ID: 412512
Cookbook: browseurl.jbs
Time: 18:40:15
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report https://spark.adobe.com/page/ntKiaikxRt9X0/ 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Dropped Files 4
Sigma Overview 4
Signature Overview 4
AV Detection: 5
Phishing: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 11
Public 12
General Information 12
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 14
ASN 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
Static File Info 48
No static file info 48
Network Behavior 48
Network Port Distribution 48
TCP Packets 48
UDP Packets 50
DNS Queries 52
DNS Answers 53
HTTPS Packets 55
Code Manipulations 62
Statistics 62
Behavior 62
System Behavior 62
Analysis Process: iexplore.exe PID: 5912 Parent PID: 792 62
General 62

File Activities 63
Registry Activities 63
Analysis Process: iexplore.exe PID: 5592 Parent PID: 5912 63
General 63
File Activities 63
Registry Activities 63
Disassembly 64

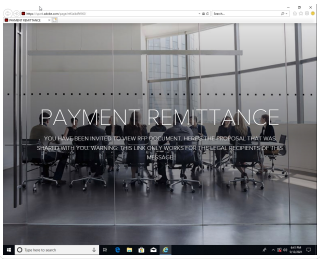
Analysis Report https://spark.adobe.com/page/ntKiaikx…

Overview

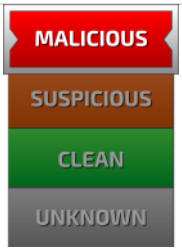
General Information

Sample URL:	http://https://spark.adobe.com/page/ntKiaikxRt9X0/
Analysis ID:	412512
Infos:	

Most interesting Screenshot:



Detection



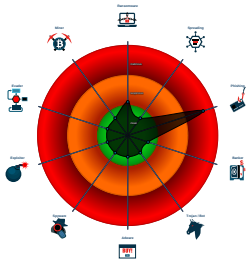
HTMLPhisher

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: 5912 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5592 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5912 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

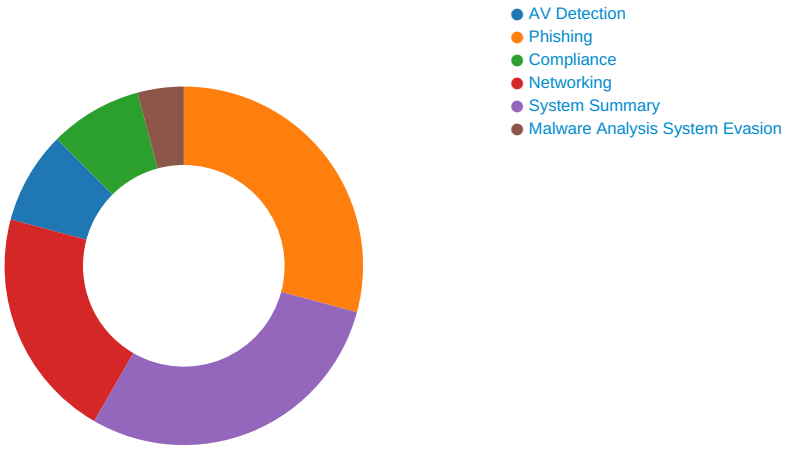
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\index[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\index[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)

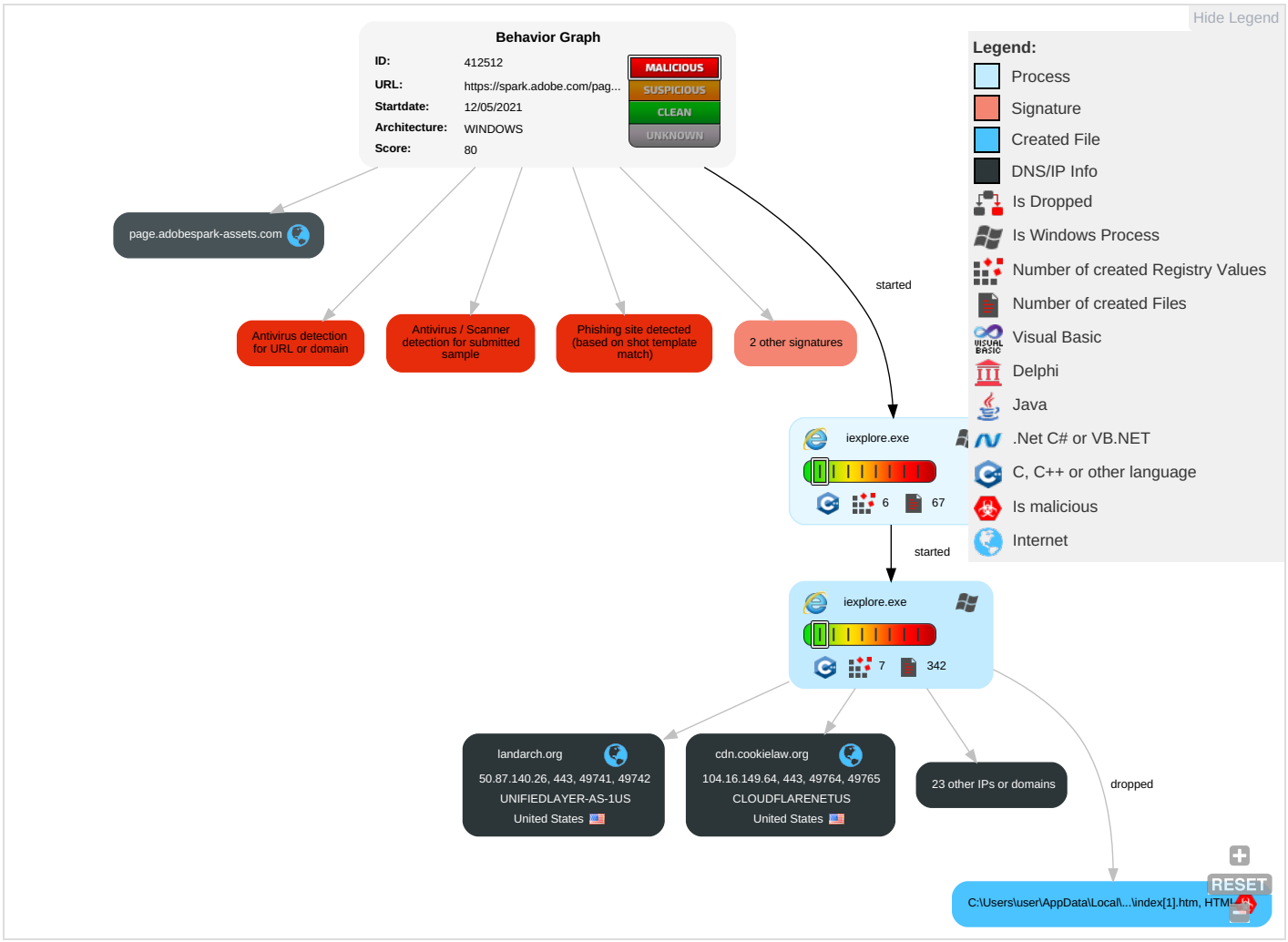
Yara detected HtmlPhish10

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	Impac
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 Partiti
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 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lockc
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 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data

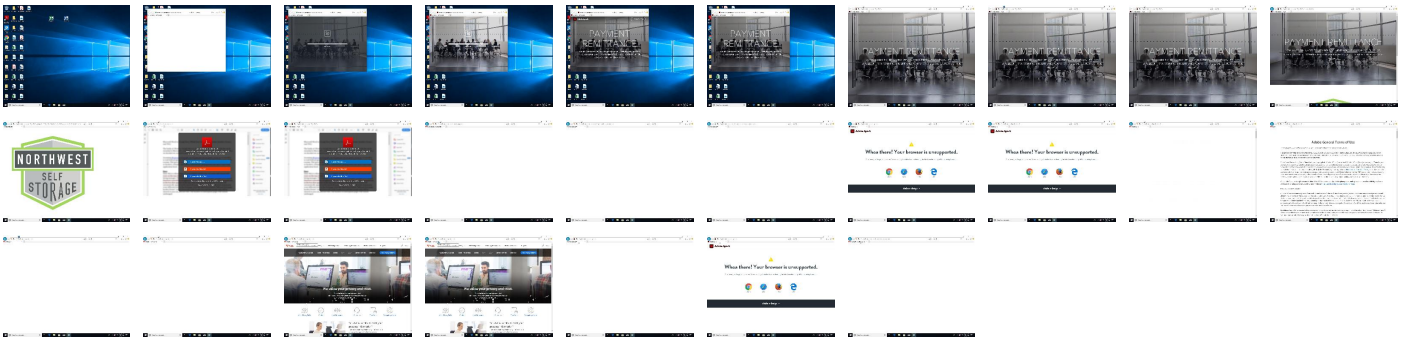
Behavior Graph

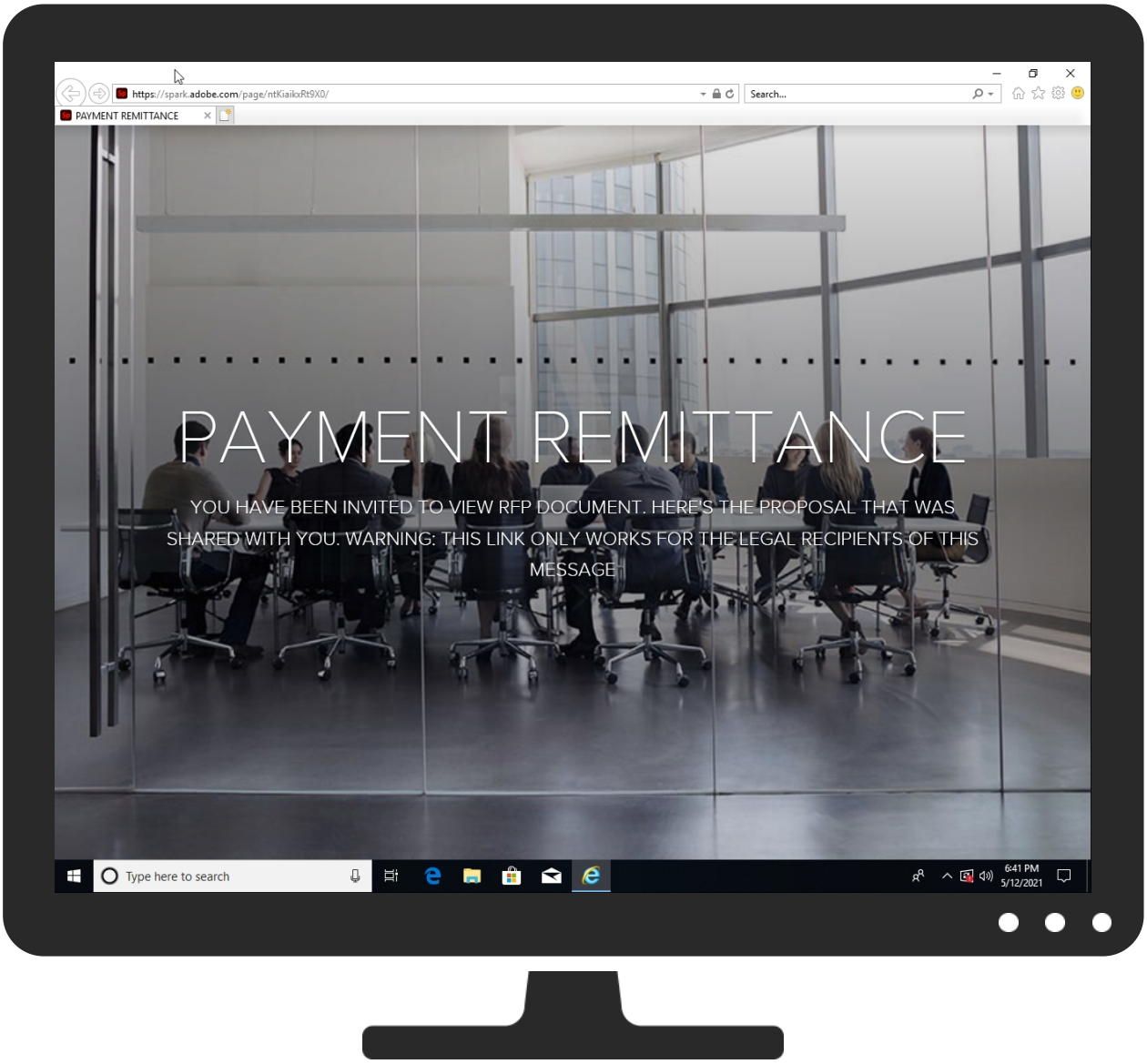


Screenshots

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/ntKiaikxRt9X0/	0%	Avira URL Cloud	safe	
http://https://spark.adobe.com/page/ntKiaikxRt9X0/	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
landarch.org	0%	Virustotal		Browse
spark.adobeprojectm.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://spark.adobe.com/page/ntKiaikxRt9X0/?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://landarch.org/h	0%	Avira URL Cloud	safe	
http://https://blog.adobespark.com/	0%	Avira URL Cloud	safe	
http://https://landarch.org/hassani/index.phpX0/images/43b32711-4358-470b-a423-45db1a503c8d.png?asset_id=34	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%	URL Reputation	safe	
http://https://ade0164.d41.co/sync/	0%	URL Reputation	safe	
http://https://ade0164.d41.co/sync/	0%	URL Reputation	safe	
http://https://www.pinterest.	0%	URL Reputation	safe	
http://https://www.pinterest.	0%	URL Reputation	safe	
http://https://www.pinterest.	0%	URL Reputation	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://landarch.org/hassani/index.php$Share	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	13.224.187.69	true	false		high
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com	52.214.120.236	true	false		high
landarch.org	50.87.140.26	true	false	• 0%, Virustotal, Browse	unknown
spark.adobeprojectm.com	13.225.74.35	true	false	• 0%, Virustotal, Browse	unknown
s3.amazonaws.com	52.217.11.150	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
adobe.com.ssl.d1.sc.omtrdc.net	35.181.18.61	true	false		unknown
api.demandbase.com	13.225.74.58	true	false		high
adobe.tt.omtrdc.net	52.51.251.137	true	false		unknown
page.adobespark-assets.com	13.224.193.29	true	false		unknown
cdn.cookielaw.org	104.16.149.64	true	false		high
geolocation.onetrust.com	104.20.184.68	true	false		high
use.typekit.net	unknown	unknown	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high
assets.adobedtm.com	unknown	unknown	false		high
cm.everesttech.net	unknown	unknown	false		high
p.typekit.net	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
dpm.demdex.net	unknown	unknown	false		high
static.adobelogin.com	unknown	unknown	false		high

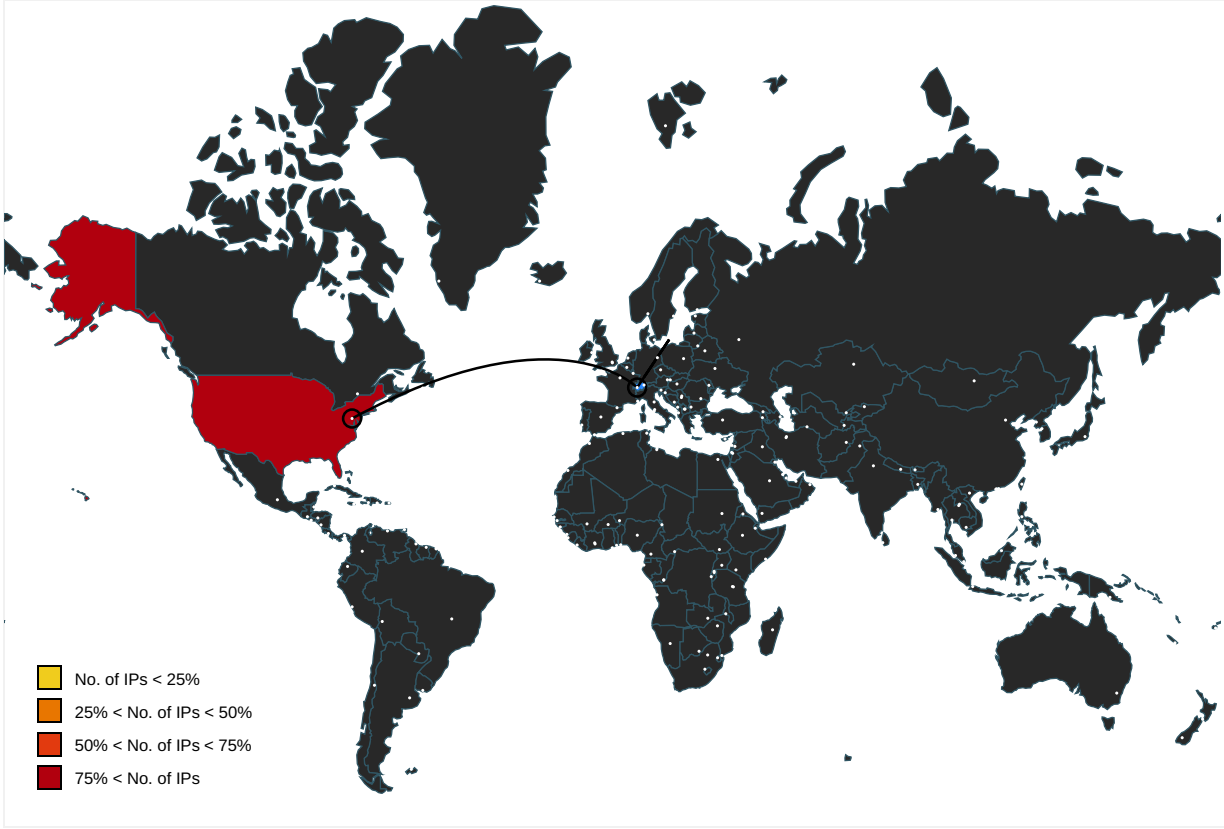
URLs from Memory and Binaries

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[2].htm0.3.dr, unsupported[1].htm.3.dr	false		high
http://https://www.linkedin.com	scripts[2].js.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	ntKiaikxRt9X0[1].htm0.3.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	index[1].htm.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	{4AAAF421-B38C-11EB-90E4-ECF4BB862DED}.dat.2.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://page.adobespark-assets.com/runtime/1.22/typekit-load.gz.js	ntKiaikxRt9X0[1].htm0.3.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	ntKiaikxRt9X0[1].htm0.3.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[2].htm0.3.dr	false		high
http://https://www.youtube.com	scripts[2].js.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://adobesparkpost.app.link/8n80l2HauZ	resume[1].htm.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
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[2].js.3.dr	false		high
http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC036830be72f242959c7b9ca66cef0c8	RC036830be72f242959c7b9ca66cef0c85-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[2].js.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://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC48990c37b3504a02838f190f73e1266	RC48990c37b3504a02838f190f73e12664-file.min[1].js.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/8f4e31/000000000000000000000132e3/27/	vtg4qoo[1].js0.3.dr	false		high
http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC6f46e43fa6d44dbeb45cc5801ffded0	RC6f46e43fa6d44dbeb45cc5801ffded0e-file.min[1].js.3.dr	false		high
http://https://landarch.org/h	{4AAAF421-B38C-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC1bc70f0c17a44296971da4381a721bd	RC1bc70f0c17a44296971da4381a721bda-file.min[1].js.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://blog.adobespark.com/	scripts[2].js.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://https://landarch.org/hassani/index.phpX0/images/43b32711-4358-470b-a423-45db1a503c8d.png?asset_id=34	~DFFE22DFC775CA8E19.TMP.2.dr	true	• Avira URL Cloud: safe	unknown
http://opensource.org/licenses/MIT).	popper.min[1].js.3.dr	false		high
http://https://kit.fontawesome.com/585b051251.js	index[1].htm.3.dr	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js	index[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://openjsf.org/	marvelcommon-51100480[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	{4AAAF421-B38C-11EB-90E4-ECF4BB862DED}.dat.2.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	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://adobespark.uservoice.com	unsupported[1].htm.3.dr	false		high
http://https://www.pinterest.	scripts[2].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ianlunn.github.io/Hover/)	hover[1].css.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://developer.akamai.com/tools/boomerang#mpulse-session-information	en[1].js.3.dr	false		high
http://https://static.adobelogin.com/imslib/imslib.min.js	login[2].htm0.3.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://www.facebook.	scripts[2].js.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/000000000000000000158d9/26/	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-00a38324dab316803fdc74cba4ad7ab9[1].js.3.dr	false		high
http://https://use.typekit.net/af/d8f71f/0000000000000000000132e1/27/	vtg4qoo[1].js0.3.dr	false		high
http://https://servedby.flashtalking.com/container/13539;99030;10307;iframe/?ftXRef=&ftXValue=&ftXType=&ftX	{4AAAF421-B38C-11EB-90E4-ECF4BB862DED}.dat.2.dr	false		high
http://https://github.com/kriskowal/q/blob/v1/LICENSE	marvelcommon-51100480[1].js.3.dr	false		high
http://underscorejs.org/LICENSE	marvelcommon-51100480[1].js.3.dr	false		high
http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC89c6d3bd15f043db95a5a0a4b5cc9da	RC89c6d3bd15f043db95a5a0a4b5cc9da0-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-6a358124[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://landarch.org/hassani/index.php	{4AAAF421-B38C-11EB-90E4-ECF4BB862DED}.dat.2.dr	true		unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://page.adobespark-assets.com/runtime/1.22/runtime.gz.css	ntKiaikxRt9X0[1].htm0.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://use.typekit.net/vtg4qoo.css	login[2].htm0.3.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-6a358124[1].js.3.dr	false		high
http://https://npms.io/search?q=ponyfill.	marvelcommon-51100480[1].js.3.dr	false		high
http://https://use.typekit.net/af/b0c5f5/0000000000000003b9b3f85/27/l?primer=7cdcb44be4a7db8877ffa5c0007b8	scripts[2].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/00000000000000000132e1	vtg4qoo[1].js0.3.dr	false		high
http://https://cdn.cookielaw.org	login[2].htm0.3.dr	false		high
http://https://use.typekit.net/af/b0c5f5/0000000000000003b9b3f85/27/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://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-6a358124[1].js.3.dr	false		high
http://https://landarch.org/hassani/index.php$Share	{4AAAF421-B38C-11EB-90E4-ECF4BB862DED}.dat.2.dr	true	• Avira URL Cloud: safe	unknown
http://https://use.typekit.net/af/97fbd1/0000000000000003b9b3f88/27/l?primer=7cdcb44be4a7db8877ffa5c0007b8	scripts[2].js.3.dr	false		high
http://https://fontawesome.com/license/free	free.min[1].css.3.dr	false		high
http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC5e5d1b9fe0a942c38190dc2199529994/RC5e5d1b9fe0a942c38190dc219952994-file.min[1].js.3.dr	RC5e5d1b9fe0a942c38190dc2199529941-file.min[1].js.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	imagestore.dat.3.dr, ntKiaikxRt9X0[1].htm0.3.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

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
50.87.140.26	landarch.org	United States		46606	UNIFIEDLAYER-AS-1US	false
52.217.11.150	s3.amazonaws.com	United States		16509	AMAZON-02US	false
52.51.251.137	adobe.tt.omtrdc.net	United States		16509	AMAZON-02US	false
52.214.120.236	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
104.20.184.68	geolocation.onetrust.com	United States		13335	CLOUDFLARENETUS	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
13.224.187.69	dd20fzx9mj46f.cloudfront.net	United States		16509	AMAZON-02US	false
13.224.193.29	page.adobespark-assets.com	United States		16509	AMAZON-02US	false
13.225.74.58	api.demandbase.com	United States		16509	AMAZON-02US	false
13.225.74.35	spark.adobeprojectm.com	United States		16509	AMAZON-02US	false
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
104.16.149.64	cdn.cookielaw.org	United States		13335	CLOUDFLARENETUS	false
35.181.18.61	adobe.com.ssl.d1.sc.omtrdc.net	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412512
Start date:	12.05.2021
Start time:	18:40:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://spark.adobe.com/page/ntKiaikxRt9X0/

Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.phis.win@3/266@19/13
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://spark.adobe.com/page/ntKiaikxRt9X0/?page-mode=static • Browsing link: https://spark.adobe.com/page/ntKiaikxRt9X0/images/43b32711-4358-470b-a423-45db1a503c8d.png?asset_id=34959966-dbbb-477c-83fe-a6a5002ee5e3&img_etag=%228d0c972e0adb28a066d197ef29ded4c8%22&size=1024 • Browsing link: https://landarch.org/hassani/index.php • Browsing link: https://spark.adobe.com/page/ntKiaikxRt9X0 • 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 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 92.122.145.220, 88.221.62.148, 23.32.238.192, 23.32.238.195, 23.37.33.211, 184.30.24.56, 69.16.175.10, 69.16.175.42, 142.250.185.202, 142.250.184.234, 104.18.22.52, 104.18.23.52, 172.64.100.17, 172.64.101.17, 152.199.19.161, 95.101.22.203, 95.101.22.195, 184.30.24.234, 20.82.209.104, 184.30.24.134, 54.171.42.33, 54.194.191.134, 99.81.11.244, 34.255.166.243, 34.250.153.194, 34.253.145.149, 92.122.213.194, 92.122.213.247, 20.54.26.129 • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded domains from analysis (whitelisted): e6653.dscf.akamaiedge.net, e4578.dscg.akamaiedge.net, cds.s5x3j6q5.hwcdn.net, ka-f.fontawesome.com.cdn.cloudflare.net, cn-assets.adobedtm.com.edgekey.net, store-images.s-microsoft.com-c.edgekey.net, spark.adobe.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, iris-de-ppe-azsc-neu.northeurope.cloudapp.azure.com, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, go.microsoft.com, use-stls.adobe.com.edgesuite.net, ssl-delivery.adobe.com.edgekey.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, kit.fontawesome.com.cdn.cloudflare.net, sstats.adobe.com, fonts.googleapis.com, p.typekit.net-v3.edgekey.net, fs.microsoft.com, stls.adobe.com-cn.edgesuite.net.globalredir.akadns.net, ajax.googleapis.com, ie9comview.vo.msecnd.net, cm.everesttech.net.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, stls.adobe.com-cn.edgesuite.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, e7808.dscg.akamaiedge.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, a1815.dscr.akamai.net, geo2.adobe.com, a1988.dscg1.akamai.net, www.adobe.com, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found.

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\2WNQG8GR\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):	835
Entropy (8bit):	4.8680506222136035
Encrypted:	false
SSDEEP:	24:WUjDSDecIZG0U1mKm6DGZGU1mKm6DGZJ6L4ZGU1mKm6DGZJ6L4ZGU1mKm6DGZJ6r:LjDSDcZksKGZbsKGZc4ZbsKGZc4ZbsK1
MD5:	51DFE3C266D9B6D17BF600BA51E64F83
SHA1:	436947A2E9A0F053F4B0022AC3A7D62DEC54D0B5
SHA-256:	065A5211FE5D7ECBAFAD91737628753F2D2910612683B1624CCFE610F222062D
SHA-512:	D187325CB6FB8D84A5B1DDED05687623020BCE763A0CDABD31EDB4EAFA7362875BCD15118AFE89944D7BFA5496DF75BFC748E80D49E32E85947C859DB120FE 7D
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="__akfp_storage_test__" value="__akfp_storage_test__" ltime="535592640" htime="30885785" /></root><root></root><root><item name="com.adobe.reactor.dataElementCookiesMigrated" value="true" ltime="612102640" htime="30885785" /></root><root><item name="com.adobe.reactor.da taElementCookiesMigrated" value="true" ltime="612102640" htime="30885785" /><item name="mar_aud" value="Bot" ltime="619592640" htime="30885785" /></root> <root><item name="com.adobe.reactor.dataElementCookiesMigrated" value="true" ltime="612102640" htime="30885785" /><item name="mar_aud" value="Bot" ltime="619592640" htime="30885785" /></root><root><item name="com.adobe.reactor.dataElementCookiesMigrated" value="true" ltime="612102640" htime="30885785" /><item name="mar_aud" value="Bot" ltime="619592640" htime="30885785" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\H1CA8U6B\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):	4.735686483572696
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsnObemKmlULF0VqHlJR3pNDra9qSfyHuZLKb:JFK1rUFjgemKm6GVqHlJR3vralnZub
MD5:	8D43B146A1B0DEE59BAC7B789BDF2A78
SHA1:	5FC314C7718C8769A9B45BDB49F74902DD30DC29
SHA-256:	2E424B6F0BFEA2EF598E430642CE39FA3776338508FEFCED79F11C70D4E0ADB4
SHA-512:	297BCC3DA1DCCBC10C03AA608ED7875DC501F9BADE0D9E7555CAD4C78068C1B9AE6549FAFFB6E2E87D91B56FECA4AB597749E185533A64A7CBB38E0DA729 611
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="com.adobe.reactor.dataElementCookiesMigrated" value="true" ltime="593612640" htime="30885785" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{4AAAF41F-B38C-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	39000
Entropy (8bit):	1.924670546422599
Encrypted:	false
SSDEEP:	192:rTZcZe2ZWl7tlpflyhMGugoftMrysf+rr3g:rVcVoPLVvgWIXGQ
MD5:	5A859B824E4FEA70AC3ADD8B76425822

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{4AAAF41F-B38C-11EB-90E4-ECF4BB862DED}.dat	
SHA1:	7DF7D67C24BDCF7D5268EBBEF75111CB9877B8B3
SHA-256:	33815E092108A0A82DA7274D2A7939545B8DB35A08C671FAE5DA442B5E73DD35
SHA-512:	06AECB44898A9472C5AF1B43C62B2329D125E9B0F2FFCC9368EA4C727A46AD023C4BC7A7CBE01039780645F166697437FDBD37918D2F059C0BB9278700E3699
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\{4AAAF421-B38C-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	200568
Entropy (8bit):	2.702986185974534
Encrypted:	false
SSDEEP:	768:t3fAsA2sdNbsGNU3EqfGXROARlKzW3/dQNGCVgyk:Sv
MD5:	DB2AB61E4594D1893EFDF1AEB328204B
SHA1:	160CDFEDFD24AA1B782DB40E4B4C16FBD68174BB
SHA-256:	98E96F4E5952FFF00E49DEF43BE81580A2F94C02B703149C5AF2C4CAD435F2CF
SHA-512:	FBFFF1CB0B39406876AFD3E5C5A26B5F467D87E12C07FA3371A2DA4790D25ADBA7E34D142381C60A983E1F55E926FFD295C5980128D922FD60457F4AC09A3D0
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\{5147B8C8-B38C-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.583455174065478
Encrypted:	false
SSDEEP:	48:IwlGcprAGwpatG4pQ9GrapbSJGQpKXG7HpRgTGIpX2fGApm:r7ZIQP6dBSDA2T0Fqg
MD5:	CCABEAA13080E3C5D60772AFD23DAEF3
SHA1:	AC2383BE9605CEFAC75F7C0ACAD310987B89DCB3
SHA-256:	80279B0A1EA395AAA9BE0D06FC308EA18BBC6E5393FAC2D40995F237F0729554
SHA-512:	EC833742BA784C88D1A5CC076E15E4559657B1A010F044C6011DAAB614408D8B6A8CBDB0C0C8862399AA9BAB8FB53AF2EB3648E5170C9402C3E94720F47B953A
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
File Type:	data
Category:	dropped
Size (bytes):	32675
Entropy (8bit):	3.246135960222112
Encrypted:	false
SSDEEP:	96:MdXG3bdWfcmTY+aRF1pXWZL2+42HGhIUc8KeLEW70sI2NmU3GwXsj70sI2NmU3G3:eXGgXTY+as02mOB8XLE7WmU3HWmUm
MD5:	868E9EB01E36819CBD6EA14B5655EEF8
SHA1:	F79039D4060813061D1C44CEFE79600FA525536F
SHA-256:	CD476D0E6ED71D0D1884EC7DAA3F1D1ECE26ABAE9AD03D197DA96A140A2447E0
SHA-512:	06ADAE5272CBCB235A3D30CAE3988F066162082B3BD9D4087FB5B783F7FFA02F3FD5F4BFDF504FCC3B77F8A60D7E86E573E5497536899A2A02AE00CCE410E791
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
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...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`.....................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\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):	4.632512639848438
Encrypted:	false
SSDEEP:	96:OyIY40FtdRYzYVaIJ5GHZa6AyAYJjojVjht4S:iwKzYslJF6vAYJQdoS
MD5:	526B16D51BF2FE4666A13EC61ECD9C72
SHA1:	DC53861E92C2891C0138E64DB9F7AA6B3F8D2AA5
SHA-256:	717CDB76535A04A9DEC6F2F6773475BE9574AE304CBA44F7E1A56CB26037D85C
SHA-512:	4FF4D28F5755B27E847A6AC756ED0B958BE75378CCD563FAFD54CD888BFC8D1B4C94C1E2C4C78C1B2EC5FAF46052D02B3003CF446C10D1650715E4119126E6 0
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\0W10PBUV\ErrorPageTemplate[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):	2168
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	24:5+j5xU5k5N0ndgvoyeP0yyiyQCDr3nowMVworDtX3orKxWxDnCMA0da+hieyuSQK:5Q5K5k5pvFehWrrarrZIrHd3FIQfOS6
MD5:	F4FE1CB77E758E1BA56B8A8EC20417C5
SHA1:	F4EDA06901EDB98633A686B11D02F4925F827BF0
SHA-256:	8D018639281B33DA8EB3CE0B21D11E1D414E59024C3689F92BE8904EB5779B5F
SHA-512:	62514AB345B6648C5442200A8E9530DFB88A0355E262069E0A694289C39A4A1C06C6143E5961074BFAC219949102A416C09733F24E8468984B96843DC222B436
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/ErrorPageTemplate.css
Preview:	.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...ma rgin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_grad ient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...back ground-color: #F4F4F4;..}.. ..a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Policies_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):	28449
Entropy (8bit):	6.1296006799069325
Encrypted:	false
SSDEEP:	768:37Y73fMwXqXlPGT4Ch21JSP39z6dHuUN+3nw:k73fMwsPGT81cwuUow
MD5:	EFB6F897542A02F53A3859AAEFBD7013
SHA1:	1CABA3B56B5AB14798C12C84C565AFE2A28DC2DD
SHA-256:	B0AE115BC1ED8A5D8D3FE58E43A43AB6B54ADC35555D38A09BB44B22A0617A78
SHA-512:	AC718B0FF41B2B34F38273E9EF7B3CD93AF51B4A3BD635F48E8D8E1F85A64AC9723E2F4AA69EC2062A152A2DC8940DC967ECA93E46DCFFD33C3B5766DB8BE 5F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/content/dam/cc1/en/privacy/images/Policies_72px_lt-gray.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Policies_72px_lt-gray[1].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\0W10PBUV\RC036830be72f242959c7b9ca66cef0c85-file.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	323
Entropy (8bit):	5.278322841738521
Encrypted:	false
SSDEEP:	6:jwkMKngJv0KgiSP8Al8VQoHDXRMvKyupXMYGGX6SHMWkiezW3T5OtunadXZfJ/u0:jvgeASPRM9ny6cYGkcOeqD5OFdXv/ZJ
MD5:	5A428FB34157B1F392C7DE7626377B24
SHA1:	F2091A253E0FB2C427BDFC8D4A722010D8B3C66D
SHA-256:	2D0998621ABC5C7B0FDBABEE2ABBD59DD09ADA2FAFFEADA530538BEF1D54439A
SHA-512:	EE84B738B8019EAC1D943A8CEB41A8C170CFF466F99FC40E1E3D1B7394D6404708A6F09BAE994F5C0E22DA10238C636AE426FC61F585C60371D732C1787980F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC036830be72f242959c7b9ca66cef0c85-file.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC036830be72f242959c7b9ca66cef0c85-file.js`..._satellite._pol l(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\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):	5.198759932624338
Encrypted:	false
SSDEEP:	12:jvgeASPRMpRHt62jA0ZPZPSwhLGGK+K4Jo70WJkwvCRBu:15Mc2jlxJSGLGUJQJkQCvu
MD5:	C2F9897B6B91AF5F5AAB06B5AAB7F380
SHA1:	3DAF3209C4B451E01DDD2560E528AC4488C797AD
SHA-256:	E4BB2E6BA91E9D30AD5F9D79B0B9BFF2709D9265806A431642B3EC36C2763100
SHA-512:	AF4E2C6FDA98E9DCB51FDEA9F823448248B79A3A4DE624FBC3BFA8450A312E3D58780F4135E6D4DEE5ED4426949B3DD26D202010B2BA0621B56C9A2ED4CBB BC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC1a4f9c4f0d8a4bba917d5412b0c552b7-file.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/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\0W10PBUV\RC1a83c357d323419db9d2ba211efeeaae-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):	1156
Entropy (8bit):	5.085318061903744
Encrypted:	false
SSDEEP:	24:15MzgA+E6K7eVgvf2l+LPPJ9ZLvaMLArqY4DPuDkpuH4R9pQFE7xJth:15MzLv7+iOl+zPJ9ZL11sYR8oh
MD5:	5EBC8AD621DAF90CB626853E4DB46C25
SHA1:	EB3CE39D4D1972CC5E33671F53D3EC43675E7DF2
SHA-256:	10C3D4D24300686F432EC8A3D6A7FEBBA5034C97AD2E3F7D00B11DD5A58CFAF5
SHA-512:	B6D51B480A872592B6017F401A24B50C767C5DF0959A9F758FC664D7337636D64A602EC1EA4FD3E3289E891F2F84E79668A3169C7545E9D71D66D565C81E4F41
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC1a83c357d323419db9d2ba211efeeaae-file.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RC1a83c357d323419db9d2ba211efeeaae-file.min[1].js	
Preview:	// For license information, see `https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/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.indexOf("/events/")||-1!==h.indexOf("magento.com")||-1!==h.indexOf("marketo.com")||"futureisyours.adobe.com"==h||"api.spark.adobe.com"==h){var dnbScript=document.createElement("script");dnbScript.src="https://ade0164.d41.co/sync/",dn

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):	5.255227719143
Encrypted:	false
SSDEEP:	48:15Mvn9KNNFeHD7Bbg8m9wPjwPbeffSQLYno4BXo5iTJWN+BJ6Nu4CuMgG+/T1zcD:1OvneNFeHDNbg76s6nSjXSiTJWMBJ6kn
MD5:	6ADCE7DE352492C057C2F0C88E7D3D98
SHA1:	0DD081C4D0D9EF30CD58EC4C3C40B7315AA231D7
SHA-256:	079FE9E5AD96322BF54FCB661F8CA26BFDCC2A7F1C2EBEF8AFEA75E05A0E85DF
SHA-512:	15FBF6140113F79BF007BB8AAAF135CC6D3BE5356890BFBB22ECC6E01749F82AD68268B9253C36103A47BC4F33FBAB28B36B485F9B639A8DDA52EA0FCF4CBEF6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC6f46e43fa6d44dbeb45cc5801ffded0e-file.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/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\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><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\SPRK_color_v2@2x[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1934
Entropy (8bit):	4.543427398694442
Encrypted:	false
SSDEEP:	48:Ci1LbWxBa8zBtKJwzWOxCKWZDPzKiODCTCZ:Zh6Ba8zbK6X3WVP2DCTCZ
MD5:	F858A5C4E786F511FABE5D35DA995F65
SHA1:	DFC968D018C16B8E4853AA17418C9F4302CADC6C
SHA-256:	CDA6CA3F0B46DB2E50DDB33DC50438CC2D1C22CF71650CD457912BDD9718A6EF
SHA-512:	ADE9CE8069690298C4A2CDE1FE1D066B8FA2D60DDD2A43177A7ADE92A648C349A05236D2C1C6EBA1A821A620E803FA68EE9FECD777FCD3CB37F961A97F6F419

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\SPRK_color_v2@2x[1].svg	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spark.adobe.com/images/SPRK_color_v2@2x.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 56 54"><defs><style>.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"><rect width="56" height="54" rx="9.91" fill="#370000" id="Outline_no_shadow" data-name="Outline no shadow"/></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 0114.3 38.12.08 12.08 0 01-2.83-.91c-.2-.09-.3-.3-.3-.62v-4.12a.22.22 0 01.09-.2.25.25 0 01.25 0 11.84 11.84 0 003.29 1.17 12.74 12.74 0 003.4.48 5.28 5.28 0 003-.65 1.91 1.91 0 00.9-1.61 2.13 2.13 0 00-.29-1.12 3.1 3.1 0 00-1-1 11.61 11.61 0 00-2-1l-1.85-.78a13.89 13.89 0 01-3.54-2.05 6 6 0 01-1.75-2.35 7.53 7.53 0 01-.49-2.7 6.64 6.64 0 014-6.2 11.25 11.25 0 014.89-1 22.84 22.84 0 013.31.23 7.22 7.22 0 012.39.71.52.52 0 01.26.48v3.89c0 .05 0 .1-.1.16s-.14.06-.24 0a9.9 9.9 0 00-2.5-.65 14.11 14.11 0 00-3.19-.25 7.28 7.28 0 00-1.81.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\browser-icon-edge[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):	3016
Entropy (8bit):	7.891883408525801
Encrypted:	false
SSDEEP:	48:cCzs80SVhdoz+n+UHXol0c61Ga6ovj4mrikoPmzz3l4NrT6xvO:cT80CAK+UHY9gGa6or4sZ3l4Nr2BO
MD5:	096DBF8523D015FB4295051DF53A52C1
SHA1:	7BB34828A6AB6CB2E6E418ADFBEACF189D07AE3E
SHA-256:	0E95127D87D4498950215D4AD1BAA56BDE661E9DC7BCE84F8249594FBCECC727
SHA-512:	DF694A7FE2BE219DE857DCBC1D9F708960D74B1BFE45AF5F2EC15974C22C15EC2D48DAA6BBA6234BF54185103A00E8EDE486C9320F6A9A8631EE9A7E93D7F5 01
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spark.adobe.com/images/landing/browser-icon-edge.png
Preview:	.PNG.....IHDR...|...|.....IDATx.....E...@.B.D...-.....K.d.P.Q.....E.* ...U.*.....`!.`!.....D..... ..$.R&..aK..9/y..wf.....z.....}...D"..f..W.....Z..`1...^...AzKpm.....l.l.l.l.....W...g ....G....0.E..t!..|w..f.....p...a.....1j.wT..}.k..0.....g.....]..f.....\[.*.4p...g...5p-p.F=...[l...v[`*p.0.7.....7b..M..f...D`.ph..3....\.Q.y.h.....>.C3.7...p5F-.....N.....).5..._pm....6.l.... 31jq.wW.....Y...<...Q.U}.....$..`K.6..0.*3....z..=...E..i.'0.*NV...)..S=[..sh.?C?.j.OW.~.|.E.X.<..n..D....:M..=[d .'>..n.,%.V.t~.[...-2...W.Q..b.p..b....E..V.&c./....0...4w..y.HV.....S.O l.....bw...h.....t.d.=R.uE.....}.k.F..|s.Uf..c.N.<a...\.....R..\N.O.i....l..x.\..2.%...E.8..p..&.ID.;.r.p..~....1m.^..^...{.....y#L.]....Y.D.....ex.D...D.t...3..Gz..Y....o..*<;.Y..%.U'..M..5. ..t&....]...."q.^..Q..<.O..}...g..W.d...(r.N_....{..d.'q....{.+X...[...X.;.ZF./.aE.Z....".%..,\o.n"t.3;..B<.u&@...p...6t2.:.D..I...uNc.x....@G#.(.=^..k..$.

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 30980, version 0.0
Category:	downloaded
Size (bytes):	30980
Entropy (8bit):	7.987621377492639
Encrypted:	false
SSDEEP:	768:Nh0Jzz1kWYZQL4lNCzPhlKCdN7GgGAvOYHqycQ:Nh6WZQclQzJ5xbvHqnQ
MD5:	01BD649595C405E61BD162E40BFF7260
SHA1:	B03670659950A40A47F9658B71F69FF14F8DA4C2
SHA-256:	2FF95F05AA71F6FE45D80A3FC8585BDE66210ECBC83A1AC494BD679A5CAE28DE
SHA-512:	9C4A5AA9CCD44CDB780515532E79BD26C2F250DAFF67FAC3CDC2B9D7067AB664F1D1301183A928BCD950123652F44781B31EEF5A22B7AC939B261D242E92F4 0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/97fbd1/00000000000000003b9b3f88/27/d? primer=7fa3915bdafdf03041871920a205bef951d72bf64dd4c4460fb992e3ecc3a862&fvd=n7&v=3
Preview:	wOFFOTTO..y.....BASE...0...F...Fe!].CFF ... ..]q..p.q...DYNA..a.....#.3GDYN..bL.....GPOS..c0...@..$..#..OS/2.....Y...`].y.cmap..w....V.....3head...x ...5...6..%ghhea..... ...$...Chmtx..up...%...H....maxp.....P.name.....E@..post..w..... ...2.....ideoromn..DFLT..cyrl..grek..latn.....Y.....x.c`d```5.:...]< ..W.f..@....^0....~.).....@...).=...x.}..n.0...t..B.\q...s.D..UB.[.v...&..l.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.....6.....

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 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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\d[2]	
SHA-512:	29A5BA44B73F6AD9F3AFA09ACA3326E1BD8FD0C79C681D91A03E12B46D09A198E2CD5A1B6AFAE7F59F2E4DFC4AC64480F0F96E22FE8879C22C3A8F52A2B98E5B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/6c57c4/00000000000000000000158d6/26/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\0W10PBUV\d[3]	
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:	A8C1BCA226F757C2BC8A096E31D2E05B2F8C184A531D93CDE6A26974A10B96005F4F341D52A80404919CE050BE8F89EE91EFC7D996936B37879DFD85CAA36E9A
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\0W10PBUV\d[4]	
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/00000000000000000000158d8/26/d?subset_id=2&fvd=i4&v=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\0W10PBUV\d[5]	
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/IY1eizt+wcCMPyv2GTPNo/B1:AgN62MlkrI23a0G+keiBL4jKoZ1
MD5:	E0F2BB6FEFF9005FADFAA0DEAC9F17D3
SHA1:	5BCF4E553881D43087F31A8B47172F1F695E461B
SHA-256:	809F249AF3A361113340A14136F8464AB4A1A23E47B05F71375115E6C23FFC92

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\d[5]	
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\0W10PBUV\d[6]	
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/50iZ9IyZPs
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\0W10PBUV\d[7]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19972, version 0.0
Category:	downloaded
Size (bytes):	19972
Entropy (8bit):	7.973644639018193
Encrypted:	false
SSDEEP:	384:Cf5Fav9bGgUEYSX1onww9sud9sYpihw+yncXRmtwE1YHoVEY:CDajJOnqucYMhW+mtMoVEY
MD5:	8A4B72CBF267D80FA1AA077748D6F386
SHA1:	BFCBD9749829EC32F8E92EDB67B2103A2B693FCB
SHA-256:	25847A66D07866EDDEA20934F252A9D9FBA7CE24FA9EB0A60FA3F3056182B93A
SHA-512:	3672D408F2B48E5986B43C90B9140325DBF9EE74A12A6E08FB893964A7E49505D5B36D87F5DDE9185C0819F913321E38EF30A9BA43745B21E35C3DDA56181913
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/e030d3/00000000000000000000158d3/26/d?subset_id=2&fvd=n1&v=3
Preview:	wOFF.....N.....\.....DYNA...`.....4.(.FFTM.....]..,GDEF.....8...B...<GDYN...P.....GPOS...0.....f.'OS/2.....W...`~wz#cmap..Ml.....+..wcvt .....R..fpgm.....e#./.gasp.....glyf...$..=b..b00...head.....4...6..<.hhea... ... ...$....hmtx..I.....lGZO.loca..K.....Y.Vmaxp...@... ... .name.....H?..post..MX..... ...(prep...x...O...O...4.....o1.....H.....x.....6.<.<.B.:.>.5.@..x.]Q.N[A.....c..hS.fB...$.W...vc9B.\.b\..P Q..k.h().A..R>.O@bfM.(....s..r..]Z.y..R.....v...t}...v.@..^.n...`3.rG....-.!.i'P....6...>.d..AK3MO....B`...0...../X....C.i*..s*..Ks....k..vp&"?..hj..@._:.z>.b.r.0...S.d".f2].T-3.up...;X.Js....U.....-.2KC...*1B.$.BN9w.?)P>..1....a..q.50.....fS.{.0~.G..o..>..6F..X.`...QU...s/.....3.%`y.._'..;6..em.C.....2....U.....tJ.....p.X...R.v....`H.F..h-;.*...d/.*.....x.c`d```b8.....x~.....''..~Ul...V.....r.....x..AN.@.....EQ..j....v.E..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\feds[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	108032
Entropy (8bit):	5.224884453933579
Encrypted:	false
SSDEEP:	1536:FiszfzkZfJe8eHg1L2+x2iSceSIfk75YRpYh1XcxfzTzkOFrCl+zasafXojdjmVL:FiSkZfJbeHg5qY1
MD5:	1F50126D124FEC7110AC54815415656A
SHA1:	4CD244BD59E0E4C7BC3A67614E25282076386F7F
SHA-256:	1021CCD72B4CD5A1C7E6D6CFCBD14669CC600DA15254943301A254B1C504CEFA
SHA-512:	C8C777D7CF8FB921DA2590E3A3D84FE3B3E19851EFBF57ADB10E64032FAACD85D162DEFC78892583B658B9B4653D04B11470FDE91BAC7E7992CAA752962182 9
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\feds[1].js	
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/etc.clientlibs/globalnav/clientlibs/base/feds.js
Preview:	window.__fedsSegmentation = '100';./*! feds v0.49.0 built on Mon, 26 Apr 2021 07:16:01 GMT */.!function(e){var t={};function n(r){if(t[r])return t[r].exports;var i=t[r]={i:r,l:!1,exports:{}};return e[r].call(i.exports,i,i.exports,n),i.l=!0,i.exports}n.m=e,n.c=t,n.d=function(e,t,r){n.o(e,t)||Object.defineProperty(e,t,{configurable:!1,enumerable:!0,get:r})},n.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};return n.d(t,"a",t),t},n.o=function(e,t){return Object.prototype.hasOwnProperty.call(e,t)},n.p="",n(n.s=167)}([,,,,function(e,t,n){"use strict";Object.defineProperty(t,"__esModule",{value:!0});var r="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(e){return typeof e}:function(e){return e&&"function"==typeof Symbol&&e.constructor===Symbol&&e!==Symbol.prototype?"symbol":typeof e};t.default=function(e){return"object"===(void 0===e?"undefined":r(e))&&!Array.isArray(e)&&null!==e}},function(e,t,n){"use strict";Object.defineProperty(t,

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://landarch.org/hassani/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\head.fp-00a38324dab316803fdc74cba4ad7ab9[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with LF, NEL line terminators
Category:	downloaded
Size (bytes):	141116
Entropy (8bit):	5.30072949013579
Encrypted:	false
SSDEEP:	1536:oh2bb1H+uuod92HpEMQqgQzDLTSYmv9Ktq2GXevsAUwx/VKbDlWJfwPf:RH+HY0zcuvsAFJs
MD5:	00A38324DAB316803FDC74CBA4AD7AB9
SHA1:	75321253B2C91E253BF2C775B589B2C096AAC1D3
SHA-256:	0CCDD4428614FDCEF969060F2ECC4EC6FF99FEFB968A49B4C987FD4506D33C81
SHA-512:	A927CF78845EFD12E39B058286E1C2ECC503B152C910F334F592A0266E0D340B5066AC6A21EB478DA39F08B647651F0DF1841E7F3D00AE44719C0FC596DDA81
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/etc.hawks.dexterlibs/dexter/clientlibs/base/head.fp-00a38324dab316803fdc74cba4ad7ab9.js
Preview:	!function(e){var t=window.webpackJsonp;window.webpackJsonp=function(n,o,a){for(var s,u,c,l=0,d=[];l<n.length;l++)u=n[l],r[u]&&d.push(r[u][0]),r[u]=0;for(s in o)Object.prototype.hasOwnProperty.call(o,s)&&(e[s]=o[s]);for(t&&t(n,o,a);d.length;)d.shift()();if(a)for(l=0;l<a.length;l++)c=i(i.s=a[l]);return c};var n={},r={6:0};function i(t){if(n[t])return n[t].exports;var r=n[t]={i:t,l:!1,exports:{}};return e[t].call(r.exports,r,r.exports,i),r.l=!0,r.exports}i.m=e,i.c=n,i.d=function(e,t,n){i.o(e,t)||Object.defineProperty(e,t,{configurable:!1,enumerable:!0,get:n})},i.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};return i.d(t,"a",t),t},i.o=function(e,t){return Object.prototype.hasOwnProperty.call(e,t)},i.p="",i.oe=function(e){throw console.error(e),e},i(i.s=584)}([,,function(e,t,n){var r=n(13),i=n(9),o=n(38),a=n(36),s=n(58),u=function(e,t,n){var c,l,d,f,h=e&u.F,p=e&u.G,v=e&u.S,g=e&u.P,m=e&u.B,b=p?r:v?r[t]||(r[t]={}):(r[t]||{}).prototype,y=p?i:i[t]||(i[t]=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\headIE.fp-f9e44dbeef5252f4d02c4ed9c4b6a618[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with LF, NEL line terminators
Category:	downloaded
Size (bytes):	71836
Entropy (8bit):	5.2834062351912525
Encrypted:	false
SSDEEP:	768:akRyhGekI/d65mve+R6ohN3KjAXCxnRGO7AevGBVGcgTSnTK3o9ufC:akRyhGek7E3KEXChwOsKTSOg
MD5:	F9E44DBEEF5252F4D02C4ED9C4B6A618
SHA1:	6EFF709B896F31AE0F73C4F493DC081D51771F20
SHA-256:	673875DD89E08974EAA386C2D7DF3F510C9D012E0DF65138347DD739F154EB1B
SHA-512:	9558927F687C05A1AF27F8E42A5592CF820A06AE6F26EC8A3F3E4BB9689FE4964A7DA6CEB23ADF99871167150E5CA3B191DC1CA6301BCF8085909EBB9E98631
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\headIE.fp-f9e44dbeef5252f4d02c4ed9c4b6a618[1].js	
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/etc.hawks.dexterlibs/dexter/clientlibs/base/headIE.fp-f9e44dbeef5252f4d02c4ed9c4b6a618.js
Preview:	// Nodelist ForEach polyfill from.// https://developer.mozilla.org/en-US/docs/Web/API/NodeList/forEach..window.NodeList&&!NodeList.prototype.forEach&&(NodeList.prototype.forEach=function(o,t){t=t||window;for(var i=0;i<this.length;i++)o.call(t,this[i],i,this)});..!function(t){var n={};function r(e){if(n[e])return n[e].exports;var o=n[e]={i:e,l:!1,exports:{}};return t[e].call(o.exports,o,o.exports,r),o.l=!0,o.exports}r.m=t,r.c=n,r.d=function(t,n,e){r.o(t,n)||Object.defineProperty(t,n,{configurable:!1,enumerable:!0,get:e})},r.n=function(t){var n=t&&t.__esModule?function(){return t.default}:function(){return t};return r.d(n,"a",n),n},r.o=function(t,n){return Object.prototype.hasOwnProperty.call(t,n)},r.p="",r(r.s=619)}([,,function(t,n,r){var e=r(13),o=r(9),i=r(38),u=r(36),c=r(58),a=function(t,n,r){var s,f,l,h,p=t&a.F,v=t&a.G,d=t&a.S,y=t&a.P,g=t&a.B,m=v?e:d?e[n]||(e[n]={}):(e[n]||{}).prototype,b=v?o:o[n]||(o[n]={}),x=b.prototype||(b.prototype={});for(s in v&&(r=n),r)l=((f=!p&&m&&void 0!==m[

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
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://landarch.org/hassani/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/IanLunn/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\index[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/t4ldtWPtY: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\0W10PBUV\index[1].htm, Author: Joe Security • Rule: JoeSecurity_HtmlPhish_7, Description: Yara detected HtmlPhish_7, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\index[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://landarch.org/hassani/index.php
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\0W10PBUV\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\info_48[1]	
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC134
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/info_48.png
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po.....X..;.=.P...../...+...9./..s.....9..|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0..''/n/.c...&.{.ht..?....A..I{.n.....|....t.....N}..%.v...:.E..i....`....a.k.mg.LX..fcFU.fO-..YEfd.}...~.''.....}!$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a...N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.(..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a).:t..e.j.W.....C<.1.....c..l1w....]3%....tR;.,..3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\launch-EN919758db9a654a17bac7d184b99c4820.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):	565896
Entropy (8bit):	5.347359122266954
Encrypted:	false
SSDEEP:	6144:uX8TWFSklmBpYQkStCSZuRmRqducXVjDXOd//k/kw8zayfjbMK7EWw317:K8aFwpY6ASZuRDucXVjDXOdQIjbM7WG
MD5:	B9CA729BCDD3D9395740E6D390EA3F3E
SHA1:	5E6F6E151C20D9DBA9D8ED1C9078E6EFD811D0B0
SHA-256:	707EA3D5A3AE334F856107C132B68D5846E68C44A32DE55751821B65F02B5C2B
SHA-512:	78F9DDC332421C79699220D72C35AFD723B002A2697D4160BE2061028F5B572E3ECCF832A94D2EAC9FB4FD7697499333A525C63081889B36AE07576758DDF827
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/launch-EN919758db9a654a17bac7d184b99c4820.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/launch-EN919758db9a654a17bac7d184b99c4820.js`..window._satellite=window._satellite||{},window._satellite.container={buildInfo:{minified:!0,buildDate:"2021-05-11T16:52:00Z",environment:"production",turbineBuildDate:"2021-04-26T16:54:28Z",turbineVersion:"27.1.3"},dataElements:{"digitalData.search.filters":{defaultValue:"",modulePath:"core/src/lib/dataElements/customCode.js",settings:{source:function(){return function(e){if(_satellite.getVar("adobe_aec_pages")&&digitalData._get("digitalData.filterInfo")&&digitalData._get("digitalData.filterInfo.filterName")){digitalData.search={},digitalData.search.filter=[],digitalData._set("digitalData.search.searchInfo.sort",digitalData.filterInfo.sortType);for(var t=digitalData.filterInfo.filterName.split("|"),n=0;n<t.length;n++)for(var a=t[n].split(":"),i=a[0],r=a[1].split(","),o=0;o<r.length;o++){var s={filterInfo:{}};s.filterInfo.category=i,s.filterInfo.keyword=r[o],digitalData.search.fil

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\legal-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):	4.957104463731007
Encrypted:	false
SSDEEP:	768:/8y3EDlwZ9bY/MKOIoLmsLa87WlIWJal0J4WWn1l8T7jqfVjDrXPIXewPoRhxfHq:/8y3EY0
MD5:	FF1E04DED681AEAC3DE29C4D2419FE91
SHA1:	C2147C7C50FB6DF21E5ECF323309AE67F6BCA247
SHA-256:	2B7F2F5C6DEE2661AFF7FA717D759C8B63328A9F3EA83556A51B64628EFBC9F7
SHA-512:	8B10CA490CE49752530938936E778BB570017999C97E2156CBC07EBABBC4ACECA0E8BCC9C22D003155A14AD0E6E7B62DDD4C8799E157A902101A321FB5F58B2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/services/feds.res_1.css/head/en/acom/corporate-mega-menu/legal-localnav.css
Preview:	/*! applauncher v0.49.0 built on Mon, 26 Apr 2021 07:16:01 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\location[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	182
Entropy (8bit):	4.685293041881485
Encrypted:	false
SSDEEP:	3:LUfGC48HlHJ2R4OE9HQnpK9fQ8I5CMnRMRU8x4RiiP22/90+apWyRHfHO:nCf4R5ElWpKWjvRMmhLP2saVO

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\location[1].js	
MD5:	C4F67A4EFC37372559CD375AA74454A3
SHA1:	2B7303240D7CBEF2B7B9F3D22D306CC04CBFBE56
SHA-256:	C72856B40493B0C4A9FC25F80A10DFBF268B23B30A07D18AF4783017F54165DE
SHA-512:	1EE4D2C1ED8044128DCDCDB97DC8680886AD0EC06C856F2449B67A6B0B9D7DE0A5EA2BBA54EB405AB129DD0247E605B68DC11CEB6A074E6CF088A73948AF2481
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location
Preview:	jsonFeed({"country":"CH","state":"ZH","stateName":"Zurich","zipcode":"8152","timezone":"Europe/Zurich","latitude":"47.43000","longitude":"8.57180","city":"Zurich","continent":"EU"});

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 very long lines
Category:	downloaded
Size (bytes):	39223
Entropy (8bit):	5.392651968365947
Encrypted:	false
SSDEEP:	768:2l1lHt/JNVFGJIeNI9ReC0bG5woJhEZHvjgDMiB+2ahy2DTcLSpcFFaTi:cFe0erbGYZHvjkM2ahy2DTEpFaTi
MD5:	F1CC0111D27785A46AC776128CAA4338
SHA1:	EEF86861279DA1BD337F658BABB0C580A97802E8
SHA-256:	F61706920A0E99524824422E39DE3E833AB92D907651671F110A93DF46CCCB86
SHA-512:	81F25A059FFA3E313BDABAAD95C228B9E3FBC096096508AC668896D86F06369026BCD1F2267D827B22E4B412ACFA66F9950CC8CD50DF75D39A3CD94C385DE80
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spark.adobe.com/sp/login?r=reader_page_bumper_createyourown
Preview:	<!DOCTYPE html>.<html lang="en-US">.<head>. <script nomodule>document.location.href = '/unsupported';</script>. <title>Make Images, Videos and Web Stories for Free in Minutes | Adobe Spark</title>. <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />. <meta name="viewport" content="width=device-width,shrink-to-fit=no,user-scalable=no,initial-scale = 1.0,maximum-scale = 1.0">.<script type="text/javascript">.;window.NREUM||(NREUM={});NREUM.init={privacy:{cookies_enabled:true}};.window.NREUM||(NREUM={}),__nr_require=function(t,e,n){function r(n){if(!e[n]){var i=e[n]={exports:{}};t[n][0].call(i.exports,function(e){var i=t[n][1][e];return r(i||e)},i,i.exports)}return e[n].exports}if("function"==typeof __nr_require)return __nr_require;for(var i=0;i<n.length;i++)r(n[i]);return r}({1:[function(t,e,n){function r(t){try{c.console&&console.log(t)}catch(e){}}var i,o=t("ee"),a=t(22),c={};try{i=localStorage.getItem("__nr_flags").split(","),console&&"function"==typeof con

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\login[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	39223
Entropy (8bit):	5.392662699053527
Encrypted:	false
SSDEEP:	768:2l1lHt/JNVFGJIeNI9ReC0bG5woJhEZHvjgDMiB+2ahy2DTcLSpcFFaTJ9:cFe0erbGYZHvjkM2ahy2DTEpFaTJ9
MD5:	D4E62BA7612CDBEB738DC325FD63C7AE
SHA1:	36B2ACD4C4F7269AC21A786A314DC1ED74C73BA5
SHA-256:	2D169A5A83D82E779F1221232DD6CF0BE3736CF1F6AA9BDA306EA7E73D03A380
SHA-512:	DC86525FA26E16246227019963192D82E9961657ABDD54BF20289DD2B99886C79ABC15C72333BD13C7E865CF3072E9A9EDE0067759ABA902F334E513B7AD85C9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spark.adobe.com/sp/login?r=reader_page_topbar_createyourown
Preview:	<!DOCTYPE html>.<html lang="en-US">.<head>. <script nomodule>document.location.href = '/unsupported';</script>. <title>Make Images, Videos and Web Stories for Free in Minutes | Adobe Spark</title>. <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />. <meta name="viewport" content="width=device-width,shrink-to-fit=no,user-scalable=no,initial-scale = 1.0,maximum-scale = 1.0">.<script type="text/javascript">.;window.NREUM||(NREUM={});NREUM.init={privacy:{cookies_enabled:true}};.window.NREUM||(NREUM={}),__nr_require=function(t,e,n){function r(n){if(!e[n]){var i=e[n]={exports:{}};t[n][0].call(i.exports,function(e){var i=t[n][1][e];return r(i||e)},i,i.exports)}return e[n].exports}if("function"==typeof __nr_require)return __nr_require;for(var i=0;i<n.length;i++)r(n[i]);return r}({1:[function(t,e,n){function r(t){try{c.console&&console.log(t)}catch(e){}}var i,o=t("ee"),a=t(22),c={};try{i=localStorage.getItem("__nr_flags").split(","),console&&"function"==typeof con

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\marvelcommon-51100480[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	204314
Entropy (8bit):	5.2927791837848055
Encrypted:	false
SSDEEP:	3072:PVrtOowrXBOn3nmm6qI8pzYfwbgUU60R6X+ltN6HBDM:NrgowXMnXT6appgUU608Y4M
MD5:	48F849DA6F644B576196923A27236F15
SHA1:	8D47A27FA948519768268ECA970AB6487771A287

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\marvelcommon-51100480[1].js	
SHA-256:	15DA34D198A8ADE100CC1A6047F99FC87FC7785754E8E1A39A49F06F5D5D5873
SHA-512:	76340CBD3DCD0D2D534679319153F10833768B4C5F713871E782D4D854746AF1E4A880224BAD3C2BDB9626F5B615DEED67B3B176D38F97EC222309E9FDFF363
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spark.adobe.com/static/marvelcommon-51100480.js
Preview:	var marvelcommon=function(t){var e={};function n(r){if(e[r])return e[r].exports;var i=e[r]={i:r,l:!1,exports:{}};return t[r].call(i.exports,i,i.exports,n),i.l=!0,i.exports}return n .m=t,n.c=e,n.d=function(t,e,r){n.o(t,e)||Object.defineProperty(t,e,{enumerable:!0,get:r})},n.r=function(t){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.definePr operty(t,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(t,"__esModule",{value:!0})},n.t=function(t,e){if(1&e&&(t=n(t)),8&e)return t;if(4&e&&"object"==typeof t &&t&&t.__esModule)return t;var r=Object.create(null);if(n.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:t}),2&e&&"string"!=typeof t)for(var i in t)n.d(r,i,f unction(e){return t[e]}.bind(null,i));return r},n.n=function(t){var e=t&&t.__esModule?function(){return t.default}:function(){return t};return n.d(e,"a",e),e},n.o=function(t,e){ret urn Object.prototype.hasOwnProperty.call(t,e)},n.p="",n(n.s=3)}([function(t,e){/*! jQuery v2.1.3 | (c) 2005, 2014 jQuery Foundati

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:	downloaded
Size (bytes):	2426
Entropy (8bit):	7.911752375782477
Encrypted:	false
SSDEEP:	48:HPiJJswAeBpYYzTXC9uWsHy0ITQEVy7+zXQrbgWVmL2F0gHbBMtL:viJJWeB2okubHX+QEVKaXQrbgdEb2
MD5:	D429C48D851C6A5FD97402FE1ECF4792
SHA1:	1247216ADE627ED5F346D0C09F707A11B902FBF9
SHA-256:	2F6C56593996954A745B48834D9914C2D00BF0236C51BADACDD92C9869129402
SHA-512:	5B90F888B95159B08607E7BFEF2CB762D4A8986D3DCF42603932B0EFDB99C66A06B5BA4DDD40B53BB633E2B8B97C81CD3572CDCEBE4A140EE4DFA17CA344E EE3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/create/media_101f95855e967721bf3a66e02d5c53da102e51674.jpeg?width=2000&format=webply&optimize=medium
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...lAW...+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_106afd3797eb2a517c646ebca3f2ca33b6f7cbc1f[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):	13470
Entropy (8bit):	7.983517407990372
Encrypted:	false
SSDEEP:	384:24JNlMW+H+3lPfzkNvpaAEykLcHypRhw2FYgJ4Z8aKCvMBr:24J3aQPfwNvppEX4Ha9KrZKRBr
MD5:	F44C4E9822BC37504FD35B946CE4D6AB
SHA1:	DE7870635E9B8B83060048B9A6237E2BA5614A61
SHA-256:	34FCF35AB3F931C64AB6B742B954D3CAFAA163787BB9660B37A7B245F8D546E1
SHA-512:	7A7C68083966A04D58495CCD15F9C5DD0AE255A34BD7847AE6D0C386E2965B8B9897F5FF1DD226BF1E13F60AE9B2A7E3A72BD8B57E683AF04114475C57DACA 4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/discover/templates/media_106afd3797eb2a517c646ebca3f2ca33b6f7cbc1f.png?width=2000&format=webply&optimize=medium
Preview:	RIFF.4..WEBPVP8 .4..0....*..k.>u4.G...!&.....eK.{....S...{..')...=.y.}.?.....#.....C.s.w..TG.....p._.~?.....>e./.g.....{?.....r.....g.....?.<[....@.Z.w.....?....3..?.....M.+.... ._._....y.....?.?....&.....?.....,...._....8...[.?._...n.....X?e.....k.=.....u.e[X.sw....q..\..5*d..o7.M.....hY....8@p.....$.N..:..P.\....?+}. ..`Fgy...!*.i...."p.P....V.J.\.{m.9R..R .v...}MFa.._+.t.n...g..~....Cr{.....Y.h..^x.a.C.$.k...Uq.k:.?.....t.-.....LX.:..z..w.S../.....R...t...%.M...\i?s.z..].3..oD...n..r...|.....M.../...X...D":._...5J...o#..<.x@.!....;...w>...OS.."*..... (`.... .i#t.]..@R./..N.NsG-..X.OQ.Q..1....=1..Zd..d.T.....a..K..FXr.<u.p-.....J..?.]...Mp).@*.I...,.e..'..+.....7.,O....xrx..G.#....k.... .PM1.L%r.=|.I.....N.?d.....,Q.NS\.p.....}. .).i....O...G...n:"...-n.qE.4.#4GS.....v..n.....L....^.....;#.'+.,...&\P.9.2....GKdL..A.3P....._.....SSD.).:.nv.....8.d.;W..$]..f.m.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_12438f0ed5e015acd4f31b04e2a0bfd095e616ecd[1].jpeg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[none]x[none], YUV color, decoders should clamp
Category:	downloaded
Size (bytes):	11994
Entropy (8bit):	7.944011736504239
Encrypted:	false
SSDEEP:	192:SI8xno2dayzZxtFj7tRY8Cr9HEz8F+8nEJ2H3lrcTxJzIr75fSEXe9mN:8xoMZxDXtC8C9kz8FxnX3lr1Bu0
MD5:	7A9C201C09A4DFD3344ED1A558BC9838
SHA1:	EFA2D3D98EE80B2B89A2FC87CD5364BC2934C7DD

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_12438f0ed5e015acd4f31b04e2a0bfd095e616ecd[1].jpeg	
SHA-256:	03EACA689BDB3B97F0C64ECA889CC949E5E35FBE229759E77C61EEC59ECD0002
SHA-512:	9063413B8E0370EF8C3E857BE4BFAF3629A99167E10CC6C0FAE454CFDCB0C516A15AD3E9949CB9BBE62FD650828ABE44DE32E8CDD657E3804DC505F832BE9(1C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/create/media_12438f0ed5e015acd4f31b04e2a0bfd095e616ecd.jpeg?width=2000&format=webply&optimize=medium
Preview:	RIFF....WEBPVP8 ....p....*8.8.>u:.J$."...H....in._..h.../E..N6.>...I...S..k..?../...{..?.....e...^.?../.F....[.2.2.....|.~...?.{....4z.....7.....{}.B....IK.....IK.....IK..... .IK.....IK.....IK.....IK.....IK.....JW/..y.[.A....n.)%/.n.f.B.R....n.)..[.>.....S...C..@....x#pn..x/.....IK.....)w.w...O.^)VMq...nKe..m...3.cn.)%/.n.f.B.R....n. ..1.d[...,^.U..mP)}..u7..BW.....3....]2.b*.....n.f.B.R....n.)%/.i.}.....(^ip.iK.sK.Ag^..1. UL.S...!.e.jM.....D..cy.l...^..$..m...HRJ_.d....(.....,J.)..H...G.x]..g..=..|n..A..&.u.n.)%/.n.f.B .R.....;.....iL-.r..z. ..!I)s!.....JC.-a~.h..vP.?C...!I).[u{7R.....W.s.=L..~*.C....*....^..|..a..".ZP..`A.k.Q...n.)%/.n.f.B..SH.4.CX.]y...u!I).[u7xVv..7-{.wy..!....n.)%/.n.f.>...x..E~1L.Nk.. .m...HQN=7..._.(MZ..%a.>...IK.....F....'a..|.....8FM...n[u{7R.....W.u!E`.Q@>..vvJ..."..O..n..xi..W...(^f.....qY..}%/.n.f.B.R....l.,%,Y.g.].

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_124e34d3819ffeb81b5d7792530ea9a99961b1948[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):	11192
Entropy (8bit):	7.981805427063665
Encrypted:	false
SSDEEP:	192:LdKp2W9606CMmRJCgF8Vu7mTAZzTTQuGH1rT8dC/PVbwA4bEKAO0DNFb:8pI06Cd7amHxTTQuS3/Pl+bEKAO0DNF
MD5:	1052D0B4FE4E3D6A976E0C0D866DA0F0
SHA1:	1C141848060AEC58146088BE62CB390B94B84A01
SHA-256:	98DB8F4F2D6892EBBF1B22663E02F4BADC8882CE22D361C057BF0456AB7112D1
SHA-512:	58845C78647D57984710FF361224093C480E03081E80F64658081541D4ACC98A32F4D24A94C9D911500C33D120B56D69B0510B18072303C5E4F17E4C3BEC6420
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/discover/templates/media_124e34d3819ffeb81b5d7792530ea9a99961b1948.png?width=2000&format=webply&optimize=medium
Preview:	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..rl..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**

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_12aa7e4bc0022e4439e60c45ad19f273e0b27517a[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):	15516
Entropy (8bit):	7.987491006007941
Encrypted:	false
SSDEEP:	384:qGrRUbYsOI12dIYrjGW/bRqAOuUnIkxXa7FNpCOnuI:qGlUMrQiCARoICamI
MD5:	CF624FF5D26B2A801821939488DEB07F
SHA1:	75F585F9DCDB8595BE6B0E4AD07975FF616C4701
SHA-256:	16C0C9C0D76D9AFD82C0D72607576D09C32F146006041B59E03C44A77AF5B60A
SHA-512:	B8EE14D92F55AB2DAE78A16930077BA15F729F9F007B52AC19A3BDDE477B1A831E1F25A208AE8B0680A7475F3E08CB4E8703825BC78B8DA1819DFCB75809516
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/discover/templates/media_12aa7e4bc0022e4439e60c45ad19f273e0b27517a.png?width=2000&format=webply&optimize=medium
Preview:	RIFF.<..WEBPVP8 .<.....*..k.>u2.G$..!*3.h...M....._b}/..}.....{.....f....?.{.....O.>....?.~.{....'...O.'._.....Ox..}@?.....C...{.W.c.w.....?.....7.....>?.n.....R.....x.....^.... <.u...wq....3...?.~P|8}../H.....W.}.'.....k.....>..../.C....._.....Y...)..o../...?..._....$-7..">....Z..#v..Q.V...z.R.O.....9.F..N..^.7Av.;..0.....<....6..}/...P....a.@./.:..}....\;-..E.n~ .0q._.t....(....;nQ.....Z.}j.nq.J....j...b..L..1.t....$?....d.q_...,Z..M.\..`.....9!.B|..$\.f..>.;....(.`.iB...}..o...Q...i....Rq.oa.{.&..x.....L.C.kg.../....0<>.2..c5...0.l{v.J@....A..~e..*..... .%Gt.Cg.,G.....v.d..t-....n..J...L.....i#.!../.2..Cz...R.K.s@j.Q.9)U..P.M.@.DJ/.[Y..~..q..._....].O..n....3.TJj.....(.K.....}...9i.....A...eUty....&..+..}.n.....4/..0y=.#.....<.S.....^i.ZtI...:..... 3q..{!.."Q0B.....E.==...0.@.iM....9..E..&.{L.0;.(...ZM..`%.....@...R.2...i.:.rD.x...a.7../.`....g|..Ge.i!..[j..k....zg..<

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_12be25e65cc93e1440bc25fe8d545d5755fbd3f9d[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):	12744
Entropy (8bit):	7.984434447626562
Encrypted:	false
SSDEEP:	384:m2VKB+rxH6ZgKPsL5Dw6qXoDYr9FplMsIyBo/1a:mfK6Zg6U5E64oK9FXMGo/E
MD5:	75340F2CA756FB72A15C6A269E20C3B6
SHA1:	96157EBE0D3D143A2C6B11F52D881C0AA9BA01E5
SHA-256:	8A1461DA7256179A86600B5C14F2BBDEF900851D8F40D82FC7B438AF8D89DEF9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_12be25e65cc93e1440bc25fe8d545d5755fbd3f9d[1].png	
SHA-512:	C72DE25E4AB647F10E062012DADE8B3FBA672A2AA529AD1EB320665F54AD40A3F5C1F32657BF424118BF7CB8018DE09A0E0C4A0BE20F42D9F0F9CE9749525E2 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/discover/templates/media_12be25e65cc93e1440bc25fe8d545d5755fbd3f9d.png?width=2000&format=webply&optimize=medium
Preview:	RIFF.1..WEBPVP8 .1.....*..k.>u2.H$..!.w.H...gn.[....IL...?L;y..lp.j.....g.?w.....".u.M.....b.i....P_.?.....-..G./..Q...w.../@.I.....O...?....;...Y.[.....?....5.s.....w./ .?..h>.?......S.W.....o...../m_...?s....O....~...'*&...H1...-....a3#..;[..z.'.-../..B..i:.&.....}.....x..G.f.,x56....N:t.k....m7.Y;.?...NW.h<<m.....U.Y.ya9.i.....O..1Y....}...q...rA.,Q... .2..;.-.N.|.~W.*Y.O%H5WP<....+4l.t|Eh.xX..ZwH.7F...h.-.VL...]0.....|...'....b..*Q.F...N.i..]lQ.....?...o....l..+..lb..\c.O.(...0.q).....>..J.(4.52.....4.)....Qr.2..h.R.^..>;.=...3.7....pr. z..*.;..&..O1)t.....{...v.32j).S.....q.....<..1.....LK....<{.M...[.g. .....KV..q.,..jO..s..4.a...b....7..G#..TaY.YO/yX=1....D...QS.."9s....yR..Q.....6.....r.Vo4R..U...[K..$..Y'.j..w.._.W..... K.....5..2...-..1.m~...2.,Y...PF..+..'./...&.....Q..QD.....N.3Y...G0...!..W|_y....a.ZK.n.l.,.J.....4.....*a.8...5\.....nA_/.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_13f1bc71a8681cdd7cb22c202f5a3c11bce1c01b5[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):	12628
Entropy (8bit):	7.982545840794857
Encrypted:	false
SSDEEP:	384:SfcrQbUMDW4yQORBvyZ5zfcSeNPW2g6hx:7uDWd97vyZ9UfNe2zhx
MD5:	C82FA189EE214CD72B7CC9BC103291C1
SHA1:	D940ABFD7668D8A04ADF4419CB8A4B44542D5781
SHA-256:	13E2F45B312E32569613AB0CB690B04F6F1FA51322678D758AA6D9568E2D8366
SHA-512:	A4A2AF1170B19070B92A78158CDB31DEF3088AE222E0D059A2AAD4C4953332E85771F16E3FE805E5A8CF97C9CDB21A88B9013730A058FA5FF989B739E3C1E66I
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/discover/templates/media_13f1bc71a8681cdd7cb22c202f5a3c11bce1c01b5.png?width=2000&format=webply&optimize=medium
Preview:	RIFFL1..WEBPVP8 @1.....*..k.>u4.H$...&r.ip..in..Tq..a?.C...s.....{....[.L.....y.....W...?..g..._...../..'.....#.?....7.....g.....?..]..../.....~....{.....?...}7.y.....{...?.... ..\|1~...@R%~..De`."..c...D.y.8._..8.F\|.i[xM.....v.a.x...R..2....+....H$.fN..kt..%j@.t...6oK...mI.4 .\..r.#im.UI....e.q.....vQ5..8o.6.D..Y.y{.\G}M.....T...iJ..}t.2zg..FD..m..}=1{.f..... pD..dd|.CC=.....\L.[l...^h..s....K.].=M&..2..J..n.....j.....&...2.]..UT.....?..3.....U....}.....2..f.Ct.a7kh`[$.x_.7&8.?..tz.....3'...?.+C...{+W.soKp+.Y.....X..~(.....A.G+...u.j. cAr2..f.....HZ..2GZ...k....5.*..T..iv:+....8Il....{..;bQ..|.....`..r.../_....R..."o.T.:...1.....X...rp%.p.&<^4.Rh.@.#...S..<..N...#....{+h>vRO.....p.``._x...6..2....(..U.U..q..3Z.3..j.....C.....(& ...X+4....H....n.]..^.c.....~@v.#C...?._x...G.....V)MP..4..'?..D...?2.r.....j..w.....Q....'....%}.....J.....0x3....\...H..'+..o....O....n..!.u..t|.(

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:	74DCB02EA68CB39DBDB43F6E9121E7D019C5F89693489DC54BFD89AD846C81F5A4F642ADCFBBC5503EAF020AFEC2F54ADE1F6D3551BF65093D8E63ABB775C EE
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_1483169d9ed54a159cea2c7282c24b5a771f38d79[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):	10386
Entropy (8bit):	7.985491005040909
Encrypted:	false
SSDEEP:	192:zOHbO4AT7Nu3Zot4hi/vR/NG8TLTOeVp0AWpuEGYLSWssKfUczrUB5:iHS4AT4OxIITfgpSYLSxsKfXf05
MD5:	4CE22C5215DDEFB3293DA733ED46267F
SHA1:	14C577DB5B066AAC812B438EE9F039EBEEBF7495
SHA-256:	9C177E49CF1A6AFD3D4DDF2C94247EF65210AFDCC8778D21F8992DE8BD54B44B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_1483169d9ed54a159cea2c7282c24b5a771f38d79[1].png	
SHA-512:	6C04C6BB9844CC30CC4963B9D5346747134B3775ECF50E852F5F099677E9F7BBC864E9F0AA91E41EDAFF5BD26C9A53BF703E57C11BC13E8C79AD9B4D532E601
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/discover/templates/media_1483169d9ed54a159cea2c7282c24b5a771f38d79.png?width=2000&format=webply&optimize=medium
Preview:	RIFF.(..WEBPVP8 ~(..p....*..k.>u:.I$."$$2.....gn..RL.0..3....s..u.17.....5zG........=3....=H<.e..d.L.......o...v...tQ...z.{s....*.>....o....^..u.....7.?..xO......#...w..jF..1.z..V....:.=/.b.B.....N>..fJ.i...I.........CV.y.i5M.}_ 2..#!r*.;..1<...PZr$.e0..z..{.@.....MAt.....w..\.^....L.vk....IW@>V..B..C.qv..+.vD3.......A.....D..r.O.R?.H.e8.G.O..Q 31.y.3H....{....$6..B..k.n^....q./.&....I.Z..i...^U.....{]zB...;....(.....M./....v+.....R.Z...n'.1-...:l.V...q0}...U.d...gD.<.d0.......B.....}.|m.........!..f....e,....}.}..5.....6.~.fL.-.AO...h...O.".1c......;4....m..!r.p.XvI.m..q.#..S...C.TYo-@.Q..v..Q.{......?>P....V.....:....M....L..R.\......p.U.Y:...x..6.u.~n3.v.....4.....$(..;N..n.....6..-..+Jf..B../.#..C.....+cz.....z.".(S..G.[.0oS..o....dg*.....~p*...F[.p..e.,\..].e..8q@rK..].P?..o....`.~.R{.w.j..(....U]..&..Vs.....[[.s..z.p.q.m.~..wb.bkT...5.....g....j4.....H..EeG+ .G4.....v].E.].)!.HCw.....p....7.....K*.....].

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_14abffd21a7d6097f1e2ae3f31e97c67849e1d60a[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	11218
Entropy (8bit):	7.97490613143463
Encrypted:	false
SSDEEP:	192:96KNpnMzq/pA4zcXFBCr64AE/Dd7hZKtcSRIf+temQmYRHy5KgszDC/3AlH:9PBMzq/pTz0nCGQ/Dd7hZBZmqRS5KfJB
MD5:	2678D0BB8ED0533BE22F7D0CA737042B
SHA1:	D71AFFB93796AA39093DCAAFCCD2F460F25F4B69
SHA-256:	8E98B9F3035D76189B158B585694058FEC1ACF935028BA2F321025D28A6A8129
SHA-512:	F0197B16FBFDFD2A170FCBEFEB164CA0B2635193F53E25875D0CDAFF492E061313850635AA53E4D039EF477C3690DCDF9F3274366DD6DB2C5F5D829C0C9EF8E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/create/media_14abffd21a7d6097f1e2ae3f31e97c67849e1d60a.png?width=2000&format=webply&optimize=medium
Preview:	RIFF.+..WEBPVP8X.............ALPH......@.i;..m.m.m.m.m.....~$.jTDL..._._.<.c....3........-....b...r...~...x44....[v..x.1.0.9...^}..(.n`g@y@T.$.....k.............Y.Z..5..........D..7.xT.~`..!....p.Jt...$.....5...y....@.q.#...;8...b..K.........'3...%...`.K>...-]...W7..9;.g..o../.d...._.@.Q.j(..1MA.............oH..6I$@n../.I.H.......u$@g.y..h).... .H..''a=r...(*.......?....... .H..D....~,9.C$.E....O...S......?...O..7.m2.P....~.>...9K.H R......?...O...S.....?...O...S.....?...-<CP.p..D...3..=,.#....h`..9L.$@q..(b.&..Y.@E.=...-z...x.[F..0.!..U.....>.q...6...MT.....ndp...w..G..S.W..!..bX.D.9.0....K.'..w...x.....y.sur...l(.].{..<.&R.P...6%.yh.l.".>..V% ....5....q..S.zv......y$.Rp....w.>.@..Wp&.@....(.@ .K.yl.y@T.0p.C.q@.g7.w...l.(F.@r.(n.....U.......U .MY...co./X.s.q...<8...VP8 .(..P....*....>.B.J%..!.1. ...M...j.(Qs...]........p.?.#.@.H5]..[...?......u.G.s.....:.T?...z....+...K......?...........G.K...{.S...../.....?...?...u/.g._..........O....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_1707de0129dfc8f4ddadb55149ab2dfd705e786b2[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):	9086
Entropy (8bit):	7.979107058438218
Encrypted:	false
SSDEEP:	192:ro5qJbhyval4dyRHzCucw8FtcwsKVZKfXXSLmkOaWtjr5DB1Hm:rYqJ1yvq4dyRHzCfw8DgsmkOaI5DrG
MD5:	81485C1DC373C58B7D6B7E09DEB1B1E1
SHA1:	72B68330FE262ED781B97B26746BB41C96F28179
SHA-256:	F9FC8250106A68777FF81B1EE71BF189AB67E68CB192275998D728CF79BB1C09
SHA-512:	3D0F19A7A83B8D66465519B9C68C2DD83C9F5502C44B99D691BEB702BCBB85BE771826867085F37B18BC1A22FBD79EE50EF36293B4111E0573DF2F3B99E82275
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/discover/templates/media_1707de0129dfc8f4ddadb55149ab2dfd705e786b2.png?width=2000&format=webply&optimize=medium
Preview:	RIFFv#..WEBPVP8 j#.......*..k.>u6.H....$......gn.q...s...=..>n.....U....+.w.....3...o.\..=.......?.....2..?...}5._..A}....?N.M.O2.@<......o.>.....Ng.._Q?..O. .9.....(?n..,.y.p...K..z(.....W....v....#$.>5o."s..)*?iY.L.[.......;.c{....\..R:..>..wf.U..g.....M..6......-.8{I.}9....=ws 1.C..*nf.AS...gw..t?.....V.iW...jF.....".}.;.Y.X..x0*.....N..}..I....h.3.4..=....2-1.V.r..r..`.....%<p."....w.R_.79.v.'....W"2....D....jY.v.|.au..x(.bI.22....=...;.t}.....0.,..t+...{.K..M..)r....1bR.T.....8*(;.....|\..Z.....K...k:...+hJSl..{.S.2a../.~n..i+...$..AY.JfU..--..Js..G.....j.....z.5...Izs.t..8JP....Q?.A.%?6...$..d.....M..Y^.....F....../Q:..m..<..'.....c.....A.*.&...."P.W."!x.70.m...3f.).....n6..d.....O...2.j....E....7.l.f.....!...nDSf..9..$.7.2&.d8....z.....pa..,.U`2.....1...p..(.oB.O.a.S...LX'.@...v..6.!.1kjnrO:....<^....'.ru.E..s8.....k...#3.....C&..S.....cT....TN.kv".8....-.*,z..I.../...A.'...}(....n..(...7W.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_18213dc89b86cad2ba1ec4d4d422be8ddbeddff77[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):	10362
Entropy (8bit):	7.981486280225858
Encrypted:	false
SSDEEP:	192:qVu9zG+97Gbx7lcUdp7yEF5lVBNeSxwydKlCfpFpopm8T3/PFDx:Mu7G0Ud4ILCyRDE3
MD5:	3EF437420507DDEA237643058194827A
SHA1:	E6342ECD457C545BBEEF97D3D1EDEB743B60D295
SHA-256:	42BF6CAA029E18AA42360773590164C56E9BFD52A1C0E7A178D64266CCC2DE6C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_18213dc89b86cad2ba1ec4d4d422be8ddbeddff77[1].png	
SHA-512:	41C923B158476946D8B6B256B258B5CEAEDEE8B37C5CD23BB7D50497B136C5B1B4BBF4AB25E92B9240A4F078771F5FA43C1D42113E795079E8BA2479D0E7D004
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/discover/templates/media_18213dc89b86cad2ba1ec4d4d422be8ddbeddff77.png?width=2000&format=webply&optimize=medium
Preview:	RIFFr(..WEBPVP8 f(..0....*..k.>u4.H...!%3.....in....N../...Y...9.....U...w.&..$.._s.5.....;.G....1?..7...P_.?.....,_..~J.e\|....^.....?.?.?..D...w.....M.....o._....8.I....._k ?.....S...._._.....B4h..L_....).1.L:.{f..Uk.#.Tt..Dq...! .Wn^b.\|C...N...xe.=u._.}.h....Klk.....g2.S^_.4Z....J.X.H.....H.*XR_...^...X.....D....x{.. ..3Y.'.@K.....g^..L...."}-~ ...*8..S.K013.4...M..i,..(...._..&h.2]...i.9.....%3.0W...S.....PU...7YnVP.lg.....g].g.f...S^....oT.....b.Y.oUt.....l.vP.,.7...`..t.M.F$q.Z...D4`.{.%.U...c.....K.|.CZ....`.3.....W....x.4 ..f../..R.>...L.jKh...?.,KYX....G-F.0.!:.....=OB.4]4...u.nWe.5.....\....6....q..<|,..?:.....*e..BaF,{...gu.c.D4.&.b..<ERC....@'..l.m.u.05...;3+....lx.....S..''..8..c.....@..;...C..+....m.D ...v.h....u..W...ip?-.L.#0.o:A....3...Q.....M..<.0.8..&..0.#.26+.O..8....'.[.s..}v.2E[7X.O.....b.ng..*./.X.....C.w..r./:<..q5...;.....2..9...j9.....Tx.. .(*Ux..H-3..P.#.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_1a92e0ac878c2fd223de53d35d857869c15554031[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):	8590
Entropy (8bit):	7.977187421262688
Encrypted:	false
SSDEEP:	192:wgqvM1TzqVApm676PjHkqGv3hnmYv67lLbMTi5SOIB9WCd:wtcTznmk+am26hvei5Jl3
MD5:	FB859E52DD20BA87612747105AC952B0
SHA1:	AD06A39BEE6B13DACDF62CE5A3FA6C4AFFBF0C89
SHA-256:	71A1DAE9A84B243FE87BF0AEA3CE75154273B5579755475FD09253E650F705A8
SHA-512:	9BB340A124CC088A5527C448D634D62D36DA8C56DA72D0786641C7CDD52E6A48E9193F8B763F4F31C06992C6C45DAF6A1A3290BD21C21CDE877D54296F5915
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/discover/templates/media_1a92e0ac878c2fd223de53d35d857869c15554031.png?width=2000&format=webply&optimize=medium
Preview:	RIFF.!..WEBPVP8 z!..P}...*..k.>u8.H..''!#.....in.:....P..H......A....vYO.'Q...o...?.....,_.<..&k^`..}.K..Q.;....3.....O9.....9.E.....#.e...._..s~.....?.o.....?.....;.)o....L0a*.... ...S...../.|.i....3p!&..<.xS.n.3...C.C._m.....(..y..M.g}.l.....rz.iM.D...Cf.....O..l.1@./.,.^A.....f...S5H..l.`z.^ o....k...).M.~.]wR.+;...t...u...8..wk..lu..$.l.....X.....A:..q..[1..^@z... ..)!:..J.7.=...x..?b.....n3@.3gn.C.42:.....?.....o .....`S?.t.b..Hm.Xtw.T?@S....~..,V..).....1.....8M.....:.....$...m..s.5.z..aeD.U.f.[..q.....,.]....o{...[E~..i.....}.-...M6wM..?O...kY tS.[..:.....pK..c.MU.0.)V''..T..J...X.Ge.....Z5[..-.8..A./y.~...T/O.5./_.}.....X.o.. .C....;....H..I...\..e....M.f..\..>.YX..K .b..#7..$.D..R.@...u.....E..t.5....VF.s.#U.i.k.[6...Yn.KM.By. J....l....&.0...;.....QM...\|..=k_..l....gvP.Q.....n.....KB....W.S...i.''.....I.}..U.....D''.2..VZ.I...7....Z ...$..1=....~..(..%..9u..c.]....4...l.t....tb.-S

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_1b1edc2eb0698cdb9a2fe1b8b32e420743c6137b4[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):	9458
Entropy (8bit):	7.978909076804826
Encrypted:	false
SSDEEP:	192:+7op9Mt9JgeFZOnME8DM+mJ80pOWvM5t+xrMfmPi4gzKkVfpR8F/7/SB:gJT38ME8HSO8Mj+xru4gOQwF/7/SB
MD5:	B1FDC53A3202237C8FD7FC9122BEBDDC
SHA1:	7A534922F4B6333901AAB35F50138B7F8ADA2E63
SHA-256:	09F6B16C71FC41F43FBD74117093D0009954793DD0126AE23A0F044311050393
SHA-512:	6B796E0C658A31760357F767AB128B2FE35E20D9F74ACC84AE8E5193735BC2DEC34BBB11B09AB782611F9022D21068C45B7E7D911B2762553ECE90603BFAFE5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/discover/templates/media_1b1edc2eb0698cdb9a2fe1b8b32e420743c6137b4.png?width=2000&format=webply&optimize=medium
Preview:	RIFF.$..WEBPVP8 .$.....*..k.>u6.H....%3.....gn..X0]f[....y..Iz/#.....k....L..^a...%.v..;...._.e.Q..%.....v....s....s...N0.G.....?v.g.....M..._.|.v.n~a..}.....g...?..... [.....w...o|..e.o.!.....p[&...9..]...''.E+.k<.''k.y.4.3Q.c.]/.[o+S.K.J7.&...TW.[.,...dl..._.P..E;l...a....d.@Q.Z.....v.@.....).R.....7t....6bb.k.qmgL.g6..;.&.L.....Cs..z..ky:9.. _.kpT.m.....Ch..P.s.t.2[]..4.....&.EZ.%.-Z.|.X..`..j.a.....l.kC.....|..o...o.....u..R.....(.s..V)..''.UGP.n.y{..k.....Y/...nUW.:]..o..1.$..\..-I.....i.d..0.....Mm.{...X4z...5...?...B.... R..J..c].d...N.5.....nB....4..B;$....8....0.$u.L.@f.Q@.w.....)h~....8.....[#.QR..8o]..De.....5'';e._....8~UBK;..b.....I.....N.v..X..aw:Y..g;..!.#..b.~.1l.[0...7F..\|g.3Z.9..n..c..w..b.~QG 7..WnW.VbH.Se..f.@3.s.. .F.Hx*w..[.....S>.....\_.....:$s..8l..''2.i...r.....^...4....WC..z2.)....(.-..o.....~..P.....7adP#!E,..8J..*.G.....q...c..3..._.g.:D`!.....p..aB

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_1d475ea237f3632359c1538d48da93b1deff5ed7e[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):	5006
Entropy (8bit):	7.962700355562703
Encrypted:	false
SSDEEP:	96:fyHCbgDyr0H1lkP+AXLiv7iffZcgBKV7jWgzU9vzVAyFELqaWK:qHCbgWY1JP+OLilVrWOyF7K
MD5:	AB3FE31B4A563F72F1975598178630DF
SHA1:	D7D90BBE9BDFAE5A4721A50828819DCD5959DE41
SHA-256:	C29607EE46628C768510C24E82A215A4998A5D6844E8BA4E8C1BA0F2944A0E2E
SHA-512:	06AF1DBEEE72021B25A24DDE247D8F69B8F9EB4933FDC432FF23CDA0D0BC3BD2938181E0DE4056F511F8C7D88E18609C65D88FBEC5A2FD92C1EEA6C33A079C7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_1d475ea237f3632359c1538d48da93b1deff5ed7e[1].png	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/discover/templates/media_1d475ea237f3632359c1538d48da93b1deff5ed7e.png?width=2000&format=webply&optimize=medium
Preview:	RIFF....WEBPVP8 z....j...*..r.>.F.L%..."2..p..in.....Q.R...v..c..7.~...I..6=n..go.`4.751..,.>.....fEXQ....z.R...\1..Z7...`P._M..4.Lc}x($bD.....,....|.K.M.~M...Y].A.....e.G..{.V.4*.'.... .../t..r..xS.x^.7N.....zP\|S.A~.4.P..s.....T..bV....q.....w....].2.V@..y..RJ..B.^4ZY(....5.'..<.....=..yz.....<l6=..>...6...Wf.^!...(..R4..7..R.r+./..?.o..Y/t.2...V.....pR.^..'.....$#Y.....5 L..mnK....8.a.v.o..MYj+."bs..{../\.j....6.....6.@..D.8.....M..(^(...q.A...}"H...S.....J.X..K....Cb..I...a...^....Y,'...*..H..-S..Y.|pFT ..1.=z.[.>.p...[Hz....YI.CG.8g...z...-1.{.!.w.w.O. |.4..M.w..."^K!....fgq..3.<1n.c(....YK.I...N.. .5.....(V./...>..IN.....{..D.j.3.QLe..Q .[.BX.....~t.M...:...$M.....y.\.IK+.U.r..5.2..ez.....c...-<...T.5...+i...X...[4._..o.K..+ ..=.qd.*.....L..q0..q1..P.....O...|..\.D5]r.....a.d``....V...9'^e$d.X],g..3.2.J.i1I.....X...,....GdG.,..V&.'.d._...a7...cS..p(g.W...8.....%.\....d.){.....G.....I..VBQ>i09D[.....9

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:	downloaded
Size (bytes):	6210
Entropy (8bit):	7.962124363478672
Encrypted:	false
SSDEEP:	192:lsF6b9jBPo5sFpZY6aFHTaPBb3K4hqzDW9Csj:lNjBQ5QLgFzaPpnhCwj
MD5:	34A9826873AB6E5600A1AB2014C94A64
SHA1:	F67628E01D5F1DBFA5095BE50B3A339CA7D03E0D
SHA-256:	7B9D3091AEDFC9C1F5C85EF03B57CC69F64A7827146648AF315EF53F587AD19D
SHA-512:	4333D5B2799FBACDC7D22DAFEA54FCE1AC4B6E9A2D85BC7659904AC140F04D64F1D0634F2DEE96A12BD818C3CA4362306270A63DD079C28AF1E0FE183192178
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/create/media_1ed4c2a2a5130e5f9cdeed32b1221f2e7d8988f38.jpeg?width=2000&format=webply&optimize=medium
Preview:	RIFF:...WEBPVP8 .....S...*....>u6.H$..!&.Y....cn.s....Ys...[..f.p..l....v..9.I.....7.?.y.f.....~[..........%._.....C..._.>.w..P/.....-/.....F...o.....?Z..y_..x.....O.....?.....q... .O.....t...=..FF...A##x.i.....fy.{.'.<....#..a....{.+...0.....g..m.F..}.t.Q...z\;.aYq... *H..-s.l.}P.5.#.R.3P....!.?...O.e;1..&H...B....CE?..k.i.....X.._#.}'....zF.p.gqL.CY?...u.8..4...;d,g.. ..t52..f..KEt.....5..m..._.p.X....6G&.....".X)..X...u.".-R_..O..?!..S.4.hd..F..i^_?..P...b..>.k.....Zh.....C-..2U@,.Y...eaM.....0....0..\....."5't..3...1....s.Sq.Y.2..c....0.....,m..... .q,..H+i.O\L.J=.....~.6N.h...l.....>.j.{.d..5y..... ....$.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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\media_1f32be53e4c9aae4eb853ad4ef058c861bf97a4d6[1].png	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/discover/templates/media_1f32be53e4c9aae4eb853ad4ef058c861bf97a4d6.png?width=2000&format=webply&optimize=medium
Preview:	RIFF.,..WEBPVP8 .+..p....*..k.>u6.H$."!&.....in.B....9..Q...<...K.....}'..._..#x?.....z.A.....t.....Oy.....?...z.....?R.....o..{.t....^....g....f.....g.?.~....._....y.}....O...o..?.... ....k.o...<....[.?.... ..?....%.....2...X..}].cZY.!...f9.b..e.....l....G+..F....c..55.r.U.<.D.yy....N.^....Lv..h.....,.7W.....).d)Pf.0(.....4.....S..\|hF..Q..+.m..Z.Z...w 5.M.....ZM'..i.{.o.. O..c.....*...8..MBt.`k..E..Y..Jl)y.."..a"E.b.>...}c....R.D.....^....w....\rpDd...f+...~....^'f.$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....d o.....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\ntKiaikxRt9X0[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	52823
Entropy (8bit):	5.222761885806773
Encrypted:	false
SSDEEP:	768:mn8+27e5FyW7F1FnWO8JARtEeqakKnA+b:mnT224W7zhWO8JCnAi
MD5:	FFB13207C301D70390BD03A3E98B019E
SHA1:	2D8067483D9DCD2B2FA77DB1045C250B3CC74E9E
SHA-256:	49C9571049526F1CAEB320AFB1D78F3A2F7F51B86B896577200F1F0D91D4A940
SHA-512:	4C568E749EDA1D4467FF740685B3CE342F16B51501A6565BBBC5B29615EDEA91C5E854534F8DB1F7F2EFC14511F23AD053F318A50BF6816E436E69BC0BEFB0B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spark.adobe.com/page/ntKiaikxRt9X0/?page-mode=static
Preview:	<!DOCTYPE html>.<html>.<head>. <meta charset="utf-8">. <title>PAYMENT REMITTANCE</title>. <meta content="yes" name="apple-touch-fullscreen" />. <meta content="yes" name="apple-mobile-web-app-capable" />. <meta content="black-translucent" name="apple-mobile-web-app-status-bar-style" />. <meta content=" width=device-width, initial-scale=1, maximum-scale=1" name="viewport" />.. <meta name="robots" content="noindex">.. <meta property="og:title" content="PAYMENT REMITTANCE">. <meta property="og:type" content="website">. <meta property="og:image" content="https://spark.adobe.com/page/ntKiaikxRt9X0/embed.jpg?bu ster=1620832842217">. <meta property="og:image:width" content="1024">. <meta property="og:image:height" content="512">. <meta property="og:site_name" c ontent="Adobe Spark">. <meta property="og:description" content="A story told with Adobe Spark">.. <meta name="twitter:card" content="summary_large_image">. <meta name="twitter:title" content=

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://landarch.org/hassani/images/office3651.png
Preview:	.PNG.....IHDR..... .....pHYs.....<eiTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?>.<x:xmpmeta xmlns:x="adob e: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="htt p://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:Creato rTool>. <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\onz5gap[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):	18234
Entropy (8bit):	5.586204667535263
Encrypted:	false
SSDEEP:	384:x2V02tpIgIPs51iRm2lIew42noFeFsP9btiCtpIaCR:8V6q1iRm2XwMqsbbt6J
MD5:	DAF93A792133E2F3BB29B04E819231C5
SHA1:	5597BCE352A8B04E573CCECA126EB4912C626A9E
SHA-256:	1B586E639CBD3E2276EB3A1DE829E913806653FE43D5C19A7ACA128A43DC69F1
SHA-512:	9B409DDCCD60E505C008B88D55052723F2A25B62ABA596A1BB9FEAC1230DD037DB551F7A5928A6ACC5E158219B441E7B9428159885D6638497B2B5F9B2D42F9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\onz5gap[1].js	
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.. *. * adobe-clean:. * - http://typekit.com/eulas/00000000000000003b9b3f85. * - http://typekit.com/eulas/00000000000000003b9b3f88. * - http://typekit.com/eulas/00000000000000003b9b3f83. * - http://typekit.com/eulas/00000000000000003b9b3f8a. * proxima-nova:. * - http://typekit.com/eulas/00000000000000003b9b3068. *. * . 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-serif",".tk-adobe-clean","\"adobe-clean\",sans-serif"],"fi":[139,7180,7182,7184,7185],"fc":[{"id":139,"family":"proxima-nova","src":"https://use.typekit.net/af/949f99/00000000000000003b9b3068/27/{format}{?primer,subset_id,fvd,v}","descript

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\otSDKStub[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	17376
Entropy (8bit):	5.343827110329912
Encrypted:	false
SSDEEP:	192:wQp/LPwSNkXylwshci9wfW0vMfPPVMmXUxcjz3ZYVO2zswGBF27iIvZo:jR7MiOsrjyMfPPGg3ZOowGv2uIvZo
MD5:	9967D00318D7874F3531B1C7FF3DD155
SHA1:	30947E4D753FEE6D3817CF08EDA4861ADAA76DED
SHA-256:	40F12E335914950B4F2058DBCBBEE727F3F7542399EC6B2E98256480EA91AA49
SHA-512:	DFA75FBADC89FB18F693F5FC1E930F00E76EB831FABFE3E13B8D090BD7B4B07508E20DC43E6F66E16E5D8DA0FFA796815083EB3813DEAF0CC49C923D5646230A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.cookielaw.org/scripttemplates/otSDKStub.js
Preview:	var OneTrustStub=function(e){"use strict";var t,o,n,a,i,r,s,l,c,p,u,d,m,h,g,f,b,A,y,C,v,I,S,w,T,L,R,B,D,_,G,E,P,U,k,O,F,V,x,N,H,M,j,K,z,q,J,W,Y,Q,X,Z,$,ee=new function(){this.optanonCookieName="OptanonConsent",this.optanonHtmlGroupData=[],this.optanonHostData=[],this.genVendorsData=[],this.IABCookieValue="",this.oneTrustIABCookieName="eupubconsent",this.oneTrustIsIABCrossConsentEnableParam="isIABGlobal",this.isStubReady=!0,this.geolocationCookiesParam="geolocation",this.EUCOUNTRIES=["BE","BG","CZ","DK","DE","EE","IE","GR","ES","FR","IT","CY","LV","LT","LU","HU","MT","NL","AT","PL","PT","RO","SI","SK","FI","SE","GB","HR","LI","NO","IS"],this.stubFileName="otSDKStub",this.DATAFILEATTRIBUTE="data-domain-script",this.bannerScriptName="otBannerSdk.js",this.mobileOnlineURL=[],this.isMigratedURL=!1,this.migratedCCTID="[[OldCCTID]]",this.migratedDomainId="[[NewDomainId]]",this.userLocation={country:"",state:""}};(o=t=t||{})[o.Unknown=0]="Unknown",o[o.BannerCloseButton=1]="BannerCloseButton",o[

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://landarch.org/hassani/images/other1.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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\outlook1[1].png	
SHA-512:	DF4A0A2F78B2013035FB738BF405119B275D4CFEC31A23071EB9AF499D5F31FDC4BE22754CE791C975D7D417E908B5CAD16F962B0ADD3DFDCDE19844D74F668
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://landarch.org/hassani/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.....l.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=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&_=1620870126590
Preview:	GIF89a.....,..... ;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\popper.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	19188
Entropy (8bit):	5.212814407014048
Encrypted:	false
SSDEEP:	384:+CbuG4xGNoDic2UjKPafxwC5b/4xQviOJU7QzxzivDdE3pcGdjkd/9jt3B+Kb964:zb4xGmiJfaf7gxQvVU7eziv+cSjknZ3f
MD5:	70D3FDA195602FE8B75E0097EED74DDE
SHA1:	C3B977AA4B8DFB69D651E07015031D385DED964B
SHA-256:	A52F7AA54D7BCAAFA056EE0A050262DFC5694AE28DEE8B4CAC3429AF37FF0D66
SHA-512:	51AFFB5A8CFD2F93B473007F6987B19A0A1A0FB970DDD59EF45BD77A355D82ABBBD60468837A09823496411E797F05B1F962AE93C725ED4C00D514BA40269D1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js
Preview:	/*. Copyright (C) Federico Zivolo 2017. Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT).. */(function(e,t){'object'==typeof exports&&'undefined'!=typeof module?module.exports=t():'function'==typeof define&&define.amd?define(t):e.Popper=t()})(this,function(){'use strict';function e(e){return e&&'[object Function]'==={}.toString.call(e)}function t(e,t){if(1!==e.nodeType)return[];var o=getComputedStyle(e,null);return t?o[t]:o}function o(e){return'HTML'===e.nodeName?e:e.parentNode||e.host}function n(e){if(!e)return document.body;switch(e.nodeName){case'HTML':case'BODY':return e.ownerDocument.body;case'#document':return e.body;}var i=t(e),r=i.overflow,p=i.overflowX,s=i.overflowY;return /(auto|scroll)/.test(r+s+p)?e:n(o(e))}function r(e){var o=e&&e.offsetParent,i=o&&o.nodeName;return i&&'BODY'!==i&&'HTML'!==i?-1!==['TD','TABLE'].indexOf(o.nodeName)&&'static'===t(o,'position')?r(o):o:e?e.ownerDocument.documentElement:document.documentElement}functio

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):	4.957104463731007
Encrypted:	false
SSDEEP:	768:/8y3EDlwZ9bY/MKOIoLmsLa87WlIWJal0J4WWn1l8T7jqfVjDrXPIXewPoRhxfHq:/8y3EY0
MD5:	FF1E04DED681AEAC3DE29C4D2419FE91
SHA1:	C2147C7C50FB6DF21E5ECF323309AE67F6BCA247
SHA-256:	2B7F2F5C6DEE2661AFF7FA717D759C8B63328A9F3EA83556A51B64628EFBC9F7
SHA-512:	8B10CA490CE49752530938936E778BB570017999C97E2156CBC07EBABBC4ACECA0E8BCC9C22D003155A14AD0E6E7B62DDD4C8799E157A902101A321FB5F58B2
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\privacy-localnav[1].css	
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 v0.49.0 built on Mon, 26 Apr 2021 07:16:01 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\privacy[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	83728
Entropy (8bit):	4.553963224742428
Encrypted:	false
SSDEEP:	384:a47VFWtdTial6cMANPnaLjReghz8lti0iLeUkUG6GHvYSECFR:aG7W/l6cjneRPz8lfeeUkFDvRECL
MD5:	555025238A60E5E78AFC041794BE982A
SHA1:	B2840842C679D0E2B7EBBCE8C8FAFC25E5506D11
SHA-256:	563C795F57ABD84045A5C2DF335E957596DAE5D362A12D83200E5DFABFB466BE
SHA-512:	6E7A3C457BF4A3BE3C00006C984BEA13CA3ED7DA477076BF9437411A87893D5B41459F82576B05BE5226CAB31A72FBD2AF6E53A5A59FD597BECA55B619D13E(2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/privacy.html
Preview:	.<!DOCTYPE HTML>.<html class="spectrum--medium" lang="en">. <head>. <title>Adobe Privacy Center</title>. <link rel="canonical" href="https://www.adobe.com/privacy.html"/>. .. . . . <link rel="alternate" hreflang="en-IE" href="https://www.adobe.com/ie/privacy.html"/>. . <link rel="alternate" hreflang="de" href="https://www.adobe.com/de/privacy.html"/>. . <link rel="alternate" hreflang="uk-UA" href="https://www.adobe.com/ua/privacy.html"/>. . <link rel="alternate" hreflang="ar-kw" href="https://www.adobe.com/mena_ar/privacy.html"/>. . <link rel="alternate" hreflang="en-us" href="https://www.adobe.com/privacy.html"/>. . <link rel="alternate" hreflang="lv-LV" href="https://www.adobe.com/lv/privacy.html"/>. . <link rel="alternate" hreflang="en-IL" href="https://www.adobe.com/il_en/privacy.html"/>. . <link rel="alternate" hrefla

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\publish.combined.fp-da9e7448205ee1bd3bef6f58dcdfba34[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	644431
Entropy (8bit):	5.272633337277513
Encrypted:	false
SSDEEP:	6144:GyojsveUZPvp2nrz3eLxtQtD3akxcZIVg:7eUZPvp2nrz3eLxtQtD3akAIVg
MD5:	DA9E7448205EE1BD3BEF6F58DCDFBA34
SHA1:	A1785DEE94C5DA9B8E50F8D86176F770BC5526FC
SHA-256:	8C4A41FDE910BBBA3704F752FA0500CC7D0DE79BE164444ACCCF0DD3B383E018
SHA-512:	AEEE94491C6FE37638B4081E2C67FA9D0903FF2DBA401635F48C5AD0AF915C4A020C4A89D0CDDCA705C5995790785DF93EF381FCAF5C8C501A1E9614F06307
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/etc.hawks.dexterlibs/hawks/clientlibs/publish.combined.fp-da9e7448205ee1bd3bef6f58dcdfba34.css
Preview:	/* The OOTB AEM 6.4 grid system.. *. * This has been modified slightly to support Dexter's. * custom breakpoints and remove fixed left / right padding.. */./*. * ADOBE CONFIDENTIAL. *. * Copyright 2015 Adobe Systems Incorporated. * All Rights Reserved.. *. * NOTICE: All information contained herein is, and remains. * the property of Adobe Systems Incorporated and its suppliers,. * if any. The intellectual and technical concepts contained. * herein are proprietary to Adobe Systems Incorporated and its. * suppliers and may be covered by U.S. and Foreign Patents,. * patents in process, and are protected by trade secret or copyright law.. * Dissemination of this information or reproduction of this material. * is strictly forbidden unless prior written permission is obtained. * from Adobe Systems Incorporated.. */./* grid component */..aem-Grid {. display: block;. width: 100%;.}..aem-Grid::before,..aem-Grid::after {. display: table;. content: " ";.}..aem-Grid::after {. clear: both;.}

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\rbi5aua[1].js	
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/00000000000000000000158d3. * - http://typekit.com/eulas/00000000000000000000158d4. * - http://typekit.com/eulas/00000000000000000000017709. * - http://typekit.com/eulas/00000000000000000000158d6. * - http://typekit.com/eulas/00000000000000000000158d7. * - http://typekit.com/eulas/00000000000000000000158d8. * - http://typekit.com/eulas/00000000000000000000158d9. * - http://typekit.com/eulas/00000000000000000000001705b. * 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:	dropped
Size (bytes):	36506
Entropy (8bit):	5.029205555305148
Encrypted:	false
SSDEEP:	384:U1qVZSpe137a6wbqWcqS5G399ah4qAUaww3boPOGGuh3f3ntOX4jQt41gvUxUPC4:UMZPjwfu/P0GLB1a4j/b/g
MD5:	E5F73B6BBF9D9D595A96BD6B2796C166
SHA1:	DFCB2DC87755FDD7C3DB7CA23EFC5697A57735FB
SHA-256:	6775C076C387B1E65CE0419958CF2A79B6886FB2B42BA82BDA261D4886725945
SHA-512:	79450647E86DFDE4BF8B723CC133AA7A48DE901BD9A1927DCB2B26383D544789D42F39860106462B8319EA33262D1BF0A3A6034CDD4E85B04B279ABFF99FA7F
Malicious:	false
Reputation:	low
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, Image */* 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(n

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\scripts[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text
Category:	dropped
Size (bytes):	36506
Entropy (8bit):	5.029205555305148
Encrypted:	false
SSDEEP:	384:U1qVZSpe137a6wbqWcqS5G399ah4qAUaww3boPOGGuh3f3ntOX4jQt41gvUxUPC4:UMZPjwfu/P0GLB1a4j/b/g
MD5:	E5F73B6BBF9D9D595A96BD6B2796C166
SHA1:	DFCB2DC87755FDD7C3DB7CA23EFC5697A57735FB
SHA-256:	6775C076C387B1E65CE0419958CF2A79B6886FB2B42BA82BDA261D4886725945
SHA-512:	79450647E86DFDE4BF8B723CC133AA7A48DE901BD9A1927DCB2B26383D544789D42F39860106462B8319EA33262D1BF0A3A6034CDD4E85B04B279ABFF99FA7F
Malicious:	false
Reputation:	low
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, Image */* 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(n

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\spark[1].svg	
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\styles[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	12401
Entropy (8bit):	4.662952324891605
Encrypted:	false
SSDEEP:	192:wh2WV+m6jCZDitH75vH1V/FAF/1Sr+aGF5OJE9h0TA9ZXn:R5171PFAF95bFQ9cXn
MD5:	C0F349AF62FA2D1E725464B22D31CDCC
SHA1:	645A7814C3FBE9578EBFDEFF1327720E6AA322EF
SHA-256:	32BB5493F1B51E6AE09315DB807602AAE9031356D170780D32D272098424FA74
SHA-512:	B2D2DBCABABAB7233DDB89D029F3DE350D040872B119C447740C1DB862FF5B3DE2BBAFA5D369CB93C88A8CD0CCC440D53CA5EDB31AFB86BF78868989E262CE0
Malicious:	false
Reputation:	low
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(/express/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\styles[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	12401
Entropy (8bit):	4.662952324891605
Encrypted:	false
SSDEEP:	192:wh2WV+m6jCZDitH75vH1V/FAF/1Sr+aGF5OJE9h0TA9ZXn:R5171PFAF95bFQ9cXn
MD5:	C0F349AF62FA2D1E725464B22D31CDCC
SHA1:	645A7814C3FBE9578EBFDEFF1327720E6AA322EF
SHA-256:	32BB5493F1B51E6AE09315DB807602AAE9031356D170780D32D272098424FA74
SHA-512:	B2D2DBCABABAB7233DDB89D029F3DE350D040872B119C447740C1DB862FF5B3DE2BBAFA5D369CB93C88A8CD0CCC440D53CA5EDB31AFB86BF78868989E262CE0
Malicious:	false
Reputation:	low
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(/express/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\themetwo.fp-abc573155522bcda0452e193dff7aa91[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):	301880
Entropy (8bit):	4.99900233389085
Encrypted:	false
SSDEEP:	384:LreqQVUz4G0X5AgD6zicPvT67qm032cRHO9y/SbOD6mCroWKa8E8UoGofHo+zwci:OzW6xPcgy/N6FroFrf+Lq7TnuWy19
MD5:	ABC573155522BCDA0452E193DFF7AA91
SHA1:	EDB2799FBA37BF41FE9C2DC898D4C0650A10DB14
SHA-256:	8602171F79058FCB3DBFA67B3DC823C3C49838E89A7D195FE9B1D7D350ABD6F7
SHA-512:	1A265935DE18CE88EB0F281C284264F530F7ACDDBABF4FC53E1DD4A1D0FC41660F68450E3B5D89DEF2B4EC56D4671695B2960C99AAB89D3F297541229AF29F5D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\themetwo.fp-abc573155522bcda0452e193dff7aa91[1].css	
IE Cache URL:	http://https://www.adobe.com/etc.hawks.dexterlibs/dexter/clientlibs/base/themetwo.fp-abc573155522bcda0452e193dff7aa91.css
Preview:	.spectrum-Icon{display:inline-block;color:inherit;fill:currentColor}.spectrum-Icon.is-animated{transition:color .15s ease-in-out,fill .15s ease-in-out}.spectrum-Icon--sizeXXS,.spectrum-Icon--sizeXXS img,.spectrum-Icon--sizeXXS svg{height:.5625rem;width:.5625rem}.spectrum-Icon--sizeXS,.spectrum-Icon--sizeXS img,.spectrum-Icon--sizeXS svg{height:.75rem;width:.75rem}.spectrum-Icon--sizeS,.spectrum-Icon--sizeS img,.spectrum-Icon--sizeS svg{height:1.125rem;width:1.125rem}.spectrum-Icon--sizeM,.spectrum-Icon--sizeM img,.spectrum-Icon--sizeM svg{height:1.5rem;width:1.5rem}.spectrum-Icon--sizeL,.spectrum-Icon--sizeL img,.spectrum-Icon--sizeL svg{height:2.25rem;width:2.25rem}.spectrum-Icon--sizeXL,.spectrum-Icon--sizeXL img,.spectrum-Icon--sizeXL svg{height:3rem;width:3rem}.spectrum-Icon--sizeXXL,.spectrum-Icon--sizeXXL img,.spectrum-Icon--sizeXXL svg{height:4.5rem;width:4.5rem}.spectrum-Icon,.spectrum-UIIcon{display:inline-block;color:inherit;fill:currentColor;pointer-events:none}.spectrum-Ico

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/products/eulas/tou_typekit. For font license. * information, see the list below.. *. * adobe-clean:. * - http://typekit.com/eulas/00000000000000000017701. * - http://typekit.com/eulas/00000000000000000017703. * - http://typekit.com/eulas/000000000000000000176ff. * - http://typekit.com/eulas/00000000000000000017706. * brandon-grotesque:. * - http://typekit.com/eulas/0000000000000000132df. * - http://typekit.com/eulas/0000000000000000132e3. * - http://typekit.com/eulas/0000000000000000132e1. *. * . 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\43b32711-4358-470b-a423-45db1a503c8d[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1024 x 922, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	120966
Entropy (8bit):	7.926493387812747
Encrypted:	false
SSDEEP:	3072:0ixbulc2qQVg7bzegOIrRftYaXlezBf62Qc:nWnVg7bzBRfGa1e42Qc
MD5:	8F1B330BF0488D06922951A0A5DD563C
SHA1:	6E6D145E3E6C4F8CCAB1D640D2542C1C6B01DB9D
SHA-256:	07206E3D4C933E24DB34C4E5E3F60D244D8951ED6C453FFC59D826E9DF861703
SHA-512:	44FC4CE206DF9E6ABE3CB5355C5A1529AA3A78D3937AE2C3737E267E88C005CD2BBC12074D0D0E716BCEBB0E50B049C000B2CD5432ED5AA1682D865E02EA5 B3F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spark.adobe.com/page/ntKiaikxRt9X0/images/43b32711-4358-470b-a423-45db1a503c8d.png?asset_id=34959966-dbbb-477c-83fe-a6a5002ee5e3&img_etag=%228d0c972e0adb28a066d197ef29ded4c8%22&size=1024
Preview:	.PNG.....IHDR.....G (....iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?>.<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 6.0-c005 79.164590, 2020/12/09-11:57:44 ">. <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/">. <xmpMM:DerivedFrom rdf:parseType="Resource"/>. </rdf:Description>. </rdf:RDF>.</x:xmpmeta>.<?xpacket end="r"?>m..".. .IDATx.....]'.....*-.e.l...c.E*.%..2.iNw..L3.2M.....6.0...;.i ..C:s .=.i.@.$.X%).v.'..*[.-..z...w.....UI*.c[.J.O..JR.^.....J..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\4bab7ca0-86ec-4407-a0cc-bdcd0798615b[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 900x550, frames 3
Category:	downloaded
Size (bytes):	88390
Entropy (8bit):	7.900448166729876
Encrypted:	false
SSDEEP:	1536:biNAOw9fXYQv8WbOhsSZzY0M+2UcFLrgpohL4vDZkwQ4kBC/uC:biNkzvnYZzY0M+CacL8Dbkg
MD5:	D99D9F15AE2582EFE209F3F64B23EC93
SHA1:	32AEAF68B17FEECE6B3B159B718282F80FEA4D69
SHA-256:	F7F25CBA15580BA1FD09904CCF4B6DE0446EF4C6931B66B9DC6E497D8FDE7F5A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\4bab7ca0-86ec-4407-a0cc-bdcd0798615b[1].jpg	
SHA-512:	8608A1B871B6551C27C4D1EA9CF6A7727CD07FE4C1A2AA3A767B03FEE4376D51F73C8AB260D786996026A88249FAEA1A95C859CAA862BFAF014EED1A2DEB46CC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spark.adobe.com/page/ntKiaikxRt9X0/images/4bab7ca0-86ec-4407-a0cc-bdcd0798615b.jpg?asset_id=c2b8e15b-b804-4e00-8532-1690a3652f5c&img_etag=%22965ca3fc5582348df483e26bdb9f2fef%22&size=1024
Preview:	......Exif..II*.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 6.0-c005 79.164590, 2020/12/09-11:57:44 "> <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#"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:76F1769CC93F11E69032ADB3F30E3F21" stRef:documentID="xmp.did:76F1769DC93F11E69032ADB3F30E3F21" stRef:originalDocumentID="xmp.did:76F1769DC93F11E69032ADB3F30E3F21"/> </rdf:Description> </rdf:RDF> </x:xmpmeta>

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:	48:97gzdbklTMl1sy6TMenl7ulGt/3GmjAAp:970sI2NmU3GY
MD5:	B28BF60DD7E50B6DFFD394EBC0F9057A
SHA1:	9EA7EED87B689757780322989EF426AEFFDC8F7A
SHA-256:	BF24C9E4D37F94D4BD2F870228FF421CA54B2949DB3391DBD3818EC0E6DB0F5F
SHA-512:	B16A7F756E38FFE4BBCC0394A6E41593CC9FE68AACA6350C1C20D10E7A284EBFC7937C15726D0F43A3ABD7C43D128A041A109CAC2C8F240707FE1997E633E05
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/content/dam/cc/Adobe_favicon.ico
Preview:	......00.... ..%.....(...0...`..... .....$..... ....A.....V.....'..... .....A.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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:	2DD8E040B9046322F4259ABC673BB1CD980E440FE0D1EE5BFD6FD6FFC14D36F810BB0222E1413ECF65A49C335F894923C365F0E7E6C0BB6DC69A4A3DBF05E46
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: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:8005f268-2f6e-41f7-b266-aa21258a942f" xmpMM:DocumentID="xmp.did:1DF2B77A0FFC11E6838996FD381AB7D0" xmpMM:InstanceID="xmp.iid:1DF2B7790FFC11E6838996FD381AB7D0" xmp:CreatorTool="Adobe Photoshop CC 2015 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="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.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\RC5e5d1b9fe0a942c38190dc2199529941-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):	5.270202121282541
Encrypted:	false
SSDEEP:	48:15MgsregiQhdsitymtCZv4j+YuteKhXSXNjTjOofbOK5b/q:1OgsrPld3tymtCpLYuteMXSXNjTjhT5q
MD5:	BC6C1B5E9A133E66815BA6F581BA25AA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\RC5e5d1b9fe0a942c38190dc2199529941-file.min[1].js	
SHA1:	9E98D1F4C3A43D08F32B0F662D7D201981ADEB53
SHA-256:	BBC2D76BAB34C7DB65F9BDBF954A5588C5064A4EFD52E56B2A8622F98240773F
SHA-512:	1A5043A3FB805DA4819572804190C76BE2364EFA3034FB2F9CFC9B7FF34823CD44ACC93F0986BFB98685287F3F3AFE54316784763588FC243B43CFE67927D64E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC5e5d1b9fe0a942c38190dc2199529941-file.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC5e5d1b9fe0a942c38190dc2199529941-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\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):	5.160871230790997
Encrypted:	false
SSDEEP:	24:15M2cSMueyrpjBKe4lllldllALxTb0aVM/:15Ms6ytdKe4lllldllABwaG/
MD5:	E3D2EAC3C1FFAFF2F21E442201AAE3F9
SHA1:	4B00AA68E25BA1A64C552996773585CD5CDF978A
SHA-256:	F4919AE5BCD1BADD605DEC5CD9171A751564905E6640E55CBDA4F6323E2B97B8
SHA-512:	D090B5A45C54844A857D8DC1A52BF6CB21D2219A3CC368FA46F701C7C140F85E0B1A213477D2C4884A9F86430BB39E04343B589D1971D990989DDEEF7E590D7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC89c6d3bd15f043db95a5a0a4b5cc9da0-file.min.js
Preview:	// For license information, see `https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/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(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\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\MEEXW4H4\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\adobe-spark[1].png	
SHA1:	11A708485B7942104D06F2FFD0F1B6713F25F941
SHA-256:	C91BD804CF36B68D89EAE5FAC4CD8F985563D322273462AF92607AB9927002F1
SHA-512:	2C26049C9A7CDCD17F75DCFB70502D28E397E27F296F5267C6478B2D4F4D263D7584AD772ED3E1C12C7FC42110260B0DCF41694DE881260B92D3E615D9BED8
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...+...;.....#.....sRGB.....8eXIfMM.*.....i.....+.....;.....D.....IDATx.._.$.].....q...H,.v,L...E!.P..R.@7'....}. ..R....3.....1.hg.P..CBA...EB. .P..'6!.>..uO....gfwgv.._..W..V...k.....s..../8...<..,.].....w.y.....9.7KaX4""..X....I..s....p.N..\....?8..+gy48"...!0.pT...W`.dNr5...8.WV..huD "..8rV,..,.....".....U.MD.|!.8._p.....:...Y...s. {.....:E.....,}....=..J..Gn..s/....u...U.....8.og...z..u...q...#....@."..k.a..VR.._K.....Y...i.|.e.~.4.eF."..#.=..._.jh`.].[#E.".+..E...W..Lffu....."E."....~!....:g.....7".L.$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.....I.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\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\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\MEEXW4H4\d[1]	
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:	E741918EF1EC6A3C0B87D996245945AEA9DB8C7D798352756F409A5E519BBF89EBF8F6AFA1E1A71D5C24C4E1C364F7C2EF38622C0897F852C6E9C7E6C27BBE9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/1da05b/00000000000000000000132df/27/d?primer=7a5a436c948772f5260024dfadc8f7cd849e1448f8bf41ba74a247e8e46f3aee&fvd=n4&v=3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\d[1]	
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$..I..$!.MJr.;).d...I... .MI....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..I.....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\MEEXW4H4\d[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 25284, version 0.0
Category:	downloaded
Size (bytes):	25284
Entropy (8bit):	7.98201537948979
Encrypted:	false
SSDEEP:	384:XVkwjUeZrzDGdbpwvwrcsOGkps3SNPnvNFbwW8yTqXCrfenp/W0BEpFc2N8F2cp:lkaOdbSo4zAYfV3jfE5Bfh2cp
MD5:	3A472B1A078B7B653C744CC55FAA5219
SHA1:	E9949514223E35D4A1E0515A312EC3664DEFDF33
SHA-256:	8812CEB05FB855A78850BB1907BC621FC487CD6D54760AC8D821D760D3BBB9E3
SHA-512:	DA09A18AED6A3C44F5009410D03623A8200ABF224AF33DDBFE34D3736AF96C6847D7A9A1CF0D94839C9ABB9546E1C7F5BCF6C305132B97BEFBD84A535F1399A 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/8f4e31/00000000000000000000132e3/27/d?primer=7a5a436c948772f5260024dfadc8f7cd849e1448f8bf41ba74a247e8e46f3aee&fvd=n7&v=3
Preview:	wOFF.....b.....DYNA...X.....$..GDYN.....h;.GPOS.....l.m2EBOS/2.....[...`}7P.VDMX.....l.tPcmap..a.....l.`pcvt ...H... ... ...Kfpgm...h.....s.Y .7gasp...l.....glyf..'D..5o..d.lN..head...t...4...6.Rl.hhea.....$....hmtx..\....!...8....loca..^.....k..maxp...8... ... ...cname.....~p.[post..`x.....F..Jprep...d...U...z.. .%x...S.X..D.s.X...Vc....jl5....m.m{:...3.....#..C.P..WB..!..K8}...'.>...6".l$"....b....F4}$*.m4b...ic...$....866q..8.q.o.@o.OB..DzCB..D$..I..$!.MJr.;).d...I... .MI....zAj..4..s... #.MO&=#..mF..)..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...ml{..:..t.....mK...:C{...t.i:..v...L/....mW..n..I.....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\MEEXW4H4\d[3]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, CFF, length 23416, version 0.0
Category:	downloaded
Size (bytes):	23416
Entropy (8bit):	7.983586847834522
Encrypted:	false
SSDEEP:	384:F30DDcDU1FW+RedG9b7Tm16n2XMc3nS3YUQIfiRgeQvYAb0HsRUgBnQc:JOA+Redq61GYU7f/eQvnUgBQc
MD5:	334521D5C314F6265FCA189A2114006F
SHA1:	F35719EE30117ADF919939AD46A98C9D3C6EEE45
SHA-256:	B4D011E6CF7EBE571E4D0C9868CD972592987E13D5BE3DDBB69C67638323A237
SHA-512:	3F6163488D3814E3CEFF964DBA451B45DE22236EED0372A82BC713950CBD0FCC41D4553414095646842B2839F12EF7A95AC943329AC0293FCC9850ECEF6C67C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/d8f71f/00000000000000000000132e1/27/d?primer=7a5a436c948772f5260024dfadc8f7cd849e1448f8bf41ba74a247e8e46f3aee&fvd=n5&v=3
Preview:	wOFFOTTO..[x.....CFF .....6V..A.....DYNA..:.....AOr.GDYN..:.....E(.GPOS..;x.....G ....OS/2...$...[...`}.N.cmap..Z4...C....M.?gasp...0.....head... 8...2...6...khhea.....$....hmtx..X.....|k .maxp.....P.name...l.....<.bpost..Z ..... ...2.....x.c`d``.b....x~...../."..]....ka.g..r...@..k.....x...j.@.....U.e..4rV...p6..h..u.Ed I.....Q....D.}.>@w=....E[]....;sg.....{.=.8a.s.!>x>...=....=..._<.q...GH.`...'...@.....o.....|.w....Q8.<.<ln.zk.....XM..T....X..Ju[..H....P..*#V.F.....F.%.uo..S.'L....U_.Q..9. u.i....W....8v.Z.r.-.u,M1.....$.A..[..Xb...3,x1..h.%iN...f(...lCg...i.-.q...C..i.....b.+M.WT..g4...;m.l...T.evv..ew')..._!}.....2..m..}..v...:....M.....]....:V\....-Y.S$.`...7.....x.c`b|..... ..i.S...C..f..`...(.....A?.A!...<.\.....1.....0.$.8.i..R``..1....x.c`d``..W.$.....d.g.....P.....x.{.X.W.....3.1.C`.1..I.5.....AQA.....e..4.(....Q@l.F.1

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, 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:	0E2ABD3D074418386C6290B0AA5EA09BB8BDC486C715EC426CE1F0D6B48C3EC2EC85EDA7BAAF31375B3481FDCE1DE7886AC0325AA7877F48516D0877F7C06A 1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\d[4]	
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..._.??.#..@.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\MEEXW4H4\d[5]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, CFF, length 46088, version 0.0
Category:	downloaded
Size (bytes):	46088
Entropy (8bit):	**7.991344892853239**
Encrypted:	**true**
SSDEEP:	768:cbb1bWj8ZMc7qG0jmQcHDJINQubS5HF9GctB7jiDbtUPL6n9MRXVFtf8u:qb108ngj4tImubIpHWHyWn9MZVfL
MD5:	F6772D5F038A33A09B062FA7D7FD1E73
SHA1:	19295E0771CD244E3C71F7D2D209B9A7309A8DE0
SHA-256:	AF6B2610431D075E5266E7D97EF7B53314F04EC64A56CD8872AD5FFB85DBA88D
SHA-512:	64179523C0D4EFAA89AA10670CB89D91D7B97C9685E5919E7E1D014602634AD98FCA376A8433A9C31B13F0E3AF944EC330A858486F58DA726EA953117FA3575C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/a0c22f/00000000000000003b9b3f84/27/d?primer=388f68b35a7cbf1ee3543172445c23e26935269fadd3b392a13ac7b2903677eb&fvd=i3&v=3
Preview:	wOFFOTTO.....BASE...D...F...Fe(}.CFF ...@.....{}.R.DYNA...H.....|.6IIGDYN.....v.A.GPOS.....0P.3.(GSUB.....t.OS/2.....[...`[.twcmap... (.....(..TIhead.....4...6..%<hhea.....$...$...^hmtx.....:.".maxp...8.....kP.name.....post..... ...2.....ideoromn..DFLT..cyrl..grek..latn.....`.....x.c` d```5.J.S,.....(.p>9..F.....|.....2...x.R.n.@...i%$T.O...];v.&.)i..T.*.z..Mc.?..F....x.>.wn..O.....Z!.j...73..g.x..p.>'.-v...8.[.....,...}.....7.....K'...S..{x.|..C.w..Q....x.j.....D..=1\ ....].U^.I1/.MY.Z-..f...7+]...U.e..e*..E...8K....`x>.....,.....ZUuZ...^.D }...J=/...J_...<^.R/e.&..d.....VZoN=O.6j.j9/sO.fq....0.'.w.;...9zDC,P".".a...8.*0...3[ac..- .....".V..f..*r..y....E....n.. 3..VDE.. ..s.06.....-..(.]....4..u...C...gdE.6.(x/A^....Cfs....p..67I.>2.o\.....Sx.._cC..M..~..-.b..'...Y....d=....[..x.c`f.....7.f.b.c0b...r333..p2.(00.300

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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):	236125
Entropy (8bit):	5.241839181610481
Encrypted:	false
SSDEEP:	1536:O9BCW6xUvmbH4bWdCQx23klSzbZYVlH3ShC2ZmwQZMLrgizZrZixqwTUQxcsVFoQ:UBCZCaHDzbSmKwQZ2k4kTRCTHSE1Q7B
MD5:	64260D8365E59085E6E91E554487EB6D
SHA1:	83272011769DF702916D6DA5875591138F616BDF
SHA-256:	194D4EA20F2C9834477F36A1A9C307F86C1E833C79420637C3CC42A17CAF1870
SHA-512:	307714B2FF3785F3E5C77C57CE55E55216EA32B7A366436A04D2D8B5F2B151E70E4242989311D170FA95757BF70130E56E42427A9F508557473ACE999BED826D
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","pccloseButtonType":"Icon","pccontinueWithoutAcceptText":"Continue without Accepting","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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\express[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	5302
Entropy (8bit):	5.328235397347705
Encrypted:	false
SSDEEP:	96:386R0lH1UHaxH1UPCR0m+ydgW3+y6aSH1UPr+ymTimrY4WjlGTLzmYaq/XYXg0e+:38s0lSaxQU0vydSy6aSQCymJpU/XYXHz
MD5:	5B7E7A2213112ADE773AA8296E5E987B
SHA1:	B02C2F41C0D16C0C65D34270B81AEC8F403DA2AC
SHA-256:	133E04A154DD5436F01589F0CAF9D504866C2EC46E719B15D4244D49629CF375
SHA-512:	C219688EDBD4C2C62B0A302F957A090F1263A407787D5D40390A9D4B6664CB359FC46FE3DCE2DC3EC0044AEDD715B0FCF461CB5812248E3B203F3A4FB6CCBE 3
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\express[1].htm	
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/?r=reader_page_logo
Preview:	<!DOCTYPE html><html>..<head>. <title>Make Social Graphics, Short Videos, and Web Pages To Stand Out.In Minutes | Adobe Spark</title>. <meta name="x-source-hash" content="TQd2yn6COm8CsXKP">. <link rel="canonical" href="https://www.adobe.com/express/">. <meta name="description" content="Adobe Spark is an online and mobile design app. Easily create stunning social graphics, short videos, and web pages that make you stand out on social and beyond.">. . <meta property="og:title" content="Make Social Graphics, Short Videos, and Web Pages To Stand Out.In Minutes | Adobe Spark">. <meta property="og:description" content="Adobe Spark is an online and mobile design app. Easily create stunning social graphics, short videos, and web pages that make you stand out on social and beyond.">. <meta property="og:url" content="https://www.adobe.com/express/">. <meta property="og:image" content="https://www.adobe.com/express/media_1414f90572f278eae7d49cf2222e9b7d0063180cd.png?width=1200&fo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\feds[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	19028
Entropy (8bit):	5.097989623681208
Encrypted:	false
SSDEEP:	384:J08heJDYD+yQUAP/92Z6Rs/AQpol4+69503RYUSs8Ukz+OsUIKn:GpSkhKbolDPu
MD5:	99ECB54FB6A6DBD6653F70898951851E
SHA1:	A1F286ABDB35080A60DC4824A24B4E7963AC1EEF
SHA-256:	F727B62A08FCEC8F20CF51B322ED7A005950499041128A02AF0EC1FC89B5CDD2
SHA-512:	0D70A24FFE03A6B7006CE249916E74DABE188BA555ABECFAFD8847FBD5146B614D022B385FC1888EB11CD55F759CD59FD6FD4B09C552D912FB8740F95D8031I4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/etc.clientlibs/globalnav/clientlibs/base/feds.css
Preview:	/*! feds v0.49.0 built on Mon, 26 Apr 2021 07:16:01 GMT */.[class*=aem-AuthorLayer] #feds-subnav{position:relative}.Subnav-wrapper li{margin:0}#AdobeSecondaryNav{max-width:100vw}#AdobeSecondaryNav.Subnav-wrapper{position:absolute;top:100%;right:0;left:0;min-height:60px;display:flex;justify-content:center;font-family:inherit;box-sizing:border-box;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale;transition:height .3s ease;z-index:1;opacity:0;transform:translateZ(0);overflow:hidden}#AdobeSecondaryNav.Subnav-wrapper--active{opacity:1;overflow:visible}#AdobeSecondaryNav.Subnav-wrapper *,#AdobeSecondaryNav.Subnav-wrapper :after,#AdobeSecondaryNav.Subnav-wrapper :before{box-sizing:border-box}.feds-header--rebranding #AdobeSecondaryNav.Subnav-wrapper{font-family:inherit}#AdobeSecondaryNav.Subnav-wrapper .Subnav-background{position:absolute;top:0;right:0;bottom:0;left:0;width:100%;height:100%;background-color:#f8f8f8;content:"";transition:opacity .3s ease;pointer-events:none

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:dP6hT1bIl4w0QUmQ10PwKLaAu5CwWavpHo4O6wgLPbJVR8XD7mycP: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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\home_icon[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	613
Entropy (8bit):	4.901403032351247
Encrypted:	false
SSDEEP:	12:t4no14t1A1dJKAvun7ZXgfaVFSdaVH3/YNVZuVAi:t4o14H0JK+un7ZXBG+P+uV
MD5:	14D743AA528E862BF7A99EBA969E7351
SHA1:	66591159910367AD593D53E73EEE1695DF0130DC
SHA-256:	4B47714B6C773114CA2087F17046FE060695BB58F39E7EDE01B94CB8BF2CB338

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\home_icon[1].svg	
SHA-512:	827EA6D9D9D93A4012065D61C562DCBD08865ABA1B260E188D5B4FF91865CB66BD0C05D81205AA1064F5C7B5C3A4302ED1F4154C3AD1075D1D4F4569980C492
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/content/dam/cc/icons/home_icon.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" height="18" viewBox="0 0 18 18" width="18">. <defs>. <style>. .a {. fill: #6E6E6E;. }. </style>. </defs>. <title>S Home 18 N</title>. <rect id="Canvas" fill="#ff13dc" opacity="0" width="18" height="18" /><path class="a" d="M17.666,10.125,9.375,1.834a.53151.53151,0,0,0-.75,0L.334,10.125a.53051.53051,0,0,0,0,.75l.979.9785A.5.5,0,0,0,1.6665,12H2v4.5a.5.5,0,0,0,.5.5h4a.5.5,0,0,0,.5-.5v-5a.5.5,0,0,1,.5-.5h3a.5.5,0,0,1,.5.5v5a.5.5,0,0,0,.5.5h4a.5.5,0,0,0,.5-.5V12h.3335a.5.5,0,0,0,.3535-.1465l.979-.9785A.53051.53051,0,0,0,17.666,10.125Z" />.</svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\httpErrorPagesScripts[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):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\icon-footer-twitter[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	764
Entropy (8bit):	4.2898721619383515
Encrypted:	false
SSDEEP:	12:tvveD/lIhNZHvr3t8bYDnNAxLgeZLU9YtxYMPWzG4BsVrvl5JiqC8n:tXeD/epp8QnNCLgQbbJMG4er1iqC8n
MD5:	41324C2374C498667DF60F5DB9ED29BC
SHA1:	E1D68AD0BCB242CC76D34A7D71C78ACFF9F25EFC
SHA-256:	1C48D8EDF7F69BC479F00DD25EB2399DD2BF6F0AA3BF128089B0A7A1D8958D5E
SHA-512:	851F947CEC590D196CFA1FD2390D4D380FB0E4F008B0813CC0A15CD1CBFEAF94883ECE65EEBEFA5C98B91E7F77EED99F213D601C49FA972B403DE9181414A955
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spark.adobe.com/images/icon-footer-twitter.svg
Preview:	<svg id="Layer_1" xmlns="http://www.w3.org/2000/svg" width="67" height="67" viewBox="0 0 67 67"><style>.st0{fill:#717f8a}</style><path class="st0" d="M38.2 22.3c-2.6 1-4.3 3.4-4.1 6.1l.1 1-1-.1c-3.8-.5-7.1-2.1-10-4.9L21.7 23l-.4 1c-.8 2.3-.3 4.7 1.3 6.3.8.9.6 1-.8.5-.5-.2-.9-.3-1-.2-.1.1.4 2.1.8 2.8.5 1.1 1.7 2.1 2.9 2.7l1 .5h-1.2c-1.2 0-1.2 0-1.1.5.4 1.4 2.1 2.8 3.9 3.5l1.3.4-1.1.7c-1.7 1-3.6 1.5-5.6 1.6-.9 0-1.7.1-1.7.2 0 .2 2.6 1.4 4 1.9 4.5 1.4 9.8.8 13.7-1.6 2.8-1.7 5.7-5 7-8.2.7-1.7 1.4-4.9 1.4-6.4 0-1 .1-1.1 1.2-2.3.7-.7 1.3-1.4 1.5-1.6.2-.4.2-.4.-.9 0-1.8.6-2 .6-1.2-.4.6-.7 1.4-1.9 1.4-2.3 0-.1-.3 0-.7.2-.4.2-1.2.5-1.8.7l-1.1.4-1-.7c-.6-.4-1.4-.8-1.8-.9-.9-.4-2.6-.4-3.5 0zM34 64C17.4 64 4 50.6 4 34S17.4 4 34 4s30 13.4 30 30-13.4 30-30 30z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jquery-3.1.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	86709
Entropy (8bit):	5.367391365596119
Encrypted:	false
SSDEEP:	1536:9NhEyjjTikEJO4edXXe9J578go6MWXqcVhrLyB4Lw13sh2bzrl1+iuH7U3gBORDT:jxcq0hrLZwpsYbmzORDU8Cu5
MD5:	E071ABDA8FE61194711CFC2AB99FE104
SHA1:	F647A6D37DC4CA055CED3CF64BBC1F490070ACBA
SHA-256:	85556761A8800D14CED8FCD41A6B8B26BF012D44A318866C0D81A62092EFD9BF
SHA-512:	53A2B560B20551672FBB0E6E72632D4FD1C7E2DD2ECF7337EBAAAB179CB8BE7C87E9D803CE7765706BC7FCBCF993C34587CD1237DE5A279AEA19911D69067E65

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jquery-3.1.1.min[1].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-3.1.1.min.js
Preview:	/*! jQuery v3.1.1 | (c) jQuery Foundation | jquery.org/license */!function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.1.1",r=function(a,b){return new r.fn.init(a,b)},s=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,t=/^-ms-/,u=/-([a-z])/g,v=function(a,b){return b.toUpperCase()};r.fn=r.prototype={jquery:q,constructor:r,length:0,toArray:function(){return f.call(this)},get:function(a){return null==a?f.call(this):a<0?this[a+this.length]:this[a]},pushStack:function(a){var b=r.merge(this.con

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jquery-3.2.1.slim.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	69597
Entropy (8bit):	5.369216080582935
Encrypted:	false
SSDEEP:	1536:qNhEyjjTikEJO4edXXe9J578go6MWX2xkjVe4c4j2ll2Ac7pK3F71QDU8CuT:Exc2yjq4j2uYnQDU8CuT
MD5:	5F48FC77CAC90C4778FA24EC9C57F37D
SHA1:	9E89D1515BC4C371B86F4CB1002FD8E377C1829F
SHA-256:	9365920887B11B33A3DC4BA28A0F93951F200341263E3B9CEFD384798E4BE398
SHA-512:	CAB8C4AFA1D8E3A8B7856EE29AE92566D44CEEAD70C8D533F2C98A976D77D0E1D314719B5C6A473789D8C6B21EBB4B89A6B0EC2E1C9C618FB1437EBC77D3A269
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-3.2.1.slim.min.js
Preview:	/*! jQuery v3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_evalUrl,-event/ajax,-effects,-effects/Tween,-effects/animatedSelector | (c) JS Foundation and other contributors | jquery.org/license */!function(a,b){"use strict";"object"==typeof module &&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\legal-localnav[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	81064
Entropy (8bit):	5.28221976381153
Encrypted:	false
SSDEEP:	1536:j6CZ7oREbUgoM7QaN2NRfXLc4kfmmNtKehLsnhS8NJUjq:j9fN2NJc4kfmmZAhTUW
MD5:	EC6073E0F05759808D53E0E08B44BE47
SHA1:	F9C144457862F8B3E443AA2DE4AA4A03A221C01C
SHA-256:	9386495B7EA3C279C17E868BE90E112BA56DA18E493ABFFA76BD9A6D34D4BC8A
SHA-512:	8308CF10230764CD49CCEE25C6376AD77FEB939AE484CE328B1DD6ADF320BCC6A1C831133497898E842AA41CEEC40B78632626F785968127D2CA7626A23D29C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/services/feds.res_1.js/head/en/acom/corporate-mega-menu/legal-localnav.js
Preview:	/*! applauncher v0.49.0 built on Mon, 26 Apr 2021 07:16:01 GMT */!function(e){var n={};function t(a){if(n[a])return n[a].exports;var o=n[a]={i:a,l:!1,exports:{}};return e[a].call(o.exports,o,o.exports,t),o.l=!0,o.exports}t.m=e,t.c=n,t.d=function(e,n,a){t.o(e,n)||Object.defineProperty(e,n,{configurable:!1,enumerable:!0,get:a})},t.n=function(e){var n=e&&e.__esModule?function(){return e.default}:function(){return e};return t.d(n,"a",n),n},t.o=function(e,n){return Object.prototype.hasOwnProperty.call(e,n)},t.p="",t(t.s=199)}({199:function(e,n,t){t(200),e.exports=t(201)},200:function(e,n,t){"use strict";var a=window.feds.utilities,o=a.loadResource,r=a.getParamValuesFromCookie,c=a.isEmptyObject,i=a.isFunction,s=a.getPropertySafely,p=a.onImsReady,l=a.isUserLoggedIn,u=new(0,a.Debug)({control:"applauncher"}),h={},d={config:{scriptPath:void 0,stylePath:void 0,theme:void 0,locale:void 0,environment:void 0}},f={assetID:{css:"applauncherCSS",js:"applauncherJS"},analyticsContext:{consumer:{name:"fe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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+5PFgeNaF8qygsP8CtlWZ+4uadJkY3lco/yIgBWzXx5Lc7XSI:RpUyyCu9mOn8CiokY1co/rgs7xSjS34
MD5:	A7B1798CC2647C575129083BA0B44B17
SHA1:	ADB860A1E675C0FBEFB38A955A5DC4AF9A025B01
SHA-256:	08F9AB3D41530F3E9D8F0780EF1A92F35ED821B5428E6B3C29DDB162F04818FA
SHA-512:	B8828CE68F5C980A9FB880997E5EBAF1533C320820ADC208AABD01B1430FE88DEB7715A900B70951A1F27081E5F6B0FC19A629F14C19552376034CEE1CAA2FF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\login-bg-thumb-1[1].jpg	
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?&.\....I.=..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

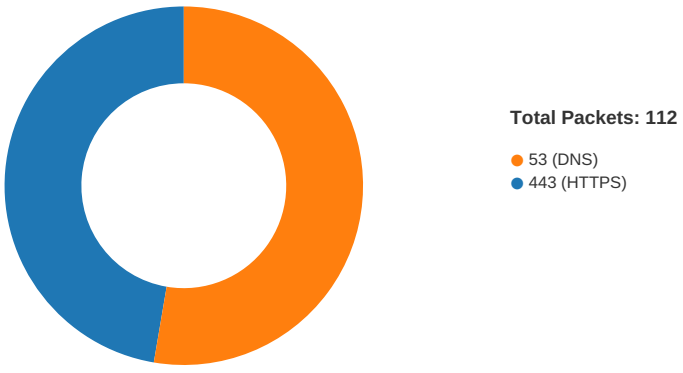
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\login[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with no line terminators
Category:	dropped
Size (bytes):	144
Entropy (8bit):	4.604190783593319
Encrypted:	false
SSDEEP:	3:QIk4Xvwg3e/QgY1ALD64XHUQZ6WVSy1ALD64XHUQZ4n:QI5oPX7Ll0AVwLl0tn
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

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:41:12.401151896 CEST	49716	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.401721954 CEST	49717	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.445152998 CEST	443	49716	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.445261002 CEST	49716	443	192.168.2.3	13.225.74.35

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:41:12.445470095 CEST	443	49717	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.445808887 CEST	49717	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.450882912 CEST	49716	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.450993061 CEST	49717	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.456763983 CEST	443	49716	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.458559990 CEST	49716	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.470412016 CEST	443	49717	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.470511913 CEST	49717	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.492022038 CEST	443	49716	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.492127895 CEST	443	49717	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.492594004 CEST	443	49717	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.492742062 CEST	443	49717	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.493778944 CEST	443	49716	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.493864059 CEST	49716	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.493907928 CEST	443	49716	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.493957996 CEST	49716	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.494524002 CEST	49717	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.496386051 CEST	443	49716	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.497271061 CEST	49716	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.500614882 CEST	443	49717	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.503211975 CEST	49717	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.533791065 CEST	49717	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.533837080 CEST	49716	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.542007923 CEST	49716	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.542459011 CEST	49717	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.542707920 CEST	49716	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.576483965 CEST	443	49716	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.576509953 CEST	443	49716	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.576561928 CEST	443	49716	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.576621056 CEST	49716	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.576646090 CEST	49716	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.577327013 CEST	49716	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.580231905 CEST	443	49717	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.580286980 CEST	443	49717	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.580368042 CEST	49717	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.580491066 CEST	443	49717	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.580552101 CEST	49717	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.581017971 CEST	49717	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.583215952 CEST	443	49716	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.583503962 CEST	443	49716	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.583597898 CEST	49716	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.583607912 CEST	443	49717	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.583652973 CEST	443	49717	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.583863020 CEST	443	49716	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.584028959 CEST	49717	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.620744944 CEST	443	49716	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.624346018 CEST	443	49717	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.984175920 CEST	443	49716	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.984211922 CEST	443	49716	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.984226942 CEST	443	49716	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.984242916 CEST	443	49716	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.984304905 CEST	49716	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.984354019 CEST	49716	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.985192060 CEST	443	49716	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.985233068 CEST	443	49716	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.985280991 CEST	49716	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.985323906 CEST	49716	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:12.986251116 CEST	443	49716	13.225.74.35	192.168.2.3
May 12, 2021 18:41:12.986346006 CEST	49716	443	192.168.2.3	13.225.74.35
May 12, 2021 18:41:13.562144041 CEST	49719	443	192.168.2.3	13.224.193.29
May 12, 2021 18:41:13.563114882 CEST	49720	443	192.168.2.3	13.224.193.29
May 12, 2021 18:41:13.564026117 CEST	49721	443	192.168.2.3	13.224.193.29
May 12, 2021 18:41:13.565155029 CEST	49722	443	192.168.2.3	13.224.193.29
May 12, 2021 18:41:13.566195965 CEST	49723	443	192.168.2.3	13.224.193.29

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:41:13.603522062 CEST	443	49719	13.224.193.29	192.168.2.3
May 12, 2021 18:41:13.603610039 CEST	49719	443	192.168.2.3	13.224.193.29
May 12, 2021 18:41:13.604329109 CEST	443	49720	13.224.193.29	192.168.2.3
May 12, 2021 18:41:13.604502916 CEST	49720	443	192.168.2.3	13.224.193.29
May 12, 2021 18:41:13.605611086 CEST	49719	443	192.168.2.3	13.224.193.29
May 12, 2021 18:41:13.605670929 CEST	443	49721	13.224.193.29	192.168.2.3
May 12, 2021 18:41:13.605757952 CEST	49721	443	192.168.2.3	13.224.193.29
May 12, 2021 18:41:13.606647015 CEST	49721	443	192.168.2.3	13.224.193.29
May 12, 2021 18:41:13.607563972 CEST	49720	443	192.168.2.3	13.224.193.29
May 12, 2021 18:41:13.607589960 CEST	443	49722	13.224.193.29	192.168.2.3
May 12, 2021 18:41:13.607683897 CEST	49722	443	192.168.2.3	13.224.193.29
May 12, 2021 18:41:13.607996941 CEST	443	49723	13.224.193.29	192.168.2.3
May 12, 2021 18:41:13.608088017 CEST	49723	443	192.168.2.3	13.224.193.29
May 12, 2021 18:41:13.608455896 CEST	49722	443	192.168.2.3	13.224.193.29
May 12, 2021 18:41:13.609265089 CEST	49723	443	192.168.2.3	13.224.193.29
May 12, 2021 18:41:13.615473032 CEST	443	49720	13.224.193.29	192.168.2.3
May 12, 2021 18:41:13.615622997 CEST	49720	443	192.168.2.3	13.224.193.29
May 12, 2021 18:41:13.616372108 CEST	443	49721	13.224.193.29	192.168.2.3
May 12, 2021 18:41:13.616468906 CEST	443	49719	13.224.193.29	192.168.2.3
May 12, 2021 18:41:13.616480112 CEST	49721	443	192.168.2.3	13.224.193.29
May 12, 2021 18:41:13.616513968 CEST	49719	443	192.168.2.3	13.224.193.29
May 12, 2021 18:41:13.620255947 CEST	443	49723	13.224.193.29	192.168.2.3
May 12, 2021 18:41:13.620309114 CEST	49723	443	192.168.2.3	13.224.193.29
May 12, 2021 18:41:13.623419046 CEST	443	49722	13.224.193.29	192.168.2.3
May 12, 2021 18:41:13.623585939 CEST	49722	443	192.168.2.3	13.224.193.29
May 12, 2021 18:41:13.648633957 CEST	443	49719	13.224.193.29	192.168.2.3
May 12, 2021 18:41:13.649158955 CEST	443	49719	13.224.193.29	192.168.2.3
May 12, 2021 18:41:13.649179935 CEST	443	49719	13.224.193.29	192.168.2.3
May 12, 2021 18:41:13.649281979 CEST	49719	443	192.168.2.3	13.224.193.29
May 12, 2021 18:41:13.649296045 CEST	49719	443	192.168.2.3	13.224.193.29
May 12, 2021 18:41:13.649311066 CEST	443	49721	13.224.193.29	192.168.2.3
May 12, 2021 18:41:13.649966002 CEST	443	49721	13.224.193.29	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:41:03.566900969 CEST	55984	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:03.618391991 CEST	53	55984	8.8.8.8	192.168.2.3
May 12, 2021 18:41:03.893721104 CEST	64185	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:03.954075098 CEST	53	64185	8.8.8.8	192.168.2.3
May 12, 2021 18:41:04.418853045 CEST	65110	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:04.467658043 CEST	53	65110	8.8.8.8	192.168.2.3
May 12, 2021 18:41:05.202028036 CEST	58361	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:05.253813982 CEST	53	58361	8.8.8.8	192.168.2.3
May 12, 2021 18:41:06.040771008 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:06.089370012 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 18:41:06.887065887 CEST	60831	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:06.938662052 CEST	53	60831	8.8.8.8	192.168.2.3
May 12, 2021 18:41:07.983275890 CEST	60100	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:08.032814026 CEST	53	60100	8.8.8.8	192.168.2.3
May 12, 2021 18:41:09.477318048 CEST	53195	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:09.530191898 CEST	53	53195	8.8.8.8	192.168.2.3
May 12, 2021 18:41:10.531835079 CEST	50141	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:10.580724001 CEST	53	50141	8.8.8.8	192.168.2.3
May 12, 2021 18:41:10.925062895 CEST	53023	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:10.982347012 CEST	53	53023	8.8.8.8	192.168.2.3
May 12, 2021 18:41:12.000463963 CEST	49563	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:12.057898998 CEST	53	49563	8.8.8.8	192.168.2.3
May 12, 2021 18:41:12.327963114 CEST	51352	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:12.388222933 CEST	53	51352	8.8.8.8	192.168.2.3
May 12, 2021 18:41:13.004811049 CEST	59349	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:13.053580046 CEST	53	59349	8.8.8.8	192.168.2.3
May 12, 2021 18:41:13.078450918 CEST	57084	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:13.137614012 CEST	53	57084	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:41:13.764828920 CEST	58823	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:13.826730013 CEST	53	58823	8.8.8.8	192.168.2.3
May 12, 2021 18:41:14.852165937 CEST	57568	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:14.909244061 CEST	53	57568	8.8.8.8	192.168.2.3
May 12, 2021 18:41:15.089215040 CEST	50540	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:15.162746906 CEST	53	50540	8.8.8.8	192.168.2.3
May 12, 2021 18:41:16.507857084 CEST	54366	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:16.560260057 CEST	53	54366	8.8.8.8	192.168.2.3
May 12, 2021 18:41:18.693429947 CEST	53034	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:18.743026018 CEST	53	53034	8.8.8.8	192.168.2.3
May 12, 2021 18:41:21.241797924 CEST	57762	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:21.292956114 CEST	53	57762	8.8.8.8	192.168.2.3
May 12, 2021 18:41:22.015003920 CEST	55435	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:22.063818932 CEST	53	55435	8.8.8.8	192.168.2.3
May 12, 2021 18:41:23.190924883 CEST	50713	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:23.239545107 CEST	53	50713	8.8.8.8	192.168.2.3
May 12, 2021 18:41:24.563947916 CEST	56132	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:24.612673044 CEST	53	56132	8.8.8.8	192.168.2.3
May 12, 2021 18:41:30.204597950 CEST	58987	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:30.255376101 CEST	53	58987	8.8.8.8	192.168.2.3
May 12, 2021 18:41:30.892107010 CEST	56579	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:30.941258907 CEST	53	56579	8.8.8.8	192.168.2.3
May 12, 2021 18:41:34.985313892 CEST	60633	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:35.047008038 CEST	53	60633	8.8.8.8	192.168.2.3
May 12, 2021 18:41:35.497230053 CEST	61292	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:35.669828892 CEST	53	61292	8.8.8.8	192.168.2.3
May 12, 2021 18:41:36.412293911 CEST	63619	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:36.418067932 CEST	64938	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:36.428987980 CEST	61946	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:36.439857960 CEST	64910	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:36.453360081 CEST	52123	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:36.475197077 CEST	53	64938	8.8.8.8	192.168.2.3
May 12, 2021 18:41:36.481283903 CEST	53	63619	8.8.8.8	192.168.2.3
May 12, 2021 18:41:36.487832069 CEST	53	61946	8.8.8.8	192.168.2.3
May 12, 2021 18:41:36.497147083 CEST	53	64910	8.8.8.8	192.168.2.3
May 12, 2021 18:41:36.517525911 CEST	53	52123	8.8.8.8	192.168.2.3
May 12, 2021 18:41:36.517729044 CEST	56130	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:36.580723047 CEST	53	56130	8.8.8.8	192.168.2.3
May 12, 2021 18:41:36.829586983 CEST	56338	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:36.890536070 CEST	53	56338	8.8.8.8	192.168.2.3
May 12, 2021 18:41:41.526017904 CEST	59420	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:41.583123922 CEST	53	59420	8.8.8.8	192.168.2.3
May 12, 2021 18:41:41.734714985 CEST	58784	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:41.792160988 CEST	53	58784	8.8.8.8	192.168.2.3
May 12, 2021 18:41:41.906120062 CEST	63978	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:41.977229118 CEST	53	63978	8.8.8.8	192.168.2.3
May 12, 2021 18:41:42.585053921 CEST	59420	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:42.633845091 CEST	53	59420	8.8.8.8	192.168.2.3
May 12, 2021 18:41:42.726495981 CEST	58784	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:42.775408030 CEST	53	58784	8.8.8.8	192.168.2.3
May 12, 2021 18:41:43.631911039 CEST	59420	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:43.695348978 CEST	53	59420	8.8.8.8	192.168.2.3
May 12, 2021 18:41:43.788244963 CEST	58784	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:43.846075058 CEST	53	58784	8.8.8.8	192.168.2.3
May 12, 2021 18:41:46.214852095 CEST	58784	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:46.264990091 CEST	53	58784	8.8.8.8	192.168.2.3
May 12, 2021 18:41:46.773161888 CEST	59420	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:46.826565981 CEST	62938	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:46.832793951 CEST	53	59420	8.8.8.8	192.168.2.3
May 12, 2021 18:41:46.908078909 CEST	53	62938	8.8.8.8	192.168.2.3
May 12, 2021 18:41:47.647465944 CEST	55708	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:47.653454065 CEST	56803	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:47.707379103 CEST	53	55708	8.8.8.8	192.168.2.3
May 12, 2021 18:41:47.712129116 CEST	53	56803	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:41:48.135555983 CEST	57145	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:48.194864035 CEST	53	57145	8.8.8.8	192.168.2.3
May 12, 2021 18:41:48.357476950 CEST	55359	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:48.417488098 CEST	53	55359	8.8.8.8	192.168.2.3
May 12, 2021 18:41:48.701155901 CEST	58306	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:48.757843971 CEST	64124	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:48.771852016 CEST	53	58306	8.8.8.8	192.168.2.3
May 12, 2021 18:41:48.823772907 CEST	53	64124	8.8.8.8	192.168.2.3
May 12, 2021 18:41:49.269100904 CEST	49361	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:49.331315041 CEST	53	49361	8.8.8.8	192.168.2.3
May 12, 2021 18:41:50.198074102 CEST	58784	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:50.250207901 CEST	53	58784	8.8.8.8	192.168.2.3
May 12, 2021 18:41:50.777009010 CEST	59420	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:50.825906992 CEST	53	59420	8.8.8.8	192.168.2.3
May 12, 2021 18:41:50.928817034 CEST	63150	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:50.990961075 CEST	53	63150	8.8.8.8	192.168.2.3
May 12, 2021 18:41:51.188599110 CEST	53279	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:51.221474886 CEST	56881	53	192.168.2.3	8.8.8.8
May 12, 2021 18:41:51.258306980 CEST	53	53279	8.8.8.8	192.168.2.3
May 12, 2021 18:41:51.294668913 CEST	53	56881	8.8.8.8	192.168.2.3
May 12, 2021 18:42:29.160867929 CEST	53642	53	192.168.2.3	8.8.8.8
May 12, 2021 18:42:29.222378016 CEST	53	53642	8.8.8.8	192.168.2.3
May 12, 2021 18:42:53.491514921 CEST	55667	53	192.168.2.3	8.8.8.8
May 12, 2021 18:42:53.550228119 CEST	53	55667	8.8.8.8	192.168.2.3
May 12, 2021 18:42:53.567498922 CEST	54833	53	192.168.2.3	8.8.8.8
May 12, 2021 18:42:53.638984919 CEST	53	54833	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 18:41:13.078450918 CEST	192.168.2.3	8.8.8.8	0x7c6b	Standard query (0)	page.adobe spark-assets.com	A (IP address)	IN (0x0001)
May 12, 2021 18:41:13.764828920 CEST	192.168.2.3	8.8.8.8	0xd40d	Standard query (0)	use.typekit.net	A (IP address)	IN (0x0001)
May 12, 2021 18:41:14.852165937 CEST	192.168.2.3	8.8.8.8	0x9af7	Standard query (0)	s3.amazona ws.com	A (IP address)	IN (0x0001)
May 12, 2021 18:41:15.089215040 CEST	192.168.2.3	8.8.8.8	0xb496	Standard query (0)	p.typekit.net	A (IP address)	IN (0x0001)
May 12, 2021 18:41:30.204597950 CEST	192.168.2.3	8.8.8.8	0x8dde	Standard query (0)	page.adobe spark-assets.com	A (IP address)	IN (0x0001)
May 12, 2021 18:41:35.497230053 CEST	192.168.2.3	8.8.8.8	0x7536	Standard query (0)	landarch.org	A (IP address)	IN (0x0001)
May 12, 2021 18:41:36.418067932 CEST	192.168.2.3	8.8.8.8	0x5cd3	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
May 12, 2021 18:41:36.428987980 CEST	192.168.2.3	8.8.8.8	0xbdf8	Standard query (0)	maxcdn.boo tstrapcdn.com	A (IP address)	IN (0x0001)
May 12, 2021 18:41:36.453360081 CEST	192.168.2.3	8.8.8.8	0xa6e7	Standard query (0)	kit.fontaw esome.com	A (IP address)	IN (0x0001)
May 12, 2021 18:41:36.517729044 CEST	192.168.2.3	8.8.8.8	0x4853	Standard query (0)	cdnjs.clou dflare.com	A (IP address)	IN (0x0001)
May 12, 2021 18:41:36.829586983 CEST	192.168.2.3	8.8.8.8	0xd4e9	Standard query (0)	ka-f.fonta wesome.com	A (IP address)	IN (0x0001)
May 12, 2021 18:41:46.826565981 CEST	192.168.2.3	8.8.8.8	0x4965	Standard query (0)	static.ado belogin.com	A (IP address)	IN (0x0001)
May 12, 2021 18:41:47.647465944 CEST	192.168.2.3	8.8.8.8	0x2b84	Standard query (0)	assets.ado bedtm.com	A (IP address)	IN (0x0001)
May 12, 2021 18:41:47.653454065 CEST	192.168.2.3	8.8.8.8	0x87ff	Standard query (0)	cdn.cookie law.org	A (IP address)	IN (0x0001)
May 12, 2021 18:41:48.135555983 CEST	192.168.2.3	8.8.8.8	0x5328	Standard query (0)	geolocatio n.onetrust.com	A (IP address)	IN (0x0001)
May 12, 2021 18:41:48.357476950 CEST	192.168.2.3	8.8.8.8	0x4128	Standard query (0)	dpm.demdex.net	A (IP address)	IN (0x0001)
May 12, 2021 18:41:49.269100904 CEST	192.168.2.3	8.8.8.8	0xb6db	Standard query (0)	api.demand base.com	A (IP address)	IN (0x0001)
May 12, 2021 18:41:50.928817034 CEST	192.168.2.3	8.8.8.8	0x81af	Standard query (0)	adobe.tt.o mtrdc.net	A (IP address)	IN (0x0001)
May 12, 2021 18:41:51.221474886 CEST	192.168.2.3	8.8.8.8	0xb461	Standard query (0)	cm.everest tech.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 18:41:12.388222933 CEST	8.8.8.8	192.168.2.3	0x2870	No error (0)	spark.adobeprojectm.com		13.225.74.35	A (IP address)	IN (0x0001)
May 12, 2021 18:41:12.388222933 CEST	8.8.8.8	192.168.2.3	0x2870	No error (0)	spark.adobeprojectm.com		13.225.74.123	A (IP address)	IN (0x0001)
May 12, 2021 18:41:12.388222933 CEST	8.8.8.8	192.168.2.3	0x2870	No error (0)	spark.adobeprojectm.com		13.225.74.86	A (IP address)	IN (0x0001)
May 12, 2021 18:41:12.388222933 CEST	8.8.8.8	192.168.2.3	0x2870	No error (0)	spark.adobeprojectm.com		13.225.74.22	A (IP address)	IN (0x0001)
May 12, 2021 18:41:13.137614012 CEST	8.8.8.8	192.168.2.3	0x7c6b	No error (0)	page.adobesparkassets.com		13.224.193.29	A (IP address)	IN (0x0001)
May 12, 2021 18:41:13.137614012 CEST	8.8.8.8	192.168.2.3	0x7c6b	No error (0)	page.adobesparkassets.com		13.224.193.108	A (IP address)	IN (0x0001)
May 12, 2021 18:41:13.137614012 CEST	8.8.8.8	192.168.2.3	0x7c6b	No error (0)	page.adobesparkassets.com		13.224.193.81	A (IP address)	IN (0x0001)
May 12, 2021 18:41:13.137614012 CEST	8.8.8.8	192.168.2.3	0x7c6b	No error (0)	page.adobesparkassets.com		13.224.193.122	A (IP address)	IN (0x0001)
May 12, 2021 18:41:13.826730013 CEST	8.8.8.8	192.168.2.3	0xd40d	No error (0)	use.typekit.net	use-stls.adobe.com.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:41:14.909244061 CEST	8.8.8.8	192.168.2.3	0x9af7	No error (0)	s3.amazonaws.com		52.217.11.150	A (IP address)	IN (0x0001)
May 12, 2021 18:41:15.162746906 CEST	8.8.8.8	192.168.2.3	0xb496	No error (0)	p.typekit.net	p.typekit.net-v3.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:41:30.255376101 CEST	8.8.8.8	192.168.2.3	0x8dde	No error (0)	page.adobesparkassets.com		13.224.193.29	A (IP address)	IN (0x0001)
May 12, 2021 18:41:30.255376101 CEST	8.8.8.8	192.168.2.3	0x8dde	No error (0)	page.adobesparkassets.com		13.224.193.108	A (IP address)	IN (0x0001)
May 12, 2021 18:41:30.255376101 CEST	8.8.8.8	192.168.2.3	0x8dde	No error (0)	page.adobesparkassets.com		13.224.193.81	A (IP address)	IN (0x0001)
May 12, 2021 18:41:30.255376101 CEST	8.8.8.8	192.168.2.3	0x8dde	No error (0)	page.adobesparkassets.com		13.224.193.122	A (IP address)	IN (0x0001)
May 12, 2021 18:41:35.669828892 CEST	8.8.8.8	192.168.2.3	0x7536	No error (0)	landarch.org		50.87.140.26	A (IP address)	IN (0x0001)
May 12, 2021 18:41:36.475197077 CEST	8.8.8.8	192.168.2.3	0x5cd3	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:41:36.487832069 CEST	8.8.8.8	192.168.2.3	0xbdf8	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
May 12, 2021 18:41:36.487832069 CEST	8.8.8.8	192.168.2.3	0xbdf8	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
May 12, 2021 18:41:36.517525911 CEST	8.8.8.8	192.168.2.3	0xa6e7	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:41:36.580723047 CEST	8.8.8.8	192.168.2.3	0x4853	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
May 12, 2021 18:41:36.580723047 CEST	8.8.8.8	192.168.2.3	0x4853	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
May 12, 2021 18:41:36.890536070 CEST	8.8.8.8	192.168.2.3	0xd4e9	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:41:46.908078909 CEST	8.8.8.8	192.168.2.3	0x4965	No error (0)	static.adobelogin.com	adobelogin-static.prod.ims.adobejanus.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:41:46.908078909 CEST	8.8.8.8	192.168.2.3	0x4965	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
May 12, 2021 18:41:46.908078909 CEST	8.8.8.8	192.168.2.3	0x4965	No error (0)	dd20fzx9mj46f.cloudfront.net		13.224.187.69	A (IP address)	IN (0x0001)
May 12, 2021 18:41:47.707379103 CEST	8.8.8.8	192.168.2.3	0x2b84	No error (0)	assets.adobedtm.com	cn-assets.adobedtm.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:41:47.712129116 CEST	8.8.8.8	192.168.2.3	0x87ff	No error (0)	cdn.cookielaw.org		104.16.149.64	A (IP address)	IN (0x0001)
May 12, 2021 18:41:47.712129116 CEST	8.8.8.8	192.168.2.3	0x87ff	No error (0)	cdn.cookielaw.org		104.16.148.64	A (IP address)	IN (0x0001)
May 12, 2021 18:41:48.194864035 CEST	8.8.8.8	192.168.2.3	0x5328	No error (0)	geolocation.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
May 12, 2021 18:41:48.194864035 CEST	8.8.8.8	192.168.2.3	0x5328	No error (0)	geolocation.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
May 12, 2021 18:41:48.417488098 CEST	8.8.8.8	192.168.2.3	0x4128	No error (0)	dpm.demdex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:41:48.417488098 CEST	8.8.8.8	192.168.2.3	0x4128	No error (0)	gslb-2.demdex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:41:48.417488098 CEST	8.8.8.8	192.168.2.3	0x4128	No error (0)	edge-irl1.demdex.net	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:41:48.417488098 CEST	8.8.8.8	192.168.2.3	0x4128	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.214.120.236	A (IP address)	IN (0x0001)
May 12, 2021 18:41:48.417488098 CEST	8.8.8.8	192.168.2.3	0x4128	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		18.200.157.96	A (IP address)	IN (0x0001)
May 12, 2021 18:41:48.417488098 CEST	8.8.8.8	192.168.2.3	0x4128	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.30.200.197	A (IP address)	IN (0x0001)
May 12, 2021 18:41:48.417488098 CEST	8.8.8.8	192.168.2.3	0x4128	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.31.176.223	A (IP address)	IN (0x0001)
May 12, 2021 18:41:48.417488098 CEST	8.8.8.8	192.168.2.3	0x4128	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.17.54.18	A (IP address)	IN (0x0001)
May 12, 2021 18:41:48.417488098 CEST	8.8.8.8	192.168.2.3	0x4128	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.250.160.147	A (IP address)	IN (0x0001)
May 12, 2021 18:41:48.417488098 CEST	8.8.8.8	192.168.2.3	0x4128	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.170.210.188	A (IP address)	IN (0x0001)
May 12, 2021 18:41:48.417488098 CEST	8.8.8.8	192.168.2.3	0x4128	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.251.129.229	A (IP address)	IN (0x0001)
May 12, 2021 18:41:48.823772907 CEST	8.8.8.8	192.168.2.3	0x534f	No error (0)	adobe.com.ssl.d1.sc.omtrdc.net		35.181.18.61	A (IP address)	IN (0x0001)
May 12, 2021 18:41:48.823772907 CEST	8.8.8.8	192.168.2.3	0x534f	No error (0)	adobe.com.ssl.d1.sc.omtrdc.net		15.237.76.117	A (IP address)	IN (0x0001)
May 12, 2021 18:41:48.823772907 CEST	8.8.8.8	192.168.2.3	0x534f	No error (0)	adobe.com.ssl.d1.sc.omtrdc.net		15.237.136.106	A (IP address)	IN (0x0001)
May 12, 2021 18:41:49.331315041 CEST	8.8.8.8	192.168.2.3	0xb6db	No error (0)	api.demandbase.com		13.225.74.58	A (IP address)	IN (0x0001)
May 12, 2021 18:41:49.331315041 CEST	8.8.8.8	192.168.2.3	0xb6db	No error (0)	api.demandbase.com		13.225.74.37	A (IP address)	IN (0x0001)
May 12, 2021 18:41:49.331315041 CEST	8.8.8.8	192.168.2.3	0xb6db	No error (0)	api.demandbase.com		13.225.74.112	A (IP address)	IN (0x0001)
May 12, 2021 18:41:49.331315041 CEST	8.8.8.8	192.168.2.3	0xb6db	No error (0)	api.demandbase.com		13.225.74.124	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 18:41:50.990961075 CEST	8.8.8.8	192.168.2.3	0x81af	No error (0)	adobe.tt.omtrdc.net		52.51.251.137	A (IP address)	IN (0x0001)
May 12, 2021 18:41:50.990961075 CEST	8.8.8.8	192.168.2.3	0x81af	No error (0)	adobe.tt.omtrdc.net		52.212.164.82	A (IP address)	IN (0x0001)
May 12, 2021 18:41:50.990961075 CEST	8.8.8.8	192.168.2.3	0x81af	No error (0)	adobe.tt.omtrdc.net		34.251.77.56	A (IP address)	IN (0x0001)
May 12, 2021 18:41:50.990961075 CEST	8.8.8.8	192.168.2.3	0x81af	No error (0)	adobe.tt.omtrdc.net		34.252.166.160	A (IP address)	IN (0x0001)
May 12, 2021 18:41:50.990961075 CEST	8.8.8.8	192.168.2.3	0x81af	No error (0)	adobe.tt.omtrdc.net		52.213.168.74	A (IP address)	IN (0x0001)
May 12, 2021 18:41:50.990961075 CEST	8.8.8.8	192.168.2.3	0x81af	No error (0)	adobe.tt.omtrdc.net		18.203.205.32	A (IP address)	IN (0x0001)
May 12, 2021 18:41:50.990961075 CEST	8.8.8.8	192.168.2.3	0x81af	No error (0)	adobe.tt.omtrdc.net		52.212.193.208	A (IP address)	IN (0x0001)
May 12, 2021 18:41:50.990961075 CEST	8.8.8.8	192.168.2.3	0x81af	No error (0)	adobe.tt.omtrdc.net		34.252.156.174	A (IP address)	IN (0x0001)
May 12, 2021 18:41:51.294668913 CEST	8.8.8.8	192.168.2.3	0xb461	No error (0)	cm.everesttech.net	cm.everesttech.net.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 18:41:12.496386051 CEST	13.225.74.35	443	192.168.2.3	49716	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	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	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		
May 12, 2021 18:41:12.500614882 CEST	13.225.74.35	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	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	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		
May 12, 2021 18:41:13.651201010 CEST	13.224.193.29	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 18:41:13.653599024 CEST	13.224.193.29	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 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		
May 12, 2021 18:41:13.657727003 CEST	13.224.193.29	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		
May 12, 2021 18:41:13.663166046 CEST	13.224.193.29	443	192.168.2.3	49723	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		
May 12, 2021 18:41:13.713536978 CEST	13.224.193.29	443	192.168.2.3	49722	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		
May 12, 2021 18:41:15.228651047 CEST	52.217.11.150	443	192.168.2.3	49726	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
May 12, 2021 18:41:15.231426954 CEST	52.217.11.150	443	192.168.2.3	49727	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		
May 12, 2021 18:41:30.353888035 CEST	13.224.193.29	443	192.168.2.3	49736	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
May 12, 2021 18:41:36.048933029 CEST	50.87.140.26	443	192.168.2.3	49741	CN=cpcontacts.landarch.org CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun May 02 08:27:37 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Sat Jul 31 08:27:37 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 12, 2021 18:41:36.051758051 CEST	50.87.140.26	443	192.168.2.3	49742	CN=cpcontacts.landarch.org CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun May 02 08:27:37 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Sat Jul 31 08:27:37 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 12, 2021 18:41:36.574934959 CEST	104.18.11.207	443	192.168.2.3	49748	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 18:41:36.590507984 CEST	104.18.11.207	443	192.168.2.3	49747	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		
May 12, 2021 18:41:36.674547911 CEST	104.16.18.94	443	192.168.2.3	49754	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		
May 12, 2021 18:41:36.675105095 CEST	104.16.18.94	443	192.168.2.3	49753	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		
May 12, 2021 18:41:47.001563072 CEST	13.224.187.69	443	192.168.2.3	49760	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
May 12, 2021 18:41:47.002485037 CEST	13.224.187.69	443	192.168.2.3	49761	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	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		
May 12, 2021 18:41:47.988857985 CEST	104.16.149.64	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		
May 12, 2021 18:41:47.989820004 CEST	104.16.149.64	443	192.168.2.3	49765	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		
May 12, 2021 18:41:48.322216034 CEST	104.20.184.68	443	192.168.2.3	49766	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		
May 12, 2021 18:41:48.344093084 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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		
May 12, 2021 18:41:48.549436092 CEST	52.214.120.236	443	192.168.2.3	49768	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		
May 12, 2021 18:41:48.552987099 CEST	52.214.120.236	443	192.168.2.3	49769	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		
May 12, 2021 18:41:48.929805040 CEST	35.181.18.61	443	192.168.2.3	49770	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		
May 12, 2021 18:41:48.935934067 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

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 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		
May 12, 2021 18:41:49.429214954 CEST	13.225.74.58	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
					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		
May 12, 2021 18:41:49.436741114 CEST	13.225.74.58	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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		
May 12, 2021 18:41:51.124383926 CEST	52.51.251.137	443	192.168.2.3	49776	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		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5912 Parent PID: 792

General

Start time:	18:41:10
Start date:	12/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff686db0000
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: 5592 Parent PID: 5912

General

Start time:	18:41:10
Start date:	12/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5912 CREDAT:17410 /prefetch:2
Imagebase:	0x290000
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