ID: 433372
Cookbook: browseurl.jbs
Time: 17:48:53
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

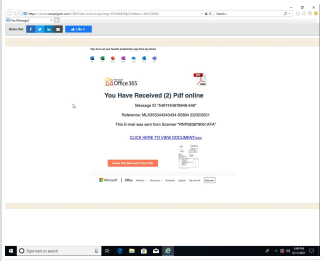
Analysis Report https://secure.campaigner.com/CSB/Pu…

Overview

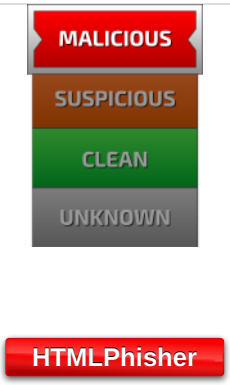
General Information

Sample URL:	http://https://secure.campaigner.com/CSB/Public/archive.aspx?args=NTIxMzE2MjA%3d&acc=NzY2ODM4
Analysis ID:	433372
Infos:	

Most interesting Screenshot:



Detection



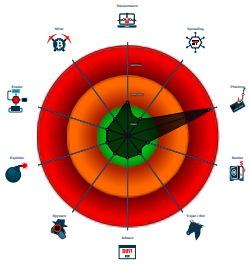
HTMLPhisher

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Phishing site detected (based on sh…
- Yara detected HtmlPhish10
- Yara detected HtmlPhish7
- Phishing site detected (based on log…
- Phishing site detected (based on va…
- Found iframes
- HTML body contains low number of …
- HTML title does not match URL

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 6112 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 2476 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6112 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

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

Phishing:

Phishing site detected (based on shot template match)

Yara detected HtmlPhish10

Yara detected HtmlPhish7

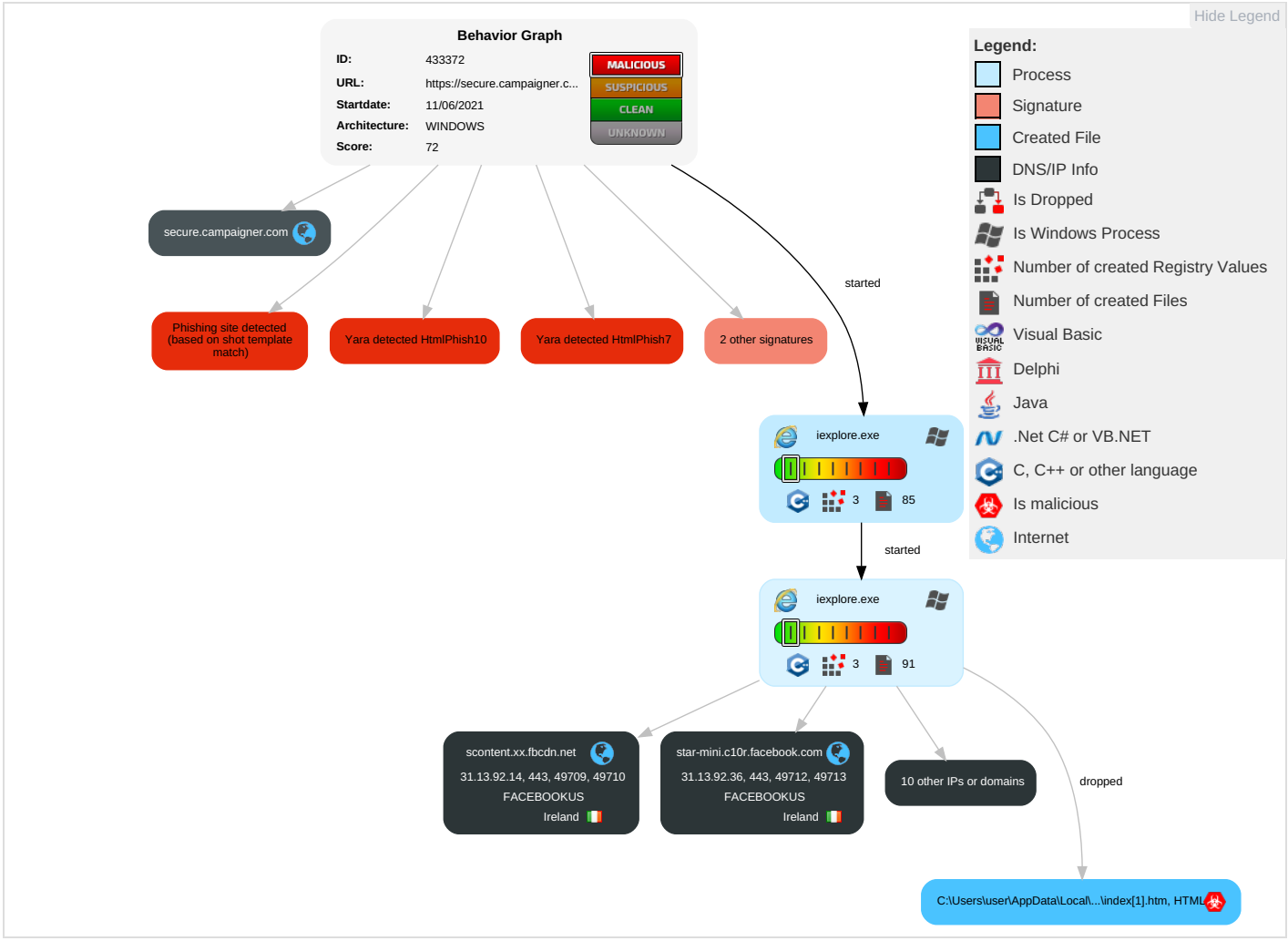
Phishing site detected (based on logo template match)

Phishing site detected (based on various OCR indicators)

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
Drive-by Compromise 1	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
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
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

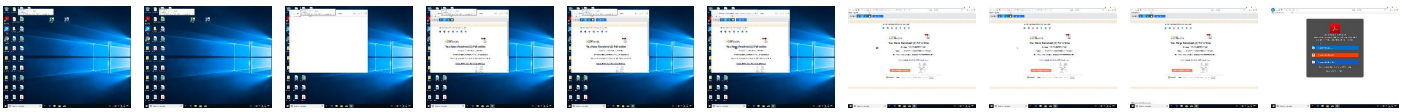
Behavior Graph

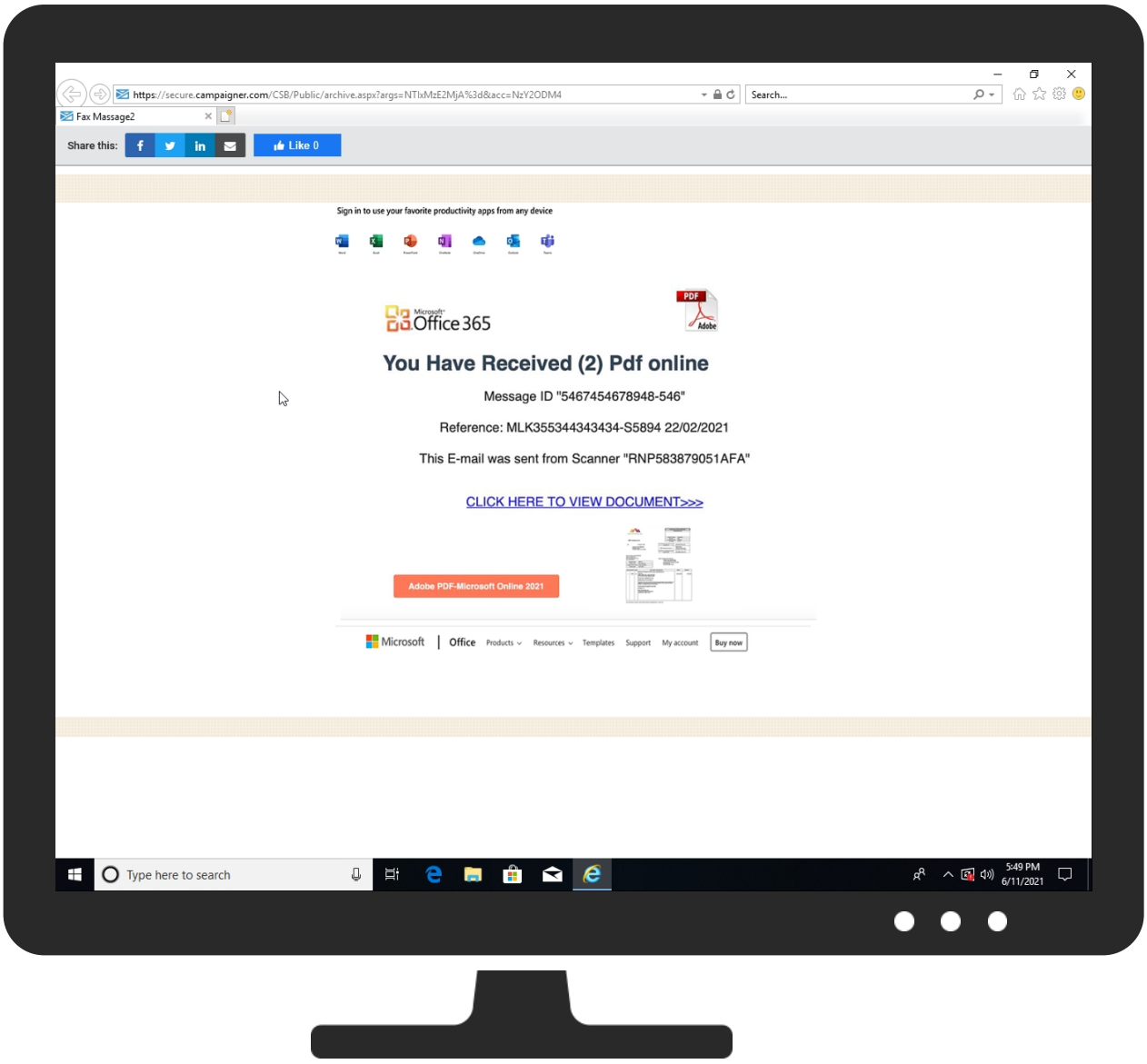


Screenshots

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://secure.campaigner.com/CSB/Public/archive.aspx?args=NTIxMzE2MjA%3d&acc=NzY2ODM4	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://macadavid.cf/0	0%	Avira URL Cloud	safe	
http://www.appcropolis.com)	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://macadavid.cf/000/index.phpblic/archive.aspx?args=NTIxMzE2MjA%3d&acc=NzY2ODM4macadavid.cf/000	0%	Avira URL Cloud	safe	
http://https://www.internalfb.com/intern/invariant/	0%	URL Reputation	safe	
http://https://www.internalfb.com/intern/invariant/	0%	URL Reputation	safe	
http://https://www.internalfb.com/intern/invariant/	0%	URL Reputation	safe	
http://https://secure.campaig	0%	Avira URL Cloud	safe	
http://ianlunn.github.io/Hover/)	0%	Avira URL Cloud	safe	
http://fontawesome.iohttp://fontawesome.iohttp://fontawesome.io/license/http://fontawesome.io/licens	0%	Avira URL Cloud	safe	
http://https://macadavid.cf/000/index.php$Share	0%	Avira URL Cloud	safe	
http://https://macadavid.cf/000/index.phpblic/archive.aspx?args=NTIxMzE2MjA%3d&acc=NzY2ODM40	0%	Avira URL Cloud	safe	
http://gsgd.co.uk/sandbox/jquery/easing/	0%	URL Reputation	safe	
http://gsgd.co.uk/sandbox/jquery/easing/	0%	URL Reputation	safe	
http://gsgd.co.uk/sandbox/jquery/easing/	0%	URL Reputation	safe	
http://https://getbootstrap.com)	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://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
star-mini.c10r.facebook.com	31.13.92.36	true	false		high
scontent.xx.fbcdn.net	31.13.92.14	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
secure.campaigner.com	216.24.224.42	true	false		high
macadavid.cf	66.29.132.67	true	false		unknown
www.facebook.com	unknown	unknown	false		high
media.campaigner.com	unknown	unknown	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://secure.campaigner.com/CSB/Public/archive.aspx?args=NTIxMzE2MjA%3d&acc=NzY2ODM4	false		high
http://https://macadavid.cf/000/index.php	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.24.224.42	secure.campaigner.com	Canada		17358	ETOLL1CA	false
31.13.92.14	scontent.xx.fbcdn.net	Ireland		32934	FACEBOOKUS	false
31.13.92.36	star-mini.c10r.facebook.com	Ireland		32934	FACEBOOKUS	false
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
66.29.132.67	macadavid.cf	United States		19538	ADVANTAGECOMUS	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433372
Start date:	11.06.2021
Start time:	17:48:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://secure.campaigner.com/CSB/Public/archive.aspx?args=NTIxMzE2MjA%3d&acc=NzY2ODM4
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:	5
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.phis.win@3/72@11/6
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://macadavid.cf/000/index.php
Warnings:	Show All

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\6AOSI0IH\secure.campaigner[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\Recovery\High\Active\RecoveryStore.{11894F34-CB18-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8537645251102173
Encrypted:	false
SSDEEP:	192:rbZEZC2/W8tn5fJIbsMhzcqBm5DfLIYcX:rt0hOIJ0m5lU
MD5:	8282550E06DBB98616F2FFEA5E1F2317
SHA1:	6C6CB6294FC81E05F9983A3F6DB4E973C9844628
SHA-256:	77BF25DE44162A49B1A1AA2A5B41562F3ECA13BDFC26C52CF08A759FA050BEC7
SHA-512:	B546D463FC8C77E45335C0837216E20D7487883345DE8B9DE9FD60EB23C02D3F0FA5F57CBCB8F289CB412F7C942908D1BD481E719633A448BF0E09E8484E23C
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\{11894F36-CB18-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	83140
Entropy (8bit):	3.406684419173062
Encrypted:	false
SSDEEP:	768:6ZR3FkbuQpJOazyvyZR3FkbuQpJOazyvO:2wppJdzFwppJdzL
MD5:	9EAF57F3B37FB0E2EAE690E37D394E4C
SHA1:	E9924B56B692526DB8A0DC7197639CED8E558B2C
SHA-256:	82890B16558282E98059AE4F49DF46358B68E34B249CE2232F6F3817FEAD6718
SHA-512:	C6E0AAA6FCC6F93EECD046ADC6D220B63F3D09C608D01067F734249D3D57E5E8846B27F7A25991AF3AFDEE08113E1CD4FDA147002867205F22A9EDD2911E9C 8
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\{180F7E13-CB18-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.565704737793303
Encrypted:	false
SSDEEP:	48:Iw9GcprEGwpa1G4pQJGrapbSOGQpKwG7HpR8TGIpG:rjZ8Qn6pBSGALToA
MD5:	52FB9C666DE08A6437EB131B48D4B0FF
SHA1:	537BC0F5ACBDA2A56AA2FBAC3E0C7389F36EFB4B
SHA-256:	6A28AE36980222CB41B3B255A248F9609C5178FA66A1C8EE94F47761CD8D1A76
SHA-512:	172436D6D0C81056BB12998202DD3D0F8F0911CF6766D291A873A0DFB194DB9B9494377B006DE6C6E27AB821F24DD4F1F75058C854B16AED4F509180EB9483CI
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.120054924391477
Encrypted:	false
SSDEEP:	12:TMHdNMNxOENaSaInWimI002EtM3MHdNMNxOENaSaInWimI00ObVbkEtMb:2d6NxO6SZHKd6NxO6SZ76b
MD5:	1DC540C2FD076E38A49504DA24685E55
SHA1:	7FFB4E5D2B55648396855F5E0898BBAD49CF091F
SHA-256:	9DEF857CB517840ED7774DB5D904EA17DABCBA03FC371CF1FD0D554B5D7990E5
SHA-512:	7469A3DE34CA9A1051E2D24D6FAABB12BB45FB048D4AC225A096AE942BC937043823B714075EE66E6DB082E260F4A57CB647B27D3C1C2C9D15021C793FE92FA B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xe556d613,0x01d75f24</date> accdate>0xe556d613,0x01d75f24</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xe556d613,0x01d75f24</date><accdate>0 xe556d613,0x01d75f24</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile ></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.131855412431883
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2k4NInWimI002EtM3MHdNMNxe2k4NInWimI00Obkak6EtMb:2d6NxriSZHKd6NxriSZ7Aa7b
MD5:	8F02BD001D937479F7BBBAD2CCC9752C
SHA1:	966F0E5D69F1D57F9B7BF336EF2E12367A26D108
SHA-256:	D616ABEF55E6761A998EE36A4552FCB5DCB6271590B1A91D448E03FACF8D3ECF
SHA-512:	54C41CEB15ACA1ECBEEBD22AFF8F6DA26894FBDE4CFE4EFFB06B8055429CB77157335A9E26581E17608779FF0B448949BD8B06100422865EF216D2794708AF2I
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xe54d4c88,0x01d75f24</date><a ccdate>0xe54d4c88,0x01d75f24</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xe54d4c88,0x01d75f24</date><a ccdate>0xe54d4c88,0x01d75f24</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Am azon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.103542125039967
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
SSDEEP:	12:TMHdNMNxvLf2InWimI002EtM3MHdNMNxvLf2InWimI00ObmZEtMb:2d6NxvhSZHKd6NxvhSZ7mb
MD5:	AAA634D73D7B2ABA56FDD34EB1F6D6B9
SHA1:	42AFBD945CEB063D6FDA126F4729BBBF59D30DC7
SHA-256:	A600305DE3CF926783459D1495CAFBFDDB07364D967DDE841E4FBB01C35520D6
SHA-512:	558DF55F37D85B26B4FD4B3B08EF98FC717A4E452F35EEC688F02E5E63249A51469C257D9F0A787D19D4854EEA29FD6B5DC5CB49D9F5473E50FDE04193759D3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xe55dfcfb,0x01d75f24</date><accdate>0xe55dfcfb,0x01d75f24</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xe55dfcfb,0x01d75f24</date><accdate>0xe55dfcfb,0x01d75f24</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.136171667762885
Encrypted:	false
SSDEEP:	12:TMHdNMNxiNaSaInWimI002EtM3MHdNMNxiNaSaInWimI00Obd5EtMb:2d6NxISZHKd6NxISZ7Jjb
MD5:	4F53945A51D3A872B3AA3DDAC5BE7D64
SHA1:	058D86103231F4388BD84E62A0E3DF0A1EC562D5
SHA-256:	0D0A52AB1280E8E3A956FD652EE343AEF89E06DFDFC7CF767E63C2C983468AE8
SHA-512:	D090AFCFE16C53B9F2034293615EAC14E1A749E89F9C5FF98A331226C4A23E5A5126F5D4BFE038D05E9EE0CFD6E5AE9BB208600020E8194370227B193FA368E5
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xe556d613,0x01d75f24</date><accdate>0xe556d613,0x01d75f24</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xe556d613,0x01d75f24</date><accdate>0xe556d613,0x01d75f24</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.115833012268
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwf2InWimI002EtM3MHdNMNxhGwf2InWimI00Ob8K075EtMb:2d6NxQwSZHKd6NxQwSZ7YKajb
MD5:	7B6E98A7A5C35306F9073443CD4FC8E1
SHA1:	5163C930EE72928B44581D8BB4B6770B7CFC43F4
SHA-256:	185148849BCE1EF2C7D22A57E37E94D777EC351FF2836F7F1EDBB43C32DF1A77
SHA-512:	FD1DACFE930CEB8ECE6060CAB96E7EB285D309E6439F608ED4E274007EE3F8CE584393689A0B68E1BA5DA3127A54CA58D6A6DD7D72F8C82754E5B1C9AB3C6E80
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xe55dfcfb,0x01d75f24</date><accdate>0xe55dfcfb,0x01d75f24</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xe55dfcfb,0x01d75f24</date><accdate>0xe55dfcfb,0x01d75f24</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.1209116472242755
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nNaSaInWimI002EtM3MHdNMNx0nNaSaInWimI00ObxEtMb:2d6Nx07SZHKd6Nx07SZ7nb
MD5:	BE8F7715097EF932AF1C1CFEEEE50C50
SHA1:	5C89297B7B1280E6E5516E67D3ECD90A5E02D94A
SHA-256:	76AC52419FA4C2D9C6DD4482B67877319D9216DC7D376A27CB4361D0772E1699

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
SHA-512:	7DD147984A981A850D254551CF9480A21DDC9934829C8DCF142D168EF19AE47A2951736AB91DCDC644E139F2060E4BA2CDCD40E9C27BC57DAFB6D8C6EBC884
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xe556d613,0x01d75f24</date><accdate>0xe556d613,0x01d75f24</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xe556d613,0x01d75f24</date><accdate>0xe556d613,0x01d75f24</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.160478625662173
Encrypted:	false
SSDEEP:	12:TMHdNMNxxNaSaInWimI002EtM3MHdNMNxxNaSaInWimI00Ob6Kq5EtMb:2d6NxtSZHKd6NxtSZ7ob
MD5:	52D037AA078AC77FBA10272DC0393583
SHA1:	3EB5E44FB08F3D130E69B8CF6C94EEDE618EC7C1
SHA-256:	8458C13283856E623F5D62DA600F73648B622127DAE0FEDD6B6F4A3E1A78D285
SHA-512:	DEE835AAE562D9CC8A24920793602C8EB5E331112D74B7D0C8E84CFA848FD59FCA11E4F44A7A07B10D951F0C37A4F1EDB8BEB8A77D4731C2453363E2AFE340E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xe556d613,0x01d75f24</date><accdate>0xe556d613,0x01d75f24</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xe556d613,0x01d75f24</date><accdate>0xe556d613,0x01d75f24</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.140304308702166
Encrypted:	false
SSDEEP:	12:TMHdNMNxcNaSaInWimI002EtM3MHdNMNxcNaSaInWimI00ObVEtMb:2d6NxiSZHKd6NxiSZ7Db
MD5:	F53CC400CE255AE8F29E181C43519EF0
SHA1:	60BF6EC3FC746C722C0B7CEE6C09B024A0EEB7B9
SHA-256:	F4B271A79A19B306C13D80D5DAA8F889A4EC84946D57447846BD199040724F68
SHA-512:	6BF4EBB62DD6A1F95081F409DA10C8C58724C64AA7116E214F5E0C88E2C3E87701ED8B5BCFFA802053E2F69282CEA7F3E3B7467F9C3B2579946CEA9397F9769
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xe556d613,0x01d75f24</date><accdate>0xe556d613,0x01d75f24</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xe556d613,0x01d75f24</date><accdate>0xe556d613,0x01d75f24</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.1216050839246146
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnNaSaInWimI002EtM3MHdNMNxfnNaSaInWimI00Obe5EtMb:2d6NxjSZHKd6NxjSZ7ijb
MD5:	C23A5FBC069337C4737405F8A5A11482
SHA1:	3E34E7EEA9D985C6DD19655BA38174CD204C1CE1
SHA-256:	C8149191BC3556D849E8BA266B868FD55C8BF20C8918B1AB6F83CBC32F06AAD0
SHA-512:	B839940F219DAB6EDF2B46C61CFA90C8B4273FA02D3F9F9E411502BA9423958F6354CD5819CDAE3261DCB228C82A385928A989B64C7513836652074BE8D783B5
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xe556d613,0x01d75f24</date><accdate>0xe556d613,0x01d75f24</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xe556d613,0x01d75f24</date><accdate>0xe556d613,0x01d75f24</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	15458
Entropy (8bit):	3.251447312915614
Encrypted:	false
SSDEEP:	96:h/KzeBIB035tlTY4aRVUnlf3fLIK5hDMQUGb5XMgwLniWQBeFIGvCztNtT8vud7Y:50235tVp9vXMdbiH+wzGaOuC8AWID
MD5:	51D0F27E039E90F513C3FAFED8D5B189
SHA1:	A2CBECA562031C260B1AF9441ACA2F2A3061D2F2
SHA-256:	58DE710D722DE893565CAD08DC0EBA80530A6D71FF9366FAFD8B7D69B4DD4749
SHA-512:	D508EB4734E87236ADE6BDC556288F8954F3B18A414A7F6B68D92A236AF89E1847BF781AAE3B6ECF08D462760A5B73609D7489EAC6E3F4E68059A510B35A75E5
Malicious:	false
Reputation:	low
Preview:	).h.t.t.p.s.:.//.s.e.c.u.r.e...c.a.m.p.a.i.g.n.e.r...c.o.m./.f.a.v.i.c.o.n...i.c.o..%.....00.... ..%.....(...0..`.... .....$..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Screen%20Shot%202021-03-04%20at%209.10.51%20PM[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 700 x 742, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	175451
Entropy (8bit):	7.984628137027263
Encrypted:	false
SSDEEP:	3072:ywyT+2i99NFbktVi9Bx00/gm++Dw6SO8jhqpJ49gvIlfqpMDIBMhsUpzRbzWLCwj:ywl2yh+Vi9E9+s3hg41lYRBGsUHNwj
MD5:	AB162FCB4910DB53D9CBBEA72AF54E44
SHA1:	8786119E313B50CAC5335329DCA141B3B15B47FF
SHA-256:	9F237C90CC3F13ACB455144E428383065A21BE9678BB1FCC720B55A8D723C25E
SHA-512:	7BC0C3A0B5B92B148E444425894F9D1218F55C84D0378C974CBFBCA9E2587645FE53EAAF04FFEA5261F1FA16998F0E28445A53390E610D8F3D7929E3091DF378
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://media.campaigner.com/media/76/766838/Screen%20Shot%202021-03-04%20at%209.10.51%20PM.png?id=p4lc0jq
Preview:	.PNG.....IHDR.....G... .IDATx^..x.....=%..B.....z.W..k..r.k.X..{.^...''..H..C .....9..c...B..O.N...7.g....Y.,.....B@...! ..@.%....-+f..! .....B@.(.''x.#..! .....B@.th.''x;t.qB@...! .....i.....e^.....o{l...NM..W..W...3M....Vq-Z.....phQ.....B...h..m.|.u.l....:u....?sn{lO.....B@....H.....n..^.W.....i~.g.FFF....X.I..v..JKKq.....c...G..''.~..'x<...>...{...1`....;.O ...D..._`....Wt.%....9rd.....|...x.....K....O[...b.!.=zt..RRR....`...j.yr....B@.t..M...|....{.z*..~;...j..p.....3q...K.v...=...''...A..a.....}@QQ.....#.q[Z...9.k..g...cK.9.Y.mf].....o...}..p.i..s..._...-..._.f....L.j.*5....x.kS.6.oK.X..a..\...#...o..Y;.....JeK.^...G...C.._~.}..g.2l.<n.....:+V.@.....N.....v.....P....;8.....~..}.....0.....Blj^v>..Eg...|..'..W^....[.v.s...*.}....0--m.vu..y...aX.c ..+.....?.F.o.....O>.....3.<....T.lrr.A..=.].vm4/g....0m.4.x.....Ayy...m!.R.].r..DP.=.....Z..&.Kqr..g..n...(..W..>.1W.v.y.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Telerik.Web.UI.WebResource[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	563609
Entropy (8bit):	5.3928957996223295
Encrypted:	false
SSDEEP:	12288:d9D37KTA+cc/hkCdO2+ipSEEhc4WeQqgKBt:d9D3eXcc/hkC42+iTEhc4WeQqgKBt
MD5:	96E892352A706077CA4F0CC78FD62A3E
SHA1:	8ED1E7EEB60E6FD6D5902F836C05581422816E6D
SHA-256:	6536E723603C358246ED61633EEB159CBC6A96C4143ACCE9D40F9AAD281CF2F1
SHA-512:	2F697CADD5EF9E575967C72F026743332FBF6E56365717970CB96581A9C708C2CB9FFB7DCD0734D76964750C214C2ED21526F087BB28B04AEA1D031879CCFBC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://media.campaigner.com/csb/Telerik.Web.UI.WebResource.axd?_TSM_HiddenField_=radScriptManager_TSM&compress=1&_TSM_CombinedScripts_=%3b%3bSystem.Web.Extensions%2c+Version%3d4.0.0.0%2c+Culture%3dneutral%2c+PublicKeyToken%3d31bf3856ad364e35%3aen-US%3aba1d5018-bf9d-4762-82f6-06087a49b5f6%3aea597d4b%3ab25378d2%3bTelerik.Web.UI%2c+Version%3d2021.1.330.45%2c+Culture%3dneutral%2c+PublicKeyToken%3d121fae78165ba3d4%3aen-US%3a6ddfaaf7-68e8-4aa2-a15d-336c3a8f9e4b%3a4877f69a%3a16e4e7cd%3a874f8ea2%3ab2e06756%3af7645509%3a24ee1bba%3a33715776%3a92fe8ea0%3af46195d3%3afa31b949%3ac128760b%3a19620875%3a490a9d4e%3abd8f85e4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Telerik.Web.UI.WebResource[1].js	
Preview:	/* START MicrosoftAjax.js */..//----------..// Copyright (C) Microsoft Corporation. All rights reserved...//----------..// MicrosoftAjax.js..Function.__typeName="Function";Function.__class=true;Function.createCallback=function(b,a){return function(){var e=arguments.length;if(e>0){var d=[];for(var c=0;c<e;c++)d[c]=arguments[c];d[e]=a;return b.apply(this,d)}return b.call(this,a)}};Function.createDelegate=function(a,b){return function(){return b.apply(a,arguments)}};Function.emptyFunction=Function.emptyMethod=function(){};Function.validateParameters=function(c,b,a){return Function._validateParams(c,b,a)};Function._validateParams=function(g,e,c){var a,d=e.length;c=c||typeof c==="undefined";a=Function._validateParameterCount(g,e,c);if(a){a.popStackFrame();return a}for(var b=0,i=g.length;b<i;b++){var f=e[Math.min(b,d-1)],h=f.name;if(f.parameterArray)h+="["+(b-d+1)+"]";else if(!c&&b>=d)break;a=Func

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\all[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	231278
Entropy (8bit):	5.454739655753128
Encrypted:	false
SSDEEP:	3072:UZMgeQ6sKf+sdHOAi/y0NSajKeffmj+0Ea:qeQ6s6+sdHi/y0N7KeffmEa
MD5:	3F5AC906F2D19512BABC05DF2534BB73
SHA1:	D9FA5BD80E7597F1BF5F7E7DA24338D2BA520521
SHA-256:	3B5423B600B5EBCD4C5FAAACB2F8FEFB14E7D6F00BA3E9461DA2F53CD401D365
SHA-512:	C666D3B56EFC147E4144DD0F0AF4F0F974E008B3C613FA5203644082F7627C306BD88BB5A31DA024E55AB90A19037F0F1994AFEC90FA1FA084199F8CBE78EB5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://connect.facebook.net/en_US/all.js?hash=ed66a72149e8650e57399b0a1a5945dc
Preview:	/*1623414081,,JIT Construction: v1003951477,en_US*/../**. * Copyright (c) 2017-present, Facebook, Inc. All rights reserved.. *. * You are hereby granted a non-exclusive, worldwide, royalty-free license to use,. * copy, modify, and distribute this software in source code or binary form for use. * in connection with the web services and APIs provided by Facebook.. *. * As with any software that integrates with the Facebook platform, your use of. * this software is subject to the Facebook Platform Policy. * [http://developers.facebook.com/policy/]. This copyright notice shall be. * included in all copies or substantial portions of the software.. *. * THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR. * IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTAB ILITY, FITNESS. * FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR. * COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER. * IN AN ACTION OF CO

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bootstrap.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	144877
Entropy (8bit):	5.049937202697915
Encrypted:	false
SSDEEP:	1536:GcoqwrUPyDHU7c7TcDEBi82NcuSELL4d/+oENM6HN26Q:VoPgPard2oENM6HN26Q
MD5:	450FC463B8B1A349DF717056FBB3E078
SHA1:	895125A4522A3B10EE7ADA06EE6503587CBF95C5
SHA-256:	2C0F3DCFE93D7E380C290FE4AB838ED8CADFF1596D62697F5444BE460D1F876D
SHA-512:	93BF1ED5F6D8B34F53413A86EFD4A925D578C97ABC757EA871F3F46F340745E4126C48219D2E8040713605B64A9ECF7AD986AA8102F5EA5ECF9228801D962F5D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css
Preview:	/*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors. * Copyright 2011-2018 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e83e8c;--red:#dc3545;--orange:#fd7e14;--yellow:#ffc107;--green:#28a745;--teal:#20c997;--cyan:#17a2b8;--white:#fff;--gray:#6c757d;--gray-dark:#343a40;--primary:#007bff;--secondary:#6c757d;--success:#28a745;--info:#17a2b8;--warning:#ffc107;--danger:#dc3545;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:576px;--breakpoint-md:768px;--breakpoint-lg:992px;--breakpoint-xl:1200px;--font-family-sans-serif:-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,sans-serif,"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol";--font-family-monospace:SFMono-Regular,Menlo,Monaco,Consolas,"Liberation Mono","Courier New",monospace}*,::after,::before{box-sizing:border-box}html{font-family:sans

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	715
Entropy (8bit):	5.152325107613811
Encrypted:	false
SSDEEP:	12:jF/iY3Q6ZN6pixIFTqF/iO6ZN6pixsiJqF/iO6ZRoT6pixUEqF/iO6ZX6pix5JY:5/iY3QYNNxb/iOYNNxsl/iOYsNxUv/iy
MD5:	896A43879DA6874AB94B9EF2B8522FAA
SHA1:	2D7CDE20E3D6CEA4C5396A60D1D1D53DC6BE0AF9
SHA-256:	0D36AB1F4829402E9E3BFBCD71AA0E967B1E376B0CA9033A97AF876D498CC1D4
SHA-512:	E1A36BAB9A813FAFD07F0463E3C2B9BC78542B8106D1BA41369F69821874413B703267EB21B0E361923C2B207F6F469191356F62A87949198CFE9F4A36D80A84
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\css[1].css	
Preview:	@font-face {. font-family: 'Roboto';. font-style: italic;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOjCnqEu92Fr1Mu51TjASc6CsI.woff) format ('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmSU5fBBc-.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOmCnqEu92Fr1Mu4mxM.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 500;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmEU9fBBc-.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\css[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	897
Entropy (8bit):	5.156418227259262
Encrypted:	false
SSDEEP:	24:5/iY3QYXNxz/iY3QYN7NxY/iOYsNxUv/iOYXNxa/iOYN7Nxn:UY3QgNwY3QCNpOLNKCOgNbOCNF
MD5:	7D735032BA95B018E621A63B5E90B575
SHA1:	EBA452D17316B6B3D7587373AFB3915E8C48F020
SHA-256:	3474E85DA1AA9D40177FC35201F82740832FC311DCCBB1D0B4538F8E74FD054E
SHA-512:	DC65057641AD42FDEC1FD4373E567498826CF3738D63729935574BA7CB580D0C3751927BCD2A1FCCC085C661F0C20177F719247C09F49E5E4C0BE6136D98037E
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Roboto';. font-style: italic;. font-weight: 500;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOjCnqEu92Fr1Mu51S7ACc6CsI.woff) format ('woff');.}.@font-face {. font-family: 'Roboto';. font-style: italic;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOjCnqEu92Fr1Mu51TzBic6CsI.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOmCnqEu92Fr1Mu4mxM.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 500;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmEU9fBBc-.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92F r1MmWUlfBBc-.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\genericopenwindowfcts[1].js	
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):	9674
Entropy (8bit):	5.152020746470073
Encrypted:	false
SSDEEP:	192:VPVvtvgYCNhvJu/vKJ2Uv9av+LvOvLvaMtvNPavExeP8PaJeIJoVKMy+pz/DOCKj:V5pgYOFJu/v62E4+L677kEx2M1q5Mu4G
MD5:	CE0D685C7FBC01050B8A48C62CAE7BB7
SHA1:	0DF38F490AF1EA4E50CCCDE9D1814FDF4B41A82E
SHA-256:	EA6FD74480EEFD16F265F8E096E25CC95C6359E0944574A0E485D0D92DA1C571
SHA-512:	696FBE55DB1C16E5E26EC62B1DA3513486B95949B2E7A9C0A8AB4F52A90A70982A63D9E16CCFA6381F28203F3335FB6C3D7FE3397FA4FB858982C0DE2915A1A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://media.campaigner.com/csb/scripts/genericopenwindowfcts.js
Preview:	/// <reference path="jquery-1.10.2-vsdoc.js" />....WinBehavior = {.. None: 0,.. Resize: 1,.. Minimize: 2,.. Close: 4,.. Pin: 8,.. Maximize: 16,.. Move: 32,.. Reload: 64,.. Default: (1 + 2 + 4 + 8 + 16 + 32 + 64)..};....function OpenWindow(navigateURL, radWindow, Width, Height, title, withTitle, advWin, showSpinner) {...if (typeof(showSpinner) == "undefined") {....return OpenWindowWithoutSpinner(navigateURL, radWindow, Width, Height, title, withTitle, advWin);...}.....var oWnd = (typeof(radWindowPlaceHolderClientID) == "undefined") ? ..... GetRadWindowManager().getWindowByName(radWindow) :.....$find(radWindowPlaceHolderClientID);...if (!oWnd) oWnd = radopen(null, radWindow);.....oWnd.set_visibleStatusbar(false);.....if (title != "").....oWnd.SetTitle(title);.....if (Width > 0 && Height > 0)....oWnd.setSize(Width, Height);.....if (advWin == undefined || advWin != "true")....oWnd.set_behaviors(WinBehavior.Close + WinBehavior.Move); //all windows should have

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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:	53A2B560B20551672FBB0E6E72632D4FD1C7E2DD2ECF7337EBAAAB179CB8BE7C87E9D803CE7765706BC7FCBCF993C34587CD1237DE5A279AEA19911D690675E65
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-3.1.1.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery-3.1.1.min[1].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\0W10PBUV\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\0W10PBUV\jquery-latest.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	104154
Entropy (8bit):	5.047474377265736
Encrypted:	false
SSDEEP:	1536:l0Cdcds8W3OBauVe+MB/ZE1ljSmvbMYdzdo56UBSpS013DGoA2JfCnyuGFXHWRdx:TnrAdoOdJAkfChcW47sb/Hr535Fqm
MD5:	DCE288F95FBF9F1DA7B4A971D6B5D5DB
SHA1:	654CF8125C4929542F1699776A38AC6DD8E153C9
SHA-256:	30D6CC2F08F3E3C540ECEF09C5833AFB939CE01AD1E971D693CEFB31F716A54D
SHA-512:	4F92825CB4DAE5CD22100C90303C92A82AC16D6A641993BA78F6B2E6E35843195A7AF4CE7237F95E2F2B58D2E3FC8BDAA608941514E9D59274C0B678D412297
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://media.campaigner.com/csb/scripts/thirdparty/jquery-latest.min.js
Preview:	/*! jQuery v3.0.0 | (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 = "3.0.0", 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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	85578
Entropy (8bit):	5.366055229017455
Encrypted:	false
SSDEEP:	1536:EYE1JVoiB9JqZdXXe2pD3PgoIiulrUndZ6a4tfOR7WpfWBZ2BJda4w9W3qG9a986:v4J+OlfOhWppCW6G9a98Hr2
MD5:	2F6B11A7E914718E0290410E85366FE9
SHA1:	69BB69E25CA7D5EF0935317584E6153F3FD9A88C
SHA-256:	05B85D96F41FFF14D8F608DAD03AB71E2C1017C2DA0914D7C59291BAD7A54F8E
SHA-512:	0D40BCCAA59FEDECF7243D63B33C42592541D0330FEFC78EC81A4C6B9689922D5B211011CA4BE23AE22621CCE4C658F52A1552C92D7AC3615241EB640F8514B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery.min[1].js	
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js
Preview:	/*! jQuery v2.2.4 | (c) jQuery Foundation | jquery.org/license */.!function(a,b){"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){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="2.2.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,function(b,c){return a.call

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\nN7EzeTFXEH[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	540652
Entropy (8bit):	5.4200131807166905
Encrypted:	false
SSDEEP:	6144:OFktGPd3BSSaUQoDePihUnbjqQExWydOxehPGMZuiF/fx/B5VNVG8S:OCy3BDen+QExWygwLNVG8S
MD5:	4502D6242E3856F4F2278E8F30F40AA3
SHA1:	8AC410ECAE52E7A4647A49A8FC5D2D2029F53A19
SHA-256:	5D890C20875889464FCE1692C6F40CE23FF22F6FCAB8A670761327E3204E0125
SHA-512:	A225FC8FF3A89F2002E6DC6604F59A73FF6AFF1B85067A6AA1F99ABF8A3B9B32AC7FE2A9CC8F5556AD7A1F2395F6134D98F1A313FF3DC570ECF6D7C4B0C518 4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.facebook.com/rsrc.php/v3iEpO4/y1/l/en_US/nN7EzeTFXEH.js?_nc_x=Ij3Wp8lg5Kz
Preview:	if (self.CavalryLogger) { CavalryLogger.start_js(["Z3urS1k"]); }..."use strict";(function(){var a=typeof globalThis!=="undefined"&&globalThis||typeof self!=="undefined"&&self||typeof global!=="undefined"&&global;if(typeof a.AbortController!=="undefined")return;var b=function(){function a(){this.__listeners=new Map()}a.prototype=Object.create(Object.prototype);a.prototype.addEventListener=function(a,b,c){if(arguments.length<2)throw new TypeError("TypeError: Failed to execute 'addEventListener' on 'CustomEventTarget': 2 arguments required, but only "+arguments.length+" present.");var d=this.__listeners,e=a.toString();d.has(e)||d.set(e,new Map());var f=d.get(e);f.has(b)||f.set(b,c)};a.prototype.removeEventListener=function(a,b,c){if(arguments.length<2)throw new TypeError("TypeError: Failed to execute 'addEventListener' on 'CustomEventTarget': 2 arguments required, but only "+arguments.length+" present.");var d=this.__listeners,e=a.toString();if(d.has(e)){var f=d.get(e);f.has(b)&&f["delete"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\socialsharinghelper[1].js	
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):	846
Entropy (8bit):	4.583882015397946
Encrypted:	false
SSDEEP:	24:L4JN6fQ+7iFreNHAzbN7tcDz/Wz5YqD3McX:KYQsicmbR6/8Yw
MD5:	48B7D1E9D67591FFE897002CC9891193
SHA1:	E6AAC6544697B2225BCC5C926DF43B1FF3A6AB26
SHA-256:	8953390791A948A028DB2ED333A6AA6057C3D541FCD872B96C41270DD9C8DFA1
SHA-512:	1C9CE0F69AC8EB54B218ECA7BB6A55B40DEFB98037030D785632D0D94CD1EE815F0CEC613DA1F879E67BB90E71EAF7625B6679A1B356012BFEC3B60943F308 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://media.campaigner.com/csb/scripts/custom/socialsharinghelper.js
Preview:	. function windowOpen(whichWindow) {.. var uri = getWindowLocation();.. uri = uri.replace('https', 'http');.. var url = encodeURIComponent(uri);.. var t = document.title;.. switch (whichWindow) {.. case "linkedIn":.. window.open("http://www.linkedin.com/shareArticle?mini=true&url=" + url + "&title=" + t, "LinkedIn", "width=700,height=500,title='Share this'");.. break;.. case "twitter":.. window.open("https://twitter.com/share?url=" + url, "Twitter", "width=500,height=400,title='Tweet this'");.. break;.. case "facebook":.. window.open("https://www.facebook.com/sharer/sharer.php?u=" + url, "facebook", "width=650,height=500,title='Share this'");.. break;.. }.. }.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\KFOjCnqEu92Fr1Mu51TjASc6CsI[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22280, version 1.1
Category:	downloaded
Size (bytes):	22280
Entropy (8bit):	7.9727639867534075
Encrypted:	false
SSDEEP:	384:P9oOx7sdtvlKnxdf5DGTHz3uPGia2ghi4OEiO+KdRialMgTC3YS95HbcW8Y:1lZsdKnxdBDwz++ia2l4OEi7KCquoS9J
MD5:	6E949B62AF2E8B6F705E35EE4DBC17F4
SHA1:	31BC06C0C932EC0176F42C6864C58D7450BBF97E
SHA-256:	917A5159BE44DE9A82072F6A1C52EF645844D6BEDF42F8FD1549CD99D6DB2CC5
SHA-512:	109EF637EF3C4FB1670DD328466BF1507F0E92D97153A71CA045F3F17F924CC92FF75777B3730CF722825C755D646A796F429F50973C64B543AA13C174D8921B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\KFOjCnqEu92Fr1Mu51TjASc6Csl[1].woff	
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOjCnqEu92Fr1Mu51TjASc6Csl.woff
Preview:	wOFF.....W.....x.....GDEF.....G...d....GPOS.....!GSUB.....OS/2...L...N...`t6.<cmap.....#cvt .....X...X/...fpgm.....4.....".gasp...@..... ....glyf...L..C`..tP>.e%hdmx..O....m....$+.-head..P....6...6...mhhea..PT...#...$...zhmtx..Px.....3J.loca..S.....maxp..U.... ... .4..name..U0.....>.post..V..... .a.dprep..V $.....?.1 .x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x...l\..F..3...N..q)..a|.....^..33..c.....p"y.iT....<Gg...!.3...T1...{.g0.u.y.....m.|.k..NF.....mox. ;...7&.Y..C.R_[.T.c..-.=...9:...a*j.G.....O.Q".6...>...(?...~...._.2:..K4....S%...jbr).....*....e.U..-..X.3.ILQ....z..!.f:...<.W.#...e.c=...&6...lc;;..3<.s<....H.i2..N..t..)Ns...#`..".).[... ._.T..T.....+l..=..O.....Z..F...r..eM.f.Y.....-...r.\.s6.r..,...:.<$..#.l..F.$.2#.e..].[.....yR...e.|{..O..`)..U.0.e.50.Z.b../cM..i.&O._..+.Y.W...;z....j.p._.o..[CL.)n'.UGx..>).X..MJ..Fr..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\KFOlCnqEu92Fr1MmEU9fBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20532, version 1.1
Category:	downloaded
Size (bytes):	20532
Entropy (8bit):	7.966425322589798
Encrypted:	false
SSDEEP:	384:tfEIIA0zhnegvIQxhXmqd8lpP/FwL0cV8yP1JSRHbNHlZL7qwZkoEu3HTbpXcyKd:tr0zhnewHxRmqd8PdwLLeR/ZLGwZLbTA
MD5:	DA2721C68B4BC80DB8D4C404F76B118C
SHA1:	3A32E8B7EFBC9DFB52F024D657B8C8C0A80E5804
SHA-256:	BD811625271ACCA47F7DAC48B460F13E08EE947B2A8E17E278C4D5CCB5D9323C
SHA-512:	5110656E41A261BD2A06F8B5B2A362FF8836B4289E1DE0777D83DB8E9D709C4C4248B67653A28FA47AD4AE823021ADBFC587900E142BF6887C2A7C936F7F4C33
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmEU9fBBc-.woff
Preview:	wOFF.....P4.....l.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...Q...`t...cmap.....#cvt .....\...\1..Kfpgm...8...2.....$.gasp...l.....glyf... x..<e..n..W..hdmx..H....m....+1.3head..IP...6...6...rhhea..I.... ...$....hmtx..I.....S.loca..L8.....maxp..N4... ... .4..name..NT.....:.post..O0..... .m.dprep..OD.....S.. .)x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x....%Y....Wm=..mo..k.m....rl...m.g"^..../..[.}.S...\.mD...1..G>..giz...=C..}.y....|o..c.x.R.r"B.....m...../.&./ 6..5D.AGX.....)<'.)....?.... .Y4>|1...ES.Gc...FO.>$.../...}RCl..T.zD..uZ4~D.._OK.$.Z.(..JR...\..\..\..\.....*'n..6:x...b,..$...?.g:./y.iLg.3..l.0.y.g..X..V...d.#O...0....b7{..>.n.iD.V....." e.\A..OR.kwp.].....6p..."ZE..%...e.u3..L..V...W.7b..L.3.L1K...Ts..$6.-b.....9...b@..!1,...v.C....{...dox.G(...|a%E:.Fn.Nn.^n.....Sf..E)...k....<g..>{....|.....DT..N....Hy.F.Jez....._? 7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\KFOlCnqEu92Fr1MmSU5fBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20404, version 1.1
Category:	downloaded
Size (bytes):	20404
Entropy (8bit):	7.970248785137973
Encrypted:	false
SSDEEP:	384:8uFoOxqigBacqKz8RGLv6K5a+jZ/rFSyeM5B8r/WjRy0BsM16t/PJ:PFlIvUKz8R+t5N53eGar/gY0Bv6tp
MD5:	BF0F407102FAF3A0B521D3B545F547A5
SHA1:	CA357CD0DE5DD0242E8EFACFB8D24AB60FDC86AB
SHA-256:	855A06974032BB69157D469ABA6F63440E8BE47C421F45C3F396F4E0B87B6DE8
SHA-512:	85359028F7FE49B1DF90B72E48DC7DE4B21F1B65E8BF109595705A3F4EAF9FA79854B5AEF060FE266291C5ECE9D04FCEAD1DE09BAA2C5E20601E1579212520C 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmSU5fBBc-.woff
Preview:	wOFF.....O.....x.....GDEF.....G...d....GPOS.....!GSUB.....OS/2...L...P...`t6..cmap.....#cvt .....X...X/...fpgm.....4.....".gasp...@.....glyf.. .L..<'..m..]5Yhdmx..Ht...m....),..head..H....6...6.Y.ihhea..I.... ...$....hmtx..I<.....Dd.loca..K.....maxp..M.... ... .4..name..M.....|..9.post..N..... .m.dprep..N.....:z /.Wx...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x...l\..F..3...N..q)..a|.....^..33..c.....p"y.iT....<Gg...!.3...T1...{.g0.u.y.....m.|.k..NF.....mox.;...7&.Y.. C.R_[.T.c..-.=...9:...a*j.G.....O.Q".6...>...(?...~...._.2:..K4....S%...jbr).....*....e.U..-..X.3.ILQ....z..!.f:...<.W.#...e.c=...&6...lc;;..3<.s<....H.i2..N..t..)Ns...#`..".).[...._.T..T... ..+l..=..O.....Z..F...r..eM.f.Y.....-...r.\.s6.r..,...:.<$..#.l..F.$.2#.e..].[.....yR...e.|{..O..`)..U.0.e.50.Z.b../cM..i.&O._..+.Y.W...;z....j.p._.o..[CL.)n'.UGx..>).X..MJ..Fr..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\OqOE21UvWe3[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	400
Entropy (8bit):	6.584211645324161
Encrypted:	false
SSDEEP:	12:6v/7P+UhU2RGLJ31m9q/NPkIzS+TmxEMXr:+6UGN3gkNxzjiEMb
MD5:	B85D112F813E876DC294B4263CE4D333
SHA1:	CA55B0C604D89034EE0249024983F7570EA2F8BB
SHA-256:	ED91FBB0CD9308F91F8E1FD93942C94EE850FC4161ED788B16F801B743C70B9B
SHA-512:	07DF881DC463F96F412DB4DBB8DB94BE66492C1E130AC2997D9ECA21DAFC23944A962A44F893F96895550EB10691F627579501E17A853A3C8A8C3861656E9506
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.facebook.com/rsrc.php/v3/y5/r/OqOE21UvWe3.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\OqOE21UvWe3[1].png	
Preview:	.PNG.....IHDR.....7.....gAMA.....a.... cHRM..z&.....u0...`..:....p..Q<....bKGD.....tIME..... .`.....IDAT(....B1.D/H.ttT....L.....h...%.AH_.<.....n.M..Y...Z_+.4.4.....3.....[J\h,C.....M..exA$.p..H....gm.f...=...$).u.zd..D4T..tx.....%tEXtdate:create.2019-02-26T15:32:06-08:00J..L...%tEXtdate:modify.2019-02-26T15:32:06-08:00;\@.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\WebResource[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	23063
Entropy (8bit):	4.7535440881548165
Encrypted:	false
SSDEEP:	384:GvUzYI+Vi4g1V5it1ONhA6w+Kv8i/4CYzLKL4DrLU0iTxZTAzIzrwDlTWMClQip9:bkON69kClQq8hDRJHp2tWU25Zt/gREVG
MD5:	90EA7274F19755002360945D54C2A0D7
SHA1:	647B5D8BF7D119A2C97895363A07A0C6EB8CD284
SHA-256:	40732E9DCFA704CF615E4691BB07AECFD1CC5E063220A46E4A7FF6560C77F5DB
SHA-512:	7474667800FF52A0031029CC338F81E1586F237EB07A49183008C8EC44A8F67B37E5E896573F089A50283DF96A1C8F185E53D667741331B647894532669E2C07
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://media.campaigner.com/csb/WebResource.axd?d=pynGkmcFUV13He1Qd6_TZItUc7uOXVQ_JJSF3nqWHTssVf86I8T6DdUK_rt6gpBWQGLL6g2&t=637453890340000000
Preview:	function WebForm_PostBackOptions(eventTarget, eventArgument, validation, validationGroup, actionUrl, trackFocus, clientSubmit) {.. this.eventTarget = eventTarget;.. this.eventArgument = eventArgument;.. this.validation = validation;.. this.validationGroup = validationGroup;.. this.actionUrl = actionUrl;.. this.trackFocus = trackFocus;.. this.clientSubmit = clientSubmit;..}..function WebForm_DoPostBackWithOptions(options) {.. var validationResult = true;.. if (options.validation) {.. if (typeof(Page_ClientValidate) == 'function') {.. validationResult = Page_ClientValidate(options.validationGroup);.. }.. }.. if (validationResult) {.. if ((typeof(options.actionUrl) != "undefined") && (options.actionUrl != null) && (options.actionUrl.length > 0)) {.. theForm.action = options.actionUrl;.. }.. if (options.trackFocus) {.. var lastFocus = theForm.elements["__LASTFOCUS"];.. if ((typeo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\adobe[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 400x400, frames 3
Category:	downloaded
Size (bytes):	30925
Entropy (8bit):	7.75667128400845
Encrypted:	false
SSDEEP:	768:nuowBuvTpjgz+wqrPZ2qh8fmyjlX6RqnxgYqwNL:nuPOpjgzPqrPZRYZGnYqYL
MD5:	BE5274AF7D8BD25B8148A190FF515399
SHA1:	B8D0850FD92EE935287E17988B89E53607808C8C
SHA-256:	26C62DBDF527B8DCBF378EA62F129CBBBA3B244730687909BA21ECD729C9D2E6
SHA-512:	64893C625BE72783088575E36EF26FF4573243F32601BDA754EDA72B7515063B5E4E4831697D16AC663529C910AE12CCD145BEC530F2A9BAE4D9324301C65667
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://macadavid.cf/000/images/adobe.jpg
Preview:	......JFIF.....C.....C.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..g.....\|?....".+....._.....4...R...'..q..~...n.7.....QXJ<...=...^.V'@U..E..5....Uz.....IE.PTe.}/p.y.....T.<...-T..\|...b.=.#IU..~....{O/...b..E.....X...G...?.....\|....._....M..g.....T~g.....<.....T~g.....3$.=._..IU.K..^.E...=.#U.._[X.R..=W...1.....QTr.\....*.7..?..6.9K..^.E.Ps.\.....%W..y...g)s[KX)<.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\all[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	3224
Entropy (8bit):	5.60595259545582
Encrypted:	false
SSDEEP:	48:g+y/clUyAQHWs5+TaorOFzyHOgeEh7z5jFqxv4tx5YHIekZ462X+w3hDuExjGx:g+5AQHAray48f5JJYHIh4PJ3hDu9
MD5:	11DEB3CE7C8C571A6C58A951F39C36E6
SHA1:	D80B9E4EE2A9AE685380B9BB3D074A211FAD9DD1
SHA-256:	17A5CEC3C4AA80C848D8A079802FA7FFE679B3389EFFFA2C0FD4403E7E9E16C7
SHA-512:	58B96ADE09471766DBF2D821CDBF2131A803F32DFCD323B81685DB315DC7000865B4B1FDAA4AAFDA0C0A759839108C90E761A20ED2CAC6987C7A5B62D9D1451
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://connect.facebook.net/en_US/all.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\all[1].js	
Preview:	/*1623426019,,JIT Construction: v1003951569,en_US*/../**. * Copyright (c) 2017-present, Facebook, Inc. All rights reserved.. *. * You are hereby granted a non-exclusive, worldwide, royalty-free license to use,. * copy, modify, and distribute this software in source code or binary form for use. * in connection with the web services and APIs provided by Facebook.. *. * As with any software that integrates with the Facebook platform, your use of. * this software is subject to the Facebook Platform Policy. * [http://developers.facebook.com/policy/]. This copyright notice shall be. * included in all copies or substantial portions of the software.. *. * THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR. * IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTAB ILITY, FITNESS. * FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR. * COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER. * IN AN ACTION OF CO

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\font-awesome[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), FontAwesome family
Category:	downloaded
Size (bytes):	165742
Entropy (8bit):	6.705073372195656
Encrypted:	false
SSDEEP:	3072:qbhEnD+IzsU9z9QJ6/P3Xe2iEiEPGFCMW1JVJG6wVTDsk6BmG6S1yKshojskO+b2:qenD+IzsU9z9QJ6/PO2FiEP2C/DVJG6I
MD5:	674F50D287A8C48DC19BA404D20FE713
SHA1:	D980C2CE873DC43AF460D4D572D441304499F400
SHA-256:	7BFCAB6DB99D5CFBF1705CA0536DDC78585432CC5FA41BBD7AD0F009033B2979
SHA-512:	C160D3D77E67EFF986043461693B2A831E1175F579490D7F0B411005EA81BD4F5850FF534F6721B727C002973F3F9027EA960FAC4317D37DB1D4CB53EC9D343A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://media.campaigner.com/csb/content/ui-theme/global/fonts/font-awesome/font-awesome.eot?
Preview:	n.....LP.....Yx.....F.o.n.t.A.w.e.s.o.m.e.....R.e.g.u.l.a.r...$.V.e.r.s.i.o.n. .4...7...0. .2.0.1.6.....F.o.n.t.A.w.e.s.o.m.e.....PFFTMk .G.....GDEF.....p... OS/2.2z@...X...`cmap..:.....gasp.....h....glyf...M.....L.head...-.....6hhea.....$hmtxEy.....loca...\.....maxp,.....8... name....gh....post.....k.... u.....xY_.<.....3.2.....3.2.....'.....@.....i.....3.....3...s.....pyrs.@. ....p.....U..... .....]..... .....y...n.....2.....@..... ....z.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\fonticons[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	23978
Entropy (8bit):	4.897762897381931
Encrypted:	false
SSDEEP:	384:lruoxXdbo67kH9fIWDUZXegau97vrefyqK477d9403:lruoxXdbU9fIWDUZXegau97W3
MD5:	D5A77A550E6D041F3C674C6D000D96BC
SHA1:	BD02DFFDCEFBCEDF943518CF6FD62DB63A578842
SHA-256:	7298AC333BEC1E6E6CDBCCFB3688F900510770EC58FA83DB582430C624E3B609
SHA-512:	68D750915818F76FFFC5E0E65E9FAE1AF32803C50F79D2FC1A44053C335BEE5738482A23BE0FFB9B988FDFBBB7F45EBCDD7B7CDE5066D96F5D114D41B9BD5C 7D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://media.campaigner.com/csb/app_themes/lightning/common/fonticons.css
Preview:	@font-face {. font-family: 'TelerikWebUI';. src: url('../Common/TelerikWebUI.eot');. src: url('../Common/TelerikWebUI.eot') format("embedded-opentype"), url('../Common /TelerikWebUI.woff') format("woff"), url('../Common/TelerikWebUI.ttf') format("truetype"); }..@font-face {. font-family: 'TelerikWebUIEditor';. src: url('../Common/Tele rikWebUI/Editor.eot');. src: url('../Common/TelerikWebUI/Editor.eot') format("embedded-opentype"), url('../Common/TelerikWebUI/Editor.woff') format("woff"), url('../Comm on/TelerikWebUI/Editor.ttf') format("truetype"); }..@font-face {. font-family: 'WebComponentsIcons';. src: url('../Common/WebComponentsIcons.eot');. src: url('../Commo n/WebComponentsIcons.eot') format("embedded-opentype"), url('../Common/WebComponentsIcons.woff') format("woff"), url('../Common/WebComponentsIcons.ttf') format("truetype"); }..@font-face {. font-family: 'Material Icons';. font-style: normal;. font-weight: 400;. src: url('../Common/fonts/material/MaterialIcons-Regul

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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/t4IdtWPtY:1nmRnAKyt48tZ
MD5:	6D1D3C4FD92B63CC534BE0EDF3AF18DC
SHA1:	5F5442FEB5BE60239F185E969C45050A7DBADE2A
SHA-256:	65ADCB045AEFB4D0028A6AF36EC9D42BBD4DAE9AFF2CF85810BB4A6F44D4B25C
SHA-512:	2D42684CF0A44E262C958172C2446974A4AE9B8D17F7208A5FCB690964EE0D56FEB157B9AB6166B8F94FBDCBA027271C36B66784655E8FD96CE0B5522FE71AA
Malicious:	**true**

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\index[1].htm	
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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\MEEXW4H4\index[1].htm, Author: Joe Security • Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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\MEEXW4H4\index[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://macadavid.cf/000/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\MEEXW4H4\like[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	46713
Entropy (8bit):	5.636671760925903
Encrypted:	false
SSDEEP:	768:tHdNBINI+AJflPD6y8E10yM0XwwAFvvBtPS/p1cdvF6pwhs0miXn:htFD6lEyyM0XnAFxNvF6pwmu
MD5:	EDA31691A276AACEEED5B06879C96312
SHA1:	D4CD262940973C93BFE960F7B931D455BB71F0D4
SHA-256:	87C743AA191AAD6BF984A6D8DE113F6902A63B5F0E18CD932BFB94B84DDD2A80
SHA-512:	120A25C0ABD24E90D982137F858A47BB215A3AF815E0759970B2C8C8D074FA79B4E48E88999B23F9B966F89D5A2E44946AAF7E4DCB277E653A6ACF3469F0C756
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html lang="en" id="facebook" class="no_svg no_js">.<head><meta charset="utf-8" /><meta name="referrer" content="default" id="meta_referrer" /><script nonce="3Mu9y0sE">window._cstart=+new Date();</script><script nonce="3Mu9y0sE">__DEV__=0;var _cavalry={data:{t_cstart:window._cstart},tti:"t_domcontent",log:function(a){this.data[a]=+new Date()},pageid:0,server:"",isb:"",send:function(){this.log("t_creport");var a=this.server+"/common/cavalry_endpoint.php",b=this.data,c=[];b.t_tti=b[this.tti];this.isb&&(b.fb_isb=this.isb);b.lid=this.pageid;for(var d in b)c.push(encodeURIComponent(d)+"="+encodeURIComponent(b[d]));new Image().src=a+"?"+c.join("&")}};_cavalry.log("t_start");_cavalry.pageid="697256409616115765-0";</script><title>Facebook</title><style nonce="3Mu9y0sE">._32qa button{opacity:.4}._59ov{height:100%;height:910px;position:relative;top:-10px;width:100%}._5ti_{background-size:cover;height:100%;width:100%}._5tj2{height:900px}._2mm3 ._5a8u .uiBoxGray{background:#fff;ma

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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://macadavid.cf/000/images/office3651.png
Preview:	.PNG.....IHDR..... .....pHYs.....<eiTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?>.<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c067 79.157747, 2015/03/30-23:40:42 ">. <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">. <rdf:Description rdf:about="". xmlns:xmp="http://ns.adobe.com/xap/1.0/". xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/". xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#". xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/". xmlns:dc="http://purl.org/dc/elements/1.1/". xmlns:tiff="http://ns.adobe.com/tiff/1.0/". xmlns:exif="http://ns.adobe.com/exif/1.0/">. <xmp:CreatorTool>Adobe Photoshop CC 2015 (Windows)</xmp:CreatorTool>. <xmp:CreateDate>2020-01-18T21:49:38+05:00</xmp:CreateDate>. <xmp:MetadataDate>2020-01-21T14:30:14+05:00</xmp:MetadataDate>. <x

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\other1[1].png	
SSDEEP:	192:ESCkiDw7e9Mg/wio0EYm9FWyo2XdJfXoOZdEDfmiIJQdiRVi/WTanY:DBiDw7eAdq+FWyo2/fXoZbDlJ0ci/BnY
MD5:	6843A244E12FAB158AA189680B5E7049
SHA1:	0E1C691F87CC4FA35C88344974F2829C40176B70
SHA-256:	3A9B144D6482B78AFC4E0A940A1D3C22240F14FA535B808CF4DAB9635339569F
SHA-512:	145010C45B6B83EA4005EB367C0507959FF0817E482F19E9973504081ACAE1B7827CBD1172CEC7732B13F4E0CEC058271BD6700444FBCF61FB6A3C068A3744C4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://macadavid.cf/000/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/ph otoshop/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\MEEXW4H4\outlook1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 26 x 26, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	771
Entropy (8bit):	7.682244426935498
Encrypted:	false
SSDEEP:	24:74yiH9yQmOntihdLl00qDeu1BcaDa0oljZG0:omOntO7v/uJDYG0
MD5:	C3FC46C5799C76F9107504028F39190F
SHA1:	519096AD3F03410CF9CE3C9B9FCCA6B439D97B23
SHA-256:	57898461712A639D119BDF88B7145919DCC8956C7A271D2E4A1084B29EAE6785
SHA-512:	DF4A0A2F78B2013035FB738BF405119B275D4CFEC31A23071EB9AF499D5F31FDC4BE22754CE791C975D7D417E908B5CAD16F962B0ADD3DFDCDE19844D74F66 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://macadavid.cf/000/images/outlook1.png
Preview:	.PNG.....IHDR.....JL.....bKGD.....IDATH....k.A..k6.b.F1..H@...j@.aQ...(.. .. .. .A..D...I.....E.....1...W...;;.Y.d.}].U5]..x"3?....!..A..y..+R2\...m.NX.=..p.0... d.^.3.....J.Z.X.).....P\..x1.3.M.0....m.....F....?...n.....I.Fo)x._ R|.s..a.T?...?.=.9.Y..u....z..|.....Wz...h..<..P.. ...$.Y.....k`/4.y/.....L.C.....".....U....7....G...'h.....1j1E..%t..... @..a.....b.ED-.Tn.<..o.D...o..(.{1l>.....".4a.:k.l./.7t./.Q-'..>.. .....'3eb..d.@=4...C....A...;..N.X3.(.....,v...+...S...W..l...@,...j.).u<..@u..0...V&.b.yp.....0..o.?..V..B =.~&m"r (...6;EP.T.....h.m".[f.U)|t..2.Q.....g.cP.W...D..[.O>..d;.yl.{/..#v.._..$.Q.....t\E..5i.q._.."/n...v.w..Uo ...#..S....^.....F..+._??.r.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\2UX7WLTfW3W8TclTUvlFyQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18520, version 1.1
Category:	downloaded
Size (bytes):	18520
Entropy (8bit):	7.9643589925817135
Encrypted:	false
SSDEEP:	384:xvNQ/HsvwkWr7N541Sdqnglu/0JTzVjV/5FOw8fhCuhOA++49:xvNQ/JkWrbOSdqnglKM9R/5FOwMhZhvk
MD5:	16E1D930CF13FB7A956372044B6D02D0
SHA1:	940B859E4F02BD3E7CF7B6CE245C197B5470302A
SHA-256:	97BB9863429AE97FCC0CD6C80D30C3F7454D0B218D4758E24C30BDA441BD39D3
SHA-512:	3B5A264D6EC34DDBE9360C34BE1DE61918010A938DEAAD6AA023771EC095AE058966E6328C7072E16BC98D623A943DB0F5534DD0C4B51D321465EA1D056FCB 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v15/2UX7WLTfW3W8TclTUvlFyQ.woff
Preview:	wOFF.....HX.....GDEF.....@...L.0..GPOS.....IGSUB.....\.....&.ROS/2.....V...`....cmap...T.....8.!Zcvt .....L...L$A..fpgm...H...;....g.\.gasp..... ...glyf.....6r..b&....hdmx..B....d.....head..Bh...6...6.F..hhea..B.....$...}hmtx..B....E...v.ZQ.loca..E.....:.!.maxp..F.... ... .name..F.....o,.post..G..... .m.dprep..G.....t ...x.....P.....@.C.e...N..4.{.qt..r.q.....#x....p#L.....si..m.:..m.m.6.m....\....v.xVm.....T....g..".*.....[..f8.....'d..o.b.....-...x@...K...Gc..k..$.w}.T7.y]....Q....eu.]qw.....2X. .\R....ujR..3wW..k.IK$.....o.....9_....-..'....d!;..G.....d....X.1..Ld...,f3...c1.Y.Z..-D.C,qlg..H{^mv;.6.-B...CN|4....k.Z..|...gR.^..?4....AxIO.?..]{)D$J.$..cJ|.V;@.....AZe/..r.) ....A~...R..O;..(.FZ..F..F|.....z1.....l<um.v...-..-..m...&..S.....R.&..#.]....).N.'|.w.....}I._....e.....% .Xv.M.....7;....%Y$.....v.w..2J.G...+.d.,.]Ke.,..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\585b051251[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	10866
Entropy (8bit):	5.182623714755422
Encrypted:	false
SSDEEP:	192:BgHN42S+9SZRvACpiIthFzoXnemF+shSGnZ+PPxQDqv7jh81Q5l8OcchIlzbCn:WRCfhFzevnEZ/h81Q5l8OsE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\585b051251[1].js	
MD5:	D8CA71772D1E86D5FB9D5E2F6CC1AE70
SHA1:	9B043E60997FE552D652E4474E16AFF923D7AA76
SHA-256:	7D840153F02AD6D91D652354E35B590721916D16C33956631EEF0E7D3B5613EE
SHA-512:	8E9DA8E9AE10EC0EB854A6E488FB4568A960EE10AF46FE4AA49F22F227CB94997F40E49E10A81E341B99489256163A2C0E065730EEA642777061CDA61B4D56C1
Malicious:	false
Reputation:	low
Preview:	window.FontAwesomeKitConfig = {"asyncLoading":{"enabled":true},"autoA11y":{"enabled":true},"baseUrl":"https://ka-f.fontawesome.com","baseUrlKit":"https://kit.fontawesome.com","detectConflictsUntil":null,"iconUploads":{},"id":132286382,"license":"free","method":"css","minify":{"enabled":true},"token":"585b051251","v4FontFaceShim":{"enabled":false},"v4shim":{"enabled":true},"version":"5.15.3"};.!function(t){"function"==typeof define&&define.amd?define("kit-loader",t):t()}((function(){"use strict";function t(e){return(t="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(t){return typeof t}:function(t){return t&&"function"==typeof Symbol&&t.constructor===Symbol&&t!==Symbol.prototype?"symbol":typeof t})(e)}function e(t,e,n){return e in t?Object.defineProperty(t,e,{value:n,enumerable:!0,configurable:!0,writable:!0}):t[e]=n,t}function n(t,e){var n=Object.keys(t);if(Object.getOwnPropertySymbols){var r=Object.getOwnPropertySymbols(t);e&&(r=r.filter((function(e){return Object.g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\585b051251[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	10866
Entropy (8bit):	5.182623714755422
Encrypted:	false
SSDEEP:	192:BgHN42S+9SZRvACpiIthFzoXnemF+shSGnZ+PPxQDqv7jh81Q5l8OcchIlzbCn:WRCfhFzevnEZ/h81Q5l8OsE
MD5:	D8CA71772D1E86D5FB9D5E2F6CC1AE70
SHA1:	9B043E60997FE552D652E4474E16AFF923D7AA76
SHA-256:	7D840153F02AD6D91D652354E35B590721916D16C33956631EEF0E7D3B5613EE
SHA-512:	8E9DA8E9AE10EC0EB854A6E488FB4568A960EE10AF46FE4AA49F22F227CB94997F40E49E10A81E341B99489256163A2C0E065730EEA642777061CDA61B4D56C1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://kit.fontawesome.com/585b051251.js
Preview:	window.FontAwesomeKitConfig = {"asyncLoading":{"enabled":true},"autoA11y":{"enabled":true},"baseUrl":"https://ka-f.fontawesome.com","baseUrlKit":"https://kit.fontawesome.com","detectConflictsUntil":null,"iconUploads":{},"id":132286382,"license":"free","method":"css","minify":{"enabled":true},"token":"585b051251","v4FontFaceShim":{"enabled":false},"v4shim":{"enabled":true},"version":"5.15.3"};.!function(t){"function"==typeof define&&define.amd?define("kit-loader",t):t()}((function(){"use strict";function t(e){return(t="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(t){return typeof t}:function(t){return t&&"function"==typeof Symbol&&t.constructor===Symbol&&t!==Symbol.prototype?"symbol":typeof t})(e)}function e(t,e,n){return e in t?Object.defineProperty(t,e,{value:n,enumerable:!0,configurable:!0,writable:!0}):t[e]=n,t}function n(t,e){var n=Object.keys(t);if(Object.getOwnPropertySymbols){var r=Object.getOwnPropertySymbols(t);e&&(r=r.filter((function(e){return Object.g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\RxZJdnzeo3R5zSexge8UUT8E0i7KZn-EPnyo3HZu7kw[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18576, version 1.1
Category:	downloaded
Size (bytes):	18576
Entropy (8bit):	7.966055167168611
Encrypted:	false
SSDEEP:	384:t1YcZxtaNVIh8bU0QoyLessKJqwvcuqWc97RFvvB/HY:bYcZxUfDQoWRqXuix5/4
MD5:	57AF64FC644194101C1593ABEA164433
SHA1:	C5E19CDC9C784C0362E7D2B7B5BE26418B07FD89
SHA-256:	08CA17DB0A1CEA494B3010B6410696744D5B6DB541EF3218C2C4860905D44868
SHA-512:	7101588CDF7BFA1D5D07B3E9E141AA3304CA144BF1CDEDE2E3795128B3B6738D1A98DC6DDC0208E92992F03E152AB976B2B6A5BB92610CD1AEF5890BA0789FD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v15/RxZJdnzeo3R5zSexge8UUT8E0i7KZn-EPnyo3HZu7kw.woff
Preview:	wOFF.....H.....D.....GPOS.....B..GSUB...`...\.....&.ROS/2.....W...`....cmap.....8.!Zcvt .....V...V..+Jfpgm.....=....{.a.gasp...T.....glyf...`..6...b2.T=.hdmx..BD...c.....head..B....6...6.{..hhea..B.....$....hmtx..C....L...v."H.loca..EL.....U.<}maxp..G.... ... ....name..G,.....-.post..G..... .m.dprep..G.....6x.....dG.....Zq.b.v2Z+.m.6.b.N....o..F..^t....U..#i.&.z...5I[.w..k....2.{.9._.#.f.Y%....._v..Wj...$'..`..6...'8.z+.....^.W....h'..^.....]...3.}..}.?.}..p..gx;{....R..Vp?...^Gw..t.....l..a...v.N.Y.hW.....:P..P..#..QJW..4V.5A.5E'.T..3t.....@..#}.O..>...B_.{.....~..-.B-.b..J..j.Q..T.5..,..qGtn...(j..).oR.v.....e1.`E:.....a2L.*.bu:.jt.<.....!|...'0..f.l..sa.....X..`1..U...@6./.. ...[..N....H.q..{.....:.*t.5..+....A.d.f.`.6..~..r]a..v.R..qz.>.#.:wF..c..T..Q4..B2.I=....J.$vM:.~._a.L...B..]oE.l.. .2a2.`~.s.....G...."X....'.]..C&L.''>,.....}..p.a..-c..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\bootstrap.min[1].css	
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):	145055
Entropy (8bit):	5.080257829501953
Encrypted:	false
SSDEEP:	1536:0RmQI6XkmulSziU5d6gF1UNaYS/Wp85r0IaLQNk6hNO6b:imQX+w0rLQNk6hNO6b
MD5:	F55371AE84173282F8995E205428B76E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\bootstrap.min[1].css	
SHA1:	39BEE99CE7418470937F106EEA42BB988607CB9C
SHA-256:	8AEF10D887509642937ECB6B9319505A4D3BB03F60F4FAC8006CC60BCED5C26D
SHA-512:	77CB637949989FCE41607744D4EA8FDD303E043AD08C334E4BFC95EAE2CF9C870B251B29EEE9D2E59299E7FF1B58A79721CED77B9A3A639A72371EBACC27B3C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://media.campaigner.com/csb/node_modules/campaigner-core/src/style/theme/campaigner/bootstrap.min.css
Preview:	:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e83e8c;--red:#dc3545;--orange:#fd7e14;--yellow:#ffc107;--green:#28a745;--teal:#20c997;--cyan:#17a2b8;--white:#fff;--gray:#6c757d;--gray-dark:#343a40;--primary:#007bff;--secondary:#6c757d;--success:#28a745;--info:#17a2b8;--warning:#ffc107;--danger:#dc3545;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:1px;--breakpoint-md:2px;--breakpoint-lg:3px;--breakpoint-xl:4px;--breakpoint-xxl:1600px;--font-family-sans-serif:"Roboto",sans-serif;--font-family-monospace:"SFMono-Regular",Menlo,Monaco,Consolas,"Liberation Mono","Courier New",monospace}@media print{*,*::before,*::after{text-shadow:none !important;box-shadow:none !important}a:not(.btn){text-decoration:underline}abbr[title]::after{content:" (" attr(title) ")"}pre{white-space:pre-wrap !important}pre,blockquote{border:1px solid #999;page-break-inside:avoid}thead{display:table-header-group}tr,img{page-break-inside:avoid}p,h2,h3{orphans:3;widows:3}h2,h3{page-break

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\bootstrap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	48944
Entropy (8bit):	5.272507874206726
Encrypted:	false
SSDEEP:	768:9VG5R15WbHVKZrycEHSYro34CrSLB6WU/6DqBf4l1B:9VIRuo53XiwWTvl1B
MD5:	14D449EB8876FA55E1EF3C2CC52B0C17
SHA1:	A9545831803B1359CFEED47E3B4D6BAE68E40E99
SHA-256:	E7ED36CEEE5450B4243BBC35188AFABDFB4280C7C57597001DE0ED167299B01B
SHA-512:	00D9069B9BD29AD0DAA0503F341D67549CCE28E888E1AFFD1A2A45B64A4C1BC460D81CFC4751857F991F2F4FB3D2572FD97FCA651BA0C2B0255530209B182F2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),require("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,n){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function s(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function r(){return(r=Object.assign||function(t){for(var e=1;e<arguments.length;e++){var n=arguments[e];for(var i in n)Object.prototype.hasOwnProperty.call(n,i)&&(t[i]=n[i])}return t}).apply(this,arguments)}e=e&&e.hasOwnProperty("default")?e.default:e,n=n&&n.hasOwnProp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\brand-icons.min[1].css	
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):	2650
Entropy (8bit):	4.97489772295558
Encrypted:	false
SSDEEP:	48:z34q4hnm4X4B4+O4JEiWBGDldWaftJt34/Nd2HlgaehE3A7CVBPY/EZ:+nKIudDJIXaJw7CVBAl
MD5:	25D66FC1FE76E57689F3868FAC16C33D
SHA1:	3AC978C8B76E329EED18AA4B5AD7A66A051B38E2
SHA-256:	409C806531699A47E585C9C4F18FA04293776D6A3E22F260DADDEDAD5BCD1049
SHA-512:	5B5A6BE47223DAF51B69FD17E024A1810F350C127EEA08CA91F5BA111978B91D096E9CEC75F9240B86CFFD55F0C92CD63788BD226302CB058E785FA3DD37672
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://media.campaigner.com/csb/content/ui-theme/global/fonts/brand-icons/brand-icons.min.css
Preview:	@charset "UTF-8";@font-face{font-family:"Brand Icons";src:url(../brand-icons/brand-icons.eot?v=0.3.2);src:url(../brand-icons/brand-icons.eot?#iefix&v=0.3.2) format("embedded-opentype"),url(../brand-icons/brand-icons.woff2?v=0.3.2) format("woff2"),url(../brand-icons/brand-icons.woff?v=0.3.2) format("woff"),url(../brand-icons/brand-icons.ttf?v=0.3.2) format("truetype"),url(../brand-icons/brand-icons.svg?v=0.3.2#brand-icons) format("svg");font-weight:400;font-style:normal}[class*=bd-],[class^=bd-]{font-family:"Brand Icons";position:relative;display:inline-block;font-style:normal;font-weight:400;text-rendering:auto;speak:none;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale;-webkit-transform:translate(0,0);transform:translate(0,0)}.bd-behance:before{content:"."}.bd-blogger:before{content:"."}.bd-delicious:before{content:"."}.bd-deviantart:before{content:"."}.bd-dribbble:before{content:"."}.bd-facebook:before{content:"."}.bd-flickr:before{content:"."}.bd-fo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\campaigner.min[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):	239487
Entropy (8bit):	5.035399127270474
Encrypted:	false
SSDEEP:	1536:x/Zy5d6gF1RNaYS/X2uTU6z/F2T/Zkrr3tN9+q4ooce+63K6yhcAsGVRsa55Y8D6:tZ5Ct3K6yhcAsGVRsa55Y8Db43PGA3jD

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\campaigner.min[1].css	
MD5:	7F81F27865AE5CAAF5157D5C72CAF463
SHA1:	18EB145F7244CC1D4B609E13A859E3FE30E70FD8
SHA-256:	68EA12246455E77EE1365F1D49A102F8EE58F89BC76E354A01A7AD6F1117A0FB
SHA-512:	1334085C574710C378E345494F57E9259A123BD8E38B6A75892EA09A4D0F208CAB0A644E66CB6F1FB5ABDBCD201C9C7275FFF27C5C5C91C3B8F5B02520ADC1A5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://media.campaigner.com/csb/node_modules/campaigner-core/src/style/theme/campaigner/campaigner.min.css
Preview:	:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e83e8c;--red:#dc3545;--orange:#fd7e14;--yellow:#ffc107;--green:#27ae60;--teal:#20c997;--cyan:#17a2b8;--white:#fff;--gray:#868e96;--gray-dark:#343a40;--primary:#3793d0;--secondary:#34495e;--success:#28a745;--info:#17a2b8;--warning:#ffc107;--danger:#dc3545;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:480px;--breakpoint-md:768px;--breakpoint-lg:992px;--breakpoint-xl:1200px;--breakpoint-xxl:1600px;--campaigner-dark-blue:#34495e;--campaigner-light-blue:#3793d0;--campaigner-green:#4eb96f;--campaigner-red:#e64d3c;--campaigner-gray:#eceff0}@media print{*,*::before,*::after{text-shadow:none !important;box-shadow:none !important}pre,blockquote{border:1px solid #999}.badge{border:1px solid #000}.table td,.table th{background-color:#fff !important}.table-bordered th,.table-bordered td{border:1px solid #ddd !important}}html{-webkit-tap-highlight-color:transparent}body{color:#424242;background-color:#fff}abbr[title],a

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 3 icons, 48x48, 32 bits/pixel, 32x32, 32 bits/pixel
Category:	downloaded
Size (bytes):	15086
Entropy (8bit):	3.1857596081402257
Encrypted:	false
SSDEEP:	96:jCKzeBIB035tlTY4aRVUnlf3fLIK5hDMQU7b5XMgwLniWQBeFIGvCztNtT8vud+b:jC0235tVp9sXMdbiH+wzGahuC8AWI4
MD5:	F896EB105D74F9E9F8F69ED1FDE1F8E3
SHA1:	E7A1DEBC6AD02BD48AAD1C4ED788842FF3F6B209
SHA-256:	34662843D486EFDC07BF3D7B6FFA08EE89D187BAB3E99DF2B798766A0E0C701F
SHA-512:	F396C5790A59FA7DBEC45201701BBF2F421A2CE91DA69B82BC7CA38425201C3DD1C6CD2D299EDD9B48378A86E42A671C4B48E51D25208CEA649B32BD0D809AEC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secure.campaigner.com/favicon.ico
Preview:	......00.... ..%..6... ....%..... .h....6..(...0...`..... ......$..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\font-awesome.min[1].css	
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):	28428
Entropy (8bit):	4.775122998814994
Encrypted:	false
SSDEEP:	384:HkyacplRUxcMikva6nYpDmFD1avUjJmpyzdHi:HkyaczawkvA6nYpDmFDfjJmmi
MD5:	361D939436923061B1C2189B0FFF7B9E
SHA1:	D4453D342EC083C9C3090B700FC97F1AF45ACB01
SHA-256:	9AFC8642689B84EB0306CC3947B009634B5B350A8E3F027FA24776E73ED056AF
SHA-512:	671D641715E2E9BB6E29540D9CDF39817C04469EBE86F6CD0D6C97314127BB731BFF71792A79A65C5997EDA3CA661D35463C58DC889738814F2CDD21B7F9A85
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://media.campaigner.com/csb/content/ui-theme/global/fonts/font-awesome/font-awesome.min.css
Preview:	@charset "UTF-8";@font-face{font-family:"Font Awesome";src:url(../font-awesome/font-awesome.eot?v=4.7.0);src:url(../font-awesome/font-awesome.eot?#iefix&v=4.7.0) format("embedded-opentype"),url(../font-awesome/font-awesome.woff2?v=4.7.0) format("woff2"),url(../font-awesome/font-awesome.woff?v=4.7.0) format("woff"),url(../font-awesome/font-awesome.ttf?v=4.7.0) format("truetype"),url(../font-awesome/font-awesome.svg?v=4.7.0#font-awesome) format("svg");font-weight:400;font-style:normal}[class*=" fa-"],[class^=fa-]{font-family:"Font Awesome";position:relative;display:inline-block;font-style:normal;font-weight:400;text-rendering:auto;speak:none;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale;-webkit-transform:translate(0,0);transform:translate(0,0)}.fa-address-book:before{content:"."}.fa-address-book-o:before{content:"."}.fa-address-card:before{content:"."}.fa-address-card-o:before{content:"."}.fa-adjust:before{content:"."}.fa-american-sign-language-interpreti

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\gmail[1].png	
MD5:	DCE2F2B0E50CB1DBB0246D152791CB46
SHA1:	D0A69C159304EDC08DB005163E7A0DAF5A1E98A6
SHA-256:	ACF087C1757F08B0CFD53D59066544D7EF0BFCC50999E77C5813739CD9DC1479
SHA-512:	91054B36EF1673B24E4FE3DC324CBE339F4E9EB72785A6A4C355C7B2A11A9A7C6E188FF9BF5B34FFDD2805D4BBED71EF6CA4975EE3E330FD8D8E383ED64B28EE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://macadavid.cf/000/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....$.@...I0.=.lY.....a...B.4g... T.9Wif..R..o.R.t'.0...?G.9i...L...*..&..s.Vgnkhn...;p[.0.5.....$.....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\PSUEOSZZ\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:	0902219B6E236FBF9D8173D1D452C8733C1BF67B0EB906CC9866EA0C27C2D08F6DA556D01475E9B54E2C6CE797B230BFBD5F39055CE0C71EA4D3E36872C3789
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://macadavid.cf/000/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\PSUEOSZZ\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:	dropped
Size (bytes):	11777
Entropy (8bit):	4.8159515725639555
Encrypted:	false
SSDEEP:	192:K2FI5vEJKnYmrDfG4RywAOT+UY/t4IdtWPtY:1nmRnAKyt48tZ
MD5:	6D1D3C4FD92B63CC534BE0EDF3AF18DC
SHA1:	5F5442FEB5BE60239F185E969C45050A7DBADE2A
SHA-256:	65ADCB045AEFB4D0028A6AF36EC9D42BBD4DAE9AFF2CF85810BB4A6F44D4B25C
SHA-512:	2D42684CF0A44E262C958172C2446974A4AE9B8D17F7208A5FCB690964EE0D56FEB157B9AB6166B8F94FBDCBA027271C36B66784655E8FD96CE0B5522FE71AA
Malicious:	false
Reputation:	low
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\PSUEOSZZ\waves.min[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):	2236
Entropy (8bit):	5.053259830891086
Encrypted:	false
SSDEEP:	48:vBtFf2k6FftjFf+Ffh6FfoFf8FfKFf1bcarXinIoSm+3:v3KTIeeGQnbcarm9+3
MD5:	C8300A2DFDEE9FAF2599A19BB0005AD9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\waves.min[1].css	
SHA1:	F53AB824F686C38070429D9627002CE110E42A8D
SHA-256:	125A82B3D393B34F1C57983398E6ECB6A845EC87F4E29FBAB98F65C25674D000
SHA-512:	CF1356C0A4752965A4314520D42B965E7D8D5F2E00B25C0396237B2C435746407DDECB8194A9362A60CA0CC7818EC08F5F77425EE3856DCBD9E72E9808DF6B8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://media.campaigner.com/csb/content/ui-theme/global/vendor/waves/waves.min.css
Preview:	.waves-effect{position:relative;cursor:pointer;display:inline-block;overflow:hidden;z-index:1;-webkit-user-select:none;-moz-user-select:none;-ms-user-select:none;user-select:none;-webkit-tap-highlight-color:transparent}.waves-effect .waves-ripple{position:absolute;border-radius:50%;width:100px;height:100px;margin-top:-50px;margin-left:-50px;opacity:0;background:rgba(0,0,0,.2);background:radial-gradient(rgba(0,0,0,.2) 0,rgba(0,0,0,.3) 40%,rgba(0,0,0,.4) 50%,rgba(0,0,0,.5) 60%,rgba(255,255,255,0) 70%);transition:all .5s ease-out;transition-property:opacity,-webkit-transform;transition-property:transform,opacity;transition-property:transform,opacity,-webkit-transform;-webkit-transform:scale(0) translate(0,0);transform:scale(0) translate(0,0);pointer-events:none}.waves-effect.waves-light .waves-ripple{background:rgba(255,255,255,.4);background:radial-gradient(rgba(255,255,255,.2) 0,rgba(255,255,255,.3) 40%,rgba(255,255,255,.4) 50%,rgba(255,255,255,.5) 60%,rgba(255,255,255,0) 70%)}.waves-ef

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\8[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=12, height=709, bps=0, PhotometricIntepretation=RGB, orientation=upper-left, width=1200], baseline, precision 8, 1200x646, frames 3
Category:	downloaded
Size (bytes):	161118
Entropy (8bit):	7.5594351594508185
Encrypted:	false
SSDEEP:	3072:WucfAcwuKGuN2q/gSsqnk4br5XUGpppLqfmazv7l04J:OMuKbYOF355XEuAv7lnJ
MD5:	F17B5B1163EFB6D2D47DE6BAE6D3A9CD
SHA1:	6D6964B34BC44C6D2B106ADE1AE675985B96D012
SHA-256:	7829F065E0E10C8466F3D57766E0719421B7B652F6A1082F21B98702F1B28A30
SHA-512:	7C0CBEF1D3CAE66A18C74544E593803C2EEC56817E762A385D54437BC7D597B2598886B0C0EDF72C6E934E9F146CEFC89392A492DB5425A1071E61CA1F15685
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://macadavid.cf/000/images/8.jpg
Preview:	.....Exif..MM.*.....(.....1.....".....2.....i.....$.....'.....'.Adobe Photoshop CC 2015 (Windows).2020:01:21 13:41:42.....0221.....r.....z.(.....%.....H.....H.....Adobe_CM.....Adobe.d.....V...."..... ?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?.....q..KJG..x.."....]..TX...[^.m...R.....X.5..j?p.A.RI%0...MN.$..@.4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\KFOjCnqEu92Fr1Mu51S7ACc6CsI[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22080, version 1.1
Category:	downloaded
Size (bytes):	22080
Entropy (8bit):	7.970620647480227
Encrypted:	false
SSDEEP:	384:BfnIIA0zhdg/5oXRAZDRsZObG141wGUaBgKYADioTCgZM6+HJtWjbmMbQMbL2nNQ:B00zhdW7ZDRsR141wYAoTCGUptzMbqnu
MD5:	FA8878D8872A2AC4BEB377CDAE15566A
SHA1:	34EE72B0E553C3EFA41A7E0DF4EB710596469A10
SHA-256:	8411023A027610AEB3DC333438E12A17222163AE78817C5395DA04548ED30150
SHA-512:	112ED53A4A18EB3378A57B154566C0F1AF438FF400EBE453253F5E2465B6A07370B447736EACB99114ED43E05CAE5A3A019BE6886D50EB15FA1E2D6F35D9AFBA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOjCnqEu92Fr1Mu51S7ACc6CsI.woff
Preview:	wOFF.....V@.....0.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...N...`t..dcmap.....#cvt .....\...\1..Mfpgm...4...2.....$.gasp...h.....glyf...t..Bf..s...hdmx..N....l....(/./head..OH...6...6...vhhea..O....#...$....hmtx..O.....*:8loca..R@.....*.imaxp..T8... ... .4..name..TX.....!.>gpost..U4..... .a.dprep..UL.....X9..x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x....%Y....Wm=..mo..k.m....rl...m.g"^..../..[.}.S...\.mD...1..G>..giz...=C..}.y....|o..c.x.R.r"B.....m.../.&./6..5D.AGX.....)<'.)....?.... .Y4>|1...ES.Gc...FO.>$../...}RCl..T.zD..uZ4~D.._OK.$.Z.(..JR...\..\..\..\.\.....*'n..6:x...b,..$...?.g:./y.iLg.3..l.0.y.g..X..V...d.#O...0....b7{..>.n.iD.V....." e.\A..OR.kwp.].....6p..."ZE..%...e.u3..L..V...W.7b..L.3.L1K...Ts..$6.-b.....9...b@..!1,...v.C...{...dox.G(...|a%E:.Fn.Nn.^n.....Sf..E)...k....<g..){....|.....DT..N....Hy.F.Jez....._?7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\KFOjCnqEu92Fr1Mu51TzBic6CsI[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 21656, version 1.1
Category:	downloaded
Size (bytes):	21656
Entropy (8bit):	7.971138981009303
Encrypted:	false
SSDEEP:	384:vfqIIA0zh/VF0+5SLHCK+yo5HHx/KnMpljPSiQZxLZtspfA9JaXWWyBuM9rgaSJV:vJ0zh/VFv0Hm15HHtKnalaiQfZtsp49o
MD5:	147F4E11CE73A22AAC9C6C2822290953

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\KFOjCnqEu92Fr1Mu51TzBic6Csl[1].woff	
SHA1:	EEFEA89A9C36F8B1A7CA99372A7E0E05C92EADD6
SHA-256:	A22585CFD64238EF14B1B383B5B9A8BAD7C89E354C09FC0886067E876687A38C
SHA-512:	3D7ADA26B281864CE394CB49974A9EA59D28FA8C2EFB006DF31DCAE66DB4684223BDB42B8234A5135BF1B4F834E91DE415E44558EB2CF2346086C8879397058
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOjCnqEu92Fr1Mu51TzBic6Csl.woff
Preview:	wOFF.....T.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...O...`u...cmap.....#cvt .....J...J..,ofpgm...$...3....c...gasp...X.....glyf... d..@...o.H.6.hdmx..MD...n....,..0head..M....6...6...`hhea..M....#...$....hmtx..N.....1)loca..P.....maxp..R.... ... .4..name..R..... .=$post..S..... .a.dprep..S.....9 ..Bx...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x....%Y....Wm=..mo..k.m....rl...m.g"^..../..[.}.S...\.mD...1..G>..giz...=C..}.y....|o..c.x.R.r"B.....m...../.&. /6..5D.AGX.....)<'.)....?.... .Y4>|1...ES.Gc...FO.>$.../...}RCl..T.zD..uZ4~D._OK.$.Z.(..JR...\..\..\..\.....*'n..6:x...b,..$...?.g:./y.iLg.3..l.0.y.g..X..V...d.#O...0....b7{..>.n.iD.V....." e.\A..OR.kwp.].....6p..."ZE..%...e.u3..L..V...W.7b..L.3.L1K...Ts..$6.-b.....9...b@..!1,...v.C....{...dox.G(...|a%E:.Fn.Nn.^n.....Sf..E)...k....<g..){....|.....DT..N....Hy.F.Jez....._? 7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\KFOlCnqEu92Fr1MmWUlfBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20396, version 1.1
Category:	downloaded
Size (bytes):	20396
Entropy (8bit):	7.974131663185347
Encrypted:	false
SSDEEP:	384:SfXdUIIA0zhyKR28ePpAwxZ5M3py8wtshtdf45DEVTGdYb7H2Q/VEgm:Svdj0zhbRmjIQ8wtsV4lEVGdY3/i/
MD5:	68D6DABFE54E245E7D5D5C16C3C4B1A9
SHA1:	7FDAB895EAEBECEDB3FB5473EAB94A1B292CEF19
SHA-256:	A01A632E56731A854F35701AA8C3A6A19A113290D9032FF9048F8064C45383BD
SHA-512:	44EB151F85178A2F9600E85AD43FAE470FABE0F247C9A03E67931B36028E600C7550D9DE2D69B3576A06577A5DEAF54822EE4BDC9DCBB47588D1972C8A959D4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmWUlfBBc-.woff
Preview:	wOFF.....O.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...Q...`u...cmap.....#cvt .....H...H+~..fpgm...$...3...._...gasp...X..... ...glyf...d..< ..l..C^]hdmx..H....m....03#7head..H....6...6...\hhea..I,... ...$.&..hmtx..IL....."J.loca..K.....maxp..M.... ... .4..name..M.....~..9.post..N..... .m.dprep..N.....)* v60x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x....%Y....Wm=..mo..k.m....rl...m.g"^..../..[.}.S...\.mD...1..G>..giz...=C..}.y....|o..c.x.R.r"B.....m...../.&. /6..5D.AGX.....)<'.)....?.... .Y4>|1...ES.Gc...FO.>$.../...}RCl..T.zD..uZ4~D._OK.$.Z.(..JR...\..\..\..\.....*'n..6:x...b,..$...?.g:./y.iLg.3..l.0.y.g..X..V...d.#O...0....b7{..>.n.iD.V....." e.\A..OR.kwp.].....6p..."ZE..%...e.u3..L..V...W.7b..L.3.L1K...Ts..$6.-b.....9...b@..!1,...v.C....{...dox.G(...|a%E:.Fn.Nn.^n.....Sf..E)...k....<g..){....|.....DT..N....Hy.F.Jez....._? 7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\KFOmCnqEu92Fr1Mu4mxM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20332, version 1.1
Category:	downloaded
Size (bytes):	20332
Entropy (8bit):	7.970235088150752
Encrypted:	false
SSDEEP:	384:U0iwaxoOUPVkOJJSu6SsCKTIRDqG9oHKwZh98OSv+MsgkAOY:75mlUmOSu1guh+fZhLSxkAr
MD5:	DC3E086FC0C5ADDC09702E111D2ADB42
SHA1:	B1138B84FF19EAC5F43C4202297529D389BD09B7
SHA-256:	EA50AC7FDDB61A5CE248A7F8B3A31A98FE16285E076B16E6DA6B4E10910724BB
SHA-512:	10123C785C396CF0844751A014413ECF4D058AD0C00CAAEF5F8FFEF504C370F03EACD0B3C2A49211EEE0877B7AE7D0EF6E01264F04FC910C2660584B5E943BE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOmCnqEu92Fr1Mu4mxM.woff
Preview:	wOFF.....Ol.....x.....GDEF.....G...d....GPOS.....!GSUB.....OS/2...L...P...`t...cmap.....#cvt .....T...T+...fpgm.....5....w.`.gasp...@.....glyf.. .L..;...m.&.x.hdmx..H....m....'/./head..H....6...6.j.zhhea..H.... ...$....hmtx..H.....]uloca..Kp.....m,maxp..Mp... ... .4..name..M.....t.U9.post..N`..... .m.dprep..Nt.....I .f..x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x...l\..F..3...N..q)..a\|.....^..33..c.....p"y.iT....<Gg...!.3...T1...{.g0.u.y.....m.|.k..NF.....mox.;...7&.Y. .C.R_[.T.c..-.=...9:...a*j.G.....O.Q".6...>...(?...~...._.2:..K4....S%...jbr).....*....e.U..-..X.3.ILQ....z..!.f:...<.W.#...e.c=...&6...lc;...3<.s<....H.i2..N..t..)Ns...#`..".).[...._..T..T.. ...+l..=..O.....Z..F...r..eM.f.Y.....-...r.\.s6.r.,...:.<$..#.l..F.$.2#.e..].[.....yR...e.|{..O..`)..U.0.e.50.Z.b../cM..i.&O._..+.Y.W...;z....j.p._.o..[CL.)n'.UGx..>).X..MJ..Fr..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\Telerik.Web.UI.WebResource[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	25236
Entropy (8bit):	5.451873216624558
Encrypted:	false
SSDEEP:	384:evx2xPyTQ+HaYO0v9IsxqWj8Dc3mJwOwTyxPC1Ggrfgkyp+:e2mlh1Is4Wj8Dc3mJwOwTR1Ggrfgkyp+
MD5:	94B23F7CCA443A0E9C3E57E86E648DB1
SHA1:	B79ED79A11494DA1ABD911ABFC5AA5C0F3B7547C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\Telerik.Web.UI.WebResource[1].css	
SHA-256:	E2610CAA52577A2E9C0D5687917B50DB29910F1C87450579825DE9D71ECF9937
SHA-512:	003A9E365209794975B911188D9A32AEC478EA0BAC58C6E25B217496D156C8BEF9FB0A5827AA6B75414F8DFC7F610EC65BADC5B973BC33D875D253892D5A3FAC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://media.campaigner.com/csb/Telerik.Web.UI.WebResource.axd?d=PMrIT5dOWaVYIcpFWUE4nGT9ocicfa2XofFEKerfqG0NFa8QfPNf_0edVcdrIlKXVLquybnZr6vWHl1Oz5ovkCSuzOKDIztFTpc5AvV6exGGiq7W0&t=637527440300000000&compress=1&_TSM_CombinedScripts_=%3b%3b%7c637562487341584209%3af7b0867a%3abd404622%3bTelerik.Web.UI%2c+Version%3d2021.1.330.45%2c+Culture%3dneutral%2c+PublicKeyToken%3d121fae78165ba3d4%3aen-US%3a6ddfaaf7-68e8-4aa2-a15d-336c3a8f9e4b%3a92753c09%3bTelerik.Web.UI.Skins%2c+Version%3d2021.1.330.45%2c+Culture%3dneutral%2c+PublicKeyToken%3d121fae78165ba3d4%3aen-US%3a7108f410-54c0-4ea8-9782-917723c63996%3a42d1d057
Preview:	/* START */../********** Social Media Settings popup **********/../********** margin: 0 0 10px;..}..#pnlSocialSharingSettings * {.. vertical-align: middle;..}..#pnlSocialSharingSettings p {.. margin: 0 0 10px;..}..#pnlSocialSharingSettings ul {.. list-style: none outside none;.. margin: 10px 0;.. padding-left: 0;..}..#pnlSocialSharingSettings li {.. padding-left: 0;..}..#pnlSocialSharingSettings li li {.. padding-left: 25px;.. margin-top: 10px;..}..#pnlSocialSharingSettings .label {.. color: #757575;.. line-height: 28px;.. padding-right: 5px;.. padding-left: 23px;..}....#pnlSocialSharingSettings span .asterisk..{...font-size: 20px; ...vertical-align: top;..}....#pnlSocialSharingInfo div..{...padding-bottom: 10px;..}....#pnlSocialSharingInfo p {.. padding-top: 10px;.. font-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\archive[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	23144
Entropy (8bit):	5.916092051785858
Encrypted:	false
SSDEEP:	384:3IQ84R+uhb0r1y2VE+7kyVYm7gcmQZSrnqqiygeD+f+h2Y+/2arAHUZh5a:3l84R+m0r8EE+7kyVB0clrnqZA+WcDOH
MD5:	A997CCCC520C1654D96D81B3F6594C5A
SHA1:	49A26166048725C46E8D03C3D6A425BB63ABB919
SHA-256:	48AC55C928300D04B5D8577959A4477EBE04DFA7389C131B7E1D8D7579E1FEE5
SHA-512:	0EEBDA6AA9B4C1234FC8A4ADF04EF8EB1474B7ACF6733E608A6DB1FECEBADEBB846F2CCC3DC0064328443F393F619470041EAC277CC2ACABC778C43CF5F0FCF4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secure.campaigner.com/CSB/Public/archive.aspx?args=NTIxMzE2MjA%3d&acc=NzY2ODM4
Preview:	..<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">..<html xmlns="http://www.w3.org/1999/xhtml">..<head id="Head1"><title>...Fax Massage2..</title>.. Stylesheets -->.. <link rel="stylesheet" href="https://media.campaigner.com/csb/node_modules/campaigner-core/src/style/theme/campaigner/bootstrap.min.css" /><link rel="stylesheet" href="https://media.campaigner.com/csb/node_modules/campaigner-core/src/style/theme/campaigner/bootstrap-extended.min.css" /><link rel="stylesheet" href="https://media.campaigner.com/csb/node_modules/campaigner-core/src/style/theme/campaigner/campaigner.min.css" />.. Plugins -->.. <link rel="stylesheet" href="https://media.campaigner.com/csb/content/ui-theme/global/vendor/waves/waves.min.css" />.. Fonts -->.. <link rel="stylesheet" href="https://media.campaigner.com/csb/content/ui-theme/global/fonts/font-awesome/font-awesome.min.css" /><link rel="stylesheet"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\bootstrap-extended.min[1].css	
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):	269032
Entropy (8bit):	5.023521491620771
Encrypted:	false
SSDEEP:	6144:FAJP66Zudd3GVRsa55/XyGMiQkhOQzGBPw2:FAJP66Zudd3GVRsa55/XyGM1
MD5:	4F62EF2F96809A353146173F765C94BA
SHA1:	E1AE433077C32C1ECDF4ACC9A252036457C0A7CE
SHA-256:	DE3E5368C90F1FE431FB2DDC40AB83DD46FBE69F837507E7CDC402801A721519
SHA-512:	392B089CDC03B95E8F3EBC32868D8163435D661ABF1E66AE76A68E22B258F21F5BE1A2D9476590F7FDB007C322E61C78599988F1E36B7910FA9DC531B159974F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://media.campaigner.com/csb/node_modules/campaigner-core/src/style/theme/campaigner/bootstrap-extended.min.css
Preview:	@charset "UTF-8";html{font-size:14px}button{color:inherit}a:active,a:hover,a:focus{outline:0}a.text-body{color:#757575}a.text-body,a.text-body:hover,a.text-body:focus{text-decoration:none}a.text-action{color:#9e9e9e}a.text-action,a.text-action:hover,a.text-action:focus{text-decoration:none}a.text-action:hover,a.text-action:focus{color:#bdbdbd}a.text-action .icon+span{margin-left:3px}a.text-like{color:#9e9e9e !important}a.text-like,a.text-like:hover,a.text-like:focus{text-decoration:none}a.text-like.active,a.text-like:hover,a.text-like:focus{color:#e53935 !important}.text-action+.text-action{margin-left:6px}b,strong{font-weight:inherit}b,strong{font-weight:500}h1,h2,h3,h4,h5,h6,.h1,.h2,.h3,.h4,.h5,.h6{text-shadow:rgba(0,0,0,.15) 0 0 1px}h1 .icon:first-child,h2 .icon:first-child,h3 .icon:first-child,h4 .icon:first-child,h5 .icon:first-child,h6 .icon:first-child,.h1 .icon:first-child,.h2 .icon:first-child,.h3 .icon:first-child,.h4 .icon:first-child,.h5 .icon:first-child,.h6 .icon:first-ch

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\combobox.campformcombo[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	5117

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\combobox.campformcombo[1].css	
Entropy (8bit):	4.982866253609158
Encrypted:	false
SSDEEP:	48:HD/xLyi9sBBdYV9CburVnbZdFNoOBPMd7JQ4Pd1yFah2VNTXH54Zjl0I:jlZYe9pVVGOJc7JQCeah2VlXH5ijT
MD5:	344B88C4A8D2591B68DB2448CE632EE9
SHA1:	F56D6F1523398EBD70A98D80CA8C0ADD074BE0A7
SHA-256:	3E8F432938BB68E2D2EE6CFB81DAE2885267C58B1ABC04F663266EB0EE028D5B
SHA-512:	0D64D67E79796030A25BA3B1D5AC11C2A3D6BFE60C6E6D91554590E244D6ABB39E5B67CBD4C895438F52D7CCEB2D2A708AFA930EAD94FC7F5E05C3D45D5951A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://media.campaigner.com/csb/app_themes/lightning/combobox.campformcombo.css
Preview:	.RadComboBox_campFormCombo {.. color: #404040;.. font-family: Arial, sans-serif; }.. .RadComboBox_campFormCombo .rcbInner {.. border-color: #B1D1EA;.. border-width:2px !important;.. color: #404040;.. background-color: #ffffff;.. padding: 4px 8px !important;.. border-radius: 4px;.. box-shadow: inset 0 1px 1px rgba(0, 0, 0, 0.075); }..... .RadComboBoxDropDown_campFormCombo .rcbInput.. {.. padding: 0 !important;.. }.... .RadComboBox_campFormCombo .rcbActionButton {.. border-color: #B1D1EA;.. color: #404040;.. background-color: #ffffff;.. padding: 6px;.. border-radius: 0 4px 4px 0; }.. .RadComboBox_campFormCombo .rcbLabel {.. padding-top: 7px; }.. .RadComboBox_campFormCombo .rcbHovered {.. border-color: #519ECC;.. color: #404040;.. background-color: #ffffff; }.. .RadComboBox_campFormCombo .rcbHovered .rcbActionButton {.. border-color: #519ECC;.. color: #404040;.. background-color: #e6e6e6; }.. .RadComboBox_campFormC

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\content-background[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 4 x 4, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	126
Entropy (8bit):	5.397826327932424
Encrypted:	false
SSDEEP:	3:yionv//thPlJ7t3lllHRthwkBDsTBZt6wVNHl2xlxQ0Lll/suB:6v/lhPJlll5nDspj7SD//suB
MD5:	196C2971B40B6E81E0C423689E54FAF8
SHA1:	35D4A81023F92531A066D1BC4C0FB876C7C3C310
SHA-256:	BCDB31B3B52F7C3F18EFB0934F0CCCD3256ECD773A4FB0C9AD99D8421E41D846
SHA-512:	C6C2D856187F1404A0A7F065973DFD3CFF3F8CB3645D3739BAF0B3F6AE4B4C677FA3EEEAAFEEC47A21E9AFA7F281C77617B68C06D8EE0826D091B9FF50AB0CAD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://media.campaigner.com/editorassets/themes/soak-it-up/content-background.png
Preview:	.PNG........IHDR.....~....tEXtSoftware.Adobe ImageReadyq.e<....IDATx.b`@..0..G.....w...>n.0....IEND.B`..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	211
Entropy (8bit):	5.026484232218891
Encrypted:	false
SSDEEP:	6:0IFFwKh+56ZRWHMqh7izlpdBEoKOEEJTONin:jFWmO6ZRoMqt6p3EondOY
MD5:	04F7435B2672FBE66984EA436E7087C6
SHA1:	44896875E69B297EB979CC0D3E8522D872656BA8
SHA-256:	F9088C15A062F0C7708C3864C5E261A2E4961DFEB0F150DF744FAEC2E3B74AD6
SHA-512:	9A1D01A7FAC3D6B205CFA37C05A93AFA9D903D4D35DCB16E31D3A31D19CD65B8DE5D66E626BC7F70D07841C779E20CD2C2DD6254824F96DE0E8E576E156F17D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Yellowtail&display=swap
Preview:	@font-face {. font-family: 'Yellowtail';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/yellowtail/v11/OZpGg_pnoDtINPfRIlLohlvHxw.woff) format('woff');.}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\free-v4-shims.min[1].css	
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\WJ8I2OL4\free.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	60351
Entropy (8bit):	4.728641238865369
Encrypted:	false
SSDEEP:	768:0Uh31IPiyXNq4YxBowbgJlkwF//zMQyYJYX9Bft6VSz8:0U0PxXE4YXJgndFTfy9lt5Q
MD5:	390B4210E10C744C3C597500BCF0B31A
SHA1:	2600C7C2F25D7DBCBC668231601E426010DC6489
SHA-256:	C2819CA1F7AD1AF7BA53C4EDFDFD395C547BCB16D29892A234D7860C689ED929
SHA-512:	E8A7E466BE8CC092E12994B51A6A8A39E2FBB66DD48221BCF499BB89365B4004D73C1909F8FE0BBBBF13907D5901D76FFE127D92FDD7493853646F83F5985CB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.3/css/free.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,.fab,.fad,.fal,.far,.fas{-moz-osx-font-smoothing:grayscale;-webkit-font-smoothing:antialiased;display:inline-block;font-style:normal;font-variant:normal;text-rendering:auto;line-height:1}.fa-lg{font-size:1.33333em;line-height:.75em;vertical-align:-.0667em}.fa-xs{font-size:.75em}.fa-sm{font-size:.875em}.fa-1x{font-size:1em}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-6x{font-size:6em}.fa-7x{font-size:7em}.fa-8x{font-size:8em}.fa-9x{font-size:9em}.fa-10x{font-size:10em}.fa-fw{text-align:center;width:1.25em}.fa-ul{list-style-type:none;margin-left:2.5em;padding-left:0}.fa-ul>li{position:relative}.fa-li{left:-2em;position:absolute;text-align:center;width:2em;line-height:inherit}.fa-border{border:.08em solid #eee;border-radius:.1em;padding:.2em .25em .15em}.fa-pul

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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\Temp\~DF8357F423EC5F7CBF.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4795834808788184
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loWF9loa9lW3NTGuZ:kBqoI1j3JGI
MD5:	74DA459EBF114AAE9330B89EE48F0E36

C:\Users\user\AppData\Local\Temp\~DF8357F423EC5F7CBF.TMP	
SHA1:	B30A548F9627C9958ECB88DC873E37D4BE7755C5
SHA-256:	D07DDDC864066782AA8664F0DA667904E3E645CBC63DC3EA24DFCCC703485267
SHA-512:	DE583CD46E965CE743EA9493B76D40D381D5BA67E83808C31C59B19E05364D88D1C80F08A44EEA90DEDD4CBBEAE91D90E62D83C55525592922417C6183D7BD 6
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFB9B088C2B4A83B25.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	88166
Entropy (8bit):	2.6843878645025265
Encrypted:	false
SSDEEP:	768:+ZR3FkbuQpJOazyvXZR3FkbuQpJOazyv:iwppJdzywppJdz
MD5:	3E46AD48745D3123A166BD2D5EE5CC07
SHA1:	86023C18EB77E89A815F3CE01D2AE9C2DC0AEB83
SHA-256:	A2E36C5610BD8F1D36AE7ACEE225C0571F86849893CE10DEAEDFF3C468C5A950
SHA-512:	3786971E91D07F31CC0F86C1584343E300FC61F20DAF4B3132141592ABBE96CC14292EB4BFADE3AF22D84B7FB02F71BC0E27BDB93955C122D9E014C1F65CB7E E
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFDC4F66DA4FD5A51A.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.3014088640290203
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laANGiL:kBqoxxJhHWSVSEabV
MD5:	CB66D5A187E60DD8C6DE8C04BF806576
SHA1:	89B1BF26A465627E9F248F82EAE0166AA8C62B76
SHA-256:	B2786488E87038B71C4DB196C2799D992565C8AF4BE7F8B42CBFCCF6A82E7152
SHA-512:	39B4558C409948375E8AD057E8F1654D169C889D041C77B39BF82D9D5B4EF5A7350E3DCECEF84997CC3220F29541C529B67F2682AF7758D720D73A661C21FF93
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 17:49:42.623706102 CEST	192.168.2.3	8.8.8.8	0x1c1e	Standard query (0)	secure.campaigner.com	A (IP address)	IN (0x0001)
Jun 11, 2021 17:49:43.428599119 CEST	192.168.2.3	8.8.8.8	0x6e0b	Standard query (0)	media.campaigner.com	A (IP address)	IN (0x0001)
Jun 11, 2021 17:49:46.062438965 CEST	192.168.2.3	8.8.8.8	0x7438	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Jun 11, 2021 17:49:46.595155001 CEST	192.168.2.3	8.8.8.8	0x788d	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Jun 11, 2021 17:50:04.747205019 CEST	192.168.2.3	8.8.8.8	0xeb75	Standard query (0)	secure.campaigner.com	A (IP address)	IN (0x0001)
Jun 11, 2021 17:50:06.999989033 CEST	192.168.2.3	8.8.8.8	0x4bc4	Standard query (0)	macadavid.cf	A (IP address)	IN (0x0001)
Jun 11, 2021 17:50:07.969733953 CEST	192.168.2.3	8.8.8.8	0xe8d7	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jun 11, 2021 17:50:07.980539083 CEST	192.168.2.3	8.8.8.8	0xdd21	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Jun 11, 2021 17:50:07.985718012 CEST	192.168.2.3	8.8.8.8	0x424d	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Jun 11, 2021 17:50:07.992800951 CEST	192.168.2.3	8.8.8.8	0x83b8	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jun 11, 2021 17:50:08.391988039 CEST	192.168.2.3	8.8.8.8	0x2d81	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 17:49:42.682534933 CEST	8.8.8.8	192.168.2.3	0x1c1e	No error (0)	secure.campaigner.com		216.24.224.42	A (IP address)	IN (0x0001)
Jun 11, 2021 17:49:43.493611097 CEST	8.8.8.8	192.168.2.3	0x6e0b	No error (0)	media.campaigner.com	akamai-118696.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:49:46.126177073 CEST	8.8.8.8	192.168.2.3	0x7438	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:49:46.126177073 CEST	8.8.8.8	192.168.2.3	0x7438	No error (0)	scontent.xx.fbcdn.net		31.13.92.14	A (IP address)	IN (0x0001)
Jun 11, 2021 17:49:46.653394938 CEST	8.8.8.8	192.168.2.3	0x788d	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:49:46.653394938 CEST	8.8.8.8	192.168.2.3	0x788d	No error (0)	star-mini.c10r.facebook.com		31.13.92.36	A (IP address)	IN (0x0001)
Jun 11, 2021 17:50:04.810801029 CEST	8.8.8.8	192.168.2.3	0xeb75	No error (0)	secure.campaigner.com		216.24.224.42	A (IP address)	IN (0x0001)
Jun 11, 2021 17:50:07.068515062 CEST	8.8.8.8	192.168.2.3	0x4bc4	No error (0)	macadavid.cf		66.29.132.67	A (IP address)	IN (0x0001)
Jun 11, 2021 17:50:08.020180941 CEST	8.8.8.8	192.168.2.3	0xe8d7	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:50:08.041990042 CEST	8.8.8.8	192.168.2.3	0xdd21	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Jun 11, 2021 17:50:08.041990042 CEST	8.8.8.8	192.168.2.3	0xdd21	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Jun 11, 2021 17:50:08.048825026 CEST	8.8.8.8	192.168.2.3	0x424d	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:50:08.054421902 CEST	8.8.8.8	192.168.2.3	0x83b8	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jun 11, 2021 17:50:08.054421902 CEST	8.8.8.8	192.168.2.3	0x83b8	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 17:50:08.455728054 CEST	8.8.8.8	192.168.2.3	0x2d81	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.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
Jun 11, 2021 17:49:46.214656115 CEST	31.13.92.14	443	192.168.2.3	49709	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 26 02:00:00 CEST 2021	Wed Aug 25 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2013	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jun 11, 2021 17:49:46.214868069 CEST	31.13.92.14	443	192.168.2.3	49710	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 26 02:00:00 CEST 2021	Wed Aug 25 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2013	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jun 11, 2021 17:49:46.744153976 CEST	31.13.92.36	443	192.168.2.3	49712	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 26 02:00:00 CEST 2021	Wed Aug 25 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2013	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jun 11, 2021 17:49:46.745537043 CEST	31.13.92.36	443	192.168.2.3	49713	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 26 02:00:00 CEST 2021	Wed Aug 25 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2013	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jun 11, 2021 17:50:07.452102900 CEST	66.29.132.67	443	192.168.2.3	49720	CN=macadavid.cf CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jun 10 02:00:00 CEST 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sat Jun 11 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jun 11, 2021 17:50:07.498461008 CEST	66.29.132.67	443	192.168.2.3	49721	CN=macadavid.cf CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jun 10 02:00:00 CEST 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sat Jun 11 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jun 11, 2021 17:50:08.143033028 CEST	104.18.11.207	443	192.168.2.3	49726	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		
Jun 11, 2021 17:50:08.144428968 CEST	104.18.11.207	443	192.168.2.3	49727	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		
Jun 11, 2021 17:50:08.149036884 CEST	104.16.19.94	443	192.168.2.3	49729	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 11, 2021 17:50:08.157022953 CEST	104.16.19.94	443	192.168.2.3	49731	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	Thu Oct 21 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6112 Parent PID: 792

General

Start time:	17:49:40
Start date:	11/06/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff696fa0000
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

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 2476 Parent PID: 6112

General

Start time:	17:49:41
Start date:	11/06/2021

Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6112 CREDAT:17410 /prefetch:2
Imagebase:	0x1180000
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 Show Windows behavior

Registry Activities Show Windows behavior

Disassembly