ID: 431204
Cookbook: browseurl.jbs
Time: 15:17:53
Date: 08/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

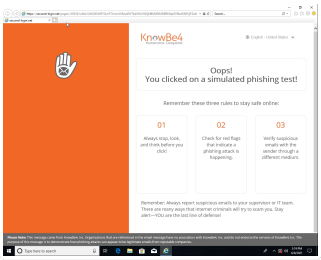
Analysis Report https://covid19.protected-forms.com/X...

Overview

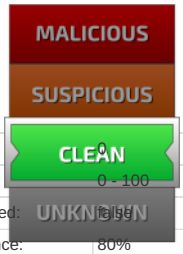
General Information

Sample URL:	https://covid19.protected-forms.com/XWkZKNVRYQmFTVmxrVkRoek9VTkdXRzVHWjNBM2...aejA5LS0yNjI0MmEyNmU5MTE4NzY5Nzk4YzQ5Nzk4MGQyMGYxNmNiYmE1MGQy?cid=874637403
Analysis ID:	431204
Infos:	

Most interesting Screenshot:



Detection

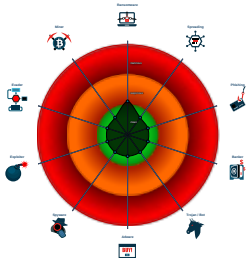


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 5852 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6000 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5852 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

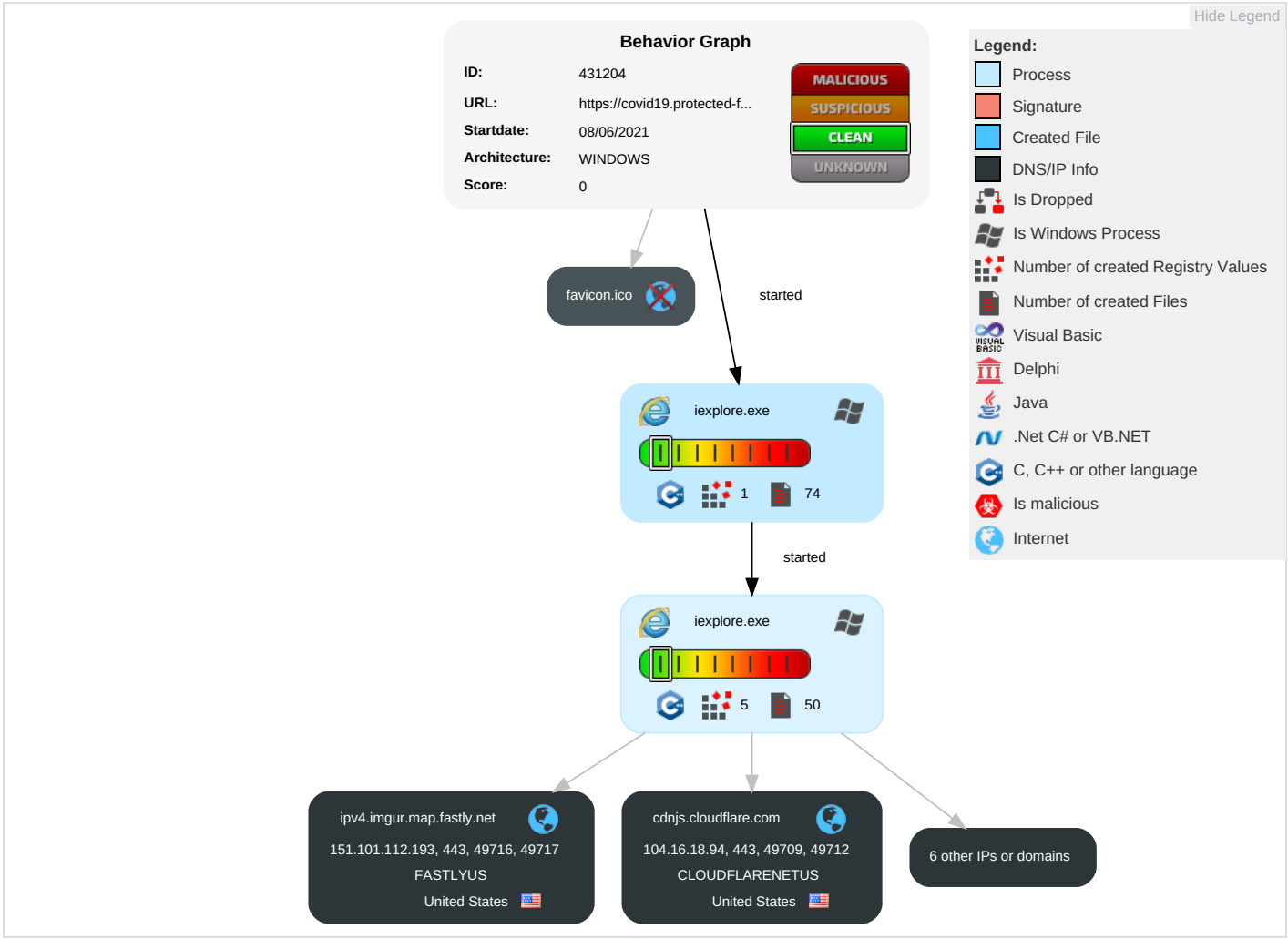
Click to jump to signature section

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

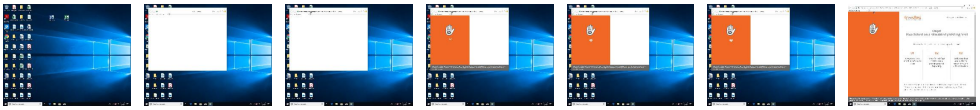
Behavior Graph

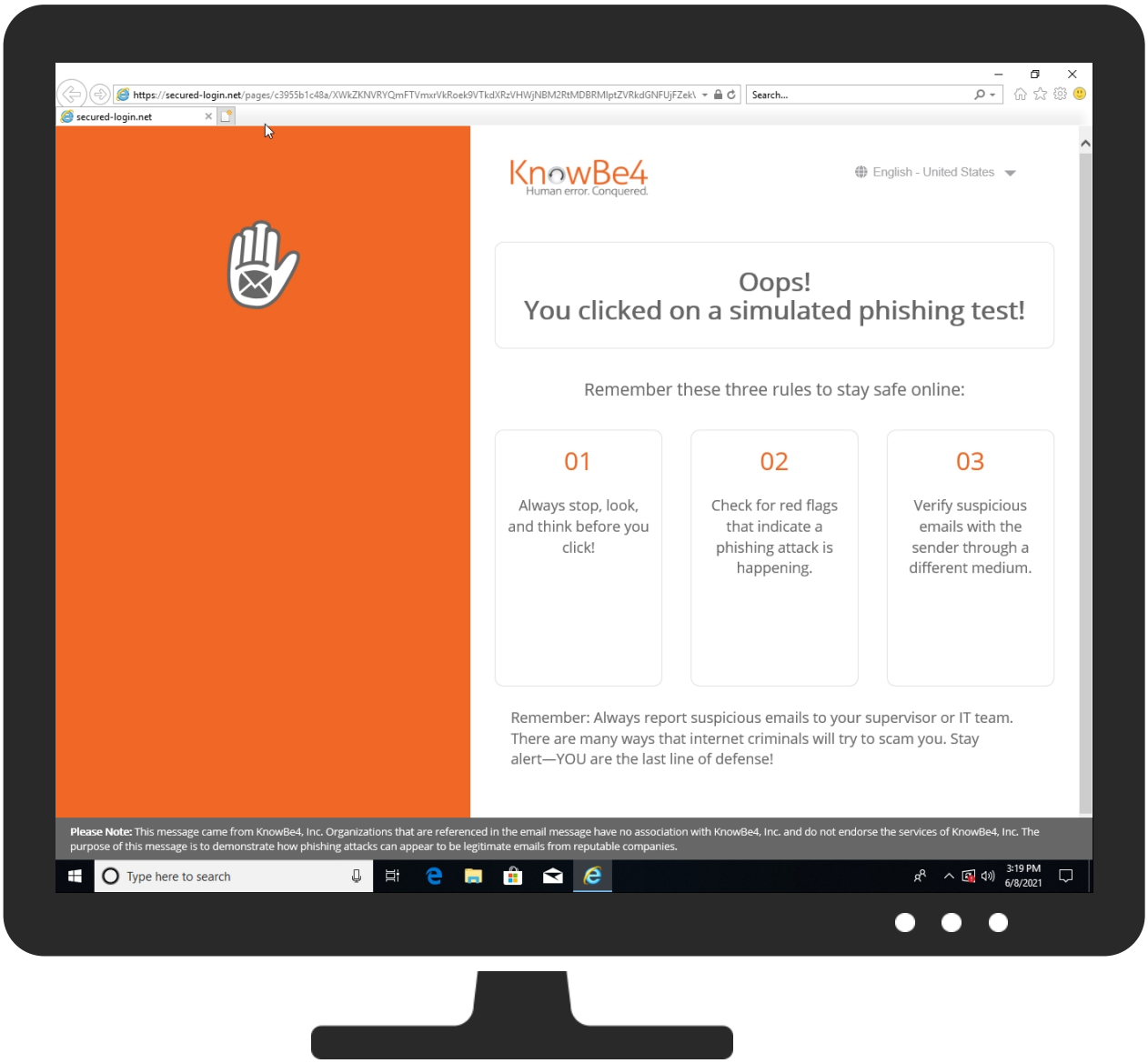


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://covid19.protected-forms.com/XWkZKNVRYQmFTVmxrVkRoek9VTkdXRzVHWjNBM2RtMDBRMlptZVRkdGNFUjFZekV6ZWxkblJEZzFiMlZCTWxoTlVXaG5aMHRoYW1kc09VSnlja2xZYkc5MlYwdzNOWFpsVERWNUsxWXZiVkJ5YURreFUzTk9kbGt4ZWtoSGRYa3dTM1ppY1hkT0x6Y3pSMFJXVjNsMWRXNVRiRnBCZURZMGJVWkNlRlJ0TVdGM1REZEhNRnA0ZW5keksyTmFZV2hPWVRGd1Z6Tm9iRFVyVlhnd1UwdHhOVkU0YTJsRGRXMDBjMlZOUFMwdGVsSnhlVlJOWkZKRlNIVjZZbEpUYkVscGJUQTJaejA5LS0yNjI0MmEyNmU5MTE4NzY5Nzk4YzQ5Nzk4MGQyMGYxNmNiYmE1MGQy?cid=874637403	0%	Virustotal		Browse
http://https://covid19.protected-forms.com/XWkZKNVRYQmFTVmxrVkRoek9VTkdXRzVHWjNBM2RtMDBRMlptZVRkdGNFUjFZekV6ZWxkblJEZzFiMlZCTWxoTlVXaG5aMHRoYW1kc09VSnlja2xZYkc5MlYwdzNOWFpsVERWNUsxWXZiVkJ5YURreFUzTk9kbGt4ZWtoSGRYa3dTM1ppY1hkT0x6Y3pTMFJXVjNsMWRXNVRiRnBCZURZMGJVWkNlRlJ0TVdGM1REZEhNRnA0ZW5keksyTmFZV2hPWVRGd1Z6Tm9iRFVyVlhnd1UwdHhOVkU0YTJsRGRXMDBjMlZOUFMwdGVsSnhlVlJOWkZKRlNIVjZZbEpUYkVscGJUQTJaejA5LS0yNjI0MmEyNmU5MTE4NzY5Nzk4YzQ5Nzk4MGQyMGYxNmNiYmE1MGQy?cid=874637403	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://covid19.protected-forms.com/XWkZKNVRYQmFTVmxrVkRoek9VTkdXRzVHWjNBM2RtMDBRMlptZVRkdGNFUjFZekV	0%	Avira URL Cloud	safe	
http://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://w3c.github.io/IntersectionObserver/#intersection-observer-interface	0%	Avira URL Cloud	safe	
http://docs.closure-library.googlecode.com/git/closure_goog_date_date.js.source.html	0%	Avira URL Cloud	safe	
http://https://www.nathanaeluser.com/blog/2013/reading-max-width-cross-browser	0%	URL Reputation	safe	
http://https://www.nathanaeluser.com/blog/2013/reading-max-width-cross-browser	0%	URL Reputation	safe	
http://https://www.nathanaeluser.com/blog/2013/reading-max-width-cross-browser	0%	URL Reputation	safe	
http://https://www.anujgakhar.com/2014/03/01/binary-search-in-javascript/	0%	URL Reputation	safe	
http://https://www.anujgakhar.com/2014/03/01/binary-search-in-javascript/	0%	URL Reputation	safe	
http://https://www.anujgakhar.com/2014/03/01/binary-search-in-javascript/	0%	URL Reputation	safe	
http://www.robertpenner.com/easing/	0%	URL Reputation	safe	
http://www.robertpenner.com/easing/	0%	URL Reputation	safe	
http://www.robertpenner.com/easing/	0%	URL Reputation	safe	
http://https://w3c.github.io/IntersectionObserver/#calculate-intersection-rect-algo	0%	Avira URL Cloud	safe	
http://flightschool.acylt.com/devnotes/caret-position-woes/	0%	URL Reputation	safe	
http://flightschool.acylt.com/devnotes/caret-position-woes/	0%	URL Reputation	safe	
http://flightschool.acylt.com/devnotes/caret-position-woes/	0%	URL Reputation	safe	
http://www.robertpenner.com/easing)	0%	URL Reputation	safe	
http://www.robertpenner.com/easing)	0%	URL Reputation	safe	
http://www.robertpenner.com/easing)	0%	URL Reputation	safe	
http://https://secured-login.ted-forms.com/XWkZKNVRYQmFTVmxrVkRoek9VTkdXRzVHWjNBM2RtMDBRMlptZVRkdGNFUjFZekV	0%	Avira URL Cloud	safe	
http://https://w3c.github.io/IntersectionObserver/#intersection-observer-entry	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn2.hubspot.net	104.17.243.204	true	false		high
s3.amazonaws.com	52.217.196.184	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
secured-login.net	34.226.85.79	true	false		unknown
landing.training.knowbe4.com	34.226.85.79	true	false		high
ipv4.imgur.map.fastly.net	151.101.112.193	true	false		unknown
covid19.protected-forms.com	unknown	unknown	false		unknown
i.imgur.com	unknown	unknown	false		high
favicon.ico	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://secured-login.net/pages/c3955b1c48a/XWkZKNVRYQmFTVmxrVkRoek9VTkdXRzVHWjNBM2RtMDBRMlptZVRkdGNFUjFZekV6ZWxkblJEZzFiMlZCTWxoTlVXaG5aMHRoYW1kc09VSnlja2xZYkc5MlYwdzNOWFpsVERWNUsxWXZiVkJ5YURreFUzTk9kbGt4ZWtoSGRYa3dTM1ppY1hkT0x6Y3pSMFJXVjNsMWRXNVRiRnBCZURZMGJVWkNlRlJ0TVdGM1REZEhNRnA0ZW5keksyTmFZV2hPWVRGd1Z6Tm9iRFVyVlhnd1UwdHhOVkU0YTJsRGRXMDBjMlZOUFMwdGVsSnhlVlJOWkZKRlNIVjZZbEpUYkVscGJUQTJaejA5LS0yNjI0MmEyNmU5MTE4NzY5Nzk4YzQ5Nzk4MGQyMGYxNmNiYmE1MGQy	false		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.217.196.184	s3.amazonaws.com	United States		16509	AMAZON-02US	false
104.17.243.204	cdn2.hubspot.net	United States		13335	CLOUDFLARENETUS	false
151.101.112.193	ipv4.imgur.map.fastly.net	United States		54113	FASTLYUS	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
34.226.85.79	secured-login.net	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	431204
Start date:	08.06.2021
Start time:	15:17:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://covid19.protected-forms.com/XWkZKNVRYQmFTVmxrVkRoek9VTkdXRzVHWjNBM2RtMDBRMlptZVRkdGNFUjFZekV6ZWxkblJEZzFiMlZCTWxoTlVXaG5aMHRoYW1kc09VSnlja2xZYkc5MlYwdzNOWFpsVERWNUsxWXZiVkJ5YURreFUzTk9kbGt4ZWtoSGRYa3dTM1ppY1hkT0x6Y3pSMFJXVjNsMWRXNVRiRnBCZURZMGJVWkNlRlJ0TVdGM1REZEhNRnA0ZW5keksyTmFZV2hPWVRGd1Z6Tm9iRFVyVlhnd1UwdHhOVkU0YTJsRGRXMDBjMlZOUFMwdGVsSnhlVlJOWkZKRlNIVjZZbEpUYkVscGJUQTJaejA5LS0yNjI0MmEyNmU5MTE4NzY5Nzk4YzQ5Nzk4MGQyMGYxNmNiYmE1MGQy?cid=874637403
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:	3
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:	• EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@3/28@7/5
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\DOMStore\E5F0NRSV\secured-login[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	39
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aK1r0aK1r0aKb:JFK1rFK1rFKb
MD5:	B9C5EB570521110110BB7DFF12AF780D
SHA1:	27F5BEBC2200FD8D0B51A93D1357EA954BE44079
SHA-256:	90171F10A6467C9DC31143859BAB69D045B67B39E2E49D92BB7168B383C4D1AB
SHA-512:	BC81539E62D643808CBDA3D86050058F379B2F0347CE65CBBA9797D386401C886B22AC4C0B2BE68197AE10C83A1E22A14232CD531C8D139DD3C031DB423EA3
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{0B1EB684-C85C-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8553166752129058
Encrypted:	false
SSDEEP:	192:r1Z6Zv2tW+teifg3pzMPxBfrDztsfZc3kjX:r7m+k+PF7/zgZV
MD5:	3C77F99155058A76E34F388D61B8CD05
SHA1:	A4D6C98759ACB77A3EE5EC4F855ACEC7297FFCD9
SHA-256:	AD10D079F96B3577FD4408AAE3066A14C6419384131CEB146D32B926B72C45CD

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{0B1EB684-C85C-11EB-90EB-ECF4BBEA1588}.dat	
SHA-512:	00D19E2C75E1E79902E2B60B62814180336761DD6A89616F491A5193418AFCE4D944A56F9324ED0E4536AA8CE7134DAFD38FE13FB0748F79FF114787DDE9D555
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\{0B1EB686-C85C-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	37278
Entropy (8bit):	2.5629326866251705
Encrypted:	false
SSDEEP:	192:rCZ9Q56zkLjx2VWjMX8z06ZQmQj06dR06T063r06106D06l06K06HBg:r+CU43gsgszEmQjd9FrHxHoRa
MD5:	2C030CAECC45179E295670925ACAB8E0
SHA1:	84DA87200B298B81789EEBD6C7ABB581E3FE2984
SHA-256:	DD4C6DC320F6ECA59129EE86E98133FB6919703274297372CBFDA24473947AAF
SHA-512:	E46CD4A6BDE6D1F7D51312B64457A9C5942391710AFD4F77E5F2CB19FDE147A157EB1CB3B4AB10B7D96F97378BCE1D9A710F9D8CB80DBECAB8F4F4C0C9E5F 07F
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\{1283C016-C85C-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5655793598973897
Encrypted:	false
SSDEEP:	48:IwwGcprMrvGwpaurEG4pQwr2GrapbSUGQpKWG7HpRWTGIpG:r0Z4ZQ60604BSMABTiA
MD5:	F3A10BEA1670E7873F1665235B761C36
SHA1:	9B779E836E315448EABBF6408A341F99931CCA5B
SHA-256:	EEDB1D745168D2BC4C33CA4C0FFA54AB77C6F0E018348B2BD539E03FD77804A1
SHA-512:	95C8A6D62F9CD996BCB78EE58EB20645F4FFBC18566991BE2AE80C920DCBC0150F5A5EF86978D76D242808C9C6FEACED18E1DF2CAB970EBBC4C7437B1DEE 2B4
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):	5.094352940015059
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEkJdo2JdanWimI002EtM3MHdNMNxOEkJdo2JdanWimI00OYGVbkEtMb:2d6NxOndbdaSZHKd6NxOndbdaSZ7YLb
MD5:	9CCC5F700E1EFFD1DFC48EB1B4C4EF62
SHA1:	65F24C0C70D642355C2B7BDEEE46638A838C94F0
SHA-256:	1C406C65E02C76D4F592E2FC74966A2251F05DFF8E94FBF2DD6F30198FB85389
SHA-512:	DF9EB922C0029A3A634EBBDD5D08B09DCC57E7470BD493DB9FB6906A7E0BC2F4F9164909F37873292B18E3083D12B72B974D092C8D2456FD32B95602F85CF74
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>0xe384ab18,0x01d75c68</date><accdate>0xe384ab18,0x01d75c68</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>0xe384ab18,0x01d75c68</date><accdate>0xe384ab18,0x01d75c68</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):	5.1103408799649355
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kh4doP4danWimI002EtM3MHdNMNxe2kh4doP4danWimI00OYGkak6t:2d6Nxro4d84daSZHKd6Nxro4d84daSZN
MD5:	53267D454C87DBA3D43B1096A5180F50
SHA1:	EB4C0942794D9A4F9BA2E8889B064A9D25430B3A
SHA-256:	93B289DB35D3B12F549BD3319FD512836B0622C56FFCB7B8A362A618B422F915
SHA-512:	C03D4517C2F132F666B90D1131DB4E7F8537B57A066FA6F2F4C5830C4E5D36C4BCBF80E93D93C527C59918597E600666EE6A723F10F8800F066AAE5319E2E9BE
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xe37d84ad,0x01d75c68</date><accdate>0xe37d84ad,0x01d75c68</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>0xe37d84ad,0x01d75c68</date><accdate>0xe37d84ad,0x01d75c68</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):	5.113782010135935
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLkJdo2JdanWimI002EtM3MHdNMNxvLkJdo2JdanWimI00OYGmZEtMb:2d6NxvOdbdaSZHKd6NxvOdbdaSZ7Yjb
MD5:	E4A9B49EA55B5FB7CC302E2D8CAB8539
SHA1:	3AA3EC9C44E0833BF17F39B46B852D855D038DE2
SHA-256:	35487F75B1A5704D328C960BD8116CA546B0B763D0EC63962A49E6F941AFD3E9
SHA-512:	E947F0A4B21FF3DD46644643AD8137750E9DC31FB492E3CB17CD2FC069FD460D6E3FBCBCD588D59AA7EF666D9C55007A378CB14516FF7659B230ED2A6770F9A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xe384ab18,0x01d75c68</date><accdate>0xe384ab18,0x01d75c68</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>0xe384ab18,0x01d75c68</date><accdate>0xe384ab18,0x01d75c68</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):	5.109820853626373
Encrypted:	false
SSDEEP:	12:TMHdNMNxikJdo2JdanWimI002EtM3MHdNMNxikJdo2JdanWimI00OYGd5EtMb:2d6NxZdbdaSZHKd6NxZdbdaSZ7YEjb
MD5:	AB5CA26470B02CD0F8559F14397A0CA9
SHA1:	345D75BA767E08F525F51CA5CA4CC29189BA3581
SHA-256:	ADB03AE80C60E2C4A7D274E813BB36BD168922ACCAEA2AD66F223A6E7CCC2C39
SHA-512:	23C5799C33FF6EC11FFFD506CE734B3DF6D092D159158A5582C2AFACF974B50DCF6F39502B3F4642D4595AD0F836CFFD4D1C38B5EBE9CE1AB8B1489AB1641E3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xe384ab18,0x01d75c68</date><accdate>0xe384ab18,0x01d75c68</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>0xe384ab18,0x01d75c68</date><accdate>0xe384ab18,0x01d75c68</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):	5.141282934460989
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwxZdobZdanWimI002EtM3MHdNMNxhGwxZdobZdanWimI00OYG8K07/:2d6NxQmdmdaSZHKd6NxQmdmdaSZ7YrKG
MD5:	B804BCD0DFDED45143161B21451534C2
SHA1:	4679161D7F3BC28C6E7941522D9A42D42D32659A
SHA-256:	B1ADD0E4E88B3EA87F42F4CA448D1912B817FF87C684B169743ADBE1E5CB009C
SHA-512:	E53293C2391B6CEFED3776673AF33C05D5E2AB5FCDDE6738EDF76BFD32E8F3849C85633E0EBACCF791571742BD1E1E44BB3C4D13C91794A715C640644884AB8
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xe38bd225,0x01d75c68</date><accdate>0xe38bd225,0x01d75c68</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>0xe38bd225,0x01d75c68</date><accdate>0xe38bd225,0x01d75c68</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):	5.098117113717454
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nkJdo2JdanWimI002EtM3MHdNMNx0nkJdo2JdanWimI00OYGxEtMb:2d6Nx0idbdaSZHKd6Nx0idbdaSZ7Ygb
MD5:	342D1A407E62AE4CF6335DFA06892F8A
SHA1:	319023494951A23C3662EBF6E07F93865F095374
SHA-256:	65917F732E1E8EE1F32B8A5923D9BB3F5D65BB6C174B291359691841DA8C468A
SHA-512:	0A0F8D6756AFF2A72B7FF353540F0E8F7C6DAB8FB84E5532484945EC1B3EB8E0AF39E7ED1C56E482FB7A783348FB5C14A40DCE41C2A046843EAD0A8F70F7EB9D
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xe384ab18,0x01d75c68</date><accdate>0xe384ab18,0x01d75c68</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>0xe384ab18,0x01d75c68</date><accdate>0xe384ab18,0x01d75c68</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):	5.133988219342853
Encrypted:	false
SSDEEP:	12:TMHdNMNxxkJdo2JdanWimI002EtM3MHdNMNxxkJdo2JdanWimI00OYG6Kq5EtMb:2d6NxodbdaSZHKd6NxodbdaSZ7Yhb
MD5:	FBA2465F8FB40BE3932F09E667807939
SHA1:	116F3D26A77A892B3EA8D8A6A8882959B34A24D9
SHA-256:	3BD7AB8FD4B76DB93DD14F3809862E3815110A816FBB5CACC15F91E3E12E4FD1
SHA-512:	3561325AA911BB103262EC4F121F174C698C24BC7D7ABFCA64E422413463618B7FF09432F8B39AD347CDB0AF0D2425A0DCC6C861C63CAA17B8E52BD9E413669
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xe384ab18,0x01d75c68</date><accdate>0xe384ab18,0x01d75c68</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>0xe384ab18,0x01d75c68</date><accdate>0xe384ab18,0x01d75c68</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\pin20259167780\msapplication.xml	

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):	5.110195498518297
Encrypted:	false
SSDEEP:	12:TMHdNMNxckJdo2JdanWimI002EtM3MHdNMNxckJdo2JdanWimI00OYGVEtMb:2d6NxPdbdaSZHKd6NxPdbdaSZ7Ykb
MD5:	2CCF1365DDB254DB2FA88563089BE85D
SHA1:	A44D61AF6E0191C479F2D0982EBEFB473DA0CDB7
SHA-256:	6993C3DE614E46A6A4B4D5284DE207C790C3EE26D0067FFEB2B384BAE4E717B9
SHA-512:	B2413E119071A04CA059628B33B09C9E88908FCADE84664AFCFD9232915A33169820B1450919F7AA10445DEC048EDDF8C4BF9B348BCE2166C8BAF8728416A49A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xe384ab18,0x01d75c68</date><accdate>0xe384ab18,0x01d75c68</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>0xe384ab18,0x01d75c68</date><accdate>0xe384ab18,0x01d75c68</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):	5.09516012991932
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnkJdo2JdanWimI002EtM3MHdNMNxfnkJdo2JdanWimI00OYGe5EtMb:2d6NxKdbdaSZHKd6NxKdbdaSZ7YLjb
MD5:	9DBBE395FAC00E5671502857EF6C7609
SHA1:	8CADD17AF0078EB56FF366E62175D3CC995F560E
SHA-256:	F412C81EF3A48D57DF92B090A0DAC42C1D4E89CC672DB21E4799200E5F473832
SHA-512:	6A9C7472177EDC76B5C64799579C7825FEE1FE59FF9CFA884E215082EE158410D9CE9376EEAD2F9FEA673DCC5B693FC7293D65B2D806C6324C3930071DBCF9
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xe384ab18,0x01d75c68</date><accdate>0xe384ab18,0x01d75c68</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>0xe384ab18,0x01d75c68</date><accdate>0xe384ab18,0x01d75c68</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\2WF3MMUU\IU9ESTP0.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	556
Entropy (8bit):	5.751255253864889
Encrypted:	false
SSDEEP:	12:3R+xnAp6Q/rPAg1tWhLJ+q3GemyuqLJ9YlWt/4AEdeIQL:3Eo6QT4eMh9+Mb7VqW5NEkj
MD5:	E29F472F8FDABCC42F4A714319354832
SHA1:	D380CD566FDE466D955AAC77C9DAB011FA43962B
SHA-256:	092879E02BB81B6B636A80A9D521FEC8A0555965886D3461E40BE1A26D24660B
SHA-512:	DB6C482DA17C86D9268B12873668757BD56F47505CC6B281D44216D54B2C309B761DAE1D20E27D8039EA9DEEE50DA068B63EE47E2FF45B063DB28A5A28A2C11
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid19.protected-forms.com/XWkZKNVRYQmFTVmxrVkRoek9VTkdXRzVHWjNBM2RtMDBRMlptZVRkdGNFUjFZekV6ZWxkblJEZzFiMlZCTWxoTlVXaG5aMHRoYW1kc09VSnlja2xZYkc5MlYwdzNOWFpsVERWNUsxWXZiVkJ5YURreFUzTk9kbGt4ZWtoSGRYa3dTM1ppY1hkT0x6Y3pSMFJXVjNsMWRXNVRiRnBCZURZMGJVWkNlRlJ0TVdGM1REZEhNRnA0ZW5keksyTmFZV2hPWVRGd1Z6Tm9iRFVyVlhnd1UwdHhOVkU0YTJsRGRXMDBjMlZOUFMwdGVsSnhlVlJOWkZKRlNIVjZZbEpUYkVscGJUQTJaejA5LS0yNjI0MmEyNmU5MTE4NzY5Nzk4YzQ5Nzk4MGQyMGYxNmNiYmE1MGQy?cid=874637403

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\IU9ESTP0.htm	
Preview:	<html>. <head>. <script>window.location.href = 'https://secured-login.net/pages/c3955b1c48a/XWkZKNVRYQmFTVmxrVkRoek9VTkdXRzVHWjNBM2RtM DBRMlptZVRkdGNFUjFZekV6ZWxkblJEZzFiMlZCTWxoTlVXaG5aMHRoYW1kc09VSnlja2xZYkc5MlYwdzNOWFpsVERWNUsxWXZiVkJ5YURreFUzTk9kbGt4Z WtoSGRYa3dTM1ppY1hkT0x6Y3pSMFJXVjNsMWRXNVRiRnBCZURZMGJVWkNlRlJ0TVdGM1REZEhNRnA0ZW5keksyTmFZV2hPWVRGd1Z6Tm9iRFVyVlhnd1Uwd HhOVkU0YTJsRGRXMDBjMlZOUFMwdGVsSnhlVlJOWkZKRlNIVjZZbEpUYkVscGJUQTJaejA5LS0yNjI0MmEyNmU5MTE4NzY5Nzk4YzQ5Nzk4MGQyMGYxNmNiY mE1MGQy';</script>. </head>. <body>. </body>.</html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\KB4-logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 200 x 75, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	5864
Entropy (8bit):	7.925096866918419
Encrypted:	false
SSDEEP:	96:YRObJZQcSGBG0v6UBnFSai6Xk2kQ6779zVD0nCXYTu4qWeG0a6lS+adxQVwZ5kkt:iO5SGBRBAkelpXY69We5IhdxQVwfkkt
MD5:	20F88CB052864EF047CBF095E46A23B0
SHA1:	5068F0745178BC0C042B6302ED114516981141BD
SHA-256:	65149B7AFD0CCFDEA4CB383944A47825F33B1A80B092ECA6F74CB01F0C186809
SHA-512:	57E78802933898C66F8E2245357883705E732F0686697601C0F3C2C96B9D345BE131DCD4C0118C657C2A55BC397044DBD06456AB68172C3867C4D055B6EC11EF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.hubspot.net/hubfs/241394/html_file/files/img/KB4-logo.png
Preview:	.PNG.....IHDR.....K.....5|.....IDATx..].x.E.....(...^ ..(.!.....ry.*".*...Q.u.s.ka.(..'....{ ...G.I.9 .#..r....a.GuO..$$...~_f..^].W...N.."@CCC..... ... ...t.....>| ...,D...9.....".I.C.R..p..Mi>.<.....E+@0 .....S...V.PpO@.$k..b...B)z.qv.p@.Z..+.v.$qi.....Hr...j.....v2.D..s!`..3B.e.&..7....H.....|.(R.$.....Z...P.*.....V.j O..6.5... .....X.....5A .h.?.p.V..A..[...._.....$.W...0..k.+.C.Ti.....T7..E..-*. ...a..gu..M....d..d.!m....%.....Q..3.S.h.T.A.2..j@...b.:.^...2..Y.....d..v?..|.7Bl.....8..y...z.... Q.o.x... .....1.. .B.PgmHX..k.....d...4.....0.....R.:{1.]....n.B.&.!...^V....d....B.....T.U~ ..I..[A...../..d....e.1..V...^.d.. *4<.|..M">!Q.N.#..M.{SR...="a...q.....Y.i.(.-.r..P. [.....X.Op(.%)o.*G%.d-.q.....mnH...@....o|^....v..36..r.q^.'..t.:@..;.O9 H.o.....+..g.cyy..38.{.....D\.v.d.@.....R..g...?z)..4..!....(V

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b[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):	4008497
Entropy (8bit):	5.095997159612487
Encrypted:	false
SSDEEP:	49152:Aw4mDiTFyA6TVfMAeuljHmcIkp5W5FHAzJ7CjhB0ZyA9At+zORaseqlyT7cZdTA8:8Z
MD5:	EA43F2BF3329E6FECFCE657D8788AFC6
SHA1:	D9C95A9DA90AEFB0D27D54001FC495A4B8040942
SHA-256:	3F9643CF23457F5E352C895A1B9B7D12BFCDA608697713C0AADDA634B1EDD7E6
SHA-512:	1D63BBB463ED835C353ADCD39D3227093115B7F7E5A4BE8B35442C8644091FD9E9B054C55ADAA4B2889856C9939F367667182E64BAD849BAE8D094BD3970088
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secured-login.net/assets/application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b.js
Preview:	// Array.fill.if (!Array.prototype.fill) {. Object.defineProperty(Array.prototype, 'fill', {. value: function(value) {.. // Steps 1-2.. if (this == null) {. throw new Ty peError('this is null or not defined');. }.. var O = Object(this);.. // Steps 3-5.. var len = O.length >>> 0;.. // Steps 6-7.. var start = arguments[1];. var relativeStart = start >> 0;.. // Step 8.. var k = relativeStart < 0 ?. Math.max(len + relativeStart, 0) :. Math.min(relativeStart, len);.. // Steps 9-10.. var end = arguments[2];. var relativeEnd = end === undefined ?. len : end >> 0;.. // Step 11.. var final = relativeEnd < 0 ?. Math.max(len + relativeEnd, 0) :. Math.min(relativeEnd, len);.. // Step 12.. while (k < final) {. O[k] = value;. k++;. }.. // Step 13.. return O;. }. });.}.// Object.values.Object.values = Object.values ? Object.values : f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\landing-watermark-8487e36eef1bec74f06631f19fea0aa171c208e2976373cda5bd0a4b9e230903[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	1471
Entropy (8bit):	4.754611179426391
Encrypted:	false
SSDEEP:	24:y40r8CQo40agx40mC400XLaR404hZYmx40vGk40vG/I40vGhH40VhZ40UrCmn:xdDgCFEiBZgnTOHTn
MD5:	15E89F9684B18EC43EE51F8D62A787C3
SHA1:	9CBAAACEAE96845ECD3497F41EE3B02588ABEC11
SHA-256:	16F13E16A7EF02FB6F94250AA1931DED83DBEE5D9FAD278E33DD5792D085194F
SHA-512:	79E0110A045F28437D192290AC9789270CB0D4E676A985564746DB439992D867BA89639D7738E2A7F7D83BBF37D9A02CAA2AE1DC4E0EE2519797E5840A47FABE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secured-login.net/assets/landing-watermark-8487e36eef1bec74f06631f19fea0aa171c208e2976373cda5bd0a4b9e230903.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\landing-watermark-8487e36eef1bec74f06631f19fea0aa171c208e2976373cda5bd0a4b9e230903[1].css	
Preview:	/* line 1, app/assets/stylesheets/landing-watermark.scss */..watermark {. -webkit-writing-mode: vertical-rl;. -ms-writing-mode: tb-rl;. writing-mode: vertical-rl;. text-orientation: sideways;.}../* line 4, app/assets/stylesheets/landing-watermark.scss */..watermark.left {. left: 0;.}../* line 7, app/assets/stylesheets/landing-watermark.scss */..watermark.right {. right: 0;.}../* line 10, app/assets/stylesheets/landing-watermark.scss */..watermark.top {. text-align: center;. -webkit-writing-mode: horizontal-tb;. -ms-writing-mode: lr-tb;. writing-mode: horizontal-tb;. top: -38px;.}../* line 15, app/assets/stylesheets/landing-watermark.scss */..watermark h1 {. -webkit-user-select: none;. -moz-user-select: none;. -ms-user-select: none;. user-select: none;. font-size: 15px;. color: #fdfdfa;. font-weight: bold;.}../* line 24, app/assets/stylesheets/landing-watermark.scss */.#template_sei .watermark.left {. margin-left: -10px;.}../* li

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\modernizr-79e0181ec91aff04bb01d87cba546535ede843f75d19f5c60f66b8dd6546971f[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	51364
Entropy (8bit):	4.630626843010533
Encrypted:	false
SSDEEP:	1536:TRCJJ/KpVsnpxvXmET56JYFE7qbe/7Y8fjWWy+4GrkfwuXxJ44ipW/VPRLq277ts:TS/FpzarzCT71Pts
MD5:	BF2F96E6233DE3D8C0346085AC28248A
SHA1:	4DB267704D7E3FB2489CF96E82862A2245CD9311
SHA-256:	EE94DDA0AF1FC5C5045741B39E54136015365EEDCA34095F1D3C666998BB442D
SHA-512:	D4DB54380D135D9F5AAA03727CC88037B014C1057A3061C3D173EB8D4CEC7E4A2F71CFCA1478E8E15C093D510EEE80668C2038691EAEB21958942089F0DD9C6C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secured-login.net/assets/modernizr-79e0181ec91aff04bb01d87cba546535ede843f75d19f5c60f66b8dd6546971f.js
Preview:	/*!. * Modernizr v2.7.1. * www.modernizr.com. *. * Copyright (c) Faruk Ates, Paul Irish, Alex Sexton. * Available under the BSD and MIT licenses: www.modernizr.com/license/. */../*. * Modernizr tests which native CSS3 and HTML5 features are available in. * the current UA and makes the results available to you in two ways:. * as properties on a global Modernizr object, and as classes on the. * <html> element. This information allows you to progressively enhance. * your pages with a granular level of control over the experience.. *. * Modernizr has an optional (not included) conditional resource loader. * called Modernizr.load(), based on Yepnope.js (yepnopejs.com).. * To get a build that includes Modernizr.load(), as well as choosing. * which tests to include, go to www.modernizr.com/download/. *. * Authors Faruk Ates, Paul Irish, Alex Sexton. * Contributors Ryan Seddon, Ben Alman. */..window.Modernizr = (function(window, document, undefined) {.. var version = '2.7.1',..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\vendor-f9f57d7be17e331a1955[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	372931
Entropy (8bit):	5.29856229717366
Encrypted:	false
SSDEEP:	6144:bczjVEg2HsGtNjvZBHPg96/6FTHL6jcYyTIU0:PsGzLkHLWJ
MD5:	0D3DDEEF42E7DD5336F27DAADB55AC92
SHA1:	7397C6CE00E6370069D944DAB49F226AA76609D2
SHA-256:	15BFAB10A07CA0B82FACA5584E364AA700D9BDB8D739FBBD4890E0782F894924
SHA-512:	F803B85D256D5B89FE4B3B9AD6967C9653E36BD95A1081898B00965C0B0079FFD343C2A07FA68CD5A380B0ED5E49E2FA6A67690547C1EC7813A6561B5F6E843
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secured-login.net/packs/js/vendor-f9f57d7be17e331a1955.js
Preview:	!function(t){var e={};function i(n){if(e[n])return e[n].exports;var r=e[n]={i:n,l:!1,exports:{}};return t[n].call(r.exports,r,r.exports,i),r.l=!0,r.exports}i.m=t,i.c=e,i.d=function(t,e,n){i.o(t,e)||Object.defineProperty(t,e,{enumerable:!0,get:n})},i.r=function(t){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(t,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(t,"__esModule",{value:!0})},i.t=function(t,e){if(1&e&&(t=i(t)),8&e)return t;if(4&e&&"object"==typeof t&&t&&t.__esModule)return t;var n=Object.create(null);if(i.r(n),Object.defineProperty(n,"default",{enumerable:!0,value:t}),2&e&&"string"!=typeof t)for(var r in t)i.d(n,r,function(e){return t[e]}.bind(null,r));return n},i.n=function(t){var e=t&&t.__esModule?function(){return t.default}:function(){return t};return i.d(e,"a",e),e},i.o=function(t,e){return Object.prototype.hasOwnProperty.call(t,e)},i.p="/packs/",i(i.s=973)}([,,,,,,function(t,e,i){function n(t,e,i){var c,u,p,d,f=t&n.F,g=t&n.G,m=t&n.P,v=t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\css2[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	204
Entropy (8bit):	5.04308254844705
Encrypted:	false
SSDEEP:	3:0SYWFFWlIYCiF15RI5XwDKLRIHDfFRWdFWLRI9j9v7fqzrZqcdJ1NAI7uRlGUBmn:0IFFm15+56ZRWHMqh7izlpddtglDxNin
MD5:	F9E67BD36470A28F1FEFC2FB4D6D0D27
SHA1:	7A40D21435164C8A55C20656FCA2F66FF92DAB75
SHA-256:	7ECE5239BC78D5E242A0CBCEC4087896A6354BD65F12874F2D3973B834F2FBC1
SHA-512:	6CEED0E07AE1072FCD63870682A9E7FB471F21F22AAF885305AA2CA142EACAA50BDB71489C403CAFFD54F3ECFC73B7D1183C7A57DE38FA3617ECD79A2AE13EB3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\css2[1].css	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css2?family=Open+Sans&display=swap
Preview:	@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/opensans/v20/mem8YaGs126MiZpBA-U1UQ.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\dd[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4524
Entropy (8bit):	5.108931295370594
Encrypted:	false
SSDEEP:	96:AG5XS7vBkRVkhmRaM44/HLPRaByA+zBRNI:AG5XABkAhmRaM44/H1CyrBRNI
MD5:	DD05B711E15EF201B07E20CB5C87F5D8
SHA1:	41B818B243140D90DA4CA917D454335B603A6BDA
SHA-256:	617F793D125F780AB7BB7C9E92AB427D9E757083E7368E241E8E8FA69F013E4F
SHA-512:	243C149BB8AAF5376EEBAC49833A59F75BA26BEC098AFD8A167D12BDACD3E80D98EE1DA1D82915CC7E4C7FAC747FBFF5D2D687D97F20BDF5C81D67CFA062F39
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s3.amazonaws.com/helpimg/landing_pages/css/dd.css
Preview:	.borderRadius{-moz-border-radius:5px; border-radius:5px; }...borderRadiusTp{-moz-border-radius:5px 5px 0 0; border-radius:5px 5px 5px 5px;}...borderRadiusBtm{-moz-border-radius:0 0 5px 5px ; border-radius:5px 5px 5px 5px;}.....ddcommon {position:relative;display:-moz-inline-stack; zoom:1; display:inline-block; *display:inline; c ursor:default;}...ddcommon ul{padding:0;margin:0;}...ddcommon ul li{list-style-type:none;}...borderRadiusTp ul li:last-child{-moz-border-radius:0 0 5px 5px ; border-radius:0 0 5px 5px;border-bottom:0 none #c3c3c3; }...borderRadiusBtm ul li:first-child{-moz-border-radius:5px 5px 0 0; border-radius:5px 5px 0 0 ;border-bottom:1 solid #c3c3c3; }.....ddcommon .disabled img, .ddcommon .disabled span, .ddcommon.disabledAll{..opacity: .5; /* standard: ff gt 1.5, opera, safari */..-ms-filter:"alpha(opacity=50)"; /* ie 8 */. .filter:alpha(opacity=50); /* ie lt 7 */..-khtml-opacity:.5; /* safari 1.x */..-moz-opacity:.5; /* ff lt 1.5, netscape */..color:#999999;..}...ddcommo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\QRF01zv[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 60 x 60, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1666
Entropy (8bit):	7.843362903299294
Encrypted:	false
SSDEEP:	48:1E3hTvNbvJkGGv0nnr5I2rk5boP0gD6EaTMN:1ERb+cr5Z1P0gD6/a
MD5:	29D583007FCD677AA31CA849478BC17A
SHA1:	F354E323218A450060852C344927C3E79D8E7B66
SHA-256:	120EE096F38C1E21083054C15F0F8CFBB02B6740A01D98068E3BE9581E83D453
SHA-512:	4AFC2641D96D1C372D091FD795D39C1AF12149B5EB30DA7BEE6FBFEA0650841067B7D259473BF65706CDD42D1EDF1CC5673B5F5556D1E91F8AE32976490A7E4D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://i.imgur.com/QRF01zv.png
Preview:	.PNG.....IHDR...<...<.....:..r...IIDATh..{.VE.....Y.E.....Uv.B....=. *{....ee....G.%....H/).UR1[.G...d...._m.....~:.|.13..~.e.;s...;g.....&g.@..w.G..K.....{.u+..^...k.....s+...e..R.z...".....l.z.....C.....V.#.}.5(..f5.N`.....e&3".x..g..w..C.....T|...v"w..Q>-(/2.x.A.L..!....r..noB..g|...|.\....U.T...<3.N-...rU.bp%.<.CE.....k....0C..|.Sw~.g....!...uf+y.KG.O+Y.h &.....F.....sB...7.|;.r|..\o.....;.$...i.wC.ICO.n.h....AJ.N.+.T).....)9..y..?.hs%.".B..k....#.S.....:..!o..Z...|.w2....a..+y.e;..A...x.p+2G/!..1..jTr.S...S.....D.<.G.z.+2..E..>.Z6L.....e.2..R ..3...~..%.C.!..f..s.'.;.M...5..k.1..L._B.vA_|.c{.....{....*...d...Y.'Q.TS:.7.....|...,.:..-...#.V.*NA..&...iO.....SEE.kW!.y.p.y.m..6b..@=.,.n..i,....q..W...w.f..bg.`|.....3.:.K.<..l.[....a..}..%_ ....{...~..j...).....n}m[...u...._....{.....,t.[..g.....&.v.j..2.r5.r5.B..jp..v-.j./.....c.s..$q@..z...oo..g?.z...%..gW.....}.6h....U....o.u.])]..@B);.o.V

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\mem8YaGs126MiZpBA-U1UQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 55324, version 1.1
Category:	downloaded
Size (bytes):	55324
Entropy (8bit):	**7.99064619923168**
Encrypted:	**true**
SSDEEP:	1536:JjsyS1KN5BvtgX74JT3XeCuDfKQDpoKyT0756MILnbr:JjdIKNTvtgX0JKFp2cSz3
MD5:	89BA4E29DC7A63CD15959A5BB068BB0E
SHA1:	250DEBBAEE6E7DC0C79F2BF23D8C84512F03BC10
SHA-256:	3ADC584FB0BEF1FBF9B1C0ECDDDE5727643B4334C734DB78B517AB112D92E1D8
SHA-512:	B7297EE98B51B5E8113CF1E50A8081B82B1A9AED9B386322AADB8CD4689D2C3335AF1858211615DB024AAA47FA3DE9E4C568D145D1C23AC45A7E20EA074D249
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\mem8YaGs126MiZpBA-U1UQ[1].woff	
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v20/mem8YaGs126MiZpBA-U1UQ.woff
Preview:	wOFF.....l<.....GDEF.....-.....4.qGPOS.....GSUB.....>.w.:OS/2...x..._...`.6..cmap.....h.....cvt ...@...Y.....M..fpgm.....~a..gasp...8..... ...#glyf...H.....'...A.head.....6...6..cphhea...,... ...$...Phmtx...L.....k.2.loca.....tmaxp..... ... . ..name.....&:A.post.....B...@...prep...,.....C...x.c`d``.a..&.V .....$..... /s..#s.s..#. .....x.U..n.P.D.....am.QmcK.....L.@g.w.$....MWS.87SM+....@..8"'..y.0RI;;>.f..^.1..W.....w\...p.0@...I..v.. ...m"D...1.....L..v7*P!.D..U.....t.)..f..1..|.. ....Y..B..WF.+[...x.c`f..8.....u..1...<.f.....{...h..... 0t.vf.....&.O.....)B..q>H..u..R``.....1.x.....;....L.j.Ms[.m.m..P.m....v.ijkb..... 8p...;..y!?.....a<L.5..v.8...}4,.K..]l.....Q..E.h. ...4.&...Cs. ...<./.....|.....C...(..>b..+..G.E."2.. .td\.\...ef.[6..d79]..}...."......%.Uu.....Du.....Tw.....{.hc.@ZGA....0..TX.k[.d\d./Y.w...q.:....;.P.H.c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\6F17TJ3O.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):	116740
Entropy (8bit):	5.949949023255428
Encrypted:	false
SSDEEP:	1536:SQcQgxpcDdaft9KG4Nm6yL1sIL5QHQGsIHBHjiulJriUVG9vFx8wQzK/4igmNO27:lcRLLmMe3juUVBlyUW
MD5:	026B7F3DA1DD3E7E9134D5971D0281C2
SHA1:	2403422DCDFF53DF424128AC6343E62B55A630D6
SHA-256:	8EDB5724DF71F88143E0C457940935AA88F8D476723628EECAECA377C3F7DB6F
SHA-512:	8B8412DC2A29EF1B3C2E46C5F0BF8737E6EAADE382E950E33E54A5A21E0E88C6E0661A1969A9532E3C0B46A3E7929145F70949B00779C7C910BBB37E9C55AF5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secured-login.net/pages/c3955b1c48a/XWkZKNVRYQmFTVmxrVkRoek9VTkdXRzVHWjNBM2RtMDBRMlptZVRkdGNFUjFZekV6ZWxkblJEZzFiMlZCTWxoTlVXaG5aMHRoYW1kc09VSnlja2xZYkc5MlYwdzNOWFpsVERWNUsxWXZiVkJ5YURreFUzTk9kbGt4ZWtoSGRYa3dTM1ppY1hkT0x6Y3pSMFJXVjNsMWRXNVRiRnBCZURZMGJVWkNlRlJ0TVdGM1REZEhNRnA0ZW5keksyTmFZV2hPWVRGd1Z6Tm9iRFVyVlhnd1UwdHhOVkU0YTJsRGRXMDBjMlZOUFMwdGVsSnhlVlJOWkZKRlNIVjZZbEpUYkVscGJUQTJaejA5LS0yNjI0MmEyNmU5MTE4NzY5Nzk4YzQ5Nzk4MGQyMGYxNmNiYmE1MGQy
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN". "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">..<html xmlns="http://www.w3.org/1999/xhtml">. <meta name="IMPORTANT" content="This page is part of a simulated phishing attack initiated by KnowBe4 on behalf of its customers." />. <meta name="IMPORTANT" content="If you have any questions please contact support@knowbe4.com." />. <meta content="IE=edge,chrome=1" http-equiv="X-UA-Compatible"/>. <meta name="robots" content="noindex, nofollow" />.. <head>. <script src="/assets/application-90929fee9f5daac0eca637129a780171565a15cebe060e2d86c95ffac685fd7b.js"></script>. <script src="/packs/js/vendor-f9f57d7be17e331a1955.js"></script>. <script src="/assets/modernizr-79e0181ec91aff04bb01d87cba546535ede843f75d19f5c60f66b8dd6546971f.js"></script>.. <script>.//<![CDATA[.window.gon={};gon.locale="en";.// .</script>.. <link rel="stylesheet" media="all" href="/assets/landing-watermark-8487e36eef1bec74f06631f19

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\bootstrap.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	121200
Entropy (8bit):	5.0982146191887106
Encrypted:	false
SSDEEP:	768:Vy3Gxw/Vc/QWlJxtQOIuiHlq5mzI4X8OAduFKbv2ctg2Bd8JP7ecQVvH1FS:nw/a1fluiHlq5mN8lDbNmPbh
MD5:	EC3BB52A00E176A7181D454DFFAEA219
SHA1:	6527D8BF3E1E9368BAB8C7B60F56BC01FA3AFD68
SHA-256:	F75E846CC83BD11432F4B1E21A45F31BC85283D11D372F7B19ACCD1BF6A2635C
SHA-512:	E8C5DAF01EAE68ED7C1E277A6E544C7AD108A0FA877FB531D6D9F2210769B7DA88E4E002C7B0BE3B72154EBF7CBF01A795C8342CE2DAD368BD6351E956195F8B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/3.3.7/css/bootstrap.min.css
Preview:	/*!. * Bootstrap v3.3.7 (http://getbootstrap.com). * Copyright 2011-2016 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). *//*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */html{font-family:sans-serif;-webkit-text-size-adjust:100%;-ms-text-size-adjust:100%}body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background-color:transparent}a:active,a:hover{outline:0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:700}dfn{font-style:italic}h1{margin:.67em 0;font-size:2em}mark{color:#000;background:#ff0}small{font-size:80%}sub,sup{position:relative;font-size:75%;line-height:0;vertical-align:baseline}sup{top:-.5em}sub{bottom:-.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr

C:\Users\user\AppData\Local\Temp\~DF820E21105090C19F.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47727203450538885
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loL9loL9lWO2B1d:kBqoIsyD3
MD5:	126553DD8C9398B5603484112FBF060B
SHA1:	1107E4ADCD8B0384E417C2D447D6627BE3E4485F
SHA-256:	620F456D12684064F3D74302D0E9E4FF67DC908A32A9B185F7C3727B97B493BB

C:\Users\user\AppData\Local\Temp\~DF820E21105090C19F.TMP	
SHA-512:	CD03588E67764A3196C73FACA67A67088C0DCF27BEEF7FF59AE94310DFBEA63B42826571902A9DAA303A956D56F16C6A76E88FFC8D516F977E61DBF2D155FD6 0
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFB81FC44A4392FBBB.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\~DFD3A635E75702A4C0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	46768
Entropy (8bit):	1.3363754736261837
Encrypted:	false
SSDEEP:	768:DIBBgTuoU7F79L8DkkNkjqk9Nksk43G7J5SN:DU
MD5:	7E05CBA1C6ED151124FC4C7DF4AAB9AB
SHA1:	921C8D8B3D16BAA43A88B79FA9ECE2E674869EB1
SHA-256:	4665549FABFE35A2A1905DCA8CDCD71386DD056843978B6239A5B4D0A62CC81D
SHA-512:	3849466ECE50DDD20FDBAD921F6AE1276DA892B13820045A0E939E21B7D0E9B9E2FB3A3657ADD31E8656780C6EC96ECB459D052A931AAA93C798BD8389D18A B
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 8, 2021 15:18:44.300211906 CEST	192.168.2.4	8.8.8.8	0x5931	Standard query (0)	covid19.protected-forms.com	A (IP address)	IN (0x0001)
Jun 8, 2021 15:18:45.271384001 CEST	192.168.2.4	8.8.8.8	0xf6d3	Standard query (0)	secured-login.net	A (IP address)	IN (0x0001)
Jun 8, 2021 15:18:46.313350916 CEST	192.168.2.4	8.8.8.8	0x36ae	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jun 8, 2021 15:18:46.328489065 CEST	192.168.2.4	8.8.8.8	0x154e	Standard query (0)	s3.amazonaws.com	A (IP address)	IN (0x0001)
Jun 8, 2021 15:18:46.414156914 CEST	192.168.2.4	8.8.8.8	0x947	Standard query (0)	cdn2.hubspot.net	A (IP address)	IN (0x0001)
Jun 8, 2021 15:18:46.422141075 CEST	192.168.2.4	8.8.8.8	0xfa49	Standard query (0)	i.imgur.com	A (IP address)	IN (0x0001)
Jun 8, 2021 15:19:02.572901011 CEST	192.168.2.4	8.8.8.8	0xd86d	Standard query (0)	favicon.ico	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 8, 2021 15:18:44.347903967 CEST	8.8.8.8	192.168.2.4	0x5931	No error (0)	covid19.protected-forms.com	landing.training.knowbe4.com		CNAME (Canonical name)	IN (0x0001)
Jun 8, 2021 15:18:44.347903967 CEST	8.8.8.8	192.168.2.4	0x5931	No error (0)	landing.training.knowbe4.com		34.226.85.79	A (IP address)	IN (0x0001)
Jun 8, 2021 15:18:44.347903967 CEST	8.8.8.8	192.168.2.4	0x5931	No error (0)	landing.training.knowbe4.com		18.233.2.161	A (IP address)	IN (0x0001)
Jun 8, 2021 15:18:45.329622984 CEST	8.8.8.8	192.168.2.4	0xf6d3	No error (0)	secured-login.net		34.226.85.79	A (IP address)	IN (0x0001)
Jun 8, 2021 15:18:45.329622984 CEST	8.8.8.8	192.168.2.4	0xf6d3	No error (0)	secured-login.net		18.233.2.161	A (IP address)	IN (0x0001)
Jun 8, 2021 15:18:46.358124018 CEST	8.8.8.8	192.168.2.4	0x36ae	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jun 8, 2021 15:18:46.358124018 CEST	8.8.8.8	192.168.2.4	0x36ae	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jun 8, 2021 15:18:46.370959044 CEST	8.8.8.8	192.168.2.4	0x154e	No error (0)	s3.amazonaws.com		52.217.196.184	A (IP address)	IN (0x0001)
Jun 8, 2021 15:18:46.460834026 CEST	8.8.8.8	192.168.2.4	0x947	No error (0)	cdn2.hubspot.net		104.17.243.204	A (IP address)	IN (0x0001)
Jun 8, 2021 15:18:46.460834026 CEST	8.8.8.8	192.168.2.4	0x947	No error (0)	cdn2.hubspot.net		104.17.241.204	A (IP address)	IN (0x0001)
Jun 8, 2021 15:18:46.460834026 CEST	8.8.8.8	192.168.2.4	0x947	No error (0)	cdn2.hubspot.net		104.17.242.204	A (IP address)	IN (0x0001)
Jun 8, 2021 15:18:46.460834026 CEST	8.8.8.8	192.168.2.4	0x947	No error (0)	cdn2.hubspot.net		104.17.244.204	A (IP address)	IN (0x0001)
Jun 8, 2021 15:18:46.460834026 CEST	8.8.8.8	192.168.2.4	0x947	No error (0)	cdn2.hubspot.net		104.17.240.204	A (IP address)	IN (0x0001)
Jun 8, 2021 15:18:46.464942932 CEST	8.8.8.8	192.168.2.4	0xfa49	No error (0)	i.imgur.com	ipv4.imgur.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jun 8, 2021 15:18:46.464942932 CEST	8.8.8.8	192.168.2.4	0xfa49	No error (0)	ipv4.imgur.map.fastly.net		151.101.112.193	A (IP address)	IN (0x0001)
Jun 8, 2021 15:19:02.616044998 CEST	8.8.8.8	192.168.2.4	0xd86d	Name error (3)	favicon.ico	none	none	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 8, 2021 15:18:44.646584034 CEST	34.226.85.79	443	192.168.2.4	49704	CN=authentlcation.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Feb 08 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Mar 10 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jun 8, 2021 15:18:44.772845984 CEST	34.226.85.79	443	192.168.2.4	49705	CN=authentlcation.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Feb 08 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Mar 10 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 8, 2021 15:18:45.710174084 CEST	34.226.85.79	443	192.168.2.4	49706	CN=secured-login.net CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sat Oct 24 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Wed Nov 24 00:59:59 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jun 8, 2021 15:18:45.717971087 CEST	34.226.85.79	443	192.168.2.4	49707	CN=secured-login.net CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sat Oct 24 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Wed Nov 24 00:59:59 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 8, 2021 15:18:46.470911980 CEST	104.16.18.94	443	192.168.2.4	49712	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jun 8, 2021 15:18:46.471295118 CEST	104.16.18.94	443	192.168.2.4	49709	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jun 8, 2021 15:18:46.553009987 CEST	104.17.243.204	443	192.168.2.4	49715	CN=hubspot.net, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sun Jun 06 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Mon Jun 06 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jun 8, 2021 15:18:46.554900885 CEST	104.17.243.204	443	192.168.2.4	49714	CN=hubspot.net, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sun Jun 06 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Mon Jun 06 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jun 8, 2021 15:18:46.554940939 CEST	151.101.112.193	443	192.168.2.4	49717	CN=*.imgur.com, O="Imgur, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jan 15 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Wed Mar 16 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 8, 2021 15:18:46.559290886 CEST	151.101.112.193	443	192.168.2.4	49716	CN=*.imgur.com, O="Imgur, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jan 15 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Wed Mar 16 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jun 8, 2021 15:18:46.657716036 CEST	52.217.196.184	443	192.168.2.4	49713	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Jun 8, 2021 15:18:46.659506083 CEST	52.217.196.184	443	192.168.2.4	49710	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5852 Parent PID: 800

General

Start time:	15:18:42
Start date:	08/06/2021
Path:	C:\Program Files\internet explorer\iexplore.exe

Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff748760000
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: 6000 Parent PID: 5852

General

Start time:	15:18:42
Start date:	08/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5852 CREDAT:17410 /prefetch:2
Imagebase:	0x270000
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