ID: 791300
Sample Name: Bordereau d'annonce de livraison.pdf
Cookbook: defaultwindowspdfcookbook.jbs
Time: 09:53:28
Date: 25/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

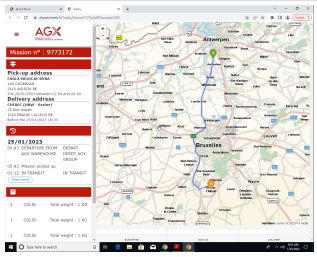
Windows Analysis Report

Bordereau d'annonce de livraison.pdf

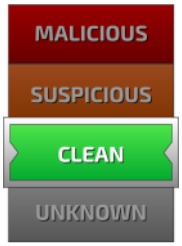
Overview

General Information

Sample Name:	Bordereau d'annonce de livraison.pdf
Analysis ID:	791300
MD5:	dc3036432aeb9c..
SHA1:	71bbfb3a441c3d..
SHA256:	d2f9be8a683358..
Infos:	



Detection

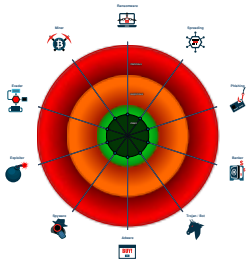


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- JA3 SSL client fingerprint seen in co…
- IP address seen in connection with …

Classification



Process Tree

- **System is w10x64**
- AcroRd32.exe (PID: 2440 cmdline: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:\Users\user\Desktop\Bordereau d'annonce de livraison.pdf MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 5040 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
- chrome.exe (PID: 3456 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 920 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --mojo-platform-channel-handle=2008 --field-trial-handle=1672,i,11613717386682731625,2570180296813603654,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 6404 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://dispatchweb.eureka-technology.fr//webmanager/authentification.aspx?TrackID=212Tja4dDEsuszajw3450 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

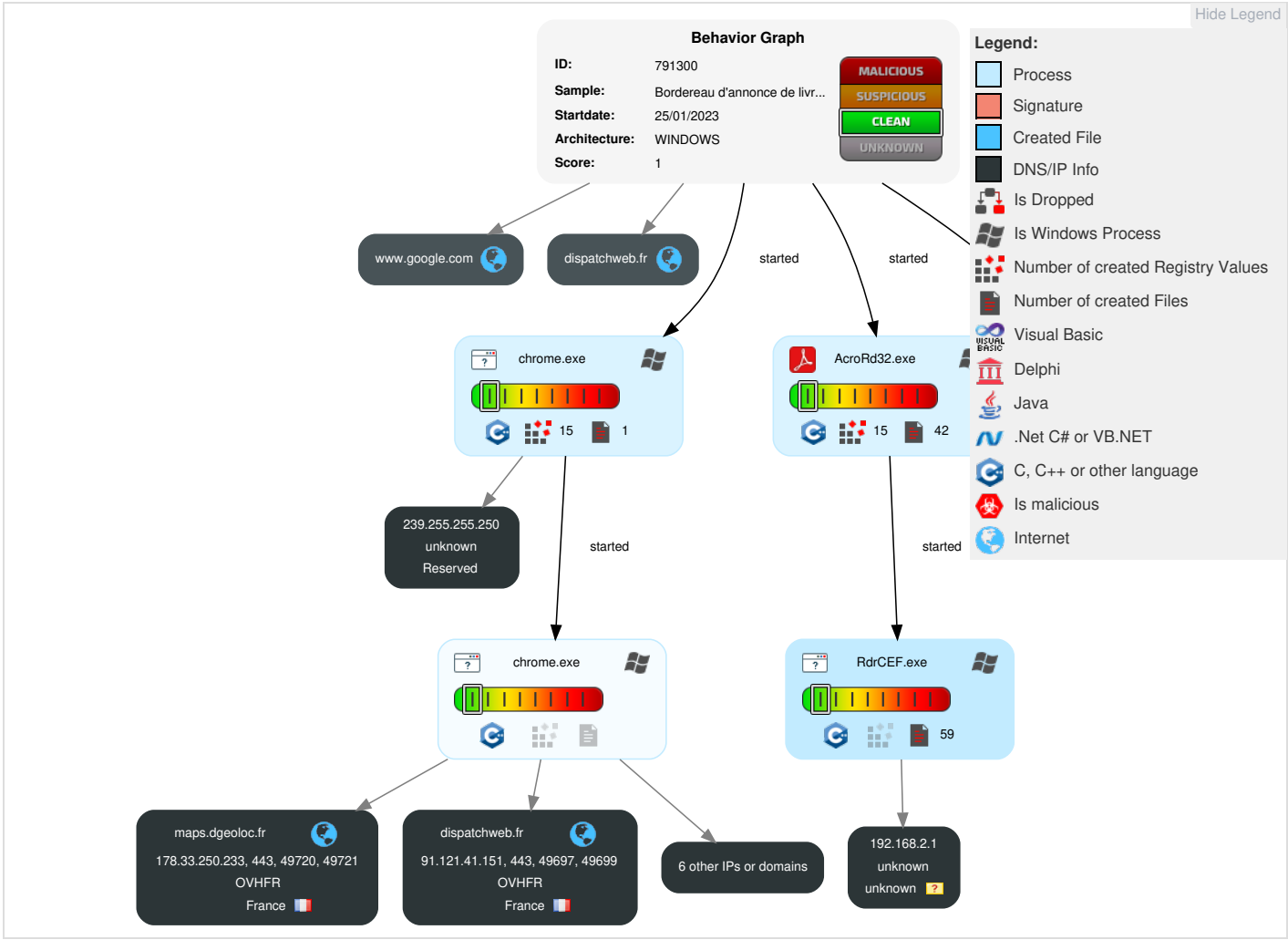
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Spearphishing Link	Windows Management Instrumentation	Path Interception	1 Process Injection	3 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	4 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

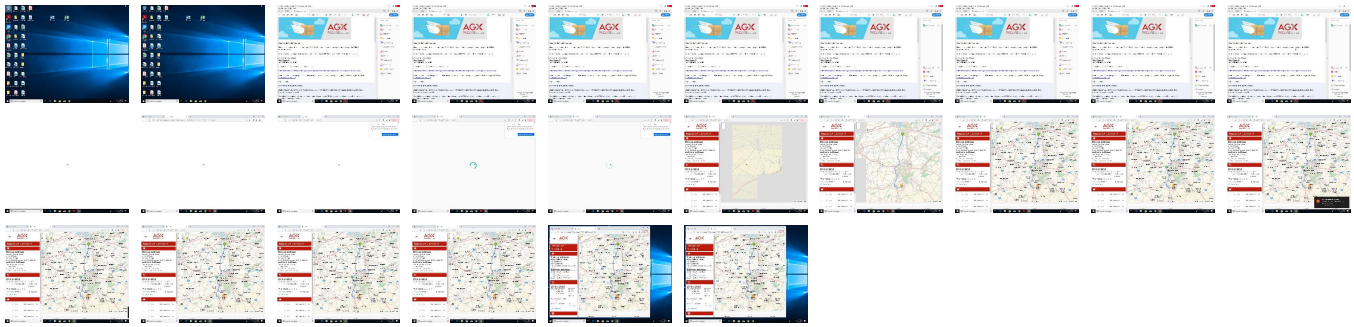
Behavior Graph

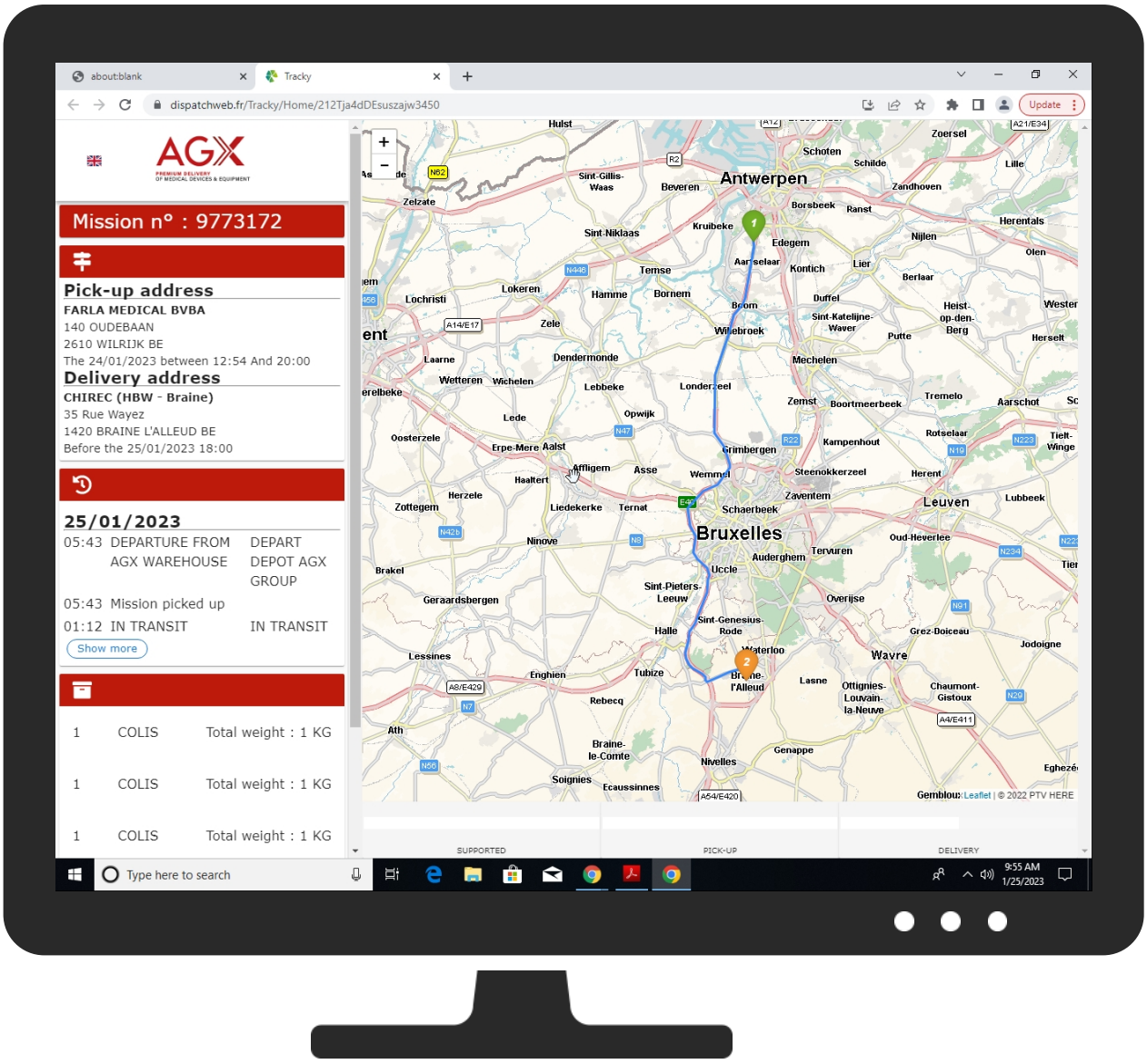


Screenshots

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
Bordereau d'annonce de livraison.pdf	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4066/2865/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-146759.09430753844,6017122.866609075,-141867.12449728715,6022014.83641933	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4066/2869/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-146759.09430753844,5997554.987368072,-141867.12449728715,6002446.957178321	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/525/344/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=508764.86026613327,6535671.666495712,547900.6187481434,6574807.424977722	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/522/342/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=391357.58482010243,6613943.183459732,430493.3433021127,6653078.941941745	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/523/344/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=430493.3433021127,6535671.666495712,469629.101784123,6574807.424977722	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4067/2869/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-141867.12449728715,5997554.987368072,-136975.15468703586,6002446.957178321	0%	Avira URL Cloud	safe	
http://https://dispatchweb.fr/Tracky/dist/css/app.css	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/525/342/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=508764.86026613327,6613943.183459732,547900.6187481434,6653078.941941745	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4068/2867/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-136975.15468703586,6007338.926988576,-132083.1848767846,6012230.896798822	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4067/2868/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-141867.12449728715,6002446.957178321,-136975.15468703586,6007338.926988576	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/525/341/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=508764.86026613327,6653078.941941745,547900.6187481434,6692214.700423751	0%	Avira URL Cloud	safe	
http://dispatchweb.eureka-technology.fr//webmanager/authentification.aspx?TrackID=212Tja4dDEsuszajw3450	0%	Avira URL Cloud	safe	
http://https://dispatchweb.fr/webmanager/WCFDispatchAPI.svc/REST_HTTPS/Json/GetListAllAttachedFilesShipment	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4066/2867/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-146759.09430753844,6007338.926988576,-141867.12449728715,6012230.896798822	0%	Avira URL Cloud	safe	
http://https://dispatchweb.fr/Tracky/serviceworker	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/524/343/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=469629.101784123,6574807.424977722,508764.86026613327,6613943.183459732	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/522/344/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=391357.58482010243,6535671.666495712,430493.3433021127,6574807.424977722	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/526/341/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=547900.6187481434,6653078.941941745,587036.3772301538,6692214.700423751	0%	Avira URL Cloud	safe	
http://https://dispatchweb.fr/webmanager/WCFDispatchAPI.svc/REST_HTTPS/Json/Shipments	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4066/2866/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-146759.09430753844,6012230.896798822,-141867.12449728715,6017122.866609075	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4069/2868/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-132083.1848767846,6002446.957178321,-127191.21506653332,6007338.926988576	0%	Avira URL Cloud	safe	
http://https://dispatchweb.fr/Tracky/dist/app.js	0%	Avira URL Cloud	safe	
http://https://dispatchweb.fr/Tracky/dist/img/favicon.ico	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4068/2868/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-136975.15468703586,6002446.957178321,-132083.1848767846,6007338.926988576	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4067/2867/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-141867.12449728715,6007338.926988576,-136975.15468703586,6012230.896798822	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4069/2865/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-132083.1848767846,6017122.866609075,-127191.21506653332,6022014.83641933	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4068/2869/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-136975.15468703586,5997554.987368072,-132083.1848767846,6002446.957178321	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/523/343/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=430493.3433021127,6574807.424977722,469629.101784123,6613943.183459732	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/526/343/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=547900.6187481434,6574807.424977722,587036.3772301538,6613943.183459732	0%	Avira URL Cloud	safe	
http://https://dispatchweb.fr/Tracky/dist/img/markers-soft.png	0%	Avira URL Cloud	safe	
http://https://dispatchweb.eureka-technology.fr/agx/common-tracky.css	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/524/342/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=469629.101784123,6613943.183459732,508764.86026613327,6653078.941941745	0%	Avira URL Cloud	safe	
http://https://dispatchweb.fr/Tracky/manifest.json	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/WMS?xtok=ac1478af-8306-4555-8eee-7e9fedb0f887&service=WMS&request=GetMap&version=1.1.1&layers=xmap-silkysand-fg&styles=&format=image%2Fpng&transparent=false&crs=null&upperCase=false&srs=EPSG%3A3857&width=884&height=843&bbox=413830.0711359443,6543162.4952676585,548970.737144136,6672035.324956465	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4069/2869/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-132083.1848767846,5997554.987368072,-127191.21506653332,6002446.957178321	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/526/344/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=547900.6187481434,6535671.666495712,587036.3772301538,6574807.424977722	0%	Avira URL Cloud	safe	
http://https://dispatchweb.fr/webmanager/WCFDispatchAPI.svc/REST_HTTPS/Json/GetTrackyConfiguration?trackId=212Tja4dDEsuszajw3450&token=	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/522/341/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=391357.58482010243,6653078.941941745,430493.3433021127,6692214.700423751	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/525/343/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=508764.86026613327,6574807.424977722,547900.6187481434,6613943.183459732	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/524/341/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=469629.101784123,6653078.941941745,508764.86026613327,6692214.700423751	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/523/342/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=430493.3433021127,6613943.183459732,469629.101784123,6653078.941941745	0%	Avira URL Cloud	safe	
http://dispatchweb.eureka-technology.fr//webmanager/authentification.aspx?TrackID=212Tja4dDEsuszajw3	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/WMS?xtok=ac1478af-8306-4555-8eee-7e9fedb0f887&service=WMS&request=GetMap&version=1.1.1&layers=xmap-silkysand-fg&styles=&format=image%2Fpng&transparent=false&crs=null&upperCase=false&srs=EPSG%3A3857&width=712&height=802&bbox=426977.2400009946,6546219.976399064,535823.5682790857,6668824.96976849	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4067/2866/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-141867.12449728715,6012230.896798822,-136975.15468703586,6017122.866609075	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/522/343/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=391357.58482010243,6574807.424977722,430493.3433021127,6613943.183459732	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4067/2865/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-141867.12449728715,6017122.866609075,-136975.15468703586,6022014.83641933	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4068/2866/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-136975.15468703586,6012230.896798822,-132083.1848767846,6017122.866609075	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/CalculateItinerary	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4066/2868/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-146759.09430753844,6002446.957178321,-141867.12449728715,6007338.926988576	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/523/341/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=430493.3433021127,6653078.941941745,469629.101784123,6692214.700423751	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4069/2867/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-132083.1848767846,6007338.926988576,-127191.21506653332,6012230.896798822	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/526/342/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=547900.6187481434,6613943.18345 9732,587036.3772301538,6653078.941941745	0%	Avira URL Cloud	safe	
http://https://dispatchweb.fr/Tracky/icon_192x192.9a7cf1309368a6585211a0524a3bcbcc.png	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/524/344/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=469629.101784123,6535671.666495 712,508764.86026613327,6574807.424977722	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4068/2865/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-136975.15468703586,6017122.866609075,-132083.1848767846,6022014.83641933	0%	Avira URL Cloud	safe	
http://https://dispatchweb.eureka-technology.fr/agx/images/header.png	0%	Avira URL Cloud	safe	
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4069/2866/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-132083.1848767846,6012230.896798822,-127191.21506653332,6017122.866609075	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.203.109	true	false		high
maps.dgeoloc.fr	178.33.250.233	true	false		unknown
www.google.com	142.250.203.100	true	false		high
dispatchweb.fr	91.121.41.151	true	false		unknown
clients.l.google.com	142.250.203.110	true	false		high
clients2.google.com	unknown	unknown	false		high
dispatchweb.eureka-technology.fr	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://dispatchweb.fr/Tracky/dist/css/app.css	false	• Avira URL Cloud: safe	unknown
http://https://dispatchweb.fr/webmanager/WCFDispatchAPI.svc/REST_HTTPS/Json/GetListAllAttachedFilesShipment	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/523/344/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=430493.3433021127,6535671.666495712,469629.101784123,6574807.424977722	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/525/344/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=508764.86026613327,6535671.666495712,547900.6187481434,6574807.424977722	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4066/2869/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-146759.09430753844,5997554.987368072,-141867.12449728715,6002446.957178321	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4066/2865/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-146759.09430753844,6017122.866609075,-141867.12449728715,6022014.83641933	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/525/342/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=508764.86026613327,6613943.183459732,547900.6187481434,6653078.941941745	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4067/2869/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-141867.12449728715,5997554.987368072,-136975.15468703586,6002446.957178321	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/522/342/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=391357.58482010243,6613943.183459732,430493.3433021127,6653078.941941745	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4068/2867/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-136975.15468703586,6007338.926988576,-132083.1848767846,6012230.896798822	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4067/2868/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-141867.12449728715,6002446.957178321,-136975.15468703586,6007338.926988576	false	• Avira URL Cloud: safe	unknown
http://https://dispatchweb.fr/Tracky/Home/212Tja4dDEsuszajw3450	false		unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/525/341/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=508764.86026613327,6653078.941941745,547900.6187481434,6692214.700423751	false	• Avira URL Cloud: safe	unknown
http://dispatchweb.eureka-technology.fr//webmanager/authentification.aspx?TrackID=212Tja4dDEsuszajw3450	false	• Avira URL Cloud: safe	unknown
http://https://dispatchweb.fr/Tracky/serviceworker	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4066/2867/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-146759.09430753844,6007338.926988576,-141867.12449728715,6012230.896798822	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/522/344/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=391357.58482010243,6535671.666495712,430493.3433021127,6574807.424977722	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/526/341/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=547900.6187481434,6653078.941941745,587036.3772301538,6692214.700423751	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/524/343/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=469629.101784123,6574807.424977722,508764.86026613327,6613943.183459732	false	• Avira URL Cloud: safe	unknown
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.81&lang=en-GB&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://dispatchweb.fr/webmanager/WCFDispatchAPI.svc/REST_HTTPS/Json/Shipments	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4066/2866/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-146759.09430753844,6012230.896798822,-141867.12449728715,6017122.866609075	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4069/2868/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-132083.1848767846,6002446.957178321,-127191.21506653332,6007338.926988576	false	• Avira URL Cloud: safe	unknown
http://https://dispatchweb.fr/Tracky/dist/app.js	false	• Avira URL Cloud: safe	unknown
http://https://dispatchweb.fr/Tracky/dist/img/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4068/2868/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-136975.15468703586,6002446.957178321,-132083.1848767846,6007338.926988576	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4067/2867/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-141867.12449728715,6007338.926988576,-136975.15468703586,6012230.896798822	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4069/2865/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-132083.1848767846,6017122.866609075,-127191.21506653332,6022014.83641933	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/526/343/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=547900.6187481434,6574807.424977722,587036.3772301538,6613943.183459732	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/523/343/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=430493.3433021127,6574807.424977722,469629.101784123,6613943.183459732	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4068/2869/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-136975.15468703586,5997554.987368072,-132083.1848767846,6002446.957178321	false	• Avira URL Cloud: safe	unknown
http://https://dispatchweb.eureka-technology.fr/agx/common-tracky.css	false	• Avira URL Cloud: safe	unknown
http://https://dispatchweb.fr/Tracky/dist/img/markers-soft.png	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/524/342/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=469629.101784123,6613943.183459732,508764.86026613327,6653078.941941745	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/WMS?xtok=ac1478af-8306-4555-8eee-7e9fedb0f887&service=WMS&request=GetMap&version=1.1.1&layers=xmap-silkysand-fg&styles=&format=image%2Fpng&transparent=false&crs=null&upperCase=false&srs=EPSG%3A3857&width=884&height=843&bbox=413830.0711359443,6543162.4952676585,548970.737144136,6672035.324956465	false	• Avira URL Cloud: safe	unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://dispatchweb.fr/Tracky/manifest.json	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4069/2869/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-132083.1848767846,5997554.987368072,-127191.21506653332,6002446.957178321	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/526/344/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=547900.6187481434,6535671.666495712,587036.3772301538,6574807.424977722	false	• Avira URL Cloud: safe	unknown

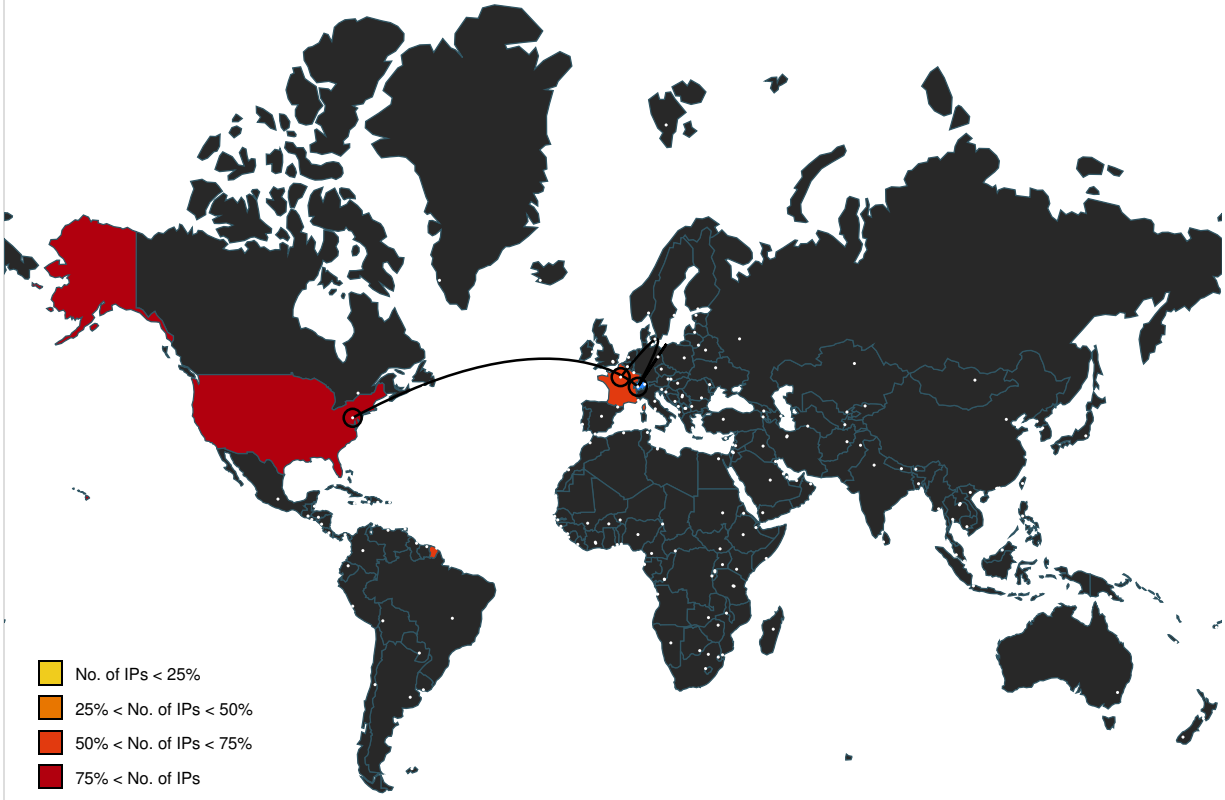
Name	Malicious	Antivirus Detection	Reputation
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/525/343/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=508764.86026613327,6574807.424977722,547900.6187481434,6613943.183459732	false	• Avira URL Cloud: safe	unknown
http://https://dispatchweb.fr/webmanager/WCFDispatchAPI.svc/REST_HTTPS/Json/GetTrackyConfiguration?trackId=212Tja4dDEsuszajw3450&token=	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/522/341/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=391357.58482010243,6653078.941941745,430493.3433021127,6692214.700423751	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4067/2866/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-141867.12449728715,6012230.896798822,-136975.15468703586,6017122.866609075	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/524/341/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=469629.101784123,6653078.941941745,508764.86026613327,6692214.700423751	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/523/342/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=430493.3433021127,6613943.183459732,469629.101784123,6653078.941941745	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/WMS?xtok=ac1478af-8306-4555-8eee-7e9fedb0f887&service=WMS&request=GetMap&version=1.1.1&layers=xmap-silkysand-fg&styles=&format=image%2Fpng&transparent=false&crs=null&upperCase=false&srs=EPSG%3A3857&width=712&height=802&bbox=426977.2400009946,6546219.976399064,535823.5682790857,6668824.96976849	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/522/343/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=391357.58482010243,6574807.424977722,430493.3433021127,6613943.183459732	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4067/2865/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-141867.12449728715,6017122.866609075,-136975.15468703586,6022014.83641933	false	• Avira URL Cloud: safe	unknown
http://https://dispatchweb.fr/Tracky/Home/212Tja4dDEsuszajw3450	false		unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4068/2866/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-136975.15468703586,6012230.896798822,-132083.1848767846,6017122.866609075	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4066/2868/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-146759.09430753844,6002446.957178321,-141867.12449728715,6007338.926988576	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/CalculateItinerary	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4069/2867/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-132083.1848767846,6007338.926988576,-127191.21506653332,6012230.896798822	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/523/341/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=430493.3433021127,6653078.941941745,469629.101784123,6692214.700423751	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/526/342/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=547900.6187481434,6613943.183459732,587036.3772301538,6653078.941941745	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/524/344/10.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=469629.101784123,6535671.666495712,508764.86026613327,6574807.424977722	false	• Avira URL Cloud: safe	unknown
http://https://dispatchweb.fr/Tracky/icon_192x192.9a7cf1309368a6585211a0524a3bcbcc.png	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4068/2865/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-136975.15468703586,6017122.866609075,-132083.1848767846,6022014.83641933	false	• Avira URL Cloud: safe	unknown
http://https://dispatchweb.eureka-technology.fr/agx/images/header.png	false	• Avira URL Cloud: safe	unknown
http://https://maps.dgeoloc.fr/eurekamaps-release-338/EurekaMaps.svc/rest_https/WMS/GetTile/xmap-gravelpit-bg/4069/2866/13.png?service=WMS&request=GetMap&layers=&styles=&format=image%2Fjpeg&transparent=false&version=1.1.1&upperCase=false&token=ac1478af-8306-4555-8eee-7e9fedb0f887&width=256&height=256&srs=EPSG%3A3857&bbox=-132083.1848767846,6012230.896798822,-127191.21506653332,6017122.866609075	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://dispatchweb.eureka-technology.fr//webmanager/authentification.aspx?TrackID=212Tja4dDEsuszajw3	Bordereau d'annonce de livraison.pdf	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
239.255.255.250	unknown	Reserved		unknown	unknown	false
178.33.250.233	maps.dgeoloc.fr	France		16276	OVHFR	false
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.121.41.151	dispatchweb.fr	France		16276	OVHFR	false
142.250.203.109	accounts.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	791300
Start date and time:	2023-01-25 09:53:28 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Bordereau d'annonce de livraison.pdf
Cookbook file name:	defaultwindowspdfcookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	11
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:	CLEAN
Classification:	clean1.winPDF@36/55@16/8
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .pdf • Found PDF document • Browse: http://leafletjs.com/ • Close Viewer • Browse: http://leafletjs.com/

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, WmiPrvSE.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.4.250, 2.21.22.155, 2.21.22.179, 142.250.203.99, 34.104.35.123
- Excluded domains from analysis (whitelisted): ssl.adobe.com.edgekey.net, armmf.adobe.com, edgedl.me.gvt1.com, e4578.dscb.akamaiedge.net, acroipm2.adobe.com.edgesuite.net, a122.dscd.akamai.net, update.googleapis.com, ctldl.windowsupdate.com, clientservices.googleapis.com, acroipm2.adobe.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:54:26	API Interceptor	1x Sleep call for process: RdrCEF.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

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):	205
Entropy (8bit):	5.60119274457905
Encrypted:	false
SSDEEP:	3:m+lvns8RzYOCGLvHkWBGKuKjXKLNjKLuVCcMN9dZktaW9/JiTFJrqzOJkvP5m1:men9YOFLvEWdM9QHcMvQtdvi7Z+P41
MD5:	24BB8FD9E518CDB1CAC5E01E185DBBB5
SHA1:	E5D3254C5906B39D344A0CE6AA64E1140C87DC29
SHA-256:	3B806AAF5E57088BF50A2D08884BBD885185EAC91B776EFB7FCC33E4C1473BCA
SHA-512:	E5E1EF9B110C3FD44D602C44CAA9616040E383B7B1613F279C264166EBCD8E335D059CF02DDC154A7CC4D97CE760C4D96B13579E3C1964D65FFE9A51EEDE6AB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .....Q/....."#.D..q.;..A.A..Eo.....d.{v.^.G...d.W.:...P..k%..A..Eo.....

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):	174
Entropy (8bit):	5.553342767149127
Encrypted:	false
SSDEEP:	3:m+lF9NX6v8RzYOCGLvHktWVjjMJOGZktdKlte98fZe/O+/rkwGhkg4m1:mi9NqEYOFLvEkJjAKtdsQ8Be7Ywcr1
MD5:	BBCB468A5DFB7C1374FA838281F6663D
SHA1:	8FFBFB64F41FA20D6D76A2CC3A62E937F96AC297
SHA-256:	5AE82E7992A8FCADDCA573359B3FAEBBE46C61379A37F64FCAB132BBCFBF9B0F

SHA-512:	896FE63964E5BFBD9453EF3B8B5A1CF6ADB22596DA4094744A4672010C8F710E66DBD504B5531FAD6153A572AA25788E8C350080737E0601BFBB10A345FA0458
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,...._keyhttps://rna-resource.acrobat.com/init.js .F....Q/....."#.D).*.;..A.A..Eo.....C.....1.x.'.vI..*|Z..o...+.4....0..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):	246
Entropy (8bit):	5.554898839285145
Encrypted:	false
SSDEEP:	6:mMyEYOFLvEWdVFLBKFjVFLBKFlQhuGBRG9t2+4t/RlUoSjGY1:DyeRVFAFjVFAFCsk+4tZlUo6
MD5:	12C73774F94AC0FE47822CC8B874A1FB
SHA1:	8556095B5FF3F8315A8B2526340BAB9D276A6768
SHA-256:	B18C7776FD065790DA9CB7A3615CB2A9E116FED61A2F96506DA28CDFE98E6155
SHA-512:	23C5DC5DA3D7D288E871A17A74419B75281E021BAD7AEA23FBE24C9B03F6E7578D024EC605CF92251CF68E55F528B6081ACA81A7E0E41C3894DF1813E26C5D D
Malicious:	false
Reputation:	low
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 .M....Q/....."#.DG.k.;..A.A..Eo..... .....hvDO.N.t@.....n.*..... ....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):	5.607888122332422
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RsrljQtz9uiWulHyA1:lbRkiD8Wl9jWus
MD5:	150E70D57AB857EB100ED1C74158D50E
SHA1:	4E92D0120692881376519 3C4DFE1C35F0DC48F54
SHA-256:	C2DC9FE340AABF112D3A1BCB5FDAC9252E522A85EBDE864D6413856A4BDABCE5
SHA-512:	1652B63D013C0B4500149DBD56AD50A6E34B5DC76F41859EE8A0A06B56479A4EE6C2E5628CB49B627F1A489963397876F8630B696DA565302517868CA1BAB015
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js .w....Q/....."#.D;R..;..A.A..Eo.....8 P..a...R.. Y....7.@..2Dm{..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.530726623968928
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVu/G5qjtsVyh9PT41:pyixRu5R2V41T
MD5:	C841E1E779EF49CC9143F9175256957D
SHA1:	AEEF82190E0EB6F94E7B7741F79E8DBBC3A6D0BD
SHA-256:	5F96D20D452874D5EEA7D488C179B1ABDB708C4E5359C26CCBE4D16C73E74BDE
SHA-512:	CE2447606BC9B2677B16ACCB61AAC005579B0FD01C1BB30ED36EA74AA27F8FFAE35EA774D1932D1459FD2B538F879F1364E9F1585F329F18C19D25093945EFC D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js .....Q/....."#.D.m.;..A.A..Eo.....Q$.....k.Q.....-_..y.....O...>..1....A..Eo.. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe

File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.598978474348319
Encrypted:	false
SSDEEP:	3:m+lifll08RzYOCGLvHkWBGKuKjXKoyNjXKLuV0GzlHfZktO+Y/l5lYo2sZl8xeGI:mvYOFLvEWdhwjQoJytu73Zll6P41
MD5:	C5898628310533AD8596302BF1B8D6D6
SHA1:	1E5B14DD635D5FC2B0DBFDDD654EC426EAE71FED
SHA-256:	BA81EF772412D5DA699E1BF18796F73A8EA1D9618380EB5D0AB964DE9B9857B6
SHA-512:	8803D779BD2B9A139B18FE3FA4886016798528B8056C641A9B733384EEB3BBCA7B9E9116A06378A0FFD34B63763CC28F5EA83C086E7B2AE3DA4147AD0251CE94
Malicious:	false
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .."...Q/....."#.D".Y.;..A.A..Eo.....c.%.....].>....uUf..N...k.....c..l.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):	209
Entropy (8bit):	5.508844885607996
Encrypted:	false
SSDEEP:	3:m+lZd8RzYOCGLvHkWBGKuKjXKX7KoQRA/KVdKLuVTG0+YoI8G9kZktmXlVcyxMtg:mJYOFLvEWdGQRQOdQE7oIF9jtGrD6g1
MD5:	C84441F9A9FC6D905D0C277658F18D01
SHA1:	918503F466AAD4D66C8C537C7B53FEF1E7BB20FE
SHA-256:	B5BC0F3F0170C9358870AA221AB1454F6C655B79D906ABBC9B78E6D89A38C59E
SHA-512:	A7BDB182C11162B6A52519B94BAD59C01217BB442F97A0FEA9B914AC7B214607EEC74A02ED3F90CC0CF3A00D8CEBD55DDA5F42D1623D6C54AF186E5FD963D9A4
Malicious:	false
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .3q...Q/....."#.D..m.;..A.A..Eo.....b+.....c..y/L....|y.n..C/I.....X7-ne.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):	179
Entropy (8bit):	5.516578320495111
Encrypted:	false
SSDEEP:	3:m+lLp08RzYOCGLvHkfaMMuVY+sGZktadVQMWqg4nRb7om5m1:mOYOFLvECMLlItxuR/41
MD5:	BFE267B86211604EDB40A4633CE25CAE
SHA1:	075E30520CDCBCA959A157C9260A248A0C39F3F1
SHA-256:	1270D8E5346E3F8B24D752EBA62C8EA5276A9800745549D678096571047A3563
SHA-512:	98361F25D416B0AF5176DB5BE05AE16A37EEAC2FB8A1D94F984B07C523E90EC60E3CEB9C35778C61E3859224A3D4E2D5DC9BA01C025103C19FF2CD84C99FA192
Malicious:	false
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .....Q/....."#.DF.*.;..A.A..Eo.....p.X.....y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.490293618680104
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtuVmzA9jtNlhby0zBUKSAA1:pRlmzA97b
MD5:	A4F93B19CFD29EC84E2E7286CD3D5722
SHA1:	D42BB31A3754A7F70DF03E8D4BBEC32654321602
SHA-256:	7D704CEBC8CFD193FB5AD8FF2D7F084C9612454F1067F8BDD35074F4635D8F65
SHA-512:	22650BAAF7F82A805779C49D5DC30A184FF5A81B84110E9EF67C64CD812A999E189F6BFE14D6DC41D0DB2B9C00EEB61958F36288756938D2F298E662F9602D7

Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .n`...Q/....."#.D.^y.;..A.A..Eo.....7O(.....Q..E.=....=h`t..t..3%A .F$..w..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):	177
Entropy (8bit):	5.507616775193039
Encrypted:	false
SSDEEP:	3:m+l64HXlA8RzYOCGLvHkjXMLOWFvczoYJZktR8/lkd1dn76KohyP5m1:md4HXXYOFLvEjMSWFvcotR8/lkjUdyPo
MD5:	3BC05C4BF3B6132ECCA39DACCBE7C98B
SHA1:	DF8844D94AF1C633AFBACBA4BB55CFE30973BF5B
SHA-256:	F8593D1DBA68829600CB748771C220EE23FB28889D582F58C1C1F001F31BB2BD
SHA-512:	ABF4D32D5B64FA6EBC0E947FC2E5A7CD244CF536BD627D824A96D45622807F2EB0165BDFA00E82C6F8B59618D74D2AF2ADE64852CD2086D810F0EA5693659E 67
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .....Q/....."#.D..*.;..A.A..Eo.....!.....PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....

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):	187
Entropy (8bit):	5.4903973245692015
Encrypted:	false
SSDEEP:	3:m+lpSUIlv8RzYOCGLvHkWBGKuK2fKVL1fAlsHRZktEfljUPqf9tsDMaPV44m1:mkl9YOFLvEWsfOLlhUtEfloPqVyM+VY1
MD5:	27916040593695B833308A43B975C3E5
SHA1:	FEB3D46D434F15E087882EC215B9D75076F8CBED
SHA-256:	F8FE21856FF2E1C28807C1725234350996303BD494E322D37BBF3AC380577343
SHA-512:	7838AB89E45B0907D07E2E8641C01F65715B5D5DFE7E1B01283EE16595CE8A02FE0DE62366925ECFB11552A37FFE3245B28D98A33B07B3523809320C340ABE4A
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ..^...Q/....."#.D."M.;..A.A..Eo....._..w.....q.O...j...._y..L^z...?..@N..A..Eo.....

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):	244
Entropy (8bit):	5.574260570987774
Encrypted:	false
SSDEEP:	6:mt9YOFLvEWdVFLBKFjVFLBKFlyotytwSeKaT9pr1:URVFAFjVFAFVgtwSeKaTL
MD5:	C5FAEBBB8AA1428D083CBC2A81E55F2D
SHA1:	0A5C3481437C19D772C7761B000EC30E19B30B93
SHA-256:	163E8081258997CCA432605BCD6F0C3CB5DB51A45BC99B2DFB6537BE614A20EB
SHA-512:	28225E5CE13BD1FF3ADC4B2E91D76DBE1A465E148F6B0CE779D81D93E7E9EC577E79E9100013209B602AC4A837CFBA3E01162A0656F48FAE5E586B12667DB3 C
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 ..3...Q/....."#.DP.t.;..A.A..Eo.....gR.D .....H...{...2../.k`..r4.C. .A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.473353666574867
Encrypted:	false

SSDEEP:	3:m+lx4F08RzYOCGLvHkWBGKuKjXKGBIEGdevA/KPWFvelK889dZktD/jyrpYFm1:ms2VYOFLvEWdvBIEGdeXu78sQtD/211
MD5:	6B24E05DE14C7E6E3D569FBD9CF857C6
SHA1:	69F49BA96ECFB2CA6770547AFA271C108E1827C6
SHA-256:	CAED0A310EF30C062DF10C10F4BDCC003066BCFDBB9103E9FAF3988D63F7106C
SHA-512:	29DC501C9F36D52DA77E726F26366442C88BCCE62340AAA5E57772C1B316AFCE8E9D871023FF736D33E48BFC9C34368A3FB9CF18537365130DA473FE24F2148
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .....Q/....."#.Dl.k.;..A.A..Eo.....-3.....A.o]@r..Q.....<w.....].n\....A..Eo .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.625632390001536
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQvTT6Rt+Lxm7OhKlvA1:RbR169RALxmJ
MD5:	EDBF6D05AC5B453CA0FEC798FDB05AA2
SHA1:	0E96F2247F0032399CF74FB87CFF7FC40D755E87
SHA-256:	31DE8653970EB087F6C14E4F1FDD10EAFD0765F17CF361760CD64AD1E1D8A087
SHA-512:	D6DA0ECE6B5B675CB066B52BB5D69FC17B66D343513957B3CD0452AA43B333B92E3793CA0AF25415EADBB1169259C9433CDBB7BA7E0D22D9E04AE0EAF6E9E567
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js .....Q/....."#.D..X.;..A.A..Eo.....n.....4T].....Tw.....(..b...EO....9.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.5775096495781655
Encrypted:	false
SSDEEP:	3:m+lx2gv8RzYOCGLvHkWBGKuKjXKX7KoQRA/KWEKPWFvWMUWZktgtFdF5YufMm1:ms2gEYOFLvEWdGQRQVuONtgPdFt1
MD5:	702AEA00FDDD933626983BA7F7A43450
SHA1:	F39EC289DED3674535FB9CADC3E87F686587A023
SHA-256:	977789AEB6672BCD7AB0CF3758CB29C40A01DC7C65D33CD8E95A96C8A38C9891
SHA-512:	E404C76BE72C25D8938472C885EE0C4605496DAA0F845F9D25886B6E2927F417A541AED6B130AB66CE4AAF765AE40C234A2FCC688FF9047CDF2C1642C268B058
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .....Q/....."#.D&.k.;..A.A..Eo.....k.N.....@..{o]...9o|..qY....T....{ ..u.b..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):	206
Entropy (8bit):	5.612572912176052
Encrypted:	false
SSDEEP:	3:m+lerlyv8RzYOCGLvHkWBGKuKjXKX+IAHKLuVsuebdZktWQlIEnNWQ1SUm1:mzyEYOFLvEWdrIOQkestVlIEt1S/1
MD5:	AC25D7C5830236F0B316C5F73AC3183D
SHA1:	52A0282749F6308C2A110EA97900891609332310
SHA-256:	66BD480F8F0B0A3E75F9D809650357A8231F0B29194AAEB75F2DEB1F56D71576
SHA-512:	4F43702AD814599C17E34491118A15FAF0924566D109E089798DCF7AAB7F425362FE27A147315634C044C53CB2539400C61A6C1A02144F7C52A706A1D9A22511
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..F...Q/....."#.DYLR.;..A.A..Eo.....;..=.....t\a.....x5.'OuE.C..@.....x..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):	218
Entropy (8bit):	5.537749611829213
Encrypted:	false
SSDEEP:	3:m+lKcv8RzYOCGLvHkWBGKuKjXKoyNH/KPWFvDTGzl/l9FGZktlClwJNqww6U+5m1:mnYOFLvEWdhwyu1Gn9DtlClwrqwK+41
MD5:	50426550BBCF881B044C7C596215751B
SHA1:	7DCDF405384F074DD0023D86A07C695A96ACADC7
SHA-256:	C77379BAF6F55CF3D51D7AD0C281A05FAA89CD275279DA704FB1AB4F6216A4E3
SHA-512:	37AB5E8FDFED56DFEA55448D8E242D10ACBB9BFB5E3D57F6A3B98A545DDE7AE5BBE01FBBB901E117E8370CCC54C71382E1DCE94042291144305CC4B4E2553C05
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .....Q/....."#.D..X.;..A.A..Eo.....H.3.....7...o..a=.98I.....(3.$ G.A..Eo.....

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):	230
Entropy (8bit):	5.614958137451049
Encrypted:	false
SSDEEP:	3:m+l26Xa8RzYOCGLvHkWBGKuKjXKeRKVlJ/2NAJVKH/KPWFv6Gz53xWZktP9llZX5:mYXYOFLvEWdrROk/RJbu825TtAfO441
MD5:	D633C202FFE91C67B0253494E6F0AEF4
SHA1:	F7E1099B501B138E14A4B5941188257007F4D516
SHA-256:	9C58E63FF8974265D297570A56CA2050584D3C284DD0CD51DEB530753E6749E2
SHA-512:	316D79C76763FD2BB11696EE08C49379D1944B2F3ADADCEC202AEADB7FA66E4EE6D1DD5CBA26E7EFB828F8359540D4BD153F39006DADB1D2D2300F3320F5BC80
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..9...Q/....."#.DN{R.;..A.A..Eo.....I.....~..rw.+[....!.)?..f.U..(=.=.A..Eo.....

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):	186
Entropy (8bit):	5.588810987211442
Encrypted:	false
SSDEEP:	3:m+lhD4ll08RzYOCGLvHkWBGKuKdTSVuE1GZktafllHzoIN1OFPL4m1:mmDEYOFLvEWXlum9tozV1QPLr1
MD5:	4893FB57F6C2C0E4F53525150B7B8381
SHA1:	A7BEE359B816C7238CFB7B141100290DF2E62397
SHA-256:	7FE18CC09BBB407CD2482C710D0C24A1D41782DB7A58A3CB1061F557F944D5F4
SHA-512:	68AC2BDCCDD941FBAD4425DAACBBA87B137DF46CD9D8E4EC967F80FB3970037088D189628F653C16667294C4710E21068AE4D6A93C185F4211EB21E5BCFA68FF
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ..R...Q/....."#.D..M.;..A.A..Eo.....9.....~]...%s..<...n.f..<.....1#..U..A..Eo.....

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):	207
Entropy (8bit):	5.566369058044112
Encrypted:	false
SSDEEP:	3:m+l+nq1A8RzYOCGLvHkWBGKuKjXKLNfKPWFviflzzYRqkZkt4FM8D6EsEJeUm1:m52YOFLvEWdMAuilEqjthEvsEJ41
MD5:	F5E585D737182D260C76FEA10DD3B2FA
SHA1:	B3A9227D8D824755E120C245FB2D436B2D5E8BD1
SHA-256:	229008D9D6EFE268A77CD121C0CE220149C1CB1903491C4D8053CBEFE32E9F46

SHA-512:	D8C21960603FCFD1FE4333076C1213969589F0F65708D15C4FD85514FBB08DAB223BA5E08CE8BB9B25E7A3428FF558CEC3B8ED2E8FEC1DA26A0A52851893D1(2
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .....Q/....."#.D..l.;..A.A..Eo.....o.....z._a...'.v.....4p3..1.']...A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.5469773549064305
Encrypted:	false
SSDEEP:	3:m+lf1UldA8RzYOCGLvHkWBGKuKjXK9QXAdWKfKPWFvmuOqkZkt8lIFoDb7T2/Mm1:mYilPYOFLvEWd8CAdAumqjt8Aong1
MD5:	8E6E9FFE8D9406D6CD40281B360A260C
SHA1:	B7BF956588A19361A628B4CB4CBB3A56857E8EA5
SHA-256:	EC865169C24029CA00FE5AA5D10D3C60E4CF0B0B9AAE03A4B2A2AFAA5C590DFD
SHA-512:	D3EDFC1ED5816995168E24696C3395C656540E04DDCCAC44B52FD48456638DB2A6B68F2F96D091268E57A95826F2742C54B37B10E28C66A5629219ADBC59776/
Malicious:	false
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .]-...Q/....."#.D..m.;..A.A..Eo.....#.....c}.H7M=M..-.....lx..R.I...}RI.$q.A..E o.....

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):	223
Entropy (8bit):	5.560466988820719
Encrypted:	false
SSDEEP:	3:m+l18t08RzYOCGLvHkWBGKuKjXKeRKVIJ/2oKPWFvCjCcGZktw/DOe28WlJLkxwS:mY8nYOFLvEWdrROk/luMCc9tGN16wG1
MD5:	6AA50751521CF277FA8770748EFE1A60
SHA1:	05AB7A39ED46C4C1511A4E75BA5BC4B62AA937E5
SHA-256:	9BAFF8DCF96CF6B09914DEB82EE68F9BFA92DF9713CD1DF2D618BAED29E036FF
SHA-512:	FFEC97D0D183B1919722D1E3C8A51E6953D88AB92AC49FADF78EBAA74E9B6DA11BC364B83D2D0EF81DA1ACD955A54E554C66D5830F3BCE6EF41F3BB612B2F EF8
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .....Q/....."#.D.'Q.;..A.A..Eo.....Lp.<.....%.k.SZ..~W.. ...:)'B..ad.....A..Eo.....

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):	213
Entropy (8bit):	5.645884863591164
Encrypted:	false
SSDEEP:	3:m+lstxt08RzYOCGLvHkWBGKuKjXKX+IAuAJVKjXKLuVY+PyAGZktB+tmPmJelc0A:mLrnYOFLvEWdrIoJUQX+qstBBeJli1
MD5:	5C7AEE6F952672DE9AB8CA71628036A7
SHA1:	C36B63A7F9400683EB068BC76F87948B05798E05
SHA-256:	C44A308DFE53975BE233829872D9F198F53941FFA9568EEDA1F615E9C3A3845E
SHA-512:	A45B7EA40DEF806B4999EBB9A13C24D15EB5A331F94D67303033A42AB7044C9BEAB000EF18E3FB7AC97FAE09E59F36B4D0A0FCA6BB2D788D291C0038F3E6C E23
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .>t...Q/....."#.D..R.;..A.A..Eo.....T.....;"./N_,.:C..2....9L.H...3:...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):	208
Entropy (8bit):	5.537896655144589
Encrypted:	false
SSDEEP:	3:m+lQ/pqv8RzYOCGLvHkWBGKuKjXKX+IALKPWFvX3M0KgfZkt56mgmOZLhT7Um1:mOEYOFLvEWdrlhu988St5zgm2d/1
MD5:	E4FF898AD53761C5344121FAC0171755
SHA1:	7C4EC34E6755385DE48C21268E2F7749FD5C8195
SHA-256:	C579C3C3E27C4834BBF64B8D651B65B217D642566729002053C879F66E28ADB1
SHA-512:	A3FDCC938DC4335557EBC6A8B6B1ABF437A4A59211E07147E2236DC4877909B7C7C55DE993F136B1DA85455475D0D6010C9423D5D0EF7E65AD67E5829FEA2E6
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .....Q/....."#.D@.P.;..A.A..Eo.....-.6.....Z.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....

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):	188
Entropy (8bit):	5.572997719999003
Encrypted:	false
SSDEEP:	3:m+l8UElLA8RzYOCGLvHkWBGKuKPK7CvJj+2oXdZktUFtGBiaQ562HvpMm1:mAElVYOFLvEW1Koj+2oXQtUFpx56uvp1
MD5:	0116C83080D8EAFA98F2B21027CAC421
SHA1:	AB4A6A6E681CBA4357FBCCDB565F3E0F2503549A
SHA-256:	DF626CF513B7F403ACBF05EA998B5EF79AEF6C6C7290AFCBD915F2FF6798E8D8
SHA-512:	E3AE70EDE55130C5917CCF80DE1E85FBE84D67B43D98AAEFCCC2AFD7850F4E62ADF1FE5918757850B2703E3F7B70BD025744294ED2A757DAC86B99D4C4CD03B0
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..i...Q/....."#.D..9.;..A.A..Eo.....N.5.....z?...SwC...^..y.....V..7R-O.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.615716655521179
Encrypted:	false
SSDEEP:	3:m+lSy/08RzYOCGLvHkWBGKuKjXKBRSJvBCv1KPWFvsOYJZktHtY8UDLY3PHVmOPj:mWYOFLvEWdBJvvuJDtHjUDLYtmOZn1
MD5:	B97CFADFCFBE5FA16DF735D885AAED72
SHA1:	6DA2E7A048E670C4ED538C6502874FC54CF4FC60
SHA-256:	D6A9BDD64FAEC870955E28D9A171D3BA19D0E89170CD6D86961887B6FEE034FB
SHA-512:	0EF5C3259E102ABED6363834989462A564E03B63DBA5FC7A9451662E9D220EA76B1E84482972A07EEF8C3EB2AFF04AD9063672FCE7A8493CDA2FF5A5D3E328E5
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js .....Q/....."#.D%.k.;..A.A..Eo.....o.^.....t.q..W.EZ....1...[.zC.7mD..A..Eo.....

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):	211
Entropy (8bit):	5.593079162066707
Encrypted:	false
SSDEEP:	3:m+lxCq//6v8RzYOCGLvHkWBGKuKCH6U4LJzWHK7WFvZTuEZktUbHllPpSKGoSSlf:msRPYOFLvEWla7zp7cuDtUBF8VPu1
MD5:	A0D1CB401673BC914B90ABEF8A5B1DA2
SHA1:	F12FA51CECFC618325DB1219C5236C51FDD493E5
SHA-256:	261128150E87726E0F57ABBEBDA774FCDD851731A45632FB8C35AF995612967A
SHA-512:	D6E884D7BD2E1F0B526ACC37239926CC135D032F8E213F9A4E26D2390C3356AB371DE002938CFF201FE6EF1381454DC2A204602395D68BE572DEA013CBF339E
Malicious:	false

Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .3....Q/....."#.D|.+.;..A.A..Eo.....I.@.....L...Im.@.....E.nW...IP..A..E o.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.575933087410918
Encrypted:	false
SSDEEP:	3:m+lQi9lC8RzYOCGLvHkWBGKuKjXKVRNUpXKLuV9S161UOGGZktm3/f6F4XVAZ+89:mKPYOFLvEWdENU9QFlxG9tJwiM3Y1
MD5:	7FC306A6217D1C072C27BC5D6751040C
SHA1:	981551C4465A1407381D53986FDE4D7B33D4D0C4
SHA-256:	59C5802A5E56232362C82F92A912F89FCF2FD867D48DE59E5E0E616693A40888
SHA-512:	4A0FFA7869B7A6003DBEB644C93EC36EA45A2A374EDB68BC911A0683B9383588FBB4E14E15DF62DFD4D094877F6EF352155CD717D01369C63479F388F81926B
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .u....Q/....."#.D..e.;..A.A..Eo.....L`.....M....m+lS..e.....<7.U.P8* .0K.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.6101610464434355
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQb/itnIjBRCh/41:XRc9vBIDi/
MD5:	F1110D8043BC2917F9DF97365AB8D16F
SHA1:	2990002DEB7EEEFA463B2B9C3B9BD0227F0DC7D0
SHA-256:	FEAB31B2A86435C6C6845DA98F2225FD373D4396DCC43C89794A2E9723325104
SHA-512:	1C59234CA2B9447A1B7D0E5BD3455F4CD8A353A685C21F0D01D414A600390F350BBAEE331FB270CE5CFC9965CBDA98F92DC07EE071CBEEBE680D073F89967A D9
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ..p...Q/....."#.D..w.;..A.A..Eo.....PJm...0x.x..RD...BB!@5..<..] ....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.57292221469655
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhukC/te9tRHl3kULIF4r1:bs6xRkieC/t6/F7LIF4
MD5:	5DC9A97BBB9C3ED2FE81C59E8CAA006E
SHA1:	96F4F4C824F05F64B9CA3B276B4D130CF6C95DD9
SHA-256:	0EFF92DD2AD306F848155CA750533FD1CB6F5D213A983B0D7A43E73D0DCDEE07
SHA-512:	42E1EA6C4144683CBE4F6C4A59C27C8A0169FF4411C8C586559A8F3AA618FB8E4519EA830B6343F8F8B7738BD4ABCFADABF28686420CCDEBB23DD9DF3F795C 4D
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ..a...Q/....."#.D...;..A.A..Eo.....Y.....P...#4..l....5. ..5..).w.. .h.~..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.497724007341834
Encrypted:	false

SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvuZ1MrzIcHkZktqeNECcu1isLK5y:mhYOFLvEWd/aFuwZ1MrVHjtREN941
MD5:	DDF40A5A6A245A580D9A5D93954BB736
SHA1:	FCE42CB796575F0C7FD4C6FDA48500C5C27EA427
SHA-256:	78CC5606BD577C0B0E911A2FE55FE80899E315D0477D4683A470CCA09F354F10
SHA-512:	D863580D66930931063CB3D5B69C99DFF6175A65B05A90A92B3213AE117963982AD68A1AC4F33566A483F02C25BB7021B7938BA13D56C489B1969DB4C13C18FC
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ..h...Q/....."#.D.my.;..A.A..Eo.....q.....a.f.m.i.o.p..3U5.....^...I.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):	208
Entropy (8bit):	5.493170049433148
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VlGXOdQt0Yjt/XTjBMqVd3G4K41:2DRuRfstjB9Vd2
MD5:	907B00301C0AEF47AEC7415831002721
SHA1:	CB2CE08CC611AA56084BDA97326F0ADA10D2E450
SHA-256:	64722F16849A49BEBB9DA468BAC1DEE41BD3DE1B8AA0BB57054AF3788B080EDC
SHA-512:	3D615F4E10EC61B68D613AD5D74928172A5BDDDD462EFC7221509D9B2D721D3593EA57E370BD0A644FA50FEB67F4228C4BCBD63E3E464CD223DCC4941D6B4 F2
Malicious:	false
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js .d....Q/....."#.D..m.;..A.A..Eo.....F.....y.$..$.v5j...T...z.]..._S....A..Eo... .....

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):	208
Entropy (8bit):	5.573932168783389
Encrypted:	false
SSDEEP:	3:m+lQyu6OA8RzYOCGLvHkWBGKuKjXK9QXAdWKjKLuVb1MO9kZktmXW4ThzJuA4biI:mkqYOFLvEWd8CAd9QWGSjtwuA424r1
MD5:	7948B250035917119D8C0AFCB36933AF
SHA1:	37BBD86D30091A1BB6265DE653B665C8041F2ACF
SHA-256:	F883B70C1E05D044104C73418FDB1B5C1037599CA082142DEB4E2D4095B11211
SHA-512:	C1E703DA39C8AE8876DB1E426853B6467F0EE3B3A1D0B869446F14261E9E590372A3420C1232F4559813277648BCA872A3315077547A50C4C2DDA07F75CE088C
Malicious:	false
Preview:	0\r..m.....P...gT...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .....Q/....."#.D=.x.;..A.A..Eo.....#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.5803340321490555
Encrypted:	false
SSDEEP:	3:m+lS5Etla8RzYOCGLvHkWBGKuKjXKVRNUp/KPWFvvS0KlR9k9kZkta/t7Ag2iHiE:moXXYOFLvEWdENUAulKlRG9jt9yC8n1
MD5:	0216A1296023732EA783E360AAD7C7AA
SHA1:	651889614191B7CB6D765E1B493B8274022BBDF1
SHA-256:	8A647BCF87B39B4D595EB646AA08A58FF87C61ED39101F46E5E4AE6C6C97D15E
SHA-512:	14767BD533738DA8B4B927B2EA40DE0DF571C58EBCD9B35DFF0959C05A8CB29E4BDE1E5E1F2B19C16D36A8CBEF48B1D6BF87499666D669DD0EACFA8649B1C 285
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .q....Q/....."#.D..W.;..A.A..Eo.....@.....8.../...;.\\o....1.....+..A..Eo .....

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):	221
Entropy (8bit):	5.625721103896448
Encrypted:	false
SSDEEP:	3:m+lFNrs8RzYOCGLvHkWBGKuKjXKeRKVlJ/2kKLuV9QyiZktG//sYWmYk5m1:mQZYOFLvEWdrROk/VQMt4sLmB41
MD5:	B00B19FDA56DFCF6BF5870B9D7C0AF6C
SHA1:	C80FAD99683C7E265D66C67F61DE70E9402A09FF
SHA-256:	510653F68CEACA2EAEE79EF568B1F3661B32AB04C93889DAE23C29FCA6946144
SHA-512:	A575E6E6584AAD19A2DE61DAD9FD7FCDC6C6D5FE6C12051577AF3E20536E22FA93D1F1A05B9DA38B5BF2EC9CC739051F0B4B712917349FB496D2902C1AB4D DD
Malicious:	false
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .Lv...Q/....."#.D.WS.;..A.A..Eo..... ./.ev.....N~..6.b.....$ .j;:C...A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.53998720717138
Encrypted:	false
SSDEEP:	3:m+lUV/la8RzYOCGLvHkWBGKuKjXKjcAW6KPWFvIycGJ49dZktFtlprobk9mZa6ta:mZ/lXYOFLvEWdccAWu6ClQtF5dm9741
MD5:	9EADC93048E1409618EB995FA2734056
SHA1:	80033B32124F7F99AF2B4B19D2662048B6D2AF73
SHA-256:	F3143C548E57A1E65C295B1AF61CC40027E468548E67DA1A5565B6C9AE8BE3A8
SHA-512:	D933A96B0CE493140BD75BF44DC7096D7CDB2836A94A1F9DBCACF51207C9C12ECD2DCB39A7E3FF0D47FAE023A1817553BA0F903AAFBA4AC2CC6A08BBB090 4CA2
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js .....Q/....."#.Do.k.;..A.A..Eo.....=.....U...I.>P...X...x..0U.~;m.x.k.A..E o.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.5548229582961675
Encrypted:	false
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFvR0+Yb0kZktjmB6shoq+Nem1:mMOYOFLvEWdwAPVu70+s0jtjmB6Jn1
MD5:	F37577F226E8CD78B5AF3C1AE2C9F06E
SHA1:	E95E42F974B4B1EEA515637ACFC50A1BEF49F69A
SHA-256:	A6599FD5077D6EAC799EF8F744AFA8ABD4AFEF5993E8622B9E772902173FF807
SHA-512:	C94013962651B8F42B61A1C4E9F92EE513C57DABFE14B230E420EBDE290A6370090E7FC5437C87102229AA7F6D030713B3CC7B13228E64702C6237532D1D0EFD
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .....Q/....."#.D=.W.;..A.A..Eo.....Lp.w.....k....F..D..O.n;[.1m.....=..A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.6116677274713425
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQEP6YqjtJMtqhcsBXIh1:mxRBJQvRqjkaB
MD5:	E3F0081B3E0D974032FB3C4E0276726D
SHA1:	0A63E49A4353780912E0E9E0DEC2C0C3F9E4650B
SHA-256:	5B04425182F042D0540A156F23855110B2AAD31BB622ED304E5E6727064A83D1

SHA-512:	37B9A16A21BDE70BB633DB6555A47051B895C2F385F9506C54089CAE8891755528002A1A5AB79EC535F3935F61F6F256A1A2B4270D8D253BE0A70309480EC00A
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .7s...Q/....."#.D..n.;..A.A..Eo.....K.....k..`..N3.... ..d..$[.....{.A..E o.....

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):	228
Entropy (8bit):	5.57731897660352
Encrypted:	false
SSDEEP:	6:msPYOFLvEWdrROk/RJUQUAdZRG9ttLc3Me/1:3RrROk/sPSsv
MD5:	46BB61EF64EE5647C7099A39323DD71D
SHA1:	D4A09F8A6CDEFAE2C4F19FF9DDDDE035DF261E0F
SHA-256:	CE666E8EFA7766F063DF9D4C14AF78ADBE0AF82A87CA81F9700C35D7D5F2E4C5
SHA-512:	F4F006D32E61623C1732F7522F4F2758CEE19626BFD813FCE2269B018B1CEF12D3A0D67DFA00AA5ECB1692C5A1B8E29D9016C46FE0E3C54347CAD6026ACBDE 4B
Malicious:	false
Preview:	0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ..w...Q/....."#.Dk.S.;..A.A..Eo.....E$.....9Q] .8O.z....=..:.N.{....N{.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	modified
Size (bytes):	1032
Entropy (8bit):	5.089680744243856
Encrypted:	false
SSDEEP:	12:iKM1Uhqu0HGc2w1riHwhGkNYMzJUQGvGyjGr+xQLeQ6RpEtFYg1MSMWKARp5QZMR:BX2vCMdYykgZ97Cxh5i/ouieMGN
MD5:	1B5D40EDDD4BEE15F0E3924B0ADD0D12
SHA1:	6131D7B9DAA7287CFD165D58464475ABD2D26944
SHA-256:	290207817D6B16616C4D694DBF66CE80918977B3D4D17115B94B86B7AA738B49
SHA-512:	9055424E083F7C0A50F6C19FFFC2CC37F6D8B9A37A847461A2D1F31753B19DCA9B9AE577D2DEFFA8BABDBF62EF03F3BB0B8B8047D4C9034FE28CE5912FE935 56
Malicious:	false
Preview:	.....5,Poy retne....).....T.....3...@....Q/.....v...q...t...Q/.....C..M.....k.....#...(...k.....]...I.....Q/.....Q/.....6<|....t...Q/.....<...W..J.t...Q/..... .oB*.t...Q/.....a.....t...Q/.....;.y~A.@....Q/.....P....V@....Q/.....F..=z;.@....Q/.....o.@....Q/.....2q....@....Q/.....*..@....Q/.....Gy.'.h.@....Q/.....k7 A.@....Q/.....:...N.A..@....Q/.....;/...@....Q/.....@....Q/.....P[. q@....Q/.....,+..._.#@....Q/.....J..j...@....Q/.....A?.2:..@....Q/.....q.@....Q/.....u\]. .q@....Q/.....!...0.o@....Q/.....*....@....Q/.....o..k..@....Q/.....^.~..z.@....Q/.....[.i..%.@....Q/.....+.{..'@....Q/.....@..x.@....Q/.....MV3..@....Q/..... .....D.4.@....Q/.....+.U.!..V@....Q/.....~.,.4>.@....Q/.....=....m..@....Q/.....*)....J:@....Q/.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	1032
Entropy (8bit):	5.089680744243856
Encrypted:	false
SSDEEP:	12:iKM1Uhqu0HGc2w1riHwhGkNYMzJUQGvGyjGr+xQLeQ6RpEtFYg1MSMWKARp5QZMR:BX2vCMdYykgZ97Cxh5i/ouieMGN
MD5:	1B5D40EDDD4BEE15F0E3924B0ADD0D12
SHA1:	6131D7B9DAA7287CFD165D58464475ABD2D26944
SHA-256:	290207817D6B16616C4D694DBF66CE80918977B3D4D17115B94B86B7AA738B49
SHA-512:	9055424E083F7C0A50F6C19FFFC2CC37F6D8B9A37A847461A2D1F31753B19DCA9B9AE577D2DEFFA8BABDBF62EF03F3BB0B8B8047D4C9034FE28CE5912FE935 56
Malicious:	false
Preview:	.....5,Poy retne....).....T.....3...@....Q/.....v...q...t...Q/.....C..M.....k.....#...(...k.....]...I.....Q/.....Q/.....6<|....t...Q/.....<...W..J.t...Q/..... .oB*.t...Q/.....a.....t...Q/.....;.y~A.@....Q/.....P....V@....Q/.....F..=z;.@....Q/.....o.@....Q/.....2q....@....Q/.....*..@....Q/.....Gy.'.h.@....Q/.....k7 A.@....Q/.....:...N.A..@....Q/.....;/...@....Q/.....@....Q/.....P[. q@....Q/.....,+..._.#@....Q/.....J..j...@....Q/.....A?.2:..@....Q/.....q.@....Q/.....u\]. .q@....Q/.....!...0.o@....Q/.....*....@....Q/.....o..k..@....Q/.....^.~..z.@....Q/.....[.i..%.@....Q/.....+.{..'@....Q/.....@..x.@....Q/.....MV3..@....Q/..... .....D.4.@....Q/.....+.U.!..V@....Q/.....~.,.4>.@....Q/.....=....m..@....Q/.....*)....J:@....Q/.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index~RF646700.TMP (copy)	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	1032
Entropy (8bit):	5.089680744243856
Encrypted:	false
SSDEEP:	12:iKM1Uhqu0HGc2w1riHwhGkNYMzJUQGvGyjGr+xQLeQ6RpEtFYg1MSMWKARp5QZMR:BX2vCMdYykgZ97Cxh5i/ouieMGN
MD5:	1B5D40EDDD4BEE15F0E3924B0ADD0D12
SHA1:	6131D7B9DAA7287CFD165D58464475ABD2D26944
SHA-256:	290207817D6B16616C4D694DBF66CE80918977B3D4D17115B94B86B7AA738B49
SHA-512:	9055424E083F7C0A50F6C19FFFC2CC37F6D8B9A37A847461A2D1F31753B19DCA9B9AE577D2DEFFA8BABDBF62EF03F3BB0B8B8047D4C9034FE28CE5912FE935 56
Malicious:	false
Preview:	.....5,Poy retne....).....T.....3...@....Q/.....v...q...t...Q/.....C..M.....k.....#...(...k.....]...I....Q/.....Q/.....6<|...t...Q/.....<...W..J.t...Q/..... .oB*.t...Q/.....a.....t...Q/.....;.y~A.@....Q/.....P....V@....Q/.....F..=z;.@....Q/.....o.@....Q/.....2q....@....Q/.....*..@....Q/.....Gy.'.h.@....Q/.....k7 A.@....Q/.....:..N.A..@....Q/.....;/...@....Q/.....@....Q/.....P[. q@....Q/.....,+..._.#@....Q/.....J..j...@....Q/.....A?.2:..@....Q/.....q.@....Q/.....u\]. .q@....Q/.....!...0.o@....Q/.....*....@....Q/.....o..k..@....Q/.....^.~..z.@....Q/.....[.i..%.@....Q/.....+.{..'@....Q/.....@..x.@....Q/.....MV3..@....Q/..... .....D.4.@....Q/.....+.U.!..V@....Q/.....~.,.4>.@....Q/.....=....m..@....Q/.....*)....J:@....Q/.....

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):	289
Entropy (8bit):	5.179751759848978
Encrypted:	false
SSDEEP:	6:kOeA+q2Pwkn2nKuAl9OmbnIFUtjeTXZmwJeT3VkwOwkn2nKuAl9OmbjLJ:kOD+vYfHAahFUtj0X/J03V5JfHAaSJ
MD5:	BA2E7A1BF90A7E84026420E0D99B44AF
SHA1:	91E9EA540C457336629E4B412F06F48C65508FB4
SHA-256:	E1681AA19F2A12A652BCBAB68BA172A6037AF4C8B0141844A1E2DCF5C8E80678
SHA-512:	A160A67B51D7EC54896414623D94BDAC5F3757EED62914EEB24087B2F887321A0706B41F236D44236921533B63849D0D5A7714F08E803183DB58604AA2F5EF41
Malicious:	false
Preview:	2023/01/25-09:54:30.493 99c Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2023/01/25-09:54:30.494 99c Recovering log #3.2023/01/25-09:54:30.494 99c 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\LOG.old (copy)	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	289
Entropy (8bit):	5.179751759848978
Encrypted:	false
SSDEEP:	6:kOeA+q2Pwkn2nKuAl9OmbnIFUtjeTXZmwJeT3VkwOwkn2nKuAl9OmbjLJ:kOD+vYfHAahFUtj0X/J03V5JfHAaSJ
MD5:	BA2E7A1BF90A7E84026420E0D99B44AF
SHA1:	91E9EA540C457336629E4B412F06F48C65508FB4
SHA-256:	E1681AA19F2A12A652BCBAB68BA172A6037AF4C8B0141844A1E2DCF5C8E80678
SHA-512:	A160A67B51D7EC54896414623D94BDAC5F3757EED62914EEB24087B2F887321A0706B41F236D44236921533B63849D0D5A7714F08E803183DB58604AA2F5EF41
Malicious:	false
Preview:	2023/01/25-09:54:30.493 99c Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2023/01/25-09:54:30.494 99c Recovering log #3.2023/01/25-09:54:30.494 99c 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\LOG.old~RF63ec52.TMP (copy)	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	289
Entropy (8bit):	5.179751759848978
Encrypted:	false
SSDEEP:	6:kOeA+q2Pwkn2nKuAl9OmbnIFUtjeTXZmwJeT3VkwOwkn2nKuAl9OmbjLJ:kOD+vYfHAahFUtj0X/J03V5JfHAaSJ

MD5:	BA2E7A1BF90A7E84026420E0D99B44AF
SHA1:	91E9EA540C457336629E4B412F06F48C65508FB4
SHA-256:	E1681AA19F2A12A652BCBAB68BA172A6037AF4C8B0141844A1E2DCF5C8E80678
SHA-512:	A160A67B51D7EC54896414623D94BDAC5F3757EED62914EEB24087B2F887321A0706B41F236D44236921533B63849D0D5A7714F08E803183DB58604AA2F5EF41
Malicious:	false
Preview:	2023/01/25-09:54:30.493 99c Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2023/01/25-09:54:30.494 99c Recovering log #3.2023/01/25-09:54:30.494 99c 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):	131072
Entropy (8bit):	0.008907738108328683
Encrypted:	false
SSDEEP:	3:ImtV/CuttMTLS/Jf0lt+urQTID7vt/lcvmllP62/X:IiV1kTLLlousTxvv6m
MD5:	0A339004BCB425813505AE2871E61E20
SHA1:	9BDA040B5589E1B919A259DB212F4CE8E32AAA8F
SHA-256:	46828E139BE167C9E36B556EB137571DE93A29930C366CE0666B1385BC106517
SHA-512:	DA3CE56FFA0538D022A80F7F6DAE1E89586E27FC484E82CCCAADC9EE163BEBBEDA2CAB446D507C622BAE868086E382F5436E328418BB877FBBF0A2192CB61DF8
Malicious:	false
Preview:	VLnk.....?......).0k.. .....U....n.. ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-230125085428Z-200.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, cbSize 65110, bits offset 54
Category:	dropped
Size (bytes):	65110
Entropy (8bit):	2.9190723357188926
Encrypted:	false
SSDEEP:	192:fVsY9Y9Qo7oDkYLec2HOY4aGeEsmTSSGCXIwNHpgGwnXkIM5++Iyybnbc5wYmoR1:fef9RGNec2uhaGe6SspgtX8L
MD5:	3389223B0B6DEAE920BD08FC359FB444
SHA1:	862EC1ED0922868213799E23C9D551AA354644BB
SHA-256:	EDA4C6BAF9838F5DE79B56EBAD10363081FF505A5F24B1057267E33E8EFFCB9E
SHA-512:	8B8B91F81BADE83E8FCA6528D58C0D440DC8A64691C88E6F991D2B521439CCE9BC3EAC8B2B43FD53E64A00AEA51DE2BEFFCC1B4B56D980DA61AE7270A4D9D52E
Malicious:	false
Preview:	BMV.......6...(...k...h..... ..........................S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S. ..S...S...S...S...S...S...S...S...S...S...S...S...T...s...v...w.. ................................S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...c ....^...S...S...W......Y...S...S..S.. .S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...S...

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, file counter 16, database pages 15, cookie 0x5, schema 4, UTF-8, version-valid-for 16
Category:	dropped
Size (bytes):	61440
Entropy (8bit):	3.5684891391199165
Encrypted:	false
SSDEEP:	384:XeT9dThhtELJ8fwRRwZsLRGlKhsvXh+vSc:CkYZsLQhUSc
MD5:	2EF6ADF7634AB2759A5E3B6737E8E460
SHA1:	F4B9C073877234CB93FADE49557A5CB132C4137A
SHA-256:	0E29E13562C09A7E98C5D8634DE8B96DEF70CB572261749EDD8B78D9656D617B
SHA-512:	51847E30453FC6BDDDC5433B21CB900C62D3ACD322476B57B65BF9C415C6E96BC4EFB8D6222E7F296D178005DC3FD1ED82A4811DE2B40D56C82DC8BE351E388
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:	SQLite Rollback Journal
Category:	dropped
Size (bytes):	8720
Entropy (8bit):	3.3182428357476597
Encrypted:	false
SSDEEP:	48:7Mw2iomVQYom1Ciniom8Vom1Nom1Aiom1RROiom1Com1pom1wUiomVKiome1RqQr:7aCginOhkUCKFjN49IVXEBodRBkc
MD5:	E7E6F67F90CEA8CFFD1C37FA29B34C68
SHA1:	CF3C52884B945F7DA22D34103CC8BAD5052EB8CD
SHA-256:	9456FFA299B1AFAFD17E6860569074A3E29A3F4A42EE05DDF74F8FB03FEC41A0
SHA-512:	4DFE45C13DD377FC25B892B377E1DCB0F4172E9A705DE40B62FBCEBD7EBC3A486FAF98F5633EAF69BCD0A732B2704697E16EE5FCD263B54F39133A1980DBB E77
Malicious:	false
Preview:	.... .c.....hH..... .....W.... <.W.L...y.....~..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeCMapFnt19.lst (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	536
Entropy (8bit):	5.17576513886526
Encrypted:	false
SSDEEP:	12:T4RFQ8idRuMgxg6dxs3yBFTtDcSTAzidRuOPgxg601s3yBFDHpcSa:kNid8HxPs3yTTtPmid8OPgx4s3yTDHBa
MD5:	4D5E3CD969F14362210F0473720C5528
SHA1:	AFD90E9888759B809F78E87D5550B601A288A0A3
SHA-256:	79D95D01FDE7FC7C890CD62734A7F203B12A5D44A56D6009D0E43E40D99682AE
SHA-512:	B10C157945432CC8944E63A28CA3420CAD0C6B87BABC77BB5437DA5E3DF0CDEB657D410F28FA61D314E86269B8D1AC5972B0792D3E78787DFCE496EEE979D 64
Malicious:	false
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-H.Registry:Adobe.Ordering:Identity.OutlineFil eName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-H.FileLength:8228.FileModTime:1426577652.%EndFont..%BeginFont.Handler:Dire ctoryHandler.FontType:CMap.CMapName:Identity-V.Registry:Adobe.Ordering:Identity.UseCMap:Identity-H.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-V.FileLength:2761.FileModTime:1426577652.%EndFont..

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.2620

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	536
Entropy (8bit):	5.17576513886526
Encrypted:	false
SSDEEP:	12:T4RFQ8idRuMgxg6dxs3yBFTtDcSTAzidRuOPgxg601s3yBFDHpcSa:kNid8HxPs3yTTtPmid8OPgx4s3yTDHBa
MD5:	4D5E3CD969F14362210F0473720C5528
SHA1:	AFD90E9888759B809F78E87D5550B601A288A0A3
SHA-256:	79D95D01FDE7FC7C890CD62734A7F203B12A5D44A56D6009D0E43E40D99682AE
SHA-512:	B10C157945432CC8944E63A28CA3420CAD0C6B87BABC77BB5437DA5E3DF0CDEB657D410F28FA61D314E86269B8D1AC5972B0792D3E78787DFCE496EEE979D 64
Malicious:	false
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-H.Registry:Adobe.Ordering:Identity.OutlineFil eName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-H.FileLength:8228.FileModTime:1426577652.%EndFont..%BeginFont.Handler:Dire ctoryHandler.FontType:CMap.CMapName:Identity-V.Registry:Adobe.Ordering:Identity.UseCMap:Identity-H.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-V.FileLength:2761.FileModTime:1426577652.%EndFont..

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	536
Entropy (8bit):	5.17576513886526
Encrypted:	false
SSDEEP:	12:T4RFQ8idRuMgxg6dxs3yBFTtDcSTAzidRuOPgxg601s3yBFDHpcSa:kNid8HxPs3yTTtPmid8OPgx4s3yTDHBa
MD5:	4D5E3CD969F14362210F0473720C5528
SHA1:	AFD90E9888759B809F78E87D5550B601A288A0A3
SHA-256:	79D95D01FDE7FC7C890CD62734A7F203B12A5D44A56D6009D0E43E40D99682AE
SHA-512:	B10C157945432CC8944E63A28CA3420CAD0C6B87BABC77BB5437DA5E3DF0CDEB657D410F28FA61D314E86269B8D1AC5972B0792D3E78787DFCE496EEE979D 64
Malicious:	false
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-H.Registry:Adobe.Ordering:Identity.OutlineFil eName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-H.FileLength:8228.FileModTime:1426577652.%EndFont..%BeginFont.Handler:Dire ctoryHandler.FontType:CMap.CMapName:Identity-V.Registry:Adobe.Ordering:Identity.UseCMap:Identity-H.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-V.FileLength:2761.FileModTime:1426577652.%EndFont..

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AcroFnt19.lst (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	9566
Entropy (8bit):	5.226610011802065
Encrypted:	false
SSDEEP:	192:eTA2j6Q6T766x626Oz6r606+6bfs6JtRZ65tsu6rtG16lMXY5B5Cfk:es4p0vTLcdflfsmtRZEtsuatG1gMlzV
MD5:	63B24EA3A13EAC476D6309BB202EF459
SHA1:	89502C393549C20C933E4553F51F74F3DBE085EF
SHA-256:	2B4BE0BED267BBD4E4FFFC912A6C7ED6A8D4735DCF9B69FF90F37CDDEF4110EA
SHA-512:	2CB315DD00867DEE3A2CBC4017B59C53B41E817216FE0111A60947E1F0D81FF6767D8F7B5C406AAF9E6516BE716A086642AFFABBEFBE4C5B260437C89E3535E C
Malicious:	false
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-H.Registry:Adobe.Ordering:Identity.OutlineFil eName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-H.FileLength:8228.FileModTime:1426577652.%EndFont..%BeginFont.Handler:Dire ctoryHandler.FontType:CMap.CMapName:Identity-V.Registry:Adobe.Ordering:Identity.UseCMap:Identity-H.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-V.FileLength:2761.FileModTime:1426577652.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:Type1.FontName:Adob ePiStd.FamilyName:Adobe Pi Std.StyleName:Regular.FullName:Adobe Pi Std.MenuName:Adobe Pi Std.StyleBits:0.WritingScript:Roman.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\Font\AdobePiStd.otf.DataFormat:sfntData.UsesStandardEncoding:yes.isCFF:yes.FileLength:92588.FileModTime :1426577650.WeightClass:400.WidthClass:5.AngleClass:0.DesignSize:240.NameArray:0,Mac,4,Adobe Pi Std.

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AdobeFnt16.lst.2620

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	9566
Entropy (8bit):	5.226610011802065
Encrypted:	false
SSDEEP:	192:eTA2j6Q6T766x626Oz6r606+6bfs6JtRZ65tsu6rtG16lMXY5B5Cfk:es4p0vTLcdflfsmtRZEtsuatG1gMlzV
MD5:	63B24EA3A13EAC476D6309BB202EF459
SHA1:	89502C393549C20C933E4553F51F74F3DBE085EF
SHA-256:	2B4BE0BED267BBD4E4FFFC912A6C7ED6A8D4735DCF9B69FF90F37CDDEF4110EA
SHA-512:	2CB315DD00867DEE3A2CBC4017B59C53B41E817216FE0111A60947E1F0D81FF6767D8F7B5C406AAF9E6516BE716A086642AFFABBEFBE4C5B260437C89E3535E C
Malicious:	false
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-H.Registry:Adobe.Ordering:Identity.OutlineFil eName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-H.FileLength:8228.FileModTime:1426577652.%EndFont..%BeginFont.Handler:Dire ctoryHandler.FontType:CMap.CMapName:Identity-V.Registry:Adobe.Ordering:Identity.UseCMap:Identity-H.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-V.FileLength:2761.FileModTime:1426577652.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:Type1.FontName:Adob ePiStd.FamilyName:Adobe Pi Std.StyleName:Regular.FullName:Adobe Pi Std.MenuName:Adobe Pi Std.StyleBits:0.WritingScript:Roman.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\Font\AdobePiStd.otf.DataFormat:sfntData.UsesStandardEncoding:yes.isCFF:yes.FileLength:92588.FileModTime :1426577650.WeightClass:400.WidthClass:5.AngleClass:0.DesignSize:240.NameArray:0,Mac,4,Adobe Pi Std.

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe

File Type:	data
Category:	dropped
Size (bytes):	63598
Entropy (8bit):	5.4331110334817385
Encrypted:	false
SSDEEP:	768:PCbGNFYGpiyVFiC0Zo3lDYe3ahiIN5kWVgsGABQFD74Yyu:J0GpiyVFiho3lDT3ahIN5VuR74K
MD5:	509C4477711D585F9775E3646E1AAE36
SHA1:	5115A6FDDDD5B76E0F0DC4C0E7A45AF8BCDF9881
SHA-256:	9C4CC4E21EACA483409F30E88BC5DE01D0A3E40ED7968FF7E45BDFA6EF4A0611
SHA-512:	7168C5F406EBBC2255A39776BA3D87851AECE3AE8D8EF2FAD64749661BD32055BC24209363F28735722BEDC7EE3456883DABD04FB22257FFEAF7F26F4DB2AC1
Malicious:	false
Preview:	4.382.88.FID.2:o:.....:F:AgencyFB-Reg.P:Agency FB.L:$....."F:Agency FB.#.94.FID.2:o:.....:F:AgencyFB-Bold.P:Agency FB Bold.L:%....." F:Agency FB.#.82.FID.2:o:.....:F:Algerian.P:Algerian.L:$.....RF:Algerian.#.93.FID.2:o:.....:F:ArialNarrow.P:Arial Narrow.L:$....."F:Arial Narrow.#.107.FID.2:o:.....:F:ArialNarrow-Italic.P:Arial Narrow Italic.L:$....."F:Arial Narrow.#.103.FID.2:o:.....:F:ArialNarrow-Bold.P:Arial Narrow Bold.L:%....."F:Arial Narrow.#.116.FID.2:o:.....:F:ArialNarrow-BoldItalic.P:Arial Narrow Bold Italic.L:%....."F:Arial Narrow.#.75.FID.2:o:.....:F:ArialMT.P:Arial.L:$....."F:Arial.#.89.FID.2:o:.....:F:Arial-ItalicMT.P:Arial Italic.L:$....."F:Arial.#.85.FID.2:o:.....:F:Arial-BoldMT.P:Arial Bold.L:$....."F:Arial.#.98.FID.2:o:.....:F:Arial-B

Static File Info

General

File type:	PDF document, version 1.3, 2 pages
Entropy (8bit):	7.964748138170801
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	Bordereau d'annonce de livraison.pdf
File size:	101827
MD5:	dc3036432aeb9c504333987852891a18
SHA1:	71bbfb3a441c3de46fe7ae52c2069afe29fee809
SHA256:	d2f9be8a683358cf7b4d012c974e7f21d0449b003068eda99b4e5d2f474a2dfe
SHA512:	e4a4c86362666690fa687906b6a5a9ef1daf5a2147fbd3e759c833103d2919beefe6a3317c56961695a04b64fd98ee4420f80035799648efd0918cb15c95c1a8
SSDEEP:	1536:h1l5pwR94e6DXVOvxhrWwqwmSA5gXUrXoKR/EKlaZyOKG/QbRhUqQpkqfR6SE:h1Cpa9eIvqgKD8sko+RhEeIkSE
TLSH:	D3A30234EA556D8DF057C126A271325BF3697EF607EC4484263CEFCF8691729B42309A
File Content Preview:	%PDF-1.3 .%.... .1 0 obj .<< ./Type /Catalog ./Pages 2 0 R ./PageMode /UseNone ./ViewerPreferences << ./FitWindow true ./PageLayout /SinglePage ./NonFullScreenPageMode /UseNone .>> .>> .endobj .5 0 obj .<< ./Length 1344 ./Filter [/FlateDecode] .>> .stre

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

Header:	%PDF-1.3
Total Entropy:	7.964748
Total Bytes:	101827
Stream Entropy:	7.973924
Stream Bytes:	100391
Entropy outside Streams:	4.863246
Bytes outside Streams:	1436
Number of EOF found:	1
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	41
endobj	41
stream	10

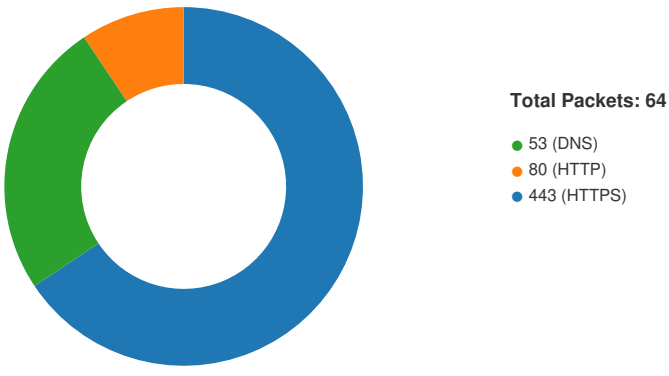
Name	Count
endstream	6
xref	1
trailer	1
startxref	1
/Page	2
/Encrypt	0
/ObjStm	0
/URI	6
/JS	0
/JavaScript	0
/AA	0
/OpenAction	0
/AcroForm	0
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0

Image Streams

ID	DHASH	MD5	Preview
9	0000000000000000	9b63798468131763faada4f71bc0d58f	
26	0000000000000000	9b080008b1d75bf2b96a4cbb49c43f29	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 09:54:49.522526979 CET	49696	443	192.168.2.4	142.250.203.110
Jan 25, 2023 09:54:49.522568941 CET	443	49696	142.250.203.110	192.168.2.4
Jan 25, 2023 09:54:49.522775888 CET	49696	443	192.168.2.4	142.250.203.110
Jan 25, 2023 09:54:49.522947073 CET	49697	80	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:49.523247004 CET	49698	443	192.168.2.4	142.250.203.109
Jan 25, 2023 09:54:49.523272038 CET	443	49698	142.250.203.109	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 09:54:49.523350000 CET	49698	443	192.168.2.4	142.250.203.109
Jan 25, 2023 09:54:49.525620937 CET	49696	443	192.168.2.4	142.250.203.110
Jan 25, 2023 09:54:49.525656939 CET	443	49696	142.250.203.110	192.168.2.4
Jan 25, 2023 09:54:49.526087046 CET	49699	80	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:49.526938915 CET	49698	443	192.168.2.4	142.250.203.109
Jan 25, 2023 09:54:49.526963949 CET	443	49698	142.250.203.109	192.168.2.4
Jan 25, 2023 09:54:49.550811052 CET	80	49697	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:49.550945997 CET	49697	80	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:49.551522970 CET	49697	80	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:49.553493023 CET	80	49699	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:49.553617954 CET	49699	80	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:49.581971884 CET	80	49697	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:49.636629105 CET	49700	443	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:49.636691093 CET	443	49700	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:49.636759043 CET	49700	443	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:49.637445927 CET	49700	443	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:49.637475967 CET	443	49700	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:49.652077913 CET	443	49698	142.250.203.109	192.168.2.4
Jan 25, 2023 09:54:49.653867006 CET	49698	443	192.168.2.4	142.250.203.109
Jan 25, 2023 09:54:49.653913021 CET	443	49698	142.250.203.109	192.168.2.4
Jan 25, 2023 09:54:49.656260967 CET	443	49698	142.250.203.109	192.168.2.4
Jan 25, 2023 09:54:49.656375885 CET	49698	443	192.168.2.4	142.250.203.109
Jan 25, 2023 09:54:49.663317919 CET	443	49696	142.250.203.110	192.168.2.4
Jan 25, 2023 09:54:49.700226068 CET	49697	80	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:49.701642990 CET	49696	443	192.168.2.4	142.250.203.110
Jan 25, 2023 09:54:49.701683044 CET	443	49696	142.250.203.110	192.168.2.4
Jan 25, 2023 09:54:49.702591896 CET	443	49696	142.250.203.110	192.168.2.4
Jan 25, 2023 09:54:49.702687979 CET	49696	443	192.168.2.4	142.250.203.110
Jan 25, 2023 09:54:49.706927061 CET	443	49696	142.250.203.110	192.168.2.4
Jan 25, 2023 09:54:49.707062006 CET	49696	443	192.168.2.4	142.250.203.110
Jan 25, 2023 09:54:49.744041920 CET	443	49700	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:49.790200949 CET	49700	443	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:49.790249109 CET	443	49700	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:49.792526007 CET	443	49700	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:49.792675018 CET	49700	443	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:50.096237898 CET	49698	443	192.168.2.4	142.250.203.109
Jan 25, 2023 09:54:50.096296072 CET	443	49698	142.250.203.109	192.168.2.4
Jan 25, 2023 09:54:50.096525908 CET	49698	443	192.168.2.4	142.250.203.109
Jan 25, 2023 09:54:50.096540928 CET	443	49698	142.250.203.109	192.168.2.4
Jan 25, 2023 09:54:50.096688986 CET	49700	443	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:50.096724987 CET	443	49700	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:50.096746922 CET	443	49698	142.250.203.109	192.168.2.4
Jan 25, 2023 09:54:50.096836090 CET	49700	443	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:50.096858978 CET	443	49700	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:50.096987009 CET	443	49700	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:50.097625971 CET	49696	443	192.168.2.4	142.250.203.110
Jan 25, 2023 09:54:50.097651958 CET	443	49696	142.250.203.110	192.168.2.4
Jan 25, 2023 09:54:50.097840071 CET	49696	443	192.168.2.4	142.250.203.110
Jan 25, 2023 09:54:50.097863913 CET	443	49696	142.250.203.110	192.168.2.4
Jan 25, 2023 09:54:50.097908974 CET	443	49696	142.250.203.110	192.168.2.4
Jan 25, 2023 09:54:50.126626968 CET	443	49700	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:50.126756907 CET	49700	443	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:50.130997896 CET	49700	443	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:50.131031990 CET	443	49700	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:50.132472038 CET	443	49696	142.250.203.110	192.168.2.4
Jan 25, 2023 09:54:50.132602930 CET	49696	443	192.168.2.4	142.250.203.110
Jan 25, 2023 09:54:50.132653952 CET	443	49696	142.250.203.110	192.168.2.4
Jan 25, 2023 09:54:50.132689953 CET	443	49696	142.250.203.110	192.168.2.4
Jan 25, 2023 09:54:50.132755995 CET	49696	443	192.168.2.4	142.250.203.110

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 09:54:50.142833948 CET	49696	443	192.168.2.4	142.250.203.110
Jan 25, 2023 09:54:50.142888069 CET	443	49696	142.250.203.110	192.168.2.4
Jan 25, 2023 09:54:50.175132990 CET	443	49698	142.250.203.109	192.168.2.4
Jan 25, 2023 09:54:50.175291061 CET	49698	443	192.168.2.4	142.250.203.109
Jan 25, 2023 09:54:50.175329924 CET	443	49698	142.250.203.109	192.168.2.4
Jan 25, 2023 09:54:50.175566912 CET	443	49698	142.250.203.109	192.168.2.4
Jan 25, 2023 09:54:50.175688982 CET	49698	443	192.168.2.4	142.250.203.109
Jan 25, 2023 09:54:50.192728043 CET	49698	443	192.168.2.4	142.250.203.109
Jan 25, 2023 09:54:50.192754984 CET	443	49698	142.250.203.109	192.168.2.4
Jan 25, 2023 09:54:50.536596060 CET	49701	443	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:50.536667109 CET	443	49701	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:50.536834002 CET	49701	443	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:50.537167072 CET	49701	443	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:50.537204027 CET	443	49701	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:50.538860083 CET	49702	443	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:50.538903952 CET	443	49702	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:50.539000034 CET	49702	443	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:50.539385080 CET	49702	443	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:50.539402962 CET	443	49702	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:50.603605986 CET	443	49701	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:50.604046106 CET	49701	443	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:50.604073048 CET	443	49701	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:50.604990005 CET	443	49701	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:50.605846882 CET	49701	443	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:50.605873108 CET	443	49701	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:50.605983019 CET	443	49701	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:50.606084108 CET	49701	443	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:50.606096029 CET	443	49701	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:50.606583118 CET	443	49702	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:50.606956005 CET	49702	443	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:50.606987953 CET	443	49702	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:50.607989073 CET	443	49702	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:50.608472109 CET	49702	443	192.168.2.4	91.121.41.151
Jan 25, 2023 09:54:50.608498096 CET	443	49702	91.121.41.151	192.168.2.4
Jan 25, 2023 09:54:50.608681917 CET	49702	443	192.168.2.4	91.121.41.151

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 09:54:49.456850052 CET	52239	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:54:49.457247972 CET	56807	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:54:49.459028006 CET	61007	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:54:49.474863052 CET	53	56807	8.8.8.8	192.168.2.4
Jan 25, 2023 09:54:49.484607935 CET	53	52239	8.8.8.8	192.168.2.4
Jan 25, 2023 09:54:49.486747980 CET	53	61007	8.8.8.8	192.168.2.4
Jan 25, 2023 09:54:49.600115061 CET	60686	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:54:49.633470058 CET	53	60686	8.8.8.8	192.168.2.4
Jan 25, 2023 09:54:52.495209932 CET	64906	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:54:52.521176100 CET	53	64906	8.8.8.8	192.168.2.4
Jan 25, 2023 09:54:52.556185961 CET	59446	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:54:52.573579073 CET	53	59446	8.8.8.8	192.168.2.4
Jan 25, 2023 09:54:54.069679022 CET	61088	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:54:54.104396105 CET	53	61088	8.8.8.8	192.168.2.4
Jan 25, 2023 09:54:57.778753996 CET	56022	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:54:57.813349962 CET	53	56022	8.8.8.8	192.168.2.4
Jan 25, 2023 09:55:04.298063993 CET	54521	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:55:04.327063084 CET	53	54521	8.8.8.8	192.168.2.4
Jan 25, 2023 09:56:24.506656885 CET	63001	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:56:24.539854050 CET	65133	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 09:56:24.546969891 CET	53	63001	8.8.8.8	192.168.2.4
Jan 25, 2023 09:56:24.571674109 CET	53	65133	8.8.8.8	192.168.2.4
Jan 25, 2023 09:56:24.830130100 CET	60998	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:56:24.849455118 CET	53	60998	8.8.8.8	192.168.2.4
Jan 25, 2023 09:57:40.247783899 CET	59818	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:57:40.282955885 CET	53	59818	8.8.8.8	192.168.2.4
Jan 25, 2023 09:57:59.579096079 CET	52259	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:57:59.579204082 CET	53887	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:57:59.597002029 CET	53	53887	8.8.8.8	192.168.2.4
Jan 25, 2023 09:57:59.607394934 CET	56218	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:57:59.611361027 CET	53	52259	8.8.8.8	192.168.2.4
Jan 25, 2023 09:57:59.626972914 CET	53	56218	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 25, 2023 09:54:49.456850052 CET	192.168.2.4	8.8.8.8	0x497e	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:54:49.457247972 CET	192.168.2.4	8.8.8.8	0x9186	Standard query (0)	dispatchweb.eureka-technology.fr	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:54:49.459028006 CET	192.168.2.4	8.8.8.8	0x6d1	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:54:49.600115061 CET	192.168.2.4	8.8.8.8	0xa5a2	Standard query (0)	dispatchweb.fr	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:54:52.495209932 CET	192.168.2.4	8.8.8.8	0x4f33	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:54:52.556185961 CET	192.168.2.4	8.8.8.8	0xe584	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:54:54.069679022 CET	192.168.2.4	8.8.8.8	0x80f7	Standard query (0)	dispatchweb.eureka-technology.fr	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:54:57.778753996 CET	192.168.2.4	8.8.8.8	0x5cc8	Standard query (0)	maps.dgeoloc.fr	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:55:04.298063993 CET	192.168.2.4	8.8.8.8	0x9765	Standard query (0)	dispatchweb.fr	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:56:24.506656885 CET	192.168.2.4	8.8.8.8	0xef4f	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:56:24.539854050 CET	192.168.2.4	8.8.8.8	0x58a6	Standard query (0)	dispatchweb.fr	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:56:24.830130100 CET	192.168.2.4	8.8.8.8	0x472c	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:57:40.247783899 CET	192.168.2.4	8.8.8.8	0x8a37	Standard query (0)	maps.dgeoloc.fr	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:57:59.579096079 CET	192.168.2.4	8.8.8.8	0x4074	Standard query (0)	dispatchweb.fr	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:57:59.579204082 CET	192.168.2.4	8.8.8.8	0xe8cf	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:57:59.607394934 CET	192.168.2.4	8.8.8.8	0x398d	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 25, 2023 09:54:49.474863052 CET	8.8.8.8	192.168.2.4	0x9186	No error (0)	dispatchweb.eureka-technology.fr	dispatchweb.fr		CNAME (Canonical name)	IN (0x0001)	false
Jan 25, 2023 09:54:49.474863052 CET	8.8.8.8	192.168.2.4	0x9186	No error (0)	dispatchweb.fr		91.121.41.151	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:54:49.484607935 CET	8.8.8.8	192.168.2.4	0x497e	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:54:49.486747980 CET	8.8.8.8	192.168.2.4	0x6d1	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false

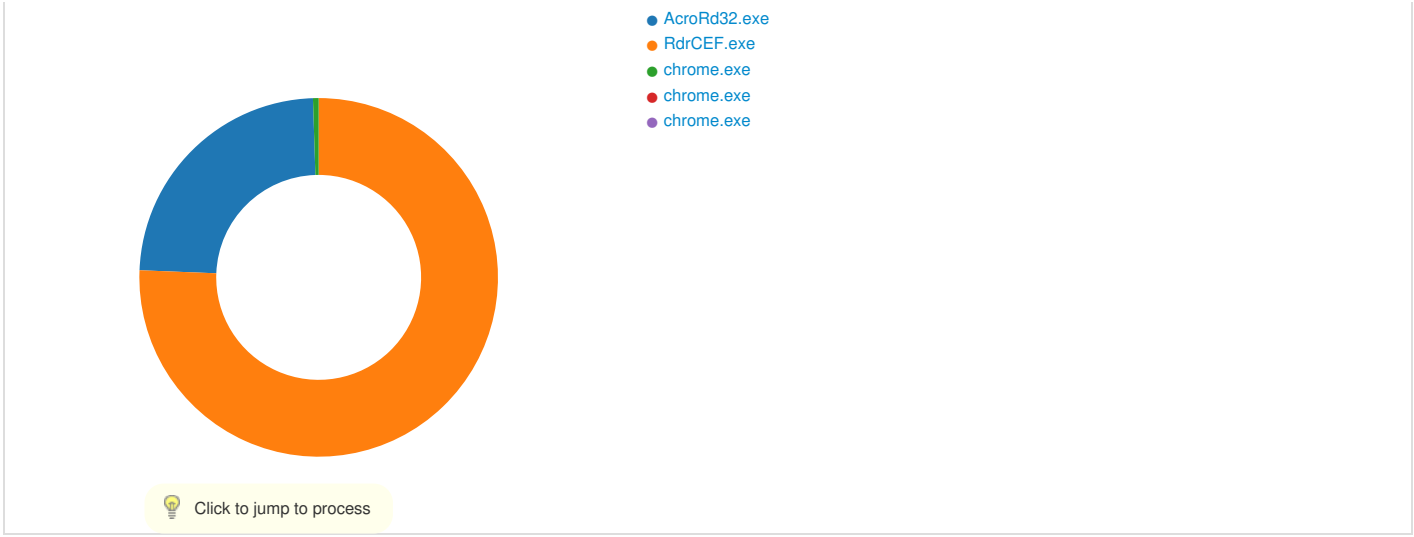
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 25, 2023 09:54:49.486747980 CET	8.8.8.8	192.168.2.4	0x6d1	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:54:49.633470058 CET	8.8.8.8	192.168.2.4	0xa5a2	No error (0)	dispatchweb.fr		91.121.41.151	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:54:52.521176100 CET	8.8.8.8	192.168.2.4	0x4f33	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:54:52.573579073 CET	8.8.8.8	192.168.2.4	0xe584	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:54:54.104396105 CET	8.8.8.8	192.168.2.4	0x80f7	No error (0)	dispatchweb.eureka-technology.fr	dispatchweb.fr		CNAME (Canonical name)	IN (0x0001)	false
Jan 25, 2023 09:54:54.104396105 CET	8.8.8.8	192.168.2.4	0x80f7	No error (0)	dispatchweb.fr		91.121.41.151	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:54:57.813349962 CET	8.8.8.8	192.168.2.4	0x5cc8	No error (0)	maps.dgeoloc.fr		178.33.250.233	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:55:04.327063084 CET	8.8.8.8	192.168.2.4	0x9765	No error (0)	dispatchweb.fr		91.121.41.151	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:56:24.546969891 CET	8.8.8.8	192.168.2.4	0xef4f	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:56:24.571674109 CET	8.8.8.8	192.168.2.4	0x58a6	No error (0)	dispatchweb.fr		91.121.41.151	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:56:24.849455118 CET	8.8.8.8	192.168.2.4	0x472c	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:57:40.282955885 CET	8.8.8.8	192.168.2.4	0x8a37	No error (0)	maps.dgeoloc.fr		178.33.250.233	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:57:59.597002029 CET	8.8.8.8	192.168.2.4	0xe8cf	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:57:59.611361027 CET	8.8.8.8	192.168.2.4	0x4074	No error (0)	dispatchweb.fr		91.121.41.151	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:57:59.626972914 CET	8.8.8.8	192.168.2.4	0x398d	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- dispatchweb.fr
- clients2.google.com
- https:
  - dispatchweb.eureka-technology.fr
  - maps.dgeoloc.fr

Statistics

Behavior



System Behavior

Analysis Process: AcroRd32.exe PID: 2440, Parent PID: 3528

General

Target ID:	0
Start time:	09:54:21
Start date:	25/01/2023
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\Desktop\Bordereau d'annonce de livraison.pdf
Imagebase:	0xdf0000
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

Registry Activities

Analysis Process: RdrCEF.exe PID: 5040, Parent PID: 2440

General

Target ID:	1
Start time:	09:54:26
Start date:	25/01/2023
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:	0x1240000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	12	13483E5	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	70	1348447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	success or wait	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	160	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	6	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	18	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	6	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	success or wait	11	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	1639	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	45	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	8	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	6	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	success or wait	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	success or wait	3	13359E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	success or wait	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	success or wait	6	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	success or wait	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	success or wait	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	success or wait	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	success or wait	18	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	success or wait	18	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	success or wait	42	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	success or wait	41	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	success or wait	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	success or wait	88	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	success or wait	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	success or wait	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	success or wait	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	success or wait	2	13359E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	42	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	45	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	success or wait	10	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	success or wait	6	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	end of file	1	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	success or wait	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	15	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	15	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	success or wait	15	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	4	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	success or wait	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	success or wait	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	8	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	success or wait	169	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	success or wait	7	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	179	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	3	13359E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	206	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	success or wait	201	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	success or wait	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	success or wait	1	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	success or wait	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	success or wait	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	success or wait	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	success or wait	14	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	success or wait	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	success or wait	324	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	success or wait	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	success or wait	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	success or wait	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	success or wait	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	success or wait	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	success or wait	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	success or wait	4	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	end of file	2	13359E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	success or wait	150	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	success or wait	10	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	success or wait	31	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	49	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	success or wait	196	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	success or wait	9	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	success or wait	1	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	success or wait	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	24	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	3	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	success or wait	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	end of file	2	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	6	13359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	2	13359E2	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	13483E5	ReadFile

Analysis Process: chrome.exe PID: **3456**, Parent PID: **4560**

General

Target ID:	2
Start time:	09:54:46
Start date:	25/01/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x7ff683680000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}	dr	unicode	0	1	success or wait	1	7FF6836DA143	RegSetValueExW

Analysis Process: chrome.exe PID: **920**, Parent PID: **3456**

General

Target ID:	3
Start time:	09:54:47
Start date:	25/01/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --mojo-platform-channel-handle=2008 --field-trial-handle=1672,i,11613717386682731625,2570180296813603654,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff683680000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **6404**, Parent PID: **4560**

General

Target ID:	4
Start time:	09:54:48

Start date:	25/01/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "http://dispatchweb.eureka-technology.fr//webmanager/authentification.aspx?TrackID=212Tja4dDEsuszajw3450
Imagebase:	0x7ff683680000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly