



ID: 402635
Sample Name: SECOURS SANITAIRE DU COVID-19.pdf
Cookbook: defaultwindowspdfcookbook.jbs
Time: 10:41:13
Date: 03/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report SECOURS SANITAIRE DU COVID-19.pdf 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 5
Sigma Overview 5
Signature Overview 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 13
Public 13
Private 13
General Information 13
Simulations 15
Behavior and APIs 16
Joe Sandbox View / Context 16
IPs 16
Domains 16
ASN 16
JA3 Fingerprints 17
Dropped Files 17
Created / dropped Files 17
Static File Info 30
General 30
File Icon 31
Static PDF Info 31
General 31
Keywords Statistics 31
Image Streams 31
Network Behavior 32
UDP Packets 32
DNS Answers 34
Code Manipulations 34
Statistics 34
Behavior 34
System Behavior 35
Analysis Process: AcroRd32.exe PID: 7040 Parent PID: 5884 35
General 35
File Activities 35
File Created 35

Copyright Joe Security LLC 2021

Registry Activities 37
Key Created 37
Key Value Created 37
Analysis Process: AcroRd32.exe PID: 7160 Parent PID: 7040 38
General 38
File Activities 38
Registry Activities 38
Analysis Process: RdrCEF.exe PID: 6580 Parent PID: 7040 38
General 38
File Activities 38
File Read 39
Analysis Process: RdrCEF.exe PID: 6960 Parent PID: 6580 43
General 43
File Activities 43
Analysis Process: RdrCEF.exe PID: 6656 Parent PID: 6580 43
General 43
File Activities 44
Analysis Process: RdrCEF.exe PID: 4420 Parent PID: 6580 44
General 44
File Activities 44
Analysis Process: RdrCEF.exe PID: 3436 Parent PID: 6580 44
General 44
File Activities 44
Analysis Process: HxOutlook.exe PID: 808 Parent PID: 800 45
General 45
File Activities 45
Registry Activities 45
Disassembly 45
Code Analysis 45

Copyright Joe Security LLC 2021

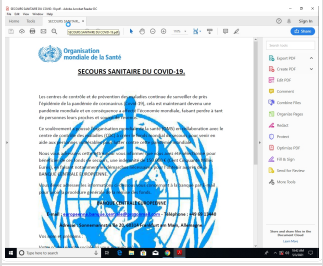
Analysis Report SECOURS SANITAIRE DU COVID-19.pdf

Overview

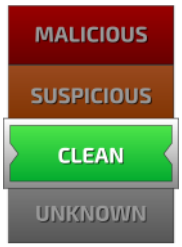
General Information

Sample Name:	SECOURS SANITAIRE DU COVID-19.pdf
Analysis ID:	402635
MD5:	b01d94c5b33ce9..
SHA1:	0a25677fb92664a.
SHA256:	f2a75542290d06d.
Infos:	

Most interesting Screenshot:



Detection

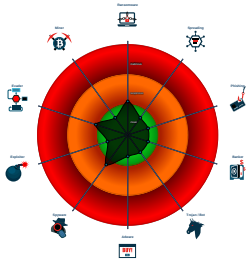


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Contains functionality to access load…
- IP address seen in connection with o…
- Queries the volume information (nam…

Classification



Startup

- **System is w10x64**
- AcroRd32.exe (PID: 7040 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\SECOURS SANITAIRE DU COVID-19.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 7160 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\SECOURS SANITAIRE DU COVID-19.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 6580 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6960 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1736,10090636952361594307,9260773660448689587,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=1248215810438557703 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=1248215810438557703 --renderer-client-id=2 --mojo-platform-channel-handle=1740 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6656 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1736,10090636952361594307,9260773660448689587,131072 --disable-features=VizDisplayCompositor --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --lang=en-US --gpu-preferences=KAAAAAAAACAAwABAQAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=8616662721456202722 --mojo-platform-channel-handle=1764 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 4420 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1736,10090636952361594307,9260773660448689587,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=13245651749807582994 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=13245651749807582994 --renderer-client-id=4 --mojo-platform-channel-handle=1860 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 3436 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1736,10090636952361594307,9260773660448689587,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=14006470410429743815 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=14006470410429743815 --renderer-client-id=5 --mojo-platform-channel-handle=2024 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
- HxOutlook.exe (PID: 808 cmdline: 'C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.8827.22055.0_x64__8wekyb3d8bbwe\HxOutlook.exe' -ServerName:microsoft.windowslive.mail.AppXfbjsbkxvprcgqg6q4c9jfr0pn3kv9x5s.mca MD5: 3F320EB023572D41D0F997F58A5B26CA)
- **cleanup**

Malware Configuration

No configs have been found

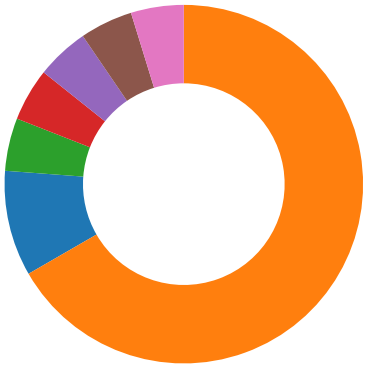
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

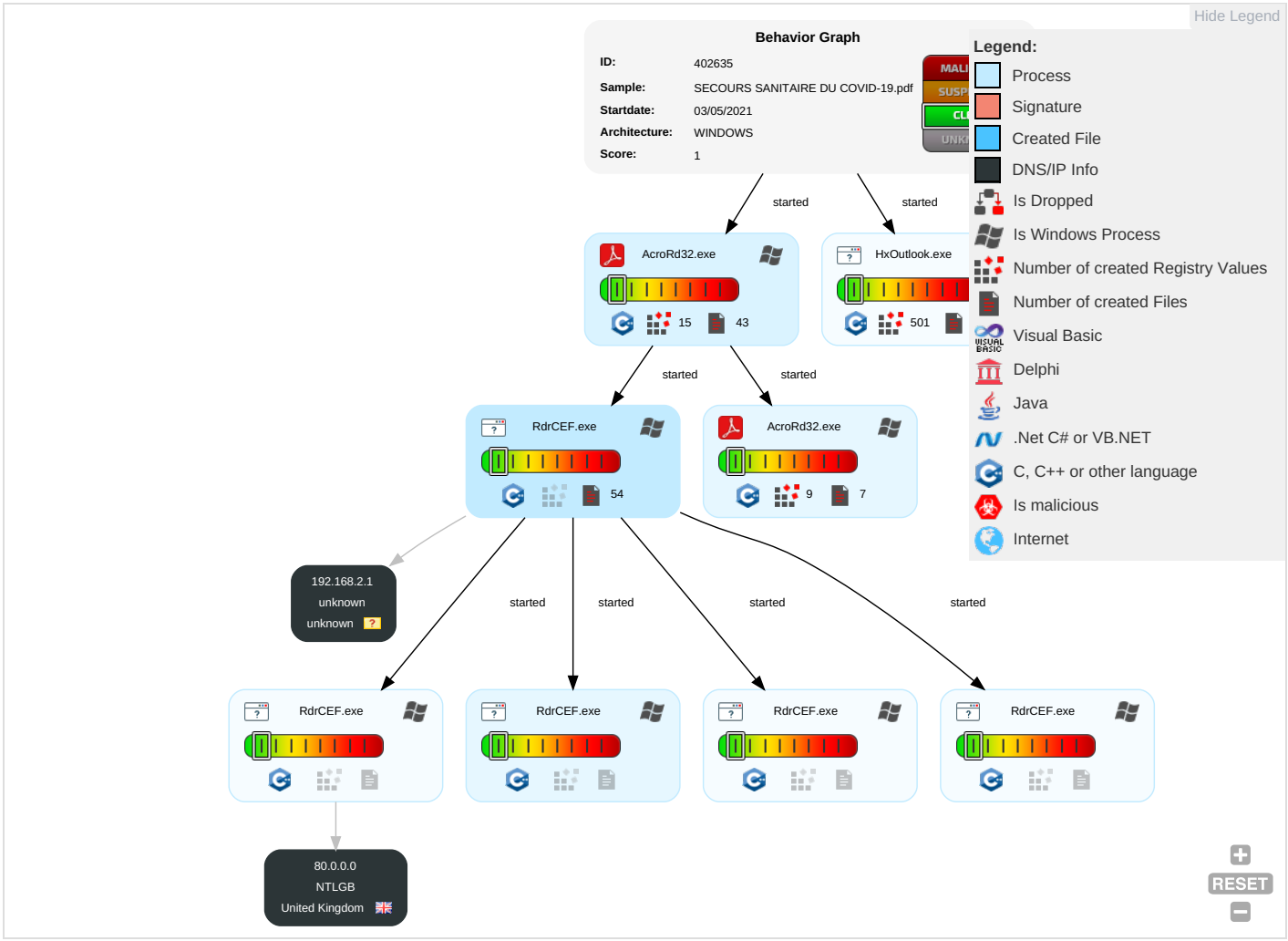
Click to jump to signature section

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
Spearphishing Link 1	Windows Management Instrumentation	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remote Track D Without Authoriz
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remote Wipe Da Without Authoriz
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

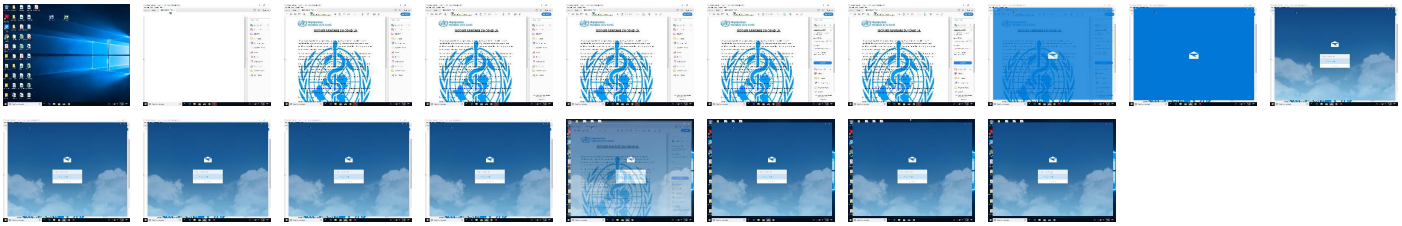
Behavior Graph

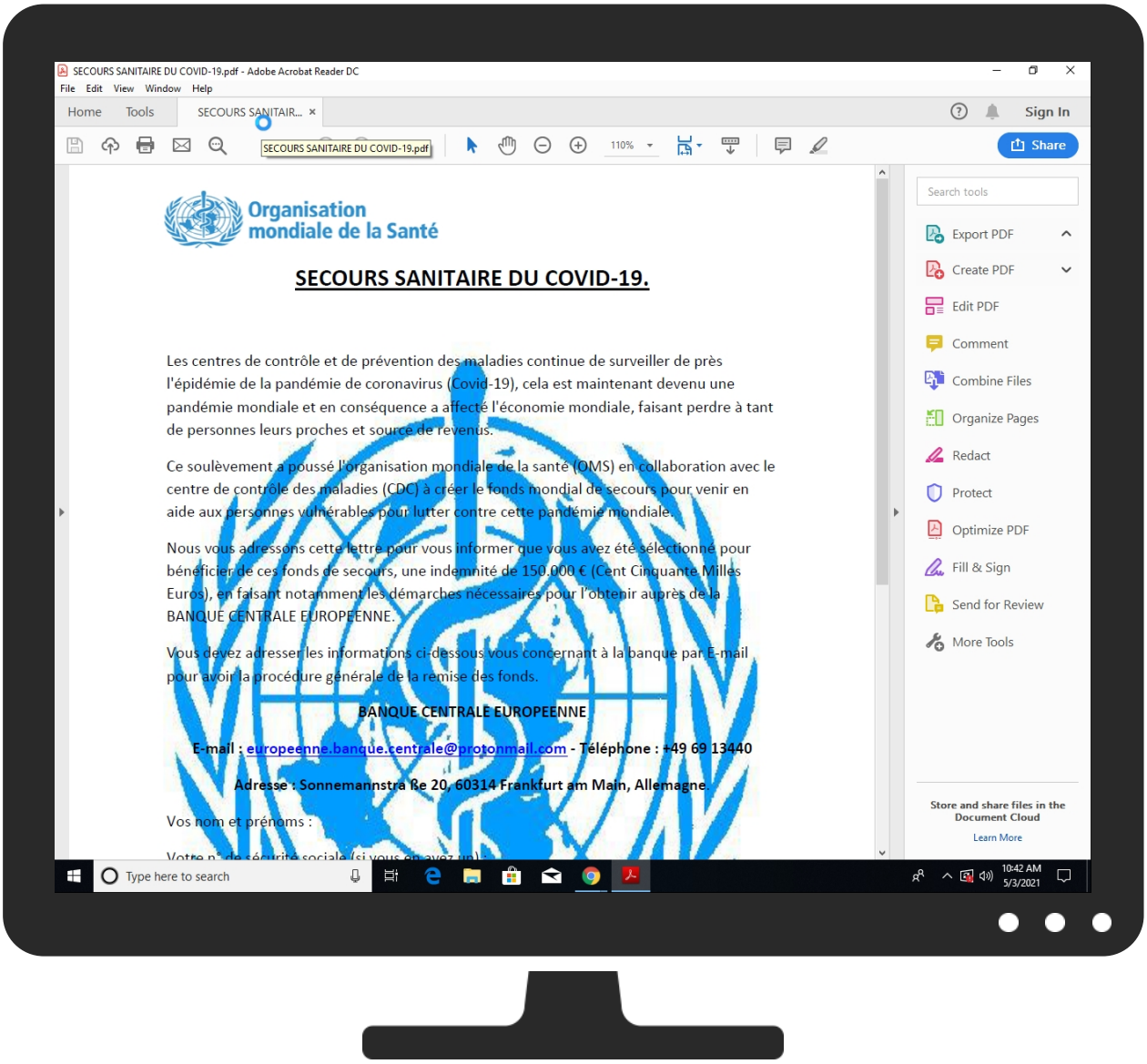


Screenshots

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
SECOURS SANITAIRE DU COVID-19.pdf	2%	Virustotal		Browse
SECOURS SANITAIRE DU COVID-19.pdf	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ns.useplus.org/ldf/xmp/1.0/P	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/awo	0%	Avira URL Cloud	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/Cu	0%	Avira URL Cloud	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://neevia.com)	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/ed	0%	Avira URL Cloud	safe	
http://ns.ado	0%	Avira URL Cloud	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/11_	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/%	0%	Avira URL Cloud	safe	
http://wwobe.com/go/ipmrh?F	0%	Avira URL Cloud	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://www.adobe.c	0%	URL Reputation	safe	
http://www.adobe.c	0%	URL Reputation	safe	
http://www.adobe.c	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/x	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/rs%w	0%	Avira URL Cloud	safe	
http://ns.useplus.org/ldf/xmp/1.0/4U	0%	Avira URL Cloud	safe	
http://neevia.com)d	0%	Avira URL Cloud	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload//;w	0%	Avira URL Cloud	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/P	0%	Avira URL Cloud	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://login.microsoftonline.com/	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://shell.suite.office.com:1443	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://autodiscover-s.outlook.com/	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://ns.useplus.org/ldf/xmp/1.0/P	AcroRd32.exe, 00000003.00000002.874799493.000000000AA87000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/awo	AcroRd32.exe, 00000003.00000002.875293664.000000000AC3B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://cdn.entity.	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high

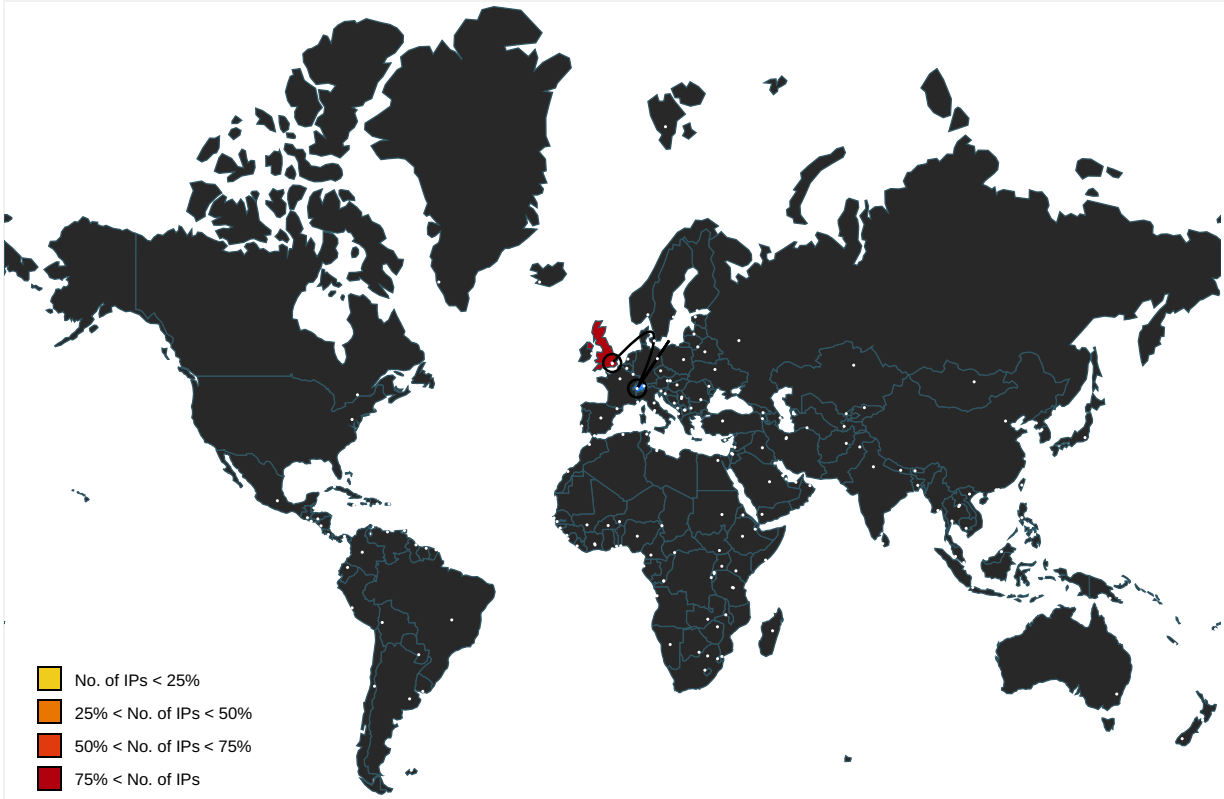
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/Cu	AcroRd32.exe, 00000003.00000002.875293664.000000000AC3B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://powerlift.acompli.net	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://neevia.com	SECOURS SANITAIRE DU COVID-19.pdf	false		high
http://https://rpsticket.partnerservices.getmicrosoftkey.com	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://cortana.ai	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://neevia.com)	AcroRd32.exe, 00000003.00000002.864216335.0000000008C8A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://www.a.com/go/cpdfrhpr	AcroRd32.exe, 00000003.00000002.877800487.000000000C945000.00000004.00000001.sdmp	false		high
http://https://api.aadrm.com/	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/type#	AcroRd32.exe, 00000003.00000002.874799493.000000000AA87000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/ed	AcroRd32.exe, 00000003.00000002.875293664.000000000AC3B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.echosign.com	AcroRd32.exe, 00000003.00000002.877743426.000000000C916000.00000004.00000001.sdmp	false		high
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://ns.ado	AcroRd32.exe, 00000003.00000002.877800487.000000000C945000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.microsoftstream.com/api/	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://cr.office.com	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://www.osmf.org/drm/default	AcroRd32.exe, 00000003.00000002.859807713.0000000007540000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/property#omponent	AcroRd32.exe, 00000003.00000002.874799493.000000000AA87000.00000004.00000001.sdmp	false		high
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	AcroRd32.exe, 00000003.00000002.859807713.0000000007540000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/11_	AcroRd32.exe, 00000003.00000002.875024481.000000000ABD0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://portal.office.com/account/?ref=ClientMeControl	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://ecs.office.com/config/v2/Office	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://graph.ppe.windows.net	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://www.aiim.org/pdfa/ns/extension/x	AcroRd32.exe, 00000003.00000002.874799493.000000000AA87000.00000004.00000001.sdmp	false		high
http://https://officeci.azurewebsites.net/api/	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://ns.useplus.org/ldf/xmp/1.0/	AcroRd32.exe, 00000003.00000002.874799493.000000000AA87000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/%	AcroRd32.exe, 00000003.00000002.875024481.000000000ABD0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://wwobe.com/go/ipmrh?F	AcroRd32.exe, 00000003.00000002.877800487.000000000C945000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://globaldisco.crm.dynamics.com	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://store.officeppe.com/addinstemplate	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	AcroRd32.exe, 00000003.00000002.874799493.000000000AA87000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://web.microsoftstream.com/video/	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://www.adobe.c	AcroRd32.exe, 00000003.00000002.877604078.000000000C88C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://dataservice.o365filtering.com/	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/field#4)	AcroRd32.exe, 00000003.00000002.874799493.000000000AA87000.00000004.00000001.sdmp	false		high
http://https://analysis.windows.net/powerbi/api	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://iptc.org/std/Iptc4xmpExt/2008-02-29/x	AcroRd32.exe, 00000003.00000002.874799493.000000000AA87000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/rs%w	AcroRd32.exe, 00000003.00000002.875293664.000000000AC3B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://outlook.office365.com/autodiscover/autodiscover.json	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://ns.useplus.org/ldf/xmp/1.0/4U	AcroRd32.exe, 00000003.00000002.874799493.000000000AA87000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://neevia.com)d	AcroRd32.exe, 00000003.00000002.875085260.000000000ABDF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://ncus.contentsync.	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload//;w	AcroRd32.exe, 00000003.00000002.875293664.000000000AC3B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://weather.service.msn.com/data.aspx	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://apis.live.net/v5.0/	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 00000003.00000002.863743684.0000000008C10000.00000004.00000001.sdmp	false		high
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://management.azure.com	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/P	AcroRd32.exe, 00000003.00000002.874799493.000000000AA87000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://wus2.contentsync.	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://www.aiim.org/pdfa/ns/schema#	AcroRd32.exe, 00000003.00000002.874799493.000000000AA87000.00000004.00000001.sdmp	false		high
http://https://o365auditrealtimeingestion.manage.office.com	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	AcroRd32.exe, 00000003.00000002.859807713.0000000007540000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/api/v1.0/me/Activities	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://api.office.net	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://incidents.diagnosticssdf.office.com	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/user/v1.0/android/policies	812A11FD-8CE3-4974-9DD1-7CD9EF661355.19.dr	false		high

Contacted IPs



Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	402635
Start date:	03.05.2021
Start time:	10:41:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SECOURS SANITAIRE DU COVID-19.pdf
Cookbook file name:	defaultwindowspdfcookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Copyright Joe Security LLC 2021

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@14/50@0/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .pdf • Found PDF document • Find and activate links • Close Viewer

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 20.50.102.62, 40.88.32.150, 52.255.188.83, 92.122.145.220, 104.43.139.144, 52.147.198.201, 93.184.220.29, 92.122.146.26, 23.32.238.129, 23.32.238.113, 23.32.238.123, 23.32.238.136, 204.79.197.222, 23.32.238.122, 92.122.213.247, 92.122.213.194, 2.20.142.209, 2.20.142.210, 52.155.217.156, 51.103.5.159, 20.54.26.129, 13.107.5.88, 13.107.42.23, 52.109.88.177, 184.30.20.56, 51.104.136.2 • Excluded domains from analysis (whitelisted): fp.msedge.net, arc.msn.com.nsatc.net, cs9.wac.phicdn.net, fs-wildcard.microsoft.com.edgekey.net, acroipm2.adobe.com, a-0019.a-msedge.net, skypedataprdcoleus15.cloudapp.net, ocsp.digicert.com, a122.dscd.akamai.net, a-0019.standard.a-msedge.net, audownload.windowsupdate.nsatc.net, officeclient.microsoft.com, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, afdo-tas-offload.trafficmanager.net, fs.microsoft.com, acroipm2.adobe.com.edgesuite.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus16.cloudapp.net, settingsfd-geo.trafficmanager.net, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, outlookmobile-office365-tas.msedge.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, settings.data.microsoft.com, europe.configsvc1.live.com.akadns.net, au.download.windowsupdate.com.edgesuite.net, client-office365-tas.msedge.net, ocos-office365-s2s.msedge.net, config.edge.skype.com.trafficmanager.net, e4578.dscb.akamaiedge.net, outlookmobile-office365-tas-msedge-net.e-0009.e-msedge.net, store-images.s-microsoft.com-c.edgekey.net, e-0009.e-msedge.net, config-edge-skype.l-0014.l-msedge.net, a1449.dscg2.akamai.net, l-0014.config.skype.com, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, arc.trafficmanager.net, 1.perf.msedge.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, config.edge.skype.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, prod.configsvc1.live.com.akadns.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ocos-office365-s2s-msedge-net.e-0009.e-msedge.net, skypedataprdcoleus17.cloudapp.net, armmf.adobe.com, config.officeapps.live.com, l-0014.l-msedge.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKey calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found. • Report size getting too big, too many NtSetValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:42:18	API Interceptor	13x Sleep call for process: RdrCEF.exe modified
10:43:04	API Interceptor	1x Sleep call for process: AcroRd32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
80.0.0.0	Autofactura generada mes de Abril 27-04-2021.pdf.exe	Get hash	malicious	Browse	
	Autofactura generada mes de Abril 27-04-2021.pdf.exe	Get hash	malicious	Browse	
	1RIA_IT_Formazione di Base Compliance_IT.pdf.exe	Get hash	malicious	Browse	
	1RIA_IT_Formazione di Base Compliance_IT.pdf.exe	Get hash	malicious	Browse	
	123.exe	Get hash	malicious	Browse	
	123.exe	Get hash	malicious	Browse	
	EiK2ZuecHv.exe	Get hash	malicious	Browse	
	File6512365134_7863_20210413.html	Get hash	malicious	Browse	
	DHL_Express_Shipments_Invoice_Confirmation_CBJ1905 17000131_74700456XXX.exe	Get hash	malicious	Browse	
	DHL_Express_Shipment_Invoice_Confirmation_CBJ19051 7000131_74700456XXXX.exe	Get hash	malicious	Browse	
	DHL_Express_Shipments_Invoice_Confirmation_CBJ1905 17000131_74700456XXX.exe	Get hash	malicious	Browse	
	DHL_Express_Shipment_Confirmation_BKKR005545473_88 700456XXXX.exe	Get hash	malicious	Browse	
	APRILQUOTATION#QQO2103060_SAMPLES_KHANG HY_CO_CORPORATION.exe	Get hash	malicious	Browse	
	#U260f8284.HTML	Get hash	malicious	Browse	
	HunpuKMHQt.exe	Get hash	malicious	Browse	
	JbQoNNPVOk.exe	Get hash	malicious	Browse	
	_vm583573758.htm	Get hash	malicious	Browse	
	March 17, 2021, 101142 AM.HTM	Get hash	malicious	Browse	
	message_zdm.html	Get hash	malicious	Browse	
	0000001_Carved.pdf	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NTLGB	8UsA.sh	Get hash	malicious	Browse	• 82.32.79.178
	x86_unpacked	Get hash	malicious	Browse	• 82.17.192.153
	Autofactura generada mes de Abril 27-04-2021.pdf.exe	Get hash	malicious	Browse	• 80.0.0.0
	Autofactura generada mes de Abril 27-04-2021.pdf.exe	Get hash	malicious	Browse	• 80.0.0.0
	rIbyGX66Op	Get hash	malicious	Browse	• 86.18.93.173
	1RIA_IT_Formazione di Base Compliance_IT.pdf.exe	Get hash	malicious	Browse	• 80.0.0.0
	1RIA_IT_Formazione di Base Compliance_IT.pdf.exe	Get hash	malicious	Browse	• 80.0.0.0
	J76uxxiy.exe	Get hash	malicious	Browse	• 86.18.99.199
	123.exe	Get hash	malicious	Browse	• 80.0.0.0
	123.exe	Get hash	malicious	Browse	• 80.0.0.0
	EiK2ZuecHv.exe	Get hash	malicious	Browse	• 80.0.0.0
	File6512365134_7863_20210413.html	Get hash	malicious	Browse	• 80.0.0.0
	DHL_Express_Shipments_Invoice_Confirmation_CBJ1905 17000131_74700456XXX.exe	Get hash	malicious	Browse	• 80.0.0.0
	DHL_Express_Shipment_Invoice_Confirmation_CBJ19051 7000131_74700456XXXX.exe	Get hash	malicious	Browse	• 80.0.0.0
	DHL_Express_Shipments_Invoice_Confirmation_CBJ1905 17000131_74700456XXX.exe	Get hash	malicious	Browse	• 80.0.0.0

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL_Express_Shipment_Confirmation_BKKR005545473_88700456XXXX.exe	Get hash	malicious	Browse	• 80.0.0.0
	APRILQUOTATION#QQO2103060_SAMPLES_KHANGHY_CO_CORPORATION.exe	Get hash	malicious	Browse	• 80.0.0.0
	#U260f8284.HTML	Get hash	malicious	Browse	• 80.0.0.0
	HunpuKMHQt.exe	Get hash	malicious	Browse	• 80.0.0.0
	1.sh	Get hash	malicious	Browse	• 62.254.90.3

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):	410
Entropy (8bit):	5.658840237319054
Encrypted:	false
SSDEEP:	6:men9YOFLvEWdM9QO+tKPi7Z+P41TK6tven9YOFLvEWdM9QQq0kHi7Z+P41TK6t:vDRM9p+tfZiEuDRM97q03ZiE
MD5:	337C928FB1EF1363A22D2EC97A480046
SHA1:	124F3495050AFB1993F430D99FD6AF3240CF789C
SHA-256:	DF9BC1D9A6C9737F0FB544179CC4398E6E0593C64C51FCA59236A97BBABE4B85
SHA-512:	D4ED73FDFA326B3C5B7F6A7AD33E8F524E19D404DA86AC09EE0C5EBF354F6826FF612E5BD87AC6FDBD556A2271B81DC970EE6C094DCA7845837E9D1EDDD35DF1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ...9../....."#.D..0..#.A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....i.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ....9../....."#.D.4...#.A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....wC.....

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):	348
Entropy (8bit):	5.59997034576216
Encrypted:	false
SSDEEP:	6:mi9NqEYOFLvEkYSlR6i8Be7Ywcr1TK6tw+i9NqEYOFLvEkuXPimi8Be7Ywcr1TKq:V9z4Slli9PQu9zOXKmi9PQ
MD5:	D6099F206D5D482E97A7CDF361D6DB7B
SHA1:	C89435F277A3C3343A9FFD0C677C58B1922BC95F
SHA-256:	E6C59BE2E032AC6E9404A6DD1C7DA1AAD75CD59FCC0B9BDB2CD8DC759EDB9EB2
SHA-512:	11029AC1CD1D21A0164B481E79A7752141C4A68DB6192D0B4BE90BB24675C3D2491810750B6C98D1C1EE93B8292D3144ACF318001F6E48B21C15CFDBA6D756F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,.....keyhttps://rna-resource.acrobat.com/init.js ..Z.9../....."#.D.....#.A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....|.U.....0\r..m.....,.....keyhttps://rna-resource.acrobat.com/init.js ....9../....."#.D..k..#.A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....].).....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	492
Entropy (8bit):	5.606656851758017
Encrypted:	false
SSDEEP:	12:DyeRVFAFjVFAF+05lUo6jVyeRVFAFjVFAF5ZI5lUo6jL:tB4v4+05SBrB4v45Z+SB

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
MD5:	A0D671963684E0B295FCA471B2FDE4B0
SHA1:	5C198D99C66B1BCA2FCBA19A5BFED05E9547C537
SHA-256:	4D7F9D569B97C14B0C46C08B5CAAB61A623C2E3524E640AC99550AA1CCC7508C
SHA-512:	662A41942D7CF0A05E644200A835291EFF928127969009C4FF6AB984B4CC2F4CD9D2872B986E3521FC5B0816F0041AC2A9C4AB5D5356CC6DE159887F9090F44D
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 ...9../....."#.D.G/..#.A..hvDO.N.t@.... .n.*..... ....A..Eo.....A..Eo.....YV. ....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view /selector.js ...9../....."#.D.....#.A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....;R%f.....

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):	5.654245396048643
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RsbQ+tjjniWulHyA1TK6thIt:IbRkiD6NtfiWuss3It
MD5:	B8C608B4C91BC43F7EB1D76607E30970
SHA1:	13FC9C010FF0A2358CF695C96837EBAD81884873
SHA-256:	4F9A9F0570CB184415C30DE9E79F71B238FD48183E62C7BF38F4393DC31A8811
SHA-512:	549EE4B81E68AE4D295F2C45C8327F052DEF8AC1FA5B0C5C318BAE9A6A6938F9DB13966333E832786283DF668762EE9051A7B3ED7E4176CDE1FA11867159C9A
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 .>Y.9../....."#.D.FF..#.A..8 P..a...R..Y....7.@..2Dm{ ..A..Eo.....A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.57241656445542
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVuxO+teRVyh9PT41TK6tNl:pyixRuuqGV41TE
MD5:	006E094A022130943516959A0D381849
SHA1:	4DF73E2C7DBBCF395F66B72E95326D52D39DC7A5
SHA-256:	B086E16883E805569B9458544C87352B1FEBC337A16CC091DD0DFE092004937F
SHA-512:	ED222E5209685E2E3C91CEE2DB581D076998F8997BAC38A3C471080CE7BC420D26C6A16D2444DEF87920CE556F9A4FC899758F4667D6A6BAE475CEAB76F3294
Malicious:	false
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js .>..9../....."#.D4....#.Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo. .....`x.....

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):	5.584610867645724
Encrypted:	false
SSDEEP:	6:mvYOFLvEWdhwjQftHfvLZIl6P41TK6tq:0Rhk4/vLZC
MD5:	42B3D69BB8DBE1EF762C3A8D84A6AA6A
SHA1:	20552CF8EB687F2A22B960D3911E50BB6BBC223D
SHA-256:	87BBB7D3AB0834D7FCC875C8279583269FBFEBB5DE2FF9008453A537D3DE68D0
SHA-512:	B05385CEB60FCDD409A0D351D1D612A8B07CF9C53CB359BB2E190AB10743D047FE367720792FCB8932C5791B322674530A9C784FA804D9723FBFAD83DA70BA1
Malicious:	false
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ....9../....."#.Dm...#.A.].>....uUf..N...k.....c..l.A..Eo.....A. .Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
Size (bytes):	209
Entropy (8bit):	5.542909074501602
Encrypted:	false
SSDEEP:	6:mJYOFLvEWdGQRQOdQ+VkG9IV6g1TK6tPyt:2RHRQCxuV1
MD5:	CE863190E0A25F362A22CF6518631483
SHA1:	BFA36C27A753E09D0DD0484F899FD4FAD2D021A3
SHA-256:	95E32B32A0F7E84992A8D53D20176B99946C34105ED7D6CF383004F4F66FBEB6
SHA-512:	5361F830F575194102E322D4A39C9DBE9ED662708C1769077121C42180CF4F2240FD0E01C9F0C5CCE727C9A7CF59B40144DE7A9D15101BC2AC3B0C08EC04E61
Malicious:	false
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .2..9../....."#.D.(...#.A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo .....w.....

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):	358
Entropy (8bit):	5.586311386306126
Encrypted:	false
SSDEEP:	6:mOYOFLvECMLBtfGLMuR/41TK6tA2OYOFLvECML/wMuR/41TK6tl9/l:Z5MnfGLMuR/E05MjwMuR/EL
MD5:	96952EF6C86E9DEE8EA9B8EA04617E51
SHA1:	EF6A3C913114299634805FBE66F4D4AE33800AC3
SHA-256:	33567F9C44E36FFA691760BF320FC5BE4B4A00B5D86ED4DA8F6C5E70AF5DFB5C
SHA-512:	83466A4F93665DC7BAC6E90B3C5153AAD2E0AA4C20A9C6CE4728AB78ED86E93A862C78115253A574D4D0B8459FCEF1DDE8EA0516CB0794A76CB5235A7564AC 60
Malicious:	false
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .a|.9../....."#.D.....#.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....[.....0\r..m.....3.... <lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ....9../....."#.D.=k..#.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....!7b.....

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):	5.519567742542208
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtugV15by0zBUKSAA1TK6tx:pRJV15beL
MD5:	44F1798CC30FF1AFC4F841BD439BF234
SHA1:	EF288D8E8F0DD06CEB945A489D9FD8325CCBA1D9
SHA-256:	1500A5CF78B0A27F3C66A2C34DBB5D88C1ED36F8E4F547DF0F9EC277AF0FBDBE
SHA-512:	057D7EEF1BD35C85DCDDB3FC2A940A0D70DD0B06AE4495FCAB8DC6A045CF8B44E7989007DAFF97583143851243F51E9FAF462EFB15968F17BC7270F489C81B D
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ....9../....."#.D.I...#.AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....A. .Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	354
Entropy (8bit):	5.555302042202179
Encrypted:	false
SSDEEP:	6:md4HXXYOFLvEjMSWFve2tvttUdyP41TK6tFZV+d4HXXYOFLvEjMSWFvqqUttUdyo:KkXxKMSCveS1tUl7WkXxKMSCvqqotUl
MD5:	48DE77E83CFA0ED9AF06CFCD3DC57358
SHA1:	D5541D50758F7895857AA371E63EF35162383D69
SHA-256:	E5C7F45ABBE964E1DB7BF3895965E59F8E174D376B253A4730DDA3D0DE2AF7F9
SHA-512:	259A7D9CB64F456F915C4DD67C0041AD11C59AE33017F2D69D140FA49D75875CFE8FD94EAB2060EC65F9C3EB17544B683B372B341C60630F9A008C053883A783
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .)z.9../....."#.DM....#.A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....O|0.....0\r..m.....1 .....5...._keyhttps://rna-resource.acrobat.com/plugins.js ....9../....."#.D.)k..#.A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....g..8.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	374
Entropy (8bit):	5.530681274058526
Encrypted:	false
SSDEEP:	6:mkl9YOFLvEWsfOL/MqJZPyyM+VY1TK6tlNMkl9YOFLvEWsfOLTIrztM75PyyM+V3:5h6OLEmPfkHNzh6OLErztI5Pfk
MD5:	749A2C6B9F47B9D9653859DEE440818A
SHA1:	4BFBF77A124F90CCB303340CC3A03105BE7A9B0A
SHA-256:	87746DE7915D9B2245B13745BFA4909189AAC1B4C2F9A7D91D6ACE92F68F31FA
SHA-512:	B64FA8473713114EB8FF83636514FDFCB5B131EA445ADD3B33A1C6D9F16AC5A601F1F59F67544481A111A037E4584B2D4F82C80FD04C0CBB8AEDB76BB27122FE
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ....9../....."#.D.....#.A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....Io;.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .J1.9../....."#.D.....#.A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....J.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	488
Entropy (8bit):	5.651667205231259
Encrypted:	false
SSDEEP:	12:URVFAFjVFAFexQGXwSeKaTLnLRVFAFjVFAF2qwSeKaTLn8:UB4v4QQgwzXLnLB4v42qwzXLn8
MD5:	B2DA8F297928D21455EB491FAEE190A2
SHA1:	65B6044DA5F17460A59D6B16EA5A88F347956BFE
SHA-256:	1BA38FA1C4611E91C4A501C5F21EEB3E3260AAC4E85F0E66D418C5A8BD66B7FE
SHA-512:	06ABEE61FB19E74924A4EDC7322925A2F18EDA3A0969B5B06F34809CBA090C3638CA612ABC6A7628B7177065FAF58A903CE5193D318411857B666B686C8D0B38
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 ....9../....."#.D.j3..#.A.....H...{...2./.k`..r4.C. .A..Eo.....A..Eo.....X.....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 .;..9../....."#.D.....#.A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....5J.....

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):	5.518423690292057
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXu1sMChR11TK6t:BsR2EsevMY
MD5:	4729B795303972774BD3F7EF2AFB41E4
SHA1:	E6D7425CE0B9CA6AF47030FE0D0F2A154894455E
SHA-256:	9C69FCE99EE6942CE2E191AD248AA3E085D53260330AF87EDDE045B312712F83
SHA-512:	12100EE216159331D588F2914DDB424BDA370FC2665E7F8AF2FC6B5721101A9CA6D47BBE1493D5FB4F4CD464377DCC0F922746344536FDB7DB5996BC8FE10BF
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .:...9../....."#.D.x...#.A.A.o]@r..Q.....<w.....].n\....A..Eo.....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):	5.599666486546901
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQntGp3B7OhKlvA1TK6t:RbR16ktUBJk
MD5:	CD4AB2BFAFFE5D8E9BA4A5C11BC52DCC
SHA1:	9834403297921A4C48AA61624998EC9C9266B6D4
SHA-256:	4400FE4E1307D536AC1D5E4C9FD0C0F042488B50F68D56C04D5BF16BE32FB559
SHA-512:	1619970D6FD798777F8CA51E87879FD5E089BDBC4EE8AAE7D61979E02BE2E804696C04A26BB9A1B3D877321400362415B0A538A5C11016BC6322D79BFA58840E
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ....9../....."#.D...#.A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....Ep.\.....

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):	5.5633842941689435
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVuvtVl9RQdFt1TK6tp:B2geRHRQSPnR0
MD5:	693519D9606A1AF2D0DBA3CB23B7CAA0
SHA1:	6AA44F76461B364C23811F390D27A618D0C348D5
SHA-256:	FE4A5495EB56426E529D1008687CD9CF03CC6BD96723A82FA96E2477FD320896
SHA-512:	7567FF24145FCEA846EA757324B76F2045DCA3435C8DC458B1AF94F25E863997732EF3BCCEA12EDD2B4FE1BE06E96CED97A26C44553BD640544154F214B26B3
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js . ..9../....."#.D.p...#.A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A. .Eo.....U.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	412
Entropy (8bit):	5.638238150124545
Encrypted:	false
SSDEEP:	6:mzyEYOFLvEWdrIOQJktU7GRt1S/1TK6t4/2zyEYOFLvEWdrIOQo6q0LMqAt1S/1E:WyeRleMU6Rt1wHyeRlMq0RAt1wxI
MD5:	0AF8AEBBA3F20E3F99E0BEEFD171362F
SHA1:	39A9CD70D34DEF454199D8D1DB3CC9984A1453A8
SHA-256:	32A55B5F288C70A3EB84B99DBCE62E3C60DE197AE3D995986391FD1FC6690CFA
SHA-512:	8629AA4BBC260955C937F5B2A97353AFF17FCE440983D339C369610390B12F3088CBCC664C7A28BEDAC0ED424AC5E32BE8160F61FC83FA0C74861B8AE997CF8
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...9../....."#.D|....#.A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo....."..... ...0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ....9../....."#.D.....#.A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....j.e. .....

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):	5.546827405526904
Encrypted:	false
SSDEEP:	3:m+lKcv8RzYOCGLvHkWBGKuKjXKoyNH/KPWFvXKFXYLeqNqww6U+5m1TK5kt:mnYOFLvEWdhwyu2XYC6qwK+41TK6t
MD5:	B06299CECB677BDAD350D72F7E1C369D
SHA1:	AC5B65628832265C630B128F98A2ED17EF34E8F7
SHA-256:	6288CFDE8A1C53547E82E3DA242C9A4B38F89FD4678A3D997312AC1FA6796202
SHA-512:	2B1D9E272C4397014DB8612AEE76D963B3056792FE67D29BC51F00F9E90084DE77D24572EAC807E70A2FADC679EE3FA197030523B0E864A90DA00C85984D55E1
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .r..9../....."#.D.n...#.A.....7...o..a=.98l.....(3.$G.A..Eo..... ...A..Eo.....O.2.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	460
Entropy (8bit):	5.602945556069899
Encrypted:	false
SSDEEP:	6:mYXYOFLvEWdrROk/RJbuyquqJrfO441TK6tB8YXYOFLvEWdrROk/RJbuUVwXfO4K:/RrROk/SVlfLElRrROk/lwXfLE9
MD5:	7D4D770BF82F685EDEA2E3D1135966D0
SHA1:	1937BAA4CEED63FE6772A666FF66E4570D67B2AF
SHA-256:	F4BC4BBF2A73869D38F5BC1F01169E757CAD54C5E062215681D2DBFF604E4D60
SHA-512:	5A3D43F64BA65B9DEE744B5CD176908AD51124CFD420DF2FCC48341FBC3FC76786F930E8A61C11BBD839CF6822C33EBEF785EF5C3635CDEDD79EE739BE004 99
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0	
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .p..9../....."#.D ....#.A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....J9.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ....9../....."#.D.....#.A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....QG.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.5601717459682245
Encrypted:	false
SSDEEP:	6:mmDEYOFLvEWXIxKS1QPLr1TK6t6mDEYOFLvEWXIcIrztCS1QPLr1TK6tZy/:xqTIKSCPLnHqT+t5CPLnvC
MD5:	FA10D7F684DAB4BA207E5C33B1C393BF
SHA1:	9415384E167CB39A167D2879E1DCDB98A99A3625
SHA-256:	F02DA55C5710B018E8E0AE9F36E858627FA9EE2A9615F68B86B3AA8E7404779B
SHA-512:	6F4138FC1F4B50DF970E7C604CC0FE267D2E0BC6237FA73C2A10388F13A900B8D1A1EAE780BF82F1F49CA503F466FA99361CDA131C33E4F19F577E48784036E9
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ...9../....."#.Do....#.A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....].....0\r..m.....:.. ..f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .@#.9../....."#.D7....#.A..~]...%s..<...n.f..<.....1#..U..A..Eo.....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):	414
Entropy (8bit):	5.620794345424888
Encrypted:	false
SSDEEP:	6:m52YOFLvEWdMAuL/M33sEJ41TK6tOlM52YOFLvEWdMAuE+xm8sEJ41TK6t5X:zRMJ/MnsD4lZRMuwm8sD3X
MD5:	5BCED708998A83A8592ECC478633FE66
SHA1:	EAF9385CCC1E257FD9BADA8A88C7A6C308D3959A
SHA-256:	49BACD9A1952DD706BF3558C4E63121AFB5DEC72D7E1F29210F07CEE5BD1720C
SHA-512:	A9D821DC9FDF18FCE5198BA3442626863C9B95794DD1B9736DACB8C28560844B9D490AF093279CD2625E8AD89A4E92B503783B6EA2F6AAEDF8A06516270C76D
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..u.9../....."#.D.....#.A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....G.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ....9../....."#.D....#.A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....".....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	420
Entropy (8bit):	5.55890951410686
Encrypted:	false
SSDEEP:	6:mYilPYOFLvEWd8CAdAuJMKGURYbSFong1TK6tE2YilPYOFLvEWd8CAdAub8wMXbh:6lJRxdU+bSFoM+qlJRY8nXbSFoMY
MD5:	F718A59CA0C550E613D275CB499A459E
SHA1:	890C8BAAF76972C668787F860716C9C81F3ACA31
SHA-256:	57E29FF5A7820D811EAA035FE39597B1DBD7037EBCAFAC527FEC1A0BEFDAB1A3
SHA-512:	CE595EE785F97C408F7503B295E1B43095D6D31CF48ACE6C20A72C4D93DBFFFD147DD09566AD35861D7E966FE0F9C735A0EA16881A4F0CBD80D8305AAAFA298
Malicious:	false
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ./..9../....."#.D.#/..#.Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....n.....0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ....9../....."#.Dt...#.Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....hc.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	446
Entropy (8bit):	5.585643937662875
Encrypted:	false
SSDEEP:	12:F8hRrROk/wXLPe2KHt8hRrROk/3tNe2tK:UPJ/wXi2ScPJ/do24

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
MD5:	DE04DA7D21B414A305EF9E5509C50865
SHA1:	83389CCABD84C76C38C3F96A9984B7FCD064855E
SHA-256:	55E180D36DE11DF3BFDD3D68871B6D62FC6AA4A13771F30A85CFA34668DF7546
SHA-512:	5BCE1E4A1EAF5850377C5ACC15F6AF2F745F2DF579395FE8268B3BF0D669BFF5E4D9A394A831A8DDA920C0EBC60A82713544B1355B9E2B26B92940F9EC482D5 4
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .?..9../....."#.D....#.A..%.k.SZ..~W.....:)'B..ad.....A..Eo..... .....A..Eo.....y.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ....9../....."#.D ...#.A..%.k.SZ..~W.....:)' B..ad.....A..Eo.....A..Eo.....~.e.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	426
Entropy (8bit):	5.656431739080202
Encrypted:	false
SSDEEP:	6:mLrnYOFLvEWdrIoJUQk9muKrNJIi1TK6tgf8LrnYOFLvEWdrIoJUQ/2KrNJIi1TM:ehRctwuKrNJICu4hRcy2KrNJIC
MD5:	2CC2F57AA05FA6C64B334291D63D1831
SHA1:	F5E11E4F9CB2EC528BD640E93908A93F31435A4A
SHA-256:	6DC1C4DE360EAA14848BC8BBC90E9702E015C5A5E78DDDC5A37C35816B086F6F
SHA-512:	4CDB0A729F24ACBB89BEA1CC3A51362CEAE773A6C4D45271F7810C02113DA53CAA86EDD4926E33E3B479E4F384ABD90B6FE20149FA26D7E46271AD5232C64F 83
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..:.9../....."#.D.....#.A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A. .Eo.....v.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ....9../....."#.Di9...#.A.;"./N_.,.:C..2....9L.H...3:...A..Eo .....A..Eo.....W..$.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.5706345669651025
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhufYLzgm2d/1TK6tGOEYOFLvEWdrIhuuqrzLzgm2d/1TK6t3:0RxuReqRDjRe
MD5:	AF845C1692A05219F57817E220B9FC07
SHA1:	0F7327BB8D65AD194D1B9B2D555AFF62D677CD7D
SHA-256:	9A82FE328FDAED47AB0270DDA6C9FB6404E9989BA7A46D5E0E441E5611410B50
SHA-512:	867615BB8CDB6E1D11E951B2C8D3EC33724016ECE899E5292F7C77B36417A00D1B4548E6C6CC03B017F4BF7E28DEAD9F99F6F496F75A9BD9C4538CD2ABDD0 A
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .Y..9../....."#.D./...#.AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.. .....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ....9../....."#.DE....#.AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo..... .....A..Eo.....y..B.....

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):	376
Entropy (8bit):	5.6348198277060115
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1KRtLckx56uvp1TK6t7f+AElVYOFLvEW1K5MUhkx56uvp1TK6t2:6JJKRtLblCJJK5MDo
MD5:	C200CDC1AB9E4D905866B0905D160165
SHA1:	25601661AB1E6E3250854ABBCB5204B2AE658D2C
SHA-256:	B0466A1B555227C060BC5DEB4C5E2BDC7CD8EC05B91F32B8F78B7F1D10BCA43D
SHA-512:	1C723A24E6871238498E0D6F39C97BB167B91BEA5A94014A97B236579D6D0BE406746E63D7818A581600FDBC51D48A0D13261C368EF39701C866CB666C0F757E
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..h.9../....."#.DW....#.Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....4\.....0\r ..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .`..9../....."#.D>...#.Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....7.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0	
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.647943744083046
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvuHKXG1WhUDLYtmOZn1TK6tn:xRBJ2qQjDcFZL
MD5:	DFC8FCF24E33ADBCD73A96B6C36349FC
SHA1:	F5244C1A590BE78CE7A645E9919042C90708E181
SHA-256:	4CD2A15CC1C19BD643FF36CBFFCAFBD85BEDC52C256BE40F67BC5B39C9F248A5
SHA-512:	BCDFB3F43A39A277C326920BF84C9CC775002918BB7475D166A17F0D0BAB99BB49C2B19ADE52BDEEDD942CA1F257F405C83A179B8829A497A09E38C72F14A7D
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ....9../....."#.D...#.A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....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):	422
Entropy (8bit):	5.648162367037879
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp7xS4QEVPu1TK6t5JsRPYOFLvEWIa7zp7sxwkkVPu1TK6tE:BPH3SScPqPHaxSc
MD5:	714A103936CE682EA58AE2FDA82568BA
SHA1:	0F8E38EE12B98267F1F218D8E3131D31FC54A213
SHA-256:	893DADDC0647D287874FCD3F94187690733175AD6217454C659978479DAEF31E
SHA-512:	28330DB7A50404F0D23A9AE948480AF10B14532CF2B6942E975BB32ECDBB9E490AC39079F0988C2FB4AC19AD69C2FE4068A636E7BCD0B04CCDD4087298DA655
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ..~.9../....."#.D|B...#.A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo....."....."....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .K..9../....."#.D..k..#.A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....

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):	5.590930277212667
Encrypted:	false
SSDEEP:	3:m+lQi9lC8RzYOCGLvHkWBGKuKjXKVRNUpXKLuVs6KXsMfl44XVAZ+8cV3vRm1TKf:mKPYOFLvEWdENU9QFxs8iM3Y1TK6to/
MD5:	834F42FDA31D52586EE3B29C53BB6B75
SHA1:	12DF6FCFFEF9C2A3FC5B4963402092D7A68866AA
SHA-256:	5BA83C44BA8D3D32CFA035BE2801C6FAA7DDDF178E4CAEE2A59B92F7D928A270
SHA-512:	22171EF60E99CD83A72599B96AA10C911A18F630AA3ADD7AFB6CFF4A639B90AC6B6139481AB056C1DB8F5C2FEC0B97CEBD42D01AE1ADF128B14C17F9E45B55A6
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .e..9../....."#.D.....#.A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.....2.&.....

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):	5.63900720028959
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQNbMXahjBRCh/41TK6tM:XRc9ibMahDi/E
MD5:	D44A1AD235DAC63E4CC042B8EBC4BCAA
SHA1:	602FD18A202E1769863868D9EB2E1D7043F37CB8
SHA-256:	1BC1E36BD57076478D6F82B02F89063F5110EFC6648B1C7C5CDEA1D903A62578
SHA-512:	B94B94EAFDD87C0B80A9E57908E8AA7716C68423BDD3BD7FF223D1FB2543576C1C43593F80BA704895CA5EB51D3C9FD5FA1E68DDB96C058487A5903E456F452
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ....9../....."#.DK....#.APJm...0x.x..RD...BB!@5..<..]....A..Eo.....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):	5.594119604100184
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhuj9qk10ULlF4r1TK6t:bs6xRkil9f1LLlF4n
MD5:	7B71BD5FC86A9D5A300A2123C71BFFF0
SHA1:	8E94C39BF41E7994F5BCEC10C51D80D2D7378857
SHA-256:	C01DE1FFD449C2E667F5A2C5DC83B7EF7EE772356A5C306CAA61120C8FDBADBE
SHA-512:	969400C32DB3E683C3D97B67FB098D2BCF34D97EA4276FA28CFD83C16A0FCDA30AE93EB70DB55212147AE79A1D3ABFF51837A0839CA9472F2B8476B161EF43E6
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.9../....."#.D..!..#.A.P...#4..l....5...5..).w.. .h.~..A..Eo.....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):	5.497259516783186
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvpbL/Ymi4cu1isLK5m1TK5ktwPl:mhYOFLvEWd/aFuD3/Ymw941TK6tY
MD5:	CB8D921D1C0646A1F8663B100E22A1FC
SHA1:	EA723C18227D4D1AA6BA5AB0907154DEF9AE8806
SHA-256:	6CC943913A00943455DB603BCDB7B1DD1C91606FB815AC31F1A2231A6BE8DE76
SHA-512:	61264CB4F8C7B8500E3493945D3D8CE49EF41BFCA1139AC0557CD94D70547EA138651CBC5B30E58B91DE90E07377549430DA6B2AD78ACFBA6ECE1A7DE9F967D
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ....9../....."#.DJy...#.A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A..Eo.....BU8.....

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):	5.523768741628341
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQ0x3oBMqVd3G4K41TK6tGll:2DRuRlaB9Vd2kgl
MD5:	754CC7A78087C68161474B9CE8D6445E
SHA1:	2E8AA17FFC75AD2CD6FF4B38A18B79D8A16498C3
SHA-256:	75245508B74ACD705D41BC5750F70814A2CC0AF1E83D793D1AC391659392848C
SHA-512:	12E993197A0B841863FADFA9892C27D541D64DDDA3D275709C0E248AE08AF400FAF906004406A58E0D476B31E38729FD64DFC9D190C5C40057CA102415F0EE08
Malicious:	false
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ....9../....."#.D.S...#.A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.....o.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.6084858877607
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9QdtuZwuA424r1TK6teulekqYOFLvEWd8CAd9QBXp6uA424rh:+RQ2tcrnD2RQEpFrn
MD5:	9BB7E229B251350A77B8F2FA1A36ED42
SHA1:	56B8790E575C9F9FE0CCCC1DD78E7F4F1D4CDE67

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
SHA-256:	97C2556436072B6A8ABBA4A7127E89E9768327D43A82364B22E4EE9F1375887E
SHA-512:	097F21E7BA434607C6C3EC319F3C3AC9330F63208068802486E5C8D0890DA24F7DEE705E2A38C1004BB5CE537222CB0B7CD4E8E569D81EA19F6640A0FD410B2
Malicious:	false
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ....9../....."#.D.U5..#.A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .c..9../....."#.D.....#.A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....[AW}.....

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):	5.542238794053818
Encrypted:	false
SSDEEP:	3:m+lS5Etla8RzYOCGLvHkWBGKuKjXKVRNUp/KPWFvSwr6KXXRMqTbg2iHio/Mm1TI:moXXYOFLvEWdENUAu1XhdyC8n1TK6t
MD5:	BDAC9A51FCA4048AA6F7F460350AA3B2
SHA1:	C489B4EAF3982ECF47CD04EF4FE0B902DE419149
SHA-256:	FD820E14608F70B35478819123A08D3A283F2931CC51DCB2EAED59695EB4B914
SHA-512:	06F143A2EE516D9ACF4E8AA79C166CEA60F92121C26FA901DAFB7A682414061D5FFAABE46A13BDCF84F412E488F9E68A2DF16C9AD288C2CC5032D66823EC66E
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ....9../....."#.D.Y...#.A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....q.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	442
Entropy (8bit):	5.634004596141614
Encrypted:	false
SSDEEP:	6:mQZYOFLvEWdrROk/VQ4x2DLmB41TK6tHtMQZYOFLvEWdrROk/VQFRW0LmB41TK6t:nRrROk/V7NmblRrROk/VaRUm
MD5:	52797E523D2CB839E6473F1F0881D40F
SHA1:	A458B8B62F00271C86D5781BD8FD6F97F8E05F9D
SHA-256:	91E81AB639F2D4B52EE75E3C0E5C853EF510902AC346CA7673C457495F21CBA7
SHA-512:	5F921C0C404885A71189F08C8590CECB92408E914D65D9190DAF3C5CDDCB0A1A2FDD2A2FCA89214D642F7201F5B953A25982FE922DD6C030756C6F29F489C93
Malicious:	false
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..=.9../....."#.D.. ..#.A ./.ev.....N~..6.b....$.j;:C...A..Eo.....A..Eo.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..#.9../....."#.D.G...#.A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.581753397329317
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWurx3H93Adm9741TK6t5H/:qxRcjhAdu7Ev
MD5:	B31D2FCBF9DCCFD78EA60D43DB5284B7
SHA1:	92457C389B4115F9874E09C4EA06529018390F2D
SHA-256:	D1998E1830B7D97F7788FE7954B9D224A0A50DFA6DD98A4AD60D5AC24DF93C5A
SHA-512:	8593F609D90BD668EBFC5D0FFEAA921F435288AC7D1EF2EC144EC0E3572AF39FCAF1B864164FAF5FFE21577C80187D156FBB080156B0CA6D967715A6C243C90
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ....9../....."#.DAb...#.A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....v.g.....

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):	5.579236928841981
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0	
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFvZ76xUeA16shoq+Nem1TK5kto9/:mMOYOFLvEWdwAPVuzIUeAYJn1TK6tg/
MD5:	3682CE97C54872F69830B4C82729FE4B
SHA1:	EE3E1C5955952E58AD3319536626644CF68A5FD6
SHA-256:	A459E0C37BA1B49ECAE1A482262704E71E21C8E0BF4877D24BE4C8D2F5D1A011
SHA-512:	A58B915D85C25C82E617E6F8AF83EBE6AE4F963740DA16F6EDA223664E56F47C8FCC2A893BC6B7C5CD57BAF551F3782E6754F62911C833A50AF10976F80968A
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .<..9../....."#.D.;...#.A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo.....sR.....

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):	5.622745630988309
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQb6axbzhcsBXIh1TK6tN:mxRBJQJMbDB0
MD5:	4136DCF3F034E8CAB28831DB1416B00F
SHA1:	9745B5B4A717FBAEB45CB5E6FCCD2F3D06C0FA47
SHA-256:	B65A76E1462D742A6FCBDA968DEE214A7DE00C6CF340BA564B33E20A2A437C51
SHA-512:	3B7CB1DECD53C8E4DB0C7E0F1F3A498619B17B55F97DF5C4558E9731EB21A1902D7D9157BED54BE3BF8A8BC88A9E6F74565676B15A8EA3D7B4D96BC197A317D9
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ....9../....."#.D;....#.A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....g.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	456
Entropy (8bit):	5.622034677317474
Encrypted:	false
SSDEEP:	6:msPYOFLvEWdrROk/RJUQuic3Me/1TK6twEsPYOFLvEWdrROk/RJUQYcMU72c3MeV:3RrROk/sLicyRrROk/sdVg2cx
MD5:	B5CA3288717F6F7128C0C4D828628742
SHA1:	2A63781D445EBE64E45649760C2B12827DA8E38A
SHA-256:	E417BA56E99122C5BE69AAEF8797A5A2130EB101B259AEA41D71A23081C61183
SHA-512:	D57493271B9411F56228648459E7549C5E9468553E4CDCDAA1B921504995293C913BD8CE40FBFC48D281849C3E1D5932EC0080ECD7276949EE819AE52E2F3E33
Malicious:	false
Preview:	0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ..?.9../....."#.DhY ..#.A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....{.B.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .X>.9../....."#.DI..#.A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....7.....

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:	Maple help database
Category:	modified
Size (bytes):	1032
Entropy (8bit):	5.147632869967255
Encrypted:	false
SSDEEP:	12:zzU4u50G8hvktMzpxmyLjFaBsyQLjwp5tP8iAcrq/c2qz:zYehstMNodZZu1cJ2qz
MD5:	A8B970F719F61524708A0A1C9966EB87
SHA1:	44679E755F59C814CE52DD679476D2A960276242
SHA-256:	502DC69FBDF39B75CA8D3DA57744EAD52E7B0466430352605537C00B6FDD5977
SHA-512:	913F99D09DC07997C912330FD56C22EF900B77FC017A625D5930C5C495051E89556D99B74816D6B1E2B948263E824D66DDB5267732EF242695EE3FA81C8A29AE
Malicious:	false
Preview:	.....(woy retne....).....T.....3.....9../.....v...q.....9../.....C..M.....k.....#...(...k.....]...I...9../.....@P.9../.....6<|...@P.9../.....<...W..J@P.9../.....oB*@P.9../.....a....@P.9../.....;.y~A...9../.....P....V...9../.....F..=z;...9../.....o...9../.....*.....9../.....2q.....9../.....Gy.'.h....9../.....k7A....9../.....:..N.A.....9../.....;/....9../.....P[. q...9../.....,+..._.#...9../.....J..j.....9../.....A?.2:.....9../.....q....9../.....u\]..q...9../.....!...0.o...9../.....*.....9../.....o..k.....9../.....^.~..z....9../.....[.i..%....9../.....+.{..'...9../.....@..x....9../.....*)....J:...9../.....&.S.....9../.....MV3.....9../.....+.U.!..V...9../.....D.4....9../.....~.,.4>....9../.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	292
Entropy (8bit):	5.232781822438356
Encrypted:	false
SSDEEP:	6:mRpVRpBwIq2Pwkn2nKuAl9OmbnIFUtp0pVRpTus9ZmwP0pVRpTusPkwOwkn2nKui:2RpyIvYfHAahFUtpmRpTus9/PmRpTuse
MD5:	B7749A589E0488EDF22368F60AA7C955
SHA1:	79AD42906790F45C78F120C823EC667669744719
SHA-256:	72C7891A795F70763BB6AE716A05C1774C40E9A26C1E9C0D14D00A38EA18A018
SHA-512:	5DDA24DE7B0727A334C3A139AA4964FC92156DEB682636092940D5541CB4BC23792744200C7E2691DDD58570EFCB6FD6820596C50BD6B0C05A547ED793F62FF
Malicious:	false
Preview:	2021/05/03-10:42:32.545 1984 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/05/03-10:42:32.546 1984 Recovering log #3.2021/05/03-10:42:32.546 1984 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):	786432
Entropy (8bit):	0.008050090959268128
Encrypted:	false
SSDEEP:	12:I+mmTsx+mmTsxlNTpyxHHyTpyxHHyTpyxHHyTpy:TmbsmbPXytHwytHwytHwy
MD5:	03B3B4BB0F979E273B32ECC52C9B0E01
SHA1:	D307CEFF6AC7E7D3E424C1A855C56168596AEF69
SHA-256:	299FDCED8539A4D45595DBB33856A5A4045215BFECDD3EB7206996390C48C643
SHA-512:	4927E9663FD9AB3DB4449C765F0A55D33DFB51029B3F129E8FD1625C0C5F5593F52E59F180A5A0D1FE49D13C16D84EF3875FAB580375CADB6C5A4CF7439EDA1
Malicious:	false
Preview:	VLnk.....?.....).0k..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210503084218Z-273.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 107 x -152 x 32
Category:	dropped
Size (bytes):	65110
Entropy (8bit):	3.5832880905359747
Encrypted:	false
SSDEEP:	1536:4JBXpwsewWWJTt6U2QsQnqj1rAZGqy6ODnN/0:etkWdt6+Dqj1rrDNs
MD5:	AD95AAA39B9C7C409E2C696F67E68571
SHA1:	53EB4E82808EB0ABEA9FE5A33401BABE2E507070
SHA-256:	E6D8B1FCF4D3D9049D5029D47D4CD3CF99D5DA82B2E37D94954724177CECED17
SHA-512:	3256CE9EF4DF9B004BEFEF28CDCCC00F5792CCBF1285C2355AE3DD75674DB619FCA179BCED462A0BAF4132A4A9420516F377923BB43E7181759A51C48DE629 7
Malicious:	false
Preview:	BMV.....6...(...k...h.... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3024000
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	3.4480587410185652
Encrypted:	false
SSDEEP:	96:k49IVXEBodRBkWCgOOh1CK649IVXEBodRBkWCg7Oh1CKK49IVXEBodRBkWCg7OhW:HedRBDedRByedRBJedRBa
MD5:	99457259B97E32517412483A62F79446
SHA1:	D1B7750C5D4BBED44CE9A4F1268F219BBECE4CEB
SHA-256:	E8DBE02FEF0EDB85E4D84C42A5EA52DB1889758069B53E4B06CA521BAA193429
SHA-512:	58EB9E08DC4583567A4AFC22F11D05E6FF762EF3245FFDC2D4D61787856AD0EA7B7F3D343AF0E3F14A0E08308BD80BFAF304A0CFB2F02BB58E666C9111451BA D
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
Preview:	SQLite format 3.....@ .....$.....1.....T...U.1.D.....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	modified
Size (bytes):	34928
Entropy (8bit):	3.3134681143807945
Encrypted:	false
SSDEEP:	96:YCgOOhZCPGf949IVXEBodRBkbCgOOh1CKbt49IVXEBodRBk1kCg7Oh1CK1d49IVa:CfiedRBeSedRBOCedRBkyedRBV
MD5:	2634950CEEB7864E07354686429346BD
SHA1:	626716ED251EC202824204457B59DAA0CBBE8A6E
SHA-256:	FA2827983AC893963EBFBAFA9E909B96A9AC5397B63FF588FB73054300B2CD3E
SHA-512:	220B56B958F4E4AEA033D8668BE50E5D560B8E2A51FF2A223022F158B422FC74CA6D74D61F721D89BB8F567228F4292999D2DF5E898A2A212C4C1E54AF3D327A
Malicious:	false
Preview:	.....h.....W....X.W .L...y.....~.....

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:PCbGNFYGpiyVFiC0ZceQYIY5Zq+Aojp+dC+3rEmEJL+Yyu:J0GpiyVFihceQ0Y5Zq+9+dR7bK
MD5:	E868918C2DF91E84CF21F54394368CCD
SHA1:	B99197D974797B32C7786D41F71F7F659DB53BF5
SHA-256:	78E14ACAEE0175D67F95A869CF1381C6D9674C0AF3C1A3E33CCF9AA338E07388
SHA-512:	89079804B888D542E6287CE4B451F8594CCEFFCC723DE22DE57335B79694CD4BF7CC02E3840B56A0AF3BABF15F2C37B9C1656A8F7BF6970C788263B3AE240EF
Malicious:	false
Preview:	4.382.88.FID.2:o:.....:F:AgencyFB-Reg.P:Agency FB.L:$....."F:Agency FB.#.94.FID.2:o:.....:F:AgencyFB-Bold.P:Agency FB Bold.L:%....." F:Agency FB.#.82.FID.2:o:.....:F:Algerian.P:Algerian.L:$.....RF:Algerian.#.93.FID.2:o:.....:F:ArialNarrow.P:Arial Narrow.L:$....."F:Arial Narr ow.#.107.FID.2:o:.....:F:ArialNarrow-Italic.P:Arial Narrow Italic.L:$....."F:Arial Narrow.#.103.FID.2:o:.....:F:ArialNarrow-Bold.P:Arial Narrow Bold.L:%..... ....."F:Arial Narrow.#.116.FID.2:o:.....:F:ArialNarrow-BoldItalic.P:Arial Narrow Bold Italic.L:%....."F:Arial Narrow.#.75.FID.2:o:.....:F:ArialMT.P:Arial .L:$....."F:Arial.#.89.FID.2:o:.....:F:Arial-ItalicMT.P:Arial Italic.L:$....."F:Arial.#.85.FID.2:o:.....:F:Arial-BoldMT.P:Arial Bold.L:$..... "F:Arial.#.98.FID.2:o:.....:F:Arial-B

C:\Users\user\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\AppData\Local\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\812A11FD-8CE3-4974-9DD1-7CD9EF661355	
Process:	C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.8827.22055.0_x64__8wekyb3d8bbwe\HxOutlook.exe
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	133362
Entropy (8bit):	5.369188672117383
Encrypted:	false
SSDEEP:	1536:XcQIKNtzBXA3gBwxpQ9DQW+zMh34ZldEKWGq7OhkXtEVRWMi9:JAQ9DQW+zSXCu
MD5:	9C2A08FAE84EAF0FDB89E5004D0778C5
SHA1:	0F4B20641CB040538462F672942F9F8F65FBD7AD
SHA-256:	FF88CB3E4C6A7215459156AA1203E419F0AD1B16A233CA17ECE1D4F5AC0EF611
SHA-512:	201AC2DBC22F48B8782EFF10C9BE79BE009DAE20BCB70654E6A6CC4F98B2C90CDCD4EAAFB329FD960DA54CA6C9A5F46138FEF8A7A8A72002239250EC492CC 2CB
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-05-03T08:43:21">.. Build: 16.0.14028.30527-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\AppData\Roaming\Office\MSO1033.acl	
Process:	C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.8827.22055.0_x64__8wekyb3d8bbwe\HxOutlook.exe

C:\Users\user\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\AppData\Roaming\Office\MSO1033.acl	
File Type:	data
Category:	dropped
Size (bytes):	37730
Entropy (8bit):	3.1247428510363253
Encrypted:	false
SSDEEP:	768:datNbFeZKdogeyHMOeYhlVi+iOFOqbPXdEmanb:4/eLAhlVJb2
MD5:	FF74919EB54CC4E2070CE60DDF91FD67
SHA1:	317A02BC24B9465BFFEB1626C69E6B5FB31A54A4
SHA-256:	6B167F57086C623B6F90AD875C963C570E48DDFAEDD49BD68AA8D678C4E8F673
SHA-512:	C58D4903C5CAF29DEE1DA72C8BBAF7E79413CE2A7F6D4C341C085D9CB51C263E2FE8067570151640FA9C178FB344E076C91A54E8DC739C430160C14952341C4
Malicious:	false
Preview:	......o.b.....R.....(.c.).....(.e.)..... ....(.r.).....(.t.m.)....."!.....& ....a.b.b.o.u.t.....a.b.o.u.t.....a.b.o.t.u.....a.b.o.u.t.....a.b.o.u.t.a.....a.b.o.u.t. .a.....a.b.o.u.t.i.t.....a.b.o.u.t. .i.t.....a.b.o.u.t.t.h.e.....a.b.o.u.t. .t.h.e.....a.b.s.c.e.n.c.e.....a.b.s.e.n.c.e.....a.c.c.e.s.o.r.i.e.s.....a.c.c.e.s.s.o.r.i.e.s.....a.c.c.i.d.a.n.t.....a.c.c.i.d.e.n.t.....a.c.c.o.m.o.d.a.t.e.....a.c.c.o.m.m.o.d.a.t.e.....a.c.c.o.r.d.i.n.g.t.o.....a.c.c.o.r.d.i.n.g. .t.o.....a.c.c.r.o.s.s.....a.c.r.o.s.s.....a.c.h.e.i.v.e.....a.c.h.i.e.v.e.....a.c.h.e.i.v.e.d.....a.c.h.i.e.v.e.d.....a.c.h.e.i.v.i.n.g.....a.c.h.i.e.v.i.n.g.....a.c.n.....c.a.n.....a.c.o.m.m.o.d.a.t.e.....a.c.c.o.m.m.o.d.a.t.e.....a.c.o.m.o.d.a.t.e.....a.c.c.o.m.m.o.d.a.t.e.....a.c.t.u.a.l.y.l.....a.c.t.u.a.l.l.y.....a.d.d.i.t.i.o.n.a.l.....a.d.d.i.t.i.o.n.a.l.....a.d.d.i.t.i.o.n.a.l.....a.d.e.q.u.i.t.....a.d.e.q.u.a.t.e.....a.d.e.q.u.i.t.e.....a.d.e.q.u.a.t.e.....a.d.n.....

C:\Users\user\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\HxmAlwaysOnLog.etl	
Process:	C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.8827.22055.0_x64__8wekyb3d8bbwe\HxOutlook.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.12044674094301783
Encrypted:	false
SSDEEP:	12:8cW6yM2xX/7EDCkpx8C8RKQ1UMCl2M+aqc2EOCScf:8rbYnpxf89SMClCaoEFSc
MD5:	5D2C70FC969426371987BA0E7FBA61C4
SHA1:	D8800B39F9010B8F43F12D57CE0B9562E0054E3C
SHA-256:	1FA6740642BED190AB3DB3D0A36A88EDAB4E6C697B98CB1738E422EADC94B694
SHA-512:	BAB8F3130851518EF5273424D79E1760DC3F9ECF460610F7EA5C9189480BCB41C56C811ABD831E804CE0706A2EB3DF7A04846ABA60C25431475099DB1DDC114
Malicious:	false
Preview:	.....B... ...(....=Q0.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.3.2.2.....@.t.z.r.e.s...d.l.l.,.-.3.2.1.....*..... .....u..].?.....H.x.M.A.l.w.a.y.s.O.n.L.o.g...C.:.\.U.s.e.r.s.\.j.o.n.e.s.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.P.a.c.k.a.g.e.s.\.m.i.c.r.o.s.o.f.t...w.i.n.d.o.w.s.c.o.m.m.u.n.i.c.a.t.i.o.n.s.a.p.p.s._.8.w.e.k.y.b.3.d.8.b.b.w.e.\.L.o.c.a.l.S.t.a.t.e.\.H.x.m.A.l.w.a.y.s.O.n.L.o.g...e.t.l.....P.P.....(...].R0.....

C:\Users\user\AppData\Local\Publishers\8wekyb3d8bbwe\Fonts\FontCache\3\ListAll.Json	
Process:	C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.8827.22055.0_x64__8wekyb3d8bbwe\HxOutlook.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	162274
Entropy (8bit):	4.937140301982904
Encrypted:	false
SSDEEP:	768:G9L4ARW9HTYUc6LnRdrlTZQw8UZwAESkPyJMTjav3V8Pe:x9HTYILnRbZQw8rrPyJMTjav3+Pe
MD5:	303758DB92B921925C82BAAD75D75EE2
SHA1:	3798F3E42978A1330083BFF70782636B00DC09F1
SHA-256:	7F325781C489C95A0B824065954736513E707695B4AA85F672B9170112B3608D
SHA-512:	DF851FF4F05848DC71AD2C39FF3A3A7AD0F2F1BD1A73FEEC461344F7C6CCAA71F7C31F38B36F243ECE9EC6BEEDAC0044F122728C544D105FEF717CA88F6B8E7
Malicious:	false
Preview:	{"MajorVersion":3,"MinorVersion":3,"Expiration":14,"Fonts":[{"a":[4294967167],"f":"Abadi","fam":[],"sf":[{"c":[1,0],"dn":"Abadi","fs":32684,"ful":[{"lcp":983040,"lsc":"Latn","ltx":"Abadi"}],"gn":"Abadi","id":"23599150064","p":[2,11,6,4,2,1,4,2,2,4],"sub":[],"t":"ttf","u":[2147483651,0,0,0],"v":197263,"w":26215680},{"c":[1,0],"dn":"Abadi Extra Light","fs":22172,"ful":[{"lcp":983041,"lsc":"Latn","ltx":"Abadi Extra Light"}],"gn":"Abadi Extra Light","id":"17682098427","p":[2,11,2,4,2,1,4,2,2,4],"sub":[],"t":"ttf","u":[2147483651,0,0,0],"v":197263,"w":13108480}]},{"a":[4294967167],"f":"Agency FB","fam":[],"sf":[{"c":[536870913,0],"dn":"Agency FB Bold","fs":54356,"ful":[{"lcp":983042,"lsc":"Latn","ltx":"Agency FB"}],"gn":"Agency FB","id":"29236703662","p":[2,11,8,4,2,2,2,2,2,4],"sub":[],"t":"ttf","u":[3,0,0,0],"v":67502,"w":45875968},{"c":[536870913,0],"dn":"Agency FB","fs":52668,"ful":[{"lcp":983042,"lsc":"Latn","ltx":"Agency FB"}],"gn":"Agency FB","id":"30332587806","p":[2,11,5,3,2,2,2,2,2

Static File Info

General

File type:	PDF document, version 1.5
Entropy (8bit):	7.985596908149084

General

TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	SECOURS SANITAIRE DU COVID-19.pdf
File size:	217281
MD5:	b01d94c5b33ce94af13c7fbee0138aeb
SHA1:	0a25677fb92664a60185d89a90cfc5cc7e13ffa7
SHA256:	f2a75542290d06da46436424170490e7d0ca564c7bcccaec4c989dacc5d1af05
SHA512:	9d497cc7fcc517b2113f79c667f71ddb5242b2416dd38d86c73c830d9651fec9b71b5f02ee9921217b2a507a69fa909ea5235dc2841a9e4a1bb26baaa6ba57ab
SSDEEP:	6144:6ng5StXd1daQ4DxYNCBHCVZCOC51X3IfPXss:6dbda3YNCBaZnC59IHXss
File Content Preview:	%PDF-1.5..%.....1 0 obj..<</Type/Page/Resources<</Font<</F1 2 0 R/F2 3 0 R/F3 4 0 R>>/ExtGState<</GS7 5 0 R/GS8 6 0 R>>/XObject<</Image9 7 0 R/Image10 8 0 R/Image11 9 0 R>>/ProcSet[/PDF/Text/ImageB/ImageC/ImageI]>>/MediaBox[0 0 595.32001 841.91998]/Conte

File Icon



Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

Header:	%PDF-1.5
Total Entropy:	7.985597
Total Bytes:	217281
Stream Entropy:	7.991285
Stream Bytes:	211389
Entropy outside Streams:	0.000000
Bytes outside Streams:	5892
Number of EOF found:	1
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	29
endobj	29
stream	8
endstream	8
xref	1
trailer	1
startxref	1
/Page	1
/Encrypt	0
/ObjStm	0
/URI	2
/JS	0
/JavaScript	0
/AA	0
/OpenAction	0
/AcroForm	0
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0

Image Streams

ID	DHASH	MD5	Preview

ID	DHASH	MD5	Preview
9	00011507377040c0	26e3b59b145aa49503f870d6143faef5	
8	0c0f474d25652b16	77341fc4c6df2d369cff35b6b6be5167	
7	200076566f4d6100	24b68c33671309aca82512630b267c45	

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 10:41:57.313810110 CEST	53723	53	192.168.2.4	8.8.8.8
May 3, 2021 10:41:57.362721920 CEST	53	53723	8.8.8.8	192.168.2.4
May 3, 2021 10:41:57.419792891 CEST	64646	53	192.168.2.4	8.8.8.8
May 3, 2021 10:41:57.468472004 CEST	53	64646	8.8.8.8	192.168.2.4
May 3, 2021 10:41:58.223249912 CEST	65298	53	192.168.2.4	8.8.8.8
May 3, 2021 10:41:58.272089005 CEST	53	65298	8.8.8.8	192.168.2.4
May 3, 2021 10:41:59.024768114 CEST	59123	53	192.168.2.4	8.8.8.8
May 3, 2021 10:41:59.076373100 CEST	53	59123	8.8.8.8	192.168.2.4
May 3, 2021 10:41:59.874557972 CEST	54531	53	192.168.2.4	8.8.8.8
May 3, 2021 10:41:59.923886061 CEST	53	54531	8.8.8.8	192.168.2.4
May 3, 2021 10:42:00.848258018 CEST	49714	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:00.913098097 CEST	53	49714	8.8.8.8	192.168.2.4
May 3, 2021 10:42:00.967181921 CEST	58028	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:01.016036034 CEST	53	58028	8.8.8.8	192.168.2.4
May 3, 2021 10:42:01.867945910 CEST	53097	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:01.919528008 CEST	53	53097	8.8.8.8	192.168.2.4
May 3, 2021 10:42:02.813402891 CEST	49257	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:02.862169981 CEST	53	49257	8.8.8.8	192.168.2.4
May 3, 2021 10:42:03.630970001 CEST	62389	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:03.679605007 CEST	53	62389	8.8.8.8	192.168.2.4
May 3, 2021 10:42:04.538417101 CEST	49910	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:04.590498924 CEST	53	49910	8.8.8.8	192.168.2.4
May 3, 2021 10:42:05.421736956 CEST	55854	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:05.473467112 CEST	53	55854	8.8.8.8	192.168.2.4
May 3, 2021 10:42:06.852875948 CEST	64549	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:06.902410030 CEST	53	64549	8.8.8.8	192.168.2.4
May 3, 2021 10:42:08.251418114 CEST	63153	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:08.300172091 CEST	53	63153	8.8.8.8	192.168.2.4
May 3, 2021 10:42:09.349334955 CEST	52991	53	192.168.2.4	8.8.8.8

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 10:42:09.401087999 CEST	53	52991	8.8.8.8	192.168.2.4
May 3, 2021 10:42:10.414978981 CEST	53700	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:10.463706970 CEST	53	53700	8.8.8.8	192.168.2.4
May 3, 2021 10:42:11.674681902 CEST	51726	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:11.726258993 CEST	53	51726	8.8.8.8	192.168.2.4
May 3, 2021 10:42:12.544550896 CEST	56794	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:12.593281984 CEST	53	56794	8.8.8.8	192.168.2.4
May 3, 2021 10:42:13.394660950 CEST	56534	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:13.443439007 CEST	53	56534	8.8.8.8	192.168.2.4
May 3, 2021 10:42:14.195210934 CEST	56627	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:14.246786118 CEST	53	56627	8.8.8.8	192.168.2.4
May 3, 2021 10:42:16.855597019 CEST	56621	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:16.904244900 CEST	53	56621	8.8.8.8	192.168.2.4
May 3, 2021 10:42:18.040407896 CEST	63116	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:18.089351892 CEST	53	63116	8.8.8.8	192.168.2.4
May 3, 2021 10:42:24.402148008 CEST	64078	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:24.450733900 CEST	53	64078	8.8.8.8	192.168.2.4
May 3, 2021 10:42:24.590516090 CEST	64801	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:24.648953915 CEST	53	64801	8.8.8.8	192.168.2.4
May 3, 2021 10:42:24.707468033 CEST	61721	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:24.765511036 CEST	53	61721	8.8.8.8	192.168.2.4
May 3, 2021 10:42:25.582075119 CEST	64801	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:25.641370058 CEST	53	64801	8.8.8.8	192.168.2.4
May 3, 2021 10:42:25.644656897 CEST	53157	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:25.675816059 CEST	61721	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:25.693293095 CEST	53	53157	8.8.8.8	192.168.2.4
May 3, 2021 10:42:25.738105059 CEST	53	61721	8.8.8.8	192.168.2.4
May 3, 2021 10:42:26.629251003 CEST	64801	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:26.686347961 CEST	53	64801	8.8.8.8	192.168.2.4
May 3, 2021 10:42:26.722731113 CEST	61721	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:26.773188114 CEST	53	61721	8.8.8.8	192.168.2.4
May 3, 2021 10:42:28.675970078 CEST	64801	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:28.726882935 CEST	53	64801	8.8.8.8	192.168.2.4
May 3, 2021 10:42:28.785445929 CEST	61721	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:28.835685015 CEST	53	61721	8.8.8.8	192.168.2.4
May 3, 2021 10:42:32.725399971 CEST	64801	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:32.790354967 CEST	53	64801	8.8.8.8	192.168.2.4
May 3, 2021 10:42:32.827301979 CEST	61721	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:32.886217117 CEST	53	61721	8.8.8.8	192.168.2.4
May 3, 2021 10:42:35.925671101 CEST	51255	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:35.977493048 CEST	53	51255	8.8.8.8	192.168.2.4
May 3, 2021 10:42:48.260906935 CEST	61522	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:48.322231054 CEST	53	61522	8.8.8.8	192.168.2.4
May 3, 2021 10:42:52.678627968 CEST	52337	53	192.168.2.4	8.8.8.8
May 3, 2021 10:42:52.741221905 CEST	53	52337	8.8.8.8	192.168.2.4
May 3, 2021 10:43:05.763780117 CEST	55046	53	192.168.2.4	8.8.8.8
May 3, 2021 10:43:05.860763073 CEST	53	55046	8.8.8.8	192.168.2.4
May 3, 2021 10:43:06.465569019 CEST	49612	53	192.168.2.4	8.8.8.8
May 3, 2021 10:43:06.523809910 CEST	53	49612	8.8.8.8	192.168.2.4
May 3, 2021 10:43:06.847274065 CEST	49285	53	192.168.2.4	8.8.8.8
May 3, 2021 10:43:06.915390015 CEST	53	49285	8.8.8.8	192.168.2.4
May 3, 2021 10:43:07.136184931 CEST	50601	53	192.168.2.4	8.8.8.8
May 3, 2021 10:43:07.158487082 CEST	60875	53	192.168.2.4	8.8.8.8
May 3, 2021 10:43:07.209224939 CEST	53	50601	8.8.8.8	192.168.2.4
May 3, 2021 10:43:07.369843960 CEST	53	60875	8.8.8.8	192.168.2.4
May 3, 2021 10:43:07.872802973 CEST	56448	53	192.168.2.4	8.8.8.8
May 3, 2021 10:43:08.004717112 CEST	53	56448	8.8.8.8	192.168.2.4
May 3, 2021 10:43:08.644046068 CEST	59172	53	192.168.2.4	8.8.8.8
May 3, 2021 10:43:08.701188087 CEST	53	59172	8.8.8.8	192.168.2.4
May 3, 2021 10:43:09.363115072 CEST	62420	53	192.168.2.4	8.8.8.8
May 3, 2021 10:43:09.420078993 CEST	53	62420	8.8.8.8	192.168.2.4
May 3, 2021 10:43:10.089914083 CEST	60579	53	192.168.2.4	8.8.8.8
May 3, 2021 10:43:10.147353888 CEST	53	60579	8.8.8.8	192.168.2.4
May 3, 2021 10:43:11.070489883 CEST	50183	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 10:43:11.180242062 CEST	53	50183	8.8.8.8	192.168.2.4
May 3, 2021 10:43:12.054069042 CEST	61531	53	192.168.2.4	8.8.8.8
May 3, 2021 10:43:12.111176968 CEST	53	61531	8.8.8.8	192.168.2.4
May 3, 2021 10:43:12.586005926 CEST	49228	53	192.168.2.4	8.8.8.8
May 3, 2021 10:43:12.643305063 CEST	53	49228	8.8.8.8	192.168.2.4
May 3, 2021 10:43:19.399790049 CEST	59794	53	192.168.2.4	8.8.8.8
May 3, 2021 10:43:19.419791937 CEST	55916	53	192.168.2.4	8.8.8.8
May 3, 2021 10:43:19.426412106 CEST	52752	53	192.168.2.4	8.8.8.8
May 3, 2021 10:43:19.448638916 CEST	53	59794	8.8.8.8	192.168.2.4
May 3, 2021 10:43:19.468446970 CEST	53	55916	8.8.8.8	192.168.2.4
May 3, 2021 10:43:19.475003958 CEST	53	52752	8.8.8.8	192.168.2.4
May 3, 2021 10:43:19.888087034 CEST	60542	53	192.168.2.4	8.8.8.8
May 3, 2021 10:43:19.949754000 CEST	53	60542	8.8.8.8	192.168.2.4
May 3, 2021 10:43:20.554986000 CEST	60689	53	192.168.2.4	8.8.8.8
May 3, 2021 10:43:20.606667995 CEST	53	60689	8.8.8.8	192.168.2.4
May 3, 2021 10:43:20.691577911 CEST	64206	53	192.168.2.4	8.8.8.8
May 3, 2021 10:43:20.797465086 CEST	53	64206	8.8.8.8	192.168.2.4
May 3, 2021 10:43:21.263777971 CEST	50904	53	192.168.2.4	8.8.8.8
May 3, 2021 10:43:21.329413891 CEST	53	50904	8.8.8.8	192.168.2.4
May 3, 2021 10:43:21.657416105 CEST	57525	53	192.168.2.4	8.8.8.8
May 3, 2021 10:43:21.722457886 CEST	53	57525	8.8.8.8	192.168.2.4
May 3, 2021 10:43:46.956523895 CEST	53814	53	192.168.2.4	8.8.8.8
May 3, 2021 10:43:47.005249023 CEST	53	53814	8.8.8.8	192.168.2.4
May 3, 2021 10:43:49.778378963 CEST	53418	53	192.168.2.4	8.8.8.8
May 3, 2021 10:43:49.851757050 CEST	53	53418	8.8.8.8	192.168.2.4
May 3, 2021 10:44:06.207426071 CEST	62833	53	192.168.2.4	8.8.8.8
May 3, 2021 10:44:06.265898943 CEST	53	62833	8.8.8.8	192.168.2.4

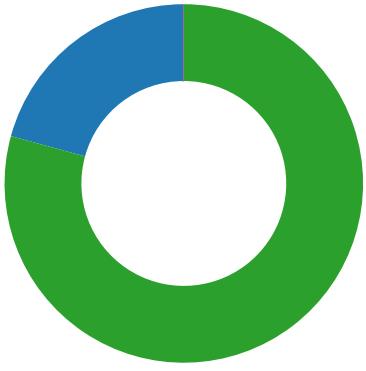
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 3, 2021 10:42:25.693293095 CEST	8.8.8.8	192.168.2.4	0x52b2	No error (0)	a-0019.a.dns.afd.azure.com	a-0019.standard.a-msedge.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: AcroRd32.exe PID: 7040 Parent PID: 5884

General

Start time:	10:42:06
Start date:	03/05/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\SECOURS SANITAIRE DU COVID-19.pdf'
Imagebase:	0x350000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx	read data or list directory | read attributes | write attributes | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3865C3	CreateDirectoryExW
C:\Users\user\AppData\Local\Temp\acrocef_low	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3AAE05	CreateDirectoryW
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	success or wait	1	39EA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210503084218Z-273.bmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	39EA85	NtCreateFile
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4183C8	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4183C8	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4183C8	HttpSendRequestA

Copyright Joe Security LLC 2021

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4183C8	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4183C8	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4183C8	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R14pat99_q1v9cu_5iw.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	39EA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	4	39EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R3wusug_q1v9cv_5iw.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	39EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rl91tqg_q1v9cw_5iw.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	39EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Re7gquq_q1v9cx_5iw.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	39EA85	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1nf02lm_q1v9cy_5iw.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	39EA85	NtCreateFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\System\Acrobatbrokerserverdispatchercpp789	success or wait	1	39CF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	39D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	39D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo	success or wait	1	39D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\NoTimeOut	success or wait	1	39D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	35EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	35EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	35EA55	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	aFS	unicode	DOS	success or wait	1	3ADF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/Users/user/Desktop/SECOURS SANITAIRE DU COVID-19.pdf	success or wait	1	3ADF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	SECOURS SANITAIRE DU COVID-19.pdf	success or wait	1	3ADF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	3ADF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	3ADF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDI	binary	2F 43 2F 55 73 65 72 73 2F 6A 6F 6E 65 73 2F 44 65 73 6B 74 6F 70 2F 53 45 43 4F 55 52 53 20 53 41 4E 49 54 41 49 52 45 20 44 55 20 43 4F 56 49 44 2D 31 39 2E 70 64 66 00	success or wait	1	3ADF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDate	binary	44 3A 32 30 32 31 30 35 30 33 31 30 34 32 31 37 2B 30 32 27 30 30 27 00	success or wait	1	3ADF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	217281	success or wait	1	3ADF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	1	success or wait	1	3ADF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	3ADF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tDIText	unicode	http://www.adobe.com/go/homeacrordrunified18_2018	success or wait	1	3ADF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	3ADF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	3ADF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sDI	binary	68 74 74 70 3A 2F 2F 77 77 77 2E 61 64 6F 62 65 2E 63 6F 6D 2F 67 6F 2F 68 6F 6D 65 61 63 72 6F 72 64 72 75 6E 69 66 69 65 64 31 38 5F 32 30 31 38 00	success or wait	1	3ADF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sDate	binary	44 3A 32 30 31 39 30 36 32 37 31 31 31 33 35 31 2D 30 37 27 30 30 27 00	success or wait	1	3ADF69	RegSetValueExW

Analysis Process: AcroRd32.exe PID: 7160 Parent PID: 7040

General

Start time:	10:42:08
Start date:	03/05/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\SECOURS SANITAIRE DU COVID-19.pdf'
Imagebase:	0x350000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	false
Has administrator privileges:	false
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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: RdrCEF.exe PID: 6580 Parent PID: 7040

General

Start time:	10:42:16
Start date:	03/05/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043
Imagebase:	0xd90000
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
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	success or wait	3	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	3	E859E2	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	3	E983E5	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	43	E98447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	110	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	2	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	4	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	2	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	11	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	2	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	4	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	2	E859E2	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	8	E859E2	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	2	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	1090	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	2	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	30	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	2	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	6	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	2	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	4	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	2	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	2	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	2	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	2	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	2	E859E2	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	2	E859E2	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	2	E859E2	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	2	E859E2	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	end of file	2	E859E2	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	E859E2	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	2	E859E2	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	4	E859E2	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	2	E859E2	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	1	E859E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	end of file	1	E859E2	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	2	E859E2	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	2	E859E2	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	E859E2	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	2	E859E2	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	2	E859E2	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	2	E859E2	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	12	E859E2	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	2	E859E2	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	12	E859E2	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	E859E2	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	28	E859E2	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	2	E859E2	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	30	E859E2	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	2	E859E2	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	44	E859E2	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	1	E859E2	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	1	E859E2	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	1	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	28	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	2	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	30	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	2	E859E2	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	E859E2	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	2	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	10	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	2	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	10	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	2	E859E2	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	10	E859E2	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	2	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	119	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	2	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	141	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	2	E859E2	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	133	E859E2	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	E859E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	24	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	end of file	1	E859E2	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	97	E859E2	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	1	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	16	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	2	E859E2	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	1	E859E2	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	1	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	3	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	1	E859E2	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	1	E859E2	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	1	E859E2	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	1	E859E2	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	1	E859E2	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	1	E859E2	ReadFile
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	1	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	1	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	1	E859E2	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	3	E859E2	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	E859E2	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	1	E859E2	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	1	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	2	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	1	E859E2	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	1	E859E2	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	1	E859E2	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	1	E859E2	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	1	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	4	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	1	E859E2	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	85	E859E2	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	1	E859E2	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	4	E859E2	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	1	E859E2	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	1	E859E2	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	1	E859E2	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	E859E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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	1	E859E2	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	1	E859E2	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	1	E859E2	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	1	E859E2	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	1	E859E2	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	1	E859E2	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	1	E859E2	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	8	E859E2	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	1	E859E2	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	1	E859E2	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	1	E859E2	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	162	E859E2	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	1	E859E2	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	1	E859E2	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	1	E859E2	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	1	E859E2	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	1	E859E2	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	1	E859E2	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	1	E859E2	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	1	E859E2	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	1	E859E2	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	1	E859E2	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	1	E859E2	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	2	E859E2	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	1	E859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	success or wait	75	E859E2	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	1	E859E2	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	6	E859E2	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	1	E859E2	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	1	E859E2	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	1	E859E2	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	16	E859E2	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	1	E859E2	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	5	E859E2	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	1	E859E2	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	E859E2	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	1	E859E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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	2	E859E2	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	1	E859E2	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	E983E5	ReadFile

Analysis Process: RdrCEF.exe PID: 6960 Parent PID: 6580

General

Start time:	10:42:20
Start date:	03/05/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1736,10090636952361594307,9260773660448689587,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=12482158104385577703 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=12482158104385577703 --renderer-client-id=2 --mojo-platform-channel-handle=1740 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xd90000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 6656 Parent PID: 6580

General

Start time:	10:42:25
Start date:	03/05/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1736,10090636952361594307,9260773660448689587,131072 --disable-features=VizDisplayCompositor --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --lang=en-US --gpu-preferences=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=8616662721456202722 --mojo-platform-channel-handle=1764 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0xd90000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 4420 Parent PID: 6580

General

Start time:	10:42:28
Start date:	03/05/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1736,100906369523615 94307,9260773660448689587,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=13245651749807582994 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=13245651749807582994 --renderer-client-id=4 --mojo-platform-channel-handle=1860 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xd90000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 3436 Parent PID: 6580

General

Start time:	10:42:30
Start date:	03/05/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1736,100906369523615 94307,9260773660448689587,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=14006470410429743815 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=14006470410429743815 --renderer-client-id=5 --mojo-platform-channel-handle=2024 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xd90000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: HxOutlook.exe PID: 808 Parent PID: 800

General

Start time:	10:43:05
Start date:	03/05/2021
Path:	C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.8827.22055.0_x64__8wekyb3d8bbwe\HxOutlook.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.8827.22055.0_x64__8wekyb3d8bbwe\HxOutlook.exe' -ServerName:microsoft.windowslive.mail.AppXfbjsbkxvprcgqg6q4c9jfr0pn3kv9x5s.mca
Imagebase:	0x7ff671ea0000
File size:	2171568 bytes
MD5 hash:	3F320EB023572D41D0F997F58A5B26CA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	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 Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis

Copyright Joe Security LLC 2021