ID: 383902
Sample Name:
DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe
Cookbook: default.jbs
Time: 12:06:34
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

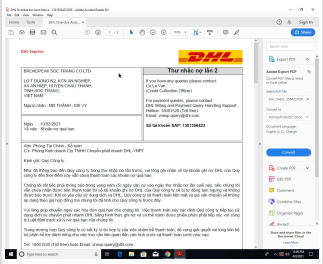
Analysis Report DHL_Express_Shipment_Invoice_Confi…

Overview

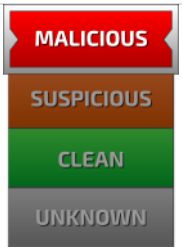
General Information

Sample Name:	DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe
Analysis ID:	383902
MD5:	4ffb9ee56baeed6..
SHA1:	2982ad3dd5578b..
SHA256:	79614387d51e43..
Tags:	DHL exe
Infos:	

Most interesting Screenshot:



Detection



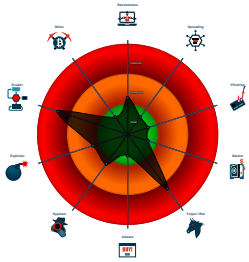
AgentTesla

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…
- 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…
- Contains functionality to access load…

Classification



Startup

- **System is w10x64**
- DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe (PID: 5644 cmdline: 'C:\Users\user\Desktop\DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe' MD5: 4FFB9EE56BAEED64D186D62DE5C56A05)
  - cmd.exe (PID: 5784 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: 5056 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - reg.exe (PID: 5424 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: 6860 cmdline: 'C:\Users\user\AppData\Roaming\Files.exe' MD5: 4FFB9EE56BAEED64D186D62DE5C56A05)
    - AcroRd32.exe (PID: 5288 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: 5336 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: 4880 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
        - RdrCEF.exe (PID: 5024 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=1732,14640126625900119066,9769525679105844933,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=2690794570082519975 --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=2690794570082519975 --renderer-client-id=2 --mojo-platform-channel-handle=1724 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
        - RdrCEF.exe (PID: 5632 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1732,14640126625900119066,9769525679105844933,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=7685701926627287920 --mojo-platform-channel-handle=1752 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
        - RdrCEF.exe (PID: 6736 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=1732,14640126625900119066,9769525679105844933,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=6749621257665537764 --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=6749621257665537764 --renderer-client-id=4 --mojo-platform-channel-handle=1852 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
        - RdrCEF.exe (PID: 6852 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=1732,14640126625900119066,9769525679105844933,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=7499266669204803197 --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=7499266669204803197 --renderer-client-id=5 --mojo-platform-channel-handle=1864 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
        - RdrCEF.exe (PID: 1332 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=1732,14640126625900119066,9769525679105844933,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=6985995476041547175 --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=6985995476041547175 --renderer-client-id=6 --mojo-platform-channel-handle=2148 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - InstallUtil.exe (PID: 5248 cmdline: C:\Users\user\AppData\Local\Temp\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
- Files.exe (PID: 6804 cmdline: 'C:\Users\user\AppData\Roaming\Files.exe' MD5: 4FFB9EE56BAEED64D186D62DE5C56A05)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.310359944.000000000425A000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.311089829.0000000004309000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000014.00000002.509008335.0000000003A9F000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.311979523.000000000044CF000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
0000001A.00000002.493944777.00000000034C1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 4 entries				

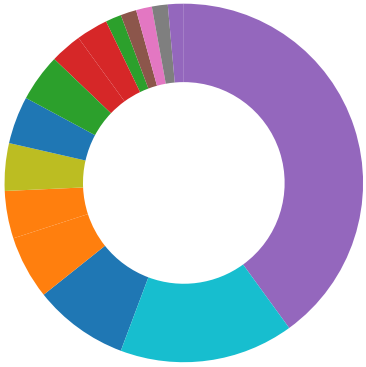
Unpacked PEs

Source	Rule	Description	Author	Strings
20.2.Files.exe.382ae38.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
20.2.Files.exe.3a9f6da.7.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe.436444a.5.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe.44cf3fa.6.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe.44cf3fa.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 16 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

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

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:

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

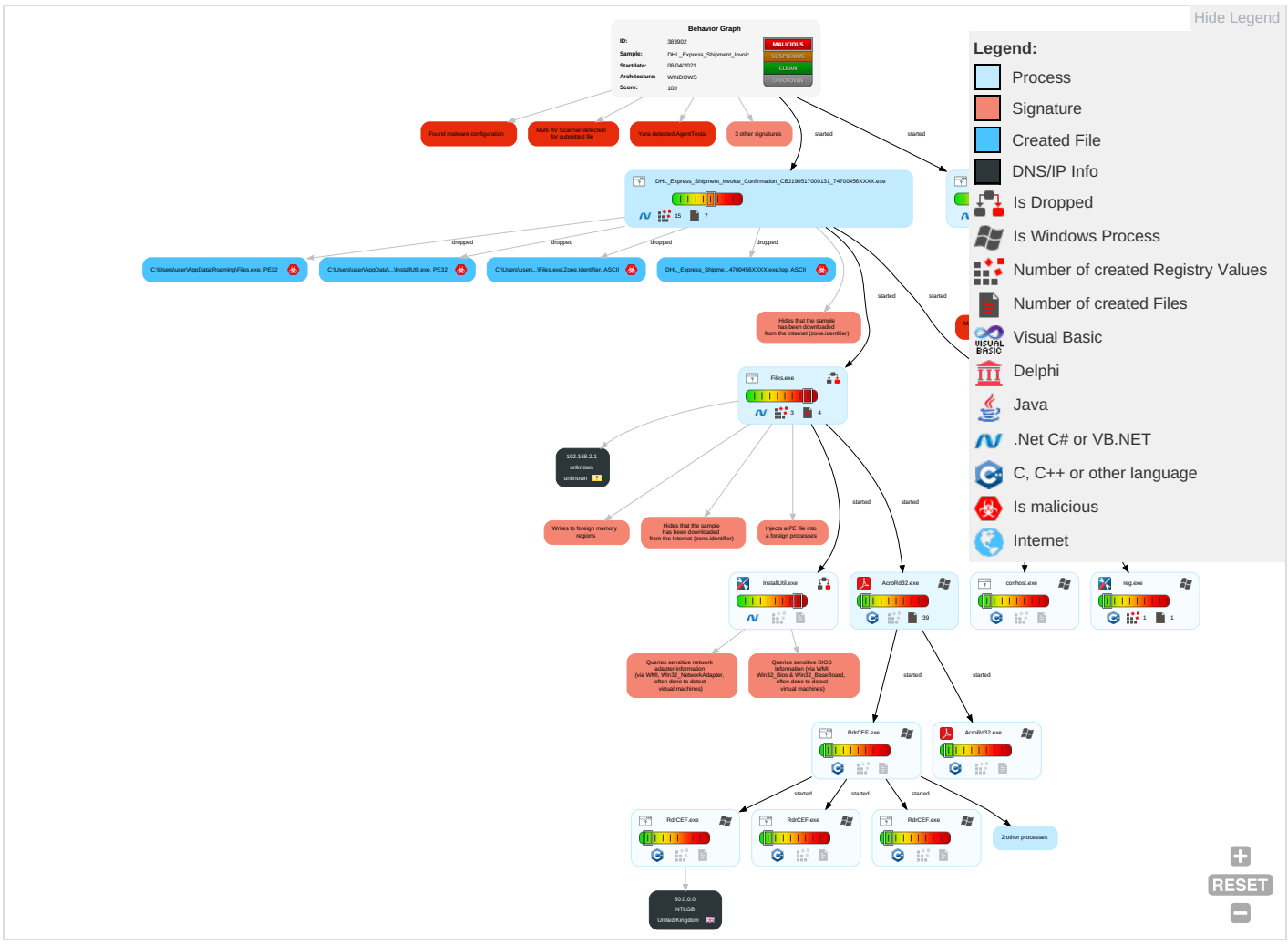
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co an
Valid Accounts 1	Windows Management Instrumentation 2 1 1	Valid Accounts 1	Valid Accounts 1	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	En Cl
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	Data from Removable Media	Exfiltration Over Bluetooth	Ju
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 2 1 2	Modify Registry 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	St
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	Pr Im
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Disable or Modify Tools 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fa Ch
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4 1	Cached Domain Credentials	Account Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mu Co
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 2 1 2	DCSync	System Owner/User Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Co Us
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Ap La
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Obfuscated Files or Information 2	/etc/passwd and /etc/shadow	File and Directory Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	W
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Software Packing 1	Network Sniffing	System Information Discovery 1 1 3	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Fil Pr

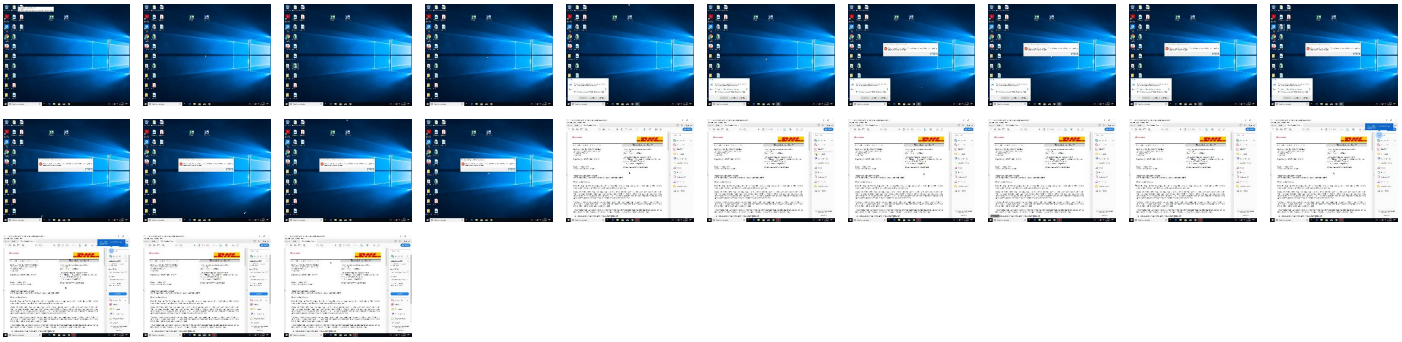
Behavior Graph

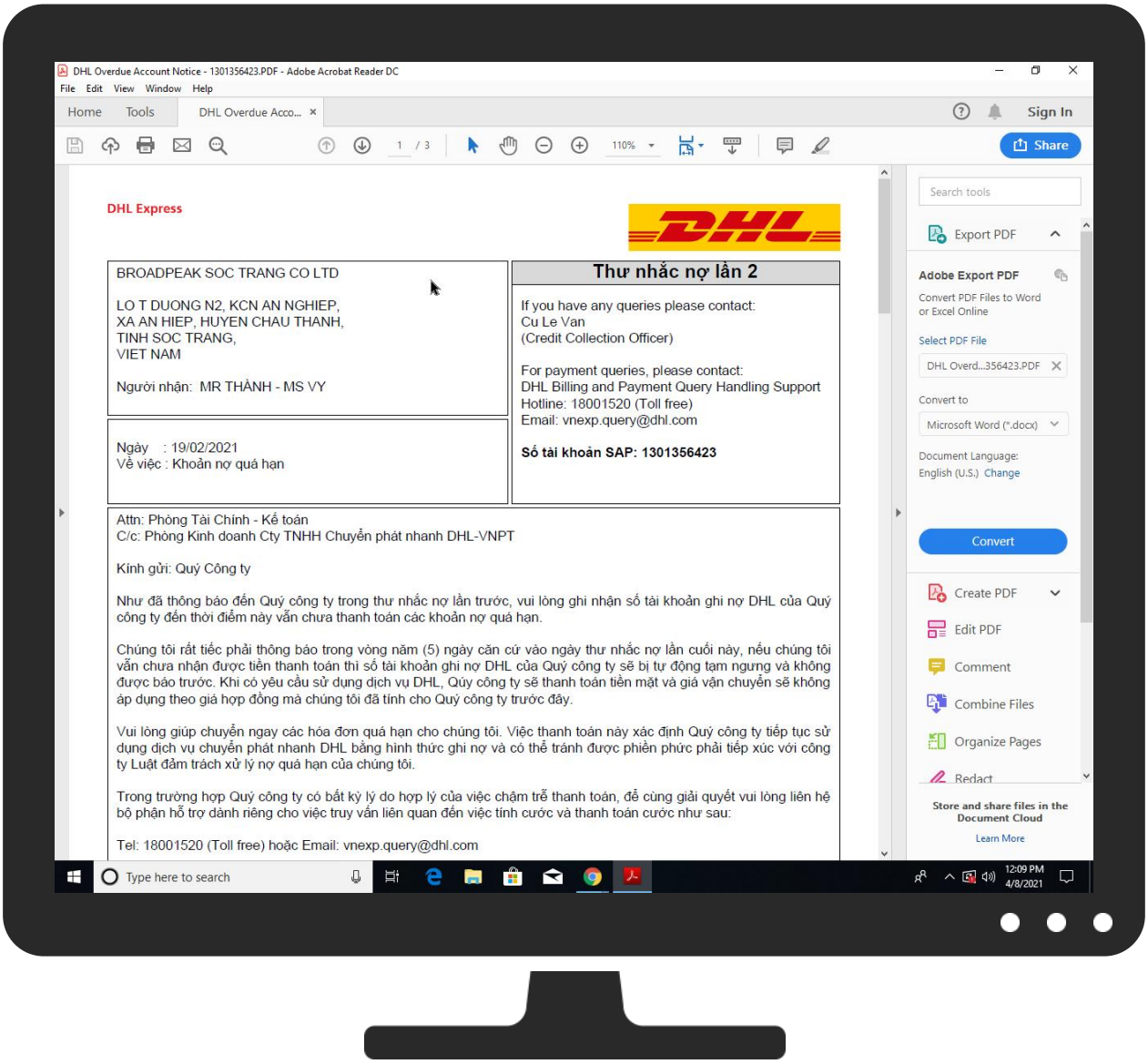


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe	19%	ReversingLabs	Win32.Trojan.Woreflint	
DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Files.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Files.exe	19%	ReversingLabs	Win32.Trojan.Woreflint	

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/D	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/P	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/J	0%	Avira URL Cloud	safe	
http://https://api.echosign.com6	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://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://iptc.org/std/Iptc4xmpCore/1.0/xmlns/d	0%	Avira URL Cloud	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://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/S	0%	Avira URL Cloud	safe	
http://ns.useplus.org/ldf/xmp/1.0/q	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://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/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://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/o	0%	Avira URL Cloud	safe	
http://BHuYIB.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	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/1.0/1.0//	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://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://https://api.echosign.comaS	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://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	
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://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://ns.adobe.c/g%%4C	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://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://iptc.org/std/Iptc4xmpExt/2008-02-29/C	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/&	0%	Avira URL Cloud	safe	
http://cipa.jp/exif/1.0/ER	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/ER	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/ER	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://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	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	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	InstallUtil.exe, 0000001A.00000002.493944777.00000000034C1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/D	AcroRd32.exe, 0000001B.00000002.525869035.000000000B118000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/P	AcroRd32.exe, 0000001B.00000002.525869035.000000000B118000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.aiim.org/pdfa/ns/schema#	AcroRd32.exe, 0000001B.00000002.531562783.000000000D613000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/J	AcroRd32.exe, 0000001B.00000002.525869035.000000000B118000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.echosign.com6	AcroRd32.exe, 0000001B.00000002.531632601.000000000D663000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	AcroRd32.exe, 0000001B.00000002.503177904.0000000007650000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cipa.jp/exif/1.0/	AcroRd32.exe, 0000001B.00000002.524330147.000000000AE76000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/d	AcroRd32.exe, 0000001B.00000002.531562783.000000000D613000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ns.adobe.c/g	DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe, 00000000.00000003.235184419.0000000007583000.00000004.00000001.sdmp, Files.exe, 00000014.00000003.336321572.000000006B23000.00000004.00000001.sdmp	false	• 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, 0000001B.00000002.503177904.0000000007650000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/S	AcroRd32.exe, 0000001B.00000002.523338894.000000000AC91000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://schema.org/WebPage	DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe, 00000000.00000002.305771748.000000000320E000.00000004.00000001.sdmp, Files.exe, 00000013.00000002.326525547.000000000293F000.00000004.00000001.sdmp, Files.exe, 00000014.00000002.494449872.00000000027F4000.00000004.00000001.sdmp, Files.exe, 00000014.00000002.494358171.000000000027DD000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/type#	AcroRd32.exe, 0000001B.00000002.531562783.000000000D613000.00000004.00000001.sdmp	false		high
http://ns.useplus.org/ldf/xmp/1.0/q	AcroRd32.exe, 0000001B.00000002.531562783.000000000D613000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.echosign.com	AcroRd32.exe, 0000001B.00000002.531632601.000000000D663000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	AcroRd32.exe, 0000001B.00000002.525869035.000000000B118000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://crl.pki.goog/GTS1O1core.crl0	DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe, 00000000.00000002.304457566.00000000013B5000.00000004.00000020.sdmp, Files.exe, 00000013.00000002.326525547.000000000293F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.npes.org/pdfx/ns/id/	AcroRd32.exe, 0000001B.00000002.524330147.000000000AE76000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/type#ty#	AcroRd32.exe, 0000001B.00000002.531562783.000000000D613000.00000004.00000001.sdmp	false		high
http://www.osmf.org/drm/default	AcroRd32.exe, 0000001B.00000002.503177904.0000000007650000.00000002.00000001.sdmp	false	• 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, 0000001B.00000002.503177904.0000000007650000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	InstallUtil.exe, 0000001A.00000002.493944777.00000000034C1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://mybill.dhl.com/	AcroRd32.exe, 0000001B.00000002.531082050.000000000D477000.00000004.00000001.sdmp, AcroRd32.exe, 0000001B.00000002.524330147.000000000AE76000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/extension/	AcroRd32.exe, 0000001B.00000002.531562783.000000000D613000.00000004.00000001.sdmp	false		high
http://ns.useplus.org/ldf/xmp/1.0/o	AcroRd32.exe, 0000001B.00000002.531562783.000000000D613000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe, 00000000.00000002.305685765.00000000031E1000.00000004.00000001.sdmp, Files.exe, 00000013.00000002.326495352.000000002911000.00000004.00000001.sdmp, Files.exe, 00000014.00000002.494308195.00000000027B1000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://BHuYlB.com	InstallUtil.exe, 0000001A.00000002.493944777.00000000034C1000.00000004.00000001.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_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe, 00000000.00000002.311089829.0000000004309000.00000004.00000001.sdmp, Files.exe, 00000014.00000002.509008335.0000000003A9F000.00000004.00000001.sdmp, InstallUtil.exe, 0000001A.00000002.485878265.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/subclip/1.0	AcroRd32.exe, 0000001B.00000002.503177904.0000000007650000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cipa.jp/exif/1.0/1.0//	AcroRd32.exe, 0000001B.00000002.524330147.000000000AE76000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/property#	AcroRd32.exe, 0000001B.00000002.531562783.000000000D613000.00000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	InstallUtil.exe, 0000001A.00000002.493944777.00000000034C1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.useplus.org/ldf/xmp/1.0/	AcroRd32.exe, 0000001B.00000002.531562783.000000000D613000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/id/	AcroRd32.exe, 0000001B.00000002.524330147.000000000AE76000.00000004.00000001.sdmp	false		high
http://https://api.echosign.comaS	AcroRd32.exe, 0000001B.00000002.524330147.000000000AE76000.00000004.00000001.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%tordir%%ha	InstallUtil.exe, 0000001A.00000002.493944777.00000000034C1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	AcroRd32.exe, 0000001B.00000002.531562783.000000000D613000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/layout/anchor	AcroRd32.exe, 0000001B.00000002.503177904.0000000007650000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	AcroRd32.exe, 0000001B.00000002.531562783.000000000D613000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfe/ns/id/	AcroRd32.exe, 0000001B.00000002.524330147.000000000AE76000.00000004.00000001.sdmp	false		high
http://ns.adobe.c/g%%4C	DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe, 00000000.00000002.316330391.0000000007583000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki.goog/gsr2/GTS1O1.crt0	DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe, 00000000.00000002.304457566.00000000013B5000.00000004.00000020.sdmp, Files.exe, 00000013.00000002.326525547.000000000293F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/repository/0	DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe, 00000000.00000002.304457566.00000000013B5000.00000004.00000020.sdmp, Files.exe, 00000013.00000002.326525547.000000000293F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://iptc.org/std/Iptc4xmpExt/2008-02-29/C	AcroRd32.exe, 0000001B.00000002.531562783.000000000D613000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/schema#;	AcroRd32.exe, 0000001B.00000002.531562783.000000000D613000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/field#x	AcroRd32.exe, 0000001B.00000002.531562783.000000000D613000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/&	AcroRd32.exe, 0000001B.00000002.525869035.000000000B118000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://cipa.jp/exif/1.0/ER	AcroRd32.exe, 0000001B.00000002.524330147.000000000AE76000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/field#	AcroRd32.exe, 0000001B.00000002.531562783.000000000D613000.00000004.00000001.sdmp	false		high
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	AcroRd32.exe, 0000001B.00000002.503177904.0000000007650000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	AcroRd32.exe, 0000001B.00000002.523338894.000000000AC91000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.aiim.org/pdfa/ns/extension/0	AcroRd32.exe, 0000001B.00000002.531562783.000000000D613000.00000004.00000001.sdmp	false		high
http://www.quicktime.com.Acrobat	AcroRd32.exe, 0000001B.00000002.503177904.0000000007650000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 0000001B.00000002.511106540.00000000085B0000.00000004.00000001.sdmp	false		high
http://crl.pki.goog/gsr2/gsr2.crl0?	DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe, 00000000.00000002.304457566.00000000013B5000.00000004.00000020.sdmp, Files.exe, 00000013.00000002.326525547.000000000293F000.00000004.00000001.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:	383902
Start date:	08.04.2021
Start time:	12:06:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	40
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@27/54@0/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.7% (good quality ratio 0.3%) • Quality average: 29.8% • Quality standard deviation: 36.3%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 52.147.198.201, 23.54.113.53, 172.217.168.4, 204.79.197.200, 13.107.21.200, 40.88.32.150, 95.100.54.203, 104.43.193.48, 20.50.102.62, 23.0.174.200, 23.0.174.185, 23.10.249.26, 23.10.249.43, 104.43.139.144, 20.54.26.129, 23.10.249.187, 23.0.174.233, 23.54.113.182 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, e4578.dscb.akamaiedge.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, acroipm2.adobe.com, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, a122.dscd.akamai.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, www.google.com, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, acroipm2.adobe.com.edgesuite.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, a-0001.a-afdentry.net.trafficmanager.net, armmf.adobe.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/383902/sample/DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe

Simulations

Behavior and APIs

Time	Type	Description
12:07:48	API Interceptor	46x Sleep call for process: DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe modified
12:07:50	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Files C:\Users\user\AppData\Roaming\Files.exe
12:07:58	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Files C:\Users\user\AppData\Roaming\Files.exe
12:08:19	API Interceptor	29x Sleep call for process: Files.exe modified
12:08:56	API Interceptor	3x Sleep call for process: RdrCEF.exe modified
12:09:22	API Interceptor	73x 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_Shipments_Invoice_Confirmation_CBJ1905 17000131_74700456XXX.exe	Get hash	malicious	Browse	
	DHL_Express_Shipment_Confirmation_BKKR005545473_88 700456XXXX.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	
	FedEx-Shipment-90161131174.jar	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NTLGB	DHL_Express_Shipments_Invoice_Confirmation_CBJ1905 17000131_74700456XXX.exe	Get hash	malicious	Browse	• 80.0.0.0
	DHL_Express_Shipment_Confirmation_BKKR005545473_88 700456XXXX.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
	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
	delZYToJxe.exe	Get hash	malicious	Browse	• 92.239.246.126

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_Shipments_Invoice_Confirmation_CBJ1905 17000131_74700456XXX.exe	Get hash	malicious	Browse	
	Sample Qoutation List.exe	Get hash	malicious	Browse	
	DHL_Express_Shipment_Confirmation_BKKR005545473_88 700456XXXX.exe	Get hash	malicious	Browse	
	APRILQUOTATION#QQO2103060_SAMPLES_KHANG HY_CO_CORPORATION.exe	Get hash	malicious	Browse	
	Thalesnano.exe	Get hash	malicious	Browse	
	DHL_SHIPMENT_ADDRESS_CONFIRMATION_000000 01.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_T RINITY_VIETNAM_CO.exe	Get hash	malicious	Browse	
	RFQ9088QTY.exe	Get hash	malicious	Browse	
	NEWQUOTATION#280321_RFQ_PRODUCTS_ENQUIRY _TRINITY_VIETNAM_CO.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):	615
Entropy (8bit):	5.635800606437158
Encrypted:	false
SSDEEP:	12:vDRM906ZiE5DRM9QCUeZiERDRM9a3ZiE:7rnEdDEFzAE
MD5:	F434E1C732245B76DEF197BD60AC16B3
SHA1:	34EA677CADEE67F095863114D9079CC410331775
SHA-256:	A586EE166BBF158BBED1C55BBE1FCC62735B343686187F85E30078DD19F38792
SHA-512:	F4AF1AC92F1AE2502875673764D295EEC0E8B2C2FBD0E0E7C1F45E69254A71E80E77471F5543B4B152618C7ADD60F6287575C18BFC60C3CF8480080333F98BC(
Malicious:	false
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ...../....."#.D...6...A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo..... .uS.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ..V/.../....."#.DTrM7...A....d.{v.^.G...d.W.:...P..k%..A..Eo..... .A..Eo.....V..(.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ...W.../....."#.D.0.7...A....d.{v.^.G...d.W.:...P..k%..A..Eo..... .....A..Eo.....OH8.....

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
Size (bytes):	696
Entropy (8bit):	5.6308436748735815
Encrypted:	false
SSDEEP:	12:V9zRDi9PQv9z0JLX9PQz9zLri9PQ59znl9PQk:XzI9PQlz0JLX9PQRzLri9PQjzl9PQk
MD5:	23A112570EBE8410ECBBD632BDCC4B84
SHA1:	DE23CD2BCBD36B5F51A701CFB98441FC2E5BD7E8
SHA-256:	FD86F7B533680463CE979D387C10D4CA3BCF1A2FE0E5D300E4F2A2C66461864B
SHA-512:	9A53081CA86D81F71EE5040648D65479ED49F6E9AE4C4092FA21AA3717127B763DF37A3FE74E301790B6758F988E6BF4146D3AFA104A65E0DEE4ACC083792EA
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0	
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ..(D.../.....''#.DZ.i3...A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....N.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .&...../.....''#.DeU.4...A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....#qA.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ...../.....''#.D..6...A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....X.+E.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ...:.../.. ...''#.D.tl7...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):	738
Entropy (8bit):	5.590037872122861
Encrypted:	false
SSDEEP:	12:DyeRVFAFjVFAFdlUo6jA5yeRVFAFjVFAFQxlUo6jUSyeRVFAFjVFAF07lUo6j:tB4v4dSBA3B4v4QxSBUSB4v4+SB
MD5:	9E11070B91A726C74C025A91A2805E79
SHA1:	50D1698FA46456415949CD608C9688F2ED85BF7E
SHA-256:	E1446F84BAAD737A0ECA35AFAC04BC783DDA51557BA49B2423BA6C4A47F85481
SHA-512:	4B9518C5C82B3318F8E2A5B9C12482EA0448033A0BD2DA1B5AFE85EE132900647D448F6854561429B45AADA71EF4E3E14EF287A57CD9503D9462DD3EE3243D2
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 ..|..../....."#.DD..6...A..hvDO.N.t@... ..n.*..... ....A..Eo.....A..Eo.....b5.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js .../.../....."#.D..K7...A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....a:.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ..|T.../....."#.D.".7...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):	5.64562470639347
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RsFCJiWulHyA1TK6ti:IbRkiDNoWuss
MD5:	03CEA3F22798C3F2ABD2A04592703148
SHA1:	8E98F928C9F0C7B0A22FF1FEAA4A7607891214E3
SHA-256:	D01339B9B6A2F7543782454E6B2060DE7E132CCFA160ED9266DF62DA608D5D93
SHA-512:	EC74B138405CAF7ACEFE259DEEBE4974DF87B897EEF39D72A9847F550C245A881C870785220111A5E8E31EAA2EF34E41C27F74EA19C838A0B9DBC9CF0BBE4C 92
Malicious:	false
Preview:	0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js ...>.../....."#.DV.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):	420
Entropy (8bit):	5.630726623968926
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVuv07KazOVVyh9PT41TK6tXllE+yiXYOFLvEWd7VIGXVuc:pyixRuAQV41TEp/zyixRuKwkV41TE
MD5:	57B4603676DE181B1632CC1B2C226526
SHA1:	12A2E9177FF2FAD71DFA754C9C7B72353F0F8811
SHA-256:	AB04AB755A0A1DD0224BE09CDCDFCEDFB7DA934D00BFC1D81DA74CDAB0E7522C
SHA-512:	7A707EC336EE3F7B369C2A5721B44F92436202B1FE444073BF4116B59E644F35E68FAD4DB05A3E2995216F4238FDB30676A2782C6899AD2B9D5CF2B2BB602312
Malicious:	false
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js .N...../....."#.D..6...Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo.. ....."".....0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js .I\V.../....."#.D...7...Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo.....U.....

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):	432
Entropy (8bit):	5.629069229869171
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
SSDEEP:	6:mvYOFLvEWdhwjQwlbNLZIl6P41TK6tXCvYOFLvEWdhwjQaJNLZIl6P41TK6tM:0RhknlbNLZCR4RhkJJNLZC
MD5:	4319A39BD72B2D68239D0D377362CBE7
SHA1:	354F33FC7EF22E05EB3C25D1F87B5EEDE804C26D
SHA-256:	5C99B08298B032E83DB656FC797FF25FF46CE7725C5A5071847F8F178277235C
SHA-512:	57DD3275011201D9969F651C750B6FB0F688FC892E363FC5FD10C77C72AB3054B048DAD970075FCE8D21B8AFA61337C6E79B7784FEAA9C87B947CA8A8AF0FB2
Malicious:	false
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ...../....."#.D_.y5...A.].>....uUf..N...k.....c..l.A..Eo.....A ..Eo.....0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .^.N.../....."#.D.>.7...A.].>....uUf..N...k.....c..l.A.. Eo.....A..Eo.....+.....

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):	418
Entropy (8bit):	5.576941520647967
Encrypted:	false
SSDEEP:	6:mJYOFLvEWdGQRQOdQNL86g1TK6tlEJYOFLvEWdGQRQOdQ8JaE96g1TK6tpl:2RHRQC6o1ERHRQCpn91
MD5:	8ACCAB8446F1CE037C0840150ACD1E4D
SHA1:	3E4A74650611DF0B220F1A4ED265B8B6EE7AFD31
SHA-256:	222EE1B16EF2B3E2F9B173A91BF67EA50A0EE5FE2C4B3632EC60D9A0EC44BA20
SHA-512:	D0CC27EF61F03238DCDE38BBD91E2D929A6D634201DC336DEC3E7B3CF6BC9D83D88407340FD9EE77BECDD16928FDAF521FA7A2F749C18144470949F05B1882 3
Malicious:	false
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .+...../....."#.D...6...A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo .....0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ..V.../....."#.D...7...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):	716
Entropy (8bit):	5.6108427126335
Encrypted:	false
SSDEEP:	12:Z5MJ13hMuR/EN5MkMuR/E1dB5MChMuR/Eu5MEoDhMuR/EA:ZS7muR/ENS9uR/EhSCmuR/EuSD6uR/EA
MD5:	3215BB3454A769DE5B581837B78C4A06
SHA1:	A6FB7833AC0985BC67DB77E4288DAEAA0EB7A21F
SHA-256:	BC76879644DF0D00F9A541F87090BE5B0D14F84B65585B116CA43B59866052B2
SHA-512:	24D344C1C4D681825E4422246D1E6C18F06D2C7E17BA088F80B2B41FDD113CDD381DC7B6A77DC553E3CE555A8D8B4874A24542A09E804B2E3A8CC71468D4D9 E
Malicious:	false
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .&-D.../....."#.D,.i3...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 ...../....."#.D){.4...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 ...../....."#.D...6...A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....{.....0\r..m.....3....<lb...._keyhttps://rna-resou rce.acrobat.com/base_uris.js .'M:.../....."#.D.7m7...A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\39c14c1f4b086971_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.579550237103362
Encrypted:	false
SSDEEP:	6:mGpYOFLvEWdzAAuUU07K/sm0bbsIDMGH41TK6t9:XfRMOU0O/XKsIZE
MD5:	CBE31ACA699EEBD37703CFD7011205BF
SHA1:	994B116E11770F64012006F1656FB2EC888B86BA
SHA-256:	C1AD4E7025284938A5BE274D428B0E2908C6D022280697978CAA20B16711B30E
SHA-512:	933ECD9E9DB65E3B6FD8EC888AB925EBD4047160B152F26FA17B90D210AB29F7E015D7EBD1E2F6BC5EE9D643E657108859BEDD6C0558815EE608BDECE4819E 4F
Malicious:	false
Preview:	0\r..m.....T....,.^...._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/selector.js .h."../....."#.D,*.7...A..`....^....L>..Xa./.....C.y.A..Eo.....A.. Eo.....e.....

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):	428
Entropy (8bit):	5.550243101685875
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtuKvMby0zBUKSAA1TK6tc4fPYOFLvEWdtuNMby0zBUKSAA1TK6tm:pR9Mbe5RSMbe
MD5:	A945C5C03E3DFDA250FA12840F97E94F
SHA1:	B258AB37EE5357072EBF2030847483F813214AFF
SHA-256:	A93477E427C316B407DA51502F7F4FC30A97D30FBD2A70DBE102F685EAA6E647
SHA-512:	203CA0864CF534F4F78B866D334AC1702FC2B8F7C9A219CB13E03306C042AD50D6559884BB0629F870F604B2A231E22FC17BDC1052BC0659AD24C55E42BE194A
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .5...../....."#.D.m.6...AQ..E.=....=h`t..t..3%A.F$..w..A..Eo..... .....A..Eo.....r.....0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ..1X.../....."#.D~7.7...AQ..E.=....=h`t..t..3%A.F$ ..w..A..Eo.....A..Eo.....

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):	708
Entropy (8bit):	5.593680028722721
Encrypted:	false
SSDEEP:	12:KkXxKMSCvActUl4wkXxKMSCvXbtUlikXxKMSCvLtUlhwkXxKMSCvlXtUl:KkXxiC/W4wkXxiCDWikXxiCzWmkXxiCo
MD5:	E6DD0FF4828F37ED362AF52065FD03A4
SHA1:	11ECAC1D098D8576DDBD51B521D31C1C6561E0FF
SHA-256:	434972F36526DE8BADAE1B55B99B69985F35A8305C508145B0E5856FB22C9981
SHA-512:	60CC1309FA953189D879C9A1821460FB104198EC3E2DCF0270F72ED6A36B38266DC1CE400D5A953994F80C6F4C599BFF53F43DA009AA295009EF21C826676474
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .>+D.../....."#.Dd.i3...A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....J.ZF.....0\r..m.....1 .....5...._keyhttps://rna-resource.acrobat.com/plugins.js ...../....."#.D.m.4...A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....|..C.....0\r..m.....1.....5...._key https://rna-resource.acrobat.com/plugins.js ...../....."#.D...6...A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....%N.....0\r..m.....1.....5..._keyhttps://rna-r esource.acrobat.com/plugins.js . K:.../....."#.DG.m7...A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....v..2.....

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):	748
Entropy (8bit):	5.630349041096794
Encrypted:	false
SSDEEP:	12:5h6OLKSakFjh6OL+iJnkzh6OLtEdjkJBh6OLXGkvH:5h6nG5h6pzh60EGJBh6Cj
MD5:	137A35F904681835A1A39B871E72AEDA
SHA1:	700C7AD1EB8B0A1815F606BE9C4DA432DE1A8BE1
SHA-256:	78CFFA3708E61C77C759B483CA9AEDF8EC07C33A89B0DEE5A71F3031C1B28EB4
SHA-512:	521C9ADB73D5673A8CF933EC0394DB56ADCCB43674487EB958AB64E81FE725E12B99A6691F7093A5376719B0DC5B4B34F00ACA2422A96A16E151D86A823BEEB C
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .7.\.../....."#.D.2.3...A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....0.....0\r..m.....;.. .I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ..*..../....."#.D.a$5...A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....!.9.....0\r..m.....;...I....._keyht tps://rna-resource.acrobat.com/static/js/desktop.js .s. .../....."#.D...7...A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....2..C.....0\r..m.....;...I....._keyhttps://rna-resou rce.acrobat.com/static/js/desktop.js ...J.../....."#.D..7...A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....I..L.....

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):	732
Entropy (8bit):	5.671971589599088
Encrypted:	false
SSDEEP:	12:URVFAFjVFAFdGwSeKaTLnN8RVFAFjVFAFnwSeKaTLnhORVFAFjVFAFLBm+wSeKa3:UB4v4owzXLnGB4v4nwzXLnQB4v4LZwzz
MD5:	D11EAF1E347123151FE599B4FF159B1C
SHA1:	1F949FC4079568C3A2DB52D0A66E473D0CF239C1
SHA-256:	6C16D2F01D36EF0E10441455F9C75F3BE55F6119B7C0A28A7DB9E3EE8F460561
SHA-512:	1630E5DE37D39E134AC454576EDADC1EA1C3DD7848398899885B8F9B2516290C45BA528199D7E81B719D78600B1F2A9B8052D2C2B325CEF2160BE7C86278A59

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0	
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 ..`..../...."#.D.F.6...A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....)I'G.....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 ...1.../...."#.D.fU7...A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....'B.....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 ..}V.../...."#.D...7...A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....]Xz;.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6267ed4d4a13f54b_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.5252538061218335
Encrypted:	false
SSDEEP:	6:mq9YOFLvEWdzAHdQEpaGX5GFCaa+41TK6tc:NRMHd/aA5Gda+E
MD5:	02AA0DD39E5741CB6B04980B6DBE4654
SHA1:	7DBB554FB50639233ADD1150C7D652723AF39B35
SHA-256:	CA051D8A10E14CBBF1A2F361FF5695CFB95CC4617ABD73CFD35F44277DD1FA64
SHA-512:	EAD74E5808890E5AF91EEA8F093A93D27BCB43896C95A2E1474F51C1E89FFEB84A0E37017BB07242A677864AA6E0DEEDA365F2C7998E9CB1FF8F55F88B6E7794
Malicious:	false
Preview:	0\r..m.....R....L....._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/plugin.js ..."../....."#.DI..7...A...G.3D.....Q.g0...._.Q.....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):	422
Entropy (8bit):	5.557797913075811
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXurFD11TK6tPeMs2VYOFLvEWdvBIEGdeXuCyJR11TK6tK:BsR2EseoFBysR2Ese6FU
MD5:	AD8E5AE899F53B8572E50835618D675F
SHA1:	B14302388AFC55E196057A47907902E3754DED4C
SHA-256:	81DCB469AE73D80D8D4A8AE3C9C60264DF2AB088E944CB6087E55A47D5D35016
SHA-512:	F7B1CFA1F15772539C41D66B7DB5A3580649D90467EEA0501B4430C06FF9EA4602568FA3BC1671F31B78887504808B04CA34F216FD8E5B8D8FB7010FF135A246
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .$1..../...."#.D.+.6...A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo.....S.....0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .z-U.../...."#.D@..7...A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo.....8.....

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):	404
Entropy (8bit):	5.683681693450438
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQSrRx4B7OhKlvA1TK6txLaVYOFLvEWdwAPCQI0O0x4B7OhKlM:RbR16fF+BJkSbR16YO0+BJk
MD5:	88D7108B998FCB9A57F299545F81866A
SHA1:	072BFD49CE5F72F7E5E100A6945956B08B7C308E
SHA-256:	93A47773EE2735BB23327FE799710ACC53DBE37E4432EA6907436472E911AA58
SHA-512:	7EFF11DF300762A472A01F03F7040B5C3C350629978D223B2F0D734EE7FF2F2AB69DE0824D281523D6F57ACCA206C947377DE2B9788FE9C6C2C684FBFCB52C6
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ...../...."#.DN.x5...A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....j.....0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js .B.N.../...."#.D...7...A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....E?'.....

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):	422
Entropy (8bit):	5.600342521671527
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0	
SSDEEP:	6:ms2gEYOFLvEWdGQRQVuQzQdFt1TK6tE8s2gEYOFLvEWdGQRQVuKlSvQdFt1TK6t:B2geRHRQJ0ir2geRHRQDli0
MD5:	78DAE877BD510F82D92DC999D09B72AC
SHA1:	DF30C16D2EDBE2CBB3BFD13CC45C2E2EBFEE4BB9
SHA-256:	FF28F4F40E0030FC799CD86D0317CDACC13FBF722BF6983A14FFA8F736E0546C
SHA-512:	4E672211D63C95704187F1DB7263FC49B6E76F5587C274355E452DA4FD9725F623B5EFD6BAC378DB846E71400CA6881B25373D0A72A4165C0D706ADAA04D7D9
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ...../....."#.D!!.6...A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A. .Eo.....W 0.....0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ...T.../....."#.Dd..7...A@..{o]...9o|..qY....T....{.. u.b..A..Eo.....A..Eo.....

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):	824
Entropy (8bit):	5.661389543444589
Encrypted:	false
SSDEEP:	12:WyeRl7Et1wZyeRlSoRt1wrlMyeRl+rAt1wMyeRlYpt1wO:WJTEfwZJ6Ufwr+JJfwMJQpfw
MD5:	47F1EB9BA042E2F5F0CDDA940EE09DC4
SHA1:	C9558BB99FB64CC2CCB35BA51CE51EB3950D15BB
SHA-256:	EA9FAE2E9AD52B507DDDD56E9D782D6F50D2DF8FEFE802EA0BB4ADE8B672ECD3
SHA-512:	98CE8C20AA688446117648B0B608B99BEA8E4F68742A16A9DB9EC1F63ABD0278B772C3297A0CE6DB7779F4356BA0C26F490CC1E7065D9BDDBBFEDCFAF6707C A6
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .6C`.../....."#.Dy..3...A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.... ..dQd.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .&H.../....."#.D..U5...A.t\a.....x5.'OuE.C..@.....x..A..Eo..... .....A..Eo.....|.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .nX%.../....."#.D...7...A.t\a.....x5.'OuE.C..@.....x..A..Eo .....A..Eo.....a.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..lL.../....."#.D...7...A.t\a.....x5.'OuE.C..@.....x..A. .Eo.....A..Eo.....@'"~.....

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):	436
Entropy (8bit):	5.599077139770709
Encrypted:	false
SSDEEP:	6:mnYOFLvEWdhwyuLilwrqwK+41TK6t0enYOFLvEWdhwyu/JAiwrqwK+41TK6t:wRh8ewK+EhRhqASwK+E
MD5:	D872BFFA7E5D4B3FFF9E413FE8C87CA5
SHA1:	9423D31FED96923E27CDE57DE4E5A157EE3931DC
SHA-256:	E811DA9B3CCDE0C2C612D7260D632A829C3A9D22F5EB898807EAD6B7A25DE2BF
SHA-512:	E4C4F6B3AE9FB4E94744420EA6CB5615EEF6F6C293E9796AC6D845BA69F2CCD025BC7FD2EDD48FCE899CA5216864583886DE952A1AC5FBD5BA7B24B7F1D28 3D
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ...../....."#.D..x5...A.....7...o..a=.98I.....(3.$G.A..Eo..... ..A..Eo.....,y.{.....0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ..%N.../....."#.Dx..7...A.....7...o..a=.98I.....(3 .$G.A..Eo.....A..Eo.....KTA.....

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):	920
Entropy (8bit):	5.662354143416874
Encrypted:	false
SSDEEP:	12:/RrROk/ElWIfLEmRrROk/7nlfLEHCvRrROk/8fLEkVRrROk/BMfLE:/PJ/E0I4mPJ/7I4HGPJ/84kVPJ/m4
MD5:	55746FE1AEBF73F23A5DAC5B8CF88634
SHA1:	07F421CA196BDBE7C102CC8F2B706E5112FA71C4
SHA-256:	BDFD32BBFCE5ACB9ED8FA8AF83340CD2AC54F8D9790BC61841E6DB775BAB3507
SHA-512:	3D2C0F4591A307B5DB2A36B2B21A3B10984BE4B89C740AB584BBB698AECBB4A3E1DE77C608072CB6539FA8F1D587795AA7197FEA84AE46CF6BC6149F45DB89 AA
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0	
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .M._.../....."#.D.w.3...A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....b.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..-..../....."#.D..T5...A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....]..@.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .T%.../....."#.DD..7...A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..iL.../....."#.D..7...A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....UT}.....

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):	744
Entropy (8bit):	5.64396843418981
Encrypted:	false
SSDEEP:	12:xqTk5CPLnZqTdUCPLnL2TqTR/PCPLnOqTo4CPLn:AA5MnoBUMnLRFPMnhbMn
MD5:	1896BD90A2A4B60DB25C248DFA516B73
SHA1:	973CB4D874CB8BA6BC028D0B80027D1BEA448984
SHA-256:	ED40F40DCB10DBE21D3C20859567F084AB1FF446CFD331D758F7688F9CC0E5B9
SHA-512:	C37EE10347C8367A2532EFF0F344C169FA42E1B3F987330930F6A02F07776E1DEC3A879133605C31964B4DE54014D929AD32850535654F5CB4984EC6504149EC
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ..9\.../....."#.D.).3...A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....!7.....0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .e...../....."#.DWZ$5...A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....Av.....0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ... .../....."#.D\..7...A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....D.=.....0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .g.J.../....."#.D.k.7...A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....0.....

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):	621
Entropy (8bit):	5.62547705918076
Encrypted:	false
SSDEEP:	6:m52YOFLvEWdMAutrJTLG/sEJ41TK6t/oW/lM52YOFLvEWdMAuWKkllfsEJ41TK6h:zRMTtG/sDlblZRMrYsDbRMhsD
MD5:	CE10371D24A3AD218CC61AA574AE5167
SHA1:	B9E97D4E2190F1DDDC6F457BB9787045F7AFEB2E
SHA-256:	6DA4400C39156CBF372C46654F8F6C786E37E96D2132876EB0BE691F5B54F625
SHA-512:	34EED70F76D3129B7170479D7C64523BE4E768B83DA1824E5736621A2B001B25C87BC58FC88789E26D4484727CC0B45DE8FBA8D8A0447B986CFEB1F3E1BCE55
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ."...../....."#.Db..6...A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....f.k.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .../.../....."#.D.EK7...A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....4.!.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .x.U.../....."#.DV(.7...A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....x.]C.....

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
Size (bytes):	630
Entropy (8bit):	5.62793551032962
Encrypted:	false
SSDEEP:	6:mYilPYOFLvEWd8CAdAu+5saT9Y2Fong1TK6tFl/MYilPYOFLvEWd8CAdAuQvxM2/:6lJRdG2FoMBUlJRZvFFoMDlJROviFoM
MD5:	529CDD0C9C9FF9C7A5F0E95EA2B7CAB8
SHA1:	7D4EFB3C2EEC456C5C5A695B3718A5A1E9357212
SHA-256:	757BB58E5D4DF784CFD5AED27D1D2581FE12A1A1F941D426C972DB90E44C11F2
SHA-512:	519EEAF738E26E4637109BC0A784E8B6BBB7554725655B3932A0CC7F405A1F2BC04814E7F9712BC0F9DB3FFBC2AE9B820E28AF4761846F4F31D0E3396BD14C5
Malicious:	false
Preview:	0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ...../....."#.D..6...Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....F.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .{./.../....."#.DyxK7...Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....yN.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..uV.../....."#.D.S.7...Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....k.....

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):	892

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
Entropy (8bit):	5.627746480316712
Encrypted:	false
SSDEEP:	24:UPJ/WvN28PJ/dN2UPJ/6N2ccPJ/0ZEN2h:cJkE0JlEcJiEcUJ8SE
MD5:	AAEC06E0773B5FADB67BBDFEC0878B9B
SHA1:	D4A7FD954814F0E1F4BA20536B311153D3697E02
SHA-256:	BF38516788A58251A1CAD8CD27BF6C1319384EFBEE276A51CCAC95B63463FA98
SHA-512:	F700AA0B678A9E7533472BFC4FF3A1680448CEECA4D08BD865124ECC74CD5E6952CEBBB1724CD8D29D621985DFE3698FCD8DF5171FF4A4DBD7624B79D1849 E
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .i._.../....."#.D.E.3...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 .A...../....."#.Dh .5...A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....x .....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ...$.../..... "#.D...7...A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....^..k.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-file s/js/selector.js .X.L.../....."#.D..7...A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....R.....

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):	852
Entropy (8bit):	5.699670903567938
Encrypted:	false
SSDEEP:	12:ehRce5CirNJICehRcG+yRrNJICFhRc6rNJICAhRcKZcrNJIC:ehZ4GJICehnZJICFhBJICAhVgJIC
MD5:	A85E2A5D927BAFB7348E00652EB300A7
SHA1:	F025644EDCCD8FBA5227272B581E021FC86D49FB
SHA-256:	A2074549875C6323605F311FB9A9B1F9DEB648C7E1DA4DE9DD7A0FC8738C843F
SHA-512:	D526C3ACCF51EAA832BA6C8A60DFC9CC049560FB7765F924AFD66D89810C955B8274EBEB3F75BE8A8B4C49B2C4ECD80281EDEA12055672ACA21848E85E00E 9B
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..F`.../....."#.D...3...A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A. .Eo.....7gf.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..n..../....."#.DfiU5...A.;"./N_.,.:C..2....9L.H...3:...A..Eo .....A..Eo.....+.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .(.%.../....."#.Dq..7...A.;"./N_.,.:C..2....9L.H.. .3:...A..Eo.....A..Eo.....c.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .aoL.../....."#.DO$.7...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):	832
Entropy (8bit):	5.653765513440349
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhugE3ypZLzgm2d/1TK6t0OEYOFLvEWdrIhugOLQqpZLzgm2d/1Z:0RW7RResRj3RRe0R2OpRReiRCrORRe1
MD5:	3E0D2D18B24B752803DCCE61D3F31FBA
SHA1:	A551C3DAC92A02216007439A5B522D8269D8F3E6
SHA-256:	A356920821004B6D358CA3C9E854F083A0B422B8EDC5727BD2228C4F231A1119
SHA-512:	973E854AEB5F4A55B0D4BDE4B56D285950991C38A52C7FA057CB1D5B5B61555ECF81A06DBA20F22566DA5C50EE67289DA3B64F94F348ECB57BF1BC4989F1397 7
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .{9_.../....."#.D...3...AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.. ....D'.y.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .H...../....."#.D..-5...AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo..... .....A..Eo.....u.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ...$.../....."#.D...7...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 ...K.../....."#.Dm..7...AZ.Z}Q..4.o....0+..[|..n:* ..U.W.A..Eo.....A..Eo.....s.....

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):	752
Entropy (8bit):	5.676151940721472
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1KBoWnkx56uvp1TK6tuMAElVYOFLvEW1KAlkx56uvp1TK6tpSeAB:6JJKBot1JJKAfPPJJKCRKJJKSk96
MD5:	4A9E77CDBA823E011C084314ADB3800D
SHA1:	5729E2A6A4EDF63FE8025600890EB29991C21D26
SHA-256:	B19F5AD4FAF6560AE15DBB7171352EDCE32808C0AB6B72D17C38233DBB0B3E64

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0	
SHA-512:	3C36A0AD55E4614A1866E9A6A4FBE939A236CF0C79455028618FD54E9D5C353D021ED448B4FA0FC13EB23997EDCF96663181E694D8FEDA128EE08D26F707A5E
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..EM.../....."#.D..3...Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....9.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...../....."#.D...4...Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....W./.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..]..../....."#.Dl..6...Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....=.N.....0\r..m.....<...)6...._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..O>.../....."#.D...7...Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....K.....

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):	428
Entropy (8bit):	5.637188232554711
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvuVt07Ka7rhUDLYtmOZn1TK6tiN/EWYOFLvEWdBJvvuA59ghUDm:xRBJnqDcFZLSLRBJLDDcFZL
MD5:	4619F702C5F70CF315F82E1627DE17ED
SHA1:	7604E205F04BD53F4ACCB38D47D92F54206EB26E
SHA-256:	7E0191EA3FDD28CD3F26E0795DB95E5ED85E8A96F6D412DF1E66E217B7C28DFD
SHA-512:	09933C87EADA3779A2C42303EC63924F2CC9C977C5F1E49F6B5274FBFE7B43D969EA8470B7287E0896FB9D6FBABECCDBB0E5498105CD83F07A46C9079CDC73C
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ..7..../....."#.D.D.6...A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....x.....0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ..0U.../....."#.D...7...A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....y.....

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):	844
Entropy (8bit):	5.659478442590167
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp7wEVPu1TK6tdsRPYOFLvEWIa7zp7zMCVPu1TK6tjO98sRPY8:BPHBcwPH6CcpO9rPHtOoscGZPHr4HcQ
MD5:	B91232700EE4F6FB155A8957D9784A83
SHA1:	5077A574B2E857C2BC117B9923A804D64D32CEFA
SHA-256:	ECFF64513DC05983129727B4D5CE126C5C29018C6884DA2A2D03ED0744060AFD
SHA-512:	F583FCB3D0C5FD8A4708DC53EC80BA976747D8745B8E4DCD669C11CF8883BE4C1CA402F6E92A54545EE220A95693A9A5D26D21BB661E31A00C47F62AB6F9D7C
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ../D.../....."#.DV.j3...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 ...../....."#.D..4...A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....V.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ...../....."#.D.M.6...A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....i=.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ..N:.../....."#.D.nm7...A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....An.....

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):	416
Entropy (8bit):	5.619900621198067
Encrypted:	false
SSDEEP:	6:mKPYOFLvEWdENU9Ql7KZlCGswiM3Y1TK6ty+KPYOFLvEWdENU9QYOPwiM3Y1TK6S:bJRT99iwr0cJRT9Qwr0O9
MD5:	725FF7E8923E26F6E5D7538F84F9CB47
SHA1:	736A1599092BA754CF2A636040FF2485DEA6F0CE
SHA-256:	B45CB77B57225E12707A8671806EAA3692BE21548284EA95A36C84A2267797A8
SHA-512:	411576937C2449CF9D57B45F217F78355C5A0C5A81D59CDFE1F352BAEA2596C216293A00CF8DB934F1B7528065B1D134D02570762EB84BDEC18F265ACE56C87I
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ...../....."#.D.5...A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.....h~.....0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ...N.../....."#.D.(.7...A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.....(Y.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.609392356648242
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQ8p+2jBRCh/41TK6tiEQt6EYOFLvEWdccAHQRMb2jBRCh/Z:XRc9x82Di/EUJRc9MMb2Di/EW
MD5:	CE382C012C2873EAC963F3F6E4D2768C
SHA1:	7D242935777EFC4472CA5F4EDE4429C9FD04DE4C
SHA-256:	44CCCFAE383CF59E84E166904BF63822E3046B5FBA6F0DD968214FC0D8E26624
SHA-512:	D0B8F4CF55F3EF27766EACC10DDFB3F03DD5D1134BD71C58DD5B4A88410CE7A1F8E554BFD36E936C5213F7AD73CC57D25F805CBA7FE08E6D68A83BFDF4EB B22
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ..e..../....."#.D9..6...APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo. .....f.....0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ..~V.../....."#.D.i.7...APJm...0x.x..RD...BB!@5..<..]....A..Eo..... .....A..Eo.....u.y.....

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):	462
Entropy (8bit):	5.587723540501075
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhuXlCwVULlF4r1TK6ti8qs6XYOFLvEWdFCi5mhuwu1uVUH:bs6xRkiFlCZLlF4nEs6xRkiKuZLlF4n
MD5:	4D6206E459D5B809AA1E2E1B2C8CC3A8
SHA1:	D4F9369CD236BF7179CABBA235947B3DD9B6398D
SHA-256:	043B37AA44B7709ACC09878F520F38DBFDF9042860FBD3FAC1BB93312ACF3E9C
SHA-512:	C661A4FD1199AC75D1159DCF1E1F283DC810639B59A3811F6C8321A9E415AEDD3693C9CCE90ED7626FE6221C44412DFD926F87E86EE341CD7A11BB5A6E2E81 A
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .e.c.../....."#.D.Y.3...A.P...#4..l....5...5..).w.. .h .~..A..Eo.....A..Eo.....n#6.....0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ...&.../..... "#.D..#7...A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....4I.....

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):	430
Entropy (8bit):	5.551280679729311
Encrypted:	false
SSDEEP:	6:mhYOFLvEWd/aFunp90EN941TK6tS2hYOFLvEWd/aFufplEN941TK6to9:WRJgY9E8mRRY9E
MD5:	51E2736354ECC588A7933BF71015E512
SHA1:	B311327A70166CB6556244794E89C8514991F767
SHA-256:	4F808C6DCCE21BCE74269A138E568E6A50D8411F85536AB9C9EA89A13EFD6EC3
SHA-512:	2DC37D7C0BB0E9A8571E9E945ADE4F1C1C9CE0878F130A911765C124C891D77FF178B295781499C4CE8895071473EA77B0079AB92D95E3D442A3F00F4CFC511
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js .(!.../....."#.D.}.6...A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A ..Eo.....u.....0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js .jBX.../....."#.D.I.7...A...a.f.m.i.o.p..3U5.....^...I.A.. Eo.....A..Eo..... .....

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):	416
Entropy (8bit):	5.59177473695395
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQ8KB9ZoBMqVd3G4K41TK6tjG9//MR9YOFLvEWd7VIGXOdQ:2DRuRuyB9Vd2kYXIDRuRUB9Vd2kZ
MD5:	FD25240E375762B496D76872957BA603
SHA1:	27B4F743F3B8AA6AB5438568E8DAB6B764BD6ED9
SHA-256:	447214E5FE1450C9509772EBCAB35324A0815E0A2BDD07381B0640725A842DD2
SHA-512:	351F4CB62950DD692531EC87C30DDD306F0AA30777D90A0D1E15ACE0B9C0EEA9648E800E8D34E6A2A9A06C75254B6E20359CFD5FC60BDB1751368C34DBAA3 B2
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0	
Preview:	0\r..m.....P...y.p....._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ..P..../....."#.D.L.6...A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.. .....0\r..m.....P...y.p....._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ...W.../....."#.D...7...A..y.$..$.v5j...T...z.]..._S....A..Eo.....A ..Eo.....4.....

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):	624
Entropy (8bit):	5.632746038815
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9QPyplmuA424r1TK6tBXEkqYOFLvEWd8CAd9QQOl+DtuA424i:+RQnRrnLURQNK+DcrnwsRQrscrn
MD5:	E5027F184BEFFD3DABD042E66D76B2B5
SHA1:	AEFF8848773DC1425DF16D99889721C1EEA8A651
SHA-256:	060501AA1A2E2FC8850E23F4CB788B7AC3E5B9A6119506BD24A2C8EA92D95DB3
SHA-512:	128E6E11E48D9AB88160E1A83FCDCCED73C6176E33101C7548C892BE432FDE1E2E7F0528A7E4A9E891F523B711464C9B15DC849D42C7FAA7D34F032DD05DEB 4
Malicious:	false
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .h...../....."#.D(|.6...A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo... ...J|?.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ...1.../....."#.D|.Q7...A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo..... .....A..Eo.....e.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ..W.../....."#.D...7...A#..@..k(v.8g..5.~_....]Pj.*..6.A.. Eo.....A..Eo.....8.....

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):	420
Entropy (8bit):	5.608867335884761
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAu9syC8n1TK6txEoXXYOFLvEWdENUAuyomuyC8n1TK6t/:xhRTU7Qn7hRTwu7QV
MD5:	0E9DF55AC17982FE6CDDEAFFE5048AC0
SHA1:	C4D90D1A16FA5404C187CCC055F6187449117B94
SHA-256:	14749286A3D496949735863BD3BF4428F831A2549BD430AE66730143679E269C
SHA-512:	5E223BC3924155370F32CE5FD427237CB78E3CEBBFA65518FDDFDEAEC8AE7446C80FFCB2C4D1A302CAC888BB9F61919FFD5C4E1ACCC08D0A66C780C797B6 2BD
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .l.../....."#.Duxx5...A8.../...;.\\o....1.....+..A..Eo.....A..Eo..... .....0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ..#N.../....."#.D..7...A8.../...;.\\o....1.....+..A..Eo.....A..Eo..... ...L~.....

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):	884
Entropy (8bit):	5.6523900434560215
Encrypted:	false
SSDEEP:	12:nRrROk/VdmZRrROk/VWKwmilRrROk/VwiVmXRrROk/VuVmCf:nPJ/mZPJ/PFGPJ/qigXPJ/wgC
MD5:	0F05F668837716B0EBE9E646E373D237
SHA1:	752CB348161E47EF07EEE6CFE79A0CBB3CA0F1B3
SHA-256:	794518E57B14CB296287EAF06CCBC8288307F947A1CC22FDCA47FF71FF3E90AC
SHA-512:	F81D80D9930D5323B59420A8891E0C0491A710DFBD2766F264486DD862267253875C367024072AC9DF66ED43A73AA97870942D320C9909E7DE5C5AFE7CE7ABCA
Malicious:	false
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..M`.../....."#.D"..3...A ./.ev.....N~..6.b.....$.j;:C...A..Eo..... .....A..Eo.....;.i.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .br..../....."#.D.sV5...A ./.ev.....N~..6. b.....$.j;:C...A..Eo.....A..Eo.....o.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ...%.../....."#.D...7.. .A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....@pb.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/pl ugin.js ...L.../....."#.D..7...A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....N.....

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
Category:	dropped
Size (bytes):	420

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0	
Entropy (8bit):	5.610193605785719
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWujqksNk+Adm9741TK6tsZ/lXYOFLvEWdccAWujOOsAdm97R:qxRch0BAdu7E6xRcpUAdu7E
MD5:	2077402C86C23EC52D32AE88E2AA524E
SHA1:	4C8AE341A3AD79380076E61D6718860B54010020
SHA-256:	248617C21EB0B7CE50E4062285C45160BAB99EB81DB94ACD6FA8EC7C6F5AE61D
SHA-512:	10A78B2A53CF43C3FF545139BE834BC8DEC4D3CB4C73310426A8F300449B2CF6C754A8F0AA98B77B5F08F3462490F71C0CCE5943C032FA4273533338A32FF1C6
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ...../....."#.D...6...A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....".....0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ...T.../....."#.D...7...A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....k.....

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):	408
Entropy (8bit):	5.598655394138875
Encrypted:	false
SSDEEP:	6:mMOYOFLvEWdwAPVuoiJn1TK6tIEMOYOFLvEWdwAPVuCCarJn1TK6t+:2R1WLW0R11L
MD5:	975ED5336C1EEABAE7980B100B4562CC
SHA1:	DCFDC07DEABDDFD537EAC6EEA58DE292821723F8
SHA-256:	A80007EAC9562C04A360482B2DDF0F4992AA300761E3338E8CFAD7BD503BA1C7
SHA-512:	8E956E5DE4FEC00B2C36AD90CC5B8320766CADCBCBEA12586161A930541DB054BC171B8C767752EF8E656B7393EC449A9DFCF5A342D2CAA8CE2CE267D206347
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .d...../....."#.D.Yx5...A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo.....v..Q.....0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .{"N.../....."#.Da..7...A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo...../\a7.....

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:	modified
Size (bytes):	424
Entropy (8bit):	5.637257560918759
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQfhoG2zhcsBXIh1TK6ta3PXYOFLvEWdBJvYQklv2zhcsBXIR:mxRBJQwodDB08xRBJQhMDB0X
MD5:	93C1DF33B4CCB48370C980A07AD308EE
SHA1:	5B058F6C542E7AA1DCDF1A6B34B0490F5F6B90F0
SHA-256:	825E39D85A7AB02637D76402221049FCDAD3C2116C7BCC43C4E288E50F313B72
SHA-512:	E54B2293BAECA8A48D9EC09FF63FD72B7D8D1583A1309D4C5A6436A2AD1085E6D6071E80506AC2407C78E13BA6D70BB17EFA35DA0E620CAF28F4C7E1A63F8DDF
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ...../....."#.D...6...A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....y.....0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .0.W.../....."#.DTn.7...A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....iJ.....

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):	912
Entropy (8bit):	5.620966123705577
Encrypted:	false
SSDEEP:	12:3RrROk/srDcOFRrROk/sYscoRrROk/sGcLRrROk/stVc:3PJ/7iPJ/ZoPJ/MLPJ/Ye
MD5:	B010C5C5F3A7D6F9D7E447D4E869B72A
SHA1:	4A1662E7A9E73F0FBDC98E8969C5E6E808ECE609
SHA-256:	0A09732B79979DAB381525D85BF61BAFDA96D7F865E74C198922934B9CE65CE8
SHA-512:	B293C39A369C693D1B468CF3569EF5408EFE23EE3CFADD45D0B5E4C75349B03F85B6ACEFAD255981EDA289EC3344EE88D7D9CC6F9EE250630D017B8479C3F7E
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0	
Preview:	0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ./h`.../....."#.D...3...A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....J.zX.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ..`..../....."#.D[.V5...A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....m.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ...%.../...."#.DN."7...A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....q.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ...L.../...."#.D..7...A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....r/.....

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):	984
Entropy (8bit):	5.040251725706932
Encrypted:	false
SSDEEP:	12:MeVl/9l/gLnl/2+/l/KLvyl/CAl/q5tbyl/iil/iHl/OHl/Wyl/jl/lsl/lA2l/I:Mfg1zZFufGMisp6r6C9QPr
MD5:	9B90244F9985CBA4985897217DD7C7AB
SHA1:	9BC5919E96D2A3CE20322AADC162056A6B6FE7EC
SHA-256:	E44D4707C1D938DE3374B96940F3B6AB183AEEDDFC92C1B25617C57337E95941
SHA-512:	15C4CB9E0569A8B9A35F369364B2C4312DF76EF721A8DA8C3CEEB4A289D5DE061D0D14EF2C0D35A1DD3FD12014BA67243DB65124376144BE2D2943FFAB742F6
Malicious:	false
Preview:	....h...oy retne....'.....'.....;.y~A..z.B_./.....*...z.B_./.....oB*.8.B_./.....#...(...A_./.....k7A..z.B_./.....D.4..z.B_./.....[.i..%..z.B_./.....<...W..J.8.B_./.....,+..._.#.z.B_./.....J..j....z.B_./.....6<|....8.B_./.....A?.2:...z.B_./.....+.{..'.z.B_./.....*)....J:.z.B_./.....2q....z.B_./.....P....V.z.B_./.....+.U.!..V.z.B_./.....P[. q.z.B_./.....!...0.o.z.B_./.....u\]..q.z.B_./.....z.B_./.....*.....z.B_./.....o..k...z.B_./.....^.~..z..z.B_./.....o..z.B_./.....Gy.'.h..z.B_./.....F..=z;..z.B_./.....3....z.B_./.....v...q...8.B_./.....C..M.....A_./.....a.....8.B_./.....~.,.4>..z.B_./.....&.S.....z.B_./.....@..x..z.B_./.....=....m...z.B_./.....;/....z.B_./.....q..z.B_./.....MV3...z.B_./.....:..N.A...z.B_./.....B_./.

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):	292
Entropy (8bit):	5.177660037147739
Encrypted:	false
SSDEEP:	6:m1IgYyq2PWXp+N2nKuAl9OmbnIFUtpkIpa1ZmwPkIRlRkwOWXp+N2nKuAl9Ombjd:CvaHAahFUtpe1/Pr5fHAaSJ
MD5:	8B17662B08835BE6D5182DBF2B9E8A19
SHA1:	76FFC66D5133CE27121E4F64879DA9A80CBDDEE0
SHA-256:	79C3AF7F150063028EBD1D78BB97385078BA312A6972F5086B8D9038AF8DCB92
SHA-512:	17A609A3D886EB08F6D5A68835A7693B89F3D56A04B232AB47A082034DF1BBFE19E1CE9D0FF64E29C33C60DA003BC863AA9262F47FF5D03F4C447AB9022E75B
Malicious:	false
Preview:	2021/04/08-12:09:02.676 1ae0 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/04/08-12:09:02.677 1ae0 Recovering log #3.2021/04/08-12:09:02.681 1ae0 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):	1703936
Entropy (8bit):	0.00887053771030707
Encrypted:	false
SSDEEP:	48:TGEiaGEiCsMiCsMiCsMi9sMhC9sMhC9sMhCAsMhCrNsMhCrNsMhCr+sMhCDo+sMB:dKKnono
MD5:	95D2D3702D0EC36BC6F781E804CCFB32
SHA1:	61EE347472500434A9BE50F864C4562EC52C9A54
SHA-256:	7E3C9563DA1084EE239D2429E2243F27B99E7F7DE6778CDC74175AACD34FD1A4
SHA-512:	4595411031E1308D3DC040814E996D0B5476B7B3E9B92ED03FF5AE75C2B7559C4611B590616BC6BD1C9334BC7E038EA09401E3BDEAEB822F34A41B41F608CAB
Malicious:	false
Preview:	VLnk.....?.....Tq.>..j.....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210408190856Z-251.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

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210408190856Z-251.bmp	
Entropy (8bit):	2.308739914604857
Encrypted:	false
SSDEEP:	192:lUzgM3fdU9rd/pIpotZ0deVfa0hLSPOhqLjo4jb6FeiRzHh/uKl+0fr5qta+OOfr:KiS0d6M+P6FvBHxN14/sMCsNj
MD5:	7CAFDE4EA3C84220C4E669A1D2DA08D2
SHA1:	16588A00CCAEB9D616DBC1B7BB885EA2AC189AEB
SHA-256:	C7B3A1B95190596236F26A416CD32B0F40C80D819BAA8EC148E9872FB361365E
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):	3.386618445800535
Encrypted:	false
SSDEEP:	96:iR49IVXEBodRBkQgOhFVCsL49IVXEBodRBkRbgOhAVCs749IVXEBodRBklbgOhBf:iGedRBoedRB+edRBtedRBr
MD5:	27BFBAEB6E132E17D30771ED105F45C3
SHA1:	B23BBF1D7C6E4FD7BD777C330A6A727D514F34D5
SHA-256:	D72FD3646B9201E2B6D17974B8789800F3CEB24DF21B62461CBF03B820CC7783
SHA-512:	56C4EBEF83D93DF6FDEC8E806E65656C863B89D18C004609F53F8E3E7954372EFA33CB870B7C61B66837DF3DA4105E246124CEF949A10364F2E1E0F008DCBE8
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):	3.2000455844552476
Encrypted:	false
SSDEEP:	96:X7OhFVCP9949IVXEBodRBkS6gOhFVCsHLR49IVXEBodRBksbgOhAVCs9d49IVXE2:XZiedRBnULGedRBiCedRBuyedRBe
MD5:	B05C5E8D023ABA2BB85A66BE2BC901F3
SHA1:	C0DA8A7354B1D097820481C01343E0E5348057B0
SHA-256:	FFE88F91976E47413E89FDD062FEC5D7EE319C3C5AB3AA2381879B5011D7E998
SHA-512:	389C0A59F111BC330633898B1A5719E2942947E64B32115CB037713D226AA0ED1AD806648A6AC80BDEE245D1BDA9F35A4F5D58211184E83DCD6FA278E607F1E
Malicious:	false
Preview:	.....p>.9..... .....X.. .h...y..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.5336	
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

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.5336	
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\Microsoft\CLR_v4.0_32\UsageLogs\DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe.log	
Process:	C:\Users\user\Desktop\DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1402
Entropy (8bit):	5.338819835253785
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84bE4KnKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7csXE8:MIHK5HKXE1qHxvbHKnYHKhQnoPtHoxHH
MD5:	3E457A94831A76170EF8D114082063EE
SHA1:	96C395587FE41523FADB9A9AC2853DF90BD530A3
SHA-256:	4728D230B92E50D7F01F3E1AD3E95D02B075178AFB80890274A59D3094F48299
SHA-512:	1507FF7C5E13DA5299E30ADC5C9137ED9A9BE3DD255925732A9C0D35C355DD5D626D72D23C8858F119A6DFC737818B84E984D6921FA227203E4EA1AB33FE5F
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,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configu

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Files.exe.log	
Process:	C:\Users\user\AppData\Roaming\Files.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1402
Entropy (8bit):	5.338819835253785
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84bE4KnKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7csXE8:MIHK5HKXE1qHxvbHKnYHKhQnoPtHoxHH
MD5:	3E457A94831A76170EF8D114082063EE
SHA1:	96C395587FE41523FADB9A9AC2853DF90BD530A3
SHA-256:	4728D230B92E50D7F01F3E1AD3E95D02B075178AFB80890274A59D3094F48299
SHA-512:	1507FF7C5E13DA5299E30ADC5C9137ED9A9BE3DD255925732A9C0D35C355DD5D626D72D23C8858F119A6DFC737818B84E984D6921FA227203E4EA1AB33FE5F
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,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configu

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Process:	C:\Users\user\Desktop\DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	41064
Entropy (8bit):	6.164873449128079
Encrypted:	false
SSDEEP:	384:FtpFVLK0MsihB9VKS7xdgE7KJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+sPZTd:ZBMs2SqdD86Iq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Joe Sandbox View:	• 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 • Filename: NEWQUOTATION#280321_RFQ_PRODUCTS_ENQUIRY_TRINITY_VIETNAM_CO.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 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_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	887296
Entropy (8bit):	6.554991291217796
Encrypted:	false
SSDEEP:	12288:yaY2pIV1Fn6OAVo1TniJM8R0aVEu0AxTd9lB3pa77FMHK25PPlXU:y65o12MCPWbAd7pk7F+K25ZU
MD5:	4FFB9EE56BAEED64D186D62DE5C56A05
SHA1:	2982AD3DD5578B7595A8A2CE6DFF5F7BCC9A1140
SHA-256:	79614387D51E432E6681D699A42018DDB1A91106B47FB2EDE9BAC493DD5814F5
SHA-512:	C0A9BD2EC83F4D8ED9207AD8FB36EB4B9EDC2B7CC116158B685F0759D356332DB0AB491D36644C17CA42ADE1E78E260940444A37371D72DBD771B102EBC773 5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 19%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....hOM.....N.... .....@.. ....`.....O..... ..... ..H.....text...T.... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....0.....H.....\...n.....1....G..B.....m.+.P.;..d.N.c.-y...-..U.~....?^.l...{`W...1..g.[...Y.....)1N.%./.....5m.R.....0_.#.G..- .o.."...W.\....'..-._F.T.}r.o.S.....I%$...&.....2;.....X...-.9F9"...v.s..fS..Q...ic%6.*.8.,.T.../.7.qW.v.D.9.....=.F%.v.....s....5V%.9.!.....'W(..+2h.w\.|s.....E...f.&%..f..U.ogJ.%.. U.JPJ...I..{.u.....K.j...2.*..[....x....*.....).....|?!.J.'<"8j.....

C:\Users\user\AppData\Roaming\Files.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\AppData\Roaming\Files.exe:Zone.Identifier	
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):	6.554991291217796
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe
File size:	887296
MD5:	4ffb9ee56baeed64d186d62de5c56a05
SHA1:	2982ad3dd5578b7595a8a2ce6dff5f7bcc9a1140
SHA256:	79614387d51e432e6681d699a42018ddb1a91106b47fb2ede9bac493dd5814f5
SHA512:	c0a9bd2ec83f4d8ed9207ad8fb36eb4b9edc2b7cc116158b685f0759d356332db0ab491d36644c17ca42ade1e78e260940444a37371d72dbd771b102ebc77305
SSDEEP:	12288:yaY2pIV1Fn6OAVo1TniJM8R0aVEu0AxTd9lB3pa77FMHK25PPlXU:y65o12MCPWbAd7pk7F+K25ZU
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....hOM.....N.... .....@.. .....`.....

File Icon

Icon Hash:	eaee8e96b2a8e0b2

Static PE Info

General

Entrypoint:	0x4ccb4e
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:	0x4D4F68B1 [Mon Feb 7 03:36:17 2011 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4

General

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xccafc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xce000	0xd8da	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xdc000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xcab54	0xcac00	False	0.617873863286	data	6.57591670371	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xce000	0xd8da	0xda00	False	0.0915818520642	data	3.77481945423	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	0x384	data		
RT_MANIFEST	0xdb6f0	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 2008 <2EFC?D72:9;F96>6826?
Assembly Version	1.0.0.0
InternalName	abbc.exe
FileVersion	6.9.12.15
CompanyName	<2EFC?D72:9;F96>6826?
Comments	7B?F?DA@6BHE@H==D
ProductName	DA4;=?2EI7C=FF5JCG
ProductVersion	6.9.12.15
FileDescription	DA4;=?2EI7C=FF5JCG
OriginalFilename	abbc.exe

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:07:16.850224972 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:07:16.863722086 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 8, 2021 12:07:17.778130054 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:07:17.790688992 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 8, 2021 12:07:19.989392042 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:07:20.008362055 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 12:07:28.127562046 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:07:28.167560101 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 8, 2021 12:07:28.438071966 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:07:28.466216087 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 8, 2021 12:07:28.487775087 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:07:28.500979900 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 8, 2021 12:07:29.315218925 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:07:29.329554081 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 8, 2021 12:07:47.464927912 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:07:47.477982998 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 8, 2021 12:07:48.817303896 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:07:48.831751108 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 8, 2021 12:07:49.468297005 CEST	63492	53	192.168.2.3	8.8.8.8

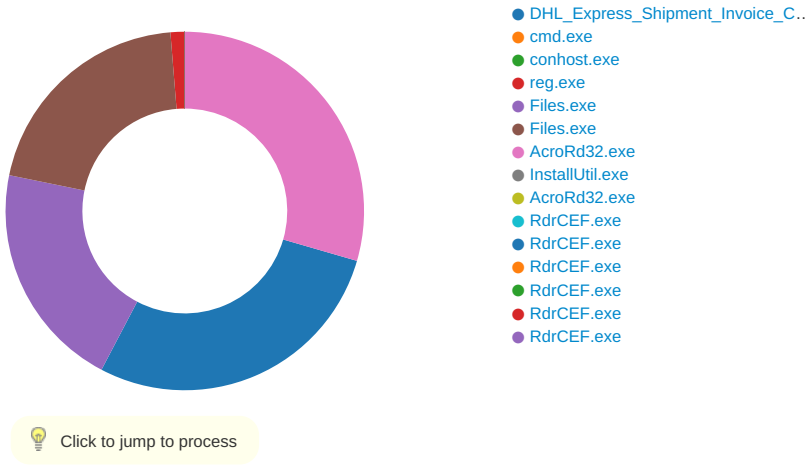
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:07:49.481710911 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 8, 2021 12:07:50.287034035 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:07:50.299288988 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 8, 2021 12:07:51.004914999 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:07:51.019094944 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 8, 2021 12:07:51.445460081 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:07:51.485548973 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 8, 2021 12:07:52.017590046 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:07:52.047310114 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 8, 2021 12:07:52.905920982 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:07:52.918490887 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 8, 2021 12:07:53.664814949 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:07:53.677771091 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 8, 2021 12:07:55.551908016 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:07:55.566189051 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 8, 2021 12:07:56.030512094 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:07:56.042367935 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 8, 2021 12:08:09.881002903 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:08:09.893765926 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 8, 2021 12:08:10.302892923 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:08:10.316248894 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 8, 2021 12:08:10.349073887 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:08:10.361949921 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 8, 2021 12:08:12.422161102 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:08:12.448431015 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 8, 2021 12:08:12.802336931 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:08:12.815521955 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 8, 2021 12:08:12.861136913 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:08:12.888497114 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 8, 2021 12:08:13.339987993 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:08:13.352734089 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 8, 2021 12:08:15.949263096 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:08:15.962547064 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 8, 2021 12:08:18.422380924 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:08:18.434819937 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 8, 2021 12:08:19.975502968 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:08:19.988317013 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 8, 2021 12:08:23.361908913 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:08:23.380319118 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 8, 2021 12:08:24.471626043 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:08:24.484843016 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 8, 2021 12:08:25.244359970 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:08:25.256722927 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 8, 2021 12:08:35.188877106 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:08:35.221174002 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 8, 2021 12:08:35.969105959 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:08:35.982182980 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 8, 2021 12:08:42.666764975 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:08:42.685354948 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 12:09:03.190666914 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:09:03.193145037 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:09:03.211342096 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 8, 2021 12:09:03.214662075 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 8, 2021 12:09:04.206573963 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:09:04.206692934 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:09:04.221847057 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 8, 2021 12:09:04.225342035 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 8, 2021 12:09:05.222249031 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:09:05.222362995 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:09:05.234791994 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 8, 2021 12:09:05.234875917 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 8, 2021 12:09:07.225281000 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:09:07.225343943 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:09:07.238141060 CEST	53	64910	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:09:07.238471985 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 8, 2021 12:09:13.201883078 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:09:13.202337980 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:09:13.216866970 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 8, 2021 12:09:13.220603943 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 8, 2021 12:09:22.358563900 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:09:22.374238968 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 8, 2021 12:09:25.308048964 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:09:25.341161966 CEST	53	56130	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process:
DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe
PID: 5644 Parent PID: 5656

General

Start time:	12:07:26
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe'
Imagebase:	0xe20000
File size:	887296 bytes
MD5 hash:	4FFB9EE56BAEED64D186D62DE5C56A05
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: 00000000.00000002.310359944.000000000425A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.311089829.0000000004309000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.311979523.00000000044CF000.00000004.00000001.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	6DFFCF06	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	6DFFCF06	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	6FD6EEB	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	6FD6EEB	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	6FD6EEB	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E30C78D	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\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 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 c0 00 00 00 02 00 00 9a 80 01 00 03 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....Z.Z.......... ....0..T...........r... ....@.. ....`.................	success or wait	1	6FD6EEB	CopyFileExW
C:\Users\user\AppData\Roaming\Files.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 b1 68 4f 4d 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 ac 0c 00 00 dc 00 00 00 00 00 00 4e cb 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....hOM.......... ....N.... ....@.. ....`.................	success or wait	4	6FD6EEB	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	6FD6EEB	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe.log	unknown	1402	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E30C907	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	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CE41B4F	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: 5784 Parent PID: 5644

General

Start time:	12:07:47

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

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5056 Parent PID: 5784

General

Start time:	12:07:47
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: reg.exe PID: 5424 Parent PID: 5784

General

Start time:	12:07:47
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:	0xca0000
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	CA5A1D	RegSetValueExW

Analysis Process: Files.exe PID: 6804 Parent PID: 3388

General

Start time:	12:08:07
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Roaming\Files.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Files.exe'
Imagebase:	0x5a0000
File size:	887296 bytes
MD5 hash:	4FFB9EE56BAEED64D186D62DE5C56A05
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 19%, ReversingLabs
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	6DFFCF06	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	6DFFCF06	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	6E30C78D	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\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	6E30C907	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	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CE41B4F	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: 6860 Parent PID: 5644

General

Start time:	12:08:09

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:	0x340000
File size:	887296 bytes
MD5 hash:	4FFB9EE56BAEED64D186D62DE5C56A05
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: 00000014.00000002.509008335.0000000003A9F000.00000004.00000001.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	6DFFCF06	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	6DFFCF06	unknown
C:\Users\user\AppData\Roaming\DHL Overdue Account Notice - 1301356423.PDF	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CE41E60	CreateFileW

File Written

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 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	6CE41B4F	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	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CE41B4F	ReadFile

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: AcroRd32.exe PID: 5288 Parent PID: 6860

General

Start time:	12:08:45
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:	0xf00000
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	object name collision	1	F365C3	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	object name collision	1	F5AE05	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.5336	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	F4EA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock5288.1.1672047883.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	F82657	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	F4EA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210408190856Z-251.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	F4EA85	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	FC83C8	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	FC83C8	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	FC83C8	HttpSendRequestA
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	FC83C8	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	FC83C8	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	FC83C8	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rri4nq2_10dppi2_448.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	F4EA85	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	3	F4EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rnn0i35_10dppi3_448.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	F4EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1dkfe5g_10dppi4_448.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	F4EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R18c7yim_10dppi5_448.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	F4EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1utfsgj_10dppi6_448.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	F4EA85	NtCreateFile

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.5336	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst	success or wait	1	F8D405	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	F4CF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	F4D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	F4D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo	success or wait	1	F4D41D	NtCreateKey

Analysis Process: InstallUtil.exe PID: 5248 Parent PID: 6860

General

Start time:	12:08:46
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:	0xf00000
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: 0000001A.00000002.493944777.00000000034C1000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

Analysis Process: AcroRd32.exe PID: 5336 Parent PID: 5288

General

Start time:	12:08:47
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:	0xf00000
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: RdrCEF.exe PID: 4880 Parent PID: 5288

General

Start time:	12:08:55
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:	0x220000
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: 5024 Parent PID: 4880

General

Start time:	12:08:58
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=1732,146401266259001 19066,9769525679105844933,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=2690794570082519975 --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=2690794570082519975 --renderer-client-id=2 --mojo-platform-channel-handle=1724 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x220000
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: 5632 Parent PID: 4880

General

Start time:	12:08:59
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=1732,1464012662590011906 6,9769525679105844933,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=7685701926627287920 --mojo-platform-channel-handle=1752 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0x220000
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: 6736 Parent PID: 4880

General

Start time:	12:09:02
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=1732,146401266259001 19066,9769525679105844933,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=6749621257665537764 --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=6749621257665537764 --renderer-client-id=4 --mojo-platform-channel-handle=1852 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x220000
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: 6852 Parent PID: 4880

General

Start time:	12:09:04
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=1732,146401266259001 19066,9769525679105844933,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=7499266669204803197 --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=7499266669204803197 --renderer-client-id=5 --mojo-platform-channel-handle=1864 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x220000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: RdrCEF.exe PID: 1332 Parent PID: 4880

General

Start time:	12:09:06
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=1732,146401266259001 19066,9769525679105844933,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=6985995476041547175 --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=6985995476041547175 --renderer-client-id=6 --mojo-platform-channel-handle=2148 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x220000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7

Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

Code Analysis