ID: 357038
Cookbook: browseurl.jbs
Time: 02:30:25
Date: 24/02/2021
Version: 31.0.0 Emerald

Table of Contents

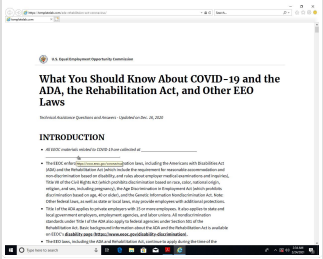
Analysis Report https://templatelab.com/ada-rehabilitaio…

Overview

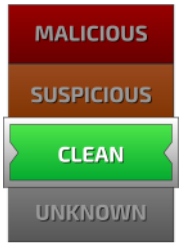
General Information

Sample URL:	http://https://templatelab.com/ada-rehabilitaion-act-coronavirus/
Analysis ID:	357038
Infos:	

Most interesting Screenshot:



Detection

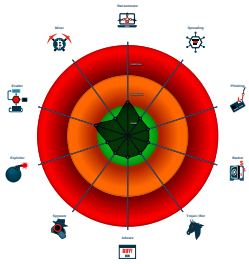


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

Contains functionality to access load…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 4600 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 2024 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4600 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - AcroRd32.exe (PID: 4792 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' /o /eo /l /b /ac /id 2024 MD5: B969CF0C7B2C443A99034881E8C8740A)
      - AcroRd32.exe (PID: 3636 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 /o /eo /l /b /ac /id 2024 MD5: B969CF0C7B2C443A99034881E8C8740A)
      - RdrCEF.exe (PID: 4816 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
        - RdrCEF.exe (PID: 6164 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1700,14431000459877472766,9177081831552403983,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAO AAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=9047234563143899772 --mojo-platform-channel-handle=1732 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
        - RdrCEF.exe (PID: 6568 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=1700,14431000459877472766,9177081831552403983,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=13126402487251577759 --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=13126402487251577759 --renderer-client-id=2 --mojo-platform-channel-handle=1752 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
        - RdrCEF.exe (PID: 6668 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=1700,14431000459877472766,9177081831552403983,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=13365710013370324663 --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=13365710013370324663 --renderer-client-id=4 --mojo-platform-channel-handle=1944 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
        - RdrCEF.exe (PID: 7100 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=1700,14431000459877472766,9177081831552403983,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=15977986577334180066 --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=15977986577334180066 --renderer-client-id=5 --mojo-platform-channel-handle=2164 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
- **cleanup**

Malware Configuration

No configs have been found

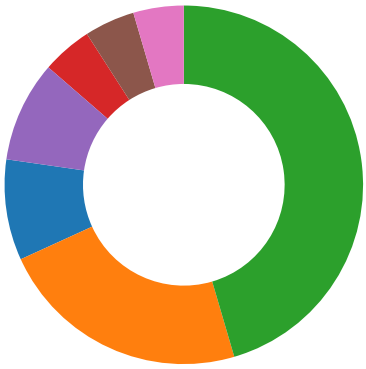
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

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

Compliance:

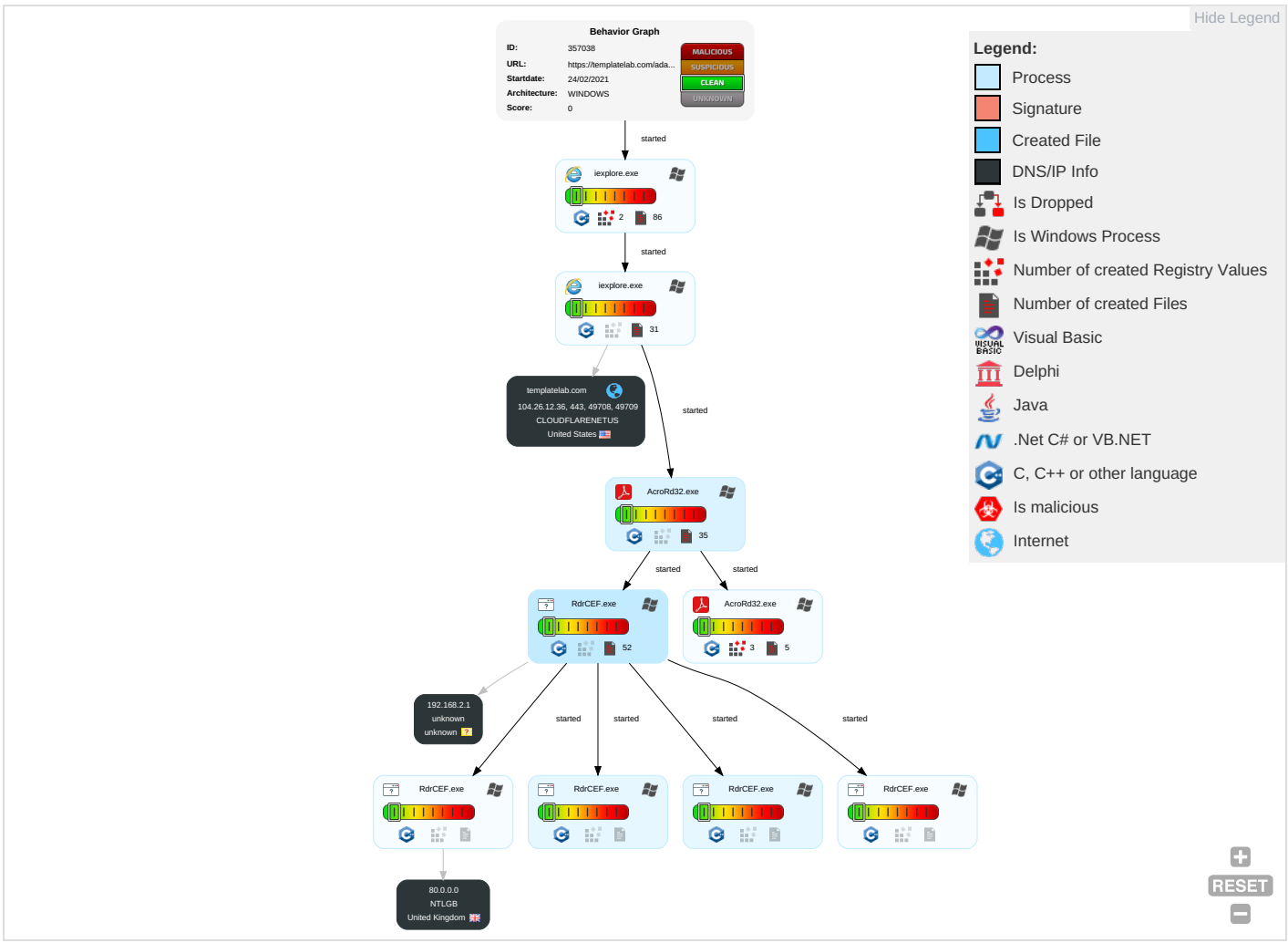
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

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	I
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	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	I S I
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	I I
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	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	I I I

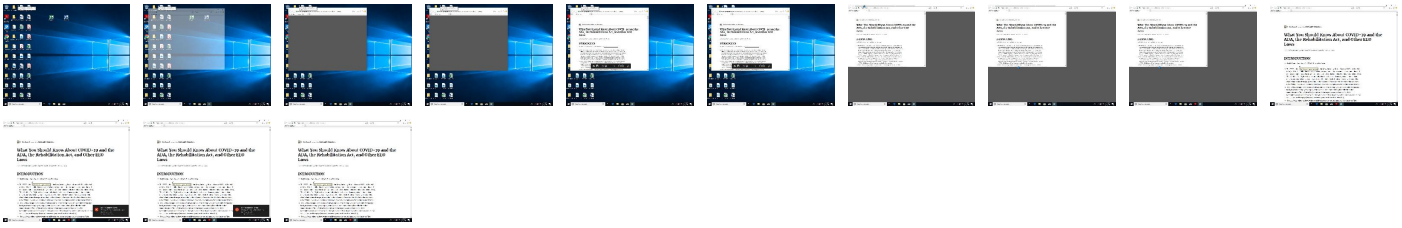
Behavior Graph

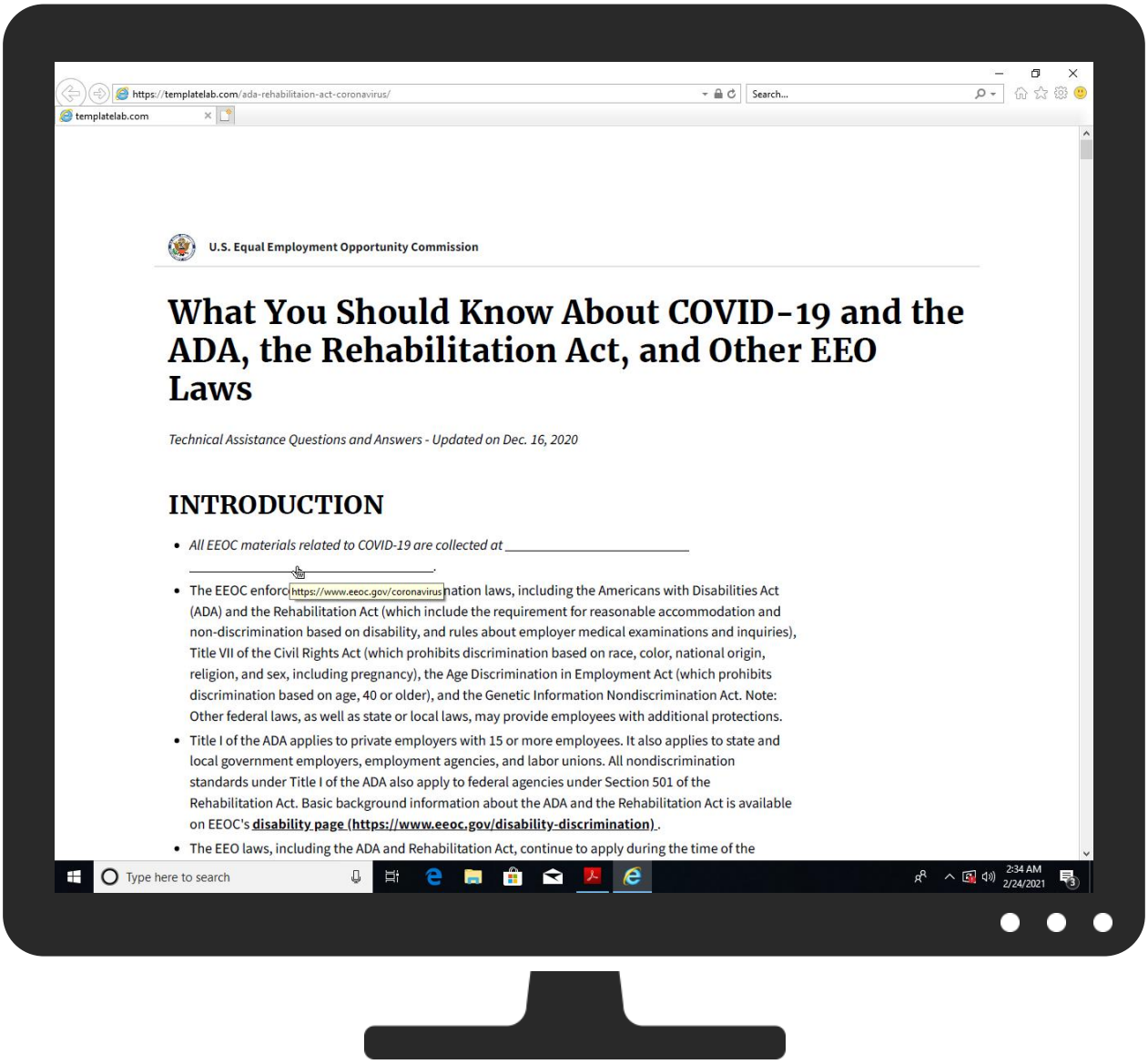


Screenshots

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
http://https://templatelab.com/ada-rehabilitaion-act-coronavirus/	0%	Virustotal		Browse
http://https://templatelab.com/ada-rehabilitaion-act-coronavirus/	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.askjan.org/	0%	Virustotal		Browse
http://www.askjan.org/	0%	Avira URL Cloud	safe	
http://w.a	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://askjan.org/topics/COVID-19.cfm	0%	Virustotal		Browse
http://https://askjan.org/topics/COVID-19.cfm	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	0%	Avira URL Cloud	safe	
http://www.askjan.org/xm	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/9l	0%	Avira URL Cloud	safe	
http://https://askjan.org/topics/COVID-19.cfm)	0%	Avira URL Cloud	safe	
http://www.askjan.org/)	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/)m	0%	Avira URL Cloud	safe	
http://https://askjan.org/topics/COVID-19.cfm2.	0%	Avira URL Cloud	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
templatelab.com	104.26.12.36	true	false		high

URLs from Memory and Binaries

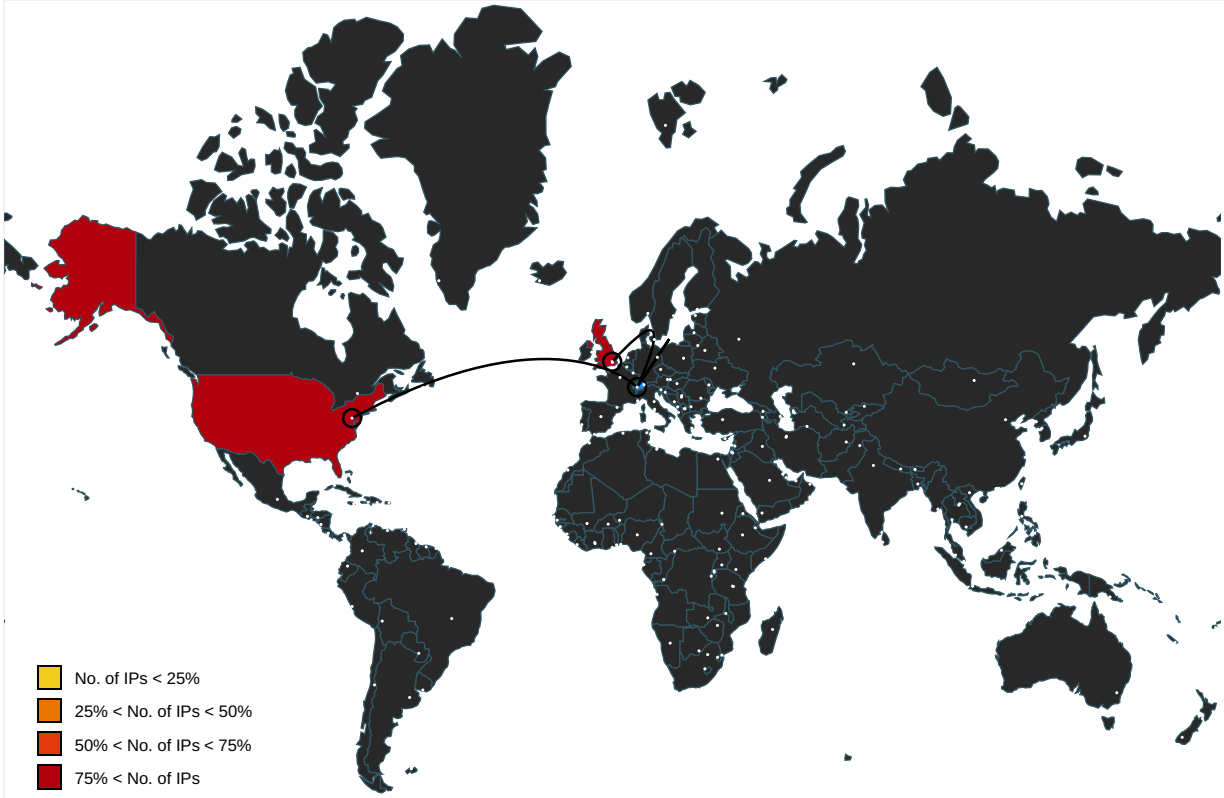
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.cdc.gov/coronavirus/2019-ncov/vaccines/different-vaccines/mrna.html)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.eeoc.gov/transcript-march-27-2020-outreach-webinar#q1~=5	AcroRd32.exe, 00000006.00000003.278360966.000000000BB75000.00000004.00000001.sdmp	false		high
http://https://www.eeoc.gov/disability-discrimination)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.eeoc.gov/transcript-march-27-2020-outreach-webinar#q17)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://templatelab.com/ada-rehabilitaion-act-coronavirus/Root	{679099D5-768B-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://www.eeoc.gov/transcript-march-27-2020-outreach-webinar#q1)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.osha.gov/SLTC/covid-19/	AcroRd32.exe, 00000006.00000003.267703684.000000000BBC4000.00000004.00000001.sdmp	false		high
http://https://www.cdc.gov/coronavirus/2019-ncov/community/organizations/testing-non-healthcare-workplaces.	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.eeoc.gov/laws/guidance/legal-rights-pregnant-workers-under-federal-law	AcroRd32.exe, 00000006.00000003.279519878.000000000B549000.00000004.00000001.sdmp	false		high
http://https://www.eeoc.gov/transcript-march-27-2020-outreach-webinar#q1	AcroRd32.exe, 00000006.00000003.278360966.000000000BB75000.00000004.00000001.sdmp	false		high
http://https://www.eeoc.gov/laws/guidance/qa-understanding-waivers-discrimination-claims-employee-severance	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://www.askjan.org/	AcroRd32.exe, 00000006.00000003.279519878.000000000B549000.00000004.00000001.sdmp, AcroRd32.exe, 00000006.00000003.267703684.000000000BBC4000.00000004.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.cdc.gov/coronavirus/2019-ncov/need-extra-precautions/people-at-higher-risk.html)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.eeoc.gov/transcript-march-27-2020-outreach-webinar#q9)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.eeoc.gov/select-task-force-study-harassment-workplace#_Toc453686319)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.cdc.gov/coronavirus/2019-ncov/need-extra-precautions/pregnancy-breastfeeding.html	AcroRd32.exe, 00000006.00000003.279519878.000000000B549000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.eeoc.gov/transcript-march-27-2020-outreach-webinar#q9	AcroRd32.exe, 00000006.00000003.278360966.000000000BB75000.00000004.00000001.sdmp	false		high
http://www.amazon.com/	msapplication.xml.1.dr	false		high
http://https://www.cdc.gov/coronavirus/2019-ncov/lab/resources/antibody-tests-guidelines.html	AcroRd32.exe, 00000006.00000003.279519878.000000000B549000.00000004.00000001.sdmp	false		high
http://https://www.cdc.gov/coronavirus/2019-ncov/symptoms-testing/symptoms.html)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.eeoc.gov/laws/guidance/enforcement-guidance-reasonable-accommodation-and-undue-hardship-	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://w.a	AcroRd32.exe, 00000006.00000003.239652748.000000000BF43000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.twitter.com/	msapplication.xml5.1.dr	false		high
http://https://www.cdc.gov/coronavirus/2019-ncov/vaccines/different-vaccines/mrna.html	AcroRd32.exe, 00000006.00000003.278360966.000000000BB75000.00000004.00000001.sdmp	false		high
http://https://www.eeoc.gov/laws/guidance/pandemic-preparedness-workplace-and-americans-disabilities-act#q7	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.eeoc.gov/wysk/message-eeoc-chair-janet-dhillon-national-origin-and-race-discrimination-d	AcroRd32.exe, 00000006.00000003.236561521.0000000009B28000.00000004.00000001.sdmp, ._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.eeoc.gov/laws/guidance/enforcement-guidance-disability-related-inquiries-and-medical-exa	AcroRd32.exe, 00000006.00000003.236561521.0000000009B28000.00000004.00000001.sdmp, ._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.cdc.gov/coronavirus/2019-ncov/community/index.html)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.cdc.gov/coronavirus/2019-ncov/community/contact-tracing-nonhealthcare-workplaces.html)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.eeoc.gov/laws/guidance/enforcement-guidance-unlawful-disparate-treatment-workers-caregiv	AcroRd32.exe, 00000006.00000003.236561521.0000000009B28000.00000004.00000001.sdmp, ._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.eeoc.gov/transcript-march-27-2020-outreach-webinar#q20)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.govinfo.gov/content/pkg/USCODE-2018-title42/html/USCODE-2018-title42-chap126-subchapI-se	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.cdc.gov/coronavirus/2019-ncov/need-extra-precautions/people-at-higher-risk.html	AcroRd32.exe, 00000006.00000003.279519878.000000000B549000.00000004.00000001.sdmp	false		high
http://https://askjan.org/topics/COVID-19.cfm	AcroRd32.exe, 00000006.00000003.267703684.000000000BBC4000.00000004.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.eeoc.gov/laws/guidance/pandemic-preparedness-workplace-and-americans-disabilities-act)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.eeoc.gov/laws/guidance/questions-and-answers-religious-discrimination-workplace)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	AcroRd32.exe, 00000006.00000003.274224374.000000000B9CD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://templatelab.com/ada-rehabilitaion-act-coronavirus/	AcroRd32.exe, 00000006.00000002.1650541564.0000000005360000.00000002.00000001.sdmp, ~DF607C8DFA7F9E2A87.TMP.1.dr	false		high
http://https://www.cdc.gov/coronavirus/2019-ncov/downloads/Essential-Critical-Workers_Dos-and-Donts.pdf)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.cdc.gov/coronavirus/2019-ncov/community/general-business-faq.html)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.cdc.gov/coronavirus/2019-ncov/need-extra-precautions/pregnancy-breastfeeding.html&	AcroRd32.exe, 00000006.00000003.279519878.000000000B549000.00000004.00000001.sdmp	false		high
http://https://www.cdc.gov/coronavirus/2019-ncov/need-extra-precautions/pregnancy-breastfeeding.html)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://https://www.govinfo.gov/content/pkg/CFR-2011-title29-vol4/xml/CFR-2011-title29-vol4-sec1630-10.xml)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.cdc.gov/coronavirus/2019-ncov/lab/resources/antibody-tests-guidelines.html#	AcroRd32.exe, 00000006.00000003.279519878.000000000B549000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.eeoc.gov/laws/guidance/legal-rights-pregnant-workers-under-federal-law)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.fda.gov/medical-devices/emergency-situations-medical-devices/faqs-diagnostic-testing-sar	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://https://www.cdc.gov/coronavirus/2019-ncov/lab/resources/antibody-tests-guidelines.html)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.cdc.gov/coronavirus/2019-ncov/community/critical-workers/implementing-safety-practices.h	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.cdc.gov/coronavirus/2019-ncov/community/organizations/businesses-employers.html)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.ecfr.gov/cgi-bin/text-idx?SID=28cadc4b7b37847fd37f41f8574b5921&mc=true&node=pt29.4.1630&	AcroRd32.exe, 00000006.00000003.236561521.0000000009B28000.00000004.00000001.sdmp, ._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.eeoc.gov/transcript-march-27-2020-outreach-webinar#q18=	AcroRd32.exe, 00000006.00000003.278360966.000000000BB75000.00000004.00000001.sdmp	false		high
http://https://www.govinfo.gov/content/pkg/CFR-2019-title29-vol4/xml/CFR-2019-title29-vol4-sec1630-14.xml)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.eeoc.gov/laws/guidance/questions-and-answers-religious-discrimination-workplaceJ	AcroRd32.exe, 00000006.00000003.279519878.000000000B549000.00000004.00000001.sdmp	false		high
http://https://www.eeoc.gov/employers/small-business/harassment-policy-tips)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://www.askjan.org/xm	AcroRd32.exe, 00000006.00000003.279519878.000000000B549000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/9l	AcroRd32.exe, 00000006.00000003.274224374.000000000B9CD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.eeoc.gov/laws/guidance/questions-and-answers-religious-discrimination-workplace_	AcroRd32.exe, 00000006.00000003.279519878.000000000B549000.00000004.00000001.sdmp	false		high
http://https://askjan.org/topics/COVID-19.cfm)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.askjan.org/)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.eeoc.gov/transcript-march-27-2020-outreach-webinar#q20	AcroRd32.exe, 00000006.00000003.278360966.000000000BB75000.00000004.00000001.sdmp	false		high
http://https://www.cdc.gov/coronavirus/2019-ncov/lab/resources/antibody-tests-guidelines.html/	AcroRd32.exe, 00000006.00000003.279519878.000000000B549000.00000004.00000001.sdmp	false		high
http://https://www.cdc.gov/coronavirus/2019-ncov/symptoms-testing/symptoms.html	AcroRd32.exe, 00000006.00000003.278360966.000000000BB75000.00000004.00000001.sdmp	false		high
http://https://www.eeoc.gov/coronavirus	AcroRd32.exe, 00000006.00000003.274224374.000000000B9CD000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/)m	AcroRd32.exe, 00000006.00000003.274224374.000000000B9CD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.eeoc.gov/laws/guidance/pandemic-preparedness-workplace-and-americans-disabilities-act#q1	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.eeoc.gov/laws/guidance/questions-and-answers-religious-discrimination-workplace	AcroRd32.exe, 00000006.00000003.279519878.000000000B549000.00000004.00000001.sdmp	false		high
http://https://www.eeoc.gov/transcript-march-27-2020-outreach-webinar#q9L	AcroRd32.exe, 00000006.00000003.278360966.000000000BB75000.00000004.00000001.sdmp	false		high
http://https://www.eeoc.gov/laws/guidance/pandemic-preparedness-workplace-and-americans-disabilities-act#q6	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://askjan.org/topics/COVID-19.cfm2.	AcroRd32.exe, 00000006.00000003.267703684.000000000BBC4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.eeoc.gov/laws/guidance/pandemic-preparedness-workplace-and-americans-disabilities-act#q5	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.eeoc.gov/sites/default/files/2020-04/pandemic_flu.pdf)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.osha.gov/SLTC/covid-19/)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://www.youtube.com/	msapplication.xml7.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.eeoc.gov/transcript-march-27-2020-outreach-webinar#q17	AcroRd32.exe, 00000006.00000003.278360966.000000000BB75000.00000004.00000001.sdmp	false		high
http://www.wikipedia.com/	msapplication.xml6.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.live.com/	msapplication.xml2.1.dr	false		high
http://https://www.cdc.gov/coronavirus/2019-ncov/community/high-risk-workers.html?deliveryName=USCDC_2067-D	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.eeoc.gov/laws/guidance/pandemic-preparedness-workplace-and-americans-disabilities-act#se	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://www.quicktime.com.Acrobat	AcroRd32.exe, 00000006.00000002.1651921116.00000000074B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.eeoc.gov/chart-risk-factors-harassment-and-responsive-strategies)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.govinfo.gov/content/pkg/CFR-2012-title29-vol4/xml/CFR-2012-title29-vol4-sec1630-2.xml)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.eeoc.gov/coronavirus)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high
http://https://www.eeoc.gov/)	._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.26.12.36	unknown	United States		13335	CLOUDFLARENETUS	false
80.0.0.0	unknown	United Kingdom		5089	NTLGB	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	357038
Start date:	24.02.2021
Start time:	02:30:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://templatelab.com/ada-rehabilitaion-act-coronavirus/
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@17/61@1/3
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Max analysis timeout: 720s exceeded, the analysis took too long • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 168.61.161.212, 92.122.145.220, 13.88.21.125, 13.64.90.137, 88.221.62.148, 52.147.198.201, 104.43.193.48, 152.199.19.161, 23.218.208.56, 92.122.146.26, 23.32.238.129, 23.32.238.123, 8.248.117.254, 8.253.95.120, 67.27.158.126, 8.248.119.254, 67.27.158.254, 51.104.144.132, 20.54.26.129, 92.122.213.194, 92.122.213.247, 52.155.217.156, 40.126.31.141, 20.190.159.134, 40.126.31.1, 40.126.31.137, 40.126.31.8, 20.190.159.138, 40.126.31.143, 40.126.31.6, 51.104.136.2, 51.11.168.232, 93.184.221.240, 51.11.168.160 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, acroipm2.adobe.com, www.tm.a.prd.aadg.trafficmanager.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, login.live.com, a122.dscd.akamai.net, audownload.windowsupdate.nsatc.net, hlb.apr-52dd2-0.edgecastdns.net, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, fs.microsoft.com, acroipm2.adobe.com.edgesuite.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus15.cloudapp.net, settingsfd-geo.trafficmanager.net, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, dub2.next.a.prd.aadg.trafficmanager.net, cs9.wpc.v0cdn.net, e4578.dscb.akamaiedge.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, go.microsoft.com, cs11.wpc.v0cdn.net, displaycatalog.mp.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, ie9comview.vo.msecnd.net, wu.ec.azureedge.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, login.msa.msidentity.com, skypedataprdcoleus16.cloudapp.net, armmf.adobe.com, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
02:31:38	API Interceptor	113x Sleep call for process: RdrCEF.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\05349744be1ad4ad_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	410
Entropy (8bit):	5.663411708004242
Encrypted:	false
SSDEEP:	6:men9YOFLvEWdM9QhSl0dHi7Z+P41TK6tMeen9YOFLvEWdM9QJci7Z+P41TK6tf:vDRM9rZiEkDRM90ZiE1
MD5:	509385F4F5457239C01B8A1111237C5C
SHA1:	92C1AD14573169F99B9F94AA116457E3605C5830
SHA-256:	C77938702DEFFDC5626D3C4A10F077D99AD87F86F34DCED4392ADC46AF002F91
SHA-512:	9A063D3E693DD67276E1C64FDA273D254F8C82A21383D3364E571BFED290F890CB1A7AFF8BED7FCF5A2E2F830B6726CD13CB919EC8ADEF90F27BD29FB22C1F CC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ..J.../....."#.D".....A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....^. 1.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ..WV../....."#.D`W5...A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A.. Eo.....z.....

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):	522
Entropy (8bit):	5.625255785235324
Encrypted:	false
SSDEEP:	6:mi9NqEYOFLvEkNm/NUV8Be7Ywcr1TK6trHlEi9NqEYOFLvEkuoV8Be7Ywcr1TK6S:V9zIqV9PQ39z79PQ19zHLRl9PQ
MD5:	09E0FF499FC5506897B2D43FD1682779
SHA1:	F48283A4FD70F5C4A5B0096067C332ECDBF2905F
SHA-256:	E3CFC58E5A5D6AB2952C268FC79A45FF0B420D1439CCF22396BDF8AD21477D59
SHA-512:	2113BF1091CE82E4786180535A3A9621C64A39DFD309018F18FAC0441EE84A2F43E0C25087923712C9C3B29B0D4767196ACE711C41C7B1512ACA77FEE1422699
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0	
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .k..../....."#.D.....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .48.../....."#.DY.....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ..C7../....."#.D.....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):	5.6132261382509805
Encrypted:	false
SSDEEP:	12:DyeRVFAFjVFAFYvmlUo6j9yeRVFAFjVFAF9slUo6ji:tB4v4OmSBTB4v4WSB
MD5:	AC31CEE6E86350530B72C6F9BF30294F
SHA1:	BEB4BAAE3A001D254A38122239E3606E3D2D159C
SHA-256:	561B08C4C4B6F3EA4EC56008E8E3A48737B11734566FDFAE8ADF6BCF05887A64
SHA-512:	1F4B7990539775106ABA174DF6287E099C79B14F78483D2E3EC90BC0C49CA3D9EAFE46EF0B06C6327BBD79F4B2ECDC04E1B6758D34A264C4885ECA6532A4C6C
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 ...../....."#.D8.....A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ..LT../....."#.D,.....A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....3.....

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):	5.657499221489002
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RsFOtgjAwciWulHyA1TK6t9:IbRkiDc84Wuss7
MD5:	3856CDAFDBCFF40AA81EB361B57A5C5C
SHA1:	960468F9EF26E7899A8BD8E22D0F0CF697344D9F
SHA-256:	08D8A1B82F7D79F0771297BA86153420FDD59389BB53EAD4FEE7C03FA33B4BDD
SHA-512:	3F01A123B3A20929D78D6BE2E45309C5D333853A1B3A6E459357C16D8FB5D37FD3E0C3812F3BB429B43FA703D819097E39247788243C527BDD674106CDDDA067
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 ...../....."#.Db.....A..8 P..a...R..Y....7.@..2Dm{..A..Eo.....A..Eo.....q.....

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+yiXYOFLvEWd7VIGXVu9mURVyh9PT41TK6t:pyixRuXmUV41TE
MD5:	874DA5FD3B5518202DFDDE876BAF4164
SHA1:	5D428D01B129DAC01E5585928B6402C61A05EBB5
SHA-256:	4F996A62F1D67E24595A1DEAD3A7D3B8A6E3BD92E58062A5FE5CF8B4A40B4E3C
SHA-512:	0C3C655BCB88FC9B68BFE83AD4C862A6170E6F7D4C667BC5A9ED3EB101A26C26EADCA46820DD6CF0F70BA6878F98C57082E36FC0F230B656FEBD5188F687938
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ...U../....."#.Dx.....Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo.....q.....

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):	5.611732583154631

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
Encrypted:	false
SSDEEP:	6:mvYOFLvEWdhwjQOxth7USLZIl6P41TK6tI:0RhkTxth7USLZC2
MD5:	A859E721CB9B1F8AFF2D625D8B588327
SHA1:	B64A15963DDC95C75DD422D88A429E03742F754E
SHA-256:	3C13D9DA8AE1A9262C3E36E493AE057FA9A1EEBB7FEE8599E64E99FE409AF7C6
SHA-512:	149DAF686F88F1F8F3D57DE8AF6171175A7EE2306A3BA7550421141746596D5924A572052DF4350FD230A136E5628519910CA5E992AC9348735188C107280EE9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ..9Q../....."#.D.t....A.].>....uUf..N...k.....c..I.A..Eo.....A..Eo.....}.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	209
Entropy (8bit):	5.500010499364551
Encrypted:	false
SSDEEP:	3:m+lZd8RzYOCGLvHkWBGKuKjXKX7KoQRA/KVdKLuVg/XslVcyxMtv9EWm1TK5ktc3:mJYOFLvEWdGQRQOdQYV6g1TK6t
MD5:	1FD634BC243C508A19EFC69CFCA05CCF
SHA1:	240E4F1CC7E756AC325F60E82807C4404CB181E3
SHA-256:	F63157D2AADDA8F0EAFF1F0BDD5E43853B3DC02023301EE301B07AA23122683B
SHA-512:	DA2DC16CA0B5F17EBF9B55614984F93AA3D2A5CA14FA54CCE0BB1ABA17063A41266BB588728EA774230E293BAEBFFB0E7BDA5D88549296D2BDCADC4A20517BB4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .$&V../....."#.D$./...A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo.....|-.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	537
Entropy (8bit):	5.641419835639063
Encrypted:	false
SSDEEP:	6:mOYOFLvECMLDB1W5MuR/41TK6t4OYOFLvECML/eh/5MuR/41TK6tneOYOFLvECMt:Z5MqMuR/E15MEMuR/EpB5MjRUMuR/E
MD5:	2E659C457623F71D0EF144CB3F6A14F3
SHA1:	13D08516B442E5217FC27802DB092F6B590CA06D
SHA-256:	1DEF800DBBB59CEAD0D16F4A2CD77017A98FC56BE88566766A1A49A0A8A3485F
SHA-512:	10153CF1D64FAD3E9BF77E64214D4875078B3D1EE79ED9E0D82C79F323CEB118F78D4FCE491D872A7480D7ED27E06A0E18BD908AE19933B969E252FCD3A4A6A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .h..../....."#.D.....A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....F.....0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ..M.../....."#.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 ..H7../....."#.D.....A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....m.....

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):	5.529216955468705
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtu+q+8/by0zBUKSAA1TK6tS:pRA/be
MD5:	E29E4D9ED6A2416AC5266D61FCF108A9
SHA1:	C2819EDFCAD280B5581C4512333B97F14104B2AF
SHA-256:	3C0787F9563BFB63DF8FA2C6B2E91D8CD0D414531B88AE2BE9A618379BA74260
SHA-512:	9D3392E63672FF1AF0C6595BCD33E5E33A360AD7725A3180FF3E60FB4B028D2C6237811E42A3249778128ABE633234FD62E2ADAFF2260EB186D0EE6255FD527A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0	
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ...V../....."#.DWz/...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):	531
Entropy (8bit):	5.556223805518441
Encrypted:	false
SSDEEP:	12:KkXxKMSCv2LtUlIkXxKMSCvltUl0kXxKMSCvQRvKtUl4:KkXxiCuLWIkXxiCtW0kXxiCYRvKW4
MD5:	0F187F02BAF376B6D2853E35BF5391E2
SHA1:	17881EA5AEBF23FD64BBF965A35BCF884059E454
SHA-256:	A6C766CF7CAAB802F99F58B4611CE107E41E6B5E607AEC910FF3DD8DEE2E9493
SHA-512:	19ED7D1C0009B4F44FE173CCC85621B40D3174CC1414DB5D1297C798E1C8A40485B051D7E6ABA94FAC57B2DC2D652702267ABA1D8739C265C7A0724AEF91D80
Malicious:	false
Reputation:	low
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .e..../....."#.D.k....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....1z.....0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .m:.../....."#.Dx.....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....Z.....0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ..F7../....."#.Da....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo...../.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	374
Entropy (8bit):	5.556501235371757
Encrypted:	false
SSDEEP:	6:mkl9YOFLvEWsfOLybWXuyyM+VY1TK6t4Mkl9YOFLvEWsfOLZoLUuyyM+VY1TK6t:5h6OLwfkIh6OLZoLUufk
MD5:	0294642A5C6B5F2F79B15F8960207136
SHA1:	8937D03A07A84103D72A13BDE127975291CDF20C
SHA-256:	4F24D5BAC8534118E5F88631091E94365957029221DE3FDF36ACA9E6E8262E74
SHA-512:	DCD2BD1572F20E34EED2FBA5FF48EF35481640BA8A3C39D64BD6EA796D8A5771C395DE8FDF4D0E06AE4A40BF7B3FBE5B9E52B60E780320C5EA29A9657D4604D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ...../....."#.D.#....A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....h5A.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .|yM../....."#.D.....A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....$$.@.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	488
Entropy (8bit):	5.615297111047129
Encrypted:	false
SSDEEP:	12:URVFAFjVFAF1ElNwSeKaTLnQRVFAFjVFAF7wlNwSeKaTLnu:UB4v41sNwzXLnQB4v47wlNwzXLnu
MD5:	883F7060C6CC4249888216F4E91A7E7F
SHA1:	DE83E1CC3BC57B082F5E88A6F289480D50B7B9D4
SHA-256:	83FE55D2D407B718336D4DA47D90A48949EB5AE282E5CF0BF954B9FE5C372896
SHA-512:	2A35675D6A2FEAE01966ABF8EE47D56DD0B198531E08BC0AD41F16C4EE9C64BA494F2A72AA699D3D2A774FAFE13B14A330FE40696540FE20457D9F2B7A768F28
Malicious:	false
Reputation:	low
Preview:	0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js ...../....."#.D.....A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....p<.....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 ...U../....."#.D..1...A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....[|M.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0	
Entropy (8bit):	5.483613368169088
Encrypted:	false
SSDEEP:	3:m+lx4F08RzYOCGLvHkWBGKuKjXKGBIEGdevA/KPWFvneTQLOw1kZyrpYFm1TK5kB:ms2VYOFLvEWdvBIEGdeXuBkY11TK6tv
MD5:	59B75D4F20F79CCBF66C64FBA021D329
SHA1:	0172AF7B29296859394EDE40F7606CB57B06D41B
SHA-256:	566A2B4F0AB7D7E6F22602E417C88CC0434432543A87EE4451EF14C3E244BBF3
SHA-512:	B13AA62365990CA4D1F4C22544C4774B622C21C45F43DBDD7B91A531CC09B3DE8D3E83A0764F6572A2989C643FCCFC5B469800DB48C2DA742FCD8514926033
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .u.T../....."#.D.u....A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo.. .....{I.....

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):	5.606452672274175
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQFoB7OhKlvA1TK6tId:RbR16vBJkq
MD5:	3201BDD8C19F0D5FA8A98513B7D859D2
SHA1:	8D3A5A564BF97DFECD57EB7C398651A15711A266
SHA-256:	736DCA5B086C09FE5CC897C134EBD80D525C8B0D6819CCF028E171855C43F1AE
SHA-512:	177B852DD84A75D7F3A0B308DAD4034FBC820D2B6663BFF0F1EDFCAF06EC5F51BAC07C4D6F809F6EC9C28A4B933ED36C48A72D550E44E9FFF7EC5D9779B6D 61
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js .a3Q../....."#.D.>....A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....3.....

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):	5.544426948197379
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVuOClgnQdFt1TK6th:B2geRHRQTClgn0L
MD5:	D71A2D79D59AC43D35352C2221498506
SHA1:	111D8CF188B37562B389E50B7D60AE204B15D3F8
SHA-256:	A13C5F263DE90B46517A51E10F33714E741B7B7A776337003A0650496DFA131A
SHA-512:	43D7C44DC64C3902375B2146645207987A41053139D9804D43A13AF55FAECF935C21E111E89A8AE80F2C1EACD18DA92C64B14A8507F501AC3EAF0E3ACCA679
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ...T../....."#.D.j....A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A..E o.....h.&.....

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):	5.608767981556398
Encrypted:	false
SSDEEP:	6:mzyEYOFLvEWdrIOQPkFyt1S/1TK6tllMzyEYOFLvEWdrIOQVMaEt1S/1TK6t:WyeRlSt1wzmyeRlSst1w
MD5:	5B3598B7CAA6741FCB4AEE9AAA688D0A
SHA1:	6BC6CB63A5F920F88EF8D4D83EE4893C4E35DA08
SHA-256:	C601343C2D01772BB4F512043D4A0D6C78DC3A0550B46F9A4FE4AAACA492C8F0
SHA-512:	876128ACC31904BD5B2CD25F276B7C6F6CEB28AED22EBF8725460EFC0636B0DF9E6491DE4A330826AC4FC08F8F23CCAFD3B7C8C37F706C256BA8AA856ECB9 50
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0	
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .J..../....."#.D.....A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....D..}..... ..0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..N../....."#.D.@....A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo..... ...^6.....

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):	5.561063199323969
Encrypted:	false
SSDEEP:	3:m+lKcv8RzYOCGLvHkWBGKuKjXKoyNH/KPWFvK/qk+WYNqww6U+5m1TK5kt7:mnYOFLvEWdhwyuCkWsqwK+41TK6t
MD5:	F836CAF6F97C061827AC1ADAB0D121FC
SHA1:	223B64FC2B2F474586D706A1B8F8C020A8964BEA
SHA-256:	4A1D3F4158E7C554DAFE50B984E5D3840FC58481A4660E7F856DD7B17261E85B
SHA-512:	3E00D51F0E1FEC93FB2170F4A571D7584309A12B29CC65C2C85263ACA31A2E11FD8BF28B004C0D41713CAC8027CC45F361AD6FE11C32D6E7927274471DEC885
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ...P../....."#.D.....A.....7...o..a=.98I.....(3.$G.A..Eo..... .A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	460
Entropy (8bit):	5.61306477595864
Encrypted:	false
SSDEEP:	6:mYXYOFLvEWdrROk/RJbumKAfO441TK6tUtMYXYOFLvEWdrROk/RJbugYfO441TKv:/RrROk/3fLEyXRrROk/ofLE
MD5:	10B13BD66F268C9F9D4896CAA91B0BAE
SHA1:	DD17CBB68DFBF383C3AA6A08D18E793649664CDE
SHA-256:	87FC8CA18A4867CEDA1B63030A9E74B1EFB27AA6D7B0EDB3438DA8468FF5005B
SHA-512:	3CE15FDB86CEECD5075301D3D84195B846FC6360BD55C17AE13C62D9D75DA54DF24D527E11196FAB3E8748A16A041ACF33B506312AE4838A4B19468E01BCB0 3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .[..../....."#.D1.....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo..... .....A..Eo.....(c.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ...N../....."#.DY.....A..~..rw.+ [....!.)?..f.U..(=.=.A..Eo.....A..Eo.....5.....

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):	5.602696007939844
Encrypted:	false
SSDEEP:	6:mmDEYOFLvEWXIC/ekK1QPLr1TK6tm9XMmDEYOFLvEWXILn1QPLr1TK6t0:xqT1mjCPLnsqTgCPLn
MD5:	32D4E0A3646099E46A1719A072E775A9
SHA1:	7E1AFFA3034C3172B5760A6962BDC73392671D2D
SHA-256:	2A531D551FC8A69F7F63624AF215F6F1AF3A735772F8502C43ECAE170B06BEA7
SHA-512:	2A513266AD2DBD275554351530DC4285AA12533CEBFE89AE784B505B0B9029FD9F9985CF4A350B148293B9F7A6182AB01068A5D4745517D79ADFD99E5F04A9D9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ...../....."#.D.....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....0\r..m.....:....f ....._keyhttps://rna-resource.acrobat.com/static/js/config.js ..jM../....."#.D+.....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo...../R.....

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):	5.638933898575436
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0	
SSDEEP:	6:m52YOFLvEWdMAu+puqQIsEJ41TK6t+M52YOFLvEWdMAuKsw+ZsEJ41TK6t4:zRM25sD8ZRMwH+ZsDW
MD5:	EC2C5F650D3794973CC6FD1E3532D872
SHA1:	C41901B26A6E8CCBB231B86492C7DD53125543BA
SHA-256:	F9C48CF28EADB848D5AEF6EFD9682BD42A54920BA62EF6B1CDBACAB69384BE38
SHA-512:	DED63B820594752BEB37AFEB6F6A81591AEE170A4600BEBBA1CCA9809F3731732EDC2C2C28B083EACE343CAD371DB09B9E0488AEB74D7881D93C4248A2C8E F2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ...../....."#.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 .I_U../....."#.Dx.....A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.. .....M.0.....

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):	5.58425963969144
Encrypted:	false
SSDEEP:	6:mYilPYOFLvEWd8CAdAuhKgBzQstSFong1TK6t7YilPYOFLvEWd8CAdAucOTtSFo/:6lJRppMSFoM/lJRuSFoMk
MD5:	C9DC1167F49C5CC7D8B6D341D249B587
SHA1:	AEC58F0357BA15B49B58231D3B3A9447F90F29BB
SHA-256:	C71D9269412464DDD3F576FD09D01D8DEF264E4ABCF024B1745794863B95B403
SHA-512:	0271071D295EE6BC5636FF47C068B3191F965D0C7E161BFCADACC9FA9230EA44352937F7795DF98CF6D54F7F274E8000BC7EBE65B0791951867B9667DBA93292
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ...../....."#.D?.....Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo. .....R.....0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .MbU../....."#.D}.....Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo..... .....A..Eo.....vV.....

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):	5.599920737713306
Encrypted:	false
SSDEEP:	6:mY8nYOFLvEWdrROk/IukBcWe16wG1TK6tN5+Y8nYOFLvEWdrROk/IuVCWe16wG18:F8hRrROk/GVe2bT8hRrROk/DCWe2
MD5:	F35FA9921656EA8CC344D8D1C0DE3C34
SHA1:	BC59DFDE306539F48BA9904B968FAEE14E616BE4
SHA-256:	61CAC52FB2518E1CDBAF6267563BBAB95EC0980AD2DCFBC79E7A41118FD500A4
SHA-512:	55931CF1DD83BCD946C0561C52B517B32563ABFB0DF07A55B68F157D459AC1EE848ADA3E56F460CC2AC5E5E1C280FC2C49E468CF05397BD3060DD3596555F3 A
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ...../....."#.D.....A..%.k.SZ..~W.....:)'B..ad.....A..Eo..... ...A..Eo.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ..N../....."#.DB{....A..%.k.SZ..~W.....:)'B..ad. .....A..Eo.....A..Eo.....f.".....

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):	5.666490303922049
Encrypted:	false
SSDEEP:	6:mLrnYOFLvEWdrIoJUQHOtFYrNJli1TK6t8/ELrnYOFLvEWdrIoJUQOagyeqrNJlb:ehRcTYrNJlCaQhRc6gYrNJICs
MD5:	97A118FB736DCD2EB4EE5BF629FDB3CE
SHA1:	1505461692769F1EA361761C7182466D9520BEE7
SHA-256:	BD442744CAE15661C115159885E8D201F97262E77296AE826FC5C6C26FB26F2D
SHA-512:	82C68503CC0EB9BE1FAF4BED45CE1AE074926F31CAC926518ADE948B0909ABCB8040F0F6AE1F47F092D53BDB48EC7F919DB7B2DF28F4966A03CE0A252A5A1D A7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0	
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ...../....."#.D.2....A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....o..J.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..N../....."#.D?.....A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....8.h.....

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):	5.583126590132488
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhuI06GTLzgm2d/1TK6tpOEYOFLvEWdrIhurz/bLzgm2d/1TK6tg:0RSG3ReNRlTRe
MD5:	777984D28446E4C40DB5B8CC40FB89CA
SHA1:	02EB5F5CCD00E65DB0314E24ECB4F0D4AF3D58A1
SHA-256:	92F9B0367B363D870BE9679BEF2B2A8B8F98286FB46434064C2B3BB1D5A987CF
SHA-512:	CFAA8CEC11B3D569233128F51E1652E88C9740FDB658B8684882CD2050A588F5A323D24B30914FEEADD211A314BD48F053CD1F8C3B3B30212778FED52E91DE9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .Ju.../....."#.D.\....AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....k..|.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ...N../....."#.D1D....AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....J..F.....

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):	5.60947798888157
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1Kdz9vkx56uvp1TK6t+AElVYOFLvEW1K+/wUvkx56uvp1TK6tZt:6JJKJ9wEJJKANwF
MD5:	84B5D07D747CE469EFBADFE7835377E8
SHA1:	D5D316737BAF9319AE1EA4686828B9C94EE9BD4C
SHA-256:	097CE832AEBCF1C754CB0BE8CF781C9CC3224BDD987D5E0F8EC8999963946442
SHA-512:	2730035F92A89DEDD15BE0611A447489B324C1B64C95D7575AC8552DA88AD287B31781D2FD28FDF7E933BC24567FFAC25A00C61A7248902A7EA243DBCD91F65
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...../....."#.D.8....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....e.z.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..3<../....."#.D.....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....{.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.628589961606053
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvuH3aGIhrhUDLYtmOZn1TK6tqv:xRBJE3B0eDcFZLUv
MD5:	D2BD14D373BC5FB9235100AAD9C2E098
SHA1:	C75DA80FFBFB2532A754D8638FE8414D7661D07F
SHA-256:	F3FA69701E453547D886716AC16081CF01D298A0423C227300DF99228B1A2755
SHA-512:	4684C4B3B65E74FA84F3DEA1DEAF766FF928C6377A3B899152743B9C74293D7FAF619371E222E0178CF5B82C42F72FA1298A4EB51908B1184415C8BB90D8E9FE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ...T../....."#.D.....A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....>.r0.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	633
Entropy (8bit):	5.603142774458485
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0	
SSDEEP:	6:msRPYOFLvEWIa7zp79jtnkVPu1TK6tLmYl2sRPYOFLvEWIa7zp7bocvHVPu1TK6e:BPHjpkcRmYTPHLHcZ/ll7PHgcA/
MD5:	E0B61E6F09E88D98CE19AB826443CA8A
SHA1:	484021DC5FC8A004CD309253824BDAA5CA91325E
SHA-256:	6ED93E4FE217DC206193BD930E25A7BD074441B619F2664B37F4064056FE6441
SHA-512:	B72E3EF37DA73894CB1B6D3870E39AE313BCD53463E77802BCFE875DA4E92953DDE3DEFF3E6D475DC4F8AC524F929A4BA4F9C928AE22D0B720EC7515A2CFE D14
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ...../....."#.D.O....A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo. .....F.e.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ..P.../....."#.D.....A...L...Im.@.....E.nW...IP..A..Eo..... A..Eo.....xA.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ..J7../....."#.Dqr....A...L...Im.@.....E.nW...IP..A..Eo.. .....A..Eo.....y.o.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.554825589691865
Encrypted:	false
SSDEEP:	3:m+lQi9lC8RzYOCGLvHkWBGKuKjXKVRNUpXKLuV9DtUTtJs4XVAZ+8cV3vRm1TK58:mKPYOFLvEWdENU9Q1biM3Y1TK6tj
MD5:	13BAB4C7DF26CDE97736FB9FD623EBDA
SHA1:	9D68BA41E4580B003E1A3C2BAABE0743F4EE76C2
SHA-256:	9257B71FABE9F61488269C4F19DC2C0A195B43D0E3F374A85C866AB18AFE1CD5
SHA-512:	541303F132CFFBF7BB9A985FAE6CA7B14E1C647C57322079F92FB33983603862BED685333E7EDCB2126A5DCA23EF60E1DE2117EE552EEC653186C9DADD2979E 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .+7Q../....."#.D.6....A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo... ...c._.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	modified
Size (bytes):	208
Entropy (8bit):	5.592807005700952
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQVeRRjBRCh/41TK6t:XRc9q2RDi/E
MD5:	A00A40653F6509405F6A5911E86646F1
SHA1:	4C5A973F61E99C081BC708B46B26678C07C60208
SHA-256:	A0EE988BCA725D638C7D7E3B6781C60F57C37142415AE6073E33DB9EFE6D1614
SHA-512:	9BC829639D1679AB588C951E60B5A5AE8CEF4E73F7D02042A93D46B46B846C2A19A0AA79BBD831A01D3D2A148EBC52A0AED2B305A60476760B470812C2D7E5E B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ..#V../....."#.Di88...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):	5.596241790228639
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhu5ubZjULlF4r1TK6t:bs6xRkiaALlF4n
MD5:	E08820A93275AB69C6403464D22C8975
SHA1:	C389E03FEDB5F12D52F0045EA3288D3AAEF6A459
SHA-256:	1271B380FEF84D3DB879F42CDD9C70F2A165DA4C854C4712BBC34590ABFC3309
SHA-512:	66E32E2BAC5F7E5E7893B6D9D34556A3436195AB2E4E137381A9C54D4EB44B5B0A3886B0CDB7C83C129DF6BC3E7D944DB92D8A1335FF217763142820D1A4B5E A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0	
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .6..../....."#.D.....A.P...#4..I....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):	5.496330535665883
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvYzxt+l/XOoGTcu1isLK5m1TK5kF:mhYOFLvEWd/aFuOzxt+0m941TK6tB
MD5:	DCC470A7A0445DB49940E03478A9CB9B
SHA1:	B0013702989508237F745D70F913639A3A0DE884
SHA-256:	EE782A5B841E8A0F142A5DD331A04EE284B05488F6DA709A889D0E78A93B1B0F
SHA-512:	F2CB7168AE91FA4BD55E0B5AC61558865DFE684D6BE429E89665A9A129CD1D99F712E1586FA3BB979DC5249EC4B0CB80F5684EBB9169B42A6414497CBF688CB2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ...V../....."#.DH./...A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A..Eo.....U^P}.....

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):	5.496430191829099
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQTq6KOMBoBMqVd3G4K41TK6tjeF:2DRuRAq7qB9Vd2kpeF
MD5:	4F232C299DB3FD474FE9894C53E0E78C
SHA1:	BBD465B85130A303A5E72A771C2549B7A746DAF7
SHA-256:	89655B01EE35290AA95798E1BC2BABEB267BC025525814829CA0C062DC0B2D6D
SHA-512:	121EB8D75541FEC81CD0D7DD6DFDD58664F2BC162A9CA21E62A5019F6789020DB1E54EE9B751B6F0545DA833094CA3067A7F6C9CDD08756BCA7E216BF95368C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js .X.V../....."#.D._/...A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.....r..Q.....

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):	5.648880476906732
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9Q9qSlbfuA424r1TK6tRo8kqYOFLvEWd8CAd9Qd/4xuA424r5:+RQsqkGrnHosRQKNrn
MD5:	9DA2DF90B5EA9221A7D11E4EC40B2685
SHA1:	C67A659FDB4DA49D8EBAB644B3BD2A9F3A0BB358
SHA-256:	F31CC5296A44C1151504266DEF76CE7BC9D78D73E7C4508F7F631FCBF4EB6703
SHA-512:	F049947CDCA6241DBA5499093FBA808BF8D2A26120971C81A0813F764B5FD00BBE394CFF04B6BC9C45ACF495D51E3EDA40CA87D706C1E410C3A549ABB9D00FC4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .KL.../....."#.D.....A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....U.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .r.V../....."#.D..9...A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....<.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.570810222625245

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0	
Encrypted:	false
SSDEEP:	3:m+lS5Etla8RzYOCGLvHkWBGKuKjXKVRNUp/KPWFvBi1x4tqug2iHio/Mm1TK5ktD:moXXYOFLvEWdENUAuriGquyC8n1TK6t
MD5:	FF2BC34B60DDCC1674777A3524C6B2A6
SHA1:	B8EEA1FB6F361F0714C8643ADFDFA6EDFA172A22
SHA-256:	D3EE344A18360E4B567C537CBD0FFAE8061EC38BC5428A073343406AC5C46D53
SHA-512:	6D7F265505CF6CCEC98FC989E9A4FDA8EED6BD33F4D850635CFC13B380624C49DD78C564172155DF6CE150517AF8B600147106C64896B76754879DAC663B948
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .$.P../....."#.D!.....A8.../..;.\\o....1.....+..A..Eo.....A..Eo.....R.. .....

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):	5.642959700259336
Encrypted:	false
SSDEEP:	6:mQZYOFLvEWdrROk/VQXOt+LmB41TK6t5eQZYOFLvEWdrROk/VQ6l6jLmB41TK6tT:nRrROk/VBmnfRrROk/Vnl6em
MD5:	D618246F63CACF177906CB21A206E6A9
SHA1:	0A75B55056F456E25A1CB18C51CD9FA7D904DD2B
SHA-256:	A7CD3CCC46EB00EE47341C8682E17664AF512D9C1703D22BBB42AA96C9A6D672
SHA-512:	D4F21E023446552D675AD02C68E57212E6A7C96E6BCFE1F7BBFB6D0E938BAE99205D797A245250DA18328ADFCF6A0542214CCBF8E35C82DA9911E9F61A0529D 9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....].....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .D..../....."#.D.....A ./.ev.....N~..6.b.....$.j;:C...A..Eo..... .....A..Eo.....0\r..m.....].....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ...N../....."#.D\.....A ./.ev.....N~..6.b.....$.j;:C.. .A..Eo.....A..Eo.....X.....

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):	5.525209097420141
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWubOvoxAdm9741TK6tST:qxRcwoxAdu7Eo
MD5:	79DB11F607143F6C66617A21A19A78DA
SHA1:	3AED1A71BD080C1243A6BF7FDCF0B500277174EE
SHA-256:	E034B9F9BFB0CB689FF378E6D0913A05317D00A325856716450B6740AA0219A1
SHA-512:	ED84E82EEC5CEAC1C2D2EB9AEEC4611E2D4F0D8DF5EBA1FCA79F9665625EC4021CA5997EA1D564A45AD617BB2A42302CE18FDA85B4E89D0C2ED3E27DE6F8 4E9A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js .+RT../....."#.DY0....A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo. .....E.....

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):	5.578131230365596
Encrypted:	false
SSDEEP:	6:mMOYOFLvEWdwAPVulSxkSPcJn1TK6tO9:2R1aSVPyLE9
MD5:	1B60FCD24D57074471DE816C2D1C30D8
SHA1:	4D3DAD8A5DBBE532B2D71C3C9AF572BDD0E06ADB
SHA-256:	3D2085436D7D863E6C6C0877C2E433BD680B9AB2C33CFF6291E8895A07582ED2
SHA-512:	D66AF8F2E0261EBF18A90DF4C22E5898026F9AAEB0BA8FD9506355E1A79E93434F127372563387B95DF25CFAAFCEEF244F3A8618C0B4BB214E6DA4A983A3D48 6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0	
Preview:	0\r..m.....L....Ey...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ...P../....."#.D.....A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo.....Vx_.....

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):	5.638359046385041
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQHxtjkzhcsBXIh1TK6thvF:mxRBJQ+LoDB0X
MD5:	D5A4F18F9E69261C1CEDDD98DE0707FB
SHA1:	3A02B660D8D465753F8D345B6EB786E2C603B4A3
SHA-256:	E330ECE9CC12C460DD62FA50618B0882CAFA4C0436EB827F0E4479F59680551E
SHA-512:	078FB3D102E2E0BC1ABF5C0F6C5F122C2EDD9190097BF67815208091A2F91F8157392E73FBBA88F241936ECA2CC79650773423FF4602036623367079A81A063B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ..(V../....."#.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):	5.596172409983089
Encrypted:	false
SSDEEP:	6:msPYOFLvEWdrROk/RJUQVWtuc3Me/1TK6tTv9/EsPYOFLvEWdrROk/RJUQh6c3Ms:3RrROk/sQcN/RrROk/s7c
MD5:	D23022D6F00EDCDF614D9B4CAAD53F3B
SHA1:	AE710EF16C51F0EA732EC85B5FC82A696746EB37
SHA-256:	585F287D51CCE3C92773F403059505646D85A117D2BF3EA8643FCBA14264CB31
SHA-512:	D90177F95B5D0AD5DE8E4602AF3B8761ED10B2FCBDBE27B163E4FA327D03B9112C7A36B8C6D741F9EEA7F3AD8F9AB90CD5080203F545AC71050B0C520056F3E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .. .../....."#.D.F....A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....6.....0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ...N../....."#.D.....A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....9+.A.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	2016
Entropy (8bit):	5.219067382957879
Encrypted:	false
SSDEEP:	24:Mfg1zZFufGMisp6r6C9QPk30lavdNMaekNVuLaY4KWcToL:h1zZ4+dsp6J30UdNIkNoLd4K7T8
MD5:	272E97EA6AD8549B833CBEDFE9A89E15
SHA1:	21F4D3E5EFBDC1988ADCF95654390A1E0BB8E9CF
SHA-256:	CE45A7BD157BD00043F0BFD58ABF01CC78ECC8C119D3874502DE5B365618E8A4
SHA-512:	FA188B6CBC785B38E3E7CFB4C2E5C6EF242CEF3CB86F690F29216C9921A19E8A9005B181F962B714A0493BA831F74BD091391D647F07BC8B0AF13F92B7A9E47
Malicious:	false
Reputation:	low
Preview:	....h...oy retne....'.....'.....;.y~A..z.B_./.....*...z.B_./.....oB*.8.B_./.....#...(...A_./.....k7A..z.B_./.....D.4..z.B_./.....[.i..%..z.B_./.....<...W..J.8.B_./.....,+..._.#.z.B_./.....J..j....z.B_./.....6<|....8.B_./.....A?.2:...z.B_./.....+.{..'.z.B_./.....*)....J:.z.B_./.....2q....z.B_./.....P....V.z.B_./.....+.U.!..V.z.B_./.....P[. q.z.B_./.....!...0.o.z.B_./.....u\]..q.z.B_./.....z.B_./.....*.....z.B_./.....o..k...z.B_./.....^.~..z..z.B_./.....o..z.B_./.....Gy.'.h..z.B_./.....F..=z;..z.B_./.....3....z.B_./.....v...q...8.B_./.....C..M.....A_./.....a.....8.B_./.....~.,.4>..z.B_./.....&.S.....z.B_./.....@..x..z.B_./.....=....m...z.B_./.....;/....z.B_./.....q..z.B_./.....MV3...z.B_./.....:..N.A...z.B_./.....B_./.....:..oy retne

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	289

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
Entropy (8bit):	5.193527794750203
Encrypted:	false
SSDEEP:	6:mKucyE9+q2PWXp+N2nKuAl9OmbnIFUtpHuck0WZmwPHu9DVkwOWXp+N2nKuAl9Oe:Xai+vaHAahFUtpHhW/PHUDV5fHAaSJ
MD5:	1312009087266904A8C3DD95DC1C2225
SHA1:	EBC12E9FD781581FB56A623C9C7DA1E04D1AE306
SHA-256:	B660A0D10D157EAF3327C360B07EA415A4E12096A7B4F36F6E1D115A29B49CEC
SHA-512:	571F35EB0E7C67B68A4CC21DD6EA8549E573F5962E4746C00D4B6E82CBC08C5FDB210C12BDC8F4D4C6F94315C7FACDE2CD847CA6536FB3BFC97B0C336FEC DF6
Malicious:	false
Reputation:	low
Preview:	2021/02/24-02:31:52.258 85c Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/02/24-02:31:52.259 85c Recovering log #3.2021/02/24-02:31:52.260 85c Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	917504
Entropy (8bit):	0.007775583823103001
Encrypted:	false
SSDEEP:	24:TGEXiXKGEXiXKGEXiXJ88hMXiXN8hMXiXTg8hMXiXTg8hMXiXT:TGEiaGEiaGEiCsMi9sMiDgsMiDgsMiD
MD5:	CFB315BC46FE90003DA8EBD9F4B3ADCC
SHA1:	D2CE24C0F4BC5B05A24FBE51370821160EAADF1B
SHA-256:	551AED495E031A34FDA7CD305771663B585FFAD758EFFBD8EE8B2EFE35E6DE8B
SHA-512:	D6C2C4979825630A8348BA0786A5F83020D3DF098FA6142E6237CBB61F92BBACC6012E045B8E681463F6D31ADB1985539A1AE93A255B22F7B99625A8B284612B
Malicious:	false
Reputation:	low
Preview:	VLnk.....?.....Tq.>..j..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3024000
Category:	modified
Size (bytes):	24576
Entropy (8bit):	3.3403364168919647
Encrypted:	false
SSDEEP:	96:iR49IVXEBodRBklOuAhFVCPL49IVXEBodRBkROu+hFVCP749IVXEBodRBkd0u3h9:iGedRBCcedRB2aedRBa
MD5:	253416C6A419AFD88D0E0F6ED0D7F343
SHA1:	454A44A39630A45C41CDBB84A3D57AA1D6A884CE
SHA-256:	170A842AB18B71E443F352B2EF4DEC833EF5A3264184BDD34521B0A1D2BA8987
SHA-512:	42E7D45D0777CD0F51B62144A5CF367C2446099E2ED71EF59390EE2DAD85E8C1DD4A4D41D09AFD00C2B08BB8348C15299A69C50CC0121239FA74F22AEBDF77 1
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....$.....1.....T...U.1.D..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	26196
Entropy (8bit):	3.1378214233821837
Encrypted:	false
SSDEEP:	96:j7OhFVCPn949IVXEBodRBknOuAhFVCPzLR49IVXEBodRBkuOu+hFVCP0d49IVXEl:jTiedRBMfLGedRB5iCedRBF
MD5:	214E6C228319F8EBB514827690822B5E
SHA1:	787415C3E9314D23543816E5BBF2E24F9120D4A8
SHA-256:	EE262C55B0EC8DD409DABAD8C771FA5D3F43B58F110D42A27679F2015773E941
SHA-512:	83E4C977F0F6D9F1E37F5DA69E758D622BF65250649FDE6C17CE33333518945A3B5D03A1F44C02E6880D97B8335F23FE7FE41FD803B3673174171066B642FD9F
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	
Reputation:	low
Preview:	.....=..... .....X.. .h...y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{679099D3-768B-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	36440
Entropy (8bit):	1.8918201286107352
Encrypted:	false
SSDEEP:	96:reZpZEe2EB5WEBDaQtEBDa52fEBDa5UnzhMEBDaLGUvEBDaLJLUMmEBDaLEUhNEI:reZpZV2wWmt6fGhMbr09aktoUSLG/
MD5:	3B639D8083A0CAC9073B1F7E93869781
SHA1:	210B2AB03C80BCD33E8405C495286BD0E26F3DEF
SHA-256:	12F853BDF9EF10129FAC88D0902FCFADD6AB7EBCFA30075BC4E691E32880390D
SHA-512:	B994BFC332B7EC4CD3EFA749091B6FF0A65A0131986FBE6591553E5D9F82981C87E734F24E06CEC3B42A77EEC62622F6AABAD965FD72D423FCD5AB1CCE030E 26
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{679099D5-768B-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24228
Entropy (8bit):	1.6386642358875172
Encrypted:	false
SSDEEP:	48:IwqGcprTGwpavG4pQ7GrapbSJGQpB6GHHpczTGUp85GzYpmKMGopRkj5QGmNpm:rOZNQh6vBSDjB2NWXMXX7g
MD5:	C254B15F6762E70792C8D9897E1EB61A
SHA1:	5B3D50B3DE8841F69D69451F6C04C3B56D911BC3
SHA-256:	5C7C8C2C8E0A3D1F8E19F04E8E9368C997E966364A4C5FDC468D442F7E5930BC
SHA-512:	54E78A7F7379232811F66EA3DE41F0BD8CCC211A3FC66E5D9985801E57DB4FC7CF05076DC9149E03DB5D5CEFCA99A41A7FBE4B0569E34142970CEF31141A9F A
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{679099D6-768B-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.564941050994423
Encrypted:	false
SSDEEP:	48:Iwe8GcproRhGwpaW8G4pQUuGrapbSxGQpKOUG7HpRO7TGIpG:regZoRQWc6UgBSLAOfTOxA
MD5:	C0E9518FA7ECFBA592540C5406BB5C00
SHA1:	5BF2C5D2422B7A492049A9B949B0D912606F03D2
SHA-256:	204F221A2E8C418B8B7047B867C1AF0165C03DA76F0273804F2390F34C6A3E2D
SHA-512:	7459834008A0C385AE33AFA24A05E1D9089D5F50980824344DA094AC28D303B352263AF0AF49B92ABF63E2B795A79D3F37C94BC6080AD2CA83713D02E7FCCB1
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.06211473015613
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEEQnWimI002EtM3MHdNMNxOEEQnWimI00ObVbkEtMb:2d6NxO8SZHKd6NxO8SZ76b
MD5:	56399DCDFCFB719D479CD4289349B9BF
SHA1:	25DDC896543BF057089BDCA49DEBBFE19E0FBF69
SHA-256:	AC70507454E42D58F00B0985199218E59CCE6DC91F36A6807747C6895FB5FB25
SHA-512:	BDF1938DD9CBB384B6FDF255E89A411478E01D060D5A8B790934C8A1AF08732DCD00C47B14C26477818C8E715030E2D341A819C9403EBE0533D6AE1A25BF4AE
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x3e2b1c0a,0x01d70a98</date><accdate>0x3e2b1c0a,0x01d70a98</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x3e2b1c0a,0x01d70a98</date><accdate>0x3e2b1c0a,0x01d70a98</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.106705720808248
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2k2ynWimI002EtM3MHdNMNxe2k2hnWimI00Obkak6EtMb:2d6NxrkSZHKd6Nxr/SZ7Aa7b
MD5:	31E3955431E612C9A1C75C2C3ACE4563
SHA1:	FE3221E469FC608A6E607A740BE8D76B192AF4B2
SHA-256:	FD891702DF25A98FF77BE6D9EA941CCCB8B7BEE4F9743B40B55CA7556D43B68A
SHA-512:	88CAB13331267E50F6160C0C38AE16C4B0FC114AC53834913293E9E6C4C5FACB7451439D09136EB9C2BEBB3C41F3BE7997365E656278E5EE078747D04E09D00E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x3df90a6b,0x01d70a98</date><accdate>0x3df90a6b,0x01d70a98</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x3df90a6b,0x01d70a98</date><accdate>0x3e0293d0,0x01d70a98</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.102472667937424
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL0AnWimI002EtM3MHdNMNxvL0AnWimI00ObmZEtMb:2d6NxvlSZHKd6NxvlSZ7mb
MD5:	21E06D1A6B03D4AAC55BBCA40C18F7AC
SHA1:	974441DDA13216428EA565429588C560992B2DD8
SHA-256:	B004DF5386D46E00EA7E02E02371B3A2916F678CB694DA14EE591AF66C021186
SHA-512:	82FAF516766B86202362D06A0D961908AF919184B79FC0C0688D44543EC7A83901EE2CB029DDF64A740447491AEBE99518C1C715E53007E4EACBDE1A30CB6643
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x3e34a537,0x01d70a98</date><accdate>0x3e34a537,0x01d70a98</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x3e34a537,0x01d70a98</date><accdate>0x3e34a537,0x01d70a98</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.065054053744519
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
SSDEEP:	12:TMHdNMNxil5uLnWimI002EtM3MHdNMNxil5uLnWimI00Obd5EtMb:2d6NxOSZHKd6NxOSZ7Jjb
MD5:	45E8C09F7BB72DEE76F94A052CC46405
SHA1:	8ECC112B01243AECD499DEC9922927AFA688A03B
SHA-256:	BDCBA5481F168BECF772FED7AC8FDC7EC8E73F5FD68C370048B8F7E1197EFBE1
SHA-512:	E2C84A2C619F4B34024A11B7D55E6F3ACD4212C6B60103038C18FC725A042B90A811890D1CB3615B4166E309121A25094A34687697ECAB78CF91277CEFEA4A7F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x3e1ccdbb,0x01d70a98</date><acc date>0x3e1ccdbb,0x01d70a98</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x3e1ccdbb,0x01d70a98</date><accdate>0x3e1cc dbb,0x01d70a98</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.114358792810135
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw0AnWimI002EtM3MHdNMNxhGw0/nWimI00Ob8K075EtMb:2d6NxQUSZHKd6NxQ7SZ7YKajb
MD5:	B0CC52A0DD36DBD063464DE9007EACBB
SHA1:	1A6D7F8E1263C96AF5FFC471E059B3DFA07F19BC
SHA-256:	CE2A1CF708DF791FB8B423CB79C266DCFC4AB81EA13E7EF9665D8B0E01480847
SHA-512:	FAE1CD3EF0867C06D1A42FE44177198E7CA334C9C4629C25D9BF704CEEAD9AD8E5C11E165DC11FC7B373E5E732D717DA7A62671823F9F9B20883A2B44551BE C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x3e34a537,0x01d70a98</date>< accdate>0x3e34a537,0x01d70a98</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x3e34a537,0x01d70a98</date><accdate>0 x3e37078a,0x01d70a98</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.065232638971414
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nZFnWimI002EtM3MHdNMNx0nZFnWimI00ObxEtMb:2d6Nx0bSZHKd6Nx0bSZ7nb
MD5:	BC7699DAF6FB271D5D25E56ED5F54F3C
SHA1:	E5C04FAC41052C232FBAEA1C8C7D1F17F863C9BE
SHA-256:	2E1FC45A963D1E811971E5787870F1ADE10897003DD9EAABD550FA0E5B228A0D
SHA-512:	0A5240AB253CA5A5CC32047D3019856A0249E19D30337E37ECC294D00253ABE068E41BF95D09F9D849B62635F0E08B5AED1B02229DBCA08A4F10913DA41AF78
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x3e1f3020,0x01d70a98</date><a ccdate>0x3e1f3020,0x01d70a98</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x3e1f3020,0x01d70a98</date><accdate>0x3 e1f3020,0x01d70a98</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.102633149471438
Encrypted:	false
SSDEEP:	12:TMHdNMNxxZFnWimI002EtM3MHdNMNxxZFnWimI00Ob6Kq5EtMb:2d6NxtSZHKd6NxtSZ7ob
MD5:	57CB9DE79F31F940AEA1D109B22C1FF9
SHA1:	3075458114DCF518545355863D3F35B17371F059
SHA-256:	7DC3BC847D60538004D48910BB74B4F939109951918283E62B2C9924CE2D4C95

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
SHA-512:	6C51060A05B6A1B79630527D0C1A760CC64A95180AEC2B8081574CEB1AACAD1A305F43683D1F148883FD0B6FF19B2E97FD98ED9ADF94FE5884C1DA3ED56AD9B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x3e1f3020,0x01d70a98</date><accdate>0x3e1f3020,0x01d70a98</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x3e1f3020,0x01d70a98</date><accdate>0x3e1f3020,0x01d70a98</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.097954004256579
Encrypted:	false
SSDEEP:	12:TMHdNMNxc5Fu3LFuhnWimI002EtM3MHdNMNxc5Fu3uLnWimI00ObVEtMb:2d6NxyF2FaSZHKd6NxyF5SZ7Db
MD5:	0A383A398EA3B00C6EA7B75909C84001
SHA1:	85D706B073BF8F20429158612547A09BAA169C8F
SHA-256:	472997C19617B814B4306D89BE179FFF8F5F086F33D6A6FCECBFFCC96A975116
SHA-512:	3D51FFE7C593974BEDB3F6E4A718A2FEFB148698BCAA56658906B816BB36E26077F7005E2134DF8F23BF2C3F74BA4A10B4E93B4788C7A18EC9B9C4112BEA7C1B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x3e1a6b76,0x01d70a98</date><accdate>0x3e1a6b76,0x01d70a98</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x3e1a6b76,0x01d70a98</date><accdate>0x3e1ccdbb,0x01d70a98</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.051140924246385
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnI5uLnWimI002EtM3MHdNMNxfnI5uLnWimI00Obe5EtMb:2d6NxlSZHKd6NxlSZ7ijb
MD5:	7E63B89D05A4B48B9850C7D5466B7E3D
SHA1:	DBF520D4F70D68F2089D229C6CC2C64DBD2001EA
SHA-256:	826B6019B9C2D6A47B1EF0144328E129D53D561980253A11096E549601FDCD8A
SHA-512:	421DD1A5AF2EC36EE8CB475C9A972B9955E01A42ED93E32141BA68BB6581BB65975354A9FB13F8142818BD78AD026E944C86433A5C1DB61A52D14D41EE683B3A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x3e1ccdbb,0x01d70a98</date><accdate>0x3e1ccdbb,0x01d70a98</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x3e1ccdbb,0x01d70a98</date><accdate>0x3e1ccdbb,0x01d70a98</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PDF document, version 1.4
Category:	dropped
Size (bytes):	574061
Entropy (8bit):	7.425377937675292
Encrypted:	false
SSDEEP:	6144:GfNu4eU9lE9D2XG3zZflur/lmuGPoBLpnXzLjY/HrRnnEWHB2p972/GpZdoru:GsNGIEaczNfrwuWo9R4REWh2y/6do6
MD5:	C59619E954F34013C5E90BDCA279BDD8
SHA1:	6FF284222A34BF076FA2DE3801A040FB05DB9326
SHA-256:	DB0F31E4517BC4C85FF2C5F22953FCF6910A8BF09ACDBD1DC032AB47F8EAB708
SHA-512:	34AF4C33EEC42F5EEBC42667BBE4FA7E7E32E36B709961881CD222133404A09BF0C76D39771BCA08BB994A1F1CCC293A41B9EBD882872AFAA89625FE40CCC592
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\._files_ada-rehabilitaion-act-coronavirus.pdf[1].pdf

Preview:	%PDF-1.4.%.....1 0 obj.<</Creator (Mozilla/5.0 \(Windows NT 10.0; Win64; x64\) AppleWebKit/537.36 \(KHTML, like Gecko\) Chrome/87.0.4280.141 Safari/537.36)./Producer (Skia/PDF m87)./CreationDate (D:20210113000916+00'00')./ModDate (D:20210113000916+00'00')>>.endobj.3 0 obj.<</ca 1./BM /Normal>>.endobj.8 0 obj.<</Type /Annot./Subtype /Link./F 4./Border [0 0 0]./Rect [63.999996 709.5 555.99994 729.5]./A <</Type /Action./S /URI./URI (https://www.eeoc.gov/)>>./StructParent 100000>>.endobj.9 0 obj.<</Type /Annot./Subtype /Link./F 4./Border [0 0 0]./Rect [80.499992 524.5 378.49997 546.5]./A <</Type /Action./S /URI./URI (https://www.eeoc.gov/coronavirus)>>./StructParent 100001>>.endobj.10 0 obj.<</Type /Annot./Subtype /Link./F 4./Border [0 0 0]./Rect [117.999992 370.00003 360 381]./A <</Type /Action./S /URI./URI (https://www.eeoc.gov/disability-discrimination)>>./StructParent 100002>>.endobj.11 0 obj.<</Type /Annot./Subtype /Link./F 4./Border [0 0 0]./Rect [80.499992 305.50003 442.49997 354.00

C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rtzb8pn_r4v8rg_2t0.tmp

<table>
<tr><td>Process:</td><td>C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>589824</td></tr>
<tr><td>Entropy (8bit):</td><td>7.999672800846399</td></tr>
<tr><td>Encrypted:</td><td>true</td></tr>
<tr><td>SSDEEP:</td><td>12288:yDa6hiOAYCNWaOYwwRuvBVXhTnWs8sqpMf3gP6c+S/1:yoOAY+pRuD9wLpG5c7/1</td></tr>
<tr><td>MD5:</td><td>B0B8E1F5741510025205BF2820E0F62F</td></tr>
<tr><td>SHA1:</td><td>D0D9D8B8CC0AFADCEC7183A139DEAE211B502E35</td></tr>
<tr><td>SHA-256:</td><td>79348EFDF990269DF14A1BFC5E015B3D484F937996B441471C9D0BC575523770</td></tr>
<tr><td>SHA-512:</td><td>4D08422C545EBD5CC7C854897B17CA7345AA3A53E0F4BBFF8AEDC6553342D8F65B195C84E2B6FCB44B1116D3A4E89DA61F86BE7BB9F9571CD3F1251E6CDE4
6D</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>Preview:</td><td>.z.@M-..M..D.%8y.i...PK|=..N.,..kF........4.:...<(.(...&.Y:M...l.....gd\"......*.J.)..H.[@..|}N[.../...........K.(.I..Q..O..6..S.R._......jm.I..R.C.<...C0...S...%..a.\r.8IH..)! ....Ge.K./..~.3*h.ET\.......UP<[[tV]..H.......-.H....9.X...c..B..1......B.......I...<vS.N.]]. ....5.h..S..,I.zl$bd[.F........B.....e...H..!...e`...Y.~3....1}.@,..1....2'.....K"...Bz...f..C...x....jy...h,..M.....V...(.k...Q....B)..q..-.hFY.$...).>..8%.Z..6..X..R5)...oN ...PP...U..(.0.!..+...!:.n.<=?c`;...."'4q..G.v..~...t.b.e._t6Mc....WHe ...+.......">q.V...........I..Db..........&..R\Y...I6YL..n.q.....K......JA.....G.._...0C.#.3-..'...#....Le(.....wn2.I.T7m..N.pmV...6.p..K..|...?..?.93).b.=....bN....m.............~*..zx..,WSB.0#L.h....{&..M..r.e....V..*..V.2........@..9W0..a!..B...e..R..r5.J1.)O..@....d....Og.......H&.5.P8.WvutG.`....D...y.<..F.E..Ud]s.p...4.[.|........6...H....>....]<...4..qL.........0F..Qm...D~%Di...59......[.6..:...9|..`p..j..k6.9</td></tr>
</table>

C:\Users\user\AppData\Local\Temp\~DF484B5CB7814FD922.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.2872161188737101
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	1F6B4CF8D0D36B82640F4BA97F7869D6
SHA1:	BD0531260F0463959E43B708F0CE3EDAE0C05FAB
SHA-256:	8AFB6CDE69CE1B20C85CDC01E3C3E023C346107690CFDD26571897558F361303
SHA-512:	0CCF4CF8525CF556B4E7121F0AB99F0A212E7AF9CB7EE2B330CB0C60CCD50F61C00C7E5357D6689591EB74A8BE2FECA86E9CB99E3449E754E43E73BDDAF37 56
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF607C8DFA7F9E2A87.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34421
Entropy (8bit):	0.3593606785968559
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwY9lwI9l2G9l2m9l/KM:kBqoxKAuvScS+LFX+KIK7kj5t
MD5:	70D92F0BC6DF9AF22D087F135B7F95C6
SHA1:	8C1A8278F19E9B2C033DBF81A046D6E61C3E784D
SHA-256:	E17C7561D8A6B50FAD72EC83B195A37F5AC720A5A9CC70F27DE46909230D833C
SHA-512:	BF6BE73B4AFC7FC8048C06DCB23024CCABBB0AD84703D09830A6F6D143E5DCAA6200582B16B7F54BD17E168673E7462E71AEE4DD4243354D9956E164D82B13 9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DF607C8DFA7F9E2A87.TMP	
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

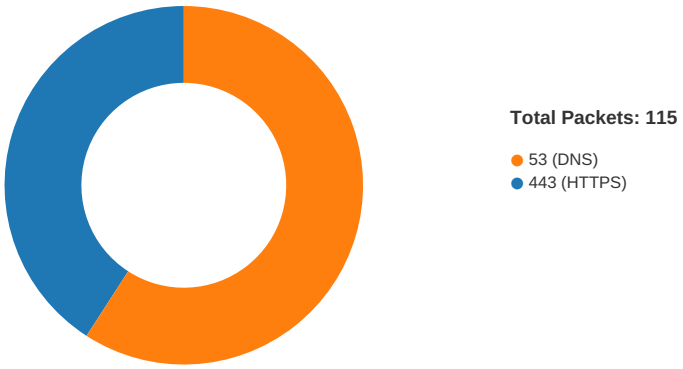
C:\Users\user\AppData\Local\Temp\~DFDA36E2CF24B83655.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13125
Entropy (8bit):	0.5414705796914808
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loE3F9loEV9lWEBfba5UfbaLVaLKaLE9U9fbaL3z:kBqoIE+EgEBDa5UDaLVaLKaLE9U9DaLD
MD5:	117D2CC7B34A7AE6272AFBDCED268642
SHA1:	283CFBB01C3C1246080DFA4C0217539BCF6B8167
SHA-256:	4048878A106D03C013E14488297814BFC451D39A0BF71469255AAF3434E9D7F6
SHA-512:	A86B4F468E3DDE10A6E67B7F566C81B53BD8A4A66F773CCCF2080376816720DE0AF0CC5DFDCD47192906FAA0BF73A8D6606AEC2F164340D8FE349BC1557A345
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 02:31:10.452581882 CET	49708	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.452611923 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.496467113 CET	443	49708	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.496510029 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.496635914 CET	49709	443	192.168.2.3	104.26.12.36

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 02:31:10.496649981 CET	49708	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.502234936 CET	49708	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.502331018 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.543520927 CET	443	49708	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.543555975 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.545130014 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.545190096 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.545294046 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.545344114 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.545600891 CET	443	49708	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.545649052 CET	443	49708	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.545670986 CET	49708	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.545720100 CET	49708	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.578891993 CET	49708	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.579061031 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.587168932 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.587219000 CET	49708	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.587380886 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.620170116 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.620212078 CET	443	49708	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.620251894 CET	443	49708	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.620285034 CET	443	49708	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.620316029 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.620342970 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.620417118 CET	49708	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.620426893 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.620452881 CET	49708	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.621927977 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.622206926 CET	49708	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.628357887 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.628402948 CET	443	49708	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.628428936 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.628465891 CET	443	49708	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.628554106 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.628611088 CET	49708	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.663223028 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.706890106 CET	443	49708	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.707348108 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.725363016 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.725465059 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.725497961 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.725537062 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.725573063 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.725622892 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.725630999 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.725933075 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.725972891 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.726013899 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.726030111 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.726056099 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.726100922 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.726157904 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.727088928 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.727212906 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.728964090 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.728996992 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.729039907 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.729060888 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.729125023 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.729224920 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.729295969 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.730218887 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.730269909 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.730319977 CET	49709	443	192.168.2.3	104.26.12.36

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 02:31:10.730345964 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.731183052 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.731214046 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.731273890 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.731296062 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.731735945 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.731827974 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.732211113 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.732242107 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.732297897 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.732323885 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.732768059 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.732810974 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.732844114 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.732867002 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.733644962 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.733685970 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.733714104 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.733745098 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.733792067 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.734164000 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.734203100 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.734246016 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.734288931 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.735075951 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.735121965 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.735147953 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.735172987 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.735209942 CET	49709	443	192.168.2.3	104.26.12.36
Feb 24, 2021 02:31:10.735799074 CET	443	49709	104.26.12.36	192.168.2.3
Feb 24, 2021 02:31:10.735848904 CET	443	49709	104.26.12.36	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 02:31:02.134903908 CET	50200	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:02.194127083 CET	53	50200	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:02.941442966 CET	51281	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:02.993671894 CET	53	51281	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:03.878885984 CET	49199	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:03.930748940 CET	53	49199	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:04.506453991 CET	50620	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:04.565588951 CET	53	50620	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:04.691340923 CET	64938	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:04.745354891 CET	53	64938	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:06.406050920 CET	60152	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:06.458194017 CET	53	60152	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:08.028995037 CET	57544	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:08.078066111 CET	53	57544	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:09.286500931 CET	55984	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:09.350085020 CET	53	55984	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:10.380068064 CET	64185	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:10.442702055 CET	53	64185	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:14.274760962 CET	65110	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:14.335056067 CET	53	65110	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:15.285407066 CET	58361	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:15.334127903 CET	53	58361	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:19.985769987 CET	63492	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:20.036031961 CET	53	63492	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:21.208309889 CET	60831	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:21.260076046 CET	53	60831	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:24.525091887 CET	60100	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:24.574295998 CET	53	60100	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:26.527470112 CET	53195	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 02:31:26.586698055 CET	53	53195	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:27.450217962 CET	50141	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:27.501142979 CET	53	50141	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:28.586872101 CET	53023	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:28.635696888 CET	53	53023	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:30.116183996 CET	49563	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:30.167900085 CET	53	49563	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:36.019351959 CET	51352	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:36.103404999 CET	53	51352	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:38.497538090 CET	59349	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:38.548839092 CET	53	59349	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:39.499543905 CET	57084	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:39.561734915 CET	53	57084	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:40.063585997 CET	58823	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:40.141583920 CET	53	58823	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:40.547781944 CET	57084	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:40.608172894 CET	53	57084	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:41.377285957 CET	58823	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:41.434948921 CET	53	58823	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:41.645049095 CET	57084	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:41.694087982 CET	53	57084	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:42.820919991 CET	58823	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:42.881659985 CET	53	58823	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:43.556452990 CET	57568	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:43.560024023 CET	50540	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:43.610340118 CET	53	50540	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:43.629554033 CET	53	57568	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:43.681735039 CET	57084	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:43.743755102 CET	53	57084	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:44.826018095 CET	58823	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:44.846801996 CET	54366	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:44.877548933 CET	53	58823	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:44.898092985 CET	53	54366	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:47.675172091 CET	57084	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:47.732661963 CET	53	57084	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:48.986982107 CET	58823	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:49.048038960 CET	53	58823	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:51.882623911 CET	53034	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:51.941235065 CET	53	53034	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:52.043083906 CET	57762	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:52.106306076 CET	53	57762	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:52.925265074 CET	53034	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:52.984061956 CET	53	53034	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:53.016654015 CET	57762	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:53.068566084 CET	53	57762	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:53.938536882 CET	53034	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:53.997539997 CET	53	53034	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:54.032243967 CET	57762	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:54.092566967 CET	53	57762	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:55.987698078 CET	53034	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:56.044977903 CET	53	53034	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:56.081679106 CET	57762	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:56.146308899 CET	53	57762	8.8.8.8	192.168.2.3
Feb 24, 2021 02:31:57.787350893 CET	55435	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:31:57.836565971 CET	53	55435	8.8.8.8	192.168.2.3
Feb 24, 2021 02:32:00.319601059 CET	53034	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:32:00.319820881 CET	57762	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:32:00.378611088 CET	53	53034	8.8.8.8	192.168.2.3
Feb 24, 2021 02:32:00.383064985 CET	53	57762	8.8.8.8	192.168.2.3
Feb 24, 2021 02:32:12.983354092 CET	50713	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:32:13.035459042 CET	53	50713	8.8.8.8	192.168.2.3
Feb 24, 2021 02:32:41.214827061 CET	56132	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:32:41.289500952 CET	53	56132	8.8.8.8	192.168.2.3
Feb 24, 2021 02:32:55.327452898 CET	58987	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 02:32:55.381863117 CET	53	58987	8.8.8.8	192.168.2.3
Feb 24, 2021 02:33:05.319782019 CET	56579	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:33:05.382313013 CET	53	56579	8.8.8.8	192.168.2.3
Feb 24, 2021 02:33:31.581924915 CET	60633	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:33:31.635411024 CET	53	60633	8.8.8.8	192.168.2.3
Feb 24, 2021 02:33:37.277899981 CET	61292	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:33:37.345736980 CET	53	61292	8.8.8.8	192.168.2.3
Feb 24, 2021 02:34:11.513262033 CET	63619	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:34:11.593604088 CET	53	63619	8.8.8.8	192.168.2.3
Feb 24, 2021 02:34:12.080183029 CET	64938	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:34:12.141688108 CET	53	64938	8.8.8.8	192.168.2.3
Feb 24, 2021 02:34:12.784651995 CET	61946	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:34:12.835294962 CET	53	61946	8.8.8.8	192.168.2.3
Feb 24, 2021 02:34:13.200692892 CET	64910	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:34:13.249723911 CET	53	64910	8.8.8.8	192.168.2.3
Feb 24, 2021 02:34:13.735620022 CET	52123	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:34:13.809444904 CET	53	52123	8.8.8.8	192.168.2.3
Feb 24, 2021 02:34:14.539700031 CET	56130	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:34:14.600574017 CET	53	56130	8.8.8.8	192.168.2.3
Feb 24, 2021 02:34:15.242712975 CET	56338	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:34:15.302308083 CET	53	56338	8.8.8.8	192.168.2.3
Feb 24, 2021 02:34:16.503912926 CET	59420	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:34:16.561539888 CET	53	59420	8.8.8.8	192.168.2.3
Feb 24, 2021 02:34:17.301743984 CET	58784	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:34:17.392858982 CET	53	58784	8.8.8.8	192.168.2.3
Feb 24, 2021 02:34:17.819847107 CET	63978	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:34:17.871792078 CET	53	63978	8.8.8.8	192.168.2.3
Feb 24, 2021 02:35:57.214157104 CET	62938	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:35:57.263014078 CET	53	62938	8.8.8.8	192.168.2.3
Feb 24, 2021 02:35:58.356678963 CET	55708	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:35:58.425540924 CET	53	55708	8.8.8.8	192.168.2.3
Feb 24, 2021 02:35:59.343054056 CET	56803	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:35:59.402821064 CET	53	56803	8.8.8.8	192.168.2.3
Feb 24, 2021 02:35:59.944483995 CET	57145	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:36:00.006732941 CET	53	57145	8.8.8.8	192.168.2.3
Feb 24, 2021 02:36:00.829632044 CET	55359	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:36:00.912097931 CET	53	55359	8.8.8.8	192.168.2.3
Feb 24, 2021 02:37:01.186105013 CET	58306	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:37:01.248966932 CET	53	58306	8.8.8.8	192.168.2.3
Feb 24, 2021 02:39:05.397289038 CET	64124	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:39:05.446048021 CET	53	64124	8.8.8.8	192.168.2.3
Feb 24, 2021 02:39:35.790736914 CET	49361	53	192.168.2.3	8.8.8.8
Feb 24, 2021 02:39:35.859466076 CET	53	49361	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 24, 2021 02:31:10.380068064 CET	192.168.2.3	8.8.8.8	0xeeb4	Standard query (0)	templatelab.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 24, 2021 02:31:10.442702055 CET	8.8.8.8	192.168.2.3	0xeeb4	No error (0)	templatelab.com		104.26.12.36	A (IP address)	IN (0x0001)
Feb 24, 2021 02:31:10.442702055 CET	8.8.8.8	192.168.2.3	0xeeb4	No error (0)	templatelab.com		104.26.13.36	A (IP address)	IN (0x0001)
Feb 24, 2021 02:31:10.442702055 CET	8.8.8.8	192.168.2.3	0xeeb4	No error (0)	templatelab.com		172.67.69.154	A (IP address)	IN (0x0001)
Feb 24, 2021 02:35:57.263014078 CET	8.8.8.8	192.168.2.3	0xb229	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

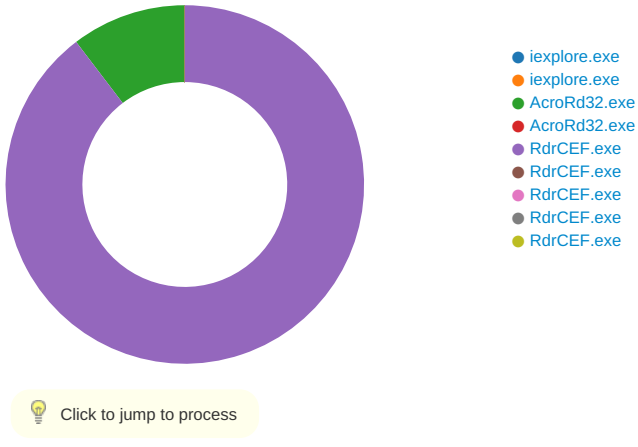
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 24, 2021 02:31:10.545190096 CET	104.26.12.36	443	192.168.2.3	49709	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Jul 18 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Sun Jul 18 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Feb 24, 2021 02:31:10.545649052 CET	104.26.12.36	443	192.168.2.3	49708	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Jul 18 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Sun Jul 18 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 4600 Parent PID: 792

General

Start time:	02:31:08
Start date:	24/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff740aa0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
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

Analysis Process: iexplore.exe PID: 2024 Parent PID: 4600

General

Start time:	02:31:08
Start date:	24/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4600 CREDAT:17410 /prefetch:2
Imagebase:	0x330000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
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

Analysis Process: AcroRd32.exe PID: 4792 Parent PID: 2024

General

Start time:	02:31:10
Start date:	24/02/2021
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' /o /eo /l /b /ac /id 2024
Imagebase:	0xe0000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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	1165C3	CreateDirectoryExW
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rtzb8pn_r4v8rg_2t0.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 | delete | read control | synchronize	device	synchronous io non alert | non directory file | delete on close	success or wait	1	12EA85	NtCreateFile
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	13AE05	CreateDirectoryW
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	1A83C8	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	1A83C8	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	1A83C8	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1A83C8	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	1A83C8	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	1A83C8	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R14wfdhi_r4v8rh_2t0.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	12EA85	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	3	12EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1l6o0iu_r4v8ri_2t0.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	12EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1a8vzpi_r4v8rj_2t0.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	12EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rkphwr6_r4v8rk_2t0.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	12EA85	NtCreateFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\Device\NamedPipe\AIPC_SRV\AcroSBL_2024_4792	unknown	1040	success or wait	3	145549	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\System\Acrobatbrokerserverdispatchercpp789	success or wait	1	12CF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\NoTimeOut	success or wait	1	12D41D	NtCreateKey

Analysis Process: AcroRd32.exe PID: 3636 Parent PID: 4792

General

Start time:	02:31:12
Start date:	24/02/2021
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 /o /eo /l /b /ac /id 2024
Imagebase:	0xe0000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	false
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	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: 4816 Parent PID: 4792

General

Start time:	02:31:37
Start date:	24/02/2021
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:	0xfc0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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	2	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	3	10B59E2	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	5	10C83E5	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	26	10C8447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	165	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	3	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	3	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	2	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	16	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	3	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	6	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	3	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	success or wait	11	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	end of file	3	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	1621	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	3	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	30	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	2	10B59E2	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	10B59E2	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	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	4	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	2	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	1	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	2	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	1	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	2	10B59E2	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	1	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	success or wait	2	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	1	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	1	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	27	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	end of file	1	10B59E2	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	10B59E2	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	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	success or wait	2	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	end of file	2	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	8	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	120	10B59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	2	10B59E2	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	10B59E2	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	10B59E2	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	134	10B59E2	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	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	25	10B59E2	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	10B59E2	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	98	10B59E2	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	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	16	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	2	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	1	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	success or wait	1	10B59E2	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	10B59E2	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	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	end of file	1	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	7	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	163	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	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	10B59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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	10B59E2	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	10B59E2	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	10B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	success or wait	2	10B59E2	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	10B59E2	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	4	unknown	1	10C83E5	ReadFile

Analysis Process: RdrCEF.exe PID: 6164 Parent PID: 4816

General

Start time:	02:31:44
Start date:	24/02/2021
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=1700,14431000459877472766,9177081831552403983,131072 --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=9047234563143899772 --mojo-platform-channel-handle=1732 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0xfc0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 6568 Parent PID: 4816

General

Start time:	02:31:45
Start date:	24/02/2021
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=1700,14431000459877472766,9177081831552403983,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=13126402487251577759 --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=13126402487251577759 --renderer-client-id=2 --mojo-platform-channel-handle=1752 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xfc0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7

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

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 6668 Parent PID: 4816

General

Start time:	02:31:48
Start date:	24/02/2021
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=1700,144310004598774 72766,9177081831552403983,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=13365710013370324663 --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=13365710013370324663 --renderer-client-id=4 --mojo-platform-channel-handle=1944 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xfc0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 7100 Parent PID: 4816

General

Start time:	02:31:53
Start date:	24/02/2021
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=1700,144310004598774 72766,9177081831552403983,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=15977986577334180066 --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=15977986577334180066 --renderer-client-id=5 --mojo-platform-channel-handle=2164 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xfc0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis