ID: 358572
Sample Name: Send-Data-City_Center_Waco_Project_Report-_#9073955_942 (1).pdf
Cookbook: defaultwindowspdfcookbook.jbs
Time: 21:21:41
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

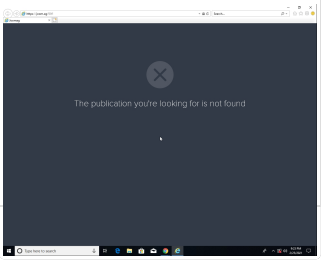
Analysis Report Send-Data-City_Center_Waco_Project_…

Overview

General Information

Sample Name:	Send-Data-City_Center_Waco_Project_Report-_#9073955_942 (1).pdf
Analysis ID:	358572
MD5:	dbfaf169fa1ba4c…
SHA1:	49602a3acf1bf41..
SHA256:	5a53c07a8d9d58..
Infos:	

Most interesting Screenshot:



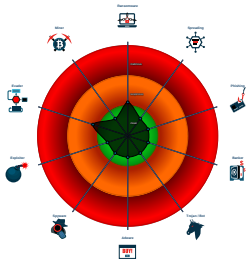
Detection

Score:	22
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

- Machine Learning detection for samp…
- Contains functionality to access load…
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- PDF has an OpenAction (likely to la…

Classification



Analysis Advice

No malicious behavior found, analyze the document also on other version of Office / Acrobat

Uses HTTPS for network communication, use the 'Proxy HTTPS (port 443) to read its encrypted data' cookbook for further analysis

Startup

- **System is w10x64**
- AcroRd32.exe (PID: 7072 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\Send-Data-City_Center_Waco_Project_Report-_#9073955_942 (1).pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 7148 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\Send-Data-City_Center_Waco_Project_Report-_#9073955_942 (1).pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 6208 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6684 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1712,3132147786374165480,18202446835359099183,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=3943672393428629375 --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=3943672393428629375 --renderer-client-id=2 --mojo-platform-channel-handle=1724 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6556 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1712,3132147786374165480,18202446835359099183,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=13600008762938548 38 --mojo-platform-channel-handle=1740 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 4240 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1712,3132147786374165480,18202446835359099183,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=511033688939430806 --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=511033688939430806 --renderer-client-id=4 --mojo-platform-channel-handle=1856 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 744 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1712,3132147786374165480,18202446835359099183,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=6159965884629463958 --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=6159965884629463958 --renderer-client-id=5 --mojo-platform-channel-handle=1860 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
  - iexplore.exe (PID: 2740 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' https://joom.ag/9JYI MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
    - iexplore.exe (PID: 4720 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2740 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

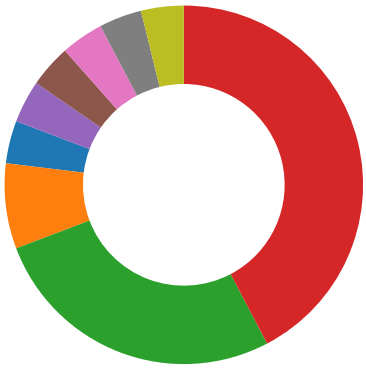
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Compliance
- Networking
- System Summary
- Data Obfuscation
- 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

AV Detection:

Machine Learning detection for sample

Compliance:

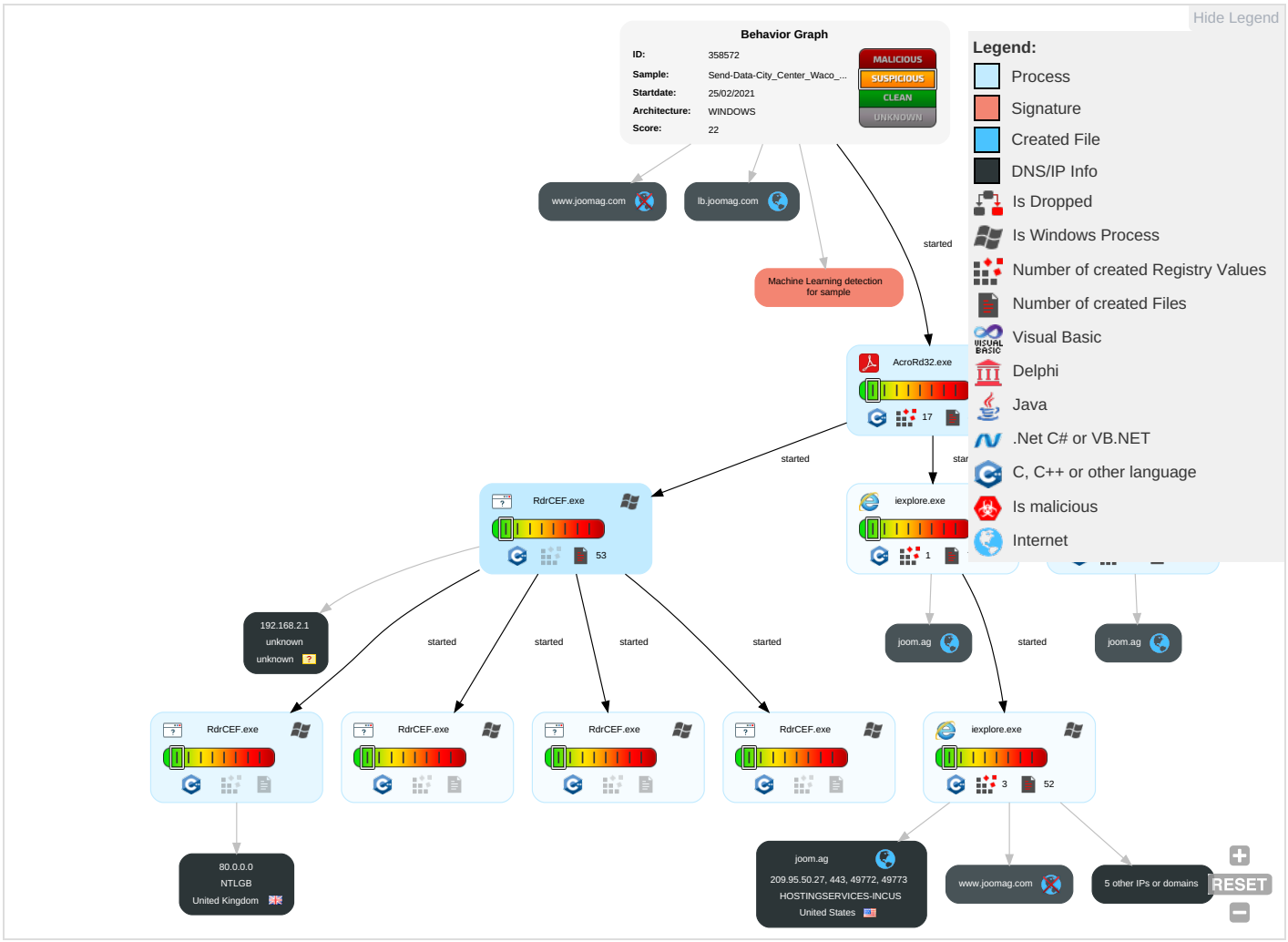
Uses new MSVCR Dlls

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 1	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

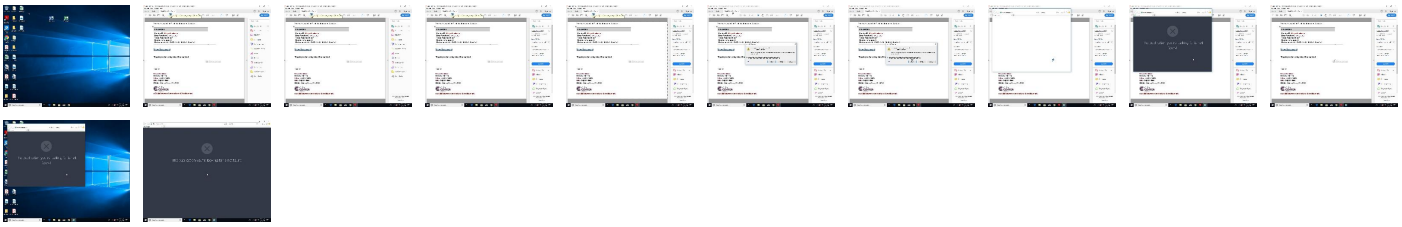
Behavior Graph

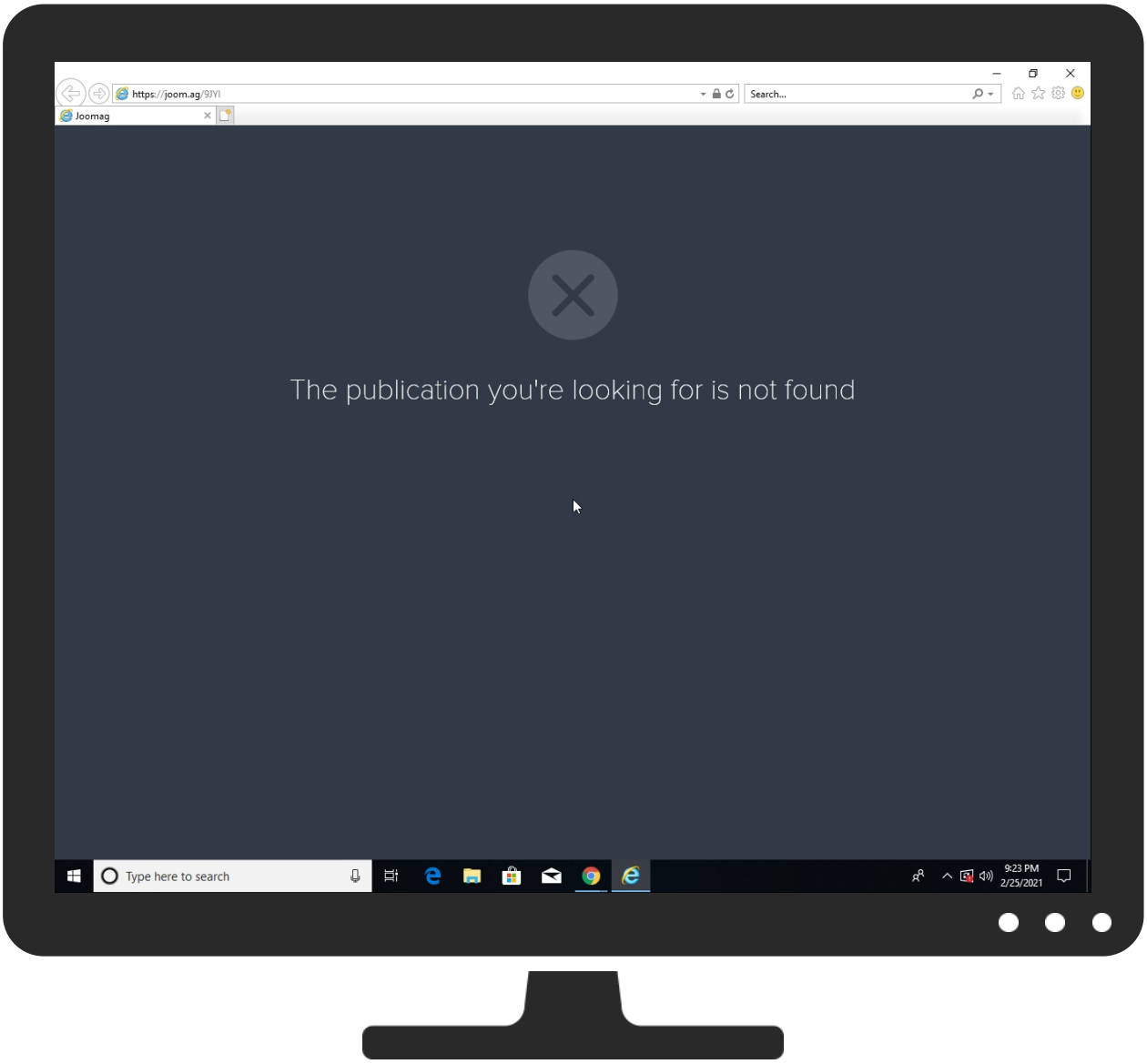


Screenshots

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
Send-Data-City_Center_Waco_Project_Report-_#9073955_942 (1).pdf	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
joom.ag	0%	Virustotal		Browse
bam-cell.nr-data.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://www.pdfescape.com8g~_)	0%	Avira URL Cloud	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://https://joom.ag/9JYI)	0%	Avira URL Cloud	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	0%	Avira URL Cloud	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/1.0/l4XRg	0%	Avira URL Cloud	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://https://www.radpdf.com)/Creator(PDFescape	0%	Avira URL Cloud	safe	
http://https://www.pdfescape.com)/CreationDate(D:20210222193218	0%	Avira URL Cloud	safe	
http://https://joom.ag/9JYIRoot	0%	Avira URL Cloud	safe	
http://www.dynaforms.com	0%	URL Reputation	safe	
http://www.dynaforms.com	0%	URL Reputation	safe	
http://www.dynaforms.com	0%	URL Reputation	safe	
http://https://joom.ag1)	0%	Avira URL Cloud	safe	
http://https://joom.ag/ZJYI)	0%	Avira URL Cloud	safe	
http://cipa.jp/exif/1.0/_1	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/_1	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/_1	0%	URL Reputation	safe	
http://https://joom.agt	0%	Avira URL Cloud	safe	
http://https://joom.ag	0%	Avira URL Cloud	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/y	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	0%	Avira URL Cloud	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://www.radpdf.com	0%	URL Reputation	safe	
http://https://www.radpdf.com	0%	URL Reputation	safe	
http://https://www.radpdf.com	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/p	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
lb.joomag.com	209.95.50.27	true	false		high
joom.ag	209.95.50.27	true	false	• 0%, Virustotal, Browse	unknown
www.joomag.com	unknown	unknown	false		high
use.typekit.net	unknown	unknown	false		high
p.typekit.net	unknown	unknown	false		high
js-agent.newrelic.com	unknown	unknown	false		high
bam-cell.nr-data.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://joom.ag/9JYI	true		unknown

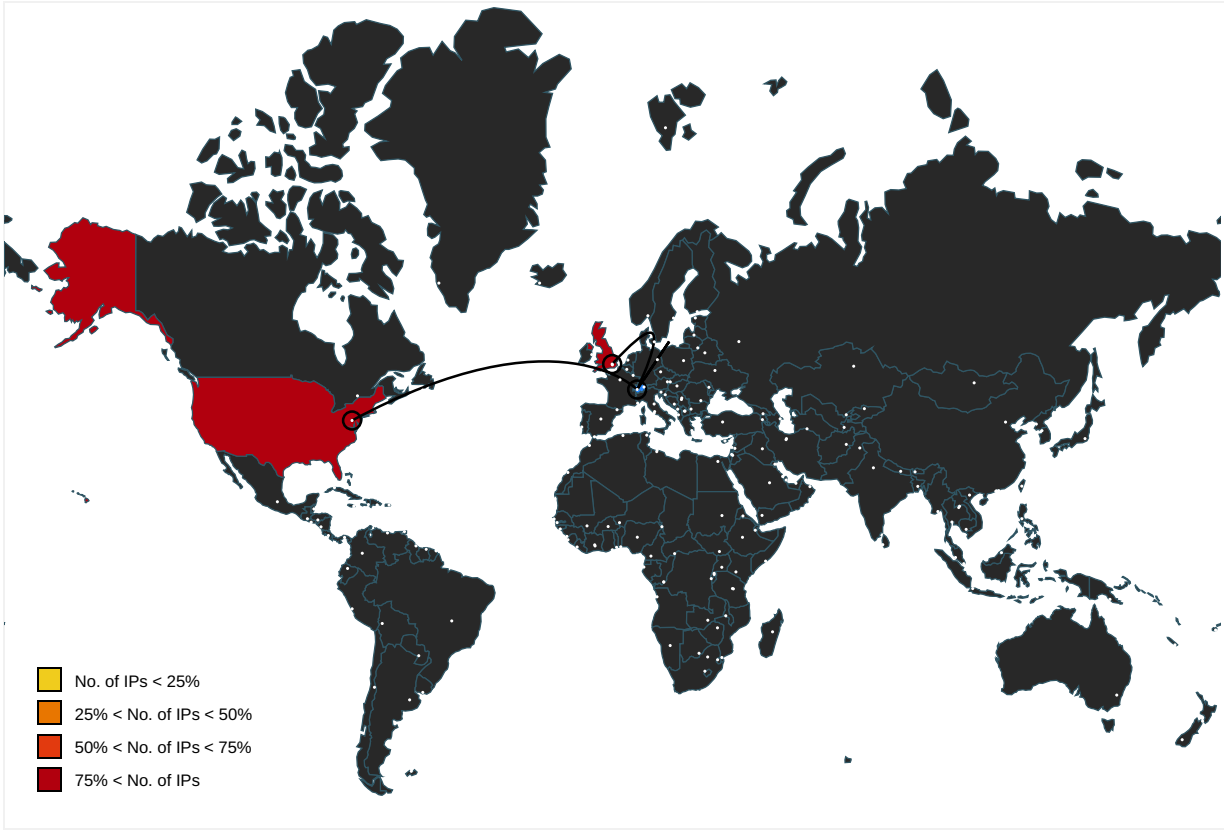
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.pdfescape.com	AcroRd32.exe, 00000001.00000002.811679843.000000000A6B1000.00000004.00000001.sdmp, AcroRd32.exe, 00000001.00000002.813758482.000000000B5B1000.00000004.00000001.sdmp, AcroRd32.exe, 00000001.00000002.813000356.000000000B26F000.00000004.00000001.sdmp, Send-Data-City_Center_Waco_Project_Report-_#9073955_942 (1).pdf	false		high
http://www.aiim.org/pdfa/ns/schema#	AcroRd32.exe, 00000001.00000002.813758482.000000000B5B1000.00000004.00000001.sdmp	false		high
http://https://www.pdfescape.com8g~_)	AcroRd32.exe, 00000001.00000002.811601438.000000000A600000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	AcroRd32.exe, 00000001.00000002.799506231.0000000007BD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://typekit.com/eulas/00000000000000000000148a0	olb8zpk[1].js.19.dr	false		high
http://https://joom.ag/9JYI)	AcroRd32.exe, 00000001.00000002.811679843.000000000A6B1000.00000004.00000001.sdmp, Send-Data-City_Center_Waco_Project_Report-_#9073955_942 (1).pdf	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfe/ns/id/(2	AcroRd32.exe, 00000001.00000002.813954896.000000000B671000.00000004.00000001.sdmp	false		high
http://www.amazon.com/	msapplication.xml.18.dr	false		high
http://cipa.jp/exif/1.0/	AcroRd32.exe, 00000001.00000002.813954896.000000000B671000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	AcroRd32.exe, 00000001.00000002.799506231.0000000007BD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.twitter.com/	msapplication.xml5.18.dr	false		high
http://typekit.com/eulas/00000000000000000000148a6	olb8zpk[1].js.19.dr	false		high
http://typekit.com/eulas/00000000000000000000148a4	olb8zpk[1].js.19.dr	false		high
http://typekit.com/eulas/00000000000000000000148a2	olb8zpk[1].js.19.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.aiim.org/pdfa/ns/type#	AcroRd32.exe, 00000001.00000002.813758482.000000000B5B1000.00000004.00000001.sdmp	false		high
http://https://use.typekit.net/af/e0b8be/00000000000000000000148a6/23/	olb8zpk[1].js.19.dr	false		high
http://https://api.echosign.com	AcroRd32.exe, 00000001.00000002.807459695.00000000092BE000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	AcroRd32.exe, 00000001.00000003.796965422.000000000B5D9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.npes.org/pdfx/ns/id/	AcroRd32.exe, 00000001.00000002.813954896.000000000B671000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/drm/default	AcroRd32.exe, 00000001.00000002.799506231.0000000007BD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://use.typekit.net/af/3ba24d/00000000000000000000148a0/23/	olb8zpk[1].js.19.dr	false		high
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	AcroRd32.exe, 00000001.00000002.799506231.0000000007BD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://joom.ag/9JYI	{51AA8483-77A7-11EB-90EB-ECF4BBEA1588}.dat.18.dr	false		unknown
http://www.aiim.org/pdfa/ns/extension/	AcroRd32.exe, 00000001.00000002.813758482.000000000B5B1000.00000004.00000001.sdmp	false		high
http://cipa.jp/exif/1.0/1.0/l4XRg	AcroRd32.exe, 00000001.00000002.813954896.000000000B671000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/type#R	AcroRd32.exe, 00000001.00000002.813758482.000000000B5B1000.00000004.00000001.sdmp	false		high
http://www.reddit.com/	msapplication.xml4.18.dr	false		high
http://www.osmf.org/subclip/1.0	AcroRd32.exe, 00000001.00000002.799506231.0000000007BD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/property#	AcroRd32.exe, 00000001.00000002.813758482.000000000B5B1000.00000004.00000001.sdmp	false		high
http://ns.useplus.org/ldf/xmp/1.0/	AcroRd32.exe, 00000001.00000002.813758482.000000000B5B1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.nytimes.com/	msapplication.xml3.18.dr	false		high
http://www.aiim.org/pdfa/ns/id/	AcroRd32.exe, 00000001.00000002.813954896.000000000B671000.00000004.00000001.sdmp	false		high
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	AcroRd32.exe, 00000001.00000002.813758482.000000000B5B1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/layout/anchor	AcroRd32.exe, 00000001.00000002.799506231.0000000007BD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	AcroRd32.exe, 00000001.00000002.813758482.000000000B5B1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfe/ns/id/	AcroRd32.exe, 00000001.00000002.813954896.000000000B671000.00000004.00000001.sdmp	false		high
http://https://use.typekit.net/af/42fca5/00000000000000000000148a4/23/	olb8zpk[1].js.19.dr	false		high
http://https://www.radpdf.com)/Creator(PDFescape	Send-Data-City_Center_Waco_Project_Report-_#9073955_942 (1).pdf	false	• Avira URL Cloud: safe	low
http://https://www.pdfescape.com)/CreationDate(D:20210222193218	Send-Data-City_Center_Waco_Project_Report-_#9073955_942 (1).pdf	false	• Avira URL Cloud: safe	low
http://https://use.typekit.net/af/bc719c/00000000000000000001499c/23/	olb8zpk[1].js.19.dr	false		high
http://https://joom.ag/9JYIRoot	{51AA8483-77A7-11EB-90EB-ECF4BBEA1588}.dat.18.dr	false	• Avira URL Cloud: safe	unknown
http://www.dynaforms.com	Send-Data-City_Center_Waco_Project_Report-_#9073955_942 (1).pdf	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://joom.ag1)	AcroRd32.exe, 00000001.00000002.814287929.000000000B74A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://joom.ag/ZJYI)	AcroRd32.exe, 00000001.00000002.811679843.000000000A6B1000.00000004.00000001.sdmp, Send-Data-City_Center_Waco_Project_Report-_#9073955_942 (1).pdf	false	• Avira URL Cloud: safe	unknown
http://https://use.typekit.net/af/3d81f6/00000000000000000000148a2/23/	olb8zpk[1].js.19.dr	false		high
http://https://use.typekit.net/af/1eef01/00000000000000000000148ac/23/	olb8zpk[1].js.19.dr	false		high
http://https://p.typekit.net/p.gif	olb8zpk[1].js.19.dr	false		high
http://cipa.jp/exif/1.0/_1	AcroRd32.exe, 00000001.00000002.813954896.000000000B671000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://joom.agt	AcroRd32.exe, 00000001.00000002.814287929.000000000B74A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.youtube.com/	msapplication.xml7.18.dr	false		high
http://https://joom.ag	AcroRd32.exe, 00000001.00000002.813758482.000000000B5B1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://typekit.com/eulas/00000000000000000000148ac	olb8zpk[1].js.19.dr	false		high
http://www.aiim.org/pdfa/ns/field#	AcroRd32.exe, 00000001.00000002.813758482.000000000B5B1000.00000004.00000001.sdmp	false		high
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	AcroRd32.exe, 00000001.00000002.799506231.0000000007BD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.wikipedia.com/	msapplication.xml6.18.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/y	AcroRd32.exe, 00000001.00000002.813413074.000000000B4B5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://typekit.com/eulas/00000000000000000001499c	olb8zpk[1].js.19.dr	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	AcroRd32.exe, 00000001.00000002.813413074.000000000B4B5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.live.com/	msapplication.xml2.18.dr	false		high
http://www.quicktime.com.Acrobat	AcroRd32.exe, 00000001.00000002.799506231.0000000007BD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 00000001.00000002.807459695.00000000092BE000.00000004.00000001.sdmp	false		high
http://https://www.radpdf.com	AcroRd32.exe, 00000001.00000002.811679843.000000000A6B1000.00000004.00000001.sdmp, AcroRd32.exe, 00000001.00000002.813758482.000000000B5B1000.00000004.00000001.sdmp, Send-Data-City_Center_Waco_Project_Report-_#9073955_942 (1).pdf	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/p	AcroRd32.exe, 00000001.00000002.813413074.000000000B4B5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
80.0.0.0	unknown	United Kingdom		5089	NTLGB	false
209.95.50.27	unknown	United States		32780	HOSTINGSERVICES-INCUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358572
Start date:	25.02.2021
Start time:	21:21:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Send-Data-City_Center_Waco_Project_Report-_#9073955_942 (1).pdf
Cookbook file name:	defaultwindowspdfcookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	SUS
Classification:	sus22.winPDF@17/78@9/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .pdf • Found PDF document • Find and activate links • Security Warning found • Close Viewer

Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.107.253.254, 204.79.197.200, 13.107.21.200, 52.255.188.83, 40.88.32.150, 52.147.198.201, 104.42.151.234, 13.64.90.137, 168.61.161.212, 23.54.113.182, 23.32.238.123, 23.32.238.129, 23.32.238.113, 23.32.238.136, 104.43.139.144, 51.104.139.180, 104.43.193.48, 52.155.217.156, 20.54.26.129, 2.20.142.209, 2.20.142.210, 92.122.213.247, 92.122.213.194, 88.221.62.148, 23.32.238.210, 23.32.238.192, 23.37.33.211, 151.101.2.110, 151.101.66.110, 151.101.130.110, 151.101.194.110, 162.247.243.147, 162.247.243.146, 51.11.168.160, 152.199.19.161 • Excluded domains from analysis (whitelisted): e6653.dscf.akamaiedge.net, arc.msn.com.nsatc.net, tls12.newrelic.com.cdn.cloudflare.net, acroipm2.adobe.com, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, use-stls.adobe.com.edgesuite.net, a122.dscd.akamai.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, www.bing.com, dual-a-0001.a-msedge.net, acroipm2.adobe.com.edgesuite.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, t-9999.fb-t-msedge.net, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, blobcollector.events.data.trafficmanager.net, t-ring.t-9999.t-msedge.net, cs9.wpc.v0cdn.net, au.download.windowsupdate.com.edgesuite.net, e4578.dscb.akamaiedge.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, iecvlist.microsoft.com, go.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, p.typekit.net-v3.edgekey.net, ie9comview.vo.msecnd.net, f4.shared.global.fastly.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, t-ring.msedge.net, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, armmf.adobe.com, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, a1988.dscg1.akamai.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:22:30	API Interceptor	11x Sleep call for process: RdrCEF.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
80.0.0.0	vUp5vjYOoL.exe	Get hash	malicious	Browse	
	2021-02-15__Mail-Degroof-Petercam_ENC.docx	Get hash	malicious	Browse	
	InformaAllSecure_Enhanced_Health_Safety_Standards_2021.docm	Get hash	malicious	Browse	
	Swift.pdf.jar	Get hash	malicious	Browse	
	0001.jar	Get hash	malicious	Browse	
	FedEx-Shipment-90161131174.jar	Get hash	malicious	Browse	
	FedEx-Shipment-61821461149.jar	Get hash	malicious	Browse	
	FedEx-Shipment-8161131174.jar	Get hash	malicious	Browse	
	agenciatributaria5668.vbs	Get hash	malicious	Browse	
	Statement for T10495.jar	Get hash	malicious	Browse	
	Statement for T10495 - 18-01-21 15-23.jar	Get hash	malicious	Browse	
	TREKSTA 2021 Business Plan..exe	Get hash	malicious	Browse	
	SPEPAY13012021-20-00000009.pdf.exe	Get hash	malicious	Browse	
	SPEPAY13012021-20-00000009.pdf.exe	Get hash	malicious	Browse	
	2EB0.tmp.exe	Get hash	malicious	Browse	
	muddydoc.exe	Get hash	malicious	Browse	
	RQMofd68Ad.exe	Get hash	malicious	Browse	
	http://https://awattorneys-my.sharepoint.com/:b:/p/fgalante/EcRfEpzLM_tOh_Roewbwm9oB4JarWh_30QaPZLGUdNbnuw?e=4%3aqmwocp&at=9	Get hash	malicious	Browse	
	http://quickneasyrecipes.co	Get hash	malicious	Browse	
	http://https://dck12-my.sharepoint.com:443/:b:/g/personal/tanya_mckelvin_k12_dc_gov/EbGhLtD47K1Cl18cC--Ad0sBxiRFwsui9s7PYb2eA-FMZg?e=4%3arCBWhd&at=9__;JQ!!P4oOa0cl!xjyiOci-WnHuSljf0v9YP9XHTo1mHg1DdlnrlGltn8ysOUKeJHjzL7gjiYG6nZ8pLQ$	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
joom.ag	http://https://t.yesware.com/tt/ae9851ab7b578dad1289f08bbf450624f7ae3a45/2ee42987f58d2f32bb36ff11a00dd921/2f4e7e35c28c3b7f4958904f5584a915/joom.ag/2VFC	Get hash	malicious	Browse	• 50.22.50.142
	http://https://joom.ag/eoFC	Get hash	malicious	Browse	• 50.22.50.142
	http://https://joom.ag/3wFC	Get hash	malicious	Browse	• 50.22.50.142
	http://https://joom.ag/qJFC	Get hash	malicious	Browse	• 50.22.50.142
	http://https://joom.ag/BRFC	Get hash	malicious	Browse	• 50.22.50.142
	http://https://joom.ag/yGUC	Get hash	malicious	Browse	• 50.22.50.142
	http://https://joom.ag/uZDC	Get hash	malicious	Browse	• 50.22.50.142
	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fjoom.ag%2f9BjC&c=E,1,FEe77b6JikuybnZvWSPMtboj3kXPvfEd96gDBaPRghPkeeNMaiZ00lHXg2CVBvQXKcXw8950i4VfR2mq9wGKru5dQgG78LY4-xUIpbnM8tgzj5oG4pdo95PFgkNDQw,,&typo=1%3e	Get hash	malicious	Browse	• 50.22.50.142
	http://https://joom.ag/iFjC	Get hash	malicious	Browse	• 50.22.50.142
	http://https://joom.ag/iFjC	Get hash	malicious	Browse	• 50.22.50.142
	http://https://joom.ag/ZLwC	Get hash	malicious	Browse	• 50.22.50.142
	http://https://joom.ag/Q2sC	Get hash	malicious	Browse	• 50.22.50.142
	http://https://joom.ag/kjjC	Get hash	malicious	Browse	• 50.22.50.142
	http://https://link.edgepilot.com/s/7e6cc1d7/tCVFnxZt8kmwbWjFZXIplA?u=https://joom.ag/rIjC	Get hash	malicious	Browse	• 50.22.50.142

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HOSTINGSERVICES-INCUS	6d0000.exe	Get hash	malicious	Browse	• 50.31.252.28
	_130_WHAT_is.html	Get hash	malicious	Browse	• 103.198.0.111
	http://https://files03.tchspt.com/temp/torbrowser-install-win64-10.0.1_en-US.exe	Get hash	malicious	Browse	• 107.182.23 9.251
	FvDtfcmdF2.exe	Get hash	malicious	Browse	• 103.198.0.111

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NTLGB	vUp5vjYOoL.exe	Get hash	malicious	Browse	• 80.0.0.0
	2021-02-15__Mail-Degroof-Petercam_ENC.docx	Get hash	malicious	Browse	• 80.0.0.0
	InformaAllSecure_Enhanced_Health_Safety_Standards_2021.docm	Get hash	malicious	Browse	• 80.0.0.0
	kF1JPCXvSq.dll	Get hash	malicious	Browse	• 82.12.157.95
	wEcncyxrEe	Get hash	malicious	Browse	• 213.48.143.199
	Swift.pdf.jar	Get hash	malicious	Browse	• 80.0.0.0
	0001.jar	Get hash	malicious	Browse	• 80.0.0.0
	FedEx-Shipment-90161131174.jar	Get hash	malicious	Browse	• 80.0.0.0
	FedEx-Shipment-61821461149.jar	Get hash	malicious	Browse	• 80.0.0.0
	FedEx-Shipment-8161131174.jar	Get hash	malicious	Browse	• 80.0.0.0
	agenciatributaria5668.vbs	Get hash	malicious	Browse	• 80.0.0.0
	Statement for T10495.jar	Get hash	malicious	Browse	• 80.0.0.0
	Statement for T10495 - 18-01-21 15-23.jar	Get hash	malicious	Browse	• 80.0.0.0
	TREKSTA 2021 Business Plan..exe	Get hash	malicious	Browse	• 80.0.0.0
	SPEPAY13012021-20-00000009.pdf.exe	Get hash	malicious	Browse	• 80.0.0.0
	SPEPAY13012021-20-00000009.pdf.exe	Get hash	malicious	Browse	• 80.0.0.0
	2EB0.tmp.exe	Get hash	malicious	Browse	• 80.0.0.0
	muddydoc.exe	Get hash	malicious	Browse	• 80.0.0.0
	RQMofd68Ad.exe	Get hash	malicious	Browse	• 80.0.0.0
	http://https://awattorneys-my.sharepoint.com/:b:/p/fgalante/EcRfEpzLM_tOh_Roewbwm9oB4JarWh_30QaPZLGUdNbnuw?e=4%3aqmwocp&at=9	Get hash	malicious	Browse	• 80.0.0.0

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	SecuriteInfo.com.Variant.Bulz.362300.21634.dll	Get hash	malicious	Browse	• 209.95.50.27
	44252636284259300000.dat.dll	Get hash	malicious	Browse	• 209.95.50.27
	RFQ.xlsx	Get hash	malicious	Browse	• 209.95.50.27
	counters.dll	Get hash	malicious	Browse	• 209.95.50.27
	mferreira@itpros.us.com.pff.HTM	Get hash	malicious	Browse	• 209.95.50.27
	Xero from mashreqbank.htm	Get hash	malicious	Browse	• 209.95.50.27
	Sprint Note tod.friedman@americansignaturefurniture.com 81454 AM .html	Get hash	malicious	Browse	• 209.95.50.27
	Outllook_Membership_Update.html	Get hash	malicious	Browse	• 209.95.50.27
	Payment.html	Get hash	malicious	Browse	• 209.95.50.27
	vmail_6512365134_7863.html	Get hash	malicious	Browse	• 209.95.50.27
	Remittance advice.htm	Get hash	malicious	Browse	• 209.95.50.27
	gQcKVtx6h0.dll	Get hash	malicious	Browse	• 209.95.50.27
	qt1dVk6hrj.dll	Get hash	malicious	Browse	• 209.95.50.27
	PnzVGXpv4C.dll	Get hash	malicious	Browse	• 209.95.50.27
	TcNpJ6Lerr.dll	Get hash	malicious	Browse	• 209.95.50.27
	doTCeuxsZh.dll	Get hash	malicious	Browse	• 209.95.50.27
	P1ON2FMKtb.dll	Get hash	malicious	Browse	• 209.95.50.27
	83dLkz7iFE.dll	Get hash	malicious	Browse	• 209.95.50.27
	Zh9kAls1Tz.dll	Get hash	malicious	Browse	• 209.95.50.27
	iyLA8EXSBg.dll	Get hash	malicious	Browse	• 209.95.50.27
37f463bf4616ecd445d4a1937da06e19	radu.capra-Payment.xlsb	Get hash	malicious	Browse	• 209.95.50.27
	Xeros from condor.htm	Get hash	malicious	Browse	• 209.95.50.27
	SecuriteInfo.com.Trojan.GenericKDZ.73162.30196.exe	Get hash	malicious	Browse	• 209.95.50.27
	mferreira@itpros.us.com.pff.HTM	Get hash	malicious	Browse	• 209.95.50.27
	Xero from mashreqbank.htm	Get hash	malicious	Browse	• 209.95.50.27
	Rep_#_475.xlsm	Get hash	malicious	Browse	• 209.95.50.27
	YjnpgCvRAb.exe	Get hash	malicious	Browse	• 209.95.50.27
	211094.exe	Get hash	malicious	Browse	• 209.95.50.27
	8zjdEb5sF0.dll	Get hash	malicious	Browse	• 209.95.50.27
	Sleaford Medical Group.exe	Get hash	malicious	Browse	• 209.95.50.27
	UAE CONTRACT SUPPLY.exe	Get hash	malicious	Browse	• 209.95.50.27
	CustomerStatement.exe	Get hash	malicious	Browse	• 209.95.50.27
	Payment.html	Get hash	malicious	Browse	• 209.95.50.27
	EmployeeAnnualReport.exe	Get hash	malicious	Browse	• 209.95.50.27
	Customer Statement.exe	Get hash	malicious	Browse	• 209.95.50.27
	Remittance advice.htm	Get hash	malicious	Browse	• 209.95.50.27
	Customer Statement.exe	Get hash	malicious	Browse	• 209.95.50.27

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Order-10236587458.exe	Get hash	malicious	Browse	• 209.95.50.27
	RFQ_1101992827736663556272772 88.exe	Get hash	malicious	Browse	• 209.95.50.27
	EMG 3.0.exe	Get hash	malicious	Browse	• 209.95.50.27

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):	615
Entropy (8bit):	5.684217252183559
Encrypted:	false
SSDEEP:	12:vDRM9Y3ZiExxDRM9eUdRZiEfDRM9E7RZiE:7fAEXNUdKELR7KE
MD5:	EA82252C85CF65B1DE5205A215C14B88
SHA1:	C6CCE813536299C1C8807162F9EB0E28582F7216
SHA-256:	D91DCF24BB4CB823BC16E1637C80471801CBD274999FD4E6472CE5D07C53E03E
SHA-512:	3A06FF79BE7A872D712E33E12FBF15B42309C1D8A1A5307F2D5CFA2395B8EC2F0E4A41FD6830D4CFAB0122DFF2FF6F8C7B5440445B80590AD9AA79609249C04
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ....2../....."#.D.....A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....*.I..... .0\r..m.....M..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ..H`2../....."#.D..b....A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo..... ...).....0\r..m.....M..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ..".2../....."#.D.....A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	522
Entropy (8bit):	5.596945211146141
Encrypted:	false
SSDEEP:	6:mi9NqEYOFLvEkwV8Be7Ywcr1TK6tYi9NqEYOFLvEkf+Cci8Be7Ywcr1TK6tnLi9w:V9zE9PQl9z/+ni9PQE9zvKKHCi9PQ+M
MD5:	1C798AEF9E49AE0DA938D5ACA698FF35
SHA1:	7AF2CD9048FAAA253A1F2E46CBBDEBBAF8F40665
SHA-256:	7922F490EE022E5245C7D2EF00661CD3D637609905143B495C123DB4C9C5C501
SHA-512:	6D52F7780C0FB3856106DD8FD28A03348C0F75C5F8EAB3AC7805491B4AD22D1DE648BF00CD318F5D76AD8D54815ECFB07ED7F60C742E36E3A121E1FC0117B8E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .5..1../....."#.Dn.....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....".a.....0\r..m.....,....._keyht tps://rna-resource.acrobat.com/init.js ...Q2../....."#.D.....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....0\r..m.....,....._keyhttps://rna-resource.acrobat.co m/init.js .$.v2../....."#.D.....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....<.c.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	738
Entropy (8bit):	5.635000447366235
Encrypted:	false
SSDEEP:	12:DyeRVFAFjVFAFulUo6j8yeRVFAFjVFAFg8XnYlUo6jQpyeRVFAFjVFAFBlUo6j:tB4v4uSBYB4v4foSBSB4v4BSB
MD5:	8F3D76D6B58DF71D566932890356E832
SHA1:	D06907192022648BB5D2BEE0144A880342BDAE5A
SHA-256:	A1886F75BBB4FCE800ED5955A85B668D1E5292A59A89A5B06580D92811EBC81F
SHA-512:	68E96D984748F8DC6A28A60B335131A70CBD0D50F187699798E04888F9EFF48041F3D9453A66EDEBBC91D8A6E37B473B2F4A7E016BB16C7E1DFFAF79824C07E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
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 ..I.2../.....''#.D.....A..hvDO.N.t@... ..n.*..... ....A..Eo.....A..Eo.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/ selector.js ..._2../.....''#.D).`....A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....i.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked -send/js/plugins/tracked-send/js/home-view/selector.js .N..2../.....''#.D.....A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....9.....

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):	464
Entropy (8bit):	5.652615208170962
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5Rsn9A0iWulHyA1TK6tlNtVYOFLvEWdFCi5RsVWHiWulHyA1a:IbRkiDE9AFWussfbRkiDbCWussc
MD5:	3927AF9F876AEA86471256D4ED25B14D
SHA1:	BF07EF978360648349346CE29D08491289904D50
SHA-256:	58F549E1BD72FF6C0A19FAE81528D9F4A35613A8990DD89815EEFF750240CAC7
SHA-512:	0129CD88137D0F26D723A0DCA859B6E6E02030A691132336BF41E28155A8DD7B9C71332442C661288D38D06B172E0FF8A995E7CA5943458FDF40EE4199A7171B
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 .c1.2../.....''#.D^.....A..8 P..a...R..Y....7.@..2Dm{ ..A..Eo.....A..Eo.....0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js ...c2../.....'' #.D&Vp....A..8 P..a...R..Y....7.@..2Dm{..A..Eo.....A..Eo.....j.8B.....

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):	5.581940373979228
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVuSTnGkVyh9PT41TK6tGO:pyixRuFkV41TEv
MD5:	AD7E7BC95D56F0D3C804A24F5172A01E
SHA1:	7C23C8E17A9D94F50A0DED99189E7C1C5B4E42C9
SHA-256:	AE800A55F398A047F708585BB1DAEEEC95F1F27E51924EC5A8192D0FEB6FCAB8
SHA-512:	B5D17AEBFFFDF39A9E9117166F86C5103C0F41E904EA4D5BAEAE2700C2C72C6AAB9FF2ABDC6288D0F1A888F182A161CE28AB90BDAFFF5994365D00202405519
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ..2.2../.....''#.D.6.....Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo. .....@.I.....

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):	5.634402013489074
Encrypted:	false
SSDEEP:	6:mvYOFLvEWdhwjQq7r+bNLZIl6P41TK6t:0RhkBv+hLZC
MD5:	5637EA07C984203222AB908131B2075C
SHA1:	5DD061BE694953DEE5D0485884CC4FBA981CEABD
SHA-256:	C72DEA99B4F5CBDFF790C28EC222A80AE7E8EAEACAF75EAA764C82B7BEA639C8
SHA-512:	C170C4BF323E046DE34435139621793FEEE02A77FAEF718D4F775BB7866F2122DEFF3A7EEDDB89CA0DAC978C9AD49555A7E02CFA0D463EBF60BF5F448B793B2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ..G.2../.....''#.D.....A.].>....uUf..N...k.....c..l.A..Eo.....A. .Eo.....[.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	209

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
Entropy (8bit):	5.5118553663883345
Encrypted:	false
SSDEEP:	3:m+lZd8RzYOCGLvHkWBGKuKjXKX7KoQRA/KVdKLuVn6algaypvGFcyxMtv9EWm1T2:mJYOFLvEWdGQRQOdQlhYF6g1TK6tS
MD5:	7AFE639E30EB9B83A244D9D80287068A
SHA1:	EC4CE5ECA05E7A24B97F28FA40B2A20E078085CC
SHA-256:	1688513F9597377CB34CF30736560561D1C25FCABB5451096AF1963BCBC36F53
SHA-512:	DF2B792E755985023634AB51BFF119A8FAC62E62996AF862E4A104169B964C9AEA5D3F313C3EB8C6A3EE751E4D565F05559C0336C0E0A10277C43754FAF2A966
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ...2../....."#.DbL.....A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo. .....S.zj.....

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):	5.6348808044349985
Encrypted:	false
SSDEEP:	12:Z5MHtMuR/EQB5MbatMuR/EbB5MUVMuR/EJY:ZSauR/EQBSbFuR/EVSUCuR/EJY
MD5:	8510850DD6FD537B926F957E8654D688
SHA1:	85EAD22C8354C15A106BFC6AD32155C164802D46
SHA-256:	8958BC5F2EB7C3C3568D34898AE1769FB11DFB8728C1E4479A420C84FA55DC4E
SHA-512:	279E0D89AF3FCCE936B6A44B88D9E408C9437A0BD27E3DBFB56E78D6E44099B1AD5A4F702C416C34162949AE3B3EE9E1AA5F474FF7330FFADB7DC157E5E5DA AA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .`..1../....."#.DY.....A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....3c./.....0\r..m.....3.... <lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ..$Q2../....."#.D.....A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....y.....0\r..m.....3....<lb... ._keyhttps://rna-resource.acrobat.com/base_uris.js ...v2../....."#.D.....A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....q.T%.....

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):	5.545314354711959
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtu/HB4CMby0zBUKSAA1TK6tOB:pRqHB45beM
MD5:	D23F84B4EF4897D85EAA4FD12C082631
SHA1:	C25E6E7B45531633B73138741208AE814CA369EB
SHA-256:	B5082E6C46F894BC918570DCCAA3BA25699A510E73A464E31321D7BD513FC0D6
SHA-512:	FBB59B496CDD14EC9ED4816ED4AFD2BB13B64E15DBA2D0173693CB50BFF92A42BA4767FF8DD5829578BD7204044458DD3C4F63EFBF5B434332B1368120CD42 2
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ....2../....."#.D.....AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....A. .Eo.....4.d.....

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):	5.5929649291744195
Encrypted:	false
SSDEEP:	12:KkXxKMSCvpuvtUlj0lakXxKMSCvXt/vtUl3QikXxKMSCv+vtUl:KkXxiCRuvWwlakXxiCZvW3bkXxiCmvW
MD5:	0DCE83EF48AB3F8547CF524CD91922DD
SHA1:	5247AB22B0C3E515B08F8C8F067B6ED75502951F
SHA-256:	B958F4A99579B4CFF048591D1E4CAC736BA550B35B0AE981F6357AAD3A425901
SHA-512:	2F749C7DD34434075151BA4698F5BFBA4EF6C43F371F73BE6678753380255C8034CE7D596863267DF4ECCA5899CC7EF3956D12770325B4BFE5D7A92E230460B3
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ._..1../....."#.DV.....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....0\r..m.....1.....5..._ keyhttps://rna-resource.acrobat.com/plugins.js .7!Q2../....."#.DV.....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....K2.5.....0\r..m.....1.....5..._keyhttps://rna-resource.acrobat.com/plugins.js ...v2../....."#.DI.....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):	561
Entropy (8bit):	5.55490502242737
Encrypted:	false
SSDEEP:	6:mkl9YOFLvEWsfOLovyM+VY1TK6tR+kl9YOFLvEWsfOLVKW/yM+VY1TK6tJkl9YO/:5h6OLfkjBh6OLZGksh6OLZRQk
MD5:	262C665B20680099769D75777E0DC68C
SHA1:	90D1CFFEC116F94526E389E481D428931C47F814
SHA-256:	063E846FB234FB13A2DA96ACB6DF24A8C6D15C29025B543CC422FA1587539A4B
SHA-512:	3D121CD31A5B75484F7E08D84BE3D7EC87D26F689631688FE51A247BEF028E80F69234E0CF6D0F91210F1994361F31E476406D6CECF8467AAA5201181809A9D3
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .`..2../....."#.D.2.....A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....`o\u.....0\r..m.....;..I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ...[2../....."#.D;.N....A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....?..z.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ...2../....."#.DSY.....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):	732
Entropy (8bit):	5.620775413690981
Encrypted:	false
SSDEEP:	12:URVFAFjVFAFLRwSeKaTLnKRVFAFjVFAFQrwSeKaTLnlRVFAFjVFAFhwSeKaTLnB:UB4v4NwzXLnKB4v4QrwzXLnlB4v4hwzz
MD5:	CC100E0AC45238AC0614A3CDAE43F702
SHA1:	3CC688C1C9C55AFCF290FB0909231FAAE26E9C77
SHA-256:	37F236FE7DAA5ED44217ACAC4356DD54AA8BED25F7BF862756A006DFC1C9F538
SHA-512:	1086F5637502FFD8BC10FA3251A035455F9E2C72442D502E0973DE2C4AC0DB776FE587AAB0FBC2432D0F426E7F0F2791532B143773084B7F68EB39E9C8BFF7C8
Malicious:	false
Preview:	0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js ....2../....."#.D.....A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....r.....0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/home-view/plugin.js .[.`2../....."#.D..e....A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....9.C.....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 ...2../....."#.D.....A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....J.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.417262657268614
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXuMdf11TK6tv9/:BsR2EseLB
MD5:	EFF8255B817B917D52ECD6440BEABDB3
SHA1:	09E125271664BC5571043F1D74AE19F074053EC3
SHA-256:	57AB402BFA3571A4403AA9C7026E54F197B979D4DC296B033F2C463D47384B22
SHA-512:	A087AD362AFC70C307FCA93B9E4767B7F303E34329FDEC61572380261605CF4334C3BFDE9952E8604781FDC4426B8D61E5E5D915CD8AB68689D8751A92063F58
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ....2../....."#.D<.....A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo.....]....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.61815825631675
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQTwCBGL4B7OhKlvA1TK6tHO:RbR16VCu4BJkNO
MD5:	0AE309079C7178ECDBFEB27844EF8A3B
SHA1:	231502EF2695213637CF7889965D117DD87AC757
SHA-256:	D0B6414989E7CD8467BF9917502C763F34A1BBCFCB93F732118EAD79895D201A
SHA-512:	D7876212DA54DA2300A0359DD927DB55A7F408207CE51268ACA400693E29802C6361B3F7BDB7A2AC7D53DBD839A3FF3CD3F44C5355F55D2D4EB32CC9A9782CE
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0	
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js .W..2../....."#.D.V.....A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....2 rk.....

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):	5.597721320225041
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVuuhGeRQdFt1TK6tll/l:B2geRHRQyi0Dl
MD5:	98CB58E46688CC77B696AF311AC7249E
SHA1:	A6CE5A2D1691971CBF7C20BF4FC43F62859A43D0
SHA-256:	BCA1EFF33A666B256707B7E5B17A595FA5CCC6B4A9DCE00A7771011490CA0239
SHA-512:	74B50CA5721874980B01A6607E33BA58CEC7FE0EE8439EA01C484A1CDC5C36582C05933FDBE10E35C1C534138F0BE408027148FF8F7B23537F165D21D9240773
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .)..2../....."#.D5.....A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A. .Eo.....Q.....

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):	618
Entropy (8bit):	5.634753205402192
Encrypted:	false
SSDEEP:	12:WyeRlsx1rz6t1wTyeRlSP6t1wFEyeRlt6t1wS:WJKz6fwTJ66fwFEJV6fw
MD5:	3537D00BD24ABD54EA291A14CF9B2904
SHA1:	84C3D801A8E538454397D4BFB2321D087A106CEC
SHA-256:	9391DF248801E348A84C524F8F562B22E9F500309D5AB23ED8421CE189CEB284
SHA-512:	B2DDACCBBB8AAF60A34A3515CA38FA11A09A2D6D9F2264084C3AFE2C577BABBD54C73B1AD199804D586E3CE56E9DB1821F54CEE470F904EECC16172ADAF0 D9DC
Malicious:	false
Preview:	0\r..m.....N.../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ./..2../....."#.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 ...^2../....."#.D..U....A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo .....lN9.....0\r..m.....N.../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..c.2../....."#.D%.....A.t\a.....x5.'OuE.C..@.....x..A..Eo..... .....A..Eo.....g.l.....

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):	5.541212398536384
Encrypted:	false
SSDEEP:	3:m+lKcv8RzYOCGLvHkWBGKuKjXKoyNH/KPWFvRDllVpkJTJNqww6U+5m1TK5ktSt:mnYOFLvEWdhwyubkJTrqwK+41TK6tS
MD5:	2F9C35CD39268A486BD7EF725C2821E1
SHA1:	C25FFEF1601B5F06767710C21A03761D48BB9148
SHA-256:	B94B349734D751108020FC8F4CE01F2BF2893E655B667B575B16E3446A15875D
SHA-512:	BE942BEA3204E1B557005E0F6DB37B664179C0A2CF11AC7BE40B60CB8454605692EDCDA059636416A848106A215AB0298328294300A6E457CF7CE752E057CF73
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .n..2../....."#.D.+.....A.....7...o..a=.98l.....(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):	690
Entropy (8bit):	5.647732920353794
Encrypted:	false
SSDEEP:	12:/RrROk/hqfLEARrROk/1HpfLEd3lRrROk/ND7YfLEF:/PJ/Q4APJ/Vp4dVPJ/ND7Y4F
MD5:	3D73D83898FA351ADC2DE3C04D872DA1
SHA1:	B61D9D97B66B3A232DB45A5E76CDCB9A09BA52B3

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0	
SHA-256:	407475D432143047539A89FAD7A4942E909F5A1C168044CA8A578E2CE98CDABB
SHA-512:	8873675BB064192990227EEB2D22EE4E5A4CABBD01BC25709AD6CA893194EDD484D38027A4836189B75635A9FA71B8633107F015DEE85FDA51C5D2651E863E8
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .]..2../....."#.Dzp.....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .W.]2../....."#.D.U....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....M.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .P=.2../....."#.D.....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	558
Entropy (8bit):	5.650252775482185
Encrypted:	false
SSDEEP:	6:mmDEYOFLvEWXIoKl111QPLr1TK6tBNMmDEYOFLvEWXIxCkS1QPLr1TK6tGEmDEY3:xqTDuCPLnrNjqTtkSCPLngqTbpCPLnN
MD5:	DAC04D32755B802ECA3F87A641972254
SHA1:	183F35DE0F04C65E55B6A590922F00194812F11D
SHA-256:	BEAEE857B99D05B616D759CD51CFA0BF97DDA4C51AEE26890DA08F43EE96E1E8
SHA-512:	E4485C5EAACB4D68EF03C720C433751715927511ADA89CAD7F0AA117F9A3015393877C48A1CBBDF20C55F3D0D3FBE1EFA3E5145EA7BFD8E2AA39F9847D9882B0
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ....2../....."#.D.&.....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....-_WW.....0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ...[2../....."#.D.N....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....v..o.....0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .F..2../....."#.D.R.....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....JV.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	621
Entropy (8bit):	5.647938852370718
Encrypted:	false
SSDEEP:	6:m52YOFLvEWdMAuuzsEJ41TK6tI/252YOFLvEWdMAuWuJzsEJ41TK6tTlE52YOFL7:zRMYsDm/jRMQwsDRRM7+3sDc
MD5:	FE35140F89E38785890B67A9E8F52D40
SHA1:	FB36A9C9D9474E2128CCDBA43F7E8A0B3832F298
SHA-256:	67DFD5F8FAAC850A18D215BE2256D8105632D554E6F065DFCA8E7273B7087780
SHA-512:	34439203B44950A2B163ABE8F29A93D0EAE8A26D4EE2C90F486EF72AEF85C6C778EACF33630B7B5EBF4888F54556AA742A45AB54EA68126EA97ABC87090FD446
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .fD.2../....."#.D.....A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .E._2../....."#.D._`....A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....r.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ....2../....."#.D.....A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....].....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	630
Entropy (8bit):	5.637062379811689
Encrypted:	false
SSDEEP:	12:6lJRdNFoMzRClJRR2FoMAGlJRZml2FoMa:YtFoMaSFoMAsycFoM
MD5:	26FB0E0C092878209693BCEDF039114A
SHA1:	B78A4C3E69E884FED8409BF3A71EBF7F4F890FF5
SHA-256:	A34B9036B20B999405F036ED67822FA0796B54B274AC605CC1DCD98B1C24B4D7
SHA-512:	91DA831BB6E312C1342473DCD9A3648CCC5461BE754799688581A06EE08CE4CE285E7DEE0194AE95D402B88B0A76FD226926863CB205189BE794351FE0B7E16
Malicious:	false
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..F.2../....."#.D.....Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .M._2../....."#.D.x`....Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .W..2../....."#.D.....Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....v.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
File Type:	data
Category:	dropped
Size (bytes):	669
Entropy (8bit):	5.637155413542381
Encrypted:	false
SSDEEP:	12:F8hRrROk/Yh+e2d8hRrROk/Ihe2Rb8hRrROk/eHe2y:UPJ/E2MPJ/12RuPJ/e+2y
MD5:	B53C99E5B707ADDAC52A413A3E6A4F56
SHA1:	11ED18438A61E0B258043010DBAEF9EB2AEC6602
SHA-256:	EB285690FBD8CF87E143CEB49CA3FFC4212AE927E0147AE6DB77B0FA0061012C
SHA-512:	157BB7F883E90F07A4510875E6FE89AFE09310E0305495AF90E5088CC0FBBC28FEAD823843E7E0F732421424B9DBEE5EE9CFB0713DC97A954D7C46D1ADE3B3D F
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ....2../....."#.D.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 ...]2../....."#.DV.U....A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo....."..f.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .U8.2../..... "#.D.q.....A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	639
Entropy (8bit):	5.680112155177416
Encrypted:	false
SSDEEP:	12:ehRcmeirNJICkhRc4hQRrNJIC9/QhRcH6irNJICwN:ehQGJICkhpQ7JIC94hOJICwN
MD5:	7F1DF2D2A8A4EA77A1520B774345F34F
SHA1:	218C554E6A21C5D68E007CE2A592F33674BFAB08
SHA-256:	C97852876E469B3509F4F5BF17BE558A6973694AD974BCEBB17809484CAEB0F2
SHA-512:	AC02D3CD6EDF8DF4C9B5E1F29625EB2122FD0B152128D0AC13D69951C17FE642F546CAA57F42CD5983F8C929F6D1793C2EE014BD13DA16DAC660A14DBA0E9 B0
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..N.2../....."#.DU.....A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A. .Eo.....N.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ...^2../....."#.D..U....A.;"./N_.,.:C..2....9L.H...3:...A..Eo .....A..Eo.....b.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .Rf.2../....."#.DV.....A.;"./N_.,.:C..2....9L.H... 3:...A..Eo.....A..Eo.....:.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	624
Entropy (8bit):	5.636500047327169
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhu4ZDOZLzgm2d/1TK6t09t2OEYOFLvEWdrIhubm7hZLzgm2d/1M:0R2lKReStkRuReNRx/Re
MD5:	9A54853F0BD409A96A1D7F72B00D23D8
SHA1:	3992B2A856991DF8D078AF74F202BA422D2E4087
SHA-256:	6D78B86E4255B14BB43F6307B38173EEF0D616C8F38AD83313BB4496119E004F
SHA-512:	D7001F37F4FAD19E0F07C713E97261B169BC4D361D9254A0E5909126AA60A8D9D82363433F5015559C57C1C106CA778E3523E2A4B3E571128754B13DD7A4CB2E
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ....2../....."#.DG9.....AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.. ....I.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .[g]2../....."#.D."S....AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo..... .....A..Eo.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .r2.2../....."#.D.>.....AZ.Z}Q..4.o....0+..[|..n:*..U.W. A..Eo.....A..Eo.....R.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	564
Entropy (8bit):	5.617035403776032
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1K82kKf2kx56uvp1TK6tnMAElVYOFLvEW1KNCvvkx56uvp1TK6t6:6JJK82kE9KJJKkwUJJK2I2w
MD5:	DAED9BC662359B42612BF06F10E7A456
SHA1:	39FE068B162EAE4E5C7029754B6A8BFB49C50FC7
SHA-256:	CC898C0FA2B6CFE76A8ECAA9E97DA36420968B318B64EFD41D493180C54AC424

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0	
SHA-512:	1FFD53E2BBC0F7242A3BA5CE9A42C5D29B77F0E7233E44783CD7907E6F2F013538A38CCD382EF547732CE69A0CCBBB801F7D8100592A4A73CEE8B51E2F4285E 4
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ....1../....."#.D.&.....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo....._.....0\r..m.....< ...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...S2../....."#.D__2....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo....."h\.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .(.x2../....."#.D.m.....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):	5.653762026783217
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvu2kyhUDLYtmOZn1TK6t0H/:xRBJziDcFZLq
MD5:	5429EEE0028657613EE4D924C74E1795
SHA1:	28DA7018EC55FDD5F44674EAF52D26A67CF0BF67
SHA-256:	8260E13AFA617A26A872FB08BD691C0F714822FA18883A98E173F48A4D1C360E
SHA-512:	032BF6A1728F7505EB37FA815FD92232C2F8575106438A98DF3EA13E614C370F4762515F77CC38FB29900E6301827711E3097A265FD7D10AE9EF90C6D6691A3C
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ....2../....."#.D.....A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A ..Eo.....Ry.....

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):	5.63016099859997
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp7bclWgVPu1TK6tOesRPYOFLvEWIa7zp7QEVPu1TK6thH/2sZ:BPH5clWgcgZPH6EcfZPHbkc
MD5:	F49CDC8A626DB2E7F225CE60328D23FE
SHA1:	49B224729753CD97383FA2422FE347088751F6FA
SHA-256:	345D987B60CE8CFAB179DA8CF9355FB6C4690FA19A1590A9D745349468AB55AB
SHA-512:	DF9A6DBDEE4EC01A8DA8A3F7F781002DAADBAE47B14538404594FF1AA0BC334B42F2DE25AABF724655C6C91D360FCCE65409DF51960C7A4A375CD4D03E6B0 FC6
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ..#.1../....."#.Dp.....A...L...Im.@.....E.nW...IP..A..Eo.....A..E o.....i.6.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ..%Q2../....."#.D.....A...L...Im.@.....E.nW...IP..A..Eo.... .....A..Eo.....B.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ...v2../....."#.Dt.....A...L...Im.@.....E.nW...IP.. A..Eo.....A..Eo.....wX.....

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):	5.581314892597284
Encrypted:	false
SSDEEP:	6:mKPYOFLvEWdENU9QJXgC4k3lowiM3Y1TK6t:bJRT96Xgpk1Pr0
MD5:	FB9EFFC776624033596C3EF311595B3C
SHA1:	5DC26748DE81F954224B485CC82D90EA0EBC05E7
SHA-256:	ECA258CA351A5EB948F80F2DB868353AAEB560A247EDB979CF1E3C606B1770CB
SHA-512:	DB5892AE0AA2A42B4DB5DB8E7E26E3CE49E132D914BF4AAEDE366FD7E7FBEBCD804D91332082E4C1D2D1B4694B72FAF2CD78539B22CFE5AC1050494B292AE 633
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .IF.2../....."#.Do.....A...M....m+lS..e....<7.U.P8*.0K.A..Eo.....A..Eo. .....dSF.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Entropy (8bit):	5.616147164221497
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQJyjBRCh/41TK6tBN:XRc9wyDi/EJ
MD5:	A84AE9B4B282B974F0FA56D8B91C2A20
SHA1:	AAFEF218364322197ACD884D54F33F0F2847F798
SHA-256:	52E0B2367F3183E1375AC3EECF2DC5CB83B4914A8B39DFAF7476B0E19D230DCB
SHA-512:	131703F1B9ABDD38E35EE1A90A6B3842F54F305F510AC083F76A32B6D8E13ECCB8B7142D15978DAEB3E7C817AD65F007D70453CAFD6A072214F38F00975A975
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ...2../....."#.D.....APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.. ....8I.M.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	462
Entropy (8bit):	5.626581072578247
Encrypted:	false
SSDEEP:	12:bs6xRkixuN2LlF4nYrs6xRkiyCnu2LlF4n8:brxpxuwoYrxpywLo
MD5:	E46C6E9C6FC9085C301AB40FB5FC2C8E
SHA1:	49D7E273FF2DED44056CEAEA4C5A4EE7FACDE321
SHA-256:	5DD4B8F315C49A20A3F96BBFA8A440CB5B12F7525BE373467B1B15F1E3B913F9
SHA-512:	8DBA5C98F4BEED712041A1EFE5A61628240691FD22CBE41D4BEFC18B686981ECC4BCCE5A19C8FF50E67AEAAB367AD791EB56C45DD05BCC995DA1FAAC4718 EA8A
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ....2../....."#.D.....A.P...#4..l....5...5..).w.. .h.~..A..Eo. .....A..Eo.....s.....0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .LJ^2../....."#.Dp_V... .A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....!.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.53095771444754
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFveawCtTkiVCcu1isLK5m1TK5kt1t:mhYOFLvEWd/aFuesN941TK6t1ll
MD5:	AC9D82C6AD322EDC35C084FF3497E63D
SHA1:	298F4009DDAD5F9ED05870F24BD0D581CE472BE5
SHA-256:	590A5131E8E4F20D4F7AF3B111DA26B84012237D4C5C15F62DE0E55035266702
SHA-512:	23750D64AEDFCB170BF12212B8A6B602F8D9BF75F1BAE8A988EC3DD5D96DBE496F6F6073F43DC3CC0129A6F18D792E48C0CCCD18A7CF917B13BBA52F40DBD 3F
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js .;..2../....."#.D.....A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A ..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.52811331906844
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQtrh+rjoBMqVd3G4K41TK6tU:2DRuR+rnB9Vd2k
MD5:	D10CA7A25A8E64C94A047CC8FB042459
SHA1:	B81CCE37F331EFE6D722476BADFC3C6C97AD10F4
SHA-256:	82762CCDF19EB745023F54CB430F7486A1CE6E7F437B9BF508E518BBC71E0394
SHA-512:	3AF83843FAF1F4C7BCE07A49D714F7A3F933E0289E7C8D8C07A1E0DB2903A4357795802272D971A0048C5105BC7910BD5E7BE673630A45F70579EDB831E2303E
Malicious:	false
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ..r.2../....."#.D.n.....A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.. .....C.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
File Type:	data
Category:	dropped
Size (bytes):	624
Entropy (8bit):	5.630982743711325
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9Q0w/cSNuA424r1TK6tkt2kqYOFLvEWd8CAd9Q2fCmuA424rP:+RQRS8rn3RQXkrnMRQ2jRIrnB
MD5:	0ACC0950A37DCC881208E547E36A7DB6
SHA1:	853C5D4DAB28944E9C0ED951731222BD5A768709
SHA-256:	2EB1F641116F19A3EA1033DDD97B30C94CC23CAA571DB4ED792D13201B6BDE55
SHA-512:	C21CCEF3F8428AA009E96A32013E3A740CD621E54FCC0B517C69AB483038901F0E2391D39503B704F8B2CB1D74347EBD01CEA2A54E23E2DB0191514DF024922
Malicious:	false
Preview:	0\r..m.....P...gT...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ....2../....."#.DxD.....A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....1=^.....0\r..m.....P...gT...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .wJ`2../....."#.D..c....A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....@.....0\r..m.....P...gT...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .O`.2../....."#.D~p.....A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....g.D.....

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):	5.551631075521991
Encrypted:	false
SSDEEP:	3:m+lS5Etla8RzYOCGLvHkWBGKuKjXKVRNUp/KPWFvXO/vRdKbg2iHio/Mm1TK5kt3:moXXYOFLvEWdENUAu0ruyC8n1TK6tt
MD5:	65EA1ED192944A70AFB304E088566A63
SHA1:	D9A81151B48D97325CD3C22B4D9080A825E3142E
SHA-256:	23425AEFE02FF0C0A8157FD26521D6430266172DB96DA1AD45F21400BF6D384E
SHA-512:	5351818B08BB104845515F84AAE3B8B13CFFE0A0C6FF169F08A937CEB05EE7DF65EE6D703A1C6D82380EE36F88BA27F4F843DB6429C1032427AAE8D061122D4
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .K..2../....."#.D.....A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....x.F.....

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):	663
Entropy (8bit):	5.6636391454954556
Encrypted:	false
SSDEEP:	12:nRrROk/VTmj/lXRrROk/VhJm8RrROk/VceMm:nPJ/ExPJ/s8PJ/eeh
MD5:	881218A82894A12972B7F0F113A44CD1
SHA1:	049A030B5C3BC3B5F8FFEF2D26539E8C31DC4DCE
SHA-256:	5AAFACE5A495E0034E1F12906E2A36DF6D0F4A6A890691010EA7F27CDF671F2B
SHA-512:	560AA9B81B538E1B1F59301792984BC2C2FE050DF913762532BA68A0ED4510EE96EA92A6536B2819826819973846B89BB5D0C081A152E2857B93BB1FDB26B400
Malicious:	false
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..Q.2../....."#.DV.....A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo..... .....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ...^2../....."#.D..U....A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....+.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..i.2../....."#.D.....A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....x.s.....

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):	5.567960078509128
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWuWDGAdm9741TK6tw:qxRcwSAdu7EW
MD5:	AEE7429194944A6C94E41B54E8067E1A
SHA1:	C10EAAF7077B0EE9857F4C7A64A0C35E08455A3C
SHA-256:	DD3D6A82CF9F44A81B312E5025D67D9590B341BD4F99CCE0A227CAA352881C94
SHA-512:	A4B5E2043E828559F85E622747B4ADCE4EDEB3768EF2A474A350BCD55BFB108149F4150162F078A4BF7B187A8FBDB064B5EFDD05B8B76EC4CD3FA771A640952 9
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0	
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js .x..2../....."#.Dq.....A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....c.....

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):	5.54261597302326
Encrypted:	false
SSDEEP:	6:mMOYOFLvEWdwAPVuQXwkTrJn1TK6tN9/l:2R16kpLT9/l
MD5:	EB9B4AD4C76C7506F4653E72003F5D43
SHA1:	9DE993086D73F2656407AB3D54889642273D0C09
SHA-256:	7E66985441E180AA2A70B13BFB22A6A526ED3DA3E7DF1FDDC5019D731FC0A556
SHA-512:	ACCC231183A15E44E23958552A034856EBAE0FE2E277895CF410CD3D53BA0C8F8DFC96975C30AE048E520CF237598AB0BF43B5C6675CF4814FEE912389454D8
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ....2../....."#.D'.....A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo.....^.kj.....

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):	5.6128533423405775
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQSQg6OzhcsBXIh1TK6tW:mxRBJQZ4ODB0Y
MD5:	AEEEC756FC7C1C2ADB4D86B9614EC9D9
SHA1:	F632BDECB555D646CC59022C59F613466384C98F
SHA-256:	EBB3EA22F73330DD0E486BB2E4B823B9C22FF896F4B21A80478ABEA0BF035407
SHA-512:	12AFEAB930DB620FD86689D0E1B55F84EA9E31F49D27114D9361B599A8022B9AFF9497B13B5354525D034192C39E7DAB3D8FC02F9A52DACB08F8F0BE5ECCE7D3
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ....2../....."#.D.....A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....*.....

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):	684
Entropy (8bit):	5.635811432383387
Encrypted:	false
SSDEEP:	12:3RrROk/sVcplRrROk/sZcZERrROk/sd+ch:3PJ/xplPJ/dKPJ/a
MD5:	D6571748A3628B18911B896E0D3AB6B8
SHA1:	B8100E4E553FEB3858EB4A6DC946B20E82181613
SHA-256:	821CD2911D172F848231F7147E18FE14ED35316DF3425515133B7120405E8FBA
SHA-512:	AB2BECD827E4D65FFBCAB4BEFD88F27A7D211E7F15CE4D0A46360575D21BFF6B3FE32B4BF1E88AC8663B3A4FFA967EC8CA82F7DC95C7F7701C2EB6B8F486DA40
Malicious:	false
Preview:	0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ..S.2../....."#.D.I.....A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....n|.....0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ..!^2../....."#.D..V....A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....U.NQ.....0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ....2../....."#.D.....A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	Maple help database
Category:	modified
Size (bytes):	1032
Entropy (8bit):	5.089070255065177
Encrypted:	false
SSDEEP:	24:28ZlTjsHYKMOYS+mRuzKNX/vAfeaL+AGbomX:28TQYKbZ9R+KNX/vAfeaLHGbLX
MD5:	A2791B105B843216FDB9263DB10CBDBB

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index	
SHA1:	6F4584EB36A4A605E67BE7701B1CFDFA81B061B5
SHA-256:	3EEF7B3C9EC6DBFC5DC57F080C40DD94E1C543DBF37B8711B36AA5886991DA19
SHA-512:	9E2CC6D5AC7EB8522D64E173F1FA58BEB1A614EBDD33E4228E13C79B1CDA27E328792161624B5217F0F4425D4912946A936C59BA858DD8747897DFF6CFD7F4E
Malicious:	false
Preview:	.....poy retne....).....T.....3.....w2../.....v...q....w2../.....C..M.....k.....#...(...k.....]...I.@fY2../.....@fY2../.....6<|.....h2../.....<...W..J..h2../..... ..oB*..h2../.....a.....h2../.....;.y~A...w2../.....P....V..w2../.....F..=z;...w2../.....o...w2../.....*....w2../.....2q.....w2../.....Gy.'.h...w2../.....k7A...w2../ .....:..N.A....w2../.....;/....w2../.....w2../.....P[. q..w2../.....,+..._#..w2../.....J..j.....w2../.....A?.2:...-.2../.....q..-.2../.....u\]..q.-.2../.....!...0.o.-.2 ../.....*.....-.2../.....o..k...-.2../.....^.~..z..-.2../.....[.i..%..-.2../.....+.{..'.-.2../.....@..x..-.2../.....*)....J:.-.2../.....&.S....-.2../.....MV3...-.2../.....+.U.!..V.- .2../.....D.4..-.2../.....~.,.4>..-.2../.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	292
Entropy (8bit):	5.16304080463964
Encrypted:	false
SSDEEP:	6:mNwpSAq2Pwkn2nKuAl9OmbnIFUtpewBhZmwPew6ezkwOwkn2nKuAl9OmbjLJ:h1vYfHAahFUtpRD/PRnz5JfHAaSJ
MD5:	B816BE5CA8C14F3FF9ED437ADF54F982
SHA1:	38287F875C90A46EABEAE26226D1891E2C184A5C
SHA-256:	C70650773B0E3A36A437D30003E25140C6AE81FF936C0013BC78015C937ECA5D
SHA-512:	6CCE4EDE99B74C62F77AB2BE3E01EAC82D688952E5CC3118A0218821BA4E702E5E04863FA96E7C9A3C7553A15354503076F576208688E05CA2F196A3AB6264AE
Malicious:	false
Preview:	2021/02/25-21:22:35.718 1970 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/02/25-21:22:35.719 19 70 Recovering log #3.2021/02/25-21:22:35.722 1970 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):	1310720
Entropy (8bit):	0.008399703044392193
Encrypted:	false
SSDEEP:	24:TmbsmbPXytHwytHwytHwytHwytHwytHwy:TmwmEHRHRHRHRHRHRH
MD5:	05C31564F5D129E37A363E150A042D4D
SHA1:	FA62CA0C75E503D2C5E83FE48A9846CD48FFF480
SHA-256:	64044EF0EAA6C2CCA1F6D5E32B8C1AD305D642A8AF7F91C89CACC2BF8642C5D1
SHA-512:	895CB367D69A3A2D619868DBDA6DA0EB5FFDC20D6B9B2740E7CAE3F9ED91F29BFB9DBA5FA68E72998E92AE68B66BAB551A53B48575B3CD1C27ABE3C923E1F DAA
Malicious:	false
Preview:	VLnk.....?.....).0k..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210225202231Z-228.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 164 x -126 x 32
Category:	dropped
Size (bytes):	82710
Entropy (8bit):	1.3553379426422076
Encrypted:	false
SSDEEP:	384:3rwzzjlpId0re08nSAph9XkYHVJY2RtXSl6:76ZpI2k1Xk8VJY2TXSl6
MD5:	088F002575E642485EB00A40EF9B3316
SHA1:	6AF76A0F6AAF97C78DDAD8903E8A4270F8926F7B
SHA-256:	84ABE3396DD1F1E40B0D25CA697A427500AE5F505A03AF3AE10B5FEE78471502
SHA-512:	97AD7461753F09A31E3EC2EC1454C53F21D3B02B3B8F2C1E728AF56396C00C609CB9D820E6A1503F3E83B41A349B67C6C60220B377FD9F4838375BA999D1E318
Malicious:	false
Preview:	BM.C.....6...(..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
File Type:	SQLite 3.x database, last written using SQLite version 3024000
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	3.4473088345974023
Encrypted:	false
SSDEEP:	96:k49lVXEBodRBkWCgOOh1CKg49lVXEBodRBkWCgJOh1CKw49lVXEBodRBkWCgJOh/:HedRBtedRBiedRBiedRBk
MD5:	C589ED87E78BBE1487525EBC0F6D5EC7
SHA1:	70E1E78E053B8EEB8BEC4DBEA13C73C6EB5CCE76
SHA-256:	15D0126CDE2794F255E2D3DF194497EB17C74FA9BDF47F0A08BCCE91A2932BE6
SHA-512:	48E2AEC0E3D96638330B77966777DFD7AE2D757984184ACC22AF7C2E4F7306BC3A0C045545C7C25D25B79724C26E48FBAFEB0443303EB68B6B4E49CBD75E665
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....1.....T...U.1.D.....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	modified
Size (bytes):	34928
Entropy (8bit):	3.3138009326939453
Encrypted:	false
SSDEEP:	96:JCgOOhZCPA949lVXEBodRBkwCgOOh1CKRt49lVXEBodRBk8CgJOh1CKHd49lVXEG:DiedRB5SedRBYCedRBeyedRBa
MD5:	18C149BF0B2A70A94B8B211CF070FF93
SHA1:	A51EF4266AD8C556446B2F0B9E31CD04F0DC97A7
SHA-256:	1DE2E4DE3D3B9CA886095CBE45F76582E13F03F8387FC49D6AF61C78033DFA02
SHA-512:	E5A164665DA6F650FF14AD96642118CFC702E878A5147A96E8775BAFEFDBA857A9DD0E44E8C8808C7A26364AB70B6814FFB73D865C5F5CC1F51D50D23DFE525
Malicious:	false
Preview:	.....W....X.W .L...y.....~.....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.7148	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	157979
Entropy (8bit):	5.174259815365338
Encrypted:	false
SSDEEP:	1536:amNTjRlaRlQShhp2VpMKRhWa11quVJzlzofqG9Z0ADWp1ttawvayKLWbVG3++:RNj3aRlQShhp2VpMKRhWa11quVJX+
MD5:	159ACCAFBA209FBC642499809CE2B513
SHA1:	6D94F57B63CE3BE71EDFB081ECB848B7D06EB2BE
SHA-256:	ACE286E29DFDB19080E514F3447F46E0E4ED658263AC209A9B4BBCECC36139D3
SHA-512:	E02BD1B88C1188CBBD4D6C1F5B31A44A278B213D991C6E9B9B06C620D66B1290DFBDF6D7BF92082D51A146C8AF772DAA659F9C2DC0A416C6BA9BE14B89C6E B8
Malicious:	false
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Marlett.FamilyName:Marlett.StyleName:Regular.MenuName: Marlett.StyleBits:0.WeightClass:500.WidthClass:5.AngleClass:0.FullName:Marlett.WritingScript:Roman.WinName:Marlett.FileLength:27724.NameArray:0,Win,1,Marlett.Na meArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleN ame:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength:1036584.N ameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-Bold MT.FamilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.FullName:Arial Bold.WritingScript:Roman.WinName:Arial Bold.FileLength:980756.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial Bold.NameAr

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AdobeFnt16.lst.7148	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	9566
Entropy (8bit):	5.226610011802065
Encrypted:	false
SSDEEP:	192:eTA2j6Q6T766x626Oz6r606+6bfs6JtRZ65tsu6rtG16lMXY5B5Cfk:es4p0vTLcdfIfsmtRZEtsuatG1gMlzV
MD5:	63B24EA3A13EAC476D6309BB202EF459
SHA1:	89502C393549C20C933E4553F51F74F3DBE085EF

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AdobeFnt16.lst.7148	
SHA-256:	2B4BE0BED267BBD4E4FFFC912A6C7ED6A8D4735DCF9B69FF90F37CDDEF4110EA
SHA-512:	2CB315DD00867DEE3A2CBC4017B59C53B41E817216FE0111A60947E1F0D81FF6767D8F7B5C406AAF9E6516BE716A086642AFFABBEFBE4C5B260437C89E3535EC
Malicious:	false
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-H.Registry:Adobe.Ordering:Identity.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-H.FileLength:8228.FileModTime:1426577652.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-V.Registry:Adobe.Ordering:Identity.UseCMap:Identity-H.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-V.FileLength:2761.FileModTime:1426577652.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:Type1.FontName:AdobePiStd.FamilyName:Adobe Pi Std.StyleName:Regular.FullName:Adobe Pi Std.MenuName:Adobe Pi Std.StyleBits:0.WritingScript:Roman.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\Font\AdobePiStd.otf.DataFormat:sfntData.UsesStandardEncoding:yes.isCFF:yes.FileLength:92588.FileModTime:1426577650.WeightClass:400.WidthClass:5.AngleClass:0.DesignSize:240.NameArray:0,Mac,4,Adobe Pi Std.

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	63598
Entropy (8bit):	5.4331110334817385
Encrypted:	false
SSDEEP:	768:PCbGNFYGpiyVFiC0Z0Plmk9slKTg9F3FnPRqt96RsItYyu:J0GpiyVFih0tmk9slhPRq/ssItK
MD5:	087C0FA445D1E6F7C6C8885CA6E650D4
SHA1:	B9599D8DC4340AF970263290E28BC1294E58C6EC
SHA-256:	083FE4D59BB6FD1C9A2A47FE6A264DA99F945826A3AD0D30D6298A9058584FFD
SHA-512:	2ABA2BFF1D47184E7D6C3896272542764588DD2E4A123179EC39E66E8331BAACA60D42207610F6B9B6C6D5052C4DC2F78278465406A4C4348C8E3A19B608C861
Malicious:	false
Preview:	4.382.88.FID.2:o:.....:F:AgencyFB-Reg.P:Agency FB.L:$....."F:Agency FB.#.94.FID.2:o:.....:F:AgencyFB-Bold.P:Agency FB Bold.L:%....."F:Agency FB.#.82.FID.2:o:.....:F:Algerian.P:Algerian.L:$.....RF:Algerian.#.93.FID.2:o:.....:F:ArialNarrow.P:Arial Narrow.L:$....."F:Arial Narrow.#.107.FID.2:o:.....:F:ArialNarrow-Italic.P:Arial Narrow Italic.L:$....."F:Arial Narrow.#.103.FID.2:o:.....:F:ArialNarrow-Bold.P:Arial Narrow Bold.L:%....."F:Arial Narrow.#.116.FID.2:o:.....:F:ArialNarrow-BoldItalic.P:Arial Narrow Bold Italic.L:%....."F:Arial Narrow.#.75.FID.2:o:.....:F:ArialMT.P:Arial.L:$....."F:Arial.#.89.FID.2:o:.....:F:Arial-ItalicMT.P:Arial Italic.L:$....."F:Arial.#.85.FID.2:o:.....:F:Arial-BoldMT.P:Arial Bold.L:$....."F:Arial.#.98.FID.2:o:.....:F:Arial-B

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\E5F0NRSV\joom[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FED
Malicious:	false
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{51AA8481-77A7-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	32856
Entropy (8bit):	1.850361690277023
Encrypted:	false
SSDEEP:	192:rmZtZh2sW/tGfrCtkBFzWV9D6sfJBOjrwGl:riDQ7l82d/pE7
MD5:	25769EE3B5C2860E1CBCD0C8DAF733E3
SHA1:	66E5A062CE8B48C6650B82C02A09F98FF9127637
SHA-256:	64B67EE5D3D9840EFB912F4F9742BBC791F3FB42A7800A279643D3BDE9687AA7
SHA-512:	5ECCEE19C5619A1C11FE9206EA6A3B88775A755FDA8B98237D3891FC469695B0D269D2D231A8DC506DC2BF9244204C18B090DCA40A1565C8820E06DB92632F8
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{51AA8483-77A7-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	23640
Entropy (8bit):	1.660827562391454
Encrypted:	false
SSDEEP:	48:IwyGcprTGwpabG4p0nRGnapP2nHGPHp/niCGgpNnNGoptn6GHYpanX+Gxp6nX4GP:rGZNQ9+dV2adiavfPqwnQhh
MD5:	FC0F51E8BD25F4BA0124AF7FE3F4618B
SHA1:	2E50CDDC363B037DAAE5EE618DE5B9B4ABCE040E
SHA-256:	1C413CFC0765B60D12BF8B576DF380F0569B153A55E8621D5D0B9C77717F25CC
SHA-512:	D64158AA0920E6610159986C4EFB2ABB3C30DB5FD681B1B398366AFBB14B52BBBE19CF6287134E2B1DD357834B9F54904A5E416DED3FC7924EA720D65341188
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{51AA8484-77A7-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5657461368197354
Encrypted:	false
SSDEEP:	48:IwfGcprCGwpa/G4pQPGrapbSwGQpKMG7HpRkTGIpG:r1ZqQR6TBS4AnTgA
MD5:	BE97B66AD40C37147E651521C987A0E5
SHA1:	F75F8118421FC93455FAEA368455319C0B8BD3A6
SHA-256:	4304BEADFD493AD5834D5280BD337CA0C1C35CFF909962BA132FEBCEF241073A
SHA-512:	9303567D2FB6A44898E2BC27F98657C2947C4FCA99910A72CD87BFF91A7E5ABC04A6389EEB356B6D08C7D1C49B9666013EFBE90F53057B255135E04A7A8AFCE
Malicious:	false
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):	5.11497446003997
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEOpxpAnWimI002EtM3MHdNMNxOEOpxpAnWimI00OYGVbkEtMb:2d6NxOeSZHKd6NxOeSZ7YLb
MD5:	D95AFE167E476A526F393A7783B61F99
SHA1:	5808B5943F9B227DA86682355C35C35320339CEB
SHA-256:	8E1879CE38AA3F85C0E292F813CC37777681A944F0D21FD737CB905A088703FC
SHA-512:	871D47E2B3E8E43C39BB53D7CE973ED8F1C6006A88E43176403B682BD0478654149E0578647EE441B2F76A11FF8616BD346DEA0CCED71461F6BDA81C92190295
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x279e553b,0x01d70bb4</date><accdate>0x279e553b,0x01d70bb4</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>0x279e553b,0x01d70bb4</date><accdate>0x279e553b,0x01d70bb4</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):	5.140365029650194
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kQEarEaAnWimI002EtM3MHdNMNxe2kQEarEaAnWimI00OYGkak6Ety:2d6Nxr1EkEnSZHKd6Nxr1EkEnSZ7Yzan
MD5:	950C05232AE113DBE1D3AFB58292D66B
SHA1:	18D5D61970EEF5E02B6FFB4998EBCBC42DBE1052
SHA-256:	EEF0C3E38A6545B3444D7C6B3EF7FE03F6E98979EC1F73F9D0048F611C7D475F

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
SHA-512:	2537A4A043868831E0B5E9CCA745CF2CCE1AB3784B39158ED97EE4447FA075E659BD73C62D126BA9051E9F91834AFC3390B511CB9B7EB3A450046EAFAB9A416F
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x27972e24,0x01d70bb4</date><accdate>0x27972e24,0x01d70bb4</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>0x27972e24,0x01d70bb4</date><accdate>0x27972e24,0x01d70bb4</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):	5.106049335139527
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLSsxsAnWimI002EtM3MHdNMNxvLSsxsAnWimI00OYGmZEtMb:2d6Nxv+IpSZHKd6Nxv+IpSZ7Yjb
MD5:	893737C2BAE8FEE61D25DF55BDC22CE1
SHA1:	7185D065D6EC82F40BD62F481357F95F13EEF771
SHA-256:	59CF29F3D8139A9FBF2199CC86BE8135CCECC3A98192DD55A88B23B1FA887783
SHA-512:	9D7DFBF349A3FDB3A5EB9FE7510F8BDFFC37DC4642F281FE9E30BBD146A7CF95C04CAAB617B5D1E6FCB8EB16324A678E375806AAC0C26648597FD4AB57B1BD45
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x27a0b797,0x01d70bb4</date><accdate>0x27a0b797,0x01d70bb4</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>0x27a0b797,0x01d70bb4</date><accdate>0x27a0b797,0x01d70bb4</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):	5.121622322015404
Encrypted:	false
SSDEEP:	12:TMHdNMNxigXAnWimI002EtM3MHdNMNxigXAnWimI00OYGd5EtMb:2d6NxUSZHKd6NxUSZ7YEjb
MD5:	B08C5DB1DAE1CF8276038922164EBBBC
SHA1:	18C1BA9BFAE52CA7C7E92D6A496F2B97884D2E28
SHA-256:	211AF6E47D3EFA083DF6EC3CB429A56682626E3B4324231F2719C6DBBAD641C1
SHA-512:	556F33606A99059C356C3054442ACD29F629E9DF0A5F681F44D144A7A57E1FA773AAA15B998A22379380ACAA0C3B0C1334DC22278BD887C35CCDC9AA27D2AF7
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x279bf2db,0x01d70bb4</date><accdate>0x279bf2db,0x01d70bb4</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>0x279bf2db,0x01d70bb4</date><accdate>0x279bf2db,0x01d70bb4</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):	5.113138891428335
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwSsxsAnWimI002EtM3MHdNMNxhGwSsxsAnWimI00OYG8K075EtMb:2d6NxQTIpSZHKd6NxQTIpSZ7YrKajb
MD5:	A95B8E22C2080D830C7324A1D5623418
SHA1:	5EB08D6A6AABDDB5E30CA2FE3D7534EF82362A84
SHA-256:	9D97CBB3169DED7A0E9FE5BFFD25CF6636FBE7A40649BC2FA323F6B43978CEDE
SHA-512:	6CD54A7B41AD0F5D21CF564776D966E4757E5D0C887B52D19DCA1A8138EC5A1DD2F818F25D539F116FB1228F4736C15DC8D7621AC89256353797A91FC6771AF
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x27a0b797,0x01d70bb4</date><accdate>0x27a0b797,0x01d70bb4</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>0x27a0b797,0x01d70bb4</date><accdate>0x27a0b797,0x01d70bb4</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):	5.118833372731758
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nOpxpAnWimI002EtM3MHdNMNx0nOpxpAnWimI00OYGxEtMb:2d6Nx07SZHKd6Nx07SZ7Ygb
MD5:	3AC8BAD85ED413A145E19109F07BBDC0
SHA1:	CA41AD1A48A6B0BF6870B76C370D06CEB132F684
SHA-256:	7D5D63B472973495EFB340C6AB57A4FF1F0214A654EE6D4D052CF055C1D87C4B
SHA-512:	600639DD4B3C333999E65A34827C66B2B447F16BC0BE2A44BA965F4D1236F2DDDB46D7E381D26186539CFE3F505BC0F52E7C8D40272360FF97EFEF924B57FB9A
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x279e553b,0x01d70bb4</date><accdate>0x279e553b,0x01d70bb4</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>0x279e553b,0x01d70bb4</date><accdate>0x279e553b,0x01d70bb4</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):	5.154609739367763
Encrypted:	false
SSDEEP:	12:TMHdNMNxxOpxpAnWimI002EtM3MHdNMNxxOpxpAnWimI00OYG6Kq5EtMb:2d6NxNSZHKd6NxNSZ7Yhb
MD5:	C5B50AD1A00891B492508AA71331F545
SHA1:	848AE0C6C5E839FC43833471CC61723CF1F53215
SHA-256:	5B43A0344F3EBBA68EA3B643B352D563454902CF31EC739EF1994D7D595D4E78
SHA-512:	4FABB36A2B4B608F6CAC6A4CC63CE49DDBDF44D636DDDB941F23FA088AEBE079F8F2B4ADBB27C8309C6D3997FEE6EF6834824D020B833AE6166FA90C1C50FAC8
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x279e553b,0x01d70bb4</date><accdate>0x279e553b,0x01d70bb4</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>0x279e553b,0x01d70bb4</date><accdate>0x279e553b,0x01d70bb4</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):	5.133133668351758
Encrypted:	false
SSDEEP:	12:TMHdNMNxcDAayAaAnWimI002EtM3MHdNMNxcDAayAaAnWimI00OYGVEtMb:2d6NxASZHKd6NxASZ7Ykb
MD5:	FC6084D56E65A9E0212AD0608EAE1BAB
SHA1:	3473A1FE135B74BEFC6BEBA9F1FAF6C06109C925
SHA-256:	FD494EC032F8488712F58C18FD810A3FDC4EAB99B58C880D2E58E5A4B2DEBDC3
SHA-512:	F77FB6CDA8C2193ADFD6D0BC9676946F22314D1B532FCDFDBA3C2A4DDB4A4C531BCF5464A14B0DACAB4E4B55BE2A3035F0EE1629C0CCD8D9DED0D95C968F473
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x279990c6,0x01d70bb4</date><accdate>0x279990c6,0x01d70bb4</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>0x279990c6,0x01d70bb4</date><accdate>0x279990c6,0x01d70bb4</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):	5.106853162151636
Encrypted:	false
SSDEEP:	12:TMHdNMNxfngXAnWimI002EtM3MHdNMNxfngXAnWimI00OYGe5EtMb:2d6NxTSZHKd6NxTSZ7YLjb

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
MD5:	47FBB07EABF6B3505DFD25CF26E2C654
SHA1:	21F86B149D0D7B84224432B94DC8D1A82AD001FF
SHA-256:	BAB6F186A0C30A0B7F20802CC8B3651337B023779DBF6D3C591693259933ADB8
SHA-512:	974410B62076996510962545D81B2595E22EE244D4C5A4AAA42A523AD89574AAFA24AD7B3CE13251FAAFFEDC8FDEBF46B6AD7A854369431AC8E6C382EFB6AE50
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x279bf2db,0x01d70bb4</date><accdate>0x279bf2db,0x01d70bb4</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>0x279bf2db,0x01d70bb4</date><accdate>0x279bf2db,0x01d70bb4</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\2WF3MMUU\d[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 61728, version 0.0
Category:	downloaded
Size (bytes):	61728
Entropy (8bit):	**7.992796812103739**
Encrypted:	**true**
SSDEEP:	1536:nl+B1ouiahr0GFFTSfPu1z6fsrFJm4w5sKV:tB1hrlF5SnK+T4w6g
MD5:	C30498C311ECC433CB7CD23D32159AFC
SHA1:	F442B2B9EAAEE7FF71F57EBAA58734B4724FAC6A
SHA-256:	9F46E13E2EC896C2461E4C55C7393A69F7E70D85276544AC2693C42F3BC1DC89
SHA-512:	B955D91B79E2E5AEB0563ECD18935DB7FC2BE3999CB613455F04131D75A8B0748E8442D760365656C9360284343161F3B6DF068E4545E71614E94E9BB7FACF88
Malicious:	false
IE Cache URL:	http://https://use.typekit.net/af/3d81f6/00000000000000000000148a2/23/d?subset_id=1&fvd=n3&v=3
Preview:	wOFF..... .....DYNA.....z.....*.FFTM.....]...GDEF.....R...Z.s..GPOS...h...#..3.M...GSUB.....P...\..H.OS/2.....Y...`~W.ocmap...\.....cvt .....*...*.. .6fpgm.....e#./.gasp.....glyf.....d..NX8.c.head.....4...6..;.hhea...T...!...$....hmtx...@.....h..}.loca...8.....6.A.Tmaxp...x... ... .B..name.....Q..p.post...H..... ... (prep.....i...v..ym.....o1.....x.....6.h.R.\.^.h.r.Y.z.`.d.m.j.t.L.F.J.f..x.]Q.N[A.....c..hS.fB...$.W...vc9B.\.b\..P Q..k.h().A..R>.O@bfM.(....s..r..]Z.y..R.....v...t}...v.@..^.n ...`3.rG....-.!.i'P....6...>.d..AK3MO....B`...0...../X....C.i*..s*..Ks....k..vp&"?..hj..@._:.z>.b.r.0...S.d".f2].T-3.up...;X.Js....U.....-.2KC...*1B.$.BN9w.?)P>..1....a..q.50.....fS.{.0~. G..o..>..6F..X.`...QU...s/.....3.%`y.._'..;6..em.C.....2....U.....tJ.....p.X...R.v....`H.F..h-;.*...d/.*.....x.c`d```b8z%1.I<..W.y..@..S.*.....`..r9.j....+..x...J.A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\olb8zpk[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	18084
Entropy (8bit):	5.567560853086973
Encrypted:	false
SSDEEP:	384:6yO2tpIgIPs51iRm2lIew42noFeFsP9btiCtpIaCR:6y8q1iRm2XwMqsbbt6J
MD5:	5076E0879850567ED8A5CE8D65F00DFD
SHA1:	1733D25CAF88876D3F6B44BFD04751E02AA717E3
SHA-256:	B7F0115AFBD3505857C7A7515CBDFD9B595A750B8A0C576DB45992C2F87C0355
SHA-512:	52A0923D550E39914EE7C239B1FB48A69A4C27E7F06206E94E7296866D17835EB053393BD89ED4C9761B07DD24B81F04FC964559B487C61DA4EE7BA4AE10CF1(
Malicious:	false
IE Cache URL:	http://https://use.typekit.net/olb8zpk.js
Preview:	/*. * The Typekit service used to deliver this font or fonts for use on websites. * is provided by Adobe and is subject to these Terms of Use. * http://www.adobe.com/products/eulas/tou_typekit. For font license. * information, see the list below.. *. * proxima-nova:. * - http://typekit.com/eulas/00000000000000000000148ac. * - http://typekit.com/eulas/00000000000000000000499c. * - http://typekit.com/eulas/00000000000000000000148a0. * - http://typekit.com/eulas/00000000000000000000148a6. * - http://typekit.com/eulas/00000000000000000000148a4. * - http://typekit.com/eulas/00000000000000000000148a2. *. * . 2009-2020 Adobe Systems Incorporated. All Rights Reserved.. */.if(!window.Typekit)window.Typekit={};window.Typekit.config={"a":"1029652","c":[".tk-proxima-nova","\"proxima-nova\",sans-serif"],"fi":[137,139,171,173 ,175,5474],"fc":[{"id":137,"family":"proxima-nova","src":"https://use.typekit.net/af/1eef01/00000000000000000000148ac/23/{format}{?primer,subset_id,fvd,v}","descriptors":

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\p[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	35
Entropy (8bit):	2.9302005337813077
Encrypted:	false
SSDEEP:	3:CUHaaatrllH5:aB
MD5:	81144D75B3E69E9AA2FA3E9D83A64D03
SHA1:	F0FBC60B50EDF5B2A0B76E0AA0537B76BF346FFC
SHA-256:	9B9265C69A5CC295D1AB0D04E0273B3677DB1A6216CE2CCF4EFC8C277ED84B39
SHA-512:	2D073E10AE40FDE434EB31CBEDD581A35CD763E51FB7048B88CAA5F949B1E6105E37A228C235BC8976E8DB58ED22149CFCCF83B40CE93A28390566A2897574A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\p[1].gif	
Malicious:	false
IE Cache URL:	http://https://p.typekit.net/p.gif?s=1&k=olb8zpk&ht=tk&h=joom.ag&f=137.139.171.173.175.5474&a=1029652&js=1.20.0&app=typekit&e=js&_=1614284611545
Preview:	GIF89a.....,.....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\cross[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	837
Entropy (8bit):	4.470357279234661
Encrypted:	false
SSDEEP:	12:tr48Ju3M656/RBR6Oz8AOuPwYHDULVWSRd9TCxg1lmrc/woKiHA2:t08Ju3MM6/RH68LO7+DSLThE6wVH2
MD5:	F58C57A574CCBB57D3ED79287B15BB59
SHA1:	232F3A24D02702188271B82D19FD709C83469E9D
SHA-256:	16F56634D8828B7755CAF0475663AF4060B9700BA20A75B9856ACC7DD76413E2
SHA-512:	23D0A12B83D64E5691AD3640AC4B8195F6132806749FA0DD6AA8C926BB1330D89516F7D28AE0574A808DBC9B24C2DD0B03A1328E4DB808D42EB7DBF10ECB3B8
Malicious:	false
IE Cache URL:	http://https://www.joomag.com/assets/img/common/cross.svg
Preview:	<svg width="110" height="110" viewBox="0 0 110 110" fill="none" xmlns="http://www.w3.org/2000/svg">. <path fill-rule="evenodd" clip-rule="evenodd". d="M55 110C85.3757 110 110 85.3757 110 55C110 24.6243 85.3757 0 55 0C24.6243 0 0 24.6243 0 55C0 85.3757 24.6243 110 55 110ZM74.1716 30.8284C75.7337 29.2663 78.2663 29.2663 79.8284 30.8284C81.3905 32.3905 81.3905 34.9232 79.8284 36.4853L60.8137 55.5L79.7144 74.4007C81.2765 75.9628 81.2765 78.4955 79.7144 80.0576C78.1523 81.6197 75.6197 81.6197 74.0576 80.0576L55.1569 61.1569L36.5993 79.7144C35.0372 81.2765 32.5045 81.2765 30.9424 79.7144C29.3803 78.1523 29.3803 75.6197 30.9424 74.0576L49.5 55.5L30.8284 36.8284C29.2663 35.2663 29.2663 32.7337 30.8284 31.1716C32.3905 29.6095 34.9232 29.6095 36.4853 31.1716L55.1569 49.8431L74.1716 30.8284Z". fill="white"/>.</svg>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\e2270d116b[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.340020120659463
Encrypted:	false
SSDEEP:	3:U3KTDW3MiqVkMWVrfUh:H6NukMWVr8h
MD5:	06DD80AEB628C60DC680BC7A4BEE6651
SHA1:	8C86EB7DDFF5E1E5D527BD7A41C9D3F6767E23E0
SHA-256:	5E864C2E3F674C60970513411EAEEEAFD2D615D842E65EC01D09CCFCB4A7B38D
SHA-512:	C6EE8252743A760AD7BEE017FF7A804B6E34236764BC5630289D5E4C7C15E38CB971F161821586F0235882FD581630F1531FD6396761BF1284581CD8C2CAC4C6
Malicious:	false
Preview:	NREUM.setToken({'stn':0,'err':1,'ins':1,'cap':0,'spa':1})

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\joomag.responsive[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	644771
Entropy (8bit):	5.247473894365514
Encrypted:	false
SSDEEP:	12288:RFv0nw5RZ35slYgBZvEVVrowG1ZAlkKDJ3bys5XrHeY01TU/S/f5q1Kcm:RF0nw5RZ35slYgBZvEVVrowG1ZAlkKDk
MD5:	ABDB67CF175491FCAFD4BB225D6540A9
SHA1:	D1D1FA2E31CE80126887B619C0136A69275B3E79
SHA-256:	DDCD972A29BC1A2552A9D740B324F8B4B8B4EEE22505E5C4D0D701ECDC5BC202
SHA-512:	F437203616C71054E11CE3900724ABD27D471B193EE576AD54072BCC5FD3021456122CF04C47B72143FD52C842F4A8CFCB402AC75DAFF73CB9354CF1CC07E40
Malicious:	false
IE Cache URL:	http://https://www.joomag.com/static/css/joomag.responsive.css?_=5.1.5.1
Preview:	@charset "UTF-8";html{font-family:sans-serif;-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background:0 0}a:active,a:hover{outline:0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:700}dfn{font-style:italic}h1{font-size:2em;margin:.67em 0}mark{background:#ff0;color:#000}small{font-size:80%}sub,sup{font-size:75%;line-height:0;position:relative;vertical-align:baseline}sup{top:-.5em}sub{bottom:-.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr{-moz-box-sizing:content-box;box-sizing:content-box;height:0}pre{overflow:auto}code,kbd,pre,samp{font-family:monospace,monospace;font-size:1em}button,input,optgroup,select,textarea{color:inherit;font:inherit;margin:0}button{overflow:visible}butto

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\d[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 58272, version 0.0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\d[1]	
Category:	downloaded
Size (bytes):	58272
Entropy (8bit):	**7.991777670773457**
Encrypted:	**true**
SSDEEP:	1536:BS7tBzduth0mIGHEosBwOfwQRKjHIqEjGlaV:BA3duz0m9HkdYi7ZjG+
MD5:	25EB786C99DB8F58DF013C81F8F14C0D
SHA1:	83FDDE6AC8D51CAD2BDF8C33813FEE6BA34002A7
SHA-256:	054E8C55D84A3EBFF0722AB57AB4A00BB60736DCFF97B81401019D714FFAF688
SHA-512:	2F554CC1A262CA515156198F027A0A0F13E430BB17392874AF265B437CAB397FD415770AB564067AE030D7341A34CBA38705788F2887F388AEAD64FBB21490D5
Malicious:	false
IE Cache URL:	http://https://use.typekit.net/af/1eef01/00000000000000000000148ac/23/d?subset_id=1&fvd=n9&v=3
Preview:	wOFF.....L.....DYNA.....z.....*.FFTM.....]...GDEF.....R...Z.s..GPOS...X.....1.\.#sGSUB...,...P...\..H.OS/2.....Y...`....cmap.....cvt .....G. .fpgm.....e#./.gasp.....glyf...|...V..@4.)<ahead.....5...6.L;jhhea...D...!...$.O..hmtx.....h..xloca.....6(..maxp...h... ... .B..name.....Q+.:.post..... ...(pr ep.....c...t.....o1.....x.....6.`.....6.>.h.....X..x.]Q.N[A.....c..hS.fB...$.W...vc9B.\.b\..P Q..k.h().A..R>.O@bfM.(....s..r..]Z.y..R.....v...t}...v.@..^.n...`3.rG....-.!. i'P....6...>.d..AK3MO....B`...0...../X....C.i*..s*..Ks....k..vp&"?..hj..@._:.z>.b.r.0...S.d".f2].T-3.up...;X.Js....U.....-.2KC...*1B.$.BN9w.?)P>..1....a..q.50.....fS.{.0~.G..o..>..6F..X.` ...QU...s/.....3.%`y.._'..;6..em.C.....2....U.....tJ.....p.X...R.v....`H.F..h-;.*...d/.*.....x.c`d```b8..b.x~.....".~U....+...b.a`d.....x...N.0.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\d[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 55916, version 0.0
Category:	downloaded
Size (bytes):	55916
Entropy (8bit):	**7.990377940984203**
Encrypted:	**true**
SSDEEP:	1536:CdrjeMTpp0yUURuaM+lCA8QMtjOdH3taxc1ax:CpZ1uylpOtq0O1ax
MD5:	642BF1228C9D1BCF62992C08DF8A92B8
SHA1:	05DA82C550C25254ACA29DAD238EABCFC149BF9C
SHA-256:	036F00B2C16BD1CA74B5384DE15D04214CC005A4476BF4A6291AD29D39885BAF
SHA-512:	C49B942716BFFF2934F2E7A70B0B230DF28E1B810BE2324EC2ED90BB9CCE48413E444F773C56FF99BBFFA940E0BD7554DD7554C1D29321AA7506750C6B858B1
Malicious:	false
IE Cache URL:	http://https://use.typekit.net/af/bc719c/00000000000000000001499c/23/d?subset_id=1&fvd=n7&v=3
Preview:	wOFF.....l.....0.....DYNA.....{....<N.bGPOS.....<..3./.k.GSUB...<.....OS/2.....Y...`...rcmap.....<.cvt .....l..fpgm.....s.U.7gasp.....glyf..!.. .....=..H..head.....6...6..<.hhea...@...!...$....hmtx.....d..."loca.....4.r .maxp...d... ... .4.>name.....E.4$.post....."..2..prep....._.....)..6....x.].=N.0...8,..H. .-+.+..R8.P.@(<.?.D..Hih\p..3]..`.....3.....k..m.....LP^.@...y.@8...xeq..X...5.~..u..~.u.....s....&.B..S0T.:.;.;.d.'.9..._.....^:w.&y..@.WTzT...6..A..1)..j.|..Wkn....P..0.....U.w,:.xb.85 .....y4X.&..k8'z.;wM.*Njp...rk.....y..._.<.....x.....Hy.....x..OJ.@.._....bdf;0P.R.$.*Cg..0.Q.....BR...x...E.x.O.9..Z..`>..U}./...x.....{...[p.]..]...../....;..... ....g.-1.....W.G..<x^.w..y.R....Q....*..X....3UM.e...6..G.Q ..L:I-+]....2.4W..4J..l..{i.....VjDM.B?.tU.... ..|.m...e..v^.ij....T.F....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\d[3]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 59940, version 0.0
Category:	downloaded
Size (bytes):	59940
Entropy (8bit):	**7.994140772663277**
Encrypted:	**true**
SSDEEP:	1536:bMRUowMIdMg7LpJ3/ReRCiVPXa6c4lqSV:4RUzhdLLp9wPXa65lD
MD5:	3AEB74FE14E1ACCAE157879343062A13
SHA1:	7A736AD47EE70212EEB9CD4179826F9CB8D55781
SHA-256:	E3E487D6036BB95CCD6D97CA641B5FA6ED85FF93E11A5649C72534AF0DD272C3
SHA-512:	111BBBA41ACCC2D47A492743F05511C354CAA6A7F61062F0D2EFCB2485DB36DBAF797C37C7C01ABA46E16FE116D81A69E13736C2BE37AE0F303648B537C250B
Malicious:	false
IE Cache URL:	http://https://use.typekit.net/af/3ba24d/00000000000000000000148a0/23/d?subset_id=1&fvd=n1&v=3
Preview:	wOFF.....$.....`.....DYNA...h...z.....*.FFTM.....]..,GDEF.....R...Z.s..GPOS...8.....3.F!"(GSUB.....P...\..H.OS/2.....Y...`~W.acmap...`.....cvt .....R ..fpgm.....e#./.gasp.....glyf...\.....K..F.rhead.....4...6..<.hhea...$...!...$...-hmtx...`.....h....loca...8.....6b4.6maxp...H... ... .B..name.....H>..post...L..... ... (prep...x...O...O...4.....o1.....H.....x.....6.<.<.B.:.>.5.@..x.]Q.N[A.....c..hS.fB...$.W...vc9B.\.b\..P Q..k.h().A..R>.O@bfM.(....s..r..]Z.y..R.....v...t}...v.@..^.n...`3.rG....-.!.i'P....6...>.d..AK3MO....B`...0...../X....C.i*..s*..Ks....k..vp&"?..hj..@._:.z>.b.r.0...S.d".f2].T-3.up...;X.Js....U.....-.2KC...*1B.$.BN9w.?)P>..1....a..q.50.....fS.{.0~.G..o..>..6F ..X.`...QU...s/.....3.%`y.._'..;6..em.C.....2....U.....tJ.....p.X...R.v....`H.F..h-;.*...d/.*.....x.c`d```b8z...x~.....".~Ul...V.....r.....R..x..ON.@..?.....v5. b;.T..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\d[4]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 60240, version 0.0
Category:	downloaded
Size (bytes):	60240
Entropy (8bit):	**7.993033134446386**
Encrypted:	**true**

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\d[4]	
SSDEEP:	1536:g/j1fMtxM2e+ZgdhJ2kNSHS/D5M46tEE+tMUl9819V:gF72e+ydL2kSHyD5ytHL1H
MD5:	1E15B536F74EF394FCEC8470F8D64323
SHA1:	50942FD78ECBA94C12DA7E63866585B26CED24C5
SHA-256:	4A4E9A7F3425D3D460A9FFC77A56391B62AF222391DB604B5924D90637549204
SHA-512:	4AB0043221C4E0CC2922ED33CD414A37861145DB3AAB79132059C8074B1F15662D030D462A63B59B51F24F74099DF7AECDDC7468C954A41B862ACDAF0A27BC4
Malicious:	false
IE Cache URL:	http://https://use.typekit.net/af/e0b8be/00000000000000000000148a6/23/d?subset_id=1&fvd=n6&v=3
Preview:	wOFF.....P.....DYNA.....z.....*.FFTM.....]...GDEF...(...R...Z.s..GPOS...|.....3.N...GSUB.....P...\..H.OS/2.....Y...`....cmap.....cvt .....0...0... Jfpgm.....e#./.gasp.....glyf...T.....F...b.head.....5...6..;.hhea...h...!...$...ihmtx...X.....h.}&.loca...d.....6.E..maxp..... ... .B.Tname.....u.C).post...x..... ...(prep..... ..s....^`.....o1.....2.....x.....6...\|.....n.....u.....x.]Q.N[A.....c..hS.fB...$.W...vc9B.\.b\..P Q..k.h().A..R>.O@bfM.(....s..r..]Z.y..R.....v...t}...v.@..^.n...`3.rG....-.!.i 'P....6...>.d..AK3MO....B`...0...../X....C.i*..s*..Ks....k..vp&"?..hj..@._:.z>.b.r.0...S.d".f2].T-3.up...;X.Js....U.....-.2KC...*1B.$.BN9w.?)P>..1....a..q.50.....fS.{.0~.G..o..>..6F..X.`. ..QU...s/.....3.%`y.._'..;6..em.C.....2....U.....tJ.....p.X...R.v....`H.F..h-;.*...d/.*.....x.c`d```b8....x~.....".~U....V.=..]...]...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\d[5]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 61612, version 0.0
Category:	downloaded
Size (bytes):	61612
Entropy (8bit):	**7.992135320284749**
Encrypted:	**true**
SSDEEP:	1536:C1QmG2C528LvuA6DfzlNxlpgCMbY9lgaiV:CCmqPG1zznxlEMma4
MD5:	D26D2BAB4625361DA030917B4FA4CBF0
SHA1:	972FF9E8DF21F1CAE4B0ABA7C36577A72E18CD8A
SHA-256:	5F8EE1622F6CDD2E3B343DB9BC25A58053C24959A7D72242E783ABD6C65A9070
SHA-512:	231BB6C230F909CD8ED5C361B8DAD45D362B9B9172FEA575FF85D82B4E20EDF800F4125971DED7EBA594F9B03906891FF74D96422B2E000FECAD6624879A7CD D
Malicious:	false
IE Cache URL:	http://https://use.typekit.net/af/42fca5/00000000000000000000148a4/23/d?subset_id=1&fvd=n4&v=3
Preview:	wOFF..... .....DYNA.....z.....*.FFTM.....]...GDEF...8...R...Z.s..GPOS.....&..3.Nm.,GSUB.....P...\..H.OS/2.....Y...`~..|cmap.....cvt .....2...2.A. 0fpgm.....e#./.gasp.....glyf.....KII.+.head.....4...6.E;.hhea...x...!...$.I.-hmtx.....hU.X.loca.....6Wm..maxp..... ... .B..name.....iW.T.post..... ... (prep.....>.....o1.....x.....6...`.n.\|.....Z.....O...t.c.....x.]Q.N[A.....c..hS.fB...$.W...vc9B.\.b\..P Q..k.h().A..R>.O@bfM.(....s..r..]Z.y..R.....v...t}...v.@..^.n... `3.rG....-.!.i'P....6...>.d..AK3MO....B`...0...../X....C.i*..s*..Ks....k..vp&"?..hj..@._:.z>.b.r.0...S.d".f2].T-3.up...;X.Js....U.....-.2KC...*1B.$.BN9w.?)P>..1....a..q.50.....fS.{.0~.G.. o..>..6F..X.`...QU...s/.....3.%`y.._'..;6..em.C.....2....U.....tJ.....p.X...R.v....`H.F..h-;.*...d/.*.....x.c`d```b8...KW<..W.y..@..S.*....+.>.(a..r9.j.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\fonts[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	3319
Entropy (8bit):	4.7944958698543045
Encrypted:	false
SSDEEP:	48:cIR3IRMV2RJERJgRcL/RIRUnIRU8V2RdRdR3tu/wIREIR/V2RtRtRnE/6IRnIR8q:cYDVmo3RHcVFw1OVp6e9V+NxI+VSGU
MD5:	C05ACE645F780FF960B1B7B7A8B21C43
SHA1:	D25960DAED67DB0FF23ABB0DA084E3BD356C45E7
SHA-256:	94A5843CF3E664CD2087A484200389FC08A4FA465C0BA3CF5B29430371A905E7
SHA-512:	E1263C2424CBD953186CAC9641BEF7DFDEE9CCEB5D383CEDA42AB674F9D7AC8392E2796370ACBD42DB8A018CD6BE9A0A5CC7BAC624E7125DAF7DAE269399 D83B
Malicious:	false
IE Cache URL:	http://https://www.joomag.com/assets/fonts/fonts.css
Preview:	@font-face {. font-family: 'playfair-display';. src: url('/assets/fonts/playfair_display/PlayfairDisplay-Regular.otf');. src: url('/assets/fonts/playfair_display/PlayfairDisplay-Regular.otf?#iefix') format('embedded-opentype'),. url('/assets/fonts/playfair_display/PlayfairDisplay-Regular.woff2') format('woff2'),. url('/assets/fonts/playfair_display/PlayfairDisplay-Regular.woff') format('woff'),. url('/assets/fonts/playfair_display/PlayfairDisplay-Regular.ttf') format('truetype'),. url('/assets/fonts/playfair_display/playfairdisplay-Regular-webfont.svg#Playfair Displaybold') format('svg');. font-weight: 400;. font-style: normal;.}..@font-face {. font-family: 'playfair-display';. src: url('/assets/fonts/playfair_display/PlayfairDisplay-Black.otf');. src: url('/assets/fonts/playfair_display/PlayfairDisplay-Black.otf?#iefix') format('embedded-opentype'),. url('/assets/fonts/playfair_display/PlayfairDisplay-Black.woff2') format('woff2'),. url('/asse

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\limitedAccessPages[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	6920
Entropy (8bit):	4.975144490577777
Encrypted:	false
SSDEEP:	96:vzjUCy0130jVOyXse08eptdTYTQ7fqCpoupLVCadogQGAE:K0MVZ8e08eRZLQo
MD5:	62E4648D1FA23E754FF92CA7B04DA2D8
SHA1:	878C7426B5976FE905E9F448307051B01C3598CF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\limitedAccessPages[1].css

SHA-256:	F91AF90E07ECDFC8E4908A0FFF3C379B97A295AD5BF56A0236898D5C5795391D
SHA-512:	CE557D5598EAA35AB0499A0302E9BF9466E0F98C879339F86B696C3B0786DE443455EFCA2E945847F811687E7944D07A859EFE5D169A4C1F9E402898E13CE010
Malicious:	false
IE Cache URL:	http://https://www.joomag.com/static/css/pages/limitedAccessPages.css?_=5.1.5.1
Preview:	body{margin:0;background-color:#313a46}.j-limited-access-page .j-message-block{position:absolute;top:17%;width:100%;padding:0 20px;text-align:center;box-sizing: border-box}.j-limited-access-page .j-message-block .j-icon{display:inline-block;height:111px;width:100%;margin:0 auto;opacity:.15}.j-limited-access-page .j-message-block .j-message{display:inline-block;width:100%;margin-top:30px;font-size:36px;font-weight:100;color:#fff;line-height:52px}@media (max-height:500px),(max-width:580px){.j-limited-access-page .j-message-block{top:50%;-webkit-transform:translateY(-50%);-moz-transform:translateY(-50%);-ms-transform:translateY(-50%);-o-transform:translate Y(-50%);transform:translateY(-50%)}.j-limited-access-page .j-message-block .j-message{margin-top:15px;font-size:28px;line-height:40px}}.j-limited-access-page.j-not-have-access-page .j-message-block .j-icon{background-image:url(/assets/img/common/lock-icon.svg);background-repeat:no-repeat;background-position:center center;backgro und-size:c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\nr-1198.min[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	28120
Entropy (8bit):	5.31469238173269
Encrypted:	false
SSDEEP:	384:yZevj5awnX8RfzD7WdPs8tzmwUyAH77jx+zJTREUi2bikgHIvYboLLAJ1fFKohtJ:yZUQKi8tzA76AFIAbo/M1jtnWE5
MD5:	59C98195BA35E0B45CBE2E5BEEBD1AC8
SHA1:	BB1DD82667456B0B608750BBF8D2871A018535B0
SHA-256:	39893061747F88B837A34D0395D05FCA83E7CD5BBF2D582D181A73C5C9A174C6
SHA-512:	9CCE07757B9475D6A3C20CAD19A4775422EED4AE018F27521D4EF29FB89C5B5CEFB3991A6CDD3E422B532C32D43699A5EE86F61FD7FEA9FCDB90F2670A40E7 62
Malicious:	false
IE Cache URL:	http://https://js-agent.newrelic.com/nr-1198.min.js
Preview:	!function(n,e,t){function r(t,i){if(!e[t]){if(!n[t]){var a="function"==typeof __nr_require&&__nr_require;if(!i&&a)return a(t,!0);if(o)return o(t,!0);throw new Error("Cannot find mo dule '"+t+"'")}var u=e[t]={exports:{}};n[t][0].call(u.exports,function(e){var o=n[t][1][e];return r(o||e)},u,u.exports)}return e[t].exports}for(var o="function"==typeof __nr_requir e&&__nr_require,i=0;i<t.length;i++)r(t[i]);return r}({1:[function(n,e,t){e.exports=function(n,e){return"addEventListener"in window?window.addEventListener(n,e,!1):"attach Event"in window?window.attachEvent("on"+n,e):void 0}},{}],2:[function(n,e,t){function r(n,e,t,r,i){l[n]||(l[n]={});var a=l[n][e];return a||(a=l[n][e]={params:t||{}},i&&(a.custom=i)),a.metrics=o(r,a.metrics),a}function o(n,e){return e||(e={count:0}),e.count+=1,f(n,function(n,t){e[n]=i(t,e[n])}),e}function i(n,e){return e?(e&&!e.c&&(e={t:e.t,min:e.t, max:e.t,sos:e.t*e.t,c:1}),e.c+=1,e.t+=n,e.sos+=n*n,n>e.max&&(e.max=n),n<e.min&&(e.min=n),e):{t:n}}function a(n,e){return

C:\Users\user\AppData\Local\Temp\~DF5B4354179DD05C79.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13077
Entropy (8bit):	0.4955820805976994
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRAF9l8fRo9lTqDvmbmm3lO7J:c9lLh9lLh9lIn9lIn9loY9loo9lWDuyz
MD5:	D286EFF91CCF1D364AC36926189BC35B
SHA1:	48EC01428E7EAF74CB536AFBFA5819E9691F9BF8
SHA-256:	8240BABF62CE3D63B03819229E19B3C071FADA1AE7AA10F3C17CEC38E2102B43
SHA-512:	5D7D6149D5DABF07513FAAB834EE2CEFCF12DE406009E7C25650226CA1E71771180200711CA98273EB75357398CCC3152448C16C38489D1664A9B37172328D27
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFC49E28F8A7C615D6.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34189
Entropy (8bit):	0.3509312238082155
Encrypted:	false
SSDEEP:	48:kBqoxKEnsnd2nO2nknP6nibnyn3nX0nX:kBqoxKEsd2O2kCiby3E
MD5:	C77CD83D641CC3147C2B7AD9955D041A
SHA1:	EC6DEB6408CD86B436E9AA37A8809C86838DAACA
SHA-256:	6D2D960FFC45D33E0D9CDD621AE1457CA9F30D29AF90D537BF18A0F38F7771D4
SHA-512:	E3403B09DA8DA93C299405F654707CB7B8BBABBE9B52A715683F71B524C9161D977F626C0553345F65B126F8C78832A13A2C790B4C2537CC28FC2F46F086B8BA
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DFC49E28F8A7C615D6.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFE5BD3A345DA22996.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.3237955894621696
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAXso0w8ysom:kBqoxxJhHWSVSEabNxv
MD5:	DD88BBD02F78022B071C53C57E054C58
SHA1:	EFEDFCD805A18A5FD5CFA3A0383CA5D4BE8133E9
SHA-256:	A75EE113E64A7B431EFD5D38FB306538BB74A2E333BC7B5F851D7135BB6A06A1
SHA-512:	EE259888612560851FB0B2D5829F5292C323C91DC4085F23C238F0CACE82A186B19769C562AC90E72A2D6810A6C20E8641C498BA577930B166EE3C90FCAA41C(
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

File type:	PDF document, version 1.4
Entropy (8bit):	7.991790163901285
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	Send-Data-City_Center_Waco_Project_Report-_#9073955_942 (1).pdf
File size:	89559
MD5:	dbfaf169fa1ba4c2a4f321a57d06a9af
SHA1:	49602a3acf1bf4199e940fa7c2d6435e900b431c
SHA256:	5a53c07a8d9d58bdc22bc1ebae72d1a20d63803ffec3b28 b667640928c45bd54
SHA512:	0f907a27e2cdd540a0bd39b038c6caf0d3264f43d3249c5 53d1024157d9fbc741b53763ab2ccc4e25896ef7e5c5067 c6ef7de83d1d545d7116e4f8c70fef9827
SSDEEP:	1536:s8lhLJjjT4kn+aBsDGnV5anmXV3Y9MCv5LMBCv nYYmxrV9Hkq5/K7PIX6H8uqPwM:FXTIaqCnvF3wMBC QYmxnEe/igxIM
File Content Preview:	%PDF-1.4.%......1 0 obj.<</Type/Page/Parent 10 0 R/C ontents 9 0 R/MediaBox[0 0 792 612]/Annots[2 0 R 4 0 R]/Resources<</ProcSet[/PDF]/XObject<</TPL1 6 0 R> >>>>.endobj.2 0 obj.<</Subtype/Link/Rect[0 1.44 792 612]/Border[0 0 0]/C[0 0 0]/F 4/NM(PDFE-48D8D76

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

Header:	%PDF-1.4
Total Entropy:	7.991790
Total Bytes:	89559
Stream Entropy:	7.995037
Stream Bytes:	87678
Entropy outside Streams:	5.332280

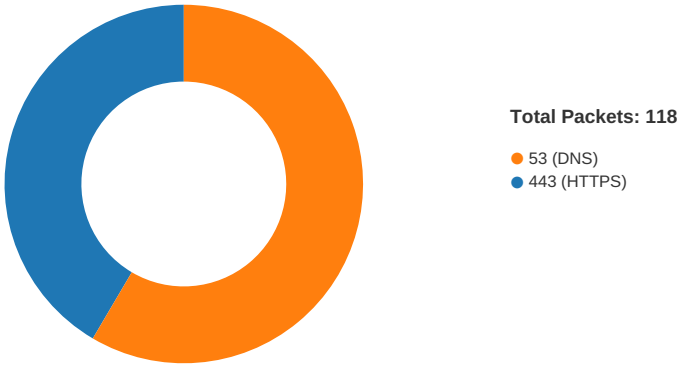
General	
Bytes outside Streams:	1881
Number of EOF found:	1
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	14
endobj	14
stream	4
endstream	4
xref	1
trailer	1
startxref	1
/Page	1
/Encrypt	0
/ObjStm	0
/URI	4
/JS	0
/JavaScript	0
/AA	0
/OpenAction	1
/AcroForm	0
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:23:30.141968012 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.142154932 CET	49773	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.264707088 CET	443	49773	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.264827013 CET	49773	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.264909983 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.264977932 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.281002045 CET	49773	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.281229019 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.403424025 CET	443	49773	209.95.50.27	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:23:30.403439045 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.403640032 CET	443	49773	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.403671026 CET	443	49773	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.403687000 CET	443	49773	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.403698921 CET	443	49773	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.403764009 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.403778076 CET	49773	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.403791904 CET	49773	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.403810024 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.403827906 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.403840065 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.403853893 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.403899908 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.403906107 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.419307947 CET	443	49773	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.419325113 CET	443	49773	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.419420004 CET	49773	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.419429064 CET	49773	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.419775963 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.419790030 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.419929028 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.449754953 CET	49773	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.449944973 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.455568075 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.455670118 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.455729008 CET	49773	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.572757959 CET	443	49773	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.572940111 CET	443	49773	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.573019981 CET	49773	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.573739052 CET	49773	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.574971914 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.574985027 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.575112104 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.575517893 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.578777075 CET	443	49773	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.578797102 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.578808069 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.578872919 CET	49773	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.578958035 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.597601891 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.597657919 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.597712994 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.597749949 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.597769022 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.597789049 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.597798109 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.597837925 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.597842932 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.597858906 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.597889900 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.597928047 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.597959995 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.597966909 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.598000050 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.598031044 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.699073076 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.699126005 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.699165106 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.699202061 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.699264050 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.699316978 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.699323893 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.702806950 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.702858925 CET	443	49772	209.95.50.27	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:23:30.703048944 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.720490932 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.720542908 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.720585108 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.720621109 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.720653057 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.720702887 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.720710039 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.720834970 CET	443	49772	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.721862078 CET	49772	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.740308046 CET	443	49773	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.840248108 CET	49776	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.840334892 CET	49778	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.840382099 CET	49777	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.962526083 CET	443	49777	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.962645054 CET	49777	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.962873936 CET	443	49778	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.962901115 CET	443	49776	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:30.962946892 CET	49778	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.962985992 CET	49776	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.963571072 CET	49776	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.963694096 CET	49778	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:30.963758945 CET	49777	443	192.168.2.4	209.95.50.27
Feb 25, 2021 21:23:31.087471008 CET	443	49776	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:31.087512970 CET	443	49777	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:31.087703943 CET	443	49776	209.95.50.27	192.168.2.4
Feb 25, 2021 21:23:31.087744951 CET	443	49776	209.95.50.27	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:22:16.306560993 CET	49714	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:16.355824947 CET	53	49714	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:17.051621914 CET	58028	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:17.100620985 CET	53	58028	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:18.045902967 CET	53097	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:18.097110033 CET	53	53097	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:18.902837992 CET	49257	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:18.953526974 CET	53	49257	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:19.964781046 CET	62389	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:20.016995907 CET	53	62389	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:20.942136049 CET	49910	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:20.993820906 CET	53	49910	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:25.508514881 CET	55854	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:25.562172890 CET	53	55854	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:26.688199043 CET	64549	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:26.737679958 CET	53	64549	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:27.487972975 CET	63153	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:27.539546013 CET	53	63153	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:30.090976000 CET	52991	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:30.139900923 CET	53	52991	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:32.793210030 CET	53700	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:32.847589016 CET	53	53700	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:34.801593065 CET	51726	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:34.853528976 CET	53	51726	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:36.847755909 CET	56794	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:36.896917105 CET	53	56794	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:37.918441057 CET	56534	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:37.925406933 CET	56627	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:37.977044106 CET	53	56534	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:37.977833986 CET	53	56627	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:39.370464087 CET	56627	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:39.370682955 CET	56534	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:39.423577070 CET	53	56627	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:22:39.433938026 CET	53	56534	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:40.385365009 CET	56534	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:40.385415077 CET	56627	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:40.434233904 CET	53	56627	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:40.435513973 CET	53	56534	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:41.055418015 CET	56621	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:41.104290009 CET	53	56621	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:42.433852911 CET	56627	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:42.433921099 CET	56534	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:42.492599010 CET	53	56534	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:42.498692036 CET	53	56627	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:42.562663078 CET	63116	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:42.614387035 CET	53	63116	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:43.756972075 CET	64078	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:43.822562933 CET	53	64078	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:44.746483088 CET	64801	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:44.798228025 CET	53	64801	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:46.438045025 CET	56534	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:46.438123941 CET	56627	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:46.489239931 CET	53	56627	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:46.489290953 CET	53	56534	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:46.557624102 CET	61721	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:46.609137058 CET	53	61721	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:50.880033970 CET	51255	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:50.935878992 CET	53	51255	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:51.810149908 CET	61522	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:51.859299898 CET	53	61522	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:52.723970890 CET	52337	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:52.783518076 CET	53	52337	8.8.8.8	192.168.2.4
Feb 25, 2021 21:22:53.989312887 CET	55046	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:22:54.046283960 CET	53	55046	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:00.868118048 CET	49612	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:00.926280975 CET	53	49612	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:01.419727087 CET	49285	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:01.478961945 CET	53	49285	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:01.837407112 CET	50601	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:01.905150890 CET	53	50601	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:02.058222055 CET	60875	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:02.109205961 CET	53	60875	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:02.595447063 CET	56448	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:02.652865887 CET	53	56448	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:03.134792089 CET	59172	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:03.229258060 CET	53	59172	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:03.772242069 CET	62420	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:03.825160027 CET	53	62420	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:04.359251976 CET	60579	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:04.411737919 CET	53	60579	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:05.752598047 CET	50183	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:05.802169085 CET	53	50183	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:06.681299925 CET	61531	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:06.773160934 CET	53	61531	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:07.231872082 CET	49228	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:07.285265923 CET	53	49228	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:11.661488056 CET	59794	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:11.713912010 CET	53	59794	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:18.465686083 CET	55916	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:18.532802105 CET	53	55916	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:21.383209944 CET	52752	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:21.391735077 CET	60542	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:21.435259104 CET	53	52752	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:21.452042103 CET	53	60542	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:23.951555967 CET	60689	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:24.013542891 CET	53	60689	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:29.167608976 CET	64206	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:23:29.201600075 CET	50904	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:29.223094940 CET	53	64206	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:29.268779993 CET	53	50904	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:30.075316906 CET	57525	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:30.126550913 CET	53	57525	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:30.761631966 CET	53814	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:30.765647888 CET	53418	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:30.819776058 CET	53	53814	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:30.825617075 CET	53	53418	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:31.764832020 CET	62833	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:31.818033934 CET	53	62833	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:31.847831011 CET	59260	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:31.901873112 CET	53	59260	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:32.099386930 CET	49944	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:32.148102999 CET	53	49944	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:55.229754925 CET	63300	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:55.284235001 CET	53	63300	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:55.959304094 CET	61449	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:56.012571096 CET	53	61449	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:57.056241989 CET	51275	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:57.122309923 CET	53	51275	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:59.140773058 CET	63492	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:59.191144943 CET	53	63492	8.8.8.8	192.168.2.4
Feb 25, 2021 21:23:59.832792044 CET	58945	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:23:59.891895056 CET	53	58945	8.8.8.8	192.168.2.4
Feb 25, 2021 21:24:00.140095949 CET	63492	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:24:00.190395117 CET	53	63492	8.8.8.8	192.168.2.4
Feb 25, 2021 21:24:00.825139046 CET	58945	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:24:00.875029087 CET	53	58945	8.8.8.8	192.168.2.4
Feb 25, 2021 21:24:01.137851954 CET	63492	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:24:01.187961102 CET	53	63492	8.8.8.8	192.168.2.4
Feb 25, 2021 21:24:01.840619087 CET	58945	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:24:01.889839888 CET	53	58945	8.8.8.8	192.168.2.4
Feb 25, 2021 21:24:03.138113976 CET	63492	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:24:03.186853886 CET	53	63492	8.8.8.8	192.168.2.4
Feb 25, 2021 21:24:03.840884924 CET	58945	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:24:03.892196894 CET	53	58945	8.8.8.8	192.168.2.4
Feb 25, 2021 21:24:07.153614044 CET	63492	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:24:07.204400063 CET	53	63492	8.8.8.8	192.168.2.4
Feb 25, 2021 21:24:07.856779099 CET	58945	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:24:07.907376051 CET	53	58945	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 21:23:18.465686083 CET	192.168.2.4	8.8.8.8	0x19c4	Standard query (0)	joom.ag	A (IP address)	IN (0x0001)
Feb 25, 2021 21:23:29.201600075 CET	192.168.2.4	8.8.8.8	0xc99f	Standard query (0)	joom.ag	A (IP address)	IN (0x0001)
Feb 25, 2021 21:23:30.075316906 CET	192.168.2.4	8.8.8.8	0x1e28	Standard query (0)	joom.ag	A (IP address)	IN (0x0001)
Feb 25, 2021 21:23:30.761631966 CET	192.168.2.4	8.8.8.8	0xe4b4	Standard query (0)	use.typekit.net	A (IP address)	IN (0x0001)
Feb 25, 2021 21:23:30.765647888 CET	192.168.2.4	8.8.8.8	0x7a4d	Standard query (0)	www.joomag.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:23:31.764832020 CET	192.168.2.4	8.8.8.8	0x8bd9	Standard query (0)	p.typekit.net	A (IP address)	IN (0x0001)
Feb 25, 2021 21:23:31.847831011 CET	192.168.2.4	8.8.8.8	0x3462	Standard query (0)	js-agent.newrelic.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:23:32.099386930 CET	192.168.2.4	8.8.8.8	0xe497	Standard query (0)	bam-cell.nr-data.net	A (IP address)	IN (0x0001)
Feb 25, 2021 21:23:55.959304094 CET	192.168.2.4	8.8.8.8	0xab5b	Standard query (0)	www.joomag.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:23:18.532802105 CET	8.8.8.8	192.168.2.4	0x19c4	No error (0)	joom.ag		209.95.50.27	A (IP address)	IN (0x0001)
Feb 25, 2021 21:23:29.268779993 CET	8.8.8.8	192.168.2.4	0xc99f	No error (0)	joom.ag		209.95.50.27	A (IP address)	IN (0x0001)
Feb 25, 2021 21:23:30.126550913 CET	8.8.8.8	192.168.2.4	0x1e28	No error (0)	joom.ag		209.95.50.27	A (IP address)	IN (0x0001)
Feb 25, 2021 21:23:30.819776058 CET	8.8.8.8	192.168.2.4	0xe4b4	No error (0)	use.typekit.net	use-stls.adobe.com.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:23:30.825617075 CET	8.8.8.8	192.168.2.4	0x7a4d	No error (0)	www.joomag.com	lb.joomag.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:23:30.825617075 CET	8.8.8.8	192.168.2.4	0x7a4d	No error (0)	lb.joomag.com		209.95.50.27	A (IP address)	IN (0x0001)
Feb 25, 2021 21:23:31.818033934 CET	8.8.8.8	192.168.2.4	0x8bd9	No error (0)	p.typekit.net	p.typekit.net-v3.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:23:31.901873112 CET	8.8.8.8	192.168.2.4	0x3462	No error (0)	js-agent.newrelic.com	f4.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:23:32.148102999 CET	8.8.8.8	192.168.2.4	0xe497	No error (0)	bam-cell.nr-data.net	tls12.newrelic.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:23:56.012571096 CET	8.8.8.8	192.168.2.4	0xab5b	No error (0)	www.joomag.com	lb.joomag.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:23:56.012571096 CET	8.8.8.8	192.168.2.4	0xab5b	No error (0)	lb.joomag.com		209.95.50.27	A (IP address)	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 25, 2021 21:23:30.419307947 CET	209.95.50.27	443	192.168.2.4	49773	CN=joom.ag, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Sep 15 16:24:35 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Sun Oct 17 16:24:35 CEST 2021 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 21:23:30.419775963 CET	209.95.50.27	443	192.168.2.4	49772	CN=joom.ag, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com /repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Sep 15 16:24:35 CEST 2020	Sun Oct 17 16:24:35 CEST 2021	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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com /repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Feb 25, 2021 21:23:31.090338945 CET	209.95.50.27	443	192.168.2.4	49776	CN=www.joomag.com, O="Joomag, Inc.", L=San Jose, ST=California, C=US, SERIALNUMBER=C3715754, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.2 =California, OID.1.3.6.1.4.1.311.60.2.1.3 =US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com /repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu Jan 28 22:07:13 CET 2021	Sun Jan 30 01:23:39 CET 2022	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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com /repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

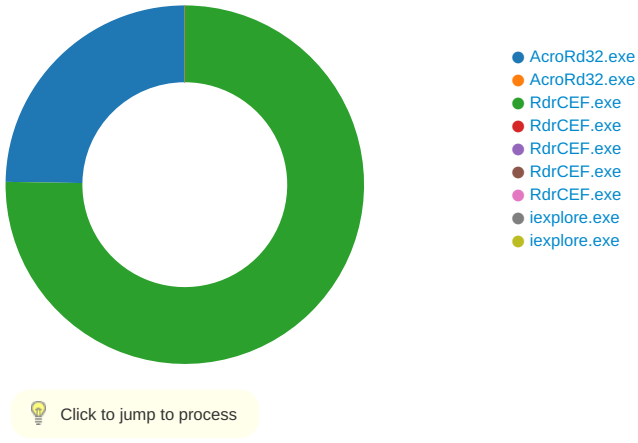
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 21:23:31.090507030 CET	209.95.50.27	443	192.168.2.4	49778	CN=www.joomag.com, O="Joomag, Inc.", L=San Jose, ST=California, C=US, SERIALNUMBER=C3715754, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.2=California, OID.1.3.6.1.4.1.311.60.2.1.3=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu Jan 28 22:07:13 CET 2021 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Sun Jan 30 01:23:39 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Feb 25, 2021 21:23:31.094206095 CET	209.95.50.27	443	192.168.2.4	49777	CN=www.joomag.com, O="Joomag, Inc.", L=San Jose, ST=California, C=US, SERIALNUMBER=C3715754, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.2=California, OID.1.3.6.1.4.1.311.60.2.1.3=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu Jan 28 22:07:13 CET 2021 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Sun Jan 30 01:23:39 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 21:23:56.266599894 CET	209.95.50.27	443	192.168.2.4	49786	CN=www.joomag.com, O="Joomag, Inc.", L=San Jose, ST=California, C=US, SERIALNUMBER=C3715754, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.2=California, OID.1.3.6.1.4.1.311.60.2.1.3=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu Jan 28 22:07:13 CET 2021 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Sun Jan 30 01:23:39 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: AcroRd32.exe PID: 7072 Parent PID: 5864

General

Start time:	21:22:22
Start date:	25/02/2021
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' 'C:\Users\user\Desktop\Send-Data-City_Center_Waco_Project_Report-_#9073955_942 (1).pdf'
Imagebase:	0x30000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx	read data or list directory | read attributes | write attributes | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	665C3	CreateDirectoryExW
C:\Users\user\AppData\Local\Temp\acrocef_low	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	8AE05	CreateDirectoryW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AdobeFnt16.lst.7148	write data or add file | append data or add subdirectory or create pipe instance | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	7EA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\acrolock7072.1.2949748092.tmp	read data or list directory | read ea | read attributes | delete | read control | synchronize	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	B2657	CreateFileW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.7148	write data or add file | append data or add subdirectory or create pipe instance | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	2	7EA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock7072.2.3432944109.tmp	read data or list directory | read ea | read attributes | delete | read control | synchronize	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	B2657	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock7072.3.1182233494.tmp	read data or list directory | read ea | read attributes | delete | read control | synchronize	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	B2657	CreateFileW
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	success or wait	1	7EA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210225202231Z-228.bmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	7EA85	NtCreateFile
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F83C8	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	F83C8	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	F83C8	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	F83C8	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	F83C8	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	F83C8	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R11o4zj2_ozzjta_5ik.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	7EA85	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	3	7EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rhhtwx6_ozzjtb_5ik.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	7EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rxhchxe_ozzjtc_5ik.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	7EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rnlja4b_ozzjtd_5ik.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	7EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R12x5u3u_ozzjte_5ik.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	7EA85	NtCreateFile

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AdobeFnt16.lst.7148	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AcroFnt19.lst	success or wait	1	BD405	NtSetInformationFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.7148	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst	success or wait	1	BD405	NtSetInformationFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.7148	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeCMapFnt19.lst	success or wait	1	BD405	NtSetInformationFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\System\Acrobatbrokerserverdispatchercpp789	success or wait	1	7CF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	7D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	7D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0 \cTab0\cPathInfo	success or wait	1	7D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\NoTimeOut	success or wait	1	7D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	3EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	3EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	3EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\TrustManager	success or wait	1	7D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\TrustManager\cDefaultLaunchURLPerms	success or wait	1	7D41D	NtCreateKey

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	aFS	unicode	DOS	success or wait	1	8DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/Users/user/Desktop/Send-Data-City_Center_Waco_Project_Report-_#9073955_942 (1).pdf	success or wait	1	8DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	Send-Data-City_Center_Waco_Project_Report-_#9073955_942 (1).pdf	success or wait	1	8DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	8DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	8DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDI	binary	2F 43 2F 55 73 65 72 73 2F 6A 6F 6E 65 73 2F 44 65 73 6B 74 6F 70 2F 53 65 6E 64 2D 44 61 74 61 2D 43 69 74 79 5F 43 65 6E 74 65 72 5F 57 61 63 6F 5F 50 72 6F 6A 65 63 74 5F 52 65 70 6F 72 74 2D 5F 23 39 30 37 33 39 35 35 5F 39 34 32 20 28 31 29 2E 70 64 66 00	success or wait	1	8DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDate	binary	44 3A 32 30 32 31 30 32 32 35 32 31 32 32 33 30 2B 30 31 27 30 30 27 00	success or wait	1	8DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	89559	success or wait	1	8DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	1	success or wait	1	8DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	8DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tDIText	unicode	http://www.adobe.com/go/homeacrordrunified18_2018	success or wait	1	8DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	8DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	8DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sDI	binary	68 74 74 70 3A 2F 2F 77 77 77 2E 61 64 6F 62 65 2E 63 6F 6D 2F 67 6F 2F 68 6F 6D 65 61 63 72 6F 72 64 72 75 6E 69 66 69 65 64 31 38 5F 32 30 31 38 00	success or wait	1	8DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sDate	binary	44 3A 32 30 31 39 30 36 32 37 31 31 31 33 35 31 2D 30 37 27 30 30 27 00	success or wait	1	8DF69	RegSetValueExW

Analysis Process: AcroRd32.exe PID: 7148 Parent PID: 7072

General

Start time:	21:22:23
Start date:	25/02/2021
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 'C:\Users\user\Desktop\Send-Data-City_Center_Waco_Project_Report-_#9073955_942 (1).pdf'
Imagebase:	0x30000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New 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: 6208 Parent PID: 7072

General

Start time:	21:22:29
Start date:	25/02/2021
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:	0xb50000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	success or wait	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	3	C459E2	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	6	C583E5	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	68	C58447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	163	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	6	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	18	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	6	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	3	C459E2	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	12	C459E2	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	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	1566	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	45	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	9	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	6	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	success or wait	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	end of file	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	success or wait	3	C459E2	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	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	success or wait	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	end of file	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	success or wait	6	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	end of file	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	success or wait	2	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	end of file	2	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	success or wait	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	end of file	3	C459E2	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	3	C459E2	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\js\selector.js	unknown	4096	end of file	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	success or wait	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	end of file	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	success or wait	18	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	end of file	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	success or wait	18	C459E2	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	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	success or wait	42	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	end of file	3	C459E2	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	45	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	end of file	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	success or wait	88	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	end of file	2	C459E2	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	3	C459E2	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	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	41	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	45	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	3	C459E2	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	14	C459E2	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	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	15	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	15	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	success or wait	15	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	end of file	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	179	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	216	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	3	C459E2	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	200	C459E2	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	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	49	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	end of file	2	C459E2	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	195	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	end of file	2	C459E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	22	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	3	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	success or wait	2	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	end of file	2	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	4	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	2	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	2	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	success or wait	1	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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	C459E2	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	C459E2	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	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	success or wait	8	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	end of file	1	C459E2	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	C459E2	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	C459E2	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	C459E2	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	C459E2	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	C583E5	ReadFile

Analysis Process: RdrCEF.exe PID: 6684 Parent PID: 6208

General

Start time:	21:22:32
Start date:	25/02/2021
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=1712,3132147786374165480,18202446835359099183,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=3943672393428629375 --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=3943672393428629375 --renderer-client-id=2 --mojo-platform-channel-handle=1724 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xb50000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 6556 Parent PID: 6208

General

Start time:	21:22:34
Start date:	25/02/2021
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=1712,3132147786374165480,18202446835359099183,131072 --disable-features=VizDisplayCompositor --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --lang=en-US --gpu-preferences=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=1360000876293854838 --mojo-platform-channel-handle=1740 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0xb50000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 4240 Parent PID: 6208

General

Start time:	21:22:36
Start date:	25/02/2021
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=1712,3132147786374165480,18202446835359099183,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=511033688939430806 --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=511033688939430806 --renderer-client-id=4 --mojo-platform-channel-handle=1856 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xb50000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 744 Parent PID: 6208

General

Start time:	21:22:40
Start date:	25/02/2021
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=1712,3132147786374165480,18202446835359099183,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=6159965884629463958 --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=6159965884629463958 --renderer-client-id=5 --mojo-platform-channel-handle=1860 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xb50000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 2740 Parent PID: 7072

General

Start time:	21:23:28
Start date:	25/02/2021

Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' https://joom.ag/9JYI
Imagebase:	0x7ff60df50000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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: iexplore.exe PID: 4720 Parent PID: 2740

General

Start time:	21:23:29
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2740 CREDAT:17410 /prefetch:2
Imagebase:	0x9c0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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

Disassembly

Code Analysis