ID: 349485
Sample Name: TETRATECH Covid-19 Stimulus Funds.pdf
Cookbook: defaultwindowspdfcookbook.jbs
Time: 23:21:18
Date: 05/02/2021
Version: 31.0.0 Emerald

Table of Contents

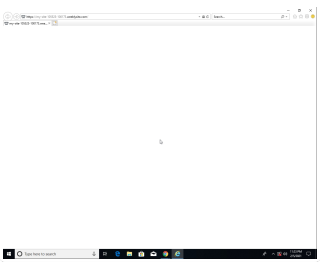
Analysis Report TETRATECH Covid-19 Stimulus Funds....

Overview

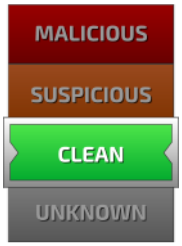
General Information

Sample Name:	TETRATECH Covid-19 Stimulus Funds.pdf
Analysis ID:	349485
MD5:	63deffe4ac48f83…
SHA1:	e7a4742dd14ad0..
SHA256:	96355ec73c87cf7..

Most interesting Screenshot:



Detection

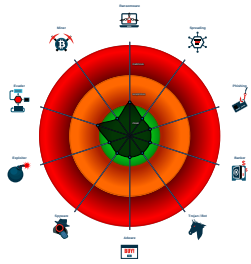


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

- Contains functionality to access load…
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…

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: 808 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\TETRATECH Covid-19 Stimulus Funds.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 6296 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\TETRATECH Covid-19 Stimulus Funds.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 6168 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6600 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=1728,5754072549746782878,9114216532001329358,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=3954240331908333317 --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=3954240331908333317 --renderer-client-id=2 --mojo-platform-channel-handle=1736 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6740 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1728,5754072549746782878,9114216532001329358,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=10276253575640265967 --mojo-platform-channel-handle=1748 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6608 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=1728,5754072549746782878,9114216532001329358,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=14130125459791333574 --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=14130125459791333574 --renderer-client-id=4 --mojo-platform-channel-handle=1844 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 7084 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=1728,5754072549746782878,9114216532001329358,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=8407246014169871722 --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=8407246014169871722 --renderer-client-id=5 --mojo-platform-channel-handle=2480 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
  - iexplore.exe (PID: 2740 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' https://my-site-105523-100173.weeblysite.com/ MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
    - iexplore.exe (PID: 4528 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

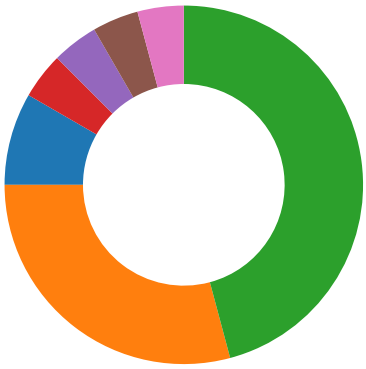
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

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



Click to jump to signature section

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

Compliance:

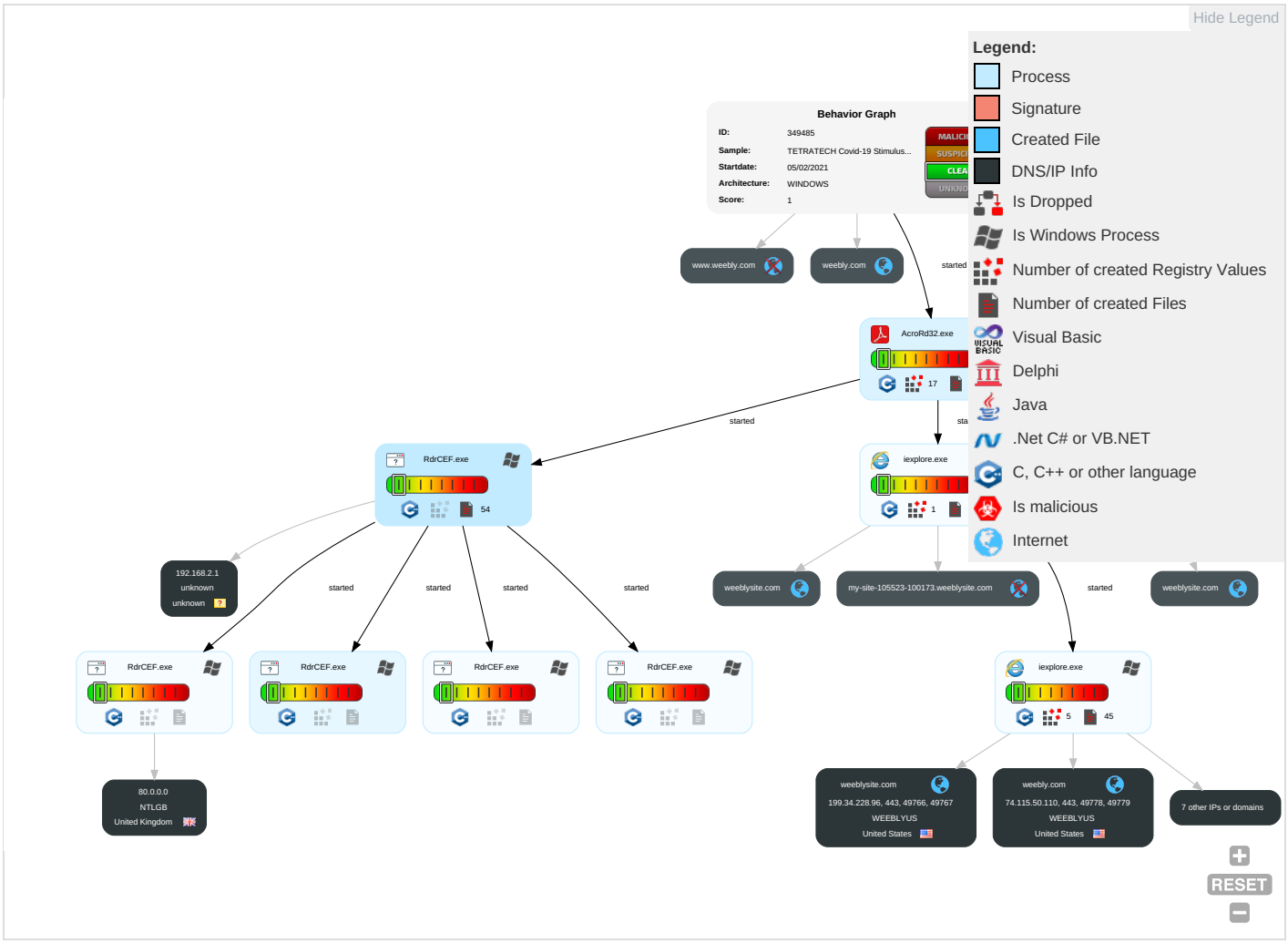
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	I
Spearphishing Link 1	Windows Management Instrumentation	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	I S I
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	Process Discovery 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

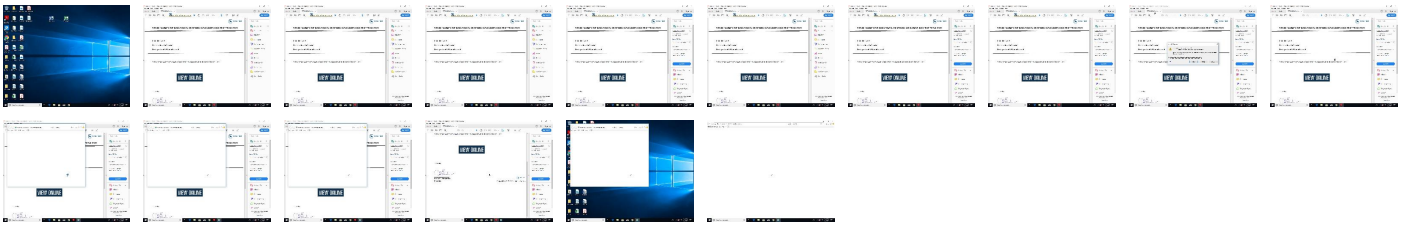
Behavior Graph

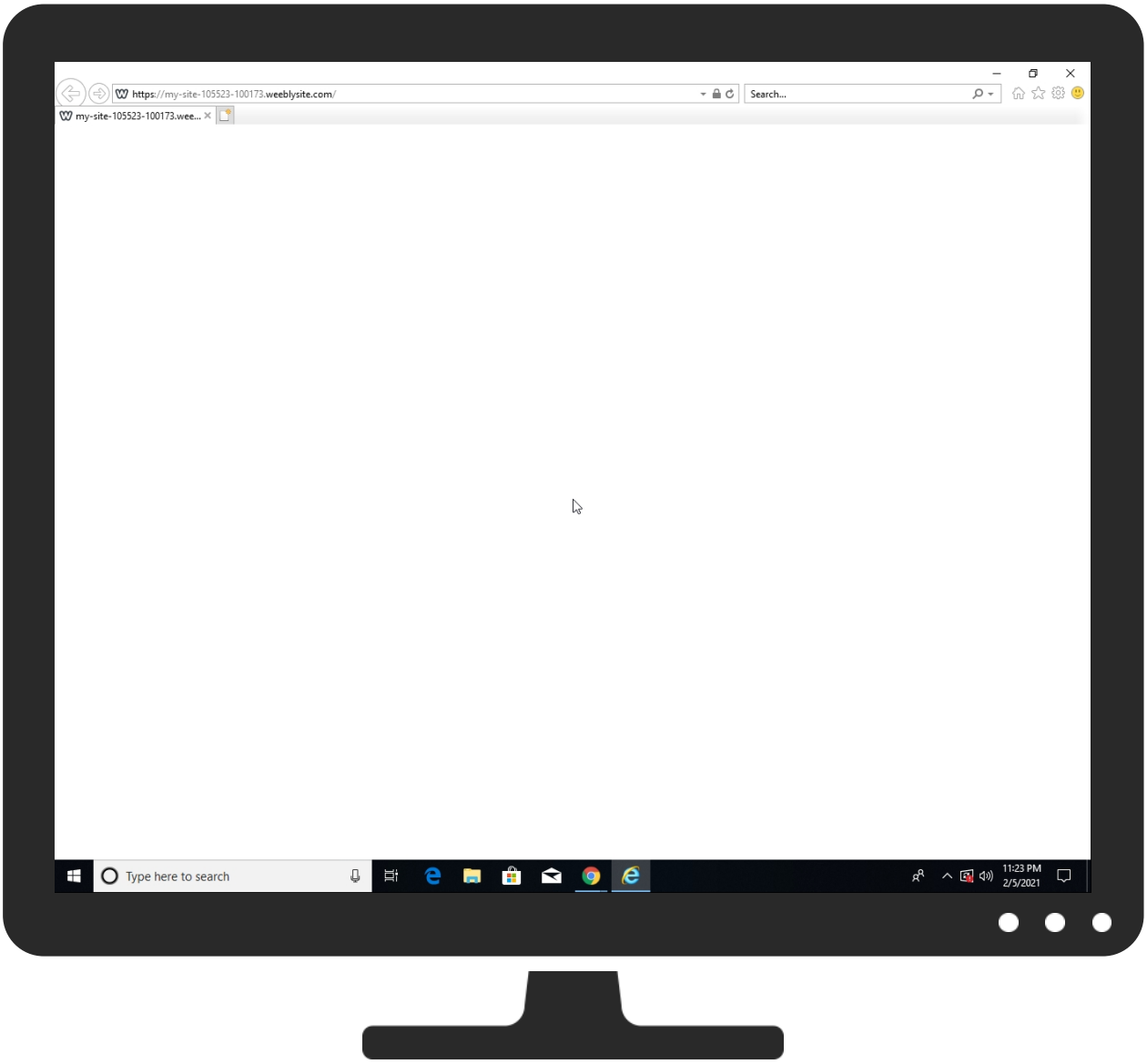


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
weebly.map.fastly.net	0%	Virustotal		Browse
weeblysite.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.npes.org/pdfx/ns/id/?n	0%	Avira URL Cloud	safe	
http://https://square.online	0%	Avira URL Cloud	safe	
http://https://my-site-105523-100173.weeblysite.com/)	0%	Avira URL Cloud	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://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://https://my-site-105523-100173.weeblysite.com/:	0%	Avira URL Cloud	safe	
http://https://images.editor.website	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/jM	0%	Avira URL Cloud	safe	
http://https://api.echosign.comH	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/A	0%	Avira URL Cloud	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://https://sandbox.square.online	0%	Avira URL Cloud	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://https://api.echosign.comRLW	0%	Avira URL Cloud	safe	
http://https://my-site-105523-100173.weeblysite.com/"	0%	Avira URL Cloud	safe	
http://https://my-site-105523-100173.weeblysite.com/Y	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://https://my-site-105523-100173.weeblysite.com/p	0%	Avira URL Cloud	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://https://ims-na1.adobelogin.com(	0%	Avira URL Cloud	safe	
http://https://.OKCancelEdit	0%	Avira URL Cloud	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://https://my-site-105523-100173.weeblysite.com/k	0%	Avira URL Cloud	safe	
http://https://f.fontdeck.com/s/css/js/	0%	Avira URL Cloud	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://cipa.jp/exif/1.0/(15)	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/(15)	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/(15)	0%	URL Reputation	safe	
http://https://my-site-105523-100173.weeblysite.com/Root	0%	Avira URL Cloud	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/4	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://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	

Source	Detection	Scanner	Label	Link
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	0%	Avira URL Cloud	safe	
http://https://my-site-105523-100173.weeblysite.com	0%	Avira URL Cloud	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://https://my-site-105523-100173.weebl	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sp-2020021412301152490000000a-1069308460.us-west-2.elb.amazonaws.com	54.212.183.219	true	false		high
weebly.map.fastly.net	151.101.1.46	true	false	• 0%, Virustotal, Browse	unknown
weeblysite.com	199.34.228.96	true	false	• 0%, Virustotal, Browse	unknown
weebly.com	74.115.50.110	true	false		high
ec.editmysite.com	unknown	unknown	false		high
my-site-105523-100173.weeblysite.com	unknown	unknown	false		unknown
cdn2.editmysite.com	unknown	unknown	false		high
www.weebly.com	unknown	unknown	false		high
cdn3.editmysite.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://my-site-105523-100173.weeblysite.com/	false		unknown

URLs from Memory and Binaries

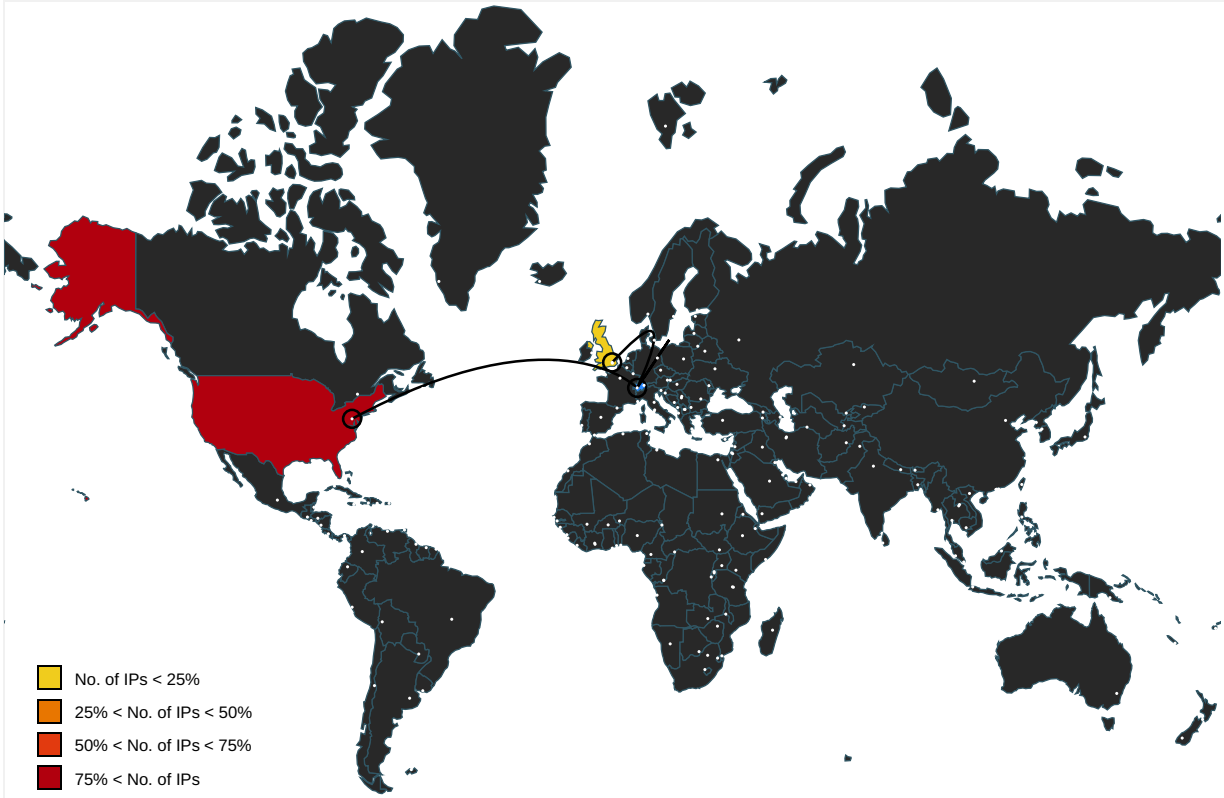
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.npes.org/pdfx/ns/id/?n	AcroRd32.exe, 00000001.00000003.804623464.000000000B3A7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/schema#b#	AcroRd32.exe, 00000001.00000002.822117594.000000000CC83000.00000004.00000001.sdmp	false		high
http://https://square.online	FVZBQN4S.htm.19.dr	false	• Avira URL Cloud: safe	unknown
http://https://use.typekit.net	site.19e2b99b084b05df36a8.en[1].js.19.dr	false		high
http://https://my-site-105523-100173.weeblysite.com/)	TETRATECH Covid-19 Stimulus Funds.pdf	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/schema#	AcroRd32.exe, 00000001.00000002.822117594.000000000CC83000.00000004.00000001.sdmp	false		high
http://https://my-site-105523-100173.weeblysite.com/	AcroRd32.exe, 00000001.00000002.806360065.00000000057D0000.00000002.00000001.sdmp, AcroRd32.exe, 00000001.00000002.819505702.000000000B13F000.00000004.00000001.sdmp, ~DF4E0B9E52D160D036.TMP.18.dr	false		unknown
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	AcroRd32.exe, 00000001.00000002.806893936.0000000007920000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.editmysite.com	FVZBQN4S.htm.19.dr	false		high
http://www.amazon.com/	msapplication.xml.18.dr	false		high
http://https://cdn3.editmysite.com/app/checkout/assets/checkout/imports.en.5190980851c8e63fd7692575cadd2295	FVZBQN4S.htm.19.dr	false		high
http://cipa.jp/exif/1.0/	AcroRd32.exe, 00000001.00000003.804623464.000000000B3A7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	AcroRd32.exe, 00000001.00000002.806893936.0000000007920000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.twitter.com/	msapplication.xml5.18.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://my-site-105523-100173.weeblysite.com/:	AcroRd32.exe, 00000001.00000002.819505702.000000000B13F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://images.editor.website	FVZBQN4S.htm.19.dr	false	• Avira URL Cloud: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/jM	AcroRd32.exe, 00000001.00000002.822117594.000000000CC83000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.echosign.comH	AcroRd32.exe, 00000001.00000002.822563679.000000000CE8C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/type#	AcroRd32.exe, 00000001.00000002.822117594.000000000CC83000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/property#V	AcroRd32.exe, 00000001.00000002.822117594.000000000CC83000.00000004.00000001.sdmp	false		high
http://https://cdn3.editmysite.com/app/checkout/assets/checkout/css/cko.e4d7b6c3391e50ded088.css	FVZBQN4S.htm.19.dr	false		high
http://www.aiim.org/pdfa/ns/id/bo	AcroRd32.exe, 00000001.00000003.804623464.000000000B3A7000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/A	AcroRd32.exe, 00000001.00000002.821877638.000000000CC18000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.echosign.com	AcroRd32.exe, 00000001.00000002.822563679.000000000CE8C000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	AcroRd32.exe, 00000001.00000002.822117594.000000000CC83000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.npes.org/pdfx/ns/id/	AcroRd32.exe, 00000001.00000003.804623464.000000000B3A7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/drm/default	AcroRd32.exe, 00000001.00000002.806893936.0000000007920000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/field#y#	AcroRd32.exe, 00000001.00000002.822117594.000000000CC83000.00000004.00000001.sdmp	false		high
http://https://cdn3.editmysite.com/app/website/js/site.19e2b99b084b05df36a8.en.js	FVZBQN4S.htm.19.dr	false		high
http://https://sandbox.square.online	FVZBQN4S.htm.19.dr	false	• Avira URL Cloud: safe	unknown
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	AcroRd32.exe, 00000001.00000002.806893936.0000000007920000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.echosign.comRLW	AcroRd32.exe, 00000001.00000002.822563679.000000000CE8C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://my-site-105523-100173.weeblysite.com/"	my-site-105523-100173.weeblysite[1].xml.19.dr	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/extension/	AcroRd32.exe, 00000001.00000002.822117594.000000000CC83000.00000004.00000001.sdmp	false		high
http://https://cdn3.editmysite.com/app/website/css/site.19e2b99b084b05df36a8.css	FVZBQN4S.htm.19.dr	false		high
http://https://cdn4.editmysite.com	FVZBQN4S.htm.19.dr	false		high
http://https://js.squareup.com/v2/paymentform	FVZBQN4S.htm.19.dr	false		high
http://www.aiim.org/pdfa/ns/extension/-29/	AcroRd32.exe, 00000001.00000002.822117594.000000000CC83000.00000004.00000001.sdmp	false		high
http://https://my-site-105523-100173.weeblysite.com/Y	AcroRd32.exe, 00000001.00000002.819505702.000000000B13F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.reddit.com/	msapplication.xml4.18.dr	false		high
http://www.osmf.org/subclip/1.0	AcroRd32.exe, 00000001.00000002.806893936.0000000007920000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/property#	AcroRd32.exe, 00000001.00000002.822117594.000000000CC83000.00000004.00000001.sdmp	false		high
http://https://my-site-105523-100173.weeblysite.com/p	AcroRd32.exe, 00000001.00000002.820173613.000000000B342000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	site.19e2b99b084b05df36a8.en[1].js.19.dr	false		high
http://ns.useplus.org/ldf/xmp/1.0/	AcroRd32.exe, 00000001.00000002.822117594.000000000CC83000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.nytimes.com/	msapplication.xml3.18.dr	false		high
http://https://ims-na1.adobelogin.com(	AcroRd32.exe, 00000001.00000002.811859867.0000000009175000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.aiim.org/pdfa/ns/field#8-02-29/m#D	AcroRd32.exe, 00000001.00000002.822117594.000000000CC83000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/id/	AcroRd32.exe, 00000001.00000003.804623464.000000000B3A7000.00000004.00000001.sdmp	false		high
http://https://.OKCancelEdit	AcroRd32.exe, 00000001.00000002.822702941.000000000CEC5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	AcroRd32.exe, 00000001.00000002.822117594.000000000CC83000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/layout/anchor	AcroRd32.exe, 00000001.00000002.806893936.0000000007920000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://my-site-105523-100173.weeblysite.com/k	AcroRd32.exe, 00000001.00000002.819505702.000000000B13F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/type##nifestItem#r	AcroRd32.exe, 00000001.00000002.822117594.000000000CC83000.00000004.00000001.sdmp	false		high
http://https://f.fontdeck.com/s/css/js/	site.19e2b99b084b05df36a8.en[1].js.19.dr	false	• Avira URL Cloud: safe	unknown
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	AcroRd32.exe, 00000001.00000002.822117594.000000000CC83000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfe/ns/id/	AcroRd32.exe, 00000001.00000003.804623464.000000000B3A7000.00000004.00000001.sdmp	false		high
http://https://cdn3.editmysite.com/app/website/	FVZBQN4S.htm.19.dr	false		high
http://cipa.jp/exif/1.0/(15)	AcroRd32.exe, 00000001.00000003.804623464.000000000B3A7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://getbootstrap.com/)	site.19e2b99b084b05df36a8[1].css.19.dr	false		high
http://https://cdn3.editmysite.com/app/checkout/assets/checkout/js/system.min.b9e210033fc5b0895164e282cbf89	FVZBQN4S.htm.19.dr	false		high
http://https://www.weebly.com/favicon.ico	imagestore.dat.19.dr, FVZBQN4S.htm.19.dr	false		high
http://https://my-site-105523-100173.weeblysite.com/Root	{B9DB4C8A-6800-11EB-90EB-ECF4BBEA1588}.dat.18.dr	false	• Avira URL Cloud: safe	unknown
http://https://feross.org	site.19e2b99b084b05df36a8.en[1].js.19.dr	false		high
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/4	AcroRd32.exe, 00000001.00000002.822117594.000000000CC83000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://cipa.jp/exif/1.0/_1	AcroRd32.exe, 00000001.00000003.804623464.000000000B3A7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.youtube.com/	msapplication.xml7.18.dr	false		high
http://www.aiim.org/pdfa/ns/field#	AcroRd32.exe, 00000001.00000002.822117594.000000000CC83000.00000004.00000001.sdmp	false		high
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	AcroRd32.exe, 00000001.00000002.806893936.0000000007920000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	site.19e2b99b084b05df36a8[1].css.19.dr	false		high
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/	AcroRd32.exe, 00000001.00000002.821877638.000000000CC18000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.live.com/	msapplication.xml2.18.dr	false		high
http://https://my-site-105523-100173.weeblysite.com	AcroRd32.exe, 00000001.00000002.821877638.000000000CC18000.00000004.00000001.sdmp, FVZBQN4S.htm.19.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.quicktime.com.Acrobat	AcroRd32.exe, 00000001.0000000 2.806893936.0000000007920000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 00000001.0000000 2.811859867.0000000009175000.0 0000004.00000001.sdmp	false		high
http:// https://cdn3.editmysite.com/app/website/js/runtime.4c27edfb5 1f63cc2e6e5.en.js	FVZBQN4S.htm.19.dr	false		high
http://https://www.weebly.com	FVZBQN4S.htm.19.dr	false		high
http://https://my-site-105523-100173.weebl	AcroRd32.exe, 00000001.0000000 2.805992709.000000000510D000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
74.115.50.110	unknown	United States		27647	WEEBLYUS	false
199.34.228.96	unknown	United States		27647	WEEBLYUS	false
54.212.183.219	unknown	United States		16509	AMAZON-02US	false
151.101.1.46	unknown	United States		54113	FASTLYUS	false
80.0.0.0	unknown	United Kingdom		5089	NTLGB	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	349485
Start date:	05.02.2021

Start time:	23:21:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TETRATECH Covid-19 Stimulus Funds.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:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.winPDF@17/74@8/6
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): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 104.42.151.234, 13.64.90.137, 23.211.4.250, 2.20.143.130, 2.20.142.203, 104.43.193.48, 51.104.139.180, 92.122.213.247, 92.122.213.194, 52.155.217.156, 20.54.26.129, 205.185.216.42, 205.185.216.10, 88.221.62.148, 152.199.19.161 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, e4578.dscb.akamaiedge.net, a1449.dscg2.akamai.net, acroipm2.adobe.com, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, a122.dscd.akamai.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, acroipm2.adobe.com.edgesuite.net, ie9comview.vo.msecnd.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, cds.d2s7q6s2.hwcdn.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, armmf.adobe.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.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
23:22:13	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
74.115.50.110	http://www.sipadmin.org	Get hash	malicious	Browse	• www.weebly.com/uploads/reseller/assets/1001-favicon.ico
199.34.228.96	http://accountonline111.weeblysite.com	Get hash	malicious	Browse	• accountonline111.weeblysite.com/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
151.101.1.46	http://www.secured-mailsharepoint.online/	Get hash	malicious	Browse	• cdn2.editmysite.com/js/wsnbn/snowday262.js
	http://www.sipadmin.org	Get hash	malicious	Browse	• cdn2.editmysite.com/fonts/Proxima-Semibold/267447_5_0.eot?
	http://volusion-cdn.com	Get hash	malicious	Browse	• cdn2.editmysite.com/components/ui-framework/fonts/proxima-nova-regular/31AC96_1_0eot?
	http://www.ghostquest.net	Get hash	malicious	Browse	• cdn2.editmysite.com/js/wsnbn/snowday262.js
	ConfidentialOneDrive (13).pdf	Get hash	malicious	Browse	• cdn2.editmysite.com/components/ui-framework/fonts/proxima-nova-regular/31AC96_1_0eot?
80.0.0.0	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	
	http://https://public.3.basecamp.com/p/2D4prniZtSHtN5Qfx4XocXX3	Get hash	malicious	Browse	
	http://https://bouthilletteparizeau-my.sharepoint.com/:b:/g/personal/jproulx_bpa_ca/EYQbKRRM1_VEjGeslLjc5GwB075qH34FcIdpShYIw3DxFA?e=4%3abltg7p&at=9	Get hash	malicious	Browse	
	ds7002.lnk	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
sp-20200214123011524900000000a-1069308460.us-west-2.elb.amazonaws.com	http://https://blackberry4660212.brizy.site/	Get hash	malicious	Browse	• 52.43.130.34
	http://https://blackberry4660212.brizy.site/	Get hash	malicious	Browse	• 52.43.130.34
	http://https://voicemailfaxxmicrosoft.weebly.com/index.html	Get hash	malicious	Browse	• 44.238.255.95
	http://https://applicationoule7siteinternet.yolasite.com	Get hash	malicious	Browse	• 52.89.248.14
	http://officemaisa.weebly.com	Get hash	malicious	Browse	• 44.240.213.40
	http://https://schoola.page.link/tobR	Get hash	malicious	Browse	• 52.89.248.14
	http://https://gjhujkbjvjhvhvjhbjk.weebly.com/	Get hash	malicious	Browse	• 44.240.213.40
	http://staffbenefitsforall.weebly.com	Get hash	malicious	Browse	• 44.240.213.40

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://doc.clickup.com/p/h/84zph-7/c3996c24fc61b45	Get hash	malicious	Browse	• 35.163.165.143
	http://https://devhuy.weebly.com	Get hash	malicious	Browse	• 35.163.165.143
	http://microsoftonlineofficeteam.weebly.com	Get hash	malicious	Browse	• 35.163.165.143
	http://https://verify-outlook-web.weebly.com/	Get hash	malicious	Browse	• 34.211.101.240
	http://https://urldefense.com/v3/__https://our4home.weebly.com/__;!!Mih3wA!Qz0aR1KaZW-jrB9FELx-FwKRvoLP2Tej_V_sM6iMx39anDNA-j7H7Aog9Wq1X_HWkx4j$	Get hash	malicious	Browse	• 52.89.244.135
	http://https://lasopausb720.weebly.com/outkast-aquemini-320-rar.html	Get hash	malicious	Browse	• 34.211.101.240
	http://nslasopa101.weebly.com	Get hash	malicious	Browse	• 44.236.21.127
	http://https://doc.clickup.com/p/h/83jc9-21/f762ea9849fc82d	Get hash	malicious	Browse	• 44.236.21.127
	http://https://fhemigiii.weebly.com/	Get hash	malicious	Browse	• 52.42.73.23
	http://https://www.canva.com/design/DAEKyhVZru8/tgMv_Re_5O0_pQ57iE7S2Q/view?utm_content=DAEKyhVZru8&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 52.42.73.23
	http://https://veriftechowa2000011.weebly.com/	Get hash	malicious	Browse	• 52.42.73.23
	http://https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiHosPY-bjsAhUtmYsKHQijCa4QFjAAegQIARAC&url=https%3A%2F%2Fpotenthacker723.weebly.com%2Fanalysis-of-competing-hypotheses-software-free-mac.html&usg=AOvVaw3aT7apVGNx2SMuBf--c0Xa	Get hash	malicious	Browse	• 44.241.221.48
weebly.map.fastly.net	http://www.secured-mailsharepoint.online/	Get hash	malicious	Browse	• 151.101.1.46
	http://https://tgdbdandh.weebly.com/	Get hash	malicious	Browse	• 151.101.1.46
	http://xr4vx.mjt.lu/lnk/AUoAABsLUG8AAAAAGfgAAACj9UAAAAAAKt8AABmeABbN0QBf4eQgZ6X6UmPITHmCxUtOpOQ3LgAWb3k/1/7xzJOeWvDV8gVh3D7WayEg/aHR0cHM6Ly9uZXd2b2ljZW1haWxkaXJlY3RvcnltZXNzYWdlLndlZWJseS5jb20v	Get hash	malicious	Browse	• 151.101.1.46
	http://https://blackberry4660212.brizy.site/	Get hash	malicious	Browse	• 151.101.1.46
	http://https://blackberry4660212.brizy.site/	Get hash	malicious	Browse	• 151.101.1.46
	http://https://voicemailfaxxmicrosoft.weebly.com/index.html	Get hash	malicious	Browse	• 151.101.1.46
	http://https://joom.ag/eoFC	Get hash	malicious	Browse	• 151.101.1.46
	http://https://0fficefax365.quip.com/FENkAKwe58Ee	Get hash	malicious	Browse	• 151.101.1.46
	http://https://applicationoule7siteinternet.yolasite.com	Get hash	malicious	Browse	• 151.101.1.46
	http://https://officemaisa.weebly.com/	Get hash	malicious	Browse	• 151.101.1.46
	http://officemaisa.weebly.com	Get hash	malicious	Browse	• 151.101.1.46
	http://https://schoola.page.link/tobR	Get hash	malicious	Browse	• 151.101.1.46
	http://https://doc.clickup.com/p/h/853bx-28/ee9d693560ec8e5	Get hash	malicious	Browse	• 151.101.1.46
	http://https://gjhujkbjvjhvhvjhbjk.weebly.com/	Get hash	malicious	Browse	• 151.101.1.46
	http://staffbenefitsforall.weebly.com	Get hash	malicious	Browse	• 151.101.1.46
	http://https://doc.clickup.com/p/h/84zph-7/c3996c24fc61b45	Get hash	malicious	Browse	• 151.101.1.46
	http://https://devhuy.weebly.com	Get hash	malicious	Browse	• 151.101.1.46
	http://microsoftonlineofficeteam.weebly.com	Get hash	malicious	Browse	• 151.101.1.46
	http://https://verify-outlook-web.weebly.com/	Get hash	malicious	Browse	• 151.101.1.46
	http://https://urldefense.com/v3/__https://our4home.weebly.com/__;!!Mih3wA!Qz0aR1KaZW-jrB9FELx-FwKRvoLP2Tej_V_sM6iMx39anDNA-j7H7Aog9Wq1X_HWkx4j$	Get hash	malicious	Browse	• 151.101.1.46

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	drTj5hZSCU.exe	Get hash	malicious	Browse	• 13.248.196.204
	PR Agreement FEB2021.xlsx	Get hash	malicious	Browse	• 18.159.48.76
	PR Office FEB05 2021 .xlsx	Get hash	malicious	Browse	• 18.159.48.76
	RqJSPKzbZN.exe	Get hash	malicious	Browse	• 99.86.162.148
	G1h589g5qV.exe	Get hash	malicious	Browse	• 34.209.40.84
	J3crPiDHbM.exe	Get hash	malicious	Browse	• 34.221.125.90
	pJJwTPDTrk.exe	Get hash	malicious	Browse	• 34.221.125.90
	6ZhcnUCHNK.exe	Get hash	malicious	Browse	• 34.221.125.90
	czYCU2Zn9v.exe	Get hash	malicious	Browse	• 34.221.125.90
	WoG4MUoiUv.exe	Get hash	malicious	Browse	• 54.215.217.171
	QaK2x5jv7i.exe	Get hash	malicious	Browse	• 54.215.217.171
	THZtxPSutu.exe	Get hash	malicious	Browse	• 34.221.125.90

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	M74VY7pu2e.exe	Get hash	malicious	Browse	• 54.190.50.234
	5XwNDrYRcS.exe	Get hash	malicious	Browse	• 34.221.125.90
	kSRc73X8kR.exe	Get hash	malicious	Browse	• 34.221.125.90
	2yyLUUryvi.exe	Get hash	malicious	Browse	• 34.221.125.90
	k3uUyLVDaM.exe	Get hash	malicious	Browse	• 54.190.50.234
	GW1TTIuSKJ.exe	Get hash	malicious	Browse	• 54.190.50.234
	H6nGMsVg7h.exe	Get hash	malicious	Browse	• 34.209.41.233
	da4tsAIXOU.exe	Get hash	malicious	Browse	• 34.209.41.233
WEEBLYUS	PR Agreement FEB2021.xlsx	Get hash	malicious	Browse	• 199.34.228.73
	Payment Advice_Pdf.exe	Get hash	malicious	Browse	• 199.34.228.170
	2S6VUd960E.exe	Get hash	malicious	Browse	• 199.34.228.73
	Bp93hBPMoi.exe	Get hash	malicious	Browse	• 199.34.228.49
	win32.exe	Get hash	malicious	Browse	• 199.34.228.68
	gPGTcEMoM1.exe	Get hash	malicious	Browse	• 199.34.228.73
	_RFQ_MVSEASAIL_34.xlsx	Get hash	malicious	Browse	• 199.34.228.68
	SKM_C221200706052800n.exe	Get hash	malicious	Browse	• 199.34.228.171
	_MVSEASEAL_RFQ_.xlsx	Get hash	malicious	Browse	• 199.34.228.77
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 199.34.228.76
	pY5XEdTwX7.exe	Get hash	malicious	Browse	• 199.34.228.167
	dir1.exe	Get hash	malicious	Browse	• 199.34.228.73
	AnGaRFyL4O.exe	Get hash	malicious	Browse	• 199.34.228.77
	YUAN PAYMENT.exe	Get hash	malicious	Browse	• 199.34.228.77
	Invoice_20210115122010.exe	Get hash	malicious	Browse	• 199.34.228.76
	Packing list #U2022 Invoice #U2022 Country of origin.exe	Get hash	malicious	Browse	• 199.34.228.164
	Dd0qD6dTem.exe	Get hash	malicious	Browse	• 199.34.228.75
	n1W2zlEddS.exe	Get hash	malicious	Browse	• 199.34.228.73
	NEW 01 13 2021.xlsx	Get hash	malicious	Browse	• 199.34.228.73
	quotation.exe	Get hash	malicious	Browse	• 199.34.228.164
WEEBLYUS	PR Agreement FEB2021.xlsx	Get hash	malicious	Browse	• 199.34.228.73
	Payment Advice_Pdf.exe	Get hash	malicious	Browse	• 199.34.228.170
	2S6VUd960E.exe	Get hash	malicious	Browse	• 199.34.228.73
	Bp93hBPMoi.exe	Get hash	malicious	Browse	• 199.34.228.49
	win32.exe	Get hash	malicious	Browse	• 199.34.228.68
	gPGTcEMoM1.exe	Get hash	malicious	Browse	• 199.34.228.73
	_RFQ_MVSEASAIL_34.xlsx	Get hash	malicious	Browse	• 199.34.228.68
	SKM_C221200706052800n.exe	Get hash	malicious	Browse	• 199.34.228.171
	_MVSEASEAL_RFQ_.xlsx	Get hash	malicious	Browse	• 199.34.228.77
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 199.34.228.76
	pY5XEdTwX7.exe	Get hash	malicious	Browse	• 199.34.228.167
	dir1.exe	Get hash	malicious	Browse	• 199.34.228.73
	AnGaRFyL4O.exe	Get hash	malicious	Browse	• 199.34.228.77
	YUAN PAYMENT.exe	Get hash	malicious	Browse	• 199.34.228.77
	Invoice_20210115122010.exe	Get hash	malicious	Browse	• 199.34.228.76
	Packing list #U2022 Invoice #U2022 Country of origin.exe	Get hash	malicious	Browse	• 199.34.228.164
	Dd0qD6dTem.exe	Get hash	malicious	Browse	• 199.34.228.75
	n1W2zlEddS.exe	Get hash	malicious	Browse	• 199.34.228.73
	NEW 01 13 2021.xlsx	Get hash	malicious	Browse	• 199.34.228.73
	quotation.exe	Get hash	malicious	Browse	• 199.34.228.164

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	1872.docx	Get hash	malicious	Browse	• 199.34.228.96 • 54.212.183.219 • 151.101.1.46 • 74.115.50.110
	ace80239facd926583cb2f9ceb84bb9c.exe	Get hash	malicious	Browse	• 199.34.228.96 • 54.212.183.219 • 151.101.1.46 • 74.115.50.110
	82e6033fb85f4abe59e16cb29c9faca2.exe	Get hash	malicious	Browse	• 199.34.228.96 • 54.212.183.219 • 151.101.1.46 • 74.115.50.110

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Invoice 1028613.html	Get hash	malicious	Browse	• 199.34.228.96 • 54.212.183.219 • 151.101.1.46 • 74.115.50.110
	ioir.png.dll	Get hash	malicious	Browse	• 199.34.228.96 • 54.212.183.219 • 151.101.1.46 • 74.115.50.110
	umAuo1QklZ.dll	Get hash	malicious	Browse	• 199.34.228.96 • 54.212.183.219 • 151.101.1.46 • 74.115.50.110
	PO_2856_from_Giancarlo_Distributing_Inc.htm	Get hash	malicious	Browse	• 199.34.228.96 • 54.212.183.219 • 151.101.1.46 • 74.115.50.110
	B33383838558-857585.htm	Get hash	malicious	Browse	• 199.34.228.96 • 54.212.183.219 • 151.101.1.46 • 74.115.50.110
	#U260e#Ufe0fmsg0100February_report_2021.HTM	Get hash	malicious	Browse	• 199.34.228.96 • 54.212.183.219 • 151.101.1.46 • 74.115.50.110
	5aa085f0fa8592460e391052db9c94cd.exe	Get hash	malicious	Browse	• 199.34.228.96 • 54.212.183.219 • 151.101.1.46 • 74.115.50.110
	ace80239facd926583cb2f9ceb84bb9c.exe	Get hash	malicious	Browse	• 199.34.228.96 • 54.212.183.219 • 151.101.1.46 • 74.115.50.110
	wys-02-03-21 Statement_763108aGF5ZGVuag==.htm	Get hash	malicious	Browse	• 199.34.228.96 • 54.212.183.219 • 151.101.1.46 • 74.115.50.110
	A6C8E866.xlsx	Get hash	malicious	Browse	• 199.34.228.96 • 54.212.183.219 • 151.101.1.46 • 74.115.50.110
	Maersk_BL Draft_copy_Shipping_documents.html	Get hash	malicious	Browse	• 199.34.228.96 • 54.212.183.219 • 151.101.1.46 • 74.115.50.110
	POrder.html	Get hash	malicious	Browse	• 199.34.228.96 • 54.212.183.219 • 151.101.1.46 • 74.115.50.110
	CONSTANTINE.xlsx	Get hash	malicious	Browse	• 199.34.228.96 • 54.212.183.219 • 151.101.1.46 • 74.115.50.110
	Document0098.html	Get hash	malicious	Browse	• 199.34.228.96 • 54.212.183.219 • 151.101.1.46 • 74.115.50.110
	#U266b Audio_47720.wavv - - Copy.htm	Get hash	malicious	Browse	• 199.34.228.96 • 54.212.183.219 • 151.101.1.46 • 74.115.50.110
	d0b443110cf5a7bd05759c00fee8fdad.exe	Get hash	malicious	Browse	• 199.34.228.96 • 54.212.183.219 • 151.101.1.46 • 74.115.50.110
	univarusa-02-02-21 Statement_367096cmFuZHkuZnJpZWRsZXk=.htm	Get hash	malicious	Browse	• 199.34.228.96 • 54.212.183.219 • 151.101.1.46 • 74.115.50.110
37f463bf4616ecd445d4a1937da06e19	wMbMIqppdf.dll	Get hash	malicious	Browse	• 74.115.50.110
	aeq6IToVRq.exe	Get hash	malicious	Browse	• 74.115.50.110
	BO61CeKOmR.exe	Get hash	malicious	Browse	• 74.115.50.110
	DHL_409011 documento de recibo,pdf.exe	Get hash	malicious	Browse	• 74.115.50.110
	cWqtbHhPkT.exe	Get hash	malicious	Browse	• 74.115.50.110
	DHL_409011 documento de recibo,pdf.exe	Get hash	malicious	Browse	• 74.115.50.110
	FACA000400007998.pdf.exe	Get hash	malicious	Browse	• 74.115.50.110
	6TIO7HUX.dll	Get hash	malicious	Browse	• 74.115.50.110
	Jvy9cK1Kjg.xlsm	Get hash	malicious	Browse	• 74.115.50.110

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	contract (78).xls	Get hash	malicious	Browse	• 74.115.50.110
	full (24).xls	Get hash	malicious	Browse	• 74.115.50.110
	_____ ___ _____ 17-11-2020.ppt	Get hash	malicious	Browse	• 74.115.50.110
	_____ __ _____ 19-10-2020.ppt	Get hash	malicious	Browse	• 74.115.50.110
	yYATxT9WWz.ppt	Get hash	malicious	Browse	• 74.115.50.110
	87ba36cf5356cc4ec3f1.ppt	Get hash	malicious	Browse	• 74.115.50.110
	pHLVDZ36iH.pps	Get hash	malicious	Browse	• 74.115.50.110
	Icon.exe	Get hash	malicious	Browse	• 74.115.50.110
	BILL.pps	Get hash	malicious	Browse	• 74.115.50.110
	company details.pps	Get hash	malicious	Browse	• 74.115.50.110
	credit card auth.ppt	Get hash	malicious	Browse	• 74.115.50.110

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):	5.679029734711339
Encrypted:	false
SSDEEP:	12:vDRM9oMZiEDHDRM92uS5itZiETDRM9aRjRZiE:7Z5EDjyS5HEnxReE
MD5:	870F4DF62CAAD2F1E9C0F36233B5A850
SHA1:	834304F185877C4695D7BA61387B698B98DCC2F3
SHA-256:	BE347C9C396F112FB269CA4512769888EA0D1CF4AA7477606E86EBECC7FA8E45
SHA-512:	25CD55E1815A7A3B6DC1E8014DA4265432BA0A485769A81D68B5C2E5E63A52D0E28F8C68505CE68B3C7D6655B1E2A04481A5D37092A278D034346F639875FFF2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .].X.4./....."#.D.{.Fq..A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....r..e.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .Dm..4./....."#.D.H.Gq..A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....1Nu.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ....4./....."#.D...Iq..A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....-z1X.....

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):	5.640640120875715
Encrypted:	false
SSDEEP:	12:V9zN4FZ9PQHl9zgDjS9PQMH9zMEhW9PQp:XzN4FZ9PQHzwjS9PQMdzMEY9PQ
MD5:	E8DC1353B14EE9DB476EFCA5986B0BD3
SHA1:	DBBDFAC5C9ACAA7A6466FE16B692BF8F07DB1DA5
SHA-256:	7E72DAEEFDB3707BA83D7F34EFD2E1529FD93FC0263C3644459F0A84BCC6FFE3
SHA-512:	3901B0F43B8393EAECB2AF7CFA348DC804724C40550797D93ABBF844C9BA3E376FE991713C1DAC6BD830DE0FA41132AA2005F8E627290669703DA5EA2749815
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .V.G.4./....."#.Dw.gFq..A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....z.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ....4./....."#.D.nGq..A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....G.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ..,.4./....."#.D...Hq..A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....`Q.....

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):	5.631355520623835

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
Encrypted:	false
SSDEEP:	12:DyeRVFAFjVFAFGQYlUo6jb5yeRVFAFjVFAFlBX9lUo6jebyeRVFAFjVFAFOE170N:tB4v4GTSBb3B4v4lBX9SBelB4v4OE1YN
MD5:	0BA8CF4C624A1AEF42B930DBC5E7DBF8
SHA1:	43640AD27D0EF7DE0EBB0CDDE9D2B5DA29B0A2BF
SHA-256:	5A8F731AC9946DB881E72F2519F0C8F1145DA38C020520579F048B1611AB66EA
SHA-512:	4E66F81F8BDB270E499203CC6B0E18C5AFBCD19866C3101D38AACAB174411CBC5DEE7655ADCC3E8ED897B4E2C740D20B75B0C986D523D161DDEEE367DF44D67
Malicious:	false
Reputation:	low
Preview:	0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ...X.4./....."#.D...Fq..A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....O!.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ..j..4./....."#.D...Gq..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 .;Z.4./....."#.D.].lq..A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....h.....

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):	5.694546279614764
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RseZFV2iWulHyA1TK6tR2NtVYOFLvEWdFCi5Rs7aaK1yj2iK:IbRkiDlFWusszYbRkiDauuWuss4
MD5:	CAD96B1CFCE45BB81E5DD5BC6A753A03
SHA1:	219E90395A5DB55CAED6393A59FA21DC3DEE170C
SHA-256:	3816C75FDC7824296A6D0540CEF106D9BB896343DB886D16541985F498AFE0B1
SHA-512:	8737B14A27698FB8737657BA2BD7C97803377829BF3011E40A9294E01C3503889FC414288063F1160FA289905B6C3F6BF2693048BF051CE2319023CE005BDFB5
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 .k.\.4./....."#.DIH.Fq..A..8 P..a...R..Y....7.@..2Dm{..A..Eo.....A..Eo.....a.....0\r..m.....h....'...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js .....4./....."#.D!..Gq..A..8 P..a...R..Y....7.@..2Dm{..A..Eo.....A..Eo.....zq.....

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):	5.600987993026847
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVuPvR7Vyh9PT41TK6t:pyixRu5J7V41TE
MD5:	2E6C005BB8B89D5E941A38A4EF0FB86F
SHA1:	0043057116B142F370066A22E06A0AA2822D1B31
SHA-256:	85D68E53649066D8FC82BC4AE90828BEEAC6B622FCF68F2F2284AE3710AC4AEA
SHA-512:	EECF5DEA36347004344046E9103993B28230E1C7351A69183CA80A11F5791B316C0392029935168E22730F9D756545BD886F4708D77150809CB74E1B0C9AA6A7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ....4./....."#.DC=.Iq..Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo.....}.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.634402013489074
Encrypted:	false
SSDEEP:	3:m+lifll08RzYOCGLvHkWBGKuKjXKoyNjXKLuVmDaemh4qhco2sZI8xeGvP5m1TK3:mvYOFLvEWdhwjQR0LLZII6P41TK6tMl
MD5:	2918D9AED71B4EE855A1C9C11BA322CE
SHA1:	C4DB94CF466990E62D4AE624788654B4EE1E2407
SHA-256:	93318DB6461CEC460B36CCFF4FEDB48CEDD9D0A717CCF1DEA45DC15346E90DA0
SHA-512:	DA975FFC54F9CCD9D66712D9C69493A632A762450BE175BAB711A32A69BEE23C67BA25D67DBA6648E353BA86B5BEFF06738F710AD972B16627C0F3FC0B421274
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ..=.4./....."#.D...Hq..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
Entropy (8bit):	5.523092282874443
Encrypted:	false
SSDEEP:	3:m+lZd8RzYOCGLvHkWBGKuKjXKX7KoQRA/KVdKLuVlTtx9eFcyxMtv9EWm1TK5ktv:mJYOFLvEWdGQRQOdQsY6g1TK6tv
MD5:	C2BD328369D1E0948D01DD05AC792713
SHA1:	540ADDA737DA61CE0229E9CB3FBA548318FE5786
SHA-256:	5EAF7A32B9A377FD82F6236C26B63FF22256C301634FBC6D094A6B76EE0E5559
SHA-512:	08A1A8E6560B383936AC29C4070957563FC447F05A349D7BD747BF82050C82BC93A25822206F3290A6DD7FA0802136E11AEECA08ABC12B96E1336A2B6A99A988
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ....4./....."#.DPr.Iq..A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo.....0T5.....

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):	5.617260579281913
Encrypted:	false
SSDEEP:	12:Z5MVYbNMuR/Ed5MZ68RNMuR/EG5MevNMuR/EX:ZSVzuR/EdSZCuR/EGSeiuR/E
MD5:	122397509A7AA7A483CBA27EFDA6415F
SHA1:	77D7D28BEA4C733E2635BD322AE62079E5291858
SHA-256:	2102D65972C513E18BDAE647CDA15114CC2D1BDE541CF4AAC130EF3C7FF99597
SHA-512:	11FA6ACC2B6AD4B425C0C0C2467B3776C0B5CFE2BB0040D1B66C86270ADCF95E6E3C4341320C2BFDF87652E265C70E1C30716A9BAA14D94904058EF38B7FAB B3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .r.H.4./....."#.D./gFq..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....!=.....0\r..m..... .3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .f.4./....."#.D7.oGq..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....0\r..m.....3....<lb.... _keyhttps://rna-resource.acrobat.com/base_uris.js ..R.4./....."#.D...Hq..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....w.f.....

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):	5.554660149104482
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtuNK1mUlby0zBUKSAA1TK6t:pRZ1Zbe
MD5:	798E18D1A0C1FCDAAA6B50C0893370E9
SHA1:	D86459999E66C13A950B0F6C8F7453DDF6DC9554
SHA-256:	B6B7295821A8E317069200EBBE18DFE561685E9CA85CD6CBE67BC926957113A8
SHA-512:	07D6A65E3692A938653C0FF4824C460A664C15AD9497B29F9E3D622072A3969BA7A7FD6AB99A2663B01952F7E57DFAA0E4A9CD17682E17B30B00570150A0CBF6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ....4./....."#.D0..Iq..AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....A..Eo.....6.....

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):	5.5765351908805405
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0	
SSDEEP:	12:KkXxKMSCvfDOtUl9kXxKMSCvF1bygytUlyCkXxKMSCvuMEHtUlJ:KkXxiCzOW9kXxiCd1b4W1kXxiC2MEHW
MD5:	B460FA1D1019C1AE1F08C96F17ABE8B3
SHA1:	4626885B65BFD5129FBF3D6230749C89B2907AA0
SHA-256:	91A93983628DCE1DE6AF1B5E49535465421D074C9BE5A9061820354609FAC5C1
SHA-512:	363A984DD7E7C5811D3D06FDDB464444F6D7C363817888D35A97FCF12884789EC6A49E59095B1FF54E32B5B604A3768C267AA3BB939F9DF064FF2BD56C5BEB2
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ...H.4./....."#.D.$gFq..A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....c.....0\r..m.....1 .....5...._keyhttps://rna-resource.acrobat.com/plugins.js ...4./....."#.Dj.nGq..A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....A.....0\r..m.....1.....5...._key https://rna-resource.acrobat.com/plugins.js ..P.4./....."#.D...Hq..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):	5.640029054802122
Encrypted:	false
SSDEEP:	6:mkl9YOFLvEWsfOLGaV16yM+VY1TK6tO+kl9YOFLvEWsfOLn6M26RU6yM+VY1TK6R:5h6OLd3XkOh6OLj21Xk2h6OLQTeXk
MD5:	2B5A5CAB2CE2B7EE8C6797F924B9EA95
SHA1:	8EF222C221038EB0E5B1BA04B9CD09174623B7B0
SHA-256:	51446491816833D75B4D5AE9E68528725AF3DAE5D25E4727C84BC149847250AB
SHA-512:	1BC689B9915801273A5A8D9184AEDFB006C514315710F5595271AD4451C4946A034053D88A99E662A71F416B25E23F904104DF3936665DF51713102E127C1048
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ...S.4./....."#.D"Q.Fq..A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....B.....0\r..m.....;.. .I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ....4./....."#.D...Gq..A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....,b.....0\r..m.....;...I....._keyhtt ps://rna-resource.acrobat.com/static/js/desktop.js .P..4./....."#.DU..Hq..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):	5.634103911647785
Encrypted:	false
SSDEEP:	12:URVFAFjVFAFnMX/KwSeKaTLnVRVFAFjVFAFCNsKwSeKaTLnheRVFAFjVFAFpMAK+:UB4v4nMX/KwzXLnVB4v4CiKwzXLnAB42
MD5:	646357742E6092D6B8F5CA1B3172FC7C
SHA1:	005FCABC866F1A90B4D78EF81BEFC4976983B12A
SHA-256:	9452AA8B4933C6D0AF32C132A3C96402DC3B1C4EDCBC9A0B738CA17716A31843
SHA-512:	54645C3F23E0BF5D581735F08FAC22A9C4A570BE56A316017A683B779E332343AA6229C07424D7182E591AEC173090AB52EDBD3B6B6603C36DA4CA11A1033EE1
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 ...X.4./....."#.D1..Fq..A.....H...{...2. ./.k`..r4.C. .A..Eo.....A..Eo.....,V.f.....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 .m.4./....."#.D?..Gq..A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/t racked-send/js/plugins/tracked-send/js/home-view/plugin.js ....4./....."#.D~Q.Iq..A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....A/.o.....

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):	5.505367351419243
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXuPgRRSY11TK6t0c:BsR2EseMgDSGP
MD5:	2C51F450EF17FC8E1A684B0D126D8244
SHA1:	9D4619FF29C6132E2671D8D13CCFB10E0FAE8A0B
SHA-256:	C2DE1A1EB2A1B07E0BB3800AA6959F04118BC3F9AFCEC53187F5003865097649
SHA-512:	7F4C3DD9CBAFA1B819B9FDDABBFF5BE4F2B5C8124E3186879CAC05A8DC65FF35F081652FE9220E1EA8F4F27BCBAB871FD0625E4C3DA6C3EB1A624B5CA8E7C84B
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ..\.4./....."#.DV..Iq..A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo. .....V.6y.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0	
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.631796313258153
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQ9sDloB7OhKlvA1TK6tp/:RbR16JDloBJk//
MD5:	205B05A0B02C6623D2A11FD09CDFF280
SHA1:	E44E4D9FF11979CD4458BBC2A667B6DDEE1475D2
SHA-256:	68245BF7164F2A0C0E4DFA072D408CB206C72B4CBD23FBDA0DB4BF2EE2FBE3DE
SHA-512:	E6AEAE4081EF78591F3E019C79203D6399D6125C55992ED3B2C98FE864D59680216C4FDEEC14DBB31F455A1DCE75BAEF02F9ED667308C63BEDD5E805BB6FD7AF
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ..9.4./....."#.D4..Hq..A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.559806628281912
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVu3XFl0QdFt1TK6t:B2geRHRQAXf00
MD5:	E140FAC95F9332AC99F342C890AE5DCE
SHA1:	89CD22AC637334B78B12D544AA033579E5C12F08
SHA-256:	7995390247B0653E83077023485C21427D58B0B1FAA607B1486DF93F0E7EF0EE
SHA-512:	45FB6240220514638FA33346649ED9DA6033E3E29C812096C2DB4F2E6BBE4E90E7D0539DF7309F059033A2F9B45CD40D5EE50BD9E5C8E386F541BE32B79B467C
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .9X.4./....."#.D...Iq..A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A..Eo.....!.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	618
Entropy (8bit):	5.68922914754152
Encrypted:	false
SSDEEP:	12:WyeRlG1ot1wyyeRlKqeAt1wx0yeRlxut1wF:WJu1ofwyJCDAfwSJZufwF
MD5:	D40F21C29C260738E14C296A3F7F9863
SHA1:	C73C6781748E6C541D8E4DDBE70B6CC86DF48CC4
SHA-256:	A05FC658A0A44C1E0C39498E9B6FDF80510FD708703FA673E111486A7CC86DDF
SHA-512:	7F5ADFABDEAC3F1945FB2DEEFCCA3AD8F2460FB68EFBE9B33DB71096F092F40CFBA2FB2E440F560AB7DDC304ACD78B3630C21F3993980F752EA2AB7C6DCB875A
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .?.U.4./....."#.Du..Fq..A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.... ..w.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .T..4./....."#.D/..Gq..A.t\a.....x5.'OuE.C..@.....x..A..Eo..... ....A..Eo.....Q.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ....4./....."#.D.S.Hq..A.t\a.....x5.'OuE.C..@.....x..A..Eo.. .....A..Eo.....{.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.547212052495281
Encrypted:	false
SSDEEP:	3:m+lKcv8RzYOCGLvHkWBGKuKjXKoyNH/KPWFvEpXVXzYNqww6U+5m1TK5ktBt:mnYOFLvEWdhwyum5ZIqwK+41TK6t
MD5:	647F72554339F87A2267564B2BAB4236
SHA1:	A7514A3C6C0F4364FF9EFA72D4D1545964EA4EA6
SHA-256:	C65A79AC0B9DE9D85095C4D469ACD4579AE1575AEAE423770679CC935E5CDDFA
SHA-512:	A9B3EEEF1644BE883734F51F1A5D56844C742C95EFDFA2DE74A7E35ABAAD9402010528BD1607905537567F9B48A7DEFB684E622A964E5A261E3D36F1B60AECC6
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0	
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ..5.4./....."#.D.x.Hq..A.....7...o..a=.98I.....(3.$G.A..Eo..... ..A..Eo.....pGbm.....

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):	5.626652993379673
Encrypted:	false
SSDEEP:	12:/RrROk/81yErfLEMXRrROk/QRfLEzXRrROk/cD0fLE:/PJ/0y24MXPJ/QR4zXPJ/cD04
MD5:	F897A048909F4090F7615BDB9F5DBACB
SHA1:	DBE9F98CF953C97773A9995F336426A61D400876
SHA-256:	78CC4025C9775B3A2601FCEC2D4A6A92EF09753F4A133AD6B4B88A60D5E9E27A
SHA-512:	9606E074D65435FFD1EE2808C86A7B11508F254607412279B3271AD2EC96F17FD58600A1DBE1CACF83946E972B917917753A48E24BE02E9A8C6E9BEA149445BB
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ...U.4./....."#.D...Fq..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 .q..4./....."#.D...Gq..A..~..rw.+ [....!.)?..f.U..(=.=.A..Eo.....A..Eo.....3-.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .= ..4./....."#.D.A.Hq..A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....H8.....

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):	5.617468319759646
Encrypted:	false
SSDEEP:	12:xqTTDeCPLnAqT4R7kCPLnyqTlj52KCPLnH:AjeMn3sRoMnVBj55MnH
MD5:	8FE7E1FB12665F90F9F776403D3C307A
SHA1:	B2D646BFF1B5DB924948ED5CFC7C4326D5388326
SHA-256:	6D54E43715F0D4C92E8A36BE9E3A8871FB2CCD842E8ABE91438D4E2F967C56D5
SHA-512:	8353DB9ECD56B790AEECDFDBE26215448013F52228E1FD46FC9CCB2F2F7C1A421A4FAF5C0FB3B69F99DF8830086E4B693A7F4E51DE5E9D85200066D87B7FFC E
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ..rS.4./....."#.D.9.Fq..A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo....."/.....0\r..m.....:. ...f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .....4./....."#.D...Gq..A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....o].....0\r..m.....:....f....._key https://rna-resource.acrobat.com/static/js/config.js ....4./....."#.D...Hq..A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....h.[.....

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):	5.670500107091724
Encrypted:	false
SSDEEP:	12:zRMzzosD1RMLlXOw9WsDFRM/ElXC7sDC:zUzbD1aXBJDFmMXFD
MD5:	9C864160AAF110E45CDCEA064CAF6B08
SHA1:	C40B306A7369E7A0C8F72B2E2E978EC0BB81949D
SHA-256:	5D5C5566011FEA542D4B7F4764EB8307B08389929A85BB9F0C3C77A623AB8B41
SHA-512:	956545616DAAB46B0EBA9CB0C96575A96F7657982FA9AA1D2D0AE17D877FBDA6D3616DE316F2567602BA2BB7FC2FED7B0727E7E9618418F8900A741BB66A928 E
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ...X.4./....."#.D.T.Fq..A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo... ...'Y.l.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .....4./....."#.D...Gq..A..z._a...'.v.....4p3..1.']...A..Eo.....A.. Eo.....l.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..L.4./....."#.D...Iq..A..z._a...'.v.....4p3..1.']...A..Eo..... .A..Eo.....(.5R.....

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):	5.631182962835045
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0	
SSDEEP:	6:mYilPYOFLvEWd8CAdAuZ+TX0Fong1TK6tzYilPYOFLvEWd8CAdAu+u7hFong1TKV:6lJRdX0FoMvlJR+7hFoMQlJR4dIFoMj
MD5:	A5E41434491CA6279E0E183B7722E914
SHA1:	D51496F5CD1A541CD8C4A12A049AED648659BFAD
SHA-256:	1CCD04333621C56D6D9F3DF54B6ED91B422574D97601329BD555837D6793A6E0
SHA-512:	5539377F5A0DE16372421D5EA14DED69AA783E039FB50A13132952C132CEC8C956651E0E6ED0E72A400BDBF1E1200B0E7D82B8D541BE71E9A7C580F7F48B192
Malicious:	false
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ...X.4./....."#.D.t.Fq..Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....k.....0\r..m.....R....\|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..f..4./....."#.D]m.Gq..Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....%iY.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..y.4./....."#.DC..Iq..Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	669
Entropy (8bit):	5.662016302101049
Encrypted:	false
SSDEEP:	12:F8hRrROk/kRinXe2wv8hRrROk/tLle2p8hRrROk/aLve2:UPJ/kRiu2PPJ/RA2wPJ/aK2
MD5:	15E3539D380587F323F2BBC369C67AA4
SHA1:	09BC03BBC437B53F71328E3857E8A7846127A0E1
SHA-256:	B93AF389BE612B64F2A3609C19B68D11556336FD914C856B1B2854DD05BD9C89
SHA-512:	CF9DA1F3DD364F981CECE597012F9F952BB9E73F801E57902BCCF20B4320A3F0A18DFBED8AF031AA802D870530114F27F2E8B6B542CC8A3073D77F3D3F26F4ED
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .?|U.4./....."#.D.Fq..A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....0@(.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .....4./....."#.D...Gq..A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....z.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ..w.4./....."#.DL6.Hq..A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....@M.....

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):	5.724253739584205
Encrypted:	false
SSDEEP:	12:ehRcgeKrNJIColIlhRco96KrNJICmhRc19PKrNJICFl:ehrJJICoQhnvJICmhSUJIC
MD5:	06706910125C59ECDA90D258DF340A3F
SHA1:	32E781284A8141650C95DC875962F82A49B27E59
SHA-256:	F7E0F63FAD8EED8712D716965DE95FE60AFE943ECF93BBBE758D0F7D40C3F6C7
SHA-512:	FCB6EA53805DB68A28D45A8F2A6F1236B9422A8B21CAD9FCD46CBEC85A80B74ACAE9EAAF7464BD00D5A7079B6B8104E6598981D339D156936F7589226D99FC4
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ...U.4./....."#.D..Fq..A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....K.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ....4./....."#.D.'.Gq..A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....".f.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .{..4./....."#.D.t.Hq..A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....1.....

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):	5.623531986027451
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhuC18ELzgm2d/1TK6tcOEYOFLvEWdrIhuYFqu637TLzgm2d/1T1:0REyKRecRqFqJ73ReXkRARaRe
MD5:	5F46861E52E9A9C17F30BDFC6F2CC5EB
SHA1:	7DD67E1B9D2C1305F6D8862C703681F9D9173A22
SHA-256:	6A88F8234E74A78776BE182B0FB20CEAA1A4ECC192C854931B6D198C336D4B72
SHA-512:	3C748D5610C4A23D6F0EE77BE11D6DFB6D9FFA4ABE8FF8ED55483E0B166AFCAC710BDFF49317147BF6A5939E6E7404E879FC1DD56C839924CADBE8E4EF0B749
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0	
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .qbU.4./....."#.D.@.Fq..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 .@...4./....."#.D.K.Gq..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 ..[.4./....."#.D}..Hq..AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....O.J.....

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):	5.638089425159187
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1KFMhkx56uvp1TK6tMMAElVYOFLvEW1KpsDsr2kx56uvp1TK6tPc:6JJKFLawJJKCDsZFuKJJKslXcX
MD5:	211AE48367AF7AA079D72F0DDA8DFF8A
SHA1:	611B6702297C6A9854DB1F08018BB62AE02C83AD
SHA-256:	51FB4E503ECF5B7926FDEE1A54E7BFE9A63EAA82EF1AE73A6146F06C69046330
SHA-512:	DC782931855533A7633A18952229F66E7132028D4E8422AAD0FE200F2E26F06B50AF63EA4E40CBFBF8058C61D5484455084327196 30FD42EE5920B6ABA2CB373
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..\J.4./....."#.D..xFq..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....Ry.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .....4./....."#.DH..Gq..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo....."....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..:.4./....."#.D.i.Hq..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....T.<.....

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):	5.625062449913702
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvujGNGjvhUDLYtmOZn1TK6txl:xRBJaGNDDcFZLH
MD5:	8D700EB5B14EF2C9D980B450A4190ADE
SHA1:	77A3F161F317DE7860470CEEA43B6EAE214A005E
SHA-256:	C5DC6614919870E6BD390244DF429A8DCA82CF4CB3DBB2E46B64E1C73D8C3683
SHA-512:	580FDCBCA79040B21E27035A17C85E99DE6233965A92BC38DA78C063E8642F1189C4439B20FABF6C840740D93AC2D7F81A03A4754A9A9217D0B3C3915BBF220
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js .g^.4./....."#.D...Iq..A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....e.....

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):	5.656032408998319
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp7KRGtgVPu1TK6tTlEsRPYOFLvEWIa7zp7jTVQVPu1TK6tMsB:BPHsGtgcVlTPHBTecBPHw1Rcr
MD5:	07E1BAB07BC3887BD2665AF4F09E08E0
SHA1:	E3494CE52DB50AB7B55CD441DCBC94496E0D02C4
SHA-256:	6890AE4C11C23137F22B1E1ED5381330DF91B9D87251968869198AA2E3748D9C
SHA-512:	6C144EB6C62F1573CF7E2E5DBAD5C824D91E380AC77F14147310EF74E99D1E8F20906FFEBD9964FFBC445A5183C3CEA700D80C1234E5CFC49E3495795DCC1B B
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .%.H.4./....."#.D.^gFq..A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....tT.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .....4./....."#.D..pGq..A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....f.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ..T.4./....."#.D...Hq..A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....sE.....

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):	5.638527077837138
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
SSDEEP:	6:mKPYOFLvEWdENU9Q95kWDiM3Y1TK6tKF:bJRT9i5kWDr0gF
MD5:	4D969F3FFA8E10F37FDDE6A635DE3A50
SHA1:	BE8D3FA32F3D58C9CAEEA4611472A1E78A7C4459
SHA-256:	22FFEF0D20BA8878FD4DC6DEFF3CAD21703F9CF19B440711CA80E0122D1AECF0
SHA-512:	35108560E304BF8FD203EAFB030F74E0CC1964F22948D83CC7B7EEC1227142A4AFD98E547C6562950BD3A1444B45EC10E94AA5EAFB1BF878CD9F95F672EE6F9A
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ..;.4./....."#.DJ..Hq..A...M....m+IS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.....I.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.598668933339767
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQPDk2jBRCh/41TK6tn9ll:XRc9MDk2Di/EJ9ll
MD5:	79E4231460ED88D769CB1B62AAEF2F6A
SHA1:	2D186EC9DCB9EC2F2D3DD36C03B6B7B66C461AB5
SHA-256:	30EE60F29CCB3EDCBD16530CE5084F2D75A2DD4C01AFAEEF6291E0C7C4F8C598
SHA-512:	19A186A38CB7DC8590D4EF7A08CC269DFED2B67E98FFF1EE3FC77C18E974647A61D8B20A8346AB643EF534AB99B386F401D9A49F1059E38AD8AD1DAD07887F2
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ....4./....."#.D...Iq..APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.....c?.....

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):	5.633005385864981
Encrypted:	false
SSDEEP:	12:bs6xRkiJ1GniLlF4nPis6xRkiRqW33eiLlF4nW:brxpJ1Fo6rxpRqm1o
MD5:	891DFE3DFEA76C3D7408EDAD301D8393
SHA1:	BDC9488237004F3A84B8AB43E51258E5D069B938
SHA-256:	C6BEE236286B4D103F14C3A44579C5AA39DD70161CB984A393E5CBFDF31E680C
SHA-512:	97D05751234BC2F6064DC29D3C78DBF0504A57961224A698C5369BC33C51AEB6197F3A02576078E56E4CEA53B24169200B2EB6D4096E82825EB434D73FCBEE60
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ..BV.4./....."#.D...Fq..A.P...#4..l....5...5..).w.. .h .~..A..Eo.....A..Eo.....{.....0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ..8..4./..... "#.D...Gq..A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....LA*.....

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):	5.5100729470258045
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvK4ptp1Hcu1isLK5m1TK5ktMlll:mhYOFLvEWd/aFupDpm941TK6tu
MD5:	894AB07F01497C7546E9B58ED3637770
SHA1:	B1CF73BAAB1B6BDDA3AAC93C3F3DB843D22346C7
SHA-256:	1BCAE435889FD1C09F58DB947FDB9683FD521C431CA625D41336EF9C9749A914
SHA-512:	F1F08ADF3A584E3E9EF1E9F088008358A0E692BE4F186D201305BFB5DF9DA06070B269759E68EDDD579C84E9660B83B528F34F5A2E158C0DA8AD6D95AAA5272D
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ....4./....."#.D}..Iq..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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0	
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.546148655243983
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQNeGSSXWBoBMqVd3G4K41TK6tf/:2DRuRGeGSNqB9Vd2kh
MD5:	F74935F6999F6C43642A60D2952EC819
SHA1:	C7749EDCC005A42A3937D87B625B698B087DFB57
SHA-256:	0AFC088E039256B49A6D10BF3344C92F0574D0FAC0298F1201612A0044498ECB
SHA-512:	60B73CCB3BB8A31C3530C01552439EE6F2DFB99EBE6FF3737131F312110B78BE7C5A9FB7611B7C745111B83E31617331F8F3DB237DCE48D2FD1297DCA78B072
Malicious:	false
Preview:	0\r..m.....P...y.p....._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ....4./....."#.D..Iq..A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.... ....q:.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	624
Entropy (8bit):	5.689504765020443
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9QtODmMGGQNuA424r1TK6tbHlEkqYOFLvEWd8CAd9QAXZuA4r:+RQCODmMGH8rndWRQjQrnLRQGLrn
MD5:	A2E0EFFFBE94970DF87AF6C0E26BDDBD
SHA1:	7F19E4B83FC64A28C55065C66B89E7E53AE2340E
SHA-256:	B2571C6EBE78839A304BE20FAFE4CEDCA8A6A62257996173B059D16B415F5810
SHA-512:	2A52F39E228BB945DA2EDB235AAFFB14AB4FC6A67BB864E1B29F4C2CFB2399DFBAC8FF66D57B0461D67813B225ADF467333DC8E1B228886537C83A30CEFFB8 DF
Malicious:	false
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ...X.4./....."#.D.L.Fq..A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo... ...X..R.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ...4./....."#.D.>.Gq..A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo..... .....A..Eo.....9.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ....4./....."#.D...Iq..A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo .....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.564881115492691
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAugM7AyC8n1TK6tg2l/:xhRTyM7A7QC2l/
MD5:	192BEEE74BC763A799DA123764464461
SHA1:	7489B293EA113D26EB013CD28C6F12947195D8AF
SHA-256:	0B44636C059D98972F6430E8EAD4377EE06D33AE3C55AA1ABF8248B6B37CA701
SHA-512:	8F1AFE0A13AA319B212078FD8EA94D03B793C948D58ABE52B94400D7E2883F068F1B844340099F18AE201B297BF7C12E466233BE7B0DF1BF4286B4CE95C99E00
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ....4./....."#.D.d.Hq..A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....4.?. .....

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):	5.69655708851955
Encrypted:	false
SSDEEP:	12:nRrROk/VRMDmDXRrROk/Vasqm5i/RrROk/VZ8ma:nPJ/0C7PJ/Is75iPJ/vxa
MD5:	08B970B3B435B2E60DCCA71B31EF742B
SHA1:	2F61EFF81BC2CA241AF8ABDB7A03D3C7F9BB4217
SHA-256:	B1944F0E31D2D30052F88B42BE43A8A13DF30E9E204888D69C6E598F6B4B71BA
SHA-512:	8AD7DDAF6F0C5AE09686709767D7EE09D4B43D28C42073C0D92AC8473750E165DDBB121955CA068B80DDEB08C1006C0FDE282C071253B2D1E61F661D939FFA 6
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0	
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ...U.4./....."#.Dt.Fq..A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....).....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .X...4./....."#.D.8.Gq..A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....".5.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ....4./....."#.D...Hq..A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....T.{.....

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):	5.60673012350949
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWuIJesG5oAdm9741TK6t:qxRcOJeToAdu7E
MD5:	837D263D7F761AF50735A8478483197F
SHA1:	0D1C53E1F2BBB922200725D0EDEF9173602A2D35
SHA-256:	7C39DC0630384E49B371EA838C49A8F783ABF58EFF18C099DD35BBDAC02C72D3
SHA-512:	46F07BB97C5A0B5A9BDBA63286790BA7E0E3DB1354FBE896FB9CEFBA20BFE0BA04BC076A89DF466E7C5CE023A29DC2753D7E76A914DBF7942010C6CF46EF46 37
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ....4./....."#.DZ..Iq..A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....z.....

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):	5.571333083562102
Encrypted:	false
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFvvERBXqmCnB6shoq+Nem1TK5ktq9:mMOYOFLvEWdwAPVuFERBXqSJn1TK6tq
MD5:	E628D039C896716C587C882C63E63B72
SHA1:	70211ED46D1A9012CB867AD0BE54004F44CCC988
SHA-256:	5F295B975A8CEB6B7D3C82582021DB8CB72C164A5230B70EE91DE91DF51ECBA3
SHA-512:	57FC50F881B832DD7DF2FE9926A0CBED6F665F51FBFB0628CB1BF07EA2CE2D0D7376816619D7757E60A2014082C31845FF57369E9F10B7AF610BE69F37330DDE
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ....4./....."#.DtE.Hq..A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.673476232413608
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQZREzhcsBXIh1TK6tu:mxRBJQcREDB0s
MD5:	F813BB7C1EC840D70FA9CBFC5F8E3C29
SHA1:	DA9084BBC76A73139104B1B7531BBDCA95047C97
SHA-256:	A2AE3F3B6441AED873FB0A145BBC80FCC4380FFF707D19A0FB8F5C046D42A699
SHA-512:	669202EA0D7167AEBEE2A5D6E803782A1669FA1E438A6C010E15ADBE3D5683223D87B0E2D7D1E8F5DC2320A7E4B65F750835066060E8742071880C0F660D2EAA
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .w(.4./....."#.D>..Iq..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):	5.6510397819075475
Encrypted:	false
SSDEEP:	12:3RrROk/sgGPc1RrROk/sWqDc9RrROk/sg6TKcC:3PJ/B91PJ/Dqg9PJ/l6nC
MD5:	C2DC298BA7FE2A0A70B56099A8E3D540
SHA1:	F7EE9F7F5E27C27F4E98FF1CF8568A01E8269AB6

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0	
SHA-256:	293B6820876E3F0AA1528F33217205323C578A3C32D91288F0E602AFA1DAF668
SHA-512:	CBE5C24A310142901814F59750983D68641ED3F350BCC2B992CA140684996D480812430114D933818BAC87F2233824DCC3F288AF0CD47D50FB221505E68116AA
Malicious:	false
Preview:	0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .b.U.4./....."#.D..Fq..A.....9Q].8O.z....=..:.N.{....N{.A ..Eo.....A..Eo.....;$G.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .....4./....."#.DK..G q..A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....f.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-sele ct/js/plugin.js ....4./....."#.D...Hq..A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....yV.....

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):	5.0486279272260015
Encrypted:	false
SSDEEP:	12:8UBuvGlwf85mMzII9xmn7L+/81xBwsZjZY5t/XA4DmDraBtHM:uFUmM6f0x6e1uuASraBts
MD5:	A6C903BEE0EFA8C233DE8CED640F7450
SHA1:	D954794107EA0E9057EAFB8A8195088ED3DEAA14
SHA-256:	F454CDAA052C9EFD314DBE8F5511B1F7415147C8C04BD1384F834C84F6224612
SHA-512:	1E2E90778E3192BACF0E011C9C79A5FE744573CABF865F1D723EFE29F77B0D0F25D599B11E24546FC1B034271E74034AFCBEF2AEFAA3064A3F5ADA033F96962
Malicious:	false
Preview:	....c..oy retne....).....T.....3.....4./.....v...q....4./.....C..M....k.....#...(...k.....]...I....4./.....4./.....6<|.....4./.....<...W..J...4./.....oB* ...4./.....a.....4./.....:.y~A....4./.....P....V...4./.....F..=z;....4./.....o....4./.....*.....4./.....2q.....4./.....Gy.'.h....4./.....k7A....4./.....:..N.A.....4./.. .....;/.....4./.....4./.....P[. q...4./.....,+..._.#...4./.....J..j.....4./.....A?.2:.....4./.....q....4./.....u\]..q...4./.....!...0.o...4./.....*.....4./.....o..k.....4 ./.....^.~..z....4./.....[.i..%....4./.....+.{..'...4./.....@..x....4./.....*)....J:...4./.....&.S.....4./.....MV3.....4./.....+.U.!..V...4./.....D.4....4./.....~.,.4>....4./.. .....

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):	5.174457876573366
Encrypted:	false
SSDEEP:	6:mLWgWDv4q2Pwkn2nKuAl9OmbnIFUtpiWgWdJZmwPiWgyNDkwOwkn2nKuAl9Ombjd:+WDv4vYfHAahFUtpOWdJ/POyND5JfHAR
MD5:	DD6BA346B16830A6F03222C267935A30
SHA1:	A26D588E992F200A65F358AD414B709F0AD20118
SHA-256:	090FA9277C99916F6F5CD57FC8B36D08B26B308A245C79E225BE7021A781908A
SHA-512:	B4CAB1ECA919A83EADD48653E018ED524601E633643C04943E34F218A1636D3CF2BD0BB4D771921589883 75C556D3E41F855EF6C02424EE392FFD2BE516A2E1
Malicious:	false
Preview:	2021/02/05-23:22:18.637 1b20 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/02/05-23:22:18.639 1b 20 Recovering log #3.2021/02/05-23:22:18.640 1b20 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-210205222213Z-184.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 117 x -152 x 32

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210205222213Z-184.bmp	
Category:	dropped
Size (bytes):	71190
Entropy (8bit):	0.9629731508669015
Encrypted:	false
SSDEEP:	96:ksYMFHjO7YMPjMgBZMPEiFb/MC8kMnk8sM0nBw4XRMEf9MA:dpZxkCUnkDx7
MD5:	7C9C92F828931D19D42758564757DC76
SHA1:	9EEF4FDC5B6EC32732D8B32C284E88E767AFBF98
SHA-256:	F37BBDBC02017A44DAE873D64D009658AE1E5D15360201CAB40AEA726767BF7E
SHA-512:	FA65A215480118FB1639C6CE69592EC3A0DC1324F59D6425EA28DA0A359823A19FBB93AAC624D13B79D9A61F90935DAD33EEC6DA3CE3FAB0C3D326F8233C3E E6
Malicious:	false
Preview:	BM.....6...(...u...h..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3024000
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	3.4470663221637086
Encrypted:	false
SSDEEP:	96:k49IVXEBodRBkWCgOOh1CKq49IVXEBodRBkWCgKOh1CK649IVXEBodRBkWCgKOh6:HedRB3edRBjedRBDedRB3
MD5:	5FC1D46148FC1567599DBF6263AC3684
SHA1:	36A8AB1FAA422D5E9994D83EB9210330EF06F539
SHA-256:	4D54524F8A26953FF4C634551BA49E7291BCE356EAF5C6C609D45D6BC539CCF9
SHA-512:	530EFD04C4B578E16D3E891217DB9689AB8F6E2036AD8131EB8700C135CDA80C180DDFB2B0815D5B596D9EB1DB91E59D5F3FEA23CB8AA7731D6D49F0E51650 9
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):	3.313208339829863
Encrypted:	false
SSDEEP:	96:BCgOOhZCPF949IVXEBodRBk8CgOOh1CKcst49IVXEBodRBkVCgKOh1CKod49IVXR:2iedRBksSedRBDCedRB1yedRBZ
MD5:	E748A287944233A519D84AD13B0E4661
SHA1:	004D199109B64388073CAD4F131B6A756475C5AD
SHA-256:	FE57E6B3CB81B778C70AF5267FD05F6AE610A9AE44798B2BD292644C68AC0F7E
SHA-512:	C8606683DE2D61FC202D4E60AD7219E609A3E12B578FC95050171695103FFC59B35F841A496BBE2F5D54C5EEECFDCAA17741A8C2E8286A1AFFCBE3D00ADA52 5
Malicious:	false
Preview:	.....0..... .....W....X.W .L...y.....~..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.6296	
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

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.6296	
SHA-512:	E02BD1B88C1188CBBD4D6C1F5B31A44A278B213D991C6E9B9B06C620D66B1290DFBDF6D7BF92082D51A146C8AF772DAA659F9C2DC0A416C6BA9BE14B89C6EB8
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.NameArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleName:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength:1036584.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-BoldMT.FamilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.FullName:Arial Bold.WritingScript:Roman.WinName:Arial Bold.FileLength:980756.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial Bold.NameAr

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AdobeFnt16.lst.6296	
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:es4p0vTLcdfIfsmtRZEtsuatG1gMIzV
MD5:	63B24EA3A13EAC476D6309BB202EF459
SHA1:	89502C393549C20C933E4553F51F74F3DBE085EF
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:PCbGNFYGpiyVFiC0Zn964/7VNfChB4Z2lJPJn3370jYyu:J0GpiyVFihnM4/7VtCUoV7sK
MD5:	13EFFC05E5ED3D13B62C54D0F5129D83
SHA1:	D2E816373C11A3D3395362BDD89F4B924CEDC73D
SHA-256:	9E7FB280A24023207FABFD42DF25B21E235A9A85D9C08D445C3CEDAD9B24DADB
SHA-512:	603418C333C9F01ACAC5A9C0AD1A4A0EE0B6112DF7E227E6CEE0327AC1AA9A997E8EFBFDFED65C05FD95AA3F03A2D2FEE11AF65EB86E1FFDB3DFF4E58497B8A8
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:AIgerian.#.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\my-site-105523-100173.weeblysite[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2696
Entropy (8bit):	5.703603606427189
Encrypted:	false
SSDEEP:	48:LvkQqDzd2oj8TdlZGRenn4nL5SYXONV5dMXtM2r12Qm4hwgjWiw8WOCGnr1g4FJB:oQqDZ2O8TdlZGRen4nL5SYXOT5SXtMEr
MD5:	4DD791E3F6C981BB0502C56D854EEC68
SHA1:	626DC166D746B38DEC7A176D9B825B30FCE6C328
SHA-256:	68D85C53808920AEA77FFFF8CC321FCC1FAA91BB4F362439388C30D1A0D5246B
SHA-512:	0E9EA4B9E1AAFF7C00240286499330809180 92FDBB85340A88D6E407044530173262CC7F1AA757AED37AF52B9131471B3821D9035BBC5505E764F76574C7319A
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\E5F0NRSV\my-site-105523-100173.weeblysite[1].xml	
Preview:	<root></root><root><item name="snowplowOutQueue_snowday__wn_post2" value="[{"evt":{"e":"pv","url":"https://my-site-105523-100173.weeblysite.com/","page":"135973448:573639115815232853","tv":"js-2.6.2","tna":"_wn","aid":"_wn","p":"web","tz":"Europe/Berlin","lang":"en-US","cs":"utf-8","f_pdf":"0","f_qt":"0","f_realp":"0","f_wma":"0","f_dir":"0","f_fla":"1","f_java":"1","f_gears":"0","f_ag":"0","res":"1280x1024","cd":"24","cookie":"1","eid":"dcdad865-269d-4e22-a980-cc59eb895f66","dtm":"1612563794668","cx

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{B9DB4C88-6800-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	32856
Entropy (8bit):	1.838137608509538
Encrypted:	false
SSDEEP:	192:rTZwZe249W4tXfaCtxVhzWJ5D6TBIyt3V8j3:rVgV4U8vB83Wfe
MD5:	02360F57BC9B79208A09994E6E33F1D0
SHA1:	0E1911D9A0383B6C66392731B0D8212CF2D0B487
SHA-256:	112C60F617232151E660843BBBBB7ABA15B0D374A032CAE186ED741722FEA310
SHA-512:	21A8FA091255D9EE8AB44220E883B8ECAE101AD74A7225CD1BAFCB347D5DDF56E1D42B33FDE0939C17C0975BD48D28974975C21D1D611F0327C7C6F0B83C677
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B9DB4C8A-6800-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	23640
Entropy (8bit):	1.731053312576663
Encrypted:	false
SSDEEP:	96:rnZYQcumoFGmitU/mSGm+tRmmN3mSSXmlh:rnZYQcuNkdU/nGJRmw3JSXsh
MD5:	318DF9F5A3BDA4EC404C3D0B93B8D5D4
SHA1:	B0C558F2782B8CE0AECD0B3AD90FCC68375E5338
SHA-256:	24A2A6004A9E2ADE32498AD4340ED4FFA728F296B2A0E0649E28FEBAC7812F8F
SHA-512:	2892D0DA2D43E0CCCE843404555B1BCAEEB5CD5488FDF113838F67364F13318C878F0AEAE056FD62F07EA5D288ED9B3E1F202C13A329B8E047DDC09E58FF340
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{C183E3BA-6800-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5667106930530297
Encrypted:	false
SSDEEP:	48:Iw1GcprwjGwpaLG4pQrGrapbSjrGQpKTG7HpR9sTGIpG:rrZcQN6fBSjFAiT94A
MD5:	E6C72D5E3E9EF8F533CC793439459EC0
SHA1:	C35C45476357A5AA003D775A4DBD683BF0294F99
SHA-256:	4E6B90978E206E603A1FDA35EFF3FA3FBB864AB98BD7E6E4320CC1C6D8A433D0
SHA-512:	58FE880D5B79F511CC7BE0925DD4919183573C8131AB7FE1817CD646D40CDAC90D247AA9C7CAA0DBBD5DB3EB2D6B1BCB43377DBE7AD0CBA5F3C5C1739261874
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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.051503649135252
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEIKMKXnWimI002EtM3MHdNMNxOEIKMKXnWimI00OYGVbkEtMb:2d6NxOHbiSZHKd6NxOHbiSZ7YLb
MD5:	3ABCC5912E9AC5CCB67664F2010E8A86
SHA1:	718E2934EAF493BC6076B47B70C3A5FA3DF0B104
SHA-256:	CD360146AC79F1C1A3F2EE56680ABD5CDE2E4A441E5E72A74614A6B49F220825
SHA-512:	83D547274E199888EE599447F114F797367439F63849DAC9CDB439CD40635E25333490877B4C12DC2448039E54F4BECC3597680C44DA7EAD223F5B898570167F
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x90e5f66a,0x01d6fc0d</date><accdate>0x90e5f66a,0x01d6fc0d</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>0x90e5f66a,0x01d6fc0d</date><accdate>0x90e5f66a,0x01d6fc0d</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):	5.058278690133668
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kKk1nWimI002EtM3MHdNMNxe2kKk1nWimI00OYGkak6EtMb:2d6NxrwSZHKd6NxrwSZ7Yza7b
MD5:	04A9213472F8DE83124EDE2CB73A7AC9
SHA1:	CC71A2B40BA4435D79E987662FBA07C236714744
SHA-256:	E4871CF76447890A94A1A0969AC6B874604E732279C6DBED1B350B3566BF9110
SHA-512:	55DD7D6D9C27D374002959059DD2882FA4FEFC1228F5CD8C23617D50783CA4CEEAABB41E7EA0A076890326ECAA4B75482FB31C580E37629660497D4AEEBADEF
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x90dc6ca3,0x01d6fc0d</date><accdate>0x90dc6ca3,0x01d6fc0d</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>0x90dc6ca3,0x01d6fc0d</date><accdate>0x90dc6ca3,0x01d6fc0d</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):	5.080026359638779
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLIKMKXnWimI002EtM3MHdNMNxvLIKMmfnWimI00OYGmZEtMb:2d6NxvsbiSZHKd6NxvsbYSZ7Yjb
MD5:	BED26AE05E6CFBF28D8EDBDAFA30F478
SHA1:	0208F67EC27E584E4EF5A8ACA2C4BFBD20968C5E
SHA-256:	2846A7A4A9FC4363458956AFEE9E0B9EE4AD600381D391BAE887993FC50EC7E1
SHA-512:	B7A6C4178295651B8C00531829A78166E47EDFBD74B8846815C6A5055F1EEA424D697B41E6A1EBBF2BD57B6E3220ED18A59D1CF0D0F1352E07B957AA116DEBAF
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x90e5f66a,0x01d6fc0d</date><accdate>0x90e5f66a,0x01d6fc0d</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>0x90e5f66a,0x01d6fc0d</date><accdate>0x90e8587f,0x01d6fc0d</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):	5.074156276513578
Encrypted:	false
SSDEEP:	12:TMHdNMNxiI1d1wnWimI002EtM3MHdNMNxiI1d1wnWimI00OYGd5EtMb:2d6NxJ1d1wSZHKd6NxJ1d1wSZ7YEjb
MD5:	EE62BE15F3E798422A010183E3FA46D3

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
SHA1:	2A79456F7069F1243E0C65D5C330E0A2BF7CC68B
SHA-256:	B28DFECFEA2F1B794632132CE7920B8F0B7D2B88F0F693381568A388B0BD695C
SHA-512:	957FFE5A944AD70D2A7C7432F47131E4AA4D289E4EE19A3EED4440473EDEE7D6B3B31742B6D90569FFD6F5760B1A45FA536AA145570E9FEA51F2AFB780E1DDE8
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x90e13143,0x01d6fc0d</date><accdate>0x90e13143,0x01d6fc0d</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>0x90e13143,0x01d6fc0d</date><accdate>0x90e13143,0x01d6fc0d</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):	5.105310520373243
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwImUmfnWimI002EtM3MHdNMNxhGwImUmfnWimI00OYG8K075EtMb:2d6NxQTlYSZHKd6NxQTlYSZ7YrKajb
MD5:	5F444512635DDDBA9B438262E2772F65
SHA1:	64BA639BB5DF74950D3CC1D8185103F7145B1952
SHA-256:	11EAE059F2909FCB82EDE19EAA3A9D020E52FBE18DB14D974E596BC75A66516E
SHA-512:	C6B1BD44D0EFAA8E710C754A2AF2F4AAD0E7A1589BB6BD49E28D1D59AA34A928F8F2787BD60ECBE76E4A5C97364D8BB8FAB630B81AC3F2AC2913838B467FD3E6
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x90e8587f,0x01d6fc0d</date><accdate>0x90e8587f,0x01d6fc0d</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>0x90e8587f,0x01d6fc0d</date><accdate>0x90e8587f,0x01d6fc0d</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):	5.034438650195903
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nINAnWimI002EtM3MHdNMNx0nINAnWimI00OYGxEtMb:2d6Nx0INASZHKd6Nx0INASZ7Ygb
MD5:	BC2EA640CB155CD158D2C3BD983363A3
SHA1:	11D96AC255820AB609FA5FF9AA3943C3FDB6D821
SHA-256:	6DEC5A64757695824D92160A5B81AB5670BE7388299B1D68860DC2900A809264
SHA-512:	B524C625513778F0A5DB85E89DEC6FB1600E0003AB0F6CCE1D6BA22870C51449D16E1283B1C11C7F69EFF368839B392E8E56E472B28B9EDEDE69B46A069CDAB
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x90e393e0,0x01d6fc0d</date><accdate>0x90e393e0,0x01d6fc0d</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>0x90e393e0,0x01d6fc0d</date><accdate>0x90e393e0,0x01d6fc0d</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):	5.073139649959207
Encrypted:	false
SSDEEP:	12:TMHdNMNxxlNAnWimI002EtM3MHdNMNxxlNAnWimI00OYG6Kq5EtMb:2d6NxmNASZHKd6NxmNASZ7Yhb
MD5:	80ABDDB06CD04717C7675CF2B1918E3B
SHA1:	12C03383CCF9FBFE68C4BF7711897027B55C2C91
SHA-256:	0B6E4FCA31634641970031126CBA9CBEF0E848D7D7127E352296F929FDDD1CB8
SHA-512:	4CFAEFDE23CFF8B765D5CF35B1B1B03898184E7CBEB35B33E5DEE851692A9303F66FE625F7875364730333E7D87D9D48C19501D490A8EB52A7A82F866CB0D68
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x90e393e0,0x01d6fc0d</date><accdate>0x90e393e0,0x01d6fc0d</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>0x90e393e0,0x01d6fc0d</date><accdate>0x90e393e0,0x01d6fc0d</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):	5.062711454643544
Encrypted:	false
SSDEEP:	12:TMHdNMNxc5AOnWimI002EtM3MHdNMNxc5/1wnWimI00OYGVEtMb:2d6NxwAOSZHKd6Nxw/1wSZ7Ykb
MD5:	CEFE86A689F53D547997154D8DA7B3E4
SHA1:	47C5B0E5268699BD9EEFC23B286BBBE36263E7F8
SHA-256:	C5FC01BAE71F6D3658CF98A1BC6F17B8D39CA2986ACFFE608072D8C983AFE546
SHA-512:	458AD5E0F9F20591C02481F6FB6396FB9B5442CEB57C60AB3E299A0E582C959BB657708EB4D5502DCB957E84276ACFEBD72FF04E91C614CA4C474A092AB69B27
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x90ded133,0x01d6fc0d</date><accdate>0x90ded133,0x01d6fc0d</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>0x90ded133,0x01d6fc0d</date><accdate>0x90e13143,0x01d6fc0d</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):	5.059823251830531
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnI1d1wnWimI002EtM3MHdNMNxfnI1d1wnWimI00OYGe5EtMb:2d6NxQ1d1wSZHKd6NxQ1d1wSZ7YLjb
MD5:	2A6568194E35650D78383B9299AA5904
SHA1:	CDFEE76B6D0AFCB2B6E99C98126BA70B59BE7913
SHA-256:	B9E598FF6D89D8A124A40667E29401CA52DBEBE8A4940C2F4CE56DD8B7E650C8
SHA-512:	EACC8227B2A80BEE5C7B3AC160E83C58CE44D6CE5CD0A9B0869407BAE457A9E62256D911B5ADACFE850B0C743CB84E10E29C17309384D837279C42C339E0C80
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x90e13143,0x01d6fc0d</date><accdate>0x90e13143,0x01d6fc0d</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>0x90e13143,0x01d6fc0d</date><accdate>0x90e13143,0x01d6fc0d</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	4392
Entropy (8bit):	4.2264716492835195
Encrypted:	false
SSDEEP:	48:x0PDoH8yAXQ8K5UvCUbpXtlhMVDBilhB7IODnNcynEJPMHErU8ACbtRKO7nheF:2DlyAXQ8yUdduBiloycKeRg8xbtsOc
MD5:	78BB90BEE9E6EC5BFCE65643D11E6DD0
SHA1:	7EAE0D2A94ADEF9F99AEDE82174FDC9DC566445B
SHA-256:	DC1AACA482B0E072ED320C70B45492BB738B396383F6A6EEF723CB37A17BD0CF
SHA-512:	1127E69C51EC528F39EF4A378D8BA952489ABF42B352C638AE0D1D30148277FE301852EA70967177AEE69FC91CF911BDCB39D7CC66F8A0027CD474DB2B3700C
Malicious:	false
Preview:	".h.t.t.p.s.:././.w.w.w...w.e.e.b.l.y...c.o.m./.f.a.v.i.c.o.n...i.c.o..... ....(.. ...@..... .....D;3.C;4.D;3.D<3.D<3.D<6.A2".Pc.....M>5.....E;4.D;3.D;3.D<3.F<5.E<4.....F?4.ID5.D<37C;3.C;2.C;2.C;2.C;3.D<3LE=3.E=2.D<3.D=3.C<2QC;2.C;2.C;2.C;2.D;3.D;46JB;.G>6.....E;4.H<5.D;3]C;2.C;2.C;2.C;2.C;2.C;2.C;2.D<2.G<3.G<4.D<3.C;2.C;2.C;2.C;2.C;2.C;2.C;2.D<3[C=7.C<4.....H<7.B;1.D<3CC;2.C;2.C;2.C;2.C;2.C;2.C;2.C;2.C;2.D<2nD<3sC;2.C;2.C;2.C;2.C;2.C;2.C;2.C;2.C;2.D<3@B:3.HA2.....D<3.E<4.C;2.C;2.C;2.C;2.D<2.C;2bD<3pC<2.C;2.C;2.C;2.C;2.C;2.C;2.C;2.D<3lD<3^D;2.C;2.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\FVZBQN4S.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	30832
Entropy (8bit):	5.412586090347367
Encrypted:	false
SSDEEP:	768:j0zrzXz6lAUfnnUfnHUxzXz6lAUfnnUfnHUReSHsAClJJE1:2zj6lAUfnUf0xzj6lAUfnUf0bwx
MD5:	2133F3DF63FE194A5CC3125CDC22FF00
SHA1:	E617454208C45AD3B9FFFBEAAE1DC936844B21B2
SHA-256:	ACDBD769356C9D217AACBA01C0473F5145DD9F930E2287376BD8BC5ACB5A08EB
SHA-512:	D2DE4EEAFE793F9952970C069A5819F5CA0CF6EE09FC45CC0AEE52E51EBFD409BB66E8A05816828615DC1EB3029A6643FFE8617260E0EE075B222D9FFC3A06E 1
Malicious:	false
IE Cache URL:	http://https://my-site-105523-100173.weeblysite.com/
Preview:	<!DOCTYPE html>.<html lang="en">.<head>. <title></title>. <meta charset="utf-8">. <meta name="viewport" content="width=device-width,initial-scale=1">. <link rel="shortcut icon" type="image/x-icon" href="https://www.weebly.com/favicon.ico">. . <meta property="og:type" content="website" />.. <script type="text/javascript" src="https://cdn3.editmysite.com/app/website/js/runtime.4c27edfb51f63cc2e6e5.en.js"></script>... <script src="https://cdn3.editmysite.com/app/checkout/assets/checkout/js/system.min.b9e210033fc5b0895164e282cbf89d5a.js"></script>... <script type="systemjs-importmap" src="https://cdn3.editmysite.com/app/checkout/assets/checkout/imports.en.5190980851c8e63fd7692575cadd2295.js"></script>... <script type="systemjs-importmap">. {"imports": {"SqPaymentForm": "https://js.squareup.com/v2/paymentform" }}. </script>.. . . .. <script type="application/javascript">. window.siteData = {"site":{"id":"fa58bb00-649e-11eb-b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\site.19e2b99b084b05df36a8.en[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with LF, NEL line terminators
Category:	downloaded
Size (bytes):	1457731
Entropy (8bit):	5.413387646407298
Encrypted:	false
SSDEEP:	12288:bpZ/xEMMRoPRNdelkcp6iLGGn7oi3AA6GFx1HsP5CG:r/xEMMgMlkk6iLGIlsc5/
MD5:	A285C062D9C60CF462DAF5E2C7096388
SHA1:	9A5809428AB807DA9A290510B5317CC91355D094
SHA-256:	FE3371FC27681F7F21A6EAD605AD304A73E76A2C5CF4A6F4D37C5EBDBC024DC7
SHA-512:	295304F21AA5C759450EEFE310F174C6A4729C4EDD45533A0382941C8112F96604B826C508340D88D7722020DAC014887535508EF069E63B3E8BAFC83F276526
Malicious:	false
IE Cache URL:	http://https://cdn3.editmysite.com/app/website/js/site.19e2b99b084b05df36a8.en.js
Preview:	(window["webpackJsonp"]=window["webpackJsonp"]||[]).push([[353,0,5,12,21,25,47],[function(e,t,r){e.exports=r(529)},function(e,t,r){"use strict";r.d(t,"g",function(){return n});r.d(t,"t",function(){return a});r.d(t,"s",function(){return i});r.d(t,"w",function(){return o});r.d(t,"n",function(){return s});r.d(t,"b",function(){return u});r.d(t,"h",function(){return c});r.d(t,"u",function(){return l});r.d(t,"d",function(){return f});r.d(t,"c",function(){return d});r.d(t,"a",function(){return v});r.d(t,"v",function(){return p});r.d(t,"l",function(){return h});r.d(t,"f",function(){return m});r.d(t,"j",function(){return g});r.d(t,"o",function(){return y});r.d(t,"p",function(){return b});r.d(t,"e",function(){return _});r.d(t,"m",function(){return w});r.d(t,"q",function(){return S});r.d(t,"i",function(){return E});r.d(t,"r",function(){return x});r.d(t,"k",function(){return O});var n="dispatcher";var a="snapshot";var i="site";var o="user";var s="pages";var u="billingFeatures";var c="featureset";v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\cko.e4d7b6c3391e50ded088[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	40067
Entropy (8bit):	5.196637135752998
Encrypted:	false
SSDEEP:	384:rAC5BSi//FlfmOvOF6mCF9NNUSGGZ/l46UCQrwcRtgxWNAH/U9nQ:rACvtXXmyOaNUSGGslR+WNAH/U9nQ
MD5:	CB016791F22B8B372133B9CBE95A2E82
SHA1:	9A5B3811D4783B3A989C16DD3170DD15EFA53EA0
SHA-256:	85B7A24005868A38ECA79E80C1EC8081CC2AC4DCECD4EC3844D534FA3C659B5A
SHA-512:	75E5EFA03C42E71E7A65615FAC8E6AA4D7871A0700659D77543951BA942BEDA2B594AD384E6BE36F0FBECAB06FFD20CC9842F2FA792255118B866FF976939CF
Malicious:	false
IE Cache URL:	http://https://cdn3.editmysite.com/app/checkout/assets/checkout/css/cko.e4d7b6c3391e50ded088.css
Preview:	.message-label[data-v-1275c96d]{font-size:14px;line-height:22px;display:flex;align-items:center}.message-label .icon[data-v-1275c96d]{margin-right:9px}.inline-message.error[data-v-1275c96d] input,.inline-message.error[data-v-1275c96d] select{border-color:#D92B2B}.inline-message.error .message-label[data-v-1275c96d]{color:#D92B2B}.inline-message.error .icon[data-v-1275c96d],.inline-message.error path[data-v-1275c96d]{fill:#D92B2B}...added-item[data-v-256fadca]{padding:12px 16px;background:rgba(0,0,0,0.05);border-radius:8px;display:flex;margin-top:16px;line-height:22px;align-items:center}.added-item .added-item-label[data-v-256fadca]{font-weight:500}.added-item .added-item-details[data-v-256fadca]{flex:1}.added-item .delete[data-v-256fadca]{display:flex;position:unset;width:16px;height:16px;cursor:pointer}.added-item .delete[data-v-256fadca]::before,.added-item .delete[data-v-256fadca]::after{content:none}...order-discount-input[data-v-67676903]{height:fit-content;margin-top:16px}.discou

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\snowday262[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\snowday262[1].js	
Category:	downloaded
Size (bytes):	75006
Entropy (8bit):	5.625174285042866
Encrypted:	false
SSDEEP:	768:YdDFSZ8JdMS1xGPlopXbk+KQZPKOf/py7pFw7N5o9qmse9fLrJIWzAfap34VEzH0:6FSZYdMS1xGNopX5LP16FuvqT7bmVF
MD5:	99BBE560926E583B8E99036251DEB783
SHA1:	8D81B73AE06F664F9D9E53DD5829A799BF434491
SHA-256:	648E766BF519673F9A90CC336CBECEDE80DCBE3419B43D36ECBB25D88F5584A3
SHA-512:	EE24915AA5C1C7C1DD571C07EFE46DFC173CB69D2DADC4C32891CE320EEF4FE1CFB614D9C212F16BFE2C83B29C6EEAB6C5A43F8E32D475DA8081B1E2D3389B4
Malicious:	false
IE Cache URL:	http://https://cdn2.editmysite.com/js/wsnbn/snowday262.js
Preview:	(function e(b,g,d){function c(n,j){if(!g[n]){if(!b[n]){var i=typeof require=="function"&&require;if(!j&&i){return i(n,!0)}if(a){return a(n,!0)}var m=new Error("Cannot find module '"+n+"'");throw m.code="MODULE_NOT_FOUND",m}var h=g[n]={exports:{}};b[n][0].call(h.exports,function(l){var o=b[n][1][l];return c(o?o:l)},h,h.exports,e,b,g,d)}return g[n].exports}var a=typeof require=="function"&&require;for(var f=0;f<d.length;f++){c(d[f])}return c})({1:[function(require,module,exports){var JSON;if(!JSON){JSON={}}(function(){var global=Function("return this")(),JSON=global.JSON;if(!JSON){JSON={}}function f(n){return n<10?"0"+n:n}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return isFinite(this.valueOf())?this.getUTCFullYear()+"-"+f(this.getUTCMonth()+1)+"-"+f(this.getUTCDate())+"T"+f(this.getUTCHours())+":"+f(this.getUTCMinutes())+":"+f(this.getUTCSeconds())+"Z":null.};String.prototype.toJSON=Number.prototype.toJSON=Boolean.prototype.toJSON=function(key){ret

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 32x32, 32 bits/pixel
Category:	downloaded
Size (bytes):	4286
Entropy (8bit):	4.191445610755576
Encrypted:	false
SSDEEP:	48:9DoH8yAXQ8K5UvCUbpXtlhMVDBilhB7IODnNcynEJPMHErU8ACbtRKO7nhe+:9DlyAXQ8yUdduBiloycKeRg8xbtsO7
MD5:	4D27526198AC873CCEC96935198E0FB9
SHA1:	B98D8B73AD6A0F7477C3397561B4AAB37BF262AA
SHA-256:	40A2146151863BCF46C786D596E81A308D1B0D26D74635BE441E92656F29B1B4
SHA-512:	1EE4B73F4DA9C2B237CD0B820FFAD8E192D9125CE7D75D8A45A8B9642CE5FE85736646CAF12D246A77364C576751C47919997D066587F17575442A9B9F7CC97E
Malicious:	false
IE Cache URL:	http://https://www.weebly.com/favicon.ico
Preview:	....(... ...@..... .....D;3.C;4.D;3.D<3.D<3.D<6.A2".Pc.....M>5.....E;4.D;3.D;3.D<3.F<5.E<4.....F?4.ID5.D<37C;3.C;2.C;2.C;2.C;3.D<3LE=3.E=2.D<3.D=3.C<2QC;2.C;2.C;2.C;2.D;3.D;46JB;.G>6.....E;4.H<5.D;3]C;2.C;2.C;2.C;2.C;2.C;2.C;2.D<2.G<3.G<4.D<3.C;2.C;2.C;2.C;2.C;2.C;2.C;2.D<3[C=7.C<4.....H<7.B;1.D<3CC;2.C;2.C;2.C;2.C;2.C;2.C;2.C;2.C;2.D<2nD<3sC;2.C;2.C;2.C;2.C;2.C;2.C;2.C;2.C;2.D<3@B:3.HA2.....D<3.E<4.C;2.C;2.C;2.C;2.D<2.C;2bD<3pC<2.C;2.C;2.C;2.C;2.C;2.C;2.C;2.D<3lD<3^D;2.C;2.C;2.C;2.C;2.C;2.E<3.D<3.....C;2.D<3FC;2.C;2.C;2.D;2.F=3.E=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\site.19e2b99b084b05df36a8[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	79720
Entropy (8bit):	5.203186431437902
Encrypted:	false
SSDEEP:	1536:t7f7w7L7IFvCCAIIrBid1Y8EKmVvtii9tvg+YXetJ0Ek9z7E5XDjKvesgJJ7ZIye:NIrBid1Y8EKmVvtii9tvg+FkW5t7Q
MD5:	E7972106050BE9746F730AF053CE7D92
SHA1:	63D43128C994625807F2CB82964113C8EBE0DF8C
SHA-256:	8991E81F3C2FE38E02BFE42F80A5B8FCF98A18C399FB6C9A6369B2398A1872C3
SHA-512:	C9401A1142BB515D2F2E29B99DD0C306AB5ED5ABAF2FA0309450853BFEE5BDE6C3C4A6B44854C54B2DE2C370B48642D1616968707E8008C4FD1E4E8ECAEC62FF
Malicious:	false
IE Cache URL:	http://https://cdn3.editmysite.com/app/website/css/site.19e2b99b084b05df36a8.css
Preview:	.cko{position:fixed;top:0;right:0;height:100vh;width:0;opacity:1;background-color:#f6f6f6;z-index:10}.cko--open{width:100%;opacity:1;overflow:scroll}.cko--close,.cko--open{transition:all .15s linear}.cko--close{width:0;opacity:0;overflow:hidden}.cko--max-width{max-width:1048px;margin:0 auto}.cko__header{position:relative;z-index:10;background-color:#fff;box-shadow:0 1px 1px rgba(0,0,0,.1);height:72px}.cko__body{z-index:0;position:relative}.cko__header-items{align-items:center;display:grid;grid-auto-flow:column;grid-template-columns:1fr 1fr 1fr;height:100%;padding:0 16px}.cko__header-title{text-align:center;font-size:22px;font-family:var(--site-title-font);font-weight:600;font-weight:var(--site-title-font-weight,600);color:inherit}.cko__back-btn{font-size:14px;color:rgba(0,0,0,.6);display:flex;align-items:center}.cko__back-btn-label{display:inherit}.cko__back-btn>svg{margin-right:24px}@media (max-width:820px){.cko__back-btn-label{display:none}.cko__header-items{grid-template-columns:1fr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\imports.en.5190980851c8e63fd7692575cadd2295[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	281

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\imports.en.5190980851c8e63fd7692575cadd2295[1].js	
Entropy (8bit):	4.759537700169148
Encrypted:	false
SSDEEP:	6:YMSfYTg/z3/H81jJHAAurBOs8xfWQXhApRKb/iLRK/HwPuRKPEaBApRKdWiLRK/X:YnfT7/H8duDwxf1eKb/ilK/HieKPEaBm
MD5:	5190980851C8E63FD7692575CADD2295
SHA1:	BFE342608CD0DBB2DE311596662ADEB4C3C21D8A
SHA-256:	2ADADFDE7AD71A7C45311ED109CA8490556DB79CBC331B0E28C747A543C89CFA
SHA-512:	643609895779DF1CF73BF41D424ECCBE0DBB2BFCBAAA10FB3C2CC858D07A13A51821C9F06FA42CC17400399B402009F8C73C8064C7F291AFB9C063946FFFA0 B
Malicious:	false
IE Cache URL:	http://https://cdn3.editmysite.com/app/checkout/assets/checkout/imports.en.5190980851c8e63fd7692575cadd2295.js
Preview:	{"imports":{"vue":"app:vue","vuex":"app:vuex","axios":"app:axios","@popperjs/core":"app:popperjs","@ecom/checkout/weebly":"/app/checkout/assets/checkout/js/en/wcko.2ebb54873e6c4d3d2a9b.js","@ecom/checkout/square":"/app/checkout/assets/checkout/js/en/scko.9d3cbc48e87b876d9f51.js"}}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\runtime.4c27edfb51f63cc2e6e5.en[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):	50873
Entropy (8bit):	5.086523486566327
Encrypted:	false
SSDEEP:	768:xwmn5fnTo0YXc+sEdt0vBrKGR1mn5fnTo0AXc+sEdt0vBrKtR464Who:xm9c+V0vB+S9c+V0vB+tOMho
MD5:	B25B52EADE9D1B51B1B5442673E57AD1
SHA1:	10E9D825A5C5AB61705EC376B254D22CEF76BC9F
SHA-256:	F12BB68015C11969976246FAF720C8085271555CFDE5B05E3BC9A189CDA4D186
SHA-512:	201DB07040226E0F03879F91A529212E5BE9D06DFC37A33C8DF27DD4AD0BFBFD285AA320EDB3EE8291D4967641CA51E48684DDB81F13D8363539AEA4D7A769 E
Malicious:	false
IE Cache URL:	http://https://cdn3.editmysite.com/app/website/js/runtime.4c27edfb51f63cc2e6e5.en.js
Preview:	(function(e){function a(a){var d=a[0];var c=a[1];var f=a[2];var r,n,i=0,s=[];for(;i<d.length;i++){n=d[i];if(Object.prototype.hasOwnProperty.call(o,n)&&o[n]){s.push(o[n][0])}o[n]=0}for(r in c){if(Object.prototype.hasOwnProperty.call(c,r)){e[r]=c[r]}}if(l)l(a);while(s.length){s.shift()()}b.push.apply(b,f||[]);return t()}function t(){var e;for(var a=0;a<b.length;a++){var t=b[a];var d=true;for(var c=1;c<t.length;c++){var f=t[c];if(o[f]!==0)d=false}if(d){b.splice(a--,1);e=r(r.s=t[0])}}return e}var d={};var c={18:0};var o={18:0};var b=[];function f(e){return r.p+"js/"+({0:"vendors~about-us-hero~about-us-landscape~about-us-landscape-mirror~about-us-options~about-us-portrai~7362e151",1:"about-us-hero~about-us-landscape~about-us-landscape-mirror~about-us-portrait~banner-1~banner-10~bann~c61dcc79",2:"vendors~about-us-options~appointment-request-1~appointment-request-2~appointment-request-create~appo~44162992",3:"vendors~about-us-options~appointment-request-options~banner-options~blog-banner-opti

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\system.min.b9e210033fc5b0895164e282cbf89d5a[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):	11088
Entropy (8bit):	5.188389415116279
Encrypted:	false
SSDEEP:	192:aG4g/Uqr/KsO4am/MZlEZgk8NOrwe6uEGYBBXzkzrSKxv1UPAm3ydv:sGCv7IG/arfh1Ae
MD5:	BE83CD0E58A98300BA6A32F4B4FDBE61
SHA1:	FA067C68357EA6755E99C9B40DB29F54529BBDAD
SHA-256:	080BDC2202C77FAD49515BAAEFFF19D76DA0F4DFC234895038CDB46EAE069447
SHA-512:	172D36DC77EF7F4F3B5218DD5C835551B0F575863F67C95434281065A8B254369D1FF46049C66335DE6460637971A0C9D93623853E260C8AD9974BB9FC108B22
Malicious:	false
IE Cache URL:	http://https://cdn3.editmysite.com/app/checkout/assets/checkout/js/system.min.b9e210033fc5b0895164e282cbf89d5a.js
Preview:	!function(){function e(e,t){return(t||"")+" (SystemJS Error#"+e+" https://git.io/JvFET#"+e+")"}function t(e,t){if(-1!==e.indexOf("\\")&&(e=e.replace(/\\/g,"/")),"/"===e[0]&&"/"===e[1])return t.slice(0,t.indexOf(":")+1)+e;if("."===e[0]&&("/"===e[1]||"."===e[1]&&("/"===e[2]||2===e.length&&(e+="/"))||1===e.length&&(e+="/"))||"/"===e[0]){var n,r=t.slice(0,t.indexOf(":")+1);if(n="/"===t[r.length+1]?"file:"!==r?(n=t.slice(r.length+2)).slice(n.indexOf("/")+1):t.slice(8):t.slice(r.length+("/"===t[r.length])),"/"===e[0])return t.slice(0,t.length-n.length-1)+e;for(var i=n.slice(0,n.lastIndexOf("/")+1)+e,o=[],s=-1,u=0;i.length>u;u++)-1!==s?"/"===i[u]&&(o.push(i.slice(s,u+1)),s=-1):"."===i[u]?"."!==i[u+1]||"/"!==i[u+2]&&u+2!==i.length?"/"===i[u+1]||u+1===i.length?u+=1:s=u:(o.pop(),u+=2):s=u;return-1!==s&&o.push(i.slice(s)),t.slice(0,t.length-n.length)+o.join("")}}function n(e,n){return t(e,n)||(-1!==e.indexOf(":")?e:t("./"+e,n))}function r(e,n,r,i,o){for(var c in e){var a=t(c,r)||c,f=e[c];if("stri

C:\Users\user\AppData\Local\Temp\~DF4E0B9E52D160D036.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34429
Entropy (8bit):	0.42706963160956224
Encrypted:	false
SSDEEP:	48:kBqoxK0mDMmD9GmDOGmDEmD5mDrmD5mDbmDU7mDU:kBqoxK0m4mZGmKGmQmtmvmNmXmcm
MD5:	A3397EBF2383D28938E4E7BF06AA0EA6
SHA1:	42394487BE37E9F3DF59A75A7D59A12C09BA097F

C:\Users\user\AppData\Local\Temp\~DF4E0B9E52D160D036.TMP	
SHA-256:	F225A41D0833AFE16AE16666D69911C579649B66DD41DA9BC090675195F55A33
SHA-512:	9D3E4E155B2FCDE921C853CEB6FBF1123838F127376A60C85B48C4C7D6E8114D96125850FF923F17F2008BA5361446E99123C9BA964AC606F069069316008E7E
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF8168651D7F77EBF4.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13077
Entropy (8bit):	0.4860306818506857
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo69loq9lWUObkfWA:kBqoIlTUOl3
MD5:	DDC94190FBDBBAF0B4BDBB68C2EC968F
SHA1:	FFA16D4E7AF339DC61C5876940DD5CE494F88990
SHA-256:	FC35199F3D8E1FEBFC8307F599AD462F4C56F6D6A7E7406E4A6D2444D22E752E
SHA-512:	FF94817589117B697C3AE3EDA794862EE3E4287C5C76571E9CE6826FE6AF381D8E37F0868D6F6E28E9B52DBA51914210BB8DE3532D7D9587305590B069D183B9
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFCE6F74C9E03934EF.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.33833118838125686
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAUu9v:kBqoxxJhHWSVSEabLh
MD5:	B96035CECEECFCA9EF5C6C7ABCEC49FB
SHA1:	BAF510D50463E9859674507676D566B1817A5C8D
SHA-256:	E3DC3015BF6FE2774BBECA1DA47D335DA6F2D5FA15C00EA7DA92D44D56DAE7FB
SHA-512:	FB3A38B693A07706C90CC0691A838EA0CAE13BFC2283681803B6E9B592B060B13D8CB55E8BB526C772DB1F1373F8C5A71E2FF09F1354C4C47F4E1DDFD6C5C5E
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

General

File type:	PDF document, version 1.5
Entropy (8bit):	7.98554851869887
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	TETRATECH Covid-19 Stimulus Funds.pdf
File size:	226510
MD5:	63deffe4ac48f83f4ee319d30e6bf44b
SHA1:	e7a4742dd14ad017c56e5a6af04e5ccfc851967b
SHA256:	96355ec73c87cf7e781723c8fe1ebc9a7e91a23cdaeef4d4cc0b65077a9c5814
SHA512:	3a3e4017609f782feb24113989a74796a81f972f81762af006563adbac1542555cb5340022eecd4d2c36f621482d55822552884594225799440 8f78efffcc334
SSDEEP:	3072:a4gDI5sBam31U9p3ejCEyIcwtcA9RkLObrFz1EQICbetmeAm0GwZXjX5fwplM4Gb:a4LsbUTAyIHttQsFzaQKYm4XUlMpui9

General

File Content Preview:	%PDF-1.5..%.....1 0 obj..<</Type/Catalog/Pages 2 0 R/Lang(en-US) /StructTreeRoot 27 0 R/MarkInfo<</Marked true>>>>..endobj..2 0 obj..<</Type/Pages/Count 1/Kids[3 0 R] >>..endobj..3 0 obj..<</Type/Page/Parent 2 0 R/Resources<</Font<</F1 5 0 R/F2 8 0 R/F3

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

Header:	%PDF-1.5
Total Entropy:	7.985549
Total Bytes:	226510
Stream Entropy:	7.995237
Stream Bytes:	217512
Entropy outside Streams:	5.078779
Bytes outside Streams:	8998
Number of EOF found:	2
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	36
endobj	36
stream	9
endstream	9
xref	2
trailer	2
startxref	2
/Page	1
/Encrypt	0
/ObjStm	1
/URI	14
/JS	0
/JavaScript	0
/AA	0
/OpenAction	0
/AcroForm	0
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0

Network Behavior

Network Port Distribution

Total Packets: 111

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 5, 2021 23:23:11.070928097 CET	49766	443	192.168.2.4	199.34.228.96
Feb 5, 2021 23:23:11.071907997 CET	49767	443	192.168.2.4	199.34.228.96
Feb 5, 2021 23:23:11.253983974 CET	443	49766	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:11.254159927 CET	49766	443	192.168.2.4	199.34.228.96
Feb 5, 2021 23:23:11.254293919 CET	443	49767	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:11.254451036 CET	49767	443	192.168.2.4	199.34.228.96
Feb 5, 2021 23:23:11.264465094 CET	49767	443	192.168.2.4	199.34.228.96
Feb 5, 2021 23:23:11.264624119 CET	49766	443	192.168.2.4	199.34.228.96
Feb 5, 2021 23:23:11.445663929 CET	443	49767	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:11.445717096 CET	443	49766	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:11.454217911 CET	443	49767	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:11.454277992 CET	443	49767	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:11.454322100 CET	443	49767	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:11.454320908 CET	49767	443	192.168.2.4	199.34.228.96
Feb 5, 2021 23:23:11.454349995 CET	443	49767	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:11.454355955 CET	49767	443	192.168.2.4	199.34.228.96
Feb 5, 2021 23:23:11.454371929 CET	49767	443	192.168.2.4	199.34.228.96
Feb 5, 2021 23:23:11.454384089 CET	443	49767	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:11.454412937 CET	49767	443	192.168.2.4	199.34.228.96
Feb 5, 2021 23:23:11.454423904 CET	49767	443	192.168.2.4	199.34.228.96
Feb 5, 2021 23:23:11.458183050 CET	443	49766	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:11.458215952 CET	443	49766	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:11.458252907 CET	443	49766	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:11.458271027 CET	49766	443	192.168.2.4	199.34.228.96
Feb 5, 2021 23:23:11.458280087 CET	443	49766	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:11.458300114 CET	49766	443	192.168.2.4	199.34.228.96
Feb 5, 2021 23:23:11.458307028 CET	49766	443	192.168.2.4	199.34.228.96
Feb 5, 2021 23:23:11.458313942 CET	443	49766	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:11.458324909 CET	49766	443	192.168.2.4	199.34.228.96
Feb 5, 2021 23:23:11.458364010 CET	49766	443	192.168.2.4	199.34.228.96
Feb 5, 2021 23:23:11.486872911 CET	49766	443	192.168.2.4	199.34.228.96
Feb 5, 2021 23:23:11.486944914 CET	49767	443	192.168.2.4	199.34.228.96
Feb 5, 2021 23:23:11.493685961 CET	49767	443	192.168.2.4	199.34.228.96
Feb 5, 2021 23:23:11.667828083 CET	443	49767	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:11.667865992 CET	443	49766	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:11.674451113 CET	443	49767	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:11.676465034 CET	443	49767	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:11.676580906 CET	49767	443	192.168.2.4	199.34.228.96
Feb 5, 2021 23:23:11.682670116 CET	443	49766	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:11.682764053 CET	49766	443	192.168.2.4	199.34.228.96
Feb 5, 2021 23:23:13.042639017 CET	443	49767	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:13.042732954 CET	49767	443	192.168.2.4	199.34.228.96
Feb 5, 2021 23:23:13.042994976 CET	443	49767	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:13.043014050 CET	443	49767	199.34.228.96	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 5, 2021 23:23:13.043030024 CET	443	49767	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:13.043050051 CET	443	49767	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:13.043066978 CET	443	49767	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:13.043076038 CET	49767	443	192.168.2.4	199.34.228.96
Feb 5, 2021 23:23:13.043083906 CET	443	49767	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:13.043098927 CET	443	49767	199.34.228.96	192.168.2.4
Feb 5, 2021 23:23:13.043118000 CET	49767	443	192.168.2.4	199.34.228.96
Feb 5, 2021 23:23:13.043147087 CET	49767	443	192.168.2.4	199.34.228.96
Feb 5, 2021 23:23:13.334856987 CET	49768	443	192.168.2.4	151.101.1.46
Feb 5, 2021 23:23:13.335717916 CET	49769	443	192.168.2.4	151.101.1.46
Feb 5, 2021 23:23:13.336879969 CET	49770	443	192.168.2.4	151.101.1.46
Feb 5, 2021 23:23:13.338346004 CET	49771	443	192.168.2.4	151.101.1.46
Feb 5, 2021 23:23:13.339452982 CET	49772	443	192.168.2.4	151.101.1.46
Feb 5, 2021 23:23:13.340393066 CET	49773	443	192.168.2.4	151.101.1.46
Feb 5, 2021 23:23:13.376327991 CET	443	49768	151.101.1.46	192.168.2.4
Feb 5, 2021 23:23:13.376487970 CET	49768	443	192.168.2.4	151.101.1.46
Feb 5, 2021 23:23:13.377023935 CET	443	49769	151.101.1.46	192.168.2.4
Feb 5, 2021 23:23:13.377123117 CET	49769	443	192.168.2.4	151.101.1.46
Feb 5, 2021 23:23:13.377445936 CET	49768	443	192.168.2.4	151.101.1.46
Feb 5, 2021 23:23:13.378211975 CET	443	49770	151.101.1.46	192.168.2.4
Feb 5, 2021 23:23:13.378304958 CET	49770	443	192.168.2.4	151.101.1.46
Feb 5, 2021 23:23:13.379736900 CET	443	49771	151.101.1.46	192.168.2.4
Feb 5, 2021 23:23:13.379831076 CET	49771	443	192.168.2.4	151.101.1.46
Feb 5, 2021 23:23:13.380778074 CET	443	49772	151.101.1.46	192.168.2.4
Feb 5, 2021 23:23:13.380906105 CET	49772	443	192.168.2.4	151.101.1.46
Feb 5, 2021 23:23:13.381762028 CET	443	49773	151.101.1.46	192.168.2.4
Feb 5, 2021 23:23:13.381838083 CET	49773	443	192.168.2.4	151.101.1.46
Feb 5, 2021 23:23:13.393583059 CET	49773	443	192.168.2.4	151.101.1.46
Feb 5, 2021 23:23:13.393820047 CET	49770	443	192.168.2.4	151.101.1.46
Feb 5, 2021 23:23:13.394026995 CET	49771	443	192.168.2.4	151.101.1.46
Feb 5, 2021 23:23:13.394252062 CET	49772	443	192.168.2.4	151.101.1.46
Feb 5, 2021 23:23:13.395234108 CET	49769	443	192.168.2.4	151.101.1.46
Feb 5, 2021 23:23:13.418884993 CET	443	49768	151.101.1.46	192.168.2.4
Feb 5, 2021 23:23:13.420269966 CET	443	49768	151.101.1.46	192.168.2.4
Feb 5, 2021 23:23:13.420299053 CET	443	49768	151.101.1.46	192.168.2.4
Feb 5, 2021 23:23:13.420314074 CET	443	49768	151.101.1.46	192.168.2.4
Feb 5, 2021 23:23:13.420500040 CET	49768	443	192.168.2.4	151.101.1.46
Feb 5, 2021 23:23:13.435028076 CET	443	49773	151.101.1.46	192.168.2.4
Feb 5, 2021 23:23:13.435055017 CET	443	49770	151.101.1.46	192.168.2.4
Feb 5, 2021 23:23:13.435307980 CET	443	49771	151.101.1.46	192.168.2.4
Feb 5, 2021 23:23:13.435492039 CET	443	49772	151.101.1.46	192.168.2.4
Feb 5, 2021 23:23:13.435977936 CET	443	49773	151.101.1.46	192.168.2.4
Feb 5, 2021 23:23:13.436002016 CET	443	49773	151.101.1.46	192.168.2.4
Feb 5, 2021 23:23:13.436022043 CET	443	49773	151.101.1.46	192.168.2.4
Feb 5, 2021 23:23:13.436135054 CET	49773	443	192.168.2.4	151.101.1.46
Feb 5, 2021 23:23:13.436184883 CET	49773	443	192.168.2.4	151.101.1.46
Feb 5, 2021 23:23:13.436253071 CET	443	49770	151.101.1.46	192.168.2.4
Feb 5, 2021 23:23:13.436278105 CET	443	49770	151.101.1.46	192.168.2.4
Feb 5, 2021 23:23:13.436332941 CET	443	49770	151.101.1.46	192.168.2.4
Feb 5, 2021 23:23:13.436325073 CET	49770	443	192.168.2.4	151.101.1.46
Feb 5, 2021 23:23:13.436387062 CET	49770	443	192.168.2.4	151.101.1.46
Feb 5, 2021 23:23:13.436393023 CET	49770	443	192.168.2.4	151.101.1.46
Feb 5, 2021 23:23:13.436397076 CET	443	49771	151.101.1.46	192.168.2.4
Feb 5, 2021 23:23:13.436486959 CET	49771	443	192.168.2.4	151.101.1.46
Feb 5, 2021 23:23:13.436501980 CET	443	49771	151.101.1.46	192.168.2.4
Feb 5, 2021 23:23:13.436525106 CET	443	49771	151.101.1.46	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 5, 2021 23:22:01.326831102 CET	55854	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:01.373547077 CET	53	55854	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:02.254363060 CET	64549	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:02.303975105 CET	53	64549	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 5, 2021 23:22:03.331855059 CET	63153	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:03.381288052 CET	53	63153	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:04.775413990 CET	52991	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:04.822120905 CET	53	52991	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:06.977586031 CET	53700	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:07.035687923 CET	53	53700	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:08.159132957 CET	51726	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:08.207243919 CET	53	51726	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:09.392519951 CET	56794	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:09.439295053 CET	53	56794	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:10.557367086 CET	56534	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:10.607116938 CET	53	56534	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:12.591830015 CET	56627	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:12.638513088 CET	53	56627	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:14.794167995 CET	56621	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:14.841516972 CET	53	56621	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:16.414706945 CET	63116	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:16.470139980 CET	53	63116	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:19.321410894 CET	64078	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:19.368093967 CET	53	64078	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:21.375675917 CET	64801	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:21.431884050 CET	53	64801	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:21.700813055 CET	61721	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:21.757580996 CET	53	61721	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:22.575033903 CET	64801	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:22.630125999 CET	53	64801	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:22.728046894 CET	61721	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:22.782929897 CET	53	61721	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:23.535001993 CET	64801	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:23.591962099 CET	53	64801	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:23.737637997 CET	61721	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:23.792864084 CET	53	61721	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:24.787940979 CET	51255	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:24.834656000 CET	53	51255	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:25.577785015 CET	64801	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:25.634980917 CET	53	64801	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:25.780981064 CET	61721	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:25.837989092 CET	53	61721	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:26.032782078 CET	61522	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:26.079581022 CET	53	61522	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:29.590395927 CET	64801	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:29.647290945 CET	53	64801	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:29.840322018 CET	61721	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:29.897238016 CET	53	61721	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:30.963644028 CET	52337	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:31.021567106 CET	53	52337	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:44.517193079 CET	55046	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:44.566812038 CET	53	55046	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:45.199079037 CET	49612	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:45.253846884 CET	53	49612	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:45.782407045 CET	49285	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:45.840017080 CET	53	49285	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:46.105431080 CET	50601	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:46.178348064 CET	53	50601	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:46.270543098 CET	60875	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:46.325598955 CET	53	60875	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:46.736594915 CET	56448	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:46.785808086 CET	53	56448	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:47.286184072 CET	59172	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:47.343275070 CET	53	59172	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:47.890847921 CET	62420	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:47.947597027 CET	53	62420	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:48.759574890 CET	60579	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:48.806091070 CET	53	60579	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 5, 2021 23:22:49.604108095 CET	50183	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:49.664829016 CET	53	50183	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:50.072247982 CET	61531	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:50.141402006 CET	53	61531	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:50.359086037 CET	49228	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:50.408670902 CET	53	49228	8.8.8.8	192.168.2.4
Feb 5, 2021 23:22:59.201644897 CET	59794	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:22:59.274576902 CET	53	59794	8.8.8.8	192.168.2.4
Feb 5, 2021 23:23:02.482851028 CET	55916	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:23:02.529567003 CET	53	55916	8.8.8.8	192.168.2.4
Feb 5, 2021 23:23:02.810981989 CET	52752	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:23:02.867043018 CET	53	52752	8.8.8.8	192.168.2.4
Feb 5, 2021 23:23:04.897449017 CET	60542	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:23:04.953701973 CET	53	60542	8.8.8.8	192.168.2.4
Feb 5, 2021 23:23:09.931444883 CET	60689	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:23:09.983541965 CET	64206	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:23:09.988842010 CET	53	60689	8.8.8.8	192.168.2.4
Feb 5, 2021 23:23:10.043382883 CET	53	64206	8.8.8.8	192.168.2.4
Feb 5, 2021 23:23:10.976067066 CET	50904	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:23:11.049283028 CET	53	50904	8.8.8.8	192.168.2.4
Feb 5, 2021 23:23:13.169562101 CET	57525	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:23:13.228676081 CET	53	57525	8.8.8.8	192.168.2.4
Feb 5, 2021 23:23:13.731795073 CET	53814	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:23:13.790132046 CET	53	53814	8.8.8.8	192.168.2.4
Feb 5, 2021 23:23:14.251444101 CET	53418	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:23:14.306564093 CET	53	53418	8.8.8.8	192.168.2.4
Feb 5, 2021 23:23:14.742306948 CET	62833	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:23:14.796880007 CET	53	62833	8.8.8.8	192.168.2.4
Feb 5, 2021 23:23:37.023575068 CET	63300	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:23:37.080565929 CET	53	63300	8.8.8.8	192.168.2.4
Feb 5, 2021 23:23:40.019639015 CET	61449	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:23:40.047358990 CET	51275	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:23:40.079654932 CET	53	61449	8.8.8.8	192.168.2.4
Feb 5, 2021 23:23:40.093957901 CET	53	51275	8.8.8.8	192.168.2.4
Feb 5, 2021 23:23:40.703638077 CET	63492	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:23:40.750466108 CET	53	63492	8.8.8.8	192.168.2.4
Feb 5, 2021 23:23:41.014720917 CET	61449	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:23:41.072427988 CET	53	61449	8.8.8.8	192.168.2.4
Feb 5, 2021 23:23:41.265325069 CET	58945	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:23:41.328866959 CET	53	58945	8.8.8.8	192.168.2.4
Feb 5, 2021 23:23:41.715421915 CET	63492	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:23:41.770649910 CET	53	63492	8.8.8.8	192.168.2.4
Feb 5, 2021 23:23:42.028099060 CET	61449	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:23:42.087745905 CET	53	61449	8.8.8.8	192.168.2.4
Feb 5, 2021 23:23:42.715954065 CET	63492	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:23:42.837986946 CET	53	63492	8.8.8.8	192.168.2.4
Feb 5, 2021 23:23:44.028640032 CET	61449	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:23:44.078160048 CET	53	61449	8.8.8.8	192.168.2.4
Feb 5, 2021 23:23:44.731652975 CET	63492	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:23:44.786854029 CET	53	63492	8.8.8.8	192.168.2.4
Feb 5, 2021 23:23:48.044318914 CET	61449	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:23:48.102760077 CET	53	61449	8.8.8.8	192.168.2.4
Feb 5, 2021 23:23:48.748472929 CET	63492	53	192.168.2.4	8.8.8.8
Feb 5, 2021 23:23:48.803256035 CET	53	63492	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 5, 2021 23:22:59.201644897 CET	192.168.2.4	8.8.8.8	0x8061	Standard query (0)	weeblysite.com	A (IP address)	IN (0x0001)
Feb 5, 2021 23:23:09.983541965 CET	192.168.2.4	8.8.8.8	0xbdf8	Standard query (0)	my-site-105523-100173.weeblysite.com	A (IP address)	IN (0x0001)
Feb 5, 2021 23:23:10.976067066 CET	192.168.2.4	8.8.8.8	0x6764	Standard query (0)	my-site-105523-100173.weeblysite.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 5, 2021 23:23:13.169562101 CET	192.168.2.4	8.8.8.8	0xebd5	Standard query (0)	cdn3.editmysite.com	A (IP address)	IN (0x0001)
Feb 5, 2021 23:23:13.731795073 CET	192.168.2.4	8.8.8.8	0x17c0	Standard query (0)	cdn2.editmysite.com	A (IP address)	IN (0x0001)
Feb 5, 2021 23:23:14.251444101 CET	192.168.2.4	8.8.8.8	0x2d43	Standard query (0)	ec.editmysite.com	A (IP address)	IN (0x0001)
Feb 5, 2021 23:23:14.742306948 CET	192.168.2.4	8.8.8.8	0x30c5	Standard query (0)	www.weebly.com	A (IP address)	IN (0x0001)
Feb 5, 2021 23:23:37.023575068 CET	192.168.2.4	8.8.8.8	0xd1de	Standard query (0)	www.weebly.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 5, 2021 23:22:59.274576902 CET	8.8.8.8	192.168.2.4	0x8061	No error (0)	weeblysite.com		199.34.228.96	A (IP address)	IN (0x0001)
Feb 5, 2021 23:22:59.274576902 CET	8.8.8.8	192.168.2.4	0x8061	No error (0)	weeblysite.com		199.34.228.97	A (IP address)	IN (0x0001)
Feb 5, 2021 23:23:10.043382883 CET	8.8.8.8	192.168.2.4	0xbdf8	No error (0)	my-site-105523-100173.weeblysite.com	weeblysite.com		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 23:23:10.043382883 CET	8.8.8.8	192.168.2.4	0xbdf8	No error (0)	weeblysite.com		199.34.228.96	A (IP address)	IN (0x0001)
Feb 5, 2021 23:23:10.043382883 CET	8.8.8.8	192.168.2.4	0xbdf8	No error (0)	weeblysite.com		199.34.228.97	A (IP address)	IN (0x0001)
Feb 5, 2021 23:23:11.049283028 CET	8.8.8.8	192.168.2.4	0x6764	No error (0)	my-site-105523-100173.weeblysite.com	weeblysite.com		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 23:23:11.049283028 CET	8.8.8.8	192.168.2.4	0x6764	No error (0)	weeblysite.com		199.34.228.96	A (IP address)	IN (0x0001)
Feb 5, 2021 23:23:11.049283028 CET	8.8.8.8	192.168.2.4	0x6764	No error (0)	weeblysite.com		199.34.228.97	A (IP address)	IN (0x0001)
Feb 5, 2021 23:23:13.228676081 CET	8.8.8.8	192.168.2.4	0xebd5	No error (0)	cdn3.editmysite.com	weebly.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 23:23:13.228676081 CET	8.8.8.8	192.168.2.4	0xebd5	No error (0)	weebly.map.fastly.net		151.101.1.46	A (IP address)	IN (0x0001)
Feb 5, 2021 23:23:13.228676081 CET	8.8.8.8	192.168.2.4	0xebd5	No error (0)	weebly.map.fastly.net		151.101.65.46	A (IP address)	IN (0x0001)
Feb 5, 2021 23:23:13.228676081 CET	8.8.8.8	192.168.2.4	0xebd5	No error (0)	weebly.map.fastly.net		151.101.129.46	A (IP address)	IN (0x0001)
Feb 5, 2021 23:23:13.228676081 CET	8.8.8.8	192.168.2.4	0xebd5	No error (0)	weebly.map.fastly.net		151.101.193.46	A (IP address)	IN (0x0001)
Feb 5, 2021 23:23:13.790132046 CET	8.8.8.8	192.168.2.4	0x17c0	No error (0)	cdn2.editmysite.com	weebly.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 23:23:13.790132046 CET	8.8.8.8	192.168.2.4	0x17c0	No error (0)	weebly.map.fastly.net		151.101.1.46	A (IP address)	IN (0x0001)
Feb 5, 2021 23:23:13.790132046 CET	8.8.8.8	192.168.2.4	0x17c0	No error (0)	weebly.map.fastly.net		151.101.65.46	A (IP address)	IN (0x0001)
Feb 5, 2021 23:23:13.790132046 CET	8.8.8.8	192.168.2.4	0x17c0	No error (0)	weebly.map.fastly.net		151.101.129.46	A (IP address)	IN (0x0001)
Feb 5, 2021 23:23:13.790132046 CET	8.8.8.8	192.168.2.4	0x17c0	No error (0)	weebly.map.fastly.net		151.101.193.46	A (IP address)	IN (0x0001)
Feb 5, 2021 23:23:14.306564093 CET	8.8.8.8	192.168.2.4	0x2d43	No error (0)	ec.editmysite.com	sp-202002141230115249000000a-1069308460.us-west-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 5, 2021 23:23:14.306564093 CET	8.8.8.8	192.168.2.4	0x2d43	No error (0)	sp-2020021 4123011524 90000000a-1069308460.us-west-2 .elb.amazo naws.com		54.212.183.219	A (IP address)	IN (0x0001)
Feb 5, 2021 23:23:14.306564093 CET	8.8.8.8	192.168.2.4	0x2d43	No error (0)	sp-2020021 4123011524 90000000a-1069308460.us-west-2 .elb.amazo naws.com		44.232.20.119	A (IP address)	IN (0x0001)
Feb 5, 2021 23:23:14.796880007 CET	8.8.8.8	192.168.2.4	0x30c5	No error (0)	www.weebly .com	weebly.com		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 23:23:14.796880007 CET	8.8.8.8	192.168.2.4	0x30c5	No error (0)	weebly.com		74.115.50.110	A (IP address)	IN (0x0001)
Feb 5, 2021 23:23:14.796880007 CET	8.8.8.8	192.168.2.4	0x30c5	No error (0)	weebly.com		74.115.50.109	A (IP address)	IN (0x0001)
Feb 5, 2021 23:23:37.080565929 CET	8.8.8.8	192.168.2.4	0xd1de	No error (0)	www.weebly .com	weebly.com		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 23:23:37.080565929 CET	8.8.8.8	192.168.2.4	0xd1de	No error (0)	weebly.com		74.115.50.110	A (IP address)	IN (0x0001)
Feb 5, 2021 23:23:37.080565929 CET	8.8.8.8	192.168.2.4	0xd1de	No error (0)	weebly.com		74.115.50.109	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 5, 2021 23:23:11.454384089 CET	199.34.228.96	443	192.168.2.4	49767	CN=*.weeblysite.com, O="Square, Inc", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Nov 14 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 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=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Feb 5, 2021 23:23:11.458313942 CET	199.34.228.96	443	192.168.2.4	49766	CN=*.weeblysite.com, O="Square, Inc", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Nov 14 01:00:00 CET 2020	Mon Nov 15 00:59:59 CET 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=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Feb 5, 2021 23:23:13.420314074 CET	151.101.1.46	443	192.168.2.4	49768	CN=editmysite.com, O="Weebly, Inc.", L=San Francisco, ST=California, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 21 20:34:09 CEST 2020 Wed Aug 19 02:00:00 CEST 2015	Thu Apr 22 20:34:09 CEST 2021 Tue Aug 19 02:00:00 CEST 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 5, 2021 23:23:13.436022043 CET	151.101.1.46	443	192.168.2.4	49773	CN=editmysite.com, O="Weebly, Inc.", L=San Francisco, ST=California, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 21 20:34:09 CEST 2020 Wed Aug 19 02:00:00 CEST 2015	Thu Apr 22 20:34:09 CEST 2021 Tue Aug 19 02:00:00 CEST 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		
Feb 5, 2021 23:23:13.436332941 CET	151.101.1.46	443	192.168.2.4	49770	CN=editmysite.com, O="Weebly, Inc.", L=San Francisco, ST=California, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 21 20:34:09 CEST 2020 Wed Aug 19 02:00:00 CEST 2015	Thu Apr 22 20:34:09 CEST 2021 Tue Aug 19 02:00:00 CEST 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		
Feb 5, 2021 23:23:13.436525106 CET	151.101.1.46	443	192.168.2.4	49771	CN=editmysite.com, O="Weebly, Inc.", L=San Francisco, ST=California, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 21 20:34:09 CEST 2020 Wed Aug 19 02:00:00 CEST 2015	Thu Apr 22 20:34:09 CEST 2021 Tue Aug 19 02:00:00 CEST 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		
Feb 5, 2021 23:23:13.436724901 CET	151.101.1.46	443	192.168.2.4	49772	CN=editmysite.com, O="Weebly, Inc.", L=San Francisco, ST=California, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 21 20:34:09 CEST 2020 Wed Aug 19 02:00:00 CEST 2015	Thu Apr 22 20:34:09 CEST 2021 Tue Aug 19 02:00:00 CEST 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		
Feb 5, 2021 23:23:13.438225985 CET	151.101.1.46	443	192.168.2.4	49769	CN=editmysite.com, O="Weebly, Inc.", L=San Francisco, ST=California, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 21 20:34:09 CEST 2020 Wed Aug 19 02:00:00 CEST 2015	Thu Apr 22 20:34:09 CEST 2021 Tue Aug 19 02:00:00 CEST 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		

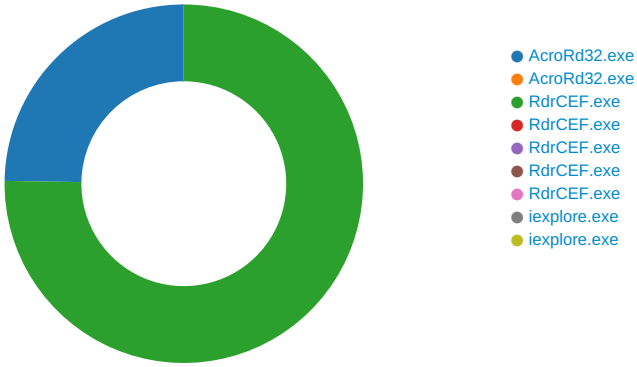
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 5, 2021 23:23:14.050132990 CET	151.101.1.46	443	192.168.2.4	49774	CN=editmysite.com, O="Weebly, Inc.", L=San Francisco, ST=California, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 21 20:34:09 CEST 2020 Wed Aug 19 02:00:00 CEST 2015	Thu Apr 22 20:34:09 CEST 2021 Tue Aug 19 02:00:00 CEST 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		
Feb 5, 2021 23:23:14.050751925 CET	151.101.1.46	443	192.168.2.4	49775	CN=editmysite.com, O="Weebly, Inc.", L=San Francisco, ST=California, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 21 20:34:09 CEST 2020 Wed Aug 19 02:00:00 CEST 2015	Thu Apr 22 20:34:09 CEST 2021 Tue Aug 19 02:00:00 CEST 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		
Feb 5, 2021 23:23:14.935049057 CET	54.212.183.219	443	192.168.2.4	49776	CN=ec.editmysite.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 09 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Oct 09 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 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 5, 2021 23:23:14.936885118 CET	54.212.183.219	443	192.168.2.4	49777	CN=ec.editmysite.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 09 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Oct 09 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Feb 5, 2021 23:23:15.679418087 CET	74.115.50.110	443	192.168.2.4	49779	CN=www.weebly.com, O="Square, Inc", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Aug 10 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Mon Aug 15 14:00:00 CEST 2022 Wed Mar 08 13:00:00 CET 2023	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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Feb 5, 2021 23:23:15.681696892 CET	74.115.50.110	443	192.168.2.4	49778	CN=www.weebly.com, O="Square, Inc", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Aug 10 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Mon Aug 15 14:00:00 CEST 2022 Wed Mar 08 13:00:00 CET 2023	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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Feb 5, 2021 23:23:37.493650913 CET	74.115.50.110	443	192.168.2.4	49780	CN=www.weebly.com, O="Square, Inc", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Aug 10 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Mon Aug 15 14:00:00 CEST 2022 Wed Mar 08 13:00:00 CET 2023	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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: AcroRd32.exe PID: 808 Parent PID: 5996

General

Start time:	23:22:06
Start date:	05/02/2021
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\TETRATECH Covid-19 Stimulus Funds.pdf'
Imagebase:	0xa00000
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	A365C3	CreateDirectoryExW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	A5AE05	CreateDirectoryW
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	success or wait	1	A4EA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210205222213Z-184.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	A4EA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AdobeFnt16.lst.6296	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	A4EA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\acrolock808.1.2277533396.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	A82657	CreateFileW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.6296	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	A4EA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock808.2.2437960247.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	A82657	CreateFileW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock808.3.3483743970.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	A82657	CreateFileW
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	AC83C8	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	AC83C8	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	AC83C8	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	AC83C8	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	AC83C8	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	AC83C8	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R2uw3yd_7nbm5d_4uw.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	A4EA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	4	A4EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rgraswz_7nbm5e_4uw.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	A4EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rkow11p_7nbm5f_4uw.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	A4EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1h6hjk9_7nbm5g_4uw.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	A4EA85	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R10dt6zc_7nbm5h_4uw.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	A4EA85	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.6296	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AcroFnt19.lst	success or wait	1	A8D405	NtSetInformationFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.6296	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst	success or wait	1	A8D405	NtSetInformationFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.6296	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeCMapFnt19.lst	success or wait	1	A8D405	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	A4CF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	A4D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	A4D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo	success or wait	1	A4D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\NoTimeOut	success or wait	1	A4D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	A0EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	A0EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	A0EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\TrustManager	success or wait	1	A4D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\TrustManager\cDefaultLaunchURLPerms	success or wait	1	A4D41D	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	A5DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/Users/user/Desktop/TETRATECH Covid-19 Stimulus Funds.pdf	success or wait	1	A5DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	TETRATECH Covid-19 Stimulus Funds.pdf	success or wait	1	A5DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	A5DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	A5DF69	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 54 45 54 52 41 54 45 43 48 20 43 6F 76 69 64 2D 31 39 20 53 74 69 6D 75 6C 75 73 20 46 75 6E 64 73 2E 70 64 66 00	success or wait	1	A5DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDate	binary	44 3A 32 30 32 31 30 32 30 35 32 33 32 32 31 33 2B 30 31 27 30 30 27 00	success or wait	1	A5DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	226510	success or wait	1	A5DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	1	success or wait	1	A5DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	A5DF47	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tDIText	unicode	http://www.adobe.com/go/homeacrordrunified18_2018	success or wait	1	A5DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	A5DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	A5DF69	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	A5DF69	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	A5DF69	RegSetValueExW

Analysis Process: AcroRd32.exe PID: 6296 Parent PID: 808

General

Start time:	23:22:07
Start date:	05/02/2021
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\TETRATECH Covid-19 Stimulus Funds.pdf'
Imagebase:	0xa00000
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: 6168 Parent PID: 808

General

Start time:	23:22:12
Start date:	05/02/2021
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:	0x850000
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	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	3	9459E2	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	9	9583E5	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	65	958447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	164	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	3	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	6	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	3	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	18	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	3	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	6	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	3	9459E2	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	9459E2	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	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	1630	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	3	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	45	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	3	9459E2	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	9459E2	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	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	6	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	3	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	3	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	3	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	3	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	3	9459E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	success or wait	2	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	end of file	3	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	38	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	42	9459E2	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	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	44	9459E2	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	9459E2	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	15	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	end of file	3	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	13	9459E2	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	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	14	9459E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	3	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	214	9459E2	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	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	success or wait	201	9459E2	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	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	42	9459E2	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	9459E2	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	184	9459E2	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	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	22	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	3	9459E2	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	9459E2	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	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	5	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	1	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	4	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	end of file	1	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	161	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	end of file	1	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	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	9459E2	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	9583E5	ReadFile

Analysis Process: RdrCEF.exe PID: 6600 Parent PID: 6168

General

Start time:	23:22:15
Start date:	05/02/2021
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=1728,5754072549746782878,9114216532001329358,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=3954240331908333317 --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=3954240331908333317 --renderer-client-id=2 --mojo-platform-channel-handle=1736 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x850000
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: 6740 Parent PID: 6168

General

Start time:	23:22:16
Start date:	05/02/2021
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=1728,5754072549746782878,9114216532001329358,131072 --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-preference s=KAAAAAAAAACAAwABAQAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAACgAAAAEAAAAIAAAAAAAAAoAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=10276253575640265967 --mojo-platform-channel-handle=1748 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0x850000
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: 6608 Parent PID: 6168

General

Start time:	23:22:18
Start date:	05/02/2021
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=1728,575407254974678 2878,9114216532001329358,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=14130125459791333574 --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=14130125459791333574 --renderer-client-id=4 --mojo-platform-channel-handle=1844 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x850000
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: 7084 Parent PID: 6168

General

Start time:	23:22:25
Start date:	05/02/2021
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=1728,575407254974678 2878,9114216532001329358,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=8407246014169871722 --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=8407246014169871722 --renderer-client-id=5 --mojo-platform-channel-handle=2480 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x850000
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: 808

General

Start time:	23:23:09
Start date:	05/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' https://my-site-105523-100173.weeblysite.com/
Imagebase:	0x7ff7ba850000
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: 4528 Parent PID: 2740

General

Start time:	23:23:10

Start date:	05/02/2021
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:	0xd20000
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

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

Disassembly

Code Analysis