ID: 432894
Cookbook: browseurl.jbs
Time: 22:02:31
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

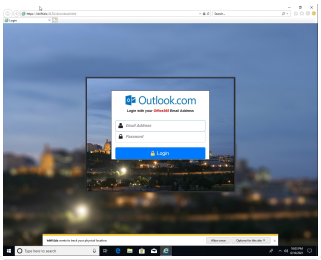
Analysis Report https://ishift.biz/ALTA/download.html

Overview

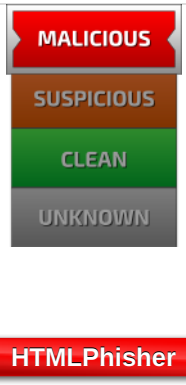
General Information

Sample URL:	http://https://ishift.biz/ALTA/download.html
Analysis ID:	432894
Infos:	

Most interesting Screenshot:



Detection



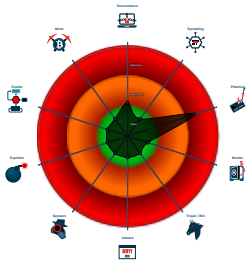
HTMLPhisher

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected HtmlPhish10
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- Suspicious form URL found

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 952 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 3160 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:952 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\download[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Phishing:

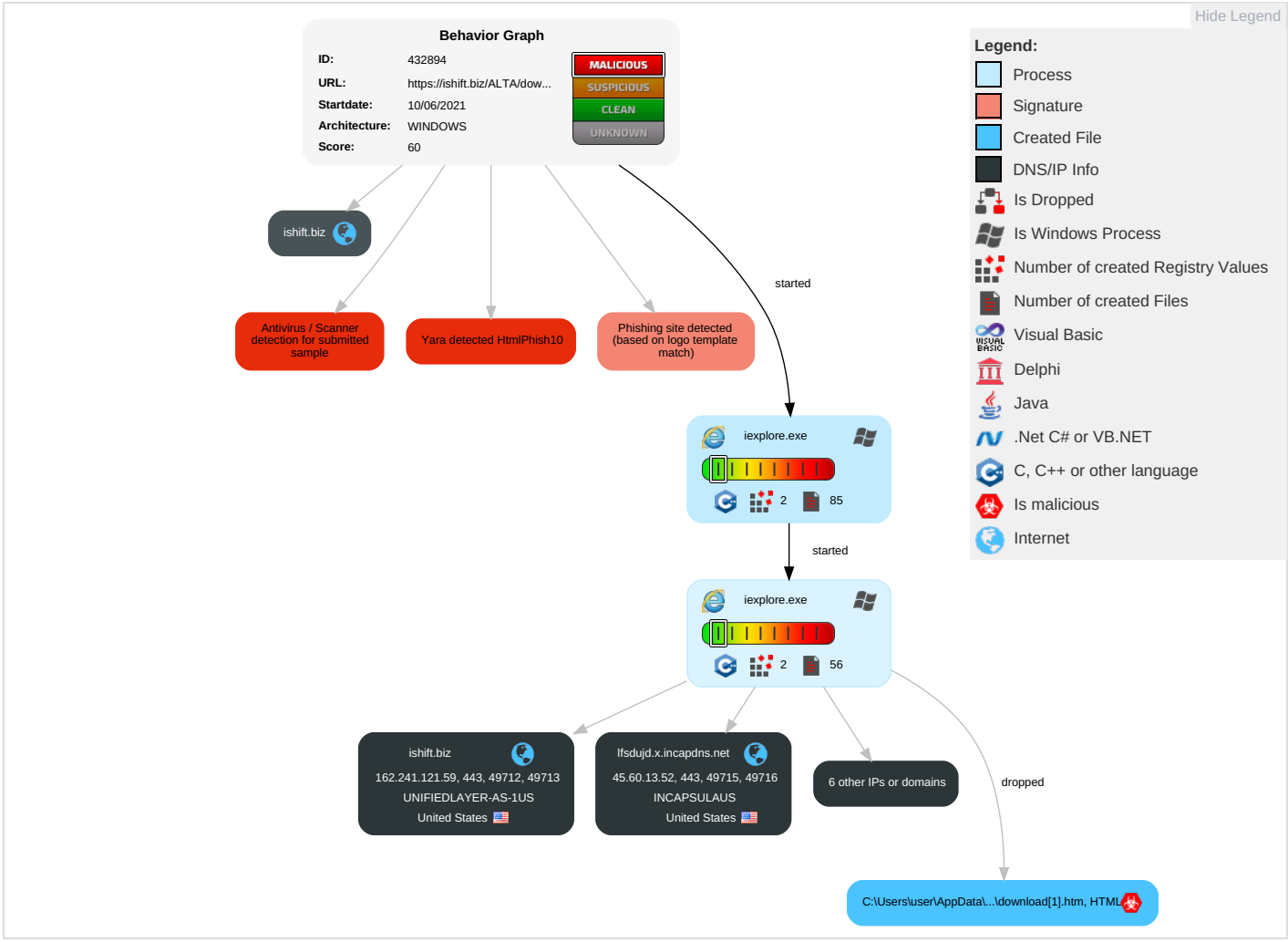
Yara detected HtmlPhish10

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impac
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partiti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lockc
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data

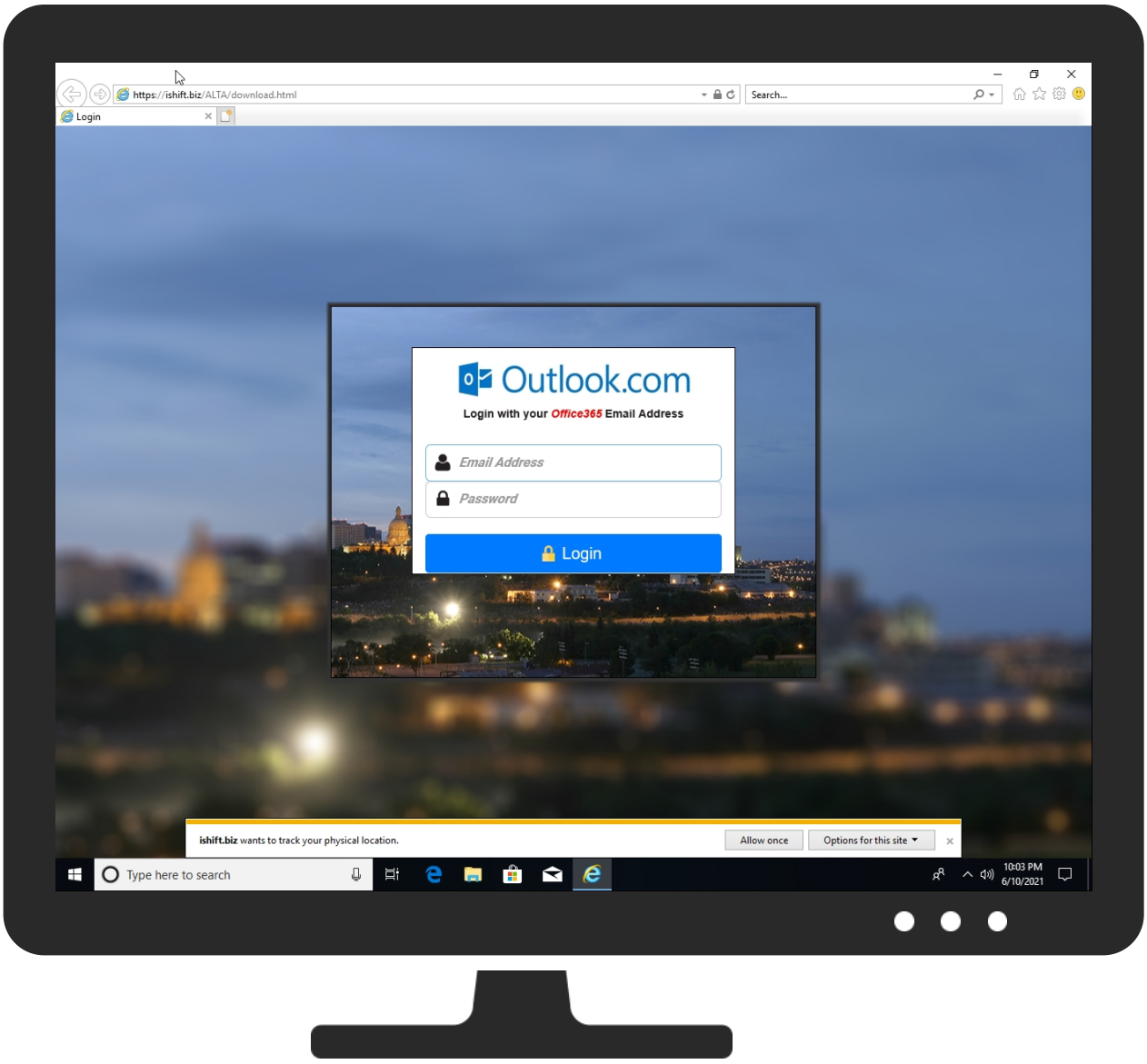
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://ishift.biz/ALTA/download.html	0%	Virustotal		Browse
http://https://ishift.biz/ALTA/download.html	0%	Avira URL Cloud	safe	
http://https://ishift.biz/ALTA/download.html	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
ishift.biz	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://ishift.biz/ALTA/download.htmll	0%	Avira URL Cloud	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://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://ishift.biz/ALTA/download.htmlRoot	0%	Avira URL Cloud	safe	
http://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ishift.biz	162.241.121.59	true	false	• 0%, Virustotal, Browse	unknown
w87gi54.x.incapdns.net	45.60.13.52	true	false		unknown
cdn2.downdetector.com	104.27.48.115	true	false		high
stats.l.doubleclick.net	74.125.140.154	true	false		high
lfsdujd.x.incapdns.net	45.60.13.52	true	false		unknown
cdn.clareitysecurity.net	unknown	unknown	false		high
collector.clareity.net	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://ishift.biz/ALTA/download.html	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
74.125.140.154	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
104.27.48.115	cdn2.downdetector.com	United States		13335	CLOUDFLARENETUS	false
45.60.13.52	w87gi54.x.incapdns.net	United States		19551	INCAPSULAUS	false
162.241.121.59	ishift.biz	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432894
Start date:	10.06.2021
Start time:	22:02:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://ishift.biz/ALTA/download.html

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:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.phis.win@3/35@6/4
Cookbook Comments:	• Adjust boot time • Enable AMSI
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\Recovery\High\Active\RecoveryStore.{54BE78B6-CA72-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8571267225488126
Encrypted:	false
SSDEEP:	96:rIZTZj2gWtNtt0Wft7UxMtXth4th1fth08X:rIZTZj2gWvtmWf1UxMZ8hfI8X

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{54BE78B6-CA72-11EB-90E4-ECF4BB862DED}.dat	
MD5:	D7A710C7243F1A8E6159C265B423445E
SHA1:	25111A5B5B5B95F2130D8547C779E3B5AF2CEF32
SHA-256:	8836ED321D9DBF3F08866336ECA9584F7E4CF1196C87C004DB7CC3A88ECFEFE0
SHA-512:	1FFD9B4EEF317EF1F3242801E994F844867BA2DFE9553F837C3A8737676EC6536E1038FC170A6136FB458BB80FE70D8605003F3535E793CE819F597A49B68BE6
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\{54BE78B8-CA72-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27416
Entropy (8bit):	1.7737304968641567
Encrypted:	false
SSDEEP:	192:rsLZCGQfH6pbkcjJ2dWnMN30/ykH/ip8zCUPmr:rgUSWOY0Mi7dM
MD5:	89FC10E2CB7AB510DA04D87C0F7AEFD3
SHA1:	B4E4EEDD2AC44792A3B39B575CB4003939D3C4A4
SHA-256:	5D09E993F655B0677598302D974EA4818CC8FCC78EA86F658598BB41DCC2246F
SHA-512:	4F361E3360A234C89446B5355BCE8D921D4CD3E38BD4A56AE8597F9D7600424634096308E2D96520F16548883952ED93A84A24DDB105C308303C152F26166233
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\{54BE78B9-CA72-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5658151371718187
Encrypted:	false
SSDEEP:	48:Iw3Gcpr2GwpafG4pQzGrapbSIGQpKuG7HpR4TGIpG:r9ZuQx6XBSwApTcA
MD5:	516049888E8B5C52F02233A26A12B82A
SHA1:	C1FCA1666768ECDB4322A6D8BF75DCC5779FFB27
SHA-256:	27BB535FF5F81F2D54FFA8BF9E857E2D4C718A9C21C16760967AF41E3F745BD9
SHA-512:	3E6D939B7C855A0AFC33B88AA497619FE5D5A9CD8AA883A544741318267B9530F167BD6FD83ED77292F8A96D7814FCFA348A70E71AC8CACB009BE78846E9995
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):	5.110636367905309
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEXiynWimI002EtM3MHdNMNxOEXiynWimI00ObVbkEtMb:2d6NxOGiySZHKd6NxOGiySZ76b
MD5:	B3B2908B4B3C0B33D5B342A3D6B1C7B9
SHA1:	3A8EB78886213E0EB3289A086827CE18854F69FA
SHA-256:	2B52D0EB60CA29D2E52B27FA62CC2A500B5107E4E824E7F418DD05544B744BBA
SHA-512:	224367F0EE5CD77443A15E74EE8A3BC5EDB44353A540996D850D43AFACDF14BD24F1025DF6D69342633D0587E7063D3FDC91F0597466A020F2AAFA8169F30B8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x2b8289ad,0x01d75e7f</date><accdate>0x2b8289ad,0x01d75e7f</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>0x2b8289ad,0x01d75e7f</date><accdate>0x2b8289ad,0x01d75e7f</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):	5.15007632750501
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kuX+XrnWimI002EtM3MHdNMNxe2kuX+XrnWimI00Obkak6EtMb:2d6Nxr0SZHKd6Nxr0SZ7Aa7b
MD5:	34295B5D315D9E4AFE5FFAA0E2C304AA
SHA1:	18A0B34E2E42A37083EF9B88F31071206815BE46
SHA-256:	7A54DEBDA454C9A5AB6BCF35A5198B1C9FC5241DCFC9ECCAA02A91B507A88810
SHA-512:	9B9AC8A9B6DAE2DE107A13D063EE689CF2E54A2347C52E878097498128089D892388CE2661A5245D3B5DC0F2B5599BC2A032E0EDE1C4446C89FA1C85770886B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x2b7b629b,0x01d75e7f</date><accdate>0x2b7b629b,0x01d75e7f</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>0x2b7b629b,0x01d75e7f</date><accdate>0x2b7b629b,0x01d75e7f</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):	5.128351843063319
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLXiynWimI002EtM3MHdNMNxvLXiynWimI00ObmZEtMb:2d6NxvDiySZHKd6NxvDiySZ7mb
MD5:	2CD29925BC10527814B1FBACE1EE2A8C
SHA1:	0325D4B84AC6C49D1C07D72A9924FE1460B582E2
SHA-256:	33C88A339688F4108973D656A10034AC14FDF9790F38DC39602E66D235252C05
SHA-512:	48B3C5B76EF6390FD3BE33EC9A8C7978CF21780BE930BFBBF2DF73136A2B0C20F63DA7EF790D6CF5C265A31CDED87480AC1D0577EC75468387408CBAB0DEB56F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x2b8289ad,0x01d75e7f</date><accdate>0x2b8289ad,0x01d75e7f</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>0x2b8289ad,0x01d75e7f</date><accdate>0x2b8289ad,0x01d75e7f</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):	5.126622095807823
Encrypted:	false
SSDEEP:	12:TMHdNMNxiXiynWimI002EtM3MHdNMNxiXiynWimI00Obd5EtMb:2d6NxYiySZHKd6NxYiySZ7Jjb
MD5:	95F5D553E1F68320C667D2E1674AD1A7
SHA1:	4EF03456B8E64D9E7B79985121EBB0BC38181890
SHA-256:	D6822DD5314C58FD278DA8A6C482C524EFBE96DCBF70929D9FCD0E5C7BCA0490
SHA-512:	0301B2FE78F621270E6B7BE220B66E7F61D108D0E363D5A048B8FB66E76C720B44751CACD1F705D170BD882FB8EAF23006AFBD285553EE6569DB41829BCBEEA4
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x2b8289ad,0x01d75e7f</date><accdate>0x2b8289ad,0x01d75e7f</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>0x2b8289ad,0x01d75e7f</date><accdate>0x2b8289ad,0x01d75e7f</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-4759708130\msapplication.xml	

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):	5.141736867454183
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwXiynWimI002EtM3MHdNMNxhGwXiynWimI00Ob8K075EtMb:2d6NxQ6iySZHKd6NxQ6iySZ7YKajb
MD5:	0C5807E7BA6D0817F64090C9639DF71A
SHA1:	FCF04E379D5CD3F8DDA8CF95051ECF93A8222B97
SHA-256:	C31E43186E888BC436BC6DB3AB7AFA15DF09B0B94B00FB3A185C9CFBFFD00550
SHA-512:	D6EBC855039CC105D6BF1698133B9E751638F21A5F23B35F5E3C886A8CF9F3AB6BD59011151362C5E929CD39E4634DC3870E8D7BC897615A0A84B4E6E5D1AF0
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x2b8289ad,0x01d75e7f</date><accdate>0x2b8289ad,0x01d75e7f</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>0x2b8289ad,0x01d75e7f</date><accdate>0x2b8289ad,0x01d75e7f</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):	5.111449820187636
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nXiynWimI002EtM3MHdNMNx0nXiynWimI00ObxEtMb:2d6Nx0XiySZHKd6Nx0XiySZ7nb
MD5:	B215EDA330C34F48769CBEA79B0FFAC7
SHA1:	71FC9DDDAAEFF42E0C655AA44EC828E181465FBB
SHA-256:	3208740FDA512E7CCBDA768DDCA005C7BCC0A5923A4368333911867680455 61E
SHA-512:	13D9A8ECF123C485EF41E8959585081D37A4A5EE034293C3576EC6F2441FABC315A23EE4F6B916431D4A46C676344AF80B3DFA0D7F2073FD58610BCD8C0CEF8
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x2b8289ad,0x01d75e7f</date><accdate>0x2b8289ad,0x01d75e7f</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>0x2b8289ad,0x01d75e7f</date><accdate>0x2b8289ad,0x01d75e7f</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\pin202591677 80\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):	5.151060069176006
Encrypted:	false
SSDEEP:	12:TMHdNMNxxXiynWimI002EtM3MHdNMNxxXiynWimI00Ob6Kq5EtMb:2d6Nx1iySZHKd6Nx1iySZ7ob
MD5:	7F42728F74E42600479EE58D1B86830C
SHA1:	73606C023254968B03A336B14BC9EC88F8C0D8BC
SHA-256:	29D4DF6D141976563F9D4A4CA9EF9CBC50D02265B8E54CC7583A7B2816703038
SHA-512:	FAE95A19CB1A1233AB8E54AD49862873E11B5579CAB92F1E816C8DD7E6C682D1F6A3CDF8ED6AECA1CBD6C1EA07E227E870A17C3386C4E195E8C138CFB4942B6F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x2b8289ad,0x01d75e7f</date><accdate>0x2b8289ad,0x01d75e7f</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>0x2b8289ad,0x01d75e7f</date><accdate>0x2b8289ad,0x01d75e7f</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):	5.13871256400149
Encrypted:	false
SSDEEP:	12:TMHdNMNxcuX+XrnWimI002EtM3MHdNMNxcuX+XrnWimI00ObVEtMb:2d6NxcSZHKd6NxcSZ7Db
MD5:	D89231E74B857B3A7413499EF7980381
SHA1:	937941EE61A201563D19D74FFD21CBEE5986D3FD
SHA-256:	03544DFF838000E44B1E188C0A83CB612A547EB6F6F7AD46C438DE3BC85376D5
SHA-512:	7B4D77BDAF5B9356C6697D9CD66451AFAC1DEEB53592BBD1A92C27E127ABB21163B273745BD5BCD220DD5C47239377FFCAB057716930B99588DA28C329FA43A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x2b7b629b,0x01d75e7f</date><accdate>0x2b7b629b,0x01d75e7f</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>0x2b7b629b,0x01d75e7f</date><accdate>0x2b7b629b,0x01d75e7f</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):	5.112143256887975
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnXiynWimI002EtM3MHdNMNxfnXiynWimI00Obe5EtMb:2d6NxPiySZHKd6NxPiySZ7ijb
MD5:	344D10CC4814CFBFC9C51AC5EE0CBCE3
SHA1:	181FA834AD87EABAF7E80A1A0253C642FC5A6C50
SHA-256:	2C6C35B8271CCF24E190C271D5C88297CC44EDA3DC26D17E5891D206E2959B37
SHA-512:	D8C48833FCD7A42FCF9DC01AAE800E03CD1B2EFC99B196B509E358E23BE29777F9D38527ADDFEBC258EA742D707B7EB9A76689D726452579B3B219EE9A75EE2E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x2b8289ad,0x01d75e7f</date><accdate>0x2b8289ad,0x01d75e7f</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>0x2b8289ad,0x01d75e7f</date><accdate>0x2b8289ad,0x01d75e7f</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\KFOlCnqEu92Fr1MmWUlfBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20396, version 1.1
Category:	downloaded
Size (bytes):	20396
Entropy (8bit):	7.974131663185347
Encrypted:	false
SSDEEP:	384:SfXdUIIA0zhyKR28ePpAwxZ5M3py8wtshtdf45DEVTGdYb7H2Q/VEgm:Svdj0zhbRmjIQ8wtsV4lEVGdY3/i/
MD5:	68D6DABFE54E245E7D5D5C16C3C4B1A9
SHA1:	7FDAB895EAEBECEDB3FB5473EAB94A1B292CEF19
SHA-256:	A01A632E56731A854F35701AA8C3A6A19A113290D9032FF9048F8064C45383BD
SHA-512:	44EB151F85178A2F9600E85AD43FAE470FABE0F247C9A03E67931B36028E600C7550D9DE2D69B3576A06577A5DEAF54822EE4BDC9DCBB47588D1972C8A959D4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmWUlfBBc-.woff
Preview:	wOFF.....O.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...Q...`u...cmap.....#cvt .....H...H+~..fpgm...$...3...._...gasp...X.....glyf...d..< ..l..C^]hdmx..H....m....03#7head..H....6...6...\hhea..I,... ...$.&..hmtx..IL.....".J.loca..K.....maxp..M.... ... .4..name..M.....~..9.post..N..... .m.dprep..N.....)*v60x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x....%Y....Wm=..mo..k.m....rl...m.g"^..../..[.}.S...\.mD...1..G>..giz...=C..}.y....|o..c.x.R.r"B.....m...../.&./6..5D.AGX.....)<'.)....?.... .Y4>|1...ES.Gc...FO.>$.../...}RCl..T.zD..uZ4~D.._OK.$.Z.(..JR...\..\..\..\.\.....*'n..6:x...b,..$...?.g:./y.iLg.3..l.0.y.g..X..V...d.#O...0....b7{..>.n.iD.V....."e.\A..OR.kwp.].....6p..."ZE..%...e.u3..L..V...W.7b..L.3.L1K...Ts..$6.-b.....9...b@..!1,...v.C....{...dox.G(...|a%E:.Fn.Nn.^n.....Sf..E)...k....<g..){....|.....DT..N....Hy.F.Jez....._?7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bootstrap.min[1].js	
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\bootstrap.min[1].js	
Category:	downloaded
Size (bytes):	35951
Entropy (8bit):	5.18015436192836
Encrypted:	false
SSDEEP:	768:b8lBD27UwlNBMl9/qahC2+jS1g8ep0skCXFXflcKGf3Z1RQ:oe78+S1Klvla3ZrQ
MD5:	8C237312864D2E4C4F03544CD4F9B195
SHA1:	253711C6D825DE55A8360552573BE950DA180614
SHA-256:	D5FD173D00D9733900834E0E1083DE86B532E048B15C0420BA5C2DB0623644B8
SHA-512:	E18A5959736A9CEEF67B40DAF7964C519C678D680BBDA8D2C7679281F5D349A286C99B96CA24E7A8E64CE987D372D74AE12DA7255C606CCFE27AC13A35B5A32
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.clareitysecurity.net/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v3.3.4 (http://getbootstrap.com). * Copyright 2011-2015 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery");+function(a){"use strict";var b=a.fn.jquery.split(" ")[0].split(".");if(b[0]<2&&b[1]<9||1==b[0]&&9==b[1]&&b[2]<1)throw new Error("Bootstrap's JavaScript requires jQuery version 1.9.1 or higher")}(jQuery),+function(a){"use strict";function b(){var a=document.createElement("bootstrap"),b={WebkitTransition:"webkitTransitionEnd",MozTransition:"transitionend",OTransition:"oTransitionEnd otransitionend",transition:"transitionend"};for(var c in b)if(void 0!==a.style[c])return{end:b[c]};return!1}a.fn.emulateTransitionEnd=function(b){var c=!1,d=this;a(this).one("bsTransitionEnd",function(){c=!0});var e=function(){c||a(d).trigger(a.support.transition.end)};return setTimeout(e,b),this},a(function(){a.support.transition=b(),a.support.transition&

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fontawesome-webfont[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), FontAwesome family
Category:	downloaded
Size (bytes):	76518
Entropy (8bit):	7.981568581630196
Encrypted:	false
SSDEEP:	1536:L09unMH4kjskxk8qYghtBzS5Q4iu8iNmVB/WBZE4NAAJRulUkqfRG3:LnnM4HXhi5ULGXAATulUhfRG3
MD5:	25A32416ABEE198DD821B0B17A198A8F
SHA1:	965CE8F688FEDBEED504EFD498BC9C1622D12362
SHA-256:	50BBE9192697E791E2EE4EF73917AEB1B03E727DFF08A1FC8D74F00E4AA812E1
SHA-512:	B580A871780ECEABE0418627EBF9557C682264947816783BEFD4A2B1F405AD5FA82582E2904AC38E35163B44C12DA84EA2825C27446457566557B4C526BB8957
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.clareitysecurity.net/fonts/fa-4.6.3/fontawesome-webfont.eot?
Preview:	.*...*.....LP.....u.....F.o.n.t.A.w.e.s.o.m.e.....R.e.g.u.l.a.r...$.V.e.r.s.i.o.n. .4...6...3. .2.0.1.6...&.F.o.n.t.A.w.e.s.o.m.e. .R.e.g.u.l.a.r.....BSGP.....)..)..Y.D.M.F..x...>.....)[..1.H..-A)F...2..i..).U.'.&a..;c..nb$':..+zAP.{u_.\;....t..r[....\C0X..'....+..=.p.'-X.Z.....H...Z..$..5.....*..V.\..2.I..WL...V=../.5x _r..S...T..N...Kg..... ....^P.Ittf..D^.X.....s.GL.wx...(..~....^....+H...K,99Xq...s.Z0I>.....T.....cA...u..1.K.Jj.T'J.....T`...,..Z@...<B..... ..(..8..cT)..b...7g.S.....AB.....a..S....|]..... ..5.R....q..+..'..X...j-S.&.....(@V..e...IZ5. PP.....:mC.z:.aM.$..:S.X.p.Pt1..).6)TqCZ..b..oTH....*..Ir.p..T".....x5../'.,.....%KT..E.)...J.2$.G..e?.....f.E.3....PF%\|.Ua..N.>e.T.7.. .3....@....BPNb^.....7$h.X..F2@...cj0.8.E.....:.....,.\..<....Z.....[....+8;...'..y5.x....N..;\oa.....i..<<<.h....."N.."m8.A.....+.7B.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\script-xkd.2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	13060
Entropy (8bit):	4.961162423903699
Encrypted:	false
SSDEEP:	192:DAEzt1oug/Ie0tnstTyhytAmoIHiCyA0fYyrAyDRHgf4SJywYJTPiQH5zbJguQFq:fZSu/gft6rpNRe4GyHfLE9M
MD5:	CE8BC4711C510E94C7D40542ED1CBEAE
SHA1:	B8CCE865F2B6AA5A95072730C8E7FED11B702124
SHA-256:	F7C087F29D01DF63F968943C63A8458D578CDA254B1D988D069756AE6A27B1B7
SHA-512:	EA04017BCC0AB4F5C1796DD01127D5391D039CA8EE8E99FCEE3E61BCA570E99E3D30567EF83174F7D89AF357DC84560B9144F874D55899956A4855ABB9A3567
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.clareitysecurity.net/js/script-xkd.2.js
Preview:	var scriptId = $('#loginscript');.var url = document.location.href;.var qaUrl = false;.var pleasewait = "Please Wait";.var disablepage = true;.var cdnUrl = "https://cdn.clareitysecurity.net";.var inputHasFocus = false;.var isValid = true;.var inputs = ".person, .lock, .pin";.var hiddenUsernameField = $("#form-clareity");.var hiddenPasswordField = $("#form-security");.var hiddenPinField = $("#form-pin");.var hasPin = false;.var hasOtp = false;.var hasCrq = false;.var login = false;.var saveUser = false;.var loginBtnId;.var warnalert = ";.var geolocationOn;.var fingerprintOn;...var ClareityTimer = {. timerID: null,. secs: 10,. onTick: null,. onEnd: null,.. initializeTimer: function (sec, onTick, onEnd) {. ClareityTimer.secs = sec + 1;. ClareityTimer.onTick = onTick;. ClareityTimer.onEnd = onEnd;. ClareityTimer.stopTheClock();. ClareityTimer.startTheTimer();. },.. stopTheClock: function() {. if (ClareityTimer.timerID) {.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\style-xkd.2[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\style-xkd.2[1].css	
Category:	downloaded
Size (bytes):	5764
Entropy (8bit):	6.051007545503987
Encrypted:	false
SSDEEP:	96:7SzE4cpZ9pMNP2R2JVmJ9pqPERTkUBN/hp1CPdakH1rSEG5SQ2bCSA+jZAZCk:mzTcpZ9pMNP2R2/m3EyTkuN/b0VfZSZN
MD5:	021E1DF61BB9805D13381529464A34B8
SHA1:	8CE8DA99588630288B762699F1E52B4211C5C892
SHA-256:	E3E343F02ABB359B929059100559BE60B2499B0183C7556D9640316B2C31DA9B
SHA-512:	79B4DACC436E5DB90CF227C9A5913F9990F4B65BF6DD93F7026B35D45CA045CDC638E33462E89E45EA806E2CE82F61F35B6D915B2C7477D34DBADEEB3F95D9D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.clareitysecurity.net/css/style-xkd.2.css
Preview:	@font-face { font-family: 'password'; font-style: normal; font-weight: 400; src: url(https://cdn.clareitysecurity.net/fonts/password.ttf);}..person{height: 46px !important;white-space: nowrap;overflow: hidden;margin-bottom: -1px;border-bottom-right-radius: 0;border-bottom-left-radius: 0;}..lock{font-family: 'password'; height: 46px !important;white-space: nowrap;overflow: hidden;border-top-left-radius: 0;border-top-right-radius: 0;}..pin{font-family: 'password'; height: 46px !important;white-space: nowrap;overflow: hidden;}..fa{position: relative;font-size: 24px}..fa-user{top: 10px;left: 12px;z-index: 9;border: 0px !important;}..fa-lock{top: 10px;left: 14px;z-index: 9;border: 0px !important;}..fa-key{top: 10px;left: 12px;z-index: 9;border: 0px !important;}..toggle-password{border: 0px !important;opacity: .6;}..form-control.empty{border:1px solid #a94442;background:#f2dede;box-shadow:0 0 0 #a94442}..form-control.empty:focus{box-shadow:0 0 3px #a94442}..fa.empty,.form-control.empty{color

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bootstrap-4.1.2.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	142041
Entropy (8bit):	5.056839531010016
Encrypted:	false
SSDEEP:	1536:T/1bwyUPAk+QYYDnDEBi82NcuSEz/ZOI/gIENM6HN26e:L1MbPN5YIENM6HN26e
MD5:	88D1B1C0FD447A75E6E60A61CA041AAE
SHA1:	5B0F9FFC6551C19931B78B109438FFBE4DD7B61B
SHA-256:	CD5525BC887734465161AF57FEAA4D63C3F5681CB477816B23B6E17D94995707
SHA-512:	7E3655F8208D87ECC6B449B38949B32A08DFFD6F7E830D0EDCC30C8AFBB49CA291DBB4FC1F9858BA0E97B315D93B9E81ED2A2DA9BB570BD3421F228B801E5EA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.clareitysecurity.net/css/bootstrap-4.1.2.min.css
Preview:	/*!. * Bootstrap v4.1.2 (https://getbootstrap.com/). * Copyright 2011-2018 The Bootstrap Authors. * Copyright 2011-2018 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e83e8c;--red:#dc3545;--orange:#fd7e14;--yellow:#ffc107;--green:#28a745;--teal:#20c997;--cyan:#17a2b8;--white:#fff;--gray:#6c757d;--gray-dark:#343a40;--primary:#007bff;--secondary:#6c757d;--success:#28a745;--info:#17a2b8;--warning:#ffc107;--danger:#dc3545;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:576px;--breakpoint-md:768px;--breakpoint-lg:992px;--breakpoint-xl:1200px;--font-family-sans-serif:-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,sans-serif,"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol";--font-family-monospace:SFMono-Regular,Menlo,Monaco,Consolas,"Liberation Mono","Courier New",monospace}*,::after,::before{box-sizing:border-box} html{font-family:san

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\font-awesome-4.6.3.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	29117
Entropy (8bit):	4.758182077430815
Encrypted:	false
SSDEEP:	384:su5yWeTUKW+KlkJ5de2UYDyVfwYUas8l8yQ/8dwwdG:3lr+Klk3Yi+fwYUf8l8yQ/eC
MD5:	9A11FBA5E34C647BBCB8F8EFE2D791CA
SHA1:	9675BB432A66AE97256734E37C099E1E6B7E0D85
SHA-256:	277F19546C365FF5A65F44FA6D7D3278A90EE38320F00D02D6386E728DF5CB42
SHA-512:	33B7DE2B3E4C4F99FC210E886D797C43B1E13A4A8D4AD0C1FC68DE909478402292455631BDF3187CF3F01DF79BB6F49AA7441742D55D46B64E4FCA939A371A5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.clareitysecurity.net/css/font-awesome-4.6.3.min.css
Preview:	/*!. * Font Awesome 4.6.3 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */@font-face{font-family:'FontAwesome';src:url('../fonts/fa-4.6.3/fontawesome-webfont.eot?v=4.6.3');src:url('../fonts/fa-4.6.3/fontawesome-webfont.eot?#iefix&v=4.6.3') format('embedded-opentype'),url('../fonts/fa-4.6.3/fontawesome-webfont.woff2?v=4.6.3') format('woff2'),url('../fonts/fa-4.6.3/fontawesome-webfont.woff?v=4.6.3') format('woff'),url('../fonts/fa-4.6.3/fontawesome-webfont.ttf?v=4.6.3') format('truetype'),url('../fonts/fa-4.6.3/fontawesome-webfont.svg?v=4.6.3#fontawesomeregular') format('svg');font-weight:normal;font-style:normal}.fa{display:inline-block;font:normal normal normal 14px/1 FontAwesome;font-size:inherit;text-rendering:auto;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}.fa-lg{font-size:1.33333333em;line-height:.75em;vertical-align:-15%}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\googletrack[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	651
Entropy (8bit):	5.280260610537334
Encrypted:	false
SSDEEP:	12:gqO1+PX73Xy3dYeRWlob6IzIwv45rPeBBAYM6Ag:RX73XyNYeRWlobjIQ49PeBBw63
MD5:	BC93BFF56601B50D782223E1226E3150
SHA1:	90EE62288A01D952A2874CCD4173868D12FF92CD
SHA-256:	00F973F96F9FCEBD037F59485A24AC1F3F073D0FB20879DDF445265C7EF77D87
SHA-512:	19EEC07DEF79DF6CA43FA9D9FEC57B05DD1C03DE741FFC2E7536B3DC641881D88235AED887F186B5039019B9AB50BA6AE61A19997850C26B77C6A941492547
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.clareitysecurity.net/sys/alberta/googletrack.js
Preview:	var mlsgooglecode = "UA-39826640-43"; // alberta.if (!mlsgooglecode){var mlsgooglecode = "UA-39826640-1";}.(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o),m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','//www.google-analytics.com/analytics.js','ga');. ga('create','UA-45101381-2','auto'); // account for all clareity login pages. ga('create', mlsgooglecode,'auto',{'name': 'newTracker'});. ga('set','forceSSL', true);. ga('send','pageview');. ga('newTracker.send','pageview');

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\login[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	assembler source, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	10321
Entropy (8bit):	5.839239930298333
Encrypted:	false
SSDEEP:	192:MDz4zGYQyyXxmEM85iMSAaRZuL7vuqR93Dpp9JA0VfZSZSBbm4ZAZCH:y8a3p3aRZu2M3NpLFZNmqBH
MD5:	134E7C6FC37EE08928A8879762F27DC0
SHA1:	F882F653C788F437DCB2C06D1C0E24D43002EE84
SHA-256:	B7E5367878F252A70A3EAECD650B0613A9BF53439C6A73FC76213FAB103BAAD9
SHA-512:	30AB31FE393DAC7BA30AAE7905F31AEE69A4E962D1FB1098DDC873565F494CDDE1F6916402BB9B73B687017D4AF7D7F4D1921BB644FBF010A7456D9864BD010 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.clareitysecurity.net/css/login.css
Preview:	body{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;margin:0;padding:0;color:#231F20;font-size:14px;font-weight:700;background:#999 url(https://cdn.clareitysecurity.net/images/linen.png)}.#loginloading{background-image:url(https://cdn.clareitysecurity.net/images/ajax.gif);width:16px;height:16px;margin:0 auto}.#disable-page-overlay{display:table;position:fixed;top:0;left:0;width:100%;height:100%}.#disable-page-overlay > div{display:table-cell;width:100%;height:100%;background:#fff;text-align:center;vertical-align:middle;color:#969696;font-size:14px;opacity:.9}.#session-dialog{display:none}.#session-dialog p.info{background-color:#FEEFB3;border-bottom:2px solid #FFD324;border-top:2px solid #FFD324;color:#9F6000;padding:5px;text-align:center;vertical-align:middle}..center{text-align:center}..center table{margin-left:auto;margin-right:auto;text-align:center}.a,a:visited{color:#2A5DB0}.a:hovor{color:#98012E}.li{list-style:none}.h1{color:#231F20;font-size:22px;text-align:center;widt

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\password[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, digitally signed, 20 tables, 1st "DSIG", 67 names, Unicode, type 1 string
Category:	downloaded
Size (bytes):	127740
Entropy (8bit):	6.037888779530314
Encrypted:	false
SSDEEP:	768:qb+KVmLhw4HZ1v+ebByRP1ZapiAGJJ+nk64x23Edi6:vjH7CRPCy
MD5:	0BF6C6D477F09BC6C4FB1C371F760B58
SHA1:	6CAF2339FB3F4CEECAE4481B8AAB0418463133AE
SHA-256:	5585D482C2EEE6ACBECA5FE3D9FFAAD32B15C5B26995EE345B0208F557571155
SHA-512:	6F7EA8FB6765D5B0D4958C60250A4AD7D5C3821A64CE7A2CC0D8799CF7490452319C4256D9DBBA35438BAE17C2C001FC91705DEFCF33623974411BF98C78074
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.clareitysecurity.net/fonts/password.ttf
Preview:	...........@DSIG$=.........\|GDEF^#]r.......GSUB.......0....JSTFm*i.........OS/2..2........VPCLT.{>C.......6cmap%.....@...*cvt .*.v..+....0fpgm.yY....l...ngasp............glyf/4.q..?$...4head.\.t...L...6hhea...........$hmtx*...... ....kern7a96..^X...`loca.`U...2.....maxp...<....... name.q.J..s.....post........A.prepR..... ...._.<...........'*......L.W......................>.N.C...W.X......................................./.V.......................3.......3.....f................z.............Mono.@. .....Q.3.>..@..................9...9.....W

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\ALTA[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	1135
Entropy (8bit):	4.931847808514373
Encrypted:	false
SSDEEP:	24:WluxlUnxeWZyoft9el9xmGJEJ9xmUw+N9xmymn69xmwnxnzQ1CO5g:qSoeWQolGmGJEBmUw+1mymn+mgFzQUgg
MD5:	DA8556A286B763705B9EC5446CD08087
SHA1:	782BEA47324771E6E43CD50C859E1E7D32FA34D9
SHA-256:	0EC1FEA1E62678B5BDE4BC257DE9623F0914EFC9C919A1C1476BCB39EB073E2A
SHA-512:	52F2BBCCEA311D26ABAE9E50F1B1A64AEEAB468DB88267E5A230301EC2C366A5B9E6604DB743E632B3D9DDD3B563027B698B67BE6D2B6C6232656D62F04307BC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ishift.biz/ALTA/
Preview:	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"><html>. <head>. <title>Index of /ALTA</title>. </head>. <body>. Index of /ALTA . <table>. <tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size</th><th>Description</th></tr>. <tr><th colspan="5"><hr></th></tr>.<tr><td valign="top"> </td><td>Parent Directory </td><td> </td><td align="right"> - </td><td> </td></tr>.<tr><td valign="top"> </td><td>IN.php </td><td align="right">2021-06-10 13:02 </td><td align="right">536 </td><td> </td></tr>.<tr><td valign="top"> </td><td>download.html </td><td align="right">2021-05-31 00:16 </td><td align="right"> 20K</td><td> </td></tr>.<tr><td valign="top"> </td><td>failedpass.php </td><td align="right

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\analytics[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	49153
Entropy (8bit):	5.520906949461031
Encrypted:	false
SSDEEP:	768:/yR3fYFBLbfs5sP5XqY3TyPnHpl1WY3SoavFVv6PU+CgYUD0lgEw0stZM:/y9gZfl5h3UHpaY3SoRCw0sk
MD5:	6DF1787C4BE82D1BB24F8BFFA10C7738
SHA1:	3634E839429E462E49C5F42B75FBFB4BA318AF6D
SHA-256:	2CB09C7B3E19BFC41743CA3624EF81C3258D56525647FEAC76AA757E0292627A
SHA-512:	CB3CE2BCEB61F390298C21E470423CCEB6DD93E648A7DD0467195B11FEF30BF7A086DFF47C4494E2533498D1448C1A22AAB1414C14FD73278F1C92E0F7BC3F54
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google-analytics.com/analytics.js
Preview:	(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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\jquery-3.3.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	86927
Entropy (8bit):	5.289226719276158
Encrypted:	false
SSDEEP:	1536:jLiBdiaWLOczCmZx6+VWuGzQNOzdn6x2RZd9SEnk9HB96c9Yo/NWLbVj3kC6t3:5kn6x2xe9NK6nC69
MD5:	A09E13EE94D51C524B7E2A728C7D4039
SHA1:	0DC32DB4AA9C5F03F3B38C47D883DBD4FED13AAE
SHA-256:	160A426FF2894252CD7CEBBDD6D6B7DA8FCD319C65B70468F10B6690C45D02EF
SHA-512:	F8DA8F95B6ED33542A88AF19028E18AE3D9CE25350A06BFC3FBF433ED2B38FEFA5E639CDDFDAC703FC6CAA7F3313D974B92A3168276B3A016CEB28F27DB071 4A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.clareitysecurity.net/js/jquery-3.3.1.min.js
Preview:	/*! jQuery v3.3.1 | (c) JS Foundation and other contributors | jquery.org/license */!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery requires a window with a document");return t(e)}:t(e)}("undefined"!=typeof window?window:this,function(e,t){"use strict";var n=[],r=e.document,i=Object.getPrototypeOf,o=n.slice,a=n.concat,s=n.push,u=n.indexOf,l={},c=l.toString,f=l.hasOwnProperty,p=f.toString,d=p.call(Object),h={},g=function e(t){return"function"==typeof t&&"number"!=typeof t.nodeType},y=function e(t){return null!=t&&t===t.window},v={type:!0,src:!0,noModule:!0};function m(e,t,n){var i,o=(t=t||r).createElement("script");if(o.text=e,n)for(i in v)n[i]&&(o[i]=n[i]);t.head.appendChild(o).parentNode.removeChild(o)}function x(e){return null==e?e+"":"object"==typeof e||"function"==typeof e?l[c.call(e)]||"object":typeof e}var b="3.3.1",w=function(e,t){return new w.fn.init(e,t)},

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\outlook-com-logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 587 x 115, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	42786
Entropy (8bit):	**7.990640331740395**
Encrypted:	**true**
SSDEEP:	768:yi7TCdcdq5gPX1y9GMisSpOvSi2UDeinV6nDcxvGhJbn9:PCdcdZPly0MiFpOvt2UdnVEAGhJJ
MD5:	978EB8B36E0AD90E4AE655C656A502C2
SHA1:	787292EAB93C8F7F0619E39FE246C35A5A39F4E2
SHA-256:	46D011C7A7CFF18C5F4E7C1E005A9BA400A0CE2AF701597150F3AB91A462A5F8
SHA-512:	6C74EF1805EA42A9EF077D93A3AEA3B7C32512B6BD9EAD116F2615A1AC9F5B276A3EFDCAD3CA00F7F60F4409C98550CB4A3B6F93FD3DF03FF5AE4C87A17E97 9F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.downdetector.com/static/uploads/logo/outlook-com-logo.png
Preview:	.PNG.....IHDR...K...s.....F.....gAMA....7.....tEXtSoftware.Adobe ImageReadyq.e<....IDATx..W.\W.&.].:"3#.@f".5A.".HV.....c=366+.V..}.}..U6f=f;.=.l..K5..j.Z..H.Uhu.s#3....Q...H...H....P. @D.E.QD.E.QD.&5...".(..".(...,E.QD.E.QD.E`)..".(..".(.K.E.QD.E.QD.X.(..".(..".RD.E.QD.E.Q..^.....k..I..._.R.(..".(...E.7..."..".(..".(./.!.P.R.BkQ...MsD.E.QD.E.....1.. .mD.E.QD.E.....L..._.u...MA6..E.QD.E.QD.t...S..x.....0E.QD.E.QD.... ..W._..sD.....+]E....}V.@..7.....`.(..".(.....N.5.d.h.6..U=..+(..h4.L.[X^^.J.8:.G.[.A`)..".(..".....,...Ax..>;[._ ....~C~.-.H..@...o.....M.J5T.M...R....6..t....AJ...D....dh.MG...T.....R...\2..".}.K...3g....&4d.4T..m`u.....,.c}..J.E@...h...G.{.;..Aa<dh..F..ol.O..@.. J...E.&....-..%..^..Tu....=..6.=... ...Ut.&.i.B..././b.-...!.j..ni...6E....*..f.^..v=.n.F.e.}4xto..b...~..UU.{uxA.&.W..h....?3..C.=.B..W$....V.U#.....i.....G.*M.....{ ....!oM2.5t...Q....d-#..".:.R.L.F..-,...u.....B;..O.,... _.4]..+X_..Vq....R..<OA.q.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\KFOlCnqEu92Fr1MmSU5fBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20404, version 1.1
Category:	downloaded
Size (bytes):	20404
Entropy (8bit):	7.970248785137973
Encrypted:	false
SSDEEP:	384:8uFoOxqigBacqKz8RGLv6K5a+jZ/rFSyeM5B8r/WjRy0BsM16t/PJ:PFlIvUKz8R+t5N53eGar/gY0Bv6tp
MD5:	BF0F407102FAF3A0B521D3B545F547A5
SHA1:	CA357CD0DE5DD0242E8EFACFB8D24AB60FDC86AB
SHA-256:	855A06974032BB69157D469ABA6F63440E8BE47C421F45C3F396F4E0B87B6DE8
SHA-512:	85359028F7FE49B1DF90B72E48DC7DE4B21F1B65E8BF109595705A3F4EAF9FA79854B5AEF060FE266291C5ECE9D04FCEAD1DE09BAA2C5E20601E1579212520C 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmSU5fBBc-.woff
Preview:	wOFF.....O.....x.....GDEF.....G...d....GPOS.....!GSUB.....OS/2...L...P...`t6..cmap.....#cvt .....X...X/...fpgm.....4.....".gasp...@.....glyf.. .L..<'..m..]5Yhdmx..Ht...m....),..head..H....6...6.Y.ihhea..I.... ...$....hmtx..I<.....Dd.loca..K.....maxp..M.... ... .4.\name..M.....\|..9.post..N..... .m.dprep..N.....:z /.Wx...1..P.....PB..U.=\|.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x...\|\..F..3...N..q)..a\|.....^..33..c.....p"y.iT....<Gg...!.3...T1...{.g0.u.y.....m.\|.k..NF.....mox.;...7&.Y.. C.R_[.T.c..-.=...9:...a*j.G.....O.Q".6...>...(?...~...._.2:..K4....S%...jbr).....*....e.U..-..X.3.ILQ....z..!.f:...<.W.#...e.c=...&6...lc;;..3<.s<....H.i2..N..t..)Ns...#`..").[...._..T..T... ..+\|..=..O.....Z..F...r..eM.f.Y.....-...r.\.s6.r..,...:.<$..#.l..F.$.2#.e..].[.....yR...e.|{..O..`)..U.0.e.50.Z.b../cM..i.&O._..+.Y.W...;z....j.p._.o..[CL.)n'.UGx..>).X..MJ..Fr..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	533
Entropy (8bit):	5.101982741986593
Encrypted:	false
SSDEEP:	12:jF/iO6ZN6pixsiJqF/iO6ZRoT6pixUEqF/iO6ZN76pixQvJY:5/iOYNNxsl/iOYsNxUv/iOYN7Nxn
MD5:	72DA71EACAE9E595F0429770C533F3E7
SHA1:	A4BB90C015F7C573F2B989490E1362412B9194AA
SHA-256:	00F13F954125777E8A26FD0E9F6BC730D763E9E59DCFB54D240602665B9B1B43
SHA-512:	EFD365A575C5DB8B1E225BB82B964DC3FC3D8FB1B8A4102160226662011363O5E06AFD8FC7FA95CCD4DE5EC3953A32677C7381323FA5C6E8E3BB74F974119E9
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmSU5fBBc-.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOmCnqEu92Fr1Mu4mxM.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmWUlfBBc-.woff) format('woff');.}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\download[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	20156
Entropy (8bit):	5.180150476815419
Encrypted:	false
SSDEEP:	384:AwqgqI/bF7B6BMyeT6ujvagei3nMtFitFCAZtFwtFNZptFwtF4UlkRPEWomSf6ZF:zqgqI/bF7B2MyYQihV8Nr8HuRPEWUf63
MD5:	48B573ECD3BD0C5542F41E04E227A8C3
SHA1:	A42C08149BA98A68D07F892287D094845A2AD643
SHA-256:	9B55076EA627C0DB732379566A40673192884E8DF62F25A7EDB1EA4B7EDF5FD2
SHA-512:	8C96E7F3454B1A825D0C77F91445A0916363181201078B6C866BAC0781898D585944662998467F033DDC3D0F62538730D36666CF8097AB7D831AEC9B8AE2E2369
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\download[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://ishift.biz/ALTA/download.html
Preview:	<!DOCTYPE html>..<html lang="en".. xmlns:db="http://www.w3.org/1999/xhtml">..<head>.. <meta charset="utf-8">.. <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">.. <title>Login</title>.. <link id="fontawesome" rel="stylesheet" type="text/css" href="https://cdn.clareitysecurity.net/css/font-awesome-4.6.3.min.css">.. <link id="favicon" rel="icon" type="image/png" href="" sizes="32x32" />.. <link id="bootstrapcss" href="https://cdn.clareitysecurity.net/css/bootstrap-4.1.2.min.css" rel="stylesheet">.. <link id="googlefont" href="https://fonts.googleapis.com/css?family=Roboto:300,400,700" rel="stylesheet">.. <link id="logincss" rel="stylesheet" href="https://cdn.clareitysecurity.net/css/login.css" />.. <style>.. body{background: url(https://cdn.clareitysecurity.net/sys/alberta/paragon-login-background.png) no-repeat center center fixed;-webkit-background-size: cover; -moz-background-size: cover; -o-background-size: cover; background

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\paragon-login-background[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 2100 x 1612, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	881145
Entropy (8bit):	**7.995109411730639**
Encrypted:	**true**
SSDEEP:	24576:Pl9IMZGUli6TBpHcgJXVdYQ8d2Pr4vtIdlkCqJ5o9aqrqdA/5:wYD56TPNYfMT4+CyGaUqWR
MD5:	0403121CD2F853E130A560A346087AAD
SHA1:	B5B6EA9FF01762D96C585295B32E78828DD07FA0
SHA-256:	17CECC18EE875908251A0AB107CC1EC9DD5FE73AF2B759CAA69316F5793C85B9
SHA-512:	3AC61060BD1C9E0DDB3C9DC87F45A9F9D670D00B6A55314627269DED91C1E4406D03768548E3DA269818B60E70BE0DDAEB43D4D1241F384CC1149BCD7DC1F2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.clareitysecurity.net/sys/alberta/paragon-login-background.png
Preview:	.PNG.....IHDR...4...L.....tx.o....tEXtSoftware.Adobe ImageReadyq.e<...(iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c067 79.157747, 2015/03/30-23:40:42 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC 2015 (Macintosh)" xmpMM:InstanceID="xmp.iid:7047D46F3DEC11E585DEA5BC37E09E30" xmpMM:DocumentID="xmp.did:7047D4703DEC11E585DEA5BC37E09E30"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:7047D46D3DEC11E585DEA5BC37E09E30" stRef:documentID="xmp.did:7047D46E3DEC11E585DEA5BC37E09E30"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>y\.B..ngIDATx..}.r..$.,.?G...q|.U..L2...L..f.+.... .8.....?p.....{.....1....3.[.....a..#..a{.H;_..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\paragon-login-bg[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 600 x 461, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	404857
Entropy (8bit):	**7.994859446686798**
Encrypted:	**true**
SSDEEP:	12288:drd1qy0ZDWfah3iO2TQehqjW2JnZcVGd5C6nm1a:RjqpsfahIhqjWCnZgWg1a
MD5:	1EEBB4FFEA2A4B3B8DAF810FC728FDF3
SHA1:	4A225532CF25483FA24F1E532FFDC33A0769EDC1
SHA-256:	1DCAB816CA5EE2317F01C1822391BCF8D8F9FDFAA3E5D776592D6C3CE6E559AF
SHA-512:	FD0100FFF46B971490A6EAC8ECF43164A4CA7A36BB72D05A5BE696176B0EACD047ADBBF2EA87F209BC71B0DFC029CCAD8B08A9FAAAC02978C42377482F2943 9B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.clareitysecurity.net/sys/alberta/paragon-login-bg.png
Preview:	.PNG.....IHDR...X.....%.....gAMA.....a.... cHRM..z&.....u0...`.:....p..Q<....bKGD.....C.....pHYs.....~.....IDATx...m=.....a...y.^... ..e1.RJyy..}.....,R.l.....8... G\..3..3.|....q...p.....x.9.{c.Z3,3...ox..=.....O....`c.a.]..n.....=.d...f.....Z..../.....8.....o.....s..].c.`...{./=..G.`.d....,.....EI.....c.....`...6.F..y..r|...]f+..cT.>/.....N.....<.. ....89..Yh..g.m.[u...;...'-..)G.....,g.-...3.v.c..1.1..m0.?...\5.3...w=.....5..g.....`.JZ86.3.>S.jN...]s..{.U.w/..R....^s...[..y.z.k..l.Wb.i./..R...l7r...`.....;e..J_R.b=P[.....5...^.m.F.v..B.(..C. %?..=...x."....L.t...,....,.....q.....e-e(,..5.*/.c....K.?k..J9.u,..y.u?B.o...0..N...}l+T..K.).5V.r.V.....a;t.L.....S.9.;ol{..v...w.....-.O.j..X..'...5`.c...v.....k....~.?.a.mY...OtZ..'eb.... ....Z...M..W.....6...../.B.e.kv.l..pB...,...^*.O7.`+.#..2.c. &...?1Q.9`?9..0:...<.Xc.....e}..Z.I..>.....-lip.T.k.0.{?..

C:\Users\user\AppData\Local\Temp\~DF35CFB899C4618C4B.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	35177
Entropy (8bit):	0.46985885107590575
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+zN/2SISxmcQzniW8znP0w8znOznozn7znq0xSR:kBqoxKAuvScS+zN/2dV/ip8zCUPrUR
MD5:	E4A1B620F7C48D5A555A3B6109AB9FC5
SHA1:	C9C66A615345989BE6365CC4986CE47E20A0718B
SHA-256:	7E029D37AFCA1F8562B6B4A746D450FD9E3BAD66822D4C81B262FC617DD563BD
SHA-512:	B573ADD9A2C131D441D25AB6470FBD28A9BE7B5D9671BBC110A4ED7502347B66A197DEEF1036E8E945AE41C850D9DE86E8994ECED52768FA500D336275959B 4
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFD05493EFF0DF9AEE.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFE2C3B5B1199B26B2.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029

C:\Users\user\AppData\Local\Temp\~DFE2C3B5B1199B26B2.TMP	
Entropy (8bit):	0.4805489731351307
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9locrF9locR9lWc3F/+hNC3F/+f5/+fZfNTC3Te:kBqoID1NhkkYhfwi
MD5:	EFB8F1F957B361E62376B5DC1B744665
SHA1:	F4307F6C98A65FB76E31E5248D72EC1578933368
SHA-256:	DE9EE1EB5FB07B5E7D6A945B6C9D3B33244CED12D51B89CC290CFF7C78B5ECA3
SHA-512:	67C27435845AEC2E89D54E5F1A95976FE84417AF1DE6390763E4C6E6AF5BB72C17A8BAEC9CEEEA53A2546F4B06F0D4AACB1FCD75FF5D114DDF069EF37DBD68A
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 22:03:19.071687937 CEST	192.168.2.3	8.8.8.8	0xda1	Standard query (0)	ishift.biz	A (IP address)	IN (0x0001)
Jun 10, 2021 22:03:19.806718111 CEST	192.168.2.3	8.8.8.8	0x3f11	Standard query (0)	cdn.clareitysecurity.net	A (IP address)	IN (0x0001)
Jun 10, 2021 22:03:19.920757055 CEST	192.168.2.3	8.8.8.8	0x3d2b	Standard query (0)	cdn2.downdetector.com	A (IP address)	IN (0x0001)
Jun 10, 2021 22:03:21.210427999 CEST	192.168.2.3	8.8.8.8	0x72b3	Standard query (0)	collector.clareity.net	A (IP address)	IN (0x0001)
Jun 10, 2021 22:03:21.574378967 CEST	192.168.2.3	8.8.8.8	0x8052	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jun 10, 2021 22:03:35.254133940 CEST	192.168.2.3	8.8.8.8	0x98a1	Standard query (0)	ishift.biz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 22:03:19.143357038 CEST	8.8.8.8	192.168.2.3	0xda1	No error (0)	ishift.biz		162.241.121.59	A (IP address)	IN (0x0001)
Jun 10, 2021 22:03:19.867199898 CEST	8.8.8.8	192.168.2.3	0x3f11	No error (0)	cdn.clareitysecurity.net	lfsdujd.x.incapdns.net		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 22:03:19.867199898 CEST	8.8.8.8	192.168.2.3	0x3f11	No error (0)	lfsdujd.x.incapdns.net		45.60.13.52	A (IP address)	IN (0x0001)
Jun 10, 2021 22:03:19.983336926 CEST	8.8.8.8	192.168.2.3	0x3d2b	No error (0)	cdn2.downdetector.com		104.27.48.115	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 22:03:19.983336926 CEST	8.8.8.8	192.168.2.3	0x3d2b	No error (0)	cdn2.downdetector.com		104.27.49.115	A (IP address)	IN (0x0001)
Jun 10, 2021 22:03:21.419161081 CEST	8.8.8.8	192.168.2.3	0x72b3	No error (0)	collector.clareity.net	w87gi54.x.incapdns.net		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 22:03:21.419161081 CEST	8.8.8.8	192.168.2.3	0x72b3	No error (0)	w87gi54.x.incapdns.net		45.60.13.52	A (IP address)	IN (0x0001)
Jun 10, 2021 22:03:21.633249044 CEST	8.8.8.8	192.168.2.3	0x8052	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 22:03:21.633249044 CEST	8.8.8.8	192.168.2.3	0x8052	No error (0)	stats.l.doubleclick.net		74.125.140.154	A (IP address)	IN (0x0001)
Jun 10, 2021 22:03:21.633249044 CEST	8.8.8.8	192.168.2.3	0x8052	No error (0)	stats.l.doubleclick.net		74.125.140.157	A (IP address)	IN (0x0001)
Jun 10, 2021 22:03:21.633249044 CEST	8.8.8.8	192.168.2.3	0x8052	No error (0)	stats.l.doubleclick.net		74.125.140.155	A (IP address)	IN (0x0001)
Jun 10, 2021 22:03:21.633249044 CEST	8.8.8.8	192.168.2.3	0x8052	No error (0)	stats.l.doubleclick.net		74.125.140.156	A (IP address)	IN (0x0001)
Jun 10, 2021 22:03:35.315823078 CEST	8.8.8.8	192.168.2.3	0x98a1	No error (0)	ishift.biz		162.241.121.59	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 10, 2021 22:03:19.496541023 CEST	162.241.121.59	443	192.168.2.3	49713	CN=ishift.biz CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Jun 09 02:00:00 CEST 2021	Wed Sep 08 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jun 10, 2021 22:03:19.497155905 CEST	162.241.121.59	443	192.168.2.3	49712	CN=ishift.biz CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Jun 09 02:00:00 CEST 2021	Wed Sep 08 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jun 10, 2021 22:03:20.006000042 CEST	45.60.13.52	443	192.168.2.3	49716	CN=cdn.clareitysecurity.net, O="CoreLogic, Inc.", L=Irvine, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Mar 31 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Tue Apr 05 14:00:00 CEST 2022 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jun 10, 2021 22:03:20.006489992 CEST	45.60.13.52	443	192.168.2.3	49717	CN=cdn.clareitysecurity.net, O="CoreLogic, Inc.", L=Irvine, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Mar 31 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Tue Apr 05 14:00:00 CEST 2022 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jun 10, 2021 22:03:20.007707119 CEST	45.60.13.52	443	192.168.2.3	49715	CN=cdn.clareitysecurity.net, O="CoreLogic, Inc.", L=Irvine, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Mar 31 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Tue Apr 05 14:00:00 CEST 2022 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jun 10, 2021 22:03:20.007829905 CEST	45.60.13.52	443	192.168.2.3	49718	CN=cdn.clareitysecurity.net, O="CoreLogic, Inc.", L=Irvine, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Mar 31 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Tue Apr 05 14:00:00 CEST 2022 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jun 10, 2021 22:03:20.029036999 CEST	45.60.13.52	443	192.168.2.3	49720	CN=cdn.clareitysecurity.net, O="CoreLogic, Inc.", L=Irvine, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Mar 31 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Tue Apr 05 14:00:00 CEST 2022 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 10, 2021 22:03:20.030994892 CEST	45.60.13.52	443	192.168.2.3	49719	CN=cdn.clareitysecurity.net, O="CoreLogic, Inc.", L=Irvine, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Mar 31 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Tue Apr 05 14:00:00 CEST 2022 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jun 10, 2021 22:03:20.238087893 CEST	104.27.48.115	443	192.168.2.3	49723	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 03 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Tue Aug 03 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jun 10, 2021 22:03:20.277014017 CEST	104.27.48.115	443	192.168.2.3	49724	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 03 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Tue Aug 03 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jun 10, 2021 22:03:21.521437883 CEST	45.60.13.52	443	192.168.2.3	49731	CN=*.clareity.net, O="CoreLogic, Inc.", L=Irvine, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jan 06 01:00:00 CET 2020 Tue Oct 22 14:00:00 CEST 2013	Mon Jan 10 13:00:00 CET 2022 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jun 10, 2021 22:03:21.537775040 CEST	45.60.13.52	443	192.168.2.3	49730	CN=*.clareity.net, O="CoreLogic, Inc.", L=Irvine, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jan 06 01:00:00 CET 2020 Tue Oct 22 14:00:00 CEST 2013	Mon Jan 10 13:00:00 CET 2022 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 10, 2021 22:03:21.754281044 CEST	74.125.140.154	443	192.168.2.3	49733	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Mon May 17 03:34:10 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 09 03:34:09 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jun 10, 2021 22:03:21.754666090 CEST	74.125.140.154	443	192.168.2.3	49732	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Mon May 17 03:34:10 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 09 03:34:09 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jun 10, 2021 22:03:35.658509970 CEST	162.241.121.59	443	192.168.2.3	49743	CN=ishift.biz CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Jun 09 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Wed Sep 08 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 952 Parent PID: 792

General

Start time:	22:03:16
Start date:	10/06/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff67e160000
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: 3160 Parent PID: 952

General

Start time:	22:03:17
Start date:	10/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:952 CREDAT:17410 /prefetch:2
Imagebase:	0x1220000
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