ID: 435106
Cookbook: browseurl.jbs
Time: 23:02:06
Date: 15/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

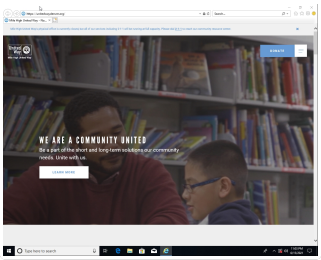
Windows Analysis Report http://www.unitedwaydenver.…

Overview

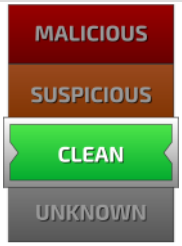
General Information

Sample URL:	http://www.unitedwaydenver.org/
Analysis ID:	435106
Infos:	

Most interesting Screenshot:



Detection

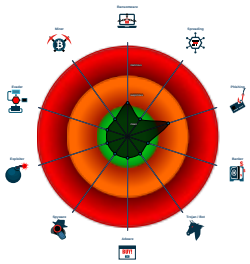


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Form action URLs do not match mai…
- Found iframes
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 5828 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5640 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5828 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

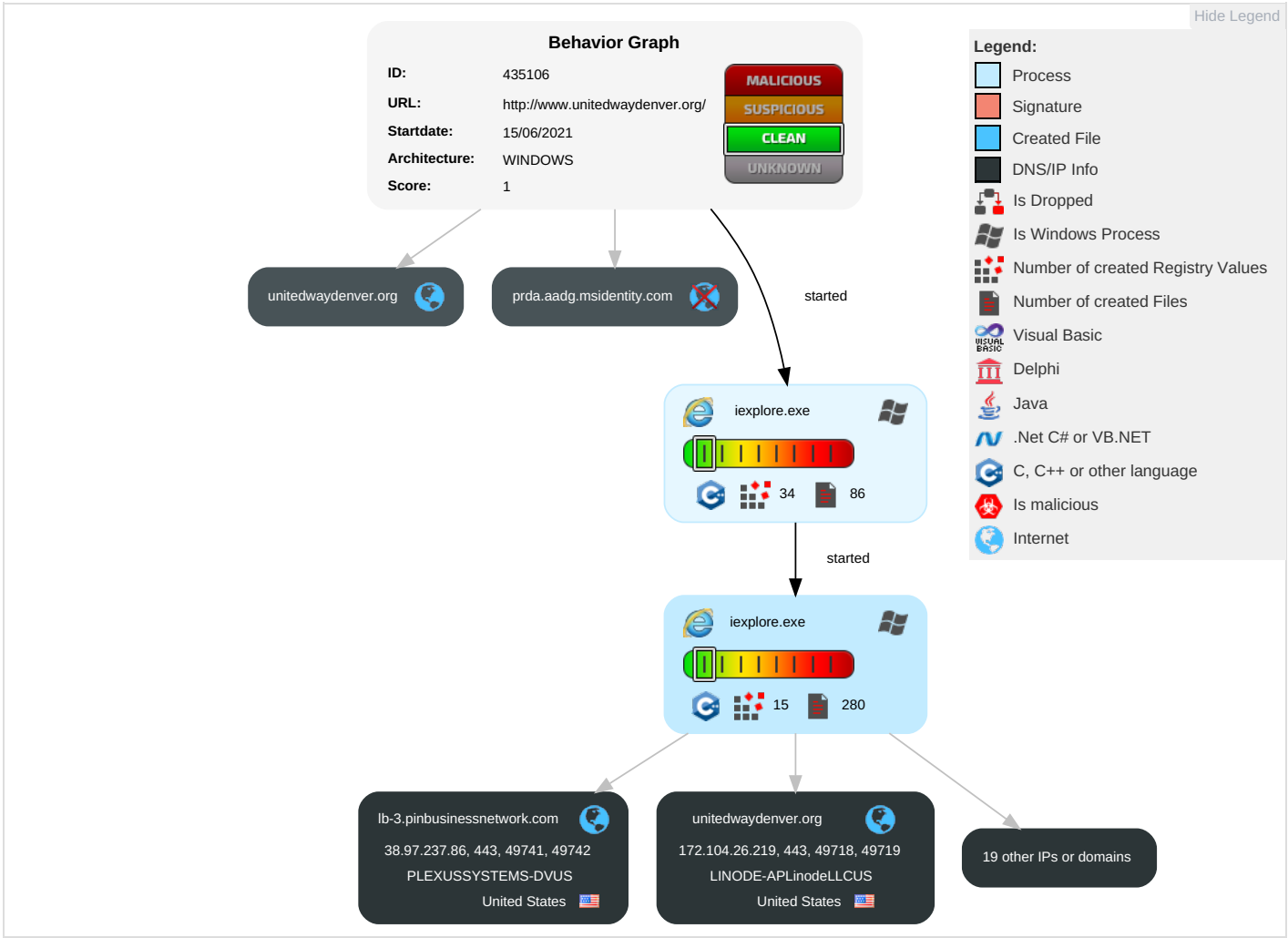
Click to jump to signature section

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
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 2	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 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap	

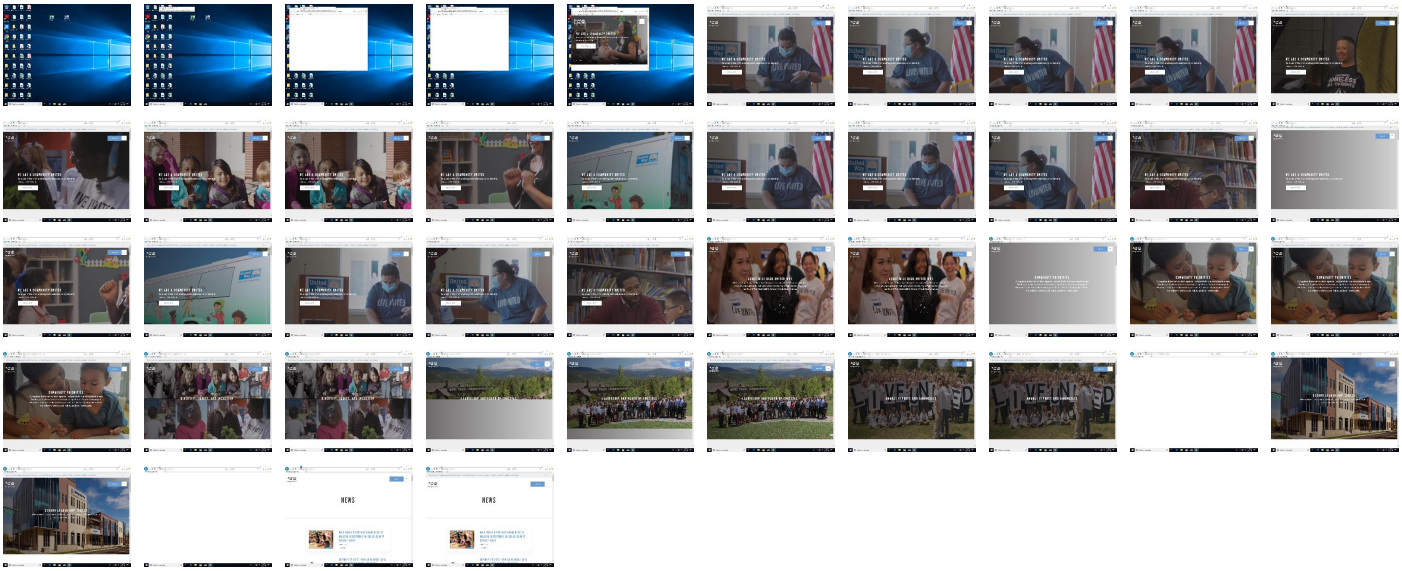
Behavior Graph

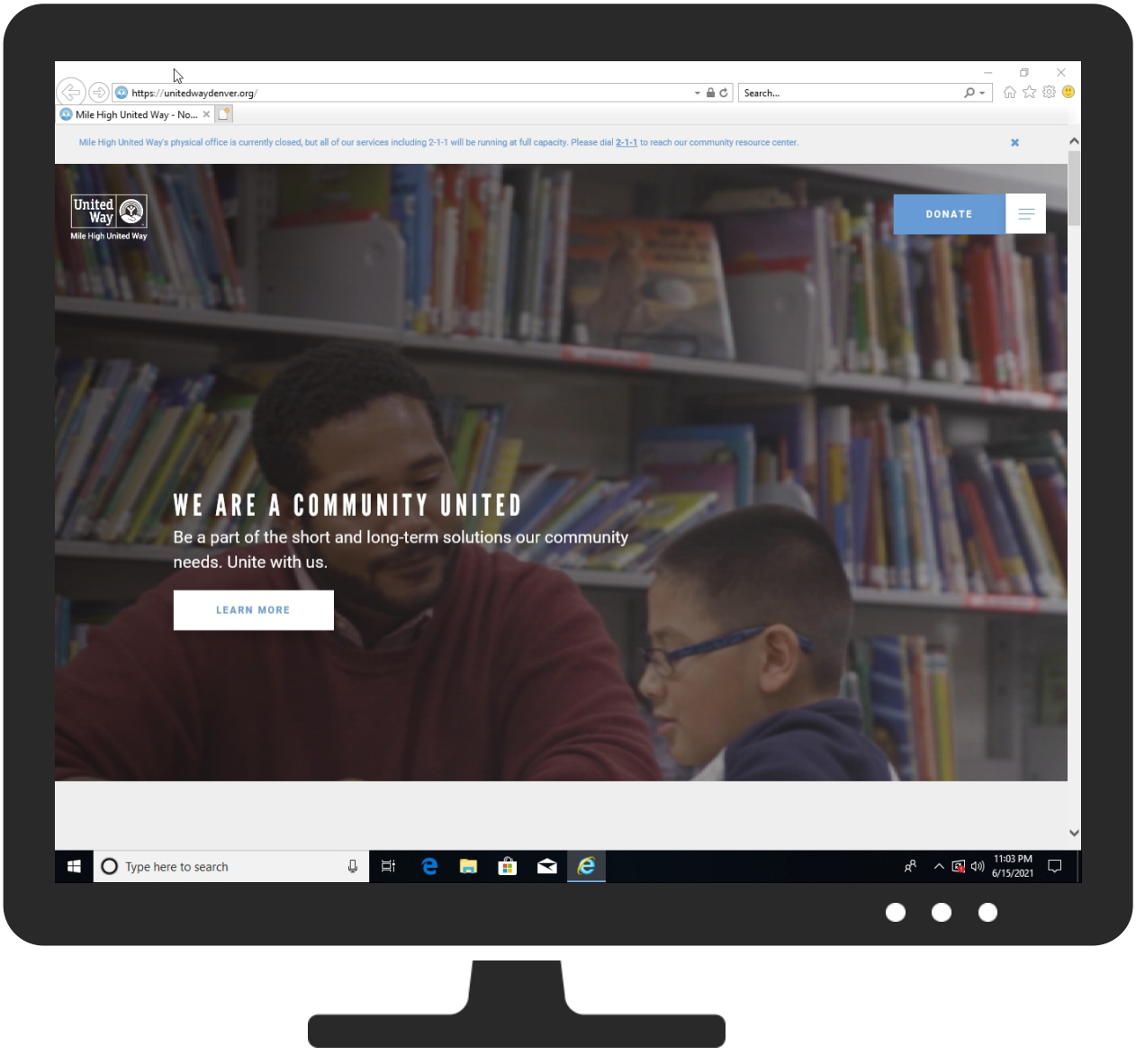


Screenshots

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://www.unitedwaydenver.org/	0%	Virustotal		Browse
http://www.unitedwaydenver.org/	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://unitedwaydenver.org/wp-content/uploads/2018/04/cropped-favicon-lightblue-32x32.png	0%	Avira URL Cloud	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://bestiejs.github.io/json3	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.google.de	142.250.186.99	true	false		high
scontent.xx.fbcdn.net	185.60.216.19	true	false		high
alb01-swappy-production-272196969.us-east-1.elb.amazonaws.com	54.174.92.145	true	false		high
pixel.sitescout.com	66.155.71.150	true	false		high
stats.l.doubleclick.net	74.125.140.156	true	false		high
www.unitedwaydenver.org	172.104.26.219	true	false		unknown
unitedwaydenver.org	172.104.26.219	true	false		unknown
prometheusintelligencetechnology.com	23.176.96.6	true	false		unknown
pixel-a.sitescout.com	66.155.71.149	true	false		high
trackingpin.com	23.176.96.22	true	false		unknown
lb-3.pinbusinessnetwork.com	38.97.237.86	true	false		unknown
ipv6.prometheusintelligencetechnology.com	unknown	unknown	false		unknown
use.typekit.net	unknown	unknown	false		high
cdn.callreports.com	unknown	unknown	false		high
pixel-sync.sitescout.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
ads.pinbusinessnetwork.com	unknown	unknown	false		unknown
p.typekit.net	unknown	unknown	false		high
dsppixel.pinbn.net	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://unitedwaydenver.org/news/	false		unknown
http://https://unitedwaydenver.org/about/	false		unknown
http://https://unitedwaydenver.org/cobank-leadership-center/	false		unknown

Name	Malicious	Antivirus Detection	Reputation
http://https://unitedwaydenver.org/leadership-and-board/	false		unknown
http://https://unitedwaydenver.org/annual-reports-and-financials/	false		unknown
http://https://unitedwaydenver.org/diversity-equity-and-inclusion/	false		unknown
http://https://unitedwaydenver.org/	false		unknown
http://www.unitedwaydenver.org/	false		unknown
http://https://unitedwaydenver.org/community-goals/	false		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.155.71.149	pixel-a.sitescout.com	Canada		13768	COGECO-PEER1CA	false
23.176.96.6	prometheusintelligencetechnology.com	United States		20029	H5-DATA-CENTERS-DENVERUS	false
38.97.237.86	lb-3.pinbusinessnetwork.com	United States		397571	PLEXUSSYSTEMS-DVUS	false
54.174.92.145	alb01-swappy-production-272196969.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
66.155.71.150	pixel.sitescout.com	Canada		13768	COGECO-PEER1CA	false
172.104.26.219	www.unitedwaydenver.org	United States		63949	LINODE-APLinodeLLCUS	false
74.125.140.156	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
185.60.216.19	scontent.xx.fbcdn.net	Ireland		32934	FACEBOOKUS	false
23.176.96.22	trackingpin.com	United States		20029	H5-DATA-CENTERS-DENVERUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	435106
Start date:	15.06.2021
Start time:	23:02:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://www.unitedwaydenver.org/
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:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.win@3/185@25/9

Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://unitedwaydenver.org/ • Browsing link: https://unitedwaydenver.org/about/ • Browsing link: https://unitedwaydenver.org/community-goals/ • Browsing link: https://unitedwaydenver.org/diversity-equity-and-inclusion/ • Browsing link: https://unitedwaydenver.org/leadership-and-board/ • Browsing link: https://unitedwaydenver.org/annual-reports-and-financials/ • Browsing link: https://unitedwaydenver.org/cobank-leadership-center/ • Browsing link: https://unitedwaydenver.org/news/
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\3CFNMO27\unitedwaydenver[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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\3CFNMO27\unitedwaydenver[1].xml	
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\DL2Z0LCB\www.google[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	108
Entropy (8bit):	4.763546360135637
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsW+pEeAq2Exzz9tALJAqSeXCmKb:JFK1rUFy+pEeAq2w5KWeXCb
MD5:	91041FBFBB1164F7C15755010B27ECCB
SHA1:	D2013798F558BFAAA54B98ED8BF376D73DE8D5EA
SHA-256:	8E64EB8DE98ECE86A64CBAF70768AFE2CA28F3657DED9C1393087A37801368C5
SHA-512:	EFC824B529A4F56F583FD5836D4D28008375E178FCBAF1D823E71EAA310A3A75E1DE73E4FF28A919BFECFECE0CC72A080EC09E7BB5AB68052AF35B24E542CFAD
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="rc::a" value="ejhhdm5ocmx3d2Jm" ltime="1125375344" htime="30892661" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\OESJ053K\prometheusintelligencetechnology[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	133
Entropy (8bit):	4.888535452481324
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsyAHyVqQLwGOXBB99jDslH9uyRhhJAqSeXCmKb:JFK1rUFncqQqBXVsldu3eXCb
MD5:	A6ABA201EA5BEC2505844BFE926D27CE
SHA1:	82F987DA1FDBE4F579A9AF9AAB9D1884BBAEDF74
SHA-256:	FFFB674CBDD01CECB51D8B00221F09440F8C0A780A02D20D7C7045878E874615
SHA-512:	80F23671023F343D1A02862FA424FF818037EF529AE44E9AAC07197B412E2B3083899DAC90F671F333B11F2481510BB54D35730ECBE70D1E37F9E52D19974E2B
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="pit_cookie" value="5c9433d4-d2d8-4839-bf9d-1454f8d61b1a" ltime="1296975344" htime="30892661" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{7D06B13D-CE68-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	39000
Entropy (8bit):	1.9241208739068183
Encrypted:	false
SSDEEP:	192:rPZwZ72hW8tVTfVVoyMAgSnSYGpfXVnirxV6fx7VWyrs1vg:rxgSQIVTjozAgSnSYGZln0/YTWks1Y
MD5:	AA6BB38475F4F1C89AF1631EB5520BEC
SHA1:	64E84DE3762A114188D787D0ACE5A341670EF888
SHA-256:	D03E26445F8F044217C7C11F788915AEC3C31771AD064E142F82D3CFF3C9653A
SHA-512:	453314517BDF0E54636093CE964EE0DD700A53F9C972F8516F89C9FC7CFDAA10B25561D5B6071487577D402AD233E4A8456C92CF3E5E785557D42CAADA2A8A5
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\{7D06B13F-CE68-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	367152
Entropy (8bit):	3.726468359709813
Encrypted:	false
SSDEEP:	3072:C252R2E2H2T1coS67LdBm1rZ1rFA5gd1ro:yS67ZAfzE
MD5:	2706EEE2359BE68227B9E7F94AA7E483

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7D06B13F-CE68-11EB-90E4-ECF4BB862DED}.dat	
SHA1:	EBBBD78A5DEAB08C3DB39329A94606E78C29F826
SHA-256:	48CD96BAB02D1EE76BFD3E0F5E63076BB2C4B1A951D42824B4A9C2F4B9B08925
SHA-512:	2EC0B25A4458526FC8334FFDD3E039E4C9E73B96E250BC7611AD68052AA32009050954F696BDA577D34FEED57C020F6BEDC109CB7A860C7CDC6485D24C5A8F F
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\{867D42D8-CE68-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5832281779024215
Encrypted:	false
SSDEEP:	48:IwUjGcprlGwpaejG4pQuGrapbS4GQpKKG7HpRZS7TGIpX24GApm:rkZvQK6gBSAAlTsxF/g
MD5:	C5E9A06586A59E2DCFBF971468DDA5C2
SHA1:	57FF97B0D6C688543D3F842555BBFAFF5EFB5957
SHA-256:	33E7530C8034D3CE8EF0A40B42662F6A1D3078CE30274E40F76D39ACCE83DF6F
SHA-512:	25F4BB945474B12A5E6F197A7FB4234AB895CDE9283117EE35639844AEE0B942A96503DF454D8694D171757F09ABEB021A173C2F413D688672BAFED1975E54E4
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):	5.090389978067921
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE5TnWimI002EtM3MHdNMNxOE5TnWimI00ObVbkEtMb:2d6NxOsSZHKd6NxOsSZ76b
MD5:	55264AAD35AB3C595F869D2B0812B93F
SHA1:	91997E653BDBC7623F43EA7C6A83D5398953485F
SHA-256:	CEAC08D0BDA00CB79DAAA614685582B824615B18390BA4A0FD1C2083708267D6
SHA-512:	EC4744DAFF9473DFE20AC952971BE58A61C24B0DD12D9C3E470A10744D266759D9F4098BCDCDA3DB7A960250565050B681F668CA4C6FB3596C9604FD2EF91B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x57ef30eb,0x01d76275</date>< accdate>0x57ef30eb,0x01d76275</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>0x57ef30eb,0x01d76275</date><accdate>0 x57ef30eb,0x01d76275</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):	5.133047716888062
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kGiYUniYrnWimI002EtM3MHdNMNxe2kGiYUu+rnWimI00Obkak6Ety:2d6Nxrzi3iCSZHKd6NxrzieASZ7Aa7b
MD5:	3D8A77AFB91082BDEBC51AFBD6CAF73D
SHA1:	DF4C36AC1518BC49F466CD80B5F215BECF1D9BF6
SHA-256:	0629DE638273F07318F592EDCCAF6DB1D3ECF45662085365D0A5ADCA87B5592F
SHA-512:	268BF0F3824877EE0560502634FF9800605D3465A6B24526F0BE03CBBDF44E05041E37B8DC0411C34FAEE61475490BF052D454812D52BE8576DE697210C94B83
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x575e9ecf,0x01d76275</date><accdate>0x575e9ecf,0x01d76275</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>0x575e9ecf,0x01d76275</date><accdate>0x5764cea6,0x01d76275</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.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):	5.112865384177348
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL5TnWimI002EtM3MHdNMNxvL5Jz+rnWimI00ObmZEtMb:2d6NxvFSZHKd6Nxvfz+rSZ7mb
MD5:	0CE46E5C6900BAFF93C121B7D8597BFE
SHA1:	DE1C69F4A9220C2D7B4F43F5C134A6D4EB6FA6F1
SHA-256:	3186C7DC0EA7B6E4C83BF36465F51FE974E9CAFD6FF6B317F8491EBC285B92D6
SHA-512:	00070A912AE570A1B86E4A1FB3568313470D14B56296473FF6933240AB7CC26115573282CD589E6C71372EE494076650407B800E6F10CF5CF395E5F4A585C2BF
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x57ef30eb,0x01d76275</date><accdate>0x57ef30eb,0x01d76275</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>0x57ef30eb,0x01d76275</date><accdate>0x57f60e5d,0x01d76275</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):	5.10609407149047
Encrypted:	false
SSDEEP:	12:TMHdNMNxi5TnWimI002EtM3MHdNMNxi5TnWimI00Obd5EtMb:2d6NxiSZHKd6NxiSZ7Jjb
MD5:	A60B43034B5D2D1655268869FE68F6F0
SHA1:	4E532F875F6F0AB216E30C07A58DF3BFF6210D3A
SHA-256:	9C226A7D3B674FADCFC38CA47D367A71D8E7F14C2011A259E8191AFDE82BEA13
SHA-512:	EB598B3D5F692ECB2DD6CCD291784D6E4471A39F3BD9E6B009C0F47A12E1DBF01556C89BCCA1BA01554A2FBC1982D8D4EC79EAF5E8F2AADDED51E538A187 4E7
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x57ef30eb,0x01d76275</date><accdate>0x57ef30eb,0x01d76275</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>0x57ef30eb,0x01d76275</date><accdate>0x57ef30eb,0x01d76275</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):	5.128094700183828
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwwz+UJz+rnWimI002EtM3MHdNMNxhGwwz+UJz+rnWimI00Ob8K075t:2d6NxQRz+gz+rSZHKd6NxQRz+gz+rSZy
MD5:	BE2E4A28E3F8D694267E5820317EAB92
SHA1:	0E1ABEDD71F936BFB94DEA7FA844AED2CCB68022
SHA-256:	79CD8FC81E88BC32FCAD62BF79D3EE91E3591754955024610B71D1438E18A572
SHA-512:	BAB77CB9037AC929367F07026948F7E406F244AB3985E66E216662D195838ED669E813227AF71910CC6979938945CB75CFFD909A84E7419447CEC971A0E2B634
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x57f60e5d,0x01d76275</date><accdate>0x57f60e5d,0x01d76275</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>0x57f60e5d,0x01d76275</date><accdate>0x57f60e5d,0x01d76275</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):	5.093542635285151
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n5TnWimI002EtM3MHdNMNx0n5TnWimI00ObxEtMb:2d6Nx05SZHKd6Nx05SZ7nb
MD5:	609C1E04027031CDE74D851D5BE0E4FD
SHA1:	D44CDAFF54D6E6946F6C28E1DF62E20F66BCE872
SHA-256:	D88124BE9BBBD0820E557C1083B7D4DDEF129DBE66F5B6E6F720A23F3D7C4CF3
SHA-512:	371DBCC8BA6CAECA2729D313270DE3CEA5EB782BE82244C9E0F2EDE01CB53EFB168D8906EA98005863029F724614F81803004FE3A22AFDB536B1E1419FD99BE A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x57ef30eb,0x01d76275</date><a ccdate>0x57ef30eb,0x01d76275</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>0x57ef30eb,0x01d76275</date><accdate>0x5 7ef30eb,0x01d76275</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):	5.130813679338616
Encrypted:	false
SSDEEP:	12:TMHdNMNxx5TnWimI002EtM3MHdNMNxx5TnWimI00Ob6Kq5EtMb:2d6Nx7SZHKd6Nx7SZ7ob
MD5:	987F941011A59DDAB4DD4948BDBABB32
SHA1:	1C7DFC16F85D7932FCCF8458775EA1088FB670A4
SHA-256:	D3C841A6C74EEC0B8213FE3F0157A5425FD957E0259C6E59CDC31B98ADE21ACD
SHA-512:	57934BF925AF16A21A8CB550963CF8DAA256B54800A0A4F893E0DC25E32E5239096A0EC0747109D33EA9F43AEB9050507CD269E3B3D7EE0132D573BDAE334C7
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x57ef30eb,0x01d76275</date>< accdate>0x57ef30eb,0x01d76275</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>0x57ef30eb,0x01d76275</date><accdate>0 x57ef30eb,0x01d76275</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):	5.165735542710001
Encrypted:	false
SSDEEP:	12:TMHdNMNxcuBvInWimI002EtM3MHdNMNxcuBvInWimI00ObVEtMb:2d6NxjVISZHKd6NxjVISZ7Db
MD5:	76B470614D414E4987342868C9966FBA
SHA1:	5A14C89C1D6B88F0ACEEF6FC34CCB9E5581A4F90
SHA-256:	4D89977B91219E4BCA65DDC72583311FB081FB516FBCF795111AAF9811907BF1
SHA-512:	A961FF1513CCBA2A16DBF75A60587A25E5A4CC7E116DE2E788AB4196360E7B16F67D9EBE63023A0B481A90931D7A87016141DE076E3CA736C3248CC031852F2/
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x577b9668,0x01d76275</date> <accdate>0x577b9668,0x01d76275</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>0x577b9668,0x01d76275</date><accdate >0x577b9668,0x01d76275</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):	5.112717387379716

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Encrypted:	false
SSDEEP:	12:TMHdNMNxfne55wnWiml002EtM3MHdNMNxfne5/nWiml00Obe5EtMb:2d6Nx2HwSZHKd6Nx2lSZ7ijb
MD5:	A1722161FBA8F1CC710D421F40A3C2C2
SHA1:	EBC0ADC4131BD723131EB47E75E88CF9754D6C95
SHA-256:	7F89253B42B36110D6D855150DF556AC3A1A8AACB6B0001A693F22A466511C79
SHA-512:	D2611B29B5641D33D40171C43CE84D1D3FC848F80A720160091E3A3F2E73B7950E64CAF1713125B990925769A88CA4B0B47EAFC8D2250259B7A7ECDFCE81FB0
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x57df8a12,0x01d76275</date><accdate>0x57df8a12,0x01d76275</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>0x57df8a12,0x01d76275</date><accdate>0x57e762d5,0x01d76275</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):	1670
Entropy (8bit):	7.609976054379221
Encrypted:	false
SSDEEP:	48:5DB7YMFdG3UFRw+D1eEQAVKComKyy9HcwOs4BMFw9K:tB7NG3UFSi1emVKC/t5BwwK
MD5:	0D46E3CBCB94088965846763CDDC05E0
SHA1:	2A26866A02BE319C0E487E87A15D1A3BA0F46259
SHA-256:	67BD894E625CF6E32BE9F64E3605820B1611D838D2A49097DDE4D0C0855165AB
SHA-512:	53195CB6ABBD8E5C540ACDFC69DBFFC9514D1BA78227A9C22CAAD261330249C45AB7C584B66DBA8C98AD0AE1FC6CFEF8598DFDCF4F2A55451A212836C6A51E1
Malicious:	false
Reputation:	low
Preview:	Z.h.t.t.p.s.:././.u.n.i.t.e.d.w.a.y.d.e.n.v.e.r...o.r.g./.w.p.-.c.o.n.t.e.n.t./.u.p.l.o.a.d.s./.2.0.1.8./.0.4./.c.r.o.p.p.e.d.-.f.a.v.i.c.o.n.-.l.i.g.h.t.b.l.u.e.-.3.2.x.3.2...p.n.g.....PNG.....IHDR... ... .szz....sIDATX..{.....#.\Di....{]..f)^h.[...H.])..b.1D....jb.-m..&M5....W(....@5.ZD...zAV.+E.....L....fg._2.o....<.9.<.%.\..]P...b:.D.Z02.~..x./a5..~..ioh.t...q>.....6.....p...R..e...pm...!|.....8..1.}..(:.....0^..=...C..*.. '.!8.`..l\...V.sX..q...4..+p7...x....d\...E...Al.x.g.8'.n..XQ.Q).P..wgQ/...^..aK..N.I...).%!Z....W.\.,k..s.0....~|=.=.....Z<...M.?.x..[...0+.>..q.....<..lN.!.l.....1vk.`q..aN.pr.h.....X.f&...M...U..t....<?.>4..(.O(.....V....@oX..WG+.....h.....r.wMJm.....f.F.(4..oR..]>.X.g.7k.L.].g.....Q.....x/._..1q.c.OL...3s?<.h.[.ve.r6.I.....2..Q5.29.41=...T.....j....=....$|%.tZ*..i..r6.....a.....0.=..i..?NH...x5..rlJ.L.....r.....(..$[.OW..[.1/...7..F.$^.Ft.".].w5.Jh....st.t..|.X...._....{\...yW.....f.bk.Z*.....`

C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\mms\TTUTR0GD\Mile-High-United-Way-nonprofit-in-Metro-Denver[1].dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	26279936
Entropy (8bit):	7.898213888151075
Encrypted:	false
SSDEEP:	786432:PN5FrufzQMVEWMiIACI4OsupFrQnma44LSC:lWzQMVgieOsWcnma42SC
MD5:	18F3F68EFC1F008EAC3D9B629F192F94
SHA1:	F55F8EE591ABDECC22FA452BDB3A8E7A018D30E9
SHA-256:	DEDDA402C8D2F9D35DDBD50EFBBCFAEED08E8586C5E9F7E817E8D3BB49C1733E
SHA-512:	8222532AB2B68E688E8CB311720FBB0CBE131A4914746DFBB2DD8533272FF5CFA6A774620A4709028CEB19E92A8CFE743EB8C0B92A9628690DF5086EB2050328
Malicious:	false
Reputation:	low
Preview:	/eyq..g@..._?.....l8Wd...^...(....d.iE.....;.c.z=f53%.c=>..8....P.....J..s.+.....%.....;.I..{I2]5.....F.*..DidK..[-.r$.<.<*.F...6....{.....X.....h0-...E.....,e.D. ..#]X.aA?>.QU.=2O...zJg.%....{=.....4.q...\L...!...Xr"B..C.c.gw.U.(..o.../.L..#...{.<.V..m...^q...@s...dH.3.W.....C%..... ..;...y.YQ~R...z.....V!#.K....X.J..... .d...W..;...].$.c)3..`..O~n...c....2z*...`..+..q.....].Nr._...{r..V_..q.j.. .{^..a.0..k<...W.F.z`.+..KE...@(..wR.@.4.w,3."...Y`J.~_.D...\."......[...P...y.iS...{]J.Z...r...,.B...9]....)I.59{U.{.....P.....VL9...3.I..M2.rI.!...7W.....V|...c....{.....=.....Bi..8..2r.9.&.....[.[.i.x.....E.A/.q..\...'..E..C.....;+%..R..R.>..X:..E..S..N.s~..|..4.....Uz_...N..N.E..w^.....,r..).....[.q..%.....y.O..9.Hc<.?`.....Q.;N.t.i.m5.C'.f...;.....[.t....|(..{.K..~.....&C.F..s..t".0>.....W7`....F0.#.....k{..7.Ig..L..;..D^.J]}.L..5..:.W..2.....O...IsHK..r.".@.....W=....m$.....v1B....._Q.._;J].....`/.

C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\mms\Z7RCNQFZ\Mile-High-United-Way-nonprofit-in-Metro-Denver[1].dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	26214400
Entropy (8bit):	7.9066909271858
Encrypted:	false
SSDEEP:	786432:PN5Fd4bncM47WMiIACI4OsupFrQnma44LSC:DgncM4zieOsWcnma42SC
MD5:	EBBE350A2E41BE9DF934A25B772025D7
SHA1:	EF38490024BFDB72411F6ED85D0276EB9BA62418
SHA-256:	0983BD2DF0BB0BF54664C314D66D660E9B9F7D3201C941593B184A96996E9EBD

C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\mms\Z7RCNQFZ\Mile-High-United-Way-nonprofit-in-Metro-Denver[1].dat	
SHA-512:	85E391FA5456CA7476D63EB3294F38FE9CF26DD4E9E5ABE323F70A2BE6EE5A22C39FE0248614CEA5AF90E7D9ADCE2E1B682F9D6E8DA4BABA88D922F2A823FF4D
Malicious:	false
Reputation:	low
Preview:	/eyq..g@.._?.....l8Wd...^...(....d.iE.....;.c.z=f53%.c=>..8....P.....J..s.+.....%.....;.I..{I2]5.....F.*..DidK..[-.r$.<.<*.F...6.....{.....X.....h0-...E.....,e.D. ..#]X.aA?>.QU.=2O.. ..zJg.%....{=.....4.q...\...!...Xr"B..C.c.gw.U.(..o.../.L..#...{.<.V..m...^q...@s...dH.3.W.....C%..... ..;..y.YQ~R...z.....V!#.K....X.J..... .d...W..;...].$.c)3..`..O~n...c....2z*...`..+..q.....].Nr._...{r..V_..q.j.. .{^..a.0..k<...W.F.z`.+..KE...@(..wR.@.4.w,3."...Y`J.~_.D...\."......[...P...y.iS...{]J.Z...r...,.B...9]....)I.59{U.{.....P.....VL9...3.I..M2.rI.!...7W.....V|...c.... {.....=.....Bi..8..2r.9.&.....[.[.i.x.....E.A/.q..\...'..E..C.....;+%..R..R.>..X:..E..S..N.s~..|..4.....Uz_...N..N.E..w^.....,r..).....[.q..%.....y.O..9.Hc<.?`.....Q.;N.t.i.m5.C'.f...;.....[.t....|(..{.K..~.....&C.F..s..t".0>.....W7`....F0.#.....k{..7.lg..L..;..D^.J]}.L..5..:.W..2.....O...lsHK..r.".@....W=....m$.....v1B....._Q.._;J].....\/.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Board_2018[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 780x330, frames 3
Category:	downloaded
Size (bytes):	130735
Entropy (8bit):	7.983807825553011
Encrypted:	false
SSDEEP:	3072:998YL717mqY4NkkuppUr4NJpBFABpxX9en8gng/m:nxY7LpUsh7A3xNe8wge
MD5:	7DE2F3D20DC71F21C403473D868BBFF8
SHA1:	C87B00D871C30ADB325EC5C441EB2C80ED85BA15
SHA-256:	49F00AC45F4B2D01126367A36241AFC52FA564A7BBEFC4D9AA8DD1B1A1F8DC80
SHA-512:	9A0BACF301AA05D6B98BA503812362237O3B09189A420DB47EBF8267A7A2396AFE4B11258D82FAA337BDC390A520763FD43AA2EBC9B5519B077B028F3F8E913
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2018/05/Board_2018.jpg
Preview:	.....Exif..II*.....Ducky.....E.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c132 79.159284, 2016/04/19-13:13:40 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="8146F9CE0312CAAB78462407EE0B8BE4" xmpMM:DocumentID="xmp.did:F54889F24DA211E79DFFAAE91C15C5CC" xmpMM:InstanceID="xmp.iid:F54889F14DA211E79DFFAAE91C15C5CC" xmp:CreatorTool="Adobe Photoshop CC 2015.5 Macintosh"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:096a4e35-47a6-4bb2-8b25-4df54ef3ebce" stRef:documentID="adobe:docid:photoshop:fa42a1e6-95f3-117a-b7d5-9ce005849654"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>...HPhotoshop 3.0.8BIM.....Z...%G.....8BIM.%

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\BusseBoard_360[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 360x200, frames 3
Category:	downloaded
Size (bytes):	28205
Entropy (8bit):	7.968085076593556
Encrypted:	false
SSDEEP:	768:8Zdfvog27gzAsMvdWTu1F1T9Dn1hj/IMFMU:A27y87rDrMkMU
MD5:	A712030F33AF040E54F2FF2D50A01847
SHA1:	E1A00D91747F60A31E994176C1CF9003537CCDFC
SHA-256:	5D3CADEBB459715A458A7B3ADF40B9FCE6816DF8E65DFA9ED10287AEBC7006FB
SHA-512:	AA627819FB49A2C1F4CB1F77A3D2618DC6C6FE0E60C76806FFD5246378BAFEA95762EDCEDC55E3089DA50F3B97704BC079FDD014399A5DF5A4532C004E727C4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2018/05/BusseBoard_360.jpg
Preview:	.....Exif..II*.....Ducky.....7.....shttp://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c140 79.160451, 2017/05/06-01:08:21 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="97E42E16D52110EFC7903EF6E760F8D2" xmpMM:DocumentID="xmp.did:623DC58E55B311E89227FBB653962E69" xmpMM:InstanceID="xmp.iid:623DC58D55B311E89227FBB653962E69" xmp:CreatorTool="Adobe Photoshop CC 2018 Macintosh"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:9d8e57a4-6ead-434c-9022-2552d6e7b6dd" stRef:documentID="xmp.did:9d8e57a4-6ead-434c-9022-2552d6e7b6dd"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\COVID19-Relief-Fund-Applications-for-Funding-is-now-open[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 1600x900, frames 3
Category:	downloaded
Size (bytes):	1022610
Entropy (8bit):	7.982281715282247
Encrypted:	false
SSDEEP:	24576:1vMld0uuzmmPLWANae5zRPUL/h8r7fHorMF4:9Mld0uuzmmP6e55UL/h8r7cMF4
MD5:	2386354AB1EA8C2AA51D50FB6DF5280F
SHA1:	48052E80F49382CE1A8B16E60855B6FBAFC63660

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\COVID19-Relief-Fund-Applications-for-Funding-is-now-open[1].jpg	
SHA-256:	A87E1C02B01FD18CF88F95ED6DFE87208D41DDB7DDFD49E3DB6CDC93C0D1A76A
SHA-512:	FDEE196C6F7D842BB98178C2990862E3697A821E5D09609E2CBD1D801CAC52A0118D40CBBBA6A8D711B049D5C052CE3B9994A3F644A70EBF62AFCF3E948E66A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2020/03/COVID19-Relief-Fund-Applications-for-Funding-is-now-open.jpg
Preview:	.....Exif..II*.....Ducky.....d.....~http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:d9c7e77a-283e-42cd-9cdf-e6990da94d48" xmpMM:DocumentID="xmp.did:51581981656311EAA60FCAADCEF1CD78" xmpMM:InstanceID="xmp.iid:51581980656311EAA60FCAADCEF1CD78" xmp:CreatorTool="Adobe Photoshop 21.0 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:d9c7e77a-283e-42cd-9cdf-e6990da94d48" stRef:documentID="xmp.did:d9c7e77a-283e-42cd-9cdf-e6990da94d48"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Creating-Economic-Opportunity-For-All-is-one-of-Mile-High-United-Ways-three-community-impact-goals-in-Metro-Denver[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=15], baseline, precision 8, 600x452, frames 3
Category:	downloaded
Size (bytes):	185293
Entropy (8bit):	7.574387588072274
Encrypted:	false
SSDEEP:	3072:dmIeu6SvjH1PMhnZpXg4/XPfwQRUMsY7sw:d6u6SvjHuhTXPw/IAw
MD5:	5D614727B275C5D01FFBE59276C49A45
SHA1:	D2D34BC638FA153FD3732EE3B058D02FB2E3701C
SHA-256:	E379A18042FBF6F055BD2F0F2393C0B50C3AA48454753F802D0418A8BC3EBDA0
SHA-512:	07508E5B9940752FB040312CDFE206F155710786F4F1BB3FB4BDA304C160BD55B78A749790FAB965C15F8FA6B98E876B3A81B22BBDFD7A50718259A231D760F9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2021/05/Creating-Economic-Opportunity-For-All-is-one-of-Mile-High-United-Ways-three-community-impact-goals-in-Metro-Denver.jpg
Preview:	.....JFIF.....H.H....V.Exif..MM.*.....&.....(.....1....&....2.....>.;.....i.....R.%.....56.....5J.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\First-mobile-preschool-in-Denver-Mile-High-United-Way[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=11], baseline, precision 8, 1193x629, frames 3
Category:	downloaded
Size (bytes):	405736
Entropy (8bit):	7.89692674008612
Encrypted:	false
SSDEEP:	6144:gKo/rqDlV2/Lns10uw/OjoYOtZJLuvBSEekjGqOLrtycv3sRWmpvI1n5Y0er9sjQ:gLGDlKbuw/OkfpEhk9b7WI1q0q9sHk
MD5:	FD0189E013F67A56B9A4BDD55E58AC1E
SHA1:	0C5EC9AEB57FE1DC1164EB50E3E0DB9DD2A98EA9
SHA-256:	8097BFD457F035AF645AABA67A49AFC1EDE4D05A2B9A4BB29B65C94E176FF680
SHA-512:	D82F3FF90B57F38CB9B5A555E08045D4071D85E5833D020C6C0DCAB6770DCA36E3C3FE12EB7411B185348F8C2750E5E411B061129C96EAD4B8BD9A0C6D3180A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2020/08/First-mobile-preschool-in-Denver-Mile-High-United-Way.jpg
Preview:	.....JFIF.....<.Exif..MM.*.....&.....(.....1....&....2.....i.....*.....r.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\From-Lost-to-Found-Finding-My-Voice-After-Leaving-the-Child-Welfare-System-Mile-High-United-Ways-Bridging-the-Gap-program-participant[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=11], baseline, precision 8, 1400x741, frames 3
Category:	downloaded
Size (bytes):	257321
Entropy (8bit):	7.793227502145313
Encrypted:	false
SSDEEP:	6144:RRXaYhfFdXMiPOvdtbmnn4GgC9BE4nqlkH+:fBNmVvbA4GpBLew+
MD5:	74B6CB6CDEB180F54BDB821757B9D5C4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\From-Lost-to-Found-Finding-My-Voice-After-Leaving-the-Child-Welfare-System-Mile-High-United-Ways-Bridging-the-Gap-program-participant[1].jpg	
SHA1:	7282C17BEE29636DB8EE22DC53562D0683999D2D
SHA-256:	328C9F44682CF730D55EE48A2C72D245A8C5F91601315B97183704E375E88222
SHA-512:	C7673D1FF68E7BCE19C9BEC036CF7AF6D0422F26B1CD90CE4BF60E019AB9FB2102F3DEAC0D3C1C9CCB8ABF6BC3C1EDA6F9A1F25CF2B1EE5337EC56B69FF8EF28
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2019/11/From-Lost-to-Found-Finding-My-Voice-After-Leaving-the-Child-Welfare-System-Mile-High-United-Ways-Bridging-the-Gap-program-participant.jpg
Preview:	......JFIF.....$ZExif..MM.*.....&.....(.....1.....&.....2.....i.....*.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Keep-the-Lights-on-Funding-for-Childcare-Providers-in-Metro-Denver-Mile-High-United-Way[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 526, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	693954
Entropy (8bit):	7.986923345392061
Encrypted:	false
SSDEEP:	12288:J++uEPiIeduQ7VNDpCm18zvN/nKtaHjjlxG2Wx2kxQTrlwYNbDm/b4ThGgNC:J++uuVOd7KxbHjjlxkx5xQT2YNbCb40/
MD5:	2252401ED5E4020ED69C245FFFCB79B8
SHA1:	BFB371239F09F03D031228334123FBCD4454F4DB
SHA-256:	01698786A72935923FB6066EB341BA9E5CC27AB226131795273A5ED6CF980B25
SHA-512:	3A2E94CC41EA89968C4C5FABF11CD56C5C399B9D38F8252017AD6384B48E4D2DACA252C548ACA206ABBD1286196AA5FF3B3C8737AA74112D49BCC863AAC6C03
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2020/06/Keep-the-Lights-on-Funding-for-Childcare-Providers-in-Metro-Denver-Mile-High-United-Way.png
Preview:	.PNG.....IHDR... .....@.i.....sRGB.....gAMA.....a.....pHYs...%...%.IR$.....IDATx^....[z...m...m.TB ..p../}.....\|.+.#....#.s.p....9>...0.1:.%@..#.9....PS.n..{.>W...L?...c./s.jv.*...9...;.n...._.....^.W..Z99~Y.....2.....\]m....TX[[W..1.....WWWe}}....)..Me...(... ...]Z.80...e6_...q...,....F.2W.F..7.`0Tz^..y.A./....E.X.5..U.....h.....rQ.....2.../.e...S.E9>zR....[.G..'..-@f...w...F...'...<...M'...(..P..t7-....n...7Ds.,....t...v..e...w]..v..''.-'.....v...X.K\|.....6n3..*..x]...sx..y..N....C."...d],.l.h..[n.&7..5....ii.v..'.3.....#..b...)...g...1p..bj.....q57.<.....J._dg.^u.j.l0..l..a..."v!=LKt....0.Z..Z....WV.:.....Mo..<.....QP...N..D.R..JC.R.u...>...o...+ml..#.Vc...u..h.Y....PG..Ma@..X..V.....n#x...N\|lm..z....y.p$.....3."..|..G..\.6=...hA...../.NW.G;.4..f...g....?.P8=..L.....D....r.J..1D>.../D;(b+..1...J+U/%[.[^$..er....EK~.&.W.....o~zT.$?...QL.~..eY...4nm...?R....}.h.^.x?...rtx.v.I6.....[8.E..iC.....[...?.....d.r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\MARTHA-DARRYL-Old-Yeller-Auto-1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=6], baseline, precision 8, 1410x661, frames 3
Category:	downloaded
Size (bytes):	286510
Entropy (8bit):	7.831771631365193
Encrypted:	false
SSDEEP:	6144:KjbaKhMFLCyF06BHQRRx1O3bNUfLkH64o1biupCYUXnYM:xlYyFbHi/+/4bima
MD5:	2048828822620D36B2027447A66B1B90
SHA1:	606186CAD0F601C3494C6D4E02805B06D4D6966F
SHA-256:	A1140C358687EA65C0647F065B5EEFFF72ADB5480551CB71F726AC5BE25BB248
SHA-512:	3C606A2A2C4254362276FD22354140B8A27B2A04641247C37D5484A0A77E56D7010A7D4E0B8C2C078D2AFDBC891B254ADB65ED5172E2DBA58862DBD3F55B24C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2020/04/MARTHA-DARRYL-Old-Yeller-Auto-1.jpg
Preview:	......JFIF.....3.Exif..MM.*.....&...b.....1.....&.....2.....i.....V...F.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Marisa-web[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=4, orientation=upper-left, xresolution=62, yresolution=70, resolutionunit=2], baseline, precision 8, 750x433, frames 3
Category:	downloaded
Size (bytes):	150870
Entropy (8bit):	7.985773857575815
Encrypted:	false
SSDEEP:	3072:PfdQko4Kyjyz5iZEqBgpo2mSn68K4aq0Qm72k+ecw:HdQkLnjyzMZ4po2368naqVm7Iecw
MD5:	8743BE9FF8BA8097078B7B2C518CEA52

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Marisa-web[1].jpg	
SHA1:	0D0C08AC3279514ADC6CBD582317C23819C301B4
SHA-256:	8F0AE5EB4456DFF33DCB0FD8889D2B982A0CAA723921088DAE360F618B0DAC73
SHA-512:	C5EE7B7D6DF9F29D625A4D1A936F3228933B526E4F175B3F7136C710EA8A0B5A4756AF7702E4D19700B603CC0A300BC382ADED31336B3355E298E0FF6BAFDBA3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2020/02/Marisa-web.jpg
Preview:	.....VExif..MM.*.....>.....F.(.....,.....,.....JFIF.....C.....C..... .....".....a.....!1.."AQ..aq.#2.....$3B...Rr.%4Cbst.....&5S..7cuv...6Dw...'(8T.....F.....!1.AQ.."aq..... .2...BR..#3b.r...C$4S...c.5s.....?..I.Pl-r..'..dc...^...cab:./.u.YM..a..Np=#.".`.....pmkzc&>.A...._.$$....q.....2.....}l/..}D..n.Xl.=p*R,m`o.....&.T.....G...z....V.bH...=y.....K|....<..c.7'..&....k$.....}...X'.[...[.....X.V.2.F.....g.....u.....M...J.O...`....8.yX....=..o.KP.TC..Q.8..l..4..x".....m..P7..b.nH.m`x....l.t....yH...+h../...@-.r...6..\.}=?^x....}...v..i....z.V.e.| A....%..~..J..s.....[...4....h.....Q.e}...}..;.+....q.....1.....hsM.....Yw.(b/..?}..F.....&

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Mile-High-United-Way-Rapid-Response-Funding-for-COVID-19-Support-in-the-Denver-Boulder-metro-area[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 1600x900, frames 3
Category:	downloaded
Size (bytes):	692650
Entropy (8bit):	7.976843401747013
Encrypted:	false
SSDEEP:	12288:GO3NQcdGfPDX7YO2FCMEFz/qBQl3fXNd18wvcJZw16BtFUM:D3NTqL74zEBWQ2fXRGDNBtiM
MD5:	E910DE427F8E165AEEF5563988CA8607
SHA1:	D8B4B2ED2D5CA1EB6626A890FBEE6BBB36D3103C
SHA-256:	9562D3640DDC47F724851893C0ACB1572307EB5E0DE8FC91D3992306213200A5
SHA-512:	23903FABB95CA7A09B7E163C234C4CDF579BFB5C2222093FD6F65BD48C0190AED8BC07C0113B35FC8C8F435C3B3ECC2F9C5E57ED1A4ED59018DB8FDE299C071
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2020/04/Mile-High-United-Way-Rapid-Response-Funding-for-COVID-19-Support-in-the-Denver-Boulder-metro-area..jpg
Preview:	......Exif..II*.....Ducky.....d.....~http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:fa1aa3fa-54be-4811-8c07-45927d9b02af" xmpMM:DocumentID="xmp.did:D78684A67B8211EABCF4C9A08B5F5C9A" xmpMM:InstanceID="xmp.iid:D78684A57B8211EABCF4C9A08B5F5C9A" xmp:CreatorTool="Adobe Photoshop 21.0 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:fa1aa3fa-54be-4811-8c07-45927d9b02af" stRef:documentID="xmp.did:fa1aa3fa-54be-4811-8c07-45927d9b02af"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Mile-High-United-Way-and-St.-Francis-Center-team-up-to-serve-more-individuals-experiencing-homelessness[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=6], baseline, precision 8, 897x580, frames 3
Category:	downloaded
Size (bytes):	197576
Entropy (8bit):	7.723763261239874
Encrypted:	false
SSDEEP:	6144:RxGKz4n9s8S0pCBDed4ndzBgQNCmgVMNgoCT9h+s:RxGK0CsydzBgQgVugoCRx
MD5:	1C5CCE47C7DAFB8A1E983ACAE5C364F9
SHA1:	106384FB38F2AF5DB0B0A4DB578BB53BA55CC154
SHA-256:	CDB288CA00BCEB2F49559DE75FE07F3DCDFC613B26F86FAE498ED88A19513BD6
SHA-512:	2A177A703CDA00F3AFA8A0F041BCFCB8C0DE84C48F9C5B1876E0430CCE15DE7838CBC2C60B134153E8C843FEAE01EE7F70C83EF4C0D1AA17CEEF23A65D3198A9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2020/11/Mile-High-United-Way-and-St.-Francis-Center-team-up-to-serve-more-individuals-experiencing-homelessness.jpg
Preview:	......JFIF.....`.`....E.Exif..MM.*.....&...b.....1.....&.....2.....i.....V...F..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Mile-High-United-Way-tiaa-volunteer-center[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=12], baseline, precision 8, 1000x750, frames 3
Category:	downloaded
Size (bytes):	297225
Entropy (8bit):	7.835882774103324

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Mile-High-United-Way-tiaa-volunteer-center[1].jpg	
Encrypted:	false
SSDEEP:	6144:AGs5p23C/NDlEWveB/4R9IG6F4I7X1mg+Lw0zJyO+w/z:A9K3CVDlEWmAYGg1mgSnYZaz
MD5:	80226A07E127AD27F8C98E35282CF60D
SHA1:	61E8F8F8F30868F23BA69F6D32A09D917F829A0B
SHA-256:	BDD6E1A183C884888D1714388EB353D587BF2C65FC6DD0B105A978B0AF4D719D
SHA-512:	9D52847AB11681E09EAC20DE106F89B748910B606F362110869F5AD358BB6D40095CC58134D08B3E2C35539611ADC00B456A833DB62E4343F3F4AE1A8CDBE4F8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2020/01/Mile-High-United-Way-tiaa-volunteer-center.jpg
Preview:	......JFIF.....H.H....\rExif..MM.*.....&.....(.....1....&....2.....i.....*.%..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\PCL_360[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 360x200, frames 3
Category:	downloaded
Size (bytes):	29602
Entropy (8bit):	7.968213545879447
Encrypted:	false
SSDEEP:	768:UCFo4ZxGGAzt0CRkhP+IShdInIvxGToMTnmiCAU:hFoK8SoxGTJDjXU
MD5:	FA9A9D9233C1C70DD1C7F98209AC17C1
SHA1:	9878087993259950CC8C5898FAE43A2B52DC34DD
SHA-256:	02BFCCA3F09C82C97F25B73021C899969F615B19B7149A0390D52D95F996600B
SHA-512:	BA82BB363BEA4439A3C0A81D316D580468187A248522060BB4D52471C6257FA36E54AC08EFB08D7E96E100F8B7B8E2E0C1E9C76161C6896A571D14F0D5D7E86
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2018/05/PCL_360.jpg
Preview:	......Exif..II*.....Ducky.....7.....shttp://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c140 79.160451, 2017/05/06-01:08:21 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="F9EE1C829459AED895C9631EC1BC082F" xmpMM:DocumentID="xmp.did:8591E8A455C011E89227FBB653962E69" xmpMM:InstanceID="xmp.iid:8591E8A355C011E89227FBB653962E69" xmp:CreatorTool="Adobe Photoshop CC 2018 Macintosh"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:a01157ac-cd0a-43dd-a55a-45bd3b7f4ccf" stRef:documentID="xmp.did:a01157ac-cd0a-43dd-a55a-45bd3b7f4ccf"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Providing-small-business-support-during-the-COVID-19-pandemic-through-Mile-High-United-Ways-United-for-Business-program[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=9, manufacturer=SONY, model=ILCE-7RM3, orientation=upper-left, xresolution=138, yresolution=146, resolutionunit=2, software=Adobe Photoshop Lightroom Classic 8.0 (Macintosh), datetime=2019:06:03 17:22:40], baseline, precision 8, 1400x933, frames 3
Category:	downloaded
Size (bytes):	255740
Entropy (8bit):	7.92262332705686
Encrypted:	false
SSDEEP:	6144:TJ48pEtdroSm3iixn56r8OdTrCXfbe+XIfd+U+5QJlW:99KdroRXNQbTrCXD3Xk55M
MD5:	8391414BF503C5B88477AE70B0BCF615
SHA1:	37F64E6AB18CA652844DFD2FD2A301D40D413D94
SHA-256:	B3C583E1D7FE5A4791D6C6F9431ABC6CE6C91FD65D1FD0C236EAD38794AC7068
SHA-512:	C19BADE6505EE07CDA488594100B14645E725E7BBB8DCD2766DE108B43846BB112819F75EE0F4E4EC53DB6E1084B89A0A8AFCE0C7BE4303C0E3F7BDF442BE760
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2021/01/Providing-small-business-support-during-the-COVID-19-pandemic-through-Mile-High-United-Ways-United-for-Business-program.jpg
Preview:	......JFIF.....,.....Exif..MM.*.....z.....(.....1....2....2.....i.....HSONY..ILCE-7RM3....,.....,....Adobe Photoshop Lightroom Classic 8.0 (Macintosh).2019:06:03 17:22:40..#.....".....'.....0.....2.....0231..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\School-readiness-in-action-mobile-preschool-Mile-High-United-Way[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=9, manufacturer=Canon, model=Canon EOS 6D Mark II, orientation=upper-left, xresolution=150, yresolution=158, resolution unit=2, software=Adobe Photoshop Lightroom 6.12 (Macintosh), datetime=2020:07:13 15:27:47], baseline, precision 8, 700x466, frames 3
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\School-readiness-in-action-mobile-preschool-Mile-High-United-Way[1].jpg	
Size (bytes):	173320
Entropy (8bit):	7.901476288269001
Encrypted:	false
SSDEEP:	3072:QBaCXL/4Gaz/VLUlf5RkK50GwBkaoYG5Blw+pWLr7eDVC8s9L++lSu3N4KFxorc8:Qr/wUf5R65VoYGjlwzf7eDVCH9Spu2rx
MD5:	1CE22F26299F2A9A743C1A28CFF7F8C2
SHA1:	26825C1BF0B87B4385859DC55965F13F1FE64370
SHA-256:	CAF65C6266289593F1C6498C65EF5F94B546955D0E5B6D32470EA7FD1F071574
SHA-512:	958FF9D7672BD3C64AFF8203DDEF19E1E4B5D1CFA7B4CE82B5D60671381BF44A15730DF86CF42F20AF6112F79C83239E5312EAACDF4E9D99A0277B54F632DC5 5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2020/08/School-readiness-in-action-mobile-preschool-Mile-High-United-Way.jpg
Preview:	......JFIF.....Exif..MM.*.....z.....(.....1.....+.....2.....i.....Canon.Canon EOS 6D Mark II.....Adobe Photoshop Lightroom 6.12 (Macintosh)..2020:07:13 15:27:47.....T.....\."....'..... ..0.....2..... .....0230.....d.....x.....00.....00.....1.....2.....4.....5.....d.....2020:07:01 14:23:50.2020:07:01 14:23:50..e`...B@.....dU.....dU.....052051006368.....F.....EF24-70mm f/2.8L II USM.5355001456.....d.....l.(.....t.....E.....H.....H.....C..... $.' ",#..(7),01444.'9=82<.342...C.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\StaffBoard[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=16, height=3648, bps=206, PhotometricIntepretation=RGB, manufacturer=Canon, model=Canon EOS 70D, orientation=upper-left, width=5472], baseline, precision 8, 1100x550, frames 3
Category:	downloaded
Size (bytes):	474955
Entropy (8bit):	7.966286966803823
Encrypted:	false
SSDEEP:	12288:NMzhAgLhVtJqbt/UOqUUD4zRvo8SSMbJlraM6Oa:WhfL/qqUU8G8SLbHrn6Oa
MD5:	178560259BE930CCD66682FEF6995B05
SHA1:	40A0C72EE24D3E403F323823B88E48032C892A48
SHA-256:	2641DAEF4A7CF3004E73D56E245D6DAC56BB82D57E233CAB81A8BC8DA09B7676
SHA-512:	CA9F3CF4F4CABF4A01EA78F3A3F8FE04000E4E1B170E536AAAC4F13D223C7BDBF276F07387296BC0194F19C56448263F09266532CF6E527DAE560C300F74312E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2018/07/StaffBoard.jpg
Preview:	.....JExif..II*.....`.....@.....(.....1...$.....2.....i.....0...%.....Canon.Canon EOS 70D.....'.....'..Adobe Photoshop CC 2018 (Macintosh).2018:07:02 13:41:37.&.....".....'.....d...0.....2.....d.....0230.....".....6.....>.....F.....N.....V.....^.....93.....93.....93.....0100.....L.....&.....f.....n.....0.....1.....v...2.....4.....5.....G.....2016:12:06 22:41:19.2016:12:06 22:41:19.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Supporting-Education-and-Academic-Success-for-children-and-young-adults-is-one-of-Mile-High-United-Ways-three-community-impact-goals-in-Metro-Denver[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=9, manufacturer=Canon, model=Canon EOS 6D Mark II, orientation=upper-left, xresolution=150, yresolution=158, resolution unit=2, software=Adobe Photoshop Lightroom 6.12 (Macintosh), datetime=2019:12:17 09:56:01], baseline, precision 8, 700x466, frames 3
Category:	downloaded
Size (bytes):	136442
Entropy (8bit):	7.875113720012493
Encrypted:	false
SSDEEP:	3072:Zc1LFPTkQwHcBeLoSgUW6jct0W5rrYkMxSY+bfLZatsiYa0ghLKbnhQrQgrQ:oZPTkQTQLoSFW6g/5rsQpatsLa0gOsM
MD5:	DDB21FACA384D6BCFEF67F7B179DF5F6
SHA1:	E2637DE6B1783B28B9A7F295B45504A4A4830A37
SHA-256:	47CBD1B04F9A0DF00A68F82151D3EF65B6C50E649882D16318BCB64EFE612BB6
SHA-512:	45AF3A4B0EB7C80EBDEB6BF0E1922BBEA76B4F9290CA0EE3B6EA636168BF6E544FBE740BDCA90EC11BD757F1D7DAECB02CD7A6D0AAF1FAE3690381859520 11EA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2021/05/Supporting-Education-and-Academic-Success-for-children-and-young-adults-is-one-of-Mile-High-United-Ways-three-community-impact-goals-in-Metro-Denver.jpg
Preview:	......JFIF.....Exif..MM.*.....z.....(.....1.....+.....2.....i.....Canon.Canon EOS 6D Mark II.....Adobe Photoshop Lightroom 6.12 (Macintosh)..2019:12:17 09:56:01.....T.....\."....'.....0.....2.....0230.....d.....x.....42.....42.....1.....2.....4.....5.....}.....2019:12:14 10:19:12.2019:12:14 10:19:12..jJ...B@.....F.....dU.....dU.....052051006368.....F.....EF24-70mm f/2.8L II USM.5355001456.....d.....l.(.....t.....H.....H.....C..... $.' ",#..(7),01444.'9=82<.342...C.....

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Tasha[1].jpg	
File Type:	[TIFF image data, big-endian, direntries=6], baseline, precision 8, 1078x1071, frames 3
Category:	downloaded
Size (bytes):	268560
Entropy (8bit):	7.817264234451491
Encrypted:	false
SSDEEP:	6144:6/X7N0RiDA5+uuw7cGOGY7fZ501P0yLYLjmmc6b:47t6uQ+7vV5jqq
MD5:	EA9652F990EC27A8F28A5638983497E9
SHA1:	82F14DA2B6D4126F927B8D07855EE447EC4CA9BF
SHA-256:	603866A02277D7329B0B048990073AEEFDEF9F6DB4B191C7E07E1EE37AB7FBCA
SHA-512:	59554E452B2821DA6C1D8346421848098CA85E4597E2BAD46436A42C1E7B2AD279AFEF508334061A52ADD34DEACF1B4F47A1CAD173D0D45AC6C1237DCC6F579
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2020/05/Tasha.jpg
Preview:	......JFIF.....,.,....;.Exif..MM.*.....&...b.....1....&....2.....i.....V..F..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Understanding-Equity-and-Our-Role-As-a-Learning-Organization-Mile-High-United-Way[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=15], baseline, precision 8, 639x404, frames 3
Category:	downloaded
Size (bytes):	74852
Entropy (8bit):	6.653078311320562
Encrypted:	false
SSDEEP:	1536:Ar+INMpO7CkNUrEfOEGQD4Ilad1TAESVCHS8qurZ:ArZM+CJrVEh7IacSAK
MD5:	21FE37299D5DE60DD22EEBEFB5AA7F7C
SHA1:	0B61420F928E40C3011F04C08C9856AF1E253246
SHA-256:	B24C105F803932FA24634B63A51B88AFF47E85E5AE98B20274E54FD52823D82A
SHA-512:	6833AA9373347E55035AF5B474C057EE896221C1B6FF1E9676F68990E5234A0BBE4D1422C8F4EE62C67E9A139DBEC75DD4D1C2F173188A7E03B73AB5DB776E9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2020/09/Understanding-Equity-and-Our-Role-As-a-Learning-Organization-Mile-High-United-Way.jpg
Preview:	......JFIF.....H.H....MfExif..MM.*.....&.....(.....1....&....2.....>.;.....i.....R.%.....5:.....5N..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\United-for-Schools-Mile-High-United-Way[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=12, height=1810, bps=0, PhotometricIntepretation=RGB, orientation=upper-left, width=2716], baseline, precision 8, 1358x905, frames 3
Category:	downloaded
Size (bytes):	272939
Entropy (8bit):	7.933455484501013
Encrypted:	false
SSDEEP:	6144:VHS5yloVFm8j1vjeZqTveBRZYM8lx/WLzwxYGJoKgTV4Uy/UVbPHR8:Vy/VF1mqj3Tx/+zkBCKgxXy/ebR8
MD5:	5D99AA18446E2B0CDB33F7F9950E3AC9
SHA1:	535CD19748805771AB9F51446B1434A45B80A52C
SHA-256:	DDCFF626C1FA96BB769D880BD9B8A9EA00FA36CB425F83D246D253A671EF4881
SHA-512:	BC9330FF359CCD8C43AF5F8F29CD72002025D2FF63A1BB491BD3D19F461E1E30D1232EC71E48EE52CD2B132954C8AE1D2E5CD2027854A7DAA92E8432688C3CE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2020/10/United-for-Schools-Mile-High-United-Way.jpg
Preview:	......JFIF.....,.,.....Exif..MM.*.....(.....1.... ....2.....i..... .....-....'..-....'.Adobe Photoshop CS6 (Macintosh).2014:05:12 14:55:02.....0221.....n.....v.(.....~.....W.....H.....H.....C..... $.' ",#.. (7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222.....j....!.....}.....!1A..Qa."q.2....#B ...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2. ..B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\api[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\api[1].js	
Category:	dropped
Size (bytes):	850
Entropy (8bit):	5.5017545950531765
Encrypted:	false
SSDEEP:	24:2jkm94/zKPccAv+KVCetg1AnDsLqo40RWUnYN:VKEctKoee1AnILrwUnG
MD5:	65B6FEB732C65BEE99FD396A3E99F27F
SHA1:	8F719875F058EEE21257BC1CBCA2A6BA1A7B9A21
SHA-256:	9B7EA780F5FF5CD8A0AD4A2700143F3661284DC98D571CB38B188C2C060FE55A
SHA-512:	433CF4B099A6CFD3D98F128F86EA8C2EAACA852A38777683C7AD14953B3A4782C54985A87F5A2FCCA67CF3C2C83159EE2BBE71713338A11274D0516E4C5B8E(
Malicious:	false
Reputation:	low
Preview:	/* PLEASE DO NOT COPY AND PASTE THIS CODE. */(function(){var w=window,C='___grecaptcha_cfg',cfg=w[C]=w[C]||{},N='grecaptcha';var gr=w[N]=w[N]||{};gr.ready=gr.ready||function(f){(cfg['fns']=cfg['fns']||[]).push(f);};w['__recaptcha_api']='https://www.google.com/recaptcha/api2/';(cfg['render']=cfg['render']||[]).push('onload');w['__google_recaptcha_client']=true;var d=document,po=d.createElement('script');po.type='text/javascript';po.async=true;po.src='https://www.gstatic.com/recaptcha/releases/6OAif-f8nYV0qSFmq-D6Qssr/recaptcha__en.js';po.crossOrigin='anonymous';po.integrity='sha384-f1gfYQgq4OmhARgCSe1q7WV7tIcPpqu0qD+jYdSEMczD1YXPg0ibdIzvD/fZzwKc';var e=d.querySelector('script[nonce]'),n=e&&(e['nonce']||e.getAttribute('nonce'));if(n){po.setAttribute('nonce',n);}var s=d.getElementsByTagName('script')[0];s.parentNode.insertBefore(po, s);})();

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\app[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	43889
Entropy (8bit):	4.660907736376996
Encrypted:	false
SSDEEP:	384:vHVnhonP9s9w5cMKUd7iMFx1CEa7lGhJxpzxy0oKH/Usb0/5CeD9QoXHSrtq4tPY:dnho75cMKQ73NJKNSo3SrEg6l7v
MD5:	CF3C4BBF2DD37F4BE1B61965529E00C0
SHA1:	8910280F3AD69496F2679B07C6875B38A54BE63D
SHA-256:	58A41AE9894DF1F295214B840EEFEFBD65A0CDF08FF1EF9078D855CF2A48BAC2
SHA-512:	A89AE362FDA68AA9D3CE541DED50F30888B125057E1576B769D7921575B50708C6AEF11C8D2A1BAA54E5149B9A81CCE30A5D4D86382CC1CE63BB875835370A2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/themes/uwmh/assets/js/app.js?ver=2.4.1
Preview:	!(function ($) {.. /**. * Modules. */. var app = {}.. /**. * Mini Helper Objects. */. var _w = {}, // Window. _s = {}; // Screen.. /**. * Module Properties. *. * config. * data. * $el. * . */. app = {.. // Config. config : {. environment : window.location.href.match(/(localhost)/g) ? 'development' : 'production',. debug : window.location.href.match(/(localhost)/g) ? true : false. },.. // Data. data : {. temp : null,. binds : {}. },.. // URLs. urls : {. social : {. facebook : '',. twitter : '',. youtube : '',. instagram : '',. pinterest : '/'. },.. },.. // Public Keys. // keys : {. // addthis : 'ra-536cbe5438ea26f8'. // },.. // Console (Client). console : {. color : {. 'error' : '#da1a1a',. 'event' : '#3d8627',. 'function' : '#3db330',. 'callback' : '#6c6c6c',. 'object' : '#ac07db',.. '

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\beefup.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	2780
Entropy (8bit):	5.0742539542058
Encrypted:	false
SSDEEP:	48:vAN7jR1rxpWhsA6Amg8KHIcA1vxXXuWaQaFfsak+7flNfs0o5Bq80N:IN7uvrmVCIf1puUaFv7tNfsPBql
MD5:	482A5BFC21690904E4DF43A630596941
SHA1:	587D8F2A1F7794491DD3529796EB9A34D4BF841E
SHA-256:	81394CB518F01D1108354E5D94553297E1B6F2E8A8FCB5A0DB7B0C8B774D07B8
SHA-512:	7FFD0E0DDEA7E80BF14BD2E40E44FBCD618F91880F74013FE7F816B5A537FC671ADA6113948177D515C4C40A84E3721F6489F06F7979A7F8B7DF17551A799AD3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/themes/uwmh/assets/components/beefup/beefup.min.js?ver=1
Preview:	/*!. * accord v1.1.4 - A jQuery Accordion Plugin. * Copyright 2016 Sascha K.nstler http://www.schaschaweb.de/. *. */!function(a){"use strict";var b={};b.defaults={trigger:".accord__head",content:".accord__body",openClass:"is-open",animation:"slide",openSpeed:200,closeSpeed:200,scroll:!1,scrollSpeed:400,scrollOffset:0,openSingle:!1,stayOpen:null,selfClose:!1,hash:!0,onInit:function(){},onOpen:function(){},onClose:function(){}},b.methods={getVars:function(b){return a.extend({},b.data("accord"),b.data("accord-options"))},animation:function(a,b,c,d){switch(a){case"slideDown":b.slideDown(c,d);break;case"slideUp":b.slideUp(c,d);break;case"fadeIn":b.fadeIn(c,d);break;case"fadeOut":b.fadeOut(c,d);break;case"show":b.show(c,d);break;case"hide":b.hide(c,d)}},getStayOpen:function(a,b){var c;return"number"==typeof b?c=a.eq(b):"string"==typeof b&&(c=a.filter(b)),c},selfClose:function(c,d){a(document).on("click",function(e){var f;a(e.target).closest(c).length||(f=c.filter("."+d.openClass),d.stayOpe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fifty-icon[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 115 x 115, 8-bit/color RGBA, non-interlaced

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fifty-icon[1].png	
Category:	downloaded
Size (bytes):	1762
Entropy (8bit):	7.828034928659294
Encrypted:	false
SSDEEP:	48:ubvVE6x4oFTjrhr5NN4a6ljt3BG0bzi26:8ruLBjbzX6
MD5:	80ED9386B39E16225609BBA8954C2A5C
SHA1:	026B365ED8B38FAF1EAEB258DDD5040C15F657D4
SHA-256:	034E49EFC2FC4A393AD168CFC78BFC1D7A5E5218671DFCBFA3ABC872CB4ED31D
SHA-512:	4E1267E9F88FCBC7DC9D3D32A26DECFAEB6F192F83837EA9C87007912D65C6476C156ACABE9F407E5ACACF2315F5ACD02BF69A5DAAE39AACDDA6BCF838B0720A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/themes/uwmh/assets/images/fifty-icon.png
Preview:	.PNG.....IHDR...s...s.....C=.....pHYs.....~.....IDATx...u.H...u.n2.....F..h#.M..`q.+G`...`P..".>..v.....{...d..GUu.....|.e..0).....@V.Zl...3:.E ....=28.....~..<..&.L.....:....]..r.\S..j<6.`..7L\$.....Dc...f@....Z..<....N.I.u..g:.)azt.b..X....a.."...z...b..._....E+Z.....H...b.*$*..L.y;=..%....d..)....h...&1S.x.1.\{.....2=r....D...07._b...U.....~.....%.ZY.V.....bQa.2{..n..\.x.Vh.....3l.3.$.m.)L..=..!.i.,....Z%U...E.....OK....a.P]..Zh.....n.`plR`..sq.U0..k..7.&...p..H.r.....J..2.f.y.....A.....4.oZg.YO..w.2....V..3....u.....%:.3Yc....9..k..}..9L...{..J...@...fmq3^.p...K#L.fmU@#r.Ma.p'.l..Un1..s..T..s.x..ufX.....\.yw>.}.....".....!.?...1...L.n..].....D..j.U.+.3@...`..U.'._q._'.9.....T..hD..2.U...o4..6....L.gJ&...Z..... .....iJ.}...fk.. .....q.&.{.9..K...IO.....b.n.Z.:.....s..6.....u..kO..+..Y`N./U..[...(0...>.m.Z....9.....@..~.....]./0...>0...^.s.L.~UxzE .$.=.+.*-./..Rx}oD...g\a&Lan

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\instagram[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 60x60, frames 3
Category:	downloaded
Size (bytes):	1521
Entropy (8bit):	6.67652053687812
Encrypted:	false
SSDEEP:	24:qK1hxWwjx82lY2T34V12jlyJ3Vv7xJGDDnbDl743UARFDabtak/1ackiWe/Zh:r6Nn28LQLJ3pdJqfDh88YLiWeRh
MD5:	EAAE8D007F876C63BF80D2E4F4913B1B
SHA1:	F897ADBF5B41B9C72BC25E17C70722CD99298259
SHA-256:	E42A0F679014EE24C49FD74F4D40E48B604638C2813CDB467B3512D2DE545D54
SHA-512:	8349D385790506075562626F948EDC42A31BB4EC28E5F269EE2715E6AFB5236A7CC81E2CDE3E5BB8AC807BB3D9A8C5604F1C50671D95DAFF4DC68DAE5B3915E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/themes/uwmh/assets/images/instagram.jpg
Preview:	.....JFIF.....d.d.....Ducky.....<...../http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c140 79.160451, 2017/05/06-01:08:21 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf :about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC 2018 Macintosh" xmpMM:InstanceID="xmp.iid:16920A3845AB11E8ACEDB7C54AC10EED" xmpMM:DocumentID="xmp.did:16920A3945AB11E8ACEDB7C54AC10EED"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:16920A3645AB11E8ACEDB7C54AC10EED" stRef:documentID="xmp.did:16920A3745AB11E8ACEDB7C54AC10EED"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	96873
Entropy (8bit):	5.372169393547772
Encrypted:	false
SSDEEP:	1536:HYE1fGBiByJsbfXXeRJ/shgWCeLLccJdZVHk04ssx+/mvaSIFSet43tpXJIGVyp3:fsAg0psxTva/FSeKy2bDD5a98Hrq
MD5:	49EDCCEA2E7BA985CADC9BA0531CBED1
SHA1:	F8747F8EE704D9AF31D0950015E01D3F9635B070
SHA-256:	1DB21D816296E6939BA1F42962496E4134AE2B0081E26970864C40C6D02BB1DF
SHA-512:	F766DF685B673657BDF57551354C149BE2024385102854D2CA351E976684BB88361EAE848F11F714E6E5973C061440831EA6F5BE995B89FD5BD2D4559A0DC4A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp
Preview:	/*! jQuery v1.12.4 | (c) jQuery Foundation | jquery.org/license | WordPress 2019-05-16 */.!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="1.12.4",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?a<0?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,fu

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\linkedin[1].jpg	
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 60x60, frames 3
Category:	downloaded
Size (bytes):	1584
Entropy (8bit):	6.806464305669082
Encrypted:	false
SSDEEP:	48:r6Nn28QhLJ31Y8Jql06H9jXCOiXHKOppgv:K2zqlddTCVXHKOMv
MD5:	8ECDD38F659D9D31127D43D5129E73BD
SHA1:	77343A68444335D115B8A350098ADF323552965C
SHA-256:	1EB18D2547013D15EA7850379B5BF760FE5EDB1793C5CEF20A4B284A5162EC59
SHA-512:	C67492E4BF88558233C498BC87BB400C66B64C4385247D506EC1BBDD1CEEE6AA1DC7B34BBB852E099E1663BAEA50BA63A36FF942A774E802D30869EAA527C8DF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/themes/uwmh/assets/images/linkedin.jpg
Preview:	......JFIF.....d.d.....Ducky.....<...../http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c140 79.160451, 2017/05/06-01:08:21 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf :about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC 2018 Macintosh" xmpMM:InstanceID="xmp.iid:16920A3C45AB11E8ACEDB7C54AC10EED" xmpMM:DocumentID="xmp.did:16920A3D45AB11E8ACEDB7C54AC10EED"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:16920A3A45AB11E8ACEDB7C54AC10EED" stRef:documentID="xmp.did:16920A3B45AB11E8ACEDB7C54AC10EED"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\logo@2x[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 236 x 144, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	11225
Entropy (8bit):	7.947296041063412
Encrypted:	false
SSDEEP:	192:KOI2kiWfMGOvEvumt/n4OdngrRr79B9tsWtzz66dh35cP:TQ9kGOvEvuQ/fgr1ptXd26PJc
MD5:	D675BAFD7CF90BAD1CF3E0784D060E4C
SHA1:	8DBF100A93CEB93EE8D298D00FD7E9908BEF3A29
SHA-256:	2E3CDEEFD6B7FBE381FBAA7F28E0D31C1A7011763679EF44BDB4EA4B8F690803
SHA-512:	00BA81DBD4FE39A7ABC6D742D84176EF7FEF2FFBD17D7223DA89797ADE2E8EA5C516B6236DE35B9CBBE7EC89FEA1C7658AFF3B7FC3C4BB7539BEFDFA4AA2212B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/themes/uwmh/assets/images/logo@2x.png
Preview:	.PNG.....IHDR.....3.....tEXtSoftware.Adobe ImageReadyq.e<...xiTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:26c3552b-0c9f-41a8-bd0a-0fb3508f82cc" xmpMM:DocumentID="xmp.did:46882E0D255611E8AC5E9986894C3AE8" xmpMM:InstanceID="xmp.iid:46882E0C255611E8AC5E9986894C3AE8" xmp:CreatorTool="Adobe Photoshop CC 2017 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:26c3552b-0c9f-41a8-bd0a-0fb3508f82cc" stRef:documentID="xmp.did:26c3552b-0c9f-41a8-bd0a-0fb3508f82cc"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>Au-...'.IDATx..]..V..^.y.TJ...T.H

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\p[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	5
Entropy (8bit):	1.5219280948873621
Encrypted:	false
SSDEEP:	3:U8n:U8n
MD5:	83D24D4B43CC7EEF2B61E66C95F3D158
SHA1:	F0CAFC285EE23BB6C28C5166F305493C4331C84D
SHA-256:	1C0FF118A4290C99F39C90ABB38703A866E47251B23CCA20266C69C812CCAFEB
SHA-512:	E6E84563D3A55767F8E5F36C4E217A0768120D6E15CE4D01AA63D36AF7EC8D20B600CE96DCC56DE91EC7E55E83A8267BADDD68B61447069B82ABDB2E92C6AB6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://p.typekit.net/p.css?s=1&k=mxg5ixn&ht=tk&f=1344.15498.15510&a=8688369&app=typekit&e=css
Preview:	/**/.

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\powered-by[1].js	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	316
Entropy (8bit):	5.060918824937915
Encrypted:	false
SSDEEP:	6:zRifjoN/Ic5EfoTrEDwCykxOnGBLgLdIC2+ZJE8NdGFJ9jp1c0c/zfykxEvH:zRwjodBCMmISwGD6e8NePjLc0czKSEf
MD5:	D3F35E758C92FDD01ED6F4ABBE928337
SHA1:	3294D0E6EE2712BEB2C3B4D5965E310DBB8BF866
SHA-256:	2CC9244E23A9CB8C4E4328C1CACB124544871E6BC864C4B8CF5EFB56EE4A562F
SHA-512:	46B556F710BEF11CB4D51E7ECF77F898C370295FFF4207A321C1C34DB74720D77A50238327F607EF8B8738DC48460598AF6FE795C7FF323731ED713565E39A30
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/plugins/feed-them-social/feeds/js/powered-by.js?ver=2.9.6.2
Preview:	jQuery(function() {jQuery(".fts-twitter-div, .fts-jal-fb-group-display, .fts-instagram, .fts-yt-videogroup, .fts-pinterest-boards-wrap").append("Powered by Feed Them Social");jQuery("body").addClass('fts-powered-by-text-popup');});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\style.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	139581
Entropy (8bit):	5.128889936839181
Encrypted:	false
SSDEEP:	768:Pyr+KZK3l9cfx1Uz6l+yQ/Ted77PF00sdf73H8ZCdARw6InFzKmB67spMYRQrTfm:Pyrt9yUz6l1kg7uNdfTXdAfY+ruJb
MD5:	0CB5800DD9B59E5D3BA40A6F1F7F8EDC
SHA1:	5F8894A597E6729E906068ADBFA8641D17B84DF1
SHA-256:	D3E22E88CBFE0E392D07F3CBA899EBD519D0C82AA6F2122810DD3F099B38AF9D
SHA-512:	606417AB8DEB2DCBD95874E7DFAD68FFA18E844BB10819EA95D9E96F4C5F1EBC06A0287A1D297FA2ABF268881A4736AF8642CC641E1A01AC8A1EA228D04198CA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/themes/uwmh/assets/css/style.min.css?ver=2.4.1
Preview:	/*!. * Font Awesome 4.4.0 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */.fa.fa-pull-left,.fa.pull-left{margin-right:.3em}.fa,.fa-stack{display:inline-block}.center,.fa-fw,.fa-li{text-align:center}.img-col.compat-object-fit img,.modal{opacity:0}.circle-icon-link:hover svg .a,.slider-featured .slide .circle-icon-link:hover svg .a{fill:#4b89cd}.tabs-section ul li,ul{list-style-position:inside}.fa,body{-moz-osx-font-smoothing:grayscale}@font-face{font-family:FontAwesome;src:url(../components/font-awesome/fonts/fontawesome-webfont.eot?v=4.4.0);src:url(../components/font-awesome/fonts/fontawesome-webfont.eot?#iefix&v=4.4.0) format('embedded-opentype'),url(../components/font-awesome/fonts/fontawesome-webfont.woff2?v=4.4.0) format('woff2'),url(../components/font-awesome/fonts/fontawesome-webfont.woff?v=4.4.0) format('woff'),url(../components/font-awesome/fonts/fontawesome-webfont.ttf?v=4.4.0) format('t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\style.min[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	53907
Entropy (8bit):	4.940786840491388
Encrypted:	false
SSDEEP:	384:F5Tku7HBZDO/KRUEqXMXRLrO+AwlVHl+vg7LKclyvNSX2GVX5Ttfr:0RXMXRLrO+AwlxI+vg7LKNcF5Bfr
MD5:	2E7E1D1C1D4D446A1B6B63295757D859
SHA1:	27A1D9DCBDC4AFF486016B5C9F3ECE6AD0C028C1
SHA-256:	8C626F0F9B5C109539B256B73E72C02B300A184F46B4535C2EB86599215C78AF
SHA-512:	7526B0ADCE5C1751D3E55BA5077C4BB5F334FAE6A73CB519E2BE07AA602ED25C307A8462AF380DA0550F56AE29C871A663F9A01E523462DFB9A378E8F26888A3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-includes/css/dist/block-library/style.min.css?ver=5.5.5
Preview:	:root{--wp-admin-theme-color:#007cba;--wp-admin-theme-color-darker-10:#006ba1;--wp-admin-theme-color-darker-20:#005a87}#start-resizable-editor-section{display:none}.wp-block-audio figcaption{margin-top:.5em;margin-bottom:1em}.wp-block-audio audio{width:100%;min-width:300px}.wp-block-button__link{color:#fff;background-color:#32373c;border:none;border-radius:28px;box-shadow:none;cursor:pointer;display:inline-block;font-size:18px;padding:12px 24px;text-align:center;text-decoration:none;overflow-wrap:break-word}.wp-block-button__link:active,.wp-block-button__link:focus,.wp-block-button__link:hover,.wp-block-button__link:visited{color:#fff}.wp-block-button__link.aligncenter{text-align:center}.wp-block-button__link.alignright{text-align:right}.wp-block-button.is-style-squared,.wp-block-button__link.wp-block-button.is-style-squared{border-radius:0}.wp-block-button.no-border-radius,.wp-block-button__link.no-border-radius{border-radius:0!important}.is-style-outline .wp-block-button__link,.wp-bl

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\tablepress-combined.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\tablepress-combined.min[1].css	
Category:	downloaded
Size (bytes):	5305
Entropy (8bit):	5.5537753329541335
Encrypted:	false
SSDEEP:	96:G5aOb5pxD2FuQThlQKA0yVqU26qGa1NjyOi0zjtoZpr1wWTsUkSzQ54T3w5p3X8Q:+nD6uQM21sZHr1JI7HD1n
MD5:	B8706FFC340B8249E650380EED7D708B
SHA1:	492D7B7F3E4C1BD6FB75A16263D0A10D144F03AA
SHA-256:	8E956F212C336D99021DEB35857269C9F08DC37301293026944895830 36B9446
SHA-512:	A1EFD4A6BD1201BD72239205B6CEF58DE2092542B9CC56E127AE870B1EF64C0899B10A639191AD5C7DBB087D13D2104FE6F6F60478ED39078CAF03C4895DF8D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/tablepress-combined.min.css?ver=16
Preview:	@font-face{font-family:TablePress;src:url(data:application/font-woff2;charset=utf-8;base64,d09GMgABAAAAAAPUAA0AAAAACZAAAAN+AAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAP0ZGVE0cGh4GYACCUhElCoQIgnILFgABNgIkAygEIAWGcgeBARv6B8iuBzK53oAhKg2KWDsrezjalSefocfD9/uZ575PSbYEqJHAldo6tMDGdCprFlHd+F9r+rZE46O2iHBJfoAuxwW0yfgKS8KGVFE4dHX1gPmgVhzwhcJbReQ9RWXcraeutbmNHE7T7B1sex8stfMfnkvv0XsgUZrYO1hirXme9TnUkBvQ22RGX50VAr48H54Cn9b8GD73edAAhjboBpIQ6kKOhCz7GA8V5HfzyeA6h0mnrFTJnPjxC7KCrl9caqIUg0EAYACGDBn6YGCxeIE+EkwANTWJX/brZpNfyE5o/7r9uPZjS4tESbCTExLCjxOEbxGi2dQeNEAXUMMlvADkqSV0IHXtkQXNOnI2ctJpRIPt8+HjNivx3rlQYA8FqGwdCxF2aZrdJluMnaqFvy+yngVKbBcn0fSOd1xTpnW4HTkptV8Gi2kvCeUHC0BD+D0VKMIqXniZPJyPya9D7gT6DvUpwJER6avgKDsOfW9jU+YGc/ng6MhA3VSar3NdtvrD9WHZurKVKYOi0RwlY9500YSuWDE084F+jMinu4sTudD5yBTTozA9Horpmb+M3TwIBHempnzdpu1/raWypX0JND/ki4p71CQQlFqnAvkijABrVFIq5BdNJbFncoBOF03/h3IINPQRBxJCYDoAOnkRIDR0w0BSmYiBzDinAuQ6eROg0DEGY6DUiEUYqKyILwFq2qS9GKhrpFsykdeFLmDjknYG4jKbNeNyQ1zhCoP840pdYiqu8jTW4mp6pMXH1HVJp8wRmHmQKTKiUOBVSMHrlKuBl	

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\tawnyheadshot-WP[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=9, manufacturer=Canon, model=Canon EOS 70D, orientation=upper-left, xresolution=142, yresolution=150, resolutionunit=2, software=Adobe Photoshop Lightroom 6.12 (Macintosh), datetime=2019:11:26 11:09:51], baseline, precision 8, 1200x800, frames 3
Category:	downloaded
Size (bytes):	418001
Entropy (8bit):	7.968081718855834
Encrypted:	false
SSDEEP:	12288:9YRVCWCWWYlwCX10BJP5pv/qBJlVEfivwvIYFz7:3Wn1QLCLljvwvH
MD5:	DF4D8D87F95FE4688AAD7988362D78AA
SHA1:	F6469369470FD1882F1E8720C94305F476F4196C
SHA-256:	B1B901E512139846FFF7F5B95C9B582CABDC106ECC48DA4EFE3ECC1733887CED
SHA-512:	F45580D03FB10BCCEF2B686DB6DB2C7CAA93DFD4E28E3F9546282C37D31125D8ECD513ACFFD10F05669FAC69A1E204E86196C107E4495935DD47DD37BE0956 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2020/01/tawnyheadshot-WP.jpg
Preview:	......Exif..MM.*.....z.....(.....1.....+.....2.....i.....Canon.Canon EOS 70D.....Adobe Photoshop Lightroom 6.12 (Macintosh).2019:11:26 11:09:51.....G.....O."....'.....0.....2.....0230.....W.....k.....81.....81..... .....1.....2.....4.....5.....}.....2018:05:12 19:08:56.2018:05:12 19:08:56..jJ...B@..... .....S.....7.....W102025018636.....i.....EF24-105mm f/4L IS USM.00007125bf.....JFIF.....C.....C..... ....".....P..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\twitter[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 60x60, frames 3
Category:	downloaded
Size (bytes):	1465
Entropy (8bit):	6.542139995418068
Encrypted:	false
SSDEEP:	24:qK1hxWwjx82lY2T34VpUYs2NzsIyJ3VSt7v5sJGDDn9lhEosNJooAu7QC56Aqov:r6Nn28/YIILJ3OmJq5vDsNJNAoXj
MD5:	19EE889EEE6615FFBF7857779A808400
SHA1:	7EE62D6EDE1F4F3D9591E386CFA7AAE63E26C62C
SHA-256:	0981FB6C8D0B37A9B6C1F4DFDFC62FF19407908C6A13526E78B125D52E5E483A
SHA-512:	171D18C411982496B7ADD30D29CBBDF07721CBC76BFE1B476B64C0D849F0986FA72D909585741EE3E91BFC1B37E7DB81A4AAC4EEE9F1A9AB1C384BC7B61FD3E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/themes/uwmh/assets/images/twitter.jpg
Preview:	......JFIF.....d.d.....Ducky.....<...../http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c140 79.160451, 2017/05/06-01:08:21 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf :about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC 2018 Macintosh" xmpMM:InstanceID="xmp.iid:29C4057F45AA11E8ACEDB7C54AC10EED" xmpMM:DocumentID="xmp.did:29C4058045AA11E8ACEDB7C54AC10EED"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:B5596204459211E8ACEDB7C54AC10EED" stRef:documentID="xmp.did:29C4057E45AA11E8ACEDB7C54AC10EED"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\uw_education_0006-sm[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 1600x1067, frames 3
Category:	downloaded
Size (bytes):	115534
Entropy (8bit):	7.961216711956724
Encrypted:	false
SSDEEP:	1536:uHuPZYZBlA4B0qSHTVszoAKuDsErVDS6eXe3p5zgZgzrxdotqYu8kmBbV0BJmIeF:ySA2IQJl8sErVDq+5pxCu8BC4
MD5:	AD4A2955BD1728678DB53E058BBC172C
SHA1:	AC8B20709275F607F9B04AA16AC67F5606FFFF97
SHA-256:	8FAB27B0118B7F5F2405D976DA1C0A5F3BEE6D25829D5ECB7A986181F894A34D
SHA-512:	FCEF44C955C5617F8CBA8E4564D6373D1DF6FF09901B23797E1CC2E9922B985775F2037390D993275D2E35AF373080C2D4D3717975071443CA59CFF57D0141D9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2018/07/uw_education_0006-sm.jpg
Preview:	......Exif..II*.....Ducky.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:BAFF8C84814011E8831EDD06777DDD6A" xmpMM:InstanceID="xmp.iid:BAFF8C83814011E8831EDD06777DDD6A" xmp:CreatorTool="Adobe Photoshop CC 2017 Macintosh"> <xmpMM:DerivedFrom stRef:instanceID="801C1E2DD39B2B4D812B720EC0BE06C0" stRef:documentID="801C1E2DD39B2B4D812B720EC0BE06C0"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....#%'%#.//33//@@@@ @@@@@@@@@@@@.....&.....&0#....#0+.'".+550055@@?@@@@@@@@@@@@..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\wp-embed.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1426
Entropy (8bit):	5.158381671009404
Encrypted:	false
SSDEEP:	24:Q77OUdqIoZ2zsben5WlLysyIOKI1mQqRhoj3v2rFEgRuLUMB9/RUCXXmC3+:Q7SUyEsyKystOKumTsOrFEmu7Bl6CX2P
MD5:	905225D5711B559D3092387D5FFBEDBD
SHA1:	6F6C39075263BAFB9E8C10F1B34A1A0F7EE03C9D
SHA-256:	5BE614BCE53F767993A5F5F14A6BADD6AAE6BF3AF7CBDBF4D31520DE49E27991
SHA-512:	5AD34CF11ACF45AE256B2641496BE13939CD5E0212810C43AB20CADBB313A1D99CB3A451148E160D80F1F952A8514480C2953BC6CA0C4697A466A01E1C3D5F8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-includes/js/wp-embed.min.js?ver=5.5.5
Preview:	/*! This file is auto-generated */.!function(c,d){"use strict";var e=!1,n=!1;if(d.querySelector)if(c.addEventListener)e=!0;if(c.wp=c.wp||{},!c.wp.receiveEmbedMessage)if(c.wp.receiveEmbedMessage=function(e){var t=e.data;if(t)if(t.secret||t.message||t.value)if(!/[^a-zA-Z0-9]/.test(t.secret)){for(var r,a,i,s=d.querySelectorAll('iframe[data-secret="'+t.secret+'"]'),n=d.querySelectorAll('blockquote[data-secret="'+t.secret+'"]'),o=0;o<n.length;o++)n[o].style.display="none";for(o=0;o<s.length;o++)if(r=s[o],e.source===r.contentWindow){if(r.removeAttribute("style"),"height"===t.message){if(1e3<(i=parseInt(t.value,10)))i=1e3;else if(~~i<200)i=200;r.height=i}if("link"===t.message)if(a=d.createElement("a"),i=d.createElement("a"),a.href=r.getAttribute("src"),i.href=t.value,i.host===a.host)if(d.activeElement===r)c.top.location.href=t.value}},e)c.addEventListener("message",c.wp.receiveEmbedMessage,!1),d.addEventListener("DOMContentLoaded",t,!1),c.addEventListener("load",t,!1);function t(){if(!n){n=!

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\youtube[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, baseline, precision 8, 60x60, frames 3
Category:	downloaded
Size (bytes):	4069
Entropy (8bit):	4.661272399225339
Encrypted:	false
SSDEEP:	48:YAN5XhwYOS0or3dkbmEk1TWE5Qiu9gT4O:55qYOFor3yzkp7kjO
MD5:	3D02E0CCCF3E7DC7EE6A2AF2EFA83067
SHA1:	FEDDF2EBE8C38E2E32BB7CB1BBFD9380293C048D
SHA-256:	BCB5982F12B44BF922A24F80360D434226DCFCD73E075B4B649EECB81EA276F6
SHA-512:	EDEB0AE54581686A46259272FFAC03B92B2949276B0ECCC45D546352897845F0583E1C52A7CD7C399284A35A16D006142CF24C74FFC6ABB69095C938F2D049A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/themes/uwmh/assets/images/youtube.jpg
Preview:	.....Phttp://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about=""/> </rdf:RDF> </x:xmpmeta>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\162229981023009[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	799950
Entropy (8bit):	5.471681693209324
Encrypted:	false
SSDEEP:	6144:Rk1HgCSntDV/HaKKV/Ha8NEPjQHguH3HpQrwz8GWyk1HgCSntDV/HaKKV/Ha8NE1:CNE7hNE7hNE78
MD5:	121F6A20727C55A24D804BA1B20421C5
SHA1:	27E8DDA65D6C9C4A5A70C2D3999A1911B8C3B226
SHA-256:	B6CCA7B5470D574354C07E0FEADA6A8568275012E2369B9E30FC84D7ADC287AC
SHA-512:	C99F4B068C77AAB30A442960708265F6CD9B588410AC8BC8518ABEFE9CB7841ABCA3652DC60524EFD2790D1524A80E6FD4D88015BE47275EEB084FF5F7FD56A E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://connect.facebook.net/signals/config/162229981023009?v=2.9.41&r=stable
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\162229981023009[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	266650
Entropy (8bit):	5.471681693209324
Encrypted:	false
SSDEEP:	6144:Rk1HgCSntDV/HaKKV/Ha8NEPjQHguH3HpQrwz8GW6:CNE78
MD5:	18C5198F1A7E742871CD721A1574C1DB
SHA1:	567E82C738E8C2D073F63F85BB504C8D4DA29496
SHA-256:	CB43DB5EBAA086040786198B5EADF48F916AE16CE91CE53035A18768F25873C7
SHA-512:	E5EF53E58C6B3E973A8055564F7AE7B19FDEC4C868D482A318192CCD783AD338A771B58EFE132E9B8C4894A82232FE3F366265AEB469379B42B3F82C4B272472
Malicious:	false
Reputation:	low
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\All-Staff-Retreat-2019-1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=15], baseline, precision 8, 1389x787, frames 3
Category:	downloaded
Size (bytes):	362669
Entropy (8bit):	7.830383052015052
Encrypted:	false
SSDEEP:	6144:iqDFl2yYLwIfCisjvoHeGOLXAojMjuBcjP2bCk6EpUW2ZVAHCC80OR1pxx:rWhQqZqojuB+CCkhOW2Z3H0O1z
MD5:	45EEC8502A17E2A560DADE645BAACA4F
SHA1:	6BADFBA97F8B43C6FE71981B4486CB923AEAE57B
SHA-256:	6DC5658E95380947F172BEF3DF4F53DC9632C08D7B56710738AEF81256EEA9F6
SHA-512:	49381DC3864FC9C7BF133F3F53F0B73599C436C0AF2013FF95F46A8F24D3FD64960497BA4B5A827B9BFEF6654EC2E7095F08048CCE5FDC0BC634E42B6CE315A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2020/12/All-Staff-Retreat-2019-1.jpg
Preview:	......JFIF.....H.H....h.Exif..MM.*.....&.....(.....1....&....2.....>.;.....i.....R.%.....56.....5J..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\BITC_1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\BITC_1[1].jpg	
File Type:	[TIFF image data, big-endian, direntries=12, height=1080, bps=0, PhotometricInterpretation=RGB, orientation=upper-left, width=1920], baseline, precision 8, 1920x1080, frames 3
Category:	downloaded
Size (bytes):	250440
Entropy (8bit):	7.9219876434981105
Encrypted:	false
SSDEEP:	6144:4u4rVKxETlatPTgOy2FHqlubHCu9oz/9IE0FwKKbe9JsSP3x:gKxiatPT5yHlujCus/eE0FwK4etP3x
MD5:	CC67A6D512629FC51E372C413FAF2C6F
SHA1:	2F0225B9845DBFE46C005158EF4FB46745D7EC79
SHA-256:	14C16B1CAFA89DCB6D991926DBE9E42475B196D06E2D6988B32E403DB74062B4
SHA-512:	C6D929B299A9AAFE7FB714C263B5C374FE94A3AED784F4C75B7752C9AD453BB285792EEB07F0CAC7560CEEC9DAA972241715E4A9F66D6962D892499DBC084DDA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2019/03/BITC_1.jpg
Preview:	.....eExif..MM.*.....8.....(.....1.....$.....2.....i.....$.....'.....'.Adobe Photoshop CC 2019 (Macintosh).2019:03:26 13:14:56.....0221.....8.....r.....z.(.....H.....H.....Adobe_CM.....Adobe.d.....Z...".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?....a-.....9...a....Q.)..|g..U.LI.t.....$.....!?.<&...0.....wG&8.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Community-ACTS-Fund-Announces-Call-for-Advisory-Council-Members-Mile-High-United-Way[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=6], baseline, precision 8, 910x563, frames 3
Category:	downloaded
Size (bytes):	69107
Entropy (8bit):	6.750146958447572
Encrypted:	false
SSDEEP:	768:08rgrL9BSQSGUZ+TFet0xCo1hHrAS+rIaYtH+sRWcAX1zswUz1Pvd2Y6D7xy5esX:08Mf9BSQS4lxBUyLA5swwlB6DM8sl0Y
MD5:	12E71DD91BA72DF6243D49FE715232FD
SHA1:	6D51E07FD1E56838FD1F233B167ED5A77F9F55EE
SHA-256:	4857FB8ED39427C1D3AC06EA766700AAB0CB7A2F1A047B702C034634CF9BC74D
SHA-512:	FFB9857489DCD1076CC69D99BBFD7C78C07962133B06C8160FAE71F3DE4CDA3803C96390EDCC295312B566D6A6E47236A18E9BB7AE29980D9658C8C68DFD8A7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2021/02/Community-ACTS-Fund-Announces-Call-for-Advisory-Council-Members-Mile-High-United-Way.jpg
Preview:	.....JFIF.....`.`....(vExif..MM.*.....&...b.....1.....&.....2.....i.....V...F.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\GQY5EXIJ.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	65613
Entropy (8bit):	5.344682700668336
Encrypted:	false
SSDEEP:	768:LvcaAJVqodD2Hh77zTIt5XYgLvVsrZAqSSnIX7j08JGUV+71/SvUlCSvUKp:rcaAJ0Hh77za1NsrhlSvU8SvUKp
MD5:	B50BD83C21D59F75DCC35C6BB1949BDA
SHA1:	118F84E4AD815BF24191D0DDD70156ECCBC549FB
SHA-256:	8B588F88749D6A754089B38862F1BB615A6A0ECDBB5D8B09B76E532B0A7B9011
SHA-512:	54DDFB335E1803BCCB05FD630A49C1CA92E58DBADCC7AB4E60A06FF0DD8325FA89A469615DE92A4E21259E1849DC430A5A9315FA563AB90530906004FF7907EB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/
Preview:	<!DOCTYPE html>.<html lang="en-US" class="no-js">.<head> <script type="text/javascript">if(!gform){document.addEventListener("gform_main_scripts_loaded",function(){gform.scriptsLoaded=!0}),window.addEventListener("DOMContentLoaded",function(){gform.domLoaded=!0});var gform={domLoaded:!1,scriptsLoaded:!1,initializeOnLoaded:function(o){gform.domLoaded&&gform.scriptsLoaded?o():!gform.domLoaded&&gform.scriptsLoaded?window.addEventListener("DOMContentLoaded",o):document.addEventListener("gform_main_scripts_loaded",o)},hooks:{action:{},filter:{}},addAction:function(o,n,r,t){gform.addHook("action",o,n,r,t)},addFilter:function(o,n,r,t){gform.addHook("filter",o,n,r,t)},doAction:function(o){gform.doHook("action",o,arguments)},applyFilters:function(o){return gform.doHook("filter",o,arguments)},removeAction:function(o,n){gform.removeHook("action",o,n)},removeFilter:function(o,n,r){gform.removeHook("filter",o,n,r)},addHook:function(o,n,r,t,i){null==gform.hooks[o][n]&&(gform.hooks[o][n]=[]);var e=gf

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Giving-children-a-strong-start-in-like-is-one-of-Mile-high-United-Ways-three-community-impact-goals-in-Metro-Denver[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=1, orientation=upper-left], baseline, precision 8, 1200x800, frames 3
Category:	downloaded
Size (bytes):	348391
Entropy (8bit):	7.92207439049405
Encrypted:	false
SSDEEP:	6144:yYPuJ9RKMHuaRQ6GcDESVCnM+iNfZOTYQcYVQSLB99ZGthjX4TnGdY9RTRYYt:y+uJ9o2ep4EPnMFNyc4QI/98jITnGO93
MD5:	DF9ED90F153D2B99C7C3E09FA706692A
SHA1:	F63D01EDDA3E723BD7929CC15C08ECC302A29DB9
SHA-256:	77B10205A098212B3658DB59A388AF22B168841DB330AD7820AE6C3D6B89A071
SHA-512:	D140875D6C44264F4950B3594D137339C2B3A852998B551FC4A13CD252BD72EA73C12D9D99BECFBDF42BB07E080C174C371CE2311A1DEC28E6CF92CEBA5B177
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2021/05/Giving-children-a-strong-start-in-like-is-one-of-Mile-high-United-Ways-three-community-impact-goals-in-Metro-Denver.jpg
Preview:	......JFIF.....H.H....."Exif..MM.*.....XICC_PROFILE.....HLino....mntrRGB XYZ .....1..acspMSFT....IEC sRGB.....-HP ....cprt...P...3desc.....lwtpt.....bkpt.....rXYZ.....gXYZ...,....bXYZ...@....dmnd...T...pdmdd.....vued...L....view.....$lumi.....meas.....$tech...0....rTRC...<....gTRC...<....bTRC...<....text....Copyright (c) 1998 Hewlett-Packard Company..desc.....sRGB IEC61966-2.1.....sRGB IEC61966-2.1.....XYZ ..... .Q.....XYZ .....XYZ .....o...8....XYZ .....b.....XYZ .....$.....desc.....IEC http://www.iec.ch.....IEC http://www.iec.ch.....desc.... ....IEC 61966-2.1 Default RGB colour space - sRGB.....IEC 61966-2.1 Default RGB colour space - sRGB.....desc.....,Reference Viewing Condition in IEC61966-2.1.....,Reference Viewi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\KFOlCnqEu92Fr1MmEU9fBBc9[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 18 tables, 1st "GDEF", 8 names, Microsoft, language 0x409, Copyright 2011 Google Inc. All Rights Reserved.Roboto MediumRegularVersion 2.137; 2017Roboto-Me
Category:	downloaded
Size (bytes):	35588
Entropy (8bit):	6.410135551455154
Encrypted:	false
SSDEEP:	768:6yVJgIpAqZsXgDNHOBBPXNOKdhT1N+06XAxGrzmoqpxk0SnuUR:enq805OBBdhT1NP6XAxGryoqp2
MD5:	4D88404F733741EAACFDA2E318840A98
SHA1:	49E0F3D32666AC36205F84AC7457030CA0A9D95F
SHA-256:	B464107219AF95400AF44C949574D9617DE760E100712D4DEC8F51A76C50DDA1
SHA-512:	2E5D3280D5F7E70CA3EA29E7C01F47FEB57FE93FC55FD0EA63641E99E5D699BB4B1F1F686DA25C91BA4F64833F9946070F7546558CBD68249B0D853949FF85C5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc9.ttf
Preview:	..... GDEF.....{....dGPOS.....|<....GSUB7b.....8....OS/2t.#...r....`cmap.....st...Lcvt 1..K..y....\fpgm..$...v.....gasp.....{.....glyf.'.....,..j.hdmx.....r\|....head...r..n....6hhea.....q. ...$hmtx..MO..n@....loca\v@z..l(....maxp.....l.... name..:...z,....post.m.d..{.... prep...)..x|...S...d...(.....o.....9.....EX../... >Y..EX../....>Y.....9.....9.....9..... ...9.....9.....01!!.!.....!.5.!.(.<..6.....}.w...x.^.^..^.....<.....9.....EX../... >Y..EX../....>Y.....+X!...Y..../01.#.!.462...."&.~.....J.JH.H.....9KK97JJ....e...@..... %...EX../..."> Y..../..../...../01..#.3..#.3..#...-#...w.}....}.....`.....EX../... >Y..EX../... >Y..EX../....>Y..EX../....>Y.....9../.....+X!...Y...../.....+X!...Y.....01.#. #.#5!.#5!.3.3.3.3.#.3.#.#.3.#...L.L...:...N.N.N.N..:..L.v.:....f....9....`...`....f.8.9...d.-.&...,...*-...9...EX../... >Y..EX../... >Y..EX.#/.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\KFOlCnqEu92Fr1MmYUtfBBc9[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 18 tables, 1st "GDEF", 8 names, Microsoft, language 0x409, Copyright 2011 Google Inc. All Rights Reserved.Roboto BlackRegularVersion 2.137; 2017Roboto-Bla
Category:	downloaded
Size (bytes):	35208
Entropy (8bit):	6.392518822467014
Encrypted:	false
SSDEEP:	768:53Dmu13ucOmpIN22bN8o6Ze0XlGV+uM49pSeCu7XniviDffw6mo/quUR:lD13DjSNz0XlG0uL9YeCu7Xn4iTo9o/4
MD5:	4D99B85FA964307056C1410F78F51439
SHA1:	F8E30A1A61011F1EE42435D7E18BA7E21D4EE894
SHA-256:	01027695832F4A3850663C9E798EB03EADFD1462D0B76E7C5AC6465D2D77DBD0
SHA-512:	13D93544B16453FE9AC9FC025C3D4320C1C83A2ECA4CD01132CE5C68B12E150BC7D96341F10CBAA2777526CF72B2CA0CD64458B3DF1875A184BBB907C5E3D71
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmYUtfBBc9.ttf

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\KFOlCnqEu92Fr1MmYUtfBBc9[1].ttf	
Preview:	..... GDEF.....z\...dGPOS.....z.....GSUB7b.....OS/2ve#...p....`cmap.....r....Lcvt ...=..xX...Zfpgm..#...ud....gasp.....zP....glyf.....,..i~hdmx.....q ....head...R..l....6hh ea.]....p....$hmtx..<...l.....locaK./...j.....maxp.....j.... name..9...x....|post.m.d..z0... prep...C..w ...8...d...(.....P...EX../....>Y..EX../....>Y.....9.....9.....9.....9.....9.....9.....0 1!!.!.....!.5.!.(.<..6.....}.w...x.^.^..^....g.....<.....9.....EX../....>Y..EX../....>Y.....+X!...Y..../01.!.!.462..."&....+.g..k.kk.k.....J__.__.....^.....&.....9...../.....9../. .....01..#.3..#.3.+..._+...v.S.8..S.8.....z..... !..9.....EX../....>Y..EX../....>Y..EX../....>Y..EX../....>Y.....9../.....+X!...Y...../.....+X!...Y.....01.#.#.#5 3.#53.3.3.3.3.!.3.!.#.3.#.d.C.C..,..E.D.E.E...,...C.@.,....f.....`...`.....f.Q.....S.&.Q...-.r.+./..9...EX../....>Y..EX.!/..!.>Y..!...9.....!..9.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Mile-High-United-Way-Nonprofit-in-Metro-Denver[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 900 x 493, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	680149
Entropy (8bit):	7.986490567055224
Encrypted:	false
SSDEEP:	12288:4+4brBNgYvglk9ZyO2U3p7q2HJBnV0euIQpFoFt+rxTisaeQwxu7rpiYDYT:TEfg6byOl+wJ/rDYKf+Aslu71iYDYT
MD5:	A5C5A2E5B416C7D233C63EAF56603A32
SHA1:	5868F7E097400EA628A15A982D9EDB04E3DE02C5
SHA-256:	2BC27DF08FEE518ED28C4358E4516D81246574E5120EDCAD5C61ABE3CB4DA928
SHA-512:	3E3E489FD31623E975A31004586B0B35C0973CA2A85C5C589F8CEAE2204F1A3F469F47E977070DBF2D65B3C900E22EC99CA8128C9756D4C9EF976BE5B85062D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2021/01/Mile-High-United-Way-Nonprofit-in-Metro-Denver.png
Preview:	.PNG.....IHDR.....A*.....sRGB.....gAMA.....a.....pHYs...%...%.IR$.....IDATx^...,...i....=e...h.....T5.$ $n(\|.^.....7-x...](.t...L9.....Ss.....Nf....ps3555..M}l.....i.j.lmf.v[... ^...Z.....:.!.".S@.Z..\7.]G.....~).^.G..V.EZ.C.)U.....".Y[...&.....N...9l.%-W....A..-.....*.e.....e.C..~W.$...sy....(.....&...;o.6..%....[-..~.....R..<..7.K.%.&^P..Z...*.l.>_..4.u...k._.).....+.E. .lv...Qm...#..F.Q}C..w...M.|"..1..J..T....p.j.j. ..$6.W..8>.A..X.._...DT34G....m....$..._...0T...Z.....w.....&.sjS...Q4.W....Z....j..R.....R.w]...D...>...n9...G...X.1}U..z.....Ef... .d..f/.m.}....U.,.o^Z..wO}.....K[._...a..s..m.q....U;..Rr..U.>E..M..l4,...8.ZX.....^\.].g...bl:o.l...8..e.I....y5.?\wt....L.....q.q{%3,..3.F#.\..*_.biY~g....n...M....l`c...s[..v?....|c..uk... ..m.l...~.....vk..*z....._...2...l-B.7...oJc_].?".x._...412]..._.....>.a;.....0.....~.._.Wo.....m.k..Z)z.....(.[.aD....6;.')?ES9..&..!..j.r..yY.H.q2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Mile-High-United-Way-launches-HIPPY-program-in-Colorado[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=10], baseline, precision 8, 900x735, frames 3
Category:	downloaded
Size (bytes):	194941
Entropy (8bit):	7.746939426015278
Encrypted:	false
SSDEEP:	3072:bsahbOiHu4tXF0+J5jk+ZrevKWjGDXURnFpapVSq2jGLyS0QZT5dKXvI:Yalxu4tXF3JdkTXjKUrpSTL3T57
MD5:	629B6102E43C4E6A39002D8EA1F62D1A
SHA1:	CF1CA7E4D14752C6F984B57F31BADF731D34FFC1
SHA-256:	B9E011D0F31309E3607894017FE18B1966421FD3FC7AF30DEE6B059C68F12638
SHA-512:	4C4701063695B7F6610B4CACA62C2E3751F216B9CD7FE2C8F378EACD60AF832BEF5957313F991E6C6ADB3111219CB4131FDD1F6D7C6D60C1B81397A5C1CB05
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2020/12/Mile-High-United-Way-launches-HIPPY-program-in-Colorado.jpg
Preview:	......JFIF.....H.H....G0Exif..MM.*.....&.....(.....1....&....2.....i..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Vanecia-Kerr-Mile-High-United-Way[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PX_COMP_STD 2019/10/20 13:54:53.956'', baseline, precision 8, 720x959, frames 3
Category:	downloaded
Size (bytes):	74985
Entropy (8bit):	7.8600066464313665
Encrypted:	false
SSDEEP:	1536:ZDh/hZS6g0FeUxO/K+LZsA6gbvjySSJ/p8qbJWGQvo3Dp:/JRgiJO/K+yA6gv8JaK3Qw9
MD5:	705650F7BB45A47AB23D0A52F9700E00
SHA1:	550706BDFDAAF8ABB50E743638171E48B370FA25
SHA-256:	A4CA64963B6D532BAF77B2243EE2F97E941DB3BB917D0120BA76A8B7F6C03B5C
SHA-512:	A78C6D1E47A9A1C0D17F5289B1B807CE24C1269187CACBAEEDDAF9F4B1556D53F62D6173753BD509AD0E42240B04BD8C50CDFF2C135CE31E72B83A0DC54B4 32
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2020/10/Vanecia-Kerr-Mile-High-United-Way.jpg

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Vanecia-Kerr-Mile-High-United-Way[1].jpg</th></tr>
<tr><td>Preview:</td><td>......JFIF............zExif..II*.......i........................D......................`..............SflyProxyVersion 1;...........R98.........ICC_PROFILE.......lcms....mntrRGB XYZ ....).9acspAPPL.... ....-lcms..desc.......^cprt...\....wtpt...h....bkpt...|....rXYZ........gXYZ........bXYZ........rTRC.......@gTRC.......@bTRC.......@desc.. ......c2...text....FB..XYZ ....-XYZ ....3....XYZ ......o...8.....XYZ ......b.........XYZ ......$.........curv..............c...k...? .Q.4!.).2.;.F.Qw].kpz....|.i.}...0.....C..........................".$$".""&,8.&(4*""0B04::>>>&.DHD<H8<><...C..........<("(<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< <<<<..._SflyProxyVersion 1;ColorManaged; PixSense Recompression: PX_COMP_STD 2019/10/20 13:54:53.956..........."...}......</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ZPDG47U0.htm</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>65613</td></tr>
<tr><td>Entropy (8bit):</td><td>5.344682700668336</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>768:LvcaAJVqodD2Hh77zTIt5XYgLvVsrZAqSSnIX7j08JGUV+71/SvUlCSvUKp:rcaAJ0Hh77za1NsrhlSvU8SvUKp</td></tr>
<tr><td>MD5:</td><td>B50BD83C21D59F75DCC35C6BB1949BDA</td></tr>
<tr><td>SHA1:</td><td>118F84E4AD815BF24191D0DDD70156ECCBC549FB</td></tr>
<tr><td>SHA-256:</td><td>8B588F88749D6A754089B38862F1BB615A6A0ECDBB5D8B09B76E532B0A7B9011</td></tr>
<tr><td>SHA-512:</td><td>54DDFB335E1803BCCB05FD630A49C1CA92E58DBADCC7AB4E60A06FF0DD8325FA89A469615DE92A4E21259E1849DC430A5A9315FA563AB90530906004FF7907
B</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>Preview:</td><td><!DOCTYPE html>.<html lang="en-US" class="no-js">.<head> <script type="text/javascript">if(!gform){document.addEventListener("gform_main_scripts_loaded",function(){gform.scriptsLoaded=!0}),window.addEventListener("DOMContentLoaded",function(){gform.domLoaded=!0});var gform={domLoaded:!1,scriptsLoaded:!1,initializeOnLoaded:function(o){gform.domLoaded&&gform.scriptsLoaded?o():!gform.domLoaded&&gform.scriptsLoaded?window.addEventListener("DOMContentLoaded",o):document.addEventListener("gform_main_scripts_loaded",o)},hooks:{action:{},filter:{}},addAction:function(o,n,r,t){gform.addHook("action",o,n,r,t)},addFilter:function(o,n,r,t){gform.addHook("filter",o,n,r,t)},doAction:function(o){gform.doHook("action",o,arguments)},applyFilters:function(o){return gform.doHook("filter",o,arguments)},removeAction:function(o,n){gform.removeHook("action",o,n)},removeFilter:function(o,n,r){gform.removeHook("filter",o,n,r)},addHook:function(o,n,r,t,i){null==gform.hooks[o][n]&&(gform.hooks[o][n]=[]);var e=gf</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\analytics[1].js</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>ASCII text, with very long lines</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>49153</td></tr>
<tr><td>Entropy (8bit):</td><td>5.520906949461031</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>768:/yR3fYFBLbfs5sP5XqY3TyPnHpl1WY3SoavFVv6PU+CgYUD0lgEw0stZM:/y9gZfl5h3UHpaY3SoRCw0sk</td></tr>
<tr><td>MD5:</td><td>6DF1787C4BE82D1BB24F8BFFA10C7738</td></tr>
<tr><td>SHA1:</td><td>3634E839429E462E49C5F42B75FBFB4BA318AF6D</td></tr>
<tr><td>SHA-256:</td><td>2CB09C7B3E19BFC41743CA3624EF81C3258D56525647FEAC76AA757E0292627A</td></tr>
<tr><td>SHA-512:</td><td>CB3CE2BCEB61F390298C21E470423CCEB6DD93E648A7DD0467195B11FEF30BF7A086DFF47C4494E2533498D1448C1A22AAB1414C14FD73278F1C92E0F7BC3F
4</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://www.google-analytics.com/analytics.js</td></tr>
<tr><td>Preview:</td><td>(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var n=this||self,p=function(a,b){a=a.split(".");var c=n;a[0]in c||"undefined"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c=c[d]&&c[d]!==Object.prototype[d]?c[d]:c[d]={}:c[d]=b};var q={},r=function(){q.TAGGING=q.TAGGING||[];q.TAGGING[1]=!0};var t=function(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])},v=function(a){for(var b in a)if(a.hasOwnProperty(b))return!0;return!1};var x=/^(?:(?:https?|mailto|ftp):|[^:/?#]*(?:[/?#]|$))/i;var y=window,z=document,A=function(a,b){z.addEventListener?z.addEventListener(a,b,!1):z.attachEvent&&z.attachEvent("on"+a,b)};var B=/:[0-9]+$/,C=function(a,b,c){a=a.split("&");for(var d=0;d<a.length;d++){var e=a[d].split("=");if(decodeURIComponent(e[0]).replace(/\+/g," ")===b)return b=e.slice(1).join("="),c?b:decodeURIComponent(b).replace(/\+/g," ")}},F=function(a,b){b&&(b=String(b).toLowerCase());if("p</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\anchor[1].htm</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>HTML document, ASCII text, with very long lines</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>130412</td></tr>
<tr><td>Entropy (8bit):</td><td>5.896725422482859</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>3072:Gaguxl//P5gOH+guxl//P8/xguxl//POwL:suf/H5buf/H7uf/Hx</td></tr>
<tr><td>MD5:</td><td>B147A676B17D1C5DEF680B95D038C556</td></tr>
<tr><td>SHA1:</td><td>25FE50C44BBAB5ACA890B0B766102F1F062C85F4</td></tr>
<tr><td>SHA-256:</td><td>8E38DE9A44349FF0689AB229E94551E9614D5CBCE5A5910F0CC847B0F9F28B18</td></tr>
<tr><td>SHA-512:</td><td>F0C6267CCA6C462BE5E7BB811CD124D04F149291300209584858D0AD68ADCA6C3304F8794EF0EFE80D845EEACBD849B56EF43DB40C9367E57F81E279170A247</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\anchor[1].htm	
Preview:	<!DOCTYPE HTML><html dir="ltr" lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.<meta http-equiv="X-UA-Compatible" content="IE=edge">.<title>reCAPTCHA</title>.<style type="text/css">.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxP.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 500;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc9.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 900;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmYUtfBBc9.ttf) format('truetype');.}..</style>.<link rel="stylesheet" type="text/css" href="https://www.gstatic.com/recaptcha/releases/6OAif-f8nYV0qSFmq-D6Qssr/styles__ltr.css">.<script nonce="T9HPZKaOG2Ae115yKvZ5Fw" type="text/javascript">window['__recaptcha_api'] = 'https://www.google.com/rec

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\anchor[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	130139
Entropy (8bit):	5.898751148848912
Encrypted:	false
SSDEEP:	3072:kYguxl//Pj0pilR37OnOkguxl//PAsjguxl//P1L9eK:Euf/HjdtZuf/HAVuf/H1hx
MD5:	AABF79095710BB9B0888A6539A647F97
SHA1:	304626F1B2A343D694FF88A1F198E7AB913091A8
SHA-256:	21737B2C89837C5A02BB49A6B179CAF1D02A65751A4040A326B445F011CA0136
SHA-512:	079188B99F8E0D0E7B4FC29B6ADD7BE231F63D2809C4935531EBFCF31A2C3CFE8D8D28C8479AD0E8E2D26F0EE26E0E3E282E22F23EB0CAAE339AC80610D950 4D
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML><html dir="ltr" lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.<meta http-equiv="X-UA-Compatible" content="IE=edge">.<title>reCAPTCHA</title>.<style type="text/css">.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxP.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 500;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc9.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 900;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmYUtfBBc9.ttf) format('truetype');.}..</style>.<link rel="stylesheet" type="text/css" href="https://www.gstatic.com/recaptcha/releases/6OAif-f8nYV0qSFmq-D6Qssr/styles__ltr.css">.<script nonce="J/kndEJmHa0SScYgBNhJKQ" type="text/javascript">window['__recaptcha_api'] = 'https://www.google.com/rec

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\api[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1700
Entropy (8bit):	5.5017545950531765
Encrypted:	false
SSDEEP:	48:VKEctKoee1AnILrwUngKEctKoee1AnILrwUnG:f7QA8suU7QA8suG
MD5:	BBB0D5EF0FC86D37D59B34DA37E0B0CA
SHA1:	5D08B57BB8673171BCE87B12F56D7A1984CC8815
SHA-256:	B1CD43699EBA21C89847BE69338DCB7E83332B51A849B52AB28CAB0F57503348
SHA-512:	E3AECB3B4EF0F0357B4A095327410F9A4C4DFA551AA618D2BBE185BF609FB043166313EF936902DB26CD3B9D74EB20FAE4FEDBB00B597DCB599371589C1B578 4
Malicious:	false
Reputation:	low
Preview:	/* PLEASE DO NOT COPY AND PASTE THIS CODE. */(function(){var w=window,C='___grecaptcha_cfg',cfg=w[C]=w[C]||{},N='grecaptcha';var gr=w[N]=w[N]||{};gr.ready=gr.ready||function(f){(cfg['fns']=cfg['fns']||[]).push(f);};w['__recaptcha_api']='https://www.google.com/recaptcha/api2/';(cfg['render']=cfg['render']||[]).push('onload');w['__google_recaptcha_client']=true;var d=document,po=d.createElement('script');po.type='text/javascript';po.async=true;po.src='https://www.gstatic.com/recaptcha/releases/6OAif-f8nYV0qSFmq-D6Qssr/recaptcha__en.js';po.crossOrigin='anonymous';po.integrity='sha384-f1gfYQgq4OmhARgCSe1q7WV7tlcPpqu0qD+jYdSEMczD1YXPg0ibdlzvD/fZzwKc';var e=d.querySelector('script[nonce]'),n=e&&(e['nonce']||e.getAttribute('nonce'));if(n){po.setAttribute('nonce',n);}var s=d.getElementsByTagName('script')[0];s.parentNode.insertBefore(po, s);})();/* PLEASE DO NOT COPY AND PASTE THIS CODE. */(function(){var w=window,C='___grecaptcha_cfg',cfg=w[C]=w[C]||{},N='grecaptcha';var gr=w[N]=w[N]||{};gr.r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\api[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	850
Entropy (8bit):	5.5017545950531765
Encrypted:	false
SSDEEP:	24:2jkm94/zKPccAv+KVCetg1AnDsLqo40RWUnYN:VKEctKoee1AnILrwUnG
MD5:	65B6FEB732C65BEE99FD396A3E99F27F
SHA1:	8F719875F058EEE21257BC1CBCA2A6BA1A7B9A21
SHA-256:	9B7EA780F5FF5CD8A0AD4A2700143F3661284DC98D571CB38B188C2C060FE55A
SHA-512:	433CF4B099A6CFD3D98F128F86EA8C2EAACA852A38777683C7AD14953B3A4782C54985A87F5A2FCCA67CF3C2C83159EE2BBE71713338A11274D0516E4C5B8E0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\api[2].js	
IE Cache URL:	http://https://www.google.com/recaptcha/api.js
Preview:	/* PLEASE DO NOT COPY AND PASTE THIS CODE. */(function(){var w=window,C='___grecaptcha_cfg',cfg=w[C]=w[C]||{},N='grecaptcha';var gr=w[N]=w[N]||{};gr.ready=gr.ready||function(f){(cfg['fns']=cfg['fns']||[]).push(f);};w['__recaptcha_api']='https://www.google.com/recaptcha/api2/';(cfg['render']=cfg['render']||[]).push('onload');w['___google_recaptcha_client']=true;var d=document,po=d.createElement('script');po.type='text/javascript';po.async=true;po.src='https://www.gstatic.com/recaptcha/releases/6OAif-f8nYV0qSFmq-D6Qssr/recaptcha__en.js';po.crossOrigin='anonymous';po.integrity='sha384-f1gfYQgq4OmhARgCSe1q7WV7tIcPpqu0qD+jYdSEMczD1YXPg0ibdIzvD/fZzwKc';var e=d.querySelector('script[nonce]'),n=e&&(e['nonce']||e.getAttribute('nonce'));if(n){po.setAttribute('nonce',n);}var s=d.getElementsByTagName('script')[0];s.parentNode.insertBefore(po, s);})();

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bframe[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	4566
Entropy (8bit):	5.557071547101286
Encrypted:	false
SSDEEP:	96:DyA1OLKIXOgKNOMK5aXBmVh4yA1OLKIXOgKNOMK5gldcV92yA1OLKIXOgKNOMK5v:NAKIVKfKgmGAKIVKfKG0IAKIVKfKJjv
MD5:	A87D9FE353DE7CA62A1009E1DEE85585
SHA1:	29A710C24D23E6EE5CEA2594A73322FF4D60B42D
SHA-256:	DC4174BDB7CEADB7C03D299D6AFF52FCAFF825D4AACA0E12AA1DAB2021D8C071
SHA-512:	6D43A423C8307119C1FC097757E03303AA616D400D66C6D9AC788215C949167D17D8BC3F8F86FADE26C425AD00B2B32F3E2762DF4A15DE86340CCD8CF1163E
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML><html dir="ltr" lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.<meta http-equiv="X-UA-Compatible" content="IE=edge">..<title>reCAPTCHA</title>.<style type="text/css">.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxP.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 500;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc9.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 900;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmYUtfBBc9.ttf) format('truetype');.}..</style>.<link rel="stylesheet" type="text/css" href="https://www.gstatic.com/recaptcha/releases/6OAif-f8nYV0qSFmq-D6Qssr/styles__ltr.css">.<script nonce="OsVoFci8aOEjM1nwC1kmgw" type="text/javascript">window['__recaptcha_api'] = 'https://www.google.com/re

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bframe[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	4566
Entropy (8bit):	5.5780494397617755
Encrypted:	false
SSDEEP:	96:DyA1OLKIXOgKNOMK553Cu3fVO3FyA1OLKIXOgKNOMK5zfm+VGgyA1OLKIXOgKNOc:NAKIVKfKP3Cu3NO3TAKIVKfKN7tAKIVK
MD5:	ED7314186EE7E7BC181281DB482D45C4
SHA1:	4E442B4DE4EEC54D2BB2ABF2AEFFDE025F31C7F6
SHA-256:	4D0EE98215146125BCF540211F7CD51F4073B44048B80B5F734372158D6EE79A
SHA-512:	31A6AA85D6FC2FD68B6B5B0DA1A698787FAC5D7B3E1BA7DC272DF2DC48C82D8DF7D8B12BD84A9FD6BD651132BDD34D916ADB070936C173B2B0E58BF81831E142
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML><html dir="ltr" lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.<meta http-equiv="X-UA-Compatible" content="IE=edge">..<title>reCAPTCHA</title>.<style type="text/css">.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxP.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 500;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc9.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 900;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmYUtfBBc9.ttf) format('truetype');.}..</style>.<link rel="stylesheet" type="text/css" href="https://www.gstatic.com/recaptcha/releases/6OAif-f8nYV0qSFmq-D6Qssr/styles__ltr.css">.<script nonce="32q4EB2apXodV9czysMzzw" type="text/javascript">window['__recaptcha_api'] = 'https://www.google.com/re

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\community-goals[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	51517
Entropy (8bit):	5.361359513437269
Encrypted:	false
SSDEEP:	768:LvcaAJxU9I2Hh77hTIC5tYgLvVsedqSi/SvUlCSvUNp:rcaAJ+e2Hh77hRjNsfSvU8SvUNp
MD5:	4536F42A6A515260EDBB42803682DCDA
SHA1:	91FC4852D809AD85F8B4F86B0DAEDF7AB03BC320
SHA-256:	FC225302DA3B6955ABE90F1097444DC3EF15B72A8AC6A5216010B0F65FFFCF31
SHA-512:	D645F091743837347C813427615DBB2235C3EBA8F3A52D9A86ED023F8AB7FAC8C303D37AFEC1AD017E4CBA8C8ED0CCFA237F4E578B3B56512431FDB81F6BD83
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\community-goals[1].htm	
IE Cache URL:	http://https://unitedwaydenver.org/community-goals/
Preview:	<!DOCTYPE html>.<html lang="en-US" class="no-js">.<head> <script type="text/javascript">if(!gform){document.addEventListener("gform_main_scripts_loaded",function(){gform.scriptsLoaded=!0}),window.addEventListener("DOMContentLoaded",function(){gform.domLoaded=!0});var gform={domLoaded:!1,scriptsLoaded:!1,initializeOnLoaded:function(o){gform.domLoaded&&gform.scriptsLoaded?o():!gform.domLoaded&&gform.scriptsLoaded?window.addEventListener("DOMContentLoaded",o):document.addEventListener("gform_main_scripts_loaded",o)},hooks:{action:{},filter:{}},addAction:function(o,n,r,t){gform.addHook("action",o,n,r,t)},addFilter:function(o,n,r,t){gform.addHook("filter",o,n,r,t)},doAction:function(o){gform.doHook("action",o,arguments)},applyFilters:function(o){return gform.doHook("filter",o,arguments)},removeAction:function(o,n){gform.removeHook("action",o,n)},removeFilter:function(o,n,r){gform.removeHook("filter",o,n,r)},addHook:function(o,n,r,t,i){null==gform.hooks[o][n]&&(gform.hooks[o][n]=[]);var e=gf

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\d[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, CFF, length 12968, version 0.0
Category:	downloaded
Size (bytes):	12968
Entropy (8bit):	7.965782458896232
Encrypted:	false
SSDEEP:	192:l3sW6ZDcG9G9xyksMQga9ddPlolPE/lseDvryBIZrtDe2TAEaKdyg5vN1CfV5Iw0:l3aZo5peddoEHL0If+ExyYvXAVg
MD5:	A97CB1BA0011BFDA645084726D854442
SHA1:	AFAF9E5EECC89ABF4244B306902CB599C53B809F
SHA-256:	4A4417CEDB74B0813411ED99C67DE7381032F6F24AFB474EB49D61B19F9A31F1
SHA-512:	83C25A4F88A70289378830DB33F4E4C9BC56DACE1A520832B81A73F874E658A56082D41C6C6CD2DD616993D0ED40C037D7CB3F25963FC23019211E52AE1D6B9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/65a1f5/00000000000000000014689/27/d?primer=7cdcb44be4a7db8877ffa5c0007b8dd865b3bbc383831fe2ea177f62257a9191&fvd=n4&v=3
Preview:	wOFFOTTO..2.....A,.....CFF .....%...):K...DYNA..(....]...rL..CGDYN..),...{...}.W".GPOS..)........pj.<tGSUB.....OS/2...@...N...`h%f.cmap..1.....$..V2gasp...D.....head...L...4...6....hhea.....$....hmtx../L.....Amaxp.....P.name.....z...post..1..... ...2.....x.c`d``...!.0...+.3.....{.0....l..;.\f.&.(....6x...N.0..OJ...j....x.&N...#.,.QE...J"....U.V...!...].-8I,Q...e....9V.|._8...W.....m.,o..~[.3...&....~..r.>....wh.....Nh.....c'.\g..M.q.-oa..[n ...R..)...{b.*q...R.=..z..8Wbp?SV>.&.K5Z...w[m.:...V....7).j...TT9.....T.DOWtH.Pv'.Xi3t.,.....G.ScfG.gx.qf.DO<E}..... 9C.4.....#.....#,KKc.....c.>.=f...'.3..!.%.B...._..~]\..7. .g..6.e.....>=....._..N....\..w.>c.,b.TsV..NE~.:..~..)=./u....W.3.^q..ue..d.....A..Y....x.c`f.c.....=.|....3 .P.p?.....lL...100.`....0.$..t.H)00...<....x.c`d``...H*.....3'.P.....n...P.....x.]z.x...'3..-.....uwX.d.P .....".&k..dBf2.d.%

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\fbevents[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	287814
Entropy (8bit):	5.395551905316836
Encrypted:	false
SSDEEP:	3072:5zNpkjSVnYDGegzNpkjSVnYDGegzNpkjSVnYDGeI:5zDCSmDG3zDCSmDG3zDCSmDGR
MD5:	9F218879971CBE6C9F7C760899B0E2E9
SHA1:	2444DDF9E99681245ED25902B3033A0174E32F7E
SHA-256:	E6689429457F5D1A7719D8F705877D2CD90CCEFE6C1B7382C7A6E2F16D1500D8
SHA-512:	141F67C89CE0C758CB515F7DC44C1069EE59707AFC3A5CBFF1DFD4A3AF78223F059F80EEE4038E67FEEC2F26FBBA1F36174785F1AB2CC57089DE8B0589F600A
Malicious:	false
Reputation:	low
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\fbevents[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	287814
Entropy (8bit):	5.395551905316836
Encrypted:	false
SSDEEP:	3072:5zNpkjSVnYDGegzNpkjSVnYDGegzNpkjSVnYDGeI:5zDCSmDG3zDCSmDG3zDCSmDGR
MD5:	9F218879971CBE6C9F7C760899B0E2E9
SHA1:	2444DDF9E99681245ED25902B3033A0174E32F7E
SHA-256:	E6689429457F5D1A7719D8F705877D2CD90CCEFE6C1B7382C7A6E2F16D1500D8
SHA-512:	141F67C89CE0C758CB515F7DC44C1069EE59707AFC3A5CBFF1DFD4A3AF78223F059F80EEE4038E67FEEC2F26FBBA1F36174785F1AB2CC57089DE8B0589F600A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\fbevents[2].js

Malicious:	false
Reputation:	low
IE Cache URL:	http://https://connect.facebook.net/en_US/fbevents.js
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\gtm[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	320226
Entropy (8bit):	5.533414806927065
Encrypted:	false
SSDEEP:	6144:gwxvi/YYrwH5PgHwxvi/Y1rwH5PgHwxvi/Y1rwH5PgM:SY2GwYNGwYNGV
MD5:	E27CC5D0017E13CE29FCA4E2CF7AA1E2
SHA1:	FCE3BD558857ADBD871B282D5AB7047B1F58CFE6
SHA-256:	B78DA990BC5BDE4BCBBD8116AD4E6D7E16D2170CE7F4B59E2B971AE3CBCC7521
SHA-512:	8628D69B1F2BC25EA696FBFEA9938680D20A74F3D96168110C1A5464B28307BEE591A73DC7A1B07C5188082C5F6CE9382F91EA95C2BC8F6999636D09C25E1C4
Malicious:	false
Reputation:	low
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"11",. . "macros":[{. "function":"__e". },{. "function":"__gas",. "vtp_cookieDomain":"auto",. "vtp_doubleClick":false,. "vtp_setTrackerName":false,. "vtp_useDebugVersion":false,. "vtp_useHashAutoLink":false,. " vtp_decorateFormsAutoLink":false,. "vtp_enableLinkId":false,. "vtp_enableEcommerce":false,. "vtp_trackingId":"UA-4803183-1",. "vtp_enableRecaptchaOpti on":false,. "vtp_enableUaRlsa":false,. "vtp_enableUseInternalVersion":false,. "vtp_enableGA4Schema":false. },{. "function":"__v",. "vtp_name": "gtm.triggers",. "vtp_dataLayerVersion":2,. "vtp_setDefaultValue":true,. "vtp_defaultValue":"". },{. "function":"__u",. "vtp_enableMultiQueryKeys":false,. "vtp_enableIgnoreEmptyQueryParam":false. },{. "function":"__aev",. "vtp_varType":"TEXT". },{.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\gtm[2].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	320226
Entropy (8bit):	5.53329194189478
Encrypted:	false
SSDEEP:	6144:gwxvi/Y1rwH5PgHwxvi/YYrwH5PgHwxvi/YurwH5PgM:SYNGwY2GwYgGV
MD5:	220D92CA5A1253FCC90D2FCD206F7198
SHA1:	24DA866D61B35CC6F9C8C2EC9A2D67DE28BA8AFC
SHA-256:	A63C3A1B4F7702B3A9C6E42F307749D9FA0BAC3E9AE3170394B34824450DE7AE
SHA-512:	C6249864778DD93C4F44BAF60AAF5DE53B4BE187C7A37A434675F15F1B84A4E09BCFE7D0BC8C0FDBF906D1C72FAE45777FBF7B25641D6DEB74AAB4D696432F 29
Malicious:	false
Reputation:	low
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"11",. . "macros":[{. "function":"__e". },{. "function":"__gas",. "vtp_cookieDomain":"auto",. "vtp_doubleClick":false,. "vtp_setTrackerName":false,. "vtp_useDebugVersion":false,. "vtp_useHashAutoLink":false,. " vtp_decorateFormsAutoLink":false,. "vtp_enableLinkId":false,. "vtp_enableEcommerce":false,. "vtp_trackingId":"UA-4803183-1",. "vtp_enableRecaptchaOpti on":false,. "vtp_enableUaRlsa":false,. "vtp_enableUseInternalVersion":false,. "vtp_enableGA4Schema":false. },{. "function":"__v",. "vtp_name": "gtm.triggers",. "vtp_dataLayerVersion":2,. "vtp_setDefaultValue":true,. "vtp_defaultValue":"". },{. "function":"__u",. "vtp_enableMultiQueryKeys":false,. "vtp_enableIgnoreEmptyQueryParam":false. },{. "function":"__aev",. "vtp_varType":"TEXT". },{.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\listening_480[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=1, copyright=II*], baseline, precision 8, 480x500, frames 3
Category:	downloaded
Size (bytes):	47107
Entropy (8bit):	7.970082184346261
Encrypted:	false
SSDEEP:	768:bbHt5nbUqFJpFSyiYQuphn3J4TpgWAAqn4ACbdPeq/qSWzM6YaWjACmcTYBEJ3sn:fPnbnFJpFSTYr7n3kuW2n4AmeqTyMJaB
MD5:	F234B8D6FAF68FEE2C5AE08EAD338245
SHA1:	91055270FA5A318FD895315D8EF4817A19F738F0
SHA-256:	BEA54A872DCAC0A0F86FB0F7FEBCD03B4E3B7E71C19297397658A0AF8263A5EE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\listening_480[1].jpg	
SHA-512:	3B344EFFB4CE977FC009DF89DC2C795C39EB6B2950C7A745D0B2B4480B1AA4056F5709DD11E688971E12D2F06ECFB43FBF17E7F26A17226F43D33124BBD5CBI A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/uploads/2018/05/listening_480.jpg
Preview:	.....$Exif..II*.....Ducky.....:.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe: ns:meta/" x:xmptk="Adobe XMP Core 5.6-c140 79.160451, 2017/05/06-01:08:21 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Descr iption rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xa p/1.0/" xmpMM:DocumentID="xmp.did:B86E033C555511E89227FBB653962E69" xmpMM:InstanceID="xmp.iid:B86E033B555511E89227FBB653962E69" xmp:CreatorT ool="Adobe Photoshop CC 2018 Macintosh"> <xmpMM:DerivedFrom stRef:instanceID="5D80FAAE513B6BDCF0FAB698B6D87062" stRef:documentID="5D80FAAE51 3B6BDCF0FAB698B6D87062"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>...HPhotoshop 3.0.8BIM.....Z...%G.....8BIM.%.....x/4b4.Xw .....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\logo-gray@2x[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 236 x 144, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	11395
Entropy (8bit):	7.953582075052842
Encrypted:	false
SSDEEP:	192:4fqwpBS8kKgJSWMjEMNZveDVlYBIw9LdPNoCIvbXn3X8tW46MbggHwNqdhcWct8d:Twp8Ju4pOBZLdPNoCG33P4Bb4qdGqCS
MD5:	A7F6F1D67BD5D12367B143D578EECE6B
SHA1:	57A813BB6ED19664B801313065490EE4D9D173CA
SHA-256:	A1684BBEEECD878DC1EEC80AE51C98269897EB1D47C1DE241B9889F3E0F2EA01
SHA-512:	A9EA9BF501F8A8095C363676AC0B9580BADD140EE7CF36A080F0118B3A2609F5287DDE072C752065C076AE522B23DA34DC1DC01BBF55ABF73057C2953C43767
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/wp-content/themes/uwmh/assets/images/logo-gray@2x.png
Preview:	.PNG.....IHDR.....3.....tEXtSoftware.Adobe ImageReadyq.e<...xiTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpme ta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http ://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:26c3552b-0c9f-41a8-bd0a-0fb3508f82cc" xmpMM:DocumentID="xmp.did:DAAE87F440F011E8 A49C906F8F232B31" xmpMM:InstanceID="xmp.iid:DAAE87F340F011E8A49C906F8F232B31" xmp:CreatorTool="Adobe Photoshop CC 2017 (Macintosh)"> <xmpMM: DerivedFrom stRef:instanceID="xmp.iid:26c3552b-0c9f-41a8-bd0a-0fb3508f82cc" stRef:documentID="xmp.did:26c3552b-0c9f-41a8-bd0a-0fb3508f82cc"/> </rdf:De scription> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>e.J...(.IDATx..]..V.....R.C3!.2..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\logo_48[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	2228
Entropy (8bit):	7.82817506159911
Encrypted:	false
SSDEEP:	48:4/6MuQu6DYYEcBDlBVzqawiHI1Oupgl8m7NCnagQJFknwD:4SabhtXqMHyCl8m7N0ag6D
MD5:	EF9941290C50CD3866E2BA6B793F010D
SHA1:	4736508C795667DCEA21F8D864233031223B7832
SHA-256:	1B9EFB22C938500971AAC2B2130A475FA23684DD69E43103894968DF83145B8A
SHA-512:	A0C69C70117C5713CAF8B12F3B6E8BBB9CDAF72768E5DB9DB5831A3C37541B87613C6B020DD2F9B8760064A8C7337F175E7234BFE776EEE5E3588DC5662419D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/recaptcha/api2/logo_48.png
Preview:	.PNG.....IHDR...0...0.....W.....gAMA.....a.... cHRM..z&.....u0...`.:....p..Q<....bKGD.....C.....pHYs.....IDATh...P....=..8.....Nx. ..PlP8..;.C.1iL#6...*.Z..!.....3.po .o.L.i.I..1fl..4..ujL&6$.....w.....,Z..z. ~.....\._.C.eK...g..%..P..L7...96..q....L.....k6...*..,xz._.....B."#...L(n..f..Yb...*.8.;....K)N...H).%.F"Ic.LB.....jG.uD..B....Tm....T. .).A.}D.f..3.V.....O.....t_..].x.{o.....*....x?!W...j..@..G=Ed.XF.....J..E?../]..?p..W..H..d5% WA+.....)2r..+..'qk8.../HS.[...u..z.P.*....-.A.}.....I .P.....S....|...)..KS4....I.....W...@....S. s..s..$`.X9.....E.x.=.u.*iJ.....k.....'...!.a....*+.....(...S..\h....@.....I.$..%.2....l.....a.|.....U...y.....t..8....TF.o.p.+.@<.g.....-.M.....:.@..(.....@.....>..=.ofm.WM{...e.,..D.r.. .....w....T.L.os..T@Rv..;.....9....56<.x.....2.k.1....dd.V.....m..y5../4|...G.p.V.....6...}.....B.....5...&..v..yTd.6...../m.K...(.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\mxg5ixn[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	10508
Entropy (8bit):	5.287785115304218
Encrypted:	false
SSDEEP:	192:p6kMCMQM7Q6kMCMQM7Q6kMCMQM7Q6kMCMQM7o:gfZ71fZ71fZ71fZ7o
MD5:	BE02EE30E270BFFDC4BFE030D2FDE1F7
SHA1:	F5CC80ED7FBF934940E18A8EC0A91A5D1F840486

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\mxg5ixn[1].css	
SHA-256:	792C8A4993AE7CE0A3BC720282B3B8D5279C9C7923CB23D1E4A1EE71449E130D
SHA-512:	2EE96A6C8C09DEED5F8F53F4288FEBE7DC7A17DB840E7D75A98A4CFB4F12F1439B83DD93ACE33CF2CD16353A29A2CC29DB97289575F6D5E44BBA6E50D2F6C44F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/mxg5ixn.css
Preview:	/*. * The Typekit service used to deliver this font or fonts for use on websites. * is provided by Adobe and is subject to these Terms of Use. * http://www.adobe.com/products/eulas/tou_typekit. For font license. * information, see the list below.. *. * league-gothic:. * - http://typekit.com/eulas/00000000000000000014689. * roboto:. * - http://typekit.com/eulas/00000000000000003b9ad05f. * - http://typekit.com/eulas/00000000000000003b9ad05b. *. * . 2009-2021 Adobe Systems Incorporated. All Rights Reserved.. */./*{"last_published":"2020-01-09 22:05:10 UTC"}*/..@import url("https://p.typekit.net/p.css?s=1&k=mxg5ixn&ht=tk&f=1344.15498.15510&a=8688369&app=typekit&e=css");..@font-face {.font-family:"league-gothic";.src:url("https://use.typekit.net/af/65a1f5/00000000000000000014689/27/l?primer=7cdcb44be4a7db8877ffa5c0007b8dd865b3bbc383831fe2ea177f62257a9191&fvd=n4&v=3") format("woff2"),url("https://use.typekit.net/af/65a1f5/00000000000000000014689/27/d?primer=7cdcb44be4a7db8877ffa5c0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\mxg5ixn[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	2627
Entropy (8bit):	5.287785115304218
Encrypted:	false
SSDEEP:	48:35Y2zQVOHN8SK+GkfGO8GbM8aGnGkGkMVUG2G/GbM7o:pbzQfX0M8TMVuM7o
MD5:	514D758AD2AF12E9A1772CAAEE0F15DF
SHA1:	DEAB71BEBD59EF1AD138B619F0C2420CBD5885A1
SHA-256:	C6956F1A65A1BFA585BC50C71C74AF4DE9A84F9860FD1D971187A8F318BD4FAC
SHA-512:	8F0D66B85F867238C298E4D914C30718B8DFF1FE61D3E86C693CC34052C3C57581907F807BB425604C51EBBEF9A220BBCEE77F11B45D94D4167C228527405780
Malicious:	false
Reputation:	low
Preview:	/*. * The Typekit service used to deliver this font or fonts for use on websites. * is provided by Adobe and is subject to these Terms of Use. * http://www.adobe.com/products/eulas/tou_typekit. For font license. * information, see the list below.. *. * league-gothic:. * - http://typekit.com/eulas/00000000000000000014689. * roboto:. * - http://typekit.com/eulas/00000000000000003b9ad05f. * - http://typekit.com/eulas/00000000000000003b9ad05b. *. * . 2009-2021 Adobe Systems Incorporated. All Rights Reserved.. */./*{"last_published":"2020-01-09 22:05:10 UTC"}*/..@import url("https://p.typekit.net/p.css?s=1&k=mxg5ixn&ht=tk&f=1344.15498.15510&a=8688369&app=typekit&e=css");..@font-face {.font-family:"league-gothic";.src:url("https://use.typekit.net/af/65a1f5/00000000000000000014689/27/l?primer=7cdcb44be4a7db8877ffa5c0007b8dd865b3bbc383831fe2ea177f62257a9191&fvd=n4&v=3") format("woff2"),url("https://use.typekit.net/af/65a1f5/00000000000000000014689/27/d?primer=7cdcb44be4a7db8877ffa5c0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\news[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	79888
Entropy (8bit):	5.316508035457387
Encrypted:	false
SSDEEP:	1536:rcaAJqHh775a0NsN1Clf4aUNHcBAVouucB5YdA5XJOx8EOa4sqboprzruLirSvUR:rFph771smFr7N4HIufv+vZp
MD5:	6CE89B061A990EA0B65DAE15B2070827
SHA1:	DB64F720ED225FF6854667CF3553B2DFFF82443B
SHA-256:	5A23A4C341A62BE304F53EC4F9E6172EA3A75B7FF5EEA74252EBBF90704FEA39
SHA-512:	D81B186C48110849B3C9F8B223295A3574BB8E91A9FD34ABCA8624676933798EC4718B473BBF99447CC6B09F51BF5242A17E1CC3C7FD0A9EBA43D0CB1983FCD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unitedwaydenver.org/news/
Preview:	<!DOCTYPE html>.<html lang="en-US" class="no-js">.<head> <script type="text/javascript">if(!gform){document.addEventListener("gform_main_scripts_loaded",function(){gform.scriptsLoaded=!0}),window.addEventListener("DOMContentLoaded",function(){gform.domLoaded=!0});var gform={domLoaded:!1,scriptsLoaded:!1,initializeOnLoaded:function(o){gform.domLoaded&&gform.scriptsLoaded?o():!gform.domLoaded&&gform.scriptsLoaded?window.addEventListener("DOMContentLoaded",o):document.addEventListener("gform_main_scripts_loaded",o)},hooks:{action:{},filter:{}},addAction:function(o,n,r,t){gform.addHook("action",o,n,r,t)},addFilter:function(o,n,r,t){gform.addHook("filter",o,n,r,t)},doAction:function(o){gform.doHook("action",o,arguments)},applyFilters:function(o){return gform.doHook("filter",o,arguments)},removeAction:function(o,n){gform.removeHook("action",o,n)},removeFilter:function(o,n,r){gform.removeHook("filter",o,n,r)},addHook:function(o,n,r,t,i){null==gform.hooks[o][n]&&(gform.hooks[o][n]=[]);var e=gf

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\prometheus_png[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 200 x 1, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	134
Entropy (8bit):	5.606197490261754
Encrypted:	false
SSDEEP:	3:yionv//thPlvutxewih/rywOpgOV5PaJERZzUTYxobWgpwH5jp:6v/lhPksJhmtz5SuRZzFYWkuBp
MD5:	9878766124E9E3B0F731F152E76DEA0A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\prometheus_png[1].png	
SHA1:	AD29A9CDA5CE4DA966D0FB82D4B5F1867D9B531B
SHA-256:	EDA9FDCC7C626E8D6AB4982A17F4E5413A68275C7233C70BBBEDB4AFCBE646B8
SHA-512:	C2AB316CB9E5F98DC9DA828897FD4CB8011DE70899558EF88089C34264E3F2B408E9819BA322B790BB495B063BE9933FA807E30350088BBD5ACB0EC19A7D97A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://prometheusintelligencetechnology.com/php/prometheus_png.php?name=pit_cookie&cookie=prometheus_png
Preview:	.PNG........IHDR...............v.....pHYs..........+.....8IDAT(.c4M....../...W~_``c.....t....f#f..?..6.w~>.(......*....J.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\styles__ltr[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):	52867
Entropy (8bit):	5.958224586944697
Encrypted:	false
SSDEEP:	768:+LUmmAWTe2uXYp8Mi+yKSrKebyBwd/Dl+x2d5YPcPoiDH1fkQJVEwY:4UcW6v+2rKwFDlDP7dnY
MD5:	B1207A1EFB3FC87C56B8EEC39EC65B4C
SHA1:	C1F3A3A13E5D0595AC22227B12FEF4949C7C79E0
SHA-256:	5FE20047C1CC1BE61A786D56C5C02B96453B9C60656D6C8429A1ADD79017E47F
SHA-512:	A4F7279F7C1BB35B9239712C4B954E752FF98739AB38520F1B8E12A75485EA6F2890EBA6AD7FDF074C94928FFA7ECA5A84B32AEAC9EBB10467AC6F082BE189E 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/recaptcha/releases/6OAif-f8nYV0qSFmq-D6Qssr/styles__ltr.css
Preview:	.goog-inline-block{position:relative;display:-moz-inline-box;display:inline-block}* html .goog-inline-block{display:inline}*:first-child+html .goog-inline-block{display:inline}.recaptcha-checkbox{border:none;font-size:1px;height:28px;margin:4px;width:28px;overflow:visible;outline:0;vertical-align:text-bottom}.recaptcha-checkbox-border{-webkit-border-radius:2px;-moz-border-radius:2px;border-radius:2px;background-color:#fff;border:2px solid #c1c1c1;font-size:1px;height:24px;position:absolute;width:24px;z-index:1}.recaptcha-checkbox-borderAnimation{background-image:url(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\swap[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	32
Entropy (8bit):	3.5931390622295662
Encrypted:	false
SSDEEP:	3:U8xf9:U8xF
MD5:	7867213E624C00E30F2110C66AB75B29
SHA1:	8DB8D0D2B891F98F0CC9BBA6BC0E70D39C80F275
SHA-256:	D18BEBA8A6DB32DD84B24258CF6542ACCA7684B030E529EF2977198993400C4B
SHA-512:	B8FAAF14E84CA9D06902EBF39616CD13029F1049F7D5BCA60A5ABF22E42381322A9E79260349BE6834EDE39C800EC1D45C20F1D260EC9C1F40DB7425C037D5E 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.callreports.com/companies/992008090/5e73f27e03b01ab4acc3/12/swap.js
Preview:	/* this account is not active */

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\tpin[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CU9yltxlHh/:m/
MD5:	DF3E567D6F16D040326C7A0EA29A4F41
SHA1:	EA7DF583983133B62712B5E73BFFBCD45CC53736
SHA-256:	548F2D6F4D0D820C6C5FFBEFFCBD7F0E73193E2932EEFE542ACCC84762DEEC87
SHA-512:	B2CA25A3311DC42942E046EB1A27038B71D689925B7D6B3EBB4D7CD2C7B9A0C7DE3D10175790AC060DC3F8ACF3C1708C336626BE06879097F4D0ECAA7F5670 1
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\tpin[1].gif	
Reputation:	low
IE Cache URL:	http://https://trackingpin.com/tpin.php?action_name=Community%20Goals%20-%20Mile%20High%20United%20Way&idsite=232&rec=1&r=453677&h=23&m=4&s=1&url=https%3A%2F%2Funitedwaydenver.org%2Fcommunity-goals%2F&_id=da982bd7b09ecc94&_idts=1623823381&_idvc=1&_idn=0&_refts=0&_viewts=1623823381&send_image=1&pdf=0&qt=0&realp=0&wma=0&dir=0&fla=1&java=1&gears=0&ag=0&cookie=1&res=1280x1024>_ms=2&pv_id=6jvlwt
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\tpin[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	62400
Entropy (8bit):	5.522642762690928
Encrypted:	false
SSDEEP:	1536:Bs2uk/OvnBWihiFK6QQVbxQFkivEN8mMsN8MVF:L/GviQqVaEXd
MD5:	2CF6FE97A112F253B2AF703295FC1C84
SHA1:	9EA9D32842D246B3EE12B264D35E386C3A754F0B
SHA-256:	B164E6A4BA2E7559725AB4B3E04B81B5240F1C542C0F035D96F5D3F454D2C999
SHA-512:	97E24E55129D311408580E33C80223EF7A8FD34740049C4E431D6AB1BEC8956D53DCF4249BCA82AB949A42E083393C5EFA258437A281D2FC626213D202B027E5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://trackingpin.com/tpin.js
Preview:	if(typeof JSON_PIWIK!=="object"&&typeof window.JSON==="object"&&window.JSON.stringify&&window.JSON.parse){JSON_PIWIK=window.JSON}else{(function(){var a={};./*!! JSON v3.3.2 | http://bestiejs.github.io/json3 | Copyright 2012-2014, Kit Cambridge | http://kit.mit-license.org */.(function(){var c=typeof define==="function" &&define.amd;var e={"function":true,object:true};var h=e[typeof a]&&a&&!a.nodeType&&a;var i=e[typeof window]&&window||this,b=h&&e[typeof module]&&module&&!module.nodeType&&typeof global=="object"&&global;if(b&&(b.global===b||b.window===b||b.self===b)){i=b}function j(ab,V){ab||(ab=i.Object());V||(V=i.Object());var K=ab.Number||i.Number,R=ab.String||i.String,x=ab.Object||i.Object,S=ab.Date||i.Date,T=ab.SyntaxError||i.SyntaxError,aa=ab.TypeError||i.TypeError,J=ab.Math||i.Math,Y=ab.JSON||i.JSON;.if(typeof Y=="object"&&Y){V.stringify=Y.stringify;V.parse=Y.parse}var n=x.prototype,u=n.toString,r,m,L;var B=new S(-3509827334573292);try{B=B.getUTCFullYear()==-109252&&B.getUTCMonth(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\tpin[2].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CU9yltxlHh/:m/
MD5:	DF3E567D6F16D040326C7A0EA29A4F41
SHA1:	EA7DF583983133B62712B5E73BFFBCD45CC53736
SHA-256:	548F2D6F4D0D820C6C5FFBEFFCBD7F0E73193E2932EEFE542ACCC84762DEEC87
SHA-512:	B2CA25A3311DC42942E046EB1A27038B71D689925B7D6B3EBB4D7CD2C7B9A0C7DE3D10175790AC060DC3F8ACF3C1708C336626BE06879097F4D0ECAA7F56701
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://trackingpin.com/tpin.php?action_name=Diversity%2C%20Equity%2C%20and%20Inclusion%20-%20Mile%20High%20United%20Way&idsite=232&rec=1&r=529335&h=23&m=4&s=8&url=https%3A%2F%2Funitedwaydenver.org%2Fdiversity-equity-and-inclusion%2F&_id=da982bd7b09ecc94&_idts=1623823381&_idvc=1&_idn=0&_refts=0&_viewts=1623823381&send_image=1&pdf=0&qt=0&realp=0&wma=0&dir=0&fla=1&java=1&gears=0&ag=0&cookie=1&res=1280x1024>_ms=11&pv_id=bbXeZ3
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\tpin[3].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CU9yltxlHh/:m/
MD5:	DF3E567D6F16D040326C7A0EA29A4F41
SHA1:	EA7DF583983133B62712B5E73BFFBCD45CC53736
SHA-256:	548F2D6F4D0D820C6C5FFBEFFCBD7F0E73193E2932EEFE542ACCC84762DEEC87
SHA-512:	B2CA25A3311DC42942E046EB1A27038B71D689925B7D6B3EBB4D7CD2C7B9A0C7DE3D10175790AC060DC3F8ACF3C1708C336626BE06879097F4D0ECAA7F56701
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\tpin[3].gif	
IE Cache URL:	http://https://trackingpin.com/tpin.php?action_name=Leadership%20and%20Board%20-%20Mile%20High%20United%20Way&idsite=232&rec=1&r=835899&h=23&m=4&s=16&url=https%3A%2F%2Funitedwaydenver.org%2Fleadership-and-board%2F&_id=da982bd7b09ecc94&_idts=1623823381&_idvc=1&_idn=0&_refts=0&_viewts=1623823381&send_image=1&pdf=0&qt=0&realp=0&wma=0&dir=0&fla=1&java=1&gears=0&ag=0&cookie=1&res=1280x1024>_ms=58&pv_id=PQShx6
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\tpin[4].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CU9yltxlHh/:m/
MD5:	DF3E567D6F16D040326C7A0EA29A4F41
SHA1:	EA7DF583983133B62712B5E73BFFBCD45CC53736
SHA-256:	548F2D6F4D0D820C6C5FFBEFFCBD7F0E73193E2932EEFE542ACCC84762DEEC87
SHA-512:	B2CA25A3311DC42942E046EB1A27038B71D689925B7D6B3EBB4D7CD2C7B9A0C7DE3D10175790AC060DC3F8ACF3C1708C336626BE06879097F4D0ECAA7F56701
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://trackingpin.com/tpin.php?action_name=Annual%20Reports%20and%20Financials%20-%20Mile%20High%20United%20Way&idsite=232&rec=1&r=920124&h=23&m=4&s=24&url=https%3A%2F%2Funitedwaydenver.org%2Fannual-reports-and-financials%2F&_id=da982bd7b09ecc94&_idts=1623823381&_idvc=1&_idn=0&_refts=0&_viewts=1623823381&send_image=1&pdf=0&qt=0&realp=0&wma=0&dir=0&fla=1&java=1&gears=0&ag=0&cookie=1&res=1280x1024>_ms=5&pv_id=mJmbjs
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\tpin[5].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CU9yltxlHh/:m/
MD5:	DF3E567D6F16D040326C7A0EA29A4F41
SHA1:	EA7DF583983133B62712B5E73BFFBCD45CC53736
SHA-256:	548F2D6F4D0D820C6C5FFBEFFCBD7F0E73193E2932EEFE542ACCC84762DEEC87
SHA-512:	B2CA25A3311DC42942E046EB1A27038B71D689925B7D6B3EBB4D7CD2C7B9A0C7DE3D10175790AC060DC3F8ACF3C1708C336626BE06879097F4D0ECAA7F56701
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://trackingpin.com/tpin.php?action_name=Book%20a%20Conference%20Room%20-%20Mile%20High%20United%20Way&idsite=232&rec=1&r=731894&h=23&m=4&s=31&url=https%3A%2F%2Funitedwaydenver.org%2Fcobank-leadership-center%2F&_id=da982bd7b09ecc94&_idts=1623823381&_idvc=1&_idn=0&_refts=0&_viewts=1623823381&send_image=1&pdf=0&qt=0&realp=0&wma=0&dir=0&fla=1&java=1&gears=0&ag=0&cookie=1&res=1280x1024>_ms=6&pv_id=Le2zev
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\webworker[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	204
Entropy (8bit):	4.845760881630304
Encrypted:	false
SSDEEP:	3:JSbMqSL1cdXWKQKIYCjogWaeTxBMqSL1cdXWKQKIYCjogWaee:PLKdXNQKIX0g4xgLKdXNQKIX0gL
MD5:	CC5C41709EC60FD3137C3BA530A4B67D
SHA1:	B2E1DBDDF072FDA7E5FF374F96EDEDA4F0D6BBB6
SHA-256:	D8C9618E5C04E0AFF09C33BE18CEC1E2AD0832D632C4780C23CC3E9927D70736
SHA-512:	4F089C5BF6EE6994DF1307CCF2F539A95226A5779C5C0F92883ADA2032BAA52E5672F24C11AEA01D62C702DE3AB3F196CEC23A9B1CE5C1111D7A23224E226E7B
Malicious:	false
Reputation:	low
Preview:	importScripts('https://www.gstatic.com/recaptcha/releases/6OAif-f8nYV0qSFmq-D6Qssr/recaptcha__en.js');importScripts('https://www.gstatic.com/recaptcha/releases/6OAif-f8nYV0qSFmq-D6Qssr/recaptcha__en.js');

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\1622299810230009[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	533300
Entropy (8bit):	5.471681693209324
Encrypted:	false
SSDEEP:	6144:Rk1HgCSntDV/HaKKV/Ha8NEPjQHguH3HpQrwz8GWyk1HgCSntDV/HaKKV/Ha8NEw:CNE7hNE78
MD5:	EFB199411623C351AD9698D5A090640B
SHA1:	0F328831C1D2928AD03904059FBFCD0F337F19D8
SHA-256:	16169E5729BF43DAE8DF284FE31516B545A59E78FEA516AA7E7A84B70F6631E2
SHA-512:	1B5CF73CA46EE1A3331561C2565684F3BE2E773FA418F0A88C8D195E7ED8EBBE791DA07C4076A7A52F3F7C80C9DCBA440FB1D9ECF18515D5E0EF340B8FA93C75
Malicious:	false
Reputation:	low
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\1622299810230009[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	266650
Entropy (8bit):	5.471681693209324
Encrypted:	false
SSDEEP:	6144:Rk1HgCSntDV/HaKKV/Ha8NEPjQHguH3HpQrwz8GW6:CNE78
MD5:	18C5198F1A7E742871CD721A1574C1DB
SHA1:	567E82C738E8C2D073F63F85BB504C8D4DA29496
SHA-256:	CB43DB5EBAA086040786198B5EADF48F916AE16CE91CE53035A18768F25873C7
SHA-512:	E5EF53E58C6B3E973A8055564F7AE7B19FDEC4C868D482A318192CCD783AD338A771B58EFE132E9B8C4894A82232FE3F366265AEB469379B42B3F82C4B272472
Malicious:	false
Reputation:	low
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 15, 2021 23:02:56.492974043 CEST	192.168.2.3	8.8.8.8	0xd8e0	Standard query (0)	www.unitedwaydenver.org	A (IP address)	IN (0x0001)
Jun 15, 2021 23:02:56.992384911 CEST	192.168.2.3	8.8.8.8	0x8aed	Standard query (0)	unitedwaydenver.org	A (IP address)	IN (0x0001)
Jun 15, 2021 23:02:57.687824011 CEST	192.168.2.3	8.8.8.8	0x7dc4	Standard query (0)	use.typekit.net	A (IP address)	IN (0x0001)
Jun 15, 2021 23:02:58.125468016 CEST	192.168.2.3	8.8.8.8	0x3d9d	Standard query (0)	p.typekit.net	A (IP address)	IN (0x0001)
Jun 15, 2021 23:02:59.635195017 CEST	192.168.2.3	8.8.8.8	0x12c2	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jun 15, 2021 23:03:00.763946056 CEST	192.168.2.3	8.8.8.8	0xf975	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Jun 15, 2021 23:03:00.771258116 CEST	192.168.2.3	8.8.8.8	0xe87b	Standard query (0)	ads.pinbusinessnetwork.com	A (IP address)	IN (0x0001)
Jun 15, 2021 23:03:00.782221079 CEST	192.168.2.3	8.8.8.8	0x3e5a	Standard query (0)	trackingpin.com	A (IP address)	IN (0x0001)
Jun 15, 2021 23:03:00.786397934 CEST	192.168.2.3	8.8.8.8	0xc0f2	Standard query (0)	cdn.callreports.com	A (IP address)	IN (0x0001)
Jun 15, 2021 23:03:00.823280096 CEST	192.168.2.3	8.8.8.8	0x411d	Standard query (0)	prometheusintelligencetechnology.com	A (IP address)	IN (0x0001)
Jun 15, 2021 23:03:00.839879036 CEST	192.168.2.3	8.8.8.8	0x6277	Standard query (0)	dsppixel.pinbn.net	A (IP address)	IN (0x0001)
Jun 15, 2021 23:03:00.893847942 CEST	192.168.2.3	8.8.8.8	0x3ceb	Standard query (0)	www.google.de	A (IP address)	IN (0x0001)
Jun 15, 2021 23:03:01.077008963 CEST	192.168.2.3	8.8.8.8	0x6b10	Standard query (0)	pixel.sitescout.com	A (IP address)	IN (0x0001)
Jun 15, 2021 23:03:02.017699003 CEST	192.168.2.3	8.8.8.8	0x3656	Standard query (0)	pixel-sync.sitescout.com	A (IP address)	IN (0x0001)
Jun 15, 2021 23:03:18.423958063 CEST	192.168.2.3	8.8.8.8	0x4b55	Standard query (0)	ipv6.prometheusintelligencetechnology.com	A (IP address)	IN (0x0001)
Jun 15, 2021 23:03:18.469506979 CEST	192.168.2.3	8.8.8.8	0xb16e	Standard query (0)	ipv6.prometheusintelligencetechnology.com	A (IP address)	IN (0x0001)
Jun 15, 2021 23:03:35.124706984 CEST	192.168.2.3	8.8.8.8	0x54c6	Standard query (0)	unitedwaydenver.org	A (IP address)	IN (0x0001)
Jun 15, 2021 23:04:17.854528904 CEST	192.168.2.3	8.8.8.8	0xf554	Standard query (0)	ipv6.prometheusintelligencetechnology.com	A (IP address)	IN (0x0001)
Jun 15, 2021 23:04:17.950468063 CEST	192.168.2.3	8.8.8.8	0xec42	Standard query (0)	ipv6.prometheusintelligencetechnology.com	A (IP address)	IN (0x0001)
Jun 15, 2021 23:04:25.235157013 CEST	192.168.2.3	8.8.8.8	0xbe6	Standard query (0)	ipv6.prometheusintelligencetechnology.com	A (IP address)	IN (0x0001)
Jun 15, 2021 23:04:25.355730057 CEST	192.168.2.3	8.8.8.8	0xf68c	Standard query (0)	ipv6.prometheusintelligencetechnology.com	A (IP address)	IN (0x0001)
Jun 15, 2021 23:04:33.150778055 CEST	192.168.2.3	8.8.8.8	0xf7ef	Standard query (0)	ipv6.prometheusintelligencetechnology.com	A (IP address)	IN (0x0001)
Jun 15, 2021 23:04:33.206275940 CEST	192.168.2.3	8.8.8.8	0xc259	Standard query (0)	ipv6.prometheusintelligencetechnology.com	A (IP address)	IN (0x0001)
Jun 15, 2021 23:04:40.353291988 CEST	192.168.2.3	8.8.8.8	0xa8d4	Standard query (0)	ipv6.prometheusintelligencetechnology.com	A (IP address)	IN (0x0001)
Jun 15, 2021 23:04:40.453577995 CEST	192.168.2.3	8.8.8.8	0xcc95	Standard query (0)	ipv6.prometheusintelligencetechnology.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 15, 2021 23:02:56.766963005 CEST	8.8.8.8	192.168.2.3	0xd8e0	No error (0)	www.unitedwaydenver.org		172.104.26.219	A (IP address)	IN (0x0001)
Jun 15, 2021 23:02:57.139736891 CEST	8.8.8.8	192.168.2.3	0x8aed	No error (0)	unitedwaydenver.org		172.104.26.219	A (IP address)	IN (0x0001)
Jun 15, 2021 23:02:57.724215031 CEST	8.8.8.8	192.168.2.3	0x7dc4	No error (0)	use.typekit.net	use-stls.adobe.com.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Jun 15, 2021 23:02:58.161792040 CEST	8.8.8.8	192.168.2.3	0x3d9d	No error (0)	p.typekit.net	p.typekit.net-v3.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 15, 2021 23:02:59.668309927 CEST	8.8.8.8	192.168.2.3	0x12c2	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jun 15, 2021 23:02:59.668309927 CEST	8.8.8.8	192.168.2.3	0x12c2	No error (0)	stats.l.doubleclick.net		74.125.140.156	A (IP address)	IN (0x0001)
Jun 15, 2021 23:02:59.668309927 CEST	8.8.8.8	192.168.2.3	0x12c2	No error (0)	stats.l.doubleclick.net		74.125.140.154	A (IP address)	IN (0x0001)
Jun 15, 2021 23:02:59.668309927 CEST	8.8.8.8	192.168.2.3	0x12c2	No error (0)	stats.l.doubleclick.net		74.125.140.157	A (IP address)	IN (0x0001)
Jun 15, 2021 23:02:59.668309927 CEST	8.8.8.8	192.168.2.3	0x12c2	No error (0)	stats.l.doubleclick.net		74.125.140.155	A (IP address)	IN (0x0001)
Jun 15, 2021 23:03:00.802674055 CEST	8.8.8.8	192.168.2.3	0xf975	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 15, 2021 23:03:00.802674055 CEST	8.8.8.8	192.168.2.3	0xf975	No error (0)	scontent.xx.fbcdn.net		185.60.216.19	A (IP address)	IN (0x0001)
Jun 15, 2021 23:03:00.807161093 CEST	8.8.8.8	192.168.2.3	0xe87b	No error (0)	ads.pinbusinessnetwork.com	lb-3.pinbusinessnetwork.com		CNAME (Canonical name)	IN (0x0001)
Jun 15, 2021 23:03:00.807161093 CEST	8.8.8.8	192.168.2.3	0xe87b	No error (0)	lb-3.pinbusinessnetwork.com		38.97.237.86	A (IP address)	IN (0x0001)
Jun 15, 2021 23:03:00.815632105 CEST	8.8.8.8	192.168.2.3	0x3e5a	No error (0)	trackingpin.com		23.176.96.22	A (IP address)	IN (0x0001)
Jun 15, 2021 23:03:00.827275038 CEST	8.8.8.8	192.168.2.3	0xc0f2	No error (0)	cdn.callreports.com	alb01-swappy-production-272196969.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jun 15, 2021 23:03:00.827275038 CEST	8.8.8.8	192.168.2.3	0xc0f2	No error (0)	alb01-swappy-production-272196969.us-east-1.elb.amazonaws.com		54.174.92.145	A (IP address)	IN (0x0001)
Jun 15, 2021 23:03:00.827275038 CEST	8.8.8.8	192.168.2.3	0xc0f2	No error (0)	alb01-swappy-production-272196969.us-east-1.elb.amazonaws.com		52.205.51.47	A (IP address)	IN (0x0001)
Jun 15, 2021 23:03:00.827275038 CEST	8.8.8.8	192.168.2.3	0xc0f2	No error (0)	alb01-swappy-production-272196969.us-east-1.elb.amazonaws.com		52.55.38.21	A (IP address)	IN (0x0001)
Jun 15, 2021 23:03:00.856892109 CEST	8.8.8.8	192.168.2.3	0x411d	No error (0)	prometheusintelligencetechnology.com		23.176.96.6	A (IP address)	IN (0x0001)
Jun 15, 2021 23:03:00.856892109 CEST	8.8.8.8	192.168.2.3	0x411d	No error (0)	prometheusintelligencetechnology.com		23.176.96.7	A (IP address)	IN (0x0001)
Jun 15, 2021 23:03:00.873161077 CEST	8.8.8.8	192.168.2.3	0x6277	No error (0)	dsppixel.pinbn.net	wl-pixel.sitescout.com		CNAME (Canonical name)	IN (0x0001)
Jun 15, 2021 23:03:00.873161077 CEST	8.8.8.8	192.168.2.3	0x6277	No error (0)	wl-pixel.sitescout.com	pixel.sitescout.com		CNAME (Canonical name)	IN (0x0001)
Jun 15, 2021 23:03:00.873161077 CEST	8.8.8.8	192.168.2.3	0x6277	No error (0)	pixel.sitescout.com		66.155.71.150	A (IP address)	IN (0x0001)
Jun 15, 2021 23:03:00.938208103 CEST	8.8.8.8	192.168.2.3	0x3ceb	No error (0)	www.google.de		142.250.186.99	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 15, 2021 23:03:01.115233898 CEST	8.8.8.8	192.168.2.3	0x6b10	No error (0)	pixel.site scout.com		66.155.71.149	A (IP address)	IN (0x0001)
Jun 15, 2021 23:03:02.058906078 CEST	8.8.8.8	192.168.2.3	0x3656	No error (0)	pixel-sync .sitescout.com	pixel-a.sitescout.com		CNAME (Canonical name)	IN (0x0001)
Jun 15, 2021 23:03:02.058906078 CEST	8.8.8.8	192.168.2.3	0x3656	No error (0)	pixel-a.si tescout.com		66.155.71.149	A (IP address)	IN (0x0001)
Jun 15, 2021 23:03:35.157032013 CEST	8.8.8.8	192.168.2.3	0x54c6	No error (0)	unitedwayd enver.org		172.104.26.219	A (IP address)	IN (0x0001)
Jun 15, 2021 23:04:34.477323055 CEST	8.8.8.8	192.168.2.3	0x305e	No error (0)	prda.aadg. msidentity.com	www.tm.a.prd.aadg.akadn s.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- www.unitedwaydenver.org

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5828 Parent PID: 792

General

Start time:	23:02:54
Start date:	15/06/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff75f800000
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: 5640 Parent PID: 5828

General

Start time:	23:02:54
Start date:	15/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5828 CREDAT:17410 /prefetch:2
Imagebase:	0x210000
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