ID: 384874
Cookbook: browseurl.jbs
Time: 00:12:49
Date: 10/04/2021
Version: 31.0.0 Emerald

Table of Contents

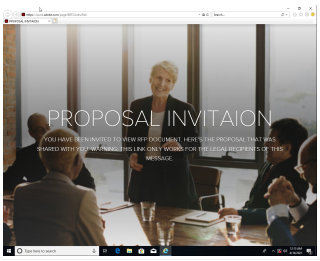
Analysis Report https://spark.adobe.com/page/BBFX2xd…

Overview

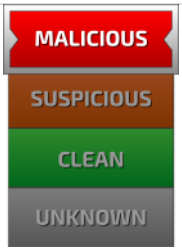
General Information

Sample URL:	http://https://spark.adobe.com/page/BBFX2xdrulRdi/
Analysis ID:	384874
Infos:	

Most interesting Screenshot:



Detection



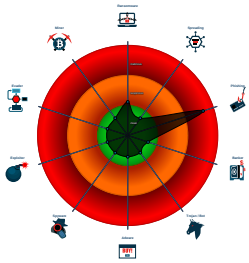
HTMLPhisher

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Phishing site detected (based on sh…
- Yara detected HtmlPhish10
- Yara detected HtmlPhish7
- HTML body contains low number of …
- HTML title does not match URL

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5808 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4084 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5808 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

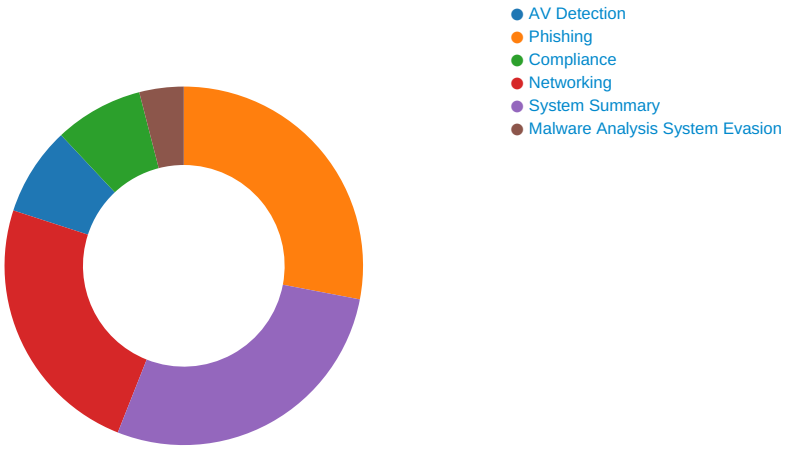
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\011[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\011[1].htm	JoeSecurity_HtmlPhish_7	Yara detected HtmlPhish_7	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:

Phishing site detected (based on shot template match)

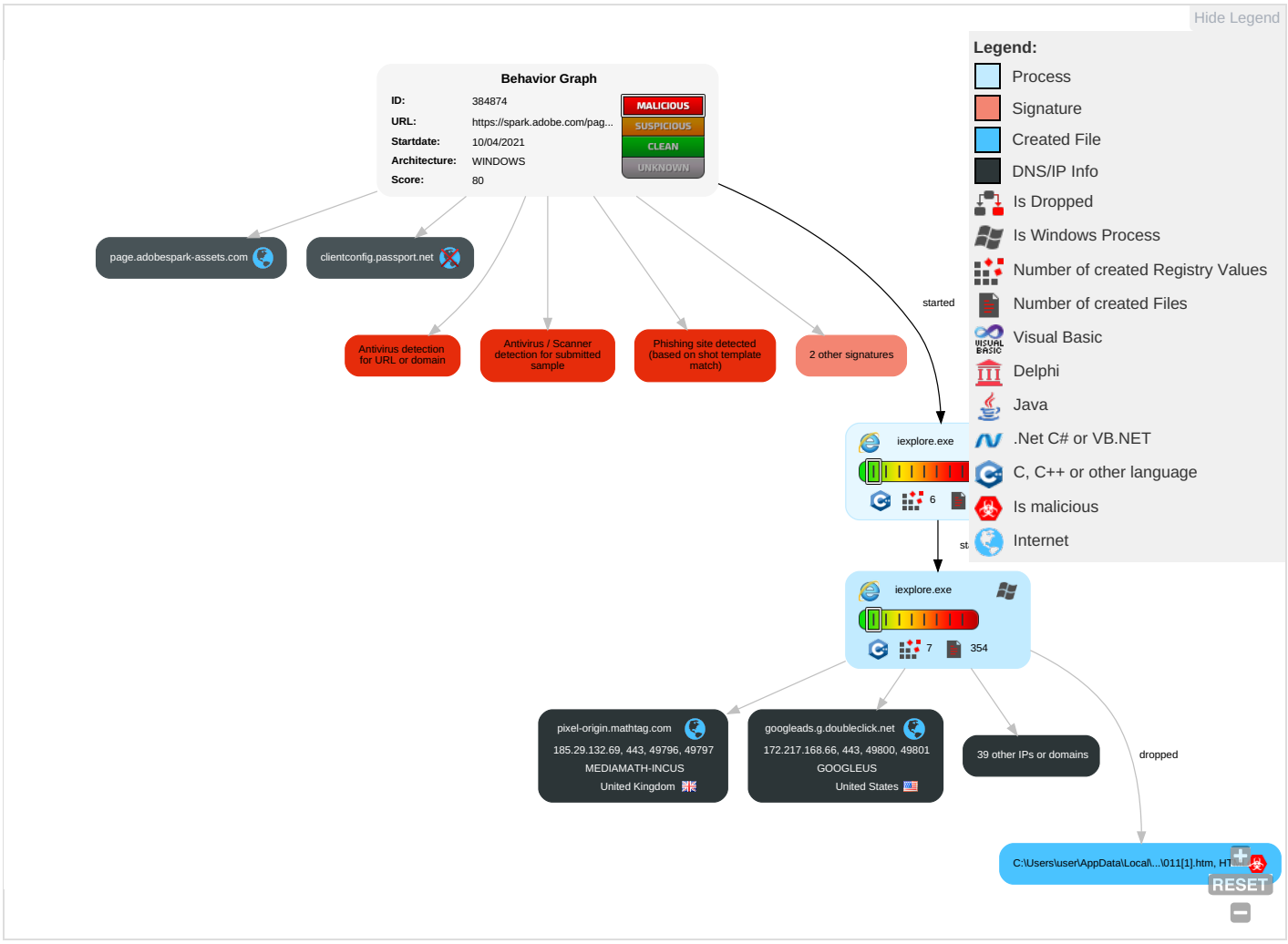
Yara detected HtmlPhish10

Yara detected HtmlPhish7

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	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	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	Modif Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carri Billin Fraud

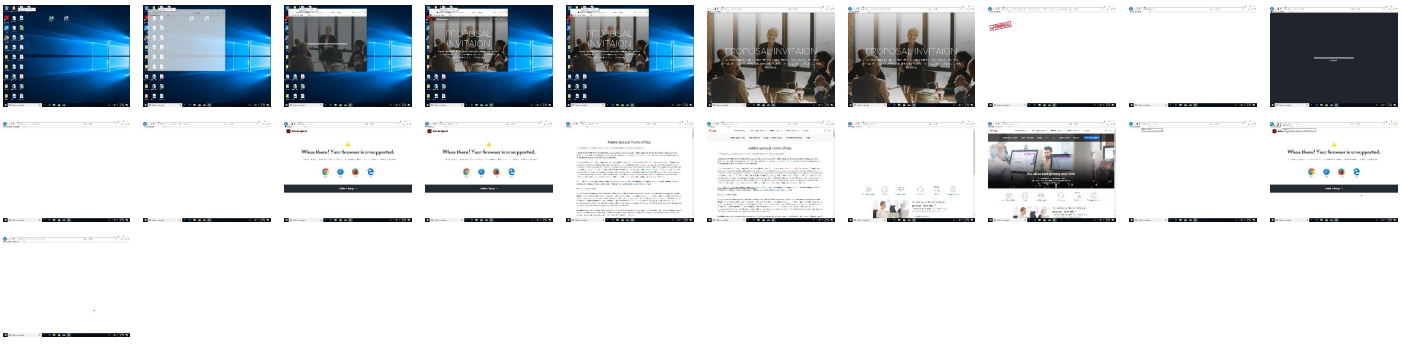
Behavior Graph

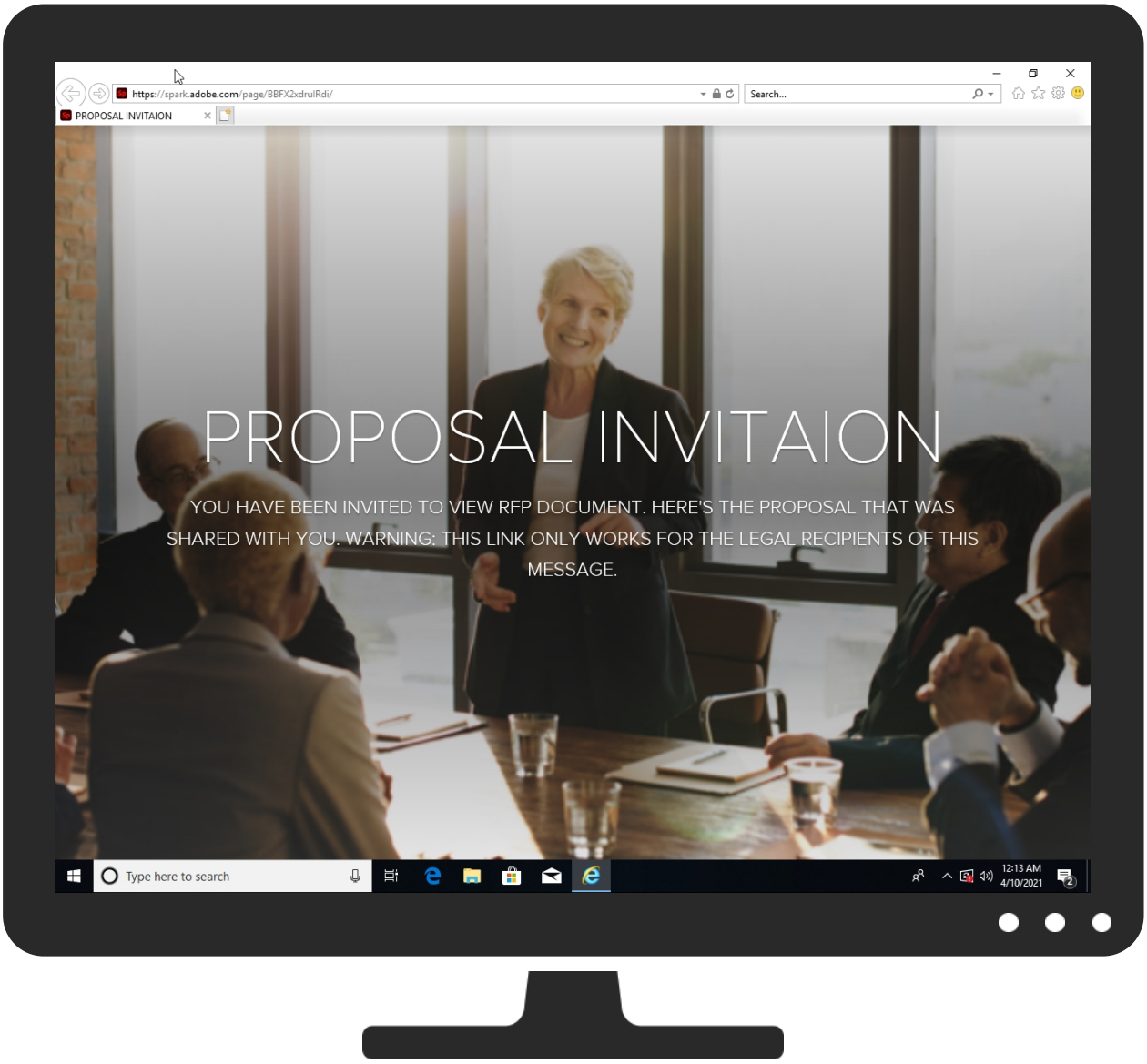


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://spark.adobe.com/page/BBFX2xdrulRdi/	1%	Virustotal		Browse
http://https://spark.adobe.com/page/BBFX2xdrulRdi/	0%	Avira URL Cloud	safe	
http://https://spark.adobe.com/page/BBFX2xdrulRdi/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
adobelogin-origin.prod.ims.adobejanus.com	0%	Virustotal		Browse
services.prod.ims.adobejanus.com	0%	Virustotal		Browse
spark.adobeprojectm.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://nicklaussglen.buzz/011/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://spark.adobe.com/page/BBFX2xdruIRdi/?page-mode=static	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://page.adobespark-assets.com/runtime/1.22/themes/crisp-fonts.gz.js	0%	Avira URL Cloud	safe	
http://https://spark.ado	0%	Avira URL Cloud	safe	
http://https://page.adobespark-assets.com/runtime/1.22/typekit-load.gz.js	0%	Avira URL Cloud	safe	
http://https://page.adobespark-assets.com/runtime/1.22/base-fonts.gz.js	0%	Avira URL Cloud	safe	
http://https://blog.adobespark.com/	0%	Avira URL Cloud	safe	
http://https://openjsf.org/	0%	URL Reputation	safe	
http://https://openjsf.org/	0%	URL Reputation	safe	
http://https://openjsf.org/	0%	URL Reputation	safe	
http://https://ade0164.d41.co/sync/	0%	Avira URL Cloud	safe	
http://https://www.pinterest.	0%	Avira URL Cloud	safe	
http://ianlunn.github.io/Hover/)	0%	Avira URL Cloud	safe	
http://https://static.adobelogin.com/imslib/imslib.min.js	0%	Avira URL Cloud	safe	
http://https://www.facebook.	0%	Avira URL Cloud	safe	
http://ianlunn.co.uk/	0%	URL Reputation	safe	
http://ianlunn.co.uk/	0%	URL Reputation	safe	
http://ianlunn.co.uk/	0%	URL Reputation	safe	
http://https://page.adobespark-assets.com/runtime/1.22/runtime.gz.css	0%	Avira URL Cloud	safe	
http://https://nicklaussglen.buzz/011/X2xdruIRdi/images/83634061-e5cf-4347-adb9-fcd6e83fb247.jpg?asset_id=b	0%	Avira URL Cloud	safe	
http://https://page.adobespark-assets.com/runtime/1.22/images/favicon.ico	0%	Avira URL Cloud	safe	
http://www.iport.it)	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dd20fzx9mj46f.cloudfront.net	13.32.16.66	true	false		high
pixel-origin.mathtag.com	185.29.132.69	true	false		high
adobelogin-origin.prod.ims.adobejanus.com	54.73.76.208	true	false	• 0%, Virustotal, Browse	unknown
services.prod.ims.adobejanus.com	52.16.185.223	true	false	• 0%, Virustotal, Browse	unknown
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high
dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com	52.30.135.179	true	false		high
spark.adobeprojectm.com	99.86.3.88	true	false	• 0%, Virustotal, Browse	unknown
idsync.rlcdn.com	35.244.174.68	true	false		high
s3.amazonaws.com	52.216.239.117	true	false		high
googleads.g.doubleclick.net	172.217.168.66	true	false		high
nicklaussglen.buzz	172.67.169.45	true	false		unknown
cdnjs.cloudflare.com	104.16.19.94	true	false		high
adobe.com.ssl.d1.sc.omtrdc.net	35.181.18.61	true	false		unknown
api.demandbase.com	99.86.3.69	true	false		high
aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com	3.127.52.31	true	false		high
demdex.net.ssl.sc.omtrdc.net	15.237.136.106	true	false		unknown
adobe.tt.omtrdc.net	52.212.164.82	true	false		unknown
www.google.ch	216.58.215.227	true	false		high
page.adobespark-assets.com	13.32.25.66	true	false		unknown
cdn.cookielaw.org	104.16.148.64	true	false		high
geolocation.onetrust.com	104.20.184.68	true	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
ims-na1.adobelogin.com	unknown	unknown	false		high
ds-aksb-a.akamaihd.net	unknown	unknown	false		high
cm.everesttech.net	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
adobedc.demdex.net	unknown	unknown	false		high
dpm.demdex.net	unknown	unknown	false		high
aa.agkn.com	unknown	unknown	false		high
static.adobelogin.com	unknown	unknown	false		high
adobe.demdex.net	unknown	unknown	false		high
use.typekit.net	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high
assets.adobedtm.com	unknown	unknown	false		high
p.typekit.net	unknown	unknown	false		high
clientconfig.passport.net	unknown	unknown	false		unknown
sync.mathtag.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://nicklaussglen.buzz/011/	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

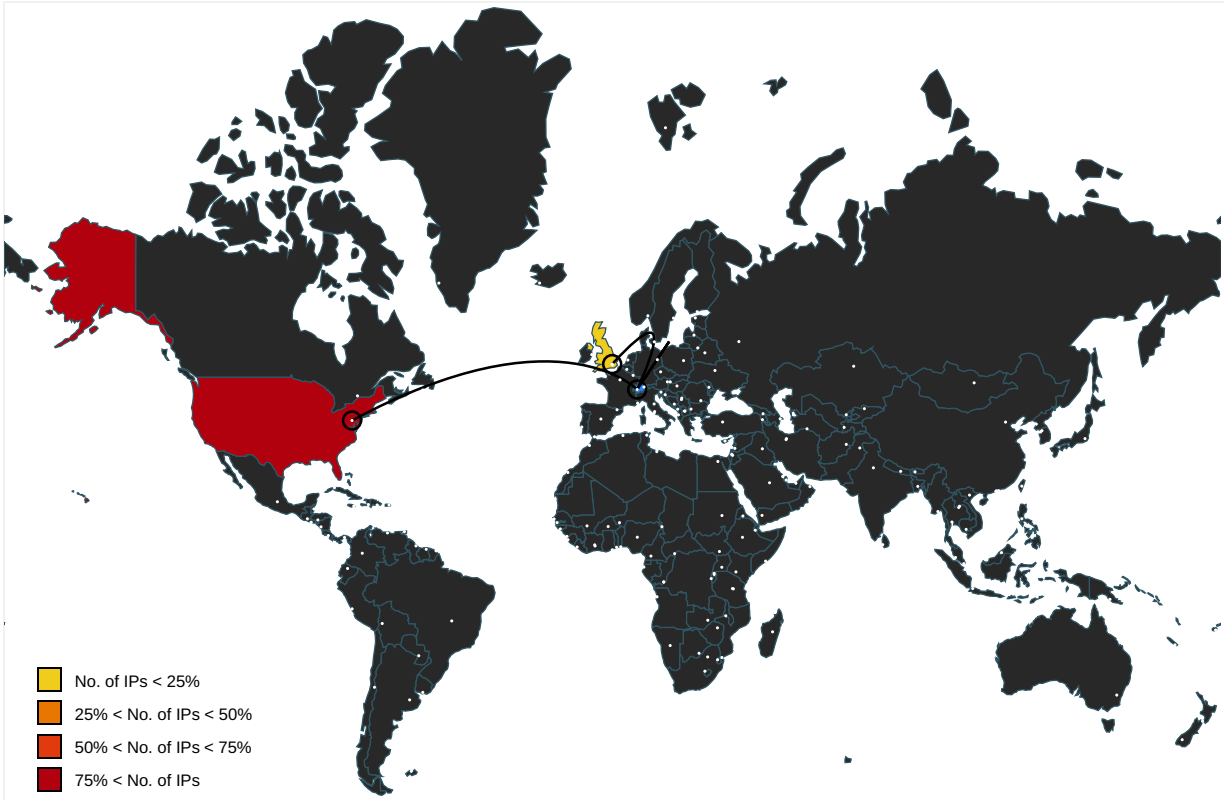
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://typekit.com/eulas/00000000000000003b9aee45	pps7abe[1].css0.3.dr	false		high
http://https://adobespark.zendesk.com/hc/en-us/categories/202688167-Adobe-Spark	login[1].htm2.3.dr, unsupported[1].htm.3.dr	false		high
http://https://www.linkedin.com	scripts[1].js1.3.dr	false		high
http://typekit.com/eulas/00000000000000003b9aee47	pps7abe[1].css0.3.dr	false		high
http://typekit.com/eulas/000000000000000000000ffd9	rbi5aua[1].js0.3.dr	false		high
http://https://use.typekit.net/vtg4qoo.js	unsupported[1].htm.3.dr	false		high
http://https://page.adobespark-assets.com/runtime/1.22/themes/crisp-fonts.gz.js	BBFX2xdruIRdi[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.instagram.com/adobe/	www.adobe.com[2].htm.3.dr	false		high
http://https://code.jquery.com/jquery-3.2.1.slim.min.js	011[1].htm.3.dr	false		high
http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/bffb9ea23c0c/RC7e9f4c1a441d45af93bf75d76d872cf	RC7e9f4c1a441d45af93bf75d76d872cf0-file.min[1].js.3.dr	false		high
http://https://use.typekit.net/af/97fbd1/00000000000000003b9b3f88/27/d?primer=388f68b35a7cbf1ee3543172445c2	pps7abe[1].css0.3.dr	false		high
http://https://use.typekit.net/af/97fbd1/00000000000000003b9b3f88/27/	onz5gap[1].js1.3.dr	false		high
http://https://spark.ado	{40F7FB7C-99CC-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://use.typekit.net/af/ad2a79/00000000000000003b9b3f8c/27/a?primer=388f68b35a7cbf1ee3543172445c2	pps7abe[1].css0.3.dr	false		high
http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/bffb9ea23c0c/RC1bc70f0c17a44296971da4381a721bd	RC1bc70f0c17a44296971da4381a721bda-file.min[1].js.3.dr	false		high
http://https://page.adobespark-assets.com/runtime/1.22/typekit-load.gz.js	BBFX2xdruIRdi[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://use.typekit.net/af/97fbd1/00000000000000003b9b3f88/27/a?primer=388f68b35a7cbf1ee3543172445c2	pps7abe[1].css0.3.dr	false		high
http://https://page.adobespark-assets.com/runtime/1.22/base-fonts.gz.js	BBFX2xdruIRdi[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://use.typekit.net/af/a0c22f/00000000000000003b9b3f84/27/a?primer=388f68b35a7cbf1ee3543172445c2	pps7abe[1].css0.3.dr	false		high
http://https://assets.adobedtm.com	login[1].htm2.3.dr	false		high
http://https://www.youtube.com	scripts[1].js1.3.dr	false		high
http://https://use.typekit.net/af/aa41d0/00000000000000003b9b3f86/27/d?primer=388f68b35a7cbf1ee3543172445c2	pps7abe[1].css0.3.dr	false		high
http://https://fontawesome.com	free.min[1].css.3.dr	false		high
http://https://static.adobelogin.com/imslib/imslib.min.js	privacy[1].htm0.3.dr	false		high
http://https://use.typekit.net/af/a0c22f/00000000000000003b9b3f84/27/d?primer=388f68b35a7cbf1ee3543172445c2	pps7abe[1].css0.3.dr	false		high
http://https://github.com/janl/mustache.js/issues/186	chrome[1].js.3.dr	false		high
http://typekit.com/eulas/000000000000000000001705b	rbi5aua[1].js0.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://use.typekit.net/af/aa41d0/00000000000000003b9b3f86/27/a?primer=388f68b35a7cbf1ee3543172445c2	pps7abe[1].css0.3.dr	false		high
http://https://www.instagram.com	scripts[1].js1.3.dr	false		high
http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/bffb9ea23c0c/RC419dbb68baed4e699648e06bb8cb651	RC419dbb68baed4e699648e06bb8cb6515-file.min[1].js.3.dr	false		high
http://https://github.com/twbs/bootstrap/graphs/contributors)	bootstrap.min[1].js.3.dr	false		high
http://https://github.com/janl/mustache.js/issues/189	chrome[1].js.3.dr	false		high
http://https://twitter.com	scripts[1].js1.3.dr	false		high
http://https://use.typekit.net/af/c8f445/00000000000000003b9aee47/27/d?primer=388f68b35a7cbf1ee3543172445c2	pps7abe[1].css0.3.dr	false		high
http://https://connect.facebook.net/en_US/fbevents.js	RC1bc70f0c17a44296971da4381a721bda-file.min[1].js.3.dr	false		high
http://https://use.typekit.net/af/8f4e31/0000000000000000000132e3/27/	vtg4qoo[1].js0.3.dr	false		high
http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/bffb9ea23c0c/RC508044d39da1421eb31de2476af8ac1	RC508044d39da1421eb31de2476af8ac1e-source.min[1].js.3.dr	false		high
http://https://blog.adobespark.com/	scripts[1].js1.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://use.typekit.net/af/e09494/00000000000000003b9aee45/27/l?primer=388f68b35a7cbf1ee3543172445c2	pps7abe[1].css0.3.dr	false		high
http://opensource.org/licenses/MIT).	popper.min[1].js.3.dr	false		high
http://https://kit.fontawesome.com/585b051251.js	011[1].htm.3.dr	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js	011[1].htm.3.dr	false		high
http://https://use.typekit.net/af/b0c5f5/00000000000000003b9b3f85/27/d?primer=388f68b35a7cbf1ee3543172445c2	pps7abe[1].css0.3.dr	false		high
http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/bffb9ea23c0c/RCbbd93c1920fd422b84787f67ddbfbe5	RCbbd93c1920fd422b84787f67ddbfbe55-file.min[1].js.3.dr	false		high
http://https://openjsf.org/	marvelcommon-bb979c0a[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://adobe.demdex.net/dest5.html?d_nsid=0	{40F7FB7C-99CC-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://use.typekit.net/af/ad2a79/00000000000000003b9b3f8c/27/d?primer=388f68b35a7cbf1ee3543172445c2	pps7abe[1].css0.3.dr	false		high
http://https://use.typekit.net/af/3d913c/000000000000000000017709/26/	rbi5aua[1].js0.3.dr	false		high
http://https://ade0164.d41.co/sync/	RC1a83c357d323419db9d2ba211efeeaae-file.min[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://adobespark.uservoice.com	unsupported[1].htm.3.dr	false		high
http://https://www.pinterest.	scripts[1].js1.3.dr	false	• Avira URL Cloud: safe	unknown
http://ianlunn.github.io/Hover/)	hover[1].css.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://static.adobelogin.com/imslib/imslib.min.js	login[1].htm2.3.dr	false	• Avira URL Cloud: safe	low
http://https://use.typekit.net/af/c8f445/00000000000000003b9aee47/27/a?primer=388f68b35a7cbf1ee3543172445c2	pps7abe[1].css0.3.dr	false		high
http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/bffb9ea23c0c/RC6f46e43fa6d44dbeb45cc5801ffded0	RC6f46e43fa6d44dbeb45cc5801ffded0e-file.min[1].js.3.dr	false		high
http://https://www.facebook.	scripts[1].js1.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://use.typekit.net/af/e09494/00000000000000003b9aee45/27/a?primer=388f68b35a7cbf1ee3543172445c2	pps7abe[1].css0.3.dr	false		high
http://https://use.typekit.net/af/edcf1e/0000000000000000000158d9/26/	rbi5aua[1].js0.3.dr	false		high
http://https://www.workfront.com/	www.adobe.com[2].htm.3.dr	false		high
http://https://use.typekit.net/af/37eaae/00000000000000003b9b3f83/27/d?primer=388f68b35a7cbf1ee3543172445c2	pps7abe[1].css0.3.dr	false		high
http://https://github.com/focus-trap/focus-trap/blob/master/LICENSE	head.fp-1c6b8ee3dfac8039d9ead67e8b6d6138[1].js.3.dr	false		high
http://https://use.typekit.net/af/d8f71f/0000000000000000000132e1/27/	vtg4qoo[1].js0.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://servedby.flashtalking.com/container/13539;99030;10307;iframe/?ftXRef=&ftXValue=&ftXType=&ftX	{40F7FB7C-99CC-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://github.com/kriskowal/q/blob/v1/LICENSE	marvelcommon-bb979c0a[1].js.3.dr	false		high
http://underscorejs.org/LICENSE	marvelcommon-bb979c0a[1].js.3.dr	false		high
http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/bffb9ea23c0c/RCe26b98274fee43abbdb260d3b3d8fef	RCe26b98274fee43abbdb260d3b3d8fefc-file.min[1].js.3.dr	false		high
http://ianlunn.co.uk/	hover[1].css.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://adobespark.zendesk.com/hc/en-us/articles/219243657	en-US_bundle-1b00eb00[1].js.3.dr	false		high
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.min[1].css.3.dr, bootstrap.min[1].js.3.dr	false		high
http://https://github.com/IanLunn/Hover	hover[1].css.3.dr	false		high
http://https://page.adobespark-assets.com/runtime/1.22/runtime.gz.css	BBFX2xdruIRdi[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://use.typekit.net/vtg4qoo.css	login[1].htm2.3.dr	false		high
http://https://adobesparkpost.app.link/nfQW2NoCVeb	express[1].htm.3.dr	false		high
http://https://use.typekit.net/af/9951d2/00000000000000000000158d7/26/	rbi5aua[1].js0.3.dr	false		high
http://https://cdn.cookielaw.org/scripttemplates/otSDKStub.js	www.adobe.com[2].htm.3.dr	false		high
http://https://adobespark.zendesk.com/hc/en-us/articles/218956027	en-US_bundle-1b00eb00[1].js.3.dr	false		high
http://https://npms.io/search?q=ponyfill.	marvelcommon-bb979c0a[1].js.3.dr	false		high
http://https://use.typekit.net/af/b0c5f5/00000000000000003b9b3f85/27/l?primer=7cdcb44be4a7db8877ffa5c0007b8	scripts[1].js1.3.dr	false		high
http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/bffb9ea23c0c/RC89c6d3bd15f043db95a5a0a4b5cc9da	RC89c6d3bd15f043db95a5a0a4b5cc9da0-file.min[1].js.3.dr	false		high
http://https://adobespark.zendesk.com/hc/en-us/requests/new	unsupported[1].htm.3.dr	false		high
http://https://ka-f.fontawesome.com	585b051251[1].js.3.dr	false		high
http://https://use.typekit.net/af/9d1933/00000000000000000001705b/26/	rbi5aua[1].js0.3.dr	false		high
http://https://www.linkedin.com/company/adobe	www.adobe.com[2].htm.3.dr	false		high
http://typekit.com/eulas/00000000000000000000132e1	vtg4qoo[1].js0.3.dr	false		high
http://https://cdn.cookielaw.org	login[1].htm2.3.dr	false		high
http://https://use.typekit.net/af/b0c5f5/00000000000000003b9b3f85/27/l?primer=388f68b35a7cbf1ee3543172445c2	pps7abe[1].css0.3.dr	false		high
http://https://twitter.com/Adobe	www.adobe.com[2].htm.3.dr	false		high
http://https://nicklaussglen.buzz/011/X2xdruIRdi/images/83634061-e5cf-4347-adb9-fcd6e83fb247.jpg?asset_id=b	~DFA6731248B7E9CF32.TMP.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://www.instagram.com/AdobeSpark	unsupported[1].htm.3.dr	false		high
http://https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location	7a5eb705-95ed-4cc4-a11d-0cc5760e93db[1].js.3.dr	false		high
http://https://opsparc.gsfc.nasa.gov/?sdid=MC95SNMJ&mv=social	en-US_bundle-1b00eb00[1].js.3.dr	false		high
http://https://use.typekit.net/af/97fbd1/00000000000000003b9b3f88/27/l?primer=7cdcb44be4a7db8877ffa5c0007b8	scripts[1].js1.3.dr	false		high
http://https://fontawesome.com/license/free	free.min[1].css.3.dr	false		high
http://https://use.typekit.net/af/cb695f/00000000000000000000017701/27/	vtg4qoo[1].js0.3.dr	false		high
http://https://page.adobespark-assets.com/runtime/1.22/images/favicon.ico	BBFX2xdruIRdi[1].htm.3.dr, imagestore.dat.3.dr, ~DFA6731248B7E9CF32.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://typekit.com/eulas/000000000000000000017706	vtg4qoo[1].js0.3.dr	false		high
http://www.iport.it)	chrome[1].js.3.dr	false	• Avira URL Cloud: safe	low
http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/bffb9ea23c0c/RC32e8eb91f06d47d18918e9b9bcc17a0	RC32e8eb91f06d47d18918e9b9bcc17a00-file.min[1].js.3.dr	false		high
http://www.opensource.org/licenses/mit-license.html	marvelcommon-bb979c0a[1].js.3.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.10.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
3.127.52.31	aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
99.86.3.88	spark.adobeprojectm.com	United States		16509	AMAZON-02US	false
104.16.148.64	cdn.cookielaw.org	United States		13335	CLOUDFLARENETUS	false
104.20.184.68	geolocation.onetrust.com	United States		13335	CLOUDFLARENETUS	false
172.217.168.66	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
13.32.25.66	page.adobespark-assets.com	United States		7018	ATT-INTERNET4US	false
52.16.185.223	services.prod.ims.adobejanus.com	United States		16509	AMAZON-02US	false
52.216.239.117	s3.amazonaws.com	United States		16509	AMAZON-02US	false
172.67.169.45	nicklaussglen.buzz	United States		13335	CLOUDFLARENETUS	false
52.212.164.82	adobe.tt.omtrdc.net	United States		16509	AMAZON-02US	false
216.58.215.227	www.google.ch	United States		15169	GOOGLEUS	false
15.237.136.106	demdex.net.ssl.sc.omtrdc.net	United States		16509	AMAZON-02US	false
52.30.135.179	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
54.73.76.208	adobelogin-origin.prod.ims.adobejanus.com	United States		16509	AMAZON-02US	false
34.251.60.147	unknown	United States		16509	AMAZON-02US	false
99.86.3.69	api.demandbase.com	United States		16509	AMAZON-02US	false
35.181.18.61	adobe.com.ssl.d1.sc.omtrdc.net	United States		16509	AMAZON-02US	false
185.29.132.69	pixel-origin.mathtag.com	United Kingdom		30419	MEDIAMATH-INCUS	false
13.32.16.66	dd20fzx9mj46f.cloudfront.net	United States		7018	ATT-INTERNET4US	false
35.244.174.68	idsync.rlcdn.com	United States		15169	GOOGLEUS	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	384874
Start date:	10.04.2021
Start time:	00:12:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://spark.adobe.com/page/BBFX2xdrulRdi/
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:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.phis.win@3/280@30/22
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://spark.adobe.com/page/BBFX2xdrulRdi/?page-mode=static • Browsing link: https://spark.adobe.com/page/BBFX2xdrulRdi/images/83634061-e5cf-4347-adb9-fcd6e83fb247.jpg?asset_id=bebefb3b-e328-4e90-9b79-8ef151037f52&img_etag=%224139c04c0058 13ba7bb7e7f7c0ec64f2%22&size=1024 • Browsing link: http://nicklaussglen.buzz/011 • Browsing link: https://spark.adobe.com/page/BBFX2xdrulRdi • Browsing link: https://spark.adobe.com/about?r=reader_page_logo • Browsing link: https://spark.adobe.com/make/logo-maker?r=reader_page_learnmore • Browsing link: https://spark.adobe.com/login?r=reader_page_bumper_createyourown • Browsing link: http://www.adobe.com/legal/terms.html • Browsing link: http://www.adobe.com/go/privacy • Browsing link: https://spark.adobe.com/login?r=reader_page_topbar_createyourown • Browsing link: https://spark.adobe.com/templates/resumes/

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 13.64.90.137, 168.61.161.212, 104.83.120.32, 23.10.249.9, 23.10.249.43, 104.83.104.145, 69.16.175.42, 69.16.175.10, 172.217.168.10, 104.18.22.52, 104.18.23.52, 172.64.202.28, 172.64.203.28, 104.83.121.10, 23.0.174.235, 23.10.249.179, 152.199.19.161, 23.54.112.23, 20.82.210.154, 23.54.113.104, 23.54.113.182, 34.250.153.194, 34.253.145.149, 54.171.42.33, 34.255.166.243, 54.194.191.134, 99.81.11.244, 23.10.249.48, 23.10.249.24, 99.86.3.4, 99.86.3.86, 99.86.3.79, 99.86.3.76, 172.217.168.4, 23.0.174.248, 8.238.36.254, 8.238.35.126, 8.241.126.249, 8.238.27.126, 8.238.29.254, 23.10.249.26, 20.54.26.129, 20.50.102.62 • Excluded domains from analysis (whitelisted): e6653.dscf.akamaiedge.net, cds.s5x3j6q5.hwcdn.net, arc.msn.com.nsatc.net, ka-f.fontawesome.com.cdn.cloudflare.net, cn-assets.adobedtm.com.edgekey.net, spark.adobe.com, fs-wildcard.microsoft.com.edgekey.net, ds-aksb-a.akamaihd.net.edgesuite.net, e11290.dspg.akamaiedge.net, e13551.dscg.akamaiedge.net, use-stls.adobe.com.edgesuite.net, ssl-delivery.adobe.com.edgekey.net, audownload.windowsupdate.nsatc.net, www.google.com, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, fonts.googleapis.com, fs.microsoft.com, stls.adobe.com-cn.edgesuite.net.globalredir.akadns.net, ajax.googleapis.com, cm.everesttech.net.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ris.api.iris.microsoft.com, a1910.dscq.akamai.net, blobcollector.events.data.trafficmanager.net, a1815.dscr.akamai.net, geo2.adobe.com, cs9.wpc.v0cdn.net, a1049.g2.akamai.net, e4578.dscg.akamaiedge.net, geo.adobe.com.edgesuite.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, iecvlist.microsoft.com, msagfx.live.com-6.edgekey.net, authgfx.msa.akadns6.net, go.microsoft.com, arc.trafficmanager.net, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, client.messaging.adobe.com, kit.fontawesome.com.cdn.cloudflare.net, sstats.adobe.com, skypedataprdcolwus17.cloudapp.net, p.typekit.net-v3.edgekey.net, geo.adobe.com, ie9comview.vo.msecnd.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, stls.adobe.com-cn.edgesuite.net, adobeid-na1.services.adobe.com, skypedataprdcoleus17.cloudapp.net, e7808.dscg.akamaiedge.net, go.microsoft.com.edgekey.net, a1988.dscg1.akamai.net, www.adobe.com • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\HN9HTZMO\www.adobe[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1085
Entropy (8bit):	4.849211398599324
Encrypted:	false
SSDEEP:	24:W0U1mKm6D+QGwU1mKm6D+QG76KQGxKQGwU1mKm6D+QG76KQGwU1mKm6D+QG76KQv:0sK+QGsK+QeQlQGsK+QeQGsK+QeQhQGL
MD5:	E6CAFAF4215882CD10CC24FA2DBE60E8
SHA1:	176C80AD9F7582C41E38073507E66CA46DA286B4
SHA-256:	15368FA41FA4F711E76A89533BD50F94D2C1C31CECC722DDCDB47874A38A2B3F
SHA-512:	F303DCD29A792854E39DBFD945D56313FEC3B10AE1B0892747DC4EEC3810E2C5ED99504CACBD12F32BD39CE1E22C5A4C6D62668F8B7BCAC2E1FB4C4696689E2
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root><item name="com.adobe.reactor.dataElementCookiesMigrated" value="true" ltime="407707872" htime="30879193" /></root><root><item name="com.adobe.reactor.dataElementCookiesMigrated" value="true" ltime="407707872" htime="30879193" /><item name="mar_aud" value="Bot" ltime="412657872" htime="30879193" /><item name="isStoragePolyfillNeeded" value="true" ltime="412657872" htime="30879193" /></root><root><item name="com.adobe.reactor.dataElementCookiesMigrated" value="true" ltime="407707872" htime="30879193" /><item name="mar_aud" value="Bot" ltime="412657872" htime="30879193" /></root><root><item name="com.adobe.reactor.dataElementCookiesMigrated" value="true" ltime="407707872" htime="30879193" /><item name="mar_aud" value="Bot" ltime="412657872" htime="30879193" /><item name="isStoragePolyfillNeeded" value="true" ltime="457067872" htime="30879193" /></root><root><item name="com.adobe.reactor.dataElementCookiesMigrated" value="true" ltime="407707872" htime="3087

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\L6XOX4GB\spark.adobe[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	134
Entropy (8bit):	4.690910364169711
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsnObemKmlULF0VqHlJR31RXuSXcqSQcFg8LKb:JFK1rUFjgemKm6GVqHlJR3LdlQGlub
MD5:	E7BD81EA782665E5333B8F19293EDC04
SHA1:	70AF32B6699DFA873925FA4091A59C7619B020FE
SHA-256:	31E881DF06EB02688335C8BA0153756D5134C88BAC13E024E66EC8E934898875
SHA-512:	0FD8A91A291167161F771D655E65F3AF7AF48F3C920D3F6B086FF3522B07EA38680DFDF35BF037B6B4775B320D1C6B611588DC2C8CC1A309F1A09688D6EB1E1F

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\L6XOX4GB\spark.adobe[1].xml	
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="com.adobe.reactor.dataElementCookiesMigrated" value="true" ltime="374807872" htime="30879193" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{40F7FB7A-99CC-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8550529677797971
Encrypted:	false
SSDEEP:	96:reZhZ02iW2gt2Df2hBM2r2Zx2ZGf2Z5cX:reZhZ02iWLtEfsBMumPficX
MD5:	D69695CDEE5A2E70CFAA7C30162270AB
SHA1:	B04F78C6CDA866B9481E293A8201F94CD9804663
SHA-256:	F51EE953ED16EC3BB6155860E5CD2025BAC1C4F2F5CDDF3B6B477F442D13EFB0
SHA-512:	9907880F5ED2C51EA7F3BB4D6573E8E9C3B75AD74392D9D219556415E0BA9D7398F0D5E4352776DA666FD374F87805CF7B9977EFC6211D762EB8558A1EBC233
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{40F7FB7C-99CC-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	192666
Entropy (8bit):	2.6384470660843373
Encrypted:	false
SSDEEP:	384:rVhCSIEsgIEA9vL98TGrqWBqYFchZLD4aLgU9YCjnFZXi+2vKSvDzLR9/rT05DeR:lPa6FZXipkNU9N/NHhGXOGqh/TGCuhW
MD5:	35470A959DEDA2F93E63E6D5766019D2
SHA1:	C5A0DB5FFF6E51880A329D3E153440769BB5B773
SHA-256:	059844192B5F55DFB29B6B1FBD3C6DDF64CC0B54563D7F91C763CBAAA2880C0F
SHA-512:	300C81040D674A4C4921790A7C329602437CBA3AAE050924912B171866775CCD951EA5ECCD29275C4C580B410F85F32718A8C1FC5655CC1ECCA3B95F923574
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{40F7FB7D-99CC-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5642337978199197
Encrypted:	false
SSDEEP:	48:IwfEGcpr5vGwpaDG4pQHGrapbSSGQpKYG7HpRu9TGIpG:rQZPQ16bBS6AjTu7A
MD5:	7342A9B8529C0421D811E8BDF44B8C10
SHA1:	F81E062675C060A2E01F7AD80F80E865970C0091
SHA-256:	E28A801050E2005D5D7FABA4190442EDF82C2C53A56BAE2BCCC7067BD2BF498D
SHA-512:	28BFC78D83026C6D7762407F574226B6972E5B6003DDDFBE3CA16DE056247D81EF0211B012DA266F6E28BC77ECC7710664C8E100D74BC6E0D4D9349BF2F9C83
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
File Type:	data
Category:	dropped
Size (bytes):	28454
Entropy (8bit):	2.066575975051226
Encrypted:	false
SSDEEP:	48:R6fVgizzxxEKzOQBbcpS5WT//zVprc7gzdbklTMl1sy6TMenl7ulGt/3GmjAA2XY:MdR70sI2NmU3G8cj70sI2NmU3Gj
MD5:	F7D09673F1BA250AD8F70E0C79FF0268
SHA1:	1EA91062D6A97026E4F154CA96A88629AB03A9CB
SHA-256:	819CA2C295C80C05A8E4210B211E229C88A0C6D14921F3BC8022F8517B96D5FA
SHA-512:	77A453177493C3F7BB043D5D27DBD941BBD4988F03155D9354920B3694F04CF2554D4031D812AC08315EE565CC0AF7B22602AA1DD2A6ACA9D1B22925594557BI
Malicious:	false
Reputation:	low
Preview:	B.h.t.t.p.s.:././.p.a.g.e...a.d.o.b.e.s.p.a.r.k.-.a.s.s.e.t.s...c.o.m./.r.u.n.t.i.m.e./.1...2.2./.i.m.a.g.e.s./.f.a.v.i.c.o.n...i.c.o.......... ....(... ...@..... ....70..7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...70.............................7`.. 7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7`.....................70..7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7... 7...7...70.................7...7...7...7...7...7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Privacy-Header-2-1440x340.jpg.img[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 1440x430, frames 3
Category:	downloaded
Size (bytes):	87554
Entropy (8bit):	7.97194369897045
Encrypted:	false
SSDEEP:	1536:jTiiUlWRB717xEVxvzDwgBFxks8cVzjNeyjFLdAZBc2:jT6AB/41is8cNRbjtdI1
MD5:	36815147C5BD0A82CF08ADF18C4CE9DB
SHA1:	F5FE3F3312117D43AF628780AD94F7409F51BC51
SHA-256:	FA058BE1A59315346088172661F221BB988B929F4FE9CA7C2C98F49970D0109D
SHA-512:	2DD8E040B9046322F4259ABC673BB1CD980E440FE0D1EE5BFD6FD6FFC14D36F810BB0222E1413ECF65A49C335F894923C365F0E7E6C0BB6DC69A4A3DBF05E4 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/content/dam/cc1/en/privacy/images/Privacy-Header-2-1440x340.jpg.img.jpg
Preview:	......Exif..II*.................Ducky.......F......http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x: xmptk="Adobe XMP Core 5.6-c111 79.158325, 2015/09/10-01:10:20 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:a bout="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:8005f268-2f6e-41f7-b266-aa21258a942f" xmpMM:DocumentID="xmp.did:1DF2B77A0FFC11E6838996FD381AB7D0" xm pMM:InstanceID="xmp.iid:1DF2B7790FFC11E6838996FD381AB7D0" xmp:CreatorTool="Adobe Photoshop CC 2015 (Macintosh)"> <xmpMM:DerivedFrom stRef:in stanceID="xmp.iid:3a3c0c1d-b343-4643-ac1e-d229304d8b58" stRef:documentID="adobe:docid:photoshop:c44cf741-5865-1179-9b5f-a5ee13961278"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d............................

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RC1a83c357d323419db9d2ba211efeeaae-file.min[1].js</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>ASCII text, with very long lines</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>1156</td></tr>
<tr><td>Entropy (8bit):</td><td>5.077167337602734</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>24:15NBgA+E6K7eVgvf2I+LPPJ9ZLvaMLArqY4DPuDkpuH4R9pQFE7xJth:15NBLv7+iOI+zPJ9ZL11sYR8oh</td></tr>
<tr><td>MD5:</td><td>79159DEA08F96563DF7B1CB8F2F8F104</td></tr>
<tr><td>SHA1:</td><td>D31D9C0DE79958224134CCE71E048F5E8F0C222A</td></tr>
<tr><td>SHA-256:</td><td>5F9120B447D391D904149C7195C4C2C1674BAB7E6733B33B2AB87B06E671D478</td></tr>
<tr><td>SHA-512:</td><td>AF836BF47E2095850EBC23FDFF860F65855AC6A1C26C5A9DCC3FBA7B252D4438C40DC8511A55F6BCBD79838A903AE5A28B9917E284CFF8C66C5BE15D8CD51 E</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/bffb9ea23c0c/RC1a83c357d323419db9d2ba211efeeaae-file.min.js</td></tr>
<tr><td>Preview:</td><td>// For license information, see `https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/bffb9ea23c0c/RC1a83c357d323419db9d2ba211efeeaae-file.js`..var w =window,l=w.location,h=l.hostname,path=l.pathname,dataElementName="digitalData.organization.dnb";if("www.adobe-students.com"==h||"www.substance3d.com" ==h||"labs.adobe.com"==h||"magazine.substance3d.com"==h||-1<h.indexOf("photoshop.com")||"stockenterprise.adobe.com"==h||"pages.adobe.com"==h||"experience-makers-international.adobe.com"==h||"trainingpartners.adobe.com"==h||-1<h.indexOf(".adobeevents.com")||"colour.adobe.com"==h||"adobehiddentreasures.com"==h| |"www.adobeexperienceawards.com"==h||-1<h.indexOf("acrobat.adobe.com")||-1!==h.indexOf("esign.adobe.com")||-1!==path.indexOf("/experience-cloud")||-1!==path.ind exOf("/events/")||-1!==h.indexOf("magento.com")||-1!==h.indexOf("marketo.com")||"futureisyours.adobe.com"==h||"api.spark.adobe.com"==h){var dnbScript=document.c reateElement("script");dnbScript.src="https://ade0164.d41.co/sync/",dn</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RC32e8eb91f06d47d18918e9b9bcc17a00-file.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	C source, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1568
Entropy (8bit):	5.262348264708631
Encrypted:	false
SSDEEP:	48:15NLsregiQhdsitymtCZv4j+YuteKhXSXNjTjOofbOK5b/q:1/srPld3tymtCpLYuteMXSXNjTjhT5q
MD5:	8182CACB5F10E58B2D252677FD907A4F
SHA1:	4E3FE688B68F8A3B28898738C3D3D4B09D262B91
SHA-256:	30481DB0B83034D8424B68915ABDE1A724F530C6BAA05F6D02199099704A5257
SHA-512:	E76600F9E1F850F20CDB1035C128766DCCD2693C321232920C3CDD7E97CB9527410F32CD96F7C185074656A430AE453D7AE6A2247B84E00E83FE289273DCFC9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/bffb9ea23c0c/RC32e8eb91f06d47d18918e9b9bcc17a00-file.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/bffb9ea23c0c/RC32e8eb91f06d47d18918e9b9bcc17a00-file.js`..!function(){var e,t,n,o,u=window,s="adobePrivacy:Privacy",a="OptanonChoice",i=new Date,r={domain:_satellite._getDomain(),path:"/",samesite:"Lax",expires:(i.setFullYear(i.getFullYear()+1),i)};t=function(){o||(o=!0,n=function(){var e,t,n,o,s,a,i,r={},d=u.OneTrust.GetDomainData().Groups;for(o=0,s=d.length;o<s;o++)if((e=d[o])&&(t=e.Hosts))for(a=0,i=t.length;a<i;a++)(n=t[a])&&(r[n.HostName]={groupId:e.CustomGroupId,hostId:n.HostId,displayName:n.displayName});_satellite.oneTrustList=r,_satellite.oneTrustIsHostEnabled=function(e){var t,n=window.OnetrustActiveGroups;return!(!(t=r[e])||-1===n.indexOf(","+t.hostId+","))},_satellite.groupEnabled=function(e){var t=window.OnetrustActiveGroups;return!(!t||-1===t.indexOf(e))},_satellite.track("initTrackConsent")},_satellite._poll(n,[function(){return u.OneTrust}],{timeout:1e4,interval:100}))},e=function(e){u

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RC6f46e43fa6d44dbeb45cc5801ffded0e-file.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2503
Entropy (8bit):	5.2508518948515235
Encrypted:	false
SSDEEP:	48:15Nln9KNNFeHD7Bbg8m9wPjwPbeffSQLYno4BXo5iTJWN+BJ6Nu4CuMgG+/T1zcD:15neNFeHDNbg76s6nSjXSiTJWMBJ6kZ1
MD5:	359974051FA15221603FAF2AEE924048
SHA1:	17E39B929C0EED34908DBD47487CF48A51ECFC5D
SHA-256:	7C5A1697C34E8EFDB2A5551B8A74C347CC028D2653B429991CFC08637DC50A0E
SHA-512:	2973F5C83A247684F1D26B1DF86A894D61674BDA8DB2780690A28E7FAA59707F8FD2AA1EB3AE59E77CFA9A39A8C60F7A1D686F769CD898C150ADFC90BEB5F0C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/bffb9ea23c0c/RC6f46e43fa6d44dbeb45cc5801ffded0e-file.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/bffb9ea23c0c/RC6f46e43fa6d44dbeb45cc5801ffded0e-file.js`..function searchAsYouType(){function g(e){for(var t=1,a=document.body.previousElementSibling?"previousElementSibling":"previousSibling";e==e[a];)++t;return t}function c(e,t,a){for(var n=a.toLowerCase(),r=0;e&&e.parentNode;){if(e=e.parentNode,r++,"tagName"===t&&e.tagName.toLowerCase()==n)return e;if("id"===t){if(e.id.toLowerCase()==n)return e}else if("className"===t){if(5<=r)return null;if(e.className.toLowerCase()==n)return e}}return null}document.getElementsByClassName("Gnav-menu-content").length&&document.getElementsByClassName("Gnav-menu-content")[0].addEventListener("click",function(e){var t;if(e.target&&("A"==e.target.nodeName||"SPAN"==e.target.nodeName||"IMG"==e.target.nodeName)){var a=e.target.className.split(" ");if(a)for(var n=0;n<a.length;n++){if(-1!==a[n].indexOf("SAYT-")&&-1===a[n].indexOf("SAYT-advancedSearch"))if(c(e.target,"id",""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RCe26b98274fee43abbdb260d3b3d8fefc-file.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	323
Entropy (8bit):	5.2371576843169505
Encrypted:	false
SSDEEP:	6:jwkMKngJv0KgiSP8AlPCtYta+ApXMYGGX6SHMWkiezW3T5OtunadXZfJ/uEK1Wd:jvgeASPRNCtca+AcYGkcOeqD5OFdXv/X
MD5:	73970CA0088737E30B6EEA7746556312
SHA1:	C82F6902CF002BD9624A388DBAC8FDAEEA53874C
SHA-256:	8F2B5B6E19D7B6105BEEE0967560631DB60F89961E99D3D9AC43942E65EF6AE9
SHA-512:	452F06711EA63E0A851E42EC8EDFE37406F3FB2CBDACCDF3BB9DE46BE38CA3F0E3053E56D69947A6EAFE78C99B0D27EE9E285A946EC116D7AEB46D18FC2A735C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/bffb9ea23c0c/RCe26b98274fee43abbdb260d3b3d8fefc-file.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/bffb9ea23c0c/RCe26b98274fee43abbdb260d3b3d8fefc-file.js`.._satellite._poll(function(){_satellite.track("trackMarketoForm")},[function(){if(document.querySelector(".marketoForm")||window.MktoForms2)return!0}],{timeout:1e5,interval:100});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\SPRK_color_hover_v3@2x[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1004
Entropy (8bit):	5.187217692853858
Encrypted:	false
SSDEEP:	12:tvG1XftzSHn4vj0SeX47LiiLAiUw/U+VH3NLzaDobULhqq9BS9C6gEKYoaWZKq2e:tu1XftHvxeIAvFiXtTbUJkUEhCP
MD5:	E9D94F821371E183B8B58F618B2FC161
SHA1:	792948E6A17CF091CCDC329A09EE22BF1A1A9CF5
SHA-256:	AC03A140536DC39782AFA5C742E10515D20C24DB3152DCB04471252C856B7FF4
SHA-512:	A9EC755233EAB39EE91630F379412BB469BADE01784095A13F7FC3E62C860E0BD0618A43554D909049B4716C0CF0F6A582E69DF3962384ACEDDBEF911013EEE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spark.adobe.com/images/SPRK_color_hover_v3@2x.svg
Preview:	<svg id="Layer_1" data-name="Layer 1" xmlns="http://www.w3.org/2000/svg" viewBox="0 0 56 54" width="56" height="54"><defs><style>.cls-1{fill:#370000;}.cls-2{fill:#fa0f00;}</style></defs><g id="Layer_2" data-name="Layer 2"><g id="Surfaces"><g id="Spark_Surface" data-name="Spark Surface"><path id="Outline_no_shadow" data-name="Outline no shadow" class="cls-1" d="M9.9,0H46.1A9.8588,9.8588,0,0,1,56,9.9V44.1A9.8588,9.8588,0,0,1,46.1,54H9.9A9.8588,9.8588,0,0,1,0,44.1V9.9A9.8588,9.8588,0,0,1,9.9,0Z"/></g></g><g id="Outlined_Mnemonics_Logos" data-name="Outlined Mnemonics Logos"><g id="Sp"><path class="cls-1" d="M0,0"/></g></g></g><path class="cls-2" d="M43.6,26.3l-15-15a1.1989,1.1989,0,0,0-1.4,0l-15.1,15a1.1989,1.1989,0,0,0,0,1.4l1.8,1.8a1.143,1.143,0,0,0,.7.3h.7V38a1.0714,1.0714,0,0,0,1,1h7.2a1.0714,1.0714,0,0,0,1-1V28.9a1.0714,1.0714,0,0,1,1-1h5.3a1.0714,1.0714,0,0,1,1,1V38a1.0714,1.0714,0,0,0,1,1H40a1.0714,1.0714,0,0,0,1-1V29.7h.7c.3,0,.4-.1.7-.3l1.8-1.8C44.1,27.2,44.1,26.6,43.6,26.3Z"/></s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\adobe-logo-gray[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 140 x 32, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	2151
Entropy (8bit):	7.859633225944545
Encrypted:	false
SSDEEP:	48:FPEsgO6wykn4cbmeXfVzSzJwbU9dZKASJ/soJ0ANfknj28W:FPEsF6wfjvdOgUDZKzXyc6j28W
MD5:	9AE66EC6AE11F8E9D108E160D2CC138C
SHA1:	2A2D777BB0F63FF0AC298BE41FE2F046D91572CB
SHA-256:	6428A477DD15F959CB1B563A0009EDAA1EF0716852763792D0C66BCF1F4AF4AE
SHA-512:	ACB85C2A7530F2581D1BC52AF334A5A46452B8EAD3F1BD46C06BB5B9FF686C19B6D24BF25D1074777505D95611321A40D0E48D81FB3BA89926AB158A4BBE63C8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s3.amazonaws.com/adobe-luca-prod-ue1-assets/experiments/base/images/adobe-logo-gray.png
Preview:	.PNG.....IHDR..... .....IDATx...oTE..?[X..,wP....`.*j./.11..51^6..O>.....e..."HA... ..h...X.~3..s.=.J.7.t....=...;..k.l|....^.N{.}.X.b.../S..G....D..R...?..IN9.8..HC.:.U....)... ...S....=a./.%)..1..].O.....U.....D..q1....).^l....~.5....r....")a...S.SG...).f.{u.....d.Q%L.....v'Pk.}V...N..ql..iL.....f....X...h....U....<6...r.9X..l..79....h.K...O`..6.X9fO.<.Gs0_.de.....I... .n..2.....o.D...f.[.Mt.]....2....3...`.j{...N.,.hS.;U_5..$..{..Wm.....R}....>L.R...Q.....v....3....k._..d.g.Y.z$@...E].L.....e.:`!.b.).m.....X....k..p..gT.....J5.,.....K....sI.....w{.....F. f%...>....S.",.u.....x<.L.9.p.,5.^[.....Y.zEa.B...uo2p/..."v.xD.... ..:.....ga|'..X.|.....I8..fq.F..c]....W!.....>&.Ob....[....]....3...y..1.V..ZEd...O...b!..}.b95."..vd.t#jp..:u..8.F.X.C.,W.....C.J .p...#.S.....I.\..A..4v9.p..,../#.c....Xz1f....u.....xj!...p. Y.N!..[.;.I..v...0P...P*...w..<.6.0..e..Z....2...D.*.....i2y...[.i\..ir....O..u.....zq

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\adobe-spark[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 299 x 59, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	5713
Entropy (8bit):	7.942941105430185
Encrypted:	false
SSDEEP:	96:swygmCeFV57fd/hMb1uJRyaYyg+1Qao2SqFf93sdo89IxzUwp:fCFV571hMxuJUaYZxa9SqFfhsdr9l1UQ
MD5:	95FC22E047BCEB4BFA6AEE7064399BBC
SHA1:	11A708485B7942104D06F2FFD0F1B6713F25F941
SHA-256:	C91BD804CF36B68D89EAE5FAC4CD8F985563D322273462AF92607AB9927002F1
SHA-512:	2C26049C9A7CDCD17F75DCFB70502D28E397E27F296F5267C6478B2D4F4D263D7584AD772ED3E1C12C7FC42110260B0DCF41694DE881260B92D3E615D9BED8
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...+...;.....#.....sRGB.....8eXIfMM.*.....i.....+.....;....D.....IDATx.._.$.].....q...H,.v,L...E!.P..R.@7'....}. ..R....3.....1.hg.P..CBA...EB. .P..'6!.>..uO....gfwgv.._..W..V...k.....s..../8...<.,.].....w.y.....9.7KaX4""..X....I..s....p.N..\....?8..+gy48"...!0.pT...W`.dNr5...8.WV..huD "..8rV,..,.....".....U.MD.|!.8._p.....:...Y...s. {.....:E.....,}....=..J..Gn..s/....u...U.....8.og...z..u...q...#....@.".k.a..VR.._K.....Y...i.|.e.~.4.eF."..#.=..._.jh`.}.[#E.".+..E...W..Lffu....."E."......~l....:g.....7".L.$G...hKD ".....B %."....C..EY.$n.1.!.....p.t|...>...K._..G.F!.8..0..P7_.0zE(..g...t...;a.p.....rV...?..'.u..9.?...?.o.F.)"....E`fg..._..{..T|n~..$zV../9.I..[..>Q.VZ.....l.I..6}.aX.G[.I..\...TC&.fD`&gu.....tRu`. Y!...Od...@....Jo.U..\..u._..."-....[..+,F....2.Q9....t."g..H....._f;.m.gVZ.Y...o../{/.'u.....gY.V.W.....i.J.:.2;..n..H.@-g..u9....}.^~....-.."

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\adobe[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\adobe[1].jpg	
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 400x400, frames 3
Category:	downloaded
Size (bytes):	30925
Entropy (8bit):	7.75667128400845
Encrypted:	false
SSDEEP:	768:nuowBuvTpjgz+wqrPZ2qh8fmyjlX6RqnxgYqwNL:nuPOpjgzPqrPZRYZGnYqYL
MD5:	BE5274AF7D8BD25B8148A190FF515399
SHA1:	B8D0850FD92EE935287E17988B89E53607808C8C
SHA-256:	26C62DBDF527B8DCBF378EA62F129CBBBA3B244730687909BA21ECD729C9D2E6
SHA-512:	64893C625BE72783088575E36EF26FF4573243F32601BDA754EDA72B7515063B5E4E4831697D16AC663529C910AE12CCD145BEC530F2A9BAE4D9324301C65667
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://nicklaussglen.buzz/011/images/adobe.jpg
Preview:	.....JFIF.....C.....C.....".....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..g.....\|?....".+....._.....4...R...'..q.. ~...n.7.....QXJ<...=...^.V'@U..E..5....Uz.....IE.PTe.}/p.y.....T.<...-T..\|...b.=.#IU..~....{O/...b..E.....X...G...?.....\|....._....M..g.....T~g.....<.....T~g.....3$.=._. IU.K..^.E...=.#U.._[X.R..=W...1.....QTr.\....*.7..?..6.9K..^.E.Ps.\.....%W..y...g)s[KX)<.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\aksb.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	13363
Entropy (8bit):	5.38931773767702
Encrypted:	false
SSDEEP:	384:b5bYu28BX+l4qMufAlXBmdWbDJyGdUpCpZv:bhY7KvedAnZv
MD5:	15DE19F42B35806FAF815298644157E0
SHA1:	62315E4A2013AAEC6AF762D71FCC800136494628
SHA-256:	7F06DEF529E0076B37F65C60085A6B1C65F1BBAB0B1F87C72C188018B5094966
SHA-512:	6506BA8B6465070FEAA86BE8803F53825B9A9922D394043CC7052CD6FBEA9548C343E6EEC7137C5D3A5BA80C11A1B02C6C6B442AE59DA3D48DEC14602062B2B B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ds-aksb-a.akamaihd.net/aksb.min.js
Preview:	/*.Copyright 2010 Google Inc..Copyright 2016 Akamai Technolgies..Licensed under the Apache License, Version 2.0 (the "License");.you may not use this file except in compliance with the License..You may obtain a copy of the License at.. http://www.apache.org/licenses/LICENSE-2.0..Unless required by applicable law or agreed to in writing, software.distributed under the License is distributed on an "AS IS" BASIS,.WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. .See the License for the specific language governing permissions and.limitations under the License...See the source code here:. http://code.google.com/p/episodes/.*/. ..!function(){function e(e,s){function u(){this.data={},this.value=[]}function d(e,t){for(var n={},r=s.getElementsByTagName(t),o=0;o<r.length;o++)e.href=r[o].src||r[o].hr ef,e.href.match(/^https?:\/\/)&&(n[e.href]=r[o]);return n}function p(e,t){if(e&&e.hasAttribute("rel"))for(var n=e.rel.split(/[\u0009\u000A\u000C\u000D\u0020]+/),r=0;r<n.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\browser-icon-chrome[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 124 x 124, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	13144
Entropy (8bit):	7.963791073584651
Encrypted:	false
SSDEEP:	384:4ivh6I4qElF6xzdN0SGd6GsRZj1Xcul1/tOP:XvhNfDxzdN4aRrc0lEP
MD5:	5CE8BC0C54510B727656B9750F4F4B37
SHA1:	CFB13C4F64CE267C2A2A67B6EA3076A86308665E
SHA-256:	71D9139914C20E72E574633CCD31802FEA9130050AF514736E2B6127061A46D0
SHA-512:	9F442960D180D6C11F2341C2D483D19D977F41D36B6CC6D370F9B7C6F472EE216452B96D6F36D4A6621AF6BC53A6291596942A3C11F62A86EB9676E338F6A038
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spark.adobe.com/images/landing/browser-icon-chrome.png
Preview:	.PNG.....IHDR...|...|.....tEXtSoftware.Adobe ImageReadyq.e<...(iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c111 79.158325, 2015/09/10-01:10:20 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap /1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC 2015 (Macintosh)" xmpMM:InstanceID="xmp.iid:87E117A00FF011E69AFE8E50F5F6CE89" x mpMM:DocumentID="xmp.did:87E117A10FF011E69AFE8E50F5F6CE89"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:87E1179E0FF011E69AFE8E50F5F6CE89" stRef:documentID="xmp.did:87E1179F0FF011E69AFE8E50F5F6CE89"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.9..../.IDATx..}..\U....{.o .nv...J*...E).."<..Q?..Q...RT.....[D.U.*.....P..{.n.u.....2wfgvggfw..L>...s..{

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bullet[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bullet[1]	
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKIv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/bullet.png
Preview:	.PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\crisp-fonts.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	139
Entropy (8bit):	4.811599389940217
Encrypted:	false
SSDEEP:	3:yLRmcpZBLvG/tLAJ2qW7RmMjuRmcszgcukrQLJkgfw0zRjf:yL/pZtvG1M2JRmMju/0gcu/LugfwmRr
MD5:	361FE227C22294543FE0FD29B8D28C0A
SHA1:	1D32C0DC6F27CA2A6C67E5C79DFC08DD39511B03
SHA-256:	17D7DDB7C7C94BA00A4F60835AC14512B6574E5D6B81E99542D44BDA414AACD0
SHA-512:	85C7DA240B8283EF24F91AFCB472AF9E9E2E91A5B6F4E7370E774A50F1BAA0F6DF47E7173854B6593FB4EC8673BF682B7122C3877902AE414F0FDD0334C937B0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://page.adobespark-assets.com/runtime/1.22/themes/crisp-fonts.gz.js
Preview:	document.write('<script src="//use.typekit.net/rbi5aua.js"><\/script>'),document.write("<script>try{Typekit.load();}catch(e){}<\/script>");

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\d[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, CFF, length 36068, version 0.0
Category:	downloaded
Size (bytes):	36068
Entropy (8bit):	7.989619253709987
Encrypted:	false
SSDEEP:	768:IyDwGKhjOoERY0ubYt8VzsS62LZB+iADpLaBAWrO5wL0q6qMxIkk:IycpjAUY6VKKTPADpkdrPBZlkk
MD5:	35870FDA65BBD420FEDAC45D4CB0F5C9
SHA1:	A9F5393402174551A2FF00C9C20739B82E138C53
SHA-256:	8792852FC7DE9DE854131ACAD09CB7867193BF1F175E83D7EE55CF0CE9E35EC2
SHA-512:	853C6F0F7605214784A792F9E192279A68F4846C9CFE7DCC6C5599EF74077E9E5CF0413DC93284155D20537F0DE9C27AFB1312CCBF8FCE2D0DCBD2B1562421E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/949f99/00000000000000003b9b3068/27/d?primer=7cdcb44be4a7db8877ffa5c0007b8dd865b3bbc383831fe2ea177f62257a9191&fvd=n7&v=3
Preview:	wOFFOTTO.....BASE...X...F...Fe!].CFF ...@..a...{..E^.DYNA..f.....z...GDEF..g....r.....GDYN..g....6...q.j=.GPOS..h....I..+.Q..GSUB..{.....!.f...OS/2... ....W...`.f..cmap...(.....>..head.....6...6...thhea.....!...$....hmtx.....iT3.maxp...8.....P.name.....fS..post..... ...X.....ideoromn..DFLT..cyrl..grek..latn..... .....Y.....v._.<.....X.....X.....7.....x...j.@....'.PB..nf.@2..Xv.BI..*.`.tU${.....>L_.G.8.....3Gw...5..Cw.yw...W.....=....}j...x....=.8>.....O...x.....x...u...}l.... z...".}...m.>..8Z.....<-tity".A0..2.E+1.RFU.Z.Y.7i..[].W:_.2.L.En....i.....|6.A..J..k1....(...2O....l<.=.]Y...}.],.r.._=..gW..'a.M.!4..B...`!p...9. f<#.-.,a...cC..#H.%r...b..8.|....56.[L.-W5.sNEHM.O<.....{N.....].n.xS.x.>.D{...J..7...A...u...j5...tN...v!....1...6.....|....Qo...`\....m...!.8...#L~.....x.c`frb.....".....l. .E....(..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\d[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 21964, version 0.0
Category:	downloaded
Size (bytes):	21964
Entropy (8bit):	7.9725559995125685
Encrypted:	false
SSDEEP:	384:ANBtlENfUp59YhNFBz4TpgYHLgvE/vvkacO8syS9taWGsSwBytxwhuAd/tDW:sN8Up8hNf4lJHLgvE/0Pbsr9tXSOytxv

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\d[2]	
MD5:	25704A0DEF6040D9ED167F36D3F28242
SHA1:	FBB0D647FC706FC8867EF28DE3A03BD42FA7BDF0
SHA-256:	246BA9C4AB21AC5BB04019666F63AA321BD893478FC4DFF77B25C86FBB5BF36F
SHA-512:	39F31749C8008B106539FB4C249280E25A8FFD9771AB8FF3C45FDF5663C7F8BFDB8CF58766AB12263DE1C7F59DCA51B1691299390975C70556E46EA289868F2D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/74fc30/00000000000000000000158d4/26/d?subset_id=2&fvd=i1&v=3
Preview:	wOFF.....U.....DYNA.....t.FFTM.....]..<GDEF...D...8...B...<GDYN...|.....j..GPOS...`...K.....L..OS/2.....Y...`~wz+cmap..U4.....+..wcvt .....$...$ ....fpgm.....e#./.gasp.....glyf.....Dy..v8.3.head.....4...6.i;.hhea...H... ...$.k.4hmtx..Q(...?...lJVC.loca..Sh.....:-Tmaxp...h... ... .name.....~v..?post..U .... (prep.....R...R].oc.....o1.....T.....x.....6.<.D.D.@.>.:.1.5.8.3.,.F.B..x.]Q.N[A.....c..hS.fB...$.W...vc9B.\.b\..P Q..k.h().A..R>.O@bfM.(....s..r..]Z.y..R.....v...t}...v.@.. ^.n...`3.rG....-.!.i'P....6...>.d..AK3MO....B`...0...../X....C.i*..s*..Ks....k..vp&"?..hj..@._:.z>.b.r.0...S.d".f2].T-3.up...;X.Js....U.....-.2KC...*1B.$.BN9w.?)P>..1....a..q.50.....fS.{. 0~.G..o..>..6F..X.`...QU...s/.....3.%`y.._'..;6..em.C.....2....U.....tJ.....p.X...R.v....`H.F..h-;.*...d/.*.....x.c`d```b8Z.2.c<..W.y..@..S.*....v.88.....q.1.....x..AN.@....@..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\d[3]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, CFF, length 66740, version 0.0
Category:	downloaded
Size (bytes):	66740
Entropy (8bit):	**7.99411972026963**
Encrypted:	**true**
SSDEEP:	1536:J4lzR3d/ZD6MCYkk+e5Hj9EgKWB/uS7wcA+vVWB:ql9NZ/CYFjjKgKU/uLzh
MD5:	02BDAC466185E4E1161BBFAB2C066327
SHA1:	5C0C5E8BDB41694C8AD5605D5C1FFF7EB0702EBA
SHA-256:	AC44BE8F65384DEF37D9091D668E54A4B79AB6A3156C5D8CFBD3268BEC558971
SHA-512:	01C761222E6DB3A3F81DAD88191BAA8A020536C4F8EF8692796B94C68AB1FDD4EF672D8DB24336E12BA32F0F96079E9D388EFD93433E9FF62BB8976596F65CD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/cb695f/00000000000000000017701/27/d?primer=7cdcb44be4a7db8877ffa5c0007b8dd865b3bbc383831fe2ea177f62257a9191&fvd=n4&v=3
Preview:	wOFFOTTO.....BASE...X...F...Fe$].CFF ...H...a.....w..DYNA.....$G9GDYN.....-...a./..GPOS.....#...T<"9.`GSUB.....0.OS/2.....Y...`\Wv.cmap...`. ..S.....lgasp.....head.....4...6..%uhhea.....!...$....hmtx...h.....x7wW.maxp...@.....^P.name.....post...L..... ...2.....ideoromn..DFLT..cyrl..grek..latn..... .....\.....x.c`d```5.z...1...+.3.....p..?.?/K... ....$...A.!x.RKn.0..9N...Qt.5.v..R 8.Wv..Y%...%.....0...]t.S...@G...M..!q.{3C.Q....<t.o.=.a...^a...>...>9....a.....J..... O.=..b.{.x{.....p.....~8|.....$.....:..U.h.84F...e].ul.J.I...f..F.u.....2.q1...,#...xr5..m..N].....N...,D..].P*..ii.e...Trx6.....6I(#...z..S]..9Tz.1rY.f....'..U.G..P..D..P".&^....8.,x].....7..... e..sl.F.Jc#.Y..s...Th.....aL.....E...t..(;..U...;...,.....^H...LJ..g.x.A^[....X.._.g6.kb..}G..%.n.e.....}.X....]?g^;~C.^4..t...<...x.c`f|.8.....).....B3.1.1*.E.Y..XX..X.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\d[4]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 24744, version 0.0
Category:	downloaded
Size (bytes):	24744
Entropy (8bit):	7.978627515034273
Encrypted:	false
SSDEEP:	384:EVkksCq/KOwmOt8IEOsyhgjzfwTJsPj6V9teCsx/Abr2k88CDW001VEKHUM7Ozip:qktXUt8he8UheCsx/AhKW0CUUV
MD5:	A14F6E1E3181DC10FDB66D2A7FB54CA7
SHA1:	605808488DD7FEC481400AA948F80E66189D25B5
SHA-256:	A4B8520DF89E973A968FCD3CF78F742E073EA9645D03ACCF360EB4AB5E6E1001
SHA-512:	E741918EF1EC6A3C0B87D996245945AEA9DB8C7D798352756F409A5E519BBF89EBF8F6AFA1E1A71D5C24C4E1C364F7C2EF38622C0897F852C6E9C7E6C27BBE 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/1da05b/00000000000000000000132df/27/d?primer=7a5a436c948772f5260024dfadc8f7cd849e1448f8bf41ba74a247e8e46f3aee&fvd=n4&v=3
Preview:	wOFF.....`.....l.....DYNA...$.....D..GDYN.....L.i.GPOS.....G..9..OS/2.....[...`\|.M.VDMX.....l.tPcmap.._.....!k`Tcvt ...H.....tfpgm...`.....s .Y.7gasp...d.....glyf..&...4...e..V .head...l...4...6..M.hhea.....$....hmtx..Z.....(.G$nloca..\.....Jmaxp..... ... ...nname.....!.,post..^t...l.....moprep...T...2...2.. ..x...S.X..D.s.X...Vc....jl5....m.m{:...3.....#..C.P..WB..!..K8}...'.>...6"l$"....b....F4}$*.m4b...ic...$....866q..8.q.o.@o.OB..DzCB..D$..l..$!.MJr.;).d...l... .Ml....zAj..4..s...#.MO&=#..m F..)..j3..f!.....6.9....c.... .....6..ln..!y(`.RP..G!....Et.....(f.S\.(B.[...K1J...RFw(AY[.r.M)...T.e..[...-Ge.<Ul...T..*Q.V...BM].*.l5j...ckP.....m-....ih.....S.&.>Mu..4..in..B.iLK.V.).u.f...i...m l{..:..t.....mK...:C{...t.i:..v...L/....mW..n..l.....N.....mo..8.0..a.....l...(..a.2..b..0..v.ct.....g.3^...;..:.(&..L.c.....T;.i..8B.x.....>&2.Nb...l.e.s.T.j..oCX`..P...";...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\d[5]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, CFF, length 58640, version 0.0
Category:	downloaded
Size (bytes):	58640
Entropy (8bit):	**7.993859236860105**
Encrypted:	**true**
SSDEEP:	768:G23+QzXz1F2u0rMcQSwJzZaudOh9lL9cvXjy+KNKzRM+17SabAK9zauA+uhRnmTM:GOzD2/rM7mWO3GjhKNKK+E6auAtMgJp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\d[5]	
MD5:	AB2058631920729DAEA04A14330239E6
SHA1:	75A3B6A23B5827E1846CBE040E40EBD6BA494272
SHA-256:	2E5A6085B998F5B4EA3EE7B2FF61C59F7A7D66F22166F49029EB42A45793A220
SHA-512:	880389F4AF9597A1B761529A5DFFC4C613F2FDAB143E7DA00BB36C0377AFD2FFF74917DDB6CD52CDED2980A19B11EDD732EC7BF381F36CB30975EFE1D2AF9043
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/b0c5f5/00000000000000003b9b3f85/27/d?primer=388f68b35a7cbf1ee3543172445c23e26935269fadd3b392a13ac7b2903677eb&fvd=n4&v=3
Preview:	wOFFOTTO.....S.....BASE...D...F...Fe$].CFF ...4...N.....DYNA.....GDYN...\|... ...QJ0..GPOS.....!...On.W;.GSUB...4.....N`^.iOS/2.....Y...`\Wv.cmap.....(..U.head.....4...6..%uhhea.....!...$...Ghmtx.....6...D.gD.maxp...,.....P.name.....post..... ...2.....ideoromn..DFLT..cyrl..grek..latn.....\..x.c`d```5.:8Gem<..W.f..@.....0....^....@.3..H..d..kx.RKn.0..9N...Qt.5.v... .Wv..Y%...%....cH.....g...g..:.X4M..''(.{ofH>..k|....l..W.Z...L.>.;.8.%'w..C..>..|r..>>S.u_2*..a.o..z....|.>:.%....o...}g.p.Ig.(...b...-....7..U....b..b..S..nt.c._.:.gz...u$.~4._O.#[..sWd.v2}''..u.U.hUws.H..(..*w./...GE..Y.<K...h...1.K.7...dF.....7.z...0.W.....8.Dc,Q!.&.....W.J,X.....V.s..a....F._M..1.._Q..RZ....cr#..^w.....e...T..?S..[...J.v7.wY1...u...{!m7.3)Y.....y.....Z.qC.#g.lN...#;.....}.aW/.s..}...~.N....7...#.C.;. .....x.c`f|.8.....).....B3.1.1*.E.Y..XX..X.....P........

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\d[6]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, CFF, length 46708, version 0.0
Category:	downloaded
Size (bytes):	46708
Entropy (8bit):	**7.9926123068799795**
Encrypted:	**true**
SSDEEP:	768:Ljq+IGHkF+BPu/95GrYWlwFegdvV4HKLXGcbdLapCdmt5FXbJ40/VnLpvLw4T2Fe:PQse4Ps95oYWluvnXFbdLaBFXrtvLw4Z
MD5:	56C4BECEB8718DBA19272C320458617D
SHA1:	5251C59F6956B0EA50D9B4A21992B869772A0AE2
SHA-256:	E89CE18105C28942D113F667B17D952129C0B66D3101DF0D38C18A42DDED47A5
SHA-512:	B3FCA99F08D59640AD8769D7E84DA332B9A5513CFD6685B2D8E8EF0677975D74B5B84DE87D0A35DECE9F6C7D49BE295A0734B83896FADA2A5160E2813189586
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/aa41d0/00000000000000003b9b3f86/27/d?primer=388f68b35a7cbf1ee3543172445c23e26935269fadd3b392a13ac7b2903677eb&fvd=i4&v=3
Preview:	wOFFOTTO...t.....T.....BASE...D...F...Fe$].CFF ...4...u.....&..DYNA.....\|..llGDYN...\|.....e..GPOS...p... ..0.....GSUB.....t.OS/2.....[...`\Xv.cmap.....(..TIhead.....4...6.:%Fhhea.....$...$.$.ihmtx...x.....VH @maxp...,.....kP.name.....~.'..post...|..... ...2.....ideoromn..DFLT..cyrl..grek..latn.....\.....x.c`d```5.:>K.z<..W.f..@.....0....n.C..L..@..._4..x.uRKn.0..9...m.U.]..@(Y..;..N...6.$.`}\.1.#....A.=I....I..8\|of..$.....p...z.X|.O.lq.....=..7.O...UN.....,v..YZ..['...W.W...|.....>v.,>E.Y>....b.*c%..Z....").]YEZ...g.....]...U.g..._g**f:..$..~?..o&....L3t;.>./UU.e!Z..B.....IY.E_z."...V.z-.4.e(...h..t]}.m.eR.z....y.x....9.!.....B...x..jh....N...3...V.F.q.....fj.S\..{.|..M..KAg.5.6AH../.bD.....A.t.UgF.n....KSAM..;..;...4.....=.V-.kr..n.lN.-.....C3....j..h.....f.w.o.oN..Wx..b.....!g.z.8.....x.c`f..8.....)....o.....`....fefba.dbQ``jg```d..G.'W O..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\d[7]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, CFF, length 58140, version 0.0
Category:	downloaded
Size (bytes):	58140
Entropy (8bit):	**7.993838405349219**
Encrypted:	**true**
SSDEEP:	1536:+dG3UnOA8RFJKrWMC4ArrtNJQCjfKxLojn:+dGk2NKrWMC42psCjSpo
MD5:	5BDBAC45C303FAE0D497E3EA06A27A7F
SHA1:	1816C0EF35D230FA3A177E9F719BA03DEEA73B25
SHA-256:	32CC0B7A4C262A62A171D801F5B0EB36E8FD320B0D10D81189F6FB4F43894621
SHA-512:	0BF6B8340105B326B32F491CF784CA487DC28DB0D8B7430CC5CA00CE89F4EB752BB078606ACF104F1F93866CC1C84E94F5A2704D604E59452BE724D21E788CD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/97fbd1/00000000000000003b9b3f88/27/d?primer=388f68b35a7cbf1ee3543172445c23e26935269fadd3b392a13ac7b2903677eb&fvd=n7&v=3
Preview:	wOFFOTTO.....Q.....BASE...D...F...Fe!].CFF ...8.....|Cz.vDYNA.....T..GDYN..... ...Q?cE.GPOS.....!a..Oz.].`GSUB...d.....N`^.iOS/2.....Y...`].y.cmap..8.....(..U.head.....5...6..%ghhea.....!...$...Bhmtx.....DD.@Cmaxp...0.....P.name.....E@..post...$..... ...2.....ideoromn..DFLT..cyrl..grek..latn.....Y.....x.c`d```5....fF<..W.f..@....^0...~.).....@..y.....x.}..n.0...t..B.\q...s.D..UB.[.v...&..I.w...%.*....@....Ix..8....r.....+|...9.....:.....w.f...C|r|..xp|...0..?..w..^{.....s...C..7.Gx.{...Y.... ..\gJ...Qe#.....N.....oW..3.zGc.?/TZMt..2....d:...8i=4^M...7.n..]..\.2...J...vb .y...t..Y.b..2..0..$^..=.}.....}uW...<y.l.E.$.=..''.HHc....s....K~.....5...Z_.i.....S>.....,..&....c...}j.g..._1...j....V.2..c.k..=....hYQe.9+V-.k}.w7..d...%...f6>.sh....;.=<..a..-5.f2...\.pGu.}W.G....kJ.....x.c`f.....).....B3.1.1..E.9..XX..X.....P.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\d[8]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, CFF, length 58264, version 0.0
Category:	downloaded
Size (bytes):	58264
Entropy (8bit):	**7.992987316761491**
Encrypted:	**true**

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\d[8]

SSDEEP:	1536:ysFA+QggYXkhr/65gGFsrge1aT8IHKksD1cUiS9XjIY:L6L1YXkJ/6KW6gQaT8IHK3fioUY
MD5:	E81C892E355CD99A8D3119D358ADA72E
SHA1:	F1267F500B7DDF4924CF599E8B53F4B389BBA362
SHA-256:	714DEFCA2714E79B9293FCC2468945C0AAFDB11D2718BC623A5C974B2A56A5B6
SHA-512:	DB31A35952B0BCF7A7668C66A68223D0E80FB73012F1CBE7D293A9AB03F8FE8F03C80827DAAB3509A0A856DF3CEA3F1990CD6621600501EA2778675AC2E757C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/37eaae/00000000000000003b9b3f83/27/d?primer=388f68b35a7cbf1ee3543172445c23e26935269fadd3b392a13ac7b2903677eb&fvd=n3&v=3
Preview:	wOFFOTTO.....T\.....BASE...D...F...Fe(].CFF ...4...2...B.<?.DYNA...h.....GDYN...`.....Q.t..GPOS.....!K..OL....GSUB.....N`^.iOS/2.....W...`[.tJcmap.....(..U.head.....4...6..%`hhea.....!...$...Khmtx...x...%...D..H.maxp...,.....P.name.....8..post..... ...2.....ideoromn..DFLT..cyrl..grek..latn.....`...x.c`d```5.Z...8...+.3.....P..?.?....1 ....$..N...x.RMn.@.}&$U7.....-+.V. 5R$"...a... {.....r....^.G.*.y<mQ.....|.g.....Cs]q6..[....+|p...0u.M...s.....f~u....._s.....{..-t.O..a.}q.M....Qz..h..w..>?._...-.X...2:..].(.]QFF/.....%..LW....oR....fz..Fe(.^8..'C+..K.`u:..g|.e...h..s.K..pS.E..EO*y...h....i..2..@....cv..9..61rQd].#U]....A.....!.Cq.FX.@.M<....q.... [....rKH.K9.fH..LeW.OM..)..o..L....j..O.".Bz|..!...b..E.R.e\.e4.U.....B..i;.X.Pel.r.....$...l..-.j.....v.l.....r.~..U[.).....u."V'F.....O.G.....x.c`f.....L,,LL,..L.@yF.(ptqr.R..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\d[9]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, CFF, length 58352, version 0.0
Category:	downloaded
Size (bytes):	58352
Entropy (8bit):	**7.992884507564213**
Encrypted:	**true**
SSDEEP:	1536:U2Ph1fS3ZeHACznHaKNlKjE39zfZB4kKAkr:Hvf2OzH/NjlSAs
MD5:	3C48D869909CC053C2EFA6800B492ADD
SHA1:	882C7495CC54A32EF795B89E9E84D1B69C3F87C5
SHA-256:	CFD20EA88B7F7A1B3E18890AAFF228FD6F134095AF8F6DB1F66E4DD551B59306
SHA-512:	0E2ABD3D074418386C6290B0AA5EA09BB8BDC486C715EC426CE1F0D6B48C3EC2EC85EDA7BAAF31375B3481FDCE1DE7886AC0325AA7877F48516D0877F7C06A1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/ad2a79/00000000000000003b9b3f8c/27/d?primer=388f68b35a7cbf1ee3543172445c23e26935269fadd3b392a13ac7b2903677eb&fvd=n9&v=3
Preview:	wOFFOTTO.....T.....BASE...D...F...Fe.].CFF ...8.....DYNA.....N..GDYN..... ...Q<@..GPOS.....!+..N`b)ihGSUB...$.....N`^.iOS/2.....W...`^B{.cmap.....(..U.head.....4...6..%phhea.....!...$...Uhmtx.....'...Dv;8.maxp...0.....P.name.....a..npost..... ...2.....ideoromn..DFLT..cyrl..grek..latn.....U.....x.c`d```5.....+...+.3.....P..._.?7.#..@.3..H..cy..x..1n.0...9N..F{..{hZ..;...@39...L.d....;w..#..=@.^.G)....F:X.....'.$.....e..j..7.....0w.f...#\|v\|A.o.{.....[...r..:..}q\|....q.....Qy.._@tJ.=....+5..U.k.\|.....H.j_V..+)&y...fkj.....\G...Q.-..1..P..p<....Vb..V..\|:...AWuZ...._._*....$eq....U0.E...Z.i..P.#.^.o.._...i.....5.T..+.Gq..&x....1$M.B.....j..O.;.?a..Gk.. m].!.@.....v.....yJ.....B....@.1ko..Y.....5O^.....B..i;...Rel.....I...;zf.k4kFs..>.sd]N...a....0..{.2z..4{...K5Y...w.q.<.....tx.c`f.`na`e``.b.```...q.F..@Qn.f&..&&....v.<#..8.8.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\en[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	214651
Entropy (8bit):	5.278628165558361
Encrypted:	false
SSDEEP:	1536:UubzCmv8xZ7obQX6BAGDcNsF+mZNdZ0ZH5wwZtafKA6OEh5qxIzwvjO+6fDG3/bm:UCCfX7iF/R8wwZQkuRJTHSE8LZ7B
MD5:	D277A48A8F4C5CF1045F852C29AC9268
SHA1:	9FDD98E0E9AC8EA7023137A932C60646321771D4
SHA-256:	E88FF7DCB3405C627C9A34CB0FAC5D866DA26E2CC56C71BD20E5483EC7D4165B
SHA-512:	9BFC72737D66183082014C032CD04E115C79E96619A5C8E1A5C2189AE5AEE49CC213DFE68B6C6CD9AA36A5919D707CE2EF4DD9EB598EEBF7E4CF7648565E654
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.cookielaw.org/consent/7a5eb705-95ed-4cc4-a11d-0cc5760e93db/394a4f88-7fe0-49f1-924d-a901a0001be9/en.json
Preview:	{"DomainData":{"pclifeSpanYr":"Year","pclifeSpanYrs":"Years","pclifeSpanSecs":"A few seconds","pclifeSpanWk":"Week","pclifeSpanWks":"Weeks","cctId":"7a5eb705-95ed-4cc4-a11d-0cc5760e93db","MainText":"Cookie Settings","MainInfoText":"<div class=\"pc-logo-button\" id=\"ot-pc-logo-button\" tabindex=\"-1\">\n <button aria-label=\"Don.t enable\" class=\"disable-all-btn\" tabindex=\"0\">\n Don.t enable\n </button>\n <button aria-label=\"Enable all\" class=\"enable-all-btn\" id=\"accept-recommended-btn-handler\" tabindex=\"0\">\n Enable all\n </button>\n <button aria-label=\"Confirm my choices\" class=\"save-and-close pc-save-and-close save-preference-btn-handler onetrust-close-btn-handler\" tabindex=\"0\">\n Confirm my choices\n </button>\n \n<div class=\"ot-general\">\n <div class=\"ot-general-width\">\n \n General information\n \n <ul aria-label=\"General Information\">\n <li id=\"ot-content-1-list\">\n <button aria-controls=\"ot-content-1\" aria-expanded=\"fa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[1]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4720

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[1]	
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 48x48, 32 bits/pixel
Category:	downloaded
Size (bytes):	9662
Entropy (8bit):	1.5933577223587498
Encrypted:	false
SSDEEP:	48:97gzdbklTMl1sy6TMenl7ulGt/3GmjAAp:970sI2NmU3GY
MD5:	B28BF60DD7E50B6DFFD394EBC0F9057A
SHA1:	9EA7EED87B689757780322989EF426AEFFDC8F7A
SHA-256:	BF24C9E4D37F94D4BD2F870228FF421CA54B2949DB3391DBD3818EC0E6DB0F5F
SHA-512:	B16A7F756E38FFE4BBCC0394A6E41593CC9FE68AACA6350C1C20D10E7A284EBFC7937C15726D0F43A3ABD7C43D128A041A109CAC2C8F240707FE1997E633E05
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/favicon.ico
Preview:	......00.... ..%.....(...0...`..... .....$..... ....A.....V.....'..... .....A.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\gmail[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1280 x 1280, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	66743
Entropy (8bit):	7.712342056984168
Encrypted:	false
SSDEEP:	1536:FxqKcVqezl0vLoYxEuKoYk5LHjGkT3b1mQOEj0+R+EH:FsK2qezl0zoYxEuKo7CYrOb+Rb
MD5:	DCE2F2B0E50CB1DBB0246D152791CB46
SHA1:	D0A69C159304EDC08DB005163E7A0DAF5A1E98A6
SHA-256:	ACF087C1757F08B0CFD53D59066544D7EF0BFCC50999E77C5813739CD9DC1479
SHA-512:	91054B36EF1673B24E4FE3DC324CBE339F4E9EB72785A6A4C355C7B2A11A9A7C6E188FF9BF5B34FFDD2805D4BBED71EF6CA4975EE3E330FD8D8E383ED64B28EE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://nicklaussglen.buzz/011/images/gmail.png
Preview:	.PNG.....IHDR.....sBIT....|.d.....pHYs...../....tEXtSoftware.www.inkscape.org..<... .IDATx...{x.u.....I.sS..9Q(..J.L&.$..V\|.....#..''...Zw.eEQv.Q..U.A]9Vh..I8...H2)`....i.....).....f.y....L.pu...{n..... .....@Is..... mj=...X<65....U.l.b.t.U...mR...e..P.i.$.i2U..@N1.f...i.s...cf.../....2ev.`..%.|.o...s..j..l.B....V&..s;b..Pfg.....!...:..5....$.@...I0.=.IY.....a...B.4g... T.9Wif..R..o.R.t'.0...?G.9i...L...*..&..s.Vgnkhn...;p[.0.5.....$.....P.....^".HL.M...@.p..;04....9.&.(i....9.sK..=&.'$m.....f..1..'...f2.Uww.....PH....@..xq....k.2..l.Luf..s5..`.|

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\hover[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	114697

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\hover[1].css	
Entropy (8bit):	4.9296726009523
Encrypted:	false
SSDEEP:	1536:67O7EesvXIPRX4PT8aZv8qoXIoqbTFaFeTxvyAZ+D7M71D:qXIPRX4PT3
MD5:	FAC4178C15E5A86139C662DAFC809501
SHA1:	EF1481841399156A880EC31B07DDA9CFAA1ACE39
SHA-256:	BB88454962767EB6F2DDB1AABAAF844D8A57DE7E8F848D7F6928F81B54998452
SHA-512:	0902219B6E236FBF9D8173D1D452C8733C1BF67B0EB906CC9866EA0C27C2D08F6DA556D01475E9B54E2C6CE797B230BFBD5F39055CE0C71EA4D3E36872C378 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://nicklaussglen.buzz/011/css/hover.css
Preview:	/*!. * Hover.css (http://ianlunn.github.io/Hover/). * Version: 2.3.2. * Author: Ian Lunn @IanLunn. * Author URL: http://ianlunn.co.uk/. * Github: https://github.com/IanLu nn/Hover.. * Hover.css Copyright Ian Lunn 2017. Generated with Sass.. */./* 2D TRANSITIONS */./* Grow */..hvr-grow {. display: inline-block;. vertical-align: middle;. -webkit-transform: perspective(1px) translateZ(0);. transform: perspective(1px) translateZ(0);. box-shadow: 0 0 1px rgba(0, 0, 0, 0);. -webkit-transition-duration: 0.3s;. transition-duration: 0.3s;. -webkit-transition-property: transform;. transition-property: transform;.}..hvr-grow:hover, .hvr-grow:focus, .hvr-grow:active {. -webkit-transform: scale(1.1);. transform: scale(1.1);.}../* Shrink */..hvr-shrink {. display: inline-block;. vertical-align: middle;. -webkit-transform: perspective(1px) translateZ(0);. transform: perspective(1px) translateZ(0);. box-shadow: 0 0 1px rgba(0, 0, 0, 0);. -webkit-transition-duration: 0.3s;. transition-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ibs_dpid=477&dpuuid=82a7a6cb192223f5461e5ea1a5d012fbbd6b7f6bb957e72b4e22f7f2013133adb0da87c991749652[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):	42
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEy:1QEoy
MD5:	D89746888DA2D9510B64A9F031EAECD5
SHA1:	D5FCEB6532643D0D84FFE09C40C481ECDF59E15A
SHA-256:	EF1955AE757C8B966C83248350331BD3A30F658CED11F387F8EBF05AB3368629
SHA-512:	D5DA26B5D496EDB0221DF1A4057A8B0285D15592A8F8DC7016A294DF37ED335F3FDE6A2252962E0DF38B62847F8B771463A0124EF3F84299F262ED9D9D3CEE4
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\initConfig[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	134
Entropy (8bit):	4.596346617979037
Encrypted:	false
SSDEEP:	3:YWADlFtcmRzHAgJw3BFtcmRzHAgJkMKRjEmb:YWATBHAgJCFBHAgJtKgQ
MD5:	E78AAE29253C4894EF77C2263DF2AF0E
SHA1:	F4BB400456EB30EB1D131549B777F405CCC1D348
SHA-256:	599A201A8BCF34F862C99ED2109D9DAB8083C751FA16AA2EE87382FDAC0E1042
SHA-512:	E4BA14CBBC16AF7E9897557DE666A9EFBFCCA8E066F1AF66D2FD583743DEBE68D9BF8A2500CD02EC7D58B1CDD0EF92EEBD20E6ACC7D1D56E29A49A755913 717F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://client.messaging.adobe.com/2.27.1/initConfig.json
Preview:	{"serverUrl": "https://server.messaging.adobe.com", "wsUrl": "https://server.messaging.adobe.com", "callAfterUpdateAccessToken": true}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\lightbox_close@2x[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 40 x 40, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1453
Entropy (8bit):	6.759166148396455
Encrypted:	false
SSDEEP:	24:B1hnBWwh82lYSKw5hVa64XVKT3JryJ3Vo5hVa6fGjwKZRfp2XOBY6:v1kvnLI600J3e7cVh2XOb
MD5:	13198D9E24E4047B757E69F32897B19D
SHA1:	868CEB3BDC559535E5E638A9E145F35005AF33C6
SHA-256:	2603DCB84908061D1A9E31DA6080328BF7867BFC4AA7A1A9A0FBD25E5942A043

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\lightbox_close@2x[1].png	
SHA-512:	86D943EFB966752531E91911D5F1A9B27CD5003D2E96F19CAE833F88DF856A59C099B237E5EEDC840E00CFF6B9F34E6583B2F2F676EFAEC5055E5030198E5810
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://page.adobespark-assets.com/runtime/1.22/images/lightbox_close@2x.png
Preview:	.PNG.....IHDR...(...(.....m....tEXtSoftware.Adobe ImageReadyq.e<...xiTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.5-c021 79.155772, 2014/01/13-19:44:00 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:0e41a95d-3ffa-4ff2-9f01-79e98faa126a" xmpMM:DocumentID="xmp.did:A061BB706D2311E4A705EAFA721C606B" xmpMM:InstanceID="xmp.iid:A061BB6F6D2311E4A705EAFA721C606B" xmp:CreatorTool="Adobe Photoshop CC 2014 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:caa2ca59-503f-4ad4-961c-e872383c57cd" stRef:documentID="xmp.did:0e41a95d-3ffa-4ff2-9f01-79e98faa126a"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>F.M.....IDATx...1J.@.....DR(.iia

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\login-bg-thumb-1[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, 50x33, frames 3
Category:	downloaded
Size (bytes):	3432
Entropy (8bit):	7.7553083669138845
Encrypted:	false
SSDEEP:	48:RyB4jSX1qpy+R4M+5PFgeNaF8qygsP8CtIWZ+4uadJkY3lco/yIgBWzXx5Lc7XSI:RpUyyCu9mOn8CiokY1co/rgs7xSjS34
MD5:	A7B1798CC2647C575129083BA0B44B17
SHA1:	ADB860A1E675C0FBEFB38A955A5DC4AF9A025B01
SHA-256:	08F9AB3D41530F3E9D8F0780EF1A92F35ED821B5428E6B3C29DDB162F04818FA
SHA-512:	B8828CE68F5C980A9FB880997E5EBAF1533C320820ADC208AABD01B1430FE88DEB7715A900B70951A1F27081E5F6B0FC19A629F14C19552376034CEE1CAA2FF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spark.adobe.com/images/login-bg-thumb-1.jpg
Preview:	.....JFIF.....C.....C.....!.2.....h ...q.@..;#.P.....(.Y...k.....e@F....P.V9.....3wz....X..u....r.!.U..(...Ki...1..y.}h..\..u..m..z...*..K.`..0.W....(.....6..7uv.48tw.....pQ.ab....j...3.....B..$.g....>..1.....p.. !L..T8.^..8u..P.W.{Z.....?.....=....?..r..y.B....."...09...4.U.;...(w.~...*.a+.E=.;..?H..5.f..i...8.n.-a....#E.....K..\..4.]'.O.%....h....I.....:?J.....r.!...!.-$.%FdD.%u.....v.T.N.6t.25..[.X. C:/.z..&....E.E.6r.;]N...8BA5..b..k.U.+...nU.y2.!..EU.....6#.X(....``.....L.FwK..ua.I...i?&.\....l.=..t..!.....bI}s)..M..I:s.X.EH.}.NIX!<.4."t.;.p5..ir...u!,Jai..K`.6._.u....O.j5w[2"...a .S.....p;.@....C6CF.b+.zi.S...iG...|}.....i.....o..|....3./..).9/.....)....."..!1A...2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\login[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with no line terminators
Category:	dropped
Size (bytes):	144
Entropy (8bit):	4.604190783593319
Encrypted:	false
SSDEEP:	3:Qlk4Xvwg3e/QgY1ALD64XHUQZ6WVSy1ALD64XHUQZ4n:Ql5oPX7Ll0AVwLl0tn
MD5:	4DF893C096E968AB098632EB452A252C
SHA1:	0ED4EC3D8D81E70B9D1A9E6E7883FD8E22377AEC
SHA-256:	668862C1854D47A4B178217DEC164025A2A4B1F45CC1409B9D02762DA50878E7
SHA-512:	E6C566F1DF10CA05D7837A9038BB0CD4607B657D5FFC4523256FE1DB1A532E27111BDCF28C230448BAD71B6CA26F37F4AB9AAAAB5318276FAD0A7CF64239B41
Malicious:	false
Reputation:	low
Preview:	Moved Permanently. Redirecting to /sp/login?r=reader_page_bumper_createyourown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\main.no-promise.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	10741
Entropy (8bit):	5.442372384249071
Encrypted:	false
SSDEEP:	192:JtsMOjdwfVbwVhYeB8qfRiaAWfjlVHY7W35Qg6SF6gZhfRmlW1YDqs+qg:JtsMydwfVsVhYhqf0aAWfjIm70eVM6gH
MD5:	CCA018E06A68F94A49E79B2B87096FBC
SHA1:	1DC051BD56CA3E2B0ED6E95AE56FC449831062D3
SHA-256:	350A14AAA52348E4768E8146C3449D7789C92344C4537CE31CF137711E5A90E1
SHA-512:	A90B93282F61F721F40E8010D6B2F9D06017F622CA5CE21E370D55C4DB0EAEDDD8DAE114C79CB12223F2024E1BCED55903CC852DD36D42C14FA89D123DA1C8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/marketingtech/main.no-promise.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\main.no-promise.min[1].js	
Preview:	!function(){"use strict";var e=document,t=Object.defineProperty,n="replace",a=function(e){return e=e[n](/%2523access_token%253D.*?%2526/gim,"%2526")[n](/%23access_token%3D.*?%26/gim,"%26")[n](/#access_token=.*?&/gim,"&")[n](/information=[^\&]+/,"")[n](/puser=[^\&]+/,"")[n](/fnuser=[^\&]+/,"")[n](/lnuser=[^\&]+/,"")};try{var o="referrer",i=e[o],r=a(i);r!==i&&t(e,o,{configurable:!0,value:r})}catch(e){}var c=window,l=c.console.log;function d(e){throw Error(e)}var s,f,u,p,h,g,b,v,m,_=c.__satelliteEmbedCode,y=c.marketingtech,E="digitalData",O=E+".",C="object",D="array",N="function",k="sub-object not ",x=k+C,S=k+D,P=/^(.+?)((?:\[(?:n|\d+)\])+?)$/,j=/n|\d+/g,w=Array.isArray,T=0,I=y&&y.digitalData&&y.digitalData.debug;if(v=function(e){return typeof e},m=function(e,t){return e.hasOwnProperty(t)},(u=(f=function(e,n){var a,o=this;if(t(o,"_id",{value:++T}),I&&l(o._id+": CREATED"),t(o,"_pending",{value:{}}),t(o,"_listeners",{value:{}}),e&&o._set(E,e),n)for(a in n)m(n,a)&&o._set(a,n[a])}).prototype)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\marvel-ui-faf07216[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	1787
Entropy (8bit):	4.813025886465329
Encrypted:	false
SSDEEP:	24:/ewdsJs+PkYbe3wgKTPJLw2bAvAEUQs1ZC7q8hDNNKkZOENYTnQ5l1egaKQKUL:kCBYbe3apyUQWGDNNKwNYT41dajV
MD5:	9B374CB80282B92896CA0F5BFAF07216
SHA1:	B31941ED10E9E8F193F5DC53A82038176576B2A1
SHA-256:	D80D62755CC96593980D61D32B743B30834D3DEF42E152168000841F143ED8A5
SHA-512:	892A94C95403380DCF02759F5AEABEFC2B9FD99CFF6899F830B3C166B9DD78520C763EFBA6989DB207D872526A2568CC3273B85120F2E4D74997E27CCF90436
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spark.adobe.com/marvel-core/css/marvel-ui-faf07216.css
Preview:	a,abbr,acronym,address,applet,article,aside,audio,b,big,blockquote,body,button,canvas,caption,center,cite,code,dd,del,details,dfn,div,dl,dt,em,embed,fieldset,figcaption,figure,footer,form,h1,h2,h3,h4,h5,h6,header,hgroup,html,i,iframe,img,input,ins,kbd,label,legend,li,mark,menu,nav,object,ol,output,p,pre,q,ruby,s,samp,section,small,span,strike,strong,sub,summary,sup,table,tbody,td,tfoot,th,thead,time,tr,tt,u,ul,var,video{box-sizing:border-box;margin:0;padding:0;border:0;font-size:100%;font:inherit;font-family:sans-serif;font-weight:300;text-rendering:optimizeLegibility;vertical-align:top}article,aside,details,figcaption,figure,footer,header,hgroup,menu,nav,section{display:block}body{line-height:1;font-size:13px}ol,ul{list-style:none}blockquote,q{quotes:none}blockquote:after,blockquote:before,q:after,q:before{content:"";content:none}table{border-collapse:collapse;border-spacing:0}body,html{height:100%}body{background-color:#555;position:relative;-webkit-font-smoothing:antialiased;-moz-os

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_101f95855e967721bf3a66e02d5c53da102e51674[1].jpeg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[none]x[none], YUV color, decoders should clamp
Category:	dropped
Size (bytes):	1347
Entropy (8bit):	7.8406745840619045
Encrypted:	false
SSDEEP:	24:1hnPiGo+gePX/M16f1Wdp/eeBemYYHTaD8aMXQ99ujDVQ0xZHy0I3:HPiJJswAeBpYYzTXC9uWsHy0I3
MD5:	3E50647F0F5E8B257F3CE0D07DA880DC
SHA1:	4C8E4A37879D13F091EFEEACD4875CACE16548C3
SHA-256:	0F370775C47928994856D39D86B0770ED0866B32AF5901C257721AC07ECB5586
SHA-512:	0D65689C76C99D92093F90AB8F3643FA6458A0D65B4CD959F31A275952A485858E8330F3DB0190E7C1CC822B51D3A46E5C7F9E0442676CD402BFE82163FA6A58
Malicious:	false
Reputation:	low
Preview:	RIFFr...WEBPVP8 f....9...*....>u8.H..".#5.....M.-.....i.....V....y..G.~.~..g..O...>.....c.c.).....u....?.{.....q...e.3.s....]..o...../j_...^Z.....:.?.y{.G..t0.K/.>Z}..l.q.j.V..z.=.(..*.2{.jQ[.U.)......2.^.....].\..n0..G.....Ki4Y=...B!:\.....\....\...g.q`n;.u..V;..d...b..iD.....D....p.Ht....Q*P.$...,5..(h(..o?.=n.R....i.!.U.`5.C$...Y!3....Gv..%....;.....:.W..g.I..<.(5..k.iU..`.j(.7.j\[.x.....0.....UZI....he.t.@jl..j..q.aL.m.8&.....|*.a...IAW...+R.....mw...Q..~S....fcCW.....gF.no....Y.m.....W..S.v.....d...v.B.....y~VbTJ..Ai./~...Flp....Kl".....j.8.....8..`..<..).?....)\.;,.....o.v.H.:.....M.s...KN.;l.e.0..Y,..1....<L$...#.....;.....1....?2Y$.n...0.....b<.\.i.{..C.|~:.e..L."8J9...q#.2*<.%U...?y.H.c.<.v.8...x.....+%.\.Vq.....Y,....=.!..d}.S.?....G..&.Q.g.....}..S..4.!...k..Y.D....?.n8.+.y...7._.[.<..V'0.(.B[.i[....b.3s..%.@u.....].....|5z.c|.F...'..M`x. E.]..I...%.c..".}.j.!.;.....}.;...N.O.r.D.R.k

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_1022d55369c9618986ad93c5a25072f4185e4b63a[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[none]x[none], YUV color, decoders should clamp
Category:	downloaded
Size (bytes):	12940
Entropy (8bit):	7.98424550109483
Encrypted:	false
SSDEEP:	192:qX673J/v8tEwqkc3MpDWpJKDcNDkTXW6TbngBAwbaaRNLf9ZzzvhWASQBTi3:467Z/vdwqMK9eTLgBAgPRpzzppSn3
MD5:	CBB822B3610F0F88F63E7CAA760AF243
SHA1:	478FFB41B30274991338A7FA1D271D77D08DC2E3
SHA-256:	2EEE17EBF0717CB72C5F48B14123ABFE9406C6D90BE3A6A9BD6BC778C5700E9B
SHA-512:	88D7E67579A9A1347851F7FA45E661BDA50EAC6EC7F023FA6D883065366926D9BBFC961BC238747CFD4BCB31FEB954E1DB5A9D94DCB62045E063DA7DD5EB6B07
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/discover/templates/media_1022d55369c9618986ad93c5a25072f4185e4b63a.png?width=2000&format=webply&optimize=medium

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_1022d55369c9618986ad93c5a25072f4185e4b63a[1].png	
Preview:	RIFF.2..WEBPVP8 x2.....*..k.>u4.H$..!'4\....bn.!...o...}..O..z.....?.}..?.K\{.+.....'.....t=i?.~.{.....[.w.../.....?.^...=.....K.....c.....C..?....7.w..=.}....}.....{....F..m .G..}.|.....z....3..Q...L.+...~.Q.....e..?.9.C.E?~.]3.T(0..C..L+s9m....h..L.W&].1r.*o.Y....9.....R..&.L.....5.[|#.x|.....E...S...xV.&..V.;.3..T..`.Lv..O.,K....{....bN.4..QU...Q..... .u ..ltV.....]vs2n*.X=NO..c.t..s,t.2.QC.?..c....{"t..~.....W..H.i.....5Z...C.X.p.Z..l.....n/...5..8!.$.,.#...../..w.. ....^q".>l.q.<.n...K.?..MG.U..N.....R....%..6..1.....{~..7.o.N._.BN.o.2 }.....4....Rc.....].O...Jw?x.. z&.....2F..5|..#z.....?n.9.....s.0.... ...hNY.p..g.Q...BGt.P.../6.I@.7w..$. .b9...O...C{9..+.....+.....a.*..!wrX..9"..).=.=.]/^....g.I.6.D9{C .;t.h...G.{.. Ks..9..o..30....."...X.H.D...4r.k...g.tf=...7..._.x.g0zLG..yiB.r.mW.9T/4'0UZ...WMVX.Vw....mBD..../4.R..N.SA...)`u90.M.-.zk..q{.....>.....fQ..EX..h

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_1137e79890ce81304b92d7de7a647c33a4dccc5cf[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[none]x[none], YUV color, decoders should clamp
Category:	downloaded
Size (bytes):	10166
Entropy (8bit):	7.980335588969246
Encrypted:	false
SSDEEP:	192:Nqz5k4EZWcOb+Pdabb/J7Kek2aDZMdjKraGVlml4jVeFqJ+0y4UNUIlt6u:NqVk4EZWtPb/J7KUrZIlml4jVe0J+0yB
MD5:	AC4B894929F12B25E4AC637F21948D49
SHA1:	BFCEBDBC9077D935395CE6B55456E3B5CC7BF51B
SHA-256:	83AD177DD306C271A7A0103CCE1606099C6901C231FE98E5A5DF2A4FEC52FEE9
SHA-512:	0C1218A5AF0F655A8E60A101529B0045E1D23C34355B6E917E84BAC884D1EEA896D0F8FBEB0D78E326D3020AAB9C5D4A1D18AF7D92B31498D950409EA1F3A17C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/discover/templates/media_1137e79890ce81304b92d7de7a647c33a4dccc5cf.png?width=2000&format=webply&optimize=medium
Preview:	RIFF.'..WEBPVP8 .'.....*..k.>u6.H$.".&.j....in.`2..o...C<.....o.....;.....n.....G....!.Y.'.O..._..%.i....g...c.....k.....,_.....#...o./.....s..._.../.....W...?.....o...u.. .....QWz%...c.h..3V...L}M..fj...Z....7..[...A1.4.}]...8&..}....kM.m..g@.5.z,.X'..I{mi..Z....D..{_^c=.8...T.z....[>.....%.....i..7~....?....g.....57.1...y.&.|..i:b5..(.y...H.N...E..3.Vw..Ji<.. .+-...Y.. .q.m:.j.D....P.>..#Vr....N..eW..?&..4:,M.{}..Ew...'...D.Y.../..W.@H...\..e...;O.E.Wr|..U..?U.nB..".C.....W.R.y.....|+Z...2..-..=)....o}t(jh|..>...H.L.:....s.....T7...._h....Z.YO.|...! ["'..9/.....f(!.7M.LS.e..i..Q..}<g..d^.V).B..u.bB.}.'..@..N...b..C.@...wL....5*...q.....$#...7e.2.Z...M...0t^.....W4HK...h....\...#.&.....f.....0@b?'...?....r].$V).....^<....4....A...S. h.....wp.SI.be+..t...>..{...2=.Z@%.....5].0.X.....Fm.R...]._. .s..'...{q.....&"K..A"...n..\.....N...}(5.....J-m.....U.u..E.K...!Hf.=...m.d"..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_11509db7f6d2114f580490ba33b5f8b113df45a01[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[none]x[none], YUV color, decoders should clamp
Category:	downloaded
Size (bytes):	12488
Entropy (8bit):	7.985091843499927
Encrypted:	false
SSDEEP:	192:g+tRi7RhoNKL/AOzYh6oOXsZgZY/bn0wtmEP/y1cjNdOucFH51xpSTpisTxGv/6i:PAFhV4h6oVwwmE3yuy1HyMSxg6j9tOBT
MD5:	C64C86FE6BF1E64917CD40F51A3F0212
SHA1:	EE0AD8959A9619AB9ECF6447A73233C38998993B
SHA-256:	E5F1BD8E854076333BB35D12C7C8AA4764F2F9692A9DB079E0D2B0EFC80BF426
SHA-512:	963B7283782186407DEA17459D9B9FF8FFBAB34574849D391688D8F0B5427FE240892C0107B3D03A4C46878CDD491E7C613DBCE9157C6C07DF15F6DB6DF35BC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/discover/templates/media_11509db7f6d2114f580490ba33b5f8b113df45a01.png?width=2000&format=webply&optimize=medium
Preview:	RIFF.0..WEBPVP8 .0.....*..k.>u2.H$..!'.[...bn.rP...d..f_.....7.....|...@.....7..u....{...~.....{.....e...l.o.....PO...}n.S?.z.~.....b...k.7.....nn..Y.....C.....=..W.....Jj...6..... ...W./...^`.....`_....e}....'.O`...e...].....7....J....#.....]f.....j.Z...-..K.<....'.9.t.i?.../.R..m=..-I.....^^:. @.GH.....6.J.?.xq.8.....w...d.D.e.xU'.H/\+.../...^.3J...8.#d.....j!..."....U.E.(.... v.....X)A...w.q w..jnlQg..h.}%H{...u..;.r..^..T.K....Z.+<g.8....'v.O.s....S.hO...xc. a..y.t.X.. %.rh..gJ.....8..+.rC.....6.%.%e$...-.2....|.g.....\....[.3..G7>.....1.N..N:.....R.EXw3in .5..j...Rm?.O=.q.....:.....'.....x.A..M.t.....N..;7.....*s....FTw7?.....3.d...`#H...o_..7...U.tV..M.p.....b..j1...K.d.m.{e~..y...O../...B6.....;...?.A.w....%.{l.$aWS..v..%&.z>Ut'.t.... .o..I.iB.K.<.{b..+.B..Y..... .+..C...1.q...r..?".Z....<.....P.....z.`[T..8|.8.....g...B.-.. 0-.p.....T....!...r.pN.....|o.=a.pR.J;r}..(.c.r..-.,..E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_11ac71813080b7ad80d8486ba8212b564a66f1d25[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[none]x[none], YUV color, decoders should clamp
Category:	downloaded
Size (bytes):	8602
Entropy (8bit):	7.980706577311374
Encrypted:	false
SSDEEP:	192:0Vb5mwlQbI9SDD9SEpabX0yTyPB5i3Ky5y6qfo5GmE:0/MqSsECXsZ5k4vmE
MD5:	3519DBDEC738221B4ED56F146889B0C5
SHA1:	8368D90BB91AB4BF312B31A0959AE311AEE8FB7E
SHA-256:	F3884FE1C01470D8BDA7E399CF81D46299FFC11C39FD6F2C74A164607505B0BB
SHA-512:	570E2481C9A11A30EE6E7025248FC2518B1416F37F2BD3134FE4EBD6BBC870E017F95CE329DAB48F3B28D4CD138AE14F8BC4AEEB175FB0710E503141F3ACDDEF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/discover/templates/media_11ac71813080b7ad80d8486ba8212b564a66f1d25.png?width=2000&format=webply&optimize=medium

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_11ac71813080b7ad80d8486ba8212b564a66f1d25[1].png</th></tr>
<tr><td>Preview:</td><td>RIFF.!..WEBPVP8 .!.......*..k.>u6.H$.".%s;@...en.K.O....W...<"......K.....;.o.O.....X.../.W...../.?P.:..~.?...^>...|.=@?..9.....n...xK...x..../..;_....'....m..}....?..........^..r.O.w..........A.k....
.....G....+............v-.7./...5.....>....y.\..WH%.. ....UY..v..l..D..|...=...Lzl(....Mi..g....y.R...X.P.1^Z.....PJ.U.sqy;..).qT..s.r.7...J.UW...]..u:..&..Vug.....wz.l2...6.6.)........x..].)Fn..X....
q.^~....^.5.Q:RT'#.W.~.>\.........JZ.=|{....e.g..S.73.R.w..dT.T.,....%.o|....8..]..:..6._...Rm1.:..>._..1..4...D.h.#.PVI)...@..=.......r....;.Lh...q.(.n...|u.C.../.......A......8..Q....H.D;..g..;Z..X.
..[..z... .~..J...j..5l..Z}.....>.GU.1.R}.qF....a.E.9..L......}{....>G$...Q......@...^.*.!.$..SML.u.....r...p....+?.Cg.....(.-.D.......v...]..n.u.Z&...&...&u..*.nT].1MS.q.......1.D|.>..o.......`?l.&.b
.....@..-..l..pe..OJ.|C/|...x.....)...&._+.A..+.=...U...?...d..^#A.:r.~...TPQ0#..R'6....y.@..d....ZLZ.u..s;l. .t.+..f.g..{.6...........D..*.J.l.p.9</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_124e34d3819ffeb81b5d7792530ea9a99961b1948[1].png</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>[none]x[none], YUV color, decoders should clamp</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>11192</td></tr>
<tr><td>Entropy (8bit):</td><td>7.981805427063665</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>192:LdKp2W9606CMmRJCgF8Vu7mTAZzTTQuGH1rT8dC/PVbwA4bEKAO0DNFb:8pI06Cd7amHxTTQuS3/Pl+bEKAO0DNF</td></tr>
<tr><td>MD5:</td><td>1052D0B4FE4E3D6A976E0C0D866DA0F0</td></tr>
<tr><td>SHA1:</td><td>1C141848060AEC58146088BE62CB390B94B84A01</td></tr>
<tr><td>SHA-256:</td><td>98DB8F4F2D6892EBBF1B22663E02F4BADC8882CE22D361C057BF0456AB7112D1</td></tr>
<tr><td>SHA-512:</td><td>58845C78647D57984710FF361224093C480E03081E80F64658081541D4ACC98A32F4D24A94C9D911500C33D120B56D69B0510B18072303C5E4F17E4C3BEC6420</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://www.adobe.com/express/discover/templates/media_124e34d3819ffeb81b5d7792530ea9a99961b1948.png?width=2000&format=webply&optimize=medium</td></tr>
<tr><td>Preview:</td><td>RIFF.+..WEBPVP8 .+......*..k.>u6.H$."!&s.p...en.O8l.@../...s^".c....f...w..0.0~...y......O...[.q.%.5....&#.......?._=.xz....9_8e...J~o...?.u.)...S....?......7./...|..W...?b=.}t.../........g.
_..~..................o....._.?.?......j...O..;?U....~..t{............8^.6p-r..{m.N.=..^...Dv.......X.#.@Z1Q..(...N].Q>;nqW"D^.N.v.=.;....=,....3.L.....Y....R."...QP9.3j."...".._7...}......z...O!.<.9B.
A6}..(N.....L.W.|..Z<....!.TR.nol%..c..S.k..K.h.....@.b..,.D...e.WF.0(2;.M.o.;N.J.M.]..9V$.o......&.V.?...4:1L..tj(...0A......l.E.cup....y!Z.......5.d:A.........D'./9.........5..rI..g8..#..B
.,..@..E...*....v..{-......[....^..8m..Yo8....B#..gs.o..sQ....s.6=..,........'.`...............".......=.0..B../.{...^]_..1.....$.......??.A.y.+..6.w..|....b.4..).RW..!...=.*Mw2...j...4...XuL..6o...Co.'..F;..f.
..xq;>...{W] XCP........|Z..6a.......wBd...v7.o2&.a...q.#A..S.....i>.8.. ...<....s..Fe.{.*]..".....K<.b.*Mc."..~.......X.kv.c..=.-u?...\._....4..D.Q.>/.imy#.z.33$.G.d**</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_127d8ddf746b3d9b821b50287212a23ace9adf57c[1].jpeg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>[none]x[none], YUV color, decoders should clamp</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>13139</td></tr>
<tr><td>Entropy (8bit):</td><td>7.88334446569705</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>192:XNa8YGB4wE/qIUZu9F4Csy9J0pvJ1xrhIFZqAN+K32K5sQ8soJCiJG1nBC/f2IXR:A3GBFJZuP4Cd0ph1XIjBsG3osiVH2cR</td></tr>
<tr><td>MD5:</td><td>76099B3F710D338A278B2B5CB8565F40</td></tr>
<tr><td>SHA1:</td><td>D6AE5760676F476DC9C559E4C71244134A87B849</td></tr>
<tr><td>SHA-256:</td><td>E29EADF05AC4870527A8DF65D31F7DB02BB30D46590CEC0166A273538A79CA6E</td></tr>
<tr><td>SHA-512:</td><td>068687F11C7F1596C7B3C5B29D8473AC1A415E6D5EC2B55B0C6C0C1A3E870944F710EC34252A343F09C8E1B835D84F4D5F4992535BFFFA56729D47746DAED6A</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>Preview:</td><td>RIFFN;..WEBPVP8 B;.......*....>u:.J$.#!......gn._....-.%..;`..M~....o./..O.o.^@.!.ox?......G.?........O.................O....~......k........?.......{^...6...K...'.?.?.}t.....i.....o.Oi/........a............u..
..O...7..}~........w.....'....,.............<.;q@.._..........E..i.....W...g....|l~.................U.'.K......%..?..e...C.......?.>....'.?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.
B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?
f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?
f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f.B.R....n.)%/..?f
.B</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_12f25246ef43123b4685f4a829d1afba8e4a646b1[1].png</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>[none]x[none], YUV color, decoders should clamp</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>9036</td></tr>
<tr><td>Entropy (8bit):</td><td>7.979243285294048</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>192:bShJQ+GGsmNrAiBacmHkZrL+d/EvBTvEnBeXHNU5PD9S+UDagS+tKo7Qb/:eO0reNHk1qYpvkBeOD9Syd+tKo0b/</td></tr>
<tr><td>MD5:</td><td>FDB7A0E70AD1278B121F752914FB73C3</td></tr>
<tr><td>SHA1:</td><td>7DA23F1E586B1EA4B12418BA3730BF3B26240FD7</td></tr>
<tr><td>SHA-256:</td><td>4F95CE6CDD0362E9C563F8F8739C82ED4FD08A909D43CD6583F44370EF94D56B</td></tr>
<tr><td>SHA-512:</td><td>2D3E1B882D5BEF85604FE0A4166BD772BCDCD57D2FA2BCBF7E7866426EBD6F48C0777D6600E079EAC89C161E2B7020EF939E6736DFE96967CAA5DF35A40B93
C</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://www.adobe.com/express/discover/templates/media_12f25246ef43123b4685f4a829d1afba8e4a646b1.png?width=2000&format=webply&optimize=medium</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_12f25246ef43123b4685f4a829d1afba8e4a646b1[1].png	
Preview:	RIFFD#..WEBPVP8 8#.....*..k.>u4.G..''!#.....en.s.._.....~.{..p.~.....@.G._k...7.../.?u.'ug._..~..'...~..Q....P/.....l.>`.....u.....?..}$...a..._.....#.{.....o.>s~...../..o.....?j....jz.. ....z.b.b..O....Z.....qA^..ZQ+..u.....9.{`&.X.W...W.(Q.D._`.Y.I9..N... ....T'.5_/!W681..z..)J;I.....`V=#.o.v.1...)EVZL...."#..<`pg..4.}6{....{..e....^..a..z._uF....p.W.k..=....{o^..=..[.@. ..@K G0..6O.W.1f2+\..+kO:...:...<.I;I.....sRV>7.....ZAU.{.....n.x.xYI.....t|..].2R...O....f.w.@.G.8..../..t...V).\.....t.4..dvo.G8.....:....0L..TK....R...G.%.IPM"B_.E...:.".@..K.... ...&.LQ.^.uTa.$JZ..9q.....o.S..x*.@U.|..n.2S...Qi.|T....2....L..?GE.K-P.m3.H.gH.b*h.^...r...L.,.A..83|.Y6.m`.....n....1X....zvr.@..~J...tJ..Sb.....I..T`.x...\...k.....swSu\...c.... .,>f..k.6#=.6.b.?...,..D...H.....S@....;.."Nr..x..V..l.o...[0..=.....q..p....V.....`.c.^.3...O....=M....|.bU.....]5YH.|. K....66.z.M...X.Cz..F...7g.H.....|....o.19

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_13f42f554dae61fb2c87c959ba3208317bb5507e0[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[none]x[none], YUV color, decoders should clamp
Category:	downloaded
Size (bytes):	11784
Entropy (8bit):	7.9831602641192365
Encrypted:	false
SSDEEP:	192:Qt+4/zDayc+lmbX0CqiTPZ6759stI2pTQX9TuTeHVt3OVZXFOLh+JPAA8WsBrfnK:sjfa9+yEC1y9D2CNKTeHVt+Vt4uoAqB2
MD5:	16667B7A0A947BA132EE07695FBFE064
SHA1:	2862AE32B7815D0EF1A59B6D5991618E3C62E74A
SHA-256:	1145213435965C31D4B56341EF55D4B24BA935AC7647A3E5A2C3A41B9E75BCBA
SHA-512:	74DCB02EA68CB39DBDB43F6E9121E7D019C5F89693489DC54BFD89AD846C81F5A4F642ADCFBBC5503EAF020AFEC2F54ADE1F6D3551BF65093D8E63ABB775CEE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/discover/templates/media_13f42f554dae61fb2c87c959ba3208317bb5507e0.png?width=2000&format=webply&optimize=medium
Preview:	RIFF....WEBPVP8 .-.....*..k.>u4.G..''!'4.....en..7........3.....{|.v.......y.~.t........%.........]e..=F.f}:}.?........e...H..~.....L.!./...v?...d..O....w.g.....................?..vRl_.b}.}....O.....~..... ...?.....W.k....i>....h.....w.......}e.....o._.....x.....F;D..t..''..Ox..v.Fc.\....c..~>..Q......A...`.f+U.Sc.r.. (..'.(..pR.[qX.,<.3L..dF''..3.:.DGI.~...9..|..L....._-...O+....tJZXs...7.`...~... v2.bp/~.....X..0q.....Rd..bI(4.Ej.?G.....J.z4.6.>a.Y.p.]...Lg.Q+E.....lX.W\.q.)...R}..5C..I.]..0...D.....22...w.....0d}..]....GF].+.#G.)"s.....N#*..Q .I...Q].....u.S`b....&:....S.L.P.... {.:/.@$b/>Ib.A_A8...Rj\\..a.P.K.XC..O(....|0...8..u..].....p..d.,A..p....^....E.....KC4...S|....Z0J}..\x...n...n.%o.R.=I....TT.JX&.i..O.]:...;(.....v.y..f...1.....c.f.K?....>..wj.....}....' .7.Ue|_....._%j.../....j.*.d+=+..Y...X..\..ok.b.>J ..*\s....!..r 0..l..u...X.g&.9.....>..O....n.X+...E./.*...~...t.....#~.2.c{EO.H..6*P.\2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_1487d92c7935ccbb3c949843f5e5ed811950def06[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[none]x[none], YUV color, decoders should clamp
Category:	downloaded
Size (bytes):	10954
Entropy (8bit):	7.980183827990017
Encrypted:	false
SSDEEP:	192:yJ0W/gIwjr6VRN5JqNMUFFY0KaSC2wJx7ADnosCCERedFO8OegQV:pvI6mvNaNVRSwUDos7lUQV
MD5:	1873FC0F0AF72F35A8F4AA458E20BCCD
SHA1:	B7D51AEE2C660794509896A565F0719B4AE296B0
SHA-256:	9F05DAD13A701D1D22A2C478FE6C32110E57994F2C2BB9341441DE85EB413F5E
SHA-512:	56E182E72A6C01958DBBA2841C55706F8653F5B7B9F0F4B9A5C28580F3B8AC74061BC9BD94BD3DA07A143D1651CF8C81247582D0FF21F50F6B6DA1C3C59EE0CC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/discover/templates/media_1487d92c7935ccbb3c949843f5e5ed811950def06.png?width=2000&format=webply&optimize=medium
Preview:	RIFF.*..WEBPVP8 .*.......*..k.>u2.H..."%.....in....U.9....#.A.....{/B........rYY'....9...o.....f.2...-...=..e.....p..|........}..9........._.?v..5.....'.O./...>.>....w....._`.............O.....~..4}..g....`? ....s.............{P.....?._...?......U....o.O..u....%...ID...e{.bX../...w.:.=C.Hf.8..o.!.6M.......c....W..$Ws.%v9bd....[T..Az..q.....[.d..g.}r-..).m_.Lo.o...l..CYC.D.......ral....C....l..hWF+.....\|. (..Q........Z...Nh.........,....!..^..&.V..U%8.e..../.;....#o..NJ...,M.Re.0..@...\|XB5.<.K&Y...m6...eNz..qPj..l..e<bx..J....hQ...4Ba....^....#...E1....H........B,0....$Y.......].$....>+..4.. 4..=`....A.e..Fh..o...E.....9.b....hwkKf.....w..m.....l.....5+.........2....Lp.=.....Ov.....<....[..._g.....e.dL.5.$.3.o....6...5.D....>..R.(.Q.<...-WT...o.3&T)7...N...X.k-d.6p.,.@.........z7A...t.. M...),.(!.........s.....i.....S..0.~k....w+..#...=.2.se>..#..!.vN]K..)7.T...?...A....v.....e.B...'...3...l.G.9....(\4.G..("#i%.~..H./T..x..#..).L[.''..]

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_164ba32a452ede9f21053d1bd33db8e5bbedc309a[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[none]x[none], YUV color, decoders should clamp
Category:	downloaded
Size (bytes):	14466
Entropy (8bit):	7.985429894432838
Encrypted:	false
SSDEEP:	384:TdczVMzmDOkWZu4LMiwArquPI+/89TunN+TwSfh:azFDnOUifquPIJMN+rfh
MD5:	43B5B2F33810AE9A370110B1571DD251
SHA1:	B6686C58FBFABAF0ED75D373A064C2096518AB3C
SHA-256:	0132AA208F0F6E35A71E963444EC930EE3BF5A44039B9406EFA28464B2C68581
SHA-512:	7C97038DE41DD7390EC6424E7C762C1D1F4433D5619EE51397385F8D52263292AF251C64A6DC3A01DD2ACB719BA3450455ECEF449F0AE3352210D00CFCC15E5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/discover/templates/media_164ba32a452ede9f21053d1bd33db8e5bbedc309a.png?width=2000&format=webply&optimize=medium

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_164ba32a452ede9f21053d1bd33db8e5bbedc309a[1].png

Preview:	RIFFz8..WEBPVP8 n8..P....*..k.>u2.G...!&..`...en...3..j+.................=g..>.....#~......G...g..O..O....4..U.....O~.............?..,N..'.W....{...O..........k.o....M;......^..C....._.?....G.O..... ?.....{...........k~....[...#.....W.................M....~.~........_......[....x...n...~..h.u4L1+E.9\..a..n"...V1c.|}..J#.....9t.X..c.. ...GHKf..z.._c.......f...-.`Kkd.............kH. S+..}.....d...V.p......T *..)M..@U..(...x.Z..R....d-..@8..%........v..@h...V@pP.W..pX..[..X.h..-~.8......8zM...+'N.E.._....L/.........>..k..;....|p.f.3.Ht....K(\.g.'?.......`......8..a..*R*...u`H<...$\|..h..d..e.Ae~ ..z.P.r..x.i.0........Y5v..IO)..{.;_....El.I...k..".n:\|U@.A..1......~B.y3D.E........WZ.6......!.....u.w...A._.+!M.Z{.J=.idz....j..._.#$....F^..G....g.P.6._.-TVM..zz....qjS..9.:.."U.f..Bo.G.p (.......=.x.n..e.+;z.^xU.....q.-.u........l&.. #E`....J..&.E\.N.4.x,kK..o...z2\............gE....))......{..-o....*.IV..y.@..Uw../w...XaS........Z..sh.zN....."<...*]m...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_181b604b63bec3b8bbee889de292d1daea1530139[1].jpeg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[none]x[none], YUV color, decoders should clamp
Category:	dropped
Size (bytes):	1345
Entropy (8bit):	6.312212937476646
Encrypted:	false
SSDEEP:	12:s6Z2EElA+BS5ag410WUZaN4cftG7xN5Vxo03KRiSl2FN4YpXeG4ScWU14zRV:s6ZzElp37ZI7Lnxz34iSqTXeysoD
MD5:	F21B58A18D9DC8520657C7B998CC095D
SHA1:	5D5866BE383604C0D999C681B22B06FBB279316C
SHA-256:	0B8DC893D118E42FEE1646C62919C26DF8849BEC04EA230679613EB9A85B5DFB
SHA-512:	046231D62D3097E85F3F7ED6B64945326A3A6DFD7F80112888D889DC9F41E4FEE1AAD3A75EF6CC77E94F48955C446176B21B85F852B0E8609A93EF510D03074F
Malicious:	false
Reputation:	low
Preview:	RIFF\ ..WEBPVP8 P ...V...*....>u:.J$."....@...in....#..~.....1..M?...s.y.o.S..C..d..z_>O.u...........{B;.....h..pE.+....Y?......3.`.....8p....8p....8p....8p....8p....8p....8p....8p....8p.... 8p....8p ....8p.. ..8p....8p....8p....8p....8p....8p....8p....8p....8p....8p....8p..f...aB...(P.B...(P.B...(P.4xj..?..............$2.6+..^.z...^.z...^.z...7.....L.C.9.O..b..s.Y.. ...^..l.,!G..d.W{*..........f{8....W,. .|..b.}5.^.z...^.z...^.z...S..9h......c.."8......]2(.y....TE..+..,..KDY4../+6t...k|.\L.5.....f.6l.f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_1b789978976aaa068321eb8d193edca9c6d7df091[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[none]x[none], YUV color, decoders should clamp
Category:	downloaded
Size (bytes):	6916
Entropy (8bit):	7.970505864307654
Encrypted:	false
SSDEEP:	192:jY+v60KbubPugHLhqcrjsi5mTs8qp7IeC:jY4dPqcvnkshp7IeC
MD5:	159346B993007B26CFB5C365CBFC890B
SHA1:	0BD84CDDB0E7B8265E0FD2A6F6CCD08BCC758F14
SHA-256:	6925260FF59BFFD1F789229D6CC10F7FC5105EDB17EDD577EEE3C9D3099E5DD5
SHA-512:	6188D2C94DADE040981908C9562EF2D665A3A8940DAD464791BC6A8204FE548F9887BF309C4CE0BFBBEBFE8B73D2719B5C2B6C6464CAC721261D20E7FF513E 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/discover/templates/media_1b789978976aaa068321eb8d193edca9c6d7df091.png?width=2000&format=webply&optimize=medium
Preview:	RIFF....WEBPVP8 ....0o...*..k.>u8.I$."!#4J(...gn.r...B&4;.......?......}.<..n...k.i..ugz7.....\|@z..^.....l.....'.O.~................/d.....;...3..._.....).....w.......}w.w.o...........G....O...0=.}Y.. .W.O.....op..?...\|1........`.etH/..h.],..x.z.z..n.B.... .RSs.*..xY..i.v$...k..|ye.E{.)I.Y...w.s..P.(...6o.60...U.V._b?P.S...O]2bZ!.m~. 0.....6....F.Pf.Y'..v..XV8..>.A.|.^....k.c.jt.Y..5f&DZT .?.i{........)do....N..Qh.Jw.[*...k.....EQ..:Hm#..N...(...Z.+.t1_...B.,%.......xg&JsU..-....7X.7..6....X ._..5.k<......T..,d...)C...jf+...Z.[q..I4).q}.....M)..tK#.*V[.:7P.Arfw...b%.~#.iZ7.[. S..,.*..UA_/...'.XW......]V.c...-.=.dcb..Iy..!....O.=F;.....l7Y..`B...{[/..Z...........w..{z..m&.....]^.}).:.J3...D.(.:V+...3....y....a.*..H....C.Mo.^....&G..<f...Fe....S.B....B..yX.0...>.....p.;Wb8p. !......`...?..G..~RF.SK.%.).e......6..H.R.o.N.>...nRe!O[|..#n.,`..Oc...P.n..DnV.!O.P{......,6.........d.W..E...Cf.x...B....`k y...........j-....j-.~~......_...]...oMo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_1e13cbc31404e8b28464e9b87cd8a6537e45b579d[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[none]x[none], YUV color, decoders should clamp
Category:	downloaded
Size (bytes):	10730
Entropy (8bit):	7.979522682402237
Encrypted:	false
SSDEEP:	192:xj8sHk6ii6qNk8+spzbLa27iidstJO9fzANJO9MO83s4Qf0NLX5CUvS0tzK2uHu:xjTHkpiggtC2uSstJqfzAdjoCtLS0tV
MD5:	2E13C36813551BA9A53B95EBE85D23B6
SHA1:	A17AD1BE00D473D2107ED041360423BABC7BDBDC
SHA-256:	368A81B50ED78494D7CE5A31D84CF6F648F14042016A20478F8B872E3D277D64
SHA-512:	52A057CCB45B9068094AE4F95E431445439145576D94FFE4AA884B157ED8E77182A04EADA29B642E529EA2929C57F32D7396F14EDA31E9EB3A321AFD01CE1D0I
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/discover/templates/media_1e13cbc31404e8b28464e9b87cd8a6537e45b579d.png?width=2000&format=webply&optimize=medium

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_1e13cbc31404e8b28464e9b87cd8a6537e45b579d[1].png	
Preview:	RIFF.)..WEBPVP8 .)..... *..k.>u6.H$."!%t<`...in.|.q....\...._.....(.....).....B{#.'.....6.).....?..|.b.Q.3.w..`/V~o....."..?...._.~.....'.?.?....>.....G...7.....?A.....?...?....I....?...t....&.....mG'...r{.mG'.s....'X..;....%I.r....|+A.|Bf..../R....:....~..&WM.v.....g....9..j&.....\W..3b.RRs..".rt.F$/..o.x..\....e...k..Xj...}7..<2.....h..L?L.NZ.n..>.C...oG.....`lA.....'.....%1^OO.M..-..x.!.H..W5....^.....s....d)gcuo.....u....Q.q..c.(..."@...0.P.....Z.r.k.....]..=.9.y1.....q.i%4#..|...#.....\.G..<...]N.....b.o..\.m...'Z.....>....VR...K.Yt=}a/..h../<R...|!.....O..Yo.....0=...#.....?.>....A.].yo.;..Z/.....a..l".1..=#=3.....Q....Lm D.F5+...Z.(H,[Y+cw.J....`.|F.-...L.Q..S:..[.Z+..0....[.g.\`..!.A.k,...M..`...H...w.%..O'....5.7...h.|..5)S.+...l.Vw..I.....&.....<.p.{.b....b..0... .0.K...N....^R.L.M...Q?...b.pl.....!*.#.^...)A.....km..8..P*.e<.....p?.~..s.....q.t....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_1e440d4fb87a5de1b4b6ff51b1ae37a2f63c40817[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[none]x[none], YUV color, decoders should clamp
Category:	downloaded
Size (bytes):	6918
Entropy (8bit):	7.965893688722397
Encrypted:	false
SSDEEP:	192:e3kbQR0EMN6e1kZc9USUPzFQ9rR5OIMElmLoJvD:SSQfMN62SU1UEjOIMEU4vD
MD5:	D7DC11770DECBFB1E45B3EC05827E4C3
SHA1:	26D620C35237CB9FC1A8673DB04CEC7A233FECC5
SHA-256:	2099419132AE52EA9AC501D2AFA724D23040657132D71B41859DE5F159A333D3
SHA-512:	B6048EE14D79432043EB4A42DD354F5C597E7C7DC9A8186BEC6F896356DB83EDDC59C346A519DCF6BA9675F8B01AA95AC5C1379AD9FCE3072E77871F7283B09
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/discover/templates/media_1e440d4fb87a5de1b4b6ff51b1ae37a2f63c40817.png?width=2000&format=webply&optimize=medium
Preview:	RIFF....WEBPVP8 ....0t...*..k.>u8.I$."!#.Jh...in.q1.....I...&...U..n...G....3..._._.....=.?(.....;x.....}+.....L.....?..o.v.....?.....K.....W..._..$?....h.s._./.....x.....q....F;..i._....W8.{.g?..b+..uup.....b.....c....$..w...../....eD.7..$.x`yA..i....K.-.3.t..D..k..(.3~...;..;Br.S.....>....&#F.EW0(.h.K1sN..5.....!~@..*...4....2].y..:..`.....^.D.....4.0...K.0..N84..w....Nh.5..d.qL..r...o{...*...#F#Y.Fi.DY.@o.....u.-QYq..n...}.q.....t.J.'Z8l...?`Q.....D..^..I....(V.u.-V...|..jvH.+i...._...V...bm.....~..Y.57.....Q.....<..7....$... ..3..Q.+.}n..k.R.3..]..p.TzN.!..y6.g...d.....L.....Y.+..Z'ElrA:4F..l}.\..>.....j.a.u...#7.....(+.5d.#..$...;K....3.rq.....K.2.U.f.%e@3.....0.....Pa..k.$..-...$.qF3.m..b3=.8...x...$....t[x/r...G.b..0.]..L.w....{09.k..'.....X >3..Tb...G....."....#.d..$...+"2c...7W7..[.b+..us~..... .uu..WL6.....A.....H8.\.....T.....k...<B...|.N.~p|W.2.....t.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_1ed4c2a2a5130e5f9cdeed32b1221f2e7d8988f38[1].jpeg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[none]x[none], YUV color, decoders should clamp
Category:	dropped
Size (bytes):	1413
Entropy (8bit):	7.8153996249014135
Encrypted:	false
SSDEEP:	24:E5nfNbY9lnUtqZobnF6AqQRTc4AiITMLUB9qbQxOJ5yjFKuxOAIij9LJDz/w:EEHnh2D46JoB9jFnDIw95s
MD5:	5B0FB730393BAD86F5EE64CB3DFE0216
SHA1:	DB6198B900F584A0799257E73BE89E97B43FA672
SHA-256:	39B52E904CCFB3BCE1CD485816D53B6F82BEBCCC69F6DEBC6D6B4B249CD9CC44
SHA-512:	23089FFB40ACB372AFD2ADFA2CE42D8D9B808B748DE55A9F8FBD1907280D2841BCFF3380B82D2F5C3BA5A42CC354FA89EAA5922B6BD262D0B7C74832FF0DA81C
Malicious:	false
Reputation:	low
Preview:	RIFF:...WEBPVP8 .....S...*....>u6.H$..!&.Y....cn.s....Ys...[..f.p..l....v..9.I.....7.?.y.f.....~[.....%._.....C..._.>.w..P/.....-/.....F...o.....?Z..y_..x.....O.....?.....q...O.....t...=..FF...A##x.i.....fy.{.'.<....#..a....{.+...0.....g..m.F..}.t.Q...z\;.aYq... *H..-s.l.}P.5.#.R.3P....!.?...O.e;1..&H...B....CE?..k.i.....X..._#.}'....zF.p.gqL.CY?...u.8..4...;d,g...t52..f..KEt.....5..m..._.p.X....6G&.....".X)..X...u.".-R_..O..?!..S.4.hd..F..i^_?..P...b..>.k.....Zh.....C-..2U@,.Y...eaM.....0....0..\....."5't..3...1....s.Sq.Y.2..c....0.....,m.....q,..H+i.O\L.J=.....~.6N.h...I.....>.j.{.d..5y..... .....$.m.BH.[+...R.}.Y+..iq6..T.s9..t.Cd)B*.>...z..p.R...Lh.....1.T.|.)K...8.F.~....~|h..@..`..&]w...M$.....".8.S.W..I.h..Y^.....Uf...l.a.vL...J.9...[+....-.s.....{...sw....z.PqqL..M....df.....%.-+m..AR.T..".S.Q...mF.:z...u%.....Qi..D...~.@>..$.i.eA.....=TjE.`-...Lz.....h.x.f..p.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_1f32be53e4c9aae4eb853ad4ef058c861bf97a4d6[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[none]x[none], YUV color, decoders should clamp
Category:	downloaded
Size (bytes):	11276
Entropy (8bit):	7.9790117603386275
Encrypted:	false
SSDEEP:	192:2OTQJTnQ9n/BDxo9OwZHYe0AlL0H//BMf0FjyaOUW1Vx36FhfFEzsFhUxLAZKpQn:pQTnQ9nvKO+Yex2Mf0xaVxKF1Kyg8ZKC
MD5:	977D1B0648E51CF1E42BC2C3925CB52E
SHA1:	351AF416E28BF5BC432716AE38A29E3D0A9D016C
SHA-256:	CC05CF4045127362307390389 81A9FA6D987AAC4C5A71EDA0C0852236CEA96FA
SHA-512:	7A2510489FCBC36F397AF94FEF0D25395F5EB64C5C7AC4D49AAE97BA181ABB2F3D8AF501A91B27D7ED34A31764DB7A7C1FA223681ACE26ACDECDA8686556AAF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/discover/templates/media_1f32be53e4c9aae4eb853ad4ef058c861bf97a4d6.png?width=2000&format=webply&optimize=medium

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_1f32be53e4c9aae4eb853ad4ef058c861bf97a4d6[1].png	
Preview:	RIFF.,..WEBPVP8 .+..p....*..k.>u6.H$."!&.....in.B....9..Q...<...K.....}'..._..#x?.....z.A.....t.....Oy.....?...z.....?R.....o..{.t....^....g....f.....g.?.~....._...y.}....O...o..?....k.o...<....[.?.... ..?....%.....2...X..}].cZY.!...f9.b..e.....I....G+..F....c..55.r.U.<.D.yy....N.^....Lv..h.....,.7W.....).d)Pf.0(.....4.....S..\|hF..Q..+.m..Z.Z...w 5.M.....ZM'..i.{.o..O..c.....*...8..MBt.`k..E..Y..Jl)y.."..a"E.b.>...}c....R.D.....^....w....\rpDd...f+...~....^'f.$c&..%5.....).h.:..b"...A.....q..:.50....d..i3.....[..:.j0...V.w..#..X.v.z...l....a.m.y...GZ.;..(...V.....}..t,.....H8...g6..h..W^."........^.0..4.7r...|.....L.....\...%.Qv.nl1..b9K.y0idg..^..U..h.Y...?...|.w.%..GW>.....,..$E..$p.R.....5.o.?....1.Hq.'.C.fE.i...zNc.\p.....co.Ee...n.R3:F./.P....do.....U,...t..i.AZIP#.#..T..p..#.>....`9...#..d./vM[..EE..t.9Dm).@.....oj..j.8ZU."..M8.2.yj...>ix....d2...%....?1..O...Bf.?..Z.}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\noscript.gz[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	6887
Entropy (8bit):	4.668876157824901
Encrypted:	false
SSDEEP:	96:/SIxZvVJlZiK1ia87ErUiLJgMio6VLtXq+eoIk/QDasFJ+kIB+oldfWJgYb4d3M:PuYiBtXjevaQDaElJgn
MD5:	BAA266F5BD7729A2ED64E929B835083A
SHA1:	6388FF647E1F0FC306C8CDA8765D90109A26DF15
SHA-256:	858FDF50C5FC5B2E92A07EBC4EE0ACA98BB5518455080ADAF3F1CD62575526EF
SHA-512:	E7DEF66977E5E95FD1F28F0CF680FE783F217E3A6BEE7285E0FC4855FA2632517D1B5E232A8698509B6DBE23B8FBD1B02ACA32169442308103E31373E3349ADB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://page.adobespark-assets.com/runtime/1.22/noscript.gz.css
Preview:	.article,.publication-viewer,.section,.wp-swipe-panel-group{overflow:visible!important}#luca-splash{display:none}.wp-swipe-panel-group-panel{display:block!important;overflow:visible!important;visibility:visible!important;-webkit-transform:none!important;-moz-transform:none!important;-o-transform:none!important;-ms-transform:none!important;transform:none!important}.section{visibility:visible!important;position:relative!important;top:auto!important;right:auto!important;bottom:auto!important;left:auto!important;max-height:none!important;box-sizing:border-box}.title-section{height:80%!important}.title-section *{-webkit-transform:none!important;-moz-transform:none!important;-o-transform:none!important;-ms-transform:none!important;transform:none!important}.title-section .title-header{overflow:hidden}.single-column-section{height:auto!important}.single-column-section .section-background{position:static!important;width:100%;height:50vh}.section-background{z-index:0!important}.fullscreen-photo-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\office3651[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 187 x 188, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	18025
Entropy (8bit):	3.011161251318808
Encrypted:	false
SSDEEP:	96:2S+WvkiqJq6Uq7NXrNG+GHhsc5yeFZV9D2Ydcx/NTV0K0VFDsCmm:2SJkiOq6Uq75shDs1kFP
MD5:	FE22440D79FFA34950F512EF4A718B2A
SHA1:	0E147E59544EE6580D3095353D4420849FA5EB8A
SHA-256:	A2F26B68A6C8810C1AEB4048C938F835A86BA83756A7A440F989B967E78F3BA8
SHA-512:	64218ECD4140DC05E50EB7BA4C9813794B8B5A4310C8308244205BA6ADA8EE7C2D1840121730A00800E41775241D8AFA02125A966064CD0EB2CC7D3E4605B81
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://nicklaussglen.buzz/011/images/office3651.png
Preview:	.PNG.....IHDR..... .....pHYs.....<eiTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?>.<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c067 79.157747, 2015/03/30-23:40:42 ">. <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">. <rdf:Description rdf:about="". xmlns:xmp="http://ns.adobe.com/xap/1.0/". xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/". xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#". xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/". xmlns:dc="http://purl.org/dc/elements/1.1/". xmlns:tiff="http://ns.adobe.com/tiff/1.0/". xmlns:exif="http://ns.adobe.com/exif/1.0/">. <xmp:CreatorTool>Adobe Photoshop CC 2015 (Windows)</xmp:CreatorTool>. <xmp:CreateDate>2020-01-18T21:49:38+05:00</xmp:CreateDate>. <xmp:MetadataDate>2020-01-21T14:30:14+05:00</xmp:MetadataDate>. <x

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\other1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 190 x 187, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	21882
Entropy (8bit):	4.268463452779894
Encrypted:	false
SSDEEP:	192:ESCkiDw7e9Mg/wio0EYm9FWyo2XdJfXoOZdEDfmiIJQdiRVi/WTanY:DBiDw7eAdq+FWyo2/fXoZbDIJ0ci/BnY
MD5:	6843A244E12FAB158AA189680B5E7049
SHA1:	0E1C691F87CC4FA35C88344974F2829C40176B70
SHA-256:	3A9B144D6482B78AFC4E0A940A1D3C22240F14FA535B808CF4DAB9635339569F
SHA-512:	145010C45B6B83EA4005EB367C0507959FF0817E482F19E9973504081ACAE1B7827CBD1172CEC7732B13F4E0CEC058271BD6700444FBCF61FB6A3C068A3744C4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://nicklaussglen.buzz/011/images/other1.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\other1[1].png	
Preview:	.PNG.....IHDR.....$.... cHRM..z&.....u0...`..:....p..Q<....sRGB.....gAMA.....a.....pHYs.....:.iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?>.<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c067 79.157747, 2015/03/30-23:40:42 ">. <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">. <rdf:Description rdf:about="". xmlns:xmp="http://ns.adobe.com/xap/1.0/". xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/". xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#". xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/". xmlns:dc="http://purl.org/dc/elements/1.1/". xmlns:tiff="http://ns.adobe.com/tiff/1.0/". xmlns:exif="http://ns.adobe.com/exif/1.0/">. <xmp:CreatorTool>Adobe Photoshop CC 2015 (Windows)</xmp:CreatorTool>. <xmp:CreateDate>2020-01-18T21:59:57+05:00</xmp:CreateDate>. <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\outlook1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 26 x 26, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	771
Entropy (8bit):	7.682244426935498
Encrypted:	false
SSDEEP:	24:74yiH9yQmOntihdLl00qDeu1BcaDa0oljZG0:omOntO7v/uJDYG0
MD5:	C3FC46C5799C76F9107504028F39190F
SHA1:	519096AD3F03410CF9CE3C9B9FCCA6B439D97B23
SHA-256:	57898461712A639D119BDF88B7145919DCC8956C7A271D2E4A1084B29EAE6785
SHA-512:	DF4A0A2F78B2013035FB738BF405119B275D4CFEC31A23071EB9AF499D5F31FDC4BE22754CE791C975D7D417E908B5CAD16F962B0ADD3DFDCDE19844D74F668
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://nicklaussglen.buzz/011/images/outlook1.png
Preview:	.PNG.....IHDR.....JL.....bKGD.....IDATH....k.A..k6.b.F1..H@...j@.aQ...(.. .. .. .A..D...I.....E.....1...W...;;.Y.d.}].U5]..x"3?....!..A..y..+R2\...m.NX.=..p.0...d.^.3.....J.Z.X.).....P\..x1.3.M.0....m.....F....?...n.....I.Fo)x._ R|.s..a.T?...?.=.9.Y..u....z..|.....Wz...h..<..P.. ...$.Y.....k`/4.y/.....L.C.....".....U....7....G...'h.....1j1E..%t.....@..a.....b.ED-.Tn.<..o.D...o..(.{1l>.....".4a.:k.l./.7t./.Q-'..>.. .....'3eb..d.@=4...C....A...;..N.X3.(.....,v...+...S...W..l...@,...j.).u<..@u..0...V&.b.yp.....0..o.?..V..B =.~&m"r(...6;EP.T.....h.m".[f.U)|t..2.Q.....g.cP.W...D..[.O>..d;.yI.{/..#v._..$.Q.....t\E..5i.q._.."/n...v.w..Uo ...#..S....^.....F..+._??.r.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\p[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	35
Entropy (8bit):	2.9302005337813077
Encrypted:	false
SSDEEP:	3:CUHaaatrllH5:aB
MD5:	81144D75B3E69E9AA2FA3E9D83A64D03
SHA1:	F0FBC60B50EDF5B2A0B76E0AA0537B76BF346FFC
SHA-256:	9B9265C69A5CC295D1AB0D04E0273B3677DB1A6216CE2CCF4EFC8C277ED84B39
SHA-512:	2D073E10AE40FDE434EB31CBEDD581A35CD763E51FB7048B88CAA5F949B1E6105E37A228C235BC8976E8DB58ED22149CFCCF83B40CE93A28390566A2897574A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://p.typekit.net/p.gif?s=1&k=rbi5aua&ht=tk&h=spark.adobe.com&f=171.172.173.174.175.176.5474.5475.146&a=1655249&js=1.20.0&app=typekit&e=js&_=1618038814081
Preview:	GIF89a.....,.....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\p[2].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	35
Entropy (8bit):	2.9302005337813077
Encrypted:	false
SSDEEP:	3:CUHaaatrllH5:aB
MD5:	81144D75B3E69E9AA2FA3E9D83A64D03
SHA1:	F0FBC60B50EDF5B2A0B76E0AA0537B76BF346FFC
SHA-256:	9B9265C69A5CC295D1AB0D04E0273B3677DB1A6216CE2CCF4EFC8C277ED84B39
SHA-512:	2D073E10AE40FDE434EB31CBEDD581A35CD763E51FB7048B88CAA5F949B1E6105E37A228C235BC8976E8DB58ED22149CFCCF83B40CE93A28390566A2897574A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://p.typekit.net/p.gif?s=1&k=rbi5aua&ht=tk&h=spark.adobe.com&f=171.172.173.174.175.176.5474.5475.146&a=1655249&js=1.20.0&app=typekit&e=js&_=1618038832651
Preview:	GIF89a.....,.....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\p[3].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	35
Entropy (8bit):	2.9302005337813077
Encrypted:	false
SSDEEP:	3:CUHaaatrllH5:aB
MD5:	81144D75B3E69E9AA2FA3E9D83A64D03
SHA1:	F0FBC60B50EDF5B2A0B76E0AA0537B76BF346FFC
SHA-256:	9B9265C69A5CC295D1AB0D04E0273B3677DB1A6216CE2CCF4EFC8C277ED84B39
SHA-512:	2D073E10AE40FDE434EB31CBEDD581A35CD763E51FB7048B88CAA5F949B1E6105E37A228C235BC8976E8DB58ED22149CFCCF83B40CE93A28390566A2897574A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://p.typekit.net/p.gif?s=1&k=vtg4qoo&ht=tk&h=spark.adobe.com&f=7180.7182.7184.22474.10294.10296.10302&a=1655249&js=1.20.0&app=typekit&e=js&_=1618038858481
Preview:	GIF89a.....,.....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\pps7abe[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	5912
Entropy (8bit):	5.2044956005117
Encrypted:	false
SSDEEP:	96:pbzQ2hl0RMFRioMWznrvMmMoZS6MaJ6QMbxkbMy9cRMxRqkM8c:pjl0RMFRioMWznrvMmMoZS6MaJ6QMbx9
MD5:	6FEB771900764877F9ED7FCCCC9428B5
SHA1:	31693DA6584BC9FAB601AFC35550AEEE6A8210C1
SHA-256:	3AC4CEB0885F766CF6E170BA7191315EA1C54287BF0947095E85D1B090A1BC35
SHA-512:	890E633998C812A19B63947F922815E14632328A9522AEBF5AFDA87D947684130C643EA48BF21124564F4DC17936DDC0F9F3907BA61594D197A797E5160B145E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/pps7abe.css
Preview:	/*. * The Typekit service used to deliver this font or fonts for use on websites. * is provided by Adobe and is subject to these Terms of Use. * http://www.adobe.com/products/eulas/tou_typekit. For font license. * information, see the list below.. *. * adobe-clean:. * - http://typekit.com/eulas/00000000000000003b9b3f85. * - http://typekit.com/eulas/00000000000000003b9b3f86. * - http://typekit.com/eulas/00000000000000003b9b3f88. * - http://typekit.com/eulas/00000000000000003b9b3f83. * - http://typekit.com/eulas/00000000000000003b9b3f8c. * - http://typekit.com/eulas/00000000000000003b9b3f84. * adobe-clean-serif:. * - http://typekit.com/eulas/00000000000000003b9aee45. * - http://typekit.com/eulas/00000000000000003b9aee47. *. * . 2009-2021 Adobe Systems Incorporated. All Rights Reserved.. */*{"last_published":"2020-01-31 14:53:09 UTC"}*/..@font-face {.font-family:"adobe-clean";.src:url("https://use.typekit.net/af/b0c5f5/00000000000000003b9b3f85/27/l?primer=388f68b35a7cbf

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\privacy-localnav[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	30599
Entropy (8bit):	4.9551477703426805
Encrypted:	false
SSDEEP:	768:Upy3EoluYZ9bY/MKOIoLmsLafZWlIWJal0J4WWn1l8T7aqfVjDWLXPIXeJPoRhxi:Upy3E73
MD5:	0953DE6B289FE2C3F316C80777DFB46B
SHA1:	BDE2E330A8D05407AC90AD37E340EFDA4B7AF263
SHA-256:	E3AAE23645D396553DB415747BD46C84B58A6793A8CF0225B63EF214108906DD
SHA-512:	5A16FC6A9C9842DCDC66517845866BEC2B4B3236E69B669C5041E3348B37A22EB1C365063465DF7843536B1C48D35304C8C5B046C4DD567DCB7A9273D593271
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/services/feds.res_1.css/head/en/acom/corporate-mega-menu/privacy-localnav.css
Preview:	/*! applauncher v0.47.0 built on Tue, 30 Mar 2021 10:12:15 GMT */.#feds-header .applauncher-element{display:none}@media screen and (min-width:600px){#feds-header .applauncher-element{display:flex}}#feds-header .applauncher-element .app-launcher-container{display:flex;align-items:center}#feds-header .applauncher-element .app-launcher-container .react-spectrum-provider{position:static}html[dir=rtl] #feds-header .applauncher-element{display:none}#feds-header .feds-appLauncher .app-launcher-overlay-container{top:0!important;left:0!important;right:0;width:auto}#feds-header .feds-appLauncher .app-launcher-popover{border-top-left-radius:0;border-top-right-radius:0;border-bottom-left-radius:4px;border-bottom-right-radius:4px;overflow:hidden}#feds-header .feds-appLauncher .spectrum-Popover-tip{display:none}#feds-header .feds-appLauncher.feds-focus-ring .app-launcher-icon{outline:none}@media screen and (min-width:1200px){#feds-header .feds-appLauncher.feds-focus-ring .app-launcher-icon{outline:2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\publish.combined.fp-edc06d2196a984377367d5bc5109f275[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\publish.combined.fp-edc06d2196a984377367d5bc5109f275[1].js	
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	716923
Entropy (8bit):	5.322748650665996
Encrypted:	false
SSDEEP:	12288:LmwBfrrsdDBry0dllnRdlln8dllnrdlln7H1urS2dllnrdllnTdllnGdllnPCrVZ:LmSfrrsdDBry0dllnRdlln8dllnrdllQ
MD5:	EDC06D2196A984377367D5BC5109F275
SHA1:	C3BE0A142BF87554AAD66BF3B666001377CEB2FD
SHA-256:	C90E4AF1B67FF9A0887FB7C870068053685E677760BD963DCFB45F3ACCD6097D
SHA-512:	CE8F10DF6293078994D4105E3E90FF812F826FFF85573C8094EAB5029348560A7EAD017DA96DA19775E4FB39A448B5AFA786F97D51AF62E2E7D243AB6AA576E8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/etc.hawks.dexterlibs/hawks/clientlibs/publish.combined.fp-edc06d2196a984377367d5bc5109f275.js
Preview:	webpackJsonp([1],{113:function(e,t,n){"use strict";Object.defineProperty(t,"__esModule",{value:!0});var i=function(){function e(e,t){for(var n=0;n<t.length;n++){var i=t[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(e,i.key,i)}}return function(t,n,i){return n&&e(t.prototype,n),i&&e(t,i),t}}(),r=u(n(126)),a=u(n(185)),o=u(n(439));function u(e){return e&&e.__esModule?e:{default:e}}var s=function(){function e(t){var n=arguments.length>1&&void 0!==arguments[1]?arguments[1]:{};!function(e,t){if(!(e instanceof t))throw new TypeError("Cannot call a class as a function")}(this,e),this.element=t,this.utils=o.default,this.properties=n,this.tools=r.default}return i(e,[{key:"bindCollection",value:function(t,n){for(var i=arguments.length,r=Array(i>2?i-2:0),o=2;o<i;o++)r[o-2]=arguments[o];var u=e.getCollection(t,this.element);if(r.includes("bindLateItems")){var s=r.filter(function(e){return"bindLateItems"!==e});this.bindOn.apply(this,[t,n].concat

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\rbi5aua[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):	19114
Entropy (8bit):	5.570400661578598
Encrypted:	false
SSDEEP:	384:KefQe2tpIgIPs51iRm2Ilew42noFeFsP9btiCtpIaCR:NQMq1iRm2XwMqsbbt6J
MD5:	D464D0A61D4E34F4C431CA31D0F7E6E8
SHA1:	73716727BFD77BA586E907A9FFC33FFC39CA73BF
SHA-256:	29B51B31FAF8A954EC0209189E1A6491AFE94CBE50D1E16679FBA7561AD2BC5C
SHA-512:	9B6FB7EBF94F0B42242A335B72B0C6A43DA7071B6AE9715FF70F96D54A4CA157D16A6F11B7D4C3573053E96DE06DD30791AB655BD55EEB5F3FB68989C3CB8B6D
Malicious:	false
Reputation:	low
Preview:	/*. * The Typekit service used to deliver this font or fonts for use on websites. * is provided by Adobe and is subject to these Terms of Use. * http://www.adobe.com/products/eulas/tou_typekit. For font license. * information, see the list below.. *. * proxima-nova:. * - http://typekit.com/eulas/000000000000000000158d3. * - http://typekit.com/eulas/000000000000000000158d4. * - http://typekit.com/eulas/0000000000000000017709. * - http://typekit.com/eulas/000000000000000000158d6. * - http://typekit.com/eulas/000000000000000000158d7. * - http://typekit.com/eulas/000000000000000000158d8. * - http://typekit.com/eulas/000000000000000000158d9. * - http://typekit.com/eulas/00000000000000000001705b. * proxima-nova-condensed:. * - http://typekit.com/eulas/00000000000000000000ffd9. *. * . 2009-2021 Adobe Systems Incorporated. All Rights Reserved.. */.if(!window.Typekit)window.Typekit={};window.Typekit.config={"a":"1655249","c":[".tk-proxima-nova","\"proxima-nova\",sans-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\scripts[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text
Category:	downloaded
Size (bytes):	35151
Entropy (8bit):	5.025822397210971
Encrypted:	false
SSDEEP:	384:U11VZSpe137a6wbqWcqS5G399ahvLAUawwbGuv3fKntOX4jQt41gvUxUPC90xb3V:UlZPjwfuLPeLvea4jexbyg
MD5:	E1E284BDDFFA22C71EF3AF64649557FF
SHA1:	07D194854C61E7F989749F5DD3F242A55570A9E0
SHA-256:	64C6F06F308ACFC0B8BAC69A181A847D2D9374E700B192382ADFE5FF178558F2
SHA-512:	3422E8037F9A7E90010923456D7CF3AC49F82E7C89F104C5755ADCE145C0B1C29C9743B0B1D1A747134647573E5FA6AF4D99C25A33B507369C893ACBFE58F457
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/scripts/scripts.js
Preview:	/*. * Copyright 2021 Adobe. All rights reserved.. * This file is licensed to you under the Apache License, Version 2.0 (the "License");. * you may not use this file except in compliance with the License. You may obtain a copy. * of the License at http://www.apache.org/licenses/LICENSE-2.0. *. * Unless required by applicable law or agreed to in writing, software distributed under. * the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR REPRESENTATIONS. * OF ANY KIND, either express or implied. See the License for the specific language. * governing permissions and limitations under the License.. */.* global window, navigator, document, fetch, performance, PerformanceObserver,. FontFace, sessionStorage */./* eslint-disable no-console */..export function toClassName(name) {. return name && typeof name === 'string'. ? name.toLowerCase().replace(/[^0-9a-z]/gi, '-'). : '';.}..export function createTag(name, attrs) {. const el = document.createElement(name);. if (ty

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\spark[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\spark[1].svg	
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	3245
Entropy (8bit):	5.201590437010129
Encrypted:	false
SSDEEP:	96:EOjZfymEL6GBGTGGcnxv1U9KByhSl+x4rvdk6:Hj1yR6GBh1ChSQSLy6
MD5:	907B6C4171506C79784218007A40BA44
SHA1:	439E9CAF7CDC5B93A3CA412EC4EDA6338997644A
SHA-256:	AC0A282DCE35E91B761D9E69142973C44CD495E468434DCF1AD249F498D00788
SHA-512:	BD968C37D67A94827BF555E5A013A45CECB0DEC045815B00091FC8BF4B9F0F32064F9ED8395D3D7A625BD287D462EA271834E65D9886EA436029045DEEEC0A4
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>. Generator: Adobe Illustrator 23.0.1, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->.<!DOCTYPE svg PUBLIC "-//W3C //DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd" [..<!ENTITY ns_extend "http://ns.adobe.com/Extensibility/1.0/">..<!ENTITY ns_ai "http://ns .adobe.com/AdobeIllustrator/10.0/">..<!ENTITY ns_graphs "http://ns.adobe.com/Graphs/1.0/">..<!ENTITY ns_vars "http://ns.adobe.com/Variables/1.0/">..<!ENTITY ns_ imrep "http://ns.adobe.com/ImageReplacement/1.0/">..<!ENTITY ns_sfw "http://ns.adobe.com/SaveForWeb/1.0/">..<!ENTITY ns_custom "http://ns.adobe.com/Ge nericCustomNamespace/1.0/">..<!ENTITY ns_adobe_xpath "http://ns.adobe.com/XPath/1.0/">.]>.<svg version="1.1" id="Livello_1" xmlns:x="&ns_extend;" xmlns:i="&ns_a i;" xmlns:graph="&ns_graphs;".. xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" viewBox="0 0 240 234".. style="enable-background:new 0 0 240 234;" xml:space="pres

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\spark_app_white@2x[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1518
Entropy (8bit):	5.00107238377263
Encrypted:	false
SSDEEP:	24:2dfkATLf3+sZ1enVMeN2zQH9nMZ2x0gWXNdIjNN4iWbJ7oIa6d06+:cfkAvfOsZ1302zUj+Td1b+Iaim
MD5:	A29E0C074D7C5E3F6A54CE20C5FEA0AF
SHA1:	8563F7581C1939067B4AA354E78341BC46BD9E1D
SHA-256:	511C77BD64C8D67BE5FC38F107B5005F32F38386A8142CE13753EDABEDD50B86
SHA-512:	50DAC8A1C88FF4369B3199091AC273A4EC482C9C944A4A93DAAF5885C30B30A96469826BE11AAAA890F5393E08FD9CA809AF9E92A836DAC40CB722C13D1E0A0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://page.adobespark-assets.com/runtime/1.22/images/spark_app_white@2x.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>. Generator: Adobe Illustrator 21.1.0, 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="66px" height="64px" viewBox="0 0 66 64" style="enable-background:new 0 0 66 64;" xml:space="preserve">.<style type="text/css">...st0{fill:none;}...st1{fill:#FFFFFF;}.</style>.<path class="st0" d="M14,62C7.4,62,2,56.6,2,50V14C2,7.4,7.4,2,14,2h38c6.6,0,12,5.4,12,12v36c0,6.6-5.4,12-12,12H14z"/>.<path class="st1" d="M52,4c5.5,0,10,4.5,10,10v36c0,5.5-4.5,10-10,10H14C8.5,60,4,55.5,4,50V14C4,8.5,8.5,4,14,4H52 M52,0H14..C6.3,0,0,6.3,0,14v36c0,7.7,6.3,14,14,14h38c7.7,0,14-6.3,14-14V14C66,6.3,59.7,0,52,0L52,0z"/>.<path class="st1" d="M15.1,42.3C14.9,42.2,15,42,15,41.8v-4.2c0-0.1,0-0.3,0.2-0.1c2,1.4,4.1,2,6.4,2c3.2,0,4.5-1.7,4.5-3.6..c0-1.7-0.9-3-3.9-4.8l-1.6-0.8c-4.5-2.5-5.9-5.1-5.9-8.5c0-4.5,3.1-8.1,9-8.1c2.6,0,4.8,0.4,5.9,1c0.2,0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\spark_logo_v2[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	2146
Entropy (8bit):	4.6117195503782
Encrypted:	false
SSDEEP:	48:Cl5MbaB081uNPETSn63o902pBDpxnzJ8bXUJnQ:8Kf84JEmuEBD3nKmQ
MD5:	7AAAA0B29E8320F055FCB0A8D8A9686C
SHA1:	812CEB49C501F9EB444AF3C8DE86D6B61D052024
SHA-256:	00E24734BE21E153DCE4E51E078A05D9A191EA74185D225C4A27B4434E7A0578
SHA-512:	C3456DFF9ACB7C31CD886866EF1E2EBFC3E950DE77E1785F644F8713C89426AE6FBB7F14A1880805A5DCF8C8327FD4DE4ADB07510537E0436B007C7A9E27B92D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s3.amazonaws.com/adobe-luca-prod-ue1-assets/experiments/chrome/images/spark_logo_v2.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 56 54" width="56px" height="54px"><defs><style>.cls-1{fill:#370000;}.cls-2{fill:#fa0f00;}</style></defs><g id="Layer_2" data-name="Layer 2"><g id="Surfaces"><g id="Spark_Surface" data-name="Spark Surface"><g id="Outline_no_shadow" data-name="Outline no shadow"><rect class="cls-1" width="56" height="54" rx="9.91"/></g></g></g><g id="Outlined_Mnemonics_Logos" data-name="Outlined Mnemonics & Logos"><g id="Sp"><path class="cls-2" d="M18.05,38.37A18.68,18.68,0,0,1,14.3,38a12.08,12.08,0,0,1-2.83-.91c-.2-.09-.3-.3-.3-.62V32.35a.22.22,0,0,1,.09-.2.25.25,0,0,1,.25,0,11.84,11.84,0,0,0,3.29,1.17,12.74,12.74,0,0,0,3.4.48,5.28,5.28,0,0,0,3-.65,1.91,1.91,0,0,0,.9-1.61,2.13,2.13,0,0,0-.29-1.12,3.1,3.1,0,0,0-1-1,11.61,11.61,0,0,0-2-1l-1.85-.78a13.89,13.89,0,0,1-3.54-2.05,6,6,0,0,1-1.75-2.35,7.53,7.53,0,0,1-.49-2.7,6.64,6.64,0,0,1,4-6.2,11.25,11.25,0,0,1,4.89-1,22.84,22.84,0,0,1,3.31.23,7.22,7.22,0,0,1,2.39.71.52.52,0,0,1,.26.48v3.89c0,.05,0,.1-.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sparkfavicon_v2[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 32x32, 32 bits/pixel
Category:	downloaded
Size (bytes):	4286
Entropy (8bit):	2.2437058322637595
Encrypted:	false
SSDEEP:	24:suZgizzxxEKfLOQQEsmcpG3xbWT//zvUUUUUUUUUUUUUUUUUUUUUUUNl:HgizzxxEKzOQBbcpS5WT//zVl
MD5:	79FBE30FC79A42EAA8A32DC344959E0E
SHA1:	09AC6EE75F9686BAD2003926C5FA8DB80777E981
SHA-256:	01F2FA23190A55B0B5F9DF0E0B66E23D136B7701BA3CC9A71FDAEDD409D92345
SHA-512:	FFCED953A2A53C1370FECE0E366D7AC304ACFFAE6E44F571BD2EFED6E225149647F64704332160AFA8DCD6C946B3AAAA6A80C5BD6900612F56687DC35ED5E 24
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spark.adobe.com/images/sparkfavicon_v2.ico
Preview:	....(... ...@..... ....70..7...7...7...7...7...7...7...7...7...7...7...7...7... 7...7...7...7...7...7...7...7...7...70..............................7`..7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7`......................70..7...7...7...7...7...7... 7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...70..................7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7...7.......... ....7...7...7...7...7...7...7...7...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\styles[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	12469
Entropy (8bit):	4.663480881606783
Encrypted:	false
SSDEEP:	192:wh2WV+m6jCZDitH75vH1V/FAF/1Sr+aGF5OJE9h0TA9Zp:R5171PFAF95bFQ9cp
MD5:	131C2C86572D622090DAA140C41C0461
SHA1:	CBA5ACF41173B2997CE5FA772F7B4A9541D1332F
SHA-256:	5DD382286A66BC807237AE04A6A2A99E9250F6F06DE0BDA8F0D9093476D66C83
SHA-512:	7793CD9D0846E15BBFD82FD278FA880B0563D1E3DC101AD9F63942777608246894A60FBFAE451D6F6BE378B03D0A1F4324D596377CC3B10976459F6AD32051F9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/styles/styles.css
Preview:	body {. font-family: 'adobe-clean', 'Adobe Clean', sans-serif;. background-color: #FFF;. color: #232323;. margin: 0;. padding: 0;. display: none;.}..body.appear { . display: block;.}../* gnav placeholder */..header {. box-sizing: border-box;. border-bottom: 1px solid #EAEAEA;. height: 153px;. background-image: url(/e xpress/icons/adobe-spark.png);. background-repeat: no-repeat;. background-size: auto 42px;. background-position: bottom 24px center;. position: relative;. background-color: white;.}..#feds-header {. opacity: 0;.}..#feds-header.appear {. opacity: 1;.}..#header-placeholder {. height: 64px;. position: absolute;. top: 0;. left: 0;. width: 100%;. z-index: 10;. -webkit-font-smoothing: antialiased;. border-bottom: 1px solid #EAEAEA;. transition: opacity 0.1s;. background-color: white;.}..#header-placeholder.disappear {. display: none;.}..#header-placeholder .desktop {. display: none;.}..#header-placeholder .mobile {.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\vtg4qoo[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):	18975
Entropy (8bit):	5.588875152231931
Encrypted:	false
SSDEEP:	384:bTz4QhLGD8h2tpIgIPs51iRm2lIew42noFeFsP9btiCtpIaCR:vz4QhLA8zq1iRm2XwMqsbbt6J
MD5:	46700293FD68A3707BEAF54E63C4D9A8
SHA1:	5F1130A35AC5C767DF52A13CC14D412B0A1CC0E9
SHA-256:	413B5751660E454D49C8430CBD09054C97E7B0560660B14892FF6048E4CDDE46
SHA-512:	FE06C4159C0968AA5DCB63DEEF234973D8B9F66C54DFCC350FA840072D5DE40F691C05844A5DA4A682F0D2ED2E5FCB90318DCAE981C7A532D2BD9A1FE5887 89
Malicious:	false
Reputation:	low
Preview:	/*. * The Typekit service used to deliver this font or fonts for use on websites. * is provided by Adobe and is subject to these Terms of Use. * http://www.adobe.com/prod ucts/eulas/tou_typekit. For font license. * information, see the list below.. *. * adobe-clean:. * - http://typekit.com/eulas/00000000000000000017701. * - http://typ ekit.com/eulas/00000000000000000017703. * - http://typekit.com/eulas/000000000000000000176ff. * - http://typekit.com/eulas/00000000000000000017706. * bra ndon-grotesque:. * - http://typekit.com/eulas/000000000000000000132df. * - http://typekit.com/eulas/000000000000000000132e3. * - http://typekit.com/eula s/000000000000000000132e1. *. * . 2009-2021 Adobe Systems Incorporated. All Rights Reserved.. */.if(!window.Typekit)window.Typekit={};window.Typekit.config={"a ":"1655249","c":[".tk-adobe-clean","\"adobe-clean\",sans-serif",".tk-brandon-grotesque","\"brandon-grotesque\",sans-serif"],"fi":[7180,7182,7184,22474,10294,10296,10302], "fc":[{"i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\011[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	11777
Entropy (8bit):	4.8159515725639555
Encrypted:	false
SSDEEP:	192:K2FI5vEJKnYmrDfG4RywAOT+UY/t4IdtWPtY:1nmRnAKyt48tZ
MD5:	6D1D3C4FD92B63CC534BE0EDF3AF18DC
SHA1:	5F5442FEB5BE60239F185E969C45050A7DBADE2A
SHA-256:	65ADCB045AEFB4D0028A6AF36EC9D42BBD4DAE9AFF2CF85810BB4A6F44D4B25C
SHA-512:	2D42684CF0A44E262C958172C2446974A4AE9B8D17F7208A5FCB690964EE0D56FEB157B9AB6166B8F94FBDCBA027271C36B66784655E8FD96CE0B5522FE71AA
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\011[1].htm, Author: Joe Security • Rule: JoeSecurity_HtmlPhish_7, Description: Yara detected HtmlPhish_7, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\011[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://nicklaussglen.buzz/011/
Preview:	...<!doctype html>..<html lang="en">..<head>.. <script src="https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>.. <script src="https://code.jquery.com/jquery-3.1.1.min.js">.. <script src="https://code.jquery.com/jquery-3.3.1.js" integrity="sha256-2Kok7MbOyxpgUVvAk/HJ2jigOSYS2auK4Pfzbm7uH60=" crossorigin="anonymous"></script>.. Required meta tags -->.. <meta charset="utf-8">.. <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">.... Bootstrap CSS -->.. <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css" integrity="sha384-Gn5384xqQ1aoWXA+058RXPxPg6fy4IWvTNh0E263XmFcJlSAwiGgFAW/dAiS6JXm" crossorigin="anonymous">.. <link href="https://fonts.googleapis.com/css?family=Yellowtail&display=swap" rel="stylesheet">.. <script src="https://kit.fontawesome.com/585b051251.js" crossorigin="anonymous"></script>.. <title>Share Point Online</title>.. <link

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\7a5eb705-95ed-4cc4-a11d-0cc5760e93db[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	3852
Entropy (8bit):	4.63636203914889
Encrypted:	false
SSDEEP:	96:OyIY40FtdRYzYValJ5GHZa6AyAYV1ej8jVjht4S:iwKzYslJF6vAYV1KMdoS
MD5:	175D27D7EB29846AF4286F09B657FB1B
SHA1:	00E648DBA69CF0C434FE0C74022D75DFABD8DB60
SHA-256:	DE1752B70D9AA03703E70ADC0E343968EBDA9661F3E06D196266DF38B3B72D60
SHA-512:	CA6453449401F922D0AE9D92DCABDC7B61DCB083E589B05F9EEA7B624CBC70E3798A43DB26D6A7C721F48C9A4CB2B163884C59750593060FB701C6975366AC2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.cookielaw.org/consent/7a5eb705-95ed-4cc4-a11d-0cc5760e93db/7a5eb705-95ed-4cc4-a11d-0cc5760e93db.json
Preview:	{"CookieSPAEnabled":false,"MultiVariantTestingEnabled":false,"UseV2":true,"MobileSDK":false,"SkipGeolocation":false,"ScriptType":"PRODUCTION","Version":"6.9.0","OptanonDataJSON":"7a5eb705-95ed-4cc4-a11d-0cc5760e93db","GeolocationUrl":"https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location","RuleSet":[{"Id":"8fc5213e-cec6-4fca-a134-aec9029b0675","Name":"Adobe_EEU_Canada","Countries":["de","no","fi","be","pt","bg","dk","lt","lu","lv","hr","fr","hu","se","si","mc","sk","mf","sm","yt","gb","ie","ca","gf","ee","mq","mt","gp","is","gr","it","es","at","re","cy","cz","ax","pl","ro","li","nl"],"States":{},"LanguageSwitcherPlaceholder":{"no":"no","de":"de","ru":"ru","fi":"fi","pt":"pt","bg":"bg","lt":"lt","lv":"lv","fr":"fr","hu":"hu","zh-Hans":"zh-Hans","default":"en","zh-Hant":"zh-Hant","uk":"uk","sk":"sk","sl":"sl","sv":"sv","ko":"ko","zh-TW":"zh-TW","zh-HK":"zh-HK","pt-BR":"pt-BR","it":"it","es":"es","zh":"zh","et":"et","cs":"cs","ar":"ar","ja":"ja","pl":"pl","ro":"ro","he":"he","

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Adobe_Corporate_Horizontal_Red_HEX[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	397
Entropy (8bit):	4.973746262232231
Encrypted:	false
SSDEEP:	6:tvKIiad4mc4sl3UtpMaguk0BNbO9Z1PHtDjt9INFW39mmJEVitksmHSXqY:tvG1KWanstDjXI4mwIUmyX7
MD5:	4BC0619E030E91ACFDA414626A41B770
SHA1:	BF0BEA50B7C0092B34EB8C06A3DDB52F37AA1860
SHA-256:	57AEBAB4A35ADC7CA5DFA15DC58A19B1457FB314881C3A4CC320CB79E8F006ED
SHA-512:	CF614C4A5C8269F4DCF01694BE15B847783DE0E6CADC914C879C46F6C4B014AF30FD4FA64F27144BA0CFB0F921E8D15BA592147AA0CE29440A18081AD9A69F4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/content/dam/cc/icons/Adobe_Corporate_Horizontal_Red_HEX.svg
Preview:	<svg id="Layer_1" data-name="Layer 1" xmlns="http://www.w3.org/2000/svg" viewBox="0 0 133.46 118.11"><defs><style>.cls-1{fill:#fa0f00;}</style></defs><polygon class="cls-1" points="84.13 0 133.46 0 133.46 118.11 84.13 0"/><polygon class="cls-1" points="49.37 0 0 0 0 118.11 49.37 0"/><polygon class="cls-1" points="66.75 43.53 98.18 118.11 77.58 118.11 68.18 94.36 45.18 94.36 66.75 43.53"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Adobe_favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 48x48, 32 bits/pixel
Category:	downloaded
Size (bytes):	9662
Entropy (8bit):	1.5933577223587498
Encrypted:	false
SSDEEP:	48:97gzdbkITMl1sy6TMenl7ulGt/3GmjAAp:970sI2NmU3GY
MD5:	B28BF60DD7E50B6DFFD394EBC0F9057A
SHA1:	9EA7EED87B689757780322989EF426AEFFDC8F7A
SHA-256:	BF24C9E4D37F94D4BD2F870228FF421CA54B2949DB3391DBD3818EC0E6DB0F5F
SHA-512:	B16A7F756E38FFE4BBCC0394A6E41593CC9FE68AACA6350C1C20D10E7A284EBFC7937C15726D0F43A3ABD7C43D128A041A109CAC2C8F240707FE1997E633E05
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/content/dam/cc/Adobe_favicon.ico
Preview:	......00.... ..%.....(...0...`..... .....$..... ....A.....V.....'..... .....A.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Contact_72px_lt-gray[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	28341
Entropy (8bit):	6.120769466888277
Encrypted:	false
SSDEEP:	768:37iSZiRcO9jD+7ZBNq+2owtRXhhMEnWLbljThoIJ5q:cRzGZBk+2owPleZX5q
MD5:	901C088DD283B59F4A43F74D798EDC60
SHA1:	959EA9066F892F103A3DDA229D67619150F7DD7B
SHA-256:	C45E2555412C2D5EC5E521ED5851B3D3665F90DD1DC645D6D59DEEFD71BC2ECB
SHA-512:	DAE5CFA3F362280B2D903FC35C6290AB28CCF5E5E5EA6C081B2EFFDBC20AA34301085DFAB35A0EFF5B6ECC7ED6C049668D95274DDF8A06314D60FD612A00455
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/content/dam/cc1/en/privacy/images/Contact_72px_lt-gray.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>. Generator: Adobe Illustrator 19.2.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->.<!DOCTYPE svg PUBLIC "-//W3C //DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd" [..<!ENTITY ns_extend "http://ns.adobe.com/Extensibility/1.0/">..<!ENTITY ns_ai "http://ns .adobe.com/AdobeIllustrator/10.0/">..<!ENTITY ns_graphs "http://ns.adobe.com/Graphs/1.0/">..<!ENTITY ns_vars "http://ns.adobe.com/Variables/1.0/">..<!ENTITY ns_ imrep "http://ns.adobe.com/ImageReplacement/1.0/">..<!ENTITY ns_sfw "http://ns.adobe.com/SaveForWeb/1.0/">..<!ENTITY ns_custom "http://ns.adobe.com/Ge nericCustomNamespace/1.0/">..<!ENTITY ns_adobe_xpath "http://ns.adobe.com/XPath/1.0/">.]>.<svg version="1.1" id="adobeNews_x5F_72_x5F_lt-ou" xmlns:x=" &ns_extend;" xmlns:i="&ns_ai;" xmlns:graph="&ns_graphs;".. xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" width=" 72px" height="72px".. viewBox="-359 271 72 72" style="enab

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\LawEnforcement_72px_lt-gray[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	28018
Entropy (8bit):	6.123287231997608
Encrypted:	false
SSDEEP:	768:3B3bnD+0T1bo4s83RvlSqEOSt1uRgzgd6Hio:I0Bo49h32I6HT
MD5:	203D2596591DD98304B03BDBCFE7948A
SHA1:	145A9AB021FA39848CBF9E95DB7132554469934C
SHA-256:	F0F7F1BB8276F731235B5519886DEF7081CE2AF2A906567888F5CC1F7BBD78C1
SHA-512:	2A36BE5EF21D35EA123BE7CFDB88BC1C025AE359E80068E9E1FAB66748E15D268A7A9162CA0FE5364F34852E5EBA88DE665C5F5710668783ADC55A91D6825629
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/content/dam/cc1/en/privacy/images/LawEnforcement_72px_lt-gray.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>. Generator: Adobe Illustrator 19.2.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->.<!DOCTYPE svg PUBLIC "-//W3C //DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd" [..<!ENTITY ns_extend "http://ns.adobe.com/Extensibility/1.0/">..<!ENTITY ns_ai "http://ns .adobe.com/AdobeIllustrator/10.0/">..<!ENTITY ns_graphs "http://ns.adobe.com/Graphs/1.0/">..<!ENTITY ns_vars "http://ns.adobe.com/Variables/1.0/">..<!ENTITY ns_ imrep "http://ns.adobe.com/ImageReplacement/1.0/">..<!ENTITY ns_sfw "http://ns.adobe.com/SaveForWeb/1.0/">..<!ENTITY ns_custom "http://ns.adobe.com/Ge nericCustomNamespace/1.0/">..<!ENTITY ns_adobe_xpath "http://ns.adobe.com/XPath/1.0/">.]>.<svg version="1.1" id="adobeNews_x5F_72_x5F_lt-ou" xmlns:x=" &ns_extend;" xmlns:i="&ns_ai;" xmlns:graph="&ns_graphs;".. xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" width=" 72px" height="72px".. viewBox="-359 271 72 72" style="enab

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\PrivacyChoices_72px_lt-gray[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	28419
Entropy (8bit):	6.117998475478093
Encrypted:	false
SSDEEP:	768:37S2WvPzXeJfwU2ihjrx8Ks+a/4TLpCknorFPBHCJ93BvxHtc6:0HzONH2ihRLM/4H8korVBiH3jZ
MD5:	775D2556523FF33568DCF0EE25C3249B
SHA1:	8575AF9EDFEB7E1A2D1B7A36DA34F13594CFD7F1
SHA-256:	241B307DFAB1F3CA3C626DF06C32F5472777A4316013981A121B951911B311FE
SHA-512:	5ED60101D06A32FDA1D8A979FFC701641577DD694987ABAE741B7B154AFDAAFBDE1A294EDB66AC14B1B8C3D82BB184B5BEE9E1F92000FF8669F8D99626645E34
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/content/dam/cc1/en/privacy/images/PrivacyChoices_72px_lt-gray.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>. Generator: Adobe Illustrator 19.2.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->.<!DOCTYPE svg PUBLIC "-//W3C //DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd" [..<!ENTITY ns_extend "http://ns.adobe.com/Extensibility/1.0/">..<!ENTITY ns_ai "http://ns .adobe.com/AdobeIllustrator/10.0/">..<!ENTITY ns_graphs "http://ns.adobe.com/Graphs/1.0/">..<!ENTITY ns_vars "http://ns.adobe.com/Variables/1.0/">..<!ENTITY ns_ imrep "http://ns.adobe.com/ImageReplacement/1.0/">..<!ENTITY ns_sfw "http://ns.adobe.com/SaveForWeb/1.0/">..<!ENTITY ns_custom "http://ns.adobe.com/Ge nericCustomNamespace/1.0/">..<!ENTITY ns_adobe_xpath "http://ns.adobe.com/XPath/1.0/">.]>.<svg version="1.1" id="adobeNews_x5F_72_x5F_lt-ou" xmlns:x=" &ns_extend;" xmlns:i="&ns_ai;" xmlns:graph="&ns_graphs;".. xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" width=" 72px" height="72px".. viewBox="-359 271 72 72" style="enab

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\RC1a4f9c4f0d8a4bba917d5412b0c552b7-file.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	458
Entropy (8bit):	5.1860245377232355
Encrypted:	false
SSDEEP:	12:jvgeASPRNNHt62jA0ZPZPSwhLGGK+K4Jo70WJkwvCRBu:15Ny2jlxJSGLGUJQJkQCvu
MD5:	1B585A1D8CEE2FE0A7D7ADA6683196EB
SHA1:	0330CB1E2AA0C09689CCD0302182E841D2659AA0
SHA-256:	B863E65E81435AB19F9E7A229DFD909AAB4AC362353F36FB7B0150AFAAC2E677
SHA-512:	1D320E150807F99FF36C07B94E06B8722E0BD329D2F0EFF4DCF6F8EA47D95087C06E73F0EEBE0F92AD51AB1332CBA068CBB7295BB1A13848DC06F2AACA4FF5DA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/bffb9ea23c0c/RC1a4f9c4f0d8a4bba917d5412b0c552b7-file.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/bffb9ea23c0c/RC1a4f9c4f0d8a4bba917d5412b0c552b7-file.js`..(0,_satellite.o neTrustIsHostEnabled)("everesttech.net")&&_satellite._loadScript("https://www.everestjs.net/static/le/last-event-tag-latest.min.js",function(){"undefined"!=typeof AdCloud Event&&AdCloudEvent(_satellite.getVar("marketingCloudOrganizationID"),_satellite.getVar("analytics_account_adbadobenonacdc"))});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\RC419dbb68baed4e699648e06bb8cb6515-file.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	6334
Entropy (8bit):	5.105794213184045
Encrypted:	false
SSDEEP:	192:i2yBkFCu1W5u6vXnFtC4tPSHmjHcm53JLgWCYTHNbvrMQ4zdphfOCq28GZMli:i2yBkFV1W5u6vXnFtjtPCmLcm53JLgWe
MD5:	99D0E6730FF593635BA7523B3E983AA8
SHA1:	AC3E540697F316031567949AEF20F0CC794EF0AF
SHA-256:	2DB62ECCDAF0E60D6AC2B125EAC9A203AB7D605B46FD4610884D6FD211D41086
SHA-512:	1806411932C1F1477BC1F2F1019B3D7E8B84AFB7C3B39FBF67ACE46FD2AE8CB5F70B6CEB79C9B6365D49DC7CB957D4338045973C2482EA045DDC566758511F7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/bffb9ea23c0c/RC419dbb68baed4e699648e06bb8cb6515-file.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/bffb9ea23c0c/RC419dbb68baed4e699648e06bb8cb6515-file.js`..!function(){var e=(0,_satellite.windowProperty)("path")||window.location.pathname,t=document.referrer,a=(window.location.href,_satellite.oneTrustIsHostEnabled),r=function(e,t){return-1!==e.indexOf(t)};if(-1!==e.search(/\/products\/xd/)&&_satellite.track("pageload-xdDownload"),a("d26x5ounzdjojj.cloudfront.net")&&-1!==e.search(/\/(uk|africa|gr_en|be_nl|be_fr|be_en|cz|cis_en|cy_en|dk|de|ee|es|fr|ie|il_en|it|lv|lt|lu_de|lu_en|lu_fr|hu|mt|mena_en|nl|no|at|pl|pt|ro|ch_de|si|sk|ch_fr|fi|se|ch_it|tr|bg|ru|cis_ru|ua|mena_ar|il_he)\//)&&(r(e,"/creativecloud/business.html")||r(e,"/creativecloud/business/teams.html")||r(e,"/creativecloud/business/teams/features.html")||r(e,"/creativecloud/business/teams/deploy-and-manage.html")||r(e,"/creativecloud/business/teams/plans.html")||r(e,"/enterprise.html")||r(e,"/business/enterprise.html")||r(e,"/creativecloud.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\RC7e9f4c1a441d45af93bf75d76d872cf0-file.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	9642
Entropy (8bit):	5.459797059181775
Encrypted:	false
SSDEEP:	192:8ZjXXA7m2ZdeLPymA60ZCMvCx0K+DQjMBg+2pTRhqOd/WcbV/OHnYdCT:8ZjXWm2ZdeLPymAVZJv+FeQgBg+cTRhm
MD5:	572171EDF0BE3F2C2529358DBCDA0F14
SHA1:	D59B6921CEDD4B358DA28AB7F7C3E68971E0DC0F
SHA-256:	E6C399387DD2327CA56EB4D9592DA5E840E7C38ADC41F1D1A28EC656E3BD3D77
SHA-512:	BC315334BDB079813DAEE5169BCFEDCD4E59EC3555C50D4419FDD128387754CBD5EBC624C2A4718A10F71058EC785B29B0689C4FC0DEC7CC35B55A0B0E02D7E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/bffb9ea23c0c/RC7e9f4c1a441d45af93bf75d76d872cf0-file.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/bffb9ea23c0c/RC7e9f4c1a441d45af93bf75d76d872cf0-file.js`..!function(){function e(){var e,t,a,n,o,i;e=window,t=document,a="script",e.twq||((n=e.twq=function(){n.exe?n.exe.apply(n,arguments):n.queue.push(arguments)}).version="1.1",n.queue=[],(o=t.createElement(a)).async=!0,o.src="//static.ads-twitter.com/uwt.js",(i=t.getElementsByTagName(a)[0]).parentNode.insertBefore(o,i)),y&&"/articles/2019/10/adobe-2019-holiday-predictions.html"==y("path")||y&&("summit.adobe.com"===y("host")||"summit-emea.adobe.com"===y("host"))&&(-1!==y("path").indexOf("/na/")||-1!==y("path").indexOf("/emea/"))||_satellite.getVar("adobe_aec_pages")||-1!==y("path").indexOf("/experience-platform.html")||"cmo.adobe.com"===y("host")?twq("init","o02t1"):"/jp/creativecloud/stock.html"==y("path")?twq("init","o1kax"):-1!=y("path").indexOf("/summit")?twq("init","o0xx1"):35==U?twq("init","nxbss"):twq("init","o1w4k"),twq("track","PageView"),-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\RC89c6d3bd15f043db95a5a0a4b5cc9da0-file.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	821
Entropy (8bit):	5.152631936032561
Encrypted:	false
SSDEEP:	24:15NUcSMueyrpjBKe4lldllALxTb0aVM/:15NS6ytdKe4lldllABwaG/
MD5:	9C5942C71644B7A92CE1A2C5542A4295
SHA1:	612AD7AA7AB647473CE759D4D9F502D231A4D25D
SHA-256:	E102C9F6F96D68452C35DEA924FA72E6881FC2238E89078E2E099C1F4D2299C8
SHA-512:	70EA258EA09E03BB8D2E959C165FB195F2F129FBB5ACF8F48A11C80BA232E55D4030530C8DEDF5C5B60350D7C53ECBE16C0BEB1D58D0A7224F7FE9BA2703E832
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/bffb9ea23c0c/RC89c6d3bd15f043db95a5a0a4b5cc9da0-file.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/bffb9ea23c0c/RC89c6d3bd15f043db95a5a0a4b5cc9da0-file.js`..!function(){function u(e){var a=1e13*(Math.random()+""),n=document.createElement("iframe");n.style.display="none",n.style.width="1",n.style.height="1",n.src=e+a+"?",document.body.appendChild(n)}var d=window;window.marketingTagInfo=[],_satellite.windowProperty=function(e,a,n){var r=d.location,t=r.hostname,c=r.pathname,s=unescape(unescape(unescape(unescape(r.href))),i=unescape(unescape(unescape(document.referrer))),o="";switch(e){case"host":o=t;break;case"path":o=c;break;case"href":o=s;break;case"referrer":o=i;break;case"dClick":u(a);break;case"substr":o=function(e,a){return-1!==e.indexOf(a)}(a,n);break;case"addPixel":marketingTagInfo.push(a);break;default:return!1}return o}}();

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\SPRK_white@2x[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1518
Entropy (8bit):	5.00107238377263
Encrypted:	false
SSDEEP:	24:2dfkATLf3+sZ1enVMeN2zQH9nMZ2x0gWXNdIjNN4iWbJ7oIa6d06+:cfkAvfOsZ1302zUj+Td1b+Iaim
MD5:	A29E0C074D7C5E3F6A54CE20C5FEA0AF
SHA1:	8563F7581C1939067B4AA354E78341BC46BD9E1D
SHA-256:	511C77BD64C8D67BE5FC38F107B5005F32F38386A8142CE13753EDABEDD50B86
SHA-512:	50DAC8A1C88FF4369B3199091AC273A4EC482C9C944A4A93DAAF5885C30B30A96469826BE11AAAA890F5393E08FD9CA809AF9E92A836DAC40CB722C13D1E0A0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spark.adobe.com/images/SPRK_white@2x.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\SPRK_white@2x[1].svg	
Preview:	<?xml version="1.0" encoding="utf-8"?>. Generator: Adobe Illustrator 21.1.0, 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="66px" height="64px" viewBox="0 0 66 64" style="enable-background:new 0 0 66 64;" xml:space="preserve">.<style type="text/css">...st0{fill:none;}...st1{fill:#FFFFFF;}.</style>.<path class="st0" d="M14,62C7.4,62,2,56.6,2,50V14C2,7.4,7.4,2,14,2h38c6.6,0,12,5.4,12,12v36c0,6.6-5.4,12-12,12H14z"/>.<path class="st1" d="M52,4c5.5,0,10,4.5,10,10v36c0,5.5-4.5,10-10,10H14C8.5,60,4,55.5,4,50V14C4,8.5,8.5,4,14,4H52 M52,0H14..C6.3,0,0,6.3,0,14v36c0,7.7,6.3,14,14,14h38c7.7,0,14-6.3,14-14V14C66,6.3,59.7,0,52,0L52,0z"/>.<path class="st1" d="M15.1,42.3C14.9,42.2,15,42,15,41.8v-4.2c0-0.1,0-0.3,0.2-0.1c2,1.4,4.1,2,6.4,2c3.2,0,4.5-1.7,4.5-3.6..c0-1.7-0.9-3-3.9-4.8l-1.6-0.8c-4.5-2.5-5.9-5.1-5.9-8.5c0-4.5,3.1-8.1,9-8.1c2.6,0,4.8,0.4,5.9,1c0.2,0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Security_72px_lt-gray-01[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	28075
Entropy (8bit):	6.122713193021488
Encrypted:	false
SSDEEP:	384:3jYU3YROQayWcpEepYNGWS8f7Bau7MfYR9/sH53ABwPJ5anlMelCeZpCZRhA6pDh:3B3elubSc7EusYi+9XlC/hAiDthP3eJy
MD5:	82139CDA626B6F7046B190923E4E1678
SHA1:	CBEF7F51F834C6EF8197ECB1AF9F7C1C1693A44D
SHA-256:	12E03ED2EEE83C341A3DE969B11CEED1849891C2775434A06438EABFC66CCA3C
SHA-512:	90ABCE4D99B32DFF9F951F5213E45C123F4F7C106991D9574530657D0BC63419BD19444055E39868B82929C1D6FA7BA9B0B3E740F52E01B87DF2A482CF17D675
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/content/dam/cc1/en/privacy/images/Security_72px_lt-gray-01.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>. Generator: Adobe Illustrator 19.2.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->.<!DOCTYPE svg PUBLIC "-//W3C //DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd" [..<!ENTITY ns_extend "http://ns.adobe.com/Extensibility/1.0/">..<!ENTITY ns_ai "http://ns .adobe.com/AdobeIllustrator/10.0/">..<!ENTITY ns_graphs "http://ns.adobe.com/Graphs/1.0/">..<!ENTITY ns_vars "http://ns.adobe.com/Variables/1.0/">..<!ENTITY ns_ imrep "http://ns.adobe.com/ImageReplacement/1.0/">..<!ENTITY ns_sfw "http://ns.adobe.com/SaveForWeb/1.0/">..<!ENTITY ns_custom "http://ns.adobe.com/Ge nericCustomNamespace/1.0/">..<!ENTITY ns_adobe_xpath "http://ns.adobe.com/XPath/1.0/">.]>.<svg version="1.1" id="adobeNews_x5F_72_x5F_lt-ou" xmlns:x=" &ns_extend;" xmlns:i="&ns_ai;" xmlns:graph="&ns_graphs;".. xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" width=" 72px" height="72px".. viewBox="-359 271 72 72" style="enab

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\base-fonts.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	72
Entropy (8bit):	4.675124266644529
Encrypted:	false
SSDEEP:	3:yLRmcpZBLvG/tLAfimqW7RmMe:yL/pZtvG1AiMRmMe
MD5:	1C75FB60A6530DC7F95725DED413DC13
SHA1:	A6F43A1C5E1039C212879090EFA6411008528FAD
SHA-256:	E99BEC104ED648FAB6ECA0D41AB2B793A05E6A3305B24483C681C5BD5CF5C325
SHA-512:	6C606EEE1E84DAD4064F4F579FE7AA95C028167474BE75A9486996E368E3717FD5252D98652F98E0128324F92957C241B44B79B6502925EF8B8F2B9F4A3A7500
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://page.adobespark-assets.com/runtime/1.22/base-fonts.gz.js
Preview:	document.write('<script src="//use.typekit.net/onz5gap.js"><\/script>');

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\d[10]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, CFF, length 66304, version 0.0
Category:	downloaded
Size (bytes):	66304
Entropy (8bit):	**7.993959805787878**
Encrypted:	**true**
SSDEEP:	1536:VeO6ShUivo8vaO8pnTzDOTXL/kxtcA+uDWB:p6DJWaO4iT7/4tzk
MD5:	9E6E819AE9D8993A2B10353EFF16497D
SHA1:	1410161D0CA8CA3966897CAB50E45A14B721C056
SHA-256:	81B4B3BC1EFD4F08F212308D9727BC21A40E38B5464B6B25EBDE1B2E24D13F05
SHA-512:	D9D88E8987EE2F45BFA0B211AAA7DFEB9C39718E9A037FAE625AF4E6806E04D4C8316B58363EEA93E9BA6C23B6F514925D4841C95CDFB103693688D5EFC71DB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/40207f/00000000000000000000176ff/27/d?primer=7cdcb44be4a7db8877ffa5c0007b8dd865b3bbc383831fe2ea177f62257a9191&fvd=n3&v=3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\d[10]	
Preview:	wOFFOTTO.....D.....BASE...X...F...Fe().CFF ...T.....6...DYNA...P.....gG9GDYN...T.../...a... GPOS.....#...T.;..GSUB...0.....0.OS/2.....Y...`[.t.cmap..... ..S.....lgasp.....head.....4...6..%`hhea...(...!...$....hmtx.....x..].maxp...L.....^P.name.....8l.post..... ...2.....ideoromn..DFLT..cyrl..grek..latn..... ....`.....x.c`d```5.*{..9...+.3.....P..?.?....1 ....$._..!x..An.@....I..jo0.>...!..$H.....`a{.=Ab.u.]...B..E..T..<...Y....3.{o....._.....k....x.....c.Mj.....f~..B.....9...s..A.V.....g.Mj.{> F...|..0.[.5>=.P..1X....}iuV..|n..)b..R..TL...b.K].X.R...M..!..H...?....N...N...p..x..21...wS.J.T.m...;.Jv..Y....e..B.....kk....o.&.rn....z~u...%. .Bq\..X.`.M.b.....)p...Y-.....r.L.`.5+..i>5.;. <..C3%'...U...X.....D..{.!F.~...8=..c.~y.{w.s.*.{..U.....*...._....~.j....*..)Sg.....R^:.u[v..m.....j.eJ.w.u.T.....Oy.s-..m.x..x.c`f.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\d[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, CFF, length 30780, version 0.0
Category:	downloaded
Size (bytes):	30780
Entropy (8bit):	7.988535310328335
Encrypted:	false
SSDEEP:	768:B4GGbSq0CiAIlwymd1yf04b80qrqH7b7V8zXe1X7QjQlWunvdoO6:B4/SqQ5wymryflbhqrqf7C6NrWunvdo3
MD5:	41291B5CC7AE5A302D0FF767D801DC05
SHA1:	A6B8FA2252C9563DE7FABC7A6F068E5D7C42383E
SHA-256:	641E63A696D3E572B940226372365DDE29D2D581D614B5FCF66323ED46A5CBDD
SHA-512:	3F6F193E7B3F5E0743427577E129D5F21E9A0598F5444A930B53573A87A562861807ACAD2CD4065BBB8FFF7C70821DC500BDBBE431662EC9C04064E975AD5B28
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/37eaae/00000000000000003b9b3f83/27/d?primer=7fa3915bdafdf03041871920a205bef951d72bf64dd4c4460fb992e3ecc3a862&fvd=n3&v=3
Preview:	wOFFOTTO..x<.....BASE...0...F...Fe().CFF .....\...o...C.DYNA..`.....3GDYN..ah.....|GPOS..bH..._..$.....OS/2.....W...`[.tJcmap..v....V.....3head... x...4...6..%`hhea..... ...$...Lhmtx..t....%...H{e!.maxp.....P.name.....8..post..v..... ...2.....ideoromn..DFLT..cyrl..grek..latn.....`.....x.c`d```5..?..N <..W.f..@.....0....6.;.c@.3..H.....x.RMn.@.}&$U7.....-+.V. 5R$"...a... {.....r....^.G.*.y<mQ....|.g.....Cs]q6..[....+|p...0u.M...s.....f~u.....`_s.....{..-t.O..a.}q.M....Qz....h..w..>?._...- .X...2:..].(.]QFF/.....%..LW....oR....fz..Fe(.^8..'C+..K.`u:..g|.e...h..s.K..pS.E..EO*y...h....i..2..@....cv..9..61rQd].#U]....A.....!.Cq.FX.@.M<....q.... [....rKH.K9.fH..LeW.OM..)..o ..L....j..O.".Bz|..!...b..E.R.e\.e4.U.....B..i;.X.Pel.r.....$...l..-.j.....v.l.....r.~..U[.).....u."V'F.....O.G.....x.c`f.....L,,LL,..L.@yF.(ptqr.R.....gc``...K..q>H...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\d[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22376, version 0.0
Category:	downloaded
Size (bytes):	22376
Entropy (8bit):	7.9745730846169725
Encrypted:	false
SSDEEP:	384:nAizO59XJQcmATaTY6S0r89SmOrPuaDuXo0J22vNYckNcL5VjWV3ncNHFb:1AQcmATaTYn0g9Wiaso0wqKNM5pmcfb
MD5:	74B4BA34F532FC0C6C7C557A65B733B6
SHA1:	CA3CF7110DF3502935D79F055BFFE00A55087C3A
SHA-256:	58C894C70D7848BD09B94AF1754E5532DCAC4189ED48F9AA3AB5E1ACEF4376C1
SHA-512:	29A5BA44B73F6AD9F3AFA09ACA3326E1BD8FD0C79C681D91A03E12B46D09A198E2CD5A1B6AFAE7F59F2E4DFC4AC64480F0F96E22FE8879C22C3A8F52A2B98E5B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/6c57c4/000000000000000000000158d6/26/d?subset_id=2&fvd=i6&v=3
Preview:	wOFF.....Wh.....|.....DYNA.....t.FFTM.....]...GDEF.....8...B...<GDYN.....j..GPOS.....J.w..OS/2...T...Y...`..zvcmap..V.....+..wcvt .....^...^ .C..fpgm...$.....e#./.gasp.....glyf.....E...s..r.Ahead.....5...6.V;.hhea..... ...$.W.phmtx..R....N...l{k,Lloca..U.....maxp..... ... .name.....#.g?post..V..... ... (prep.....t....i.D.....o1.....=.....x.....6...|.....@.k.....u.e.....R.7.9.;.F.....x.]Q.N[A.....c..hS.fB...$.W...vc9B.\.b\..P Q..k.h().A..R>.O@bfM. (....s..r..]Z.y..R.....v...t}...v.@..^.n...`3.rG....-.!.i'P....6...>.d..AK3MO....B`...0...../X....C.i*..s*..Ks....k..vp&"?..hj..@._:.z>.b.r.0...S.d".f2].T-3.up...;X.Js....U.....-.2KC...*1B.$.BN 9w.?)P>..1....a..q.50.....fS.{.0~.G..o..>..6F..X.`...QU...s/.....3.%`y.._'..;6..em.C.....2....U.....tJ.....p.X...R.v....`H.F..h-;.*...d/.*.....x.c`d```

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\d[3]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22492, version 0.0
Category:	downloaded
Size (bytes):	22492
Entropy (8bit):	7.974382432382698
Encrypted:	false
SSDEEP:	384:yDLC8fp6SXkpD0a74PboHnd4VZK1Jnn3J0YjWkPpSjYmRja+eUZ5EJSyT7MYLQ:iW8h6rD0ak8nyZ2ysrpeYmRcdfE
MD5:	A2CAF0BD8F7084A90E2053AD61157C78
SHA1:	9E35E2810DCCB3C791CEB2818B16EFA9328C307E
SHA-256:	6537EEA8561F3D0903E4CAABB123C0AF961A09218290C678285B7C27ED335E54
SHA-512:	1FAE0E3EC674A092FAD4813182C77144F698AEA5715BD94540CF4AB8CF865165CD1BC57A56E56254B3F8C0E9F10227FCFCE33FA2020D616CB0D7ADA1CBBB89DC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/fe9c8e/000000000000000000000158d8/26/d?subset_id=2&fvd=i4&v=3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\d[3]	
Preview:	wOFF.....W.....P.....DYNA.....t.FFTM.....]...GDEF.....8...B...<GDYN.....j..GPOS.....-...J.E..OS/2...X...Y...`~.zEcmap..WD.....+..wcvt .....\...\ ...Xfpgm... .....e#./.gasp.....glyf.....E1..s.C..head.....4...6.W;.hhea..... ...$.Y.4hmtx..S0...E...lg.5.loca..Ux.....maxp..... ... ....name.....post..W0..... ... (prep.....:.....o1.....'.....x.....6...`.n.|.....x.....u.....q.....k.>.W.....~.^.N.s...H.7.9.;.c.J.L.F...P..x.]Q.N[A.....c..hS.fB...$.W...vc9B.\.b\..P Q..k.h().A..R>.O@bfM. (....s..r..]Z.y..R.....v...t}...v.@..^.n...`3.rG....-.!.i'P....6...>.d..AK3MO....B`...0...../X....C.i*..s*..Ks....k..vp&"?..hj..@._:.z>.b.r.0...S.d".f2].T-3.up...;X.Js....U.....-.2KC...*1B. $.BN9w.?)P>..1....a..q.50.....fS.{.0~.G..o..>..6F..X.`...QU...s/.....3.%`y.._'..;6..em.C.....2....U.....tJ.....p.X...R.v....`H.F..h-;.*...d/.*.....x.c`d```b8./

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\d[4]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20932, version 0.0
Category:	downloaded
Size (bytes):	20932
Entropy (8bit):	7.97207524312144
Encrypted:	false
SSDEEP:	384:3wgN6IL9Cl+QE5TQoI23a0zC9/lY1eizt+wcCMPyv2GTPNo/B1:AgN62MlkrI23a0G+keiBL4jKoZ1
MD5:	E0F2BB6FEFF9005FADFAA0DEAC9F17D3
SHA1:	5BCF4E553881D43087F31A8B47172F1F695E461B
SHA-256:	809F249AF3A361113340A14136F8464AB4A1A23E47B05F71375115E6C23FFC92
SHA-512:	8426F3F16F8B9FABC3F47DD3984156C723387E0F1FC804B25FE427B9B120E78CB376185BE701555ACBC9E26D2A8611F598C9DCB393B0950369A653632901F9C4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/edcf1e/00000000000000000000158d9/26/d?subset_id=2&fvd=n3&v=3
Preview:	wOFF.....Q.....DYNA.....4.(.FFTM.....]...GDEF...H...8...B...<GDYN.....GPOS...`.....@...YOS/2.....W...`~wz1cmap..Q,.....+..wcvt .....*...* ...6fpgm.....e#./.gasp.....glyf...(..@...e.....head.....4...6..;.hhea...P... ...$....hmtx..M@.....lVRI.loca..O`.....maxp...p... ... ....name.....Q%.{.post..Q..... ... (prep.....i...v..ym.....o1.....x.....6.h.R.\.^.h.r.Y.z.`.d.m.j.t.L.F.J.f..x.]Q.N[A.....c..hS.fB...$.W...vc9B.\.b\..P Q..k.h().A..R>.O@bfM.(....s..r..]Z.y..R.....v...t}...v.@..^. n...`3.rG....-.!.i'P....6...>.d..AK3MO....B`...0...../X....C.i*..s*..Ks....k..vp&"?..hj..@._:.z>.b.r.0...S.d".f2].T-3.up...;X.Js....U.....-.2KC...*1B.$.BN9w.?)P>..1....a..q.50.....fS.{.0~ .G..o..>..6F..X.`...QU...s/.....3.%`y.._'..;6..em.C.....2....U.....tJ.....p.X...R.v....`H.F..h-;.*...d/.*.....x.c`d```b8Z...h<..W.y..@..S.*.....`..r9.j....l..x...J.@

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\d[5]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 24436, version 0.0
Category:	downloaded
Size (bytes):	24436
Entropy (8bit):	7.978037120154255
Encrypted:	false
SSDEEP:	384:b2q7Hwg9s0WrCWQYOL4VhwnhHa63bzKnWhF52DHilk+9y5yS6P8N:KqrsYL4vwh663fKW/50iZ9lyZPs
MD5:	6D26AE32705F04BD2CCC4DC335F15809
SHA1:	6F67C23951FB9426FA426436CCC1CE1E6FDDF220
SHA-256:	6E52D4DF448460F8B6C6C8DC776745BE4C85A9D18981772A89C9876B4E19FB37
SHA-512:	687973BC1D027B36AC99E2B7AA9928B35148E7AA742B13FCF2A20B0947B7ED27EA470E770856711C584221E88F3FBEA5AA3A93A58DC59DB7794320E9B11F019A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/9d1933/00000000000000000001705b/26/d?subset_id=2&fvd=i3&v=3
Preview:	wOFF.....`_t.....BASE.....F...Fe!].DYNA.....bGDYN.....#...Q.4.xGPOS.....dG...OS/2...X...\...`.}..cmap..].....8..}.cvt .....R....6...fpgm...0.....p ...Ygasp.....glyf.....BX..w....Mhead.....6...6....hhea.....''...$....hmtx..WX...+...z....loca..Y...._.....4..maxp..... ... .B..name.....yJ..post..[.....Q..$uprep..... R.>.....ideoromn..DFLT..cyrl..grek..latn.....Y.....x.c` .X..>.>.l.....=.g.....0.FU.....l...,o.....4.=H..1...BX8a..x.Viw.F..yI..,%.-ja..i.F&l...A.c].....;... ._.d.s.7~Z../$...p...w.....e.Z...../...&..<..M.Q\|(;{!e....Q.....DD"P...D...Y.d\|.QF..WM.-=..[.A.U.~.:.;..f3th=.%U.U.H.=R.e..+I+....W.P.N"i....H..g..h5..(.l..(R$..A.y.....V.K.. ../y.w9?)..[.-9...#;8;]....V.7.d;.U.....[6;.....L/4#X*_!..O(..HV..S....l.D.z....O..8bJ\3F.twtB.u....=.....w.....Q.'.DJ..M.6..XI.Jj.+&Ny..._.v..3.8....C.VNTr<..i&S.vR.hJ.(%.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\d[6]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20540, version 0.0
Category:	downloaded
Size (bytes):	20540
Entropy (8bit):	7.970560806372044
Encrypted:	false
SSDEEP:	384:Fo1SMQ+uypEPZJnq9tVxtO0TKJOOr4ohDCR/Iowk+hkFo31JAM7/Se:FoQ9+u7nSBM0+4ohDiQhkS3cMDSe
MD5:	F7DFBBC4491156A7123A80DD7F9A1AA7
SHA1:	643F976CF7504CBF212657C25BE954A73F7F3F04
SHA-256:	6778F1BCD6798ADE72372490A2BC16AD9BE3A23996E86878AF0C8F429B429CB9
SHA-512:	D9689A58CA5C421105B1846BD35C51C0AAA7B3D928F2EE04BF00D3679FFCE90FBA5C12829626F090CED0ECDE1158D5A7068AB7EC401B2ACDC25DB4324940F8 04
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/3d913c/00000000000000000000017709/26/d?subset_id=2&fvd=n6&v=3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\d[6]	
Preview:	wOFF.....P<.....DYNA.....4.(.FFTM.....]...GDEF...d...8...B...<GDYN.....GPOS...|...x...@.z..OS/2.....Y...`..zpcmap..O.....+..wcvt .....0...0 ...Jfpgm.....e#./.gasp.....glyf.....>...b...`.head.....5...6..;.hhea...l... ...$...*hmtx..K....-...lx.8.loca..M.....U.Rmaxp..... ... ...Tname.....u....post..O..... ...(prep.. .....s....^`.....o1.....2.....x.....6...|.....n.....u.....x.]Q.N[A.....c..hS.fB...$.W...vc9B.\.b\..P Q..k.h().A..R>.O@bfM.(....s..r..]Z.y..R.....v...t}...v.@..^.n...`3.rG...-. !.i'P....6...>.d..AK3MO....B`...0...../X....C.i*..s*..Ks....k..vp&"?..hj..@._:.z>.b.r.0...S.d".f2].T-3.up...;X.Js....U.....-.2KC...*1B.$.BN9w.?)P>..1....a..q.50.....fS.{.0~.G..o..>..6F..X .`...QU...s/.....3.%`y.._'..;6..em.C.....2....U.....tJ.....p.X...R.v....`H.F..h-;.*...d/.*.....x.c`d```b8z.;.h<..W.y..@..S.*V...+.....T.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\d[7]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20720, version 0.0
Category:	downloaded
Size (bytes):	20720
Entropy (8bit):	7.971274872077512
Encrypted:	false
SSDEEP:	384:ep0ld6FR9PFBI+qyX9W69gNqcJddRjJpyZc+2HC9j2SDGDYfLrDYSzJgIY:K0ld6VtBI+qy069gAa1Jx+G6zDGDYfH0
MD5:	185A2AFC0935C94FBB5683112A905CE2
SHA1:	4EB450182B9C658C6916CDDED80D3922E90DDCD8
SHA-256:	F81CA8209A0526BEF58A70CF4288A1B1F8A02D8B1F7F8E3BC4B8A179323A1DFD
SHA-512:	A8C1BCA226F757C2BC8A096E31D2E05B2F8C184A531D93CDE6A26974A10B96005F4F341D52A80404919CE050BE8F89EE91EFC7D996936B37879DFD85CAA36E9 A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/9951d2/00000000000000000000158d7/26/d?subset_id=2&fvd=n4&v=3
Preview:	wOFF.....P.....`.....DYNA.....4.(.FFTM.....]...GDEF...p...8...B...<GDYN.....GPOS.....@.J.OS/2.....Y...`~.z~cmap..PX.....+..wcvt .....2...2. A.0fpgm.....e#./.gasp.....glyf...L..?...bT.@..head.....4...6.E;.hhea...x... ...$.I..hmtx..L`...,...le.BVloca..N.....maxp..... ... ....name.....iZ.[.post..PD..... ... (prep.....>.....o1.....x.....6...`.n.|.....Z.....O...t.c.....x.]Q.N[A.....c..hS.fB...$.W...vc9B.\.b\..P Q..k.h().A..R>.O@bfM.(....s..r..]Z.y..R.....v...t}...v.@..^.n. ..`3.rG....-.!.i'P....6...>.d..AK3MO....B`...0...../X....C.i*..s*..Ks....k..vp&"?..hj..@._:.z>.b.r.0...S.d".f2].T-3.up...;X.Js....U.....-.2KC...*1B.$.BN9w.?)P>..1....a..q.50.....fS.{.0~.G ..o..>..6F..X.`...QU...s/.....3.%`y.._'..;6..em.C.....2....U.....tJ.....p.X...R.v....`H.F..h-;.*...d/.*.....x.c`d```b8Z.9.?...+.<....._K`.....p.....@.@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\d[8]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, CFF, length 66508, version 0.0
Category:	downloaded
Size (bytes):	66508
Entropy (8bit):	**7.994636853689064**
Encrypted:	**true**
SSDEEP:	1536:4p7762bluKjsVQJU/x14nXWjvxpGeDKTeEPiBlnQcA+yWB:q362bluKjqQWr4nG7xpP2PiEz0
MD5:	49B061D6468547558176037211AA630C
SHA1:	B02FD5987ED77AF837699BB13C7E838018943423
SHA-256:	F89C62C68380B4BB548E4E24E284348FE9E98730F54F7E0C8942F6AA3BE9DA37
SHA-512:	406D0D0BF1A669E16B9CA101B2DA10C222BBB780DF7B2CB235E2C9F765351846F2A94044C55B0080B875E951FC87462A76B29BE8CD4605EB4D462D321347A49(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/eaf09c/00000000000000000017703/27/d?primer=7cdcb44be4a7db8877ffa5c0007b8dd865b3bbc383831fe2ea177f62257a9191&fvd=n7&v=3
Preview:	wOFFOTTO.....BASE...X...F...Fe!].CFF ...L.....dX.\\DYNA.....GG9GDYN.....1...a....GPOS...P..#...THAH.5GSUB.....0.OS/2.....Y...`] .y.cmap...x...S.....lgasp.....head.....5...6..%ghhea... ...!...$....hmtx.....xg.P.maxp...D.....^P.name.....E..post...d..... ...2.....ideoromn..DFLT..cyrl..grek ..latn.....Y.....x.c`d```5._..._<..W.f..@....^0....~.).....@.....N...x...n.@.....!.V,.@.cGV.FB$m..j.H..6N<i..`O#...@..X.$<.....#g.....x....^}.-.x.S..t1.|.....,=.b..... .....S.J|...e..s.O.....;.]j>z>D.|.|.W...1...R.b.....}muQ..ra...R.3)Fy.....T..1...s..c.g...d8..O....'M.....FW...-...X*..+c...H*....t..].|=.e"..R.....o.fm.....:T.^Q..z...c(.S.....a..w.KN{. l...M]..tu9...k.b.L.N...v...Y..R.[0....1...C*/..8.^...GM..r....jvfx..<.o..t.P.....=Kv-.kr..n.....5.%.9].>q.....f:.3<C.e9.-5.:Yz4O....:e....+b.}.oS..1x.c`f.....).....B3.1.1..E.9..XX

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\d[9]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, CFF, length 67148, version 0.0
Category:	downloaded
Size (bytes):	67148
Entropy (8bit):	**7.993959168595968**
Encrypted:	**true**
SSDEEP:	1536:nxeF+rR7LkiELPhmOHVSAJTtSrsJBD7JVstEBSQm+aScA+tWB:wEkJzh7S2xysvPst2SQSSzR
MD5:	227960928668E1D655DBAAAE5FE23C11
SHA1:	128EF93AB71A18BA1DB0855C165D050ED8702037
SHA-256:	DFD5B4454E0BEF1EBBE0940DFA3BFB117BEE9E3DF150FA55BE633114816E7179
SHA-512:	BDB17CBB62E2C6B4AF737C7201214A563C27CDC38E1924B2C6EB351950F81A06A10E2DFDD783C82AB108D9758D77DA0A45BA82B08C210F4D8977A33AA6364B B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\d[9]	
IE Cache URL:	http://https://use.typekit.net/af/4b3e87/00000000000000000017706/27/d?primer=7cdcb44be4a7db8877ffa5c0007b8dd865b3bbc383831fe2ea177f62257a9191&fvd=n9&v=3
Preview:	wOFFOTTO...L.....BASE...X...F...Fe.].CFF ...T...G...CP...DYNA.....G9GDYN.....1...e. .GPOS.....#...S4...0GSUB...x.....0.OS/2.....Y...`^B{.cmap.....S.....lgasp.....head.....4...6..%phhea...(...!...$....hmtx.....x.nD.maxp...L.....^P.name.....]post..... ...2.....ideoromn..DFLT..cyrl..grek..latn..... ..U.....x.c`d```5.2)1O.....(.p>9..F.W.....5.....;...x...n.0....'E..}..{hZ..8...@29....~hH....;t.#.....y..@.(.5.!.!....RW.....[x...G....65[.....z~..A.?X...rU.....s....#.....<{>F...| ..2.;X..<.P..1Z....}eu^..bi.)c.WR..L...Vb.+]..l.W...1..e:...,#.....z<.:.S.:.....E.....P*...c....T..6..T.. .d..HF.....X...v.~.....G.....9. .Bq\.FX.`.M.c....s..e....h.3v.....8.fH....4gM..+...X ..R....Y..KD....D.....?..=N.<..._.....y.....C...U....[.....~.lN.~.....W..{.\^;..?.._..a...T...t.....K.Y....}...2..x.c`f.`na`e``.b.```...q.F..

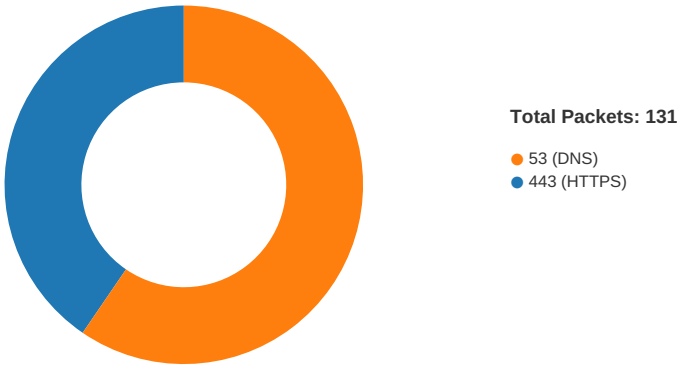
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\free-v4-shims.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	26701
Entropy (8bit):	4.829823522211244
Encrypted:	false
SSDEEP:	192:dP6hT1bll4w0QUmQ10PwKLaAu5CwWavpHo4O6wgLPbJVR8XD7mycP:0hal4w0QK+PwK05eavpmgPPeXD7mycP
MD5:	8A99CE81EC2F89FBCA03F2C8CF1A3679
SHA1:	58F9EF32D12A5DA52CBAB7BD518BCC998FC59EF9
SHA-256:	362DAEAF1F7E05FEE9A609E549F148AACBE518C166FBD96EAD69057E295742AF
SHA-512:	930F28449365FAED13718BB8F332625DB110ABB08C3778DC632FDF00A0187A61A086B5EB4765FFC1923B64E2584C02592A213914B024DE6890FF3DBFC3A12FE5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.3/css/free-v4-shims.min.css?token=585b051251
Preview:	/*!. * Font Awesome Free 5.15.3 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.fa-glass:before{content:"\f000"}.fa.fa-meetup{font-family:"Font Awesome 5 Brands";font-weight:400}.fa.fa-star-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-star-o:before{content:"\f005"}.fa.fa-close:before,.fa.fa-remove:before{content:"\f00d"}.fa.fa-gear:before{content:"\f013"}.fa.fa-trash-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-trash-o:before{content:"\f2ed"}.fa.fa-file-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-file-o:before{content:"\f15b"}.fa.fa-clock-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-clock-o:before{content:"\f017"}.fa.fa-arrow-circle-o-down{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arrow-circle-o-down:before{content:"\f358"}.fa.fa-arrow-circle-o-up{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arro

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 10, 2021 00:13:33.698609114 CEST	49714	443	192.168.2.3	99.86.3.88

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 10, 2021 00:13:33.699453115 CEST	49715	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.716392994 CEST	443	49714	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.716480017 CEST	49714	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.717025995 CEST	443	49715	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.717118025 CEST	49715	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.730917931 CEST	49714	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.731264114 CEST	49715	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.749066114 CEST	443	49715	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.749100924 CEST	443	49714	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.749569893 CEST	443	49715	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.749629021 CEST	443	49715	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.749660969 CEST	49715	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.749692917 CEST	49715	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.750097990 CEST	443	49714	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.750159979 CEST	443	49714	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.750174999 CEST	49714	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.750207901 CEST	49714	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.751389980 CEST	443	49715	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.751454115 CEST	49715	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.752636909 CEST	443	49714	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.752717018 CEST	49714	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.792843103 CEST	49714	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.800923109 CEST	49714	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.801173925 CEST	49714	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.804059982 CEST	49715	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.804426908 CEST	49715	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.811260939 CEST	443	49714	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.811503887 CEST	443	49714	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.811530113 CEST	443	49714	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.811563015 CEST	49714	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.811578989 CEST	49714	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.814867020 CEST	49714	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.819473028 CEST	443	49714	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.819504023 CEST	443	49714	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.819564104 CEST	49714	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.820548058 CEST	443	49714	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.822967052 CEST	443	49715	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.823297977 CEST	443	49715	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.823371887 CEST	49715	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.823394060 CEST	443	49715	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.823430061 CEST	443	49715	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.823443890 CEST	49715	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.823462963 CEST	443	49715	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.823508024 CEST	49715	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.824028969 CEST	49715	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.834805965 CEST	443	49714	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.843689919 CEST	443	49715	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.976757050 CEST	443	49714	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.976810932 CEST	443	49714	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.976844072 CEST	49714	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.976880074 CEST	49714	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.976895094 CEST	443	49714	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.976946115 CEST	49714	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.976989031 CEST	443	49714	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.977049112 CEST	443	49714	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.977062941 CEST	49714	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.977097034 CEST	49714	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.977135897 CEST	443	49714	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.977189064 CEST	49714	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:33.977255106 CEST	443	49714	99.86.3.88	192.168.2.3
Apr 10, 2021 00:13:33.977308035 CEST	49714	443	192.168.2.3	99.86.3.88
Apr 10, 2021 00:13:34.226249933 CEST	49717	443	192.168.2.3	13.32.25.66
Apr 10, 2021 00:13:34.226324081 CEST	49718	443	192.168.2.3	13.32.25.66
Apr 10, 2021 00:13:34.226382017 CEST	49719	443	192.168.2.3	13.32.25.66

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 10, 2021 00:13:34.226537943 CEST	49721	443	192.168.2.3	13.32.25.66
Apr 10, 2021 00:13:34.228977919 CEST	49720	443	192.168.2.3	13.32.25.66
Apr 10, 2021 00:13:34.246128082 CEST	443	49717	13.32.25.66	192.168.2.3
Apr 10, 2021 00:13:34.246243000 CEST	49717	443	192.168.2.3	13.32.25.66
Apr 10, 2021 00:13:34.246294022 CEST	443	49719	13.32.25.66	192.168.2.3
Apr 10, 2021 00:13:34.246332884 CEST	443	49721	13.32.25.66	192.168.2.3
Apr 10, 2021 00:13:34.246375084 CEST	49719	443	192.168.2.3	13.32.25.66
Apr 10, 2021 00:13:34.246396065 CEST	49721	443	192.168.2.3	13.32.25.66
Apr 10, 2021 00:13:34.246838093 CEST	443	49718	13.32.25.66	192.168.2.3
Apr 10, 2021 00:13:34.246905088 CEST	49718	443	192.168.2.3	13.32.25.66
Apr 10, 2021 00:13:34.247765064 CEST	49719	443	192.168.2.3	13.32.25.66
Apr 10, 2021 00:13:34.247931957 CEST	49721	443	192.168.2.3	13.32.25.66
Apr 10, 2021 00:13:34.248065948 CEST	49718	443	192.168.2.3	13.32.25.66
Apr 10, 2021 00:13:34.248238087 CEST	49717	443	192.168.2.3	13.32.25.66
Apr 10, 2021 00:13:34.248339891 CEST	443	49720	13.32.25.66	192.168.2.3
Apr 10, 2021 00:13:34.248415947 CEST	49720	443	192.168.2.3	13.32.25.66
Apr 10, 2021 00:13:34.248977900 CEST	49720	443	192.168.2.3	13.32.25.66
Apr 10, 2021 00:13:34.267683029 CEST	443	49718	13.32.25.66	192.168.2.3
Apr 10, 2021 00:13:34.267718077 CEST	443	49721	13.32.25.66	192.168.2.3
Apr 10, 2021 00:13:34.267744064 CEST	443	49719	13.32.25.66	192.168.2.3
Apr 10, 2021 00:13:34.268086910 CEST	443	49717	13.32.25.66	192.168.2.3
Apr 10, 2021 00:13:34.268198967 CEST	443	49720	13.32.25.66	192.168.2.3
Apr 10, 2021 00:13:34.270477057 CEST	443	49721	13.32.25.66	192.168.2.3
Apr 10, 2021 00:13:34.270565987 CEST	443	49721	13.32.25.66	192.168.2.3
Apr 10, 2021 00:13:34.270627975 CEST	49721	443	192.168.2.3	13.32.25.66
Apr 10, 2021 00:13:34.270647049 CEST	443	49719	13.32.25.66	192.168.2.3
Apr 10, 2021 00:13:34.270657063 CEST	49721	443	192.168.2.3	13.32.25.66
Apr 10, 2021 00:13:34.270720959 CEST	49719	443	192.168.2.3	13.32.25.66
Apr 10, 2021 00:13:34.270740986 CEST	443	49719	13.32.25.66	192.168.2.3
Apr 10, 2021 00:13:34.270781994 CEST	443	49718	13.32.25.66	192.168.2.3
Apr 10, 2021 00:13:34.270801067 CEST	49719	443	192.168.2.3	13.32.25.66
Apr 10, 2021 00:13:34.270821095 CEST	443	49718	13.32.25.66	192.168.2.3
Apr 10, 2021 00:13:34.270850897 CEST	49718	443	192.168.2.3	13.32.25.66
Apr 10, 2021 00:13:34.270858049 CEST	443	49717	13.32.25.66	192.168.2.3
Apr 10, 2021 00:13:34.270876884 CEST	49718	443	192.168.2.3	13.32.25.66

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 10, 2021 00:13:26.084743023 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:26.098263025 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:26.743391991 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:26.756259918 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:28.783396006 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:28.796034098 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:29.785873890 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:29.800055981 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:30.875521898 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:30.888339996 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:31.794219971 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:31.806829929 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:32.640404940 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:32.658068895 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:32.907984018 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:32.920464039 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:33.666501999 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:33.685065985 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:33.987905025 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:34.002188921 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:34.028723955 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:34.052000046 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:34.327567101 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:34.345911980 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:34.785366058 CEST	51352	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 10, 2021 00:13:34.798561096 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:34.900216103 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:34.918562889 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:34.984005928 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:34.995883942 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:37.096035004 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:37.108901024 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:37.751969099 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:37.763875961 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:38.394282103 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:38.406500101 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:39.140880108 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:39.153683901 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:40.309778929 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:40.322937965 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:41.017162085 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:41.030693054 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:41.990106106 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:42.002836943 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:42.788173914 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:42.800685883 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:50.329257011 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:50.348932981 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:55.412990093 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:55.440908909 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:56.311939001 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:56.321948051 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:56.327569962 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:56.334685087 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:56.338673115 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:56.346791029 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:56.347423077 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:56.369658947 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:56.372658014 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:56.388122082 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:56.716064930 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:56.740333080 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:56.897068977 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:56.916155100 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:58.844281912 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:58.864701986 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 10, 2021 00:13:58.967509985 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:13:58.997611046 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:00.357062101 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:00.405704975 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:02.666625023 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:02.680577040 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:03.292304993 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:03.304373980 CEST	53	58784	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:03.688955069 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:03.700861931 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:04.158212900 CEST	63978	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:04.176050901 CEST	53	63978	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:04.189017057 CEST	62938	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:04.210196972 CEST	53	62938	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:04.231224060 CEST	55708	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:04.244791985 CEST	53	55708	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:04.282654047 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:04.294415951 CEST	53	58784	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:04.520596027 CEST	56803	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:04.540147066 CEST	53	56803	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:04.613967896 CEST	57145	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:04.632487059 CEST	53	57145	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:04.701109886 CEST	59420	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 10, 2021 00:14:04.712992907 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:04.743746996 CEST	55359	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:04.772862911 CEST	53	55359	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:05.335861921 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:05.349673986 CEST	53	58784	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:05.568598986 CEST	58306	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:06.603461027 CEST	58306	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:06.622138977 CEST	53	58306	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:07.407435894 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:07.420248985 CEST	53	58784	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:07.452305079 CEST	64124	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:07.465358019 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:07.478389025 CEST	53	64124	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:07.482660055 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:08.104727983 CEST	49361	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:08.144102097 CEST	53	49361	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:08.186899900 CEST	63150	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:08.208889008 CEST	53	63150	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:08.289767981 CEST	53279	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:08.310302973 CEST	53	53279	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:09.035003901 CEST	56881	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:09.055123091 CEST	53	56881	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:09.468426943 CEST	53642	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:09.478692055 CEST	55667	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:09.488442898 CEST	53	53642	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:09.517644882 CEST	53	55667	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:09.881845951 CEST	54833	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:09.904239893 CEST	53	54833	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:09.921065092 CEST	62476	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:09.938982010 CEST	53	62476	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:10.509546041 CEST	49705	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:10.524863958 CEST	53	49705	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:11.062341928 CEST	61477	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:11.074913025 CEST	53	61477	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:11.199322939 CEST	61633	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:11.211601019 CEST	55949	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:11.212421894 CEST	53	61633	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:11.226878881 CEST	53	55949	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:11.423629045 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:11.435487986 CEST	53	58784	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:11.457293987 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:11.469759941 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:11.647739887 CEST	57601	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:11.660322905 CEST	49342	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:11.663407087 CEST	53	57601	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:11.699817896 CEST	53	49342	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:11.838848114 CEST	56253	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:11.852219105 CEST	53	56253	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:11.949879885 CEST	49667	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:11.962807894 CEST	53	49667	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:12.579571009 CEST	55439	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:12.598095894 CEST	53	55439	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:21.035571098 CEST	57069	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:21.049418926 CEST	53	57069	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:35.207228899 CEST	57659	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:35.225761890 CEST	53	57659	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:46.687089920 CEST	54717	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:46.721230984 CEST	53	54717	8.8.8.8	192.168.2.3
Apr 10, 2021 00:14:57.048913002 CEST	63975	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:14:57.061575890 CEST	53	63975	8.8.8.8	192.168.2.3
Apr 10, 2021 00:15:01.624288082 CEST	56639	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:15:01.642493963 CEST	53	56639	8.8.8.8	192.168.2.3
Apr 10, 2021 00:15:31.531090975 CEST	51856	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:15:31.543818951 CEST	53	51856	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 10, 2021 00:15:34.028466940 CEST	56546	53	192.168.2.3	8.8.8.8
Apr 10, 2021 00:15:34.054826021 CEST	53	56546	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 10, 2021 00:13:34.028723955 CEST	192.168.2.3	8.8.8.8	0x290a	Standard query (0)	page.adobe spark-assets.com	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:34.327567101 CEST	192.168.2.3	8.8.8.8	0x274	Standard query (0)	use.typekit.net	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:34.785366058 CEST	192.168.2.3	8.8.8.8	0x46e	Standard query (0)	s3.amazonaws.com	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:34.900216103 CEST	192.168.2.3	8.8.8.8	0x18e8	Standard query (0)	p.typekit.net	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:50.329257011 CEST	192.168.2.3	8.8.8.8	0xa581	Standard query (0)	page.adobe spark-assets.com	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:55.412990093 CEST	192.168.2.3	8.8.8.8	0x5c4d	Standard query (0)	nicklaussglen.buzz	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:56.321948051 CEST	192.168.2.3	8.8.8.8	0x775d	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:56.327569962 CEST	192.168.2.3	8.8.8.8	0x93af	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:56.369658947 CEST	192.168.2.3	8.8.8.8	0x1b55	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:56.716064930 CEST	192.168.2.3	8.8.8.8	0xe178	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:56.897068977 CEST	192.168.2.3	8.8.8.8	0xa7d	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:58.967509985 CEST	192.168.2.3	8.8.8.8	0x64c1	Standard query (0)	clientconfig.passport.net	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:04.158212900 CEST	192.168.2.3	8.8.8.8	0x6fd6	Standard query (0)	assets.adobedtm.com	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:04.189017057 CEST	192.168.2.3	8.8.8.8	0x1a50	Standard query (0)	cdn.cookielaw.org	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:04.520596027 CEST	192.168.2.3	8.8.8.8	0x2079	Standard query (0)	dpm.demdex.net	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:04.613967896 CEST	192.168.2.3	8.8.8.8	0x63df	Standard query (0)	geolocation.onetrust.com	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:05.568598986 CEST	192.168.2.3	8.8.8.8	0x33af	Standard query (0)	api.demandbase.com	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:06.603461027 CEST	192.168.2.3	8.8.8.8	0x33af	Standard query (0)	api.demandbase.com	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:07.452305079 CEST	192.168.2.3	8.8.8.8	0x1195	Standard query (0)	static.adobelogin.com	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:08.186899900 CEST	192.168.2.3	8.8.8.8	0x7518	Standard query (0)	adobe.tt.omtrdc.net	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:09.468426943 CEST	192.168.2.3	8.8.8.8	0x8f2f	Standard query (0)	adobe.demdex.net	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:09.478692055 CEST	192.168.2.3	8.8.8.8	0xed83	Standard query (0)	cm.everesttech.net	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:09.881845951 CEST	192.168.2.3	8.8.8.8	0xea2	Standard query (0)	ims-na1.adobelogin.com	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:11.062341928 CEST	192.168.2.3	8.8.8.8	0xed96	Standard query (0)	aa.agkn.com	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:11.199322939 CEST	192.168.2.3	8.8.8.8	0x3e4a	Standard query (0)	adobedc.demdex.net	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:11.211601019 CEST	192.168.2.3	8.8.8.8	0x46af	Standard query (0)	sync.mathtag.com	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:11.647739887 CEST	192.168.2.3	8.8.8.8	0xa420	Standard query (0)	idsync.rlcdn.com	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:11.660322905 CEST	192.168.2.3	8.8.8.8	0x113d	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:11.949879885 CEST	192.168.2.3	8.8.8.8	0x8668	Standard query (0)	www.google.ch	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:12.579571009 CEST	192.168.2.3	8.8.8.8	0x2490	Standard query (0)	ds-aksb-a.akamaihd.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 10, 2021 00:13:33.685065985 CEST	8.8.8.8	192.168.2.3	0xd6ac	No error (0)	spark.adobeprojectm.com		99.86.3.88	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 10, 2021 00:13:33.685065985 CEST	8.8.8.8	192.168.2.3	0xd6ac	No error (0)	spark.adobeprojectm.com		99.86.3.6	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:33.685065985 CEST	8.8.8.8	192.168.2.3	0xd6ac	No error (0)	spark.adobeprojectm.com		99.86.3.34	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:33.685065985 CEST	8.8.8.8	192.168.2.3	0xd6ac	No error (0)	spark.adobeprojectm.com		99.86.3.17	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:34.052000046 CEST	8.8.8.8	192.168.2.3	0x290a	No error (0)	page.adobespark-assets.com		13.32.25.66	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:34.052000046 CEST	8.8.8.8	192.168.2.3	0x290a	No error (0)	page.adobespark-assets.com		13.32.25.7	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:34.052000046 CEST	8.8.8.8	192.168.2.3	0x290a	No error (0)	page.adobespark-assets.com		13.32.25.45	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:34.052000046 CEST	8.8.8.8	192.168.2.3	0x290a	No error (0)	page.adobespark-assets.com		13.32.25.102	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:34.345911980 CEST	8.8.8.8	192.168.2.3	0x274	No error (0)	use.typekit.net	use-stls.adobe.com.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 00:13:34.798561096 CEST	8.8.8.8	192.168.2.3	0x46e	No error (0)	s3.amazonaws.com		52.216.239.117	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:34.918562889 CEST	8.8.8.8	192.168.2.3	0x18e8	No error (0)	p.typekit.net	p.typekit.net-v3.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 00:13:50.348932981 CEST	8.8.8.8	192.168.2.3	0xa581	No error (0)	page.adobespark-assets.com		13.32.25.45	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:50.348932981 CEST	8.8.8.8	192.168.2.3	0xa581	No error (0)	page.adobespark-assets.com		13.32.25.66	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:50.348932981 CEST	8.8.8.8	192.168.2.3	0xa581	No error (0)	page.adobespark-assets.com		13.32.25.7	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:50.348932981 CEST	8.8.8.8	192.168.2.3	0xa581	No error (0)	page.adobespark-assets.com		13.32.25.102	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:55.440908909 CEST	8.8.8.8	192.168.2.3	0x5c4d	No error (0)	nicklaussglen.buzz		172.67.169.45	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:55.440908909 CEST	8.8.8.8	192.168.2.3	0x5c4d	No error (0)	nicklaussglen.buzz		104.21.95.21	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:56.334685087 CEST	8.8.8.8	192.168.2.3	0x775d	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 00:13:56.347423077 CEST	8.8.8.8	192.168.2.3	0x93af	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:56.347423077 CEST	8.8.8.8	192.168.2.3	0x93af	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:56.388122082 CEST	8.8.8.8	192.168.2.3	0x1b55	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 00:13:56.740333080 CEST	8.8.8.8	192.168.2.3	0xe178	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:56.740333080 CEST	8.8.8.8	192.168.2.3	0xe178	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Apr 10, 2021 00:13:56.916155100 CEST	8.8.8.8	192.168.2.3	0xa7d	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 00:13:58.997611046 CEST	8.8.8.8	192.168.2.3	0x64c1	No error (0)	clientconfig.passport.net	authgfx.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 00:14:04.176050901 CEST	8.8.8.8	192.168.2.3	0x6fd6	No error (0)	assets.adobedtm.com	cn-assets.adobedtm.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 00:14:04.210196972 CEST	8.8.8.8	192.168.2.3	0x1a50	No error (0)	cdn.cookielaw.org		104.16.148.64	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 10, 2021 00:14:04.210196972 CEST	8.8.8.8	192.168.2.3	0x1a50	No error (0)	cdn.cookielaw.org		104.16.149.64	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:04.540147066 CEST	8.8.8.8	192.168.2.3	0x2079	No error (0)	dpm.demdex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 00:14:04.540147066 CEST	8.8.8.8	192.168.2.3	0x2079	No error (0)	gslb-2.demdex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 00:14:04.540147066 CEST	8.8.8.8	192.168.2.3	0x2079	No error (0)	edge-irl1.demdex.net	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 00:14:04.540147066 CEST	8.8.8.8	192.168.2.3	0x2079	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.30.135.179	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:04.540147066 CEST	8.8.8.8	192.168.2.3	0x2079	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		108.128.151.168	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:04.540147066 CEST	8.8.8.8	192.168.2.3	0x2079	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.212.101.97	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:04.540147066 CEST	8.8.8.8	192.168.2.3	0x2079	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.246.133.154	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:04.540147066 CEST	8.8.8.8	192.168.2.3	0x2079	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.17.73.77	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:04.540147066 CEST	8.8.8.8	192.168.2.3	0x2079	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.49.59.93	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:04.540147066 CEST	8.8.8.8	192.168.2.3	0x2079	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		108.128.151.98	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:04.540147066 CEST	8.8.8.8	192.168.2.3	0x2079	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		63.33.120.132	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:04.632487059 CEST	8.8.8.8	192.168.2.3	0x63df	No error (0)	geolocation.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:04.632487059 CEST	8.8.8.8	192.168.2.3	0x63df	No error (0)	geolocation.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:04.772862911 CEST	8.8.8.8	192.168.2.3	0x910e	No error (0)	adobe.com.ssl.d1.sc.omtrdc.net		35.181.18.61	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:04.772862911 CEST	8.8.8.8	192.168.2.3	0x910e	No error (0)	adobe.com.ssl.d1.sc.omtrdc.net		15.237.136.106	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:04.772862911 CEST	8.8.8.8	192.168.2.3	0x910e	No error (0)	adobe.com.ssl.d1.sc.omtrdc.net		15.237.76.117	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:06.622138977 CEST	8.8.8.8	192.168.2.3	0x33af	No error (0)	api.demandbase.com		99.86.3.69	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:06.622138977 CEST	8.8.8.8	192.168.2.3	0x33af	No error (0)	api.demandbase.com		99.86.3.61	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:06.622138977 CEST	8.8.8.8	192.168.2.3	0x33af	No error (0)	api.demandbase.com		99.86.3.93	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:06.622138977 CEST	8.8.8.8	192.168.2.3	0x33af	No error (0)	api.demandbase.com		99.86.3.127	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:07.478389025 CEST	8.8.8.8	192.168.2.3	0x1195	No error (0)	static.adobelogin.com	adobelogin-static.prod.ims.adobejanus.com		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 00:14:07.478389025 CEST	8.8.8.8	192.168.2.3	0x1195	No error (0)	adobelogin-static.prod.ims.adobejanus.com	dd20fzx9mj46f.cloudfront.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 10, 2021 00:14:07.478389025 CEST	8.8.8.8	192.168.2.3	0x1195	No error (0)	dd20fzx9mj46f.cloudfront.net		13.32.16.66	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:08.208889008 CEST	8.8.8.8	192.168.2.3	0x7518	No error (0)	adobe.tt.omtrdc.net		52.212.164.82	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:08.208889008 CEST	8.8.8.8	192.168.2.3	0x7518	No error (0)	adobe.tt.omtrdc.net		34.252.156.174	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:08.208889008 CEST	8.8.8.8	192.168.2.3	0x7518	No error (0)	adobe.tt.omtrdc.net		34.252.166.160	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:08.208889008 CEST	8.8.8.8	192.168.2.3	0x7518	No error (0)	adobe.tt.omtrdc.net		52.213.168.74	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:08.208889008 CEST	8.8.8.8	192.168.2.3	0x7518	No error (0)	adobe.tt.omtrdc.net		52.18.150.20	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:08.208889008 CEST	8.8.8.8	192.168.2.3	0x7518	No error (0)	adobe.tt.omtrdc.net		52.51.251.137	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:08.208889008 CEST	8.8.8.8	192.168.2.3	0x7518	No error (0)	adobe.tt.omtrdc.net		18.203.205.32	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:08.208889008 CEST	8.8.8.8	192.168.2.3	0x7518	No error (0)	adobe.tt.omtrdc.net		52.19.133.54	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:09.055123091 CEST	8.8.8.8	192.168.2.3	0xdab8	No error (0)	services.prod.ims.adobejanus.com		52.16.185.223	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:09.055123091 CEST	8.8.8.8	192.168.2.3	0xdab8	No error (0)	services.prod.ims.adobejanus.com		46.137.124.64	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:09.055123091 CEST	8.8.8.8	192.168.2.3	0xdab8	No error (0)	services.prod.ims.adobejanus.com		54.76.80.163	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:09.055123091 CEST	8.8.8.8	192.168.2.3	0xdab8	No error (0)	services.prod.ims.adobejanus.com		52.213.176.171	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:09.055123091 CEST	8.8.8.8	192.168.2.3	0xdab8	No error (0)	services.prod.ims.adobejanus.com		54.73.76.208	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:09.055123091 CEST	8.8.8.8	192.168.2.3	0xdab8	No error (0)	services.prod.ims.adobejanus.com		34.249.255.145	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:09.488442898 CEST	8.8.8.8	192.168.2.3	0x8f2f	No error (0)	adobe.demdex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 00:14:09.488442898 CEST	8.8.8.8	192.168.2.3	0x8f2f	No error (0)	gslb-2.demdex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 00:14:09.488442898 CEST	8.8.8.8	192.168.2.3	0x8f2f	No error (0)	edge-irl1.demdex.net	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 00:14:09.488442898 CEST	8.8.8.8	192.168.2.3	0x8f2f	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.251.60.147	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:09.488442898 CEST	8.8.8.8	192.168.2.3	0x8f2f	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.246.39.225	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:09.488442898 CEST	8.8.8.8	192.168.2.3	0x8f2f	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.50.19.208	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:09.488442898 CEST	8.8.8.8	192.168.2.3	0x8f2f	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.246.92.224	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:09.488442898 CEST	8.8.8.8	192.168.2.3	0x8f2f	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.49.59.93	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:09.488442898 CEST	8.8.8.8	192.168.2.3	0x8f2f	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.171.219.200	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 10, 2021 00:14:09.488442898 CEST	8.8.8.8	192.168.2.3	0x8f2f	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.30.200.197	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:09.488442898 CEST	8.8.8.8	192.168.2.3	0x8f2f	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.30.135.179	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:09.517644882 CEST	8.8.8.8	192.168.2.3	0xed83	No error (0)	cm.everesttech.net	cm.everesttech.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 00:14:09.904239893 CEST	8.8.8.8	192.168.2.3	0xea2	No error (0)	ims-na1.adobelogin.com	adobelogin.prod.ims.adobejanus.com		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 00:14:09.904239893 CEST	8.8.8.8	192.168.2.3	0xea2	No error (0)	adobelogin.prod.ims.adobejanus.com	adobelogin-origin.prod.ims.adobejanus.com		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 00:14:09.904239893 CEST	8.8.8.8	192.168.2.3	0xea2	No error (0)	adobelogin-origin.prod.ims.adobejanus.com		54.73.76.208	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:09.904239893 CEST	8.8.8.8	192.168.2.3	0xea2	No error (0)	adobelogin-origin.prod.ims.adobejanus.com		46.137.124.64	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:09.904239893 CEST	8.8.8.8	192.168.2.3	0xea2	No error (0)	adobelogin-origin.prod.ims.adobejanus.com		54.76.80.163	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:09.904239893 CEST	8.8.8.8	192.168.2.3	0xea2	No error (0)	adobelogin-origin.prod.ims.adobejanus.com		52.213.176.171	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:09.904239893 CEST	8.8.8.8	192.168.2.3	0xea2	No error (0)	adobelogin-origin.prod.ims.adobejanus.com		34.249.255.145	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:09.904239893 CEST	8.8.8.8	192.168.2.3	0xea2	No error (0)	adobelogin-origin.prod.ims.adobejanus.com		52.16.185.223	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:11.074913025 CEST	8.8.8.8	192.168.2.3	0xed96	No error (0)	aa.agkn.com	aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 00:14:11.074913025 CEST	8.8.8.8	192.168.2.3	0xed96	No error (0)	aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com		3.127.52.31	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:11.074913025 CEST	8.8.8.8	192.168.2.3	0xed96	No error (0)	aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com		52.28.42.15	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:11.074913025 CEST	8.8.8.8	192.168.2.3	0xed96	No error (0)	aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com		52.29.225.117	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:11.074913025 CEST	8.8.8.8	192.168.2.3	0xed96	No error (0)	aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com		52.58.248.2	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:11.212421894 CEST	8.8.8.8	192.168.2.3	0x3e4a	No error (0)	adobedc.demdex.net	demdex.net.ssl.sc.omtrdc.net		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 00:14:11.212421894 CEST	8.8.8.8	192.168.2.3	0x3e4a	No error (0)	demdex.net.ssl.sc.omtrdc.net		15.237.136.106	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:11.212421894 CEST	8.8.8.8	192.168.2.3	0x3e4a	No error (0)	demdex.net.ssl.sc.omtrdc.net		35.181.18.61	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:11.212421894 CEST	8.8.8.8	192.168.2.3	0x3e4a	No error (0)	demdex.net.ssl.sc.omtrdc.net		15.237.76.117	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 10, 2021 00:14:11.226878881 CEST	8.8.8.8	192.168.2.3	0x46af	No error (0)	sync.mathtag.com	pixel-origin.mathtag.com		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 00:14:11.226878881 CEST	8.8.8.8	192.168.2.3	0x46af	No error (0)	pixel-origin.mathtag.com		185.29.132.69	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:11.226878881 CEST	8.8.8.8	192.168.2.3	0x46af	No error (0)	pixel-origin.mathtag.com		185.29.132.68	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:11.226878881 CEST	8.8.8.8	192.168.2.3	0x46af	No error (0)	pixel-origin.mathtag.com		185.29.133.208	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:11.226878881 CEST	8.8.8.8	192.168.2.3	0x46af	No error (0)	pixel-origin.mathtag.com		185.29.135.233	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:11.663407087 CEST	8.8.8.8	192.168.2.3	0xa420	No error (0)	idsync.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:11.699817896 CEST	8.8.8.8	192.168.2.3	0x113d	No error (0)	googleads.g.doubleclick.net		172.217.168.66	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:11.962807894 CEST	8.8.8.8	192.168.2.3	0x8668	No error (0)	www.google.ch		216.58.215.227	A (IP address)	IN (0x0001)
Apr 10, 2021 00:14:12.598095894 CEST	8.8.8.8	192.168.2.3	0x2490	No error (0)	ds-aksb-a.akamaihd.net	ds-aksb-a.akamaihd.net.edgesuite.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- nicklaussglen.buzz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49739	172.67.169.45	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Apr 10, 2021 00:13:55.476660967 CEST	2620	OUT	GET /011 HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: nicklaussglen.buzz Connection: Keep-Alive
Apr 10, 2021 00:13:55.516447067 CEST	2621	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 09 Apr 2021 22:13:55 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Fri, 09 Apr 2021 23:13:55 GMT Location: https://nicklaussglen.buzz/011 cf-request-id: 095a4bfea5000008ab501cd000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=PREWFLNt7%2FsNGUfhgonfbOB6Mq6tm%2FaMjcKSzO9vVtRItdLuOvwq62ExLlr6iL8HrSZkfBWqAwkREz5zpKzQhPrwIUSYHJnULa122NdxJnoVVCA%3D"}]} NEL: {"max_age":604800,"report_to":"cf-nel"} Vary: Accept-Encoding Server: cloudflare CF-RAY: 63d715dddafa08ab-CDG alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Apr 10, 2021 00:13:56.028934002 CEST	2627	OUT	GET /011/ HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: nicklaussglen.buzz

Timestamp	kBytes transferred	Direction	Data
Apr 10, 2021 00:13:56.064976931 CEST	2628	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 09 Apr 2021 22:13:56 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Fri, 09 Apr 2021 23:13:56 GMT Location: https://nicklaussglen.buzz/011/ cf-request-id: 095a4c00ce000008abe9048000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=j6pb2TibtiS85oxLE9iV0c9h0O4e0jmRjQkmP6TzxIHFGPh2lNvDu2kPPGSExhro3re0DoMPl7nie1r9g7ZEGbCJ9yFGZgzmV2G5B7cqGRY5uNg%3D"}]} NEL: {"max_age":604800,"report_to":"cf-nel"} Vary: Accept-Encoding Server: cloudflare CF-RAY: 63d715e14b5808ab-CDG alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

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
Apr 10, 2021 00:13:33.751389980 CEST	99.86.3.88	443	192.168.2.3	49715	CN=spark.adobe.com, OU=IT, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jun 05 02:00:00 CEST 2020	Fri Jun 10 14:00:00 CEST 2022	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Apr 10, 2021 00:13:33.752636909 CEST	99.86.3.88	443	192.168.2.3	49714	CN=spark.adobe.com, OU=IT, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jun 05 02:00:00 CEST 2020	Fri Jun 10 14:00:00 CEST 2022	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Apr 10, 2021 00:13:34.274477959 CEST	13.32.25.66	443	192.168.2.3	49718	CN=spark.adobe.com, OU=IT, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jun 05 02:00:00 CEST 2020	Fri Jun 10 14:00:00 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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Apr 10, 2021 00:13:34.274578094 CEST	13.32.25.66	443	192.168.2.3	49721	CN=spark.adobe.com, OU=IT, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jun 05 02:00:00 CEST 2020	Fri Jun 10 14:00:00 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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

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 SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Apr 10, 2021 00:13:34.274692059 CEST	13.32.25.66	443	192.168.2.3	49717	CN=spark.adobe.com, OU=IT, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jun 05 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Fri Jun 10 14:00:00 CEST 2022 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Apr 10, 2021 00:13:34.275279999 CEST	13.32.25.66	443	192.168.2.3	49719	CN=spark.adobe.com, OU=IT, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jun 05 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Fri Jun 10 14:00:00 CEST 2022 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Apr 10, 2021 00:13:34.276529074 CEST	13.32.25.66	443	192.168.2.3	49720	CN=spark.adobe.com, OU=IT, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jun 05 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Fri Jun 10 14:00:00 CEST 2022 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Apr 10, 2021 00:13:35.003166914 CEST	52.216.239.117	443	192.168.2.3	49725	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Apr 10, 2021 00:13:35.004014015 CEST	52.216.239.117	443	192.168.2.3	49724	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 10, 2021 00:13:55.797686100 CEST	172.67.169.45	443	192.168.2.3	49740	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, 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	Fri Apr 09 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Sat Apr 09 01:59:59 CEST 2022 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		
Apr 10, 2021 00:13:56.384464025 CEST	104.18.10.207	443	192.168.2.3	49745	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, 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	Mon Mar 01 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Tue Mar 01 00:59:59 CET 2022 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		
Apr 10, 2021 00:13:56.388806105 CEST	104.18.10.207	443	192.168.2.3	49746	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, 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	Mon Mar 01 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Tue Mar 01 00:59:59 CET 2022 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		
Apr 10, 2021 00:13:56.777604103 CEST	104.16.19.94	443	192.168.2.3	49751	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		
Apr 10, 2021 00:13:56.851736069 CEST	104.16.19.94	443	192.168.2.3	49752	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 10, 2021 00:14:04.289658070 CEST	104.16.148.64	443	192.168.2.3	49764	CN=cookielaw.org, 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 Jul 01 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Jul 01 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 10, 2021 00:14:04.292761087 CEST	104.16.148.64	443	192.168.2.3	49763	CN=cookielaw.org, 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 Jul 01 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Jul 01 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 10, 2021 00:14:04.625648975 CEST	52.30.135.179	443	192.168.2.3	49766	CN=*.demdex.net, OU=Digital Marketing, O=Adobe Systems Incorporated, L=San Jose, ST=California, 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	Wed Dec 02 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Mon Jan 03 00:59:59 CET 2022 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		
Apr 10, 2021 00:14:04.627218962 CEST	52.30.135.179	443	192.168.2.3	49765	CN=*.demdex.net, OU=Digital Marketing, O=Adobe Systems Incorporated, L=San Jose, ST=California, 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	Wed Dec 02 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Mon Jan 03 00:59:59 CET 2022 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 10, 2021 00:14:04.661990881 CEST	104.20.184.68	443	192.168.2.3	49767	CN=onetrust.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, 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	Fri Feb 12 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Sat Feb 12 00:59:59 CET 2022 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		
Apr 10, 2021 00:14:04.662791014 CEST	104.20.184.68	443	192.168.2.3	49768	CN=onetrust.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, 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	Fri Feb 12 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Sat Feb 12 00:59:59 CET 2022 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		
Apr 10, 2021 00:14:04.826406002 CEST	35.181.18.61	443	192.168.2.3	49772	CN=sstats.adobe.com, O=Adobe Systems Incorporated, L=San Jose, 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	Mon May 18 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 25 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					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		
Apr 10, 2021 00:14:04.827088118 CEST	35.181.18.61	443	192.168.2.3	49771	CN=sstats.adobe.com, O=Adobe Systems Incorporated, L=San Jose, 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	Mon May 18 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 25 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					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		
Apr 10, 2021 00:14:06.666062117 CEST	99.86.3.69	443	192.168.2.3	49774	CN=api.demandbase.com, O="Demandbase, Inc.", L=San Francisco, ST=California, C=US, SERIALNUMBER=C3920817, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.2=California, OID.1.3.6.1.4.1.311.60.2.1.3=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Fri Oct 09 23:16:41 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Thu Oct 28 02:17:28 CEST 2021 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Apr 10, 2021 00:14:06.680181980 CEST	99.86.3.69	443	192.168.2.3	49775	CN=api.demandbase.com, O="Demandbase, Inc.", L=San Francisco, ST=California, C=US, SERIALNUMBER=C3920817, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.2=California, OID.1.3.6.1.4.1.311.60.2.1.3=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Fri Oct 09 23:16:41 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Thu Oct 28 02:17:28 CEST 2021 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Apr 10, 2021 00:14:07.572196007 CEST	13.32.16.66	443	192.168.2.3	49777	CN=static.adobelogin.com, OU=IT, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 18 02:00:00 CEST 2019 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Wed Sep 22 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 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 SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 10, 2021 00:14:07.572917938 CEST	13.32.16.66	443	192.168.2.3	49776	CN=static.adobelogin.com, OU=IT, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 18 02:00:00 CEST 2019 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Wed Sep 22 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 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 SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					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		
Apr 10, 2021 00:14:08.346175909 CEST	52.212.164.82	443	192.168.2.3	49779	CN=*.tt.omtrdc.net, O=Adobe Inc., L=SAN JOSE, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 02 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Wed Nov 10 00:59:59 CET 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Apr 10, 2021 00:14:09.143362045 CEST	52.16.185.223	443	192.168.2.3	49782	CN=ims-na1.adobelogin.com, O=Adobe Inc., L=San Jose, ST=ca, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Feb 24 01:00:00 CET 2021 Wed Sep 23 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Tue Mar 01 00:59:59 CET 2022 Mon Sep 23 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 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		
Apr 10, 2021 00:14:09.606714010 CEST	34.251.60.147	443	192.168.2.3	49783	CN=*.demdex.net, OU=Digital Marketing, O=Adobe Systems Incorporated, L=San Jose, ST=California, 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	Wed Dec 02 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Mon Jan 03 00:59:59 CET 2022 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		
Apr 10, 2021 00:14:09.629462957 CEST	34.251.60.147	443	192.168.2.3	49784	CN=*.demdex.net, OU=Digital Marketing, O=Adobe Systems Incorporated, L=San Jose, ST=California, 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	Wed Dec 02 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Mon Jan 03 00:59:59 CET 2022 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		
Apr 10, 2021 00:14:10.224874973 CEST	54.73.76.208	443	192.168.2.3	49787	CN=ims-na1.adobelogin.com, O=Adobe Inc., L=San Jose, ST=ca, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Feb 24 01:00:00 CET 2021 Wed Sep 23 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Tue Mar 01 00:59:59 CET 2022 Mon Sep 23 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 SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 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		
Apr 10, 2021 00:14:10.226058006 CEST	54.73.76.208	443	192.168.2.3	49788	CN=ims-na1.adobelogin.com, O=Adobe Inc., L=San Jose, ST=ca, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Feb 24 01:00:00 CET 2021 Wed Sep 23 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Tue Mar 01 00:59:59 CET 2022 Mon Sep 23 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 SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		

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 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		
Apr 10, 2021 00:14:11.150460958 CEST	3.127.52.31	443	192.168.2.3	49793	CN=*.agkn.com CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, 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	Sat Jul 25 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006 Mon Nov 06 13:23:33 CET 2017	Sun Sep 18 14:00:00 CEST 2022 Mon Nov 10 01:00:00 CET 2031 Sat Nov 06 13:23:33 CET 2027	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 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		
					CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Apr 10, 2021 00:14:11.170991898 CEST	3.127.52.31	443	192.168.2.3	49794	CN=*.agkn.com CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, 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	Sat Jul 25 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006 Mon Nov 06 13:23:33 CET 2017	Sun Sep 18 14:00:00 CEST 2022 Mon Nov 10 01:00:00 CET 2031 Sat Nov 06 13:23:33 CET 2027	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 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		
					CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Apr 10, 2021 00:14:11.254590988 CEST	185.29.132.69	443	192.168.2.3	49796	CN=*.mathtag.com, O="MediaMath, Inc.", L=New York, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Apr 15 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Fri Apr 22 14:00:00 CEST 2022 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Apr 10, 2021 00:14:11.255317926 CEST	185.29.132.69	443	192.168.2.3	49797	CN=*.mathtag.com, O="MediaMath, Inc.", L=New York, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Apr 15 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Fri Apr 22 14:00:00 CEST 2022 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

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 SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Apr 10, 2021 00:14:11.258827925 CEST	15.237.136.106	443	192.168.2.3	49795	CN=adobedc.demdex.net, O=Adobe Systems Incorporated, L=San Jose, 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 Oct 14 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Mon Nov 15 00:59:59 CET 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		
Apr 10, 2021 00:14:11.694964886 CEST	35.244.174.68	443	192.168.2.3	49798	CN=*.rlcdn.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB 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	Thu Feb 25 01:00:00 CET 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Tue Mar 29 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					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		
Apr 10, 2021 00:14:11.695251942 CEST	35.244.174.68	443	192.168.2.3	49799	CN=*.rlcdn.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB 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	Thu Feb 25 01:00:00 CET 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Tue Mar 29 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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		
Apr 10, 2021 00:14:11.740823984 CEST	172.217.168.66	443	192.168.2.3	49800	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Mar 16 20:28:05 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jun 08 21:28:04 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Apr 10, 2021 00:14:11.742754936 CEST	172.217.168.66	443	192.168.2.3	49801	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Mar 16 20:28:05 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jun 08 21:28:04 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Apr 10, 2021 00:14:12.015117884 CEST	216.58.215.227	443	192.168.2.3	49805	CN=*.google.ch, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Mar 16 20:36:16 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jun 08 21:36:15 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Apr 10, 2021 00:14:12.015203953 CEST	216.58.215.227	443	192.168.2.3	49804	CN=*.google.ch, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Mar 16 20:36:16 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jun 08 21:36:15 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5808 Parent PID: 792

General

Start time:	00:13:31
Start date:	10/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7d1060000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 4084 Parent PID: 5808

General

Start time:	00:13:32
Start date:	10/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5808 CREDAT:17410 /prefetch:2
Imagebase:	0x1120000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly