

ID: 404273
Cookbook: browseurl.jbs
Time: 21:18:34
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report https://spark.adobe.com/page/ql80qXs9cgl3o/ 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
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 9
Public 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 20
No static file info 20
Network Behavior 21
Snort IDS Alerts 21
Network Port Distribution 21
TCP Packets 21
UDP Packets 23
DNS Queries 24
DNS Answers 24
HTTPS Packets 25
Code Manipulations 25
Statistics 25
Behavior 25
System Behavior 26
Analysis Process: iexplore.exe PID: 4316 Parent PID: 792 26
General 26
File Activities 26
Registry Activities 26

Copyright Joe Security LLC 2021

Analysis Process: iexplore.exe PID: 5848 Parent PID: 4316 26
General 26
File Activities 27
Registry Activities 27
Disassembly 27

Copyright Joe Security LLC 2021

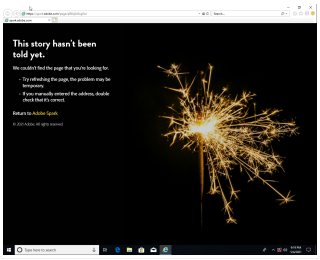
Analysis Report https://spark.adobe.com/page/ql80qXs9…

Overview

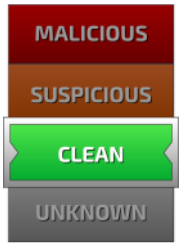
General Information

Sample URL:	http://https://spark.adobe.com/page/ql80qXs9cgl3o/
Analysis ID:	404273
Infos:	

Most interesting Screenshot:



Detection

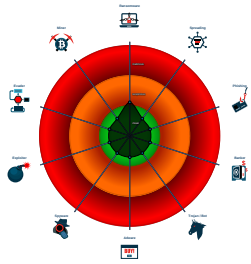


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 4316 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5848 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4316 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

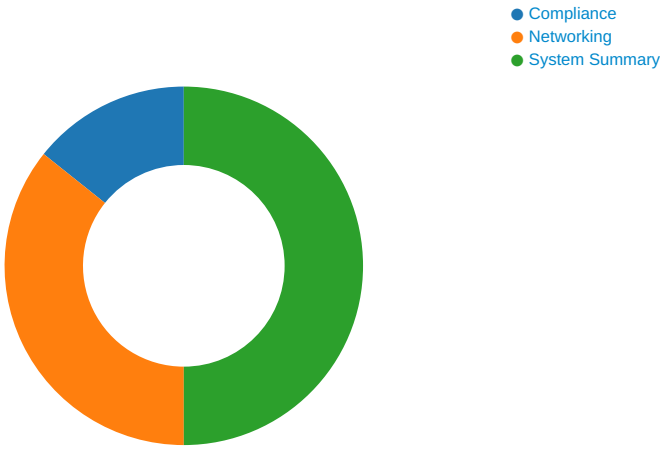
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Copyright Joe Security LLC 2021



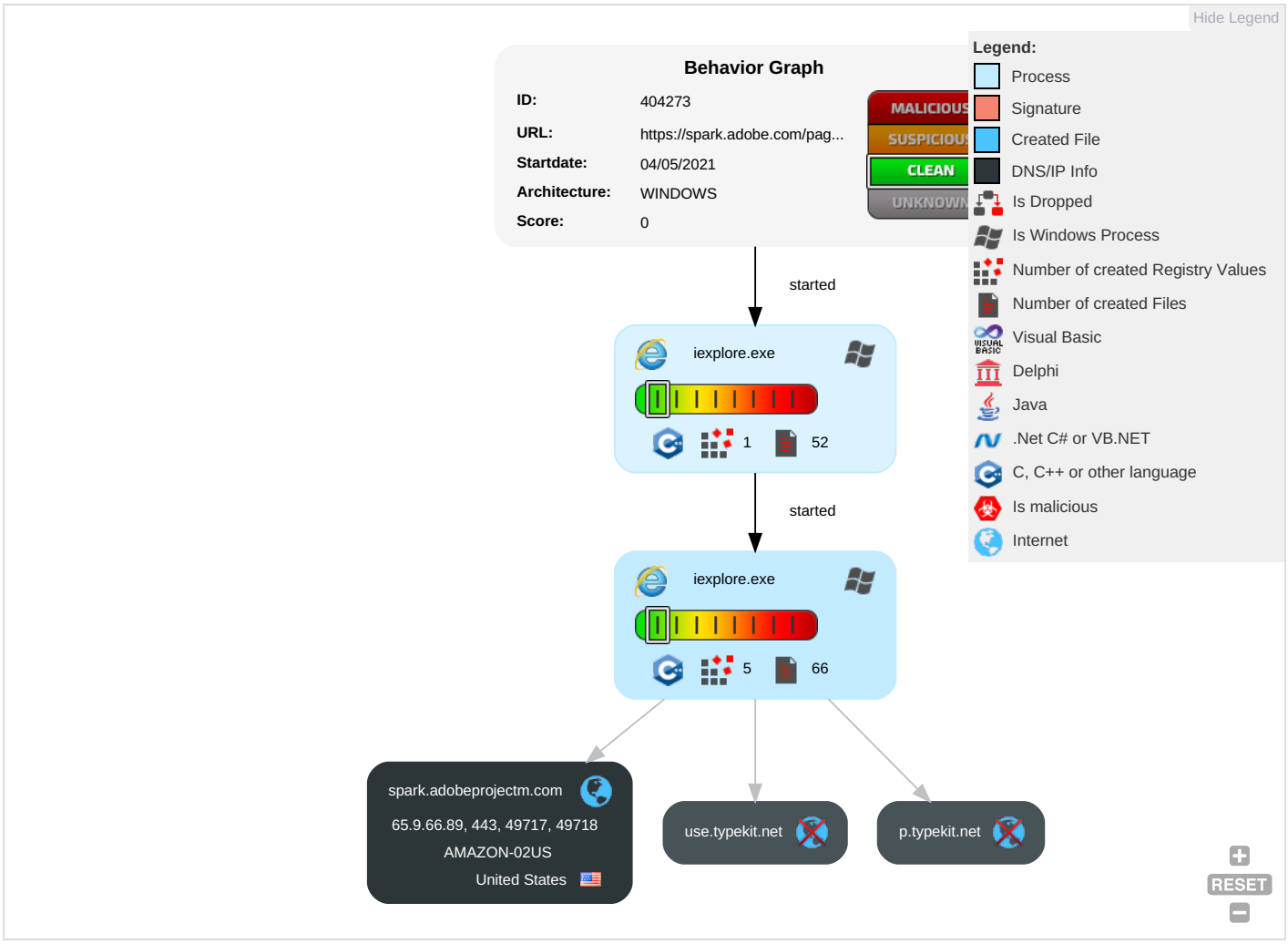
Click to jump to signature section

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impac
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory 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	Application Window Discovery	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

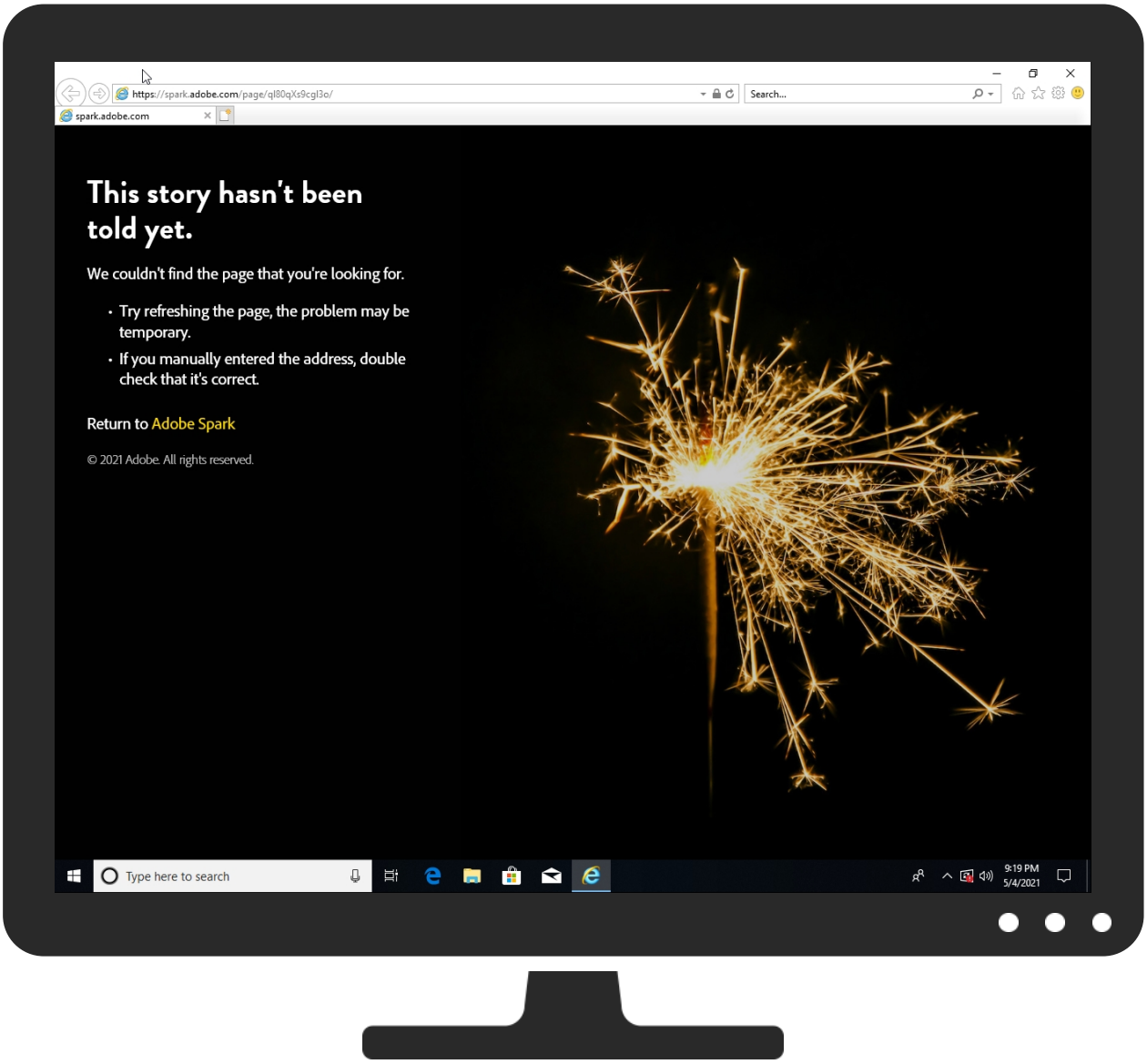


Screenshots

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/ql80qXs9cgl3o/	1%	Virustotal		Browse
http://https://spark.adobe.com/page/ql80qXs9cgl3o/	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
spark.adobeprojectm.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://www.pinterest.	0%	Avira URL Cloud	safe	
http://https://www.facebook.	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://https://blog.adobespark.com/	0%	Virustotal		Browse
http://https://blog.adobespark.com/	0%	Avira URL Cloud	safe	
http://https://spark.adobe.co	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

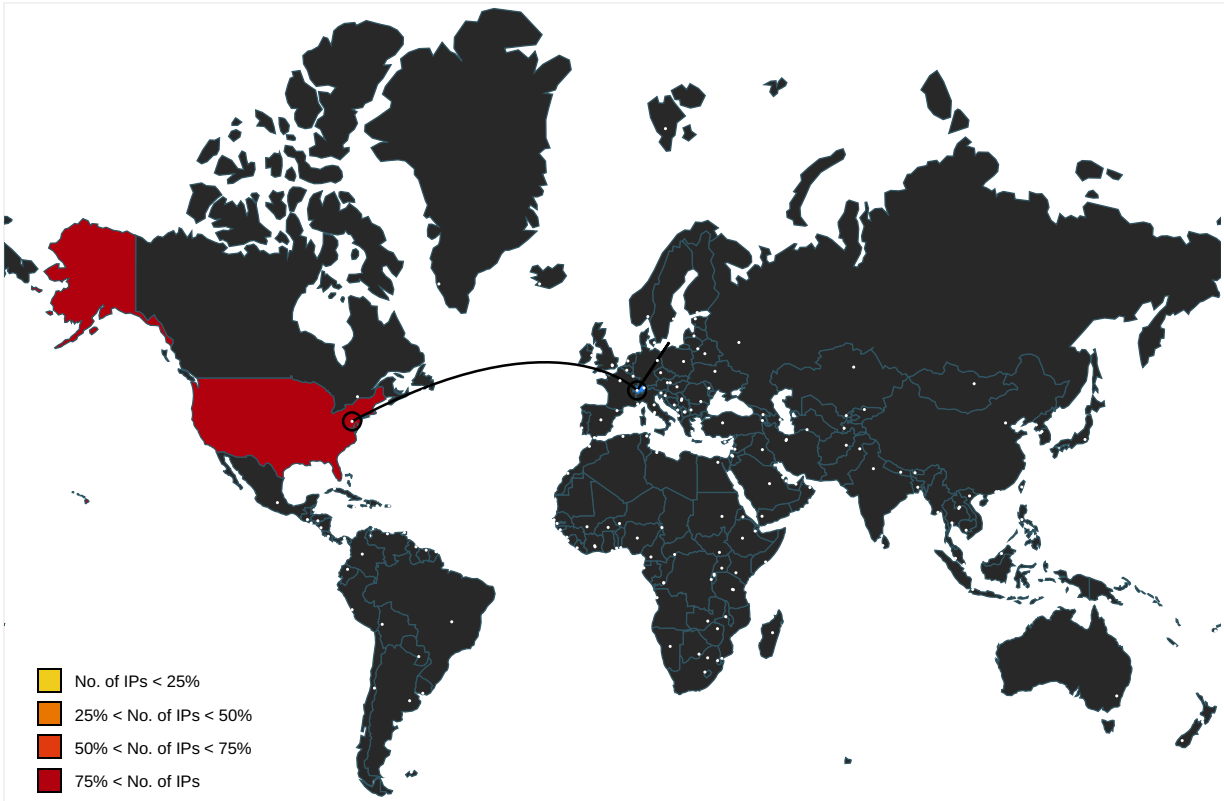
Name	IP	Active	Malicious	Antivirus Detection	Reputation
spark.adobeprojectm.com	65.9.66.89	true	false	• 0%, Virustotal, Browse	unknown
use.typekit.net	unknown	unknown	false		high
p.typekit.net	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.pinterest.	scripts[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	scripts[1].js.2.dr	false		high
http://https://www.linkedin.com	scripts[1].js.2.dr	false		high
http://https://use.typekit.net/af/b0c5f5/00000000000000003b9b3f85/27/l?primer=7cdcb44be4a7db8877ffa5c0007b8	scripts[1].js.2.dr	false		high
http://https://www.facebook.	scripts[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://typekit.com/eulas/000000000000000000000132e1	vtg4qoo[1].js.2.dr	false		high
http://https://use.typekit.net/af/eaf09c/00000000000000000000017703/27/	vtg4qoo[1].js.2.dr	false		high
http://https://use.typekit.net/af/1da05b/000000000000000000000132df/27/	vtg4qoo[1].js.2.dr	false		high
http://https://use.typekit.net/af/d8f71f/000000000000000000000132e1/27/	vtg4qoo[1].js.2.dr	false		high
http://https://use.typekit.net/af/97fbd1/00000000000000003b9b3f88/27/l?primer=7cdcb44be4a7db8877ffa5c0007b8	scripts[1].js.2.dr	false		high
http://https://use.typekit.net/af/4b3e87/00000000000000000000017706/27/	vtg4qoo[1].js.2.dr	false		high
http://https://www.youtube.com	scripts[1].js.2.dr	false		high
http://https://use.typekit.net/af/cb695f/00000000000000000000017701/27/	vtg4qoo[1].js.2.dr	false		high
http://typekit.com/eulas/00000000000000000000017706	vtg4qoo[1].js.2.dr	false		high
http://https://www.instagram.com	scripts[1].js.2.dr	false		high
http://typekit.com/eulas/000000000000000000000132df	vtg4qoo[1].js.2.dr	false		high
http://https://p.typekit.net/p.gif	vtg4qoo[1].js.2.dr	false		high
http://https://twitter.com	scripts[1].js.2.dr	false		high
http://typekit.com/eulas/000000000000000000000176ff	vtg4qoo[1].js.2.dr	false		high
http://https://use.typekit.net/af/8f4e31/000000000000000000000132e3/27/	vtg4qoo[1].js.2.dr	false		high
http://typekit.com/eulas/00000000000000000000017701	vtg4qoo[1].js.2.dr	false		high
http://https://adobesparkpost.app.link/jsoIbkwCVeb	express[1].htm.2.dr	false		high
http://typekit.com/eulas/00000000000000000000017703	vtg4qoo[1].js.2.dr	false		high
http://https://blog.adobespark.com/	scripts[1].js.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://use.typekit.net/af/40207f/00000000000000000000176ff/27/	vtg4qoo[1].js.2.dr	false		high
http://https://use.typekit.net/af/ad2a79/00000000000000003b9b3f8c/27/l?primer=7cdcb44be4a7db8877ffa5c0007b8	scripts[1].js.2.dr	false		high
http://typekit.com/eulas/000000000000000000000132e3	vtg4qoo[1].js.2.dr	false		high
http://https://adobesparkpost.app.link/nfQW2NoCVeb	express[1].htm.2.dr	false		high
http://https://spark.adobe.co	{13BDDBCD-AD59-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false	• Avira URL Cloud: safe	unknown

Copyright Joe Security LLC 2021

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
65.9.66.89	spark.adobeprojectm.com	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404273
Start date:	04.05.2021
Start time:	21:18:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://spark.adobe.com/page/ql80qXs9cgl3o/
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:	6
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:	CLEAN
Classification:	clean0.win@3/32@2/1

Copyright Joe Security LLC 2021

Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://spark.adobe.com/?r=404

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\EQAWN5DV\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):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Reputation:	low
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\IB42RK38\www.adobe[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	26

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\IB42RK38\www.adobe[1].xml	
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aK1r0aKb:JFK1rFKb
MD5:	132294CA22370B52822C17DCB5BE3AF6
SHA1:	DD26B82638AD38AD471F7621A9EB79FED448A71C
SHA-256:	451ABBE0AEFC000F49967DABF8D42344D146429F03C8C8D4AE5E33FF9963CF77
SHA-512:	6D5808CAD199A785C82763C68F0AE1F4938C304B46B70529EA26B3D300EF9430AD496C688D95D01588576B3A577001D62245D98137FD5CD825AD62E17D36F15C
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{13BDDBCB-AD59-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8544858181680879
Encrypted:	false
SSDEEP:	192:rHZgZ629W4t3qf6T1rMSzN5Sr/bSDHUfSDj5Ti7X:r5w5U83oG1I6N5a/bCa0i7
MD5:	F2F8D3A1AF543051613C5A868850489F
SHA1:	49E3F72E929DC9F5E55549CCBB1CF86B2C3B971B
SHA-256:	8158736C5054DFB3BBF82A03A292BC0801FF6C837F7FF35C8097C953A29D5B49
SHA-512:	B5492C2BE2A0888ED3F99DEDA7174570F1FE8C3A509794FB7AEF60AD3F7662E49BC3A64F93DE2293EECBBE41F2FB0898B6CF0CB55386E4C33BC3242A88434E7
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\{13BDDBCD-AD59-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	38436
Entropy (8bit):	1.9253864727501795
Encrypted:	false
SSDEEP:	192:r7ZUQw6WkgjF26WgMoYR7rRcKLRQJ/91acPlQ6QDGwKQdjDQDVDtQEeg:rNdbXi851pRt+9qd/ev
MD5:	0BB5152DE431059AA0377DF011B2E06C
SHA1:	A73E4859239E9CDF1B08B53968DE81F8DD6671EC
SHA-256:	25A7CAD4C4BC9478C9D3BC747BF8559ABA03A5DACA7390D04E30308E6A5A3DB6
SHA-512:	A04B9CB3D1933AF7FE0DE699D23CAB5387B578EDB3179C945033137AE7E2944D9476955658C3E5E88F69EDB74F426BBF99C92867FC5847BEB1DDA2488E957B8
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\{1AABAF24-AD59-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5619011610195248
Encrypted:	false
SSDEEP:	48:IwhGcprUGwpaJG4pQ5GrapbShZGQpKVG7HpRwaTGIpG:rXZsQL6ZBShzAETweA
MD5:	0415F5E35BBCF76A1927BA505F2BC8E6
SHA1:	3F7309E95CF8CC3D4EFFD104575521386AF1FDA1
SHA-256:	1D38B92F17DA55EFDCAE23410E2AC354B3A65933960E0F323DE5345BC77F5CF5
SHA-512:	5124694F8A8C19AF047FB5FB2B168B28BCFABB4260FF09D16F969F059511520EDE34B290750764663A5E321157C8A9A33B356D93B08303489413BC3AD4BBF6DE
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1AABAF24-AD59-11EB-90E5-ECF4BB2D2496}.dat	
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\wlm7n14\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	9766
Entropy (8bit):	1.6435779311501328
Encrypted:	false
SSDEEP:	48:qrc7gzdbklTMl1sy6TMenl7ulGt/3GmjAA+:d70sI2NmU3GD
MD5:	D5A3A5AFB62136B46B7935CA55C430BF
SHA1:	FA4A601513B38BB626E4F2795526CC7573C54BB9
SHA-256:	C126AA57A97F1FBADF673D3ED50AA3EAD912A2996630CCA183F4B6EE5570E493
SHA-512:	423801DF482CF0F20D8DD64FBAB6050B675793EA5694D8F725E5A302E927A9EE6DD88C429DE4B6B7754726FBC19551FF3CA8F28222692D0F3D2A973D61782D65
Malicious:	false
Reputation:	low
Preview:	!.h.t.t.p.s.:./.w.w.w...a.d.o.b.e...c.o.m./.f.a.v.i.c.o.n...i.c.o..%.....00.... ..%.....(...0...`.... .....$.....A.....V.....'.....A.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\7O7MVXIS.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	226
Entropy (8bit):	4.932539664066224
Encrypted:	false
SSDEEP:	6:q50HFIHfBNLceWIAlWtKZDTVEX25MRJVx7uBEwLad0GL:m0Hi/JWImPZDZEX25Mxx7uBEpjL
MD5:	4694F3450C9406D96176366FE5288BCE
SHA1:	598B7D44048C31A32F62F1DD16115636A65CCB10
SHA-256:	154C0CA6448DEA5DFBB2025635CD28797BE4A8948184EDA3ACB2CDCC9F70B9F7
SHA-512:	0D318B8C9EDB27752773F2ECE41E8B9187F82771FD9554CB00A63D3997162581EC8FFACB96D13DF34AF59BC02246D8C67E42A4EA3C01CDC43FF0D0183865764
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spark.adobe.com/?r=404
Preview:	<html class="x5html" lang="en-US">.<head>. <title>Make Images, Videos and Web Stories for Free in Minutes | Adobe Spark</title>. <meta http-equiv="refresh" content="0;URL='https://adobe.com/express/'" />.</head>.</html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\d[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, CFF, length 67148, version 0.0
Category:	downloaded
Size (bytes):	67148
Entropy (8bit):	**7.993959168595968**
Encrypted:	**true**
SSDEEP:	1536:nxeF+rR7LkiELPhmOHVSAJTtSrsJBD7JVstEBSQm+aScA+tWB:wEkJzh7S2xysvPst2SQSSzR
MD5:	227960928668E1D655DBAAAE5FE23C11
SHA1:	128EF93AB71A18BA1DB0855C165D050ED8702037
SHA-256:	DFD5B4454E0BEF1EBBE0940DFA3BFB117BEE9E3DF150FA55BE633114816E7179
SHA-512:	BDB17CBB62E2C6B4AF737C7201214A563C27CDC38E1924B2C6EB351950F81A06A10E2DFDD783C82AB108D9758D77DA0A45BA82B08C210F4D8977A33AA6364B B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/4b3e87/00000000000000000000017706/27/d? primer=7cdcb44be4a7db8877ffa5c0007b8dd865b3bbc383831fe2ea177f62257a9191&fvd=n9&v=3
Preview:	wOFFOTTO...L.....BASE...X...F...Fe.].CFF ...T...G...CP...DYNA.....G9GDYN.....1...e. .GPOS.....#...S4...0GSUB...x.....0.OS/2.....Y...`^B{.cmap..... S.....lgasp.....head.....4...6..%phhea...(...!...$....hmtx.....x.nD.maxp...L.....^P.name.....]post..... ...2.....ideoromn..DFLT..cyrl..grek..latn..... ..U.....x.c`d```5.2)1O.....(.p>9..F.W.....5.....;...x...n.0....'E..}..{hZ..8...@29.....~hH....;t.#.....y..@.(.5.!.!....RW.....[x...G....65[.....z~..A.?X...rU.....s....#.....<{>F...| ..2.;X..<.P..1Z....}eu^..bi.)c.WR..L...Vb.+]..l.W...1..e:...,#.....z<.:.S.:.....E.....P*...c....T..6..T.. .d..HF.....X...v.~.....G.....9. .Bq\.FX.`.M.c....s..e....h.3v.....8.fH....4gM..+...X ..R....Y..KD....D.....?..=N.<..._.....y.....C...U....[.....~.IN.~.....W..{.\^;..?.._..a...T...t.....K.Y....}...2..x.c`f.`na`e``.b.```...q.F..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\d[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, CFF, length 66304, version 0.0
Category:	downloaded
Size (bytes):	66304
Entropy (8bit):	**7.993959805787878**
Encrypted:	**true**
SSDEEP:	1536:VeO6ShUivo8vaO8pnTzDOTXL/kxtcA+uDWB:p6DJWaO4iT7/4tzk
MD5:	9E6E819AE9D8993A2B10353EFF16497D
SHA1:	1410161D0CA8CA3966897CAB50E45A14B721C056
SHA-256:	81B4B3BC1EFD4F08F212308D9727BC21A40E38B5464B6B25EBDE1B2E24D13F05
SHA-512:	D9D88E8987EE2F45BFA0B211AAA7DFEB9C39718E9A037FAE625AF4E6806E04D4C8316B58363EEA93E9BA6C23B6F514925D4841C95CDFB103693688D5EFC71DAB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/40207f/00000000000000000000176ff/27/d?primer=7cdcb44be4a7db8877ffa5c0007b8dd865b3bbc383831fe2ea177f62257a9191&fvd=n3&v=3
Preview:	wOFFOTTO.....D.....BASE...X...F...Fe(].CFF ...T.....6...DYNA...P.....gG9GDYN...T.../...a... GPOS.....#...T.;..GSUB...0.....0.OS/2.....Y...`[.t.cmap.....S.....lgasp.....head.....4...6..%`hhea...(...!...$....hmtx.....x..].maxp...L.....^P.name.....8I.post..... ...2.....ideoromn..DFLT..cyrl..grek..latn.....`.....x.c`d```5.*{..9...+.3.....P..?.?....1 ....$..._.!x..An.@....I..jo0.>...!..$H.....`a{.=Ab.u.]...B..E..T..<...Y....3.{o...._.....k....x.....c.Mj.....f~..B.....9...s..A.V.....g.Mj.{>F...|..0.[.5>=.P..1X....}iuV..|n..)b..R..TL...b.K].X.R...M..!..H...?....N...N...p..x..21...wS.J.T.m...;.Jv..Y....e..B.....kk....o.&.rn....z~u...%. .Bq\..X.`.M.b.....)p...Y-.....r.L.`.5+..i>5.;.<..C3%'...U...X.....D..{.!F.~...8=..c.~y.{w.s.*.{..U.....*...._....~.j....*..)Sg.....R^:.u[v..m.....j.eJ.w.u.T.....Oy.s-..m.x..x.c`f.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 48x48, 32 bits/pixel
Category:	downloaded
Size (bytes):	9662
Entropy (8bit):	1.5933577223587498
Encrypted:	false
SSDEEP:	48:97gzdbklTMl1sy6TMenl7ulGt/3GmjAAp:970sI2NmU3GY
MD5:	B28BF60DD7E50B6DFFD394EBC0F9057A
SHA1:	9EA7EED87B689757780322989EF426AEFFDC8F7A
SHA-256:	BF24C9E4D37F94D4BD2F870228FF421CA54B2949DB3391DBD3818EC0E6DB0F5F
SHA-512:	B16A7F756E38FFE4BBCC0394A6E41593CC9FE68AACA6350C1C20D10E7A284EBFC7937C15726D0F43A3ABD7C43D128A041A109CAC2C8F240707FE1997E633E05
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/favicon.ico
Preview:	......00.... ..%.....(...0...`..... .....$..... ....A.....V.....'..... .....A.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\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
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/GenericCustomNamespace/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_ai;" 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\9QTQHWWN\media_102523b575492841801eee551ccfbc5fca141ecdf[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\media_102523b575492841801eee551ccfbc5fca141ecdf[1].png	
File Type:	RIFF (little-endian) data, Web/P image
Category:	dropped
Size (bytes):	1411
Entropy (8bit):	7.818219608643177
Encrypted:	false
SSDEEP:	24:siUhSf+2M0ZpZqCvr/ocRQAOFf/CfKj6jGvFy0PCEU+zQaqTHZ0VwUP:siUhA7LvrgUSJ/T+CvFycxU+lqTU
MD5:	772490EB047C5C65E7330F3FB6F5667A
SHA1:	0DDB87B9A34F56EA10A21A6380EB41A8D099F29B
SHA-256:	31A87540565B694BD962F57353178772EFFD54CE6EFCF8F8E69D1AF8D7D1AA66
SHA-512:	1E9B35BFAB3B32CDC0E224E208E6FB0A0508906E053F4538329580F3DB7291EC94409E317659DF0C88F1EF618D0FF6E78E7A45FE9FB9E94FE77D898121E3F033
Malicious:	false
Reputation:	low
Preview:	RIFF....WEBPVP8X.....a..;..ALPH.`....Gn$l.z).V$..pU...#.?..a.....D>.....~.....O..~...S>._..K.S1/Q.....f...P....J.X..I:Q.z..$.V.....8r.F.d.....{.{DL...=.&..3.DS...ie.`.....V?..V.h..j.....@C?..p.].n..$lg.R+...$\...$A.$....<.T...YDfF...EL.-....irC.p....&.{...m.h.>..II.q&..]...b]..w_....u..d..I.El.DR.\vf.....IV.h.O..s.{A..~c....$l..2....{.{.75f...U.!...TDH$..WD..d..t..@...A^..$.$ld....F.....xd.)..E"...6....Va.N.....#.....R.. ...$.$..~..".3..Q....3[.T._5.C.6m.B.Dc...s.s...".b....h..~.sc>{.>."l=.:..U."...@f.....,L.b.\.W.....).....ps.}.#D.n.<...d.....frd.....4.j.Zw...{;.p.DP...H6..}.P...+.5X<v..:.."....g[j.... .:/.&.'<.?yx.Ew..&}y..9g....S..=....s..*.[x..Z ?/..W8.....g...d{....m....C..5...=.D/.l..;`{Yf..ko.@.....RZ....._?.....m...E...D.....&...=P..<...4.hJ.\..#..1f..NF...7..>..A.7G.E.....p7>..m.....ma.sy..m..DF...3..@../..^.<.....4...L.<zJ./.!.bkX+8....J..#}...j...o...|..r.../W.i..O.P.. H.D9G.{

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\media_1a3a5d0b4d3b4cdafd28d6e4e2582aa89694802d1[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):	4558
Entropy (8bit):	7.958882710309189
Encrypted:	false
SSDEEP:	96:TlffEfmVIHeCGEiM71+w0aiQMH+8o7sBW1mJuF3xZN0ICzBjm11p9N4F:lfYmVcutM7Qw0zx+8oYspJN0IC01b4F
MD5:	052165C682929705609F7693A800066F
SHA1:	A29DA6BBCA865268645015C4669E6003197578AD
SHA-256:	DDCFB48F42BE1B0425CEF45361A5FD64F967484CD7925078A109B8522CA27644
SHA-512:	C1156D247C7AC6C512E92A91C0E322AAB2FF1F28A0AE6D93943678111CAF2E462AD45E93575439B36B2B749ABE5D30B41BAAB618E70A72ACB93B2840DA71D03 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/media_1a3a5d0b4d3b4cdafd28d6e4e2582aa89694802d1.png?width=2000&format=webply&optimize=medium
Preview:	RIFF....WEBPVP8 ....0a...*....>.>.!%.".(Rm`...in.K....g]_...R.........O...M.....r?K......N.....k.....?.x.j..`.....~..m....>.?.....j.z.....m.MS.v..6.&3c."..O8=BS..RA.....Po|.u.X.<.WAF;\..A.T.....7.o.L.....s..c....,...4....P....t....QK.6..9..>...'.....5.b..."_..&\W...R@..?+....O_U.1,...Z....`.|A.[..B....c..a..Z..."R.6.....L....D.l..`.n.a.7..W[^O....2...u...L?Q..Nx.V.@...8X'.....@.N.L..... t.y.....~...;.*..DZ0V.....['.....;..QS..[w.)..<.m.).....E.z.O...>.V..."L.....}..r@Y.9...a..o.x...'.!.6T....-ro....)~...h...,b5..+;.....F.....]...D.}.....6Wqj:.t..pe...8....zfB..z.U..9znLu..[..r4..e..D....a.....M..9.WY\tG..s.,<.~Y#...e..iM..k...3..K@.`;.0xf..#...QB...G..*..-K..&.AZ...b.W.C.n%..sB.sj}Zu....6.&..;^X...Xv.....V..&..;P.....Z....B.....0.....K.....*.....T.*g..u}.....\5<.uz8.Y5...+.Jo.....LD._.e....E)zp.[..r...x,F..I...._..*.{;.....{...?..7...V|C=x.*8...{`..r.k....g.9..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\media_1edd2ae4453e3478187f2c8b4963eb73bac41e495[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):	4344
Entropy (8bit):	7.952890511525727
Encrypted:	false
SSDEEP:	96:8AyF0DIrSu1GUbv8+oDJtGqT2n0axa5pd9Vbb9Se0x1A5z/:tK5bvMDKqT2XxaN9VfkXx+5z/
MD5:	1865D8BADE74D4ED8F4FD39F389A9330
SHA1:	829785B4A2D366B45F25AE9FE170B4C29AAF86D5
SHA-256:	B560317586E901FC12C86874B1D2F3A08B1B6A4FD620354EF7E86861965E90F0
SHA-512:	CF5FCE12AB037FDC05D2578D4E5E4CF58AB42CE5419A7197FAA0AEC48B9DA78E9E0183A3CE639DF039E12DEB2A0D795DD4A6F754103A8512829227A99A789AE3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/media_1edd2ae4453e3478187f2c8b4963eb73bac41e495.png?width=2000&format=webply&optimize=medium
Preview:	RIFF....WEBPVP8 .....d...*....>.D.I%.#!&5.....gn.p.....u.M.....G..r~`..'..y.y....@.#.F.....-._.....f.....-._.....=..I...^....;.O.k.B.?:...[.v@_.8o(.....5N.....LP.m...W.LP.m...W.FZ={Y?.qz.b.e.,N8...M....1z..d{,..~I.[.-..@..B.CE...Gv...!A{.02W\zC.+t.[{2....X.O\h...Y.I7...1@FdB+ DV.L.....K...`.O.....D...._.....6.f..}.D1R..o.....B.".D&<..<0jb...C6...%u.....<s.bX.xJ...]n...vO6~K.)..MOwJ..>.....-.X.J.....0/.F..d..e.hs9.L.I..4{X.R6..V9i..z4..k88..Ms.F.o.J.mD..#.w..#.7@.....p...a.....J%@.'..F<....M.....S.v...$.,.S.6.{..r.*.,...R..L . .?..D...Q-.. u5....{V.EE..L=D.v..R{.M.T.F.`9..c.....p.@....e.N.M..@b...\.j.M.H.....d....3....4.G.}.r...U.ws..?..x..iF.\.n../..y...H.0PJ.)s.....z.y..uJ.<.(...A.R.yU..OX.N.c.,.....h....:E.7.*W.Z`..P..&...O!.V..]...zF..hd.j..b..hd.j..b....Mf.?....e.[.r..[(.D_..lS|.?..$..|..Jh.w...j.]..............ye.dH!..e..[xB.....U3M.N.....>>FL$\`..;9.u..'...m.NB....s..i..}.b.\0y$..P.....C.pt.x?h...^...q..%V.1.~.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\p[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\p[1].gif	
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&_=1620188370470
Preview:	GIF89a.....,.....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\scripts[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text
Category:	downloaded
Size (bytes):	36369
Entropy (8bit):	5.028473190816657
Encrypted:	false
SSDEEP:	384:U1qVZSpe137a6wbqWcqS5G399ahCqAUaww3boPOGGuh3f3ntOX4jQt41gvUxUPCr:UMZPjwfuVP0GLB1a4j/b4g
MD5:	696D0CC440A9A38E23EE9B7B623060B8
SHA1:	70D6991B1983E3B7D1777429533C060982799FF6
SHA-256:	338460BD7A0F7D02FBE0808DBD34F9B6062313EB86A82CE37355829C73BC7B23
SHA-512:	191E2DDFCB32CB46730353764CE3DA83DF020623537F21348EF347437D15BAE5830C1F05FE4856289E6ACEF36799BA01F661C5C4EE6D384626D30B61CA3000BA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/scripts/scripts.js
Preview:	/*. * Copyright 2021 Adobe. All rights reserved.. * This file is licensed to you under the Apache License, Version 2.0 (the "License");. * you may not use this file except in compliance with the License. You may obtain a copy. * of the License at http://www.apache.org/licenses/LICENSE-2.0. *. * Unless required by applicable law or agreed to in writing, software distributed under. * the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR REPRESENTATIONS. * OF ANY KIND, either express or implied. See the License for the specific language. * governing permissions and limitations under the License.. */* global window, navigator, document, fetch, performance, PerformanceObserver,. FontFace, sessionStorage, 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\9QTQHWWN\sparkle[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=1, copyright=prasongtakham - Fotolia], baseline, precision 8, 1048x1220, frames 3
Category:	downloaded
Size (bytes):	343155
Entropy (8bit):	7.955083951473548
Encrypted:	false
SSDEEP:	6144:n/e86Bp6ZeijUctZWrbLqujo+JDXk6Znj17kumuYzPgb7B5vJZ75Fp4L9so:nm8Wp6ZeiAu0b/o+JD9nj17k3uJb7BLc
MD5:	AB8CE04630449D7E879067D69E50866C
SHA1:	BCEFB08C972A510CAFB7CFED4A95DD752A69AEB6
SHA-256:	36C2625BEC8642B8109C72C20D2A44285855C47705B6E08A34748D61A6041A70
SHA-512:	A481487C66CDA05CE54A204DA144D83E4F8ACCCDE58934A0796B05A75C23BE5DA7FA5E200FBE4C46DED8477376E87E49F1EDBB478AEEC093F5BEFE38C0A6A617
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spark.adobe.com/images/sparkle.jpg
Preview:	.....<Exif..II*.....prasongtakham - Fotolia.....Ducky.....P.....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-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: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/" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" xmpMM:OriginalDocumentID="B4B5CF0DC2EF4C5E356A23E0E117F0E3" xmpMM:DocumentID="xmp.did:EFDF917F158711E69DE3C69564F4666D" xmpMM:InstanceID="xmp.iid:EFDF917E158711E69DE3C69564F4666D" xmp:CreatorTool="Adobe Photoshop CC 2015 (Macintosh)" photoshop:AuthorsPosition="Christmas sparkler on black background. Bengal fire"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:6FB0B9F9158711E69DE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\vtg4qoo[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\vtg4qoo[1].js	
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
IE Cache URL:	http://https://use.typekit.net/vtg4qoo.js
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/00000000000000000176ff. * - http://typekit.com/eulas/00000000000000000017706. * brandon-grotesque:. * - http://typekit.com/eulas/00000000000000000132df. * - http://typekit.com/eulas/00000000000000000132e3. * - http://typekit.com/eulas/00000000000000000132e1. *. * . 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\G62TDH9B\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:	downloaded
Size (bytes):	5713
Entropy (8bit):	7.942941105430185
Encrypted:	false
SSDEEP:	96:swygmCeFV57fd/hMb1uJRyaYyg+1Qao2SqFf93sdo89lxzUwp:fCFV571hMxuJUaYZxa9SqFfhsdr9l1UQ
MD5:	95FC22E047BCEB4BFA6AEE7064399BBC
SHA1:	11A708485B7942104D06F2FFD0F1B6713F25F941
SHA-256:	C91BD804CF36B68D89EAE5FAC4CD8F985563D322273462AF92607AB9927002F1
SHA-512:	2C26049C9A7CDCD17F75DCFB70502D28E397E27F296F5267C6478B2D4F4D263D7584AD772ED3E1C12C7FC42110260B0DCF41694DE881260B92D3E615D9BED8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/icons/adobe-spark.png
Preview:	.PNG.....IHDR...+...;.....#.....sRGB.....8eXIfMM.*.....i.....+.....;....D.....IDATx.._.$.].....q...H,.v,L...E!.P..R.@7'....}. ..R....3.....1.hg.P..CBA...EB. .P..'6!.>..uO....gfwgv.._..W..V...k.....s..../8...<..,.].....w.y.....9.7KaX4""..X....I..s....p.N..\....?8..+gy48"...!0.pT...W`.dNr5...8.WV..huD "..8rV,..,.....".....U.MD.|!.8._p.....:....Y...s. {.....:E.....,}....=..J..Gn..s/....u...U.....8.og...z..u...q...#....@."..k.a..VR.._K.....Y...i.|.e.~.4.eF."..#.=..._jh`.].[#E.".+..E...W..Lffu....."E."....~I....:g....7".L.$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\G62TDH9B\d[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, CFF, length 66740, version 0.0
Category:	downloaded
Size (bytes):	66740
Entropy (8bit):	**7.99411972026963**
Encrypted:	**true**
SSDEEP:	1536:J4lzR3d/ZD6MCYkk+e5Hj9EgKWB/uS7wcA+vVWB:ql9NZ/CYFjjKgKU/uLzh
MD5:	02BDAC466185E4E1161BBFAB2C066327
SHA1:	5C0C5E8BDB41694C8AD5605D5C1FFF7EB0702EBA
SHA-256:	AC44BE8F65384DEF37D9091D668E54A4B79AB6A3156C5D8CFBD3268BEC558971
SHA-512:	01C761222E6DB3A3F81DAD88191BAA8A020536C4F8EF8692796B94C68AB1FDD4EF672D8DB24336E12BA32F0F96079E9D388EFD93433E9FF62BB8976596F65CD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/cb695f/00000000000000000017701/27/d? primer=7cdcb44be4a7db8877ffa5c0007b8dd865b3bbc383831fe2ea177f62257a9191&fvd=n4&v=3
Preview:	wOFFOTTO.....BASE...X...F...Fe$].CFF ...H...a.....w..DYNA.....$G9GDYN.....-...a./..GPOS.....#...T<"9.`GSUB.....0.OS/2.....Y...`\Wv.cmap...`. ..S.....lgasp.....head.....4...6..%uhhea.....!...$....hmtx...h.....x7wW.maxp...@.....^P.name.....post...L..... ...2.....ideoromn..DFLT..cyrl..grek..latn..... .....\.....x.c`d```5.z...1...+.3.....p..?.?/K... ....$...A.!x.RKn.0..9N...Qt.5.v..R 8.Wv..Y%...%.....0...]t.S...@G...M..!q.{3C.Q....<t.o.=.a...^a...>...>9....a.....J..... O.=..b.{.x{.....p.....~8|.....$....:..U.h.84F...e].ul.J.I...f..F.u.....2.q1..,.#...xr5..m..N].....N...D..].P*..ii.e...Trx6.....6I(#...z..S]..9Tz.1rY.f....'..U.G..P..D..P".&^....8..,x].....7..... e..sl.F.Jc#.Y..s...Th.....aL.....E...t..(;..U...;....,.....^H...LJ..g.x.A^[....X..._.g6.kb..}G..%.n.e.....}.X....]?g^;~C.^4..t...<...x.c`f|.8.....).....B3.1.1*.E.Y..XX..X.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\d[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, CFF, length 66508, version 0.0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\d[2]	
Category:	downloaded
Size (bytes):	66508
Entropy (8bit):	**7.994636853689064**
Encrypted:	**true**
SSDEEP:	1536:4p7762bluKjsVQJU/x14nXWjvxpGeDKTeEPiBlnQcA+yWB:q362bluKjqQWr4nG7xpP2PiEz0
MD5:	49B061D6468547558176037211AA630C
SHA1:	B02FD5987ED77AF837699BB13C7E838018943423
SHA-256:	F89C62C68380B4BB548E4E24E284348FE9E98730F54F7E0C8942F6AA3BE9DA37
SHA-512:	406D0D0BF1A669E16B9CA101B2DA10C222BBB780DF7B2CB235E2C9F765351846F2A94044C55B0080B875E951FC87462A76B29BE8CD4605EB4D462D321347A49(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/eaf09c/00000000000000000017703/27/d?primer=7cdcb44be4a7db8877ffa5c0007b8dd865b3bbc383831fe2ea177f62257a9191&fvd=n7&v=3
Preview:	wOFFOTTO.....BASE...X...F...Fe!].CFF ...L.....dX.\\DYNA.....GG9GDYN.....1...a....GPOS...P..#...THAH.5GSUB.....0.OS/2.....Y...`].y.cmap...x...S.....lgasp.....head.....5...6..%ghhea... ...!...$....hmtx.....xg.P.maxp...D.....^P.name.....E..post...d..... ...2.....ideoromn..DFLT..cyrl..grek..latn.....Y.....x.c`d```5._.._<..W.f..@....^0....~.).....@.....N...x...n.@.....!.V,.@.cGV.FB$m..j.H..6N<i..`O#...@..X.$<.....#g.....x....^}.-.x.S..t1.|.....,=.b.....S.J|...e..s.O.....;.]>z>D.|.|.W...1...R.b.....}muQ..ra...R.3)Fy.....T..1...s..c.g...d8..O....'M.....FW...-...X*..+c...H*....t..].|=.e"..R.....o.fm.....:T.^Q..z...c(.S.....a..w.KN{.l...M]..tu9...k.b.L.N...v...Y..R.[0....1...C*/..8.^...GM..r....jvfx..<.o..t.P.....=Kv-.kr..n.....5.%.9].>q.....f:.3<C.e9.-5.:Yz4O....:e....+b.}.oS..1x.c`f.....).....B3.1.1..E.9..XX

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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):	5.327769834291597
Encrypted:	false
SSDEEP:	96:386R0lH1UHaxH1UPCR0m+ydgW3+y6aSH1UPr+ymTimsDY4WjlGTLzmYaq/XYXg0X:38s0lSaxQU0vydSy6aSQCym0pU/XYXHH
MD5:	2B51B2A95E670886D5FE8F6BA31D15C0
SHA1:	8D0BF64A9D4F43915E76A51883582716E0B6BB0E
SHA-256:	CB03E38789436048C334D1E7A8F63D2490062E70A9B42A81DB82D28EBE001BD4
SHA-512:	8F3A3F417B8E5D8424F41649B72DB5488211ADD30ED0C81E12C4356BC684D335A1B5892DFE6972AD536BE8421B6D26C253D8EA8078D300E783733168EBA168C(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.adobe.com/express/
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\G62TDH9B\sparkle-mobile[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=1, copyright=prasongtakham - Fotolia], baseline, precision 8, 800x853, frames 3
Category:	downloaded
Size (bytes):	199797
Entropy (8bit):	7.959176396571337
Encrypted:	false
SSDEEP:	6144:YqiP+QzbMseCbkcVq0lSe7mplYuOKaLYoLtyeJHNCx:RiLMsbbkcF3YLOKalLtyeJHNE
MD5:	C593E1A3F325847A5323407D0541A6D8
SHA1:	D0C6050C396DEDCAD0C555B36ED9C6F1561B590E
SHA-256:	F401189E1BF233A2F84B43B9606182C8924556330A93E26421FAC5BF672071E4
SHA-512:	22AAC37CFA9208D404F347E3D7534A7E8146B05E2913689D120E3C136C5BA743E562B7BA278B08792DD68AE9EF2C3097BADD6AA9091661F60EF71A710C9D771(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spark.adobe.com/images/sparkle-mobile.jpg
Preview:	.....<Exif..II*.....prasongtakham - Fotolia.....Ducky.....P.....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-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: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/" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" xmpMM:OriginalDocumentID="B4B5CF0DC2EF4C5E356A23E0E117F0E3" xmpMM:DocumentID="xmp.did:6FB0B9FE158711E69DE3C69564F4666D" xmpMM:InstanceID="xmp.iid:6FB0B9FD158711E69DE3C69564F4666D" xmp:CreatorTool="Adobe Photoshop CC 2015 (Macintosh)" photoshop:AuthorsPosition="Christmas sparkler on black background. Bengal fire"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:dc9dbb5c-aa4f-4c3c-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\d[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\d[1]	
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:	DA09A18AED6A3C44F5009410D03623A8200ABF224AF33DDBFE34D3736AF96C6847D7A9A1CF0D94839C9ABB9546E1C7F5BCF6C305132B97BEFBD84A535F1399 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\OTUW0Q90\d[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 24744, version 0.0
Category:	downloaded
Size (bytes):	24744
Entropy (8bit):	7.978627515034273
Encrypted:	false
SSDEEP:	384:EVkksCq/KOwmOt8IEOsyhgjzfwTJsPj6V9teCsx/Abr2k88CDW001VEKHUM7Ozip:qktXUt8he8UheCsx/AhKW0CUUV
MD5:	A14F6E1E3181DC10FDB66D2A7FB54CA7
SHA1:	605808488DD7FEC481400AA948F80E66189D25B5
SHA-256:	A4B8520DF89E973A968FCD3CF78F742E073EA9645D03ACCF360EB4AB5E6E1001
SHA-512:	E741918EF1EC6A3C0B87D996245945AEA9DB8C7D798352756F409A5E519BBF89EBF8F6AFA1E1A71D5C24C4E1C364F7C2EF38622C0897F852C6E9C7E6C27BBE 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/1da05b/00000000000000000000132df/27/d? primer=7a5a436c948772f5260024dfadc8f7cd849e1448f8bf41ba74a247e8e46f3aee&fvd=n4&v=3
Preview:	wOFF.....`.....l.....DYNA...$.....D..GDYN.....L.i.GPOS.....G..9..OS/2.....[...`|.M.VDMX.....l.tPcmap.._.....!k`Tcvt ...H.....tfpgm...`.....s .Y.7gasp...d.....glyf..&...4...e..V .head...l...4...6..M.hhea.....$....hmtx..Z.....(.G$nloca..\.....Jmaxp..... ... ...nname.....!.,post..^t..l.....moprep...T...2...2.. ..x...S.X..D.s.X...Vc....jl5....m.m{:...3.....#..C.P..WB..!..K8}...'.>...6".l$"....b....F4}$*.m4b...ic...$....866q..8.q.o.@o.OB..DzCB..D$..I..$!.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\OTUW0Q90\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 l.....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..l.5.....AQA.....e..4.(....Q@l.F.1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\marvel-error[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):	924
Entropy (8bit):	5.029738060904558
Encrypted:	false
SSDEEP:	24:ahn5WpBEtrbpBTVaMFwM9GLkxpVEC5WpBxGmKiE:ahn5sEtrbpS2wSyA55sQ//
MD5:	79B47B015C1477CD1BD76054F7714790
SHA1:	F2A370BFAE9826864EE658D08C7096309258674D
SHA-256:	19236BBB9A1AD33D606EBBFF8140BB11EAE1B00325BBC79328AA4C84D3A5F8F1
SHA-512:	2081D83CEB4F2C725CA09DDD41FB806E7622B7BE19BE4A77FF9DFBF2E5331C01D843F7A40402FE648DBFFCE1650E88478987BE16D11E891C8B95A801472B96E7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://spark.adobe.com/css/marvel-error.css
Preview:	html{font-size:20px;font-family:adobe-clean,Helvetica,Tahoma,sans-serif;color:#fff;background-image:url(../images/sparkle.jpg);background-position:100% 0;background-repeat:no-repeat;background-color:#010101;background-size:contain}body,html{height:100%;margin:0;padding:0}#shim{min-width:100%;min-height:100%;background-color:rgba(0,0,0,.2)}#content{padding:2rem;width:20rem}h1{font-size:2rem;font-weight:600;line-height:1.1em;margin:0 0 1rem;font-family:brandon-grotesque,adobe-clean,sans-serif}h2,p{font-size:1rem}h2{font-weight:100}h2,p{margin:0 0 1rem}p{font-weight:400;line-height:1.4em}li{padding-bottom:.4em}a{text-decoration:none;color:#ffda00}#copyright{color:#fff;opacity:.8;font-weight:100;font-size:.8rem;margin-top:1rem}@media only screen and (max-width:800px){html{background-size:cover;background-image:url(../images/sparkle-mobile.jpg);background-position:-72%}#content{padding:1rem;width:80%;margin:0 auto}}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\media_1414f90572f278eae7d49cf2222e9b7d0063180cd[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	dropped
Size (bytes):	11032
Entropy (8bit):	7.971910061017487
Encrypted:	false
SSDEEP:	192:OvaQ0itv25JIQNCSCNXgB1dbwIAKlf0AT4CdwFi3yhfEheV7dpPPKeQgE:OvftCIQ6NQnNhnJGFi3CEg7pPogE
MD5:	160AAF0C588420621064BB8B738D0759
SHA1:	93DA63EC7D8E6EBC2DDB8F8552855A9DE0E51435
SHA-256:	AA1D8FC359B75F9C0E622A3F74859AA3CC3C77B0F60FBEE5F86C869AD80FE96C
SHA-512:	94EA9D6B7BC35EA6B87E2951FD5651CAF144E0B399CCD29C3D946842015D8013E6B189EEBB2B676E0E81C4F3F6CDFB9EDD57C278E3F80F19810AD157A43B284
Malicious:	false
Reputation:	low
Preview:	RIFF....WEBPVP8X.....ALPH.S....X...mj...&|.....<.".?.#R.....5.....|.#..R..J...J.M..I "..]........4...."..}.:..PD'1Q.Py..O.7^.t..0.....$e\..$.:P.M,.j.t..Z.T.ng=(..p.R.G0.`.Lf..#....m.HR.]..........R..Tq^.&'g..4=c.N.,...i.U.....YMP..M..Q.$9n$!..o.4..$.P@.!v#&..d[m.'Dy..r.]....y..M.d....&/f^..._.....9.>..TM...-.A..I.ms...%.s.:....b.....d..~3..1..ql.}...=W.o..m{.[3kf.Aw.R?~".Y.....DD.,.v.FA.....h..84u`..A.+..4..a...../..q...rp..+.`..Xd.....G.a....sv0yV.\Q.r..B.....'.<)!~..\...O.... .....4.........{..^.]0~s..a.LN%....*.7N..h.........u.!...x.F?..jZ.fE...q.....V..J..g-sz8)*.."@.?...;=..Sr....8..wN.{...X...G.....Y...N!'.>cy.....k-s6>.x..x<..VV..W\..pP....!.(..8.a>\.Q.../...A(Y.....q.....].-!...n..B...%.B3....*f.'u.AS.....m..k.t...o.....\...\...R].sj5\.'.[b.....V..y.....Y....c.+..9..`....E...Y...D- kX....0=.....9..U.U. ....m...N...z...F;.I.j...C1/.#.7e...K.>J.i..%...0Y...v*...[.N....P@....M.....5l

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\styles[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
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
IE Cache URL:	http://https://www.adobe.com/express/styles/styles.css
Preview:	body {. font-family: 'adobe-clean', 'Adobe Clean', sans-serif;. background-color: #FFF;. color: #232323;. margin: 0;. padding: 0;. display: none;.}..body.appear {. display: block;.}../* gnav placeholder */..header {. box-sizing: border-box;. border-bottom: 1px solid #EAEAEA;. height: 153px;. background-image: url(/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 {.

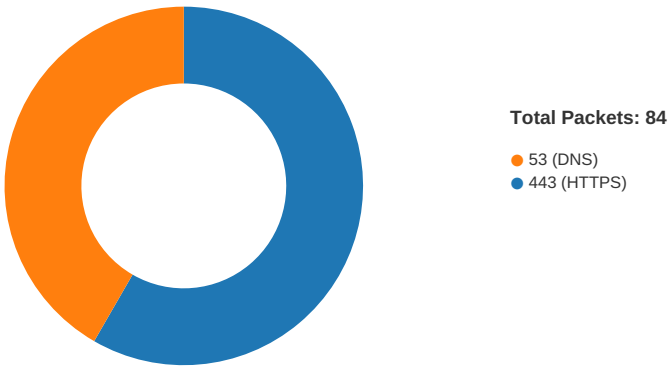
C:\Users\user\AppData\Local\Temp\~DF88ABC3EC2C072926.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4795079618992878
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loO9lo+9lW9LG49848OKYC:kBqoIJf3JDjC
MD5:	C203DCBBCCDE77DA4CB1989C5B6218A3
SHA1:	89710CACE5B312CD789157B59DDCA16DD22ED342
SHA-256:	75A3D8F80F55AF3E5CC17E2AD1C090541C997D8A283E4AE748213098065209CA
SHA-512:	618A9EDB2FE53CE09F209A765399CBE54EEBF1AC6E195DB213CB9889468357BD9B58595B85A7C9BABAFFFFD06DA8904F2251852107F3450D04DBF83DF71B436F
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-21:19:23.841240	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-21:19:23.876219	ICMP	449	ICMP Time-To-Live Exceeded in Transit			84.17.52.126	192.168.2.6
05/04/21-21:19:23.879850	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-21:19:23.916971	ICMP	449	ICMP Time-To-Live Exceeded in Transit			5.56.20.161	192.168.2.6
05/04/21-21:19:23.918132	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-21:19:23.954289	ICMP	449	ICMP Time-To-Live Exceeded in Transit			91.206.52.152	192.168.2.6
05/04/21-21:19:23.955181	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-21:19:27.947924	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-21:19:31.950697	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-21:19:35.949169	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-21:19:39.949139	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-21:19:44.193694	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-21:19:47.949801	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-21:19:51.950900	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-21:19:56.580972	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-21:20:00.451246	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-21:20:05.002628	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:19:29.424854040 CEST	49718	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.424860001 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.465289116 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.465461016 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.466023922 CEST	443	49718	65.9.66.89	192.168.2.6

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:19:29.466125011 CEST	49718	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.477466106 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.477747917 CEST	49718	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.517931938 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.518037081 CEST	443	49718	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.518090010 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.518107891 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.518182039 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.518246889 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.523978949 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.524091005 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.573962927 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.581975937 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.582223892 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.615988016 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.617367029 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.617408037 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.617438078 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.617463112 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.618470907 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.623554945 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.623578072 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.623636007 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.624149084 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.658912897 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.686976910 CEST	443	49718	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.687020063 CEST	443	49718	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.687088966 CEST	49718	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.687115908 CEST	49718	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.689364910 CEST	443	49718	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.689444065 CEST	49718	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.693439960 CEST	49718	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.693830013 CEST	49718	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.733845949 CEST	443	49718	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.734112978 CEST	443	49718	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.744318008 CEST	443	49718	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.744338036 CEST	443	49718	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.744395018 CEST	49718	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.744421959 CEST	49718	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.745270967 CEST	49718	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.788077116 CEST	443	49718	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.931777954 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.931830883 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.931847095 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.931865931 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.931899071 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.931935072 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.932979107 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.933005095 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.933043003 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.933072090 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.934025049 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.934061050 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.934097052 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.934127092 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.935175896 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.935199976 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:29.935237885 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:29.935273886 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:30.035300016 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:30.075820923 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:30.081435919 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:30.081522942 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:30.081535101 CEST	443	49717	65.9.66.89	192.168.2.6

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:19:30.081587076 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:30.447011948 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:30.487381935 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:30.549091101 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:30.549118042 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:30.549231052 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:30.549529076 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:30.549546957 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:30.549588919 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:30.549626112 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:30.550704002 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:30.550728083 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:30.550774097 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:30.550792933 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:30.551810026 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:30.551834106 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:30.551863909 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:30.551886082 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:30.552964926 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:30.552989960 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:30.553034067 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:30.553051949 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:30.554069996 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:30.554094076 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:30.554152012 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:30.554167032 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:30.555217028 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:30.555238962 CEST	443	49717	65.9.66.89	192.168.2.6
May 4, 2021 21:19:30.555284977 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:30.555327892 CEST	49717	443	192.168.2.6	65.9.66.89
May 4, 2021 21:19:30.556381941 CEST	443	49717	65.9.66.89	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:19:20.080442905 CEST	60342	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:20.132062912 CEST	53	60342	8.8.8.8	192.168.2.6
May 4, 2021 21:19:21.007925987 CEST	61346	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:21.057579041 CEST	53	61346	8.8.8.8	192.168.2.6
May 4, 2021 21:19:21.945843935 CEST	51774	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:21.994668007 CEST	53	51774	8.8.8.8	192.168.2.6
May 4, 2021 21:19:23.100554943 CEST	56023	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:23.149233103 CEST	53	56023	8.8.8.8	192.168.2.6
May 4, 2021 21:19:23.761771917 CEST	58384	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:23.826944113 CEST	53	58384	8.8.8.8	192.168.2.6
May 4, 2021 21:19:24.326505899 CEST	60261	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:24.379858971 CEST	53	60261	8.8.8.8	192.168.2.6
May 4, 2021 21:19:25.538597107 CEST	56061	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:25.587310076 CEST	53	56061	8.8.8.8	192.168.2.6
May 4, 2021 21:19:26.575781107 CEST	58336	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:26.624511957 CEST	53	58336	8.8.8.8	192.168.2.6
May 4, 2021 21:19:27.914014101 CEST	53781	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:27.972896099 CEST	53	53781	8.8.8.8	192.168.2.6
May 4, 2021 21:19:28.168101072 CEST	54064	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:28.225626945 CEST	53	54064	8.8.8.8	192.168.2.6
May 4, 2021 21:19:29.342041969 CEST	52811	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:29.382855892 CEST	55299	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:29.407989025 CEST	53	52811	8.8.8.8	192.168.2.6
May 4, 2021 21:19:29.434315920 CEST	53	55299	8.8.8.8	192.168.2.6
May 4, 2021 21:19:30.062124968 CEST	63745	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:30.120755911 CEST	53	63745	8.8.8.8	192.168.2.6
May 4, 2021 21:19:31.314312935 CEST	50055	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:31.373014927 CEST	53	50055	8.8.8.8	192.168.2.6
May 4, 2021 21:19:31.850470066 CEST	61374	53	192.168.2.6	8.8.8.8

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:19:31.899132967 CEST	53	61374	8.8.8.8	192.168.2.6
May 4, 2021 21:19:32.937266111 CEST	50339	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:32.986105919 CEST	53	50339	8.8.8.8	192.168.2.6
May 4, 2021 21:19:34.311631918 CEST	63307	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:34.360912085 CEST	53	63307	8.8.8.8	192.168.2.6
May 4, 2021 21:19:35.398838997 CEST	49694	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:35.447650909 CEST	53	49694	8.8.8.8	192.168.2.6
May 4, 2021 21:19:40.766297102 CEST	54982	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:40.817517996 CEST	53	54982	8.8.8.8	192.168.2.6
May 4, 2021 21:19:43.726123095 CEST	50010	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:43.777686119 CEST	53	50010	8.8.8.8	192.168.2.6
May 4, 2021 21:19:46.100318909 CEST	63718	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:46.159532070 CEST	53	63718	8.8.8.8	192.168.2.6
May 4, 2021 21:19:46.168098927 CEST	62116	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:46.219646931 CEST	53	62116	8.8.8.8	192.168.2.6
May 4, 2021 21:19:47.748469114 CEST	63816	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:47.797012091 CEST	53	63816	8.8.8.8	192.168.2.6
May 4, 2021 21:19:50.181298018 CEST	55014	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:50.249802113 CEST	53	55014	8.8.8.8	192.168.2.6
May 4, 2021 21:19:50.396979094 CEST	62208	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:50.477375031 CEST	53	62208	8.8.8.8	192.168.2.6
May 4, 2021 21:19:50.665829897 CEST	57574	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:50.714833975 CEST	53	57574	8.8.8.8	192.168.2.6
May 4, 2021 21:19:57.451323986 CEST	51818	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:57.500381947 CEST	53	51818	8.8.8.8	192.168.2.6
May 4, 2021 21:19:57.894099951 CEST	56628	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:57.945606947 CEST	53	56628	8.8.8.8	192.168.2.6
May 4, 2021 21:19:58.804778099 CEST	60778	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:58.854065895 CEST	53	60778	8.8.8.8	192.168.2.6
May 4, 2021 21:19:58.903506994 CEST	56628	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:58.955224037 CEST	53	56628	8.8.8.8	192.168.2.6
May 4, 2021 21:19:59.809660912 CEST	60778	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:59.860707045 CEST	53	60778	8.8.8.8	192.168.2.6
May 4, 2021 21:19:59.922667027 CEST	56628	53	192.168.2.6	8.8.8.8
May 4, 2021 21:19:59.974107027 CEST	53	56628	8.8.8.8	192.168.2.6
May 4, 2021 21:20:00.825419903 CEST	60778	53	192.168.2.6	8.8.8.8
May 4, 2021 21:20:00.874016047 CEST	53	60778	8.8.8.8	192.168.2.6
May 4, 2021 21:20:01.935656071 CEST	56628	53	192.168.2.6	8.8.8.8
May 4, 2021 21:20:01.987121105 CEST	53	56628	8.8.8.8	192.168.2.6
May 4, 2021 21:20:02.999303102 CEST	60778	53	192.168.2.6	8.8.8.8
May 4, 2021 21:20:03.049530983 CEST	53	60778	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 21:19:30.062124968 CEST	192.168.2.6	8.8.8.8	0xed86	Standard query (0)	use.typekit.net	A (IP address)	IN (0x0001)
May 4, 2021 21:19:31.314312935 CEST	192.168.2.6	8.8.8.8	0x8bf1	Standard query (0)	p.typekit.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:19:29.407989025 CEST	8.8.8.8	192.168.2.6	0x705a	No error (0)	spark.adobeprojectm.com		65.9.66.89	A (IP address)	IN (0x0001)
May 4, 2021 21:19:29.407989025 CEST	8.8.8.8	192.168.2.6	0x705a	No error (0)	spark.adobeprojectm.com		65.9.66.74	A (IP address)	IN (0x0001)
May 4, 2021 21:19:29.407989025 CEST	8.8.8.8	192.168.2.6	0x705a	No error (0)	spark.adobeprojectm.com		65.9.66.79	A (IP address)	IN (0x0001)
May 4, 2021 21:19:29.407989025 CEST	8.8.8.8	192.168.2.6	0x705a	No error (0)	spark.adobeprojectm.com		65.9.66.47	A (IP address)	IN (0x0001)
May 4, 2021 21:19:30.120755911 CEST	8.8.8.8	192.168.2.6	0xed86	No error (0)	use.typekit.net	use-stls.adobe.com.edgesuite.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:19:31.373014927 CEST	8.8.8.8	192.168.2.6	0x8bf1	No error (0)	p.typekit.net	p.typekit.net-v3.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:19:46.159532070 CEST	8.8.8.8	192.168.2.6	0xfd82	No error (0)	spark.adobeprojectm.com		65.9.66.89	A (IP address)	IN (0x0001)
May 4, 2021 21:19:46.159532070 CEST	8.8.8.8	192.168.2.6	0xfd82	No error (0)	spark.adobeprojectm.com		65.9.66.74	A (IP address)	IN (0x0001)
May 4, 2021 21:19:46.159532070 CEST	8.8.8.8	192.168.2.6	0xfd82	No error (0)	spark.adobeprojectm.com		65.9.66.79	A (IP address)	IN (0x0001)
May 4, 2021 21:19:46.159532070 CEST	8.8.8.8	192.168.2.6	0xfd82	No error (0)	spark.adobeprojectm.com		65.9.66.47	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 21:19:29.523978949 CEST	65.9.66.89	443	192.168.2.6	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 4, 2021 21:19:29.689364910 CEST	65.9.66.89	443	192.168.2.6	49718	CN=spark.adobe.com, OU=IT, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jun 05 02:00:00 CEST 2020 Fri 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 4, 2021 21:19:46.248049974 CEST	65.9.66.89	443	192.168.2.6	49730	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	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					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

● iexplore.exe
● iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 4316 Parent PID: 792

General

Start time:	21:19:26
Start date:	04/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	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	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: 5848 Parent PID: 4316

General

Start time:	21:19:27

Start date:	04/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4316 CREDAT:17410 /prefetch:2
Imagebase:	0xb50000
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

Copyright Joe Security LLC 2021