E0B7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.echosign.comRL(	AcroRd32.exe, 00000014.00000002.650509786.000000000E418000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://mybill.dhl.com/P	AcroRd32.exe, 00000014.00000002.649611201.000000000E0B7000.00000004.00000001.sdmp	false		high
http://https://mybill.dhl.com/DwgP	AcroRd32.exe, 00000014.00000003.515935868.000000000BAF4000.00000004.00000001.sdmp	false		high
http://crl.mu	Files.exe, 0000000E.00000003.465280195.000000000155B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.adobe.c/g1	DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe, 00000000.00000003.354223291.000000000723A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/field#	AcroRd32.exe, 00000014.00000003.515935868.000000000BAF4000.00000004.00000001.sdmp	false		high
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	AcroRd32.exe, 00000014.00000002.611035366.0000000008270000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/YO	AcroRd32.exe, 00000014.00000003.515935868.000000000BAF4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://ns.adobe.c/g8	DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe, 00000000.00000003.366225487.000000000721C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.adobe.c/g%%	DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe, 00000000.00000002.425786361.000000000723B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	AcroRd32.exe, 00000014.00000003.515935868.000000000BAF4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.quicktime.com.Acrobat	AcroRd32.exe, 00000014.00000002.611035366.0000000008270000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 00000014.00000002.619503674.0000000009487000.00000004.00000001.sdmp	false		high
http://crl.pki.goog/gsr2/gsr2.crl0?	DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe, 00000000.00000002.416790426.00000000012EC000.00000004.00000020.sdmp, Files.exe, 0000000A.00000003.411483153.000000000100B000.00000004.00000001.sdmp, Files.exe, 0000000E.00000003.465280195.000000000155B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/zu	AcroRd32.exe, 00000014.00000003.515935868.000000000BAF4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.ado/1	DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe, 00000000.00000002.425822118.000000000724B000.00000004.00000001.sdmp, Files.exe, 0000000E.00000003.469317818.00000000074A3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
80.0.0.0	unknown	United Kingdom		5089	NTLGB	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383910
Start date:	08.04.2021
Start time:	12:13:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.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:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@25/53@0/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.1%) • Quality average: 25.1% • Quality standard deviation: 37.1%
HCA Information:	• Successful, ratio: 97% • 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): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 23.54.113.53, 52.147.198.201, 172.217.168.4, 204.79.197.200, 13.107.21.200, 104.43.193.48, 13.88.21.125, 20.82.210.154, 23.10.249.43, 23.10.249.26, 8.238.35.254, 67.26.73.254, 8.238.85.254, 8.238.29.254, 8.241.79.126, 52.155.217.156, 20.54.26.129, 52.255.188.83, 23.54.113.182, 23.10.249.187, 23.0.174.233, 92.122.144.200, 20.50.102.62 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, e4578.dscb.akamaiedge.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, acroipm2.adobe.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, a122.dscd.akamai.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, www.google.com, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, acroipm2.adobe.com.edgesuite.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, armmf.adobe.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • 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. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:14:12	API Interceptor	46x Sleep call for process: DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_747 00456XXX.exe modified
12:14:12	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Files C:\Users\user\AppData\Roaming\Files.exe

Time	Type	Description
12:14:20	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Files C:\Users\user\AppData\Roaming\Files.exe
12:14:35	API Interceptor	33x Sleep call for process: Files.exe modified
12:15:17	API Interceptor	3x Sleep call for process: RdrCEF.exe modified
12:15:40	API Interceptor	127x Sleep call for process: InstallUtil.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
80.0.0.0	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_Confirmation_BKKR005545473_88700456XXXX.exe	Get hash	malicious	Browse	
	APRILQUOTATION#QQO2103060_SAMPLES_KHANG HY_CO_CORPORATION.exe	Get hash	malicious	Browse	
	#U260f8284.HTML	Get hash	malicious	Browse	
	HunpuKMHQt.exe	Get hash	malicious	Browse	
	JbQoNNPVOk.exe	Get hash	malicious	Browse	
	_vm583573758.htm	Get hash	malicious	Browse	
	March 17, 2021, 101142 AM.HTM	Get hash	malicious	Browse	
	message_zdm.html	Get hash	malicious	Browse	
	0000001_Carved.pdf	Get hash	malicious	Browse	
	BWKPI3LiLi.jar	Get hash	malicious	Browse	
	BWKPI3LiLi.jar	Get hash	malicious	Browse	
	fakeadmin.pdf	Get hash	malicious	Browse	
	x4F1uS8nAq.exe	Get hash	malicious	Browse	
	vUp5vjYOoL.exe	Get hash	malicious	Browse	
	2021-02-15__Mail-Degroof-Petercam_ENC.docx	Get hash	malicious	Browse	
	InformaAllSecure_Enhanced_Health_Safety_Standards_2021.docm	Get hash	malicious	Browse	
	Swift.pdf.jar	Get hash	malicious	Browse	
	0001.jar	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NTLGB	DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe	Get hash	malicious	Browse	• 80.0.0.0
	DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe	Get hash	malicious	Browse	• 80.0.0.0
	DHL_Express_Shipment_Confirmation_BKKR005545473_88700456XXXX.exe	Get hash	malicious	Browse	• 80.0.0.0
	APRILQUOTATION#QQO2103060_SAMPLES_KHANG HY_CO_CORPORATION.exe	Get hash	malicious	Browse	• 80.0.0.0
	#U260f8284.HTML	Get hash	malicious	Browse	• 80.0.0.0
	HunpuKMHQt.exe	Get hash	malicious	Browse	• 80.0.0.0
	1.sh	Get hash	malicious	Browse	• 62.254.90.3
	PDFXCview.exe	Get hash	malicious	Browse	• 82.38.144.251
	JbQoNNPVOk.exe	Get hash	malicious	Browse	• 80.0.0.0
	_vm583573758.htm	Get hash	malicious	Browse	• 80.0.0.0
	March 17, 2021, 101142 AM.HTM	Get hash	malicious	Browse	• 80.0.0.0
	message_zdm.html	Get hash	malicious	Browse	• 80.0.0.0
	0000001_Carved.pdf	Get hash	malicious	Browse	• 80.0.0.0
	BWKPI3LiLi.jar	Get hash	malicious	Browse	• 80.0.0.0
	BWKPI3LiLi.jar	Get hash	malicious	Browse	• 80.0.0.0

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2ojdmC51As.exe	Get hash	malicious	Browse	• 62.30.7.67
	fakeadmin.pdf	Get hash	malicious	Browse	• 80.0.0.0
	8dazsN65iH.exe	Get hash	malicious	Browse	• 80.193.200.66
	Y17R73rU50.exe	Get hash	malicious	Browse	• 92.239.246.126
	x4F1uS8nAq.exe	Get hash	malicious	Browse	• 80.0.0.0

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	
	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_6620200947535257662_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	
	QUOTATIONs#280321_RFQ_PRODUCTS_ENQUIRY_TRINITY_VIETNAM_CO.exe	Get hash	malicious	Browse	
	RFQ9088QTY.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\05349744be1ad4ad_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	410
Entropy (8bit):	5.649486083749248
Encrypted:	false
SSDEEP:	6:men9YOFLvEWdM9Qa07aUV2Kwi7Z+P41TK6tI8en9YOFLvEWdM9QrcCoBwi7Z+P41:vDRM9Z07aUVjZiEmxDRM9bC8ZiE
MD5:	9B2A85F52DAFC1D3D74CFFEC023D30DE
SHA1:	C15D0A07FC6C5CB5D30F31827B3612B7C680C3BA
SHA-256:	11B853D48952AFA8D2F5C0ABC42007FE7A400B4EB3EF14925D16A23349722C42
SHA-512:	36FDC2EBB4C7DD48B12F93EC5524FFBBB6D6072A26B7F00D4F434F40A2A9FE061AEE5C5F6D1A18F2397470EC7ADCB0AE6A0D974B1E35AAD13AE7320C2B8332F3
Malicious:	false
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ..qi'../....."#.D.....A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....G1i.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .h..'../....."#.D._....A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....Q.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0	
Size (bytes):	522
Entropy (8bit):	5.625131008109145
Encrypted:	false
SSDEEP:	6:mi9NqEYOFLvEkq+S8Be7Ywcr1TK6tMFEi9NqEYOFLvEk9Z8Be7Ywcr1TK6tt2i9f:V9znS9PQKP9zdZ9PQN9zd9vZ9PQ
MD5:	20CDAA68271E6CF1CD6A26D1BAF8C62C
SHA1:	819230CBE0179A48EE07B97DEFF0476EDA396236
SHA-256:	69A4EDFDC7E3A9E8F6AB5DD2E05DD6879EF277BCBEF41E96B052AECF5D49B0E1
SHA-512:	2F6EE88318C5E9EFBE18CBCD9489D6690CDB27D30DC89F9CCBE7046A5A25A23FEA9319411A44DB1C5CF4576DF729875ABB3274D4F2E8B73AFE2FE4DF9698F94C
Malicious:	false
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ....'../....."#.D.&....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....8.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .5.R'../....."#.D.I.....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....9.7.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ...~'../....."#.D.2....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....".....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	492
Entropy (8bit):	5.607305864953384
Encrypted:	false
SSDEEP:	12:DyeRVFAFjVFAFwulUo6jrjyeRVFAFjVFAFNCa9EQlUo6j:tB4v4wuSBrNB4v4MMEQSB
MD5:	CDA6BAD75B9877FE5156D66556051E81
SHA1:	E46F836F348977AE9768854059564297617FC62A
SHA-256:	A9A9725C38A050FB748D6BBAEB42D8D77320313D329915604C18F2E17057BFCE
SHA-512:	9405529718A39AD601F5804F12634ED529F4ADF703A7C8F4E2CB93F60909BD75DEC8CAD59045C3DA7CD2A4E1836BB52B6C747CA6F40E31C2A5E47920AC1D0CA
Malicious:	false
Preview:	0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ...h'../....."#.D..~....A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....'.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js .Y.'../....."#.D..V....A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....<.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0ace9ee3d914a5c0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.648267715238674
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RsGuCSw0iWulHyA1TK6tY/l:IbRkiDuyWussO/l
MD5:	0F7CE487CCF03F080B74E70133674655
SHA1:	043CAA29AECC5A8A72BC55CBBDEB9A97C53BF0FD
SHA-256:	285C49C09A2F95434F61A8751317DE4DD07B3DD6609E3E2A4FAC0B1DFDFA8793
SHA-512:	52CE4E273BA158D462D9C164D17E1C4EF0093246735649B9D170FB0D9DB4B5BDDCCA13B186C4365FF8650C5FA5831DF9F789D6297DF4548EB5D99505F22416E
Malicious:	false
Preview:	0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js .;.p'../....."#.D.7.....A..8 P..a...R..Y....7.@..2Dm{ ..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.576011266846673
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVuW9rlKSPVyh9PT41TK6t:pyixRualtPV41TE
MD5:	877292CC777490FF2F544286AA024493
SHA1:	003D8DF6D1347CFB1F424950116D206AE524014C
SHA-256:	97E096F405164EA40F284A5DE01485780FA4F27236F1063A12945FB2862FBB6A
SHA-512:	B3ADA393DE9AF2E08A450A5365C198EC695ECA5729E81331FF3C13C469E07BB21B191D615FC10F949B7B67885515DABD4893E0EC0D960DA77156FDA272D1D008
Malicious:	false
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ..v.'../....."#.D.xZ....Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo.....3..).....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.621647904682762
Encrypted:	false
SSDEEP:	6:mvYOFLvEWdhwjQJFGlbNLZIl6P41TK6t1JF:0Rhk/bNLZCbJ
MD5:	74C998969873C15ABD6E2A0652920298
SHA1:	2CE69628318E96AFBBD45EC99AB725B2302A2376
SHA-256:	82605AE1576E779354BDBB944C39B660B1CDA3E53FCCF30F93AA0A897E7B5E43
SHA-512:	2F59D46A46AE82C173A3D596181C709C3A8B9CC0516726348D8B872982411AE773F53F32FB73496F17A08852CB998A754FE078169860094A4BEEAE3548D93286
Malicious:	false
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ...'../....."#.D.x7....A.].>....uUf..N...k.....c..I.A..Eo.....A. .Eo.....G.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	209
Entropy (8bit):	5.552478452492033
Encrypted:	false
SSDEEP:	3:m+lZd8RzYOCGLvHkWBGKuKjXKX7KoQRA/KVdKLuVFc0cBwwCktcyxMtv9EWm1TKk:mJYOFLvEWdGQRQOdQei/6g1TK6tl
MD5:	42F591C5C311BBC83EAB707402C3A0E6
SHA1:	303C901CE7123BC146B51E5FBFEFFB626EC97F59
SHA-256:	8E75B4E31BFBCDA0FECE8AD300ECE4BA6EAB9EBD1B39DC60C5D95EC6FECB4524
SHA-512:	109654EDB48E222659E2B2882DD16A828F0DB6994581CFC3699F776B95306BDC04E6395974B923AF0011EB397B48060776C4BDCBDC777B6694A208632242F9AA
Malicious:	false
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ....'../....."#.D..Z....A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo .....@.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	537
Entropy (8bit):	5.623883263376499
Encrypted:	false
SSDEEP:	12:Z5MsnL9eMuR/EJ5MK+IMuR/Es5MkMuR/EFS:ZSeJvuR/EJSlJuR/EsS9uR/Ec
MD5:	66B0615AC8CA36906997BA88BFCB65F6
SHA1:	22289ECE6D3FA7A89C94B74DADA09F2062AB6BB7
SHA-256:	77D745D46223D314F6FB0179365CF0CC8782AD54772E077C56CFF19D29E07991
SHA-512:	59677A852D820317117756FA0E07ACF726828E2C70F4C63ACDC8DC07378E039F8478DCBD81C4FD32D6A2C9C3072EBB9A25C61BAAFA4FF578C65C71D9C4BF5E A
Malicious:	false
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .G..'../....."#.DnN....A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....4.nY.....0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ...R'../....."#.D.....A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .f..'../....."#.DP.....A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....z. !.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.53530636662749
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtunnMby0zBUKSAA1TK6tE:pRMMbe
MD5:	DF1E13FBEFFA4965A10715978EB44BCA
SHA1:	26BB4305B95895763A651DF5FFC97784F66B1103
SHA-256:	D63A39707B787EAE6051F8EB6A8A6FE8C84D462C16E53FB82200D8CC6DC5524C
SHA-512:	EC4D6348E39672AB1B9FE70FD62A504385904F23436A802FDB098E8AE4028EA6CF4390CECA88790F6F70D7FA3BD36CCA8DF4C2B318C3DD249AAF546DDEDF56 6E
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0	
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .'Z.'../....."#.D|.[....AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....A..Eo.....Cf.e.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	531
Entropy (8bit):	5.593891450853813
Encrypted:	false
SSDEEP:	12:KkXxKMSCvxqotUlDLkXxKMSCvYO5VtUlrakXxKMSCvpV2otUl:KkXxiCDWXkXxiCAGVWrakXxiCj7W
MD5:	3788B90FDBC3A38C21921335237918AC
SHA1:	8F4D07176741754C995B5BDBA6E1F1A2A1442CB6
SHA-256:	7B69253C2594C4BDEA183B901B31118DA9742071C77FE06BC9E58DD3C6E91F72
SHA-512:	EFDF5C1ED37AB30F459BAFD23FE8C507569867786C3E4B7C89C8F240C89408D1DECA8C80695BF6C85A9398F7481BCEA56117C6663C8C9357A60A59CF2C669F
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .Z..'../....."#.D=C....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....K.'.....0\r..m.....1.....5.... _keyhttps://rna-resource.acrobat.com/plugins.js ...R'../....."#.D.....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....0.].....0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .&..'../....."#.D.....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....P.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	374
Entropy (8bit):	5.587078998822293
Encrypted:	false
SSDEEP:	6:mkl9YOFLvEWsfOLaC/yM+VY1TK6toEkl9YOFLvEWsfOLgXH7yM+VY1TK6t:5h6OLwkebh6OLfX6k
MD5:	8A6D2ADCCC0A7180AF5F506C09D10909
SHA1:	59CEABC74963001601828AC2B3601FC9D83BEE20
SHA-256:	7A6B90267B881DA24CBCC2383796634893AE2D8FD2B821D089E6C5B749A5D2C1
SHA-512:	4F6252997FAA7FF5AABC7401C5C9FACE9521B5B1EDB61956E01582D221604D57D52C2D7193C5106CB3657E9FAA2E6D7AAC791DD2FFC5D2071AFF89EE8BBF95 5C
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ..`'../....."#.Do.Z....A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo....."".....0\r..m.....;... I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ....'../....."#.D.x....A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....R+.`.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	488
Entropy (8bit):	5.635851424958865
Encrypted:	false
SSDEEP:	12:URVFAFjVFAF6YwSeKaTLnr8RVFAFjVFAFGj+wSeKaTLn0:UB4v47wzXLnr8B4v4Gj+wzXLn0
MD5:	FE73B7C3E88D54CCA6841FE3AE905E73
SHA1:	8A646B226B89168A86B46333DF7A9BE8FE8E70FF
SHA-256:	3730E39CFC5DA0065E52EDB53635D93BDAC994FE981F4341FDAAA7779897C2D2
SHA-512:	B594469D03F9DE73287D496F36F4279DAC1619A087DF74EF29F631D806ACB0AC34DECF3B56D34178EDE56990D10102243EE6C447B1944F0F88E65F62A35F318E
Malicious:	false
Preview:	0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js .+.j'../....."#.D.....A.....H...{...2. ./.k`..r4.C. .A..Eo.....A..Eo.....z.....0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js ..y.'../....."#.D.Fc....A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.520747031503777
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXulKKwnY11TK6tR:BsR2EsehG
MD5:	F1127D6F8B74B18678E05C4FEEC68E03
SHA1:	9385E3D2F8D0510E8FCE700A0A24EA946BFEA5F5

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0	
SHA-256:	3FC0094D5124A84226BF0E7083879CAE2008C3C41D6FA83073F58FB1C7A5A5A0
SHA-512:	F5874C35470BB1F3ADA42215D527968595532A9508F7931CBC29BD03D4236E1524201C1B60F8710F18F5E1DD385A3224A3D77E44CBEA78A5395771CE65B9EDB9
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ...'../....."#.D..Y....A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo.....4-:!.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.675137340496587
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQsaRx4B7OhKlvA1TK6tN/:RbR16S+BJkT/
MD5:	35638D87AF5C9F565C9D0BB74CE60674
SHA1:	F6B83A2FEC108AFC56AF907E10D5CEFE0ED94E37
SHA-256:	3B16699A8AEE93CBA0BBF566D82F53E31162F264F3E04858C86BFF527B745496
SHA-512:	9794365C4EA8E7E122A83A91C1F9D5CA2B75B25957204203ED0A625044AC1554E7F0DBB6F187D77D66456DE3758512A2F96899635E70C8148D545A82BE167F56
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js .>..'../....."#.D$.6....A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....Y.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.584664981352227
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVuhh+9s0QdFt1TK6tf:B2geRHRQi+9R0
MD5:	3EDE8F7B602703AE692720C099EB53E8
SHA1:	E168D177ED642247E1D456A74A7B74A5EE16B797
SHA-256:	F1932E051F932D5D977B8EEDF74B1125CD350E5F188AABDC57DFC5AE4AEF3C61
SHA-512:	67EAA9AF19FD6ADB1363833C9BE0522599FB4360D067DA452E151D905960AC3D810DD9F8F52546E1E3CBA46230DB8EDB251AB804A9318F2DFD36E256735B7FD9
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ....'../....."#.D..X....A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A..Eo.....5.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	412
Entropy (8bit):	5.610115448939757
Encrypted:	false
SSDEEP:	6:mzyEYOFLvEWdrIOQ+CxoAt1S/1TK6tr4zyEYOFLvEWdrIOQFXwRt1S/1TK6t9f:WyeRl9At1wJIyeRl2ARt1wLf
MD5:	AAC4A82B150973E7DCB3AD9C0E0C9C0A
SHA1:	7EDCAF6570D5E40B0E6473B34CB5C263CC10E145
SHA-256:	B4E859CE77ABF2FC23D4CE6CA6AFA11EF6DDCB2C55381141A7ED69369D8A8F24
SHA-512:	61AEE93BE374AA172C264551F5D6B632CAD9AE02EAD50892DB1FCCF6FAEE732EBD42B012A1D3CDA5E7997E4440DB4057E6A8BE8C3D53495ED8DDDE14017B9F4C
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...d'../....."#.Dn4j....A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....VQ.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .-f.'../....."#.D.J)....A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....K.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.523417299803233
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0	
SSDEEP:	6:mnYOFLvEWdhwyuC3C1wfwrqwK+41TK6tqj:wRhO1w7wK+EM
MD5:	ADC9CA08A9D3769F9EB351A45832C4DC
SHA1:	BC71783972D4E957C3F6A459D68759FF95F9C307
SHA-256:	0EE958F2E0C23D4DED7F7B92CEBAA341479E74775FC527E7BE8C2B955BE89EBB
SHA-512:	60C2434697599A3DE9EC3707A951624F6D5713E19AC6F800D83CEFFBC87D3A5839D435F346A4C7CA0398E97C9C81D5E791532C489D7EF9304B42B2B261867592
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .e..'../....."#.D:t6....A.....7...o..a=.98I.....(3.$G.A..Eo..... ...A..Eo.....U>\.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	460
Entropy (8bit):	5.574909441382291
Encrypted:	false
SSDEEP:	6:mYXYOFLvEWdrROk/RJbuDqN7K/V9wIfO441TK6tG/2YXYOFLvEWdrROk/RJbuzXd:/RrROk/Ma7K9rfLEQvRrROk/8XrIfLE
MD5:	B324608B24E4D3C8C6C420C40B8C081B
SHA1:	3824F08BCBBDF4AA682FD6045A7891BD949650D9
SHA-256:	C760EBA681103F51F1FB3D7D18C57B1908978695D093393623F3B9213C48FB1E
SHA-512:	B4DB899F1243964D45910FDBDB23DF6FD22167CC25558010BA508DFC6130536499F8BBCC832F911880716EE5C889E4F979E467A40B879CD83A37CD8BA2A943C
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ...d'../....."#.D..j....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo..... .....A..Eo.....c.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..b.'../....."#.D..)....A..~..rw.+[... .!.)?..f.U..(=.=.A..Eo.....A..Eo.....eL.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.582806357092511
Encrypted:	false
SSDEEP:	6:mmDEYOFLvEWXI+PzS1QPLr1TK6tV+mDEYOFLvEWXIhM9S1QPLr1TK6tpFw:xqTTWCPLn7ZqTrSCPLnX6
MD5:	15E276BF73543AACAB5280561C4D377E
SHA1:	B0225570EE173E92EA3F0BCE03B15025B8B017E1
SHA-256:	27F00438314AED2B99F21125550C2F7864456DF969C4D56CF12098069436DC8A
SHA-512:	97CCCC48AA9F4C286FB2A1843B7D81C6BAED0940B3F193E35F5FA0CD40E370F6FA1ABF71EC3669129B1736896F304D838A825635A4B1D647D7FF815EDD0B6F9 A
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .2.`'../....."#.D..Z....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....A@.....0\r..m.....:. ...f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ..v.'../....."#.DEc.....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....KC.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	414
Entropy (8bit):	5.61137373061839
Encrypted:	false
SSDEEP:	6:m52YOFLvEWdMAuUjlsEJ41TK6tD52YOFLvEWdMAuht4ZsEJ41TK6tJl:zRMOsDcRMhusD3l
MD5:	A17957321C961253A8792A0996B04F42
SHA1:	216276DBB0A6DDD1FD50E618E25627F61EEC9754
SHA-256:	6CAA3509942B0053EFADEFF2B974190799CBE1322120809F709611118C8A01F3
SHA-512:	0F63A4152B61E28F0877592CF103FC17128B50E805E7F7E6B41E8EBC2B9C6F5683A8DB62F98C54C572BA4BE70F0141DCA09A45B76104E9946A5CD8C8E7DEE75
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..h'../....."#.D..~....A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....g..... ...0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ....'../....."#.D<.Z....A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo..... ' .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0	
Size (bytes):	420
Entropy (8bit):	5.597368232288721
Encrypted:	false
SSDEEP:	6:mYilPYOFLvEWd8CAdAuTaGTFong1TK6tf/MYilPYOFLvEWd8CAdAu3DPFong1TKA:6lJR6a+FoMxMlJR0DPFoMp
MD5:	A1E36A937D5DADF4C89FE46EFDF15701
SHA1:	9E7FBC7FAD7DD6C4FFDE2C224EECA1386DB84140
SHA-256:	A8CB025417FDB267ACB6E0D8E7F3A52D8F4C421FE656C929FBD3BFC460A644C4
SHA-512:	3D423485D3EC957C1CA3C468A038506B0065EF7514FC2209E0D9B02F9EB645B7A1D825B40673E304E44FF37F2B88135EB538FAD9FF7BE1C3262AFD8F61FE6914
Malicious:	false
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ...h'../....."#.D..~....Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....U~".....0\r..m.....R....\|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..r.'../....."#.DsKZ....Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....y?D.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	446
Entropy (8bit):	5.5968749719835635
Encrypted:	false
SSDEEP:	6:mY8nYOFLvEWdrROk/Iu9ODOe16wG1TK6t1lMY8nYOFLvEWdrROk/IuqHOe16wG1w:F8hRrROk/6Oe2B8hRrROk/8Oe2
MD5:	AC01E414A668F2178DDBF2C1E86CBF6E
SHA1:	E60EC8485777A46E544DD609B96F914D75879286
SHA-256:	870C546F0F6E582107329CE6B86C6AB13821F4892E2EBA307F0D95F50A11D1A2
SHA-512:	F152EBD864F46D959AFD094A7E8C4B89807E427F0B8B3A79B71CF6029672131CCCCA2CDE0E492A890F2E1D3CC4A89E905A9B73070F10B613D5FED443C724ED1
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ...c'../....."#.DB.j....A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....}.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ....'../....."#.D=.(....A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....r4.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	426
Entropy (8bit):	5.682441869271413
Encrypted:	false
SSDEEP:	6:mLrnYOFLvEWdrIoJUQl007atrNJli1TK6tGLrnYOFLvEWdrIoJUQ8yRrNJli1TK8:ehRcW0CErNJlC4hRczyRrNJlCf
MD5:	E1B87821BB473ECBE96614841A6F4E87
SHA1:	846EC39EC41413CA9EAE33B2EA771A75A66E6FD2
SHA-256:	1B6122748B849A598CE31960A9AC24DC413426B5CBA058C5CFC93D455371D066
SHA-512:	48CCF602DC1076791D05360853C829ADD411E35F78DF812CC6486DE52BF03B5B8AFDF4A6B69B739CCCAB5F5CAABB2EE9B716D6BEB710568B715BEDA19A58951
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..d'../....."#.D.-l....A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....b..L.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..i.'../....."#.DV.)....A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....#.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.5570371111666255
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhubyG3m4pZLzgm2d/1TK6tdeOEYOFLvEWdrIhuy7oUpZLzgm2dj:0RhVZRRewRsRRe
MD5:	E7A5869FC4FFE47778D9BFA5ED25C884
SHA1:	270A8FD63D6AF93A8D5E2A5BB16E09FDDA31677F
SHA-256:	DB6E7B748F95A2FA1D2E53EAE4D662573DCC0ADF354D02C34F5E1C9DD8F9CED7
SHA-512:	03F83A4734E2A039A79B50855D74748A51F66189C3FEE8653D3DFEB666E215EF564D07EA8276F8C841D65A6E30F7F0FBC1FDDC2FD61E1D4DBF2DA949A1EE6027
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0	
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ...c'../....."#.D..i....AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo....."....."....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ....'../....."#.D..'....AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....U.L.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	564
Entropy (8bit):	5.669757633374453
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1Kgbukx56uvp1TK6thAElVYOFLvEW1Kzw+l4Okx56uvp1TK6tS9+:6JJKunJJKNl4VlJJKoMS
MD5:	C8311DCDBF51398B5AC7110B316FCCAD
SHA1:	F51C9821A46EDF0E413CE229868D04DF0E41BF3B
SHA-256:	B47D655D3ACCFD7AA05400D528C6943C2DFEE4DA94DB3D74EEDEC95AEB814EBE
SHA-512:	C7ACCE82C09F115FE2555F44482D3B58537F74AE5F6D04F79A56FBF0022488E30AB69DA8557230CFB19255045C8832026CE6D1A1ECAA194B712B7465C9F0EAC
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...'../....."#.D.....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .$.U'../....."#.D..3....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....H.!.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .b.'../....."#.DN.....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....J.D.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.625724643605647
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvu7nUkrhUDLYtmOZn1TK6tv:xRBJ4noDcFZLF
MD5:	86A8D5C6A531F0F4D66DC98D1AA5C9D9
SHA1:	E688C6C27D3FEF519A31701E975FD559E664F060
SHA-256:	9143CB2D5FDC029CD9F8C3AE8264EC1BA5A7BCF44D1DC7D926D9FC90F2B09E1E
SHA-512:	5A770A2A4B636419874D5EF9F812607A313AD336A0261A765B855A7820EDCE937D917E53612A479CA5802C1FAFCD6BAB8E65EC6EDBF07CB15C0CBA8D2B773BA5
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ...'../....."#.D8.Y....A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....h.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	633
Entropy (8bit):	5.661778929580385
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp71VPu1TK6ttsRPYOFLvEWIa7zp7gcnkVPu1TK6tx+sRPYOFw:BPHrcwPHOekcFPHIcu
MD5:	74931E2D5D5F21C7A1E4556342017B29
SHA1:	51E015DE03841F807ABF4320DB1F91F169198770
SHA-256:	258BAC39432E0F9D8033C11302B7E046CABB6AC98327E9E25197AE09A279FBE1
SHA-512:	9A89565F4CF846FD33AD816AF0A060E7797E9820476390AD3028DA2471668B34D0FCD187C22B69A9718613DFDDC24A0F4680469D3DCD4125E25ACFBCCB1E0C
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .. .'../....."#.DV.....A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....p^.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ...R'../....."#.D.&.....A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....~.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .+6.'../....."#.D/2....A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....l.T?.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.567590118692123
Encrypted:	false
SSDEEP:	6:mKPYOFLvEWdENU9Ql+KJGswiM3Y1TK6t:bJRT9m+2wr0

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
MD5:	0EF3C8AF730CA72E162086AB6D52D254
SHA1:	4C00EAF306903107AB9B7A4947D5BA5EB9F3DB25
SHA-256:	3D4717327B8AE6DFB9FD588B3E3E491E25A89EEE04B474268CAA264EC3C8079D
SHA-512:	CB1823E553CFE24E4EC5D010ACB9081111EF85C50B0BD2298E386C938749EC7CA9B0D35D85DC41CE4E0889E0227E151C8D935AAAE8F61D3B138D3C947DD47 41
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ...'../....."#.D.U=....A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.. .....).....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	modified
Size (bytes):	208
Entropy (8bit):	5.610161046443436
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQPOOvIjBRCh/41TK6t:XRc9KOOQDi/E
MD5:	9C3E674919A4C085905ECB3C3D998C08
SHA1:	41781B64366A2C44CE3D8CC7FB2C76E825C27AC8
SHA-256:	D7801E11608841C2A09AAD8A03790BC43A2C327F5DE67A0A50057D1756F7B29E
SHA-512:	2CCA5675B68643895A1B252363755FF59914CA71A1140BC1455922B47F8339E9B569C0591E7D015BE8BFF47B71B80457E386FCF050E5C556C5DA98DD2C6F5A66
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ....'../....."#.D.Pg....APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo. .....dFv.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.567713260073735
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhuv+tVULlF4r1TK6t1X:bs6xRkivLlF4n
MD5:	493DCC03662A0B7D31239FFAD93424E6
SHA1:	DCC84F60B8F8EB5DB84A8383C12990D7F0A4646A
SHA-256:	EA862198BE210CEDB5E13B397C9926A0B218ED65D83B74F94DDDED8B3281B24B
SHA-512:	5B3EB67FBDA8EC2D4D616D1C92719723C5863150872F5C495C73D90178B27339C031483FA05E4D14F3CC225A09263DE524E4311114BC655DC55BCC6ACB98C8F
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .N.e'../....."#.DC.n....A.P...#4..l....5...5..).w.. .h .~..A..Eo.....A..Eo.....|c.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.48093498187934
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvm6KlhECcu1isLK5m1TK5ktBlX:mhYOFLvEWd/aFu46+hEN941TK6t
MD5:	A2E2F68EA758A3FA9BA6EAD7D586296D
SHA1:	6B49D0220A108F922D22602E4161028BC5E0E813
SHA-256:	D31D8695F2E93A2E9C26189B592612C33E10BEBD768521BBB6B96569898D4032
SHA-512:	9EF16613094132AF98E7196813707D773593EAE5547DA613EE6C8D0D4C14C6C733AC025B253E9CFC47B57A4532A7CE5DDFC661037304BA8AC5B6F1AE4073531
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ..x.'../....."#.D..\....A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A ..Eo.....u.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.514153357012957

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0	
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQ7Fq52oBMqVd3G4K41TK6t:2DRuRswpB9Vd2k
MD5:	654536BA5EBE92F3F1D028604F526449
SHA1:	8E7BBD5415907E3B790F8D6976E18F8D1C2D5FAB
SHA-256:	0F424BFF56E3AF4F99D5169D79B33EB071DC0DBF7FBD442C1D0F3CF5E148BB67
SHA-512:	34EDEAA4CE8B932609101D37B8820CFCFE5CF08A5C8B50312F8C064F49030C8A5ABF18A5E3E418014F38764FDD4721F7C8F702CF1E73A556202FBC8E2FC301F
Malicious:	false
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ..B.'../....."#.De.[....A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.. ....g.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.594834305397403
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9Qzl0cJkHNuA424r1TK6t18kqYOFLvEWd8CAd9Qv6+FGHNuAD:+RQk0BH8rnzsRQxsGcrn4
MD5:	DC4C7ED80D38A795A0606EE888E19185
SHA1:	3984A1F7FAD07EA59C34528830829201EE11EEDC
SHA-256:	91218F3A4F9738BE4C15F813290F4F05847B16BE5FC301B1DE955E969FA3A84A
SHA-512:	4912881F09D8AF76226BEE3E30394F4F8D089F5EB5CE9EEF273F61A8CC130AAA18DF1AD242F8AE543E3CB416491877D1386D67A186C7A7F16AB775831C39DF2
Malicious:	false
Preview:	0\r..m.....P...gT...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .yti'../....."#.D.....A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo... ....G).....0\r..m.....P...gT...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .5$.'../....."#.D4.g....A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo..... .....A..Eo.....". .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.570810222625246
Encrypted:	false
SSDEEP:	3:m+lS5Etla8RzYOCGLvHkWBGKuKjXKVRNUp/KPWFvWMOy9Ag2iHio/Mm1TK5ktoY/:moXXYOFLvEWdENUAu32yC8n1TK6to
MD5:	32841D4B75FDEDA20FED58B84F775A18
SHA1:	584473113B95C083158D3DDFCB7F389E8BBC7751
SHA-256:	D19ED05B1247260E1B3BAB340DDF6E5B50BAB635F1D2BCACFE3F9CFE8C8D9C4A
SHA-512:	16C2B7091DB4243BFDE6959BAEE0165CDA1AF044AE38D0ADD5E1620D68A90671CECDC042995BA41DA1742536D5DE32CF4DC46525AB0530CD987FABF73CA95 F5
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .3..'../....."#.D.26....A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....6U .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	442
Entropy (8bit):	5.624581978412246
Encrypted:	false
SSDEEP:	6:mQZYOFLvEWdrROk/VQB7K/5Ck0LmB41TK6tblEQZYOFLvEWdrROk/VQVBLmB41TL:nRrROk/VTnVm1ldRrROk/V6EmD
MD5:	8CC41E9004FD40DFD27072B03F4962AE
SHA1:	4F5AB109220F439A5DAF967F48D4C30081F70F07
SHA-256:	7B7BB7EE0F19B145162F1D0202D445B894B4F1BFAC18E7775D3759CA909BC51D
SHA-512:	13F7A11BCED1227AB3F912A67D206870E0C943C53FC866E655663FF8BCA42C493B3D19756016121712FA38D594196872C91105108399CFF5512A7BE8A09584A2
Malicious:	false
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .F.d'../....."#.D.4m....A ./.ev.....N~..6.b.....$.j;:C...A..Eo..... .....A..Eo.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..p.'../....."#.D..*....A ./.ev.....N~..6.b.....$.j; :C...A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0	
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.578158694938062
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWuit/G+Adm9741TK6tj:qxRcgtu+Adu7E
MD5:	BDCD7D23B2258743E202748249FB74A7
SHA1:	FE7857DB87832DC0B112F009096C6F0BF0ED0365
SHA-256:	703EDE13E7A3BBD989B82D43FAC8F293FF9E4FD690D66E9A212FF47DDBFD1954
SHA-512:	F2F3142B2678D2B1CABC282C26CF3BEA96E4D388CE36A8AC4FB7D9FD576DEBD87A6C91F85C8B525FB598EF900F92FC6EC1947E9EAAD90791A8935D40FB8F5 E8
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ....'../....."#.D..W....A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..E o.....?.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.568327308796968
Encrypted:	false
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFvcW+XCZB6shoq+Nem1TK5ktE9lt:mMOYOFLvEWdwAPVuR+3Jn1TK6tU
MD5:	C8D80D9DA1D24240112F144BF341BFA3
SHA1:	9934570CBCD302235CDFE4C354EBB57E8DAA6928
SHA-256:	04075E1F428601C228E3B827C99D4BE7DBC33BD615459354BD224A9495D0AC68
SHA-512:	38CBE18A2156587B70F073F84C78DF4CE4A414DC331DAD4E1A0F6EB61C19333BBD8892BD07B781B3D13249B72B5A3A584FA63E2F6ADA535D8D063830CBB96B A
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ....'../....."#.D&.5....A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo..... ..7\\.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.6069801701809725
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQ7AUkr2zhcsBXIh1TK6t:mxRBJQSAUkSDB0
MD5:	49FD81AAFED89A4AC63BC03B475BEB42
SHA1:	F571843796CDF0CE543BEAC08ACA943D03C1A6DF
SHA-256:	9CC46F77405F2369685D1A956EABF41A395D375D9BEF81E4450565EF9C7B30A7
SHA-512:	9CE8F99BD2F5C6FF114631E2711E7F61B619E0FA1312FB6BD9AC70C0902DFF078094885AAD003900599FCA27239647062D990BFEFED23D0E4E1C55F8FE709356
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .M..'../....."#.D.q[....A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....N>j .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	456
Entropy (8bit):	5.617343963529279
Encrypted:	false
SSDEEP:	6:msPYOFLvEWdrROk/RJUQt/ac3Me/1TK6tTsPYOFLvEWdrROk/RJUQTysvc3Me/13:3RrROk/s7cgRrROk/s92c
MD5:	321A1C958989E9124F73AF855FAE3E0A
SHA1:	4F79C7A89AA5132D1830BDEDD598C16381160F1C
SHA-256:	A4AADA353F57A5640FE71DD72D31226EB391661E60B59409B916862B47B6CB00
SHA-512:	CC1FF6C655B75812272366A8A5BDFC2A19F2128CBBF568EECBFFEC1F364E8812902EF67A2EB9EF624C4C259483E6ED1137E4FF8C2C634C7C0ECA4F67275D5B 8
Malicious:	false
Preview:	0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .q.d'../....."#.DLkl....A.....9Q].8O.z....=..:.N.{....N{.A..Eo..... .....A..Eo.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .I..'../....."#.D".)....A..... 9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	2016
Entropy (8bit):	5.298320850418362
Encrypted:	false
SSDEEP:	24:YBwGnoTj663MK8mSBzg5PBqPkVHCLenRYM97X5hv9v3YUME9CYx:JGnojTcmSBooPklqp6L5hv9PYu9Cy
MD5:	27EDA708CC9511B05AA69425C8CE6691
SHA1:	4B16F73299479A5F4D7817D0BF5628DDB945C32C
SHA-256:	8407566865FEAF77CC716F3B1FAB562410C9CD1B52A29B1881AD014085F50ECD
SHA-512:	054E52853AFB762D4265EF051967A5AFB06046695591EC69AF020DFBE980F2C3EF6D3B82ED3CB9628AF5D4AC29A3CB9B8693D8C77EA625F5C7AFC50B6EA6BADA
Malicious:	false
Preview:	....U...oy retne....'.....'.....;.y~A.@.....*..@.....oB*@.....#...(@.....k7A.@.....D.4.....[.i..%.....<...W..J@.....,+..._.#@.....J..j.....6<|...@.....A?.2:.....+.{..'.....*)....J:.....2q....@.....P....V@.....+.U.!..V.....P[. q@.....!...0.o.....u\]..q.....@.....*.....o..k.....^.~..z.....o.@.....Gy.'.h.@.....F..=z;.@.....3...@.....v...q..@.....C..M..@.....a....@.....~.,.4>.....&.S.....@..x.....=....m.....;/...@.....q.....MV3.....:..N.A..@.....P{.oy retne

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	298
Entropy (8bit):	5.18646822875509
Encrypted:	false
SSDEEP:	6:m1zUIq2PN72nKuAl9OmbnIFUtpkzCZZmwPkzPkwON72nKuAl9OmbjLJ:SvVaHAahFUtpp/PO5OaHAaSJ
MD5:	2673F1A5497DCA4FEAEE64E4DBA108B7
SHA1:	4581CC93D4BB555EFA07D655AE61B635D7C690DE
SHA-256:	C64D90B5D467F2C98AD493CC00A603E31135C8611EDEC8C7AF48CD21E91A8754
SHA-512:	A77430CFAEDB1D9CBA566B3ED764037D2449E5713F5E6A3CF8FA6315B52879E4968D07C1059C7B5AFC3B46F3ABC7547FA98D471BB0EF4294765776246852688
Malicious:	false
Preview:	2021/04/08-12:15:24.714 1774 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/04/08-12:15:24.716 1774 Recovering log #3.2021/04/08-12:15:24.717 1774 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	917504
Entropy (8bit):	0.007716873612814605
Encrypted:	false
SSDEEP:	24:T+X8I5mv+X8I5mv+X8I5myrY5mrY5mmHY5mmHY5mm:To35Oo35Oo3525T5K5K5
MD5:	545783574F55AE7B68107D94104DF5DC
SHA1:	A165613C78A951FE14CC2DE4C0119545FB09CB97
SHA-256:	4FD5A8538D675D352B60CCF8E1EE7BC3A43F35696354EAFF170465BBD8D6D2B0
SHA-512:	8E235F34944EF6299185ACA3691FA27C31BD81110EE08898801A333A0D4C6F89D398AAC6AEC54C1CAA649C592C3F9F008DF7124C216A0AFEAC8087AB2DC00B9A
Malicious:	false
Preview:	VLnk.....?.....`.N.7..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-2104081915182-254.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 107 x -152 x 32
Category:	dropped
Size (bytes):	65110
Entropy (8bit):	2.308739914604857
Encrypted:	false
SSDEEP:	192:lUzgM3fdU9rd/pIpotZ0deVfa0hLSPOhqLjo4jb6FeiRzHh/uKl+0fr5qta+OOfr:KiS0d6M+P6FvBHxN14/sMCsNj
MD5:	7CAFDE4EA3C84220C4E669A1D2DA08D2
SHA1:	16588A00CCAEB9D616DBC1B7BB885EA2AC189AEB
SHA-256:	C7B3A1B95190596236F26A416CD32B0F40C80D819BAA8EC148E9872FB361365E

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210408191518Z-254.bmp	
SHA-512:	E116DEF7BF4391BE0B7656C1E917AE17FBD57DAB6793CF3C1492842DEF5F987B11AC63D94F17257EFCEBA463117243FB964FF2913360E90ADD11137D8EDEABD
Malicious:	false
Preview:	BMV.....6...(...k...h..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3024000
Category:	modified
Size (bytes):	32768
Entropy (8bit):	3.3872651543384076
Encrypted:	false
SSDEEP:	96:iR49IVXEBodRBkQcOhFVCsL49IVXEBodRBkRrcOhAVCs749IVXEBodRBklrcOhxn:iGedRBUedRBKedRBFedRBD
MD5:	1AEEE96A71BE7C2DC794D08F8B65678C
SHA1:	8E1E1F86E9D4328439EC07EF38808636FEE4943D
SHA-256:	7B638E5EA9E02FCA33DB5CB2919F11CB2F99819CB5272E6DF854AC3506AC95F0
SHA-512:	508E640F11628A2736BF6776D2061F35B7BE6E405974710EC97F9302FE1F437704882BDC468340FCF3607FDE581D71F5B9E93C87D7042B1C8D9A0C571A707A9B
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....1.....T...U.1.D..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	34928
Entropy (8bit):	3.200004728622764
Encrypted:	false
SSDEEP:	96:Y7OhFVCPX9v949IVXEBodRBkkcOhFVCsSLR49IVXEBodRBk/rcOhAVCsjd49IVXH:YbNiedRBaLGedRB7CedRBryedRB1
MD5:	BEC63880ACFCFCACB2AA5B5857830AB0
SHA1:	14BD9DC588CEECC301E79F33BDF754C4653FFBCB
SHA-256:	3B880DE069F85AE02E3ABEE7C0F96A17CB9EBE7D84C0EDC6B740CDA43C6AD30E
SHA-512:	F49F52F40FA498B7A46BE5A67E1489A7414508470CAFA0829E338C426AD4191937396E6F003C78DD558E93C85A5DFB611DC67ACF65D433FC29FD7A10F4496613
Malicious:	false
Preview:	.....=..... .....X.. .h...y..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.2200	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	157443
Entropy (8bit):	5.172039478677
Encrypted:	false
SSDEEP:	1536:amNTjRlaRlQShhp2VpMKRhWa11quVJzlzofqG9Z0ADWp1ttawvayKLWbVG3+2:RNj3aRlQShhp2VpMKRhWa11quVJX2
MD5:	A2C6972A1A9506ACE991068D7AD37098
SHA1:	BF4D2684587CF034BCFC6F74CED551F9E5316440
SHA-256:	0FB687D20C49DDBADD42ABB489C3B492B5A1893352E2F4B6AA1247EFE7363F65
SHA-512:	4D03884CA5D1652A79E6D55D8F92F4D138C47D462E05C3E6A685DA6742E98841D9C63720727203B913A179892C413BFB33C05416E1675E0CF80DA98BE90BA5E4
Malicious:	false
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Marlett.FamilyName:Marlett.StyleName:Regular.MenuName:Marlett.StyleBits:0.WeightClass:500.WidthClass:5.AngleClass:0.FullName:Marlett.WritingScript:Roman.WinName:Marlett.FileLength:27724.NameArray:0,Win,1,Marlett.NameArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleName:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength:1036584.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-BoldMT.FamilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.FullName:Arial Bold.WritingScript:Roman.WinName:Arial Bold.FileLength:980756.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial Bold.NameAr

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	63598
Entropy (8bit):	5.433041226997456
Encrypted:	false
SSDEEP:	768:PCbGNFYGpiyVFiCUZ580DPHhph04VFrJ0ksUtNryIYyu:J0GpiyVFiB580bHhppFrW98K
MD5:	9A84047E9C495B0F1A4F1C8C15ECD091
SHA1:	0EA42385B524A56F5094539893215868B40DD448
SHA-256:	7D77DCA41F62F9607B87A1F90FDB12ED01AC0534BAE25E3826612F62A0533722
SHA-512:	9D977D220FCE94D8480F36C3FDE3CE1DE0AF64A6D0A69872C2ED1E85924C8DC1D03BCAF24CA2ABB5403A9F26035FF05E7C37E3231A0AE9DEE8FB06EEECD5 84C
Malicious:	false
Preview:	4.382.88.FID.2:o:.....:F:AgencyFB-Reg.P:Agency FB.L:$....."F:Agency FB.#.94.FID.2:o:.....:F:AgencyFB-Bold.P:Agency FB Bold.L:%....." F:Agency FB.#.82.FID.2:o:.....:F:Algerian.P:Algerian.L:$.....RF:Algerian.#.93.FID.2:o:.....:F:ArialNarrow.P:Arial Narrow.L:$....."F:Arial Narr ow.#.107.FID.2:o:.....:F:ArialNarrow-Italic.P:Arial Narrow Italic.L:$....."F:Arial Narrow.#.103.FID.2:o:.....:F:ArialNarrow-Bold.P:Arial Narrow Bold.L:%..... ....."F:Arial Narrow.#.116.FID.2:o:.....:F:ArialNarrow-BoldItalic.P:Arial Narrow Bold Italic.L:%....."F:Arial Narrow.#.75.FID.2:o:.....:F:ArialMT.P:Arial .L:$....."F:Arial.#.89.FID.2:o:.....:F:Arial-ItalicMT.P:Arial Italic.L:$....."F:Arial.#.85.FID.2:o:.....:F:Arial-BoldMT.P:Arial Bold.L:$..... "F:Arial.#.98.FID.2:o:.....:F:Arial-B

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe.log	
Process:	C:\Users\user\Desktop\DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1402
Entropy (8bit):	5.338819835253785
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4bE4K5AE4Kzr7K84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoesX3:MIHK5HKXE1qHbHK5AHKzvKviYHKhQnoe
MD5:	F2152F0304453BCFB93E6D4F93C3F0DC
SHA1:	DD69A4D7F9F9C8D97F1DF535BA3949E9325B5A2F
SHA-256:	5A4D59CD30A1AF620B87602BC23A3F1EFEF792884053DAE6A89D1AC9AAD4A411
SHA-512:	02402D9EAA2DF813F83A265C31D00048F84AD18AE23935B428062A9E09B173B13E93A3CACC6547277DA6F937BBC413B839620BA600144739DA37086E03DD8B4F
Malicious:	**true**
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, PublicKeyT oken=b77a5c561934e089",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.303 19_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b0 3f5f7f11d50a3a",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.Co

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:MLUE4K5E4Ks2E1qE4bE4K5AE4Kzr7K84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoesX3:MIHK5HKXE1qHbHK5AHKzvKviYHKhQnoe
MD5:	F2152F0304453BCFB93E6D4F93C3F0DC
SHA1:	DD69A4D7F9F9C8D97F1DF535BA3949E9325B5A2F
SHA-256:	5A4D59CD30A1AF620B87602BC23A3F1EFEF792884053DAE6A89D1AC9AAD4A411
SHA-512:	02402D9EAA2DF813F83A265C31D00048F84AD18AE23935B428062A9E09B173B13E93A3CACC6547277DA6F937BBC413B839620BA600144739DA37086E03DD8B4F
Malicious:	false
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, PublicKeyT oken=b77a5c561934e089",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.303 19_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b0 3f5f7f11d50a3a",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.Co

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Process:	C:\Users\user\Desktop\DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Size (bytes):	41064
Entropy (8bit):	6.164873449128079
Encrypted:	false
SSDEEP:	384:FtpFVLK0MsihB9VKS7xdgE7KJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+sPZTd:ZBMs2SqdD86Iq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe, Detection: malicious, Browse • Filename: DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.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_6620200947535257662_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 • Filename: QUOTATIONs#280321_RFQ_PRODUCTS_ENQUIRY_TRINITY_VIETNAM_CO.exe, Detection: malicious, Browse • Filename: RFQ9088QTY.exe, Detection: malicious, Browse
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\DHL Overdue Account Notice - 1301356423.PDF	
Process:	C:\Users\user\AppData\Roaming\Files.exe
File Type:	PDF document, version 1.3
Category:	dropped
Size (bytes):	149430
Entropy (8bit):	5.992880402670265
Encrypted:	false
SSDEEP:	1536:WXGnpGkkQ5KXOAEM3pqfGkkQ5KXO3GkkQ5KXOJa+Ur+KFg+jBfMev0CSrSmq:WXMFAEMOrJRUSTC
MD5:	CBAF67B05E781DEE65A10D6459DA8E2F
SHA1:	29E06F15D8D14745EEEBA6F9EC502FFC3F4B27B4
SHA-256:	BC4D8009C636CCCA89801D5FCEA5BA5370070B9F0777B11B1B0AF46A61D8BAB5
SHA-512:	5389614083FE85074EE0A266BA4E8867A69D5A84AE834ECBF7A7C85503313FD223297A6638C9532B7C3F5D58447FCDFABF63CD09E02B2130631AFF8E45D0C52E
Malicious:	false
Preview:	%PDF-1.3..%.....%RSTXPDF3 Parameters: DJRSTXh..%Devtype ZPDFUC Font HELVE normal Lang EN Script: 0 ->/C001..2 0 obj..<<../Type /FontDescriptor. ./Ascent 718../CapHeight 718../Descent -207../Flags 32../FontBBox [-166 -225 1000 931]../FontName /Helvetica../ItalicAngle 0../StemV 105..>>..endobj..3 0 obj../ WinAnsiEncoding..endobj..4 0 obj..<<../Type /Font../Subtype /Type1../BaseFont /Helvetica../Name /C001../Encoding 3 0 R../Widths..[0275 0275 0354 0554 0554 0888 0667 0192 0333 0333 0388 0583 0275 0333 0275 0275 0554 0554 0554 0554 0554 0554 0554 0554 0554 0554 0554 0554 0275 0275 0583 0583 0583 0554 1017 0667 0667 0721 0721 0667 0608 0775 0721 0275 0500 0667 0554 0833 0721 0775 0667 0775.. 0721 0667 0608 0721 0667 0942 0667 0667 0608 0275 0275 0275 0471 0554 0333 0554 0554 0500 0554 0554 0275 0554 0554 0221 0221 0500 0221 0833 0554 0554 0554 0554 0333 0500 0275 0554 0500 0721 0500 0500 0500 0333 0258 0333 0583].. /FirstChar 32../LastChar 126../FontDescriptor 2 0 R..>>..endobj..%Devtype ZPDFUC

C:\Users\user\AppData\Roaming\Files.exe	
Process:	C:\Users\user\Desktop\DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	885248
Entropy (8bit):	6.568125199548058
Encrypted:	false
SSDEEP:	12288:FRTnpIV1Fn6OAVo1TgtJM8RgakW010CjZH+TqUXHImiN+cHK25HJP+rXU:e65o1mMCTv01LVH+OUXHjiN+OK254rU
MD5:	56796A808359F3EACD3DFAE75E530C7F
SHA1:	2A640C1CEDA881FC552148022FA5CD69DF349884
SHA-256:	966F5FDA32AC9AD436CDEB47D024FB831705D8E14FA83EE74A48483260871EC2
SHA-512:	79FAB6BDFD6713F2670A0647F266F10CFCA7D115698EC0C3A49DA01865C95DF10EA2DC3278D607DCFB81C344D82D659E8AB253895252B269B428FB5FEA09B3E2

C:\Users\user\AppData\Roaming\Files.exe	
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 21%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...~/.E..... .....@.. ....`.....O..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....V...I.....F....A..B.....O.O.O.F6d.B.pixM.ZM^R.F.dgB.pIxS.2M.R.F6d.B.pcxU.XMaR.F)d&B.p&xU.7MtR.F d.B`.e.a.l.....,.*....#....f....\.....,.3y'...#z.....,.3y'...#o.....,.38'...#D.....,.3;'...#g.....,.3.'...#z.....,.3u'...#K.....,.3.'...#y.....>@641..i.m.k.h.....b...>.....Z.....d....l..... .....b.....9./.1.....1.....)....E.....!.....6..b.b.b.]9U1Rm`...kUI~o.]

C:\Users\user\AppData\Roaming\Files.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.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**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.568125199548058
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_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe
File size:	885248
MD5:	56796a808359f3eacd3dfae75e530c7f
SHA1:	2a640c1ceda881fc552148022fa5cd69df349884
SHA256:	966f5fda32ac9ad436cdeb47d024fb831705d8e14fa83ee74a48483260871ec2
SHA512:	79fab6bdfd6713f2670a0647f266f10cfca7d115698ec0c3a49da01865c95df10ea2dc3278d607dcfb81c344d82d659e8ab253895252b269b428fb5fea09b3b2
SSDEEP:	12288:FRTnpIV1Fn6OAVo1TgtJM8RgakW010CjZH+TqUXHImiN+cHK25HJP+rXU:e65o1mMCTv01LVH+OUXHjiN+OK254rU
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...~/.E..... .....@.. ..... `.....

File Icon

Icon Hash:	eaee8e96b2a8e0b2

Static PE Info

General	
Entrypoint:	0x4cc3ee
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:	0x45A02F7E [Sat Jan 6 23:23:42 2007 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
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xcc39c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xce000	0xd8ce	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0xca3f4	0xca400	False	0.618625183483	data	6.59017232026	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xce000	0xd8ce	0xda00	False	0.0915997706422	data	3.77392773799	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	0x378	data		
RT_MANIFEST	0xdb6e4	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 1995 =<J2I?@7679HG9E:
Assembly Version	1.0.0.0
InternalName	ADEHL.exe
FileVersion	2.3.4.5
CompanyName	=<J2I?@7679HG9E:
Comments	J;>@G:J<IF4@46=G2
ProductName	E39@C?GE45CJFEDF@;G7I79
ProductVersion	2.3.4.5
FileDescription	E39@C?GE45CJFEDF@;G7I79
OriginalFilename	ADEHL.exe

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:13:44.692187071 CEST	55074	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:13:44.710947990 CEST	53	55074	8.8.8.8	192.168.2.6
Apr 8, 2021 12:13:48.461441994 CEST	54513	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:13:48.474347115 CEST	53	54513	8.8.8.8	192.168.2.6
Apr 8, 2021 12:13:54.786256075 CEST	62044	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:13:54.799201012 CEST	53	62044	8.8.8.8	192.168.2.6

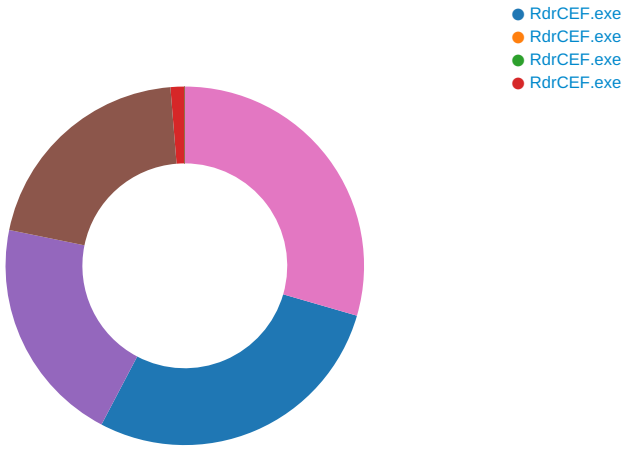
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:13:55.064605951 CEST	63791	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:13:55.091429949 CEST	53	63791	8.8.8.8	192.168.2.6
Apr 8, 2021 12:13:55.127460003 CEST	64267	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:13:55.154321909 CEST	53	64267	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:02.664515018 CEST	49448	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:02.677510977 CEST	53	49448	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:03.444828033 CEST	60342	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:03.457454920 CEST	53	60342	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:04.427092075 CEST	61346	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:04.442265987 CEST	53	61346	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:05.075366974 CEST	51774	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:05.089565992 CEST	53	51774	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:17.357986927 CEST	56023	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:17.370615005 CEST	53	56023	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:17.941585064 CEST	58384	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:17.956495047 CEST	53	58384	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:18.010484934 CEST	60261	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:18.024709940 CEST	53	60261	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:18.872725964 CEST	56061	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:18.885907888 CEST	53	56061	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:19.562911987 CEST	58336	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:19.576028109 CEST	53	58336	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:20.221409082 CEST	53781	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:20.234348059 CEST	53	53781	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:20.796654940 CEST	54064	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:20.817250013 CEST	53	54064	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:20.927850962 CEST	52811	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:20.940795898 CEST	53	52811	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:22.236346960 CEST	55299	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:22.249532938 CEST	53	55299	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:23.012193918 CEST	63745	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:23.025168896 CEST	53	63745	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:24.099628925 CEST	50055	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:24.112262964 CEST	53	50055	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:25.082479000 CEST	61374	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:25.095473051 CEST	53	61374	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:26.410445929 CEST	50339	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:26.422473907 CEST	53	50339	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:31.304470062 CEST	63307	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:31.330244064 CEST	53	63307	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:31.579363108 CEST	49694	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:31.605487108 CEST	53	49694	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:31.624037981 CEST	54982	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:31.636534929 CEST	53	54982	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:35.991292000 CEST	50010	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:36.004492044 CEST	53	50010	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:36.305973053 CEST	63718	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:36.318394899 CEST	53	63718	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:36.327076912 CEST	62116	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:36.339858055 CEST	53	62116	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:40.349153042 CEST	63816	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:40.362489939 CEST	53	63816	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:42.946789980 CEST	55014	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:43.036472082 CEST	53	55014	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:43.584944963 CEST	62208	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:43.598397017 CEST	53	62208	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:44.048079014 CEST	57574	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:44.215498924 CEST	53	57574	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:44.900172949 CEST	51818	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:44.913167000 CEST	53	51818	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:45.333678007 CEST	56628	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:45.507448912 CEST	53	56628	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:46.604232073 CEST	60778	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:46.617578030 CEST	53	60778	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:14:47.196903944 CEST	53799	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:47.223007917 CEST	53	53799	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:47.439229012 CEST	54683	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:47.524363041 CEST	53	54683	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:48.379645109 CEST	59329	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:48.393110991 CEST	53	59329	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:48.917035103 CEST	64021	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:48.929457903 CEST	53	64021	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:49.927990913 CEST	56129	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:49.942594051 CEST	53	56129	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:50.279433012 CEST	58177	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:50.292776108 CEST	53	58177	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:50.293411016 CEST	50700	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:50.306689978 CEST	53	50700	8.8.8.8	192.168.2.6
Apr 8, 2021 12:14:54.429207087 CEST	54069	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:14:54.450268984 CEST	53	54069	8.8.8.8	192.168.2.6
Apr 8, 2021 12:15:24.995263100 CEST	61178	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:15:25.013184071 CEST	53	61178	8.8.8.8	192.168.2.6
Apr 8, 2021 12:15:25.214766979 CEST	57017	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:15:25.233650923 CEST	53	57017	8.8.8.8	192.168.2.6
Apr 8, 2021 12:15:25.339226961 CEST	56327	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:15:25.380691051 CEST	53	56327	8.8.8.8	192.168.2.6
Apr 8, 2021 12:15:25.998588085 CEST	61178	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:15:26.016844034 CEST	53	61178	8.8.8.8	192.168.2.6
Apr 8, 2021 12:15:26.201585054 CEST	57017	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:15:26.214500904 CEST	53	57017	8.8.8.8	192.168.2.6
Apr 8, 2021 12:15:27.045583963 CEST	61178	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:15:27.058372021 CEST	53	61178	8.8.8.8	192.168.2.6
Apr 8, 2021 12:15:27.248514891 CEST	57017	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:15:27.261347055 CEST	53	57017	8.8.8.8	192.168.2.6
Apr 8, 2021 12:15:29.092494965 CEST	61178	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:15:29.106081009 CEST	53	61178	8.8.8.8	192.168.2.6
Apr 8, 2021 12:15:29.288110971 CEST	57017	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:15:29.306121111 CEST	53	57017	8.8.8.8	192.168.2.6
Apr 8, 2021 12:15:33.144721031 CEST	61178	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:15:33.157649994 CEST	53	61178	8.8.8.8	192.168.2.6
Apr 8, 2021 12:15:33.337380886 CEST	57017	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:15:33.350656033 CEST	53	57017	8.8.8.8	192.168.2.6
Apr 8, 2021 12:15:36.228770018 CEST	50243	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:15:36.242151976 CEST	53	50243	8.8.8.8	192.168.2.6
Apr 8, 2021 12:15:40.901048899 CEST	62055	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:15:40.927284002 CEST	53	62055	8.8.8.8	192.168.2.6

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process:
DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe
PID: 6572 Parent PID: 5880

General

Start time:	12:13:51
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe'
Imagebase:	0xaf0000
File size:	885248 bytes
MD5 hash:	56796A808359F3EACD3DFAE75E530C7F
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: 00000000.00000002.420461900.000000000411A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.420573412.00000000041C8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.420839951.000000000438E000.00000004.00000001.sdmp, Author: Joe Security
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	6E0ECF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6E0ECF06	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	6DB6EEB	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	6DB6EEB	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	6DB6EEB	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3FC78D	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 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 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 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 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L....Z.Z..... ....0..T.....r... .....@.. ....`.....	success or wait	1	6DB6EEB	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 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 7e 2f a0 45 00 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 a4 0c 00 00 dc 00 00 00 00 00 00 ee c3 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...~/.E.......... ....@.. ....`................	success or wait	4	6DB6EEB	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	6DB6EEB	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL_Express_Shipments_Invoice_Confirmation_CBJ190517000131_74700456XXX.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	6E3FC907	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	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0C5705	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	6E0203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0CCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF31B4F	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: 6884 Parent PID: 6572

General

Start time:	12:14:10
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:	0x2a0000
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: 6892 Parent PID: 6884

General

Start time:	12:14:11
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 6920 Parent PID: 6884

General

Start time:	12:14:11
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:	0xa60000
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	A65A1D	RegSetValueExW

Analysis Process: Files.exe PID: 6184 Parent PID: 3440

General

Start time:	12:14:28
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:	0x780000
File size:	885248 bytes
MD5 hash:	56796A808359F3EACD3DFAE75E530C7F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 21%, 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	6E0ECF06	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	6E0ECF06	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	6E3FC78D	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	6E3FC907	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	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0C5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0CCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF31B4F	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: 6484 Parent PID: 6572

General

Start time:	12:14:32
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:	0xd30000
File size:	885248 bytes
MD5 hash:	56796A808359F3EACD3DFAE75E530C7F
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: 0000000E.00000002.618305567.000000000436D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.617790683.00000000041A7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.617678751.00000000040F8000.00000004.00000001.sdmp, Author: Joe Security
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	6E0ECF06	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	6E0ECF06	unknown
C:\Users\user\AppData\Roaming\DHL Overdue Account Notice - 1 301356423.PDF	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF31E60	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\DHL Overdue Account Notice - 1301356423.PDF	unknown	149430	25 50 44 46 2d 31 2e 33 0d 0a 25 e2 e3 cf d3 0d 0a 25 52 53 54 58 50 44 46 33 20 50 61 72 61 6d 65 74 65 72 73 3a 20 44 4a 52 53 54 58 68 0d 0a 25 44 65 76 74 79 70 65 20 5a 50 44 46 55 43 20 20 20 46 6f 6e 74 20 48 45 4c 56 45 20 20 20 20 6e 6f 72 6d 61 6c 20 4c 61 6e 67 20 45 4e 20 53 63 72 69 70 74 3a 20 20 30 20 2d 3e 2f 43 30 30 31 0d 0a 32 20 30 20 6f 62 6a 0d 0a 3c 3c 0d 0a 2f 54 79 70 65 20 2f 46 6f 6e 74 44 65 73 63 72 69 70 74 6f 72 0d 0a 2f 41 73 63 65 6e 74 20 37 31 38 0d 0a 2f 43 61 70 48 65 69 67 68 74 20 37 31 38 0d 0a 2f 44 65 73 63 65 6e 74 20 2d 32 30 37 0d 0a 2f 46 6c 61 67 73 20 33 32 0d 0a 2f 46 6f 6e 74 42 42 6f 78 20 5b 2d 31 36 36 20 2d 32 32 35 20 31 30 30 30 20 39 33 31 5d 0d 0a 2f 46 6f 6e 74 4e 61 6d 65 20 2f 48 65 6c 76 65 74	%PDF-1.3..%.....%RSTXPDF3 Parameters: DJRSTXh..%Devtype ZPD FUC Font HELVE normal Lang EN script: 0 ->/C001..2 0 obj..<<../Type /FontDescr<wbr>iptor../Ascent 718../CapHeight 718../Descent -207../Flags 32../FontBBox [-166 -225 1000 931]../FontName /Helvet	success or wait	1	6CF31B4F	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	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0C5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0CCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF31B4F	ReadFile

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: AcroRd32.exe PID: 5488 Parent PID: 6484

General

Start time:	12:15:08
Start date:	08/04/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true

Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\AppData\Roaming\DHL Overdue Account Notice - 1301356423.PDF'
Imagebase:	0x1330000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx	read data or list directory | read attributes | write attributes | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	13665C3	CreateDirectoryExW
C:\Users\user\AppData\Local\Temp\acrocef_low	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	138AE05	CreateDirectoryW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.2200	write data or add file | append data or add subdirectory or create pipe instance | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	137EA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock5488.1.643841821.tmp	read data or list directory | read ea | read attributes | delete | read control | synchronize	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	13B2657	CreateFileW
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	success or wait	1	137EA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210408191518Z-254.bmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	137EA85	NtCreateFile
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	13F83C8	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13F83C8	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13F83C8	HttpSendRequestA

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	13F83C8	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13F83C8	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13F83C8	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1wgyjdf_c0mwgf_1p4.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	137EA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	4	137EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R12m6lka_c0mwgg_1p4.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	137EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1tp87kq_c0mwgh_1p4.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	137EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rq1kxua_c0mwgi_1p4.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	137EA85	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R19dssv0_c0mwgj_1p4.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	137EA85	NtCreateFile

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.2200	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst	success or wait	1	13BD405	NtSetInformationFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\System\Acrobatbrokerserverdispatchercpp789	success or wait	1	137CF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	137D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	137D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo	success or wait	1	137D41D	NtCreateKey

Analysis Process: AcroRd32.exe PID: 2200 Parent PID: 5488

General

Start time:	12:15:09
Start date:	08/04/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\AppData\Roaming\DHL Overdue Account Notice - 1301356423.PDF'
Imagebase:	0x1330000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: InstallUtil.exe PID: 1208 Parent PID: 6484

General

Start time:	12:15:09
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Imagebase:	0x8e0000

File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
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: 00000015.00000002.604942356.0000000002D01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000015.00000002.604942356.0000000002D01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000015.00000002.593141973.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

Analysis Process: RdrCEF.exe PID: 6524 Parent PID: 5488

General

Start time:	12:15:16
Start date:	08/04/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043
Imagebase:	0xf10000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RdrCEF.exe PID: 5372 Parent PID: 6524

General

Start time:	12:15:19
Start date:	08/04/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1712,240186317792708 4696,18206753643728564179,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=7717275198719545956 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=7717275198719545956 --renderer-client-id=2 --mojo-platform-channel-handle=1724 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xf10000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RdrCEF.exe PID: 5424 Parent PID: 6524

General

Start time:	12:15:22
Start date:	08/04/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1712,2401863177927084696,18206753643728564179,131072 --disable-features=VizDisplayCompositor --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --lang=en-US --gpu-preferences=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=14898531479645788559 --mojo-platform-channel-handle=1744 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0xf10000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RdrCEF.exe PID: 5720 Parent PID: 6524

General

Start time:	12:15:24
Start date:	08/04/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1712,2401863177927084696,18206753643728564179,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=9725964129438127640 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=9725964129438127640 --renderer-client-id=4 --mojo-platform-channel-handle=1816 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xf10000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RdrCEF.exe PID: 3120 Parent PID: 6524

General

Start time:	12:15:27
Start date:	08/04/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true

Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1712,240186317792708 4696,18206753643728564179,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=2964269592299071020 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=2964269592299071020 --renderer-client-id=5 --mojo-platform-channel-handle=2148 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xf10000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis