ID: 431202
Cookbook: browseurl.jbs
Time: 15:15:11
Date: 08/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

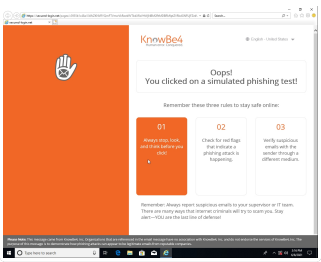
Analysis Report https://covid19.protected-forms.com/X...

Overview

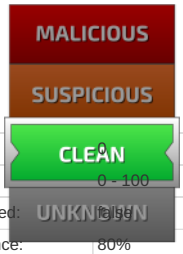
General Information

Sample URL:	https://covid19.protected-forms.com/XWkZKNVRYQmFTVmxrVkRoek9VTkdXRzVHWjNBM2...aejA5LS0yNjI0MmEyNmU5MTE4NzY5Nzk4YzQ5Nzk4MGQyMGYxNmNiYmE1MGQy?cid=874637403
Analysis ID:	431202
Infos:	

Most interesting Screenshot:



Detection

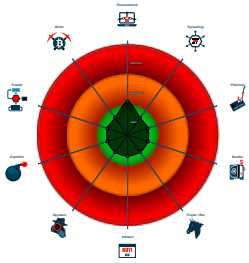


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 5948 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4768 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5948 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

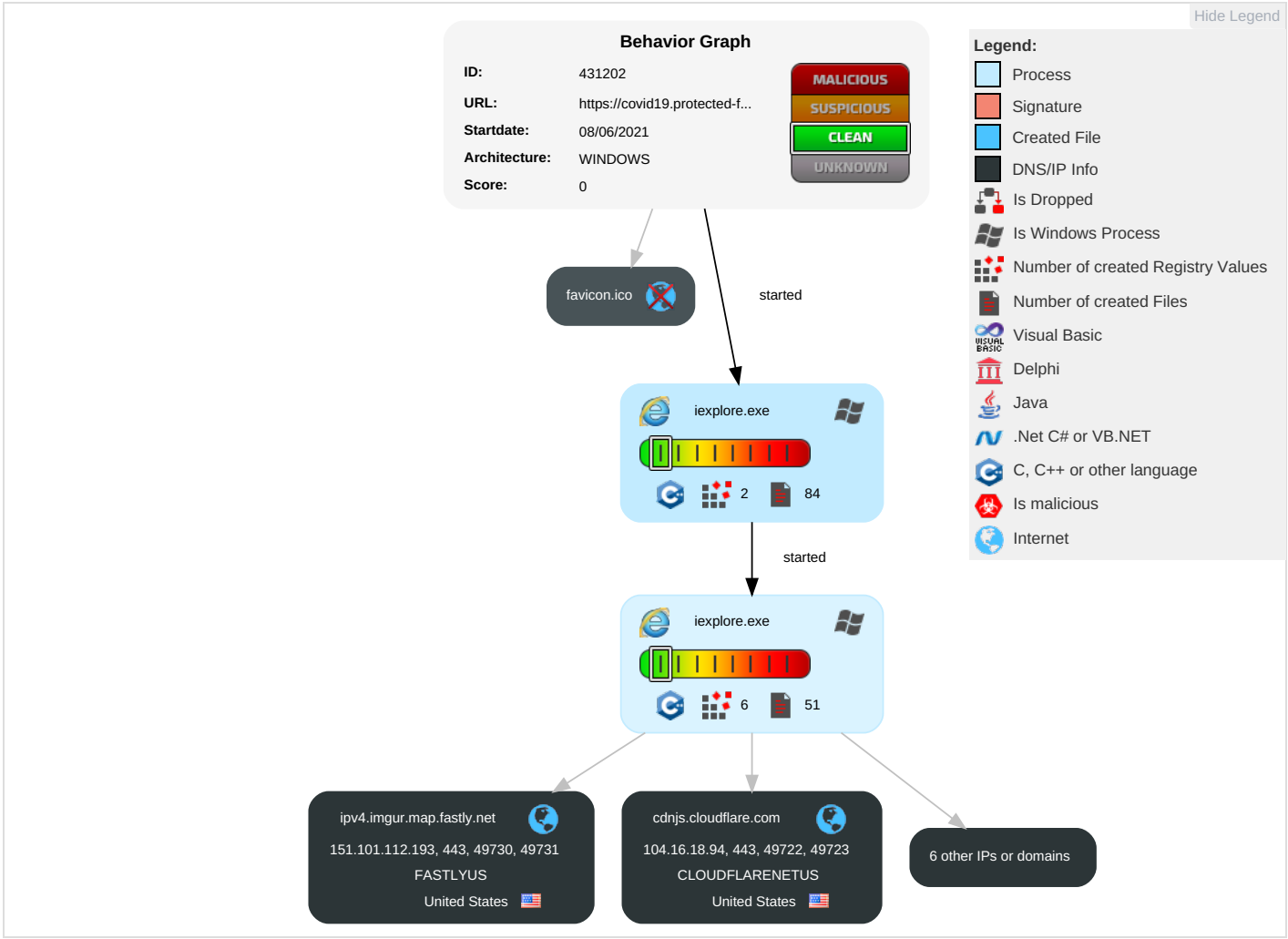
Click to jump to signature section

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

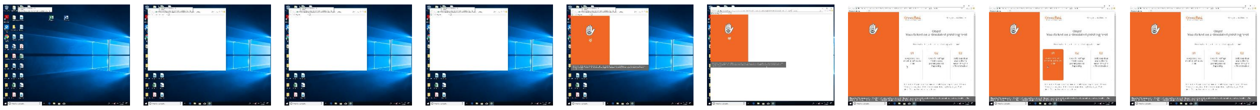
Behavior Graph

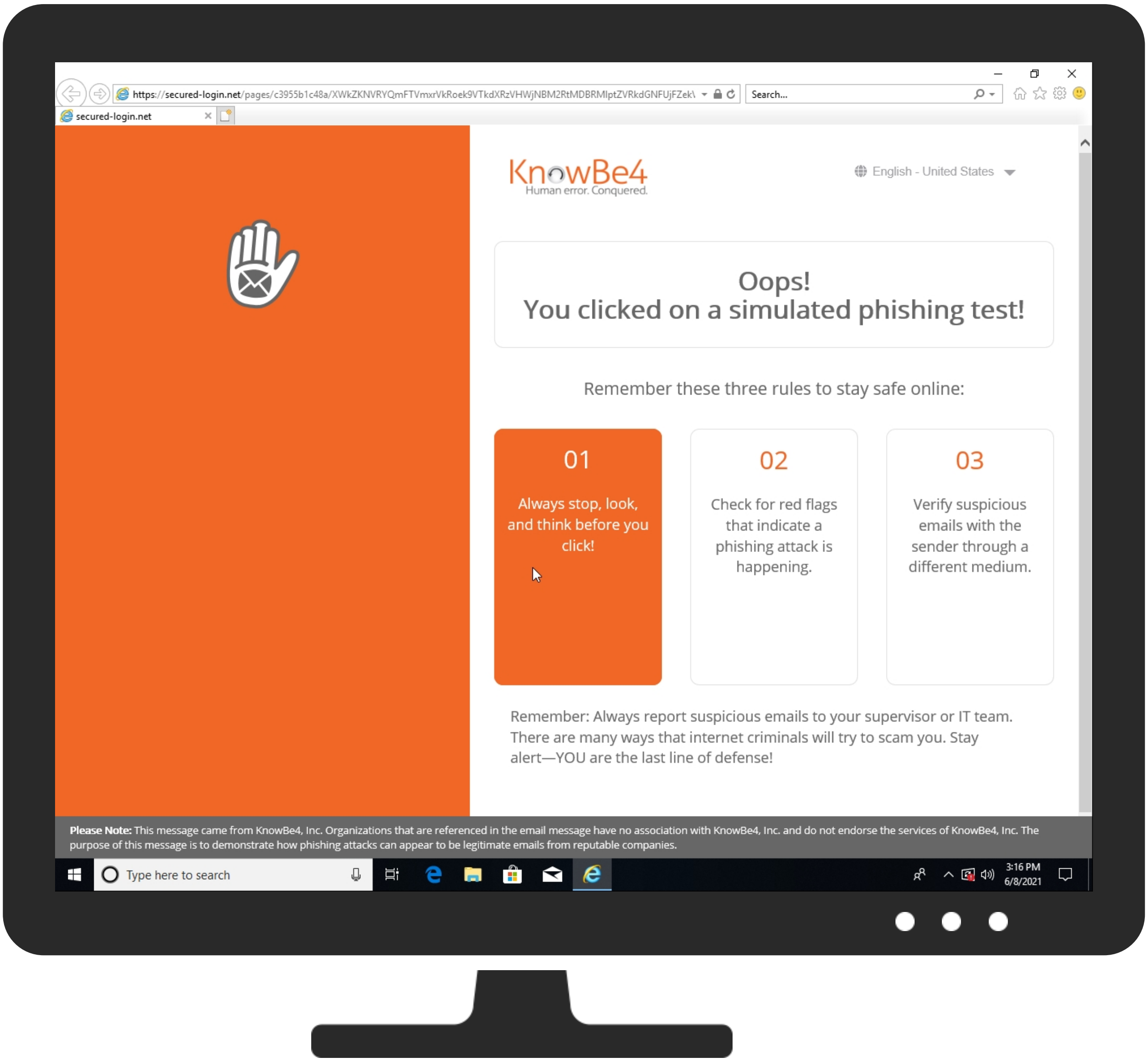


Screenshots

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/XWkZKNVRYQmFTVmxrVkRoek9VTkdXRzVHWjNBM2RtMDBRMlptZVRkdGNFUjFZekV6ZWxkblJEZzFiMlZCTWxoTlVXaG5aMHRoYW1kc09VSnlja2xZYkc5MlYwdzNOWFpsVERWNUsxWXZiVkJ5YURreFUzTk9kbGt4ZWtoSGRYa3dTM1ppY1hkT0x6Y3pSMFJXVjNsMWRXNVRiRnBCZURRZMGJVWkNlRlJ0TVdGM1REZEhNRnA0ZW5keksyTmFZV2hPWVRGd1Z6Tm9iRFVyVlhnd1UwdHhOVkU0YTJsRGRXMDBjMlZOUFMwdGVsSnhlVlJOWkZKRlNIVjZZbEpUYkVscGJJUQTJaejA5LS0yNjI0MmEyNmU5MTE4NzY5Nzk4YzQ5Nzk4MGQyMGYxNmNiYmE1MGQy?cid=874637403	0%	Virustotal		Browse
http://https://covid19.protected-forms.com/XWkZKNVRYQmFTVmxrVkRoek9VTkdXRzVHWjNBM2RtMDBRMlptZVRkdGNFUjFZekV6ZWxkblJEZzFiMlZCTWxoTlVXaG5aMHRoYW1kc09VSnlja2xZYkc5MlYwdzNOWFpsVERWNUsxWXZiVkJ5YURreFUzTk9kbGt4ZWtoSGRYa3dTM1ppY1hkT0x6Y3pSMFJXVjNsMWRXNVRiRnBCZURRZMGJVWkNlRlJ0TVdGM1REZEhNRnA0ZW5keksyTmFZV2hPWVRGd1Z6Tm9iRFVyVlhnd1UwdHhOVkU0YTJsRGRXMDBjMlZOUFMwdGVsSnhlVlJOWkZKRlNIVjZZbEpUYkVscGJJUQTJaejA5LS0yNjI0MmEyNmU5MTE4NzY5Nzk4YzQ5Nzk4MGQyMGYxNmNiYmE1MGQy?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://chmln.github.io/flatpickr/examples/#flatpickr-external-elements	0%	Virustotal		Browse
http://https://chmln.github.io/flatpickr/examples/#flatpickr-external-elements	0%	Avira URL Cloud	safe	
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.nathanaeljones.com/blog/2013/reading-max-width-cross-browser	0%	Avira URL Cloud	safe	
http://https://www.anujgakhar.com/2014/03/01/binary-search-in-javascript/	0%	Avira URL Cloud	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	104.17.242.204	true	false		high
s3.amazonaws.com	52.216.88.141	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
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
52.216.88.141	s3.amazonaws.com	United States		16509	AMAZON-02US	false
104.17.242.204	cdn2.hubspot.net	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:	431202
Start date:	08.06.2021
Start time:	15:15:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 49s
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:	13
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@3/28@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\DNTVAT8O\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):	26
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aK1r0aKb:JFK1rFKb
MD5:	132294CA22370B52822C17DCB5BE3AF6
SHA1:	DD26B82638AD38AD471F7621A9EB79FED448A71C
SHA-256:	451ABBE0AEFC000F49967DABF8D42344D146429F03C8C8D4AE5E33FF9963CF77
SHA-512:	6D5808CAD199A785C82763C68F0AE1F4938C304B46B70529EA26B3D300EF9430AD496C688D95D01588576B3A577001D62245D98137FD5CD825AD62E17D36F15C
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{1BEF76F7-C8A7-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8604726868512316
Encrypted:	false
SSDEEP:	48:IwuGcprXjGwpLThG/ap8oGIpct7bWGvnZpvt7UGoHqp9t7wGo4FpmtK+GWRn9thw:ryZX9ZJ2IWtDttHftHFMtRtftrft5cX
MD5:	4B8E727B034DED882A2E1FF805C7D8DD
SHA1:	B46C78A1FC9773B7E080BC88C49CE1E476CFE0C7
SHA-256:	98A06AE0D94C08A4F1D7558AA33D83754760F446D43E959C821915B6FBF92C64
SHA-512:	97F95B8084B32E8743462EEBAB18F69DCB208B3D33FCC9C2E7B7520BDE487BBF55CBD235A500010577D989A4C49833F47A7CB5DE43BA69B5BC07BD5247341BC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{1BEF76F7-C8A7-11EB-90E4-ECF4BB862DED}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1BEF76F9-C8A7-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	37278
Entropy (8bit):	2.565041504864698
Encrypted:	false
SSDEEP:	192:rJZu9QC6AkAjl2VWrMD8c06hQmPj06jR06T063r06106D06l06K06HKg:r/uCtNCcsYwc8mPjH9FrHxHoRN
MD5:	AAB70BC27375039AB0983CDA3C690392
SHA1:	7D4348FEFF6DA0AEA8C5E88AFD870F99DC89D281
SHA-256:	1E2ED73139CC5EA42331A6593C5FB5320DAF05EF65E1D6F9F88317675DC858B5
SHA-512:	B116FEEA051402917290D6C06798CDCDE316065CD1BBEEF341006C77AF83D32FAB7698DD3BD947205F3ED0D0DAA423439E4759074FFA9D1D2592E7A7CEC5A0 5
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\{23ACB7E6-C8A7-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5642020207394023
Encrypted:	false
SSDEEP:	48:IwZGcprYjGwpalG4pQ5GrapbSpGQpK7G7HpRLTGIpG:r/ZY9Q36ZBSjA6ThA
MD5:	094CC6C276C1742A6028DCFE83B061AB
SHA1:	9D7E8D3EE6BA5AB47887252D2E11CB2A10720375
SHA-256:	5088EF53C8BEECCD7141B4BDF2E8F3A096D494595025D700BCB56DDED3B28A44
SHA-512:	D2D5A17A74B621C915001E597FF91125F50CCCA78BBF3A2136B21C6C7565803E57651D509A287F2C7FA89FDD190D7C1C48C9919FE842EF491538791419A1FBA7
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):	5.0666373075347355
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEBQ0nWimI002EtM3MHdNMNxOEBqV9nWimI00ObVbkEtMb:2d6NxOaQ0SZHKd6NxOaiSZ76b
MD5:	4FE1FC58F23CD253D8FF5A19CF1084B2
SHA1:	B1A599F75C8A648ABB08A6628E447EB63250F741
SHA-256:	D042165B69F135631F7831816D55D872048A142ECB1311C8AF22D005DF45523D
SHA-512:	4E27E0EE08F05FD34F7B18941E44A048289ADA04B99BAF31866C286DAD4764870610865FF30E2FD550500EC1AC11BB7033979B0009BF844B497B0034FA3FF441
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xf4ada3c0,0x01d75cb3</date>< accdate>0xf4ada3c0,0x01d75cb3</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>0xf4ada3c0,0x01d75cb3</date><accdate>0 xf4b72d3c,0x01d75cb3</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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.071032646743542
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kBQ0nWimI002EtM3MHdNMNxe2kBQ0nWimI00Obkak6EtMb:2d6Nxr6Q0SZHKd6Nxr6Q0SZ7Aa7b
MD5:	9BEE7E96DE811B3C4B133A3B80AD4496
SHA1:	282C77920950555AAE0945609F1F7E17EA021795
SHA-256:	26E21A93FB7F091EA3E33FC1A8199B367ECD1AB527534DF9DE17EC679EBA5891
SHA-512:	326C619EC102CDFEFCAACEDD16E90E7494235A8CA7156EE966DF2FF35387E964DD094F38651603820530B7744D0AF2AACB9FB10C812066CB277FE5B5D617D6 E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xf4ada3c0,0x01d75cb3</date><a ccdate>0xf4ada3c0,0x01d75cb3</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>0xf4ada3c0,0x01d75cb3</date><accdate>0xf 4ada3c0,0x01d75cb3</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):	5.115478915032624
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLrVJV9nWimI002EtM3MHdNMNxvLrVJV9nWimI00ObmZEtMb:2d6NxvXSZHKd6NxvXSZ7mb
MD5:	7EBD26A93E47E7BF75EEDF417184D109
SHA1:	C1C8CD1DEA0B359BA02CFEC9D74CA514807EA57E
SHA-256:	1274E400A4B2A995551E12B2B2697A61A3BF982CDAAF5DF2C8D81B78759B89F6
SHA-512:	9BCF5673E6A69D1B7FC1CF411E19EFC60C9BFF97791CAADCE55FD13A93E079D3DE65428F2B819BF19DD4E7C5DD5A0DB53949DBF22EE3281E62993716A8BC5 3B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xf4b72d3c,0x01d75cb3</date> <accdate>0xf4b72d3c,0x01d75cb3</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>0xf4b72d3c,0x01d75cb3</date><accda te>0xf4b72d3c,0x01d75cb3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipe dia.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):	5.066050376733735
Encrypted:	false
SSDEEP:	12:TMHdNMNxiBQ0nWimI002EtM3MHdNMNxiBQ0nWimI00Obd5EtMb:2d6NxAQ0SZHKd6NxAQ0SZ7Jjb
MD5:	275E15C0A486DA583D99797DAC78B497
SHA1:	50A7D5651F361A080AC715410599DE4DA4A4CB80
SHA-256:	5CCDEEA47FD75B6294CF9F1F82AF22D5BA41AE8059421E19FBF3757B8FB3CB7D
SHA-512:	B58F83A111809A80CCA2DA14B5EA2C2B43F9FD5078D5ADC4ED89E92BA77AF767FC2DFB4953BFD4744FAFE62A3C44BE5FF6EAF93D1160BB8B7C348587AA8BA 0EE
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xf4ada3c0,0x01d75cb3</date><acc date>0xf4ada3c0,0x01d75cb3</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>0xf4ada3c0,0x01d75cb3</date><accdate>0xf4ada 3c0,0x01d75cb3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Entropy (8bit):	5.1255465699733
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwrVJV9nWimI002EtM3MHdNMNxhGwrVJV9nWimI00Ob8K075EtMb:2d6NxQeSZHKd6NxQeSZ7YKajb
MD5:	5E953CD9CDCF1E69A4022F19FE2F66CC
SHA1:	23F4642613FDBB4812D3E2F1237B5DEA1944C090
SHA-256:	AE0577A63A93CB0E2F97FEDA6A15B1A5122E194871150245A916A8D1B00C785E
SHA-512:	50D06E3F36F17F0D44CA353C3706AD09145B927D8C193DAE0D82468736D2215E95E303FCB0FCDE4403B7ED45DBAE535694C25788FD93DE52F7B6461EA62E6F9
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xf4b72d3c,0x01d75cb3</date><accdate>0xf4b72d3c,0x01d75cb3</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>0xf4b72d3c,0x01d75cb3</date><accdate>0xf4b72d3c,0x01d75cb3</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):	5.051434655959557
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nBQ0nWimI002EtM3MHdNMNx0nBQ0nWimI00ObxEtMb:2d6Nx0BQ0SZHKd6Nx0BQ0SZ7nb
MD5:	E857EB182C16DE328BEFF3DCAF8DB4A3
SHA1:	A05C2DCDE275F4DDC7DFD1BA12340F48862BE953
SHA-256:	30F749915D4B1F555F874E6012DEA2F7C36575931802D9D34ADDEB25C2F275A1
SHA-512:	61DCA551C03F6FCC3324465D47960958D89E04A824BCF01EF8EA2E720FA56A0EA3A4AC224D6301C0F915F19D58642A562A0DC44E6AC600D888080612D11B4CF
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xf4ada3c0,0x01d75cb3</date><accdate>0xf4ada3c0,0x01d75cb3</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>0xf4ada3c0,0x01d75cb3</date><accdate>0xf4ada3c0,0x01d75cb3</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\pin202591677780\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):	5.091319364540433
Encrypted:	false
SSDEEP:	12:TMHdNMNxxBQ0nWimI002EtM3MHdNMNxxBQ0nWimI00Ob6Kq5EtMb:2d6NxDQ0SZHKd6NxDQ0SZ7ob
MD5:	25B3BA7147256064794F2674577822BC
SHA1:	372545A6B1CE30205C718EBE653E592D61C63725
SHA-256:	621E04B3D56EA36132DE78935B6C8239AC6A0E2C469D488D04E217CEB3CF569D
SHA-512:	D5FED61DDCD993AC61E13922B3DFE72E7DE2D30BBEBA7AA50377373F8D4229C6E9B54B46250347A29C402EC6C431F5A3ED764774C4235FAC98E68DDFF47CF37
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xf4ada3c0,0x01d75cb3</date><accdate>0xf4ada3c0,0x01d75cb3</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>0xf4ada3c0,0x01d75cb3</date><accdate>0xf4ada3c0,0x01d75cb3</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):	5.064562415132592
Encrypted:	false
SSDEEP:	12:TMHdNMNxcBQ0nWimI002EtM3MHdNMNxcBQ0nWimI00ObVEtMb:2d6NxyQ0SZHKd6NxyQ0SZ7Db
MD5:	483351B8DCBB7CC81F3DC30128590F48
SHA1:	634DD82A05860F82389B59CD47316050002FAD32

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
SHA-256:	FA8DEA79CF52BE219B88DCC72FDE9A1A9CF04B6F28E4E7651B72111ABD24F460
SHA-512:	1E3988D20333DA52054DA9D92E807F77FE9D4E4055123F5B75064B5D2D7D9782617E50485176C3ED6D1EBF85ACC609B15E5644D156834318D29F557C77B89BE5
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xf4ada3c0,0x01d75cb3</date><accdate>0xf4ada3c0,0x01d75cb3</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>0xf4ada3c0,0x01d75cb3</date><accdate>0xf4ada3c0,0x01d75cb3</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):	5.052128092659896
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnBQ0nWiml002EtM3MHdNMNxfnBQ0nWiml00Obe5EtMb:2d6NxZQ0SZHKd6NxZQ0SZ7ijb
MD5:	952E66772BFE9848BF841897D7CEA4F7
SHA1:	0545075FD127E97E427C91CF02F9694B6370F4F1
SHA-256:	E6ABFDA804EA2E41F733E371E47A2085A3BB5C646B94926AD1EA9ADBF9BBDCCB
SHA-512:	5626C165D6646DD500008E2A1499AE58AFD8E37F8B1287EB34C17155E33331F8701A0DA3B47C8FAE00197314AA26569AC6E9D0DF3DCE457CEBABE339ECAAA3B6
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xf4ada3c0,0x01d75cb3</date><accdate>0xf4ada3c0,0x01d75cb3</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>0xf4ada3c0,0x01d75cb3</date><accdate>0xf4ada3c0,0x01d75cb3</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\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 TypeError('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\0W10PBUV\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\landing-watermark-8487e36eef1bec74f06631f19fea0aa171c208e2976373cda5bd0a4b9e230903[1].css

Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secured-login.net/assets/landing-watermark-8487e36eef1bec74f06631f19fea0aa171c208e2976373cda5bd0a4b9e230903.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\0W10PBUV\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:	D4DB54380D135D9F5AAA03727CC88037B014C1057A3061C3D173EB8D4CEC7E4A2F71CFCA1478E8E15C093D510EEE80668C2038691EAEB21958942089F0DD9C
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\0W10PBUV\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\MEEXW4H4\N7K4C4D4.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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\N7K4C4D4.htm	
SHA1:	2403422DCDFF53DF424128AC6343E62B55A630D6
SHA-256:	8EDB5724DF71F88143E0C457940935AA88F8D476723628EECAECA377C3F7DB6F
SHA-512:	8B8412DC2A29EF1B3C2E46C5F0BF8737E6EAADE382E950E33E54A5A21E0E88C6E0661A1969A9532E3C0B46A3E7929145F70949B00779C7C910BBB37E9C55AF5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secured-login.net/pages/c3955b1c48a/XWkZKNVRYQmFTVmxrVkRoek9VTkdXRzVHWjNBM2RtMDBRMlptZVRkdGNFUjFZekV6ZWxkblJEZzFiMlZCTWxoTlVXaG5aMHRoYW1kc09VSnlja2xZYkc5MlYwdzNOWFpsVERWNUsxWXZiVkJ5YURreFUzTk9kbGt4ZWtoSGRYa3dTM1ppY1hkT0x6Y3pSMFJXVjNsMWRXNVRiRnBCZURZMGJVWkNlRlJ0TVdGM1REZEhNRnA0ZW5keksyTmFZV2hPWVRGd1Z6Tm9iRFVyVlhnd1UwdHhOVkU0YTJsRGRXMDBjMlZOUFMwdGVsSnhlVlJOWkZKRlNlVjZZbEpUYkVscGJUQTJaejA5LS0yNjI0MmEyNmU5MTE4NzY5Nzk4YzQ5Nzk4MGQyMGYxNmNiYmE1MGQy
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\MEEXW4H4\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/a1fIuiHlq5mN8lDbNmPbh
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\Microsoft\Windows\INetCache\IE\MEEXW4H4\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
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\PSUEOSZZ\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

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\KB4-logo[1].png</th></tr>
<tr><td>SSDEEP:</td><td>96:YRObJZQcSGBG0v6UBnFSai6Xk2kQ6779zVD0nCXYTu4qWeG0a6lS+adxQVwZ5kkt:iO5SGBRBAkelpXY69We5IhdxQVwfkkt</td></tr>
<tr><td>MD5:</td><td>20F88CB052864EF047CBF095E46A23B0</td></tr>
<tr><td>SHA1:</td><td>5068F0745178BC0C042B6302ED114516981141BD</td></tr>
<tr><td>SHA-256:</td><td>65149B7AFD0CCFDEA4CB383944A47825F33B1A80B092ECA6F74CB01F0C186809</td></tr>
<tr><td>SHA-512:</td><td>57E78802933898C66F8E2245357883705E732F0686697601C0F3C2C96B9D345BE131DCD4C0118C657C2A55BC397044DBD06456AB68172C3867C4D055B6EC11EF</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://cdn2.hubspot.net/hubfs/241394/html_file/files/img/KB4-logo.png</td></tr>
<tr><td>Preview:</td><td>.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~ ..l..[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...@....ol^....v..36..r.q^.'..t.:@..;.O9 H.o......+..g.cyy..38.{...........D\.v.d.@.....R..g...?z)..4..!....(V</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\QRF01zv[1].png</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>PNG image data, 60 x 60, 8-bit/color RGBA, non-interlaced</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>1666</td></tr>
<tr><td>Entropy (8bit):</td><td>7.843362903299294</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>48:1E3hTvNbvJkGGv0nnr5I2rk5boP0gD6EaTMN:1ERb+cr5Z1P0gD6/a</td></tr>
<tr><td>MD5:</td><td>29D583007FCD677AA31CA849478BC17A</td></tr>
<tr><td>SHA1:</td><td>F354E323218A450060852C344927C3E79D8E7B66</td></tr>
<tr><td>SHA-256:</td><td>120EE096F38C1E21083054C15F0F8CFBB02B6740A01D98068E3BE9581E83D453</td></tr>
<tr><td>SHA-512:</td><td>4AFC2641D96D1C372D091FD795D39C1AF12149B5EB30DA7BEE6FBFEA0650841067B7D259473BF65706CDD42D1EDF1CC5673B5F5556D1E91F8AE32976490A7E4
D</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://i.imgur.com/QRF01zv.png</td></tr>
<tr><td>Preview:</td><td>.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......;.$...i.wC.ICO.n.h....AJ.N.+.T).........)9..y..?.hs%.".B..k....#.S.....:..!o..Z...|.w2....a..+y.e;..A...x.p+2G/!..1..jTr.S...S.....D.<.G.z.+2..E..>.Z6L.......e.2..R
..3...~..%.C.!..f..s.'.;.M...5..k.1..L._B.vA_|.c{......{....*...d...Y.'Q.TS:.7.......|...,.:..-...#.V.*NA..&...iO.....SEE.kW!.y.p.y.m..6b..@=.,.n..i,....q..W...w.f..bg.`|......3.:.K.<..I.[....a..}..%_
....{...~..j...)......n}m[...u...._....{....,.t.[..g.....&.v.j..2.r5.r5.B..jp..v-.j./.....c.s..$q@..z...oo..g?.z...%..gW.......}.6h....U....o.u.])]..@B);.o.V</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\PGAYGPRO.htm</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>HTML document, ASCII text, with very long lines</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>556</td></tr>
<tr><td>Entropy (8bit):</td><td>5.751255253864889</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>12:3R+xnAp6Q/rPAg1tWhLJ+q3GemyuqLJ9YlWt/4AEdeIQL:3Eo6QT4eMh9+Mb7VqW5NEkj</td></tr>
<tr><td>MD5:</td><td>E29F472F8FDABCC42F4A714319354832</td></tr>
<tr><td>SHA1:</td><td>D380CD566FDE466D955AAC77C9DAB011FA43962B</td></tr>
<tr><td>SHA-256:</td><td>092879E02BB81B6B636A80A9D521FEC8A0555965886D3461E40BE1A26D24660B</td></tr>
<tr><td>SHA-512:</td><td>DB6C482DA17C86D9268B12873668757BD56F47505CC6B281D44216D54B2C309B761DAE1D20E27D8039EA9DEEE50DA068B63EE47E2FF45B063DB28A5A28A2C1
1</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://covid19.protected-
forms.com/XWkZKNVRYQmFTVmxrVkRoek9VTkdXRzVHWjNBM2RtMDBRMlptZVRkdGNFUjFZekV6ZWxkblJEZzFiMlZCTWxoTlVXaG5aMHRoYW1kc09VSnlja2xZYkc5
MlYwdzNOWFpsVERWNUsxWXZiVkJ5YURreFUzTk9kbGt4ZWtoSGRYa3dTM1ppY1hkT0x6Y3pSMFJXVjNsMWRXNVRiRnBCZURZMGJVWkNlRlJ0TVdGM1REZEhNR
nA0ZW5keksyTmFZV2hPWVRGd1Z6Tm9iRFVyVlhnd1UwdHhOVkU0YTJsRGRXMDBjMlZOUFMwdGVsSnhlVlJOWkZKRlNIVjZZbEpUYkVscGJUQTJaejA5LS0yNjI0Mm
EyNmU5MTE4NzY5Nzk4YzQ5Nzk4MGQyMGYxNmNiYmE1MGQy?cid=874637403</td></tr>
<tr><td>Preview:</td><td><html>. <head>.   <script>window.location.href = 'https://secured-login.net/pages/c3955b1c48a/XWkZKNVRYQmFTVmxrVkRoek9VTkdXRzVHWjNBM2RtM
DBRMlptZVRkdGNFUjFZekV6ZWxkblJEZzFiMlZCTWxoTlVXaG5aMHRoYW1kc09VSnlja2xZYkc5MlYwdzNOWFpsVERWNUsxWXZiVkJ5YURreFUzTk9kbGt4Z
WtoSGRYa3dTM1ppY1hkT0x6Y3pSMFJXVjNsMWRXNVRiRnBCZURZMGJVWkNlRlJ0TVdGM1REZEhNRnA0ZW5keksyTmFZV2hPWVRGd1Z6Tm9iRFVyVlhnd1Uwd
HhOVkU0YTJsRGRXMDBjMlZOUFMwdGVsSnhlVlJOWkZKRlNIVjZZbEpUYkVscGJUQTJaejA5LS0yNjI0MmEyNmU5MTE4NzY5Nzk4YzQ5Nzk4MGQyMGYxNmNiY
mE1MGQy';</script>. </head>. <body>. </body>.</html>.</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\dd[1].css</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>UTF-8 Unicode text, with CRLF line terminators</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>4524</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\dd[1].css	
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; cursor: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\WJ8I2OL4\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
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\Temp\~DF8AF1BA4D4EA076FE.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4837867861775243
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9losF9loM9lWNzDz+qWq:kBqoIHhNzDz+2
MD5:	9D6E0BBB0C5E099357D6BFD216B16786
SHA1:	751DBA195A2FCC517177E6F6D78C1496AE8F8EB9
SHA-256:	4C7BD8E1D53D0DC11C81EF08AEB94F1BFA9A5A870BFFA6DB6188BA90039C05E7
SHA-512:	A6795A63A758E675E20135E14A0C6A58FCC7401A0E872793F1B77DACC24B896DC517C7157F3B344ECB000CF78724C4FF49675CCECE8223CD7CDC6F99A8ACF9C
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF8C6F444256A1F16A.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.7402921304129136

C:\Users\user\AppData\Local\Temp\~DF8C6F444256A1F16A.TMP	
Encrypted:	false
SSDEEP:	48:kBqoxxJhHWSVSEabKn0Tqzd9ZN+N8/V/G6LiEgdCvJMBmYIjDBgdEJdOcfdoddLj:kBqoxDhHWSVSE+8lN+N8/VeMvrzE7T
MD5:	F330EC49875C490BFB38FCDD3B00A562
SHA1:	446BB8CF8A49DDBD79040BE763D36EEF40C4E458
SHA-256:	C0C2134B09D8A66960D65C75DED3944A522BF474F73C5AE4DEF307B10216BF2D
SHA-512:	D191C0600CBAA928F35FB035F3EED88363D16EA3E2943EE0B2F42E0A99898BE8D2158737964CD6D494879053B769E4ED0DC991DD7B736526EC30CFA79955A85
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFF6FF6DAE3469FA3D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	46768
Entropy (8bit):	1.252252212779373
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+lLpY7jc06Qme06y06T063r06106D06l06K06H:kBqoxKAuqR+lLpY7jc2me09FrHxHoR
MD5:	CD4FBF9B9F21BC8E55B470496038D806
SHA1:	EF3F53868847C835F665F13E2ED010C429904768
SHA-256:	4C76D2A0FD090A0861EE23571810CC93185DC35178D355111E5D63E5EB125F25
SHA-512:	211A2185B28F529A7F977439A466F5011BD09EC3CFD6E611579BCF19F242AAD34FB6A7D1098B65699C58C4241B017BD97875CE6BAA09B1A815AE253B4DDA45B
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 15:16:04.710412979 CEST	192.168.2.3	8.8.8.8	0x7e18	Standard query (0)	covid19.protected-forms.com	A (IP address)	IN (0x0001)
Jun 8, 2021 15:16:05.867662907 CEST	192.168.2.3	8.8.8.8	0x6d6f	Standard query (0)	secured-login.net	A (IP address)	IN (0x0001)
Jun 8, 2021 15:16:07.156884909 CEST	192.168.2.3	8.8.8.8	0x1776	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jun 8, 2021 15:16:07.194660902 CEST	192.168.2.3	8.8.8.8	0x3e93	Standard query (0)	s3.amazonaws.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 8, 2021 15:16:08.369627953 CEST	192.168.2.3	8.8.8.8	0x62ad	Standard query (0)	cdn2.hubspot.net	A (IP address)	IN (0x0001)
Jun 8, 2021 15:16:08.521433115 CEST	192.168.2.3	8.8.8.8	0x4ec1	Standard query (0)	i.imgur.com	A (IP address)	IN (0x0001)
Jun 8, 2021 15:16:22.337836981 CEST	192.168.2.3	8.8.8.8	0xc8c6	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 15:16:04.761859894 CEST	8.8.8.8	192.168.2.3	0x7e18	No error (0)	covid19.protected-forms.com	landing.training.knowbe4.com		CNAME (Canonical name)	IN (0x0001)
Jun 8, 2021 15:16:04.761859894 CEST	8.8.8.8	192.168.2.3	0x7e18	No error (0)	landing.training.knowbe4.com		34.226.85.79	A (IP address)	IN (0x0001)
Jun 8, 2021 15:16:04.761859894 CEST	8.8.8.8	192.168.2.3	0x7e18	No error (0)	landing.training.knowbe4.com		18.233.2.161	A (IP address)	IN (0x0001)
Jun 8, 2021 15:16:05.919404984 CEST	8.8.8.8	192.168.2.3	0x6d6f	No error (0)	secured-login.net		34.226.85.79	A (IP address)	IN (0x0001)
Jun 8, 2021 15:16:05.919404984 CEST	8.8.8.8	192.168.2.3	0x6d6f	No error (0)	secured-login.net		18.233.2.161	A (IP address)	IN (0x0001)
Jun 8, 2021 15:16:07.199359894 CEST	8.8.8.8	192.168.2.3	0x1776	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jun 8, 2021 15:16:07.199359894 CEST	8.8.8.8	192.168.2.3	0x1776	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jun 8, 2021 15:16:07.237591028 CEST	8.8.8.8	192.168.2.3	0x3e93	No error (0)	s3.amazonaws.com		52.216.88.141	A (IP address)	IN (0x0001)
Jun 8, 2021 15:16:08.417982101 CEST	8.8.8.8	192.168.2.3	0x62ad	No error (0)	cdn2.hubspot.net		104.17.242.204	A (IP address)	IN (0x0001)
Jun 8, 2021 15:16:08.417982101 CEST	8.8.8.8	192.168.2.3	0x62ad	No error (0)	cdn2.hubspot.net		104.17.240.204	A (IP address)	IN (0x0001)
Jun 8, 2021 15:16:08.417982101 CEST	8.8.8.8	192.168.2.3	0x62ad	No error (0)	cdn2.hubspot.net		104.17.241.204	A (IP address)	IN (0x0001)
Jun 8, 2021 15:16:08.417982101 CEST	8.8.8.8	192.168.2.3	0x62ad	No error (0)	cdn2.hubspot.net		104.17.243.204	A (IP address)	IN (0x0001)
Jun 8, 2021 15:16:08.417982101 CEST	8.8.8.8	192.168.2.3	0x62ad	No error (0)	cdn2.hubspot.net		104.17.244.204	A (IP address)	IN (0x0001)
Jun 8, 2021 15:16:08.564176083 CEST	8.8.8.8	192.168.2.3	0x4ec1	No error (0)	i.imgur.com	ipv4.imgur.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jun 8, 2021 15:16:08.564176083 CEST	8.8.8.8	192.168.2.3	0x4ec1	No error (0)	ipv4.imgur.map.fastly.net		151.101.112.193	A (IP address)	IN (0x0001)
Jun 8, 2021 15:16:22.380919933 CEST	8.8.8.8	192.168.2.3	0xc8c6	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

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 15:16:05.042069912 CEST	34.226.85.79	443	192.168.2.3	49716	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 15:16:05.046890020 CEST	34.226.85.79	443	192.168.2.3	49715	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 15:16:06.198681116 CEST	34.226.85.79	443	192.168.2.3	49718	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 15:16:06.206151962 CEST	34.226.85.79	443	192.168.2.3	49719	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 15:16:07.311980963 CEST	104.16.18.94	443	192.168.2.3	49722	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 15:16:07.312531948 CEST	104.16.18.94	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	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 15:16:08.347281933 CEST	52.216.88.141	443	192.168.2.3	49726	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 15:16:08.436007977 CEST	52.216.88.141	443	192.168.2.3	49727	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 15:16:08.529680967 CEST	104.17.242.204	443	192.168.2.3	49728	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		

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 15:16:08.529840946 CEST	104.17.242.204	443	192.168.2.3	49729	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 15:16:08.755610943 CEST	151.101.112.193	443	192.168.2.3	49731	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 15:16:08.755628109 CEST	151.101.112.193	443	192.168.2.3	49730	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		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5948 Parent PID: 792

General

Start time:	15:16:02
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:	0x7ff688160000
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: 4768 Parent PID: 5948

General

Start time:	15:16:03
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:5948 CREDAT:17410 /prefetch:2
Imagebase:	0x11c0000
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