ID: 338148
Sample Name: Information-Account-Prime-Disable-Service.pdf
Cookbook: defaultwindowspdfcookbook.jbs
Time: 18:06:30
Date: 11/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

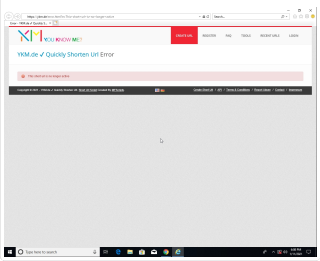
Analysis Report Information-Account-Prime-Disable-Ser…

Overview

General Information

Sample Name:	Information-Account-Prime-Disable-Service.pdf
Analysis ID:	338148
MD5:	7ef4760a44a8cc6..
SHA1:	19af34bf781eb79..
SHA256:	29c631b5ce054c…

Most interesting Screenshot:



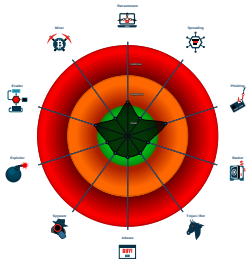
Detection

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

Signatures

- Machine Learning detection for samp…
- Contains functionality to access load…
- Found iframes
- HTML title does not match URL
- 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: 5948 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\Information-Account-Prime-Disable-Service.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 5956 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\Information-Account-Prime-Disable-Service.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 5060 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6344 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=1676,6902283869037015468,17832798338356840690,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=13817734648253318396 --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=13817734648253318396 --renderer-client-id=2 --mojo-platform-channel-handle=1720 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6372 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1676,6902283869037015468,17832798338356840690,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=11890072385820109879 --mojo-platform-channel-handle=1748 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6424 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=1676,6902283869037015468,17832798338356840690,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=1881667437359436119 --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=1881667437359436119 --renderer-client-id=4 --mojo-platform-channel-handle=1860 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6560 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=1676,6902283869037015468,17832798338356840690,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=5458918827524385669 --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=5458918827524385669 --renderer-client-id=5 --mojo-platform-channel-handle=1864 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6676 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=1676,6902283869037015468,17832798338356840690,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=13143280483817159406 --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=13143280483817159406 --renderer-client-id=6 --mojo-platform-channel-handle=2140 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
  - iexplore.exe (PID: 4736 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' https://t.umblr.com/redirect?z=https%3A%2F%2Fykm.de%2F65f0a4768a364c17&t=MDZmNTEyZmUxYzY5ZjJkNjc3MDI5MTI0MjhiODVlNzBhYTAzZWMzZCwwY2IyNWEwNWYyMzA5MGNlNzYxMzg5ZTFhMTcwMTA4Y2U5NmEwYzZl&ts=1610149120 MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
    - iexplore.exe (PID: 1048 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4736 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

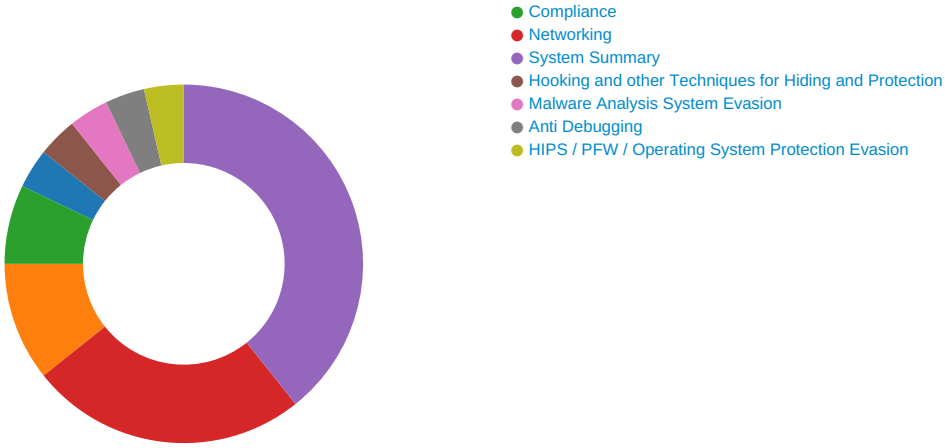
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Phishing



Click to jump to signature section

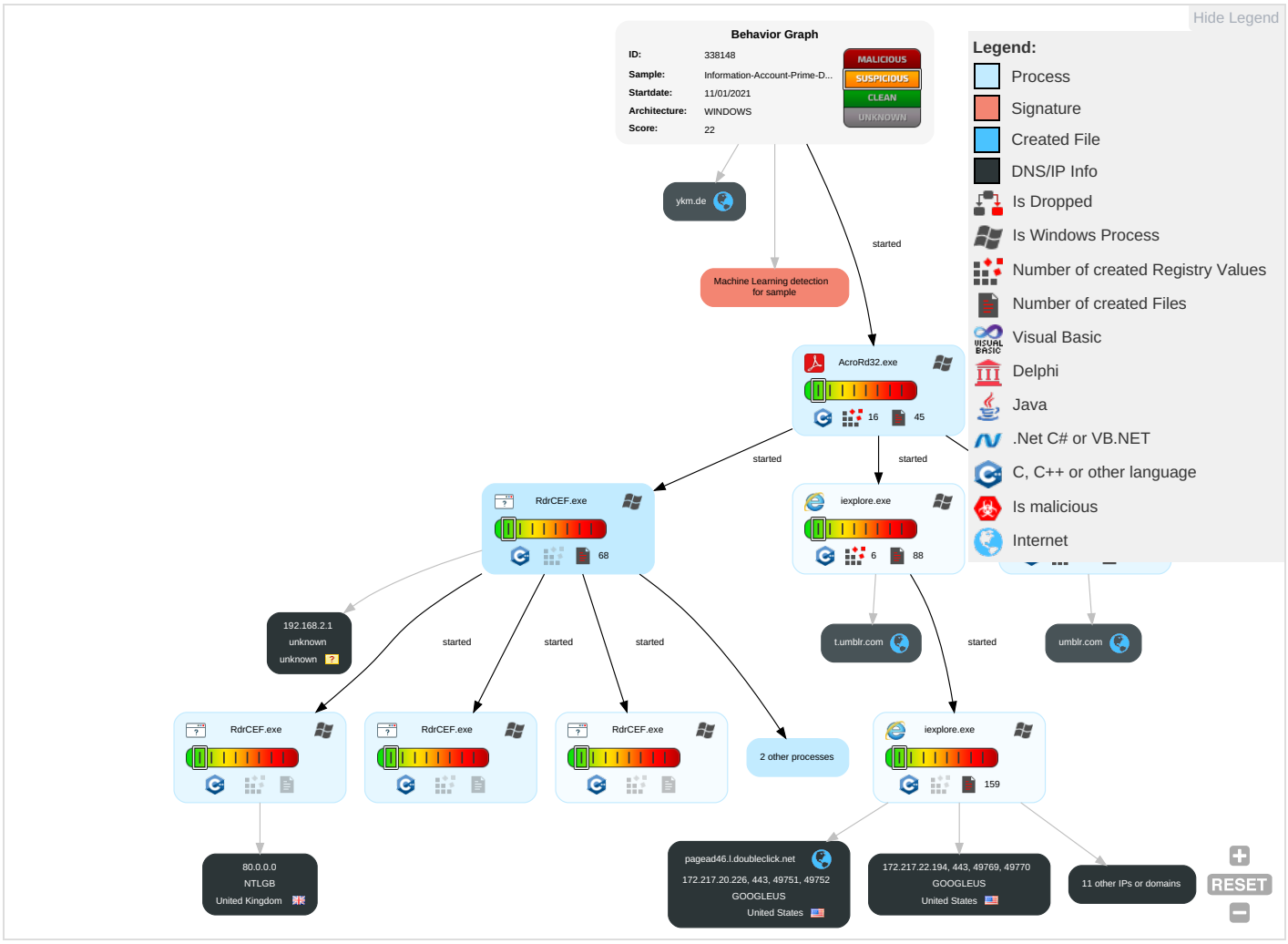
AV Detection:

Machine Learning detection for sample

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Spearphishing Link 1	Windows Management Instrumentation	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Drive-by Compromise 1	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
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

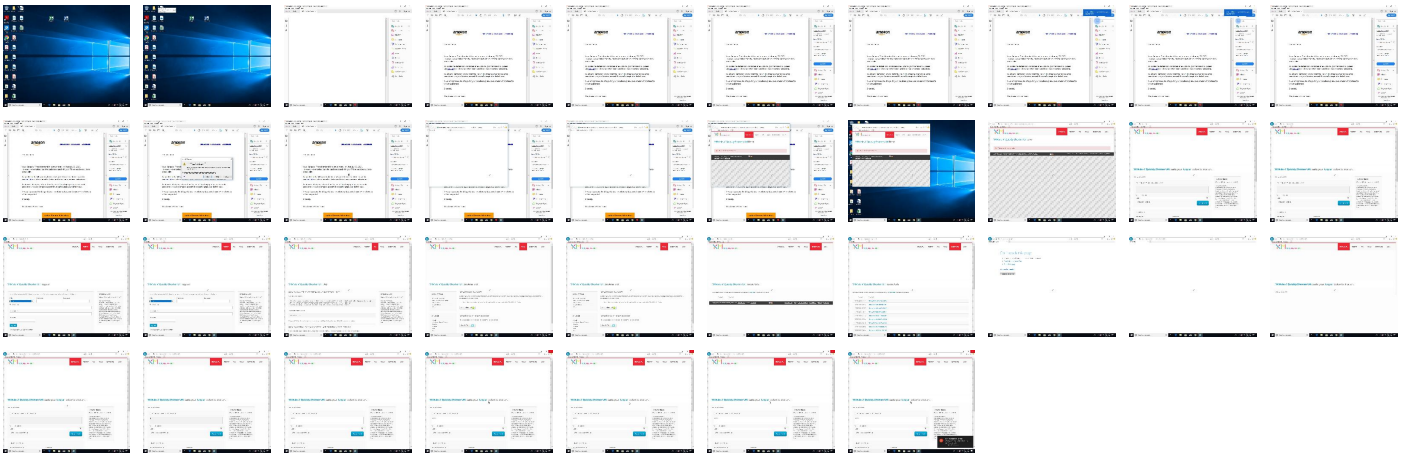
Behavior Graph

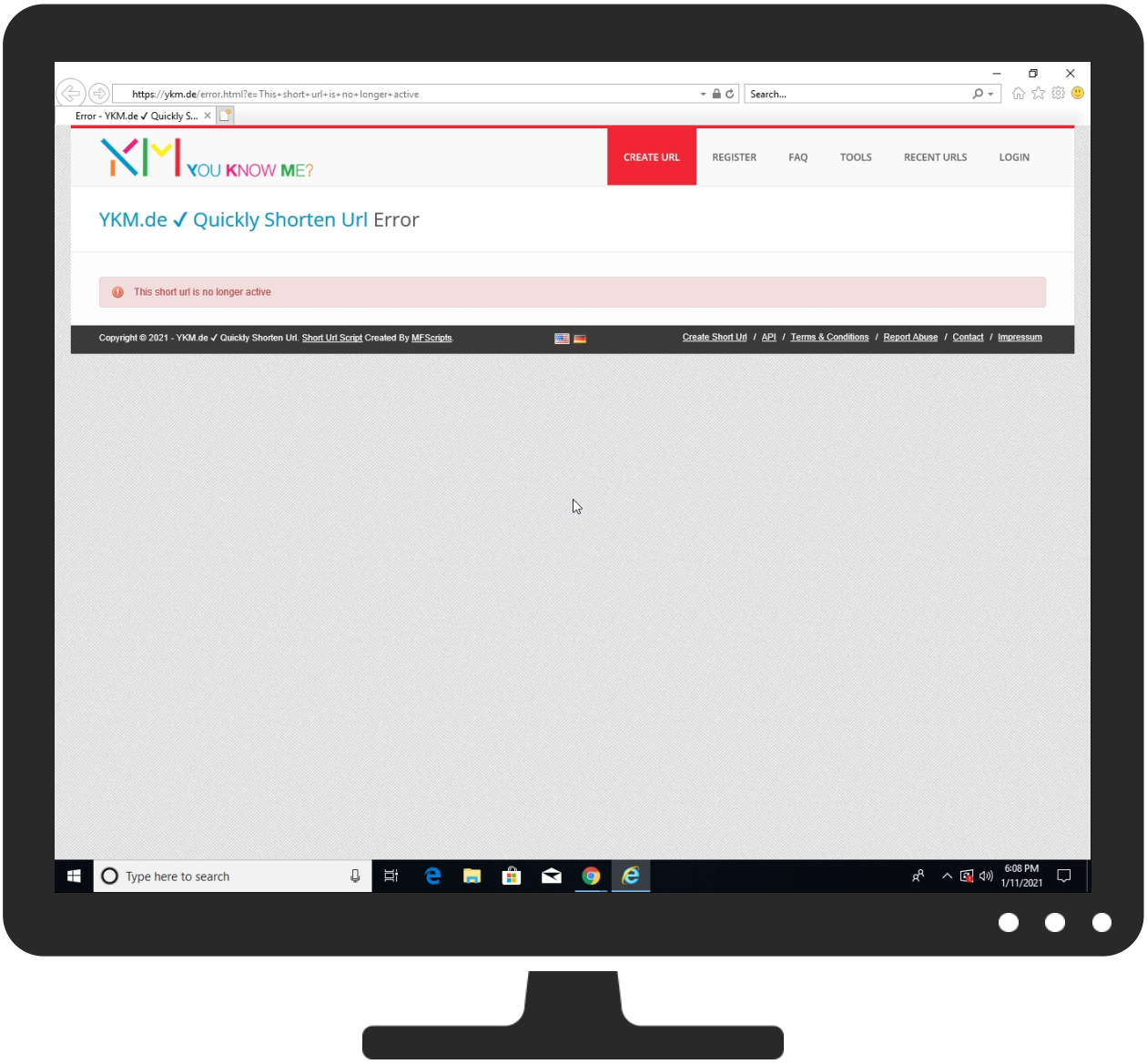


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Information-Account-Prime-Disable-Service.pdf	0%	Virustotal		Browse
Information-Account-Prime-Disable-Service.pdf	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
ykm.de	4%	Virustotal		Browse
adservice.google.co.uk	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://ykm.de/api.html#activate	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://ykm.de/themes/ykm/styles/css/font-awesome.min.css	0%	Avira URL Cloud	safe	
http://https://ykm.de/api.html	0%	Avira URL Cloud	safe	
http://https://ykm.de/index.html?agreeTerms=1&submitted=1&longUrl=	0%	Avira URL Cloud	safe	
http://https://ykm.de/themes/ykm/styles/css/bootstrap-responsive.css	0%	Avira URL Cloud	safe	
http://https://ykm.de/contact.html	0%	Avira URL Cloud	safe	
http://https://ykm.de/tools.html	0%	Avira URL Cloud	safe	
http://https://ykm.de/rror.html?e=This	0%	Avira URL Cloud	safe	
http://ykm.de/a	0%	Avira URL Cloud	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://https://ykm.de/themes/ykm/js/theme/custom.js	0%	Avira URL Cloud	safe	
http://https://ykm.de/index.html?_t=Deutsch	0%	Avira URL Cloud	safe	
http://https://ykm.de/faq.htmlhtml	0%	Avira URL Cloud	safe	
http://https://ykm.de/api.html#createBasic	0%	Avira URL Cloud	safe	
http://https://ykm.de/themes/ykm/js/theme/testimonialrotator.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://https://ykm.de/themes/ykm/styles/css/docs.css	0%	Avira URL Cloud	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://ykm.de/member_login.htmlhort	0%	Avira URL Cloud	safe	
http://www.alexanderdickson.com/	0%	Avira URL Cloud	safe	
http://https://ykm.de/themes/ykm/images/star_icon.png	0%	Avira URL Cloud	safe	
http://maps.google.co.uk/maps?oe=utf-8&client=firefox-a&rlz=1R1GGLL_en-GB___GB423&um=1&ie=UTF-8&q=go	0%	Avira URL Cloud	safe	
http://www.adobe.coH	0%	Avira URL Cloud	safe	
http://https://ykm.de/api.html#createOptions	0%	Avira URL Cloud	safe	
http://https://ykm.de/themes/ykm/styles/css/builder.css	0%	Avira URL Cloud	safe	
http://https://ykm.de/register.htmlis	0%	Avira URL Cloud	safe	
http://https://ykm.de/api.html#disable	0%	Avira URL Cloud	safe	
http://https://wurlie.net	0%	Avira URL Cloud	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://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://cipa.jp/exif/1.0/ER_1	0%	Avira URL Cloud	safe	
http://https://ykm.de/themes/ykm/js/ZeroClipboard/ZeroClipboard.min.js	0%	Avira URL Cloud	safe	
http://https://ykm.de/themes/ykm/js/theme/jquery.waitforimages.js	0%	Avira URL Cloud	safe	
http://https://ykm.de/faq.htmlhtmlis	0%	Avira URL Cloud	safe	
http://https://ykm.de/themes/ykm/styles/screen.css	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	0%	Avira URL Cloud	safe	
http://https://wurlie.net/r_login.htmlhort	0%	Avira URL Cloud	safe	
http://https://ykm.de/register.htmlNRegister	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/xW	0%	Avira URL Cloud	safe	
http://https://ykm.de/themes/ykm/js/theme/jquery.easing.1.3.js	0%	Avira URL Cloud	safe	
http://https://ykm.de/themes/ykm/images/logo/_default.png	0%	Avira URL Cloud	safe	
http://https://ykm.de/api.html#list	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://https://ykm.de/themes/ykm/styles/css/layouts/orange.css	0%	Avira URL Cloud	safe	
http://https://ykm.de/themes/ykm/images/favicon.ico	0%	Avira URL Cloud	safe	
http://https://ykm.de/report_url.html	0%	Avira URL Cloud	safe	
http://https://ykm.de/forgot_password.html	0%	Avira URL Cloud	safe	
http://gsgd.co.uk/sandbox/jquery/easing/	0%	URL Reputation	safe	
http://gsgd.co.uk/sandbox/jquery/easing/	0%	URL Reputation	safe	
http://gsgd.co.uk/sandbox/jquery/easing/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/.	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/#	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://html5shim.googlecode.com/svn/trunk/html5.js	0%	Avira URL Cloud	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://https://ykm.de	0%	Avira URL Cloud	safe	
http://https://ykm.de/api.html#info	0%	Avira URL Cloud	safe	
http://https://ykm.de/index.html?_t=English	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pagead46.l.doubleclick.net	172.217.20.226	true	false		high
umblr.com	74.114.154.17	true	false		high
partnerad.l.doubleclick.net	172.217.23.34	true	false		high
ykm.de	104.28.25.219	true	false	• 4%, Virustotal, Browse	unknown
t.umblr.com	74.114.154.21	true	false		high
googlehosted.l.googleusercontent.com	172.217.23.1	true	false		high
href.li	192.0.78.27	true	false		high
googleads.g.doubleclick.net	unknown	unknown	false		high
www.googletagservices.com	unknown	unknown	false		high
themes.googleusercontent.com	unknown	unknown	false		high
adservice.google.co.uk	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://ykm.de/register.html	true		unknown
http://https://ykm.de/bookmarklet.html	true		unknown
http://https://ykm.de/faq.html	true		unknown
http://https://ykm.de/member_login.html	true		unknown

URLs from Memory and Binaries

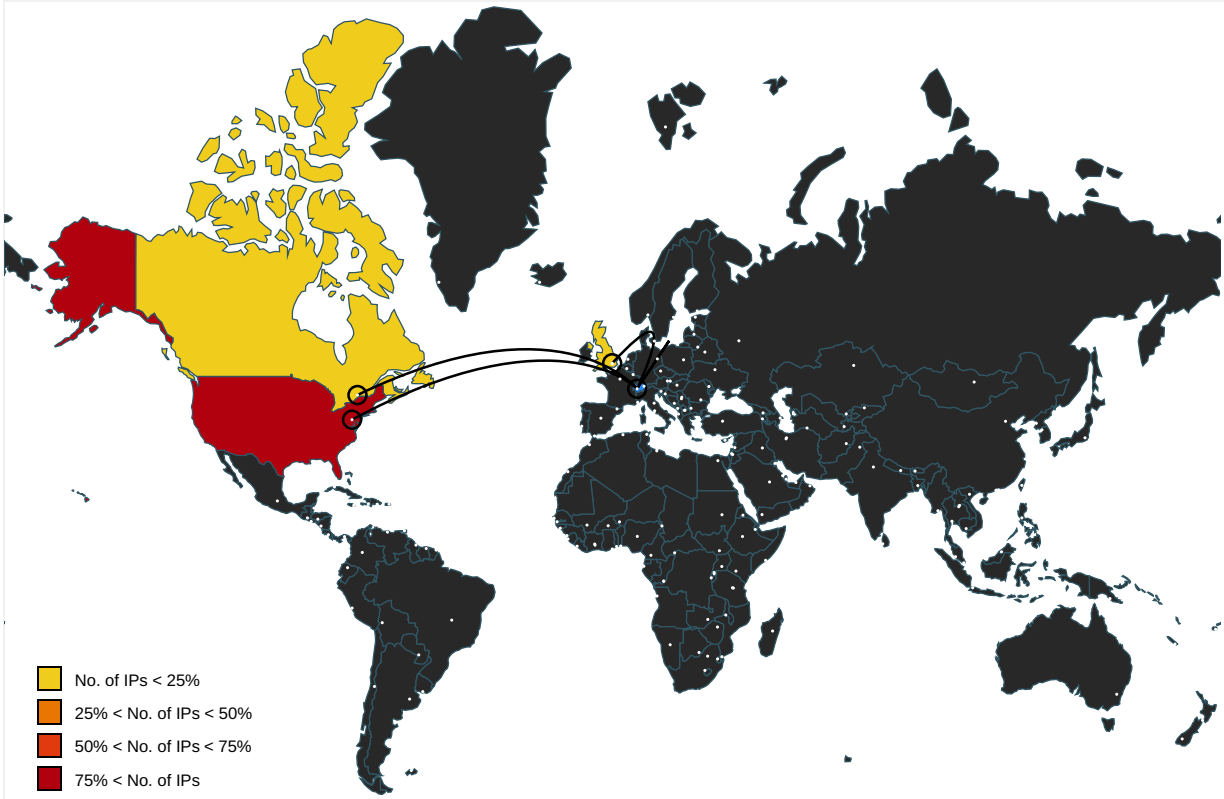
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ykm.de/api.html#activate	bookmarklet[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/extension/K	AcroRd32.exe, 00000001.00000002.393703092.000000000CE06000.00000004.00000001.sdmp	false		high
http://https://ykm.de/themes/ykm/styles/css/font-awesome.min.css	register[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://ykm.de/api.html	register[1].htm.24.dr, bookmarklet[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://ykm.de/index.html?agreeTerms=1&submitted=1&longUrl=	index[2].htm.24.dr, bookmarklet[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://ykm.de/themes/ykm/styles/css/bootstrap-responsive.css	register[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://daringfireball.net/2010/07/improved_regex_for_matching_urls	jquery.tweet[1].js.24.dr	false		high
http://https://ykm.de/contact.html	register[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://ykm.de/tools.html	register[1].htm.24.dr, bookmarklet[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://bugs.jquery.com/ticket/12282#comment:15	jquery.min[1].js.24.dr	false		high
http://dev.w3.org/csswg/cssom/#resolved-values	jquery.min[1].js.24.dr	false		high
http://www.opensource.org/licenses/mit-license.php	jquery.autosize-min[1].js.24.dr	false		high
http://https://ykm.de/rror.html?e=This	~DF006BB75F40C378F3.TMP.23.dr, {0E7866F9-547B-11EB-90E4-ECF4BB862DED}.dat.23.dr	false	• Avira URL Cloud: safe	unknown
http://ykm.de/a	faq[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ykm.de/recent_urls.html	~DF006BB75F40C378F3.TMP.23.dr, index[2].htm.24.dr, {0E7866F9-547B-11EB-90E4-ECF4BB862DED}.dat.23.dr, recent_urls[1].htm.24.dr	false		unknown
http://www.osmf.org/drm/default	AcroRd32.exe, 00000001.00000002.376215224.0000000007C90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.24.dr	false		high
http://https://cdn.ampproject.org/amp4ads-host-v0.js	f[1].txt0.24.dr	false		high
http://www.reddit.com/	msapplication.xml4.23.dr	false		high
http://https://ykm.de/themes/ykm/js/theme/custom.js	register[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://ykm.de/index.html?_t=Deutsch	~DF006BB75F40C378F3.TMP.23.dr, index[2].htm.24.dr, {0E7866F9-547B-11EB-90E4-ECF4BB862DED}.dat.23.dr	false	• Avira URL Cloud: safe	unknown
http://https://ykm.de/bookmarklet.html	~DF006BB75F40C378F3.TMP.23.dr, {0E7866F9-547B-11EB-90E4-ECF4BB862DED}.dat.23.dr, bookmarklet[1].htm.24.dr	false		unknown
http://bugs.jquery.com/ticket/12359	jquery.min[1].js.24.dr	false		high
http://https://ykm.de/faq.htmlhtml	~DF006BB75F40C378F3.TMP.23.dr	false	• Avira URL Cloud: safe	unknown
http://https://ykm.de/api.html#createBasic	bookmarklet[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://search.twitter.com/operators)	jquery.tweet[1].js.24.dr	false		high
http://https://t.umblr.com/redirect?z=https%3A%2F%2Fclick-email2.giize.com%2F_PeXKkjgCsfgwYIEhjR9526431&t=N	AcroRd32.exe, 00000001.00000002.380628525.0000000009560000.00000004.00000001.sdmp	false		high
http://https://ykm.de/themes/ykm/js/theme/testimonialrotator.js	register[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://bugzilla.mozilla.org/show_bug.cgi?id=649285	jquery.min[1].js.24.dr	false		high
http://html.orange-idea.com/veles/images/read_more.png	docs[1].css.24.dr	false		high
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	AcroRd32.exe, 00000001.00000002.393703092.000000000CE06000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ykm.de/themes/ykm/styles/css/docs.css	register[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://cipa.jp/exif/1.0/(15)	AcroRd32.exe, 00000001.00000002.394253994.000000000CF38000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ykm.de/member_login.htmlhort	{0E7866F9-547B-11EB-90E4-ECF4BB862DED}.dat.23.dr	false	• Avira URL Cloud: safe	unknown
http://www.alexanderdickson.com/	jquery.waitforimages[1].js.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://ykm.de/themes/ykm/images/star_icon.png	index[2].htm.24.dr, IUE4OCQZ.htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://t.umblr.com	AcroRd32.exe, 00000001.00000002.394314194.000000000CF4A000.00000004.00000001.sdmp	false		high
http://maps.google.co.uk/maps?oe=utf-8&client=firefox-a&rlz=1R1GGLL_en-GB___GB423&um=1&ie=UTF-8&q=go	faq[1].htm.24.dr, index[2].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/schema#c	AcroRd32.exe, 00000001.00000002.393703092.000000000CE06000.00000004.00000001.sdmp	false		high
http://www.adobe.coH	AcroRd32.exe, 00000001.00000003.373081997.000000000D2C6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://googleads.g.doubleclick.net	f[1].txt0.24.dr	false		high
http://https://ykm.de/api.html#createOptions	bookmarklet[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 00000001.00000002.380377428.0000000009470000.00000004.00000001.sdmp	false		high
http://https://bugzilla.mozilla.org/show_bug.cgi?id=491668	jquery.min[1].js.24.dr	false		high
http://https://ykm.de/themes/ykm/styles/css/builder.css	register[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://ykm.de/register.htmlis	{0E7866F9-547B-11EB-90E4-ECF4BB862DED}.dat.23.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.mfscripts.com/htmlhort	{0E7866F9-547B-11EB-90E4-ECF4BB862DED}.dat.23.dr	false		high
http://https://ykm.de/api.html#disable	bookmarklet[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/schema#	AcroRd32.exe, 00000001.00000002.393703092.000000000CE06000.00000004.00000001.sdmp	false		high
http://https://wurlie.net/	~DF006BB75F40C378F3.TMP.23.dr, {0E7866F9-547B-11EB-90E4-ECF4BB862DED}.dat.23.dr	false		unknown
http://https://wurlie.net	register[1].htm.24.dr, index[2].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.mfscripts.com/	~DF006BB75F40C378F3.TMP.23.dr	false		high
http://www.amazon.com/	msapplication.xml.23.dr	false		high
http://https://ykm.de/register.html	~DF006BB75F40C378F3.TMP.23.dr, faq[1].htm.24.dr	false		unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://cipa.jp/exif/1.0/	AcroRd32.exe, 00000001.00000002.394253994.000000000CF38000.00000004.00000001.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, 00000001.00000002.376215224.0000000007C90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cipa.jp/exif/1.0/ER_1	AcroRd32.exe, 00000001.00000002.394253994.000000000CF38000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.twitter.com/	msapplication.xml5.23.dr	false		high
http://https://ykm.de/themes/ykm/js/ZeroClipboard/ZeroClipboard.min.js	register[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://jsperf.com/getall-vs-sizzle/2	jquery.min[1].js.24.dr	false		high
http://www.aiim.org/pdfa/ns/schema#z	AcroRd32.exe, 00000001.00000002.393703092.000000000CE06000.00000004.00000001.sdmp	false		high
http://https://ykm.de/themes/ykm/js/theme/jquery.waitforimages.js	register[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://ykm.de/faq.htmlhtmlis	{0E7866F9-547B-11EB-90E4-ECF4BB862DED}.dat.23.dr	false	• Avira URL Cloud: safe	unknown
http://https://ykm.de/themes/ykm/styles/screen.css	register[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	AcroRd32.exe, 00000001.00000002.393703092.000000000CE06000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://wurlie.net/r_login.htmlhort	{0E7866F9-547B-11EB-90E4-ECF4BB862DED}.dat.23.dr	false	• Avira URL Cloud: safe	unknown
http://https://ykm.de/register.htmlNRegister	~DF006BB75F40C378F3.TMP.23.dr	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/property#B	AcroRd32.exe, 00000001.00000002.393703092.000000000CE06000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/extension/	AcroRd32.exe, 00000001.00000002.393703092.000000000CE06000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/xW	AcroRd32.exe, 00000001.00000002.392044752.000000000B3C1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://ykm.de/themes/ykm/js/theme/jquery.easing.1.3.js	register[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://ykm.de/themes/ykm/images/logo/_default.png	register[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://ykm.de/api.html#list	bookmarklet[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://www.nytimes.com/	msapplication.xml3.23.dr	false		high
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	AcroRd32.exe, 00000001.00000002.393703092.000000000CE06000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ykm.de/themes/ykm/styles/css/layouts/orange.css	register[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://ykm.de/themes/ykm/images/favicon.ico	register[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfe/ns/id/	AcroRd32.exe, 00000001.00000002.394253994.000000000CF38000.00000004.00000001.sdmp	false		high
http://https://cdn.ampproject.org/rtv/%	f[1].txt0.24.dr	false		high
http://https://googleads.g.doubleclick.net	f[1].txt0.24.dr	false		high
http://https://ykm.de/report_url.html	register[1].htm.24.dr, index[2].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://www.newmediacampaigns.com/page/jquery-flickr-plugin	jflickrfeed.min[1].js.24.dr	false		high
http://https://ykm.de/forgot_password.html	member_login[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://href.li/?https://ykm.de/65f0a4768a364c1717&t=MDZmNTEyZmUxYzY5ZjJkNjc3MDI5MTI0MjhiODVlNzBhYTA	~DF006BB75F40C378F3.TMP.23.dr, {0E7866F9-547B-11EB-90E4-ECF4BB862DED}.dat.23.dr	false		high
http://fontawesome.io/license	font-awesome.min[1].css.24.dr	false		high
http://gsgd.co.uk/sandbox/jquery/easing/	jquery.easing.1.3[1].js.24.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/.	AcroRd32.exe, 00000001.00000002.393703092.000000000CE06000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://themeforest.net/user/OrangeIdea/portfolio	docs[1].css.24.dr	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/#	AcroRd32.exe, 00000001.00000002.393703092.000000000CE06000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://html5shim.googlecode.com/svn/trunk/html5.js	register[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	AcroRd32.exe, 00000001.00000002.376215224.0000000007C90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.wikipedia.com/	msapplication.xml6.23.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ykm.de	register[1].htm.24.dr, faq[1].htm.24.dr, index[2].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://ykm.de/api.html#info	bookmarklet[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://ykm.de/index.html?_t=English	~DF006BB75F40C378F3.TMP.23.dr, index[2].htm.24.dr, {0E7866F9-547B-11EB-90E4-ECF4BB862DED}.dat.23.dr	false	• Avira URL Cloud: safe	unknown
http://www.live.com/	msapplication.xml2.23.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.28.25.219	unknown	United States		13335	CLOUDFLARENETUS	false
172.217.22.194	unknown	United States		15169	GOOGLEUS	false
192.0.78.27	unknown	United States		2635	AUTOMATTICUS	false
74.114.154.21	unknown	Canada		2635	AUTOMATTICUS	false
172.217.23.2	unknown	United States		15169	GOOGLEUS	false
172.217.23.1	unknown	United States		15169	GOOGLEUS	false
172.217.23.66	unknown	United States		15169	GOOGLEUS	false
172.217.23.34	unknown	United States		15169	GOOGLEUS	false
80.0.0.0	unknown	United Kingdom		5089	NTLGB	false
172.217.20.226	unknown	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	338148
Start date:	11.01.2021
Start time:	18:06:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Information-Account-Prime-Disable-Service.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:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	SUS
Classification:	sus22.winPDF@19/166@10/11
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 • Browsing link: https://ykm.de/ • Browsing link: https://ykm.de/index.html • Browsing link: https://ykm.de/register.html • Browsing link: https://ykm.de/faq.html • Browsing link: https://ykm.de/tools.html • Browsing link: https://ykm.de/recent_urls.html • Browsing link: https://ykm.de/member_login.html • Browsing link: https://wurlie.net/ • Browsing link: https://www.mfscripts.com/ • Browsing link: https://ykm.de/index.html?_t=English+%28en%29 • Browsing link: https://ykm.de/index.html?_t=Deutsch+%28de%29

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, RuntimeBroker.exe, backgroundTaskHost.exe, UsoClient.exe, audiodg.exe, BackgroundTransferHost.exe, HxTsr.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.64.90.137, 40.88.32.150, 92.122.146.26, 2.20.142.203, 2.20.143.130, 51.104.139.180, 104.79.90.110, 92.122.213.194, 92.122.213.247, 67.27.159.126, 8.248.139.254, 8.253.204.121, 8.248.135.254, 67.26.73.254, 51.103.5.186, 20.54.26.129, 88.221.62.148, 172.217.23.40, 172.217.23.46, 216.58.207.129, 152.199.19.161, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, e4578.dscb.akamaiedge.net, partner.googleadservices.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, adservice.google.com, acroipm2.adobe.com, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, par02p.wns.notify.windows.com.akadns.net, go.microsoft.com, emea1.notify.windows.com.akadns.net, www.googletagmanager.com, a122.dscd.akamai.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.google-analytics.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, www-google-analytics.l.google.com, acroipm2.adobe.com.edgesuite.net, ie9comview.vo.msecnd.net, www-googletagmanager.l.google.com, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, pagead2.googlesyndication.com, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, armmf.adobe.com, tpc.googlesyndication.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtCreateFile calls found. • 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
18:07:28	API Interceptor	13x Sleep call for process: RdrCEF.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
74.114.154.21	http://g1security.co.tz	Get hash	malicious	Browse	
	http://https://parg.co/bdZz	Get hash	malicious	Browse	
	APPLE Invoice.docx	Get hash	malicious	Browse	
	Receipt-LifeTime.docx	Get hash	malicious	Browse	
	http://https://t.umblr.com/redirect?z=https%3A%2F%2Fmusic-city-shop.com%2F%2F%2F%2Foverride%2Fclasses%2Fstock%2Fsan%2F%2F%2F%2F%2F%2F%2F%2F%2F%2F%2F%2F%2F%2F%2F%2F%2F%2F%2F%2F%2F%2F%2F%2F%2F%2F%2F%2Fvia.php&t=NGQ3MjEzY2E1YTAyZGMxMDVkMmUzZWMzNmQwNWY2YTliNmJhNmNhMyx1Rno5SkZyYg%3D%3D&b=t%3AhKGM0jeSxf1q_W_X9lISHg&p=https%3A%2F%2Fjosephatheo.tumblr.com%2Fpost%2F190844014194%2Fhttpsmusic-city-shopcomoverrideclassessto&m=1	Get hash	malicious	Browse	
172.217.23.2	e-card.jpg .exe	Get hash	malicious	Browse	
	http://https://luacclibrary-my.sharepoint.com/:b:/g/personal/polson_luacc_com/EfAoFE3NqkFOtaxmNOJG-7cBczwxxIkQeEoohauxLQI30g?e=RpwCpr	Get hash	malicious	Browse	
	http://https://recovermy3-account.com/	Get hash	malicious	Browse	
	http://https://recovermy3-account.com/	Get hash	malicious	Browse	
	http://103.40.8.188/ap/signin?key=a@b.c	Get hash	malicious	Browse	
	http://https://nishimurakoumuten.com/assets/images/wood/outlookexpress/index.php%3Femail=	Get hash	malicious	Browse	
	http://https://web.eventwoaccess.com/goglobal/goglobal/register?_ga=2.243374789.1555520295.1604500994-391290916.1603882332	Get hash	malicious	Browse	
	http://https://online.flippingbook.com/view/96105/	Get hash	malicious	Browse	
	MicrosoftEmail_Reactivation.html	Get hash	malicious	Browse	
	http://pages.clarizen.com/dc/WRXScLcEN1dR4zDWjpu2BD-3pt2XB3qp-KL2mI6LZblQM73ILB5KRoOqFh6ia76X8jiCjQMqbHUZD8L1oOtOBN-vidy9gluYXpASVTJdCJvbv96N51bho8TJNt7usuzrbaJdT1t3zkAoWDj9BSWVMRLwHOG6X1GflqGf-28MD5Ao0SuF67rlnl4XrEkl6nfOwISnDXI86dg16RUtbnIqIrCRYgqLfOUIyl8BVAmPtagKUgC416wwB-hScG15PSuL6nwULWA-pOqMMwhGOKwA541dR6pQd6E7O879rt-hrUonz5Meop9AKoUOBOyCgYDoEi5efSrQD6V2yRvKU2jgXH6SA9n_y73Iob-zgjqlZee6ZhARRWHeAkHSf6b0XPqJlpJefnOiA8zP5VfcG4Yqv75Cn30Al7AVRBByak96JmCjgg473RrceLfBDsIV-HM0tkIprVEjnTA_45hEyRXnR0IhVe2Ixc0NVjqoAO2zmDSNgnsRpzlpQOY1Hpg2aIKk71PnHgeeQeqhvjeq1BSvGw==/c0n03POB033T2MqZt0CgL00	Get hash	malicious	Browse	
	http://https://app.box.com/s/kt9kxlxan0dxlfcjanytk37vf78687xc	Get hash	malicious	Browse	
	http://sfpartnersllc.bubbleapps.io/version-test/index?debug_mode=true	Get hash	malicious	Browse	
	http://https://securemail.usablecs.com/enduser/msg.html?x=d-ac8b3d51e0180abf7a45357f2b6c3b76d7642d23ff7dda12b28b53cbb804d6eb2474e7fe993d4d60804022fb4c14d8b5a9aa43c9561242d49b5d07d57cf93ce6	Get hash	malicious	Browse	
	http://aanqylta.com	Get hash	malicious	Browse	
	http://dechielfirearms.com/mlired/	Get hash	malicious	Browse	
	http://https://online.pubhtml5.com/rkho/ldvq/	Get hash	malicious	Browse	
	http://https://online.pubhtml5.com/xdrd/migk	Get hash	malicious	Browse	
	http://https://www.yumpu.com/en/document/read/64446890/fax-document	Get hash	malicious	Browse	
	http://https://online.pubhtml5.com/ugab/jobu/	Get hash	malicious	Browse	
	http://dbms.pamllaw.com/667697573657070652e6d6172746940626d732e636f6d	Get hash	malicious	Browse	
104.28.25.219	ReceiptDOC#KXJAISF2154915.docx	Get hash	malicious	Browse	
172.217.22.194	http://149.129.50.37/	Get hash	malicious	Browse	
	http://https://panoramacharter.xyz	Get hash	malicious	Browse	
	http://tantric-goddess.org	Get hash	malicious	Browse	
	http://slimware.com	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	obliczanie-pierwiastka-dowolnego-stopnia-w-excelu[1].htm	Get hash	malicious	Browse	
	http://https://cutt.ly/lgD28dp	Get hash	malicious	Browse	
	http://tftpd32.jounin.net	Get hash	malicious	Browse	
	7CFPFFfS4g	Get hash	malicious	Browse	
	http://https://stqtvqfuafwykkyhsgsppgpgmvncrulddrdu-dot-solar-vertex-285913.rj.r.appspot.com/#mlarson@jhhc.com	Get hash	malicious	Browse	
	HappyMod-Download-2-6-0.apk	Get hash	malicious	Browse	
	http://https://www.yumpu.com/en/document/read/64446890/fax-document	Get hash	malicious	Browse	
	http://https://googleads.g.doubleclick.net/pcs/click?xai=AKAOjssIdZGtK2LGw4coQMwtQcONuf8cVZUVHUrlFgT33_wiLCuxpoweUvHdBH9neY4iW-CZh2SzgITptx6j64F0B2pEU0uoeRfmKTeyn7LSG5Irubqjv6IFl9MeqTp84ZT99WRJlZDMgrwUaUI7QjgNwL22AVveJm980wuVNryiILT2WhxCPmcY8M7PVIOygAXT_382p7PUn7bIByn2OjlTfCiaqta3tAhZWCuROeXZPznm5cGhgUYspVywPb8Y8GbuT5pyEUyF89icmqe5zg&sig=Cg0ArKJSzFtr0kI2Y6LI&adurl=https%3A%2F%2Fmediterraneanfencing.com%2Foffice%2Flive%3Femail%3DY3JhaWcuaGF5ZGVuQGluc3Blcml0eS5jb20%3D&nx=CLICK_X&ny=CLICK_Y	Get hash	malicious	Browse	
	Acunetix Premium v13.0.200930102 Activation Tool.exe	Get hash	malicious	Browse	
	http://dbms.pamllaw.com/667697573657070652e6d6172746940626d732e636f6d	Get hash	malicious	Browse	
	http://cutt.ly/	Get hash	malicious	Browse	
	http://https://www.canva.com/design/DAEJRw-Cekg/yqHz7lRXkcf0H9s6UXEU-Q/view?utm_content=DAEJRw-Cekg&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	
	http://https://www.canva.com/design/DAEJRw-Cekg/yqHz7lRXkcf0H9s6UXEU-Q/view?utm_content=DAEJRw-Cekg&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	
	http://https://microsjrl6f22qp9ra0hepfa60rlke.oa.r.appspot.com/?c=mmm014am00am0m04am04am1m015am015ammmm00am1m0m08am014am1m013am016am2m01am1.m01am3m09a	Get hash	malicious	Browse	
	http://https://czohsdpvklpderkoidxjbenlqmeiqupjgfjg-dot-glenxpecial3009493.ey.r.appspot.com/#fsifuentes@greendotcorp.com	Get hash	malicious	Browse	
	http://mediaonetv.in	Get hash	malicious	Browse	
192.0.78.27	http://ssqi.com	Get hash	malicious	Browse	• stats.wordpress.com/e-202009.js

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
pagead46.l.doubleclick.net	e-card.htm .exe	Get hash	malicious	Browse	• 172.217.23.66
	e-card.jpg .exe	Get hash	malicious	Browse	• 172.217.23.2
	http://https://1drv.ms:443/o/s!BAXL7VqGJe6lg0eKk2MZcT_c29ga?e=Qdftz9F3oESsQIuV76Ppsw&at=9	Get hash	malicious	Browse	• 142.250.180.66
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 216.58.198.2
	http://https://wfuwdbjwquoiynfb-dot-tundasma.el.r.appspot.com/#test@test.com	Get hash	malicious	Browse	• 172.217.16.162
	http://https://www.ensonoelevate2021.com/event/8e8c2672-3b18-40b1-8efc-026ab72e6424/summary?environment=P2&5S%2CM3%2C8e8c2672-3b18-40b1-8efc-026ab72e6424=	Get hash	malicious	Browse	• 142.250.180.98
	http://https://bit.ly/3aA3uVV	Get hash	malicious	Browse	• 142.250.180.66
	http://ovd.ru/forum/register.php?a=act&u=84666&i=25545989	Get hash	malicious	Browse	• 142.250.180.162
	http://https://pdfsharedmessage.xtensio.com/7wtcdlta	Get hash	malicious	Browse	• 216.58.198.34
	http://free.atozmanuals.com	Get hash	malicious	Browse	• 172.217.168.34
	http://https://alijafari6.wixsite.com/owa-projection-aspx	Get hash	malicious	Browse	• 172.217.168.34
	http://https://j.mp/2MBbcFI	Get hash	malicious	Browse	• 216.58.215.226
	details.html	Get hash	malicious	Browse	• 172.217.168.34
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 172.217.168.34

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://www.canva.com/design/DAESYWKuLHs/avvDNRvDuj_tk82H9Q45ZQ/view?utm_content=DAESYWKuLHs&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 172.217.168.2
	details.html	Get hash	malicious	Browse	• 172.217.16.162
	http://https://notification1.bubbleapps.io/version-test?debug_mode=true	Get hash	malicious	Browse	• 172.217.168.66
	http://quickneasyrecipes.co	Get hash	malicious	Browse	• 172.217.168.66
	http://https://xmailexpact.wixsite.com/mysite	Get hash	malicious	Browse	• 172.217.168.66
	http://https://veringer.com/wp-includes/wwii11/GXQb6HLGz4AV965RfN9795cyETWfmdzBUarzFg4YkqaJnfdTD/	Get hash	malicious	Browse	• 172.217.168.34
umblr.com	PRODUCT INQUIRY BNQ1.xlsx	Get hash	malicious	Browse	• 74.114.154.18
	http://WWW.ALYSSA-J-MILANO.COM	Get hash	malicious	Browse	• 74.114.154.18
	http://https://www.women.com/alexa/quiz-dialect-test	Get hash	malicious	Browse	• 192.0.77.40
	Amazon-Service-Center[2368].docx	Get hash	malicious	Browse	• 74.114.154.17
	Amazon-Service-Center[2368].docx	Get hash	malicious	Browse	• 74.114.154.17
	http://https://parg.co/bdZz	Get hash	malicious	Browse	• 74.114.154.21
	APPLE Invoice.docx	Get hash	malicious	Browse	• 74.114.154.17
	APPLE Invoice.docx	Get hash	malicious	Browse	• 74.114.154.21
	Tax Invoice-Castle-Clash-War-Empire.docx	Get hash	malicious	Browse	• 74.114.154.17
	Tax Invoice-Castle-Clash-War-Empire.docx	Get hash	malicious	Browse	• 74.114.154.17
	Receipt-LifeTime.docx	Get hash	malicious	Browse	• 74.114.154.21
	Receipt-LifeTime.docx	Get hash	malicious	Browse	• 74.114.154.17
	iNYNU6VuC7.exe	Get hash	malicious	Browse	• 66.6.32.21
partnerad.l.doubleclick.net	http://https://1drv.ms:443/o/s!BAXL7VqGJe6lg0eKk2MZcT_c29ga?e=Qdftz9F3oESsQIuV76Ppsw&at=9	Get hash	malicious	Browse	• 142.250.180.98
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 142.250.180.98
	http://ovd.ru/forum/register.php?a=act&u=84666&i=25545989	Get hash	malicious	Browse	• 216.58.206.66
	http://https://notification1.bubbleapps.io/version-test?debug_mode=true	Get hash	malicious	Browse	• 216.58.215.226
	http://https://veringer.com/wp-includes/wwii11/GXQb6HLGz4AV965RfN9795cyETWfmdzBUarzFg4YkqaJnfdTD/	Get hash	malicious	Browse	• 216.58.215.226
	http://encryptdrive.booogle.net	Get hash	malicious	Browse	• 216.58.215.226
	http://getfreshnews.com/nuoazaojrnvenpyxyse	Get hash	malicious	Browse	• 172.217.18.98
	http://s3-eu-west-1.amazonaws.com/hjdpjni/ogbim#qs=r-acacaeeikdgeadkieeefjaehbihababababaefahcaccajbiackdcagfkbkacb	Get hash	malicious	Browse	• 172.217.18.98
	http://https://fdkl5.csb.app/	Get hash	malicious	Browse	• 172.217.18.98
	http://https://shocking-foregoing-driver.glitch.me	Get hash	malicious	Browse	• 172.217.18.98
	http://https://www.chronopost.fr/fclV2/authentification.html?numLt=XP091625009FR&profil=DEST&cc=47591&type=MASMail&lang=fr_FR	Get hash	malicious	Browse	• 172.217.18.98
	http://ferreirainvestig.com.br/Activacion/cuenta-cdqd/	Get hash	malicious	Browse	• 172.217.18.98
	http://https://survey.alchemer.com/s3/6089047/Contract-Addendum	Get hash	malicious	Browse	• 172.217.18.98
	http://https://holidaysintorrox.com	Get hash	malicious	Browse	• 172.217.18.98
	http://perpetual.veteran.az/673616c6c792e64756e6e6540706572706575475616c2e636f6d2e6175	Get hash	malicious	Browse	• 172.217.18.98
	http://www.cqdx.ru	Get hash	malicious	Browse	• 216.58.215.226
	http://view.e.business.officedepot.com/?qs=3fe5dee3fd6dc334e57f4fe8c13caa1dc833d1845b46e0df5e76d8dcd189c65840b833e5f8853ee5eca50625943bfd8b71f0d693bc12eda6d7c035c0df2243dc5fe3f7c370b5320b8fd654c8b827b865	Get hash	malicious	Browse	• 216.58.215.226
	http://https://designsbytony.co/signin/	Get hash	malicious	Browse	• 216.58.215.226
	http://https://designsbytony.co/signin/	Get hash	malicious	Browse	• 216.58.215.226
	http://https://www.fosshub.com/Calibre.html/calibre-5.6.0.msi	Get hash	malicious	Browse	• 172.217.21.194

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.18733.rtf	Get hash	malicious	Browse	• 162.159.133.233
	mal.exe	Get hash	malicious	Browse	• 172.67.193.152
	Client.vbs	Get hash	malicious	Browse	• 162.159.134.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PURCHASE ORDER-34002174.doc	Get hash	malicious	Browse	• 162.159.130.233
	IRS Notice Letter pdf document.exe	Get hash	malicious	Browse	• 172.67.209.95
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.5396.rtf	Get hash	malicious	Browse	• 162.159.130.233
	n#U00b0 761.doc	Get hash	malicious	Browse	• 162.159.133.233
	SecuriteInfo.com.Variant.Graftor.893032.186.exe	Get hash	malicious	Browse	• 104.31.70.209
	imagnpdf0440690129912239vistaprevia02052329503adobeplayer02304293.exe	Get hash	malicious	Browse	• 104.23.98.190
	SEA LION LOGISTICS-URGENT QUOTATION.exe	Get hash	malicious	Browse	• 23.227.38.74
	R1G9cMpG36BO2Sg.exe	Get hash	malicious	Browse	• 172.67.188.154
	099898892.exe	Get hash	malicious	Browse	• 23.227.38.74
	Invoice #756-77988-23989646.exe	Get hash	malicious	Browse	• 104.27.138.99
	e-card.htm .exe	Get hash	malicious	Browse	• 104.27.201.87
	e-card.jpg .exe	Get hash	malicious	Browse	• 104.27.201.87
	QyS0Q13lBd.exe	Get hash	malicious	Browse	• 104.31.71.209
	SEe64c0h6A.exe	Get hash	malicious	Browse	• 172.67.188.154
	b88rKzKJmJ.exe	Get hash	malicious	Browse	• 104.28.5.151
	36bjGck9ps.exe	Get hash	malicious	Browse	• 104.28.5.151
	_00AC0000.exe	Get hash	malicious	Browse	• 172.67.218.107
GOOGLEUS	mal.exe	Get hash	malicious	Browse	• 34.102.136.180
	Client.vbs	Get hash	malicious	Browse	• 34.102.136.180
	SecuriteInfo.com.Trojan.Inject4.6535.29715.exe	Get hash	malicious	Browse	• 34.102.136.180
	IRS Notice Letter pdf document.exe	Get hash	malicious	Browse	• 216.58.207.179
	s3CRQNulKZ.exe	Get hash	malicious	Browse	• 172.217.20.227
	PO 24000109490.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	n#U00b0 761.doc	Get hash	malicious	Browse	• 34.102.136.180
	ptrb-ES-2999223.msi	Get hash	malicious	Browse	• 172.217.23.1
	SEA LION LOGISTICS-URGENT QUOTATION.exe	Get hash	malicious	Browse	• 35.246.6.109
	099898892.exe	Get hash	malicious	Browse	• 34.102.136.180
	e-card.htm .exe	Get hash	malicious	Browse	• 172.217.23.35
	e-card.jpg .exe	Get hash	malicious	Browse	• 172.217.23.35
	QN08qH1zYv.exe	Get hash	malicious	Browse	• 34.102.136.180
	VHspB1u63F.exe	Get hash	malicious	Browse	• 216.239.38.21
	Scan_order.exe	Get hash	malicious	Browse	• 172.217.23.1
	correos-1.apk	Get hash	malicious	Browse	• 216.58.198.42
	correos-1.apk	Get hash	malicious	Browse	• 216.58.198.10
	parler.apk	Get hash	malicious	Browse	• 216.58.198.10
	parler.apk	Get hash	malicious	Browse	• 142.250.180.131
	Riskware.apk	Get hash	malicious	Browse	• 216.58.198.10
AUTOMATTICUS	20210111140930669.exe	Get hash	malicious	Browse	• 192.0.78.24
	099898892.exe	Get hash	malicious	Browse	• 192.0.78.24
	QN08qH1zYv.exe	Get hash	malicious	Browse	• 192.0.78.25
	RF-E68-STD-2020-106.xlsx	Get hash	malicious	Browse	• 192.0.78.24
	PO21010699XYJ.exe	Get hash	malicious	Browse	• 192.0.78.24
	http://mckeepropainting.com/.adv3738diukjuctdyakbd/dhava93vdia11876dkb/ag38vdua3848dk/sajvd9484auad/ajd847vauadja/101kah474sbbadad/wose/Paint20200921_2219.pdf.html	Get hash	malicious	Browse	• 192.0.77.48
	catalogo TAWI group.exe	Get hash	malicious	Browse	• 192.0.78.25
	http://herculematerilesede.tumblr.com/	Get hash	malicious	Browse	• 192.0.77.40
	http://free.atozmanuals.com	Get hash	malicious	Browse	• 192.0.73.2
	http://https://canningelectricinc.wordpress.com/	Get hash	malicious	Browse	• 192.0.79.33
	rib.exe	Get hash	malicious	Browse	• 192.0.78.12
	http://getfreshnews.com/nuoazaojrnvenpyxyse	Get hash	malicious	Browse	• 192.0.73.2
	Rfq_Catalog.exe	Get hash	malicious	Browse	• 192.0.78.24
	P.O-45.exe	Get hash	malicious	Browse	• 192.0.78.25
	Rfq_Catalog.exe	Get hash	malicious	Browse	• 192.0.78.25
	http://https://create.piktochart.com/output/51658503-cfo-capabel	Get hash	malicious	Browse	• 192.0.73.2
	Quote.exe	Get hash	malicious	Browse	• 192.0.78.25
	http://https://sharepointsfile.eu-gb.cf.appdomain.cloud/redirect/?param=YW50d2VycGVuLmNlbnRydW1AY20uYmU=	Get hash	malicious	Browse	• 192.0.73.2

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://s3-eu-west-1.amazonaws.com/hjdpjni/ogbim#qs=r-acacaeeikdgeadkieeefjaehbihabababaefahcaccajbiackdcagfkbkacb	Get hash	malicious	Browse	• 192.0.73.2
	http://https://aftersync.com/blog/rightqlik-quick-access-to-common-operations-on-qlikview-files	Get hash	malicious	Browse	• 192.0.77.48

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	sfk_setup.exe	Get hash	malicious	Browse	• 74.114.154.21 • 172.217.23.2 • 172.217.23.1 • 104.28.25.219 • 172.217.23.66 • 172.217.23.34 • 172.217.22.194 • 192.0.78.27 • 172.217.20.226
	P166824.htm	Get hash	malicious	Browse	• 74.114.154.21 • 172.217.23.2 • 172.217.23.1 • 104.28.25.219 • 172.217.23.66 • 172.217.23.34 • 172.217.22.194 • 192.0.78.27 • 172.217.20.226
	e-card.htm .exe	Get hash	malicious	Browse	• 74.114.154.21 • 172.217.23.2 • 172.217.23.1 • 104.28.25.219 • 172.217.23.66 • 172.217.23.34 • 172.217.22.194 • 192.0.78.27 • 172.217.20.226
	e-card.jpg .exe	Get hash	malicious	Browse	• 74.114.154.21 • 172.217.23.2 • 172.217.23.1 • 104.28.25.219 • 172.217.23.66 • 172.217.23.34 • 172.217.22.194 • 192.0.78.27 • 172.217.20.226
	Payment.exe	Get hash	malicious	Browse	• 74.114.154.21 • 172.217.23.2 • 172.217.23.1 • 104.28.25.219 • 172.217.23.66 • 172.217.23.34 • 172.217.22.194 • 192.0.78.27 • 172.217.20.226
	Test.HTM	Get hash	malicious	Browse	• 74.114.154.21 • 172.217.23.2 • 172.217.23.1 • 104.28.25.219 • 172.217.23.66 • 172.217.23.34 • 172.217.22.194 • 192.0.78.27 • 172.217.20.226
	mailsearcher32.dll	Get hash	malicious	Browse	• 74.114.154.21 • 172.217.23.2 • 172.217.23.1 • 104.28.25.219 • 172.217.23.66 • 172.217.23.34 • 172.217.22.194 • 192.0.78.27 • 172.217.20.226
	mailsearcher64.dll	Get hash	malicious	Browse	• 74.114.154.21 • 172.217.23.2 • 172.217.23.1 • 104.28.25.219 • 172.217.23.66 • 172.217.23.34 • 172.217.22.194 • 192.0.78.27 • 172.217.20.226

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Curriculo Laura.xlsm	Get hash	malicious	Browse	• 74.114.154.21 • 172.217.23.2 • 172.217.23.1 • 104.28.25.219 • 172.217.23.66 • 172.217.23.34 • 172.217.22.194 • 192.0.78.27 • 172.217.20.226
	prints carlos bolsonaro.docm	Get hash	malicious	Browse	• 74.114.154.21 • 172.217.23.2 • 172.217.23.1 • 104.28.25.219 • 172.217.23.66 • 172.217.23.34 • 172.217.22.194 • 192.0.78.27 • 172.217.20.226
	http://https://friskyferals.info/cgjx	Get hash	malicious	Browse	• 74.114.154.21 • 172.217.23.2 • 172.217.23.1 • 104.28.25.219 • 172.217.23.66 • 172.217.23.34 • 172.217.22.194 • 192.0.78.27 • 172.217.20.226
	http://https://marseral.am/wp-includes/aw?i=i&0=leo.cai@mainfreightasia.com	Get hash	malicious	Browse	• 74.114.154.21 • 172.217.23.2 • 172.217.23.1 • 104.28.25.219 • 172.217.23.66 • 172.217.23.34 • 172.217.22.194 • 192.0.78.27 • 172.217.20.226
	http://https://bit.ly/35cYpiT	Get hash	malicious	Browse	• 74.114.154.21 • 172.217.23.2 • 172.217.23.1 • 104.28.25.219 • 172.217.23.66 • 172.217.23.34 • 172.217.22.194 • 192.0.78.27 • 172.217.20.226
	http://mckeepropainting.com/.adv3738diukjuctdyakbd/dhava93vdia11876dkb/ag38vdua3848dk/sajvd9484auad/ajd847vauadja/101kah474sbbadad/wose/Paint20200921_2219.pdf.html	Get hash	malicious	Browse	• 74.114.154.21 • 172.217.23.2 • 172.217.23.1 • 104.28.25.219 • 172.217.23.66 • 172.217.23.34 • 172.217.22.194 • 192.0.78.27 • 172.217.20.226
	http://https://new-fax-messages.mydopweb.com/	Get hash	malicious	Browse	• 74.114.154.21 • 172.217.23.2 • 172.217.23.1 • 104.28.25.219 • 172.217.23.66 • 172.217.23.34 • 172.217.22.194 • 192.0.78.27 • 172.217.20.226
	http://https://survey.alchemer.com/s3/6130663/Check-11-Payment	Get hash	malicious	Browse	• 74.114.154.21 • 172.217.23.2 • 172.217.23.1 • 104.28.25.219 • 172.217.23.66 • 172.217.23.34 • 172.217.22.194 • 192.0.78.27 • 172.217.20.226
	http://https://proudflex.org	Get hash	malicious	Browse	• 74.114.154.21 • 172.217.23.2 • 172.217.23.1 • 104.28.25.219 • 172.217.23.66 • 172.217.23.34 • 172.217.22.194 • 192.0.78.27 • 172.217.20.226

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://www.food4rhino.com/app/human	Get hash	malicious	Browse	• 74.114.154.21 • 172.217.23.2 • 172.217.23.1 • 104.28.25.219 • 172.217.23.66 • 172.217.23.34 • 172.217.22.194 • 192.0.78.27 • 172.217.20.226
	http://https://www.food4rhino.com/app/elefront	Get hash	malicious	Browse	• 74.114.154.21 • 172.217.23.2 • 172.217.23.1 • 104.28.25.219 • 172.217.23.66 • 172.217.23.34 • 172.217.22.194 • 192.0.78.27 • 172.217.20.226
	http://https://smlfinance.com/wp-content/uploads/2021/DHL2021/MARKET/	Get hash	malicious	Browse	• 74.114.154.21 • 172.217.23.2 • 172.217.23.1 • 104.28.25.219 • 172.217.23.66 • 172.217.23.34 • 172.217.22.194 • 192.0.78.27 • 172.217.20.226

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):	820
Entropy (8bit):	5.702678492090885
Encrypted:	false
SSDEEP:	12:vDRM98k6eZiEDDRM9MiVZiEADRM9vWVZiEkDRM9GxZiE:7tXE3FieE2YWeEiVqE
MD5:	B3E5B0C4E783901AE9D4CD907D7EA4F3
SHA1:	6DFB9CFC5BEA3BF1F2AB8B012803601E6FE3C196
SHA-256:	8AF87AAACB16F7EA0A95A6E8D27445D26739AD8481A605AACA3B2ECA661A0076
SHA-512:	997537C175ECB0933E8F6E4B386A7796709D8E0787A8862211D6481A2B26C9F80E93AB4686078D508A7F1EC90C0925CB3AB634BD54347048F1BFA222CE72300E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .....@./....."#.D.7p.A..A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo..... .@.?.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .=.?.@./....."#.Dw...A..A....d.{v.^.G...d.W.:...P..k%..A..Eo..... .A..Eo.....&.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .f[Z.@./....."#.D `v.A..A....d.{v.^.G...d.W.:...P..k%..A..Eo..... .....A..Eo.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .`.|.@./....."#.DIJ..A..A....d.{v.^.G...d.W.:...P..k%. .A..Eo.....A..Eo.....v,;.....

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):	696
Entropy (8bit):	5.651138238886709
Encrypted:	false
SSDEEP:	12:V9zr899PQnl9zI9PQYP9zfaS9PQ2d9zPZ9PQ:XzQ99PQnnzI9PQYFzSS9PQazPZ9PQ
MD5:	0FD5A50978A2EDECFDCBDEF0A04B0D53
SHA1:	07070AA69C16343C2CED3600E4E124EE369B2CC2
SHA-256:	8D0601114B8C5F0AFFAFEAB171A152DC0580EE83D22219A9E67B7E362A6ABD1E
SHA-512:	E297AAB9B278DCDA3FE2B78CCD19CE3E1A9CA0556D9E6AE8ADDD81784FCA4362C32DF564DE53976DB707282DE98F345598E2DB9255C6BA7094B78237335D02E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0	
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .....@./....."#.Db.%.A..A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....F.l.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ...+.@./....."#.D...A..A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....vY.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .2.G.@./....."#.D`['.A..A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ..ql.@./... .."#.D...A..A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....?..#.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	984
Entropy (8bit):	5.616926894389946
Encrypted:	false
SSDEEP:	24:tB4v4oRHSBXB4v4DxYSBCB4v4nG4SBTB4v4OSB:nMBtSBRMAySBSMcSBtMFSB
MD5:	D53EE18CBC236E3A5995638C3998972B
SHA1:	92BAD5F782232EEED1156FC1D0BE31AAA3B9A54A
SHA-256:	046F92FAC9FB343BE9502E71BAF9424F8780EC6A2A51EADA66E2B5B795A1261D
SHA-512:	8B52A142EAFB81CE725626299333D1506C9375A9792C4B8752756128392730B3968F03368319F6DC45D1AFAB1688F196D5ABA83ECF073D41E7851E01687EFE4E
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 .....@./....."#.D.+n.A..A..hv DO.N.t@.....n.*..... ....A..Eo.....A..Eo.....wdl.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ..*=.@./....."#.D...A..A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....W.&.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ..YZ.@./....."#.D..u.A..A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....b(.J.....0\r..m..... v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ...{.@./....."#.DJ...A..A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....Nc.....

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):	5.687561447312121
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RswMte+mk6iiWulHyA1TK6tu+NtVYOFLvEWdFCi5RsMtWiWt:lbRkiDMteU6nWusswwbRkiDJ9Wusss
MD5:	0553D89A70CE1F6435CD3D2C176E03B4
SHA1:	863EB0123A414AA6AB5B7BC31A6954F7F8711BFB
SHA-256:	56AF2AC1581172025A556CF111DE9C2C43956BC2B72B033FC42BF69072A14027
SHA-512:	D16D0BA64099DE482BFE96111145763A9289553F1E1522EE276F94A70C193E8291804DE3336B1151A8F0D2E285B7770EB245BDE6EAFF80C445E9F41E98D6E724
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 ....@./....."#.D...A..A..8 P..a...R..Y....7.@..2Dm{.. A..Eo.....A..Eo.....~.....0\r..m.....h....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js .s(_.@./....."#.D ...A..A..8 P..a...R..Y....7.@..2Dm{..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	420
Entropy (8bit):	5.608377047902467
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVu1RPVyh9PT41TK6t72+yiXYOFLvEWd7VIGXVutTAMVyhy:pyixRu1V41TEnyixRu/V41TE
MD5:	D09D2DAD435D62C0FBCEC2A31C76409D
SHA1:	EDE572E0C62C55FE2556E6310FC0E4FAD6DA1BAB
SHA-256:	857F99554AEC6DDAF99780310E173BFF4CB602FEBB6903E60AD64F1F37166841
SHA-512:	D95B97011AB7E1844E427B5647452D0DC052BF06C6272047CB8AF4B4C930B8107B082ED7032A56722A8F9E49AC4AF30F5F887D95EDFE306D558AC29A84EC951
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ..b?.@./....."#.DN&..A..Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo. .....'.....0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js .H.{.@./....."#.D....A..Ak.Q.....-_..y.....O...>..1....A..Eo..... .....A..Eo.....j.N?.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.65652213540904
Encrypted:	false
SSDEEP:	6:mvYOFLvEWdhwjQdyulECLZIl6P41TK6tqevYOFLvEWdhwjQxgZl/WJLZIl6P41Tn:0RhkQy5CLZC7RhkcgbuJLZC
MD5:	088589183E175B8AB7E64B395CD9EFD2
SHA1:	20D83F612A906C1BF2E1F4C7D6C934DAEF8BECB2
SHA-256:	BB6C243810BB55C87704885631481E83C4B7682B4E9F4DFD0BC18BF3F7517647
SHA-512:	459F1E1AAED0ED2BB74A91535406E0AF1B443533DE5CB4E5B899DB1A564A279FC4D94E23FA5F4911B06C576EEB91D396EB0BA79A7A4D3299855EDC217953C6 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ...9.@./....."#.D.H..A..A.].>....uUf..N...k.....c..l.A..Eo.....A ..Eo.....W.6o.....0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ...x.@./....."#.D.J..A..A.].>....uUf..N...k.....c..l.A.. Eo.....A..Eo.....H.....

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):	418
Entropy (8bit):	5.542143667721754
Encrypted:	false
SSDEEP:	6:mJYOFLvEWdGQRQOdQynWv06g1TK6tTtMJYOFLvEWdGQRQOdQV5nv06g1TK6tF:2RHRQCBW81wRHRQCU01
MD5:	FE0953743595685AD4A77457107369E7
SHA1:	231F2414EBAA22A83BB778CDB5140FA125B02CE3
SHA-256:	8D49E189BFBA58E2EEF66C92457CDC1ED3657E82C2619889ADE0C337257FC769
SHA-512:	D25DDA04F10C3E023ECDA2E9D91D32EFF5E2AE4093C5152882E0D0C551ED4704AA5DC9BE566C6D4487DEBF9CA5625F86E671BEA2C19CE96675F3A3FEBF242 E3E
Malicious:	false
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .J~?.@./....."#.DsH..A..A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo .....0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .z.|.@./....."#.DNa..A..A..c..y/L....|y.n..C/I.....X7-ne.A..Eo..... .....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	716
Entropy (8bit):	5.6090334555231625
Encrypted:	false
SSDEEP:	12:Z5MlVtZMuR/EC5MPz/NMuR/E+5MIUMuR/Ej5MShMuR/Ee:ZSlVteuR/ECS7yuR/E+SEuR/EjSFuR/E
MD5:	B92F35D7EE2D2491D066FD9C537F3007
SHA1:	3595853EF6EF085733716B6F34775F78BAAFAAC3
SHA-256:	FBE8121891F7CACC95F49B9BB616D106DD0EBF41EE02A705C37EA3D8D1086753
SHA-512:	C05BB1FCF6FA3A7BF265D7B0F1CB9CE295A370D5577AAA9A46EDB0A963581F907A55681E197FF65BE23852962E14CDDA6FF8AC97CD64633BEAB38C1EAD32F8 C1
Malicious:	false
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .z...@./....."#.Da5&.A..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....+..L.....0\r..m..... .3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ...+.@./....."#.D.4..A..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 ...G.@./....."#.D..'.A..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....J.....0\r..m.....3....<lb...._keyhttps ://rna-resource.acrobat.com/base_uris.js .&.l.@./....."#.Dd...A..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo....._b.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\39c14c1f4b086971_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.626248984885863
Encrypted:	false
SSDEEP:	6:mGpYOFLvEWdzAAukoTK5m0bbsIDMGH41TK6tAF:XfRM6oO8KsIZES
MD5:	E98725ACFF8FA4945F931A522438BD97
SHA1:	DC0495C5FE156B2A4995F3F429EAC12882690FCF
SHA-256:	2F4FAC6463BCEF513B103BD6DAF07A21B8BC076BE61E76EAE1CAA9883FDF9266

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\39c14c1f4b086971_0	
SHA-512:	A3F565ACCB4C5D8DF2DE8DBC97F8E70E8BCE0F861F59D6F6EF61EC3BAB5F8B65AD1E1A99494430E3C11B0F7B397EB2BFB1D88B42E0A7A7346B1AD05CA564C38A
Malicious:	false
Preview:	0\r..m.....T....,.^...._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/selector.js .YFJ.@./....."#.D..0.A..A..`.....^....L>..Xa./.....C.y.A..Eo.....A..Eo.....#..G.....

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):	428
Entropy (8bit):	5.550479329638553
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtuNLF0by0zBUKSAA1TK6tbe4fPYOFLvEWdtuYu35by0zBUKSAA13:pRfbeVxRfkbe
MD5:	E97B09BFA213868C826E58A2BC7D29B6
SHA1:	A1DD88C4CD6741A44421DDB82315B32B61304781
SHA-256:	B38BB006BB2860C60FA1AA3C1235B695B89ADE0099CF740752144A040F4CBA68
SHA-512:	9718238C00BF5BD9C75BBFC93A5D75C26C4105A2B62C9297E33CDC3B9140D16BD9F3D4B7867191B45E1945A38C56F1A68899068C42D0B5AC1FFBCEF820478A
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ..%@.@./....."#.D....A..AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....A..Eo.....c.B.....0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .?)}.@./....."#.Dp#..A..AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	708
Entropy (8bit):	5.600721338054688
Encrypted:	false
SSDEEP:	12:KkXxKMSCvUeu+4ytUllkXxKMSCvWO24tUlC4kXxKMSCvKmtUlJ4kXxKMSCvYMtUj:KkXxiCekWlkXxiCrWC4kXxiCymWmkXxc
MD5:	CAD3E1FB3E8609482C29ED4ADEA303DF
SHA1:	828FD267BEF522AF799E4BA205DD0C29C9A612A0
SHA-256:	A277E1FB7DFA4F55671FC37AE911FC976A1F5F96EC46C55EE67DC93E7EBD1B04
SHA-512:	668D9B28F104C5BFC1ECD7E6DEFF6DAB96E1C1DEB84D8231C7E664D95643B520CD4110C933DDE48DD0B363D3D4FDF9D325CEC30429730F3E4C94B48DB2E4A5
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .)...@./....."#.D..&.A..A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....n.....0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ..+.@./....."#.D....A..A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....&<.....0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ...G.@./....."#.Dn.'.A..A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....k.....0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .T.l.@./....."#.D....A..A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....{Nl.....

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):	748
Entropy (8bit):	5.6211519322545005
Encrypted:	false
SSDEEP:	12:5h6OL0L2Jnk+h6OLJk3h6OLg+Ukzh6OLOnk:5h6RLn+h6r3h6l+Bzh6fk
MD5:	091E2DCEB714876C00AC2DBD4DE87DFA
SHA1:	783A571B190F6B52200C9C59D2E4B214718E758E
SHA-256:	E35FDBF9005E221D9889AE6F7765DB95AA9E7B7956F7DD6201BFD39B4432804A
SHA-512:	0BC505B32DF88D4BA132E890ADECE55B23151F94D9EB522A30F1194CB04E3266309B3D6D7E3E33E84B7CE90336D0E9B7B9DEAB078937FC5B017AD5DCE1979E7D
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ..>..@./....."#.D.R\.A..A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....N.o1.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ...6.@./....."#.DI,..A..A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....Y.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .D.U.@./....."#.D.@`.A..A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....z.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ...v.@./....."#.D.D..A..A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....?.J.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0	
Size (bytes):	976
Entropy (8bit):	5.649984606670983
Encrypted:	false
SSDEEP:	24:UB4v4w3wzXLnxfB4v4OvwzXLn9cB4v4/FvwzXLnHB4v4dwzXLnr:8MdMbnfMzEbn2M8FEbnhMrbnr
MD5:	06C733BA2BD9D4DCF54F23F97E76851F
SHA1:	7B2781E3B0332032EDDABAA8941238BAE83DB562
SHA-256:	5EB9223F3E79BBFC27DD29F339F771ABC5828B5727ED707B205556D0ED8AB4AC
SHA-512:	98E84D4FAE777BB8EF80506DF6BA778DD70F1FC3D01A09E403FA755DE08DFA975DFF59DB772398AB8F34DFF760BAC8E8E0C8BBF8E841A1A5E9586F5ECB095F AE
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 ..'..@./....."#.DR.s.A..A.....H...{...2. ./.k`..r4.C. .A..Eo.....A..Eo.....NjoR.....0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js ..d?.@./....."#.D....A..A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....<.....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 .v^Z.@./....."#.D$.{.A..A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....@.4.....0\r..m.....t...R.1<...._ke yhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js ..%|.@./....."#.D....A..A.....H...{...2../.k`..r4.C. .A..Eo..... .....A..Eo.....(.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6267ed4d4a13f54b_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.546160280053087
Encrypted:	false
SSDEEP:	6:mq9YOFLvEWdzAHdQ2ouAkAK5GFCaa+41TK6tm:NRMHdt75Gda+Eg
MD5:	76B9964BDC4E4376390FDC647F2064C8
SHA1:	8A408A186CF98F1E58A0281C21517ADEE7B226C0
SHA-256:	7E392F013A6E8B1EDFBA76212D5ED2F96783BF5226934346FF20C0EEDAD5B8AA
SHA-512:	592B288D4A1AB9D5AC3DEAD1E1E3C1303ABC884EDA17D2FF55A52BE9F993951CFE890E335C59A6A0CC1D85195C2990A9A95423B6C5626AAA278656DAE7856F 2D
Malicious:	false
Preview:	0\r..m.....R....L....._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/plugin.js ..cJ.@./....."#.D..1.A..A...G.3D.....Q.g0...._.Q.....A..Eo.....A..E o.....2.w1.....

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):	422
Entropy (8bit):	5.527925631329872
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXu0bgZtcjc11TK6tm2s2VYOFLvEWdvBIEGdeXuD9D5113:BsR2Ese9b6D0RsR2EsemX
MD5:	D9B568D20C3C950C5D0B264FBAAD497E
SHA1:	1FFC8F3FA8C6E5A8DE08CC15D6F1DC6CA16260E5
SHA-256:	824A478A2E2461DAF7DDD9F5711730A59BCF5EB91AF1797F08A7348186E196E2
SHA-512:	6D1FFE1530F76D5BEC1D3FE060341F1D5D411B0F3352625D7C708FE81FBDD266A0EFDEA5D3B656009EBB865645E7302A0C10705FD3401626505B8FD0B569F5B
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .g.>.@./....."#.D....A..A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo .....6.....0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ..{.@./....."#.D+...A..A.A.o]@r..Q.....<w.....].n\....A..Eo..... .....A..Eo.....F#.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	404
Entropy (8bit):	5.669187766254238
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQSZtQ+kF+B7OhKlvA1TK6tVaVYOFLvEWdwAPCQ3uoqxV+B7OB:RbR169eIJkGbR16wGrIJkP
MD5:	49B3C43CC904ED507E1C7A3BDA4491CA
SHA1:	5E2F8BD9362B26CFE39CA28FC5C5D1DC28E406DC
SHA-256:	0A60FFCC515895765A0C605AD4DC33290F33980159AB870F7CCB784B62B9064D
SHA-512:	D54578643BA5A317BC08070EAF6503143806F3DBD3D1871AF4FB0534A5B93C2E432FBF67FC23E41861B3EC400137228198DEC80BFF507DAA903296DC0B577467
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0	
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js .:.9.@./....."#.D....A..A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....I .OQ.....0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ...x.@./....."#.D....A..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):	422
Entropy (8bit):	5.572214235255749
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVu2lTlV0QdFt1TK6tss2gEYOFLvEWdGQRQVu0ou4TxeQdFX:B2geRHRQb00R2geRHRQPS00
MD5:	AE2308E2F677D3E4943B317706E82EB4
SHA1:	6FA3FCA9DF15D4C5F4A0E367D6214CD19CCF809C
SHA-256:	D599F175FB490FDC23D39847722C8635C8580F02335488FC70DAED64E3A77293
SHA-512:	859D850A4D2D4B95C42FA0E9604903A59B377CA7DE63F487F9C0FE5B4D7F1E7CB251665509A91AE7953F45A5E8AF252FD0ADD63A0921BC8478E10020334FE03
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .oT=.@./....."#.Do...A..A@..{o]...9o|..qY....T....{..u.b..A..Eo..... .....A..Eo.....0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ...{.@./....."#.D.C..A..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):	824
Entropy (8bit):	5.667148665594576
Encrypted:	false
SSDEEP:	12:WyeRlTuYt1wHyeRlY8yt1whyeRlv72Rt1wpyeRl5yt1we:WJKYfwHJQBfwhJH72RfwpJEfw
MD5:	6AC420B618A4EB617F3FD00C8AA468EE
SHA1:	DE9540EA1D819C7ACA6A781FB2A5914801F942C0
SHA-256:	6A2C86571271594BCCC504E1F52C460F16C486BEFB597E197597457E4E263BFA
SHA-512:	80FA8EB30B879B65F65A82487336CDB14216411732C797F0AD50EE2B93BA924F0DD322481A08A31CC0D57221B1F1A19843079B2CE022E456779654D1EB17C923
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .....@./....."#.D`.d.A..A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.... ...;5.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .~.7.@./....."#.D....A..A.t\a.....x5.'OuE.C..@.....x..A..Eo..... ....A..Eo.....x.e.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .i.V.@./....."#.D.&j.A..A.t\a.....x5.'OuE.C..@.....x..A..Eo. .....A..Eo.....vK.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ._Bw.@./....."#.D....A..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):	436
Entropy (8bit):	5.586306964324677
Encrypted:	false
SSDEEP:	6:mnYOFLvEWdhwyu5X+JCqwK+41TK6tQ2nYOFLvEWdhwyu/GoKtcCqwK+41TK6tK:wRhHwK+EFRhIGXGwK+E
MD5:	4B2877EBD1DDB3E45F4686DBA8A10011
SHA1:	DB2F61A8D8B1D86DE70A4393551216B592FE1C40
SHA-256:	9919029F6316E5C768FAA432F7BCE5E1424268F57C530D4DCF37EF7F8CFCFA4D
SHA-512:	8EA831D872911C43C180DDA06BA1CCC0C05D8F2B1E163EF0DEAFCDBF9CC2DDAE4A427343D8B857C24E5D00E90D8BD7FAF6FDE2D846C8EFFDAD7C49F0ADA DFA3F
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .6?9.@./....."#.D#...A..A.....7...o..a=.98I.....(3.$G.A..Eo..... ...A..Eo.....9.g.....0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .0.x.@./....."#.D....A..A.....7...o..a=.98I.....(3.$G.A..Eo.....A..Eo.....pZ.....

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):	920
Entropy (8bit):	5.666060176446061
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0	
SSDEEP:	24:/PJ/lmi4hPJ/Obi4rPJ/6Ii4KPJ/AIi4:XJNmi4FJWbi47Jni4mJxi4
MD5:	54034BD6D0F181C967EC2C070FF0E9F4
SHA1:	B34656593B703AFD7861C57A27B44866F298BB88
SHA-256:	6847CB4F7967CD9D4099191974975E833DB007A8FF888AA9D692068C573FF8BA
SHA-512:	310979E04053A350673AF95B3A25BBD450E5F251A717D49D5F1D24DBB408E71CD4C53E19BC429B0D53EE767C4E18BA2286BABBCF807DCF5CB06622247BDF99B
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .R...@./....."#.D..d.A..A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....1.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..7.@./....."#.D)...A..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 ...V.@./....."#.D..i.A..A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....+{&.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..@w.@./....."#.D.o..A..A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....$.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	744
Entropy (8bit):	5.665543055845509
Encrypted:	false
SSDEEP:	12:xqTHVtOCPLnKfqT/p2CPLnP5qTaCPLnQqTYVCPLn:ArOMnRN2MnQ+MnHaMn
MD5:	99E96A7853AE33735D652CF943014E7E
SHA1:	B306FC89D5BA3D344A3B17D4DF85D595615FA08A
SHA-256:	2EAD6DE9B60FD4D5DF8FE70706DC50F809593E0E1F66EC879D5705C9CFE7DE94
SHA-512:	5FF2444FA4C5BE3179526A4F8DAB167F25025045F7FEEE709D0BAE7DF75D9E16063BB078777EE0205808834FB76F8DD5271F16938582A5C02B042F329054C6C4
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .o...@./....."#.D.D\.A..A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....,N.$.....0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ...6.@./....."#.DW&..A..A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....u.d.....0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .w.T.@./....."#.Dk._.A..A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....M.....0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ...v.@./....."#.D.;..A..A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....d.....

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):	828
Entropy (8bit):	5.652145869007757
Encrypted:	false
SSDEEP:	12:zRMe/fsDXRM8i/sDmBRMkIsD0ZRMnbsD:zB0DXDPDm1D0ZRD
MD5:	5E0F2B8E8D7B3B49797C95961C8A375E
SHA1:	1A072345985393F736663E7E7C71F96D54608AA8
SHA-256:	8FF9D0B3CA29F6C3D445B6E0940341660A607FCB7EE365F1C4CBF8CCA3631EA8
SHA-512:	E772CC76F8EFD30A06403F2CB675711E472162474F8D2C1AE516038C55B45B2F2B5DAF141A1D6DE349B24D7DB2307CEC7B5B9320635AD8D7970F2213915B20A
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..k..@./....."#.D..m.A..A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....4.D.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .'.>.@./....."#.D8...A..A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....~`.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ...Y.@./....."#.D..t.A..A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....8.G.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ...{.@./....."#.D....A..A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....u.....

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):	840
Entropy (8bit):	5.658295069135241
Encrypted:	false
SSDEEP:	6:mYilPYOFLvEWd8CAdAuGl9J3+Fong1TK6tEYilPYOFLvEWd8CAdAuO+A+uFong18:6lJR/yoM6lJRJoM/lJR57oM0lJREoM2
MD5:	C13AC2CCCEBEA918257A7E5CE957A27E
SHA1:	6ECCAAF05E944D5618A81999CA3D5E0FD88EBB90
SHA-256:	D5DACA9C0E86653D4FEA03BCF552BF1BE0505A133A52F667B37805FA677D5A1C
SHA-512:	9071CE7AEDCCBE989729205B5CF8CD9342AEED395800FC30801F038896F37B6E5281FAD8FFBD5299795B01477AC328619BDC8D33C218AAB27604142F652A7FB
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0	
Preview:	0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .!...@./....."#.D..n.A..Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....0\r..m.....R....\|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .._?.@./....."#.D....A..Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .-.Y.@./....."#.D..t.A..Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....I.f.....0\r..m.....R....\|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ...{.@./....."#.D....A..Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....MB*.....

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):	892
Entropy (8bit):	5.6643903340722686
Encrypted:	false
SSDEEP:	12:F8hRrROk/1zCn2in8hRrROk/Dsow2l8hRrROk/p2H/8hRrROk/DRL20:UPJ/Ni21PJ/Dfw20PJ/p2KPJ/DRL20
MD5:	4D6CFE24674B2DE2104BF5977088BCD0
SHA1:	81E09431DC7400AE0DE3540F6B949EADE9B485EC
SHA-256:	F083CC2FAD2C6E95740B3157881F1D94B897EFD802103742A1F686D306CFBBBA
SHA-512:	1F872A5CDD56B8DE59E27134724692A8BD7E246B5D05059869E2BF961C1379D0FBFE16388F9C000C7BDE9C4BA36F552A97AE8E706131699E421B9CC4AE52D9B
Malicious:	false
Preview:	0\r..m....._...h...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ..`..@./....."#.DX.d.A..A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....(!Vx.....0\r..m....._...h...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ...7.@./....."#.Dv...A..A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....L%fQ.....0\r..m....._...h...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .q.V.@./....."#.D.zi.A..A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....A.....0\r..m....._...h...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ...w.@./....."#.D.^..A..A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....?.c.....

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):	852
Entropy (8bit):	5.726870878511555
Encrypted:	false
SSDEEP:	12:ehRcc9zINJICk4hRcJYKNJICW4hRcWNJICZmhRcCFNJIC7:ehNSJICk4hoJICHhzJICEhtDJIC7
MD5:	28274758A469456740351E4384D684B9
SHA1:	CA0CF4F4B274CA5556A85ED6705FD990E6E3C534
SHA-256:	11A51610B2ADD0E4A565771E191234A3C17F2544B155FE878BD98FC7CA09B240
SHA-512:	2882B27E019C08E3D7ED964AA1C1EE717295FAD5E17D448EEF21FD2196244452D1E75B39CEE61E77A1AEB1F9B5321644D40BA310E8B156D79229AFA6BACDA7CD
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .q...@./....."#.D..d.A..A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....,.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .B.7.@./....."#.D....A..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 ...V.@./....."#.D.Yj.A..A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .Glw.@./....."#.DG...A..A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....[_g.....

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):	832
Entropy (8bit):	5.643315886583072
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhuSlp+2bLzgm2d/1TK6tsOEYOFLvEWdrIhuFekg8Lzgm2d/1TKF:0RAlEKReQRQiReVvR1l6//Re3R2KRer
MD5:	C97C23937618BE7ABA252605A2C7B6D9
SHA1:	9CC4821A40C53FC0162F47E83CE84CAC0C76BAD8
SHA-256:	4A59AA1C4FE5CFF197DF52F30EB3E698B1279071B0E26FAB8670EB94FC4B5153
SHA-512:	86E8F60F310C516A245648EC7F15DEE4EC2B972855163662EEA026486C1ACD8A2082A668DC2A139CAE1C98C9E921D45B6AABDCD3A70F3CEEE8F1ACBDE7ED4E26
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .....@./....."#.DL8b.A..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 .Mu7.@./....."#.D>...A..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 .|.V.@./....."#.D..h.A..AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....hg.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ...w.@./....."#.DG...A..AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....I9.v.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0	
File Type:	data
Category:	dropped
Size (bytes):	752
Entropy (8bit):	5.6420531520072545
Encrypted:	false
SSDEEP:	12:6JJKb/tI7JJKgK+lgJJKcoIhl/JJKgWoMfahII:6JIb/O7JIgegJIf/JI5nVI
MD5:	E6BA47C7A3A07BAD5540ADE1EB406070
SHA1:	29F07020A0A90CFD992C1CAAADB4DCE51DCD7300
SHA-256:	B012C400E3E04B714BB118BF0BC38DB08B11C0B77398FB20E92571D2A29EC489
SHA-512:	43F6A2A9F1BBD0192F727B5E7A3BA58A46EB14DE66DA421BD2875468572C41534CC455CA5FFEC0BBEB64C5B6A5A98C8CEAFA47630F428C4B1A28B054D9550586
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .._..@./....."#.D.x<.A..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....E)z.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...-.@./....."#.Dl...A..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...I.@./....."#.D.n:.A..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....9.%.....0\r..m.....<...)6.....keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...n.@./....."#.D....A..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....?.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	428
Entropy (8bit):	5.68094770908088
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvulZCzrhUDLYtmOZn1TK6tZm8WYOFLvEWdBJvvuwyuu0lihUDLL:xRBJJzeDcFZLPmTRBJ6OlXDcFZL
MD5:	5AD4F6908E9AFAF3D67BCC098971A643
SHA1:	AC683FDA21A52CFFAB78E9D1D7039FEF5971AF73
SHA-256:	FB2995E3625BC5FEA48127C8866A9FE86B71B00BA16DC801FEEC93A370C60E5B
SHA-512:	381D161C5B2D3C2EE64C0B0A2CEEB444E0BCDA0BE85A08F937023048656BBFD63B39DFB52EB0F0005C167C9748ED50C2A78CBD0F43910AE616D77390F0B2D36
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js .*.>.@./....."#.D....A..A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....P.....0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js .1.{.@./....."#.DZ+..A..A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....d.....

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):	844
Entropy (8bit):	5.6397099584839525
Encrypted:	false
SSDEEP:	12:BPHm9RcQPHvZgE4RcnlZPH09S7czPHYog7c:BPHURcQPHvZEcrPH0l7czPHYog7c
MD5:	293A21870ADB88923EB7ADE6641F8EAF
SHA1:	A49405BEA2D562C85DFB07D86F7C0586D493393B
SHA-256:	F11EAC4AB747616A204ADD8D7AA9F815B92C1F89BFBCB1552787233D826FBE26
SHA-512:	36D5023E9712E4348DD6CF5641D62E6730DB2B4C7E14D03F3DE6100ADC292B6F0B3D8A86075B96E6AFD89E5661E2A8EFB4727B472746E98FD9C5D2E3F0CC28
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .....@./....."#.D#.&.A..A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....&.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .y.+.@./....."#.D.a..A..A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....@.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .<.H.@./....."#.D..'.A..A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .Z.I.@./....."#.Dj2..A..A..L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....L..!.....

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):	416
Entropy (8bit):	5.603377762145338
Encrypted:	false
SSDEEP:	6:mKPYOFLvEWdENU9Q4Tn/k6diM3Y1TK6tZNMKPYOFLvEWdENU9QhxeiM3Y1TK6tN:bJRT9d/bdr07TJRT92er0
MD5:	DFF31E91CAAD0675D742A5B0E3FFB33B
SHA1:	E3F7E1012588F5E5B830AB070C4A88C8F810D016
SHA-256:	147868E72A1A59C1CDE3285EDA0DC50DF1393580BD4E2BEA91A3FCDDEC390C09

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
SHA-512:	1D3047B519156DB6257807714EB01ECDB9473DF1789F55EF8AD192BAF2FEC79EADA01922D8C59FB98864B9E424C5399879DE05723F6AB17B2DEF9574A93A9B0
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .8.9.@./....."#.D....A..A...M....m+lS..e.....<7.U.P8*.0K.A..Eo..... ....A..Eo.....=#i.....0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .y.x.@./....."#.Dd"..A..A...M....m+lS..e.....<7.U. P8*.0K.A..Eo.....A..Eo.....p.....

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):	416
Entropy (8bit):	5.629798235677845
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQuTjL8QjBRCh/41TK6t1d//MQt6EYOFLvEWdccAHQZ8pyj3:XRc9/LhDi/E3Rc9OxDi/E/
MD5:	BF6E5E6D20E5BD94D0C552BD2E77AEF8
SHA1:	6C29B1C37BFC76820E112026B68901D417ACD4CB
SHA-256:	9EC224E3B160BB827E5580DB334716D9657518BF41C7B72489E668E767A93737
SHA-512:	4687E3FA5CA1CC9D4E99AE5690F2ED9A7082C0B8CFFD5C3F5A362A8FA25F99566CEACF5E604F8A29D7A80CD2ECFE836309A22A837B5C17CA67A6D28B5CD48 BC
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .4f?.@./....."#.D....A..APJm...0x.x..RD...BB!@5..<..]....A..Eo..... ....A..Eo.....6\.1.....0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .r.|.@./....."#.D]...A..APJm...0x.x..RD...BB!@5..<..]....A.. Eo.....A..Eo.....^.}w.....

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):	5.5987639281311665
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhuCHlQyxULlF4r1TK6t7v+qs6XYOFLvEWdFCi5mhubtEJc:bs6xRki6QpLlF4n5js6xRkiRELlF4nV
MD5:	9FA2F9AE25DE88DB001BC9E54A4323F2
SHA1:	789E90872E3EA7246619E5FFEE4971D5E56590AB
SHA-256:	660E53056386DEC5394D9BBD05E3372F2B4F074001C9A710DDD68E5221694CA7
SHA-512:	012A2E2E5AE471077C7125D5EA8F23219CA2A2BBC8D35AAD66A2A778DA33D77BA723B0E696D5FE6BD70961392FB3B04A7B27C02E2B6A2B4D8EE422EA4D38EA A0
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .....@./....."#.D:.e.A..A.P...#4..l....5...5..).w.. .h .~..A..Eo.....A..Eo.....Q.u.....0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ..W.@./..... #.D..k.A..A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.56812339725298
Encrypted:	false
SSDEEP:	6:mhYOFLvEWd/aFuJ4tAo8Y941TK6tthYOFLvEWd/aFuZTh6i8Y941TK6t:WR4X8Y9EfRB6fY9E
MD5:	CC5C0A52AFCB27701C553EF5F1B5A993
SHA1:	69BB2BB3F07E2FE920EFDE337B0CD420B3A56A35
SHA-256:	A2F7C68AA18099D1A02273ADDF4EC1763A856FC936064CEA479021A8FE51293C
SHA-512:	78AD0C7033C8E0A7146DD3ED501A53C80BDA1B807E6F822BAD3EA15DD45448159D80F65A6E765715624C0D0FC6CEC9B5CB56496F6174F3EDA5930ADFAD9DD 99
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ..2@.@./....."#.D....A..A...a.f.m.i.o.p..3U5....^...I.A..Eo.....A ..Eo.....v.....0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ..V}.@./....."#.D^...A..A...a.f.m.i.o.p..3U5....^...I.A.. Eo.....A..Eo.....I.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	modified
Size (bytes):	416

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0	
Entropy (8bit):	5.585850714245512
Encrypted:	false
SSDEEP:	12:2DRuRyI2oB9Vd2k7lODRuRRTWoB9Vd2k:8xlvbdT7+mPbdT
MD5:	E9AC958175E99D878AE5BA5F1DC8DAD2
SHA1:	A1C30175259A236C67B12463360AE6928866C5A5
SHA-256:	0E227BBD198C5A31C7076FB1233318C05751F260AA7E99C605B6DEA489679C68
SHA-512:	A5CF13BE96C9F135431D4076D2B4EEF7F66011B5F01534E747DBF15C62E2D1E953CBBCA1DBE57D5F95370E70C98B8C5D711CE32BF9DCCEE9242F9884515C697
Malicious:	false
Preview:	0\r..m.....P...y.p....._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js .I.@./.....".D.j..A..A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.....0\r..m.....P...y.p....._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ..$}.@./.....".D.H..A..A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.....f(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):	832
Entropy (8bit):	5.641536709495563
Encrypted:	false
SSDEEP:	12:+RQRdkcrn72RQC6crny8RQVDrnTRQyZ2rn:+amAn72TjnfAnT96n
MD5:	1689CB1605CDEC6336085B2A04797E09
SHA1:	F0E18951B2756F2387A70AF45CC755E5B1B854C1
SHA-256:	CFDC657BFA75EC24FCC399D834C6EE45C37CE0A81EBBA68BABE9F6685692AC2A
SHA-512:	52C8BD4CEF674398EE497ABCB14A251D9CEC113DBB38779BCA20209FA6007EBDAB59FFEEF754545BD05A98DB6E8792BDF10621D3BFD2E4ECC593114264CCA1C5
Malicious:	false
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .....@./....."#.D?.r.A..A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....B.c?.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ...?.@./....."#.D\...A..A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....f}.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ..\Z.@./....."#.D4ix.A..A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....4.Z.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .q }.@./....."#.D....A..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):	420
Entropy (8bit):	5.587870288603734
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAuBoud3ryC8n1TK6tj598oXXYOFLvEWdENUAunP9Oa43ryC8u:xhRT73r7QlhRTIoJr7Q
MD5:	78DF120D508E6B4F50C86319DF2DDD99
SHA1:	8D5B2311785D84B95639C777B0E61C62FA12F516
SHA-256:	993A62A420FDBE27529D9AC385AF6DEA47AF38FE96D45C64C2F95E6A44858C24
SHA-512:	FB584FF9D36A528246A2A56809890A33DADEC15B9D8E4DEC5018A8CBA372B840B7D1CB645EDE9FD863C0E7A6FC9C7FC7F101E4061F21A37C5FA6E799F73AC03C
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .A=9.@./....."#.D....A..A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....e.f.....0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .(.x.@./....."#.D....A..A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....VC.....

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):	884
Entropy (8bit):	5.6653885267159225
Encrypted:	false
SSDEEP:	12:nRrROk/V3/6mJdRrROk/VI3KomgRrROk/VQmxzRrROk/V2BTm:nPJ/xrzPJ/7gPJ/XxzPJ/oy
MD5:	2503FC887EEFEA2A634CC8F7AFEC1C96
SHA1:	F7D10B82527CF98CDC7D8A9EA47EDD4F2B391747
SHA-256:	4FDEB33D09150FEB46326AE020D1CE0D369ECA115945317243F1201321ABC47A
SHA-512:	78DD177F3960AB17EB571B8685F61948F5A18A9B2CCAD43AF8C08A5C048B0B7EA05F086EF8B2765AF4265523D742622FA91062A623523BB8F2DE6A5DE421A690
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 .....@./....."#.DS[e.A..A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....g.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .9.7.@./....."#.DnN..A..A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....0X.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ...V.@./....#.D!.j.A..A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....5&.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..mw.@./....."#.D....A..A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....~d.....

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):	420
Entropy (8bit):	5.598806930063381
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWu+T6aJKzAdm9741TK6tm/lMZ/lXYOFLvEWdccAWu/syzAdB:qxRcYFjdu7Eo6xRc9Cdu7E
MD5:	CB519DB625D190E0BD864AF2FE4F0982
SHA1:	999131A5D7164BD6E392D9EA6708C08D092EC581
SHA-256:	4E040C70E02967ABFB2E9905902FBD08573A26EDD8A3DA9FDF47A9E330E9271E
SHA-512:	9C90172FD679AB182111C820F5F86F131BDF6311E322D13F6377C062EB1D8B8DBB8FB0A230BEBAB93537ABEC8C422DB672A05D39966DB434D52D4AE50D22E1E1
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ..,=.@./....."#.D%...A..A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....3.....0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js .0c{.@./....."#.D....A..A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....KR.....

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):	408
Entropy (8bit):	5.60630221706492
Encrypted:	false
SSDEEP:	6:mMOYOFLvEWdwAPVuoRouQhkJn1TK6ti2MOYOFLvEWdwAPVu2/u2KkJn1TK6tk:2R1DRaqLBR1HKqLC
MD5:	F26B9A1D7E939433FCED6850228ED663
SHA1:	ECAA63DF1F1ECFFC2C0B9D33E91C56102D5B324B
SHA-256:	FC1A4BB97790CA8BABDDEDCFCDECD5DF0E602BE6055319597645D94314AD34A3
SHA-512:	DCB8E2DDFC60754144537046D9579645A03538D144ABC1345378C066826DE980BE62C7CB5C583C12FAA4A73DDAD152875175C46A4C3BE41A7AD04DC2B7EC3DC
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .):9.@./....."#.D....A..A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo.....D.....0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .G.x.@./....."#.D|...A..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):	424
Entropy (8bit):	5.68687260025801
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQspG94zhcsBXIh1TK6t2l23PXYOFLvEWdBJvYQhCkG94zhcx:mxRBJQjDB0AWxRBJQIdDB07
MD5:	B46902F311BC7FB41891281556E78E25
SHA1:	C94B89D9DFA75EAE4304020F4B6F90F9096003C3
SHA-256:	DD264173C7137172B657E770234072B6750C4DB7F02B4DF61AC05DF130ED12E3
SHA-512:	6B56EDFC7CD356A02A78A823011D334FE2F155E4E7BADDC8626800A64D5A41BCD3286CCE280ACD4A8853D3F4275805AD8F8C9F315D0B7C46D4184CCFB6A5BF5
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ...?.@./....."#.D....A..A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....W.....0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .5.|.@./....."#.D_...A..A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....s.....

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):	912

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0	
Entropy (8bit):	5.641631907790579
Encrypted:	false
SSDEEP:	12:3RrROk/s9/+7cedRrROk/sk7clRrROk/saL7ciHRrROk/skL7cg:3PJ/E/zedPJ/elPJ/aiHPJ/P0
MD5:	02034B3952BA47C65131E11D294BD5F0
SHA1:	5A8EA433DFA9B603DFFC24A7E351D3D3809993DB
SHA-256:	258DEEEE0565E9431088587D10642DE88A7EA5154EF37999DA8280D8A236ABD0
SHA-512:	4789BDB1397B9805928AA7AC423F8EC7F71260121A04C63192C21207E13B17431B46EBF16BC37C14D5A5E38580E489BE8BFDE3EED5D93C153656FB0A40DE2BB
Malicious:	false
Preview:	0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .....@./....."#.D.e.A..A.....9Q].8O.z....=..:.N.{....N{.A ..Eo.....A..Eo.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ...7.@./....."#.D....A. .A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/j s/plugin.js ...V.@./....."#.D..j.A..A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....~+/W.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plu gins/desktop-connector-files-select/js/plugin.js ..nw.@./....."#.D....A..A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	2064
Entropy (8bit):	5.258385491138858
Encrypted:	false
SSDEEP:	24:Mfg1zZFufGMisp6r6C9QPCkteWkXqnM5MIyMhwuZ5xYMLBoMoH3XD1OFG3WBoIXN:h1zZ4+dsp60Nz6AlM9lYI
MD5:	D7E3FFD69E7359BAEF5CE234617580C7
SHA1:	8ED3B0159B84800031F445E0CB0680B6068BA4F8
SHA-256:	08728D0EF2D975051623F02CC1945127BB69A212A64888246C639BACC60F7F19
SHA-512:	51D24AD3CFD3044D66F2D519A67615A95F622B3E6D347A73CEABD1DBBA6A69B79388BB76FE218A045B68B25BDC32B38A8C9F8EA243594DA1C3A5406A51E233 B0
Malicious:	false
Preview:	....h...oy retne....'.....'.....;.y~A..z.B_./.....*...z.B_./.....oB*.8.B_./.....#...(...A_./.....k7A..z.B_./.....D.4..z.B_./.....[.i..%..z.B_./.....<...W..J.8.B_./ .....,+..._.#.z.B_./.....J..j....z.B_./.....6<|....8.B_./.....A?.2:...z.B_./.....+.{..'.z.B_./.....*)....J:.z.B_./.....2q....z.B_./.....P....V.z.B_./.....+.U.!..V.z.B_./..... .....P[. q.z.B_./.....!...0.o.z.B_./.....u\]..q.z.B_./.....z.B_./.....*.....z.B_./.....o..k...z.B_./.....^.~..z..z.B_./.....o..z.B_./.....Gy.'.h..z.B_./.....F..=z;..z. B_./.....3....z.B_./.....v...q...8.B_./.....C..M.....A_./.....a.....8.B_./.....~.,.4>..z.B_./.....&.S.....z.B_./.....@..x..z.B_./.....=....m...z.B_./.....;/....z.B_./..... .....q..z.B_./.....MV3...z.B_./.....:..N.A...z.B_./.....B_./.0.....oy retne

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	292
Entropy (8bit):	5.239876567987421
Encrypted:	false
SSDEEP:	6:mJz1q2PWXp+N2nKuAl9OmbnIFUtpoQAZZmwPo1okwOWXp+N2nKuAl9OmbjLJ:Yz1vaHAahFUtpo//Poy5fHAaSJ
MD5:	65A2265F7CB8745AED2EC853BEB59BB6
SHA1:	876B7B2BAE729D086FFA786F831C9AA64DF4E587
SHA-256:	2BEB8414DFDBBE876924641A2576DE4C5237371FB61CC164078FB402D6A1904C
SHA-512:	46691A498F162400B2F92417E007BB8E0744449A4AE863D4F8CB3288F073AF0C7EDAC5FB76ADF704ED94DAB51DB2980F456EA84C7D87F03165B54D1F0E3E455
Malicious:	false
Preview:	2021/01/11-18:07:33.622 1994 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/01/11-18:07:33.623 19 94 Recovering log #3.2021/01/11-18:07:33.624 1994 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):	1835008
Entropy (8bit):	0.009582006888757566
Encrypted:	false
SSDEEP:	48:TGEiaGEiCsMi9sMiDgsMiDgsMiDdsMhCDdsMhCDOsMhCDo+sMhCDo+sMhCDo+sM5:trrCCXonononononono
MD5:	33F24B6D329F01A8F81AFC1B3E2C6E7F
SHA1:	6088252E3E8BFA2180B74D1FCABCA58A817D14F0
SHA-256:	361223C095F871E0BB736E5E473347AC1508951ED7639469F1976297C9BA6064
SHA-512:	F8BCD8F46FBD8067F7802044D1EDB9A8ECFA768D889BCEBA6E71FEA7CE95109965470F17B18D55676FD582B4901C130E58FF8458DF8BDB9D7CA1D6ED3A3E91 3C
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links	
Preview:	VLnk.....?.....Tq.>..j..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210112020728Z-201.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
Category:	dropped
Size (bytes):	71190
Entropy (8bit):	0.8518006993848117
Encrypted:	false
SSDEEP:	96:kSUECGQMQd4Mo0BUpdbQPFER2pGWUDTUppYX152CG9GkAfw55WGW3F5M1JTHGZMS:uthdFEXz5hZD
MD5:	D5D65186305BC515846A1CD8B4996B5D
SHA1:	1D8B42971F92331CCCE4E7E3B0B22E93BA928123
SHA-256:	E092B9F6505771F8A66ECE515E7BFA5B291576EBE06CD97A2194382CC6A614A7
SHA-512:	A5C94AF9305CD2DE42B6AAB1A2C417F177F44E38782B98137D2BEB97FCBD03907C4BADEA08FA3EC1A81790412D3948A8AFF63B52D57B9F1D3CBE465E371E5E 48
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:	modified
Size (bytes):	32768
Entropy (8bit):	3.386475011094444
Encrypted:	false
SSDEEP:	96:iR49IVXEBodRBkQkOhFVCsL49IVXEBodRBkRykOhAVCs749IVXEBodRBklykOhaS:iGedRBsedRBxedRBVedRBu
MD5:	A659C217283598C661FCC45899695A0E
SHA1:	AA20CC1F7EBB46D2C0B3B676EEB7A4DFCAD88C8E
SHA-256:	7457114E3835B49515C4DAF68B14536200073F56B31059620FDF2A5CA8037198
SHA-512:	6122A690603D63A77C0422896851FEDB51DA79619B65D72A689255493138835BF02117DC9484E4AABEDEC0464210F42E9C9D894C55750F77F541845B0473BE7E
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:	dropped
Size (bytes):	34928
Entropy (8bit):	3.199459618739851
Encrypted:	false
SSDEEP:	96:d7OhFVCPD949IVXEBodRBk3kOhFVCsALR49IVXEBodRBkWykOhAVCs7d49IVXEBh:dviedRBNLGedRBpCedRB4yedRBZ
MD5:	B32EEA558BA8D2FAA53715B0DC73471A
SHA1:	7AB85D382CE3CF0170373DCA26EE51E301D07AF8
SHA-256:	AD5C2486FFB7518B36E2B847EF8E063BEF5752E81B45BC3AF65B7BB043304023
SHA-512:	2AF0FF241BE303D19378F40B5C8D4B20936D2CDED2B2717AD4D5BE0B28182AAC7BEAE7033BE7B25E9A28FCEF76EC7709ECCEC18510DB84CCD9DA97ACA35F DBA8
Malicious:	false
Preview:	.....=.I..... .....X.. .h...y..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.5956	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	157443

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.5956	
Entropy (8bit):	5.172039478677
Encrypted:	false
SSDEEP:	1536:amNTjRlaRlQShhp2VpMKRhWa11quVJzlzofqG9Z0ADWp1ttawvayKLWbVG3+2:RNj3aRlQShhp2VpMKRhWa11quVJX2
MD5:	A2C6972A1A9506ACE991068D7AD37098
SHA1:	BF4D2684587CF034BCFC6F74CED551F9E5316440
SHA-256:	0FB687D20C49DDBADD42ABB489C3B492B5A1893352E2F4B6AA1247EFE7363F65
SHA-512:	4D03884CA5D1652A79E6D55D8F92F4D138C47D462E05C3E6A685DA6742E98841D9C63720727203B913A179892C413BFB33C05416E1675E0CF80DA98BE90BA5E4
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\Microsoft\Internet Explorer\DOMStore\CKHMOFCB\ykm[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):	148652
Entropy (8bit):	5.091705378315703
Encrypted:	false
SSDEEP:	768:uM8M8MpMpMsMAMcMpMpMIMIMFMFMHMHMvMvMiMiMkMwMwMHMHMAMAM9MAM+MzMzN:t
MD5:	2BC983FC5FD2C8490C0768871AC91F05
SHA1:	7C4BF75169118FB8B7DF02E20B39737CC287176F
SHA-256:	8770437D92C735E29E0CD91C947A0EBFA25153EDBD4AC5C2AA4C9EB24DB156B6
SHA-512:	F2A73BF24E16EBA57C54515C2235F2DE96377230C71E6FCAA7D0F891378055BE929514E494BCC702E49DB42F6FEE640EDBDFE9F8CAAB9BF9697DBEF3540DE3DE
Malicious:	false
Preview:	<root></root><root><item name="goog_pem_mod" value="30" ltime="3553952688" htime="30861447" /></root><root><item name="goog_pem_mod" value="30" ltime="3553952688" htime="30861447" /><item name="google_experiment_mod47" value="580" ltime="3554112688" htime="30861447" /><item name="google_experiment_mod34" value="251" ltime="3554112688" htime="30861447" /><item name="google_experiment_mod53" value="114" ltime="3554112688" htime="30861447" /><item name="google_experiment_mod36" value="656" ltime="3554112688" htime="30861447" /><item name="google_experiment_mod37" value="41" ltime="3554112688" htime="30861447" /><item name="google_experiment_mod44" value="894" ltime="3554112688" htime="30861447" /></root><root><item name="goog_pem_mod" value="30" ltime="3553952688" htime="30861447" /><item name="google_experiment_mod47" value="580" ltime="3554112688" htime="30861447" /><item name="google_experiment_mod34" value="251" ltime="3554112688" htime="30861447" /><item name="google_experiment_mod53

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{0E7866F7-547B-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	32856
Entropy (8bit):	1.8506950905142427
Encrypted:	false
SSDEEP:	192:rrZWZ62N9Wqtpfu+t93/XWJXfBttxWt13un3:r9S5NUiZRcZFA8
MD5:	D9E60C03A87694609F903D2413375586
SHA1:	FCE4300C7A506B2B4DD8288813F330D873271571
SHA-256:	0065355D3DCB9564022FCB9844C75A2E0EF0BDF1416233BB2DC37E0464856E54
SHA-512:	ABAAA1E4C284B7F94BB49D0309564234FC0F83E9A97EFCFD7E458180637E944F238F10008D8E2C02327123D616264224D8C84A36EB06FC3A2DF46FCE562D23B5
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0E7866F9-547B-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	497472
Entropy (8bit):	3.360979994397474
Encrypted:	false
SSDEEP:	3072:k0yeRCsexC0+7Ps9M5Qe/gxUxC0+7Ps9M5Qe/gxR049:X
MD5:	8E3D37D42F199A18FBB14B42C4456078
SHA1:	0A70693D59EE7FD2F9570E780C9493343A696638
SHA-256:	4E549749316BE49EE087C95F0CF2210FAEFD3963CDFCDA367BA95310E0C7847B

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0E7866F9-547B-11EB-90E4-ECF4BB862DED}.dat	
SHA-512:	0A45891F21015A7383F05D48F51DC74B38662DC075C5C868F87E835A39CCC7919AD921C1FEED4B28EE4D10C8239F5BB94597C280C4CCB027AE23860C71D68F
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1551FE3F-547B-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5671212813916753
Encrypted:	false
SSDEEP:	48:IwJ7GcprOGwpaLG4pQQGrapbSErGQpKyG7HpR7sTGIpG:rLZmQN6uBSEFAdT74A
MD5:	8F977B16C19F9FA032F527C5911FC51C
SHA1:	507551C738676FA941D4A2C7D6A623C91B13EE3E
SHA-256:	4133F2E7B4376C943CE0524C3CEF18BE0D3442FB807981EDA084BDA62E6055CF
SHA-512:	9448D21FBAD9F437274EC70F716B4B0B7C89422FF5499D3A300F649136313A184A57CB32D12CAB15D19E8E57A16D15DF731133A094601F060A89C5D60B3111FC
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.070829975620784
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEnVMoVMf4nWimI002EtM3MHdNMNxOEnVMoVMf4nWimI00ObVbkEtMb:2d6NxO2Pw4SZHKd6NxO2Pw4SZ76b
MD5:	EFAB90AD33E2D8DDA74DF9ABBAB3D2BA
SHA1:	DB39D39190545BA6B02234C39ADA5E5F0982CEA7
SHA-256:	B7FAA8975D15B8B413F42DA6C5323F8A7B4B60F1003171FF6100DE010F696152
SHA-512:	9F885CFEF0943CEE2B93A8806C15C2A17BE6E8C92A4AD555E7CA5FF8B4AD1DA726A515BFBBBE88E6B1D33005F904F435B728A327510A144AE0FDC20FDDF313A4
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xe657adeb,0x01d6e887</date><accdate>0xe657adeb,0x01d6e887</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>0xe657adeb,0x01d6e887</date><accdate>0xe657adeb,0x01d6e887</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):	5.157787853271403
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kWhcMDhcMf4nWimI002EtM3MHdNMNxe2kWhcMDhcMf4nWimI00ObkS:2d6NxrdhcQhcw4SZHKd6NxrdhcQhcw4o
MD5:	5E6BA57CC06A35CE63E4B1C5C98CE5F4
SHA1:	C7366A89704C7DF60D28D0F413FACF5B4BAEF340
SHA-256:	DDF5D05229917A4D1F974E029BD611517760F3205C34DABDB2E24D3FEB01B938
SHA-512:	A159654B34DE2F4FD088217FBB70482F1E76F4F56D77ECD5F1D733DEDF92822DEA6DF79F2C461B52B717B7C5D5BF328C6D4399621EDBBE63EFC6CE92F1B8799
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xe64e24b9,0x01d6e887</date><accdate>0xe64e24b9,0x01d6e887</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>0xe64e24b9,0x01d6e887</date><accdate>0xe64e24b9,0x01d6e887</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):	5.091447693204191
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL3bFMwbFMf4nWimI002EtM3MHdNMNxvL3bFMwbFMf4nWimI00ObmZEs:2d6NxvjJ9Jw4SZHKd6NxvjJ9Jw4SZ7mb
MD5:	5421213E6082F41321F376E7E4D8AE40
SHA1:	750C3AF0557CE099EE36B24A6E90C5B37D9DFC57
SHA-256:	E463D06F6CE34689E936A6DDC74C836BD0A71509FAB0752524D595BFCD46101E
SHA-512:	49FD738DD2A339811BDACE582CFAB2A5463296148B38C082AE4C6AA0AD509A6491A6072CEF1AEA031CAC559F036181E453BC61FE608FC9415965EDD32F0890D 3
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xe65a1083,0x01d6e887</date> <accdate>0xe65a1083,0x01d6e887</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>0xe65a1083,0x01d6e887</date><accda te>0xe65a1083,0x01d6e887</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipe dia.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):	5.137668419403086
Encrypted:	false
SSDEEP:	12:TMHdNMNxiIMRMf4nWimI002EtM3MHdNMNxiIMRMf4nWimI00Obd5EtMb:2d6Nx9Gw4SZHKd6Nx9Gw4SZ7Jjb
MD5:	471DFCF4557DC7CFED16C92C18F67F64
SHA1:	6341A7C18A1D44B4A50A929E7220B967C39822B4
SHA-256:	283D2C9B1FBA5D69AD48D3558ADC750627895DA4EFAE73A246C13FB821E334ED
SHA-512:	3F77C73D073AA6083DEEC0CE06881F2A7F98D4BFB1F8C051CCFF9E86F6DC5BA5EA7B11CEB9E25F26AC18F23C35B85935B01BD0EB0C51A7A0EE894DEDAC54 2FD
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xe652e959,0x01d6e887</date><acc date>0xe652e959,0x01d6e887</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>0xe652e959,0x01d6e887</date><accdate>0xe652e 959,0x01d6e887</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):	5.106863354651443
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw3bFMwbFMf4nWimI002EtM3MHdNMNxhGw3bFMwbFMf4nWimI00Ob8V:2d6NxQqJ9Jw4SZHKd6NxQqJ9Jw4SZ7YV
MD5:	734FC0C37998172077227BD425EC5088
SHA1:	B36924ACD78ACFDDFC6E010411E65B7CE9859D36
SHA-256:	DA8DB2BE7E728176C2384BB0C6D7D5DB44C25034338DA7E333C9BD77E63F80E8
SHA-512:	8810D418B6B8243E0DE3B41B999B08D85098C96898BAA549836066D22F9315C5AE15D2DB6EFEE0DED1FB54296D6398C35C9E7FB0A749B5645AF5EF8EDCDB72 1
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xe65a1083,0x01d6e887</date> accdate>0xe65a1083,0x01d6e887</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>0xe65a1083,0x01d6e887</date><accdate>0 xe65a1083,0x01d6e887</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):	5.117128886789481
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
SSDEEP:	12:TMHdNMNx0nMBcMpBcMf4nWimI002EtM3MHdNMNx0nMBcMpBcMf4nWimI00ObxEty:2d6Nx0dPw4SZHKd6Nx0dPw4SZ7nb
MD5:	CF4D2E8A29452D75CEBEE8498047763D
SHA1:	DE8A85D65B388A79803FA3C9CD90A028EFEFA6E1
SHA-256:	933D08AF6A0338A1D8CDF6C2A4DBEEEC0C39FF2A0EAF56A1766887A9B07ECEF5
SHA-512:	583DD5796C3000447417F87D6AF3F0E2F501E358003A88DC33C078BE07E9F5297AC183929889A9AAA8BB0A6D62CA9CF1FD4C81BE30299920F9B9CB8F8882B2B4
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xe6554b8f,0x01d6e887</date><accdate>0xe6554b8f,0x01d6e887</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>0xe6554b8f,0x01d6e887</date><accdate>0xe6554b8f,0x01d6e887</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):	5.154292066887897
Encrypted:	false
SSDEEP:	12:TMHdNMNxxMBcMpBcMf4nWimI002EtM3MHdNMNxxMBcMpBcMf4nWimI00Ob6Kq5Es:2d6NxTPw4SZHKd6NxTPw4SZ7ob
MD5:	594CA1B7CC3E295F663E83B0B4AB6F82
SHA1:	694F633B6186E51DC92CD1CFEDB3513A893B7760
SHA-256:	E01130391FBA7C9ADEF392075C736CD1CA9BB1D29E17F59900C714E8D4AD140A
SHA-512:	0A1CADD1668E55D99E2BB5110FD21A6E5192B4A4A2DD57CE64291A6B8245F0CE2C5E2497BBF1F4DEE3C964C13C0E007F3CC42DCB8A76445AD39E2BBEC5CF03C2
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xe6554b8f,0x01d6e887</date><accdate>0xe6554b8f,0x01d6e887</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>0xe6554b8f,0x01d6e887</date><accdate>0xe6554b8f,0x01d6e887</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):	5.113761539596227
Encrypted:	false
SSDEEP:	12:TMHdNMNxcdAcMQAcMf4nWimI002EtM3MHdNMNxcdAcMRMf4nWimI00ObVEtMb:2d6NxydPdw4SZHKd6NxydGw4SZ7Db
MD5:	65070A00E61F8ACF4A58ED7CF69DBD64
SHA1:	B3770B35657332D0825CC4058A6A2979D59C93E5
SHA-256:	255EF8032B1BDE611906ECDEB6367ABC0F19B8D4DF981DFDE06F734157D0007A
SHA-512:	04CADCD647506E4904A7D24ADCF2070394151BE8E4EB1823F0190943706686AFFF866924F88F83D2E5724F86074B780FD848EBB051DAA47DB57809ED481816025
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xe65086e6,0x01d6e887</date><accdate>0xe65086e6,0x01d6e887</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>0xe65086e6,0x01d6e887</date><accdate>0xe652e959,0x01d6e887</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):	5.123088082869807
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnIMRMf4nWimI002EtM3MHdNMNxfnIMRMf4nWimI00Obe5EtMb:2d6NxwGw4SZHKd6NxwGw4SZ7ijb
MD5:	43BA3283C293ABD32D0EA2BF724C90BD
SHA1:	5CD8F03F2E7D684D957C5E490C919D310C6BF489
SHA-256:	0D594DDDAAE0B75E4EA16177C785BA90AD2F751AAD13D7566E69CD868FC403AA
SHA-512:	AB76C5FB577C27B9BCE76DC5ED6D7409A2241BA470C6456FA05BDFC044593F5198202A9F22A5C06851A6BEA1A0021C93A753D58C90D5726C63AF9EB48A7E0070
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xe652e959,0x01d6e887</date><a ccdate>0xe652e959,0x01d6e887</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>0xe652e959,0x01d6e887</date><a ccdate>0xe652e959,0x01d6e887</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Go ogle.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1264
Entropy (8bit):	2.1527581361537425
Encrypted:	false
SSDEEP:	6:0YOIvvcAMlGx/i1dFlVPmaYOIvvcAMlGxlKVR1HPmt:5Obplki1dFXmbObploKVzvmt
MD5:	C7A2538BAE3CAD6509487B90E2BBBCE8
SHA1:	153BDF91A5A417542B43D89F06C3E30E3C083873
SHA-256:	BE35E083C6DB6CA5F1108856081CADB9FDD768AE7DAFD5FDC42414AF3357C017
SHA-512:	D73054B27249BF3C39CDD73B50EAA25281DB9D29CD4708B32D658E13155601799E415512A19DBEAA6BB4460D4CCD31C05A2EDCE5EFFCE298721F68F80DBBA(9A
Malicious:	false
Preview:	..h.t.t.p.s.:./.y.k.m...d.e./.f.a.v.i.c.o.n...i.c.o.>.....(.....(..... ....h.t.t.p.s.:./.y.k.m...d.e./.f.a.v.i.c.o.n...i.c.o..... .....(... ...@... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\DXI1ORHCpsQm3Vp6mXoaTXhCUOGz7vYGh680lGh-uXM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22656, version 1.1
Category:	downloaded
Size (bytes):	22656
Entropy (8bit):	7.977267678934457
Encrypted:	false
SSDEEP:	384:raUkzOoQUm7Ed4aTRrH9uIJcFvggUg2qh86vYk8lDRSf5shb6dddddvKy9E:raUkSoxmi42ZhiFvHj2486vYZRKIbOE
MD5:	7C5D9F078BEA8C1FC0B21A764B832138
SHA1:	2505FE5F361045BE53FB71AFB8B105E319393389
SHA-256:	7E7FD69FF0A1671B508800F38F6AD3690650C27C0A1F3F505629ECBE6BA51942
SHA-512:	5BC9B3556843516059669640935806 05A3504CB0C775F3A331BB413EB5CC1999437914FC14776CD05C42305F13F6B130E71ABB2E02128B773EF8DF842431D171
Malicious:	false
IE Cache URL:	http://https://themes.googleusercontent.com/static/fonts/opensans/v6/DXI1ORHCpsQm3Vp6mXoaTXhCUOGz7vYGh680lGh-uXM.woff
Preview:	wOFF.....X.....FFTM...l.....\.\iOS/2.....]..`...cmap.....h.....cvt ...P...]....fpgm.....~a..gasp...\.....#glyf...l..8"..U.~Q.\head..@....3...6.q..hhea..@. .....$...8hmtx..@.....Xy.[4kern..B.....#.....loca..Q.....lmaxp..R.... ... ...Uname..R.....M.post..U....x....x..prep..Wd.....:..]....o1.....B.....\x.c`f.`.a`e.`..j...(.../2.1..`b.ff cfeabby....A!...A.....6..".-..L.....Ar,...@r...s.....x.c```f.`..F..X..1.,.....:.....L.n1.Q.Q.R.SPR.RpQ(QX..?X.... ..a.....K.....?.....}.`.M.6>X.`.....4.....l.pe.L@..]..+,.l...\.<.\| ...B.".b...R.2.r...J.*.j...Z.:.z...F.&.f...V.6.v...N...n...^.>.~...A.!.a...Q.1.q....m..g.[.h...W.^.f..u.6n.e..{v...P...y.baA6CY.C.,.b...r..rj.V.jL...sk...Z..>r...s.N.d8.p...K@..3..Zz.{..'L.: .a.....=^..p..(...K{.x.c.a.g.c..$K..$..`.g.e..... .....R.g.....?.....x.)d.....$...."....0.#@2....0.....x.uU.S.F....."S.0.!.n..`.t..@)lm..u.b.3+.A"&cz.C...H

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\EInbV5DfGHOiMmvb1Xr-hnhCUOGz7vYGh680lGh-uXM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22944, version 1.1
Category:	downloaded
Size (bytes):	22944
Entropy (8bit):	7.971252540494737
Encrypted:	false
SSDEEP:	384:hUT65+9ZqAMaCMUkyKV0YWnAUuLoWKlhx8OuuiL3ShGAshb6ddddddvaSZ:hUT65g8AikyKinAUuLo/pVgklbny
MD5:	F9F5441393891F990AE6AFD069E86613
SHA1:	767B7D4E0FADB12BF6FB015E76AC21AD3EEDCACA
SHA-256:	CAE22D14E699BFF969A782A9A166C6CE43FA857CF1F63A5AF8B2C4CA09B8217A
SHA-512:	8748ED37F2830FAB72796B7E7542583EE0830E6356097FBD1E33054C5A5290DFEE5AE95F733A67CE6F8B35E20B69BB0A77CED9C3A49A8F9CC7C6393C51BC65D 5
Malicious:	false
IE Cache URL:	http://https://themes.googleusercontent.com/static/fonts/opensans/v6/EInbV5DfGHOiMmvb1Xr-hnhCUOGz7vYGh680lGh-uXM.woff
Preview:	wOFF.....Y.....h.....FFTM...l.....\.2.OS/2.....^...`...qcmap.....h.....cvt ...P...g.....o.[fpgm.....s.ugasp...l.....#glyf...|..9)..V...~3head..A....4...6....hhea..A. .....$....hmtx..A.....X.?.kern..D.....#.....loca..R(.....)...maxp..S.... ... .u.Dname..S.....z.post..W....x....x..prep..X.....1..S.....o1.....L.....Wx.c`fY.....:....Q.B3_dHcb .`b..dc.`abby....A!...A.....ah..e.P``...c.e....\.kW....x.c```f.`..F..X..1.,.....:.....L.n1.Q.Q.R.SPR.RpQ(QX..?X.... ..a.....K.....?.....}.`.M.6>X.`.....4.....l.pe.L@..]..+,.l...\. <.|...B.".b...R.2.r...J.*.j...Z.:.z...F.&.f...V.6.v...N...n...^.>.~...A.!.a...Q.1.q....m..g.[.h...W.^.f..u.6n.e..{v...P...y.baA6CY.C.,.b...r..rj.V.jL...sk...Z..>r...s.N.d8.p...K@..3..Zz.{..'L.:.a... ..=^..p..(...K{.x.c.a.g``..$K..(..`.e.a.a`....C..L..@t.....A..L..&.....1\gta.e....320.0...2.g.j...=...x..U.O.G..Y..0d.....2.].vI...Jaj{..nZ.A.%=.A..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\MTP_ySUJH_bn48VBG8sNSnhCUOGz7vYGh680lGh-uXM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22604, version 1.1
Category:	downloaded
Size (bytes):	22604
Entropy (8bit):	7.975270797522764
Encrypted:	false
SSDEEP:	384:5/UizWtMNrcEK2lvVuj8USPW1A7aZ+zLTo+SkM41+p8yshb6dddddvSEzkA:dUi5rK8N00u1A7zOwLyIbIh
MD5:	33B67BE977ACF26D66961D95DF64C1B8
SHA1:	8D05328ABAF7121EF858219E1E642B98597C9144
SHA-256:	A851D97FCC71C78CA279754FABC2289A600AABECEC4D9E4387CAB9C7400AA2D0
SHA-512:	621920075BC0BDEB0DF983B8E40D4B2F718DFD1CE49AB8FFB6CB94B44B80368B9099E024E3C60A58D49D468ABF4D9F347A4A6B928C0D0CA8BABCB3F72746FD B3
Malicious:	false
IE Cache URL:	http://https://themes.googleusercontent.com/static/fonts/opensans/v6/MTP_ySUJH_bn48VBG8sNSnhCUOGz7vYGh680lGh-uXM.woff
Preview:	wOFF.....XL.....FFTM...l.....\.2.OS/2.....^...`....cmap.....h.....cvt ...P...[.....4fpgm.....~a..gasp...X.....glyf...d..8...T..2b.head..@h...4...6. 5..hhea..@.....$....hmtx..@.....X..P.kern..B.....#.....loca..P.....maxp..R.... ... .R.?name..R.....post..U....x....x..prep..WD.....x..n.....o1.....L.}.....bx.c`f.a.``e. `..j...(.../2.1~c``.fgc.`abby....A!...A.....ah..e.P``...c.b....\....o..x.c``f.`..F..X..1..,.....:.....L.n1.Q.Q.R.SPR.RpQ(QX..?X.... ..a.....K.....?.....}.`.M.6>X.`.....4.....l.p e.L@..]..+,.l...\.<.|...B.".b...R.2.r...J.*.j...Z.:.z...F.&.f...V.6.v...N...n...^.>.~...A.!.a...Q.1.q....m..g.[.h...W.^.f..u.6n.e..{v...P...y.baA6CY.C.,.b...r..rj.V.jL...sk...Z..>r...s.N.d8. p...K@..3..Zz.{..'L.:.a.....=^..p..(...K{.x.c.a.g.c..$KY...e@.,A.".m....x.....3.....?.[.o...2...:...a..b.)@.Y.....v1.b4d...36 ..x.uU.S.F....."S.0.!.n..`.t..@)lm..u.b.3+.A"&cz.C...H..'r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\PRmiXeptR36kaC0GEAetxkCDe67GEgBv_HnyvHTfdew[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 21504, version 1.1
Category:	downloaded
Size (bytes):	21504
Entropy (8bit):	7.971786766447748
Encrypted:	false
SSDEEP:	384:3aUR65+w/hUzXsrqAH6y+iQSGnR8OR05Ok1rBFshb6dddddvErVR8Q:qUR65JWwqAH6JSGnR8O8nIbJnp
MD5:	CBBCF9A611C26C27252829FF4C8449E7
SHA1:	BFF19768A4218854193C18C65895AF20D71CEEA1
SHA-256:	7F268D600F53E6CF94E5DCE1534AC0E8694FCFF3A50394638313781719779 90D
SHA-512:	5BEDF6CBDC3BFADC6D35EB74EEF2D7A69F0B3BC29914695F853729A1D16320A95646F46D1606035B93B97BF1FEA75189B905FAF912E80660B3DCF6071A47B0E 8
Malicious:	false
IE Cache URL:	http://https://themes.googleusercontent.com/static/fonts/opensans/v6/PRmiXeptR36kaC0GEAetxkCDe67GEgBv_HnyvHTfdew.woff
Preview:	wOFF.....T.....FFTM...l.....\../OS/2.....^...`...Ecmap.....h.....cvt ...P...o.....fpgm.....s.ugasp...t.....#glyf.....3P..I.>.<.head..;....4...6.H..hhea..<. ...!...$....hmtx..<,... ...X.A&.kern..>L.....#.....loca..L`.....|.k,maxp..N.... ... .name..N0.....;....post..Q`...y....l..prep..R....!...@..R.....o1.....e.....Yx.c`f.gV``e.`..j...(.. ./2.11s01qs.1s.01.<``z.....k....0.p.2E(00....n.R@..[.....x.c```f.`..F..X..1.,.....:.....L.n1.Q.Q.R.SPR.RpQ(QX..?X.... ..a.....K.....?.....}.`.M.6>X.`.....4.....l.pe.L@..]..+ ,.l...\.<.|...B.".b...R.2.r...J.*.j...Z.:.z...F.&.f...V.6.v...N...n...^.>.~...A.!.a...Q.1.q....m..g.[.h...W.^.f..u.6n.e..{v...P...y.baA6CY.C.,.b...r..rj.V.jL...sk...Z..>r...s.N.d8.p...K@..3..Zz.{..'L. :.a.....=^..p..(...K{.x.c.a.g.c..$KY...e@.,..".9....x.....3.....e..=L.....`.Q..1.Q.....uF.F[F}..4#.....-.p..... ..x..U.O.G..Y..0d.....2.].vI...Jaj{..nZ.A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ZeroClipboard.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	29973
Entropy (8bit):	5.375774377884238
Encrypted:	false
SSDEEP:	768:2MkhrOFro75Mhy/J/eHjogJRsn68K9f71taqhTgY6g+f6A+r2Z:ZkZOxo7f/oHTJRs631tVhkY6g+SO
MD5:	997A9DCE7DC693A1F1D257480D0FF39C
SHA1:	76D4CCE32D630D2E7BC6258C8DD5D8825D812B83
SHA-256:	1EE1E41295C9A0E494D7290A97C7DF2BB8F50BE5978342FC6D68EF98A10AEE54
SHA-512:	50FB9FA03EBB082DB7D5B40C10B38F6DBD05D2E4F19770B80BA43F572E859D729BE6EF78155A605B33515FD795138367735B8FA2DBBE2CCADFF00E368DD3AA FD
Malicious:	false
IE Cache URL:	http://https://ykm.de/themes/ykm/js/ZeroClipboard/ZeroClipboard.min.js
Preview:	/*!. * ZeroClipboard. * The ZeroClipboard library provides an easy way to copy text to the clipboard using an invisible Adobe Flash movie and a JavaScript interface.. * C opyright (c) 2009-2014 Jon Rohan, James M. Greene. * Licensed MIT. * http://zeroclipboard.org/. * v2.2.0. * Subversion: "4+c8xqv+FPZ/Zcns21/yraTgJzE5b/j5w63ecG1 n5AU=". */.!function(a,b){"use strict";var c,d,e,f=a,g=f.document,h=f.navigator,i=f.setTimeout,j=f.clearTimeout,k=f.setInterval,l=f.clearInterval,m=f.getComputedStyle,n=f .encodeURIComponent,o=f.ActiveXObject,p=f.Error,q=f.Number.parseInt||f.parseInt,r=f.Number.parseFloat||f.parseFloat,s=f.Number.isNaN||f.isNaN,t=f.Date.now,u=f.O bject.keys,v=f.Object.defineProperty,w=f.Object.prototype.hasOwnProperty,x=f.Array.prototype.slice,y=function(){var a=function(a){return a};if("function"==typeof f.wrap&& "function"==typeof f.unwrap)try{var b=g.createElement("div"),c=f.unwrap(b);1===b.nodeType&&c&&1===c.nodeType&&(a=f.unwrap)}catch(d){}return a}(),z=function(a){r eturn x.ca

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV_recent_urls.ajax[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV_recent_urls.ajax[1].htm	
Category:	downloaded
Size (bytes):	5173
Entropy (8bit):	5.1306137724634
Encrypted:	false
SSDEEP:	48:Y1zmLofIX1vWBb5HWD6cOtGX3vdkzaGr8RW8RmU1keT8:Z0fIX1vWBxWD6cOtGXezagSWSmU1kk8
MD5:	B1F05D74585E4BE6C8688DAD5494AB79
SHA1:	E0903446045D622C3BE425BE766D2671B1A909A6
SHA-256:	F30B4498678799374F8BD7032C6278285F2169873175E41C2388D8BEC52D3CAA
SHA-512:	81E2F230B76ED5025A37EDD31676BB1213DB12D9810B4E8D53D2FFEA0A379939F1A529809A956BD0028807F82C83A9800233E5168154FF7C2DAA169C00CD9B5A
Malicious:	false
IE Cache URL:	http://https://ykm.de/_recent_urls.ajax.php?sEcho=1&iColumns=2&sColumns=&iDisplayStart=0&iDisplayLength=30&iSortingCols=1&iSortCol_0=0&sSortDir_0=asc&bSortable_0=false&bSortable_1=false
Preview:	{"sEcho":1,"iTotalRecords":"2050","iTotalDisplayRecords":"2050","aaData":[["11\/01\/2021 16:07:51","<a href=\"https:\/\/ykm.de\/312ec217f37310d6\" target=\"_blank\"><span class=\"mobileHide\">https:\/\/ykm.de<\/span>\/312ec217f37310d6<\/a>"],["11\/01\/2021 09:52:32","<a href=\"https:\/\/ykm.de\/95a0db859db4e0b7\" target=\"_blank\"><span class=\"mobileHide\">https:\/\/ykm.de<\/span>\/95a0db859db4e0b7<\/a>"],["10\/01\/2021 14:28:27","<a href=\"https:\/\/ykm.de\/054e9d62dc204a68\" target=\"_blank\"><span class=\"mobileHide\">https:\/\/ykm.de<\/span>\/054e9d62dc204a68<\/a>"],["09\/01\/2021 06:58:01","<a href=\"https:\/\/ykm.de\/f4b5b0c66b58ab0e\" target=\"_blank\"><span class=\"mobileHide\">https:\/\/ykm.de<\/span>\/f4b5b0c66b58ab0e<\/a>"],["08\/01\/2021 10:07:03","<a href=\"https:\/\/ykm.de\/0e31787b0a830c44\" target=\"_blank\"><span class=\"mobileHide\">https:\/\/ykm.de<\/span>\/0e31787b0a830c44<\/a>"],["07\/01\/2021 11:54:40","<a href=\"https:\/\/ykm.de\/6b689707bce52a76\" target=\"_bla

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ads[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	14108
Entropy (8bit):	5.556388878043573
Encrypted:	false
SSDEEP:	192:TtjY0I6p44JlVyjORGpM8O6njXIVhSa0pZrPhoG8FZ7BGUSczOZeYmfJ5iJRLJxP:TG0MHqR2Baca8ZrPuGiZ1OZmfTiJVfUl
MD5:	524C4EB9FD782257406546FF4F14F138
SHA1:	DCC91AFF7289F7743B2BB8BDA1D58B528530C015
SHA-256:	0D23F4A226212BD190A27972F8DCCD95180C79AFD6BC1AF982DE12722E1454D1
SHA-512:	1AEDEC383BD77152B8DDCE5E1D2E1ABB97E0B9B53E213E491F09B6D769D53C68CBBAF6A5F23E871A957AF3668611AEB7EE14D984160D25AE85CA084559E990 1A
Malicious:	false
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?guci=1.2.0.0.2.2.0.0&client=ca-pub-8989771679754051&output=html&adk=1812271804&adf=3025194257&lmt=1610417345&plat=1%3A32776%2C2%3A32776%2C9%3A32776%2C10%3A32%2C11%3A32%2C16%3A8388608%2C17%3A32%2C24%3A32%2C25%3A32%2C30%3A1081344%2C32%3A32%2C40%3A32&format=0x0&url=https%3A%2F%2Fykm.de%2F&ea=0&flash=29.0.0&pra=5&wgl=1&dt=1610417344754&bpp=97&bdt=365&idt=202&shv=r20201203&cbv=r20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D8b5e4409b88a7409-224663149da600da%3AT%3D1610384913%3ART%3D1610384913%3AS%3DALNI_MaRpNz1-0IYcClgw8Hhh0iIAUFJCA&nras=1&correlator=4708315792234&frm=20&pv=2&ga_vid=2041299598.1610417313&ga_sid=1610417345&ga_hid=1361912638&ga_fc=1&u_tz=-480&u_his=2&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=-12245933&ady=-12245933&biw=1263&bih=906&scr_x=0&scr_y=0&eid=42530671%2C21068769&oid=3&pvsid=3832476064384589&pem=30&rx=0&eae=2&fc=1920&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7Cs%7C&abl=NS&fu=8192&bc=1&ifi=0&uci=a!0&dtd=378
Preview:	<script>window.sra_later_blocks = [];</script><script>window.sra_later_blocks.push({creative:'',reactiveConfig:{"adClient":"ca-pub-8989771679754051","adFormat":8,"adKey":1812271808,"adWidth":1263,"adHeight":906,"fillMessage":[]},trafficSource:2});</script><script data-jc="39" data-jc-version="r20201203">(function(){/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0 */ function aa(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}function ba(a){if(!(a instanceof Array)){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];a=b?b.call(a):{next:aa(a)};for(var c=[];!(b=a.next()).done;)c.push(b.value);a=c}return a}var fa="function"==typeof Object.create?Object.create:function(a){function b(){}b.prototype=a;return new b},n; if("function"==typeof Object.setPrototypeOf)n=Object.setPrototypeOf;else{var p;a:{var ha={i:!0},ia={};try{ia.__proto__=ha;p=ia.i;break a}catch(a){}p=!1}n=p?function(a,b){a.__proto__=b;if(a.__proto_

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ads[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	405
Entropy (8bit):	5.441110174389376
Encrypted:	false
SSDEEP:	12:hax/XKB0OoLu4UlJ2fR4E+/tFiYSB0Fgdu43o9fZdZrhtFiYG:haoDCfJ2fYVF5Kpp3iZd5F5G
MD5:	65019203CAF94BFC2DD97A7C11A2FC0A
SHA1:	253326F9502A2700F4A7EF2356049978835E69E6
SHA-256:	46DB2594E5DE14DF96DB3E122643E3B0AE8066AF8A699A20C34BA1A040967115
SHA-512:	75EC264039010420554D85744EC3C2BAFFA487F68CCBBE6C6091EC0305DA1734489D21D9516F056EA21806FB10551CFD90D6CED00A38A0024B99268C4AF6705(
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ads[2].htm	
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?guci=1.2.0.0.2.2.0.0&client=ca-pub-8989771679754051&output=html&h=280&adk=3088186576&adf=3175363789&pi=t.aa~a.1255761255~rp.4&w=1200&fwrn=4&fwrnh=100&lmt=1610417347&rafmt=1&to=qs&pwprc=4778228967&psa=1&format=1200x280&url=https%3A%2F%2Fykm.de%2Findex.html&flash=29.0.0&fwr=0&rpe=1&resp_fmts=3&wgl=1&adsid=NT&dt=1610417346856&bpp=22&bdt=514&idt=305&shv=r20201203&cbv=r20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D8b5e4409b88a7409-224663149da600da%3AT%3D1610384913%3ART%3D1610384913%3AS%3DALNI_MaRpNz1-0IYcClgw8Hhh0iIAUFJCA&prev_fmts=0x0&nras=1&correlator=5281413869788&frm=20&pv=1&ga_vid=2041299598.1610417313&ga_sid=1610417347&ga_hid=113105145&ga_fc=0&u_tz=-480&u_his=3&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=32&ady=85&biw=1263&bih=906&scr_x=0&scr_y=0&eid=21068769&oid=3&pvsid=1654621586386755&pem=30&rx=0&eae=0&fc=1920&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7CeE%7C&abl=CS&pfx=0&fu=8320&bc=1&ifi=1&uci=a!1&xpc=chLf4BaLjs&p=https%3A//ykm.de&dtd=378
Preview:	<!DOCTYPE html><html><head><script>window.top.postMessage('{"msg_type":"resize-me","key_value":[{"key":"r_nh","value":"0"},{"key":"qid","value":"CKv9kbavlO4CFdVR4AodZ30EDA"}],"googMsgType":"sth"}', '*');</script><script>window.top.postMessage('{"msg_type":"adsense-labs","key_value":[{"key":"settings","value":"[\\\"ca-pub-8989771679754051\\\",[[1]]]"}],"googMsgType":"sth"}', '*');</script></head></html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ads[3].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	14108
Entropy (8bit):	5.556230132069357
Encrypted:	false
SSDEEP:	384:ToI0MHqR2Baca8ZrPuGiZ1OZmfTiJVfUI:TlHqR2BaQZrWGmcP
MD5:	0FBCB91C2863D070EDBFFBEEC677F74B
SHA1:	BD0E2057823F0815A914018D1633ADEAA0EE175F
SHA-256:	F5DDB7072327B926FD281249441CDD7A14E9F2DF41CE8CDE5600085B24591BB4
SHA-512:	BE73513ECE8E17890F5BB66CE847386857E0C4BC7E53BB7C12681DA18131DE6A4EB7E4ABA570C5F011D89348D0C21403FBA0FD86ECD50C128F840842ECEDE548
Malicious:	false
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?guci=1.2.0.0.2.2.0.0&client=ca-pub-8989771679754051&output=html&adk=1812271804&adf=3025194257&lmt=1610417360&plat=1%3A32776%2C2%3A32776%2C9%3A32776%2C10%3A32%2C11%3A32%2C16%3A8388608%2C17%3A32%2C24%3A32%2C25%3A32%2C30%3A1081344%2C32%3A32%2C40%3A32&format=0x0&url=https%3A%2F%2Fykm.de%2Frecent_urls.html&ea=0&flash=29.0.0&pra=5&wgl=1&dt=1610417360304&bpp=76&bdt=587&idt=259&shv=r20201203&cbv=r20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D8b5e4409b88a7409-224663149da600da%3AT%3D1610384913%3ART%3D1610384913%3AS%3DALNI_MaRpNz1-0IYcClgw8Hhh0iIAUFJCA&nras=1&correlator=464880232668&frm=20&pv=2&ga_vid=2041299598.1610417313&ga_sid=1610417361&ga_hid=361796023&ga_fc=1&u_tz=-480&u_his=7&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=-12245933&ady=-12245933&biw=1280&bih=906&scr_x=0&scr_y=0&eid=21068769&oid=3&pvsid=1862184718256542&pem=30&rx=0&eae=2&fc=1920&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7Cs%7C&abl=NS&fu=8192&bc=1&ifi=0&uci=a!0&dtd=347
Preview:	<script>window.sra_later_blocks = [];</script><script>window.sra_later_blocks.push({creative:'',reactiveConfig:{"adClient":"ca-pub-8989771679754051","adFormat":8,"adKey":1812271808,"adWidth":1280,"adHeight":906,"fillMessage":[]},trafficSource:2});</script><script data-jc="39" data-jc-version="r20201203">(function(){/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0 */ function aa(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}function ba(a){if(!(a instanceof Array)){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];a=b?b.call(a):{next:aa(a)};for(var c=[];!(b=a.next()).done;)c.push(b.value);a=c}return a}var fa="function"==typeof Object.create?Object.create:function(a){function b(){}b.prototype=a;return new b},n; if("function"==typeof Object.setPrototypeOf)n=Object.setPrototypeOf;else{var p;a:{var ha={i:!0},ia={};try{ia.__proto__=ha;p=ia.i;break a}catch(a){}p=!1}n=p?function(a,b){a.__proto__=b;if(a.__proto_

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ads[4].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	3166
Entropy (8bit):	4.663077055101726
Encrypted:	false
SSDEEP:	48:0hOji9IzM0xTn5YuVR4QARJxRlWrwJxUTmWfWR:TN/JnbVqQAJR0rwJxUTs
MD5:	FFC05C21EE29B5935567EC6F9D49AA9A
SHA1:	8547E775F79A6C30D58E3321E85158657045D158
SHA-256:	BBB482B766186E2550D8C640BE59961AF9A8A7CB8141F462147BA1B1822FEB29
SHA-512:	582268646E233EC3D6F4FC1ADB3D5C73F5F09C3A69D6B362622D029CCB61188514377C6AD163E507BBCBB5BAD78B2DABDAC6BA45B5EE50607C127F5FFD42098
Malicious:	false
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?guci=1.2.0.0.2.2.0.0&client=ca-pub-8989771679754051&output=html&adk=1812271804&adf=3025194257&lmt=1610417363&plat=1%3A32776%2C2%3A32776%2C9%3A32776%2C10%3A32%2C11%3A32%2C16%3A8388608%2C17%3A32%2C24%3A32%2C25%3A32%2C30%3A1081344%2C32%3A32%2C40%3A32&format=0x0&url=https%3A%2F%2Fykm.de%2Fmember_login.html&ea=0&flash=29.0.0&pra=5&wgl=1&dt=1610417362885&bpp=27&bdt=546&idt=197&shv=r20201203&cbv=r20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D8b5e4409b88a7409-224663149da600da%3AT%3D1610384913%3ART%3D1610384913%3AS%3DALNI_MaRpNz1-0IYcClgw8Hhh0iIAUFJCA&nras=1&correlator=3237432082960&frm=20&pv=2&ga_vid=2041299598.1610417313&ga_sid=1610417363&ga_hid=40148678&ga_fc=1&u_tz=-480&u_his=8&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=-12245933&ady=-12245933&biw=1280&bih=906&scr_x=0&scr_y=0&eid=21068083%2C21068769%2C21069109&oid=3&pvsid=3325573467270068&pem=30&rx=0&eae=2&fc=1920&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7Cs%7C&abl=NS&fu=8192&bc=1&ifi=0&uci=a!0&dtd=278

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ads[4].htm	
Preview:	<!doctype html><html><head></head><body></body></html><script>var apcnf = '{"googMsgType":"apcnf","config":"[[[[null,0,null,[],null,null,\\\"BODY\\\"],2,[\\\"10px\\\",\\\"10px\\\",true],[4],null,[],[],1,[],[],[]],[[null,0,null,[],null,null,\\\"DIV.top_line\\\"],4,[\\\"10px\\\",\\\"10px\\\",true],[4],null,[],[],1,[],[],[]],[[null,0,null,[],null,null,\\\"DIV.page_head\\\"],4,[\\\"10px\\\",\\\"10px\\\",true],[2],null,[],[],1,[],[],[]],[[null,0,null,[],null,null,\\\"DIV.tag_line\\\"],4,[\\\"30px\\\",\\\"10px\\\",true],[2],null,[],[],1,[],[],[]],[[null,0,null,[],null,null,\\\"BODY\\\"],3,[\\\"10px\\\",\\\"10px\\\",true],[2],null,[],[],1,[],[],[]],[[null,0,null,[],null,null,\\\"DIV.main_content_area\\\\u003eDIV.container\\\\u003eDIV.row\\\\u003eDIV\\\\u003eDIV.alert.alert-error\\\"],4,[\\\"10px\\\",\\\"21.7391px\\\",true],[2],null,[],[],1,[],[],[]],[[null,0,null,[],null,null,\\\"DIV.main_content_area\\\\u003eDIV.container\\\\u003eDIV.row\\\\u003eDIV\\\\u003eDIV.row\\\"],4,[\\\"10px\\\",\\\"1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ads[5].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	405
Entropy (8bit):	5.414111767810088
Encrypted:	false
SSDEEP:	12:hax/XKB0OoLu4UlJ2fR0STtFiYSB0Fgdu43o9fZdZrhtFiYG:haoDCfJ2f9hF5Kpp3iZd5F5G
MD5:	B1D32081B8B9DBFC2E51C2280C0A8541
SHA1:	C71CAFF1EB606FA811883B79F009667A97E6AD95
SHA-256:	B5B169670BF5496037938435E8A26FC05A2220B3E07182EE4321C5694B29F478
SHA-512:	799EE12E0A0A8556F9B61180F9AAC6CCF5D5E3048D7869C33D98DD0EDA10661A7CA01B97D985AF2EF0720F5013C7122D22174402BAC92C5B3D7BBD9B367652A4
Malicious:	false
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?guci=1.2.0.0.2.2.0.0&client=ca-pub-8989771679754051&output=html&h=280&adk=3088186576&adf=3175363789&pi=t.aa~a.1255761255~rp.4&w=1200&fwrn=4&fwrnh=100&lmt=1610417367&rafmt=1&to=qs&pwprc=4778228967&psa=1&format=1200x280&url=https%3A%2F%2Fykm.de%2Findex.html%3F_t%3DEnglish%2B%2528en%2529&flash=29.0.0&fwr=0&rpe=1&resp_fmts=3&wgl=1&adsid=NT&dt=1610417366983&bpp=11&bdt=817&idt=249&shv=r20201203&cbv=r20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D8b5e4409b88a7409-224663149da600da%3AT%3D1610384913%3ART%3D1610384913%3AS%3DALNI_MaRpNz1-0IYcClgw8Hhh0iIAUFJCA&prev_fmts=0x0&nras=1&correlator=8142626605308&frm=20&pv=1&ga_vid=2041299598.1610417313&ga_sid=1610417367&ga_hid=1627427382&ga_fc=0&u_tz=-480&u_his=13&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=32&ady=85&biw=1263&bih=906&scr_x=0&scr_y=0&eid=44731609%2C21067213%2C21068769%2C21069710&oid=3&pvsid=2002097160963238&pem=30&rx=0&eae=0&fc=1920&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7CeE%7C&abl=CS&pfx=0&fu=8320&bc=1&ifi=1&uci=a!1&xpc=23MpO6K52T&p=https%3A//ykm.de&dtd=448
Preview:	<!DOCTYPE html><html><head><script>window.top.postMessage('{"msg_type":"resize-me","key_value":[{"key":"r_nh","value":"0"},{"key":"qid","value":"CJHu4r-vlO4CFWavewodK5kF7A"}],"googMsgType":"sth"}', '*');</script><script>window.top.postMessage('{"msg_type":"adsense-labs","key_value":[{"key":"settings","value":"[\\\"ca-pub-8989771679754051\\\",[[1]]]"}],"googMsgType":"sth"}', '*');</script></head></html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\custom[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1470
Entropy (8bit):	4.404026044513129
Encrypted:	false
SSDEEP:	24:EtEo8IXnVCEQG+ZGMR5hDn7RC5CEMbyFqIm4RUpCeoGunlNdynhHUp:EtEo7nVCEU9g5CExFqIm4RUpCeo5lNdl
MD5:	82EC7434A30AAAC78C2254C9A6DD2BD9
SHA1:	9D13544CB5C4D2A21887DE1FCE36673414CAE51F
SHA-256:	08CF37457213462052C6597A2D774BFD0D83400C927C2D973400F89C0E707FA5
SHA-512:	4E40C4A8C11AE3C26EF305D6A361FBB3B27DCE1F5F9CC9FE7F4DBB86DAB00B5844ED72E87D44ECB4981D5A97E00EC42D070AD0AB8424B568C4717B8D8BBBA838
Malicious:	false
IE Cache URL:	http://https://ykm.de/themes/ykm/js/theme/custom.js
Preview:	jQuery.noConflict()(function($){.... // Create the dropdown base.. $("<select />").appendTo("nav");.... // Create default option "Go to..." .. $("<option />", {.. "selected": "selected",.. "value" : "",.. "text" : "Please choose page" .. }).appendTo("nav select");.. //new dropdown menu.. $("nav a").each(function() {.. var el = $(this);.. var perfix = '';.. switch(el.parents().length){.. case(11):.. perfix = '';.. break;.. case(13):.. perfix = '-- ';.. break;.. default:.. perfix = '';.. break;.... }.. $("<option />", {.. "value" : el.attr("href"),.. "text" : perfix + el.text()..}).appendTo("nav select");..... $("nav select").change(function() {.. window.location = $(this).find("option:selected").val();.. });.. });..});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\down[1]	
Malicious:	false
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\error[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	65318
Entropy (8bit):	4.984216586859167
Encrypted:	false
SSDEEP:	768:DrSf5IDJrNPzq2aZwurmWLctQkDaqW26b0JTo2+jM2QsSDx+k49ixfHVkYCkennw:fptur+2qW2lJTo2+jMRHUnktX7B
MD5:	82AB8E3D232B419F328A129BA4E0B2BE
SHA1:	16CA9C7D0B9EE67DDCAF2B73377C0CDEDC7FDD07
SHA-256:	4E23DCB4AD205C9E5831932AC3D09DB814DC1664E0B8516665EC1FC4D89A4CFD
SHA-512:	0D630B115BD98885102C1B3541ECE29923CC93CA070031D16E65BDE3235606A5359F64C7501359A1509DD5C338CBB25F95106986AB1FAB20C0E790C2CF200EB
Malicious:	false
IE Cache URL:	http://https://ykm.de/error.html?e=This+short+url+is+no+longer+active
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "https://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">.<html dir="ltr" lang="en-US">. <head>. <meta charset="utf-8">. <title>Error - YKM.de ✔ Quickly Shorten Url</title>. <meta content="width=device-width, initial-scale=1.0" name="view port">. <meta name="description" content="An error occurred" />. <meta name="keywords" content="error, tiny, url, script, occurred" />. <meta name="copyright" content="Copyright © 2021 - YKM.de ✔ Quickly Shorten Url" />.. styles -->. <link href="https://ykm.de /themes/ykm/styles/css/bootstrap.css" rel="stylesheet"/>. <link href="https://ykm.de/themes/ykm/styles/css/bootstrap-responsive.css" rel="stylesheet"/>. <link href="https://ykm.de/themes/ykm/styles/css/wide_layout.css" rel="stylesheet"/>. <link href="https://ykm.de/themes/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\f[1].txt	
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):	10035
Entropy (8bit):	6.016410080199775
Encrypted:	false
SSDEEP:	192:9wZjVJvxzwRXhpSfsjHVm8r/Wd0EBi+H8SB:+pJBeRaAfraiqB
MD5:	CA2868DDEA7BE26C23852BABE55BC03D
SHA1:	716D04449F4402B6C06CC652224A821B1ECD0E39
SHA-256:	4ED263AD8C1F51F9C78219BF7C8450A26C65E6641A1A551C7A3B2AFA97BD7C4F
SHA-512:	710F7F9746F65CAAA6D3C48A39AA69F9BCF4EB2A61FB8E66017BD5932DEEFFF79C556DB6B9546A3BDF27AD4587D7B5692EEEB1DAC4E507DF0BCEDD43DEE4 3069
Malicious:	false
IE Cache URL:	http://https://pagead2.googlesyndication.com/getconfig/sodar?sv=200&tid=gda&tv=r20201203&st=env
Preview:	{"sodar_query_id":"Eob8X_PZBtOngAfum4OIBg","injector_basename":"sodar2","bg_hash_basename":"YaMN4Oy8AhH-iW3da0J-Nuczn6meMMc-yumwdmwlUIQ","bg _binary":"RPilNgFbO9A5mbOmRPnJH5NAYB7mxC47B/g85oE9Ab7MlAsIxAbDFRc5l2t4Qyv1jAb4zYsxG10M6uEGJvxjY8XzEpuz48jYgZuc00lUUqaNn575pOGDRXLA DAqydkltZtORBOzjGG2qVGPmbqrMshrIUF3sEXUhJ691rLLBxtQu9gLgSwlX7N+HWrq2rfxluDcewkrSaud9MjZPc2VdB4HRugMaHq6k6ygy4AfCpZzDqBLBL/shu0jaOT m3csNNlPmRAFoRc8DfNifRFokq+6fXD5/4wSzrE85nWDfbqk8vL89tjOZOIfjVhHKqknmjVowKAoTti7HIhPDhX0E03dTYuFiqqHEo4yPsG4jG9AU5jxXnqokHdQN6lXp+ O76WrnflcjJi+3Xl/g6f5Vsrb7odwHVP58qUW7Qai6HX+9C52YkSTyHGFgBw+dgPK3tufFm3CqyaFBm18+If0xlv6ebCNYBUbRHohUrtfFF1PI4b3cOP2tLUdqD+QtsEKc 5fmk+Y+TPKFrjwjp8h8qx14RgJmr4PG6MFmBivLTn1IqWkH88luvjwqoTuSAlqcZ3Toepifv/MhWYe7u1W4l0SAbgo0f8dzA334QWvhIHqxj49JRg1H2JcAwpDgKYfVYhm woRZ1upYB4PgOsbtzcR5FAJitFQW5L2iVLXGWwhFZ5r8KoDZnKb5I48N1n9ox7HPvGU8m6E4inndjVpVndbqG84RWM/cmRA1lAb77xBxCGYILYhnjzI0rInKcgNPWwY8x4 6VFsyEhAH5TkE9ZeZkf3gRGJXUjNLIWNBMYXl1gCDo/ut4WDO64sQ0J30NNE0215outY3LdAJb/5MvsG

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\f[2].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	135658
Entropy (8bit):	5.527456277707522
Encrypted:	false
SSDEEP:	3072:5SocAkHlGEk9PfRUoKcXPao1i7lHjeidOR2:upoOKcCMi7lDeBR2
MD5:	EBBB9B99F39DD8DD5B87F4A6563053A9
SHA1:	9B1B0A438F72CB73172304086E79B45269BDE70D
SHA-256:	CA1EA37E2772D92801DB83691BFD5FF2395CA21C5AFA6E650BF0EBB32F501C38
SHA-512:	00E91619964832642B983AEFEDA9D1CBBAF68E2B9062A751DECDE2292407E3E1CDFD6C9056087EB9618A765C32D0FC22F6A785BDFAE963913FD4F80C01679C C
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\f[2].txt	
Preview:	(function(){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .var n;function aa(a){var b=0;return function(){return b<a.length?{don e:!1,value:a[b++]}:{done:!0}}}var ba="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a; a[b]=c.value;return a}; .function ca(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}var da=ca(this),ea="function"===typeof Symb ol&&"symbol"===typeof Symbol("x"),q={},fa={};function t(a,b){var c=fa[b];if(null==c)return a[b];c=a[c];return void 0!==c?c:a[b]} .function x(a,b,c){if(b)a:{var d=a.split(".");a=1===d.length;var e=d[0],f;!a&&e in q?f=q:f=da;for(e=0;e<d.length-1;e++){var g=d[e];if(!(g in f))break a;f=f[g]}d=d[d.length-1];c=ea&&"es6"===c?f[d]:null;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\faq[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	67815
Entropy (8bit):	4.979610005460299
Encrypted:	false
SSDEEP:	768:0HSf5IDJrNPzq2aZwurmWLctQkDaqW26b0JTo2+jM2QsSDx+k49ixfHVkYCkennA:0Hptur+2qW2lJTo2+jMRHUnk4h4X7B
MD5:	83476F85DE708E1ABD64D58E4226C684
SHA1:	0A6CC0CF350B7E7F4C0E2FA8D350D3C3F946E6DB
SHA-256:	AE96DFB24041AB9570E233789FAF56474505B261C13185DBC87B912460091169
SHA-512:	B568744C0770847C205A4D299C7003925BD0FE9722380C41340DA49654ABB344E33B39DAADAB9419BA5A9393E40C6D00CED948B465AFE9FADE38E562BCD16F8 F
Malicious:	false
IE Cache URL:	http://https://ykm.de/faq.html
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "https://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">.<html dir="ltr" lang="en-US">. <head>. <meta charset="utf-8">. <title>FAQ - YKM.de ✔ Quickly Shorten Url</title>. <meta content="width=device-width, initial-scale=1.0" name="viewpo rt">. <meta name="description" content="Frequently Asked Questions" />. <meta name="keywords" content="faq, frequently, asked, questions, short, url, site" />. <meta name="copyright" content="Copyright © 2021 - YKM.de ✔ Quickly Shorten Url" />.. styles -->. <link href=" https://ykm.de/themes/ykm/styles/css/bootstrap.css" rel="stylesheet"/>. <link href="https://ykm.de/themes/ykm/styles/css/bootstrap-responsive.css" rel="sty lesheet"/>. <link href="https://ykm.de/themes/ykm/styles/css/wide_layout.css" rel="stylesheet"/>. <link href

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\font-awesome.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	23757
Entropy (8bit):	4.758786109395766
Encrypted:	false
SSDEEP:	192:nqHtZX8W+ab2edrKeTUKuErArKlcZJVrJ3ee+cR6waYm215bvfhf5DrkHUasT:is5yWeTUKb+KlkJ5de2UYmyTfhYUasT
MD5:	FBAB9BD833DFD405FE5119ACC3AD60B8
SHA1:	70E968A95DE272546B8D4155F08DD186920B1438
SHA-256:	53486122A592B9C53DA3905FDF3447489D9CFE384A5F119E84BEB2A3A1DF2EA5
SHA-512:	9133B3EE57AB6F13BE5C284FC4F93076E34ED32A55FF1EEB29C6555FF290A56D04C45301E1DAE331D7CD9690F006FD987B0F28810AABFE741DC65D55B6A5D69 9
Malicious:	false
IE Cache URL:	http://https://ykm.de/themes/ykm/styles/css/font-awesome.min.css
Preview:	/*!. * Font Awesome 4.3.0 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */@font-face{font-family:'FontAwesome';src:url('../../fonts/fontawesome-webfont.eot?v=4.3.0');src:url('../../fonts/fontawesome-webfont.eot?#iefix&v=4.3.0') format('emb edded-opentype'),url('../../fonts/fontawesome-webfont.woff2?v=4.3.0') format('woff2'),url('../../fonts/fontawesome-webfont.woff?v=4.3.0') format('woff'),url('../../fonts/ fontawesome-webfont.ttf?v=4.3.0') format('truetype'),url('../../fonts/fontawesome-webfont.svg?v=4.3.0#fontawesomeregular') format('svg');font-weight:normal;font-style:nor mal}.fa{display:inline-block;font:normal normal normal 14px/1 FontAwesome;font-size:inherit;text-rendering:auto;-webkit-font-smoothing:antialiased;-moz-osx-font- smoothing:grayscale;transform:translate(0, 0)}.fa-lg{font-size:1.33333333em;line-height:.75em;vertical-align:-15%}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\httpErrorPagesScripts[1]	
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jflickrfeed.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	1731
Entropy (8bit):	5.1282546572483225
Encrypted:	false
SSDEEP:	48:U7TGMFvLAmzFXIJ1CVK/lV463kG7M1DxErroUaf6:U7aMFvLAmzhKDxkG7M1DxEr9
MD5:	EDDDF66884FE1A84ED2BFADF5DE6B61C
SHA1:	CD8B2CDC1137045FD67FDD1CF3CAD81E2752B717
SHA-256:	7331E568D44900F570F233A6CC0022A6A8F272F6FDABCAE6DDC2092FE1C00C1A
SHA-512:	74B63994F53A8964CD48B520165D62679E5B1A88DA17CD54E2DB32C87F1EDC3A6E7EE68F9F4FF5B2C29D7D75B38CDAD2BC0AF80CBEE2F50EDE9F41D91BE3F17E
Malicious:	false
IE Cache URL:	http://https://ykm.de/themes/ykm/js/theme/jflickrfeed.min.js
Preview:	/*..* Copyright (C) 2009 Joel Sutherland..* Licenced under the MIT license..* http://www.newmediacampaigns.com/page/jquery-flickr-plugin..*..* Available tags for templates:..* title, link, date_taken, description, published, author, author_id, tags, image*..*/..(function($){$.fn.jflickrfeed=function(settings,callback){settings=$.extend(true,{flickrbase:'http://api.flickr.com/services/feeds/',feedapi:'photos_public.gne',limit:20,qstrings:{lang:'en-us',format:'json',jsoncallback:'?'},cleanDescription:true,useTemplate:true,itemTemplate:'',itemCallback:function(){}},settings);var url=settings.flickrbase+settings.feedapi+'?';var first=true;for(var key in settings.qstrings){if(!first)..url+='&';url+=key+'='+settings.qstrings[key];first=false;}..return $(this).each(function(){var $container=$(this);var container=this;$.getJSON(url,function(data){$.each(data.items,function(i,item){if(i<settings.limit){if(settings.cleanDescription){var regex=/<p>(.*?)<\/p>/g;var input=item.description;if(regex.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery.autosize-min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2122
Entropy (8bit):	5.335066184702954
Encrypted:	false
SSDEEP:	48:UUCzaxmriWU3Tp7sryHyw8hd1o8tvVpZVIbGX3VR7vcDwESO:DCzrwjp7srw+7bHZKbgnrcUVO
MD5:	B5C0EF55A224ABF5047E9DC3B4FC1225
SHA1:	83149C43EFFB6156970D096EF45C64D185A1A1FC
SHA-256:	0DB91532815790FA85AE602886D621FB2BD429BA2C9C85AAC1D31751E3FDBADB
SHA-512:	3BB5D44F2C7F81377FA301D5852B325C86245B3E2852C0767471474DF92DF7F8E7593A3660BD4A6F3AB9AA7F31730C1236D5E957514D16B25DB3AF8B8BDE5D3
Malicious:	false
IE Cache URL:	http://https://ykm.de/themes/ykm/js/jquery.autosize-min.js
Preview:	/*!..jQuery Autosize v1.16.7..(c) 2013 Jack Moore - jacklmoore.com..updated: 2013-03-20..license: http://www.opensource.org/licenses/mit-license.php.*/.(function(e){var t,o,n={className:"autosizejs",append:"",callback:!1},i="hidden",s="border-box",a="lineHeight",l='<textarea tabindex="-1" style="position:absolute; top:-999px; left:0; right:auto; bottom:auto; border:0; -moz-box-sizing:content-box; -webkit-box-sizing:content-box; box-sizing:content-box; word-wrap:break-word; height:0 !important; min-height:0 !important; overflow:hidden;"/>',r=["fontFamily","fontSize","fontWeight","fontStyle","letterSpacing","textTransform","wordSpacing","textIndent"],c="oninput",h="onpropertychange",p=e(l).data("autosize",!0)[0];p.style.lineHeight="99px","99px"===e(p).css(a)&&r.push(a),p.style.lineHeight="",e.fn.autosize=function(a){return a=e.extend({},n,a||{}),p.parentNode!==document.body&&(e(document.body).append(p),p.value="\n\n\n",p.scrollTop=9e4,t=p.scrollHeight===p.scrollTop+p.clientHeight),this.e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery.dataTables.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	69604
Entropy (8bit):	5.377786670862721
Encrypted:	false
SSDEEP:	1536:9Wbx6yktBJR6wIsJLl8Td/7oHfCkYQJtpG3:EOMoa
MD5:	737F853E9FD6A31D62F5028E88663C9F
SHA1:	CF144F2AB49F53A69FBFE10D3588FC23437D2736
SHA-256:	6C3CA64B7ACFDD29B3CA6F1B9B46696369ABD462D4546182085C347F72211841
SHA-512:	C148B09FBA278EA4A75F57817A8BE87ABD06F9A6D9A46A23619A32A4BCD4CA4AC89E73D969ECD359BFB2B6B09C7A25E6F5BEC05B9435928F585847C47026D9C
Malicious:	false
IE Cache URL:	http://https://ykm.de/themes/ykm/js/jquery.dataTables.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery.dataTables.min[1].js	
Preview:	/*. * File: jquery.dataTables.min.js. * Version: 1.8.0. * Author: Allan Jardine (www.sprymedia.co.uk). * Info: www.datatables.net. * . * Copyright 2008-2011 Allan Jardine, all rights reserved.. *. * This source file is free software, under either the GPL v2 license or a. * BSD style license, as supplied with this software.. * . * This source file is distributed in the hope that it will be useful, but . * WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY . * or FITNESS FOR A PARTICULAR PURPOSE. See the license files for details.. */.(function(i,wa,p){i.fn.dataTableSettings=[];var D=i.fn.dataTableSettings;i.fn.dataTableExt={};var o=i.fn .dataTableExt;o.sVersion="1.8.0";o.sErrMode="alert";o.iApiIndex=0;o.oApi={};o.afnFiltering=[];o.aoFeatures=[];o.ofnSearch={};o.afnSortData=[];o.oStdClasses={sPa gePrevEnabled:"paginate_enabled_previous",sPagePrevDisabled:"paginate_disabled_previous",sPageNextEnabled:"paginate_enabled_next",sPageNextDisabled:"p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\plus_icon[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 25 x 25, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1109
Entropy (8bit):	7.721087930383875
Encrypted:	false
SSDEEP:	24:igbkIviVBfjhqJ62Aan+JDTCy6s+SoxdP8NA:iGkIviVBfjh467N5ZFoxdPF
MD5:	5E2E68BFB694C0E19F505FEA933FA54D
SHA1:	7DC975D8EE927EF6619AD5E73554685525B67C6A
SHA-256:	19820A113BB1D006964AC41987870D4888583C97D0BBCC5171B3A729428541DB
SHA-512:	5525A80E7019C3240F15F724A624C389FA0AABF129B2D3B488DD221A2C55B2887D99C2FE4C3A7BC3E648F3A0C97A5F0F656E523D4E9BAF8123DED955B740951
Malicious:	false
IE Cache URL:	http://https://ykm.de/themes/ykm/images/plus_icon.png
Preview:	.PNG.....IHDR.....c....sBIT....|.d.....pHYs.....~.....tEXtCreation Time.18/01/2010..H....tEXtSoftware.Adobe FireworksO..N....IDATH...K..U....V..t.$31!.....B@..9 t.&.p.F.5_@D..\..\...q'.P...3d.....:...3!...s...=...s.yHDp..@n\.....8V..O.....M.u..kq.,N}..0..>~..{...%.... .d...z..i..'m..-=^... D..x8..$.6...8.=QE.C..<.(.D.P*...#.]T.s...j....P.H)a.8.....m. <G..w342.zz/$...B#cf....i.F.B-..Q<..<.K..;.-:..(..rc...p..aN.....xK.4..... uJl.<a...,...o....I*..!.$""B...._.)...b.$.aT.(.pe]}...vU.z...."<,,=Z....T/]y..v.T.....y.....F.....6.....Q. 0/\|..+u.2m..U.x4.....!d<.....ax8..4.Q...Y...;./.3.k...7O%Z...(...3.c(. ...%..t...wA...p.6.w/..6..v.%.yH6.Qo.!.'p....@[..q.....=..j.)s.e..c.P\|.{!pD...#O....0..la.u1....h,.X...i...@.....8/(j^.%....im.y...t.I..Mg.*.....M$`..X.|P.....}...Y..."..dgg....q..r..8..F.u..=...2"Hmn...?~<..zE..Z.H.#.y.R...D..$.....8l.....Y._.pvG.....`.u..D#a.....X .&EM.5.. ..5..I.<.i%U

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\runner[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	12318
Entropy (8bit):	5.314497117961088
Encrypted:	false
SSDEEP:	192:I7UTGaZMNZU5mFCD+hgnFGzb90VzsiKvWJ9jkyN88:y4AFcZn8F0VzseJQ8
MD5:	892009D341852C0AE2F39AAADC568D6C
SHA1:	B645A3A8CD30464433BAA0ABEE04396D5BDE0525
SHA-256:	E46E226858CB1C57593472A14B545F60F1A7CD2BE103EB0F711917A4F2A01308
SHA-512:	4B7ACD8B3C7E89CFFA18C6BBDF31EF317EAB82CCE271D93133E6DD71EE0B5DEA5E8A4FA51DBCB0D10F00B46E501750AEFA263A66FB2F18F562D8666C3892C E5A
Malicious:	false
IE Cache URL:	http://https://tpc.googlesyndication.com/sodar/sodar2/220/runner.html
Preview:	<!DOCTYPE html>.<meta charset=utf-8><script>.(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.'use strict';function m(a) {var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}function p(a){var b="undefined"!=typeof t.Symbol&&u(t.Symbol,"iterator")&&a[u(t.Symb ol,"iterator")];return b?b.call(a):{next:m(a)}}var aa="function"==typeof Object.create?Object.create:function(a){function b(){}b.prototype=a;return new b},v="function"==t ypeof Object.defineProperties?Object.defineProperty:function(a,b,d){if(a==Array.prototype||a==Object.prototype)return a;a[b]=d.value;return a};.function ba(a){a=["object" ==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var d =a[b];if(d&&d.Math==Math)return d}throw Error("Cannot find global object");}var w=ba(this),x="function"===typeof Symbol&&"symbol"===typeof Symbol("x"),t={},y={} ;function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\KQGQMC7O.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	465
Entropy (8bit):	5.314069571660964
Encrypted:	false
SSDEEP:	12:hYzx7BqhCnmr7ctQtqqJmrLgFBQt+4Nbx8oA2HVt:hYzxBqhCY42RIt+4NBA2b
MD5:	88BF24642893F2E9F7592E0FD3464D46
SHA1:	2C543C8DA2D86ABF50B007B07E8DB8EE8F6F82ED
SHA-256:	D326EED23F9D217734D32A76AD6448D9769AD9441A37A30CE3134877636F0DFA
SHA-512:	0B166D21BF489225D2BBCAEAD4468150FC2D02E8ACDC33436582D3E779F1E70438F7A1B4F9E2E264E00155FC3307AB1D2A19A8A3247B588DDC46C44D5949115
Malicious:	false
IE Cache URL:	http://https://href.li/?https://ykm.de/65f0a4768a364c17
Preview:	<!DOCTYPE html>.<html><head>.<title>href.li</title>.<meta http-equiv="Refresh" content="0; url=https://ykm.de/65f0a4768a364c17" />.<meta name="referrer" content ="no-referrer" />.<script type="text/javascript">./* <![CDATA[*/.window.location.replace("https:\/\/ykm.de\/65f0a4768a364c17" + window.location.hash);./* */.</script>. </head>.<body> Redirecting.. https://ykm.de/65f0a4768a364c17 </body></html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\PRmiXeptR36kaC0GEAetxh_xHqYgAV9Bl_ZQbYUxnQU[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 21524, version 1.1
Category:	downloaded
Size (bytes):	21524
Entropy (8bit):	7.968787463619674
Encrypted:	false
SSDEEP:	384:xUtz2PcceIA3bILf1sBZc6wUYkFtB+e+YTr6/UGVA7HCshb6dddddvXTR+Vw:xUtSUc8kf1eZzdntB2YKbVAmIb0U2
MD5:	C7BDA75B1D04DD8C00F5E057D3489E21
SHA1:	7C183A9BB69A412B6BC9D4FD0D51056C6168AE56
SHA-256:	630D5A53820A8FEC8C0C4583F1A276DF0A8FB41091D448E0162CB50A80053B4E
SHA-512:	52261BBDE700D3C5E437BAB485FDD0CD15F3BF806DDD45F5630D57D12BA39CD22EF32F1C22CCA467965ECE6B2588430BA0817A6A3BAB3A7178329212BB5A95B2
Malicious:	false
IE Cache URL:	http://https://themes.googleusercontent.com/static/fonts/opensans/v6/PRmiXeptR36kaC0GEAetxh_xHqYgAV9Bl_ZQbYUxnQU.woff
Preview:	wOFF.....T.....FFTM...l.....\..OS/2.....^...`..hcmap.....h.....cvt ...P...^.....M..fpgm.....~a..gasp...\.....#glyf...l..3...J@..1_head..;....3...6....hhea..<0...!...$.(..hmtx..<T...*...XK?L3kern..>.....#.....loca..L.....z.i,maxp..ND... ... .t..name..Nd...%.....s.post..Q....y....l..prep..S.....$...J.....o1.....cl.....^x.c`f.....:....Q.B3_dHcb.`b.ffcfeabby....A!...A.....ah..e.P``...c.g....\.~.....x.c```f.`..F..X..1.,.....:.....L.n1.Q.Q.R.SPR.RpQ(QX..?X.... ..a.....K.....?.....}.`.M.6>X.`.....4.....l.pe.L@..]..+,.l...\.<.|...B.".b...R.2.r...J.*.j...Z.::z...F.&.f...V.6.v...N...n...^.>.~...A.!.a...Q.1.q....m..g.[.h...W.^.f..u.6n.e..{v...P...y.baA6CY.C.,.b...r..rj.V.jL...sk...Z..>r...s.N.d8.p...K@..3..Zz.{..'L.:.a.....=^..p..(...K{.x.c.a.g.c.. .P...,..`....b`....C..D@$P..)._.....a .p@.0.(.@.8. ..0....a8.....x.uU.S.F....."S.0.!.n..`.t..@)lm..u.b.3+.A"&cz.C...H

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ads[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	14108
Entropy (8bit):	5.556388878043573
Encrypted:	false
SSDEEP:	192:TtjY0I6p44JlVyjORGpM8O6njXIVhSa0pZrPhoG8FZ7BGUSczOZeYmfJ5iJRLJxP:TG0MHqR2Baca8ZrPuGiZ1OZmfTiJVfUI
MD5:	524C4EB9FD782257406546FF4F14F138
SHA1:	DCC91AFF7289F7743B2BB8BDA1D58B528530C015
SHA-256:	0D23F4A226212BD190A27972F8DCCD95180C79AFD6BC1AF982DE12722E1454D1
SHA-512:	1AEDEC383BD77152B8DDCE5E1D2E1ABB97E0B9B53E213E491F09B6D769D53C68CBBAF6A5F23E871A957AF3668611AEB7EE14D984160D25AE85CA084559E9901A
Malicious:	false
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?guci=1.2.0.0.2.2.0.0&client=ca-pub-8989771679754051&output=html&adk=1812271804&adf=3025194257&lmt=1610417349&plat=1%3A32776%2C2%3A32776%2C9%3A32776%2C10%3A32%2C11%3A32%2C16%3A8388608%2C17%3A32%2C24%3A32%2C25%3A32%2C30%3A1081344%2C32%3A32%2C40%3A32&format=0x0&url=https%3A%2F%2Fykm.de%2Fregister.html&ea=0&flash=29.0.0&pra=5&wgl=1&dt=1610417348751&bpp=37&bdt=482&idt=181&shv=r20201203&cbv=r20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D8b5e4409b88a7409-224663149da600da%3AT%3D1610384913%3ART%3D1610384913%3AS%3DALNI_MaRpNz1-0IYcClgw8Hhh0iIAUFJCA&nras=1&correlator=6343227133430&frm=20&pv=2&ga_vid=2041299598.1610417313&ga_sid=1610417349&ga_hid=488988360&ga_fc=1&u_tz=-480&u_his=4&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=-12245933&ady=-12245933&biw=1263&bih=906&scr_x=0&scr_y=0&eid=21068769%2C21068945&oid=3&pvsid=387605769970244&pem=30&rx=0&eae=2&fc=1920&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7Cs%7C&abl=NS&fu=8192&bc=1&ifi=0&uci=a!0&dtd=341
Preview:	<script>window.sra_later_blocks = [];</script><script>window.sra_later_blocks.push({creative:'',reactiveConfig:{"adClient":"ca-pub-8989771679754051","adFormat":8,"adKey":"1812271808,"adWidth":1263,"adHeight":906,"fillMessage":[]},trafficSource:2});</script><script data-jc="39" data-jc-version="r20201203">(function(){/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0 */ function aa(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}function ba(a){if(!(a instanceof Array)){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];a=b?b.call(a):{next:aa(a)};for(var c=[];!(b=a.next()).done;)c.push(b.value);a=c}return a}var fa="function"==typeof Object.create?Object.create:function(a){function b(){}b.prototype=a;return new b},n; if("function"==typeof Object.setPrototypeOf)n=Object.setPrototypeOf;else{var p;a:{var ha={i:!0},ia={};try{ia.__proto__=ha;p=ia.i;break a}catch(a){}p=!1}n=p?function(a,b){a.__proto__=b;if(a.__proto_

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ads[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	405
Entropy (8bit):	5.446669463410376
Encrypted:	false
SSDEEP:	12:hax/XKB0OoLu4UlJ2fRqitFiYSB0Fgdu43o9fZdZrhtFiYG:haoDCfJ2fdF5Kpp3iZd5F5G
MD5:	4C1A813F381606F5AA9A15C99FC7777B
SHA1:	B57AD3878F5CACACCA2BCC34F727231B2C86643A
SHA-256:	6A82422D188A97B0A571AC79818E4FF580141BE71B165E20CD04547F3ECE2585
SHA-512:	0F5177D911E9A55BBA2EC8355A0604344F6D1966257BAC8F4B6B3D58869AB64ED7F6DC3EC00E916F8CE5BEB98EB1F9B7A4746D151F3E47B3ED1A2C36E26FC5E
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ads[2].htm	
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?guci=1.2.0.0.2.2.0.0&client=ca-pub-8989771679754051&output=html&h=280&adk=3088186576&adf=3175363789&pi=t.aa~a.1255761255~rp.4&w=1200&fwrn=4&fwrnh=100&lmt=1610417349&rafmt=1&to=qs&pwprc=4778228967&psa=1&format=1200x280&url=https%3A%2F%2Fykm.de%2Fregister.html&flash=29.0.0&fwr=0&rpe=1&resp_fmts=3&wgl=1&adsid=NT&dt=1610417348788&bpp=10&bdt=515&idt=314&shv=r20201203&cbv=r20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D8b5e4409b88a7409-224663149da600da%3AT%3D1610384913%3ART%3D1610384913%3AS%3DALNI_MaRpNz1-0IYcClgw8Hhh0iIAUFJCA&prev_fmts=0x0&nras=1&correlator=6343227133430&frm=20&pv=1&ga_vid=2041299598.1610417313&ga_sid=1610417349&ga_hid=488988360&ga_fc=0&u_tz=-480&u_his=4&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=32&ady=85&biw=1263&bih=906&scr_x=0&scr_y=0&eid=21068769%2C21068945&oid=3&pvsid=387605769970244&pem=30&rx=0&eae=0&fc=1920&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7CeE%7C&abl=CS&pfx=0&fu=8320&bc=1&ifi=1&uci=a!1&xpc=hZWRzNH2jw&p=https%3A//ykm.de&dtd=400
Preview:	<!DOCTYPE html><html><head><script>window.top.postMessage('{"msg_type":"resize-me","key_value":[{"key":"r_nh","value":"0"},{"key":"qid","value":"COzZiLevlO4CFRfG7Qod744N3w"}],"googMsgType":"sth"}', '*');</script><script>window.top.postMessage('{"msg_type":"adsense-labs","key_value":[{"key":"settings","value":"[\\\"ca-pub-8989771679754051\\\",[[1]]]"}],"googMsgType":"sth"}', '*');</script></head></html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ads[3].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	14108
Entropy (8bit):	5.556388878043573
Encrypted:	false
SSDEEP:	192:TtjY0I6p44JlVyjORGpM8O6njXIVhSa0pZrPhoG8FZ7BGUSczOZeYmfJ5iJRLJxP:TG0MHqR2Baca8ZrPuGiZ1OZmfTiJVfUI
MD5:	524C4EB9FD782257406546FF4F14F138
SHA1:	DCC91AFF7289F7743B2BB8BDA1D58B528530C015
SHA-256:	0D23F4A226212BD190A27972F8DCCD95180C79AFD6BC1AF982DE12722E1454D1
SHA-512:	1AEDEC383BD77152B8DDCE5E1D2E1ABB97E0B9B53E213E491F09B6D769D53C68CBBAF6A5F23E871A957AF3668611AEB7EE14D984160D25AE85CA084559E9901A
Malicious:	false
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?guci=1.2.0.0.2.2.0.0&client=ca-pub-8989771679754051&output=html&adk=1812271804&adf=3025194257&lmt=1610417367&plat=1%3A32776%2C2%3A32776%2C9%3A32776%2C10%3A32%2C11%3A32%2C16%3A8388608%2C17%3A32%2C24%3A32%2C25%3A32%2C30%3A1081344%2C32%3A32%2C40%3A32&format=0x0&url=https%3A%2F%2Fykm.de%2Findex.html%3F_t%3DEnglish%2B%2528en%2529&ea=0&flash=29.0.0&pra=5&wgl=1&dt=1610417366935&bpp=48&bdt=783&idt=188&shv=r20201203&cbv=r20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D8b5e4409b88a7409-224663149da600da%3AT%3D1610384913%3ART%3D1610384913%3AS%3DALNI_MaRpNz1-0IYcClgw8Hhh0iIAUFJCA&nras=1&correlator=8142626605308&frm=20&pv=2&ga_vid=2041299598.1610417313&ga_sid=1610417367&ga_hid=1627427382&ga_fc=1&u_tz=-480&u_his=13&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=-12245933&ady=-12245933&biw=1263&bih=906&scr_x=0&scr_y=0&eid=44731609%2C21067213%2C21068769%2C21069710&oid=3&pvsid=2002097160963238&pem=30&rx=0&eae=2&fc=1920&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7Cs%7C&abl=NS&fu=8192&bc=1&ifi=0&uci=a!0&dtd=272
Preview:	<script>window.sra_later_blocks = [];</script><script>window.sra_later_blocks.push({creative:'',reactiveConfig:{"adClient":"ca-pub-8989771679754051","adFormat":8,"adKey":1812271808,"adWidth":1263,"adHeight":906,"fillMessage":[]},trafficSource:2});</script><script data-jc="39" data-jc-version="r20201203">(function(){/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0 */ function aa(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}function ba(a){if(!(a instanceof Array)){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];a=b?b.call(a):{next:aa(a)};for(var c=[];!(b=a.next()).done;)c.push(b.value);a=c}return a}var fa="function"==typeof Object.create?Object.create:function(a){function b(){}b.prototype=a;return new b},n; if("function"==typeof Object.setPrototypeOf)n=Object.setPrototypeOf;else{var p;a:{var ha={i:!0},ia={};try{ia.__proto__=ha;p=ia.i;break a}catch(a){}p=!1}n=p?function(a,b){a.__proto__=b;if(a.__proto_

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ads[4].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	14108
Entropy (8bit):	5.556230132069357
Encrypted:	false
SSDEEP:	384:ToI0MHqR2Baca8ZrPuGiZ1OZmfTiJVfUI:TlHqR2BaQZrWGmcP
MD5:	0FBCB91C2863D070EDBFFBEEC677F74B
SHA1:	BD0E2057823F0815A914018D1633ADEAA0EE175F
SHA-256:	F5DDB7072327B926FD281249441CDD7A14E9F2DF41CE8CDE5600085B24591BB4
SHA-512:	BE73513ECE8E17890F5BB66CE847386857E0C4BC7E53BB7C12681DA18131DE6A4EB7E4ABA570C5F011D89348D0C21403FBA0FD86ECD50C128F840842ECEDE548
Malicious:	false
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?guci=1.2.0.0.2.2.0.0&client=ca-pub-8989771679754051&output=html&adk=1812271804&adf=3025194257&lmt=1610417369&plat=1%3A32776%2C2%3A32776%2C9%3A32776%2C10%3A32%2C11%3A32%2C16%3A8388608%2C17%3A32%2C24%3A32%2C25%3A32%2C30%3A1081344%2C32%3A32%2C40%3A32&format=0x0&url=https%3A%2F%2Fykm.de%2Findex.html%3F_t%3DDeutsch%2B%2528de%2529&ea=0&flash=29.0.0&pra=5&wgl=1&dt=1610417368907&bpp=78&bdt=381&idt=214&shv=r20201203&cbv=r20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D8b5e4409b88a7409-224663149da600da%3AT%3D1610384913%3ART%3D1610384913%3AS%3DALNI_MaRpNz1-0IYcClgw8Hhh0iIAUFJCA&nras=1&correlator=2042136898454&frm=20&pv=2&ga_vid=2041299598.1610417313&ga_sid=1610417369&ga_hid=18271482&ga_fc=1&u_tz=-480&u_his=14&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=-12245933&ady=-12245933&biw=1280&bih=906&scr_x=0&scr_y=0&eid=42530671%2C21068769%2C21068946&oid=3&pvsid=2852579933633363&pem=30&rx=0&eae=2&fc=1920&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7Cs%7C&abl=NS&fu=8192&bc=1&ifi=0&uci=a!0&dtd=301

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ads[4].htm	
Preview:	<script>window.sra_later_blocks = [];</script><script>window.sra_later_blocks.push({creative:'',reactiveConfig:{"adClient":"ca-pub-8989771679754051","adFormat":8,"adKey":1812271808,"adWidth":1280,"adHeight":906,"fillMessage":[]},trafficSource:2});</script><script data-jc="39" data-jc-version="r20201203">(function(){/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0 */ function aa(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}function ba(a){if(!(a instanceof Array)){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];a=b?b.call(a):{next:aa(a)};for(var c=[];!(b=a.next()).done;)c.push(b.value);a=c}return a}var fa="function"==typeof Object.create?Object.create:function(a){function b(){}b.prototype=a;return new b},n; if("function"==typeof Object.setPrototypeOf)n=Object.setPrototypeOf;else{var p;a:{var ha={i:!0},ia={};try{ia.__proto__=ha;p=ia.i;break a}catch(a){}p=!1}n=p?function(a,b){a.__proto__=b;if(a.__proto_

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bookmarklet[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	67688
Entropy (8bit):	5.00104730175302
Encrypted:	false
SSDEEP:	768:ySf5IDJrNPzq2aZwurmWLctQkDaqW26b0JTo2+jM2QsSDx+k49ixfHVkYCkennap:yptur+2qW2lJTo2+jMRHUnk1X7B
MD5:	DD0ECF49ED8AE46D14265E646AC20416
SHA1:	108200228194F599729DAD117C055DE036CA2B9B
SHA-256:	9623428A90973E3168741CD34A374043533C6474FB0037C558D76FB1CF5B7E82
SHA-512:	FB51FF7A9676C5BED05287273199E0D0A2C02C74B7EDA92083CB2E80A28B7BA5BBF5BFA2FAE20729D6E9C3D27C4732CC5F18E281419C999C0C24B8497DD79D4
Malicious:	false
IE Cache URL:	http://https://ykm.de/bookmarklet.html
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "https://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">.<html dir="ltr" lang="en-US">. <head>. <meta charset="utf-8">. <title>Bookmarklet - YKM.de ✔ Quickly Shorten Url</title>. <meta content="width=device-width, initial-scale=1.0" name="viewport">. <meta name="description" content="Bookmarklet" />. <meta name="keywords" content="bookmarklet, tools, short, url, bookmarklet, api, application, programming, interface, short, url, site" />. <meta name="copyright" content="Copyright © 2021 - YKM.de ✔ Quickly Shorten Url" />.. styles -->. <link href="https://ykm.de/themes/ykm/styles/css/bootstrap.css" rel="stylesheet"/>. <link href="https://ykm.de/themes/ykm/styles/css/bootstrap-responsive.css" rel="stylesheet"/>. <link href="https://ykm.de/themes/ykm/styles/css/wide_layout.css"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";....//used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\exclamation[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	701
Entropy (8bit):	7.537917344298478
Encrypted:	false
SSDEEP:	12:6v/7CLruYCttluR6xaz7NDUP6n2gjrCzl/lC/4WqJSGZH40AC7gxcyWRQyq1:/zCttX6xalUP62YrY9lC/4HJjY0AC5b8
MD5:	E4DD51F46566ED3CEACDC900BF2FDF01
SHA1:	A460CC5CEACA30E0338EA784C6A0A83EFDCFCA31
SHA-256:	C89B56C55B934B1F05EF01D47AA7169B5CA0322C37D1FCF62B067D660EB29F12
SHA-512:	5A2C8A83C8D83B8CF0EA64CE79421B74373F2198938F60BF3218FABD0BD28796FE7812A95FF2A2B3A16D8DEE5F100A6DF10BBEF575EAAFB20DCE5D77AF4A600D
Malicious:	false
IE Cache URL:	http://https://ykm.de/themes/ykm/images/vc/exclamation.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\exclamation[1].png	
Preview:	.PNG.....IHDR.....a....gAMA....7.....tEXtSoftware.Adobe ImageReadyq.e<...OIDAT8...K.a.....SA..oc....6...PD.C.....D....@.Zx.h1.N..."..C.N...:v....f.}.....6uv... y..y.1....=!..4.vCv..$...H.S8d.....*P....M`+..S...n.v~c..H.Vr}....O.....KW...55Bb.`l..`yj`yk.1.Aj...E.....@..E.....oqS.2.F..E....6...4(l=...$6#.1![.?....@Dw$-W....fW.&D.$.F. n>.SR..Ju....Z.NWc#di.....@%.....b_s..R.....^...t&:?.!Dm.S.Q..e.JWe.J.q..MT.....'D....B.....:RE.._.as..3....C2..Vz9W....[...9..w.U....*B4!B..|..z.....PJ.fVc..d.Em...Z..V.w! ...O...p.....zp.!Mu..S..>x.....9.f.0..U..x8...G.Hv.=}..u..G.B...y=.-..Ka..J....8.K.+${.?.....`.....v...L...3.7.....Lj.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\f[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	264759
Entropy (8bit):	5.510025846690705
Encrypted:	false
SSDEEP:	6144:eVBPIYlHjj7AqqIoY/a9HAMW9lCjd5NVdhwJaD:wjHjj7jqIoY/a3MlOd5NVvwJ2
MD5:	C0E5468CC4FA9759A9A598B46332A373
SHA1:	9EE21C4F50688881C561DD76C0A720D59F8500E2
SHA-256:	6FD9072EE947E4D641435B2E0EA0ACA3E5619275936FB6FFF0FDCE4284C169AB
SHA-512:	5021CC885133ADAF2A81E7E49B0FEB13F60EBC2959421EA8112654A8889BB3B60DABC0F4B3FA514A051247B41EA744801EB5A44AF8183F92DF3E4EB0E31223D8
Malicious:	false
IE Cache URL:	http://https://pagead2.googlesyndication.com/pagead/js/r20201203/r20190131/show_ads_impl.js
Preview:	(function(window,document,location){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .var p;function ba(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}var ca="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a}; .function ea(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}var ha=ea(this),ia="function"===typeof Symbol&&"symbol"===typeof Symbol("x"),r={},ka={};function t(a,b){var c=ka[b];if(null==c)return a[b];c=a[c];return void 0!==c?c:a[b]} .function w(a,b,c){if(b)a:{var d=a.split(".");a=1===d.length;var e=d[0],f;!a&&e in r?f=r:f=ha;for(e=0;e<d.length-1;e++){var g=d[e];if(!(g in f))break a;f=f[g]}d=d[d.length-1];c=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\f[2].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	107
Entropy (8bit):	4.687983113383467
Encrypted:	false
SSDEEP:	3:oVewGL34zhoJMd/xC0MId/avHvpHlxfYf:ogwcozOJe/xeq/Ynxwf
MD5:	D9C47F48660B656705D0FF86FC850DE8
SHA1:	BCEB9478F69CDFC2EB87AE6B80E95DBAAC8B6769
SHA-256:	A4A1824DEFEC1084CA81D496EE77891684C26196924BDC4FC21DD3482CE15E14
SHA-512:	0CDE289EAD00BD9B3BDD614FEC5B5EB132FDD0D9EEF5136F7E6EA0081F7D8DBF8144EE90067C8C25C4547FAC4ADC8FEA1B028930C9EDCF023151758BF6671D6A
Malicious:	false
Preview:	processGoogleToken({"newToken":"","validLifetimeSecs":300,"freshLifetimeSecs":300,"1p_jar":"","pucrd":""});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\f[3].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	107
Entropy (8bit):	4.687983113383467
Encrypted:	false
SSDEEP:	3:oVewGL34zhoJMd/xC0MId/avHvpHlxfYf:ogwcozOJe/xeq/Ynxwf
MD5:	D9C47F48660B656705D0FF86FC850DE8
SHA1:	BCEB9478F69CDFC2EB87AE6B80E95DBAAC8B6769
SHA-256:	A4A1824DEFEC1084CA81D496EE77891684C26196924BDC4FC21DD3482CE15E14
SHA-512:	0CDE289EAD00BD9B3BDD614FEC5B5EB132FDD0D9EEF5136F7E6EA0081F7D8DBF8144EE90067C8C25C4547FAC4ADC8FEA1B028930C9EDCF023151758BF6671D6A
Malicious:	false
Preview:	processGoogleToken({"newToken":"","validLifetimeSecs":300,"freshLifetimeSecs":300,"1p_jar":"","pucrd":""});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\f[4].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	12
Entropy (8bit):	3.188721875540867

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\f[4].txt	
Encrypted:	false
SSDEEP:	3:tDKn:tDK
MD5:	124D3918819AB4C349A7F9FA979BEF07
SHA1:	6AD167D76A8768130783CD19AA6D8143C0B1BF37
SHA-256:	DAA795332E5DBCF893ADF2D5F3349F02B8C1CB957FF3B5F4C11B742E33C3376F
SHA-512:	4F7F15B28C6B38FC66002DBEE29688B801A689B716093BA63ADBE23FFFE144621198973A8AC4981FF2D20881BD4C84E45130A631E5B9A5EAE3A5FE26C106F7D(
Malicious:	false
IE Cache URL:	http://https://partner.googleadservices.com/gampad/cookie.js?domain=ykm.de&callback=_gfp_s_&client=ca-pub-8989771679754051&cookie=ID%3D8b5e4409b88a7409-224663149da600da%3AT%3D1610384913%3ART%3D1610384913%3AS%3DALNI_MaRpNz1-0IYcClgw8Hhh0iIAUFJCA
Preview:	_gfp_s_({});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\f[5].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	406810
Entropy (8bit):	5.526906160512109
Encrypted:	false
SSDEEP:	12288:uaOKcLi7lDeBRhanKcLi7lDeBRhanKcLi7lDeBR2:bOpi7lDeBRMnpi7lDeBRMnpi7lDeBR2
MD5:	E98155B0C409B8FCF45F0E1A91601A1F
SHA1:	D4A46C7F13A907C87B7B06E8F814F793598C67C1
SHA-256:	E44CE986B3DB384C20B5E1739EE5D646B2A72BD770E6B2E23F9719E459BBE498
SHA-512:	E6FE9AA840062EF8C9D8A66D6AF58BD033DF8611FBF1F764B8FE50B2F5C41B311106699B80C921F6E86EE4C4E479CAB525A317E4B228DDB7B7F9C13849AAB54 8
Malicious:	false
IE Cache URL:	http://https://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js
Preview:	(function(){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .var n;function aa(a){var b=0;return function(){return b<a.length?{don e:!1,value:a[b++]}:{done:!0}}}var ba="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a; a[b]=c.value;return a}; .function ca(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}var da=ca(this),ea="function"===typeof Symb ol&&"symbol"===typeof Symbol("x"),q={},fa={};function t(a,b){var c=fa[b];if(null==c)return a[b];c=a[c];return void 0!==c?c:a[b]} .function x(a,b,c){if(b)a:{var d=a.split(".");a=1===d.length;var e=d[0],f;!a&&e in q?f=q:f=da;for(e=0;e<d.length-1;e++){var g=d[e];if(!(g in f))break a;f=f[g]}d=d[d.length-1];c=ea&&"es6"===c?f[d]:null;

Static File Info

General

File type:	PDF document, version 1.5
Entropy (8bit):	7.991996531902045
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	Information-Account-Prime-Disable-Service.pdf
File size:	197654
MD5:	7ef4760a44a8cc65c4261a5227fdad25
SHA1:	19af34bf781eb79717cc1db64d3d1923da115fe6
SHA256:	29c631b5ce054c8b4b11fbaa06aa26d5edeb9e06d53315d7eddbe18469b15b20
SHA512:	5950c1c0e62f68ebf3467022c9fa0893b120ba6a832de4f58a3dcf5580387938cf71ed26ea5d0fd7f951cc076959c0b4780784f0cc02ca172b3dd19ae068e8f7
SSDEEP:	3072:XV++GPt/KcCzjYpV5ICPFIi1sUNfHJwcWQeuUtl+v52dVE5LXQtBqSmqWY96Pi3A:X0huj05ICtIDUV+QZUd52mXQDRd6jLj
File Content Preview:	%PDF-1.5..%.....2 0 obj..<</Outlines 4 0 R /AcroForm 5 0 R /Pages 6 0 R /StructTreeRoot 7 0 R /Type/Catalog/MarkInfo 8 0 R /Lang(en-US)>>..endobj..11 0 obj..<</StructParents 0/Resources 17 0 R /MediaBox[0 0 612 792]/Contents[18 0 R 19 0 R 20 0 R]/Pa

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

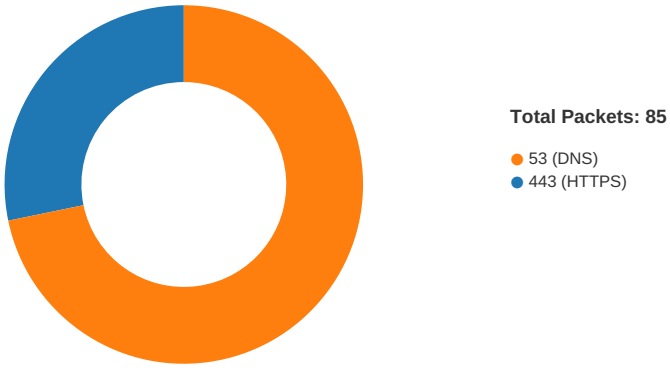
Header:	%PDF-1.5
Total Entropy:	7.991997
Total Bytes:	197654
Stream Entropy:	7.992311
Stream Bytes:	194726
Entropy outside Streams:	5.376200
Bytes outside Streams:	2928
Number of EOF found:	1
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	22
endobj	22
stream	15
endstream	15
xref	0
trailer	0
startxref	1
/Page	1
/Encrypt	0
/ObjStm	3
/URI	0
/JS	0
/JavaScript	0
/AA	0
/OpenAction	0
/AcroForm	1
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:08:29.679091930 CET	49743	443	192.168.2.3	74.114.154.21
Jan 11, 2021 18:08:29.679336071 CET	49744	443	192.168.2.3	74.114.154.21
Jan 11, 2021 18:08:29.811475039 CET	443	49744	74.114.154.21	192.168.2.3
Jan 11, 2021 18:08:29.811723948 CET	49744	443	192.168.2.3	74.114.154.21
Jan 11, 2021 18:08:29.815804005 CET	443	49743	74.114.154.21	192.168.2.3
Jan 11, 2021 18:08:29.815958023 CET	49743	443	192.168.2.3	74.114.154.21
Jan 11, 2021 18:08:29.829678059 CET	49743	443	192.168.2.3	74.114.154.21
Jan 11, 2021 18:08:29.829741955 CET	49744	443	192.168.2.3	74.114.154.21
Jan 11, 2021 18:08:29.961832047 CET	443	49744	74.114.154.21	192.168.2.3
Jan 11, 2021 18:08:29.962877989 CET	443	49744	74.114.154.21	192.168.2.3
Jan 11, 2021 18:08:29.962896109 CET	443	49744	74.114.154.21	192.168.2.3
Jan 11, 2021 18:08:29.962904930 CET	443	49744	74.114.154.21	192.168.2.3
Jan 11, 2021 18:08:29.962965965 CET	49744	443	192.168.2.3	74.114.154.21
Jan 11, 2021 18:08:29.963021994 CET	49744	443	192.168.2.3	74.114.154.21
Jan 11, 2021 18:08:29.966074944 CET	443	49743	74.114.154.21	192.168.2.3
Jan 11, 2021 18:08:29.967022896 CET	443	49743	74.114.154.21	192.168.2.3
Jan 11, 2021 18:08:29.967052937 CET	443	49743	74.114.154.21	192.168.2.3
Jan 11, 2021 18:08:29.967061996 CET	443	49743	74.114.154.21	192.168.2.3
Jan 11, 2021 18:08:29.967145920 CET	49743	443	192.168.2.3	74.114.154.21
Jan 11, 2021 18:08:29.967190981 CET	49743	443	192.168.2.3	74.114.154.21
Jan 11, 2021 18:08:30.007456064 CET	49744	443	192.168.2.3	74.114.154.21
Jan 11, 2021 18:08:30.007581949 CET	49743	443	192.168.2.3	74.114.154.21
Jan 11, 2021 18:08:30.013442039 CET	49744	443	192.168.2.3	74.114.154.21
Jan 11, 2021 18:08:30.013617039 CET	49743	443	192.168.2.3	74.114.154.21
Jan 11, 2021 18:08:30.013752937 CET	49744	443	192.168.2.3	74.114.154.21
Jan 11, 2021 18:08:30.139843941 CET	443	49744	74.114.154.21	192.168.2.3
Jan 11, 2021 18:08:30.139863014 CET	443	49744	74.114.154.21	192.168.2.3
Jan 11, 2021 18:08:30.140055895 CET	49744	443	192.168.2.3	74.114.154.21
Jan 11, 2021 18:08:30.141961098 CET	49744	443	192.168.2.3	74.114.154.21
Jan 11, 2021 18:08:30.144124031 CET	443	49743	74.114.154.21	192.168.2.3
Jan 11, 2021 18:08:30.144144058 CET	443	49743	74.114.154.21	192.168.2.3
Jan 11, 2021 18:08:30.144294024 CET	49743	443	192.168.2.3	74.114.154.21
Jan 11, 2021 18:08:30.145456076 CET	443	49744	74.114.154.21	192.168.2.3
Jan 11, 2021 18:08:30.145592928 CET	49744	443	192.168.2.3	74.114.154.21
Jan 11, 2021 18:08:30.145612001 CET	49743	443	192.168.2.3	74.114.154.21
Jan 11, 2021 18:08:30.150314093 CET	443	49743	74.114.154.21	192.168.2.3
Jan 11, 2021 18:08:30.150572062 CET	49743	443	192.168.2.3	74.114.154.21
Jan 11, 2021 18:08:30.185497046 CET	443	49744	74.114.154.21	192.168.2.3
Jan 11, 2021 18:08:30.242336035 CET	443	49744	74.114.154.21	192.168.2.3
Jan 11, 2021 18:08:30.242358923 CET	443	49744	74.114.154.21	192.168.2.3
Jan 11, 2021 18:08:30.242487907 CET	49744	443	192.168.2.3	74.114.154.21
Jan 11, 2021 18:08:30.274169922 CET	443	49744	74.114.154.21	192.168.2.3
Jan 11, 2021 18:08:30.321077108 CET	443	49743	74.114.154.21	192.168.2.3
Jan 11, 2021 18:08:30.520701885 CET	49746	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.520772934 CET	49745	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.560379028 CET	443	49746	192.0.78.27	192.168.2.3
Jan 11, 2021 18:08:30.560560942 CET	49746	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.560735941 CET	443	49745	192.0.78.27	192.168.2.3
Jan 11, 2021 18:08:30.560868979 CET	49745	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.561495066 CET	49746	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.562606096 CET	49745	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.601162910 CET	443	49746	192.0.78.27	192.168.2.3
Jan 11, 2021 18:08:30.602421999 CET	443	49745	192.0.78.27	192.168.2.3
Jan 11, 2021 18:08:30.602686882 CET	443	49746	192.0.78.27	192.168.2.3
Jan 11, 2021 18:08:30.602730989 CET	443	49746	192.0.78.27	192.168.2.3
Jan 11, 2021 18:08:30.602766991 CET	443	49746	192.0.78.27	192.168.2.3
Jan 11, 2021 18:08:30.602804899 CET	443	49746	192.0.78.27	192.168.2.3
Jan 11, 2021 18:08:30.602838039 CET	443	49746	192.0.78.27	192.168.2.3
Jan 11, 2021 18:08:30.602835894 CET	49746	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.602890015 CET	49746	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.602895975 CET	49746	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.602900982 CET	49746	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.602905989 CET	49746	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.604007959 CET	443	49745	192.0.78.27	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:08:30.604048967 CET	443	49745	192.0.78.27	192.168.2.3
Jan 11, 2021 18:08:30.604095936 CET	443	49745	192.0.78.27	192.168.2.3
Jan 11, 2021 18:08:30.604109049 CET	49745	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.604127884 CET	443	49745	192.0.78.27	192.168.2.3
Jan 11, 2021 18:08:30.604146957 CET	49745	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.604154110 CET	443	49745	192.0.78.27	192.168.2.3
Jan 11, 2021 18:08:30.604155064 CET	49745	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.604177952 CET	49745	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.604198933 CET	49745	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.614984989 CET	49746	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.615323067 CET	49745	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.615569115 CET	49746	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.615814924 CET	49746	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.615948915 CET	49745	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.654861927 CET	443	49746	192.0.78.27	192.168.2.3
Jan 11, 2021 18:08:30.654917955 CET	443	49746	192.0.78.27	192.168.2.3
Jan 11, 2021 18:08:30.655034065 CET	49746	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.655062914 CET	49746	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.655075073 CET	443	49746	192.0.78.27	192.168.2.3
Jan 11, 2021 18:08:30.655178070 CET	49746	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.655297041 CET	443	49745	192.0.78.27	192.168.2.3
Jan 11, 2021 18:08:30.655333996 CET	443	49745	192.0.78.27	192.168.2.3
Jan 11, 2021 18:08:30.655385017 CET	49745	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.655428886 CET	49745	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.655793905 CET	49746	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.655822992 CET	443	49745	192.0.78.27	192.168.2.3
Jan 11, 2021 18:08:30.655916929 CET	49745	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.656451941 CET	49745	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.694619894 CET	443	49746	192.0.78.27	192.168.2.3
Jan 11, 2021 18:08:30.737988949 CET	443	49746	192.0.78.27	192.168.2.3
Jan 11, 2021 18:08:30.738162041 CET	443	49745	192.0.78.27	192.168.2.3
Jan 11, 2021 18:08:30.741610050 CET	443	49746	192.0.78.27	192.168.2.3
Jan 11, 2021 18:08:30.741688967 CET	49746	443	192.168.2.3	192.0.78.27
Jan 11, 2021 18:08:30.913810968 CET	49747	443	192.168.2.3	104.28.25.219
Jan 11, 2021 18:08:30.913988113 CET	49748	443	192.168.2.3	104.28.25.219
Jan 11, 2021 18:08:30.964390993 CET	443	49747	104.28.25.219	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:07:15.082787037 CET	63492	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:15.133477926 CET	53	63492	8.8.8.8	192.168.2.3
Jan 11, 2021 18:07:17.848589897 CET	60831	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:17.899476051 CET	53	60831	8.8.8.8	192.168.2.3
Jan 11, 2021 18:07:18.689126968 CET	60100	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:18.739985943 CET	53	60100	8.8.8.8	192.168.2.3
Jan 11, 2021 18:07:19.551877022 CET	53195	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:19.600889921 CET	53	53195	8.8.8.8	192.168.2.3
Jan 11, 2021 18:07:20.352287054 CET	50141	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:20.402973890 CET	53	50141	8.8.8.8	192.168.2.3
Jan 11, 2021 18:07:21.390645027 CET	53023	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:21.447299957 CET	53	53023	8.8.8.8	192.168.2.3
Jan 11, 2021 18:07:22.411628962 CET	49563	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:22.459542036 CET	53	49563	8.8.8.8	192.168.2.3
Jan 11, 2021 18:07:23.247694969 CET	51352	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:23.295924902 CET	53	51352	8.8.8.8	192.168.2.3
Jan 11, 2021 18:07:24.236397028 CET	59349	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:24.284581900 CET	53	59349	8.8.8.8	192.168.2.3
Jan 11, 2021 18:07:25.407299995 CET	57084	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:25.455385923 CET	53	57084	8.8.8.8	192.168.2.3
Jan 11, 2021 18:07:26.174740076 CET	58823	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:26.222839117 CET	53	58823	8.8.8.8	192.168.2.3
Jan 11, 2021 18:07:28.544013977 CET	57568	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:28.591912031 CET	53	57568	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:07:30.834924936 CET	50540	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:30.886509895 CET	53	50540	8.8.8.8	192.168.2.3
Jan 11, 2021 18:07:32.637150049 CET	54366	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:32.685198069 CET	53	54366	8.8.8.8	192.168.2.3
Jan 11, 2021 18:07:37.471669912 CET	53034	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:37.523184061 CET	57762	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:37.531240940 CET	53	53034	8.8.8.8	192.168.2.3
Jan 11, 2021 18:07:37.579356909 CET	53	57762	8.8.8.8	192.168.2.3
Jan 11, 2021 18:07:38.476430893 CET	53034	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:38.532776117 CET	53	53034	8.8.8.8	192.168.2.3
Jan 11, 2021 18:07:38.554502964 CET	57762	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:38.610837936 CET	53	57762	8.8.8.8	192.168.2.3
Jan 11, 2021 18:07:39.513818026 CET	53034	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:39.570086002 CET	53	53034	8.8.8.8	192.168.2.3
Jan 11, 2021 18:07:39.603315115 CET	57762	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:39.659866095 CET	53	57762	8.8.8.8	192.168.2.3
Jan 11, 2021 18:07:41.551980972 CET	53034	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:41.601960897 CET	57762	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:41.610306978 CET	53	53034	8.8.8.8	192.168.2.3
Jan 11, 2021 18:07:41.662192106 CET	53	57762	8.8.8.8	192.168.2.3
Jan 11, 2021 18:07:45.560746908 CET	53034	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:45.607273102 CET	57762	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:45.609107018 CET	53	53034	8.8.8.8	192.168.2.3
Jan 11, 2021 18:07:45.663758993 CET	53	57762	8.8.8.8	192.168.2.3
Jan 11, 2021 18:07:47.522798061 CET	55435	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:47.570918083 CET	53	55435	8.8.8.8	192.168.2.3
Jan 11, 2021 18:07:47.827960014 CET	50713	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:47.889096975 CET	53	50713	8.8.8.8	192.168.2.3
Jan 11, 2021 18:07:57.834151983 CET	56132	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:07:57.893569946 CET	53	56132	8.8.8.8	192.168.2.3
Jan 11, 2021 18:08:04.344733000 CET	58987	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:08:04.392877102 CET	53	58987	8.8.8.8	192.168.2.3
Jan 11, 2021 18:08:05.635572910 CET	56579	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:08:05.683706045 CET	53	56579	8.8.8.8	192.168.2.3
Jan 11, 2021 18:08:16.188895941 CET	60633	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:08:16.248855114 CET	53	60633	8.8.8.8	192.168.2.3
Jan 11, 2021 18:08:17.386396885 CET	61292	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:08:17.448159933 CET	53	61292	8.8.8.8	192.168.2.3
Jan 11, 2021 18:08:19.350106955 CET	63619	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:08:19.406378984 CET	53	63619	8.8.8.8	192.168.2.3
Jan 11, 2021 18:08:28.328044891 CET	64938	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:08:28.370690107 CET	61946	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:08:28.385905981 CET	53	64938	8.8.8.8	192.168.2.3
Jan 11, 2021 18:08:28.429976940 CET	53	61946	8.8.8.8	192.168.2.3
Jan 11, 2021 18:08:29.576900005 CET	64910	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:08:29.634318113 CET	53	64910	8.8.8.8	192.168.2.3
Jan 11, 2021 18:08:30.461541891 CET	52123	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:08:30.512422085 CET	53	52123	8.8.8.8	192.168.2.3
Jan 11, 2021 18:08:30.820807934 CET	56130	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:08:30.903435946 CET	53	56130	8.8.8.8	192.168.2.3
Jan 11, 2021 18:08:31.322091103 CET	56338	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:08:31.322222948 CET	59420	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:08:31.378379107 CET	53	56338	8.8.8.8	192.168.2.3
Jan 11, 2021 18:08:31.386152029 CET	53	59420	8.8.8.8	192.168.2.3
Jan 11, 2021 18:08:33.223202944 CET	63978	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:08:33.279501915 CET	53	63978	8.8.8.8	192.168.2.3
Jan 11, 2021 18:08:33.318430901 CET	62938	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:08:33.385756016 CET	53	62938	8.8.8.8	192.168.2.3
Jan 11, 2021 18:08:33.479324102 CET	55708	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:08:33.483834982 CET	56803	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:08:33.534841061 CET	57145	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:08:33.535969973 CET	53	55708	8.8.8.8	192.168.2.3
Jan 11, 2021 18:08:33.544028044 CET	55359	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:08:33.548053980 CET	53	56803	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:08:33.598793030 CET	53	57145	8.8.8.8	192.168.2.3
Jan 11, 2021 18:08:33.613570929 CET	53	55359	8.8.8.8	192.168.2.3
Jan 11, 2021 18:08:33.635623932 CET	58306	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:08:33.712842941 CET	53	58306	8.8.8.8	192.168.2.3
Jan 11, 2021 18:08:34.162838936 CET	64124	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:08:34.227082968 CET	53	64124	8.8.8.8	192.168.2.3
Jan 11, 2021 18:08:50.585608006 CET	63150	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:08:50.633673906 CET	53	63150	8.8.8.8	192.168.2.3
Jan 11, 2021 18:08:58.298696041 CET	53279	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:08:58.349755049 CET	53	53279	8.8.8.8	192.168.2.3
Jan 11, 2021 18:08:59.266722918 CET	56881	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:08:59.314686060 CET	53	56881	8.8.8.8	192.168.2.3
Jan 11, 2021 18:08:59.315339088 CET	53279	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:08:59.366202116 CET	53	53279	8.8.8.8	192.168.2.3
Jan 11, 2021 18:09:00.266427040 CET	56881	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:09:00.323133945 CET	53	56881	8.8.8.8	192.168.2.3
Jan 11, 2021 18:09:00.340462923 CET	53279	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:09:00.391385078 CET	53	53279	8.8.8.8	192.168.2.3
Jan 11, 2021 18:09:00.749717951 CET	53642	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:09:00.818535089 CET	53	53642	8.8.8.8	192.168.2.3
Jan 11, 2021 18:09:01.369740009 CET	56881	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:09:01.417722940 CET	53	56881	8.8.8.8	192.168.2.3
Jan 11, 2021 18:09:02.330012083 CET	53279	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:09:02.380928993 CET	53	53279	8.8.8.8	192.168.2.3
Jan 11, 2021 18:09:03.360776901 CET	56881	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:09:03.408582926 CET	53	56881	8.8.8.8	192.168.2.3
Jan 11, 2021 18:09:06.330986023 CET	53279	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:09:06.381650925 CET	53	53279	8.8.8.8	192.168.2.3
Jan 11, 2021 18:09:07.362776041 CET	56881	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:09:07.410654068 CET	53	56881	8.8.8.8	192.168.2.3
Jan 11, 2021 18:10:03.609783888 CET	55667	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:10:03.668994904 CET	53	55667	8.8.8.8	192.168.2.3
Jan 11, 2021 18:10:04.197865963 CET	54833	53	192.168.2.3	8.8.8.8
Jan 11, 2021 18:10:04.256731987 CET	53	54833	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 11, 2021 18:08:17.386396885 CET	192.168.2.3	8.8.8.8	0x5cc1	Standard query (0)	umblr.com	A (IP address)	IN (0x0001)
Jan 11, 2021 18:08:28.370690107 CET	192.168.2.3	8.8.8.8	0x6ae3	Standard query (0)	t.umblr.com	A (IP address)	IN (0x0001)
Jan 11, 2021 18:08:29.576900005 CET	192.168.2.3	8.8.8.8	0xf008	Standard query (0)	t.umblr.com	A (IP address)	IN (0x0001)
Jan 11, 2021 18:08:30.461541891 CET	192.168.2.3	8.8.8.8	0xe5f4	Standard query (0)	href.li	A (IP address)	IN (0x0001)
Jan 11, 2021 18:08:30.820807934 CET	192.168.2.3	8.8.8.8	0x1be6	Standard query (0)	ykm.de	A (IP address)	IN (0x0001)
Jan 11, 2021 18:08:33.223202944 CET	192.168.2.3	8.8.8.8	0x15c	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Jan 11, 2021 18:08:33.318430901 CET	192.168.2.3	8.8.8.8	0xa103	Standard query (0)	themes.googleusercontent.com	A (IP address)	IN (0x0001)
Jan 11, 2021 18:08:33.534841061 CET	192.168.2.3	8.8.8.8	0x8115	Standard query (0)	adservice.google.co.uk	A (IP address)	IN (0x0001)
Jan 11, 2021 18:08:33.635623932 CET	192.168.2.3	8.8.8.8	0x34ba	Standard query (0)	www.googletagservices.com	A (IP address)	IN (0x0001)
Jan 11, 2021 18:09:00.749717951 CET	192.168.2.3	8.8.8.8	0x3781	Standard query (0)	ykm.de	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 11, 2021 18:08:17.448159933 CET	8.8.8.8	192.168.2.3	0x5cc1	No error (0)	umblr.com		74.114.154.17	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 11, 2021 18:08:17.448159933 CET	8.8.8.8	192.168.2.3	0x5cc1	No error (0)	umblr.com		74.114.154.21	A (IP address)	IN (0x0001)
Jan 11, 2021 18:08:28.429976940 CET	8.8.8.8	192.168.2.3	0x6ae3	No error (0)	t.umblr.com		74.114.154.21	A (IP address)	IN (0x0001)
Jan 11, 2021 18:08:28.429976940 CET	8.8.8.8	192.168.2.3	0x6ae3	No error (0)	t.umblr.com		74.114.154.17	A (IP address)	IN (0x0001)
Jan 11, 2021 18:08:29.634318113 CET	8.8.8.8	192.168.2.3	0xf008	No error (0)	t.umblr.com		74.114.154.21	A (IP address)	IN (0x0001)
Jan 11, 2021 18:08:29.634318113 CET	8.8.8.8	192.168.2.3	0xf008	No error (0)	t.umblr.com		74.114.154.17	A (IP address)	IN (0x0001)
Jan 11, 2021 18:08:30.512422085 CET	8.8.8.8	192.168.2.3	0xe5f4	No error (0)	href.li		192.0.78.27	A (IP address)	IN (0x0001)
Jan 11, 2021 18:08:30.512422085 CET	8.8.8.8	192.168.2.3	0xe5f4	No error (0)	href.li		192.0.78.26	A (IP address)	IN (0x0001)
Jan 11, 2021 18:08:30.903435946 CET	8.8.8.8	192.168.2.3	0x1be6	No error (0)	ykm.de		104.28.25.219	A (IP address)	IN (0x0001)
Jan 11, 2021 18:08:30.903435946 CET	8.8.8.8	192.168.2.3	0x1be6	No error (0)	ykm.de		172.67.153.240	A (IP address)	IN (0x0001)
Jan 11, 2021 18:08:30.903435946 CET	8.8.8.8	192.168.2.3	0x1be6	No error (0)	ykm.de		104.28.24.219	A (IP address)	IN (0x0001)
Jan 11, 2021 18:08:31.386152029 CET	8.8.8.8	192.168.2.3	0xe0fd	No error (0)	pagead46.l.doubleclick.net		172.217.20.226	A (IP address)	IN (0x0001)
Jan 11, 2021 18:08:33.279501915 CET	8.8.8.8	192.168.2.3	0x15c	No error (0)	googleads.g.doubleclick.net	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jan 11, 2021 18:08:33.279501915 CET	8.8.8.8	192.168.2.3	0x15c	No error (0)	pagead46.l.doubleclick.net		172.217.23.34	A (IP address)	IN (0x0001)
Jan 11, 2021 18:08:33.385756016 CET	8.8.8.8	192.168.2.3	0xa103	No error (0)	themes.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 11, 2021 18:08:33.385756016 CET	8.8.8.8	192.168.2.3	0xa103	No error (0)	googlehosted.l.googleusercontent.com		172.217.23.1	A (IP address)	IN (0x0001)
Jan 11, 2021 18:08:33.548053980 CET	8.8.8.8	192.168.2.3	0x476a	No error (0)	partnerad.l.doubleclick.net		172.217.23.34	A (IP address)	IN (0x0001)
Jan 11, 2021 18:08:33.598793030 CET	8.8.8.8	192.168.2.3	0x8115	No error (0)	adservice.google.co.uk	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jan 11, 2021 18:08:33.598793030 CET	8.8.8.8	192.168.2.3	0x8115	No error (0)	pagead46.l.doubleclick.net		172.217.23.2	A (IP address)	IN (0x0001)
Jan 11, 2021 18:08:33.613570929 CET	8.8.8.8	192.168.2.3	0x4ca4	No error (0)	pagead46.l.doubleclick.net		172.217.23.66	A (IP address)	IN (0x0001)
Jan 11, 2021 18:08:33.712842941 CET	8.8.8.8	192.168.2.3	0x34ba	No error (0)	www.googletagservices.com	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jan 11, 2021 18:08:33.712842941 CET	8.8.8.8	192.168.2.3	0x34ba	No error (0)	pagead46.l.doubleclick.net		172.217.22.194	A (IP address)	IN (0x0001)
Jan 11, 2021 18:09:00.818535089 CET	8.8.8.8	192.168.2.3	0x3781	No error (0)	ykm.de		172.67.153.240	A (IP address)	IN (0x0001)
Jan 11, 2021 18:09:00.818535089 CET	8.8.8.8	192.168.2.3	0x3781	No error (0)	ykm.de		104.28.24.219	A (IP address)	IN (0x0001)
Jan 11, 2021 18:09:00.818535089 CET	8.8.8.8	192.168.2.3	0x3781	No error (0)	ykm.de		104.28.25.219	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
Jan 11, 2021 18:08:29.962896109 CET	74.114.154.21	443	192.168.2.3	49744	CN=umblr.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Nov 30 14:00:38 CET 2020	Sun Feb 28 14:00:38 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=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Jan 11, 2021 18:08:29.967052937 CET	74.114.154.21	443	192.168.2.3	49743	CN=umblr.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Nov 30 14:00:38 CET 2020	Sun Feb 28 14:00:38 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=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Jan 11, 2021 18:08:30.602766991 CET	192.0.78.27	443	192.168.2.3	49746	CN=tls.automattic.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Dec 13 22:13:03 CET 2020	Sat Mar 13 22:13:03 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=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Jan 11, 2021 18:08:30.604095936 CET	192.0.78.27	443	192.168.2.3	49745	CN=tls.automattic.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Dec 13 22:13:03 CET 2020	Sat Mar 13 22:13:03 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=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Jan 11, 2021 18:08:31.019426107 CET	104.28.25.219	443	192.168.2.3	49747	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jul 09 02:00:00 CEST 2020	Fri Jul 09 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 11, 2021 18:08:31.022233963 CET	104.28.25.219	443	192.168.2.3	49748	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jul 09 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Fri Jul 09 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 11, 2021 18:08:31.495069981 CET	172.217.20.226	443	192.168.2.3	49751	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:42:47 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:42:46 CET 2021 Wed Dec 15 01:00:42 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jan 11, 2021 18:08:31.496062040 CET	172.217.20.226	443	192.168.2.3	49752	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:42:47 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:42:46 CET 2021 Wed Dec 15 01:00:42 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jan 11, 2021 18:08:33.384989023 CET	172.217.23.34	443	192.168.2.3	49754	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:42:47 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:42:46 CET 2021 Wed Dec 15 01:00:42 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jan 11, 2021 18:08:33.385695934 CET	172.217.23.34	443	192.168.2.3	49753	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:42:47 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:42:46 CET 2021 Wed Dec 15 01:00:42 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 11, 2021 18:08:33.493690968 CET	172.217.23.1	443	192.168.2.3	49755	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:47:09 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:47:08 CET 2021 Wed Dec 15 01:00:42 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jan 11, 2021 18:08:33.514311075 CET	172.217.23.1	443	192.168.2.3	49757	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:47:09 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:47:08 CET 2021 Wed Dec 15 01:00:42 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jan 11, 2021 18:08:33.514806986 CET	172.217.23.1	443	192.168.2.3	49758	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:47:09 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:47:08 CET 2021 Wed Dec 15 01:00:42 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jan 11, 2021 18:08:33.516001940 CET	172.217.23.1	443	192.168.2.3	49756	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:47:09 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:47:08 CET 2021 Wed Dec 15 01:00:42 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jan 11, 2021 18:08:33.517822981 CET	172.217.23.1	443	192.168.2.3	49760	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:47:09 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:47:08 CET 2021 Wed Dec 15 01:00:42 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 11, 2021 18:08:33.522711039 CET	172.217.23.1	443	192.168.2.3	49759	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:47:09 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:47:08 CET 2021 Wed Dec 15 01:00:42 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jan 11, 2021 18:08:33.649666071 CET	172.217.23.34	443	192.168.2.3	49763	CN=*.googleadservices.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:46:48 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:46:47 CET 2021 Wed Dec 15 01:00:42 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jan 11, 2021 18:08:33.681428909 CET	172.217.23.34	443	192.168.2.3	49764	CN=*.googleadservices.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:46:48 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:46:47 CET 2021 Wed Dec 15 01:00:42 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jan 11, 2021 18:08:33.724786043 CET	172.217.23.2	443	192.168.2.3	49766	CN=*.google.co.uk, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:51:09 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:51:08 CET 2021 Wed Dec 15 01:00:42 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jan 11, 2021 18:08:33.725270987 CET	172.217.23.2	443	192.168.2.3	49765	CN=*.google.co.uk, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:51:09 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:51:08 CET 2021 Wed Dec 15 01:00:42 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

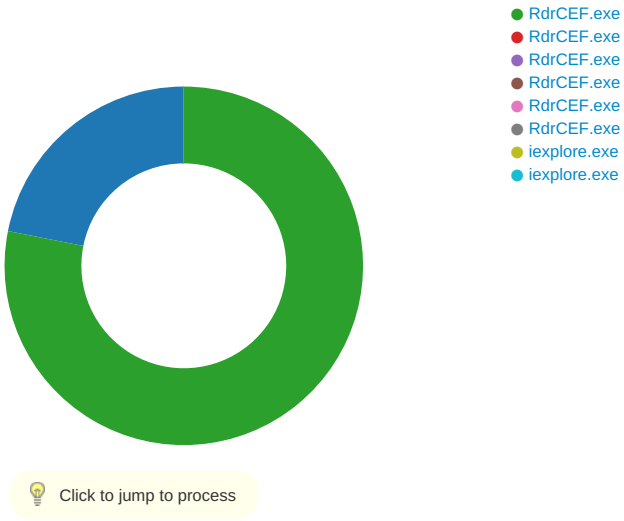
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 11, 2021 18:08:33.728147984 CET	172.217.23.66	443	192.168.2.3	49768	CN=*.google.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:42:53 CET 2020	Tue Mar 09 15:42:52 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jan 11, 2021 18:08:33.728528976 CET	172.217.23.66	443	192.168.2.3	49767	CN=*.google.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:42:53 CET 2020	Tue Mar 09 15:42:52 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jan 11, 2021 18:08:33.835603952 CET	172.217.22.194	443	192.168.2.3	49769	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:42:47 CET 2020	Tue Mar 09 15:42:46 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jan 11, 2021 18:08:33.836500883 CET	172.217.22.194	443	192.168.2.3	49770	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:42:47 CET 2020	Tue Mar 09 15:42:46 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Code Manipulations

Statistics

Behavior

● AcroRd32.exe
● AcroRd32.exe



System Behavior

Analysis Process: AcroRd32.exe PID: 5948 Parent PID: 5544

General

Start time:	18:07:20
Start date:	11/01/2021
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\Information-Account-Prime-Disable-Service.pdf'
Imagebase:	0x3a0000
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	3D65C3	CreateDirectoryExW
C:\Users\user\AppData\Local\Temp\acrocef_low	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3FAE05	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	3EEA85	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210112020728Z-201.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	3EEA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.5956	write data or add file | append data or add subdirectory or create pipe instance | write ea | read attributes | write attributes | read control | sync hronize	device	synchronous io non alert | non directory file	success or wait	1	3EEA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock5948.1.241158583.tmp	read data or list directory | read ea | read attributes | de lete | read control | synchronize	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	422657	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	4683C8	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	4683C8	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	4683C8	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4683C8	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	4683C8	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	4683C8	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rc4bt2d_p7y4ku_4lg.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	3EEA85	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	4	3EEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1leo5qo_p7y4kv_4lg.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	3EEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1h5abst_p7y4kw_4lg.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	3EEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1mtl1w8_p7y4kx_4lg.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	3EEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1nl40nt_p7y4ky_4lg.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	3EEA85	NtCreateFile

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.5956	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst	success or wait	1	42D405	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	3ECF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	3ED41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	3ED41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo	success or wait	1	3ED41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\NoTimeOut	success or wait	1	3ED41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	3AEA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	3AEA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	3AEA55	RegCreateKeyExW
\Device\HarddiskVolume4\Users\user\Desktop\Software\Adobe\Acrobat Reader\DC\TrustManager	success or wait	1	3ED41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\TrustManager\cDefaultLaunchURLPerms	success or wait	1	3ED41D	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	3FDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/Users/user/Desktop/Information-Account-Prime-Disable-Service.pdf	success or wait	1	3FDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	Information-Account-Prime-Disable-Service.pdf	success or wait	1	3FDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	3FDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	3FDF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDI	binary	2F 43 2F 55 73 65 72 73 2F 68 61 72 64 7A 2F 44 65 73 6B 74 6F 70 2F 49 6E 66 6F 72 6D 61 74 69 6F 6E 2D 41 63 63 6F 75 6E 74 2D 50 72 69 6D 65 2D 44 69 73 61 62 6C 65 2D 53 65 72 76 69 63 65 2E 70 64 66 00	success or wait	1	3FDF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDate	binary	44 3A 32 30 32 31 30 31 31 31 31 38 30 37 32 38 2D 30 38 27 30 30 27 00	success or wait	1	3FDF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	197654	success or wait	1	3FDF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	1	success or wait	1	3FDF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	3FDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tDIText	unicode	http://www.adobe.com/go/homeacrordrunified18_2018	success or wait	1	3FDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	3FDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	3FDF69	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	3FDF69	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 30 32 33 33 34 2D 30 37 27 30 30 27 00	success or wait	1	3FDF69	RegSetValueExW

Analysis Process: AcroRd32.exe PID: 5956 Parent PID: 5948

General

Start time:	18:07:21
Start date:	11/01/2021
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\Information-Account-Prime-Disable-Service.pdf'
Imagebase:	0x3a0000
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: 5060 Parent PID: 5948

General

Start time:	18:07:27
Start date:	11/01/2021
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:	0xe50000
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	4	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	4	F459E2	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	15	F583E5	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	99	F58447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	219	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	4	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	8	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	4	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	24	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	4	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	8	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	4	F459E2	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	16	F459E2	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	4	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	2181	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	4	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	60	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	4	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	12	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	4	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	7	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	4	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	4	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	4	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	4	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	4	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	success or wait	4	F459E2	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	4	F459E2	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	4	F459E2	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	4	F459E2	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	4	F459E2	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	4	F459E2	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	8	F459E2	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	4	F459E2	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	4	F459E2	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	4	F459E2	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	F459E2	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	F459E2	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	4	F459E2	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	4	F459E2	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	4	F459E2	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	4	F459E2	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	24	F459E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	end of file	4	F459E2	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	24	F459E2	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	4	F459E2	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	56	F459E2	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	4	F459E2	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	60	F459E2	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	4	F459E2	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	87	F459E2	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	F459E2	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	4	F459E2	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	4	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	56	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	4	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	60	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	4	F459E2	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	20	F459E2	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	4	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	20	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	4	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	20	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	4	F459E2	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	20	F459E2	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	4	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	240	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	4	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	288	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	4	F459E2	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	266	F459E2	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	4	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	50	F459E2	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	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	success or wait	196	F459E2	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	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	31	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	4	F459E2	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	F459E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	end of file	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	9	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	3	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	success or wait	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	end of file	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	success or wait	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	end of file	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	success or wait	2	F459E2	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	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	success or wait	6	F459E2	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	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	success or wait	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	end of file	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	4	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	success or wait	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	end of file	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	success or wait	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	end of file	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	8	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	success or wait	169	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	end of file	2	F459E2	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	8	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	end of file	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	success or wait	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	end of file	2	F459E2	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	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	end of file	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	success or wait	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	end of file	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	success or wait	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	end of file	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	success or wait	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	end of file	2	F459E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	success or wait	16	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	end of file	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	success or wait	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	end of file	2	F459E2	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	325	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	end of file	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	success or wait	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	end of file	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	success or wait	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	end of file	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	success or wait	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	end of file	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	success or wait	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	end of file	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	success or wait	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	end of file	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	success or wait	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	end of file	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	success or wait	4	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	end of file	2	F459E2	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	150	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	end of file	2	F459E2	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	12	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	end of file	2	F459E2	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	32	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	end of file	2	F459E2	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	10	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	end of file	2	F459E2	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	2	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	end of file	2	F459E2	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	4	F459E2	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	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main-selector.css	unknown	4096	success or wait	1	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main-selector.css	unknown	4096	end of file	1	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main.css	unknown	4096	success or wait	4	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main.css	unknown	4096	end of file	1	F459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\selector.js	unknown	4096	success or wait	1	F459E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\selector.js	unknown	4096	end of file	1	F459E2	ReadFile
unknown	unknown	4096	success or wait	24	F459E2	ReadFile
unknown	unknown	4096	end of file	1	F459E2	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	F583E5	ReadFile

Analysis Process: RdrCEF.exe PID: 6344 Parent PID: 5060

General

Start time:	18:07:30
Start date:	11/01/2021
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=1676,690228386903701 5468,17832798338356840690,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=13817734648253318396 --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=13817734648253318396 --renderer-client-id=2 --mojo-platform-channel-handle=1720 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xe50000
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: 6372 Parent PID: 5060

General

Start time:	18:07:31
Start date:	11/01/2021
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=1676,690228369037015468,17832798338356840690,131072 --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=11890072385820109879 --mojo-platform-channel-handle=1748 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0xe50000
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: 6424 Parent PID: 5060

General

Start time:	18:07:33
Start date:	11/01/2021
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=1676,6902283869037015468,17832798338356840690,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=1881667437359436119 --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=1881667437359436119 --renderer-client-id=4 --mojo-platform-channel-handle=1860 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xe50000
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: 6560 Parent PID: 5060

General

Start time:	18:07:37
Start date:	11/01/2021
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=1676,6902283869037015468,17832798338356840690,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=5458918827524385669 --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=5458918827524385669 --renderer-client-id=5 --mojo-platform-channel-handle=1864 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xe50000
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: 6676 Parent PID: 5060

General

Start time:	18:07:39
Start date:	11/01/2021
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=1676,6902283869037015468,17832798338356840690,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=13143280483817159406 --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=13143280483817159406 --renderer-client-id=6 --mojo-platform-channel-handle=2140 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xe50000
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: 4736 Parent PID: 5948

General

Start time:	18:08:27
Start date:	11/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' https://t.umblr.com/redirect?z=https%3A%2F%2Fykm.de%2F65f0a4768a364c17&t=MDZmNTEyZmUxYzY5ZjJkNjc3MDI5MTI0MjhiODVlNzBhYTAzZWMzZCwwY2IyNWEwNWYyMzA5MGNlNzYxMzg5ZTFhMTcwMTA4Y2U5NmEwYzZl&ts=1610149120
Imagebase:	0x7ff702c60000
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	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 1048 Parent PID: 4736

General

Start time:	18:08:27
Start date:	11/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4736 CREDAT:17410 /prefetch:2
Imagebase:	0x1b0000
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

Disassembly

Code Analysis