ID: 444764
Sample Name: Strategic Procurement Services Supplier Notice COVID19 June 30 2021.pdf
Cookbook: defaultwindowspdfcookbook.jbs
Time: 16:53:04
Date: 06/07/2021
Version: 32.0.0 Black Diamond

Table of Contents

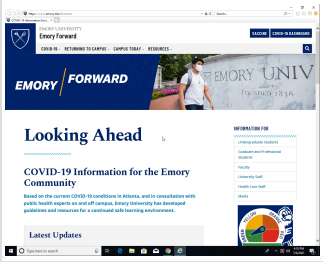
Windows Analysis Report Strategic Procurement Servic…

Overview

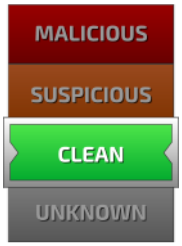
General Information

Sample Name:	Strategic Procurement Services Supplier Notice COVID19 June 30 2021.pdf
Analysis ID:	444764
MD5:	39bc0abebb458b..
SHA1:	785637468cdd2a..
SHA256:	d41884b2af00861.
Infos:	

Most interesting Screenshot:



Detection

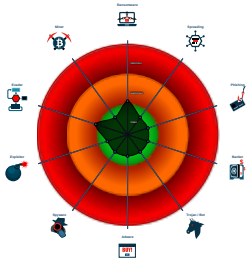


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

- 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

Process Tree

- **System is w10x64**
- AcroRd32.exe (PID: 3068 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\Strategic Procurement Services Supplier Notice COVID19 June 30 2021.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 3424 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\Strategic Procurement Services Supplier Notice COVID19 June 30 2021.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 6140 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6204 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=1720,1139489186481270161 7,5421238245506412973,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=3994307663767611292 --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=3994307663767611292 --renderer-client-id=2 --mojo-platform-channel-handle=1752 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6232 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1720,1139489186481270161 7,5421238245506412973,131072 --disable-features=VizDisplayCompositor --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --lang=en-US --gpu-preferences=KAAAAAAAACAAwABAQAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=2914443920406660741 --mojo-platform-channel-handle=1772 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6364 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=1720,1139489186481270161 7,5421238245506412973,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=10280300687710209152 --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=10280300687710209152 --renderer-client-id=4 --mojo-platform-channel-handle=1852 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6492 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=1720,1139489186481270161 7,5421238245506412973,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=5121740222193972291 --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=5121740222193972291 --renderer-client-id=5 --mojo-platform-channel-handle=2240 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
  - iexplore.exe (PID: 2424 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' https://www.emory.edu/forward/ MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
    - iexplore.exe (PID: 2908 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2424 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

Jbx Signature Overview

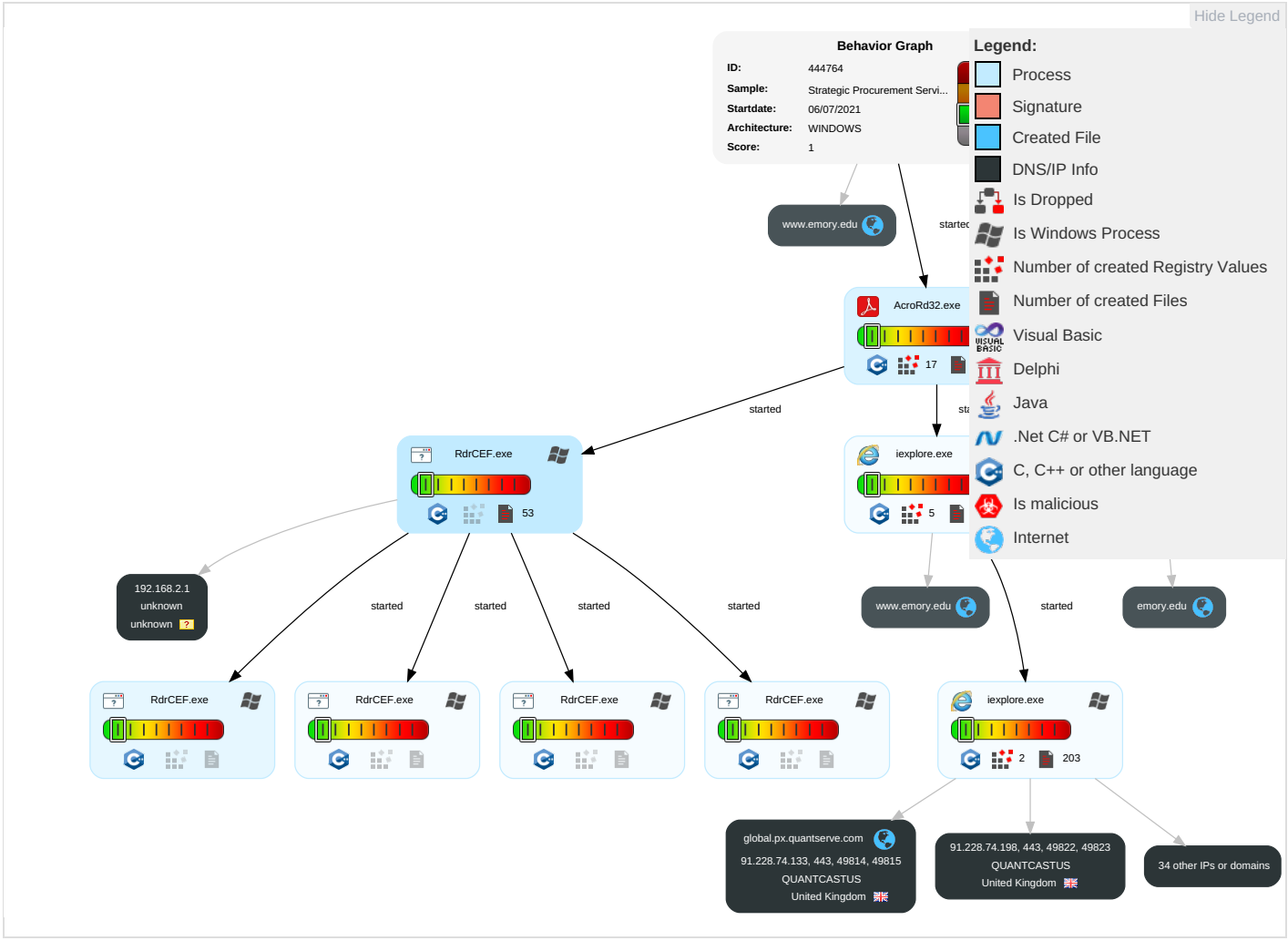
Click to jump to signature section

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	I
Spearphishing Link 1	Windows Management Instrumentation	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	I S I
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	I I
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	I I I

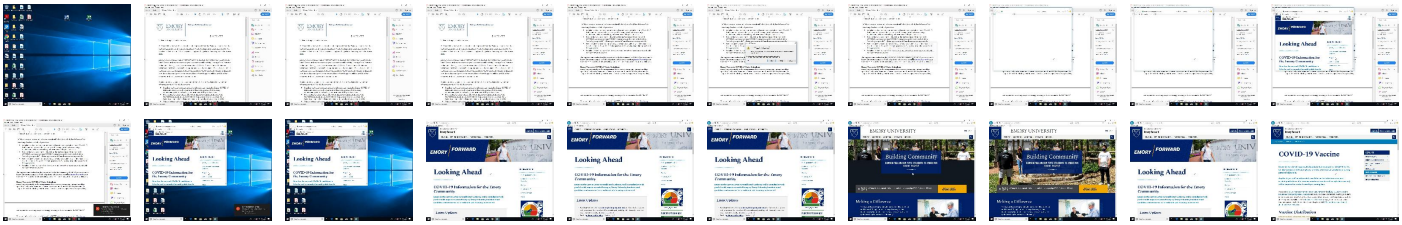
Behavior Graph

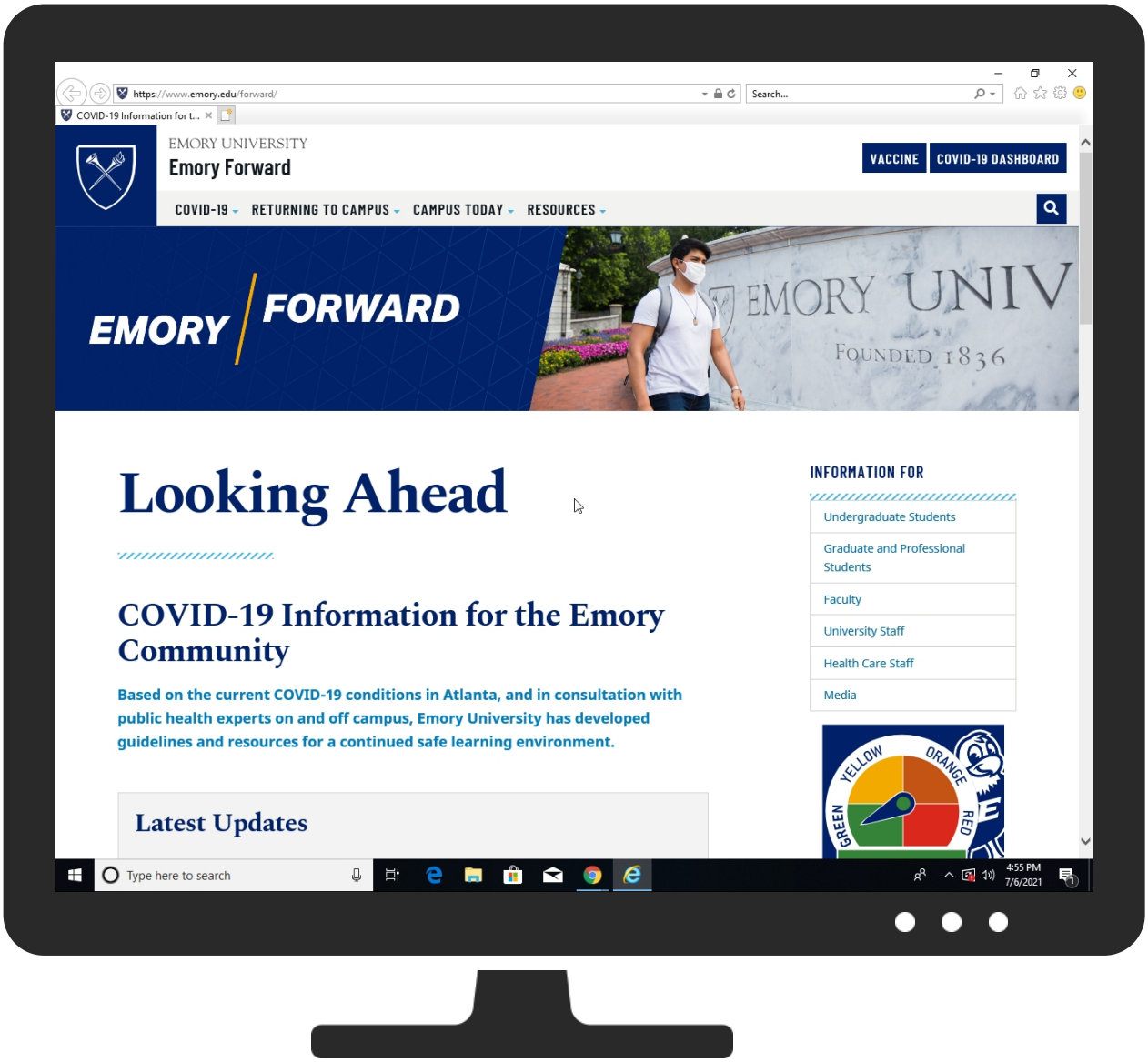


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Strategic Procurement Services Supplier Notice COVID19 June 30 2021.pdf	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
siteimproveanalytics.com	1%	Virustotal		Browse
66356337.global.siteimproveanalytics.io	0%	Virustotal		Browse
rules.quantcount.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/F	0%	Avira URL Cloud	safe	
http://https://fontawesome.comhttps://fontawesome.comFont	0%	Avira URL Cloud	safe	
http://https://raw.githubusercontent.com/stefanpenner/es6-promise/master/LICENSE	0%	Virustotal		Browse
http://https://raw.githubusercontent.com/stefanpenner/es6-promise/master/LICENSE	0%	Avira URL Cloud	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://https://api.echosign.comRL	0%	URL Reputation	safe	
http://https://api.echosign.comRL	0%	URL Reputation	safe	
http://https://api.echosign.comRL	0%	URL Reputation	safe	
http://https://api.echosign.comRL	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/I	0%	Avira URL Cloud	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/imensions#	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.google.de	142.250.201.195	true	false		high
siteimproveanalytics.com	172.64.172.12	true	false	• 1%, Virustotal, Browse	unknown
d2fashanjl7d9f.cloudfront.net	13.224.99.16	true	false		high
stats.l.doubleclick.net	64.233.166.155	true	false		high
global.px.quantserve.com	91.228.74.133	true	false		high
www.emory.edu	170.140.125.16	true	false		high
fontawesome-cdn.fonticons.netdna-cdn.com	23.111.9.35	true	false		high
ana-cf-col-elb-78-567119012.eu-central-1.elb.amazonaws.com	18.195.138.231	true	false		high
cs491.wac.edgecastcdn.net	192.229.233.25	true	false		high
emory.edu	170.140.125.20	true	false		high
scontent.cdninstagram.com	157.240.17.63	true	false		high
img.juicer.io	104.26.12.87	true	false		high
scontent.xx.fbcdn.net	157.240.17.15	true	false		high
template.emory.edu	170.140.125.169	true	false		high
googleads.g.doubleclick.net	172.217.16.98	true	false		high
www.juicer.io	104.26.13.87	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
cs672.wac.edgecastcdn.net	192.229.233.50	true	false		high
pbs.twimg.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
secure.quantserve.com	unknown	unknown	false		high
pixel.quantserve.com	unknown	unknown	false		high
66356337.global.siteimproveanalytics.io	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
connect.facebook.net	unknown	unknown	false		high
rules.quantcount.com	unknown	unknown	false	• 1%, Virustotal, Browse	unknown
stats.g.doubleclick.net	unknown	unknown	false		high
use.fontawesome.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
platform.twitter.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.emory.edu/forward/covid-19/operating-condition-status.html	false		high
http://https://www.emory.edu/forward/covid-19/dashboard/index.html	false		high
http://https://www.emory.edu/forward/	false		high
http://https://www.emory.edu/forward/#main	false		high
http://https://www.emory.edu/forward/covid-19/healthy-behaviors.html	false		high
http://https://www.emory.edu/forward/covid-19/vaccine.html	false		high
http://https://www.emory.edu/forward/covid-19/index.html	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.111.9.35	fontawesome-cdn.fonticons.netdna-cdn.com	United States		33438	HIGHWINDS2US	false
192.229.233.25	cs491.wac.edgecastcdn.net	United States		15133	EDGECASTUS	false
172.217.16.98	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
157.240.17.15	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
170.140.125.169	template.emory.edu	United States		3512	EUSHCUS	false
104.26.13.87	www.juicer.io	United States		13335	CLOUDFLARENETUS	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
18.195.138.231	ana-cf-col-elb-78-567119012.eu-central-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
170.140.125.16	www.emory.edu	United States		3512	EUSHCUS	false
91.228.74.198	unknown	United Kingdom		27281	QUANTCASTUS	false
91.228.74.133	global.px.quantserve.com	United Kingdom		27281	QUANTCASTUS	false
192.229.233.50	cs672.wac.edgecastcdn.net	United States		15133	EDGECASTUS	false
157.240.17.63	scontent.cdninstagram.com	United States		32934	FACEBOOKUS	false
172.64.172.12	siteimproveanalytics.com	United States		13335	CLOUDFLARENETUS	false
64.233.166.155	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
13.224.99.16	d2fashanjl7d9f.cloudfront.net	United States		16509	AMAZON-02US	false
104.26.12.87	img.juicer.io	United States		13335	CLOUDFLARENETUS	false
170.140.125.20	emory.edu	United States		3512	EUSHCUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	444764
Start date:	06.07.2021
Start time:	16:53:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Strategic Procurement Services Supplier Notice COVID19 June 30 2021.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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.winPDF@17/197@23/19
EGA Information:	Failed
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://www.emory.edu/forward/#main • Browsing link: http://www.emory.edu/ • Browsing link: https://www.emory.edu/forward/index.html • Browsing link: https://www.emory.edu/forward/covid-19/vaccine.html • Browsing link: https://www.emory.edu/forward/covid-19/dashboard/index.html • Browsing link: https://www.emory.edu/forward/covid-19/index.html • Browsing link: https://www.emory.edu/forward/covid-19/if-you-feel-sick.html • Browsing link: https://www.emory.edu/forward/covid-19/quick-guides.html • Browsing link: https://www.emory.edu/forward/covid-19/operating-condition-status.html • Browsing link: https://www.emory.edu/forward/covid-19/testing/index.html • Browsing link: https://www.emory.edu/forward/covid-19/healthy-behaviors.html
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:54:03	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
23.111.9.35	http://1minutemarketing.net/	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://www.visioncraftng.com/wp-admin/paclm/aTOOClFPHUo66z	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://giftbuying411.com/wp-includes/64358352543832/1xd5izerfl-00002/	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://www.00rcasey.sebelt.com/?VGH=cmNhc2V5QGNnc2luYy5jb20=	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://www.00dhoy.sebelt.com/?VGH=ZGhveUBjZ3NpbmMuY2E=	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://casehunter.com.br	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://alaksir.com/Scripts/TW6LJpx/	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://azetta.org/Manage-AbsaOnlineBanking-httpsib.absa.co.zaabsa-onlinelogin.jsp-Logon-AbsaExpress/~AbsaOnline%206-1.htm	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://bluetechprism.com/css/9zWF1bV_EzUmPytyJH5nFH6_sector/individual_n8i69k9xbanwxg_cnav2o/549242_o6OPbP/	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://magecart.net	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://https://protect-us.mimecast.com/s/uOyvC4xWr5FzL0Zyux-GUS?domain=t.yesware.com	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://https://telegra.ph/Notification-Checkpoin2020-07-12-2?fbclid=IwAR3CW1pVoB2bo4DBxz90-mn4s4lYZcDve12Q_Z31J30jf9ZtOUBqmdx9ZjE	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://bespokemerchandises.com	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://v.ht/5DsS	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://lavicentelopezcaferesto.com.ar/aquawestdubbo/prop/normal/	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://earningtipsbd.com/pn/Buy-Sell_Agreement_0786719_04272020.zip	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://https://onedrive.live.com/view.aspx?resid=1A4116533EC50398!1032&authkey=!AEhxS1cHS1VlwMY	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://www.8888scents.com/js/	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://sakshampharmaceuticals.com/wp-includes/wglyons.php?t=VHVlLCAxNCBBcHIgMjAyMCAyMjowMTMwMA==	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://rjsimmonscpa.com/colopeaks	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
siteimproveanalytics.com	http://delivery.unlocklocks.com/HSOMEU?id=124732=Jx8EBwNQDgsBTwECUwcIUlUBUx0=QgtZWk8ADFsJdkUDDQ9cU1AITVAdXENVHwYOUlwHUlMHUgMPUFtXAVMPTwoQF0QMHktdXV9aR1cRThYXC10MAl4OWlUKEE1XDVscKjcseXNkW1BcT0UD&fl=DBdARkJeFhdeXFVXEVleAwhYDxhRB1tCAA8AVRBTHQELDhtTYg1eVkAc	Get hash	malicious	Browse	• 172.64.196.24
	http://https://whitesrvrental.com/3/662656c696e64612e626f734073796e6368726f6e6f73732e636f6d	Get hash	malicious	Browse	• 172.64.173.12
	http://https://gs635.scout.es/DocuSign	Get hash	malicious	Browse	• 172.64.173.12
	http://https://is.gd/NLY8Sb	Get hash	malicious	Browse	• 172.64.139.5
	http://https://omgzone.co.uk/	Get hash	malicious	Browse	• 172.64.139.5
	undefined.html	Get hash	malicious	Browse	• 172.64.138.5
	http://https://bgqfwsaw9whw.com/we/ds/dxl/dive/index.php	Get hash	malicious	Browse	• 172.64.139.5
	http://https://www.bestflbeachhouse.com/Urgent-docs/microsoft/	Get hash	malicious	Browse	• 172.64.139.5
	http://https://jalapao.store/farmacia/ds/dxl/dive/index.php	Get hash	malicious	Browse	• 172.64.138.5
	http://https://jalapao.store/farmacia/ds/dxl/dive/index.php	Get hash	malicious	Browse	• 172.64.139.5
	http://cosc.arch.tamu.edu/about/calendar/	Get hash	malicious	Browse	• 172.64.139.5
	http://r20.rs6.net/tn.jsp?f=001L9_vuReWv_sY1xVTZ3gwwgIL5IcRWtElxx50KxqssS6FgVa7EB4wnrzoQqhSsZWeFWwm3wgobfyhSAtbxhqwNtJR11Jp2Ln_6wYMhJDjIppaiMadEwE1eWNQnrvbxWtbkHxqUHWKhn_EOnB9D8WjPAAuSCZqzP63KZpc4vQb9zPbw8Q4duT663aQvBY0fGMBxGIHUo8vWoU=&c=VM-5pbDrRz8T6minLtK_L_KnoeHLemQXy-M1xYTNHTKMU5T-Cf1kDw==&ch=tO1O9dqeQxoDrl41-7sB7Kc7Kyv2aMvTHXOivYv_0_rUtKETpB-gTw==	Get hash	malicious	Browse	• 172.64.138.5

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://r20.rs6.net/tn.jsp?f=001L9_vuReWv_sY1xVTZ3gwwgIL5IcRWtElxx50KxqssS6FgVa7EB4wnrzoQqhSsZWef8sg7GZo0ArPVe_wXw3fxISCjici4ar-nMFdeloUkVG4F3FjILmslz_1kDByCHA5GV2rxMQ0EvXjdI0p8xBmzubSH3LCGn_epppo-9tIh4BdICOoGoR9Ow==&c=VM-5pbDrRz8T6minLtK_L_KnoeHLemQXy-M1xYTNHTKMU5T-Cf1kDw==&ch=tO1O9dqeQxoDrl41-7sB7Kc7Kyv2aMvTHXOivYv_0_rUtKETpB-gTw==	Get hash	malicious	Browse	• 172.64.139.5
	http://now.eloqua.com/es.asp?s=566810826&e=19496138&elqTrackId=a0951024370a4562b829ccb7f0eb1a6b&elq=433cfefb92f2448aac82f33a3affbe34&elqaid=40163&elqat=1&elqCampaignId=21133	Get hash	malicious	Browse	• 172.64.139.5
	http://now.eloqua.com/es.asp?s=566810826&e=19496138&elqTrackId=a0951024370a4562b829ccb7f0eb1a6b&elq=433cfefb92f2448aac82f33a3affbe34&elqaid=40163&elqat=1&elqCampaignId=21133	Get hash	malicious	Browse	• 172.64.138.5
	http://https://devteam.in/mme/Exc/MukeSpark-601897j69i60j69i57j69i60l33666j07&sourceidv	Get hash	malicious	Browse	• 172.64.110.36
	http://https://sep.covwarkitc.nhs.uk:10443/register/001U2FsdGVkX1-NOgr4vHG3DedyOqHyWmHFao2S-CbiobEBWlMH04TYNg/	Get hash	malicious	Browse	• 172.64.110.36
	http://https://surveyonline.co.in/html/Exc1/Exc/MukeSpark-601897j69i60j69i57j69i60l33666j07&sourceidv/index.php	Get hash	malicious	Browse	• 172.64.110.36
	http://vnca.me/uot8888	Get hash	malicious	Browse	• 172.64.160.18
	http://https://www.freesamplegiveaway.com.au/promo/?url=https://mail.hostmeister.com/accounts/gov.html&data=02|01|andrew.neate@essentialenergy.com.au|72001045184f4f5b959d08d5ce75cacd|76c58198c5744bd984c3598d38f5b8c7|0|0|636641927670289172&sdata=r1fL2agE8GNJp3EMf83qvS7xy0YiHhkDcX+eSYLoi0Y=&reserved=0	Get hash	malicious	Browse	• 104.25.137.118
www.google.de	60e40fb428612.dll	Get hash	malicious	Browse	• 142.250.201.195
	vNiyRd4GcH.exe	Get hash	malicious	Browse	• 142.250.186.35
	DocuSign-June-SOA-Dues.261.htm	Get hash	malicious	Browse	• 142.250.184.227
	XqnM8G36Ih.exe	Get hash	malicious	Browse	• 142.250.184.195
	bmaphis@cardinaltek.com_16465506 AMDocAtt.HTML	Get hash	malicious	Browse	• 142.250.184.195
	VM_5823_05_24_2-2.html	Get hash	malicious	Browse	• 142.250.184.195
	HRXoZLG4ym.exe	Get hash	malicious	Browse	• 142.250.184.195
	Hngx5CdG2D.exe	Get hash	malicious	Browse	• 142.250.181.227
	muestra6999.exe	Get hash	malicious	Browse	• 142.250.181.227
	E1a92ARmPw.exe	Get hash	malicious	Browse	• 172.217.16.99
	crt9O3URua.exe	Get hash	malicious	Browse	• 172.217.16.99
	E1a92ARmPw.exe	Get hash	malicious	Browse	• 172.217.16.99
	Ref#Doc30504871 Wyg.htm	Get hash	malicious	Browse	• 172.217.16.99
	ManyToOneMailMerge Ver 18.2.dotm	Get hash	malicious	Browse	• 216.58.207.131
	Sleek_Free.exe	Get hash	malicious	Browse	• 216.58.207.131
	wzdu53.exe	Get hash	malicious	Browse	• 216.58.207.131
	teX5sUCWAg.exe	Get hash	malicious	Browse	• 142.251.36.227
	teX5sUCWAg.exe	Get hash	malicious	Browse	• 142.251.36.227
	SetupFA.exe	Get hash	malicious	Browse	• 172.217.20.3
	aydrxnitvo.exe	Get hash	malicious	Browse	• 172.217.23.67

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
EDGECASTUS	Ovolohotels-BAD-LINK.html	Get hash	malicious	Browse	• 152.199.23.37
	PAYMENT.HTML	Get hash	malicious	Browse	• 152.199.23.37
	Invoice History-Jroof(Acct. 2632169).html	Get hash	malicious	Browse	• 152.199.23.37
	Zakelijke voorstellen van VGD in Europe.html	Get hash	malicious	Browse	• 152.199.21.175
	New Text Document.htm	Get hash	malicious	Browse	• 152.199.21.175
	obfuscated-html.html	Get hash	malicious	Browse	• 152.199.23.37
	1.htm	Get hash	malicious	Browse	• 152.199.21.175
	#Ud83d#Udcde_#U25b6Play_to_Listen.htm	Get hash	malicious	Browse	• 152.199.21.175
	message_zdm.html	Get hash	malicious	Browse	• 93.184.219.157

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	xJP0w1Ze2J.apk	Get hash	malicious	Browse	• 152.199.19.160
	5QsVJCRQdn.exe	Get hash	malicious	Browse	• 93.184.221.240
	EdQZWKJ8hC.exe	Get hash	malicious	Browse	• 93.184.221.240
	ZDX1RKucBg.exe	Get hash	malicious	Browse	• 93.184.221.240
	#Ud83d#Udcde_Message_Received_05_19_21.htm	Get hash	malicious	Browse	• 152.199.21.175
	SwiftDocument.HTML	Get hash	malicious	Browse	• 152.199.23.37
	7#U1d05.html	Get hash	malicious	Browse	• 152.195.51.15
	6mmD0o5tfL.exe	Get hash	malicious	Browse	• 93.184.220.29
	May Release Check #39733.html	Get hash	malicious	Browse	• 152.199.23.37
	8BDBD0yy0q.apk	Get hash	malicious	Browse	• 68.232.34.193
	8BDBD0yy0q.apk	Get hash	malicious	Browse	• 68.232.34.193
HIGHWINDS2US	TestTakerSBBrowser.exe	Get hash	malicious	Browse	• 23.111.9.35
	Ndt-global_Fax_Message.htm	Get hash	malicious	Browse	• 23.111.9.35
	Dot Billing.htm	Get hash	malicious	Browse	• 23.111.9.35
	PAYMENT CONFIRMATION JUNE .htm	Get hash	malicious	Browse	• 23.111.9.35
	HSBC_Payment_slip_for Outstanding 001005l.htm	Get hash	malicious	Browse	• 23.111.9.35
	Fax_Payment_return906-906.htm	Get hash	malicious	Browse	• 23.111.9.35
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• 173.245.219.131
	Omegabuilders NDA file attach...htm	Get hash	malicious	Browse	• 23.111.9.35
	#U27bf V___oi__c_____ePl_a_yb__ac___k __f__or___ ___Phollerbach_____ _____Skylinenet.htm	Get hash	malicious	Browse	• 23.111.9.35
	ATT00001.htm	Get hash	malicious	Browse	• 23.111.9.35
	invoice_sh.html	Get hash	malicious	Browse	• 23.111.9.35
	Untitled attachment 00005.htm	Get hash	malicious	Browse	• 23.111.9.35
	Evershedsnicea NDA file attach...htm	Get hash	malicious	Browse	• 23.111.9.35
	Paid INV for Robert.landis Khs-net.htm	Get hash	malicious	Browse	• 23.111.9.35
	saturo[1].htm	Get hash	malicious	Browse	• 23.111.9.64
	9553d0dcdf7b666c65cb7d42c092927c8aeae349ef30a.exe	Get hash	malicious	Browse	• 23.111.9.38
	ATT11972.HTM	Get hash	malicious	Browse	• 23.111.9.35
	Remittance_Advice.html	Get hash	malicious	Browse	• 23.111.9.35
	Statement - Past Due.html	Get hash	malicious	Browse	• 23.111.9.35
	VoicePlayback for Mjsansegundo Hispasat.htm	Get hash	malicious	Browse	• 23.111.9.35

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	VM52MC9YQDUO0P.html	Get hash	malicious	Browse	• 170.140.125.16 • 23.111.9.35 • 192.229.233.25 • 91.228.74.198 • 172.217.16.98 • 91.228.74.133 • 192.229.233.50 • 157.240.17.63 • 157.240.17.15 • 172.64.172.12 • 64.233.166.155 • 13.224.99.16 • 104.26.12.87 • 170.140.125.169 • 104.26.13.87 • 170.140.125.20 • 104.16.18.94 • 18.195.138.231
	RFQ40110 (2).html	Get hash	malicious	Browse	• 170.140.125.16 • 23.111.9.35 • 192.229.233.25 • 91.228.74.198 • 172.217.16.98 • 91.228.74.133 • 192.229.233.50 • 157.240.17.63 • 157.240.17.15 • 172.64.172.12 • 64.233.166.155 • 13.224.99.16 • 104.26.12.87 • 170.140.125.169 • 104.26.13.87 • 170.140.125.20 • 104.16.18.94 • 18.195.138.231

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	runsys32.dll	Get hash	malicious	Browse	• 170.140.125.16 • 23.111.9.35 • 192.229.233.25 • 91.228.74.198 • 172.217.16.98 • 91.228.74.133 • 192.229.233.50 • 157.240.17.63 • 157.240.17.15 • 172.64.172.12 • 64.233.166.155 • 13.224.99.16 • 104.26.12.87 • 170.140.12 5.169 • 104.26.13.87 • 170.140.125.20 • 104.16.18.94 • 18.195.138.231
	2790000.dll	Get hash	malicious	Browse	• 170.140.125.16 • 23.111.9.35 • 192.229.233.25 • 91.228.74.198 • 172.217.16.98 • 91.228.74.133 • 192.229.233.50 • 157.240.17.63 • 157.240.17.15 • 172.64.172.12 • 64.233.166.155 • 13.224.99.16 • 104.26.12.87 • 170.140.12 5.169 • 104.26.13.87 • 170.140.125.20 • 104.16.18.94 • 18.195.138.231
	2770174.dll	Get hash	malicious	Browse	• 170.140.125.16 • 23.111.9.35 • 192.229.233.25 • 91.228.74.198 • 172.217.16.98 • 91.228.74.133 • 192.229.233.50 • 157.240.17.63 • 157.240.17.15 • 172.64.172.12 • 64.233.166.155 • 13.224.99.16 • 104.26.12.87 • 170.140.12 5.169 • 104.26.13.87 • 170.140.125.20 • 104.16.18.94 • 18.195.138.231
	q7p7x4f4gX.dll	Get hash	malicious	Browse	• 170.140.125.16 • 23.111.9.35 • 192.229.233.25 • 91.228.74.198 • 172.217.16.98 • 91.228.74.133 • 192.229.233.50 • 157.240.17.63 • 157.240.17.15 • 172.64.172.12 • 64.233.166.155 • 13.224.99.16 • 104.26.12.87 • 170.140.12 5.169 • 104.26.13.87 • 170.140.125.20 • 104.16.18.94 • 18.195.138.231

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	q7p7x4f4gX.dll	Get hash	malicious	Browse	• 170.140.125.16 • 23.111.9.35 • 192.229.233.25 • 91.228.74.198 • 172.217.16.98 • 91.228.74.133 • 192.229.233.50 • 157.240.17.63 • 157.240.17.15 • 172.64.172.12 • 64.233.166.155 • 13.224.99.16 • 104.26.12.87 • 170.140.12 5.169 • 104.26.13.87 • 170.140.125.20 • 104.16.18.94 • 18.195.138.231
	PO # 2367.html	Get hash	malicious	Browse	• 170.140.125.16 • 23.111.9.35 • 192.229.233.25 • 91.228.74.198 • 172.217.16.98 • 91.228.74.133 • 192.229.233.50 • 157.240.17.63 • 157.240.17.15 • 172.64.172.12 • 64.233.166.155 • 13.224.99.16 • 104.26.12.87 • 170.140.12 5.169 • 104.26.13.87 • 170.140.125.20 • 104.16.18.94 • 18.195.138.231
	(1) Voice note-Dassault-aviation.htm	Get hash	malicious	Browse	• 170.140.125.16 • 23.111.9.35 • 192.229.233.25 • 91.228.74.198 • 172.217.16.98 • 91.228.74.133 • 192.229.233.50 • 157.240.17.63 • 157.240.17.15 • 172.64.172.12 • 64.233.166.155 • 13.224.99.16 • 104.26.12.87 • 170.140.12 5.169 • 104.26.13.87 • 170.140.125.20 • 104.16.18.94 • 18.195.138.231
	mJSDCeNxFi.exe	Get hash	malicious	Browse	• 170.140.125.16 • 23.111.9.35 • 192.229.233.25 • 91.228.74.198 • 172.217.16.98 • 91.228.74.133 • 192.229.233.50 • 157.240.17.63 • 157.240.17.15 • 172.64.172.12 • 64.233.166.155 • 13.224.99.16 • 104.26.12.87 • 170.140.12 5.169 • 104.26.13.87 • 170.140.125.20 • 104.16.18.94 • 18.195.138.231

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	3rc4z6ltNu.dll	Get hash	malicious	Browse	• 170.140.125.16 • 23.111.9.35 • 192.229.233.25 • 91.228.74.198 • 172.217.16.98 • 91.228.74.133 • 192.229.233.50 • 157.240.17.63 • 157.240.17.15 • 172.64.172.12 • 64.233.166.155 • 13.224.99.16 • 104.26.12.87 • 170.140.12 5.169 • 104.26.13.87 • 170.140.125.20 • 104.16.18.94 • 18.195.138.231
	3rc4z6ltNu.dll	Get hash	malicious	Browse	• 170.140.125.16 • 23.111.9.35 • 192.229.233.25 • 91.228.74.198 • 172.217.16.98 • 91.228.74.133 • 192.229.233.50 • 157.240.17.63 • 157.240.17.15 • 172.64.172.12 • 64.233.166.155 • 13.224.99.16 • 104.26.12.87 • 170.140.12 5.169 • 104.26.13.87 • 170.140.125.20 • 104.16.18.94 • 18.195.138.231
	iew852qEQI.exe	Get hash	malicious	Browse	• 170.140.125.16 • 23.111.9.35 • 192.229.233.25 • 91.228.74.198 • 172.217.16.98 • 91.228.74.133 • 192.229.233.50 • 157.240.17.63 • 157.240.17.15 • 172.64.172.12 • 64.233.166.155 • 13.224.99.16 • 104.26.12.87 • 170.140.12 5.169 • 104.26.13.87 • 170.140.125.20 • 104.16.18.94 • 18.195.138.231
	6us663UjcE.dll	Get hash	malicious	Browse	• 170.140.125.16 • 23.111.9.35 • 192.229.233.25 • 91.228.74.198 • 172.217.16.98 • 91.228.74.133 • 192.229.233.50 • 157.240.17.63 • 157.240.17.15 • 172.64.172.12 • 64.233.166.155 • 13.224.99.16 • 104.26.12.87 • 170.140.12 5.169 • 104.26.13.87 • 170.140.125.20 • 104.16.18.94 • 18.195.138.231

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	6us663UjcE.dll	Get hash	malicious	Browse	• 170.140.125.16 • 23.111.9.35 • 192.229.233.25 • 91.228.74.198 • 172.217.16.98 • 91.228.74.133 • 192.229.233.50 • 157.240.17.63 • 157.240.17.15 • 172.64.172.12 • 64.233.166.155 • 13.224.99.16 • 104.26.12.87 • 170.140.12 5.169 • 104.26.13.87 • 170.140.125.20 • 104.16.18.94 • 18.195.138.231
	xbK9XyU4LW.dll	Get hash	malicious	Browse	• 170.140.125.16 • 23.111.9.35 • 192.229.233.25 • 91.228.74.198 • 172.217.16.98 • 91.228.74.133 • 192.229.233.50 • 157.240.17.63 • 157.240.17.15 • 172.64.172.12 • 64.233.166.155 • 13.224.99.16 • 104.26.12.87 • 170.140.12 5.169 • 104.26.13.87 • 170.140.125.20 • 104.16.18.94 • 18.195.138.231
	xbK9XyU4LW.dll	Get hash	malicious	Browse	• 170.140.125.16 • 23.111.9.35 • 192.229.233.25 • 91.228.74.198 • 172.217.16.98 • 91.228.74.133 • 192.229.233.50 • 157.240.17.63 • 157.240.17.15 • 172.64.172.12 • 64.233.166.155 • 13.224.99.16 • 104.26.12.87 • 170.140.12 5.169 • 104.26.13.87 • 170.140.125.20 • 104.16.18.94 • 18.195.138.231
	juON02msHS.dll	Get hash	malicious	Browse	• 170.140.125.16 • 23.111.9.35 • 192.229.233.25 • 91.228.74.198 • 172.217.16.98 • 91.228.74.133 • 192.229.233.50 • 157.240.17.63 • 157.240.17.15 • 172.64.172.12 • 64.233.166.155 • 13.224.99.16 • 104.26.12.87 • 170.140.12 5.169 • 104.26.13.87 • 170.140.125.20 • 104.16.18.94 • 18.195.138.231

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	juON02msHS.dll	Get hash	malicious	Browse	• 170.140.125.16 • 23.111.9.35 • 192.229.233.25 • 91.228.74.198 • 172.217.16.98 • 91.228.74.133 • 192.229.233.50 • 157.240.17.63 • 157.240.17.15 • 172.64.172.12 • 64.233.166.155 • 13.224.99.16 • 104.26.12.87 • 170.140.12 5.169 • 104.26.13.87 • 170.140.125.20 • 104.16.18.94 • 18.195.138.231
	HCqVspxrwz.exe	Get hash	malicious	Browse	• 170.140.125.16 • 23.111.9.35 • 192.229.233.25 • 91.228.74.198 • 172.217.16.98 • 91.228.74.133 • 192.229.233.50 • 157.240.17.63 • 157.240.17.15 • 172.64.172.12 • 64.233.166.155 • 13.224.99.16 • 104.26.12.87 • 170.140.12 5.169 • 104.26.13.87 • 170.140.125.20 • 104.16.18.94 • 18.195.138.231
37f463bf4616ecd445d4a1937da06e19	VM52MC9YQDUO0P.html	Get hash	malicious	Browse	• 170.140.125.16
	My_Cursor.exe	Get hash	malicious	Browse	• 170.140.125.16
	rJbYiGadPw.exe	Get hash	malicious	Browse	• 170.140.125.16
	VRs7XsYEZI.exe	Get hash	malicious	Browse	• 170.140.125.16
	y22xwbo269.exe	Get hash	malicious	Browse	• 170.140.125.16
	Delivery Reciept.exe	Get hash	malicious	Browse	• 170.140.125.16
	DhA18Qpbxl.docx	Get hash	malicious	Browse	• 170.140.125.16
	9cYXsscTTT.exe	Get hash	malicious	Browse	• 170.140.125.16
	Oxtmkfwscwhsuadcadttcuzcvsdzksccal.exe	Get hash	malicious	Browse	• 170.140.125.16
	Oxtmkfwscwhsuadcadttcuzcvsdzksccal.exe	Get hash	malicious	Browse	• 170.140.125.16
	Satinalma Sifarisinin siyahisi.exe	Get hash	malicious	Browse	• 170.140.125.16
	bGk64hnnAZ.exe	Get hash	malicious	Browse	• 170.140.125.16
	aiwXQo9A8t.exe	Get hash	malicious	Browse	• 170.140.125.16
	lv.exe	Get hash	malicious	Browse	• 170.140.125.16
	mJSDCeNxFi.exe	Get hash	malicious	Browse	• 170.140.125.16
	iew852qEQI.exe	Get hash	malicious	Browse	• 170.140.125.16
	C1jT7pIYSJ.exe	Get hash	malicious	Browse	• 170.140.125.16
	SWIFT 00838303383 pdf.exe	Get hash	malicious	Browse	• 170.140.125.16
	eOKc6P237n.exe	Get hash	malicious	Browse	• 170.140.125.16
	V5PUg1V7w4.exe	Get hash	malicious	Browse	• 170.140.125.16

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\05349744be1ad4ad_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	410
Entropy (8bit):	5.631367386364176
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\05349744be1ad4ad_0	
SSDEEP:	6:men9YOFLvEWdM9Qzalpqzwi7Z+P41TK6tu+en9YOFLvEWdM9QBwXlyOFwi7Z+P45:vDRM9VQzLZiEknDRM9WQyOFLZiE
MD5:	B8036E53DE5494EB3838E4323B1FDC17
SHA1:	D09D7136ACABB24F2B694DE579558FA2EE7CB280
SHA-256:	E673F3F0C08A5EF8D66B32EAB0A800A025D224760C9B05A8147F6997DBB32B61
SHA-512:	C42C1519FB501B85AF15021B5BBDEB887AA901D7742FE9C1BACC8F313FCADFECC227FA1ECAC3E57EA305E373CC9731CE4595102E994591C22AEEC1D96783A A4
Malicious:	false
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ..-\l.%/....."#.D..J;9.A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....r.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .r+zl.%/....."#.D.z.K;9.A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....H.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.567201181259089
Encrypted:	false
SSDEEP:	6:mi9NqEYOFLvEk7ql6B8Be7Ywcr1TK6tri9NqEYOFLvEkXEna/liWZ8Be7Ywcr1Te:V9zy69PQU9z3oet9PQ
MD5:	03899E0B104923ADF93F133A9D4B7F72
SHA1:	49AA730ED60E83F8B1FB95CDE55EAFB197BD3229
SHA-256:	DB0DAB34F044329F3694B17FCAA3FAA84F5B50BBD81220BAF4FE2BA7393696F6
SHA-512:	8AB6065AA61BC7D438FFF212526043E895B596A0F3159785C826569C97C89A8BED295EDE1B685DCC152A41FD6A449231CA04D243A97177476D24AA675C6DCC5
Malicious:	false
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .>/II.%/....."#.DZ.3J;9.A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....O.3.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ..el.%/....."#.Dz.J;9.A.1.x.'.vl..*|Z..o...+.4....0..A..Eo.....A..Eo.....O. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	492
Entropy (8bit):	5.602075088215726
Encrypted:	false
SSDEEP:	12:DyeRVFAFjVFAFMHXtQlUo6jvyeRVFAFjVFAF1tiKlUo6j:tB4v4wOSBRB4v4HrSB
MD5:	7DC82A76072DC5BF469CC2F7A4FF2A32
SHA1:	04C109F9B0629D352CD146ACA3D1C1E96B5F10FC
SHA-256:	CEB087CD25E4D206725AE9E8B122033304BC35781A702DC7E5052B1490C5D80E
SHA-512:	7A339266F39149B048697475F2929CF8B8729091C24DFF610B2560E9ECBE73DDDDCDBD4415739F6DA5D780842D4701E2F223EACAA6FD07B89C2DC94ACE0577F
Malicious:	false
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 ..r[l.%/....."#.D.).J;9.A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....l.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ..xl.%/....."#.Dqs.K;9.A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....Q]GN.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0ace9ee3d914a5c0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.612183218980479
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RsgrXlWO9V2iWulHyA1TK6tlt:lbRkiDb1WoFWussS
MD5:	A401DAB9358E6938629E282830DF8E8B
SHA1:	011152C467696D1D7A80463C19F7D85268D9DCDA
SHA-256:	074CE86F9EF8528E937BD3AA09511C5F876F10354270DB227DE2D1C54EE97A09
SHA-512:	C253F66208CD015AA2258070B6AA57AF39952AEBA9151266771377C17169FE95DB4DE9BDB142E76A7651CE82D0E48B165D3AE359E01CCC05608F67A74C3B57E
Malicious:	false
Preview:	0\r..m.....h....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js .r.al.%/....."#.D.+.J;9.A..8 P..a...R..Y....7.@..2Dm{ ..A..Eo.....A..Eo.....*.e.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0	
Size (bytes):	210
Entropy (8bit):	5.523061669328752
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVu0l6oVyh9PT41TK6tE:pyixRuyFV41TEu
MD5:	F2A4E446BB6307C55BAA92ECD5D94165
SHA1:	1DB581D79D3DFCCEE448A37BC5A945E20BE5BDEC
SHA-256:	C0F3ECDC02A4894074C70A57C0379CBE3739C4588FC911F78FB734AA0D25E335
SHA-512:	B837033F651D5DE417BD81C5F1F70CBE42B84A309276DAA132019EE902E2A20B1AB1D23BE99C8E70CF5E3C24C2B82EEEFE5385EBAD3AC02562C0812FDD3C9 4E
Malicious:	false
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ...yl.%/....."#.D...K;9.Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo. .....pA.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.610581425397747
Encrypted:	false
SSDEEP:	3:m+lifll08RzYOCGLvHkWBGKuKjXKoyNjXKLuVoYlNXLrSco2sZI8xeGvP5m1TK59:mvYOFLvEWdhwjQ2lJSLZII6P41TK6tm
MD5:	84757453D09423B72796D2C461B3BAF0
SHA1:	2E93FD5D042A0C69082D163ADA79EF273D6B5213
SHA-256:	99B8A3D3C6E99943E549106D31B3EC2FB9AB6202B5351E1BB2E057F0982BE486
SHA-512:	E0788D60376F949D659E2299DFEC85F66BE617C82F4DE6E621B8621959B2D9C5AE43B2AD967488CF16F1DD048D325A83A21479F87F67B58343F0803CBE42A243
Malicious:	false
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ..ul.%/....."#.D..J;9.A.].>....uUf..N...k.....c..l.A..Eo.....A.. Eo.....PqM.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	209
Entropy (8bit):	5.522026165522653
Encrypted:	false
SSDEEP:	6:mJYOFLvEWdGQRQOdQ5YXlDK76g1TK6ti:2RHRQCQY1271
MD5:	49350D11BACE5E5932C6A51BD6A2F3A6
SHA1:	ECD35625A14B850365FC9208FD787A23F714FD89
SHA-256:	CDF655F96E3CAD097D33E63F8721D8B568EB116F08EA46A8D584D6CE39594D2B
SHA-512:	3F7621C252C0C2F90FA119BF013AFC494CF2B7E938D6D99D35FDCB5FE2395D00BEBB27210EF0B59FAC463BD5A8DD1630AF7B88D97A3B67D9E930FFDB9570F9 FA
Malicious:	false
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ...yl.%/....."#.D_..K;9.A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo .....F%S.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.535300440652965
Encrypted:	false
SSDEEP:	6:mOYOFLvECMLko+tlZJsyNMuR/41TK6tjBOYOFLvECMLBY/l/iNMuR/41TK6tKd:Z5MP+XXbNMuR/EQ5Mq6NMuR/E
MD5:	DB12BA863F31B823862FD8C160DA8850
SHA1:	F7C14EBE7FDF7662364B409DE68C1163281F2A37
SHA-256:	EE21A89CC58AAF10E8E863055B9849C98F855CD6F0A8925A070EE3D73439D3DF
SHA-512:	468E7EF79D42B596BDAC4DDB60FF792D98B8103A144DDF38E5C9782262D7AD97FC7AA7FB66FE53E9EA33DA37365EF7D83F0A7FAB4BA000C184D87004A774DE D7
Malicious:	false
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ..3Il.%/....."#.DWB3J;9.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....?M.A.....0 \r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .T.el.%/....."#.D..J;9.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....\:.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.491158493224576
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtu6FqlscYby0zBUKSAA1TK6tVMt:pRascYbeTE
MD5:	5F601961F4C5B59DBB999415449EA68C
SHA1:	FFCD7729A39E473C446D97B6C6C707753FDF3F9C
SHA-256:	A4CCA91E8E995883B250DD2E8EDEC32872978FAA6241C71ABAAF470C79A9E4D0
SHA-512:	950121A62EFD3817FF3DBF71E0EB94A1A279411CE2F16435368FAA629EDEABEAC9BCEF2B3DD5DC5FD66300D71B4DC10FB2898C0584F7ADA5F7993B863ADED A28
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .s.zl.%/....."#.D8..K;9.AQ..E.=....=h`t..t..3%A.F$..w..A..Eo..... .....A..Eo....._..Q.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	354
Entropy (8bit):	5.576863420904836
Encrypted:	false
SSDEEP:	6:md4HXXYOFLvEjMSWFv2XlyctUdyP41TK6tO8d4HXXYOFLvEjMSWFvNJ+l/lnkbcJ:KkXxKMSCv21yctUlbkXxKMSCvNIXnwcW
MD5:	18C1BC7D81E81365ABA76449A8407589
SHA1:	A6FAA5FDCDEDBA8007FA279A473897AB5F6F39C3
SHA-256:	88880A945D51AAD4D83AC5E47FE9DA05A41A35C16C2F1301424828B0D388B894
SHA-512:	04C3EB5E310241A39511D9A89DA758BC1733FA3C44AC19F5EB2DAA61C57BCCDB8FD2489E45A0FF34F42745CF30393FBF8AD2A26E26A67B2EC70152D19C7DD5 F7
Malicious:	false
Preview:	0\r..m.....1.....5..._keyhttps://rna-resource.acrobat.com/plugins.js ..1Il.%/....."#.D.)3J;9.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 ...el.%/....."#.Df.J;9.A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....x.?.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	374
Entropy (8bit):	5.6024840107885225
Encrypted:	false
SSDEEP:	6:mkl9YOFLvEWsfOL6BlMkJyM+VY1TK6tPCNMkl9YOFLvEWsfOLoZlEyM+VY1TK6tE:5h6OLg+kVCBh6OLob1k
MD5:	8998634AA86B6651792C68CBE544F2CF
SHA1:	D0B205039A28F7B441561FE5E12C536E967C5304
SHA-256:	28374F1610E0F06A067E71112130ABE1CADB6980F0A7C7FB009588D71F8652A0
SHA-512:	A982C8522BA8037C526A5EE1EEC9FE9333DE955B1CB021626DF90D03A6BC353FF0036A87F715B3286F30D1D3922AD86031B3E526747048B58927A5B7460FA485
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .&.Ul.%/....."#.Du.iJ;9.A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....&v.....0\r.. m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ...rl.%/....."#.D4..J;9.A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	488
Entropy (8bit):	5.62611979250714
Encrypted:	false
SSDEEP:	12:URVFAFjVFAFyXelKwSeKaTLnNRVFAFjVFAFepWKwSeKaTLn:UB4v4yu0wzXLnNB4v4kBwzXLn
MD5:	F78E633D1937613D5ACDAADD31E43126
SHA1:	DFCABF326896070D4EA7A04B3D143D02A99B336C
SHA-256:	CB3226BF7D254242ED27CD0D135D987619574C9A6B317F6EE32C9E975CC9D4BE
SHA-512:	60FDF678DEDF2D21F69838652757A666439D389C3E3D1DA7658FD9F901B9E19D0192400F55EE2642682E3A4708D63CC83AAC423E8CC1352B6E5FA8E38182511F
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0	
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 .52\l.%/....."#.D}>.J;9.A.....H...{...2. ./.k`..r4.C. .A..Eo.....A..Eo.....V.....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 .F.yl.%/....."#.D.g.K;9.A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....9..2.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.441209077030568
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXuzpY/l4H11TK6tJl:BsR2EsewatQvl
MD5:	B74BE37ED647FFEFDEB1563F937C39B2
SHA1:	13A3EFE6C11F9D17376D528E721944A44B510CEA
SHA-256:	C9111AA6D6EC4AAC5E628D2B210600C87C80A9E1B39839F071117C2180CBE8F4
SHA-512:	86F4B7B3F9005A34E2F3F9103DF39B8A583DE0E88073724F327F4551E10787C0264251ED580243011772DCCE6321439BFA7A692F3155D9557C213787DE74F62E
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .<.xl.%/....."#.D...K;9.A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.606324793318914
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQ8ltltlrR+B7OhKlvA1TK6tB//:RbR165lXtKBJk
MD5:	C6345AA4E1D8ED9A0167ED4C31098EF1
SHA1:	1E118335ACBC1D5BE48908BABD64C4A44FD7D7AD
SHA-256:	11993DDC87D729B5E3EA4105D57CC2C0AEA1AC5EFD66AEA9D00A9E98537BD5F4
SHA-512:	18C4BF06E64C28086A8071DAAEA695BAC5E2FBEFE5FE9C4DFB9E5E643E7F1A04159A42A82308C12B5270FA7CC15A615B6FB7FE73ECD2164AAC528E6E9FED385D
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js .7.ul.%/....."#.DOt.J;9.A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....% P.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.562129969493633
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVuO/lhQdFt1TK6t0:B2geRHRQ7th0e
MD5:	65992BBD3E3D5A597B99DD76F6997AAC
SHA1:	419008081C7D8D8953A46B37931AE10ACE1154A5
SHA-256:	999097674E9582EF216BD7478E38D0FBDF7700DD26C66F4A1D4E3B38EE08454D
SHA-512:	00294BBB27B178B7B3CF9B136A49943D5C7A4A519E34A7FA08357D9BB98C10613B6891EBBF887FA3359C203902FDC4AF2CB38CC199CA4F7F73E8F06AD28B61A9
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ...xl.%/....."#.D...K;9.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):	412
Entropy (8bit):	5.6014811540458425
Encrypted:	false
SSDEEP:	6:mzyEYOFLvEWdrIOQtfleyt1S/1TK6tKzyEYOFLvEWdrIOQlfl1HL9Fyt1S/1TK66:WyeRlwNeyt1wQyeRlYNNbyt1w
MD5:	0E3B1F3840C30339B01274E334A560BC
SHA1:	02A1DBBECD0FEB106240012450699DAF50B96718

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0	
SHA-256:	D2AA310B19EECF8B23BBC96045AFCAAF4F9009EE0BF03D913CEC7D521C52F50E
SHA-512:	BD8B83EB3632C6EF3CD232C74216F7A13DA4ACEC34990FF2521C1DEA6A5DECB242FF6DFAA3F381932CBF8A943E2D4CF340FE851C05E1C7DEB39C9F1C87F6E DCA
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..zXl.%/....."#.D.<vJ;9.A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.... .."..D.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...rl.%/....."#.D...J;9.A.t\a.....x5.'OuE.C..@.....x..A..Eo..... .....A..Eo.....D..3.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.53167617200027
Encrypted:	false
SSDEEP:	6:mnYOFLvEWdhwyuxXlF9JCqwK+41TK6t0:wRhqHJjwK+EO
MD5:	106D12C771D0BD71661291836E29C22C
SHA1:	07BC837D93C846273DBD9C091ACF424CEBE3F5D3
SHA-256:	2DBC106330FB121169A5411E8C7182FEDE9C8C494DDD65C4DBE95D4301E20AE0
SHA-512:	B36B5CB399EA5D46D1518D3A341E2F4BBA83F498DCE8551DE015767BA0C1F97B6ECD5D20C4D7B69788EEC1C7F1196A28DCDFD42F0BC301FF8F95FDDC986BE DB5
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ..Eul.%/....."#.DR..J;9.A.....7...o..a=.98I.....(3.$G.A..Eo..... ...A..Eo.....f.c.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	460
Entropy (8bit):	5.6047835337528635
Encrypted:	false
SSDEEP:	12:/RrROk/nCLGfIfLET3RrROk/x4bveNIfLEB:/PJ/nCLKI4T3PJ/x4bGNI4B
MD5:	C4206C2D9F611E5AE3C01DB4E981AF64
SHA1:	D1FEB36CB22B6B218D6BA22B1961F0DB60FA9917
SHA-256:	E65EAFE7B57B43DFE6BB796ECD0BA20C97EDEC32EB10B9E05C274EC394722B70
SHA-512:	3226FC40A701CCF0DE40B3B1F7F981F2C50311398C217B89AB2FC9A8ECD98F841EBA4A47ABE4A49B3EB24FAF19ECEAAB5B78D3FF7AF8FE7362B5EBEF1AC4C 366
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..xXl.%/....."#.Dx.uJ;9.A..~..rw.+[....!.)?..f.U..(=.=. A..Eo.....A..Eo.....O.G.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .~.rl.%/....."#.D. ..J;9.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):	372
Entropy (8bit):	5.59600185472567
Encrypted:	false
SSDEEP:	6:mmDEYOFLvEWXIEtlqUuc1QPLr1TK6tc2mDEYOFLvEWXI+a/luK1QPLr1TK6tS:xqTHqU9CPLneBqTQBCPLn
MD5:	AAFE94154D023A0919ED512F88934DEE
SHA1:	4388BEE76CBCF5B53ED498AF9408490893D5D062
SHA-256:	3C82A1D5137F6C31A23811AE5965183058AC9E899D96F8F9B27BEBA4AC47E350
SHA-512:	C54C13265AC617CA345805F18D978468D906BFFCB60B371566E28CBD6450E8BA396935283F3BF1B4CC972D6770F9EAE1AE4259DFF21CF40063ED7375CBED916
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ./LUl.%/....."#.D.1iJ;9.A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....0\r..m.....:. ...f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .`.ql.%/....."#.Dq..J;9.A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....9.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	414

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0	
Entropy (8bit):	5.64236402200417
Encrypted:	false
SSDEEP:	6:m52YOFLvEWdMAusRflEhLsEJ41TK6tb52YOFLvEWdMAuudNa/lMd69kjLsEJ41T/:zRMKRN6sDERMgNatusD
MD5:	748842A3BD8D7F10891DD872B942CF59
SHA1:	58E1A28EB3359BC004E8C27D61E20E8062387597
SHA-256:	6E886D9164FAA0963E90565060FB2E77AE9C67C07D79F14358137E9FD24C77EA
SHA-512:	08AD58DCAAD4D44748D8BDF23CCF02DE2D741FC081E0F3206360FCE97D509A7B2F735B669BBDF8DE00465F293C2CC038F50E1B80D83EF30484C57649868A3DE
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..l[l.%/....."#.D..J;9.A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo..... ..F.al.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .?.xl.%/....."#.D.O.K;9.A..z._a...'.v.....4p3..1.']...A..Eo..... .....A..Eo.....g.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	420
Entropy (8bit):	5.561782573835897
Encrypted:	false
SSDEEP:	6:mYilPYOFLvEWd8CAdAuhl4TFong1TK6t6YilPYOFLvEWd8CAdAu1laAgl+Fong1M:6lJRiMFoM4lJRCaAgYFoMa
MD5:	2F9CD65101ECA8A412ED0A2F1B7D6CA9
SHA1:	AB43E799CEA3F2117F8493D3782E81990787E0D5
SHA-256:	D5D54E81C3CBD2551B247C1CE345D2F4E0C8CD1A151F12A8FFEFDB55F1C45515
SHA-512:	351B593D167063C2E1BAD862BE9B7A28C233B2DD9A8F879EFB1B9ED284A649977CE66EAD8E7D69609990871891DA6788556A96286E4BB775B67DC8797D2B7B0
Malicious:	false
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .so[l.%/....."#.D...J;9.Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....<.~.....0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ...yl.%/....."#.D.e.K;9.Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....B.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	446
Entropy (8bit):	5.552864707967124
Encrypted:	false
SSDEEP:	6:mY8nYOFLvEWdrROk/Iue/l5e16wG1TK6tT9l/2Y8nYOFLvEWdrROk/Iu6Iflbe12:F8hRrROk/g5e2F9l/V8hRrROk/fbe2
MD5:	1878E7D60B0734584D30F1B15E046A64
SHA1:	A728711E4A79C822919E477B108070811933AD00
SHA-256:	46DA81DF68DA583D6CA2AAA5A077A43131A94248E5F79A93E72C8C3BCA800E35
SHA-512:	3494F17B34BFB5A89987E782FAFBC8B95082350F58A4393DB63AC205A1D93D6EBA1DBC1A0B48A3AE201C09F1390292703CB53180DEB776AA610D90AC806D77CE
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ...Wl.%/....."#.D|.tJ;9.A..%.k.SZ..~W.....:)'B..ad.....A..Eo.. .....A..Eo.....%.h.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .).rl.%/....."#.DXu.J;9.A..%.k.SZ ..~W.....:)'B..ad.....A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	426
Entropy (8bit):	5.651222876148405
Encrypted:	false
SSDEEP:	6:mLrnYOFLvEWdrIoJUQvlK7rNJli1TK6tLMLrnYOFLvEWdrIoJUQVFlKirNJli1TA:ehRcqK7rNJlCahRcmffrNJlCj
MD5:	A04BAE023E8FB7BB7FD682A03C5D2565
SHA1:	EB7035711890EE2585B1AA2638AF44199308412F
SHA-256:	D63AAC188FFFF431CC85EEBF3C070935CD40FA8909FBDFFF2DF853B3F93AE9EB
SHA-512:	91AA56E8726D8E6ECC3961B73B21C2DCE834613A1067F130BE2594BFD0B4F35CD524A691E8038FE6F59E59428AFC82A5963ED5E5881821BB0A8FC02A823A310
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .+}Xl.%/....."#.D..vJ;9.A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A. .Eo.....@m$g.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ...sl.%/....."#.D...J;9.A.;"./N_.,.:C..2....9L.H...3:...A..Eo .....A..Eo.....+.-.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.574094460638712
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhu5//lPoLzgm2d/1TK6tm2OEYOFLvEWdrIhuSl6DGLzgm2d/1T/:0RZP+Re8kRIWgRe1
MD5:	814D84F315D1BC5A569EF81A3097CE64
SHA1:	32573CDD3B15E60B6A17ABF49FDB1E5FD398C058
SHA-256:	3A143A6E9C6CA881B4BFB31E9825AF2E67E3F415CA94894B988F65A1B9750743
SHA-512:	C521CB0DC1B0CA657483A04BA5065B936F327BE65357499D886E91AAF80205AC16A90ECE472AFE8F8121BF7ED32486F4DAA719974C2B05AB740A01FE5327652
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ...Wl.%/....."#.D..tJ;9.AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....97.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ...rl.%/....."#.D.?.J;9.AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....;.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	376
Entropy (8bit):	5.638992316282802
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1Kfa/lBMvkx56uvp1TK6tgAElVYOFLvEW1K0lKkx56uvp1TK6tV:6JJKfeGwuJJKc5T
MD5:	57CDE4F6BB0A5B8253509EBE5E59A85F
SHA1:	1E5433E076F1D41FAED0FC8DC42990CFA57FC17C
SHA-256:	82A8CC487C1334FCE2A15C4620F33F7B090C6DB4C1AE74D40C8F018F6B91E9DC
SHA-512:	D68E9C86617452549158E1D3A7BFDF2C530A37BBFADE651035B50CEE5634C991D2BE73A590298D8AE3CD910DF9AC4B6666DB8E680B65328C22ACAEBE7D864F26
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .X.Kl.%/....."#.Da.EJ;9.Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....z.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..ghl.%/....."#.D]..J;9.Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....*.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.603505543128248
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvuhY/l6hYvhUDLYtmOZn1TK6tJu:xRBJyYt6hYKDcFZL
MD5:	370B3A4A2B23A22EBA030DC362CBB1FE
SHA1:	39EDF4A342CA68A929AAAED9205E7F6BC47A9D09
SHA-256:	C6B18E87672CFCAB7044C66D55272A988BC7071E691E88558769C7E0F25B1299
SHA-512:	84F3A220882151EFFC90BC5C62D2607295D797DD63F800F71E4DB0DDA82D6A20785B342D334D629B76714ECDC2BBD718A1E92D55AB46BDF1D22E002BA29FAC4
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js .J.xl.%/....."#.D'3.K;9.A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....\KD.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	422
Entropy (8bit):	5.5908391440584415
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp72tloGkVPu1TK6t9sRPYOFLvEWIa7zp7P2A+l/laVPu1TK6t:BPHIoHc0PHxeac
MD5:	7C0EED4CEEAA2D297BF5D1FBC1FD21AB
SHA1:	A4A577DBD994FC5FB2EC6A1B2FEF59A50F6522D2
SHA-256:	610666F491B799035631CDDB9FAB797A5F9815B67031AD750D2E6E018E13F5B8
SHA-512:	45B3E9B60019E21A5CD8CC71636444F59B62C7845927E96862260385E6CACA1DE6B312B9F933F32D923F1CBB4ADC461C809B50C0843BD816952B0FC3C03456A
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0	
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ..@II.%/....."#.Dn.3J;9.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 ...el.%/....."#.D/..J;9.A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.577205503307506
Encrypted:	false
SSDEEP:	6:mKPYOFLvEWdENU9QvItlT4DiM3Y1TK6tq:bJRT9bXkr0
MD5:	852AA07E458CAFA2CB3943C2D4A52343
SHA1:	5EF5367E110B2473E09F90821F40D87916471F29
SHA-256:	C85E875BD90F0493D153242E97682F042700131CF9DB74780FA6775AE8C85750
SHA-512:	87272C565400C7CE5494123103092E3D69ACAA7D5B5540ABB866923789346134961174D3530D0633C441626F76F0F811379F6897365AD094E8F832B76D1CEB71
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .u.ul.%/....."#.D)..J;9.A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.....<.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	modified
Size (bytes):	208
Entropy (8bit):	5.627034964733469
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQulGjBRCh/41TK6tb:XRc9tGDi/E
MD5:	A9E94D7D10F512914A9C9368566457C6
SHA1:	2BF1CC43EBB46F13A8D09D3626CF939C55B85762
SHA-256:	F3BE540F2EEEA605B2849359B369DDD2DD8A3C9848E06AD24B2D096702038E65
SHA-512:	DFDC5647393EAD423F16A6D03306A270EC356910EF7F13498FBA79DB7A7A2E9E33145C6D3F6C0E8F22D7171AF88E4D6B41577A481E04AF266B2C259738885C3
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ...yl.%/....."#.DQ..K;9.APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.....8..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):	231
Entropy (8bit):	5.595809472176217
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhuhqlzULlF4r1TK6th/:bs6xRkiCQLlF4nX/
MD5:	03E60F16E916F9DE235FA0A258E4A4C4
SHA1:	D9308770E2BD87083FE44882320EC8F27831AE27
SHA-256:	165BE7724CEE3D4FCD68985DEF46A3C4238E0D2254B058F9A62A9096949F9A53
SHA-512:	7FB5E3CCC760D18FC554E9001331D2B411930F0690D6FF0C8CA72DE5F7BD70040E3A0A452DE7EACDB47AA5788FB27B07A099A2493406782B0B8DF4A0EE01B0/E
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .q.Xl.%/....."#.D..wJ;9.A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....'*.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.502660723567978
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFv7IwXlpV9Lqrcu1isLK5m1TK5kt2:mhYOFLvEWd/aFuRIwXlMY941TK6t2
MD5:	26BFC865D110BA26219B4A5FA121E16E
SHA1:	DAAA63997044968FA4C1FFA243424236FD659985

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0	
SHA-256:	8360F9E2DB277B7CA49C92EA583749D8CAA33710C3D8BC8E79F2D4F8479D4F3F
SHA-512:	BF0F4A932BB5E7ABA1597C2A5F532A74D44EE11893D674C6C001C61395C5B719FD5715902571DB5D84934DA52EECAF31C9D6E2F4321047F829BCBC8E59A75D(
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ...zl.%/....."#.D...K;9.A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A ..Eo.....R.o.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.4917734433973155
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQQ4flbrWBoBMqVd3G4K41TK6t:2DRuRubrWqB9Vd2k
MD5:	2BE56A74D2F3D7A32CF17623D7C6A45B
SHA1:	3C77BB1693B2CAA2AA00C6C97AFEF8172573241F
SHA-256:	EBD544D3635F10C60271C70EA79362F03CB8AB51CD054AFCBC2F3128AE194A90
SHA-512:	201477968F002303AD1F73CE3DDC172A04AFB6AA9061476E3B270D845FAE7A62704F396AA8243E46087C97F99861F3ABFEBC98EA69110253B56EF73F9D902D42
Malicious:	false
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ..xzl.%/....."#.Do..K;9.A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.. ....c%=g.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.603431399923493
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9QbalOoNuA424r1TK6tflekqYOFLvEWd8CAd9QkXlvmuA424L:+RQhwrnT2RQF1Rrn
MD5:	8A11C6631DCF4EF5156606CEB5A04366
SHA1:	20720B5E07EEF7F29658DC8F53333E571FB323E4
SHA-256:	ED006E7A049F25458DF91D32985B3C606E3A3D6F057826250990859368A632D5
SHA-512:	0DCD15A74322157A495055DD5424026E8DEEB922288BA575BEB681D3FEB7028503EAD2D934ED8E56D2B6D27C4EAF8B341DCC7D18B462FC32F7352721ECCFEE 75
Malicious:	false
Preview:	0\r..m.....P...gT...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ..0\l.%/....."#.D}X.J;9.A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo... ....g.....0\r..m.....P...gT...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ..ezl.%/....."#.DT..K;9.A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo..... .....A..Eo.....w.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.551762603577627
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAuNXlrJxyC8n1TK6tq:xhRT/1rJx7Qs
MD5:	A2D576F9F879D0833F29088651D410B4
SHA1:	72A52B9CBF481719B91B2298AA514704AE37E826
SHA-256:	1942C3854242099F1E6E2167997A8E2698A6919E79BC5B4879FB0C4066959565
SHA-512:	9F2F751BA4A93BC279AED17CAE92A8B5A7A65B35FC26EBCEBF6D9E850340BA5745FACAFA776A01FC118B696E8DBFEFF3CAB6AD28040875CCEEB45E6F60A1 566A
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ..CuI.%/....."#.D...J;9.A8.../...;.\\o....1.....+..A..Eo.....A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	442
Entropy (8bit):	5.613722331987245
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0	
SSDEEP:	6:mQZYOFLvEWdrROk/VQrlC8LmB41TK6t5leQZYOFLvEWdrROk/VQXFlS/LmB41TKj:nRrROk/VSCdmFRrROk/VQSimCt
MD5:	B471509454780A0A0F1E95443C53E420
SHA1:	D7F7013284D195533ED414E052B777A6347271D8
SHA-256:	08AE7DD2C3A66EDFA15D8F5A063114F43F2C7A69AD1FC777E6C112073DDB59E3
SHA-512:	72E962E2E13643B6C62B8263CD75E683ADC27B93B7C23A0BDDF99F4A0825838CF97D83A052681DE216DF2391867D438AE57A89E9F4B970391D81263632EFB118
Malicious:	false
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ...Xl.%/....."#.D..vJ;9.A ./.ev.....N~..6.b....$.j;:C...A..Eo.....A..Eo.....*d.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .u.sl.%/....."#.D...J;9.A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.587682504461872
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWuaG/lHAdm9741TK6t:qxRcDtHAdu7E
MD5:	28738F638533B799A6EA6B18A5BE42C9
SHA1:	BB3D2534C39BB486BD525F86D9781544DE02FA3D
SHA-256:	B039F9AC16AAF5551A78E23708589AC12F98C26DA95307F4058B6A199155896A
SHA-512:	619A569A59FA696A0C4580DCB74565FDDD81FE6D8479CB8E368D6D78F460FE67915D6556841B327EF6F45DF59CD875960510D27F37B8D0CB9EDB1659F94D1C5
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ...xl.%/....."#.Dd..K;9.A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....).'.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.54501903672754
Encrypted:	false
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFv732Aql08Gc7nB6shoq+Nem1TK5kU:mMOYOFLvEWdwAPVuR3nql0TJn1TK6tr
MD5:	D5CB0B0D3B77A4151870945CF4E9E464
SHA1:	34DDCF0019951E38517C661DBBC74E3998E0CCEE
SHA-256:	3FF8ED566DFDA22173BD7289D809FC7ABD5DCB7235C4AE5D4E6E9172AD7A0C05
SHA-512:	52ABD0E21825C1339CADC15526FC5E86C5482E5CAC4837B5C57F9905191FE9939462F08A404DFDF751DFF1CCDBD115094FE4F88300E0FEC79C06875C8A3CAA7
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ..Aul.%/....."#.D...J;9.A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo.....}.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.622745630988309
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQ1lD2zhcsBXIh1TK6t:mxRBJQwD2DB0
MD5:	5640D42FD6DF3A69A368F639214B13A2
SHA1:	61DF7F7ED725C2CD1F0FC2B3DE235336DA45E293
SHA-256:	F34317AC5292CD2252DA43FF55AB5476FB77C4EC8CAFA6AF804A3EB37DCD2764
SHA-512:	3F676A7F33EE75F1233F5BDCA6B1756D6D09EF5E75A1F9CC996FA7B6B68BF1DE5D09FD8E2EB3179F8CB5BF34408A7C081D97D573EC2ACD700C4DB939AB588AE
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ..$zl.%/....."#.DH..K;9.A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....gJ.6.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0	
Size (bytes):	456
Entropy (8bit):	5.582817865573499
Encrypted:	false
SSDEEP:	6:msPYOFLvEWdrROk/RJUQwXl6vD2c3Me/1TK6tl/l2sPYOFLvEWdrROk/RJUQwNq9:3RrROk/sJ16vCcGFRrROk/sKUqDc/E
MD5:	92DFAAF044C041DB1A3F4E514BC2F830
SHA1:	E237341971645783FCDF9368550BD022EAC3FD00
SHA-256:	3C4D713E75DCEE13371EC683EDEEC99E31DFE08FE1C36210951CCC2E451DD809
SHA-512:	A5A4FF28C329F25CEE54C2659CE7C531E82445EEA2E07873C10A5A66FBF0D7BF65102A7363C604E011ADAA9B7860A9D14280BD5B473A060CEFB5D6949796FDD
Malicious:	false
Preview:	0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .t.Xl.%/....."#.D.!wJ;9.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 ..5sl.%/....."#.D.s. J;9.A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....'.M.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	2016
Entropy (8bit):	5.317744599802361
Encrypted:	false
SSDEEP:	48:JGnojTcmSBoAClnFZ4Nq8rZ0OEyLqAos1gAbH+6fUMPdYyy+HnO+NW83PFEUZ:JjgoAWnDOq8rZ0PyLbos1gAbe6fUMFYc
MD5:	E0E0906FA0FE8CAE5B949A6C54AFFC4A
SHA1:	E9D5F853296F19C625B9D00255192868E3309D6B
SHA-256:	DA245279CE40E165BE77924D46A1A3FD73B43BB24E6D03A77CAD049F958027BB
SHA-512:	D60E53A99F36EBEB38D2B23BE621F79891E61244D45EDED8849EEEC87C2BD6423A3AE9C7CEE72829C81D46360481E399BE318BB252807EB1AAA59121B8981B4 2
Malicious:	false
Preview:	....U...oy retne....'.....'.....:.y~A.@.....*..@.....oB*@.....#...(@.....k7A.@.....D.4.....[.i..%.....<...W..J@.....,+..._.#@.....J..j.....6<|...@.....A?.2·.....+.{..'.....*)....J·.....2q....@.....P....V@.....+.U.!..V.....P[. q@..... .....!...0.o.....u\].q.....@.....*.....o..k.....^.~..z.....o.@.....Gy.'.h.@.....F..=z;.@.....3...@.....v... q..@.....C..M..@.....a....@.....~.,.4>.....&.S.....@..x.....=....m.....;/...@.....q.....MV3.....:..N. A..@.....PUoy 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):	295
Entropy (8bit):	5.272348053206672
Encrypted:	false
SSDEEP:	6:m0kt+q2PN72nKuAl9OmbnIFUtpp9ZmwPpqtVkwON72nKuAl9OmbjLJ:HvVaHAahFUtp3/PgT5OaHAaSJ
MD5:	8C0BC11E0D5BB78072D85599903BB678
SHA1:	4BE980B4EBE046889009679A0B44B028ED699D7B
SHA-256:	296FB4313951FE303952AC3DA875F81840DB4B1F38584525E93114B41481B8E7
SHA-512:	6D5C54ABF61874CA66AB6334EF947C8B0FF3A400714E76065579120E4CC85AF128A6883C53117F194A8B67CD030A6A0AEB7CE6816A365BFF8659B4954AA7D5B8
Malicious:	false
Preview:	2021/07/06-16:54:17.792 fd8 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/07/06-16:54:17.797 fd8 Recovering log #3.2021/07/06-16:54:17.798 fd8 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	917504
Entropy (8bit):	0.007716873612814605
Encrypted:	false
SSDEEP:	24:T+X8l5mv+X8l5mv+X8l5myrY5mrY5mmHY5mmHY5mm:To35Oo35Oo3525T5K5K5
MD5:	545783574F55AE7B68107D94104DF5DC
SHA1:	A165613C78A951FE14CC2DE4C0119545FB09CB97
SHA-256:	4FD5A8538D675D352B60CCF8E1EE7BC3A43F35696354EAFF170465BBD8D6D2B0
SHA-512:	8E235F34944EF6299185ACA3691FA27C31BD81110EE08898801A333A0D4C6F89D398AAC6AEC54C1CAA649C592C3F9F008DF7124C216A0AFEAC8087AB2DC00B9 A
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links	
Preview:	VLnk.....?.....`.N.7..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-2107062354O3Z-235.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):	2.0066673006294153
Encrypted:	false
SSDEEP:	192:23D3cOfU2isjTt9XGEIcbPonFGBQrQWuotxd4R:/OjjTr7x
MD5:	D7BA4A15B490369B33E2E5E5FB6D81D9
SHA1:	4C855ED1F6E77284AB7DDE413875D7C1910115DC
SHA-256:	E8AE3F694EC5CCC7A357BFCF09FFE640F60985CC824BEFA23227E9316FBB21EC
SHA-512:	CC51EB7BF082C62EC16B3FE4063E9E955F4358CD927314B31BB570705759177560F5C9BD76867B01D5646B4503B298E63ACA3FCB1E7052EDB905AE4B6CAAE39
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):	3.3876983002458725
Encrypted:	false
SSDEEP:	96:iR49IVXEBodRBkQ+OhFVCsL49IVXEBodRBkRB+OhAVCs749IVXEBodRBklB+Ohjv:iGedRBCedRBGedRBHedRB7
MD5:	3DFA292128D4D162F20A5CCD82468E0A
SHA1:	A8F10A38C0EDE5C62ACD6A6C2DA56F87D195B03D
SHA-256:	B446C7AE19B33360182D9F9F3C5A724B85769AE2B7929BCA64DF3867442ACF11
SHA-512:	730056FB3B937721682FD4727FC5E633575E0B0853B8A2E8C3F5579DEF6F392C2438E4A55903DFBED1D4637A25E7C50E0C954D03AFC1A886FCAD46358B4478F7
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):	3.20154677468842
Encrypted:	false
SSDEEP:	96:O7OhFVCPz949IVXEBodRBkD+OhFVCs6WLR49IVXEBodRBk2VB+OhAVCsUd49IVXN:O3iedRBCLGedRBdrCedRBZyedRBB
MD5:	74BBDB67932F7DE27A4C20678FD3C6EB
SHA1:	D979C210B726BFDC6CF05289B8F69B38997753C7
SHA-256:	9B42E906203D81F843045E6C6EB526EC515F301B29AD642CFF7817636E05585B
SHA-512:	5B42159404A7A46A9045935267FA31FD402FBA20CA3D23845337DD7D363403C603E7E3FA249DB2686C6B622A048236F2A7F4EEFD8F3D245F311B944E9F48ADFD
Malicious:	false
Preview:	.....*!..... .....X.. .h...y..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	63598
Entropy (8bit):	5.433041226997456

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin	
Encrypted:	false
SSDEEP:	768:PCbGNFYGpiyVFiCUZUlEoXqPkXMwL1H3C83U5jHfEnKYyu:J0GpiyVFiBUlEo+kXt+tHcnKK
MD5:	E35BC6F1B2EA5C3545B445700ED41B57
SHA1:	10213B0F707F8F3B402E6891AA2360AAF1FF9566
SHA-256:	6CE79445962FF9076A162B49122D7E46E06B7D895697F51411327564712CC7F4
SHA-512:	36363F9A86BDC0954C17D9DBAB6F3E4B90A06B2A809D66363E90E0DD119D657596AD3FE1E0135575EDB80936154A05EF8DBBDBE487F703465CE42A984C6292C
Malicious:	false
Preview:	4.382.88.FID.2:o:.....:F:AgencyFB-Reg.P:Agency FB.L:$....."F:Agency FB.#.94.FID.2:o:.....:F:AgencyFB-Bold.P:Agency FB Bold.L:%....." F:Agency FB.#.82.FID.2:o:.....:F:Algerian.P:Algerian.L:$.....RF:Algerian.#.93.FID.2:o:.....:F:ArialNarrow.P:Arial Narrow.L:$....."F:Arial Narr ow.#.107.FID.2:o:.....:F:ArialNarrow-Italic.P:Arial Narrow Italic.L:$....."F:Arial Narrow.#.103.FID.2:o:.....:F:ArialNarrow-Bold.P:Arial Narrow Bold.L:%..... ....."F:Arial Narrow.#.116.FID.2:o:.....:F:ArialNarrow-BoldItalic.P:Arial Narrow Bold Italic.L:%....."F:Arial Narrow.#.75.FID.2:o:.....:F:ArialMT.P:Arial .L:$....."F:Arial.#.89.FID.2:o:.....:F:Arial-ItalicMT.P:Arial Italic.L:$....."F:Arial.#.85.FID.2:o:.....:F:Arial-BoldMT.P:Arial Bold.L:$..... "F:Arial.#.98.FID.2:o:.....:F:Arial-B

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{A3D7A502-DEB5-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	32856
Entropy (8bit):	1.8435308876571492
Encrypted:	false
SSDEEP:	96:rorZq69Znv2ftsWfUstfuff5gtfvoi1WfEaRfbUTfJ4tfronl3:rorZqmZnv2FsWMstGfytnPWLaStTy3
MD5:	2AC0E759CB9C03CC70B6B1D111B5C86A
SHA1:	5BA3C73BF2C85CB7F2462387D382D6A0E8FF4CE3
SHA-256:	D4D457AFD968EB57C3B13AA5C3B06D68B64D049604075C312D22BAAD6B7A9E9F
SHA-512:	C66225E00983DDA866A124B1C00A056C7C9DB07D0DBFC7A1410915A36DB6C50A2358632D2494B1CE9848DC74888202BFB9A3DC7D81C02603E419CCD9530AD4
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r. y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{A3D7A504-DEB5-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	178844
Entropy (8bit):	2.58455486974587
Encrypted:	false
SSDEEP:	384:rwEEzfhCW3uY6j6zh1Hl0Ril/J+tvlRL48xMYKzcpKkTiVHM959KX/tlcGbG/lwW:AHEi2dE9n6kWsdguKft/RShft/RS927
MD5:	0048852D904F03470BDFD84CA797B804
SHA1:	404C26C94FB2A07D60139F53EA7A7C63988DF3DF
SHA-256:	DA1C98037CA2F41266ECEFA4A5DA3623EE1DA489A0B1AA650404DE0657E5BBC8
SHA-512:	617F9681FA5FF8724C982915404D6890E1B6381FD88E2EAE14E2DB937A5D733E61C6761EF79122B133EE2548C4F2DA8997D57D321B3B296C4719A13B9F3E552C
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r. y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{AB09A3DF-DEB5-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.564034352497865
Encrypted:	false
SSDEEP:	48:IwcGcprBjGwpakG4pQoGrapbSMGQpKOG7HpRkTGIpG:rAZB9QU62BSEAJTgA
MD5:	9D3F2E87F867F7D739FA1BD013B4CE5A
SHA1:	42516BB0E8E6C196D4E9A80FB0172A9B012B3EBE
SHA-256:	9B07FD634054C1D398A15EC20E8B7A00CFBBB2CB3FD30B0A4E9B0AA1E080F761
SHA-512:	8302520CA75BF1D98C198564B5C75DCBEF984F118686AB8FE69883D47B2D9E3C5ABEF6FBA12C06F96B7D704E87784297D98BCA907A14F32363C4FAE200F414B
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{AB09A3DF-DEB5-11EB-90E5-ECF4BB2D2496}.dat

Preview:	....R.o.o.t. .E.n.t.r.y..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\wlm7n14\imagestore.dat

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1510
Entropy (8bit):	2.5652328565697715
Encrypted:	false
SSDEEP:	12:IH/7pl4oIvmM0/7D3dXSXKZHlVJdslU/0FklVE:IH34JvC/7D3tSX6JumGklVE
MD5:	9BB949877273BA9140172287F55488CB
SHA1:	99FBD5BAA19D1BE784BD91ECAE79BCCD4CA6EC70
SHA-256:	FCADAE122AF138F8DB04A4716874C725847A2BC7658972612D9CA9A6584D1B6D
SHA-512:	ED4707D40AC1B051357563DB58F6E2BB275223EA0DDDE2D6B4FE43AB9358DB1E057C8F3930778A71134CA00204EB6F7F72D005577E713446D2DDB97F362E0DA
Malicious:	false
Preview:	!.h.t.t.p.s.:././.w.w.w...e.m.o.r.y...e.d.u./.f.a.v.i.c.o.n...i.c.o.~.................h.......(....... ....@............................oj....[=9.........wWR.............hJE......c^............h@:..li.............qLF.....nUQ.........................e?:.........zWR..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\209943939_1211950259242452_4312132841934873397_n[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 640x640, frames 3
Category:	dropped
Size (bytes):	141852
Entropy (8bit):	7.981060771321214
Encrypted:	false
SSDEEP:	1536:tfFMO5YrRj5Fnu2wXa0HFBrOHg7GZMT1/6PGaE5B1Z/nKXyDrLkec8wqIchaZg/R:ViO5kGHqpHg6k/rr1F5rweCNcsZhUPZ
MD5:	280CBE93DF02F2398BCCBCBA284EF0FB
SHA1:	64F7B2CBEB0BC29A1D0AB66A984346D98AD88FCA
SHA-256:	5FA4F15E078F0FEBC43D2D46B07E091B439AEDB40FD2BF35BB7DB00FBD03E6DE
SHA-512:	E7E9B63C63A4843B7DB0591952CC895BE98DDE082A0AEDF6B6CE8140AD898743610D0C0BB2AB6E9A91F3AB81FF3E4A1F8670457B4716EF4F44BC93A6FEA684 B
Malicious:	false
Preview:	......JFIF.............|Photoshop 3.0.8BIM.......`..(.ZFBMD2300096b010000072100004c3c0000054b0000a7e70000e51001007a610100b4890100d9b101001c2a0200....C...................................%...#... , #&')*)..-0-(0%()(...C...........(...(((..........."...S.I.~...j....9..8.Fo`. ."p..'..J..P.m.sn,...Yb...O...a..^.Y..K........).W.R............V......j..L.uu.A.*8%G.Ke2..".Eq....g.1$>..C........v....Er...e....).Z...j.dP =.........8...e..L.....k{-.f.......R.......%.b...............G..a... ..{\|K..k.+$_^4..t`..R..U.j....4..`s.`.Q.1p. >=c+..+.....Y.1....U^.T/...n..d...C...@A...<...d.cE..Q=J...U*;.5.I....]......".....R.2..".Br[.l\+.....,...V .....h...Lcv&.M...r[..x[.._pX>(..3%.A ._J...,..#.)M=&Q^~...]...D.Q...:.4.'._..2d...r.l.j.v4.g.V.$\.+.R......$..N\u.Y.._E..j...t).Q......S.c.../ggE..X...5+9..-.:,.>6...|~.6.z...YUHvvjY..4_.Us....j]..E.\.U.7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\210548092_204008588391281_1201898774073587 61_n[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 640x443, frames 3
Category:	dropped
Size (bytes):	42841
Entropy (8bit):	7.984929334355975
Encrypted:	false
SSDEEP:	768:l1arWCDn4VfbaFoxig5/GJYLkk0GdADGt4NSQR/rSNV3a2yrS2btX8tPx8:Hnw4ViqmYLBADWOSMGNU1jstm
MD5:	2B1BCA9691F48C5D4D298D30B6D4D32C
SHA1:	35845E27BA5E13073FF2A89698262557443D6CC1
SHA-256:	C9159A2325AD618D94EC1408EB012EB7A2CD9D84B0E1EFF0232D70D5B10B777A
SHA-512:	DC9857C11B45A9EA21C7E00CCEC1A4760FDCA7484FCD3DEC30F418FF7C63EA2D34B8498A7A04E26A81B5B5C9BC9A142CD6CEF22DF174255058486C7A0BE14 19
Malicious:	false
Preview:	......JFIF.............|Photoshop 3.0.8BIM.......`..(.ZFBMD2300096a01000069120000041a00002b200000c4490000f2590000fc6b0000e1830000708f000059a70000....C...................................%...#... , #&')*)..-0-(0%()(...C...........(...(((..........."...X...H......cC.N.q.. ....I;B20..0. .N.9 .w..@(....F.6...J..&......dD...e.biXQ...H..6..B. \......d..BI."V.D.4.8.....Q....i.....#.90..Q..H.'7......4...$...<.q)PD.p..A...jD.).#.......89.f.D.aF.....R0..A...Q03...B.. F.LcN.S..b........".JV.M*.....#R.F.`...a:.*gd')".1.....L.NF8.T.jW...8.V...H.!.Z...D...T.Lm+.*Fh.F.h....Q...%.w..4F$...I.&..l.....................f.=.j....).p...hQJ...i+-J...B.F*r.].!..1...5 .L.l0@6..v.!]..P..(B......iXQ).Q..2t!N...R!$.H.I&n..;..!........674..q. ...V.l:.d.X....d....1.U.^.2.zL,..U....m<]@..Xd.B.......T..Z'rB.'aD..5...v#sYJ70)E.H.L.Gvr........A3.ct.o4R.9 "M..h..U..........4.b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\646589415962224[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\646589415962224[1].js	
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	532532
Entropy (8bit):	5.472425458154517
Encrypted:	false
SSDEEP:	6144:Rk1HgCSntDV/HaK8V/Ha8NEPjQHguH3HpQrwz8GWZk1HgCSntDV/HaK8V/Ha8NEN:kNE7mNE75
MD5:	A237047DBC3F474B118603B1DBDA1214
SHA1:	CE58CCBC23A694E01CC1C213DAE640F60D9E537E
SHA-256:	AB0027317A6EBA804A695A14CE1527C7E93446DE057E218B4A417F55E32C046E
SHA-512:	CC7C24155DF0B2FD94DAC47BF14C20AE953E4F1A9D8EAE32792647A46A36B02BD77FBE99A43342AF8B9A18BA8C80720A892B8EF6F4A552BA7FFD4B6E2D7526B7
Malicious:	false
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\EKKT6VV0.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	244
Entropy (8bit):	5.074369462473063
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwol6hEr6VX16hu9nPic44XVl4KDOJi+KqD:J0+ox0RJWWPXl4KDURT
MD5:	DA8A260D1D0B756E4EAA969ECB1D75A9
SHA1:	9B3A1065E6F952EB27F16FCCF660DC38B405EAED
SHA-256:	BA013AB3A3862ACF08C0FDCE72A2627D25E9CD4F8930E632F55D6453CBEF9B0D
SHA-512:	979D374007612905BCFAEC4C97B2A9376E86C1A43BED89555B29D52E3D567E316AC7C6853C3384975C643C00A23FBF09464463D7EDBF44D12ADF8C78FE83B07
Malicious:	false
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>301 Moved Permanently</title>.</head><body>. Moved Permanently . The document has moved here. .</body></html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS_0000_0082003-17ab-f017-emory[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=12, height=1080, bps=0, PhotometricIntepretation=RGB, orientation=upper-left, width=1920], baseline, precision 8, 1920x1080, frames 3
Category:	dropped
Size (bytes):	161821
Entropy (8bit):	7.921371120948713
Encrypted:	false
SSDEEP:	3072:QDkDEm1oS1PFSvPXJhcva4uWoVcrUCoZJk0EFp61C/FW76b1YtAvnmL/kbJIFyM5:51oaPF0PXPmhuWScY9jFEFM1D7G16AvO
MD5:	BB2A9F6A69B8F14AD7F8C563C620400E
SHA1:	5462713B7C4EF74CE09A810329B80B667D49FCE4
SHA-256:	553B2C1788290D9BA8CD86965661DC8A0E51FE0C3E1E7CC42C608B4FC2D3AF4D
SHA-512:	7E4851EFAD4F1D849E1C40E74A64EA28CBBA638640F147E9DF2DD88EECD829EC288F428F028030AB2C1D229D869B9DBD4B4BA45654D0DCCAF7AB468BD72B694
Malicious:	false
Preview:	.....6Exif..MM.*.....8.....(.....1....!....2.....i.....$.....'.....'.Adobe Photoshop 21.2 (Macintosh).2020:07:24 01:27:01.....0231.....8.....r.....z.(.....H.....H.....Adobe_CM.....Adobe.d.....Z...."..... .....?.....3.....!.1.AQa."q.2....B#$.R.b34r ..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv..... ...'7GWgw.....?..+I.....'.....r..5..(....`...Jb.....k.mcznN.Q`..o.vS.....n..o..>5.>.V.. .

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS_0000_0101401-15bm-f613-experience[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=12, height=1080, bps=0, PhotometricIntepretation=RGB, orientation=upper-left, width=1920], baseline, precision 8, 1920x1080, frames 3
Category:	dropped
Size (bytes):	98915
Entropy (8bit):	7.720955404720064
Encrypted:	false
SSDEEP:	3072:sNENiypdDG6/mKuA38tywjz2DXSrueNHff:yq1pBGehug8f8XGuC

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS_0000_0101401-15bm-f613-experience[1].jpg	
MD5:	2EAD8D76B5EFA0EDBAC205E9B7EF4457
SHA1:	814AB3E7E29445C058E5DB4425109FC7D4C0EB1C
SHA-256:	1897CD36DB9149258ECD1E5F462944C9B2E3CDD3051D89E22ABA207DD2A6308E
SHA-512:	677E4C70702255D888998C3698424051F89FB48B2417F6B424EF5DA54F2DE6A389C169C61E06F1450A4DDEF407EFD66D4BC24054F1CF7C113DC6BB0BBD4C508
Malicious:	false
Preview:	.....Exif..MM.*.....8.....(.....1.....!.....2.....i.....$.....'.....'.Adobe Photoshop 21.2 (Macintosh).2020:07:24 01:27:01.....0231.....8.....r.....z.(.....Z.....H.....H.....Adobe_CM.....Adobe.d.....Z....".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?....!..Y..C....B.[..P..N...d....8'.d..?....?r...$jG.S.....I.`$5Aaic..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS_0001_0110803-12bm-f123-apply[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=12, height=1080, bps=0, PhotometricIntepretation=RGB, orientation=upper-left, width=1920], baseline, precision 8, 1920x1080, frames 3
Category:	dropped
Size (bytes):	170275
Entropy (8bit):	7.922110199517245
Encrypted:	false
SSDEEP:	3072:slLMQflLMQRgchsZzKmXqdP/myLH7Y2dILC3VcWzPiQVlJPYe0mI2j6+yKUknJnH:qfNCqlLHkoclTPiQOdYgTTnh9vL
MD5:	690440FA2869004AFB7AD697BAE3FC4A
SHA1:	E7603E778D95C926CE779BE60D68D08D19C6B245
SHA-256:	E0728AD494E94E09025359A31777AC21D978563E454E70C38BE583EF0603CCBC
SHA-512:	AB595278A06353DA95DBBCFFDFABCB5B4FF03F6E05CFF23326C21F03EFC59660849F65A003819C1843BE9A3CC04F49D0EF9076723AC2DADD08B68027F2AE6A3
Malicious:	false
Preview:	.....Exif..MM.*.....8.....(.....1.....!.....2.....i.....$.....'.....'.Adobe Photoshop 21.2 (Macintosh).2020:07:24 01:27:03.....0231.....8.....r.....z.(.....H.....H.....Adobe_CM.....Adobe.d.....Z....".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?.....5...i-k.2c...X..ah./.H?.B.`..=....R...2.....[..."...lq%.a..#O.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS_0003_0050902-11kh200-_man_alumni[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=12, height=452, bps=0, PhotometricIntepretation=RGB, orientation=upper-left, width=820], baseline, precision 8, 820x452, frames 3
Category:	dropped
Size (bytes):	45331
Entropy (8bit):	7.675937689821755
Encrypted:	false
SSDEEP:	768:RI3JSM79l3JSeeX9oDgMSWxtOh4vlHcqRfj2kAnN5ek4dhyGZktlsZmiXkCN+:istseDUMrtQ4vi6mN5qdhpktVXkC0
MD5:	8DE1889498A01C77342B79CFF3F71470
SHA1:	FB207F2B3B9FA2B2BC9A7431D4BD1E875BA34F2F
SHA-256:	E133FDAF775592BD95BD01D683F0FA000DD4B61D4539FB84DB93BB891A1A55DA
SHA-512:	7FEAABC3B661B9DFAEE85C2B01E16A89DF5667E03A6D4B1B60B86EBD1EBF49E31F42CF329696FA026F8076717289BF0322EE9934E1547EA6D7FCE923756E2955
Malicious:	false
Preview:	.....=Exif..MM.*.....4.....(.....1.....!.....2.....i.....$.....'.....'.Adobe Photoshop 21.2 (Macintosh).2020:07:24 01:27:04.....0231.....4.....r.....z.(.....H.....H.....Adobe_CM.....Adobe.d.....X....".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?..V.2...%Ui.F.....x.8h...~.-..cl.a....].. y.U...ma-..9K.trF..<.Gz....^u.6a0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS_0005_0063001-17sn-608-hs[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=12, height=452, bps=0, PhotometricIntepretation=RGB, orientation=upper-left, width=820], baseline, precision 8, 820x452, frames 3
Category:	dropped
Size (bytes):	39997
Entropy (8bit):	7.659018818494641
Encrypted:	false
SSDEEP:	768:L8Bc7y8BUmRHBg+xWsmg+leMsc2XiLaa8:LgpgUGHBgM3mg+2XiLaa8
MD5:	B11859AB46B1C80204B8F37E6B956A24
SHA1:	C6E929A26C484B2E978D4D7B6C9804AB42E8E0F6
SHA-256:	48EC6ECD1D2163F9058C42CA51E108478C994E98182BCF71E4592CE4D39199D6
SHA-512:	1947233C60431F41C5390CDF584061E19154DE5ACE8AAAAFA28699E6F0D065C62F44574F0558CFE1C834E122F9F988719DD4B42B3AAADE31AF732C7489AC03E
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS_0005_0063001-17sn-608-hs[1].jpg	
Preview:	.....qExif..MM.*.....4.....(.....1.....!.....2.....i.....$.....'.....'.Adobe Photoshop 21.2 (Macintosh).2020:07:24 01:27:06.....0231.....4.....r.....z.(.....H.....H.....Adobe_CM.....Adobe.d.....X...".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?...n..._%[..>A...N.....V{.CV....<.E.....?*..\O.....w.=.I$.U$.@J~.R.A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS_0006_mm21502-19jk-f055-monks02-global[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=12, height=756, bps=0, PhotometricIntepretation=RGB, orientation=upper-left, width=756], baseline, precision 8, 756x756, frames 3
Category:	dropped
Size (bytes):	159257
Entropy (8bit):	7.864375771740883
Encrypted:	false
SSDEEP:	3072:3Kc+lKc+nq7jylYgvbwH9HrKpAeFX/mp/eYeLjiPttAT9ttecu:b+o+nXlngHrKnpaveLjiP+tte1
MD5:	91F8907AFA9CF2718E8277E395D1C3D2
SHA1:	5A86A0C5D5631C708CAEC8B0DE7BA29BFACA8B28
SHA-256:	F5B0C64196AE0D86A032B84A60B456519EF0FE91F09C23A6FAE079979F064DAE
SHA-512:	639898D726320CA001A6C3F2F0B3D7AC47FB4662B616E12FE628ECCE670D3763773923B7DA60627759F56AE03C18C817D5E976637D3877D8D5D54C488C110675
Malicious:	false
Preview:	....3.Exif..MM.*.....(.....1.....!.....2.....i.....$.....'.....'.Adobe Photoshop 21.2 (Macintosh).2020:07:24 01:27:06.....0231.....r.....z.(.....1.....H.....H.....Adobe_CM.....Adobe.d.....".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?.....e6..;.0!.....-...X....ou'.....:.V.....m5?.._...?.w.....N..E..G

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\analytics[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	49377
Entropy (8bit):	5.521008419138659
Encrypted:	false
SSDEEP:	768:/yR3fYFBCwsNDsP5XqY0TyPnHpl1TY3SoavyVv6PU+CgYUD0lgEw0stZK:/y9g1r5h0UHp/Y3SowCw0sy
MD5:	042B7183D8645F5CF9D0D6ACD5FF8358
SHA1:	447A98467EA31E253ECB63EE8564C8B5E1E77D58
SHA-256:	73D6A5EA11FB7BF6E6A6CCD44B1635D52C79B0A00623D0387C9DDDD4B7C68E89
SHA-512:	72AA2F221BB5EFEC3A9C0CBC2D01DEBD827361369F7E84AA613D4CA70838FF68EA2C3300167FB263A4F416A857BABF0354A1FF8B3EC669BF88452633981CA18F
Malicious:	false
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var n=this||self,p=function(a,b){a=a.split(".");var c=n;a[0]in c||"undefined"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c=c[d]&&c[d]!==Object.prototype[d]?c[d]:c[d]={}:c[d]=b};var q={},r=function(){q.TAGGING=q.TAGGING||[];q.TAGGING[1]=!0};var t=function(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])},v=function(a){for(var b in a)if(a.hasOwnProperty(b))return!0;return!1};var x=/^(?:(?:https?|mailto|ftp):|[^:/?#]*(?:[/?#]|$))/i;var y=window,z=document,A=function(a,b){z.addEventListener?z.addEventListener(a,b,!1):z.attachEvent&&z.attachEvent("on"+a,b)};var B=/:[0-9]+$/,C=function(a,b,c){a=a.split("&");for(var d=0;d<a.length;d++){var e=a[d].split("=");if(decodeURIComponent(e[0]).replace(/\+/g," ")===b)return b=e.slice(1).join("="),c?b:decodeURIComponent(b).replace(/\+/g," ")}},F=function(a,b){b&&(b=String(b).toLowerCase());if("p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\enquire.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	2235
Entropy (8bit):	5.067360026835807
Encrypted:	false
SSDEEP:	48:aq7LrWSQIowJMQoq1pTiChqAo4UwrbuKboJ99PyfAyDlfABH:aILrWiowJPdjDmlyfDlfIH
MD5:	36EFB75FE7D6BDF57BD8B5856B3158F6
SHA1:	50BCD0539CF62F9E93C036C42E825DC47F8D0202
SHA-256:	AF448B0067D5A192653A9E6FACBDB9656AB7075D3BF45236BDD24CC7948A3FDE
SHA-512:	943D2E4703FAF50F22E7FC6012092DD86A30EFF3D2CAD5BDA21A892A025E6B89C85B88CCA29840E5082CB14885205137D9460EA87FDFADFA1B38FA7BE8CDA4EB
Malicious:	false
Preview:	/*!. * enquire.js v2.1.1 - Awesome Media Queries in JavaScript. * Copyright (c) 2014 Nick Williams - http://wicky.nillia.ms/enquire.js. * License: MIT (http://www.opensource.org/licenses/mit-license.php). */..!function(a,b,c){var d=window.matchMedia;"undefined"!=typeof module&&module.exports?module.exports=c(d):"function"==typeof define&&define.amd?define(function(){return b[a]=c(d)}):b[a]=c(d)}("enquire",this,function(a){"use strict";function b(a,b){var c,d=0,e=a.length;for(d;e>d&&(c=b(a[d],d),c!==!1);d++);}function c(a){return"[object Array]"===Object.prototype.toString.apply(a)}function d(a){return"function"==typeof a}function e(a){this.options=a,!a.deferSetup&&this.setup()}function f(b,c){this.query=b,this.isUnconditional=c,this.handlers=[],this.mql=a(b);var d=this;this.listener=function(a){d.mql=a,d.assess()},this.mql.addListener(this.listener)}function g(){if(!a)throw new Error("matchMedia not present, legacy browsers require a polyfill");this.queries={},this.browserIsIncapable=!

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\eu-logo-shield[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	4146
Entropy (8bit):	3.901697979836071
Encrypted:	false
SSDEEP:	96:3ISvgMYz9FLNVizjti3SiuEXjtyEy80/kNU1ZDJboXRh:4SYTzjLGzjtiiyfHTULDJbKh
MD5:	912157A5A1A3BFDE8D6BAFFA6439ABE9
SHA1:	043308ED242B1E341FD6E7D90A1C5BBE8B6272DD
SHA-256:	C23069910C8082C909297C2CEF2E3FAF3B328B9EBFD9DE2751883AD70512691D
SHA-512:	1E245926469B68F9281F493FEBFDA5CF90B2BF4A16CCA6B59F65370D17B78D74239504FC466923F316426747B18C4A38FE9BC564A6DCBA3B1D9EF217F8DC9C8
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 80.5 87.97">.. <g fill="#fff">.. <path d="M39.75 85.27C-1.69 66.1 3.28 23.3 3.3 3.29l73.33.07c-.02 20.01 4. 59 62.83-36.88 81.91zM3.3-.02L.14 3.32c0 2.39-.09 5.4-.11 6.88-.28 23.51 1.29 60.07 39.54 77.78 20.24-9.39 35.55-25.51 39.57-50.5 2.34-14.47.94-28.21 1-37.45z".. />.. <path d="M24.09 52.54l-6.82 7.29c-.22.24-.25.49-.11.64a2.29 2.29 0 0 0 .59.51c.18 0 .31.12.63-.22.13-.15 3.36-3.26 7.17-6.93a3.92 3.92 0 0 1-.72-.5 7.93 7.93 0 0 1-.74-.79zm1.96-.83a12.2 12.2 0 0 0 2 1.43l-.67.64c-.25.28-1.2-.16-2.12-1s-1.45-1.7-1.19-2l.74-.67a9.1 9.1 0 0 0 1.24 1.6zm33.5 8.08a2 2 0 0 0 .63-1.17l.66.3 2c.19.21 0 1-.58 1.59s-1.45.81-1.65.6l-.35-.72a1.93 1.93 0 0 0 1.29-.62zm-1.01-1.08a2 2 0 0 0 .53-.84l.43.3c.14.15 0 .64-.44 1.08s-1.06.59-1.21.44l-.25-.47a2.59 2.59 0 0 0 .94-.51zm2.05-33.47l-.78.69c-1.07.41-3.49-1.44-5.4-3.12-1.28-1.12-3.84-3.94-3.11-5.08l.32-.33-.58-.34a1.42 1.42 0 0 0-.82-.15c-.3 0-.55.16-.57.41a4.14 4.14 0 0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\fa-regular-400[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Font Awesome 5 Free Regular family
Category:	dropped
Size (bytes):	34350
Entropy (8bit):	6.318944818536342
Encrypted:	false
SSDEEP:	384:k+ILSQt3owpXUazLuDULbNVTH/oOkKQB3l+89AyI6WcRwk1cQUt1:kBLSe3yy6DOP/oDB29uc51cQU/
MD5:	AD3A7C0D77E09602F4AB73DB3660FFD8
SHA1:	3306178C90D9DF939D2A5EABF533BA3650FBE80E
SHA-256:	C4F72714221008F5BDFCC90821CCD835CCE9524C7EC99AD5D947488930FE1623
SHA-512:	BD350DEC9B8A10C70254336909489498ADC6D4B29F4B72A603FFD30640CB388421887B42C9C7DB54E1C8FA78BB50EF0960058E86550A67BD3BF55136B4F0BB8
Malicious:	false
Preview:	.....LP.....*l.....6.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .R.e.g.u.l.a.r.....R.e.g.u.l.a.r...L.3.3.1...2.6.4. .(.F.o.n.t. .A.w.e.s.o.m.e. .v.e.r. s.i.o.n.:. .5...1.4...0.)...6.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .R.e.g.u.l.a.r.....PFFTM.T.....GDEF.*.....OS/2A.S....X...`cmap.....gasp.....glyf|.7.... ..n.head. FQ.....6hhea.5.....$hmtx...t.....Tloca.e.....6maxp.....8... name9.1*..w....[post.iA...}.....KC...l*_.<.....4.z.....4.|..... ...@.....L.f...G.L.f.....PfEd.....T.....:..... .....@.....@.....@.....@.....@...@.....@...@..... .....`.....@.....@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\fa-solid-900[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Font Awesome 5 Free Solid family
Category:	dropped
Size (bytes):	204266
Entropy (8bit):	6.3434506602344545
Encrypted:	false
SSDEEP:	6144:wt+wVGtMonODzpN2BDXTIRSwRKSK3NC5RMi:YW3nODze58Rjg+59
MD5:	89BD2E38475E441A5CD70F663F921D61
SHA1:	96A5637429426764EA9B28BF4D1EB55AE10DE57E
SHA-256:	5C44F9D868C55913CA587E0399FC6DF18F157C544A0B366AE544A83D32F057D5
SHA-512:	AB5942A644C077C8004D326DB0B36CC6B90BFE05B09B5104800D275F8388B3B7D0166635A1172BAF8871790704175456A0F95E167B8EF0E28226FD3219B37154
Malicious:	false
Preview:	.....LP.....{.D:.....2.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .S.o.l.i.d.....S.o.l.i.d...L.3.3.1...2.6.4. .(.F.o.n.t. .A.w.e.s.o.m.e. .v.e.r.s.i.o.n.:. .5...1.4...0.)...2.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .S.o.l.i.d.....PFFTM.T.....GDEF.*.....OS/23.V`...X...`cmap.u.....`....gasp.....glyf.#.B..-....phead.TQ.....6 hhea.C.+.....$hmtx.....loca..kh...(....maxp.L.`...8... name".&&...D...+postU.....p..1.....KC.:D.{_.<.....4.x.....4.|.....]. .....@..... .....L.f...G.L.f.....PfEd.....T.....:..... .....@.....@. .....@.....@.....@..... ...@.....`.....@.....@.....@.....@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\fading-hero-events[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	298
Entropy (8bit):	4.621858688563654
Encrypted:	false
SSDEEP:	6:Uy+kXAE8kk3w7lXAEXoPAIYNuk3jwiGBKR:Uy+kXAE8kk3w5XAEY6uk3j3GBo
MD5:	98B6B42B0728A507CFCE7CDAD6FCCE4C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\fading-hero-events[1].js	
SHA1:	DFCA4F48BCEF2B3F4C837A2E92F0DCCF3DA7AAFF
SHA-256:	A0A4E410C118233F97B6556B2B5B9DA4FB73500A80ADD941B265307047926215
SHA-512:	9C48C4E12BEE1DCE33B88AD4E7632FB2588999DE03EA78BC5A539F879A43D88C903B2F361722FE1749DF02CFEABB0B3785D9BDF67F19D16F96FD6F76ACE8D4 4E
Malicious:	false
Preview:	/* exported FadingHeroEvents */./* global FadingHeroHandler */..var FadingHeroEvents = (function () {. var pageLoad = function() {. $('.js-fading-hero').each(function() {. FadingHeroHandler.init($(this));. });. };.. return {. init: function () {. pageLoad();. }. };.}());.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\fbevents[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	96774
Entropy (8bit):	5.393912266105669
Encrypted:	false
SSDEEP:	1536:xM+OWtI6ay9Xes12KqQqfUThe7Kdv0a9slOs1jaV7vu5Dm20C+QNSMngySZYSlI3:xzOW5jSVnYDGeB
MD5:	7127530AC0B994CF8243B0BC94C07D9D
SHA1:	35253EA4698F395A6D7D846D81D01987AC96A433
SHA-256:	F2A2056B7A1C989899886A9B194E93912B7D11767239E956DE73D5C2EA237B32
SHA-512:	443F305B0AF8BC7AFFE1A76E72CD5689F67C0BEEA9838EAD0A3DD0F0090C95F693838D2D483334F9DF2D6E9A97F62A9541A5A9E3A346DC6391405DCED35762 6
Malicious:	false
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\filterable-handler[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	7489
Entropy (8bit):	4.663141401356554
Encrypted:	false
SSDEEP:	96:PbKP+9VvG9QKAPA5LAKT1AlcoAjhVEd2Ge:PO+94uKqA5LAK+WoAFVEd2
MD5:	AB655C45F7B0CA198C81A1ED0CA555E3
SHA1:	B29C1CAB2B7A773EEE34836B3CED4725B334FF64
SHA-256:	5DFACF6FF93D6717DA1C3BD57CFCF45BB98BDE3781B57C0CDA3392FE92C2C321
SHA-512:	4F8828D97CF0CF601C028B54628E323C1DEB05864FC76A1FDC65E216A16C2DA56EF5B2DA0DC80F7FA37AA38FBD799DC44EA131D84DA86A3CC7D1519F6E694 2
Malicious:	false
Preview:	/* exported FilterableHandler */../* global ExpandoHandler */....var FilterableHandler = (function() {.. var mobile = false;.. var filterTagTemplate = $('.js-filterable__tag-tem plate').html();.... return {.. checkItemGroups: function($element) {.. $element.find('.js-filterable__item-group').each(function() {.. var $group = $(this);.. var $shownItems = $group.find('.js-filterable__item.is-shown');.. if ($shownItems.length) {.. $group.show();.. if ($group.hasClass('js-expando')) {.. Ex pandoHandler.expand($group);.. }.. }.. else {.. $group.hide();.. }.. });.. },.. clearForm: function($element) {.. var $form = $element. find('.js-filterable__form');.. $form.data('filterable-clearing', true);.. $form.find('.js-filterable__filter').each(function(){.. var $filterValue = $(this);.. if(!$filte rValue.prop('checked', false)) {.. $filterValue

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\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:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C038 4
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\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\3Y2ADQKS\image[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	34
Entropy (8bit):	2.882524990934808
Encrypted:	false
SSDEEP:	3:CUXCXk5q:4k5q
MD5:	A82BA3A9D42148E9CF209DF13D8C3F3D
SHA1:	DBA80835D31175BDCF0BCAD1ABAFEFB06D86E304
SHA-256:	1E85EC81B9800B4C443D39CACA0D0926089A3AC201120DB1CEB45B93789480B8
SHA-512:	97777A4B16BEDD7547A46B1AB1D146C50C1547BBE23C70708806A357352A1291A4EB6CDAE049D0E334F33903DBC98D7054EB5BFF84DAB0EDCD091241EBBE5353
Malicious:	false
Preview:	GIF89a.....,.....L.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\index[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	66922
Entropy (8bit):	5.184071539590738
Encrypted:	false
SSDEEP:	768:YEIIGuF7zp2CHp+ADZX46b4ab9Q+K2FpWSw6phtkDJW0H:YzYRp3HcADJ43ab9Q+K2FpWSdphSDJWW
MD5:	6F09D7C7A01049FB05B594EA963FC8CD
SHA1:	8E14E02ADCBCB9D846B557E6F4129E68EBC51B94
SHA-256:	BCECEFE4A79E6B54A643BC7E9DD6485C04D16DE39CB835D7FB8422EE5161F65F
SHA-512:	1CE67F6F14B9B37D48E226A76A304C907F56990D9450B58D9B30F44BD807909EB6A14E51DE6772DA5BE0707FDD5D60CC0CCF9B4532D3B601ADDB692DFC0207D
Malicious:	false
Preview:	<!DOCTYPE html><html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en"> Level 0 --><head> Level 10.10.00.00.00 --> Standard Metadata --><meta content="text/html; charset=utf-8" http-equiv="Content-Type"/><meta content="en-us" http-equiv="Content-Language"/><meta content="IE=edge" http-equiv="X-UA-Compatible"/><meta content="width=device-width, initial-scale=1" name="viewport"/><meta content="Emory University" name="copyright"/><meta content="ff9bba470ae720982aa51447058a2be9" name="cms-id"/><meta content="" name="description"/> Opengraph Metadata --><meta content="university" property="og:type"/><meta content="Home | Emory University | Atlanta GA" property="og:title"/><meta content="" property="og:description"/><meta content="https://www.emory.edu/home/index.html" property="og:url"/><meta content="https://www.emory.edu/home/_includes/images/sections/index/2021/06/hero-cbsc-1.jpg" property="og:image"/><meta content="https://www.emory.edu/home/_includes/images/s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\index[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	45822
Entropy (8bit):	4.7243259989892055
Encrypted:	false
SSDEEP:	384:ARspBOLIY5JdEMK+XmkdQwp2CnHkAF2CxuWLPm+OMFc9fQZYDFRm9rPgQpVYUw:WsMIGuF0zp2CHnrm/ifYDFRgbgQzYUw
MD5:	7DC115EA5AC50DD4B095B1B2374E7025
SHA1:	CF1A307FBE0CB25C9C81FC136574640C40593237
SHA-256:	AC4B0342F5B043BFD84DF1477946417E732868BFC44687C72479BC684E083EE9
SHA-512:	AD422F02D910C1DF516FC3D558E0955587F7E601EEBF1E170A0D88FC79BA5393971B198C49536A81353F8302BDA42E822D8F0F1C92CDA545E2F035873C37FBF6
Malicious:	false
Preview:	<!DOCTYPE html><html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en"> Level 0 --><head> Level 10.10.00.00.00 --> Standard Metadata --><meta content="text/html; charset=utf-8" http-equiv="Content-Type"/><meta content="en-us" http-equiv="Content-Language"/><meta content="IE=edge" http-equiv="X-UA-Compatible"/><meta content="width=device-width, initial-scale=1" name="viewport"/><meta content="Emory University" name="copyright"/><meta content="fd6dd2bf0ae72098631b3bcc8b8c18fa" name="cms-id"/><meta content="" name="description"/> Opengraph Metadata --><meta content="university" property="og:type"/><meta content="COVID-19 | Emory University | Atlanta GA" property="og:title"/><meta content="" property="og:description"/><meta content="https://emory.edu/forward/covid-19/index.html" property="og:url"/><meta content="summary" property="twitter:card"/><meta content="COVID-19 | Emory University | Atlanta GA" property="twitter:title"/><meta content="" property="twitter:d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\index[3].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	42718
Entropy (8bit):	4.897444856975573
Encrypted:	false
SSDEEP:	384:qOkpBOLIY5JdEMK+XmkdQwp2CnHbAJ4Rxu7/bupIE+mkDgfpVYUQ:bkMIGuF0zp2CHxm/buhkDgfzYUQ
MD5:	60F962E9080B281059C2717953DB5E41
SHA1:	5DD6F07ABE2248BCD3294A66B589C75AFC500C4E
SHA-256:	86A3D7CE5951FD8A4F7E50D48B1EC252B3B4F1EA9AE723BECEAA4CC26C8D646E
SHA-512:	DA7096558C167CC1D1E40386A6F0CAA5012425B0AA7A7C680726A938D2E65C76F8C01400FC06137BF6D9B0FF6D7A24B8A70D2CB03961EE24E39E53D7AA39D28
Malicious:	false
Preview:	<!DOCTYPE html><html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en"> Level 0 --><head> Level 10.10.00.00.00 --> Standard Metadata --><meta content="text/html; charset=utf-8" http-equiv="Content-Type"/><meta content="en-us" http-equiv="Content-Language"/><meta content="IE=edge" http-equiv="X-UA-Compatible"/><meta content="width=device-width, initial-scale=1" name="viewport"/><meta content="Emory University" name="copyright"/><meta content="07ec81ba0ae72098631b3bccfe9ba43c" name="cms-id"/><meta content="" name="description"/> Opengraph Metadata --><meta content="university" property="og:type"/><meta content="COVID-19 Testing | Emory University | Atlanta GA" property="og:title"/><meta content="" property="og:description"/><meta content="https://emory.edu/forward/covid-19/testing/index.html" property="og:url"/><meta content="summary" property="twitter:card"/><meta content="COVID-19 Testing | Emory University | Atlanta GA" property="twitter:title"/><meta conten

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\o-0TIpQlx3QUIC5A4PNr4Az5ZuyDzWs[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19572, version 1.1
Category:	dropped
Size (bytes):	19572
Entropy (8bit):	7.976622136328915
Encrypted:	false
SSDEEP:	384:cox8g6/pTjbiLYDo5X5Ilw5oC2mRd7fm49USzW1MZTK8EXRLsLWmdiAwR495/TqC:cox8Ezw+oVYfX9fKKKzeW4V95LqC
MD5:	D00289FE37460C9FCA4CF0069DE9474F
SHA1:	82DC56D86DAE2C82A460D605224FF88993B70470
SHA-256:	AB1F4D76A9EA35614D7F242451526B4E029A04C3BE01BDEB9C9EC19D0AEC68AC
SHA-512:	7963C067735D7B52FC162612986359DB5F500D2AD9E94ACC88907657C64DC0880D58C2EB120C377D7A8417151F733DFC69D0F9A44D32BEC0D7B1DE405D956C4
Malicious:	false
Preview:	wOFF.....Lt.....q.....GDEF.....<...R....GPOS.....W...GSUB.....&...&5.N.OS/2.....]...`}G.ecmap...\.....cvt .....0.fpgm.....s-.pgasp... ..... .#glyf...0..8c..Q.u.\.head..D....6...6..k(hhea..D...."...$....hmtx..D.....d....loca..G.....wc.4maxp..H.... ... .name..H.....(RE.post..I..... .].fprep..I.....qx.....D.....y.B3x c..C..]....G+t5..a.i2.KM.M.k:.....x.\...%A.E.._.m.m.mEk.m...F0.&N..#7.Y.....x..N.Is'L...1.gR.. .p .Y.=.x.&.I..W.A.q.KV....p...HY.....e#m.i..b.....9`>..2s.....[8T...4.B.....mw..... M.z..o...}y`...i.....P...[...].Z!.....%1.....\...<U.Q.Zd....I#Z...t....Bq....T..M?J3@.g.....S...*+.L5v.F.b..9.1Zp.....[...T_..~<.9.y.....I6r...#.HV.JY%.e...O..U.b.kd...ZU.J}i$ ..8...T...Y....-{d...r0...Pi+.....* .,)E(...62..,7V...D.pa..^af.G..hI.a...+..@.....6;.|MzC....q.....I1...^..*=&o..&...b...?+.....e}$.H.!K.v3....C.8.S..s.%y..)Q.B.+..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\pattern-bg-blue[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	2411
Entropy (8bit):	5.173386650684766
Encrypted:	false
SSDEEP:	24:2d3ATLf5Y6oj8T76ZgEP/SHEIgGWe/yemScoea2TxeKye+mMzFp2vGpghGlYh1SU:c3Avfu6Y9GPHTj3ea29Eu2J5DE
MD5:	6E67473478CA1BF6AD8E11590C4CC897
SHA1:	1BD63A6C62033E9D15FBB1ED697B0592FD4F38CD
SHA-256:	F9B3DF3E4117ED5FD0EBCD8AEC6EE8BCC643057D5C8AF5498AC0BF7733B2BC23
SHA-512:	7448136E6CC162B27583632D5ABBDB2E3CB28D4C3BC7A21A3885147269908525AAF2A090C4AA6B4B60D92FBA6CC5870B1F541B5F85D8DBA15576C71F2AEE707 1
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>. Generator: Adobe Illustrator 22.1.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->.<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px".. width="800.2px" height="226px" viewBox="0 0 800.2 226" style="enable-background:new 0 0 800.2 226;" xml:space="preserve">.<style type="text/css">...st0{opacity:0.2;}...st1{fill:none;stroke:#007DBE;stroke-width:0.75;stroke-miterlimit:10;}.</style>.<g class="st0">..<path class="st1" d="M228.7,0.1h228.6V113H228.7V0.1z"/>..<path class="st1" d="M342.9,113l-57-56.6l57-56.3 M228.7,56.4L285,0.1 M228.7,56.4h57.1 M285.9,56.4V113 M342.9,0.1V113 M342.9,0.1...L457.3,113 M228.7,113H0.1V0.1h228.6L228.7,113L228.7,113z"/>..<path class="st1" d="M114.6,113l57-56.6l-57-56.3 M228.7,56.4L172.4,0.1 M228.7,56.4h-57.1 M171.6,56.4V113 M114.6,0.1V113... M114.6,0.1L0.1,113"/>..<g>...<path class="st1" d="M228.7,113h228.6v112.9H228.7V113z"/>...<path class="s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\quantcast[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.072223661202982

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\quantcast[1].js	
Encrypted:	false
SSDEEP:	12:tlOu3xRxDSirWc/yXm/+FDRWUkE62lrs4rke:uuhSs9yXX1RWUn62O4rX
MD5:	557EEE2A969F0E65A6953779DFAEDA4D
SHA1:	411E92B234BB98F95B084DB7C77DB22A281BD29D
SHA-256:	3A5F90BD4021D2ECFF5696793820406498BD4D7C5E3D36BEBE259164F5FB4E69
SHA-512:	ACE8E88D824EA6763C9582E34689968041D6F72678F4D521E88872DAC345519475085B014403C1496B17AED9E6D0EE0B0E41D69D06FB4EBCAB5EF21E3E321C7
Malicious:	false
Preview:	var _qevents = _qevents || [];....(function() {..var elem = document.createElement('script');..elem.src = (document.location.protocol == "https:" ? "https://secure" : "ht tp://edge") + ".quantserve.com/quant.js";..elem.async = true;..elem.type = "text/javascript";..var scpt = document.getElementsByTagName('script')[0];..scpt.parentNode.ins ertBefore(elem, scpt);..})();...._qevents.push({..qacct:"p-N9sBKx_5YpWtv"..});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\quick-guides[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	40964
Entropy (8bit):	4.81085894678576
Encrypted:	false
SSDEEP:	384:aeCpBOLIY5JdEMK+XmkdQwp2CnHkABv5eCxulwqDdJxsnrO3gQpVYUw:vCMIGuF0zp2CHNgwqDdJxsnrO3gQzYUw
MD5:	0CF733E5D6E0E143B58EB18D72F9FECB
SHA1:	CBDD286362D1C24C89BB04C68056C2E8C316E1AD
SHA-256:	8F45EFCCBCCE22EF3864EFBE5D1ECCCB42A4007651EDA8704DCCBB3691FC86C9
SHA-512:	4EA17529F2921361358DA9A7C2B2954EF455BA8051F92F3170DD9A1C2627B351446ECB1711B90D84E602D5DFB6E8B14B07F65AB2A3E3A3B6147644A5A6EEE2D2
Malicious:	false
Preview:	<!DOCTYPE html><html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en"> Level 0 --><head> Level 10.10.00.00.00 --> Standard Metadata --><meta c ontent="text/html; charset=utf-8" http-equiv="Content-Type"/><meta content="en-us" http-equiv="Content-Language"/><meta content="IE=edge" http-equiv="X-UA-Compa tible"/><meta content="width=device-width, initial-scale=1" name="viewport"/><meta content="Emory University" name="copyright"/><meta content="73e55e620ae720987 c4580f4ca1f0cea" name="cms-id"/><meta content="" name="description"/> Opengraph Metadata --><meta content="university" property="og:type"/><meta con tent="Quick Guides | Emory University | Atlanta GA" property="og:title"/><meta content="" property="og:description"/><meta content="https://emory.edu/forward/covid-19/quick-guides.html" property="og:url"/><meta content="summary" property="twitter:card"/><meta content="Quick Guides | Emory University | Atlanta GA" property="twitt er:title"/><meta content="" prop

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\rules-p-N9sBKx_5YpWtv[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	3
Entropy (8bit):	1.584962500721156
Encrypted:	false
SSDEEP:	3:P:P
MD5:	8A80554C91D9FCA8ACB82F023DE02F11
SHA1:	5F36B2EA290645EE34D943220A14B54EE5EA5BE5
SHA-256:	CA3D163BAB055381827226140568F3BEF7EAAC187CEBD76878E0B63E9E442356
SHA-512:	CA4B6DEFB8ADCC010050BC8B1BB8F8092C4928B8A0FBA32146ABCFB256E4D91672F88CA2CDF6210E754E5B8AC5E23FB023806CCD749AC8B701F79A691F03C 7A
Malicious:	false
Preview:	{}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\search-module[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	269
Entropy (8bit):	4.344377748778062
Encrypted:	false
SSDEEP:	6:UjbMJKWgN8vrxJTXgNMz1+LB7FSIvpEeomNaDkH:UjbMJKlN8FJTXgM1+FFXpESaAH
MD5:	DE6B599A208BB3F0E128257DAFEC9531
SHA1:	D715BC7512066B4B0FBE44BE4F604970695AD5E7
SHA-256:	240A62690ACD8A57B4B8D138818CBD75277E8299F444070F51E6533C91204C21
SHA-512:	B28BBBB85761C82CE10EDB116A03F5143812EFDAC5DEC95FFEAEE2B708273818D5752F7A1457058F47D884F190A3CF5D65DF5C687873535AD1711787B7E22A8
Malicious:	false
Preview:	/* global NeboInitializer: false */./* global SearchEvents */..NeboInitializer.register(. (function () {. return {. init: function () {. SearchEvents.init();. },. t oString: function() {. return 'Search Module';. }. };. })().);.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\select-events[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	283
Entropy (8bit):	4.56192683762452
Encrypted:	false
SSDEEP:	3:Uy83KRCyvKwLqAVP0m2AoKRCWQLGNazcN0XE7zPWsVhaNDQCFEN6qAb3IfdFQRkX:UyWKw8N2AlQKwXozPtaNWAswiGBKR
MD5:	5ECD7BEAF8BFE8EA3D1E64A53DA690EC
SHA1:	96E76BC85DACA85C48F8CF01F64C0BE4794D25BB
SHA-256:	ED32F9AB21F5180D2BDFB452E2173112051398974B1B7544910F3F28B5249556
SHA-512:	C2CC9ACCA1BCC18E9D58F50BD6A32DB4EB3C7DFC7845D7FC9D8EFBE1F8E22BA118938F07EC36BC8D32BF06D3144F1F749B00F7E45CF1ADC8EDD00C1FFCA42CA
Malicious:	false
Preview:	/* exported SelectEvents */./* global SelectHandler */..var SelectEvents = (function () {. var pageLoad = function() {. $('select.js-select').each(function() {. SelectHandler.init($(this));. });. };.. return {. init: function () {. pageLoad();. }. };.}());.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\site[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	assembler source, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	9063
Entropy (8bit):	5.061021785630453
Encrypted:	false
SSDEEP:	192:gcfK9hx+uZxMxYxkx0x/Axzx0+wx6nz6xIx6nz6ny6nZx+a9//9Liys83dpoFBTd:q7yd3dpUWsT
MD5:	42A0BB5515F244BA9227095FB44943D7
SHA1:	5D16ED48F56484F6DE33B33972A5AB90BC55E58E
SHA-256:	6C6488A6F19B8AFB3E7234F0C2F9415E2595C3BDACE3E062691B14787A157885
SHA-512:	8A5D1AC99548FC4974703C625BCCBD5C7FB6AE1C11D404C2A701989EA846AE5804D7BE37E2F87D133A3370B6712A81FE5FB6BC4ED4A4CD4557EE06FEE079708
Malicious:	false
Preview:	.modal-content h2, .modal-content .h2 {.. font-size: 1.75rem;..}...modal-content h3, .modal-content .h3 {.. font-size: 1.5rem;..}...select-dropdown {... position: relative;... padding-right: 2.5rem;... overflow-x: hidden;... font-size: 0.875rem;... text-align: left;... text-overflow: ellipsis;... background-color: #fff;... border: 1px solid #d0d0ce;..}.. .select-dropdown::after {... position: absolute;... top: 50%;... right: 1rem;... -webkit-transform: translateY(-50%);... transform: translateY(-50%);... content: "\f0dc";..}.. .select-dropdown:focus {... z-index: 9999 !important;..}.. .select-dropdown-menu {... top: -3px !important;... width: 100%;... max-height: 225px;... overflow-y: scroll;..}.. .select-dropdown-menu .custom-control, .select-dropdown-menu .custom-control-label {... display: block;... width: 100%;..}.. .select-dropdown-menu .custom-control {... padding: 0;..}.. .select-dropdown-menu .custom-control-label {... padding: 0.15rem 0.15rem 0.15rem 2.5rem;..}.. .select

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\site[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	280
Entropy (8bit):	5.300800681979485
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwol6hEr6VX16hu9nPrX6krkaND+MUId+KqD:J0+ox0RJWWPrXV4aND+MTIT
MD5:	4863BB35113BAB3FD0004C267D4C0CD7
SHA1:	2C27AB2CA686822F7C728DA829356DF1F1E6D8D9
SHA-256:	EC92DA398F6F3C9D2F2011B6F6F32A926DFA8B98A5E9D23368F136CD713807BF
SHA-512:	37D54E625611BF4C34458F9F670FA00D924ECADCB9E594F7F970D86C0E710FE2D5754BBBDB5DA34874747E46342ED441BDBF6A034F83E457E88A4C9EFD811D03
Malicious:	false
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>301 Moved Permanently</title>.</head><body>. Moved Permanently . The document has moved here. .</body></html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\site[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	5059
Entropy (8bit):	5.201091656796225
Encrypted:	false
SSDEEP:	96:2c0hBn43orbomTqQKbld+jVyeYRyuJG9svxBZ2B:2Fj2+omTC+c9vxBZ2B
MD5:	AC963B44D063C903EDBA8FBA198648C4
SHA1:	961CBD16F161E723E53139D8C445A33E0261F6AA
SHA-256:	969AB65DE8ADC193799BF7977D22262DF0797B7706E885068BE368E4B00A5808

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\site[1].js	
SHA-512:	2FD93533678C2BF38E89938E4D5D26A4002860296126E74A77182C83D10B9AF5680C605B6F724EC96EE4AFE8EFF83D4C228591C2212F098D0F082E2BAD65FC73
Malicious:	false
Preview:	(function ($) {...if (!$) throw "jQuery library is required."....//Global reference...const $doc = $(document);...const $body = $('body');.....let $headerMegamenu = $('.header-megamenu');...let $megamenu = $('.megamenu');...let $megaToggle = $('.navbar-megamenu .dropdown-toggle');...let $playBtn = $('.video__btn');...let $alphaToggle = $('.js-filterable__order-toggle');.....let $selectDropdown = $('.select-dropdown');...let $selectDropdownMenu = $('.select-dropdown-menu');...let $selectCheckbox = $(".select-dropdown-menu input[type=checkbox]");.....//Ready function...$doc.ready(function () {......// Megamenu expanded = header turns blue....$megaToggle.click(function () {.....if (!($(this).parent().hasClass('show'))) {......$headerMegamenu.addClass('bg-primary');.....} else {......$headerMegamenu.removeClass('bg-primary');.....}....});......// If clicking outside megamenu, remove blue BG class....$body.click(function (e) {.....if (!($(e.target).closest(".navbar-megamenu").length > 0))

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\student-sitting-on-grass-quad[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, baseline, precision 8, 432x244, frames 3
Category:	dropped
Size (bytes):	33736
Entropy (8bit):	7.981122825350079
Encrypted:	false
SSDEEP:	768:KfI4UTRjZexkU8G5M14qcw4XTBi8UweW8320n+qdkq:Kf/UTRjZeqxG59XD4lW15qx
MD5:	771CADF93271C5D5A47A87EDF59DF8D1
SHA1:	1BA7AEC842DC3A1C42F786AD99FB630098B6579B
SHA-256:	09FDAB7ED31A416FB5BE1699A63421AA04F970AFA1FB2EDF8FECEE8462852347
SHA-512:	06326ADFF4C872E257E5C6457EAF6A372C82C4B9B2148441AA7CC7197EE3265EDD74F0510809C19925B4B75B6CFB0862CF25F6C6E070CF10B5EB5A02403B66A
Malicious:	false
Preview:	....! !%%%%%%%%%%%.......... ... %%%.... .6....Adobe.d...!.1."AQ.2aq#B....R..r$3b....%.4C.....5Scs.....................!..1AQ.."a2q.......B....R.#3b.r.......... ..?......q).r..y.6.FV7N.....A..9E..6..[M..k..7.............t...d.y@.&.R.-...5.qK..<...0X=.H.d#*xR3....D...o .I.Z.....n..b;.9.k=..^.O..UV...:a2J.;....j.7l(.h2B.S.h.:.A......G...7_..e..r[.."8. .}.J.R.A..,.7...2......k].=..`.h...D.|.$5&Y..F..;.L..*..e.. .N...rd.iP.........p...z.{.>...1..$..G....^v..^.......rB.8"...6W....[6.......Y..MJ8.........%.!..W.M....z...X.W.[..C.v>.Q:......I.Hb"C.8&... ..$`.`...N....U.F...j./d...(..3..{sM....^...bI.<..?z.z.Pj.4....+.G..hn. >!iut.!..}.J....z....Kp...=.y......*..O...5.+!v7>...#....X.[E..g<Q.#....a....T.7?..v........y3y*.T.K_.q.7....m.!..f4...x..=;s]<. ..J...c..<.}?z

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\vaccine[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	49459
Entropy (8bit):	4.990580136642374
Encrypted:	false
SSDEEP:	768:lJMIGuF0zp2CHLW9z9rRIVDLjZR9ejjATKAoBgQzYUw:lJMYGp3HCZrRIVxejjAeAoSQzY3
MD5:	A75FF6CD8DE4DCCD74D310E45A12A34E
SHA1:	A39C85A551B681BE171B9D74697F0A5F4AF81B7F
SHA-256:	60D037A4A9C3889CA5C915885661E8A3C8A8021DDADB587A9D1E09B17265F02B
SHA-512:	35F29BE66773A339833C04108C526DED03634441D1D90C12F0259D62C1C8BBE0EA4EC6CCE3085C50AFAB7FA457C395B2CD69DA215E484B4A0592726C84F5B05
Malicious:	false
Preview:	<!DOCTYPE html><html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en"> Level 0 --><head> Level 10.10.00.00.00 --> Standard Metadata --><meta content="text/html; charset=utf-8" http-equiv="Content-Type"/><meta content="en-us" http-equiv="Content-Language"/><meta content="IE=edge" http-equiv="X-UA-Compatible"/><meta content="width=device-width, initial-scale=1" name="viewport"/><meta content="Emory University" name="copyright"/><meta content="e380b47a0ae720987c778c0848b4c050" name="cms-id"/><meta content="" name="description"/> Opengraph Metadata --><meta content="university" property="og:type"/><meta content="COVID-19 Vaccine | Emory University | Atlanta GA" property="og:title"/><meta content="" property="og:description"/><meta content="https://emory.edu/forward/covid-19/vaccine.html" property="og:url"/><meta content="summary" property="twitter:card"/><meta content="COVID-19 Vaccine | Emory University | Atlanta GA" property="twitter:title"/><meta content="" p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\widgets[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	97358
Entropy (8bit):	5.185445434545827
Encrypted:	false
SSDEEP:	1536:NNVr5gFSc3jyl5BdEvyjkcahO6wXaa17GH2umrAMMOTMSD2/:95Vy+Rez7xiZThD2/
MD5:	9EB59E5602FEF4B3EBF6090856FF21DB
SHA1:	4312BA68D48BCA7C31D6DAFC18FCB30A31EF14B1
SHA-256:	A12B87855B6403C6F73092396D80541A6984AAE03097A637769291D9CAD15D19
SHA-512:	DCD7B5136BCEDCD16B256B82024EA54B089468DAD65A333D00170E8F2B65CCC6450BFBEE591FDFD3A58994123B82FBFB640468FE2A3C6428D6BAB7E4B0682973
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\widgets[1].js	
Preview:	Function&&Function.prototype&&Function.prototype.bind&&(/(MSIE ([6789]|10|11))|Trident/.test(navigator.userAgent)||(window.__twttr&&window.__twttr.widgets&&window.__twttr.widgets.loaded&&window.twttr.widgets.load&&window.twttr.widgets.load(),window.__twttr&&window.__twttr.widgets&&window.__twttr.widgets.init||function(t){function e(e){for(var n,i,o=e[0],s=e[1],a=0,c=[];a<o.length;a++)i=o[a],r[i]&&c.push(r[i][0]),r[i]=0;for(n in s)Object.prototype.hasOwnProperty.call(s,n)&&(t[n]=s[n]);for(u&&u(e);c.length;)c.shift()()}var n={},r={1:0};function i(e){if(n[e])return n[e].exports;var r=n[e]={i:e,l:!1,exports:{}};return t[e].call(r.exports,r,r.exports,i),r.l=!0,r.exports}i.e=function(t){var e=[],n=r[t];if(0!==n)if(n)e.push(n[2]);else{var o=new Promise(function(e,i){n=r[t]=[e,i]});e.push(n[2]=o);var s,a=document.getElementsByTagName("head")[0],u=document.createElement("script");u.charset="utf-8",u.timeout=120,i.nc&&u.setAttribute("nonce",i.nc),u.src=function(t){return i.p+"js/"+({0:"moment~ti

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\646589415962224[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	798798
Entropy (8bit):	5.472425458154517
Encrypted:	false
SSDEEP:	6144:Rk1HgCSntDV/HaK8V/Ha8NEPjQHguH3HpQrwz8GWZk1HgCSntDV/HaK8V/Ha8NEj:kNE7mNE7mNE75
MD5:	AD1EFE46438E1DF908A8A15E2C5441F5
SHA1:	4AF38D3B07B5D28A9E7C77E6C8FA477C1F1234E9
SHA-256:	10F2ADEBA482C83A40C15CF088ED5B1AD1CF6186C8EC2F8B22C7CF59ABAD6C48
SHA-512:	C413683F7268F7491BD5EC3B8D2D22FA371E3F60A2807013FBB2CDB54178F566B452360897DDCE7D2B514FD683E8D8A110D262B5124AE29A652366B54FC75117
Malicious:	false
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN_0000_0052802-15kh-f178-_man_research[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=12, height=452, bps=0, PhotometricIntepretation=RGB, orientation=upper-left, width=820], baseline, precision 8, 820x452, frames 3
Category:	dropped
Size (bytes):	56032
Entropy (8bit):	7.817727959740995
Encrypted:	false
SSDEEP:	768:VdnZQOa9d74nZQOa9BgtJAtFJPhUmjva9J/qf/Ita076aFfUPJPrFKXfCu:VPQ0Q3gktZUmDa9J/2f0OamyCu
MD5:	B29A326C3C74E753D6B64BF3ED6448E8
SHA1:	9D3A250FC709E9E56A4AD20F38F65CF92E0C0953
SHA-256:	8CA195F24A9849C2D938E58BE2CDE9D88E8E8BD5E0582C0985EB291692BDD6E1
SHA-512:	C5985779FCACF94A74D785321AF6D8A7158F3B55C6604D54688D7E6C26993ADBA8568ED3BDF078F0A17D8EAB96FC3CD23651FF99D94486C904DB1C985E862E
Malicious:	false
Preview:	......Exif..MM.*.....4.....(.....1.....!.....2.....i.....$.....'.....'.Adobe Photoshop 21.2 (Macintosh).2020:07:24 01:27:00.....0231.....4.....r.....z.(.....@.....H.....H.....Adobe_CM.....Adobe.d.....X....".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?.o.=A.G..&.ve..~.w..-...w..]..~ekC.}_..e3.>.....8..S^.I.j...[:{...^#37

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN_0000_0102205-15kh-f152-_raw_arts[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=12, height=756, bps=0, PhotometricIntepretation=RGB, orientation=upper-left, width=756], baseline, precision 8, 756x756, frames 3
Category:	dropped
Size (bytes):	66241
Entropy (8bit):	7.823124118811826
Encrypted:	false
SSDEEP:	1536:muq4OMWuq4OM9pp4OVEygfUvui45uUpv3W32h1:bOcOkeLfCZVUpPWQ
MD5:	D6813A6AC706722B70CF20ECD5B9D102
SHA1:	50958D295FF6E5231C2A712C825AA51A8571F670
SHA-256:	9C1DA6FF3ED399BD5C8AD65FB24E2D42A74CBC8A401531CAACAE26A4C9A107EE
SHA-512:	B1AAB9F3412186E0B4A417C85449230304AF25460860BCF81C427F7F51CAC41F6BF68306A774E4BC3610D8738E4EB7E5D247267E3632B3124A3E46B9F84E35BF
Malicious:	false
Preview:	....!.Exif..MM.*.....(.....1.....!.....2.....i.....$.....'.....'.Adobe Photoshop 21.2 (Macintosh).2020:07:24 01:27:02.....0231.....r.....z.(..... E.....H.....H.....Adobe_CM.....Adobe.d.....".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?.7.,..}i.=....".$..n-../o.....d3..Z.....h3...o..j^....:.-x..v ..~9\

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN_0003_0033001-14kh-f325-_raw_atlanta[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=12, height=756, bps=0, PhotometricIntepretation=RGB, orientation=upper-left, width=756], baseline, precision 8, 756x756, frames 3
Category:	dropped
Size (bytes):	80124
Entropy (8bit):	7.841600156306258
Encrypted:	false
SSDEEP:	1536:cpJWjAYpJWjAoObfnv/iyWFR8ZyFpqZoND2Lk8D6L2wQ++PQiq0Y5WKZI:cTWkYTWkJTnHqFR8GEUADRnlP8WKZI
MD5:	6000E240146270CC34F5D64280CE0F19
SHA1:	D671F31A136079F0E3462D38B03B20CDCF9BD912
SHA-256:	09DDFF374D5BB0F9590DEF4C62C1FC6BF94774C13FA5FCC930ADB77374441A7B
SHA-512:	1E580639AD9EDA1391A464C34D7DAF500CBCDF63651B5C5E76D9AEABBCF5B69C75D433C311678A07E1F18277008765E819D842069CE2BD49DF45674B165BA5E
Malicious:	false
Preview:	.....`Exif..MM.*.....(.....1.....!.....2.....i.....$.....'.....'.Adobe Photoshop 21.2 (Macintosh).2020:07:24 01:27:04.....0231.....r.....z.(.....H.....H.....Adobe_CM.....Adobe.d.....".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?..P.. ..Vib.xJ..-.t.%J[T.O.%Jc.Z.BP.).Z.$.).hSM.R..S...$h..FB.....HJ"...R.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN_0004_0110903-17ab-f001-give[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=12, height=452, bps=0, PhotometricIntepretation=RGB, orientation=upper-left, width=820], baseline, precision 8, 820x452, frames 3
Category:	dropped
Size (bytes):	43496
Entropy (8bit):	7.704646154123888
Encrypted:	false
SSDEEP:	768:GQZH9wbX7hQZH9wbSdll++IbfLwkAavR0x54wMUc1osDsoWO:GAH6bVAH6bSdl1wkAnxqUW1soWO
MD5:	6625D6B92DF936C7E46C1F7D3238DA60
SHA1:	D305CBE4E9399E6B6590CFE5460CEC7942DB9FA5
SHA-256:	33F15C75D0DDB1969DD854D7DD17A27D3734022040B45A9DD7970637D781B47D
SHA-512:	5A3EC54C882CB4CE358F660FD7B32B18101B487C9C9E0576341CC265DD0397ED9546A5D4D65500AAE6619AAAB4B179390B17669B8D289875A4875A498F71F14A
Malicious:	false
Preview:	......Exif..MM.*.....4.....(.....1.....!.....2.....i.....$.....'.....'.Adobe Photoshop 21.2 (Macintosh).2020:07:24 01:27:05.....0231.....4.....r.....z.(.....H.....H.....Adobe_CM.....Adobe.d.....X....".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?...0z_..:.b*.l<.....2...sL.....I..t..]..7R.....X..C.v...->(p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\additional[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:F:F
MD5:	7215EE9C7D9DC229D2921A40E899EC5F
SHA1:	B858CB282617FB0956D960215C8E84D1CCF909C6
SHA-256:	36A9E7F1C95B82FFB99743E0C5C4CE95D83C9A430AAC59F84EF3CBFAB6145068
SHA-512:	F90DDD77E400DFE6A3FCF479B00B1EE29E7015C5BB8CD70F5F15B4886CC339275FF553FC8A053F8DDC7324F45168CFFAF81F8C3AC93996F6536EEF38E5E407
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\all[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	58935
Entropy (8bit):	4.71737763289683
Encrypted:	false
SSDEEP:	768:qEC31IPiyXNq4/xBowbHJmkwFR/sMQyYJYX9BftF5Qzl:qEPPxXE4/XJH8dF+fy9ltkB
MD5:	84D8AD2B4FCDC0F0C58247E778133B3A
SHA1:	6F33EAE92D42FE209167139940A0AD6A3C6C167E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\all[1].css	
SHA-256:	14CBD9B866A9B092E3A2E03A93B128DA5BACA005FD8B44A1956146EAAB7B48B7
SHA-512:	D4F28E808639F7127C0A8F3E344E8567E2CE0192A3CBE298F22AB41B80770B2798EB0607377CADF4F5B45E94AB8959643177B8D0F4CA9D7ACB9D9F7E7E40DAA2
Malicious:	false
Preview:	/*!. * Font Awesome Free 5.14.0 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */..fa,.fab,.fad,.fal,.far,.fas{-moz-osx-font-smoothing:grayscale;-webkit-font-smoothing:antialiased;display:inline-block;font-style:normal;font-variant:normal;text-rendering:auto;line-height:1}.fa-lg{font-size:1.33333em;line-height:.75em;vertical-align:-.0667em}.fa-xs{font-size:.75em}.fa-sm{font-size:.875em}.fa-1x{font-size:1em}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-6x{font-size:6em}.fa-7x{font-size:7em}.fa-8x{font-size:8em}.fa-9x{font-size:9em}.fa-10x{font-size:10em}.fa-fw{text-align:center;width:1.25em}.fa-ul{list-style-type:none;margin-left:2.5em;padding-left:0}.fa-ul>li{position:relative}.fa-li{left:-2em;position:absolute;text-align:center;width:2em;line-height:inherit}.fa-border{border:.08em solid #eee;border-radius:.1em;padding:.2em .25em .15em}.fa-pu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\angle-grid-bg[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	16969
Entropy (8bit):	4.910400482887004
Encrypted:	false
SSDEEP:	384:OO+jwVZg8G4rjRQ+h/f8NJ0+/CtLR0qUYy4z7neMqODjmrsqBFuA5k0Z9Mdjzrs3:J1l+i3zsze8iHXHW7ozLClQRKElxSzIa
MD5:	766EAA289C451EAD91C70985372EAE78
SHA1:	89D3E395A13399EC64D67FAE081E239B82AE4715
SHA-256:	BFA113AB3E0DCFEEE5CC32AD42301987B79C946A283BA6F83FDBD84C59CB93E0
SHA-512:	951594B649AF7A10283325AE6E33D19BD4C0523E0835D69674C5C6A1BE19BE93B5C64C68F268A994815E9A7BF686176BF37344AD5F5689B35A553E2D080CF513
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 24.1.3, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 2135.498 1159.608" style="enable-background:new 0 0 2135.498 1159.608;" xml:space="preserve">..<style type="text/css">....st0{clip-path:url(#SVGID_2_);}....st1{fill:none;stroke:#0030B0;stroke-width:2;stroke-miterlimit:10;}..</style>..<g>...<defs>....<rect id="SVGID_1_" width="2135.498" height="1159.608"/>...</defs>...<clipPath id="SVGID_2_">....<use xlink:href="#SVGID_1_" style="overflow:visible;"/>...</clipPath>...<g class="st0">....<g>.....<rect x="1125.617" y="808.492" class="st1" width="400.743" height="197.903"/>.....<polyline class="st1" points="1325.765,1006.395 1225.766,907.219 1325.74,808.492 ..."/>.....<line class="st1" x1="1125.617" y1="907.219" x2="1224.345" y2="808.492"/>.....<line class="st1" x1="1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\background_gradient[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	dropped
Size (bytes):	453
Entropy (8bit):	5.019973044227213
Encrypted:	false
SSDEEP:	6:3llVuiPjlXJYhg5suRd8PImMo23C/kHrJ8yA/NIeYoWg78C/vTFvbKLAh3:V/XPYhiPRd8j7+9LoIrobtHTdbKi
MD5:	20F0110ED5E4E0D5384A496E4880139B
SHA1:	51F5FC61D8BF19100DF0F8AADAA57FCD9C086255
SHA-256:	1471693BE91E53C2640FE7BAEECBC624530B088444222D93F2815DFCE1865D5B
SHA-512:	5F52C117E346111D99D3B642926139178A80B9EC03147C00E27F07AAB47FE38E9319FE983444F3E0E36DEF1E86DD7C56C25E44B14EFDC3F13B45EDEDA064DB5A
Malicious:	false
Preview:	......JFIF.....d.d......Ducky.......P......Adobe.d..... ....W..... .....Qa.....?.....%.....x......s...Z.....j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.....p.....A.....BP..qD.(.....ntH.@.....h?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\calendar-events[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1000
Entropy (8bit):	4.6973618567584285
Encrypted:	false
SSDEEP:	24:DOlwSfPFS50v+ZO9AfPjCWssUquU0fb5OOoODe:qxf45CV9Af7BssKjfsOZDe
MD5:	2FC52945CE0C038C15ADEC9448D3F9EC
SHA1:	A384DFD6E13808E6E3A0D06748F9BC170D4A2485
SHA-256:	84AC4E278DCCB511BAE2E01E294F7770360E0B82B4B5492E385B2AA671151CEF
SHA-512:	C66241A7962118E73722A7E1989A13FAFD0FD3CFC40754C86B1C6DC8755AA44840243A12215CC7F7FF0DFA0A1DA4EB3E44CF3A7E65A6DDA92F36C98CA78E184
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\calendar-events[1].js	
Preview:	/* exported CalendarEvents */../* global CalendarHandler */....var CalendarEvents = (function() {.... var formChange = function() {.. $('.js-events__form').on('change', function() {.. // We don't want to respond to form changes.. // while the filters are being cleared... if (! $(this).data('filterable-clearing')) {.. CalendarHandler.update($(this).closest('.js-events')); .. }.. });.. };.. .. var formReset = function() {.. $('.js-events__form').on('reset', function(event) {.. event.preventDefault();.. var $element = $(this).closest('.js-filterable');.. FilterableHandler.clearForm($element);.. FilterableHandler.updateFilterTags($element);.. });.. };.... var pageLoad = function() {.. $('.js-events').each(function() {.. CalendarHandler.init();.. CalendarHandler.update($(this));.. });.. };.... return {.. init: function() {.. pageLoad();.... formChange();.. formReset();.. }.. };..}());

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\calendar-handler[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	6937
Entropy (8bit):	4.820088294668489
Encrypted:	false
SSDEEP:	192:sMxHfBnL4pKgKnX/3sLV3pCNbrmWYHalrfMw:nfpIZqaWt
MD5:	306C0438B79400D162303695ECFC1125
SHA1:	A2E47DD8DB4973A4130BC50D8ED94159324CBB96
SHA-256:	57268A5FE6F9BAC386AC178F584512E7A1BC3CB6E72F4C5789420EBDB5B55542
SHA-512:	77BCFC52FA7D8695C266A80C92DC79405C70D5E13A32E4E280DC2E2E7F5892CF62089EB77280ECE95EBB4A8296EF26CFD7323F3D51E16678C9C731FBE7F1A54
Malicious:	false
Preview:	/* global FilterableHandler */ ../* exported CalendarHandler */....var CalendarHandler = (function() {.... var loading = false;.. var resultsShown;.... var monthNames = ['January', 'February', 'March', 'April', 'May', 'June', 'July', 'August', 'September', 'October', 'November', 'December'];.... // HTML templates used for rendering HTML from JSON.. var eventTemplate;.. // var filterTagTemplate;.... var registerTemplates = function() {.. eventTemplate = $('.js-events__event-template').html();.. // filterTagTemplate = $('.js-events__filter-tag-template').html();.. };.... return {.. // Return date in the formay yyyymmdd.. formatDate: function(date) {.. var year = date.getFullYear().toString();.. var month = (date.getMonth() + 1).toString();.. if (month.length < 2) {.. month = '0' + month;.. }.. var day = date.getDate().toString();.. if (day.length < 2) {.. day = '0' + day;.. }.. return year + month + day;.. },.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\count-up-events[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	297
Entropy (8bit):	4.6767503541546676
Encrypted:	false
SSDEEP:	6:Uy5wMezY+FXwrGDGCLKtAEaNAmyVRcSunR1M:UyKMeVurG6CL0AEG/yVihfM
MD5:	19381F1B41EBC9CDCBD1BB694C787B1B
SHA1:	EED3BA9C21698135162D504E1ED317647BDDD6AA
SHA-256:	BD5517542C16ADB94CAFFAB7E0C836280FAE0CA90882E5610F68537FB78E8642
SHA-512:	6E319D773835C0E723CB4601E2F73122416F0FB7A88BCC6AD02663542C6E32583805380CDD75628AC8178D02A2FCBA9BD12853751AE80D951575942D15F23EFD
Malicious:	false
Preview:	/* exported CountUpEvents */../* global CountUpHandler */....var CountUpEvents = (function() {.... var pageLoad = function() {.. $('.js-countup').each(function() {.. CountUpHandler.init($(this));.. });.. };.... return {.. init: function() {.. pageLoad();.. }.. };..}());

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\countup.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4702
Entropy (8bit):	4.9558844652214535
Encrypted:	false
SSDEEP:	96:RsH6HUqlSOayE+46RbYi4laJ+bcyaYXaeaA4:Rs/P+48bZGv4
MD5:	D5C3E88A2F3FF9DE8E6FED6BD9229380
SHA1:	E401EE142178C2660BA2C632CDF425F79F85000E
SHA-256:	2C11E1FC129518C99997D192027C4940562698E6EDE1DE2C85D4A85D70F45B16
SHA-512:	8E13F07845416EFD460A942B54FB988313E2CBB33DA45938F8E7845B88AA829D64A20CFC29A791B76411478D2BC173ED970B0B9ED1CE64AF3D1A250AC07B6E3
Malicious:	false
Preview:	var __assign=this&&this.__assign||function(){return(__assign=Object.assign||function(t){for(var i,a=1,s=arguments.length;a<s;a++)for(var n in i=arguments[a])Object.prototype.hasOwnProperty.call(i,n)&&(t[n]=i[n]);return t}).apply(this,arguments)},CountUp=function(){function t(t,i,a){var s=this;this.target=t,this.endVal=i,this.options=a,this.version="2.0.4",this.defaults={startVal:0,decimalPlaces:0,duration:2,useEasing:!0,useGrouping:!0,smartEasingThreshold:999,smartEasingAmount:333,separator:",",decimal:".",prefix:"",suffix:""},this.finalEndVal=null,this.useEasing=!0,this.countDown=!1,this.error="",this.startVal=0,this.paused=!0,this.count=function(t){s.startTime||(s.startTime=t);var i=t-s.startTime;s.remaining=s.duration-i,s.useEasing?s.countDown?s.frameVal=s.startVal-s.easingFn(i,0,s.startVal-s.endVal,s.duration):s.frameVal=s.easingFn(i,s.startVal,s.endVal-s.startVal,s.duration):s.countDown?s.frameVal=s.startVal-(s.startVal-s.endVal)*(i/s.duration):s.frameVal=s.startVal+(s.endVal-s.st

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\decal-on-floor-600x339[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\decal-on-floor-600x339[1].jpg	
File Type:	[TIFF image data, little-endian, direntries=15, height=3200, bps=194, PhotometricInterpretation=RGB, description=0071401-20KH Return to Campus scenes COVID 19. Shot for CPA, Laura Redfern, manufacturer=Canon, model=Canon EOS 5D Mark III, orientation=upper-left, width=4800], baseline, precision 8, 432x244, frames 3
Category:	dropped
Size (bytes):	214715
Entropy (8bit):	7.941753242965893
Encrypted:	false
SSDEEP:	3072:2aSBnpNdiCouUMUGpJGE3vaY8CKqn21wdX4sGwDh4x4PxyMhB6KUL+wX9G:2ael9mM1pEE/aUKq6/wDY4pyGIHLlI
MD5:	28E7E230259E509BC7DC42AA0D5E270A
SHA1:	B1090BDAA30F8CC1549D353524B3482414BDF24C
SHA-256:	DA6730C11DA4AE928A7EA0429D9AEE0351E445C8EE58314F335FEC3FDE571F29
SHA-512:	161DC4FA631F0E75659D6CB0C325688A44E74184BB706666EAD516EEE4D10300150F90F87172A2750A58C192CCBCD25265A2017E369CFE7A81709832F69E2BA3
Malicious:	false
Preview:	....&0Exif..II*.....K...../.....7...(.....1.....?...2.....^...i.....t.....0071401-20KH Return to Campus scenes COVID 19. Shot for CPA, Laura Redfern.Canon.Canon EOS 5D Mark III.....'.....'..Adobe Photoshop CC (Macintosh).2020:07:17 10:42:35... .....'.....0.....2.....0230.....2.....:.....B.....J.....R.....00.....00.....Z...b.....1.....j...2.....w...4.....5.....<.....2020:07:14 09:33:36.2020:07:14 09:33:36..!Z.@B...T-.@B.....F..... ....422023005384.F.....EF70-200mm f/2.8L IS II USM.00004338c3.....

Static File Info

General

File type:	PDF document, version 1.7
Entropy (8bit):	7.875769083539466
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	Strategic Procurement Services Supplier Notice COVID19 June 30 2021.pdf
File size:	122992
MD5:	39bc0abebb458b279afe35c3a7ce62f9
SHA1:	785637468cdd2a1b5f816576d8c1b521445ffbc3
SHA256:	d41884b2af008616298459822a9f842e668b652d73cd7b8acbc113c4aed3c928
SHA512:	3f8fc3cb9a85f0061ca743be6c813a99f9dfb25678a7fa963d314d004bae64473fdf530d4f99e185cb14dd544fa629367c932f46772dc8fdd12c465554f06a60
SSDEEP:	1536:Vlieu5Seg3WON0jNFmgKTTjmQwiMNiWbY2ZEOezsQiKGirIgb8GeYHyjCFHO:XipFRFSiXiERRs1rMGeCHO
File Content Preview:	%PDF-1.7..%.....1 0 obj..<</Type/Catalog/Pages 2 0 R/Lang(en-US) /StructTreeRoot 44 0 R/MarkInfo<</Marked true>>/Metadata 194 0 R/ViewerPreferences 195 0 R>>..endobj..2 0 obj..<</Type/Pages/Count 3/Kids[3 0 R 27 0 R 41 0 R] >>..endobj..3 0 obj..<</Type/

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

Header:	%PDF-1.7
Total Entropy:	7.875769
Total Bytes:	122992
Stream Entropy:	7.966900
Stream Bytes:	107827
Entropy outside Streams:	0.000000
Bytes outside Streams:	15165
Number of EOF found:	2
Bytes after EOF:	

Keywords Statistics

Image Streams

ID	DHASH	MD5	Preview
26	d3cbcbd7c3000200	e74ff4756671c4e7a9fdf80e66d4fe24	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 6, 2021 16:55:19.420888901 CEST	192.168.2.6	8.8.8.8	0x239d	Standard query (0)	emory.edu	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:30.470453978 CEST	192.168.2.6	8.8.8.8	0xe504	Standard query (0)	www.emory.edu	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:31.780875921 CEST	192.168.2.6	8.8.8.8	0x3966	Standard query (0)	www.emory.edu	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:32.784977913 CEST	192.168.2.6	8.8.8.8	0xc14	Standard query (0)	template.emory.edu	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:32.791687965 CEST	192.168.2.6	8.8.8.8	0x57b	Standard query (0)	use.fontawesome.com	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:32.888217926 CEST	192.168.2.6	8.8.8.8	0x7dc4	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:33.125878096 CEST	192.168.2.6	8.8.8.8	0x16b7	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:33.162501097 CEST	192.168.2.6	8.8.8.8	0x31cc	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:33.393528938 CEST	192.168.2.6	8.8.8.8	0x43bf	Standard query (0)	emory.edu	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:34.135431051 CEST	192.168.2.6	8.8.8.8	0x5436	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:35.264009953 CEST	192.168.2.6	8.8.8.8	0x6f05	Standard query (0)	www.google.de	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:35.605926991 CEST	192.168.2.6	8.8.8.8	0xfa30	Standard query (0)	platform.twitter.com	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:37.132889986 CEST	192.168.2.6	8.8.8.8	0x5edc	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:59.993778944 CEST	192.168.2.6	8.8.8.8	0xad9d	Standard query (0)	www.emory.edu	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:05.237380981 CEST	192.168.2.6	8.8.8.8	0x2b33	Standard query (0)	siteimproveanalytics.com	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:07.747484922 CEST	192.168.2.6	8.8.8.8	0x3bac	Standard query (0)	secure.quantserve.com	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:07.805912971 CEST	192.168.2.6	8.8.8.8	0x6a2c	Standard query (0)	66356337.global.siteimproveanalytics.io	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:07.934437990 CEST	192.168.2.6	8.8.8.8	0x75a2	Standard query (0)	www.juicer.io	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:08.018229961 CEST	192.168.2.6	8.8.8.8	0xb42f	Standard query (0)	rules.quantcount.com	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:08.314413071 CEST	192.168.2.6	8.8.8.8	0x5ae3	Standard query (0)	pixel.quantserve.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 6, 2021 16:56:08.712498903 CEST	192.168.2.6	8.8.8.8	0x2155	Standard query (0)	img.juicer.io	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:08.715594053 CEST	192.168.2.6	8.8.8.8	0x7cc1	Standard query (0)	pbs.twimg.com	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:08.963123083 CEST	192.168.2.6	8.8.8.8	0x370a	Standard query (0)	scontent.cdninstagram.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 6, 2021 16:55:19.475716114 CEST	8.8.8.8	192.168.2.6	0x239d	No error (0)	emory.edu		170.140.125.20	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:30.630331039 CEST	8.8.8.8	192.168.2.6	0xe504	No error (0)	www.emory.edu		170.140.125.16	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:31.840899944 CEST	8.8.8.8	192.168.2.6	0x3966	No error (0)	www.emory.edu		170.140.125.16	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:32.837865114 CEST	8.8.8.8	192.168.2.6	0x57b	No error (0)	use.fontawesome.com	fontawesome-cdn.fonticons.netdna-cdn.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 16:55:32.837865114 CEST	8.8.8.8	192.168.2.6	0x57b	No error (0)	fontawesome-cdn.fonticons.netdna-cdn.com		23.111.9.35	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:32.934745073 CEST	8.8.8.8	192.168.2.6	0x7dc4	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 16:55:32.947621107 CEST	8.8.8.8	192.168.2.6	0xc14	No error (0)	template.emory.edu		170.140.125.169	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:33.182132006 CEST	8.8.8.8	192.168.2.6	0x16b7	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 16:55:33.182132006 CEST	8.8.8.8	192.168.2.6	0x16b7	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:33.220406055 CEST	8.8.8.8	192.168.2.6	0x31cc	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:33.220406055 CEST	8.8.8.8	192.168.2.6	0x31cc	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:33.561404943 CEST	8.8.8.8	192.168.2.6	0x43bf	No error (0)	emory.edu		170.140.125.20	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:34.191210032 CEST	8.8.8.8	192.168.2.6	0x5436	No error (0)	googleads.g.doubleclick.net		172.217.16.98	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:35.321556091 CEST	8.8.8.8	192.168.2.6	0x6f05	No error (0)	www.google.de		142.250.201.195	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:35.671968937 CEST	8.8.8.8	192.168.2.6	0xfa30	No error (0)	platform.twitter.com	cs472.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 16:55:35.671968937 CEST	8.8.8.8	192.168.2.6	0xfa30	No error (0)	cs472.wac.edgecastcdn.net	cs1-apr-8315.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 16:55:35.671968937 CEST	8.8.8.8	192.168.2.6	0xfa30	No error (0)	cs1-apr-8315.wac.edgecastcdn.net	wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 16:55:35.671968937 CEST	8.8.8.8	192.168.2.6	0xfa30	No error (0)	cs1-lb-eu.8315.ecdns.net	cs491.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 16:55:35.671968937 CEST	8.8.8.8	192.168.2.6	0xfa30	No error (0)	cs491.wac.edgecastcdn.net		192.229.233.25	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:37.178869963 CEST	8.8.8.8	192.168.2.6	0x5edc	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 16:55:37.178869963 CEST	8.8.8.8	192.168.2.6	0x5edc	No error (0)	stats.l.doubleclick.net		64.233.166.155	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:37.178869963 CEST	8.8.8.8	192.168.2.6	0x5edc	No error (0)	stats.l.doubleclick.net		64.233.166.156	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 6, 2021 16:55:37.178869963 CEST	8.8.8.8	192.168.2.6	0x5edc	No error (0)	stats.l.doubleclick.net		64.233.166.157	A (IP address)	IN (0x0001)
Jul 6, 2021 16:55:37.178869963 CEST	8.8.8.8	192.168.2.6	0x5edc	No error (0)	stats.l.doubleclick.net		64.233.166.154	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:00.054117918 CEST	8.8.8.8	192.168.2.6	0xad9d	No error (0)	www.emory.edu		170.140.125.16	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:05.299197912 CEST	8.8.8.8	192.168.2.6	0x2b33	No error (0)	siteimproveanalytics.com		172.64.172.12	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:05.299197912 CEST	8.8.8.8	192.168.2.6	0x2b33	No error (0)	siteimproveanalytics.com		172.64.173.12	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:07.808046103 CEST	8.8.8.8	192.168.2.6	0x3bac	No error (0)	secure.quantserve.com	2kpixel.quantserve.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 16:56:07.808046103 CEST	8.8.8.8	192.168.2.6	0x3bac	No error (0)	2kpixel.quantserve.com	global.px.quantserve.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 16:56:07.808046103 CEST	8.8.8.8	192.168.2.6	0x3bac	No error (0)	global.px.quantserve.com		91.228.74.133	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:07.808046103 CEST	8.8.8.8	192.168.2.6	0x3bac	No error (0)	global.px.quantserve.com		91.228.74.198	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:07.808046103 CEST	8.8.8.8	192.168.2.6	0x3bac	No error (0)	global.px.quantserve.com		91.228.74.134	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:07.808046103 CEST	8.8.8.8	192.168.2.6	0x3bac	No error (0)	global.px.quantserve.com		91.228.74.189	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:07.808046103 CEST	8.8.8.8	192.168.2.6	0x3bac	No error (0)	global.px.quantserve.com		91.228.74.226	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:07.864487886 CEST	8.8.8.8	192.168.2.6	0x6a2c	No error (0)	66356337.global.siteimproveanalytics.io	eu-central-1.global.siteimproveanalytics.io		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 16:56:07.864487886 CEST	8.8.8.8	192.168.2.6	0x6a2c	No error (0)	eu-central-1.global.siteimproveanalytics.io	ana-cf-col-elb-78-567119012.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 16:56:07.864487886 CEST	8.8.8.8	192.168.2.6	0x6a2c	No error (0)	ana-cf-col-elb-78-567119012.eu-central-1.elb.amazonaws.com		18.195.138.231	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:07.864487886 CEST	8.8.8.8	192.168.2.6	0x6a2c	No error (0)	ana-cf-col-elb-78-567119012.eu-central-1.elb.amazonaws.com		52.57.38.161	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:07.998485088 CEST	8.8.8.8	192.168.2.6	0x75a2	No error (0)	www.juicer.io		104.26.13.87	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:07.998485088 CEST	8.8.8.8	192.168.2.6	0x75a2	No error (0)	www.juicer.io		104.26.12.87	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:07.998485088 CEST	8.8.8.8	192.168.2.6	0x75a2	No error (0)	www.juicer.io		172.67.71.67	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:08.075237036 CEST	8.8.8.8	192.168.2.6	0xb42f	No error (0)	rules.quantcount.com	d2fashanjl7d9f.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 16:56:08.075237036 CEST	8.8.8.8	192.168.2.6	0xb42f	No error (0)	d2fashanjl7d9f.cloudfront.net		13.224.99.16	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:08.075237036 CEST	8.8.8.8	192.168.2.6	0xb42f	No error (0)	d2fashanjl7d9f.cloudfront.net		13.224.99.26	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:08.075237036 CEST	8.8.8.8	192.168.2.6	0xb42f	No error (0)	d2fashanjl7d9f.cloudfront.net		13.224.99.5	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:08.075237036 CEST	8.8.8.8	192.168.2.6	0xb42f	No error (0)	d2fashanjl7d9f.cloudfront.net		13.224.99.112	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 6, 2021 16:56:08.372996092 CEST	8.8.8.8	192.168.2.6	0x5ae3	No error (0)	pixel.quantserve.com	global.px.quantserve.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 16:56:08.372996092 CEST	8.8.8.8	192.168.2.6	0x5ae3	No error (0)	global.px.quantserve.com		91.228.74.198	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:08.372996092 CEST	8.8.8.8	192.168.2.6	0x5ae3	No error (0)	global.px.quantserve.com		91.228.74.226	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:08.372996092 CEST	8.8.8.8	192.168.2.6	0x5ae3	No error (0)	global.px.quantserve.com		91.228.74.133	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:08.372996092 CEST	8.8.8.8	192.168.2.6	0x5ae3	No error (0)	global.px.quantserve.com		91.228.74.189	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:08.372996092 CEST	8.8.8.8	192.168.2.6	0x5ae3	No error (0)	global.px.quantserve.com		91.228.74.134	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:08.776500940 CEST	8.8.8.8	192.168.2.6	0x7cc1	No error (0)	pbs.twimg.com	cs196.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 16:56:08.776500940 CEST	8.8.8.8	192.168.2.6	0x7cc1	No error (0)	cs196.wac.edgecastcdn.net	cs2-wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 16:56:08.776500940 CEST	8.8.8.8	192.168.2.6	0x7cc1	No error (0)	cs2-wac-eu.8315.ecdns.net	cs672.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 16:56:08.776500940 CEST	8.8.8.8	192.168.2.6	0x7cc1	No error (0)	cs672.wac.edgecastcdn.net		192.229.233.50	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:08.776524067 CEST	8.8.8.8	192.168.2.6	0x2155	No error (0)	img.juicer.io		104.26.12.87	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:08.776524067 CEST	8.8.8.8	192.168.2.6	0x2155	No error (0)	img.juicer.io		104.26.13.87	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:08.776524067 CEST	8.8.8.8	192.168.2.6	0x2155	No error (0)	img.juicer.io		172.67.71.67	A (IP address)	IN (0x0001)
Jul 6, 2021 16:56:09.022571087 CEST	8.8.8.8	192.168.2.6	0x370a	No error (0)	scontent.cdninstagram.com		157.240.17.63	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
Jul 6, 2021 16:55:32.320278883 CEST	170.140.125.16	443	192.168.2.6	49761	CN=www.emory.edu, O=Emory University, L=Atlanta, ST=Georgia, C=US CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Jul 02 02:00:00 CEST 2021	Sun Jul 03 01:59:59 CEST 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Mon Oct 06 02:00:00 CEST 2014	Sun Oct 06 01:59:59 CEST 2024		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jul 6, 2021 16:55:32.320323944 CEST	170.140.125.16	443	192.168.2.6	49762	CN=www.emory.edu, O=Emory University, L=Atlanta, ST=Georgia, C=US CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Jul 02 02:00:00 CEST 2021 Mon Oct 06 02:00:00 CEST 2014 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Sun Jul 03 01:59:59 CEST 2022 Sun Oct 06 01:59:59 CEST 2024 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	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=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Mon Oct 06 02:00:00 CEST 2014	Sun Oct 06 01:59:59 CEST 2024		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jul 6, 2021 16:55:32.950488091 CEST	23.111.9.35	443	192.168.2.6	49768	CN=*.fontawesome.com, O=Fonticons Inc, L=Bentonville, ST=Arkansas, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 13 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Wed Dec 15 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jul 6, 2021 16:55:33.051548958 CEST	23.111.9.35	443	192.168.2.6	49767	CN=*.fontawesome.com, O=Fonticons Inc, L=Bentonville, ST=Arkansas, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 13 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Wed Dec 15 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jul 6, 2021 16:55:33.260615110 CEST	157.240.17.15	443	192.168.2.6	49777	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 26 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 25 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jul 6, 2021 16:55:33.263571978 CEST	157.240.17.15	443	192.168.2.6	49778	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 26 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 25 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jul 6, 2021 16:55:33.401835918 CEST	170.140.125.169	443	192.168.2.6	49771	CN=template.emory.edu, O=Emory University, L=Atlanta, ST=Georgia, C=US CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue May 25 02:00:00 CEST 2021 Mon Oct 06 02:00:00 CEST 2014 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Sun Jun 26 01:59:59 CEST 2022 Sun Oct 06 01:59:59 CEST 2024 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	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=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Mon Oct 06 02:00:00 CEST 2014	Sun Oct 06 01:59:59 CEST 2024		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 6, 2021 16:55:33.434844017 CEST	104.16.18.94	443	192.168.2.6	49779	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	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 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		
Jul 6, 2021 16:55:33.448102951 CEST	104.16.18.94	443	192.168.2.6	49780	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	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 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		
Jul 6, 2021 16:55:33.448143005 CEST	170.140.125.169	443	192.168.2.6	49772	CN=template.emory.edu, O=Emory University, L=Atlanta, ST=Georgia, C=US CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue May 25 02:00:00 CEST 2021 Mon Oct 06 02:00:00 CEST 2014 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Sun Jun 26 01:59:59 CEST 2022 Sun Oct 06 01:59:59 CEST 2024 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	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=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Mon Oct 06 02:00:00 CEST 2014	Sun Oct 06 01:59:59 CEST 2024		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jul 6, 2021 16:55:33.555205107 CEST	170.140.125.169	443	192.168.2.6	49775	CN=template.emory.edu, O=Emory University, L=Atlanta, ST=Georgia, C=US CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue May 25 02:00:00 CEST 2021 Mon Oct 06 02:00:00 CEST 2014 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Sun Jun 26 01:59:59 CEST 2022 Sun Oct 06 01:59:59 CEST 2024 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Mon Oct 06 02:00:00 CEST 2014	Sun Oct 06 01:59:59 CEST 2024		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jul 6, 2021 16:55:33.713128090 CEST	170.140.125.169	443	192.168.2.6	49776	CN=template.emory.edu, O=Emory University, L=Atlanta, ST=Georgia, C=US CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue May 25 02:00:00 CEST 2021 Mon Oct 06 02:00:00 CEST 2014 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Sun Jun 26 01:59:59 CEST 2022 Sun Oct 06 01:59:59 CEST 2024 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	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=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Mon Oct 06 02:00:00 CEST 2014	Sun Oct 06 01:59:59 CEST 2024		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 6, 2021 16:55:34.068545103 CEST	170.140.125.20	443	192.168.2.6	49781	CN=emory.edu, O=Emory University, L=Atlanta, ST=Georgia, C=US CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Mar 10 01:00:00 CET 2021 Mon Oct 06 02:00:00 CEST 2014 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Mon Apr 11 01:59:59 CEST 2022 Sun Oct 06 01:59:59 CEST 2024 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	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=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Mon Oct 06 02:00:00 CEST 2014	Sun Oct 06 01:59:59 CEST 2024		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jul 6, 2021 16:55:34.101130962 CEST	170.140.125.20	443	192.168.2.6	49782	CN=emory.edu, O=Emory University, L=Atlanta, ST=Georgia, C=US CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Mar 10 01:00:00 CET 2021 Mon Oct 06 02:00:00 CEST 2014 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Mon Apr 11 01:59:59 CEST 2022 Sun Oct 06 01:59:59 CEST 2024 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	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=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Mon Oct 06 02:00:00 CEST 2014	Sun Oct 06 01:59:59 CEST 2024		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jul 6, 2021 16:55:34.335458994 CEST	172.217.16.98	443	192.168.2.6	49786	CN=*.g.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon Jun 07 03:34:07 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Aug 30 03:34:06 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Jul 6, 2021 16:55:34.382344961 CEST	172.217.16.98	443	192.168.2.6	49785	CN=*.g.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon Jun 07 03:34:07 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Aug 30 03:34:06 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	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 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Jul 6, 2021 16:55:35.852812052 CEST	192.229.233.25	443	192.168.2.6	49799	CN=*.twimg.com, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Nov 05 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020	Wed Nov 10 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jul 6, 2021 16:55:35.853638887 CEST	192.229.233.25	443	192.168.2.6	49800	CN=*.twimg.com, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Nov 05 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020	Wed Nov 10 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jul 6, 2021 16:55:37.291974068 CEST	64.233.166.155	443	192.168.2.6	49801	CN=*.g.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon Jun 07 03:34:07 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Aug 30 03:34:06 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	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 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Jul 6, 2021 16:55:37.340747118 CEST	64.233.166.155	443	192.168.2.6	49802	CN=*.g.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon Jun 07 03:34:07 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Aug 30 03:34:06 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	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 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Jul 6, 2021 16:56:00.532000065 CEST	170.140.125.16	443	192.168.2.6	49803	CN=www.emory.edu, O=Emory University, L=Atlanta, ST=Georgia, C=US CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Jul 02 02:00:00 CEST 2021 Mon Oct 06 02:00:00 CEST 2014 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Sun Jul 03 01:59:59 CEST 2022 Sun Oct 06 01:59:59 CEST 2024 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Mon Oct 06 02:00:00 CEST 2014	Sun Oct 06 01:59:59 CEST 2024		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: AcroRd32.exe PID: 3068 Parent PID: 6068

General

Start time:	16:53:53
Start date:	06/07/2021
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\Strategic Procurement Services Supplier Notice COVID19 June 30 2021.pdf'
Imagebase:	0x90000
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

Show Windows behavior

File Created

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: AcroRd32.exe PID: 3424 Parent PID: 3068

General

Start time:	16:53:55
Start date:	06/07/2021
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\Strategic Procurement Services Supplier Notice COVID19 June 30 2021.pdf'
Imagebase:	0x90000
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

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: RdrCEF.exe PID: 6140 Parent PID: 3068

General

Start time:	16:54:02
Start date:	06/07/2021
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:	0xbf0000
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

Show Windows behavior

File Read

Analysis Process: RdrCEF.exe PID: 6204 Parent PID: 6140

General

Start time:	16:54:06
Start date:	06/07/2021
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=1720,11394891864812701617,5421238245506412973,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=3994307663767611292 --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=3994307663767611292 --renderer-client-id=2 --mojo-platform-channel-handle=1752 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xbf0000
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

Show Windows behavior

Analysis Process: RdrCEF.exe PID: 6232 Parent PID: 6140

General

Start time:	16:54:08
Start date:	06/07/2021
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=1720,11394891864812701617,5421238245506412973,131072 --disable-features=VizDisplayCompositor --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --lang=en-US --gpu-preferences=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=2914443920406660741 --mojo-platform-channel-handle=1772 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0xbf0000
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 Show Windows behavior

Analysis Process: RdrCEF.exe PID: 6364 Parent PID: 6140

General

Start time:	16:54:13
Start date:	06/07/2021
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=1720,11394891864812701617,5421238245506412973,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=10280300687710209152 --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=10280300687710209152 --renderer-client-id=4 --mojo-platform-channel-handle=1852 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xbf0000
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 Show Windows behavior

Analysis Process: RdrCEF.exe PID: 6492 Parent PID: 6140

General

Start time:	16:54:15
Start date:	06/07/2021
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=1720,11394891864812701617,5421238245506412973,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=5121740222193972291 --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=5121740222193972291 --renderer-client-id=5 --mojo-platform-channel-handle=2240 --allow-no-sandbox-job /prefetch:1

Imagebase:	0xbf0000
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 Show Windows behavior

Analysis Process: iexplore.exe PID: 2424 Parent PID: 3068

General

Start time:	16:55:29
Start date:	06/07/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' https://www.emory.edu/forward/
Imagebase:	0x7ff721e20000
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 Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 2908 Parent PID: 2424

General

Start time:	16:55:29
Start date:	06/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2424 CREDAT:17410 /prefetch:2
Imagebase:	0x20000
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 Show Windows behavior

Registry Activities Show Windows behavior

Disassembly

Code Analysis